Relativity aiR

Admin Guide

October 7, 2026

For the most recent version of this document, visit our **documentation website**.

Table of Contents

1 Admin guide overview **30**

1.1 Navigation 30

1.1.1 Logging in 30

1.1.2 Tab navigation 31

1.1.3 All tabs menu 33

1.1.4 Tab strip 34

1.1.5 User options 36

1.1.6 Permissions 40

1.1.7 Creating a dashboard 40

1.1.8 Adding widgets to a dashboard 41

1.1.9 Saving changes to a dashboard 41

1.1.10 Deleting a dashboard 41

1.1.11 Renaming a dashboard 41

1.1.12 Resetting your password 42

1.1.13 Favorites 43

1.1.14 Quick nav 43

1.2 Logging into Relativity aiR 44

1.2.1 Logging in to Relativity aiR with a password 45

1.2.2 Password 45

1.2.3 Two-factor authentication 45

1.2.4 OpenID Connect 48

1.2.5 SAML 2.0 49

1.2.6 Creating or resetting a password 49

2 Relativity applications **50**

2.1 Permissions 50

2.2 System secured applications 51

2.2.1 Applications installed in the Application Library 51

2.2.2 Applications installed in workspaces 52

2.3 Relativity custom applications 52

2.4 Administering Relativity applications 52

2.4.1 Auditing Relativity applications 53

2.5 Global applications 53

2.5.1 Viewing global applications ... 53
2.6 Exporting applications ... 54
2.6.1 Downloading application .rap files ... 55
2.6.2 Avoiding errors during application export ... 55
2.6.3 Application state settings on export ... 57
2.6.4 Exporting an application ... 57
2.7 Locking and unlocking applications ... 58
2.7.1 Locking an application ... 58
2.7.2 Customizing locked applications ... 59
2.7.3 Modifying saved searches in a locked application ... 60
2.7.4 Unlocking an application ... 60
2.8 Installing applications ... 60
2.8.1 Installing applications to the Application Library ... 61
2.8.2 Pushing an application from the Application Library to a workspace ... 61
2.8.3 Installing applications to workspaces ... 62
2.9 Troubleshooting application installation errors ... 67
2.9.1 Installation error list ... 67
2.9.2 Resolving installation errors ... 68
2.9.3 Pre and Post Install event handler errors ... 69
2.9.4 Checking the error statuses ... 69
2.10 Uninstalling and deleting applications ... 69
2.10.1 Uninstalling applications ... 69
2.10.2 Deleting applications ... 71
2.11 Upgrading applications ... 72
2.11.1 Upgrading an application ... 72
2.11.2 Troubleshooting application upgrades ... 74
3 Audit ... 74
3.1 Key benefits ... 74
3.2 Permissions ... 74
3.3 Supported Audit tab functionality ... 75
3.3.1 Audit agents ... 75
3.4 Audit tab ... 76
3.4.1 Advanced Filtering Audit records ... 77
3.4.2 Details column ... 78

3.4.3 Exporting workspace audits ... 80
3.5 Instance audits ... 81
3.5.1 Filtering on multi-workspace audits ... 82
3.5.2 Reverting audited actions ... 82
3.6 Audit Migration Reports tab ... 83
3.6.1 Migration Error Report ... 83
3.6.2 Migration Error Retry Script ... 85
3.6.3 Migration Status Report ... 85
3.7 Audit Workspace Settings tab ... 86
3.7.1 HistoryTabVisibleOnUpgrade ... 86
3.8 Audited actions ... 87
4 Authentication ... 89
4.1 Choosing your authentication setup ... 89
4.2 Permissions ... 90
4.3 Authentication overview ... 90
4.3.1 Authentication methods ... 90
4.3.2 Authentication object model ... 91
4.3.3 Authentication object permissions ... 92
4.4 Configuring authentication providers ... 92
4.4.1 Creating authentication providers ... 92
4.4.2 Assigning a login method to individual users ... 93
4.4.3 Enabling Relativity aiR Connect ... 93
4.5 Authentication provider settings ... 93
4.6 Centralized Authentication ... 94
4.6.1 Prerequisites ... 94
4.6.2 Centralized Authentication workflow ... 94
4.6.3 Setting up your Authentication Provider ... 94
4.6.4 Password Provider setup ... 95
4.6.5 Inviting users ... 99
4.6.6 Managing user transition ... 100
4.6.7 User accepts the invitation ... 101
4.6.8 Existing Relativity aiR users ... 104
4.6.9 Logging in to Relativity aiR ... 105
4.7 SSO setup ... 108

4.7.1 Supported identity providers ... 108
4.7.2 Prerequisites ... 109
4.7.3 Registration workflow ... 109
4.7.4 SSO setup wizard ... 109
4.7.5 Considerations ... 111
4.7.6 Related topics ... 111
4.7.7 Okta (Org2Org) ... 111
4.7.8 Microsoft Entra ID ... 115
4.7.9 Google Workspace ... 117
4.7.10 Custom SAML 2.0 ... 119
4.7.11 Custom OpenID Connect ... 121
4.8 Managing user authentication methods ... 123
4.8.1 Invitation workflow ... 123
4.8.2 Manually setting passwords ... 127
4.8.3 OpenID Connect ... 127
4.8.4 SAML 2.0 ... 128
4.9 Microsoft Entra ID - OpenID Connect ... 128
4.9.1 Registering an Azure application and credentials ... 128
4.9.2 Configuring Entra ID OpenID Connect ... 129
4.10 SAML 2.0 provider ... 130
4.10.1 Considerations ... 131
4.10.2 Configuring a SAML 2.0 authentication provider ... 131
4.10.3 Configuring specific SAML providers ... 131
4.11 OpenID Connect ... 137
4.11.1 Configuring an OpenID Connect authentication provider ... 137
4.11.2 OpenID Connect authentication provider flows ... 139
4.11.3 Just-in-time provisioning ... 139
4.11.4 Okta OpenID Connect ... 141
4.11.5 Relativity OpenID Connect ... 142
4.12 OAuth2 clients ... 144
4.12.1 Permissions ... 145
4.12.2 Creating or editing an OAuth2 client ... 145
4.12.3 Resetting a client secret ... 147
4.12.4 Deleting an OAuth2 client ... 148

Viewing an OAuth2 client audit history ... 148
4.13 Authentication providers ... 148
4.13.1 Supported authentication providers ... 148
4.13.2 Assigning login methods ... 149
4.13.3 Related topics ... 149
4.14 Relativity aiR Connect ... 149
4.14.1 Enabling Relativity aiR Connect ... 149
4.14.2 Connecting users to different instances ... 151
4.14.3 Navigating between instances ... 152
4.14.4 Updating Relativity aiR Connect after a URL change ... 152
4.14.5 Billing information ... 152
4.14.6 Frequently asked questions ... 153
4.15 SSO Troubleshooting console ... 153
4.15.1 Considerations ... 153
4.15.2 Viewing the SSO Troubleshooting console ... 153
4.16 Federated instances ... 154
4.16.1 Creating or editing a federated instance ... 154
4.16.2 Deleting a federated instance ... 155
Updating a federated instance after an instance URL change ... 156
Viewing a federated instance audit history ... 156
5 Batches ... 156
5.1 Batch fields in Relativity ... 157
5.2 Creating and editing batch sets ... 157
5.2.1 Batch Sets for Reviewers ... 158
5.2.2 Fields ... 158
5.2.3 Batch Set console ... 159
5.2.4 Auto Batching Status ... 160
5.3 Deleting an individual batch ... 160
5.4 Deleting a batch set ... 160
5.5 Searching for documents not in existing batch sets ... 161
5.6 Batching process overview ... 161
5.6.1 No Batch Unit Field or Family Field configured ... 161
5.6.2 Batch Unit Field configured; No Family Field configured ... 162
5.6.3 Batch Unit Field and Family Field configured ... 162

5.6.4 No Batch Unit Field configured; Family Field configured 162
5.6.5 Exceeding the maximum batch size 163
5.7 Assigning batches and checking batches in and out 163
5.7.1 Assign a batch or check a batch out 163
5.7.2 Reassign a batch or check a batch in 164
5.8 Building views for checked-out documents 164
5.8.1 Build a checked-out documents view 164
6 Choices 165
6.1 Accessing the Choice editor 165
6.1.1 Accessing the Choice editor from the Fields tab 165
6.1.2 Accessing the Choice editor from the Choices tab 166
6.1.3 Accessing the Choice editor from layouts 167
6.2 Permissions 168
6.3 Adding choices 170
6.3.1 Adding a choice from the Fields tab 170
6.3.2 Adding a choice from the Choices tab 170
6.3.3 Adding a choice from a layout 171
6.3.4 Adding multiple choices 171
6.4 Editing choices 172
6.4.1 Editing choice names 172
6.4.2 Editing choice details 172
6.5 Choice detail fields 172
6.6 Deleting choices 174
6.7 Performing mass operations on choices 174
6.8 Organizing choices 175
6.8.1 Dragging and dropping choices 175
6.8.2 Alphabetizing choices 176
6.8.3 Reordering top level choices 176
6.9 Fields in workspaces 177
6.10 Admin choices 177
6.10.1 Admin fields 178
7 Clients 178
7.1 Permissions 178
7.2 Creating or editing a client 179

7.2.1 Fields ... 179
7.3 Enabling client domains on a client ... 179
8 Dashboards ... 180
8.1 Permissions ... 182
8.2 Creating a dashboard ... 182
8.3 Adding widgets to a dashboard ... 183
8.4 Saving changes to a dashboard ... 183
8.5 Deleting a dashboard ... 183
8.6 Renaming a dashboard ... 183
8.7 Filtering a dashboard ... 184
8.8 Exporting a dashboard ... 184
8.9 Commonly-used dashboards ... 186
8.9.1 Communicators ... 187
8.9.2 Data Load QC ... 187
8.9.3 Database Stats ... 188
8.9.4 Document Characteristics ... 189
8.9.5 Review Prioritization ... 189
8.9.6 Review Progress/QC ... 190
8.9.7 Privilege Review/QC ... 191
8.9.8 Search Term Review ... 192
8.9.9 Pre-Production QC ... 193
8.9.10 Email Threading ... 194
8.9.11 Language Identification ... 195
8.9.12 Special considerations ... 196
9 Fields ... 196
9.1 Fields permissions ... 196
9.2 System fields ... 197
9.3 Creating and editing fields ... 198
9.4 Fields ... 199
9.4.1 Field information ... 199
9.4.2 Field settings ... 200
9.4.3 Advanced settings ... 202
9.4.4 List and Dashboard Settings ... 208
9.4.5 Choices ... 209

9.5 Field types ... 210
9.5.1 Fixed-length text ... 210
9.5.2 Long text ... 211
9.5.3 Date ... 211
9.5.4 Whole number ... 211
9.5.5 Decimal ... 211
9.5.6 Currency ... 211
9.5.7 Yes/No ... 211
9.5.8 Single choice ... 212
9.5.9 Multiple choice ... 212
9.5.10 User ... 212
9.5.11 File ... 212
9.5.12 Single object ... 213
9.5.13 Multiple object ... 213
9.5.14 Fields and performance ... 213
9.5.15 Linking Fields to Field Categories ... 214
9.6 Applying propagation to documents ... 214
9.6.1 Propagating to documents in multiple groups ... 215
10 Field categories ... 216
10.1 Creating a field category ... 217
10.2 Viewing fields associated with a field category ... 217
10.3 Link a field or fields to a field category ... 218
10.4 Unlink a field or fields from a field category ... 219
11 Filters ... 219
11.1 Showing and hiding filters in the item list ... 219
11.2 Filter types ... 221
11.2.1 Using Boolean filters ... 221
11.2.2 Using numeric filters for numbers ... 222
11.2.3 Using List filters ... 223
11.2.4 Using date filters ... 225
11.2.5 Using multi-list filters ... 227
11.2.6 Using text box filters ... 229
11.2.7 Text box filter search examples ... 230
11.2.8 Using advanced text box filtering ... 231

11.3 Changing item sets per page ... 233
11.4 Saving filters as a search ... 233
12 Groups ... 233
12.1 System groups ... 233
12.2 Creating and editing groups ... 234
12.3 Fields ... 234
12.4 Adding users to groups ... 235
12.5 Adding external users through groups ... 236
12.6 Adding or removing groups from a client domain ... 237
13 Imaging ... 238
13.1 Security permissions for imaging ... 238
13.2 Troubleshooting imaging ... 239
13.3 Image on the fly ... 239
13.4 Mass image ... 239
13.5 Imaging profiles ... 240
13.5.1 Creating and editing an imaging profile ... 240
13.5.2 Fields ... 240
13.5.3 Native file imaging profile validation ... 249
13.5.4 Viewing imaging profile details ... 250
13.6 Imaging sets ... 251
13.6.1 Imaging set workflow ... 252
13.6.2 Creating and editing an imaging set ... 252
13.6.3 Fields ... 252
13.7 Image upload ... 254
13.7.1 Required security permissions ... 254
13.7.2 Uploading an image ... 255
13.7.3 Replacing an image ... 256
13.7.4 Warnings and error messages ... 257
13.7.5 Audits for image upload ... 258
13.8 Application Field Codes ... 259
13.8.1 Application Field Codes in Relativity ... 259
13.8.2 Application Field Code formats ... 261
13.8.3 Creating or editing an Application Field Code ... 261
13.8.4 Fields ... 261

13.8.5 Linking an Application Field Code to a native imaging profile ... 262
13.9 Running an imaging set ... 263
13.9.1 Special considerations ... 263
13.9.2 Unsupported file types ... 263
13.9.3 Imaging Set console ... 264
13.9.4 Imaging profile caching ... 265
13.9.5 Password Bank ... 265
13.10 Monitoring imaging status ... 265
13.11 Imaging errors ... 267
13.11.1 Viewing imaging errors ... 267
13.11.2 Imaging error scenarios ... 270
13.11.3 Error email notification ... 270
13.11.4 Retrying imaging errors ... 270
13.11.5 Password Bank in imaging workflow ... 271
13.12 Imaging Warnings ... 272
13.12.1 Special considerations ... 272
13.12.2 Imaging Warnings tab ... 272
13.12.3 All imaging warnings ... 274
13.12.4 Core Reviewer layouts ... 275
13.12.5 Re-imaging emails with tables ... 276
13.13 QC Review ... 278
13.13.1 Hiding images for QC ... 278
13.13.2 Releasing images ... 279
13.14 Imaging jobs in the Imaging Queue ... 280
13.15 Native imaging - dithering algorithm options ... 282
13.15.1 Dithering algorithm details ... 282
13.16 Imaging native types ... 295
13.16.1 Editing a native type ... 296
13.16.2 Generating a complete list of native types and their respective imaging engines ... 296
13.17 Supported file types for imaging ... 297
13.17.1 Categories ... 297
14 Instance Details tab ... 299
14.1 Security ... 299
14.1.1 Manage Permissions ... 300

14.1.2 Group Permissions Report 300
14.2 Message of the Day 300
15 Keyboard shortcuts 301
15.1 Keyboard shortcuts legend 301
15.2 Special considerations for keyboard shortcuts 303
15.3 Document field type shortcuts 304
15.4 Document choice shortcuts 304
15.5 Creating keyboard shortcuts 305
16 Layouts 305
16.1 Layouts permissions 305
16.2 Creating and editing layouts 306
16.3 Layout Information fields 306
16.3.1 Changing layouts 308
16.4 Using the layout builder 309
16.4.1 Layout Options console 309
16.4.2 Creating and editing a layout group 310
16.4.3 Saving the layout 312
16.5 Adding a choice to a layout 312
16.6 Pop-ups on the layout 312
16.7 Adding and editing an object list 312
16.7.1 Adding and editing an object list 313
16.8 Adding fields and text 314
16.8.1 Layout options 314
16.8.2 Adding fields to a category 316
16.8.3 Removing fields from a category 316
16.8.4 Making a field one or two column 317
16.8.5 Making a field read-only 317
16.8.6 Other fields considerations 317
16.8.7 Field properties 317
16.9 Creating a new category 318
16.9.1 Adding and editing categories 318
16.9.2 Category properties 319
16.10 Copy from Previous 319
16.10.1 Adding the Copy from Previous toolbar 320

16.10.2 Using Copy from Previous ... 321
16.11 Using the rich text editor ... 322
16.11.1 Rich text editor features ... 322
17 Lists ... 326
17.1 Enabling lists on an object ... 326
17.2 Viewing items in a list ... 327
17.2.1 Incorporating a list of documents as a search criterion in a saved search ... 327
17.2.2 Creating a view from a saved list ... 327
18 Relativity Script Library ... 328
18.1 Australian Document ID ... 329
18.1.1 Special considerations ... 329
18.1.2 Downloading the script from the Community ... 330
18.1.3 Installing to the Relativity Script Library ... 330
18.1.4 Installing Australian Document ID application to a workspace ... 330
18.1.5 Running the solution ... 330
18.2 Billing statistics - case rollup ... 331
18.3 Billing statistics - users ... 331
18.4 Choice field stratified sampling ... 331
18.4.1 Special considerations ... 331
18.4.2 Inputs ... 332
18.4.3 Results ... 332
18.5 Copy To Legacy Document Fields ... 332
18.6 Create sample set ... 332
18.7 Forgotten password reset audit ... 332
18.8 Globally administer keyboard shortcuts ... 332
18.8.1 Category ... 333
18.8.2 Special considerations ... 333
18.8.3 Inputs ... 333
18.8.4 Results ... 333
18.9 Propagate sent date to family documents ... 333
18.9.1 Special considerations ... 333
18.9.2 Inputs ... 334
18.9.3 Results ... 334
18.10 Billing statistics - Relativity aiR - case rollup ... 334

18.11 Report sample-based statistics ... 334
18.11.1 Report types ... 334
18.11.2 Inputs ... 335
18.11.3 Results ... 335
18.12 Reviewer statistics ... 336
18.12.1 Inputs ... 336
18.12.2 Results ... 336
18.13 Set duplicate flag field ... 338
18.13.1 Special considerations ... 338
18.13.2 Inputs ... 338
18.13.3 Results ... 339
18.14 Set extracted text size field ... 339
18.15 Set native file size field v4 ... 339
18.15.1 Special considerations ... 339
18.15.2 Inputs ... 340
18.15.3 Results ... 340
18.16 Set production beg/end attach fields ... 340
18.17 Set Relativity folder path field ... 340
18.17.1 Special considerations ... 340
18.17.2 Inputs ... 341
18.17.3 Results ... 341
18.18 Upgrade legacy applications ... 341
18.18.1 Inputs ... 341
18.18.2 Results ... 342
19 Markups ... 342
19.1 Permissions ... 342
19.2 Highlights ... 343
19.2.1 Creating highlights ... 343
19.3 Redactions ... 343
19.3.1 Creating basic redactions ... 343
19.3.2 Creating inverse redactions ... 344
19.3.3 Creating full-page redactions ... 344
19.3.4 Creating mass redactions ... 345
19.4 Editing markups ... 346

19.5 Deleting markups ... 346
19.5.1 Working with overlapping markups ... 346
19.5.2 Working with markups outside of page boundaries ... 347
19.5.3 Editing redaction text with a markup set ... 348
19.5.4 Editing redaction text ... 348
19.5.5 Editing font size in text box redactions ... 349
19.6 Mass deleting markups ... 349
19.7 Controlling markup visibility ... 349
19.8 Viewing markup history ... 350
19.9 Using the Markup Navigation pane ... 350
20 Markup sets ... 350
20.1 Permissions ... 351
20.2 Creating and editing a markup set ... 351
20.3 Fields ... 352
20.4 Copying markup sets ... 352
21 Mass operations ... 353
21.1 List of standard mass operations ... 353
21.2 Mass operations permissions ... 355
21.3 Mass Operation Jobs status ... 356
21.4 Cancel production job ... 357
21.4.1 Security configuration ... 357
21.4.2 Using Cancel Production Job ... 358
21.5 Mass edit ... 358
21.5.1 Working with multi-choice fields on the mass edit form ... 360
21.6 Mass copy ... 361
21.7 Mass move ... 362
21.8 Mass delete ... 362
21.8.1 Mass delete permissions ... 363
21.8.2 Performing a mass delete on other objects ... 364
21.8.3 Enabling or disabling snapshot auditing on delete ... 365
21.9 Mass Operation Jobs status ... 366
21.10 Mass replace ... 367
21.11 Mass image ... 368
21.12 Tally/sum/average ... 369

21.12.1 Considerations ... 369
21.13 Mass export to file ... 371
21.13.1 Considerations ... 371
21.13.2 Using mass export to file ... 371
21.13.3 Fields ... 371
21.14 Move to folder path ... 372
21.14.1 Prerequisites for the move to folder path mass operation ... 372
21.14.2 Running the move to folder path mass operation ... 374
21.15 Mass Save as List ... 376
21.16 Mass PDF ... 377
21.16.1 Considerations ... 377
21.16.2 PDF permissions ... 378
21.16.3 PDF profile ... 378
21.16.4 Creating PDF ... 379
21.16.5 Branding PDF ... 385
21.16.6 Creating PDFs via mass operation ... 387
21.17 PDF Queue ... 391
21.17.1 Permissions ... 392
21.17.2 PDF Queue columns ... 392
21.17.3 Cancel a PDF job ... 393
21.18 Mass convert ... 395
21.18.1 Conversion options ... 395
21.18.2 Limitations ... 395
21.19 Retry Production Job ... 395
21.19.1 Security configuration ... 395
21.19.2 Retrying production jobs ... 396
21.20 Set long text field size ... 396
21.20.1 Before you begin ... 396
21.20.2 Using the mass operation ... 397
21.21 Invite users ... 397
22 Matters ... 398
22.1 Permissions ... 398
22.2 Creating or editing a matter ... 399
22.3 Adding or removing matters from a client domain ... 400

23 Client domains ... **400**
23.1 Client domains software architecture ... 401
23.2 Client domains cloud infrastructure ... 401
23.3 Considerations before enabling client domains ... 402
23.4 Enabling client domains on a client ... 402
23.5 Client domain admins ... 403
23.5.1 Client domain admin considerations ... 403
23.5.2 Default instance permissions ... 406
23.5.3 Assigning a client domain admin ... 407
23.6 Client domain limitations and considerations ... 407
23.7 Adding or removing objects from a client domain ... 410
23.8 Deleting a client domain ... 410
24 OCR ... **411**
24.1 Document characteristics that affect OCR quality ... 411
24.2 Creating and editing an OCR profile ... 412
24.2.1 OCR profile fields ... 412
24.3 Creating and editing an OCR set ... 414
24.3.1 OCR set fields ... 414
24.4 Running an OCR set ... 416
24.5 Viewing OCR text ... 418
24.6 OCR queue ... 419
24.6.1 Permissions ... 419
24.6.2 OCR queue fields ... 420
24.6.3 Change job priority ... 421
24.7 OCR on redacted production documents ... 421
24.7.1 Before you begin ... 421
24.7.2 Running the OCR job ... 421
24.7.3 Exporting a production ... 421
25 Pivot ... **422**
25.1 Pivot profiles ... 422
25.1.1 Creating or editing a pivot profile ... 422
25.2 Running Pivot reports ... 424
25.2.1 Pivot color map ... 424
25.2.2 Adding a Pivot widget ... 425

25.2.3 Pivot options ... 426
25.2.4 Working with Pivot chart results ... 428
25.2.5 Working with Pivot table results ... 431
26 Persistent highlight sets ... 433
26.1 Getting started with persistent highlight sets ... 434
26.1.1 Showing and hiding persistent highlight sets in the Viewer ... 435
26.1.2 Navigating persistent highlight hits in the Viewer ... 437
26.1.3 Recent searches in the Persistent Highlight Sets pane ... 439
26.1.4 Navigating highlighted terms in the Viewer ... 439
26.1.5 Persistent highlight set behavior across Viewers ... 441
26.1.6 Persistent highlight behavior ... 442
26.2 Using multiple persistent highlight sets ... 442
26.3 Performance considerations ... 443
26.3.1 Individual document size ... 443
26.3.2 Number of terms ... 444
26.3.3 Types of operators used ... 444
26.3.4 Local machine ... 444
26.4 Creating persistent highlight sets ... 444
26.4.1 Fields ... 445
26.5 Entering highlight terms ... 445
26.5.1 Color-coding persistent highlights ... 446
26.5.2 Guidelines for adding terms or phrases ... 447
26.6 Using the highlight fields source ... 448
26.6.1 Best practices ... 450
26.7 Creating efficient searches for persistent highlighting ... 451
26.7.1 Using terms search ... 451
26.7.2 Using highlight fields ... 453
27 Printing in Relativity ... 454
27.1 Save as PDF ... 454
27.2 Mass PDF ... 454
28 Production ... 454
28.1 Security permissions to run productions ... 454
28.2 Upgrading production ... 455
28.3 Basic production workflow ... 455

28.4 Production information 455
28.4.1 Production information tab 456
28.5 Production sets 457
28.5.1 Creating and editing a production set 457
28.5.2 Basic Settings 458
28.5.3 Numbering 459
28.5.4 Branding 465
28.5.5 Sorting 467
28.5.6 Post Production 468
28.5.7 Other 470
28.5.8 Viewing production set details 471
28.5.9 Tracking multiple redaction sets 472
28.5.10 Advanced Formatting for Branding 472
28.6 Production data source 479
28.6.1 Adding a production data source 479
28.7 Placeholders 481
28.7.1 Creating an image placeholder 482
28.7.2 Creating a custom placeholder 482
28.7.3 Creating a PDF placeholder 483
28.7.4 Previewing placeholders 484
28.8 Production console 484
28.8.1 Manage Production 485
28.8.2 Run Production 486
28.8.3 Post Production 486
28.8.4 Advanced Options 487
28.8.5 Stage and run a production 487
28.8.6 Stage a production 493
28.8.7 View documents 495
28.8.8 Check for production conflicts 496
28.9 Run a production 497
28.9.1 Checking production status 497
28.10 Production errors 499
28.10.1 Staging errors 499
28.10.2 Validation errors 499

28.10.3 Branding errors ... 500
28.11 Re-production ... 501
28.11.1 Special considerations ... 501
28.11.2 Security configuration ... 502
28.11.3 Re-production types ... 503
28.11.4 Re-production scenarios ... 506
28.11.5 Re-produce documents ... 508
28.11.6 Re-production job status ... 509
28.11.7 Re-production views ... 510
28.12 Branding queue ... 511
28.12.1 Permissions ... 511
28.12.2 Branding queue fields ... 512
28.13 Production queue ... 512
28.13.1 Permissions ... 512
28.13.2 Change job priority ... 514
28.13.3 Retry Production Job mass operation ... 514
28.13.4 Cancel Production Job mass operation ... 514
28.13.5 Production queue fields ... 515
29 Redact ... 515
29.1 Example workflow ... 516
29.2 Installing Redact to a workspace ... 516
29.3 Before you begin ... 517
29.4 File size considerations ... 517
29.5 Redact supported file types ... 517
29.6 Permissions ... 517
29.6.1 All Redact permissions ... 518
29.6.2 Native PDF Redactions permissions ... 519
29.6.3 Native Excel Redactions permissions ... 519
29.6.4 Image Redactions permissions ... 520
29.6.5 Redact Mass Operations permissions ... 520
29.6.6 Markup set permissions ... 520
29.6.7 Permissions for redacting documents outside of Relativity ... 521
29.7 Automated spreadsheet markup project ... 521
29.7.1 Supported file types ... 521

29.7.2 Preparing Excel documents ... 521
29.7.3 Before you begin ... 521
29.7.4 Creating a spreadsheet markup project manually ... 522
29.7.5 Creating a spreadsheet markup project using .csv or .xlsm rules ... 523
29.7.6 Fields ... 524
29.7.7 Running the project ... 528
29.7.8 Reviewing markups ... 528
29.7.9 Reviewing the original native document ... 528
29.8 Automated image markup project ... 528
29.8.1 Before you begin ... 528
29.8.2 Creating an image markup project manually ... 528
29.8.3 Creating an image markup project using .csv or .xlsm rules ... 529
29.8.4 Fields ... 530
29.8.5 Running the project ... 533
29.8.6 Reviewing markups ... 534
29.9 Automated image template markup project ... 534
29.9.1 Before you begin ... 534
29.9.2 Creating an image template markup project ... 534
29.9.3 Fields ... 535
29.9.4 Running the project ... 536
29.9.5 Reviewing markups ... 536
29.10 Automated PDF markup project ... 536
29.10.1 Before you begin ... 536
29.10.2 Supported file types ... 536
29.10.3 Creating a PDF markup project manually ... 536
29.10.4 Creating a PDF markup project using .csv or .xlsm rules ... 537
29.10.5 Fields ... 538
29.10.6 Running the project ... 541
29.10.7 Removing a markup applied by a project ... 541
29.10.8 Reviewing markups ... 542
29.11 Automated production preparation project ... 542
29.12 Automated spreadsheet propagation project ... 542
29.12.1 Preparing Excel documents ... 542
29.12.2 Before you begin ... 542

29.12.3 Creating a spreadsheet propagation markup project 543
29.12.4 Fields 543
29.12.5 Running the project 544
29.12.6 Reviewing markups 544
29.12.7 Reviewing the original native document 545
29.13 Blackout migration 545
29.13.1 Limitations 545
29.13.2 Production preparation 546
29.14 Convert Markups 547
29.14.1 Changing markup types 547
29.14.2 Reviewing converted markups 547
29.15 Manual markups with spreadsheet files 547
29.15.1 Preparing Excel documents 548
29.15.2 Excel file markup considerations 548
29.15.3 Supported file types 548
29.15.4 .csv file markup considerations 548
29.15.5 Applying markups to .csv files 549
29.15.6 Applying markups to Excel files 549
29.15.7 Convert Spreadsheets Markup 553
29.15.8 Inverting markups 553
29.15.9 Excel document keyboard shortcuts 553
29.15.10 Reviewing markups 554
29.15.11 Reviewing the original native document 554
29.15.12 Downloading and exporting marked up documents 554
29.16 Manual markups with PDF files 555
29.16.1 PDF markup considerations 555
29.16.2 Supported file types 555
29.16.3 PDF basic redactions 555
29.16.4 PDF highlights 555
29.16.5 Rejecting highlights or markups 556
29.16.6 Reviewing markups 556
29.16.7 Downloading and exporting marked up documents 556
29.17 Redact Audits 556
29.18 Redact Client Usage Report 557

29.19 Redact External Markups 558
29.19.1 Example workflow 559
29.19.2 File size considerations 559
29.19.3 Adding documents to External Markups tab 560
29.19.4 Recommended uses of External Markups 560
29.19.5 External Markups tab columns 561
29.20 Redact Language Support 561
29.20.1 Language settings in Relativity 561
29.20.2 Entering Language Codes in an image markup project 562
29.21 Redact project best practices 562
29.21.1 Use the minimum number of projects 562
29.21.2 Revert before experimenting with a new project 562
29.21.3 Update rules in an existing project rather than creating a new one 562
29.21.4 Maintain one data source per project 562
29.21.5 Use separate markup sets if multiple projects must cover the same documents with the same rules 563
29.21.6 Other overlapping scenarios 563
29.21.7 Audit your projects before running 563
29.22 Redact Project Status 563
29.22.1 Redact queue priority 564
29.22.2 Redact project Priority queue 564
29.22.3 Removing a project from the Priority queue 564
29.23 Redact Reports 564
29.23.1 Available report fields 565
29.23.2 Generate a Markup or Document Report 565
29.23.3 Redact specific fields 565
29.24 Redact Settings 567
29.25 PDF annotation and attachment markups 567
29.25.1 PDF annotation redactions 567
29.25.2 Redacting PDF attachments 568
29.26 Regular expression examples 569
29.26.1 Before you begin 569
29.26.2 Email addresses and phone numbers regular expressions 569
29.26.3 Universal regular expressions 571
29.26.4 Financial accounts regular expressions 572

29.26.5 Government identification numbers regular expressions ... 574
29.27 Reviewing markups to ensure accuracy ... 577
29.27.1 Using the Redact Navigation card to review markups ... 577
29.27.2 Using the Redact navigation card in the Image Viewer ... 579
29.27.3 Review image markups using Quality Review ... 579
29.27.4 Delete Native Markups ... 580
29.28 Running and reverting a Redact project ... 580
29.28.1 Running a project ... 580
29.28.2 Redact project performance expectations ... 581
29.28.3 Stopping a project that is running ... 583
29.28.4 Reverting a project ... 584
29.29 Searching for documents with Redact fields ... 585
29.29.1 Creating a saved search using Redact fields ... 585
29.30 Using Find and Redact ... 586
30 Sampling ... 587
30.1 Permissions ... 588
30.2 Enabling sampling on an object ... 589
30.3 Generating a sample ... 590
30.3.1 Creating a fixed size sample set ... 591
30.3.2 Creating a percentage sample set ... 591
30.3.3 Creating a statistical sample set ... 592
31 Scripts ... 592
31.1 Script compatibility and updates ... 593
31.2 Creating a new library script ... 593
31.3 Selecting an existing library script ... 595
31.4 Creating a new workspace script ... 596
31.5 Adding a library script to the script tab ... 597
31.6 Running a library script ... 597
32 Script groups ... 597
32.1 Setting up a script group ... 597
33 Search terms reports ... 599
33.1 Search terms reports ... 599
34 Searching ... 599
34.1 Filters ... 600

34.2 Search panel ... 600
34.3 Keyword searches ... 600
34.4 Saved searches ... 600
34.5 dtSearch ... 600
34.6 Analytics ... 600
34.7 Regular expressions ... 601
34.8 Assist ... 601
34.9 Additional features ... 601
35 Security and permissions ... 601
35.1 Levels of Security in Relativity ... 602
35.2 Instance security ... 603
35.2.1 Features ... 604
35.2.2 Granular permissions ... 604
35.2.3 Tab Visibility tab ... 605
35.2.4 Admin Operations tab ... 607
35.2.5 Group Permissions report ... 608
35.2.6 Uneditable admin permission settings for the Everyone group ... 608
35.2.7 Script and application library permissions ... 609
35.2.8 System administrator privileges ... 610
35.3 Setting instance permissions ... 610
35.3.1 Groups Management tab ... 611
35.3.2 Features tab ... 615
35.3.3 Granular permissions ... 619
35.3.4 Tab Visibility tab ... 620
35.3.5 Admin Operations tab ... 621
35.4 Workspace security ... 622
35.4.1 Features ... 622
35.4.2 Legacy granular permissions ... 622
35.4.3 Object list ... 623
35.4.4 Browsers ... 633
35.4.5 Mass operations ... 633
35.4.6 Admin operations ... 635
35.4.7 Customer lockbox ... 636
35.4.8 Workspace admin group ... 636

35.4.9 Relativity aiR lockbox ... 637
35.5 Feature permissions ... 639
35.5.1 Currently modernized features ... 640
35.5.2 Considerations ... 643
35.5.3 Using the Features tab ... 644
35.5.4 Feature permission behavior ... 647
35.5.5 Frequently asked questions ... 650
35.5.6 Workspace-level permissions ... 651
35.6 Setting workspace permissions ... 661
35.6.1 Group Management ... 662
35.6.2 Features tab ... 665
35.6.3 Granular permissions ... 667
35.6.4 Tab Visibility tab ... 668
35.6.5 Other Settings tab ... 670
35.6.6 Saving permissions for a group ... 671
35.7 Relativity object security ... 671
35.7.1 Securing a folder for selected groups ... 673
35.8 Preview security ... 674
35.8.1 Previewing security from the Workspace Details tab ... 675
35.8.2 Previewing security from the Groups tab ... 675
35.8.3 Previewing security from the Users tab ... 676
35.8.4 Preview security audit ... 676
35.9 Permissions scenarios ... 676
35.9.1 Hierarchical structure ... 676
35.9.2 Client domains ... 677
35.9.3 User groups ... 677
35.9.4 Template groups ... 677
35.9.5 Object-level permissions ... 679
35.9.6 Item-level permissions ... 679
35.9.7 Document unitization ... 680
35.9.8 Scenarios ... 681
35.9.9 Frequently asked questions ... 683
36 Tabs ... 688
36.1 Permissions ... 688

36.2 Creating and editing tabs ... 689
36.3 Fields ... 690
36.3.1 Tab Information ... 690
36.3.2 Tab Location ... 691
36.4 Nesting children tabs ... 692
37 Users ... 692
37.1 User status ... 692
37.2 Creating and editing a user ... 692
37.3 Adding a user log-in type ... 693
37.4 Fields ... 693
37.5 Viewing user audit records ... 698
37.6 Sending messages to users ... 699
37.7 Bounce list removal ... 699
37.8 Forcing users to log out ... 700
37.9 Adding or removing users from a client domain ... 700
37.10 Auto-disable users ... 701
38 Views ... 702
38.1 Permissions ... 703
38.2 Workspace system views ... 704
38.3 System views from Home ... 705
38.4 Creating a view ... 706
38.4.1 Creating a view with field categories ... 706
38.4.2 Creating a view without field categories ... 707
38.5 Information tab ... 708
38.6 Other tab ... 709
38.7 Fields tab ... 709
38.8 Conditions tab ... 710
38.9 Sort tab ... 712
38.10 Editing view information ... 712
38.11 Linking a dashboard to a view ... 713
38.12 Displaying family groups in a view ... 714
38.12.1 Creating the family group view ... 714
39 Viewer ... 715
39.1 Permissions ... 715

39.2 Native Viewer 717
39.2.1 Navigating the Native Viewer 718
39.2.2 Copying text in the Viewer 723
39.2.3 Streaming audio and video files 724
39.2.4 Document Intelligence 725
39.3 Image Viewer 728
39.3.1 Navigating the Image Viewer 728
39.3.2 Saving an image as a PDF 732
39.4 Extracted Text Viewer 733
39.4.1 Navigating the Extracted Text Viewer 733
39.4.2 Extracted Text Viewer toolbar options 734
39.4.3 Left drawer Viewer options 735
39.4.4 Right drawer Viewer options 736
39.4.5 Document actions menu 736
39.4.6 Viewer settings menu 737
39.4.7 Viewer breadcrumbs 737
39.5 Productions Viewer 737
39.5.1 Navigating the Productions Viewer 737
39.5.2 Imaging on the fly 740
39.6 PDF Viewer 741
39.6.1 PDF Viewer toolbar options 742
39.6.2 Left drawer Viewer options 742
39.6.3 Right drawer Viewer options 743
39.6.4 Document actions menu 744
39.6.5 Viewer settings menu 745
39.6.6 Viewer Breadcrumbs 745
39.7 Document actions menu 745
39.8 Viewer settings menu 747
39.9 Pop Out Viewer 748
39.9.1 Standalone Viewer 750
39.9.2 Document preview panel 751
39.10 Related items card 752
39.10.1 Document actions in the related items card 753
39.11 Document and Production History card 754

39.11.1 Document and Production History card permissions ... 755
39.12 Documents card ... 755
39.12.1 Email thread visualization tool ... 756
39.13 .eml and .msg header dates and times in the Viewer ... 756
39.14 Thumbnail Viewer ... 757
39.15 Document Compare ... 757
39.16 Viewer-supported file types ... 759
39.16.1 Categories ... 760
39.16.2 Viewer audio and video-supported file types ... 771
39.16.3 Troubleshooting errors ... 771
39.16.4 Supported audio file types ... 772
39.16.5 Supported video file types ... 772
39.16.6 Text-only designation ... 774
39.16.7 File ID only designation ... 775
40 Workspaces ... 776
40.1 Permissions ... 776
40.2 Creating and editing a workspace ... 777
40.3 Fields ... 778
40.4 Viewing workspace details ... 782
40.4.1 Deleting a workspace ... 782
40.5 Using the utilities console ... 783
40.5.1 System Settings ... 783
40.6 Managing system keyboard shortcuts ... 783
40.7 Viewing the personal items of workspace users ... 785
40.8 Cold storage management ... 785
40.9 Adding and editing production restrictions ... 785
40.9.1 Managing production restrictions in templates ... 786
40.10 Workspace admin group ... 786
40.11 Repository workspaces in Relativity aiR ... 787
40.11.1 Setting up a repository workspace ... 787
40.11.2 Example 1 ... 787
40.11.3 Example 2 ... 788
40.11.4 Special considerations ... 788
40.12 Document and item list navigation ... 789

40.12.1 Permissions ... 789
40.12.2 Browsers panel ... 790
40.12.3 View bar ... 794
40.12.4 Document Preview panel ... 795
40.12.5 Item list ... 798
40.13 Cold Storage ... 801
40.13.1 Permissions ... 801
40.13.2 Migrating a Workspace to Cold Storage ... 801
40.13.3 Retrieving a Workspace from Cold Storage ... 803
40.13.4 Deleting a workspace from Cold Storage ... 805
40.13.5 Frequently Asked Questions (FAQ) ... 806
40.13.6 Troubleshooting Cold Storage Operations ... 806
40.14 Recycle Bin ... 807
40.14.1 Billing and permissions ... 807
40.14.2 Moving to the Recycle Bin ... 807
40.14.3 Managing workspaces in the recycle bin ... 808
41 Resources ... 808
41.1 Tutorials ... 809
41.2 Relativity Community ... 809
41.3 Relativity Support team ... 809

1 Admin guide overview

The Admin guide will help give you the knowledge to effectively manage Relativity's flexibility and granular security rights. This can help in providing an intuitive interface for your users. This guide explains the majority of features available to you in Relativity.For more information about features not discussed int his guide, review our available information on the Relativity aiR documentation site.

1.1 Navigation

Relativity is an application with many screens and functions. This section describes the Review Interface you use to review documents and some of the standard procedures you'll need to perform as you use the product.

1.1.1 Logging in

Relativity offers several ways to log in and it's possible to have two or more methods available to you. Your system admin will provide you with all the information you need to log on. Contact your system admin if you have additional questions.

For procedures to log in, see Logging in to Relativity.

1.1.2 Tab navigation

When you log in to Relativity, you see tabs displayed in the sidebar on the left side of the page. You may also be able to access tabs using the tab strip, which runs horizontally across the top of the page.

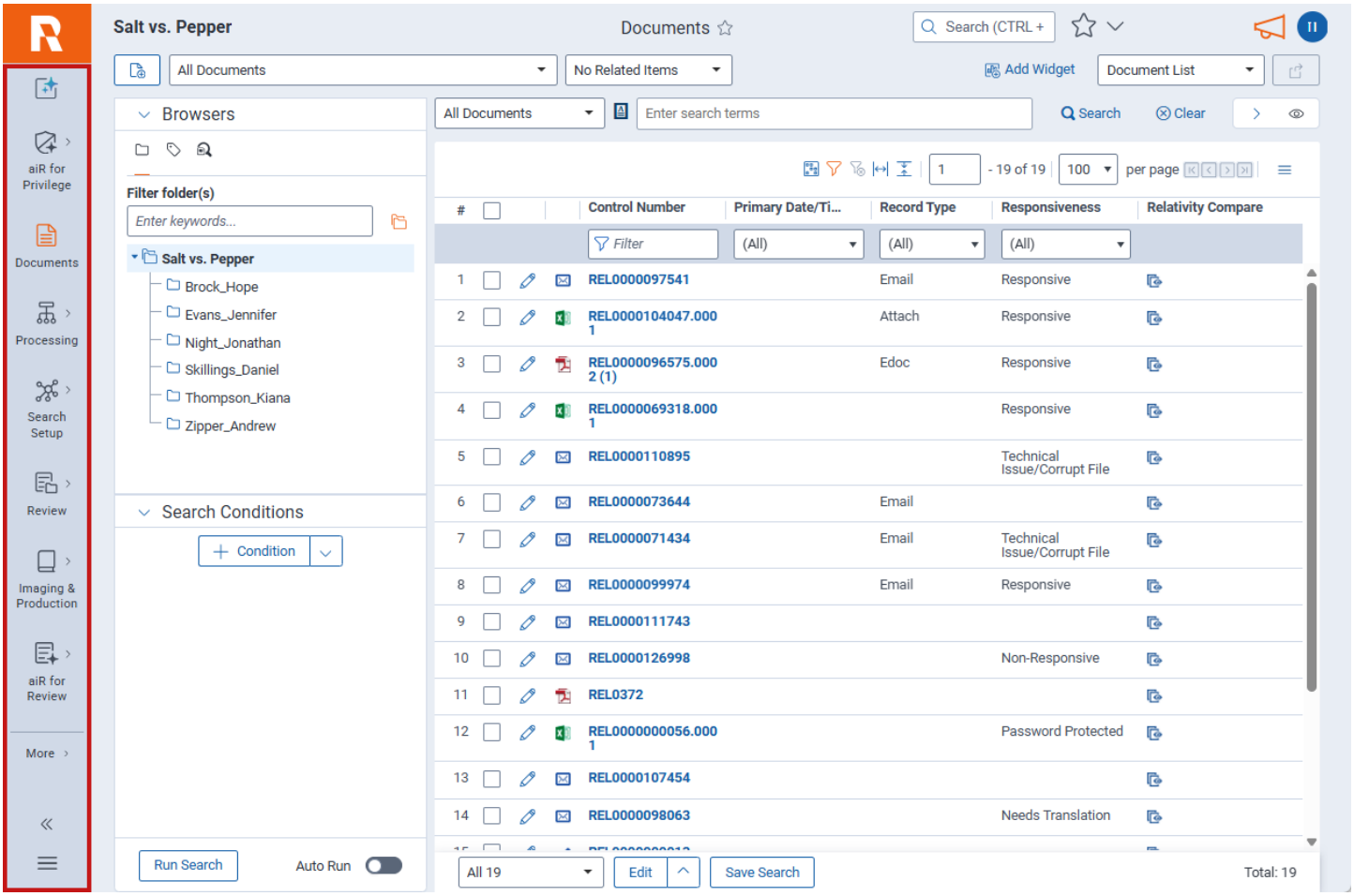
The sidebar and tab strip display the currently available tabs whether you are on the instance or workspace-level. The active tab in the sidebar is indicated by the tab icon displaying in orange and in the tab strip, the active tab is indicated by an orange line displaying under the name.

The tabs are arranged based on the order value for each tab.

You can navigate tabs using the following features.

1.1.2.1 Sidebar

The sidebar allows you to place tabs that you commonly use on the left-side of Relativity so that you can access them at your convenience.

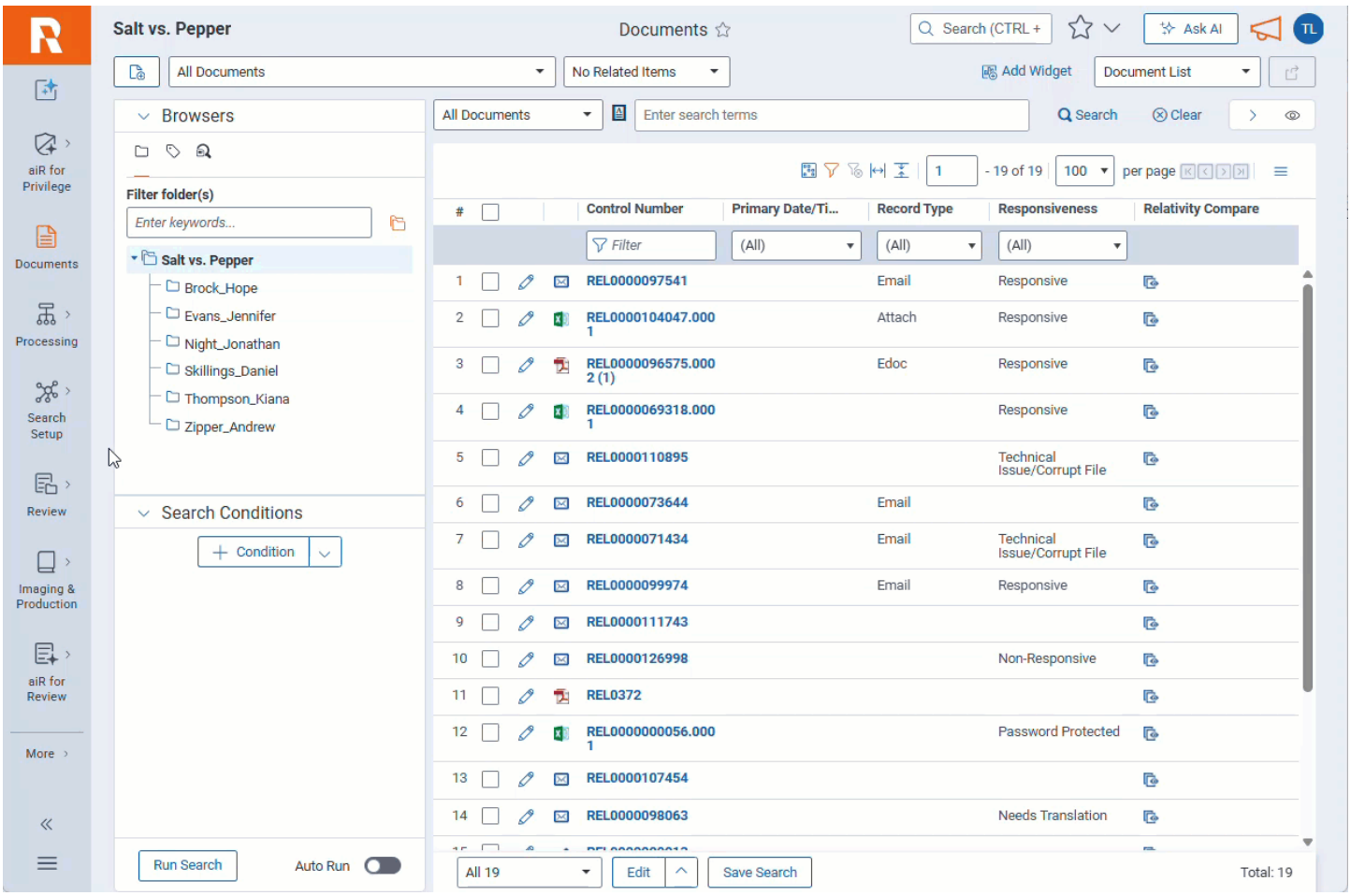


Tabs are ordered from top to bottom of the sidebar based on the value entered in the **Order** field. The lowest order value displays at the top and the highest value displays at the bottom.

The total number of tabs that display in the sidebar is determined by the resolution of your browser.

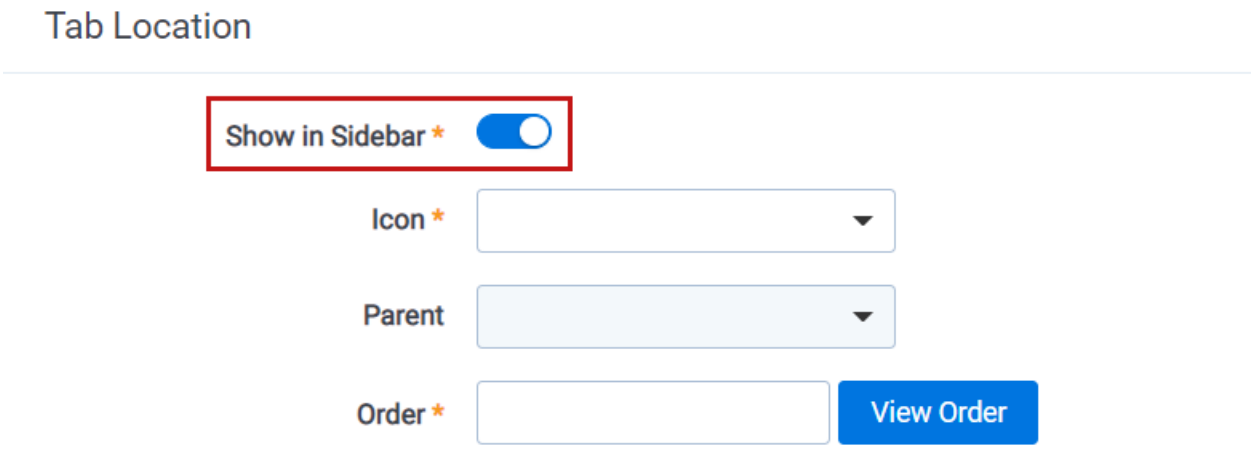
Tabs that have been assigned to the sidebar and do not fit, are available by hovering your cursor over the **More** icon.

If a tab has one or more child tabs, you can view and select those tabs by hovering over the parent tab's row in the fly-out menu.



The More icon will display with an orange bar on the right side **More** to indicate that the active tab is located in the More menu.

To add a new or pre-existing tab to the sidebar, toggle the **Show in Sidebar** on and click **Save**.

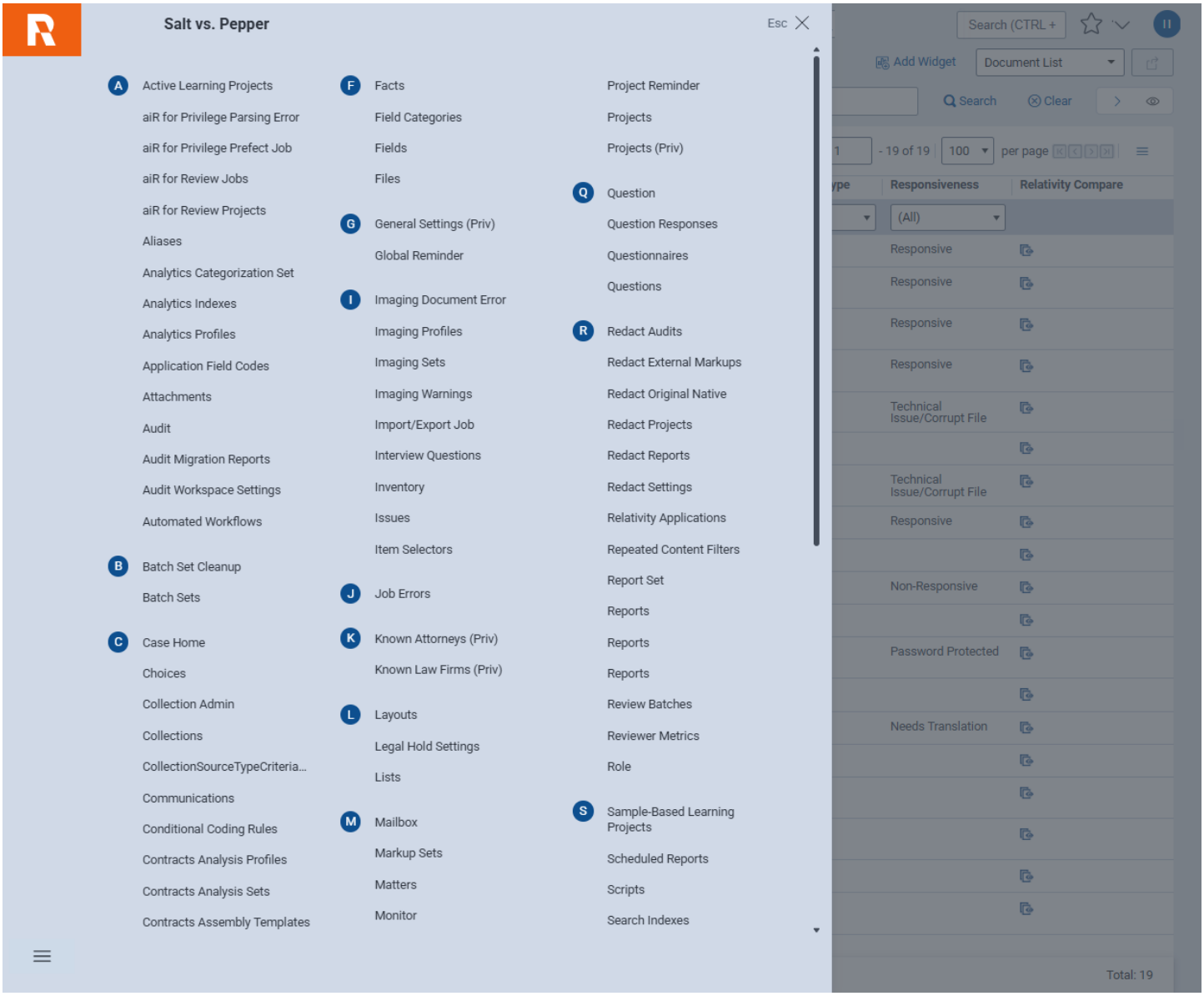


Tabs can display in the sidebar with their name and icon. Alternatively, you can click the collapse arrow icon to only display the icon for each tab. This reduces the width of the sidebar and increases the number of icons that can display



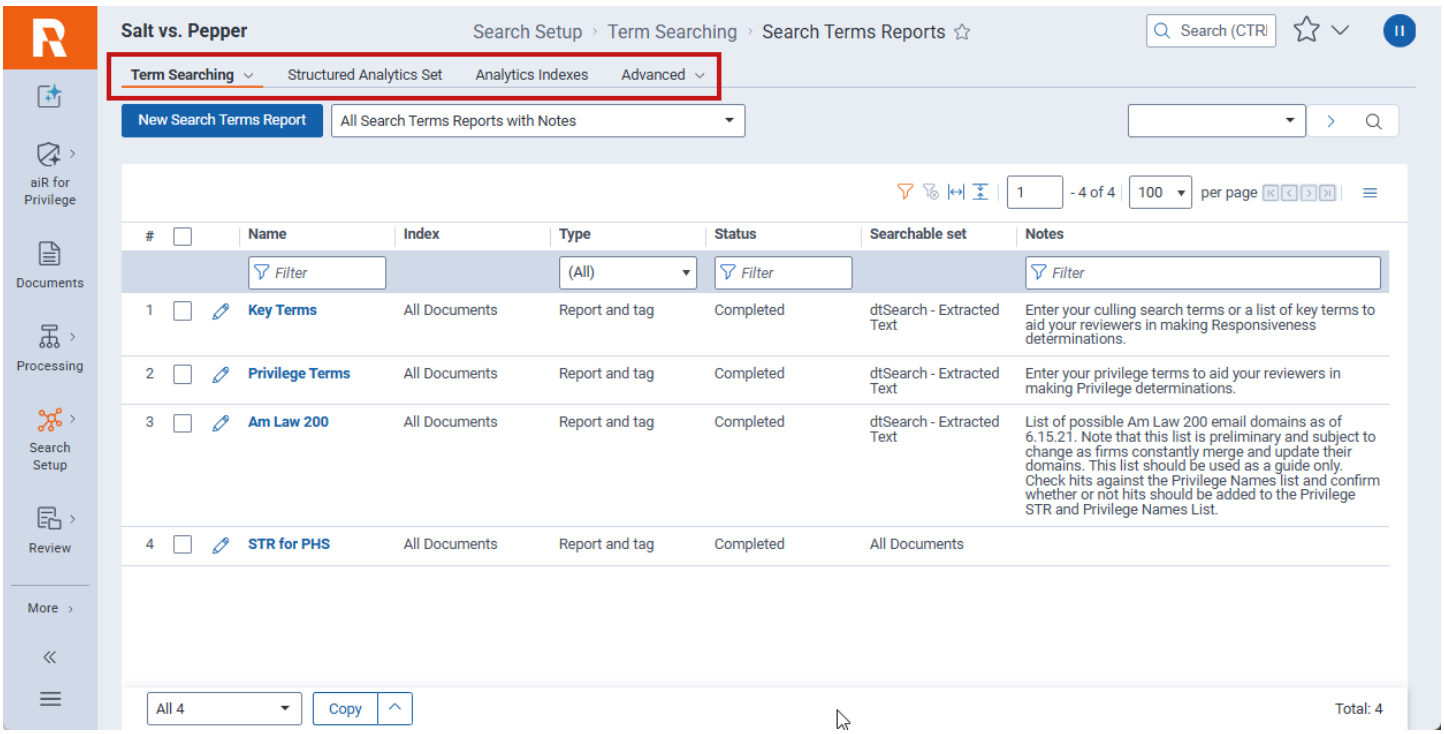
1.1.3 All tabs menu

Click the  icon at the bottom of the sidebar to display the All tabs menu. Every child tab that a user can view, as determined by their permissions, will display in the menu in alphabetic order. This menu does not display parent tabs.



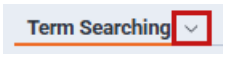
1.1.4 Tab strip

If you select a tab that either has child tabs or is a child tab to a parent tab, the tab strip will display horizontally across the top of Relativity. If a tab in the tab strip has one or more children tabs, hover your cursor over it to view and select the desired tab. Depending on the size of your browser, there may be more tabs than can display in the tab strip. You can hover your cursor over **More** in the tab strip to view additional tabs in a fly-out menu.

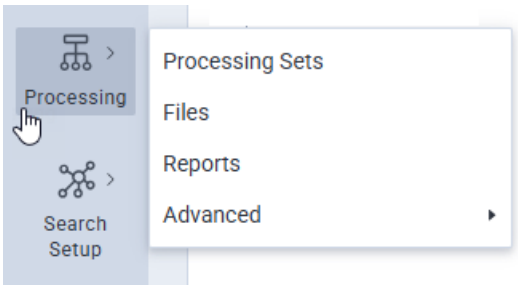


1.1.4.1 Parent and child tab display

Parent tabs can be displayed in the sidebar or the tab strip. Tabs that have child tabs in the tab strip will display with an arrow on the right side.

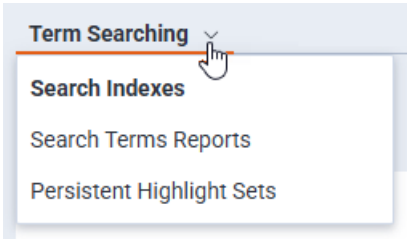


To view the child tabs of a parent tab in the sidebar or tab strip, hover your cursor over the parent tab and the child tabs will display in a fly-out menu.



When you select a child tab from the sidebar or the tab strip, you are taken to that page. For example, Production Sets.

In addition to an orange bar displaying underneath the parent tab in the sidebar, the child tab and the path to reach the active tab is highlighted in blue to help you track your location in the sidebar or the tab strip.



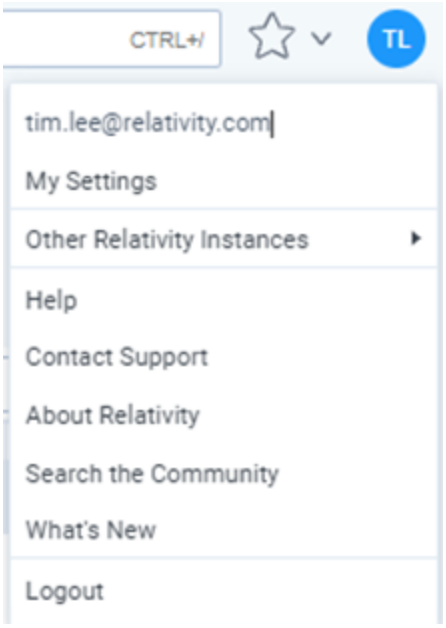
Instead of clicking the drop-down arrow, you can also click the parent tab itself. Clicking the parent tab takes you to the default child tab, which is identified by the order setting for each child tab.

1.1.5 User options

When you first log in to Relativity, you see the default Home tab. Relativity displays the Workspaces tab as your default Home tab when you navigate to Home. You can change the default Home tab to be any tab you want.

A system admin is a user with rights to see every item in a Relativity environment.

System admins have access to admin tabs, which allow them to create and edit new clients, matters, users, groups, and views, among other capabilities. You can grant many admin permissions to groups as needed for the various roles certain users might have in your organization. A system admin has full rights to view all tabs within the Relativity environment. You can grant lower level admin groups access to the particular admin tabs necessary to fulfill their roles.



The Relativity Instances section includes federated instances you have access to. Federated instances links allow reviewers to easily switch to other Relativity environments. For more information, see Federated instances.

The user drop-down menu options are:

- **My Settings**—opens a pop-up where users can change their personal settings. See My settings on the next page for more information.
- **Other Relativity instances**—hover your cursor over this option to display a fly-out menu of federated instances that have been linked to your current one. Click on the desired federated instance to switch to that linked instance.
- **Help**—launches the Relativity documentation website in your internet browser. The documentation site provides all Relativity user, system admin, and systems documentation in a navigable format.
- **Contact Support**—opens a new window in your internet browser containing the Technical Support page of the Relativity website where you can open a support ticket.
- **About Relativity**—opens a pop-up displaying the Relativity version number, your instance details, and licensing agreement information.
- **Search the Community**—opens a new window in your internet browser containing the Relativity Community page where you can find applications for Relativity to download, stay up to date on the latest Relativity events, and interact with other Relativity users.

- **What's New**—opens a side panel that gives you the opportunity to learn about new and noteworthy updates and enhancements directly in Relativity aiR.
- **Logout**—logs users out of Relativity.

1.1.5.1 Changing the default Home tab

Relativity displays the Workspaces tab as your default Home tab when you navigate to Home. You can change the default Home tab to be any tab that is available for default and that is not a specific tab within a workspace.

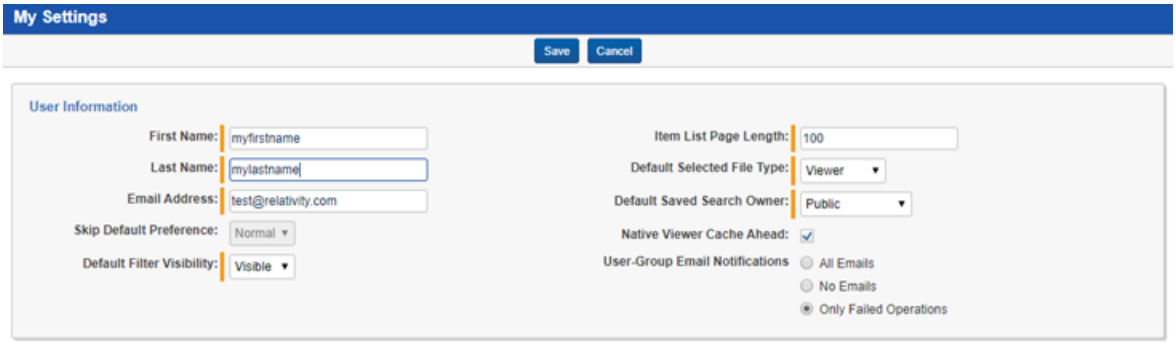
Perform the following steps to change the default Home tab:

1. Navigate to the **Tabs** tab.
2. Click on the tab you want to set as the default Home tab.
3. Click the **Edit** icon in the row of the tab you wish to edit.
4. Toggle the **Set as Default Tab** field on.
5. Click **Save**.

Note: If a user is not a member of a group with permission to view the tab set as the default Home tab, Relativity redirects to the lowest ordered tab the user's permissions allow.

1.1.5.2 My settings

Clicking **My Settings** from within the user drop-down menu opens a settings mode pop-up, which displays your user information. Click **Edit** to change your settings.



- **First name**—your first name.
- **Last name**—your last name.

  Note: Your first and last name appear as your username throughout Relativity.

- **Email address**—your email address and login.
- **Skip Default Preference**—when reviewing documents, skip prevents a reviewer seeing documents that are already coded, depending on the selected view. Choose one of the following options:
  - **Normal**—this setting disables the skip feature.
  - **Skip**—this setting turns on the skip feature.
- **Default Filter Visibility**—determines whether or not the filters for columns in views display by default.
  - **Hidden**—hides filters by default.
  - **Visible**—displays filters by default.

- **Item list page length**—a numeric field indicating the default list length for all lists in Relativity. It can be set from 1-200.
- **Default Selected File Type**—the default viewer mode used when first loading the Viewer. Viewer, Native, Image, Long Text, or Production. If the mode selected is not available, the Viewer will instead use the first available option. See Viewer on page 715 for details.
- **Default Saved Search Owner**—determines whether saved searches are public or private by default. If set to Public, the search is public and all users with rights to it can see it. If set to Logged in User, the search is private and only the logged in user is able to see it.

  Note: Depending on your permissions, you may not have rights to edit the **Default Saved Search Owner** field.

- **Native Viewer Cache Ahead**—if checked, this field pre-loads the next native document in your review queue when the active document is loaded.

  Note: In modern browsers, this setting may have a reduced impact on document load performance compared to earlier browser versions. For more effective pre-loading behavior, administrators can request an adjustment to the PreConvertCacheSize instance setting (kCura.EDDS.Web), which controls how many documents are pre-converted in the background for the Native, Image, and Production viewers. Contact Relativity Support to modify instance settings in Relativity aiR.

- **User-Group Email Notifications**—user's preference for email notifications when adding or deleting Users or Groups.
  - **All Emails**—receive all email notifications.
  - **No Emails**—receive no email notifications.
  - **Only Failed Operations**—receive email notifications on failed operations only.

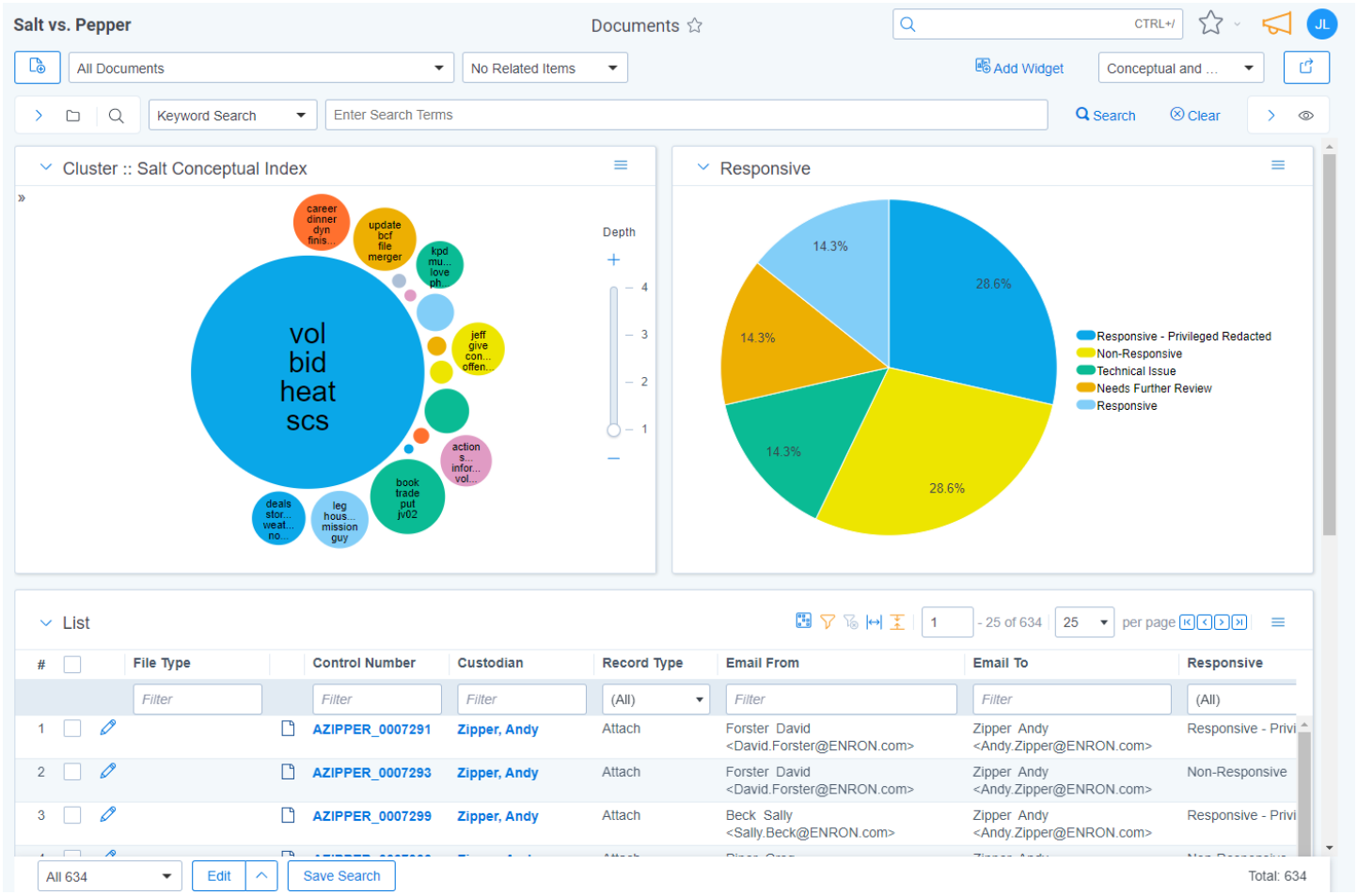
  Note: Depending on your permissions, you may not have rights to edit the **User-Group Email Notifications** field.

After changing your settings as needed, click **Save**.

1.1.5.3 Dashboards

When you've created a page configuration you'd like to preserve, you can create a customized dashboard. You can save multiple dashboards to quickly change the page configuration. The item list and any widgets on the dashboard will update automatically in response to filtering or searching. Dashboards only report on data within the workspace you are in.

Note: For a list of dashboards that provide an effective starting point for administrators to help review teams visualize their data set, see Common commonly-used dashboards in the Admin Guide.



The page initially appears with the folder browser on the top left, the search panel on the bottom left and the item list to the right. Within this new framework, you have multiple options for customizing your display.

You can resize, move, or collapse any panel on the page, including any widgets you create.

- To resize any panel, hover over the line separating the item list from the panel until you see the mouse pointer change to horizontal arrows, then click and drag.
- To move, hover over the top of the panel until you see the Multi-Direction Cursor icon. Then, click and drag the panel to the new location.
- To collapse the search panel or browser pane, click the Collapse icon. Once collapsed, click the **Show Browser Panel** icon to restore the browser pane or the **Show Search Panel** icon to restore the search panel.

Additionally, you can drag and drop panels to rearrange on the page. Click any panel and drag it to a new location. The other panels will automatically move to accommodate the panel you're dropping.

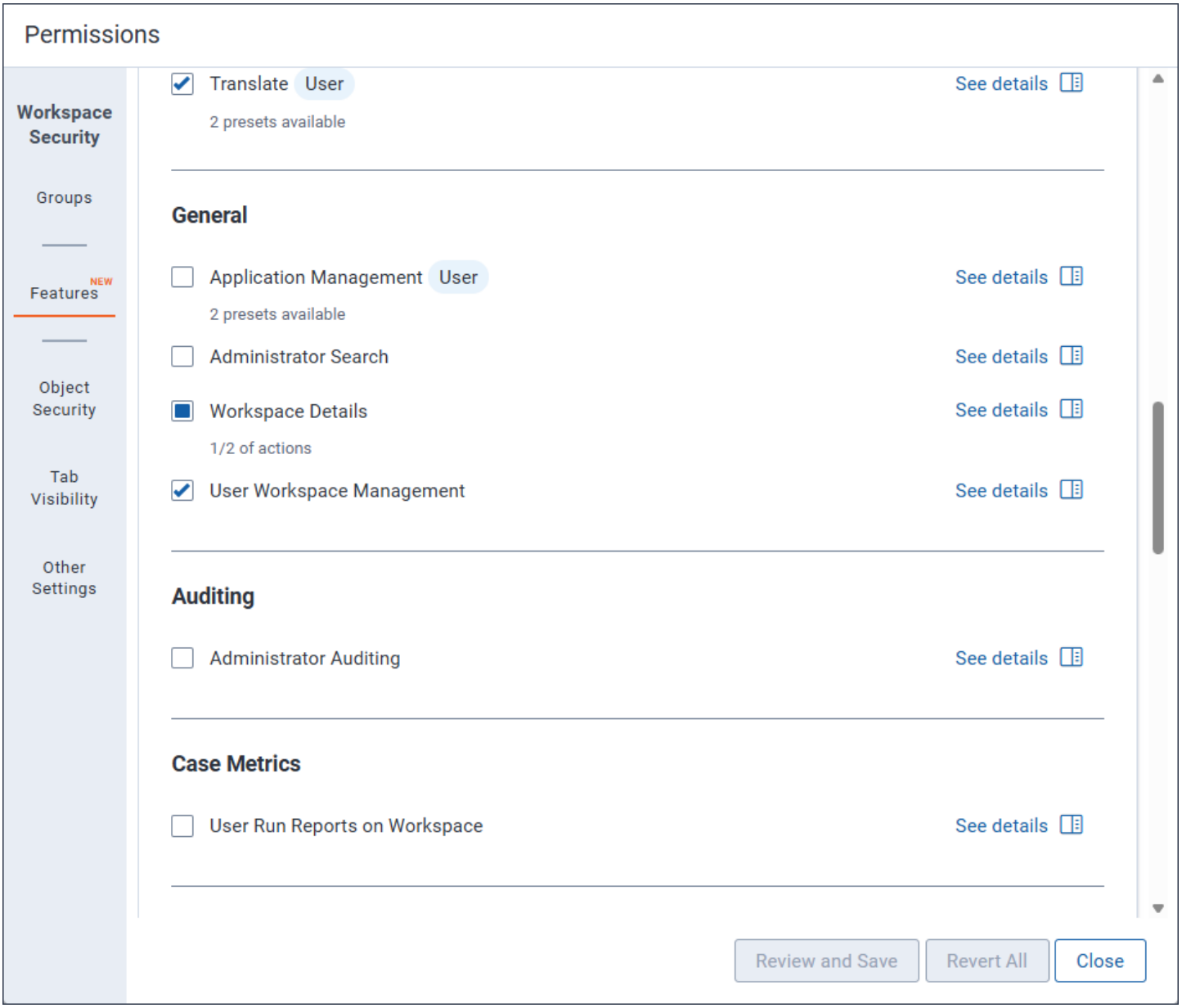
Dashboards and widgets can be copied over to newly created workspaces if they are part of a template. Dashboards only report on data within the workspace you are in if data is loaded in the workspace.

Note: You must have the correct workspace permissions to add, edit, or save a dashboard and to save pivot widgets to your dashboard.
You can also export individual Pivot widgets to Excel or to PNG format from each widget's context menu. See Exporting a Pivot widget in the Admin Guide for more information.

Note: To enable the Add Widgets button and Pivot functionality for an Relativity Dynamic Object (RDO), you must select Enabled for the **Pivot** property in the Object Type Information section for the object.

1.1.6 Permissions

Manage permissions for this feature on the Features tab. Grant the full feature for a group, or customize access with individual actions. For an overview of features and actions, see Feature permissions.



1.1.7 Creating a dashboard

To create a dashboard:

1. Click the **Dashboards** drop-down menu in the top right corner of the screen.

   Note: You can only access the drop-down if Pivot is Enabled for the given object type.

2. Click **New Dashboard** to save the current page configuration as a new dashboard.
3. Enter a name and an order number for the dashboard.

Note: The dashboard with the lowest order number will appear by default when you log in to Relativity.

1.1.8 Adding widgets to a dashboard

You can add the following widgets to customize your dashboard:

- **Pivot charts and tables**—you can use Pivot to summarize data in tables or charts to visually analyze trends in your data.
- **Cluster visualizations**—on the Documents tab, you can use Relativity Cluster Visualization to render your cluster data as an interactive visual map by adding a Cluster Visualization widget. This offers you a quick overview of your document cluster sets and quickly drill into each cluster set to view sub-clusters and conceptually-related clusters of documents. Please note that there may be only one cluster visualization widget per dashboard.
- **Communication Analysis**—after running the name normalization operation within structured analytics, you can use this widget to visualize communication frequencies, patterns, and networks between the entities linked to the documents in the view.

Note: When you reach the maximum number of widgets allowed on a dashboard, the **Add Widget** button will be grayed out and a tooltip displays when you hover over it that lets you know the reason you cannot add any additional widgets to your dashboard. This is controlled by the **MaxNumberDashboardWidgets** instance setting.

1.1.9 Saving changes to a dashboard

You can also make changes on the fly and save a dashboard with the changes. If a dashboard has not been saved, an orange notification displays in the Dashboard drop-down menu until it is saved.

1. Click the Dashboards drop-down menu in the top right corner of the screen to display the list of dashboards available on the current tab.
2. Click **Save** to save the changes to the existing dashboard. Click **Save As** to save the page configuration as a new dashboard, and then enter a **Name** and **Order** number.

Note: If a dashboard is part of a locked application, the option to save the dashboard is unavailable.

1.1.10 Deleting a dashboard

To delete a dashboard from the current tab you are in, click the **Delete** icon to the right of the dashboard you want to delete in the Dashboards drop-down menu.

Click **Delete** in the Delete Dashboard Confirmation pop-up window to delete the dashboard.

Note: If a dashboard is part of a locked application, the option to delete the dashboard is unavailable.

1.1.11 Renaming a dashboard

To rename a dashboard:

1. Click on the **Edit** icon next to the name of the dashboard in the Dashboard drop-down menu.
2. Enter a **Name** and an **Order** number for the dashboard. The order number controls the order in which the dashboard displays in the list.
3. Click **Save** to save your changes.

Note: If a dashboard is part of a locked application, the option to edit the dashboard is unavailable.

1.1.11.1 Using the search panel

While working in the Document list in the new UI framework, you can use the search panel to filter your data.

1.1.12 Resetting your password

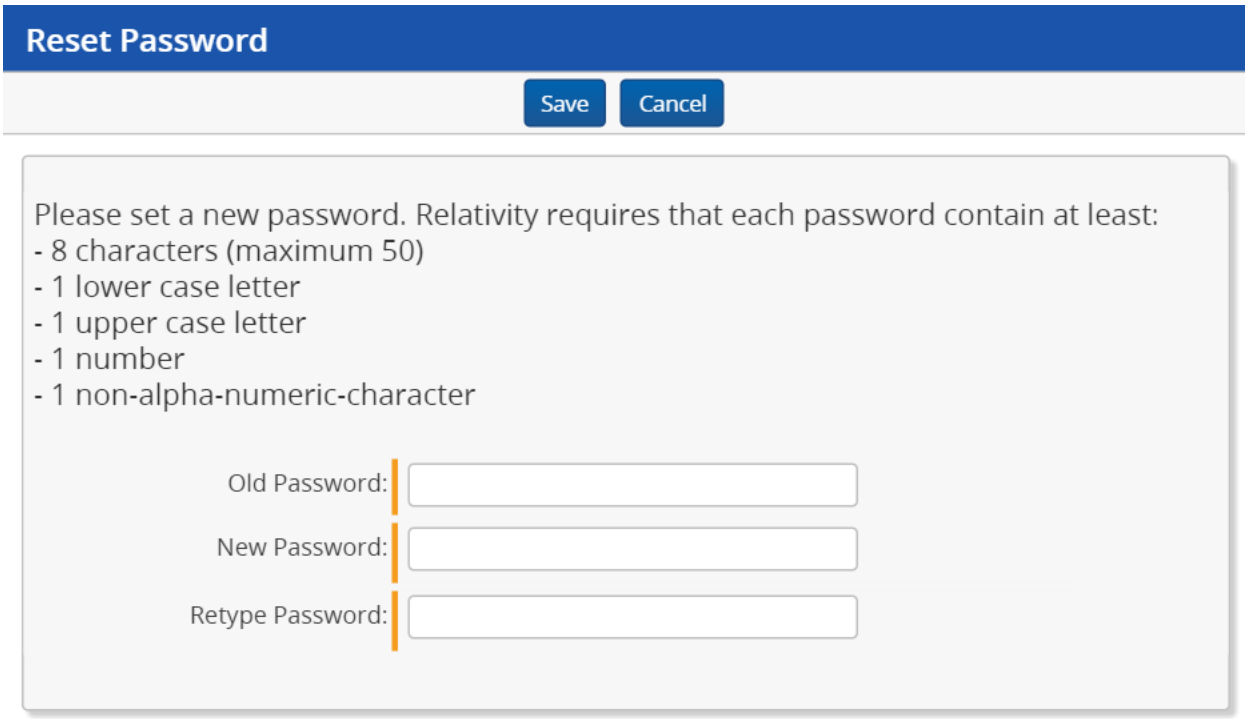
There are two ways you can reset your password if your system admin has given you the appropriate permissions. You can use the **Reset Password** option inside Relativity or the **Forgot your password?** link on the Relativity login screen.

Note: If your password has expired, the Reset Password dialog appears automatically when you log in to Relativity. Your system admin determines when your password expires and the number of previous passwords that you cannot reuse.

1.1.12.1 Resetting your password inside Relativity

If you're already logged in to Relativity, you can reset your password by clicking **Reset Password** in the Home drop-down menu. This directs you to a Reset Password pop-up dialog.

Enter your old password, then enter and retype your new password. Click **Save**.



You can use your new password next time you log in to Relativity.

1.1.12.2 Resetting your password outside Relativity

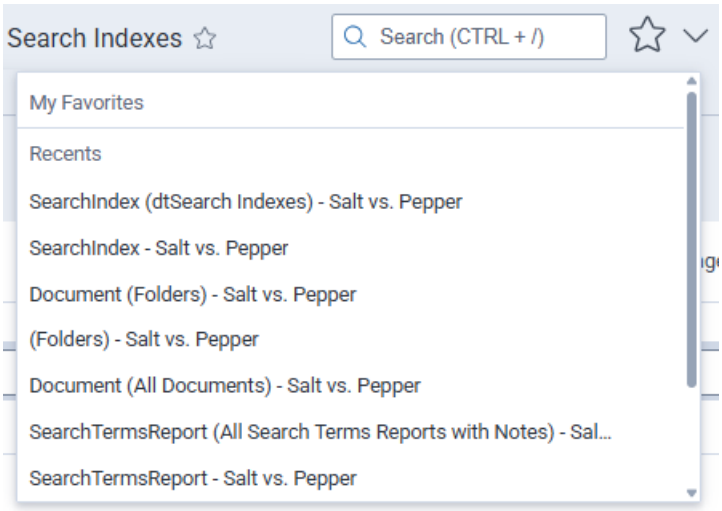
If you cannot log in to Relativity because you've forgotten your password, perform the following steps to reset your password.

1. Click **Forgot your password?** on the login screen.
2. Enter your email address in the pop-up dialog.
   Relativity sends an email to the address you provide. You should receive this message within a few minutes. If you do not receive an email, check your spam or junk mail folder.

3. Click the link in the email to reset your password. This link will be active for 15 minutes and expires after that time. If the link has expired, or if you click the link more than once, you'll have to generate a new password reset request.
4. The link directs you to a page where you can create a new password.
5. Enter a new password and retype it, then click **Submit**. After your password successfully resets, you'll get a message prompting you to log in with your new password. An email will be sent to the address you entered, notifying you that your password reset was successful.

1.1.13 Favorites

The Favorites menu contains all your bookmarks (Favorites) and the last 10 pages in your browsing history (Recents). The Favorites menu can be accessed by clicking the **Favorites** icon in the upper-right part of the page.



Use Favorites to quickly navigate the Relativity application. If you visit a particular page on a regular basis, minimize the number of clicks it takes to get there by adding the page as a favorite.

To mark a page as a favorite, click the star to the right of the breadcrumbs at the top of the page. The star turns blue and Relativity adds the page to the Favorites section. Relativity doesn't limit the number of pages you can mark as a favorite.

Relativity records pages in the Recents section on each page load. That means that pop-up windows aren't recorded as Recents.

Note: If you're a system admin, you can turn off this feature by editing the RecentHistoryEnabled and FavoritesEnabled instance setting values. You can also change the number of Recents the Favorites menu displays by editing the RecentHistoryNumberOfItemsDisplays instance setting value.

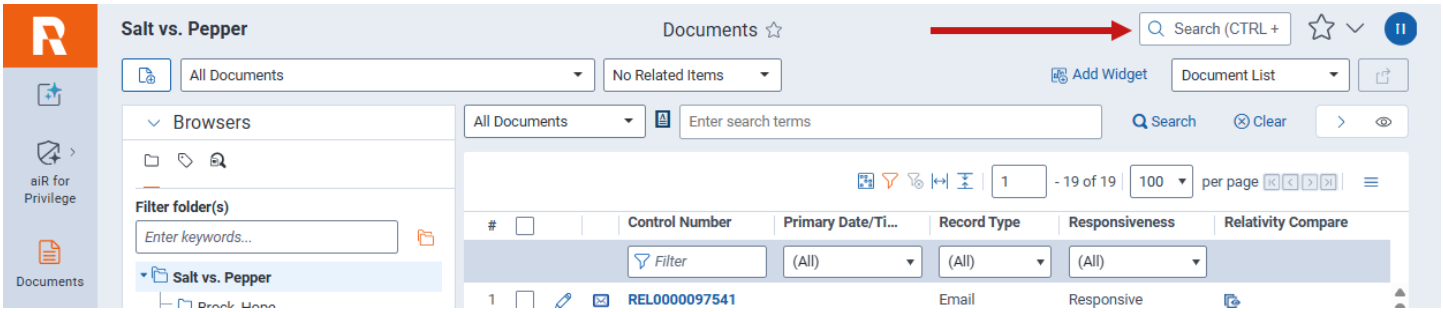
1.1.14 Quick nav

Quick nav can be used to quickly search for and navigate to any workspace or tab in Relativity, including parent tabs that might not otherwise be visible. Each user can only find and access a tab if they were granted the corresponding Tab Visibility permission.

To access quick nav, click the Quick nav search box in the upper right corner of Relativity, or use the keyboard shortcut **Ctrl+/**.

Note: Verify that the quick nav Ctrl+/ keyboard shortcut works on custom pages. Contact Customer Support with any problems.

Open quick nav, and type the name of any tab or workspace.



Any tab or workspace that contains the character string within the name appears in the list of results. Results appear after you type more than one character, and they refine with each character you type. The results link you directly to the tab or workspace in Relativity.

Note: In Relativity terms, the search works the same as a leading and trailing wildcard search.

You can click on any result or use the up and down arrow keys to move through the results. Press **Enter** to navigate to the selected item.

Your search remains until the page is refreshed or you navigate to a new tab. The Esc key also clears your search from quick nav. If no text is entered in the quick nav search field, the Esc key closes quick nav. You can also click anywhere outside the quick nav window to close it.

Quick nav displays three types of results in the following order:

- **Workspace tabs**—lists all workspace tabs that fit the search criteria and are available with your permission settings.

  Note: This item only appears when you are in a workspace.

- **Admin Tabs**—lists all admin tabs that fit the search criteria and are available with your permission settings.
- **Workspaces**—lists all workspaces that fit the search criteria and are available with your permission settings. Click the workspace to go to the default tab for that workspace.

Quick nav results only reflect items available with your permission settings.

The following list highlights more features of quick nav functionality.

- Type the word "home" in quick nav to navigate to your default Home tab.
- Quick nav is enabled or disabled with the QuickNavEnabled instance setting.
- Quick nav is available to look up workspaces and admin tabs from Home for groups assigned the **Use Quick Nav** admin permission, and it is available to look up tabs in a workspace for groups assigned the **Use Quick Nav** workspace permission.
- The maximum number of returned quick nav search results is limited to any number between 2-50, but the default is 20.
- The maximum number of searchable characters is 50.

1.2 Logging into Relativity aiR

Relativity aiR offers several ways to log in and it is possible to have two or more methods available to you. As a Relativity aiR user, your Relativity aiR admin provides you with all the information you need to log in.

Note: For help with single sign-on error messages, please see the SSO Troubleshooting console on page 153.

1.2.1 Logging in to Relativity aiR with a password

1. Enter your **Username**.
2. Click **Continue**.
3. Enter your password.
4. Click **Login**.

Notes: The **Forgot your password?** link only displays if the admin enables Allow Password Recovery via Email setting, for more information see the Authentication Guide. If you forgot your password, select **Forgot your password?** on the login page. If this link does not appear, contact your Relativity admin. Being asked to change your password is different. You set the new password only after logging in with your current password.

1.2.2 Password

This method uses only a username and a password. Your Relativity aiR admin provides you with the following:

- Login email address.
- Password request email.

Prior to logging in, if you have not already, create your password. See Creating or resetting a password on page 49.

To log in:

1. Log in to your Relativity aiR environment using your organization's unique URL.
2. Log in with your password. See Logging in to Relativity aiR with a password above

1.2.3 Two-factor authentication

The two-factor authentication method requires a passcode in addition to the username and password. The system emails you the passcode during login and is different each time. Your Relativity aiR admin provides you with the following:

- Login email address.
- Password request email.

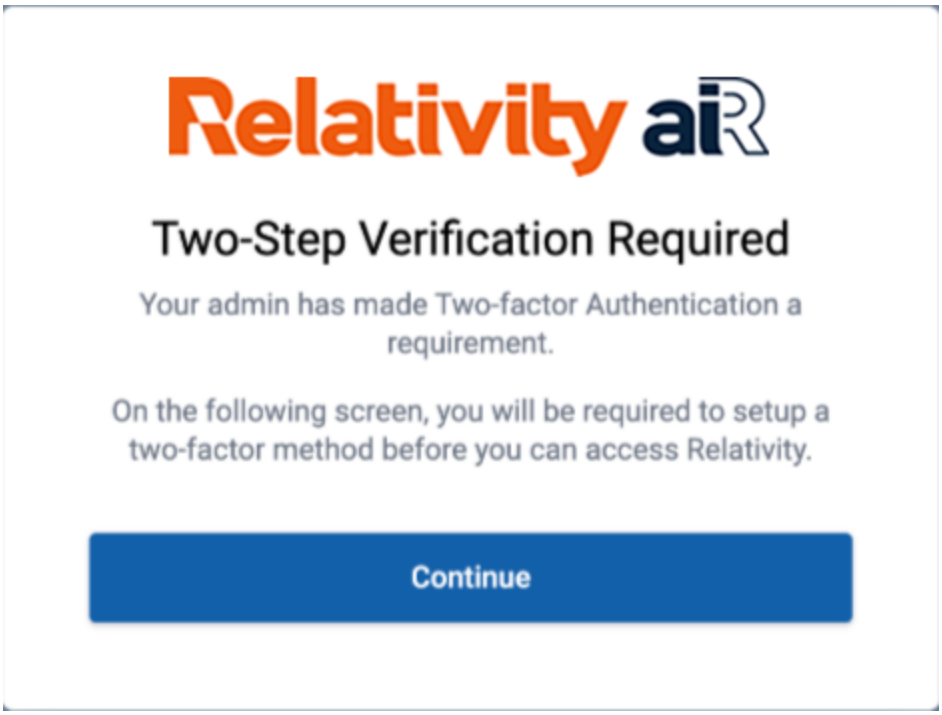
Prior to logging in, if you have not already, create your password. See Creating or resetting a password on page 49.

Prior to logging in, if you have not already, download the required two-factor authentication app. When using the authenticator app for the first time, Relativity will need to connect your profile to the app.

To connect your authentication app,

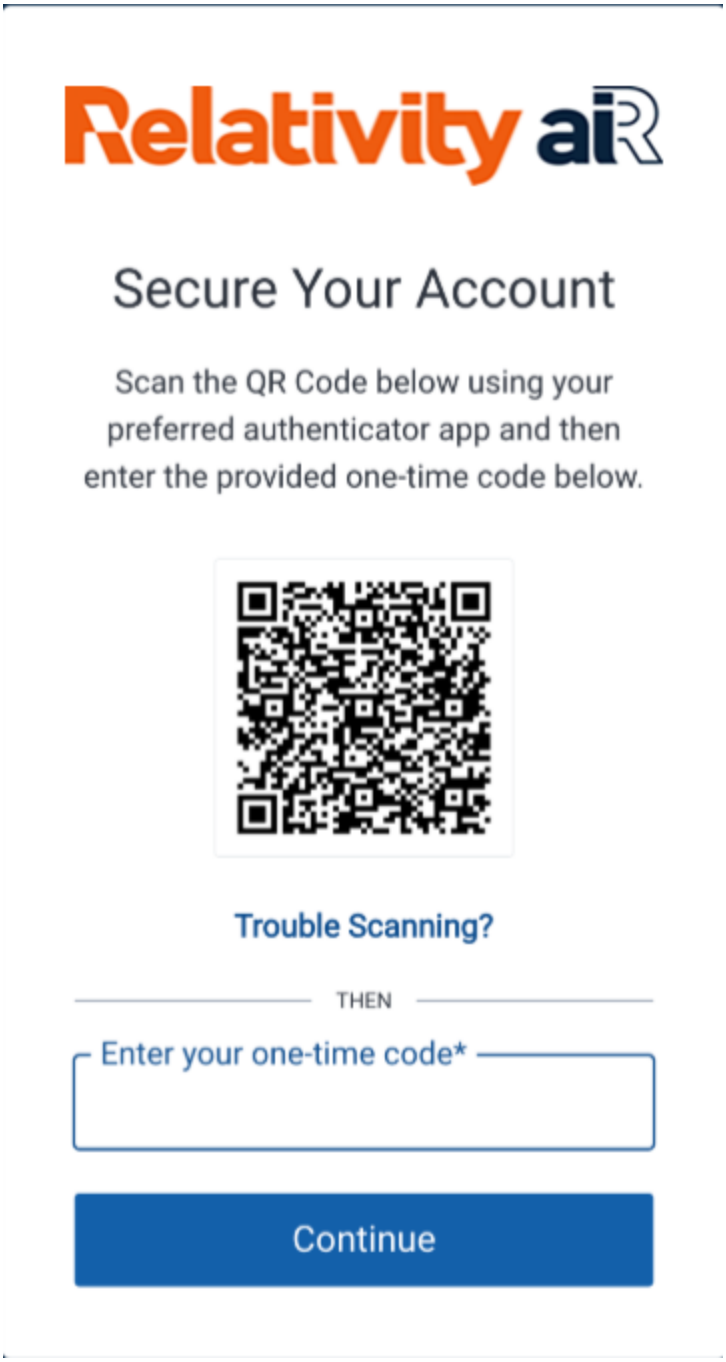
1. Enter your username.
2. Enter your password.

3. On the Two-Step Verification Required step, click **Continue**.



4. Open your authenticator app on your device.
5. In your app, tap the button to add a new account.

6. Hold phone up and scan the QR code provided by Relativity.



If you are unable to scan the QR code, click the **Can't scan QR code?** link below the QR code. Once clicked, a code will appear. Enter the code into your authenticator app on your phone. Once entered into the authenticator app, you can continue to the next step.

7. Click **Next**.
8. Re-enter your email and password.
9. Enter the authentication code in the app.
10. Click **Next**.
11. Click **Done**.

To log in with an authenticator app method:

1. Log in to your Relativity aiR environment using your organization's unique URL.
2. Log in with your password.
3. Follow the instructions on the app or enter the authentication code from the authentication app.
4. Click **Next**.

To log in with the Relativity email method:

1. Log in to your Relativity aiR environment using your organization's unique URL.
2. Log in with your password. An **Authenticate Login** dialog appears. The system immediately emails you a passcode, and the passcode will be different each time.
3. Enter that value in **Passcode**.



4. Click **Login**.

1.2.4 OpenID Connect

This method requires you to have an OpenID Connect account. Your Relativity aiR provides you with the following:

- OpenID Connect account username from the identify provider's side.
- Relativity OpenID Connect button name on the login page.

To log in:

1. Log in to your Relativity aiR environment using your organization's unique URL.
2. Click the Relativity OpenID Connect button name.
3. Enter your username.
4. Click **Logon**.
5. Authenticate with your OpenID provider.

1.2.5 SAML 2.0

This method requires you to have an account with SAML 2.0 authentication provider set up by your Relativity aiR admin. Your admin provides you with a Relativity account with a SAML 2.0 login method.

To log in:

1. Log into the SAML 2.0 provider system.
2. Navigate to the Relativity aiR instance using a shortcut in the SAML 2.0 provider interface or a bookmark in your browser. You are automatically logged in.

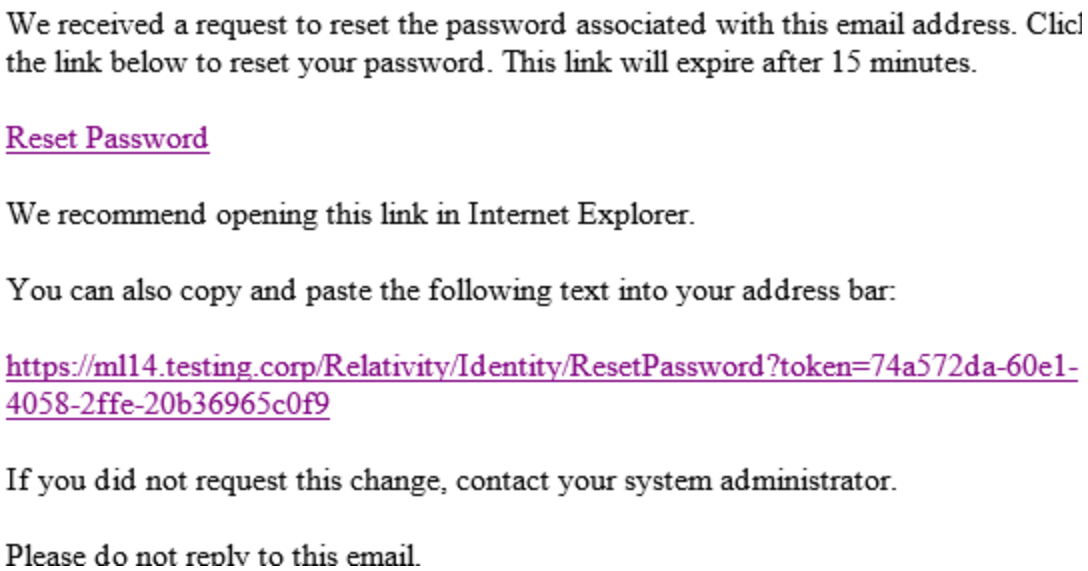
1.2.6 Creating or resetting a password

Use this procedure if you are logging in to Relativity aiR for the first time or if you are resetting your password. Your system admin must send you a password reset email.

Note: Relativity Support cannot reset user passwords. If the "Forgot your password?" link is not displayed on the Relativity aiR login page (which indicates that self-service password recovery has been disabled by a system administrator), you must contact your Relativity aiR system administrator to reset the password. Relativity Support does not perform password resets on behalf of users.

Note: If you are a system admin, the Password Reset Email will not be sent to you. For more information, see the Authentication Guide.

1. Within the password request email, click **Reset Password** or enter the full URL into your browser.


We received a request to reset the password associated with this email address. Clicl
the link below to reset your password. This link will expire after 15 minutes.

Reset Password

We recommend opening this link in Internet Explorer.

You can also copy and paste the following text into your address bar:

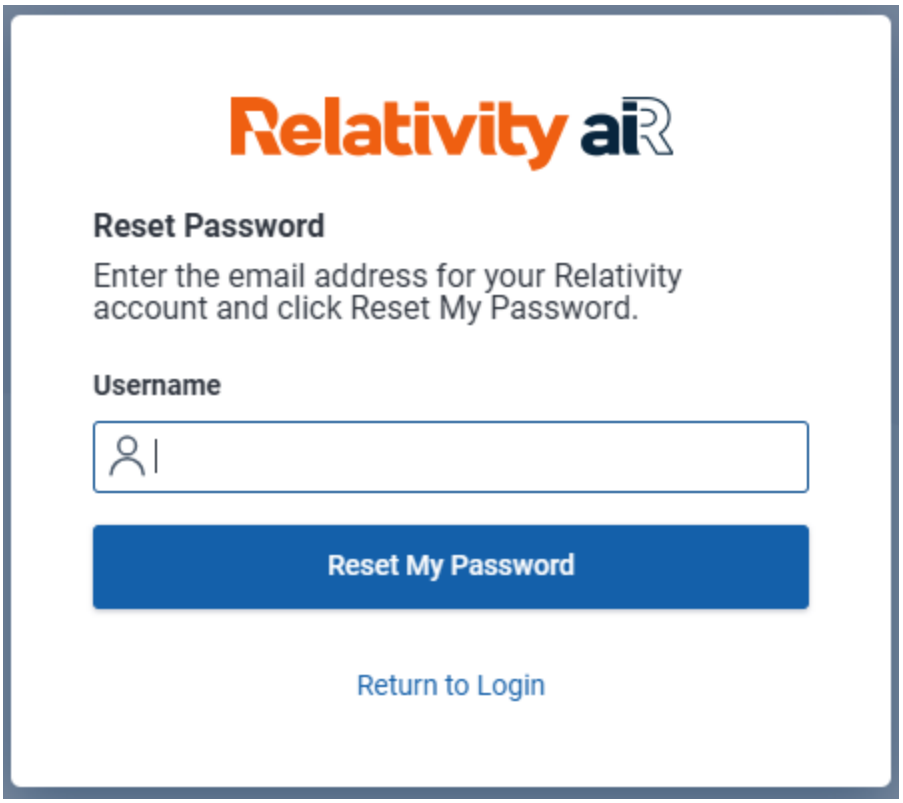
https://ml14.testing.corp/Relativity/Identity/ResetPassword?token=74a572da-60e1-4058-2ffe-20b36965c0f9

If you did not request this change, contact your system administrator.

Please do not reply to this email.

2. Enter a password following the restrictions listed on the screen. You must remember this password to log in. The link within the email is valid for 15 minutes, and you can only use the most recent email. Although, once the password is set, you do not have to log in immediately.

   Note: The following non-alpha-numeric characters are not allowed: \, ", <, >, £ in passwords.



3. Click **Submit**.
4. Click **Return to RelativityOne**.

2 Relativity applications

Relativity applications extend core functionality by providing specialized features or workflows. When you install Relativity, your environment is automatically updated with several applications that are called "system secured."

In addition, you may have workflow requirements or other business needs that require custom applications designed specifically for your organization. Business analysts or third-party developers can implement these applications using Relativity Dynamic Objects (RDOs), the Application Deployment System (ADS), and custom code. For more information about integrations built by Relativity or our Community, see the App Hub.

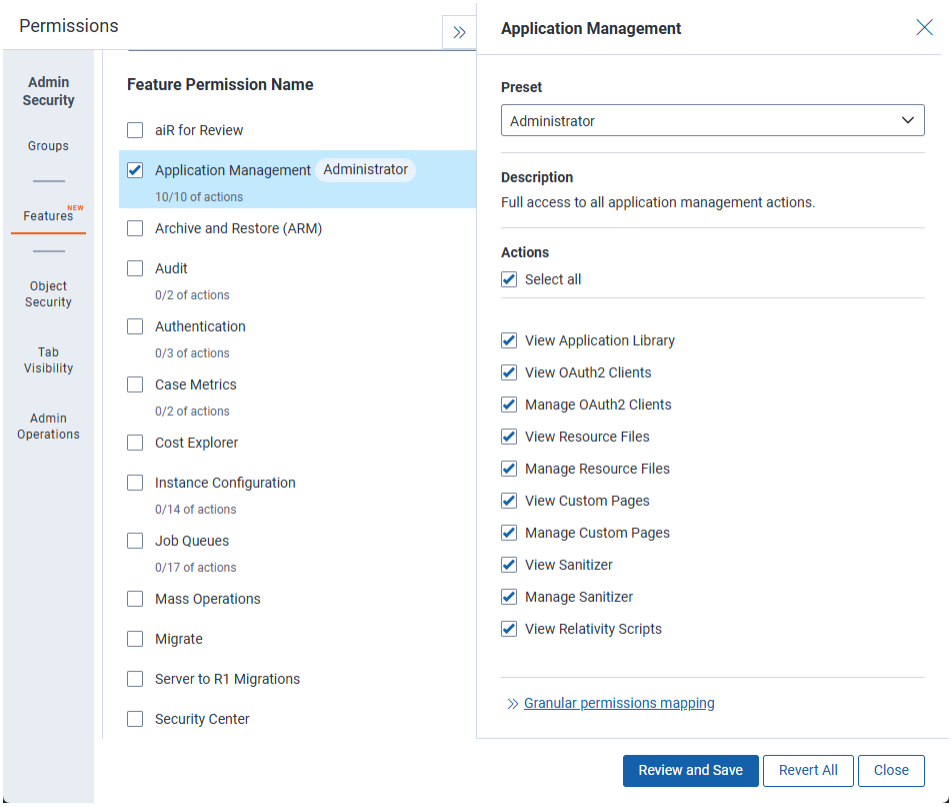
2.1 Permissions

Application administration is an admin-level task. For example, only System Administrators can remove applications from the Application Library.

Installed applications also determine which features you can grant on the Features tab. A feature only appears there when its application is installed in the workspace.

Manage these permissions on the Features tab, under the Application Management feature. Grant a group access by feature, or by individual actions. For an overview of features and actions, see Feature permissions.

The following actions are available for this feature:



2.2 System secured applications

Relativity comes with several key out-of-box features called system secured applications, which you can find in the Application Library or at the workspace level.

In contrast to custom applications, you can't modify or edit system secured applications.

2.2.1 Applications installed in the Application Library

The Application Library tab includes these system secured applications:

- Analytics
- Analytics Core

  Note: The Analytics Core application must be present in all workspaces, and may not be uninstalled.

- Case Dynamics
- Integration Points
- Processing (requires licensing)
- Production
- Conditional Coding Rules
- Legal Hold
- Review Center
- Set Extracted Text Size

2.2.2 Applications installed in workspaces

In a workspace, the Relativity Applications tab includes system secured applications:

- Imaging on page 238
- OCR on page 411
- Lists on page 326
- Search terms reports on page 599

2.3 Relativity custom applications

Custom applications extend the existing Relativity functionality by providing new solutions for case management, review processes, specific workflows, or other business needs for your organization. For example, you might want to develop an application to manage tasks and projects or to facilitate a large-scale review of structured data.

You can implement custom applications using the following features in Relativity:

- **RDOs** - You can develop Relativity dynamic objects that represent real world business entities that your organization uses, such as custodians, contacts, or companies. In addition, you can create custom workflows that use your objects by designing views, layouts, tabs, and other Relativity objects. You don't need any programming experience just the appropriate security permissions to build these objects. For example, the sample application Media Tracker illustrates how to use RDOs, views, and layouts to track content received from vendors, clients, and opposing counsel. See Building Media Tracker with RDOs on the Relativity Documentation Site.
- **ADS** - You can use the ADS to package the RDOs, layouts, views, fields, and other Relativity components that you want included in your custom application. The ADS provides you with a framework available through the Relativity UI for packing the components that you create, as well as custom code developed to add advanced functionality to your applications. By using the ADS, you can export your applications for installation across workspaces and on other Relativity instances. You don't need any programming experience to package your applications with the ADS, but you must have the required security permissions. For more information about the ADS, see the Relativity Developers Site.

  Note: When you add a field with propagation enabled to a custom application and deploy it to other workspaces or instances with ADS, Relativity disables that field on deployment. **Propagation isn't supported by the ADS deployment code**. To keep behavior consistent, don't rely on Propagation for fields you package and push with ADS. Configure those fields without propagation, or apply the equivalent logic through application workflows or custom code after deployment.

- **Custom code** - You can add advanced functionality to your custom applications by developing custom code for event handlers, agents, and custom pages. After building files or assemblies with your custom code, you can easily upload them to Relativity for inclusion in your applications. For more information about event handlers, agents, and custom pages, see the Relativity aiR Developers site.

2.4 Administering Relativity applications

You can perform various admin tasks with custom applications that use the Application Deployment System (ADS). These administrative tasks include installing applications in your Relativity environment, exporting applications for installation on other Relativity environments or for further customization, and removing them from workspaces or your environment.

You can manage custom applications developed with ADS through the Relativity UI by performing these and other tasks:

- **Install applications** - Add custom applications to your Relativity environment by installing them in the Application Library or on individual workspaces. In addition, you can push an application installed on a workspace to the Application Library.
- **Export applications** - Export applications from one workspace for deployment in another workspace. You can also install exported applications in the Application Library on another Relativity instance. In addition, you can export applications for further customization.
- **Uninstall or delete applications** - Remove applications that you no longer need from a workspace. You can choose to delete just the application or uninstall the applications and its related components.
- **Upgrade applications** - Add new or updated features to an existing custom application.

2.4.1 Auditing Relativity applications

The **SystemLastModifiedBy** field on the Relativity Application page identifies the user who last made a major change to the core application object.

Note: This field doesn't update for minor changes such as adding fields, editing items through team-specific interfaces, or adjusting isolated settings because these actions don't affect the core application object.

If you need to track detailed or incremental changes, click the **View Audit** button. It logs a wider range of actions and gives a more complete picture of logged changes in the application. For more information, see Audit.

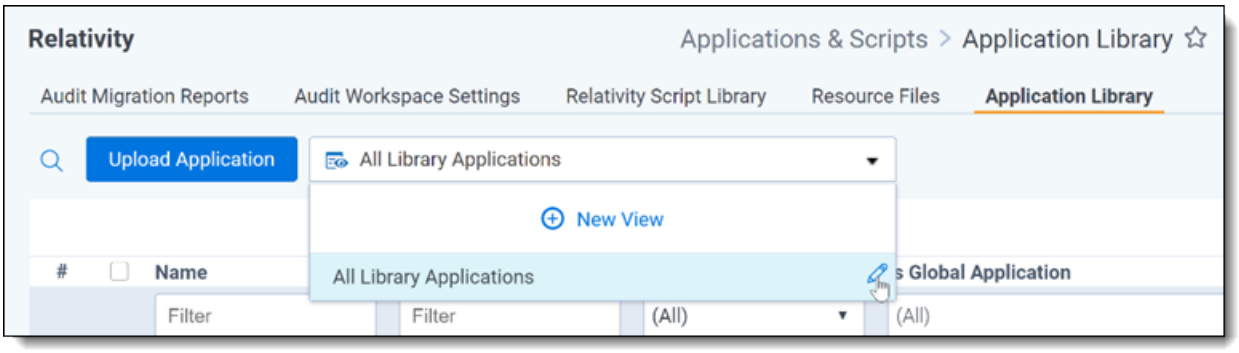
2.5 Global applications

Global applications are applications installed on the admin level of a Relativity instance. Their schema versions are not validated, they don't support RDOs, object-type or workspace-based event handlers.

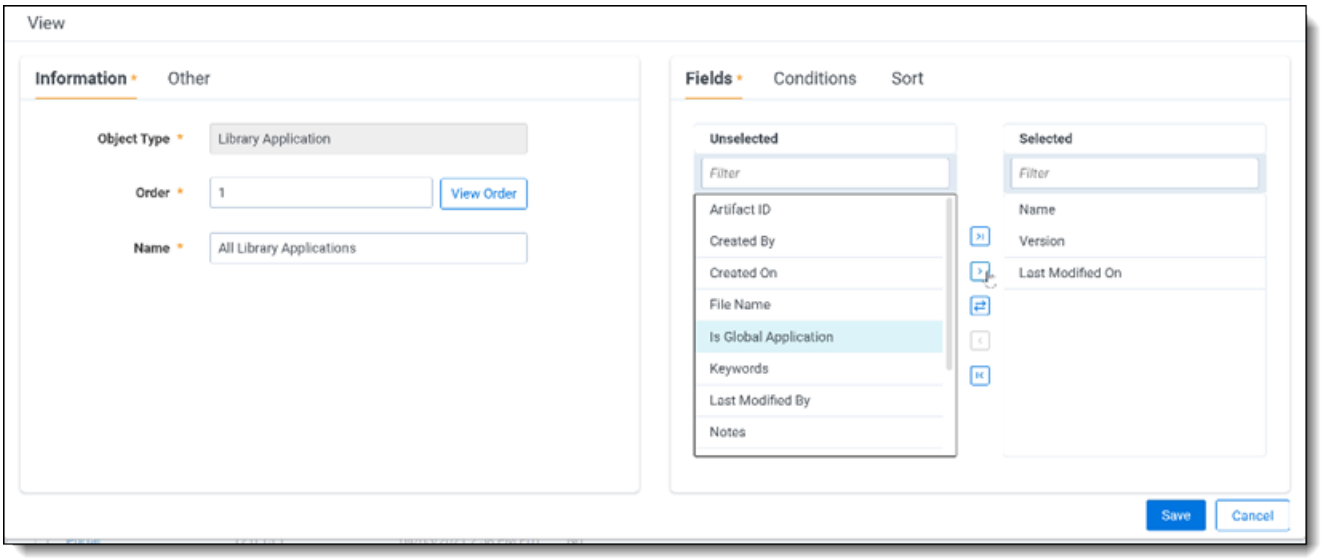
2.5.1 Viewing global applications

Administrators of production environments can view global applications in the Application Library. They cannot install them into workspaces. Complete the following steps to view which applications are applied to the environment globally:

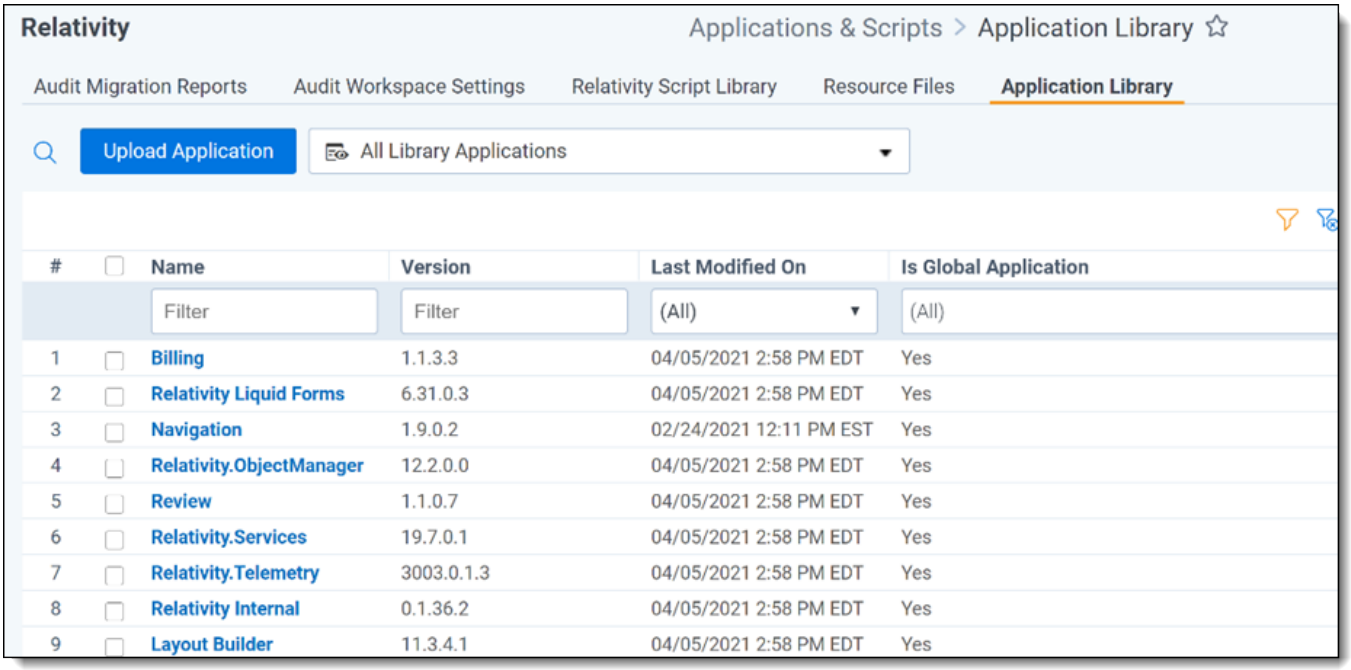
1. Navigate to the **Application Library** tab.
2. In the Views tab in a workspace, click the icon next to All Library Applications.



3. On the right side of the newly opened View window, select **Is Global Application** under **Unselected**.



4. Move the **Is Global Application** in your view to the right box, **Selected**. You can move fields between boxes by:
    - Double-clicking the field name.
    - Using the arrows between the boxes.
5. Click **Save**.
6. The **Is Global Application** column is added to the Application Library.

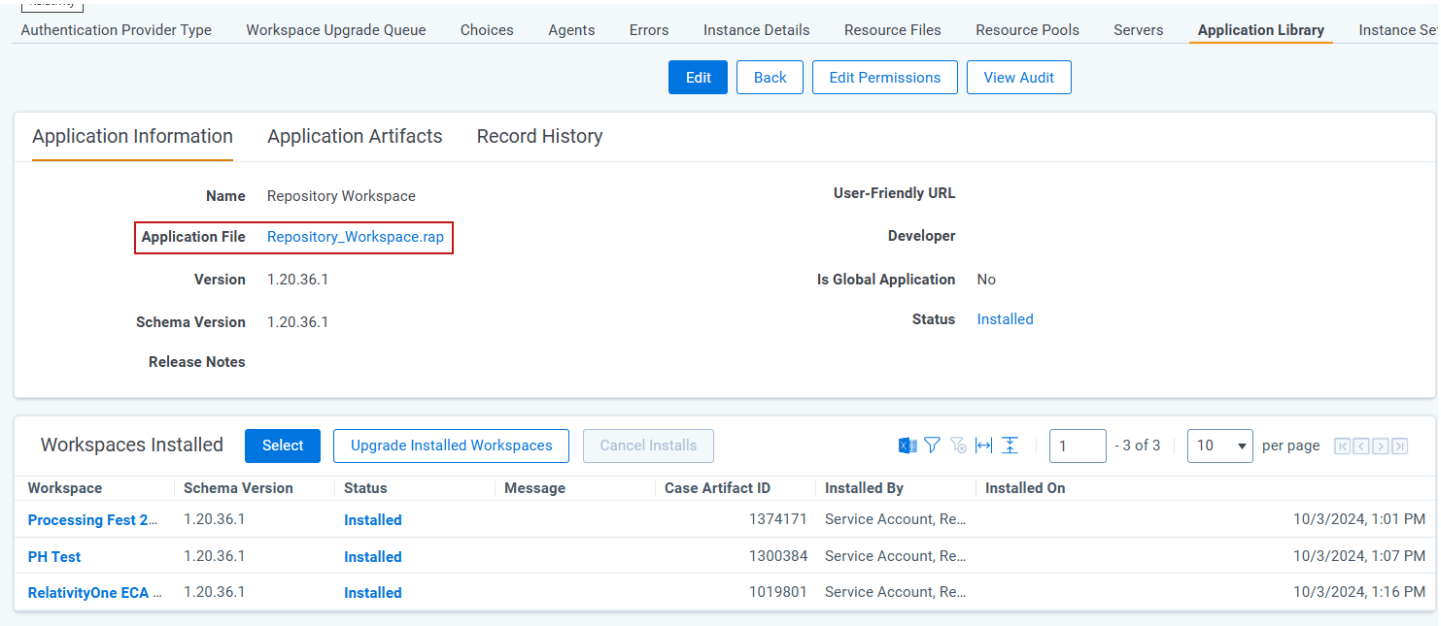


2.6 Exporting applications

You can export applications that you want to install in other workspaces or instances of Relativity. Additionally, you may want to export an application for upgrading in your development environment. You can export applications as RAP files.

2.6.1 Downloading application .rap files

In the Application Library, click on an application to open the details window. You can download the Application File by clicking the link.



2.6.2 Avoiding errors during application export

You can't export an application until you manually resolve all errors listed through the Show Errors link on the application console.

To help you reduce or avoid these errors before you're ready to export the application, consider the following actions:

Object you're adding	Notes for preparing the application for export	Error you'll avoid
Object type	Make sure the Dynamic field on all object types you add to the application is set to Yes.	Object Type <Name of Object Type> is not exportable because it is not dynamic.
	Add all object types to the application before adding event handlers.	The <Name of Object Type> object type is associated with the <Name of Event Handler> event handler. Please add the object type to your application in order to proceed.
	Add the objects to the application before adding the fields.	The <Name of Object> object associated with Document field <Name of Field> is required in order to proceed. Please add this object to your application.
	Add all layouts to the application before adding the object types.	The <Name of Object> object that owns the <Name of Layout> layout must be added to your application in order to proceed.
Tab	Make sure none of the tabs you link to from your application are parent tabs.	The <Name of Tab> tab is a parent tab. Parent tabs cannot be included in an application. If your application contains any non-parent tabs they will be placed under an auto-generated tab named after the application on install. Please remove this tab from your application to proceed.

Object you're adding	Notes for preparing the application for export	Error you'll avoid
	Add all object types to your application before adding tabs separately.	The <Name of Tab> tab is associated with the <Name of Object Type> object type. Please add this object type to your application in order to proceed.
View	Add the views to the application before adding the layouts and fields.	The <Name of View> view includes the following field(s): Field X, Field Y, etc. Please add the field(s) to your application in order to proceed.
	Add the views to the application before adding the layouts and fields.	The <Name of View> view is referenced in the <Name of Layout> layout. Please add this view to your application in order to proceed.
	Add all views to the application before adding the object types, with the exception of any non-dynamic object types.	The <object type> associated with the <view name> is required in order to proceed. Please add this object to your application.
Layout	Add the layouts to the application before adding the fields.	The <Name of Layout> layout includes the following field(s): Field X, Field Y, etc. Please add the field(s) to your application in order to proceed.
	Add the views to the application before adding the layouts and fields.	The <Name of Layout> layout includes popup pickers using the following view(s): View X, View Y, etc. Please add the view(s) to your application in order to proceed.
Field	Make sure all views, including relational views, are added to the application before you add the fields.	The field <Name of Field> is a relational field. The view, Family Documents, associated with this relational field must be added to your application in order to proceed.
	Make sure all unsupported fields are removed from the application.	Relativity applications don't support the Batch::Assigned To field. Remove Batch::Assigned To field from your application to proceed.
	Add all fields to your application before adding the choices with which they are associated.	The Handler associated with the choice <Name of Choice> is required in order to proceed. Please add this field to your application.
	Remove all system fields from the application.	The Document field <Name of Field> is a System field. You must remove this field from the application in order to proceed.
	Add all fields to the application before adding object types, with the exception of any non-dynamic object types.	The <object type> associated with the <field name> is required in order to proceed. Please add this object to your application.
Dashboard	Make sure all the fields found in the dashboards you include in the application are added to the application.	The <Name of Dashboard> dashboard associated with the <Name of Object Type> object type includes the following field(s): Field X, Field Y, etc. Please add the field(s) to your application in order to proceed.

Object you're adding	Notes for preparing the application for export	Error you'll avoid
Agent	Make sure the correct agents are attached with the application.	<Name of Agent> agent is not assigned to the correct application domain.
Rule	Add all object types to your application before adding object rules separately.	The <Name of Rule> Object Rule is associated with the <Name of Object Type > Object Type. Please add the Object Type to your application in order to proceed.
Saved Search	Add all choices to the application before adding the saved searches.	The <Name of Saved Search> saved search is associated with the <Name of Choice> choice. Please add this choice to your application in order to proceed.
	Add all fields to the application before adding the saved searches that contain them.	The <Name of Saved Search> saved search includes the following field(s) in its conditions: Field X, Field Y, etc. Please add these field(s) to your application in order to proceed.
Event Handler	Make sure all event handlers that you intend to add to the application are correctly configured.	Event Handler <Name of Event Handler> is not assigned to the correct application domain.
Mass Operation	Add all object types to the application before adding the mass operations with which they are associated.	The <Name of Mass Operation> mass operation is associated with the <Name of Object Type> object type. Please add the Object Type to your application in order to proceed.
System Artifact	Remove all system artifacts from the application.	You have included one or more System Artifacts in the application. You must remove these artifacts to proceed: Artifact X, Artifact Y, etc.

2.6.3 Application state settings on export

When you export an application, Relativity automatically updates the following state settings on the application:

- **Locking** - Relativity automatically locks any unlocked applications on export. See Locking and unlocking applications.
- **applicationIsDirty flag** - Relativity automatically resets the **applicationIsDirty** to false on any unlocked applications with the applicationIsDirty flag set to true. The value of false indicates that application is in a clean, unedited state. This flag determined the type of upgrade required for an application installed in a workspace.
- **Application version** - Relativity increments the revision number of the application version with each export if the application is unlocked, the application schema has been modified, or if Developer Mode is enabled.
-

Additionally, Relativity automatically increments the version of any application that contains saved searches, which have been modified. For more information, see Modifying saved searches in a locked application on the Relativity RelativityaiR Documentation site.

2.6.4 Exporting an application

During export, Relativity automatically assigns a version number to any application that doesn't already have a version.

Note: If you are writing custom code, you can also use the Export API to export an application programmatically. For more information, see Export (.NET) on the Relativity aiR Developers site.

Use the following procedure to export an application:

1. In the target workspace, select the **Relativity Applications** tab.
2. Click the name of the application that you want to export.
3. Click **Export Application** in the **Application Console**.



4. If your application contains external resources, click **Export** on the Confirm Application Export dialog. Relativity only displays this dialog for applications with external resources, such as custom pages. It exports those applications as a RAP files.

   Note: If you export an application with a Single or Multiple Choice field without choices, you receive a message asking if you want to continue with the export. Click **OK** on this message dialog.

5. Click **Save** or **Save As** to download the file to your selected location.
6. Click **Refresh Page** in the **Application Console**. You can find the RAP file for your application in the folder that you selected. Upload this file to the workspace or Relativity instance where you want to deploy the application.

2.7 Locking and unlocking applications

In Relativity, you can edit applications by unlocking them. You can also lock applications to prevent any modifications to them. On the Relativity Application tab, use the **Lock Application** and **Unlock Application** buttons to perform these operations. You need the appropriate system admin permissions to lock or unlock an application. For more information, see Workspace security.

You can't lock or unlock system secured applications that are shipped with Relativity. The Relativity Application tab doesn't display these options for system secured applications. See System secured applications.

2.7.1 Locking an application

You can't edit a locked application or any of its components except for saved searches, layout, views and default tab. On the details view of the application, you can't add new components to an application, delete them, or unlink them. On the details view of a specific component, you can't edit any of its fields without receiving an error message.

For example, you attempt to modify a locked application that contains a custom Entities object. Because the application is locked, you can't remove this object from the application through its details view. You also can't add or remove a field from the Entities object through its details view. For information about saved searches, see Customizing locked applications on the next page. For information about layouts, views, and default tab, see Customizing locked applications on the next page.

If you attempt to edit any of the following components in a locked application, you receive an error message:

- Choice
- Field
- Layout
- Object Type
- Relativity Script

- Tab
- View
- Dashboard

Note: Relativity automatically locks an unlocked application on export. See Exporting applications.

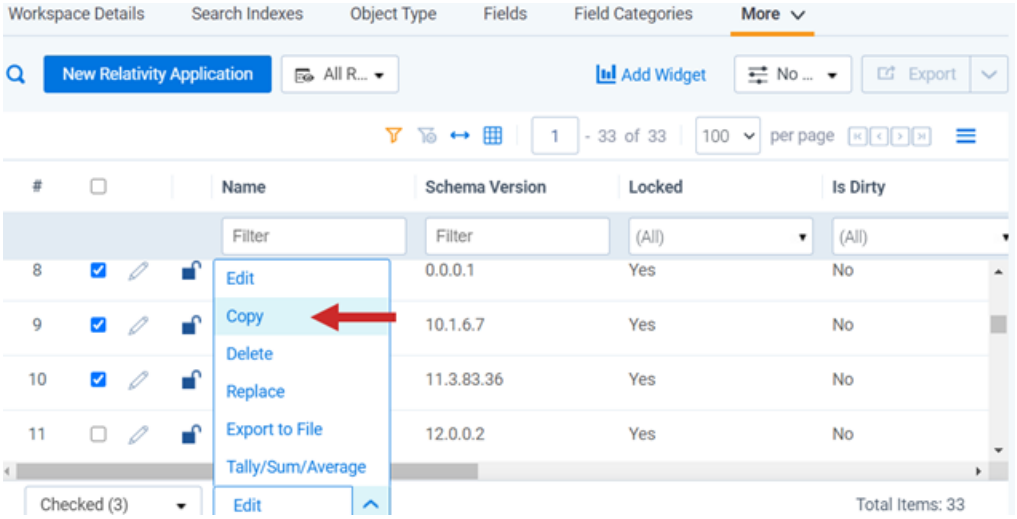
Use the following procedure to lock an application:

1. Navigate to the workspace containing the application that you want to lock.
2. Click the **Relativity Applications** tab.
3. Click the name of the application that you want to lock.
4. Click **Lock Application** in the Application Console.

2.7.2 Customizing locked applications

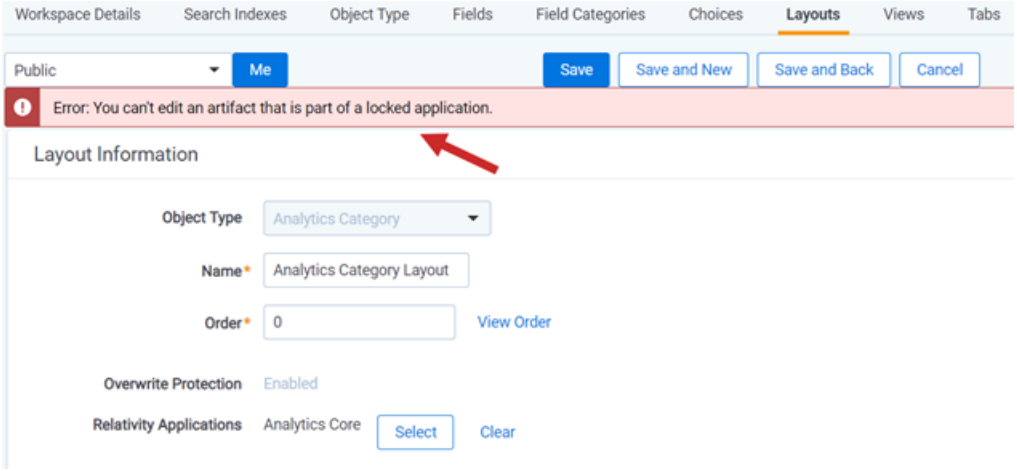
You can make the following customizations to locked applications without unlocking the application:

- You can set a tab in a locked application as the default tab for the workspace.
- You can use the Copy mass operation to copy views and layouts in a locked application.



  - The copied views and layout are identical to the original and can be customized.

- When you open views and layouts in a locked application, Relativity displays a user-friendly alert:



If you later upgrade the application, Relativity preserves any changes made to the customized layouts, views, and default tab.

2.7.3 Modifying saved searches in a locked application

You can perform the following tasks to modify saved searches included in locked applications:

- Move a saved search to a different folder in the saved searches browser. For more information, see Saved search on the Relativity RelativityaiR Documentation site.
- Change the index type for a saved search.

If you later upgrade the application, Relativity preserves any changes made to the saved searches. It also increments the version when you export an application with modified saved searches.

2.7.4 Unlocking an application

When an application is unlocked, you can add components to it, delete them, or unlink them. You can also edit the fields on any the components in an unlocked application. For example, you want to modify an unlocked application with a custom view. You can add or remove columns from the view when you unlock the application. Consequently, you only want to unlock an application when you purposely want to update it.

The RelativityApplication object has the **applicationIsDirty** property. This property is set to true when you unlock an application. The current state of an unlocked application is unknown because users may inadvertently modify it. The **applicationIsDirty** property also determines the type of upgrade installation required for an application in a workspace.

Use the following procedure to unlock an application:

1. Navigate to the workspace containing the application that you want to unlock.
2. Click the **Relativity Applications** tab.
3. Click the name of the application that you want to unlock.
4. Click **Unlock Application** in the Application Console.
5. Click **OK** on the confirmation message. You can now edit the application by adding or removing components. In addition, you can update individual components by adding, removing, or making other changes to their fields.

2.8 Installing applications

Relativity provides you with several different options for installing applications. You can:

- Install an application that exists as an external file to the Application Library. The application becomes available for installation to all workspaces. This is useful for when you need to install an individual application .xml file or .rap file to multiple workspaces that Relativity support provided to you. For more information, see Installing an application from an external file to the Application Library below.
- Push an application that exists in a single workspace to the Application Library, so the application is available for installation to other workspaces. This is useful for when you install an individual application .xml file or .rap file to a single workspace, and then decide to install the application to other workspaces. For more information, see Pushing an application from a workspace to the Application Library below.
- Push an application from the Application Library to one or more workspaces. For more information, see Pushing an application from the Application Library to a workspace below.
- Install an application from the Application Library to a workspace. This is the standard route of adding an application after you install or upgrade to a new version of Relativity and have access to the most up-to-date Application Library. For more information, see Installing applications from the Application Library on the next page.
- Install an application that does not exist in the Application Library to a workspace as an external file. This is useful for when you need to install an individual application .xml file or .rap file that was not included in a Relativity upgrade or installation to a single workspace. For more information, see Installing an application from an external file to a workspace on page 63.

2.8.1 Installing applications to the Application Library

You can add applications across multiple workspaces by installing them to the Application Library. You can do this by installing applications as external files or pushing them from a single workspace.

2.8.1.1 Installing an application from an external file to the Application Library

If you're a Relativity aiR customer, and you wish to install an application from an external file to the Application Library, contact Support before doing so, as your application may require agent configuration or other infrastructure components.

2.8.1.2 Pushing an application from a workspace to the Application Library

When you want to add any application in a workspace to the Application Library, you can use **Push To Library** available on the detail view of an application. You can then install the application to workspaces throughout your Relativity environment. In Relativity, confirm that you have the appropriate system admin permissions to install an application. For more information, see Workspace security on page 622.

Note: You override any existing applications with the same GUID when you push an application from a workspace to the library.

1. Navigate to a workspace where the application you want to add to the Application Library is installed.
2. Click the **Relativity Applications** tab.
3. Click the name of the application to display its detail view.
4. Click **Push To Library** in the Relativity Application console.

2.8.2 Pushing an application from the Application Library to a workspace

To install an application from the Application Library to one or more workspaces, perform the following steps:

See an animated GIF of the installation steps

1. Navigate to the **Application Library**.
2. Open the application you wish to install on at least one workspace.

3. In the **Workspaces Installed** list, select **Install to All Workspaces** or select the workspaces you want to install the application to through the following steps:
    a. Click **Select**.
    b. In the column on the left, select the workspaces you want to install the application to.
    c. Use the single arrow between the columns to move the selected workspaces over to the column on the right.
    d. Click **Apply**.
4. Verify that the workspaces show up in the associated list view below with an initial status of **Pending installation** and then a status of **Installed**.

Once installation is complete, navigate to any of the workspaces you selected, select the Relativity Applications tab, and verify that the application was installed.

2.8.3 Installing applications to workspaces

You can install applications to workspaces from the Application Library tab or by importing an external application file.

Note: When you install an application, all components are public regardless of the permissions that you assign to them in your application. The ADS framework ignores any permissions or security assigned to a component added to an application during deployment in a workspace.

2.8.3.1 Installing applications from the Application Library

If you added the application to the Application Library, you can install it to the current workspace without importing an external file to Relativity. In Relativity, confirm that you have the appropriate system admin permissions to install an application. For more information, see Workspace security on page 622.

Use the following procedure to install an application from the Application Library:

1. Navigate to a workspace where you want to install the application.
2. Click the **Workspace Admin** tab and the **Relativity Applications** tab.
3. Click **New Relativity Application** to display an application form.
4. Click the **Select from Application Library** radio button in the Application Type section.

    Note: Global applications are not listed in the **Select from Application Library** option when attempting to add an application to a workspace.

5. Click  in the **Choose from Application Library** field.
6. Select the application that you want to add to your workspace on the Select Library Application dialog. This dialog displays only applications added to the Application Library.
7. Click **Ok** to display the application in the **Choose from Application Library** field. The application form also displays the following fields:
    - **Version**—displays the version of the application that you are installing.
    - **User-friendly URL**—displays a user-friendly version of the application's URL. This field may be blank.
    - **Application Artifacts**—displays object types and other application components.
8. (Optional) Click **Clear** to remove the application from the form.

9. Map fields if necessary to prevent installation errors. If your application does not contain any fields corresponding to those currently in the workspace, the following message displays. Otherwise, the Map Fields section displays a mapping grid. For more information, see Mapping fields on page 65.



10. Click **Import** to save your mappings and import the application.
Relativity installs the application into the workspace.
11. Review the import status of the application. Verify that the install was successful or resolve errors. See Viewing import status on page 66 and Troubleshooting application installation errors on page 67.

2.8.3.2 Installing an application from an external file to a workspace

You can install an application to the current workspace by importing an external file if the application has not been added to the Application Library tab. Relativity automatically stores shared components the application uses in the Application Library and overwrites any lower versions. Shared components may include event handlers, scripts, custom pages, mass operations, or agents. In Relativity, confirm that you have the appropriate system admin permissions to install an application. For more information, see Workspace security.

Note: You can also use the Application Install API to import an application programmatically. For more information, see Application Install (.NET) on the Relativity aiR Developers site.

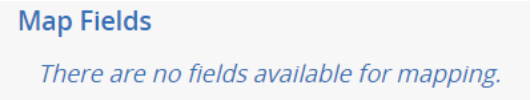
Use the following procedure to install an application from an external file:

1. Navigate to a workspace.
2. Click the **Relativity Applications** tab.
3. Click **New Relativity Application** to display an application form.
4. Click **Import from File** in the Application Type section.
5. Click  in the **File** field to browse for the application file.

Note: Relativity Applications use .rap files. If you upload the wrong file type, the following error message appears: *The uploaded file is not a valid Relativity Application file*.

If the application includes a custom page of a restricted file type, you receive an error message and cannot install the application. See Best practices for custom pages on the Relativity aiR Developers site.

6. Click **Open** to upload the file to Relativity. The application form displays the following fields:
   - **Application Name**—displays the name of the application.
   - **Version**—displays the version of the application you're installing.
   - **File Name**—displays the name of the application file. To remove the file from the form, click **Clear** in this field.
7. Expand the tree to view the artifacts associated with your application in the Application Artifacts section. This hierarchy tree includes Object Types, External Tabs, Scripts, Custom Pages, Agent Types, as well as Pre and Post Install Event Handlers contained in your application.
8. Map fields if necessary to prevent installation errors. If your application does not contain any fields corresponding to those currently in the workspace, the following message displays. Otherwise, the Map Fields section displays a mapping grid. For more information, see Mapping fields on page 65.



9. Click **Import** to save your mappings and import the application. Relativity installs the application into the workspace.
10. Review the import status of the application. Verify that the install was successful or resolve errors. See Viewing import status on page 66 and Troubleshooting application installation errors on page 67.

2.8.3.3 Installing applications containing saved searches

Relativity applications may contain saved searches that use keyword, dtSearch, and Analytics indexes. When you install the application, Relativity creates the folder structure used to organize the searches in the saved search browser of the workspace. It adds the saved search to the correct folder by matching the globally unique identifier (GUID). If it does not find a match, Relativity continues to traverse the folder structure to the root before creating the required folder. Otherwise, it adds any new or updated saved searches to the existing folder with the matching GUID, even if the user has moved the folder to a new location in the saved search browser. For more information, see Customizing locked applications on page 59.

Note: While Relativity 9 and above assigns a GUID to any saved search added to an application, older versions of Relativity do not use GUIDs to identify saved searches. You can build an application using a saved search in a template workspace created before upgrading to Relativity 9 or above. However, deploying your application in a workspace created with this template results in duplicate copies of the saved search. Since Relativity identifies saved searches by GUID, it does not recognize that the legacy search in the workspace is the same as the search in the application, so it creates a new one with the matching GUID.

In general, you install these applications following the same steps used for other applications, but you may want to complete the verification steps before you install them in a workspace. If the workspace does not contain a dtSearch or an Analytics index with the same name as the one included in the application, Relativity creates it using the system defaults. The post-installation steps require you to build the index after Relativity completes this process. For information about building applications with saved searches, see the Creating an application in Relativity on the Relativity RelativityaiR Developers site.

Note: When you install an application, all saved searches are public regardless of the permissions that you assigned to them in your application or folder structure. The ADS framework ignores any permissions or security assigned to a saved search added to an application during deployment in a workspace.

Before you begin

You may want to complete the following verification steps before you install an application containing saved searches using dtSearch and Analytics indexes to avoid possible errors:

- **Saved searches using dtSearches**—confirm that a file share for this index type exists in your environment. The Relativity installer requires you to create this file share during the installation of the primary SQL Server. For more information, see Relativity installation on the Relativity RelativityaiR Documentation site.
- **Saved searches using Analytics indexes**—confirm that an Analytics server is installed in your Relativity environment. For more information, see Upgrading or installing Analytics on the Relativity RelativityaiR Documentation site.

Installation steps

To install the application, follow the instructions in Installing applications from the Application Library on page 62 or Installing an application from an external file to a workspace on the previous page.

Post-installation steps

If your workspace already contains a dtSearch or Analytics index, Relativity automatically maps it to the saved search using the index name and type. It ignores any spaces or case differences in the index name.

If your workspace does not contain an index with a matching name or type, Relativity creates a shell for a dtSearch or Analytics index. You need to complete one of the following steps to build the index:

- **dtSearch index**—navigate to the Search Indexes tab in Relativity, and click the **Edit** link for your dtSearch index. Select settings for the **Order**, **Searchable set**, **Index share**, or other fields as necessary, and save your changes. Next, build the index by using **Build Index: Full** option on the index details page. For more information, see dtSearch on the Relativity RelativityaiR Documentation site.
- **Analytics index**—navigate to the Search Indexes tab in Relativity, and click the **Edit** link for your Analytics index. Select settings for **Analytics profile**, **Analytics server**, **Data source**, **Training data source**, and fields as necessary. Next, build the index. For more information, see Analytic Indexes on the Relativity RelativityaiRDocumentation site.

2.8.3.4 Mapping fields

When you import an application, you can optionally map the fields that are similar to those in an application currently installed on the workspace. You can use mapping to avoid having multiple copies of a field that stores similar information in your workspace.

For example, you might import a new application that contains a long text field on a Document object called *Email Cc*, but your workspace already contains another application with a similar field on the Document object called *Email Cc Addresses*. Instead of two fields storing similar information, you might want all applications to use the same field for this metadata. By mapping these fields, you can avoid renaming the new field and using two different fields to store this metadata in your workspace.

Use these guidelines when mapping an application to workspace fields:

- **Fixed length text fields**—you can map application fields of this type only to workspace fields of equal or lesser length. Workspace fixed text fields that have a length longer than the application fields are not displayed in the Workspace Fields column of the mapping interface.
- **Renaming fields**—you can rename a field after you map it without impacting future application upgrades.
- **Renaming fields and exporting**—if you rename a field in an application installed on Workspace A, and then export the application, this field is still renamed when you import the application to Workspace B. This practice does not apply to Document System Fields.
- **Target workspace fields renamed**—when you map an application field to a workspace field, the application renames the workspace field to match the application field. The application now owns the field.
- **Handling of removed components**—if you remove a component from an application installed in Workspace A, and the export the application, this component is still part of the application when you import it to Workspace B. In other words, the component that you removed from Workspace A imports to Workspace B. Application components include choices, fields, object rules, and others.

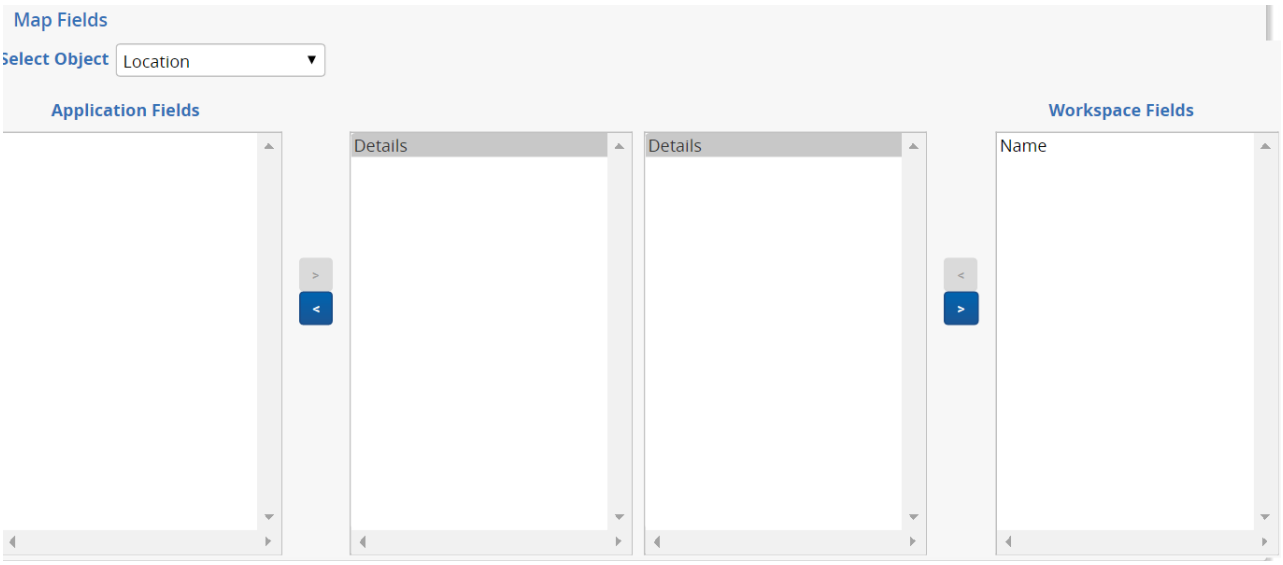
Use the following procedure to map application fields to workspace fields:

1. Complete the steps for installing an application described in the previous sections.
2. Locate the Map Fields section on the application form. The Map Fields section displays the mapping interface if the application contains fields corresponding to those in the workspace.



3. Complete these steps to map the available application fields of your choice through the Field Mapping interface:
    - Highlight a field in the Application Fields box, and then click the arrow to move it to the center box. The Workspace Fields box displays the fields in the target workspace that may match the application field. The Workspace Fields box does not display any fields when no matches exist.
    - Highlight a field in the Workspace Fields box, and then click the left arrow to move it to the center box.

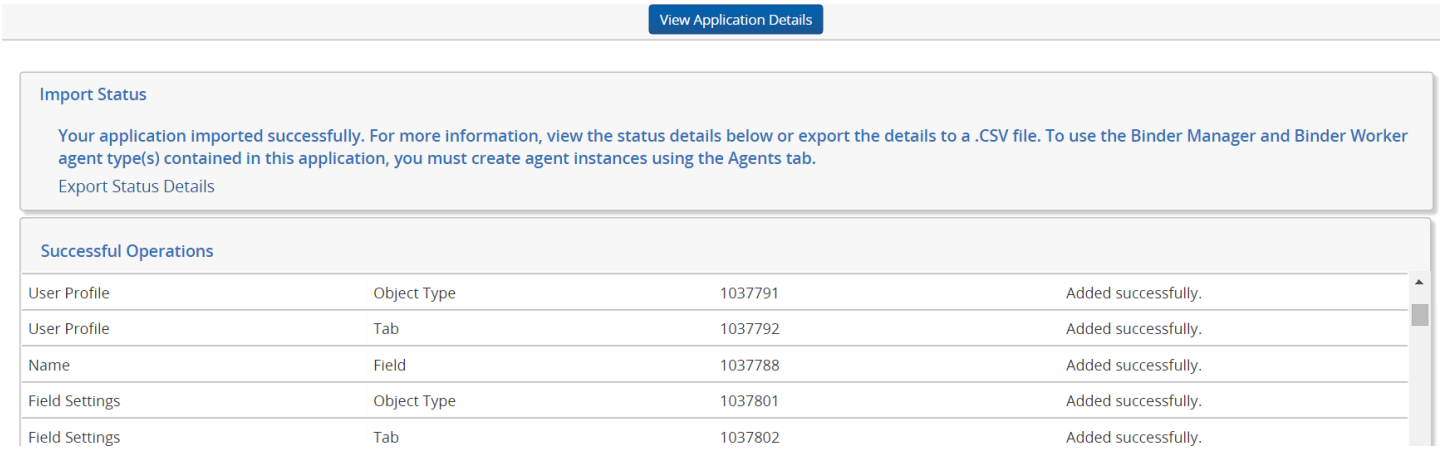
    Note: You can also double-click a field name to move it to a mapping box. To remove a field from the mapping box, use the left arrow for the application fields, and right arrow for the workspace fields.



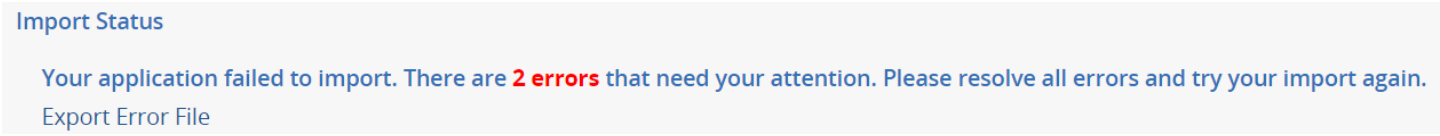
2.8.3.5 Viewing import status

After you install an application through the Relativity Application tab, you can view the status page, which appears immediately after this process completes. The **Import Status** section indicates whether your installation was successful.

The Artifact Name section displays a list of all the artifacts in your application, which includes its Artifact Type, Artifact ID, and installation status. For artifacts installed without errors, the Status column displays the message *Updated successfully*.



For unsuccessful installations, the Import Status section indicates that your application installation failed as illustrated in the following message. The message lists the number of errors encountered during the installation. In addition, the Status column describes each error that occurred during a failed installation. For more information, see Troubleshooting application installation errors.



To export the Status section report to a .csv file, you can click the **Export Status Details**. You can also view status information for the installation of an application from the Application Library tab. Click on an application to display a detail view, and then click its **Installed** link to display the status page.

2.9 Troubleshooting application installation errors

You can use this page to identify the causes of common application installation errors.

2.9.1 Installation error list

Use the following table to identify common causes of errors that may occur when you attempt to install an application. You can resolve some of these errors manually through the target workspace or you may be able to resolve them as you install the application.

Error sources	Possible resolutions
Application contains duplicate Object Type or field names	• Rename the item in the target workspace • Rename the item in the application • Remove the item from the application • Remove the item from the target workspace • Map fields before installing
Application file contains a relational field that uses a friendly name that a relational field in the target workspace already uses	• Change the friendly name of the relational field in the target workspace

Error sources	Possible resolutions
	• Change the friendly name of the relational field in the application • Map fields before installing
Application contains an Object Type that already exists in the target workspace inside a locked application	• Unlock the application in the target workspace • Remove the object type from the application
Application has a malformed file	• Re-export the application and try again
Application contains an external resource of a restricted file type	• Remove the external resource from the application and re-install

2.9.2 Resolving installation errors

You can resolve conflicts through the Import Status page without having to modify the application or its artifacts in the current workspace. This page displays errors by type, such as locking errors, name conflicts, or other errors.

You can view the Artifact Name, Artifact Type, and Artifact ID of the component associated with an error, as well as the error status. In the artifact status section, you may have the option to resolve an error before retrying the installation. Error resolution options vary according to error type.

After you finish resolving errors, click **Retry Import**. Relativity disables this button until you resolve all the errors.

2.9.2.1 Locking conflicts

To resolve a locking conflict, select the **Unlock** checkbox, and then click **Retry Import**.

You can use this operation to temporarily unlock the application while you resolve a locking conflict during installation. After you successfully import the application, Relativity locks the application again so that you can't inadvertently modify it. See Locking and unlocking applications.

2.9.2.2 Name conflicts

You can rename the conflicting artifact so that you can import the components of your application.

Use the following procedure to resolve these errors:

1. Select an option in the **Resolve Errors** drop-down menu. Available options include Rename and Map Field.
2. Perform one of the following tasks:
   - **Rename** - Enter a new name in this field to resolve the Name Conflict error. When you've entered a valid name, a green check mark appears next to the new name field.
   - **Map Field** - When you select this option, Relativity automatically maps the field that you're importing to the conflicting field in the target workspace.

2.9.2.3 Other errors

For other errors, the Resolve Errors column may display a message that you can only resolve the error manually in the workspace. You must resolve the issue in the target workspace before proceeding with the application import.

2.9.3 Pre and Post Install event handler errors

Your applications may contain custom code for Pre and Post Install event handlers that run during installation. These event handlers configure your Relativity environment so that it can support your applications. If an error occurs while the event handlers are running, the application fails to install. The third-party developer who created your application may provide custom error messages to help you resolve these types of installation failures.

2.9.3.1 Failure of Pre Install event handler

When a Pre Install event handler fails, you may receive an error message that indicates the status of the event handler.

In this case, follow the instructions provided in the message. After you resolve the error, reimport the application.

2.9.3.2 Failure of Post Install event handler

Post Install event handlers execute after the Application Deployment System (ADS) has updated all of the components in the application. When a Post Install event handler fails, an error message appears on the details view of the application.

2.9.4 Checking the error statuses

When a Pre or Post Install event handler fails from the Application Library, you can check the status of that error.

Use this procedure to check the error statuses:

1. From **Home**, click the **Application Library tab**.
2. Click on the name of your application.
3. In the Workspaces Installed section, locate the workspace containing the application with errors, and then click the **Errors** link to display a pop-up containing an import status message.
   You can review the error message returned by the failed event handler during the last installation attempt.

2.10 Uninstalling and deleting applications

You can control the applications that workspaces contain by exporting, uninstalling, and deleting them. When you export an application, you have a file that you can use to import it into other workspaces. You can also uninstall or delete applications that you no longer want in a workspace.

2.10.1 Uninstalling applications

When you uninstall an application, Relativity deletes all child objects and associative objects, unless other applications or dependencies prevent their removal. Relativity also deletes any saved searches your application includes, but retains the associated indexes in the workspace because they are not part of the application. You need system admin permissions to lock or unlock an application. For more information, see Workspace security.

For example, you might need to uninstall an application that you accidentally deployed to a template case. If you want to remove only the application instance or if you created an application that you haven't added to the library, consider deleting it instead of uninstalling it. See Deleting applications on page 71.

Note: Applications installed via the Application Library can only be removed by System Administrators.

2.10.1.1 Uninstalling an application

Use the following steps to uninstall an application.

To ensure optimum performance of Relativity, uninstall applications only during off-hours when users aren't actively reviewing documents in any workspaces.

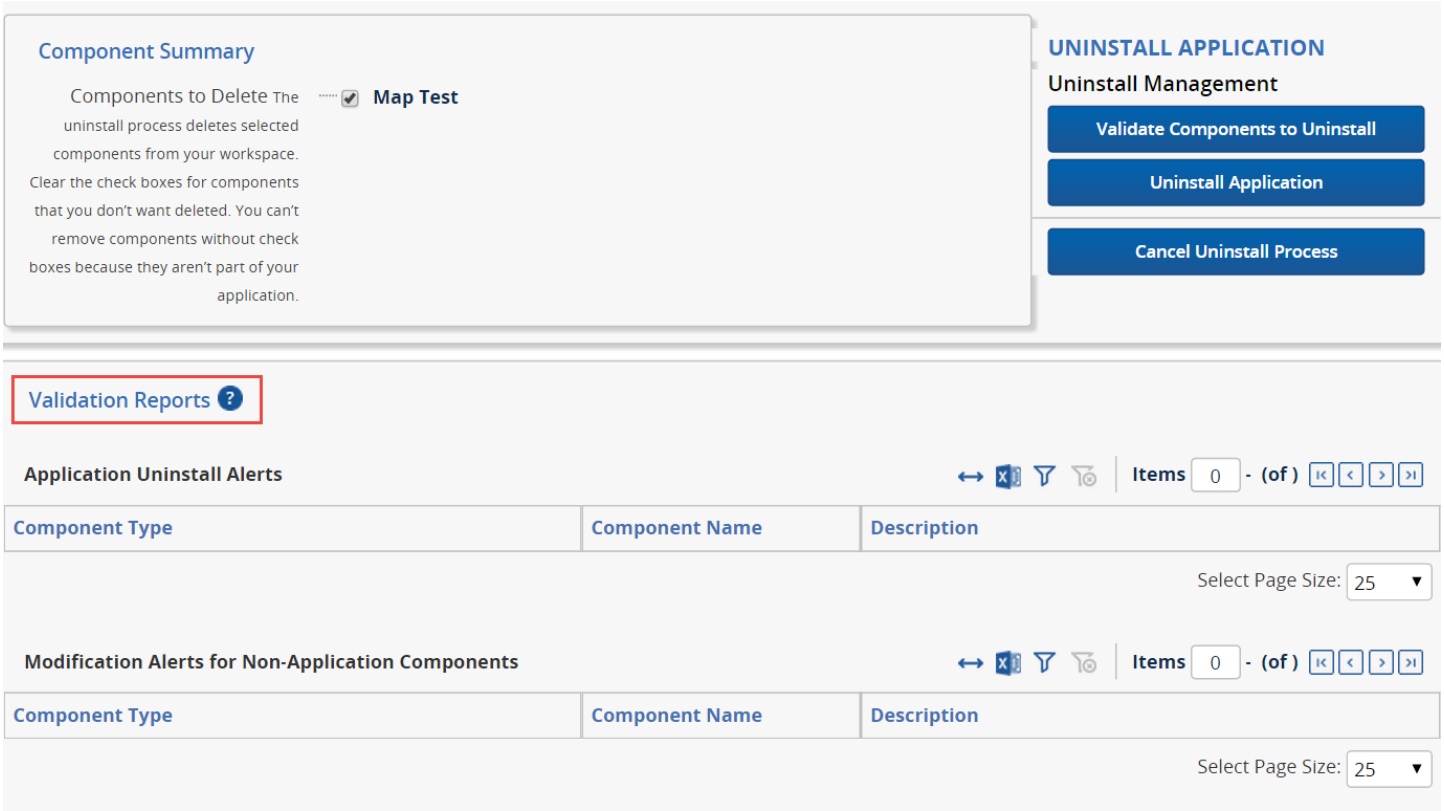
1. Select the **Relativity Applications** tab in the workspace that contains the application you want to uninstall.
2. Click the application name to display the details view.
3. Click **Unlock Application**, if necessary. You can't uninstall a locked application.
4. Click **Uninstall Application** to display the Component Summary page. This page lists object types fields, event handlers, custom pages, and other components of your application.
5. (Optional) Click  to expand the list of components. The hierarchy tree shows the parent-child relationships for component types in your application.
6. (Optional) Clear the check box for any components that you don't want to uninstall.
7. Click **Validate Components to Uninstall** to view the Application Uninstall Alerts and Modification Alerts for Non-Application Components reports. See Uninstall and modification alerts below.
8. Click **Uninstall Application**. When the confirmation message appears, click **Yes** to complete uninstalling the application. You can manually uninstall custom pages if your application includes these components. See Manually uninstalling custom pages on the next page.

2.10.1.2 Uninstall and modification alerts

The process of uninstalling an application deletes the same components that you would delete manually through the Relativity UI. When you delete components manually, Relativity provides you with the option to view a dependencies report. You can also view reports that provide information about object dependencies, and modifications to existing objects, during the uninstallation process:

- **Application Uninstall Alerts** - lists dependencies that may prevent the removal of an application component. For example, Relativity doesn't remove an object type referenced by a locked application or the parent object of a child that you want to retain in the workspace.
- **Modification Alerts for Non-Application Components** - lists components that aren't part of the application but must be modified to uninstall the application. Other objects may reference components deleted during the uninstall process. For example, Relativity may delete an object type referenced by an unlocked application.

To view these reports, click **Validate Components to Uninstall** on the Component Summary page. See Uninstalling an application on the previous page.



2.10.1.3 Viewing application uninstall errors

Relativity displays the view for the Relativity Applications tab after you click Uninstall Application on the Component Summary page. When an application fails to uninstall properly, Relativity locks the application and generates a list of errors that occurred during the uninstall process. The application also continues to appear in the list view of the Relativity Applications tab.

To view uninstall errors, click the application name in the list view to display the details page, and then click **Show Errors**.

2.10.1.4 Auditing the uninstall process

When you uninstall an application, Relativity audits deleted and updated components. You can view this audit information from the History tab in a workspace by selecting the All History view and filtering on a specific action. In addition, you can view changes to specific objects by clicking View Audit on their details page.

If you want to disable auditing for update or delete actions during the uninstall process, set the AuditApplicationUninstallEnabled AuditApplicationUninstallenabled instance setting to False.

2.10.1.5 Manually uninstalling custom pages

Note: Contact Relativity Support if you need to manually uninstall custom pages associated with applications.

2.10.2 Deleting applications

When you delete an application instance, Relativity deletes child objects and unlinks associative objects, but it doesn't delete the associative objects from the workspace. To delete these objects, uninstall the application. Deleting an application instead of uninstalling it can be useful when building and testing an application that hasn't been added to the application library.

For complete details on uninstalling applications, see Uninstalling applications on page 69.

Use these steps to delete an application:

1. Select the **Relativity Applications** tab in the workspace containing the application that you want to delete.
2. Unlock the application if necessary. You can't delete a locked application. See Locking and unlocking applications on page 58.
3. Click the application name to display the details view.
4. Click **Delete**.
5. (Optional) Click **Dependencies** in the pop-up window to view a report containing the following information:
    - Child objects to be deleted with the application
    - Associative objects to be unlinked from the application
6. Click **Delete**. Relativity deletes the application and its children and unlinks any associative objects.

2.11 Upgrading applications

You can upgrade an existing application by using the Upgrade Application option available on its detail view.

2.11.1 Upgrading an application

Before you upgrade an application, review the following information:

- Some Relativity applications are pre-populated with instances of object types used to store settings, which you can modify to control application functionality. Upgrading the application resets these instances, so any modifications made to them are lost. As a best practice, create new instances of these object types in your application instead of modifying the default settings. For example, you might create a new profile with your custom settings in the Imaging application.

  Note: You can avoid resetting instances of object types by developing applications that use Post Install event handlers set to run only once. Using these event handlers, you can create instances of objects and set default values on them during the initial application installation, but not on subsequent upgrades. See Post Install event handlers on the Relativity aiR Developers site.

- Relativity preserves modifications made to saved searches included in locked applications. For more information, see Modifying saved searches in a locked application on the Relativity RelativityaiR Documentation site.
- Confirm that any existing application jobs have completed before upgrading out-of-the-box Relativity applications, such as OCR, search terms report, transform set, or imaging. You may interrupt the current job if you upgrade the application while it is running.

2.11.1.1 Upgrading an application in a workspace

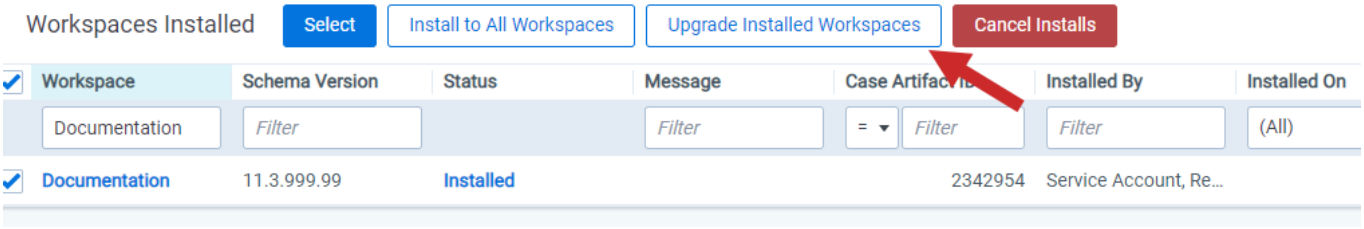
Use the following procedure to upgrade an application:

1. Confirm that you have the appropriate system admin permissions to install an application in Relativity. For more information, see Workspace security.
2. Select the **Relativity Applications** tab in the target workspace.
3. Click the name of the application that you want to upgrade.
4. Click **Upgrade Application** in the Relativity Application console. If you don't see this button, then you don't have the appropriate system admin permissions.
5. Select **Import from file** in the Application Type field.
6. Click **Browse** to select a application file.

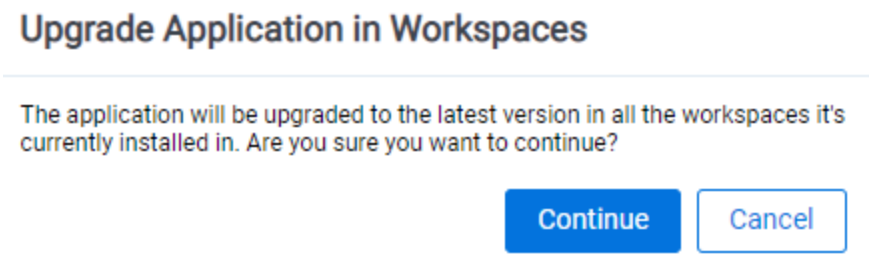
7. Click **Open** on the browse dialog.
8. Click **Upload** to initiate upgrade script.

2.11.1.2 Upgrading an application through the Application Library

1. Confirm that you have the appropriate system admin permissions to install an application in Relativity. For more information, see Instance Security.
2. Select the **Application LIbrary** tab.
3. Click the name of the application that you want to upgrade.
4. In the Workspaces Installed associated object, select the workspaces in which you want to upgrade the application and click **Upgrade Installed Workspaces**. If you don't see this button, then you don't have the appropriate system admin permissions.



5. Click **Continue** on the confirmation modal to proceed with upgrading the application in all the workspaces it's installed in.



6. Select **Import from file** in the Application Type field.

Relativity will upgrade the selected application, and the new version will be visible in the applications list in the workspaces it's installed in.

2.11.1.3 Application resource file purge

The application upgrade process purges assembly resource files (DLLs) that aren't associated with the newer application version:

- Physically deletes all DLL resource files that were part of the original application version.
- Removes event handler associations on objects types such as Document or Entities.
- Remaps object references in the workspace database to reference the new DLL.
- Eliminates workspace references to resources that no longer exist.
- If an agent of a removed type is currently running, it will complete its work and then self-destruct.

The following application components are not deleted by the upgrade process:

- Object types (fields, views, layouts, etc.)
- Scripts

- Saved searches
- Dashboards

2.11.2 Troubleshooting application upgrades

You can use the following information to identify and resolve issues that may occur when upgrading your applications.

2.11.2.1 Exporting choices attached to single or multiple choice fields

When you update an existing application with a single or multiple choice field, you can make the choices attached to these fields available for export by setting the **Auto Add Choices** field property to **Yes**.

2.11.2.2 Custom pages not working properly when multiple application versions exist on the same server

If you have an application with custom pages in Workspace A, and import a new version of the same application to Workspace B on the same server, then the custom pages may not function as expected since they are outdated. However, they continue to display as components of the application.

2.11.2.3 Applications can't be downgraded

You can't import an application with an earlier version number into the Relativity applications library. However, an application with an earlier version number can exist in a workspace even though the application in the environment's library has a higher version number.

3 Audit

Use the Audit application to monitor and report on user activity in your Relativity instance. With Audit, you can quickly identify trends and actions using interactive pivots and visualizations.

3.1 Key benefits

- Create custom dashboards by building multiple widgets and lists.
- View audit records at the instance level directly in the Relativity UI.
- Search millions of audit records to find specific actions, such as reviewer coding decisions or user login activity.
- Export audit data quickly to meet stakeholder reporting needs.

To learn more about common workflows, see Recipes.

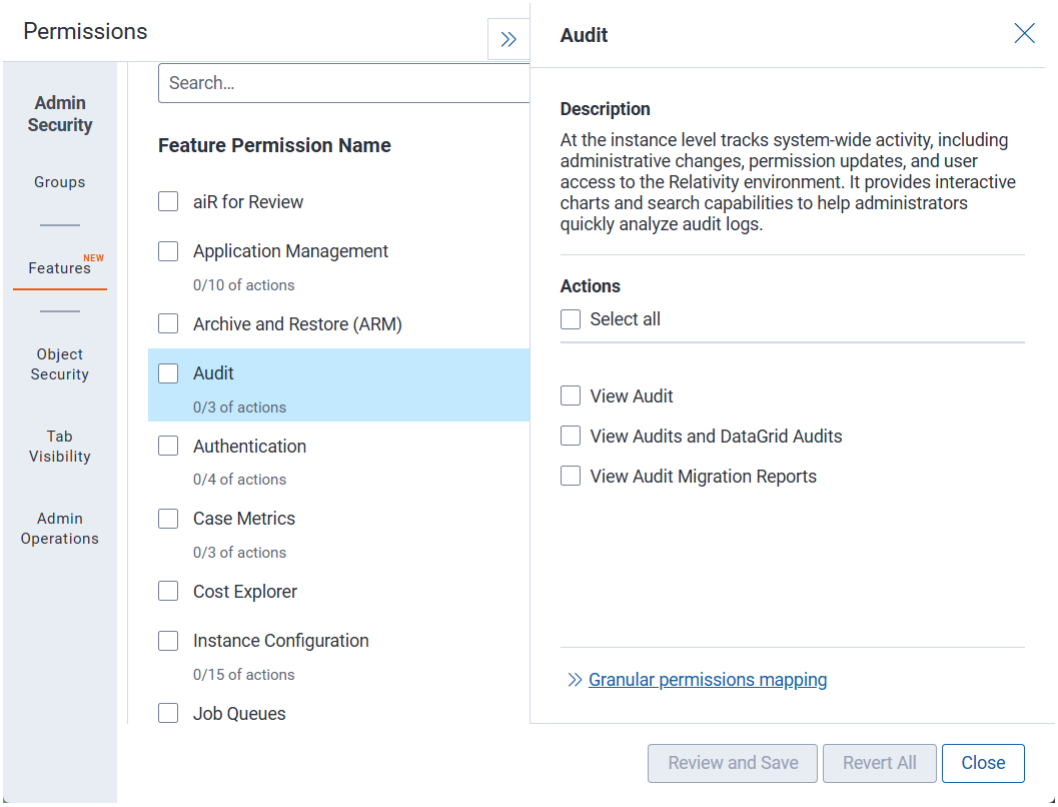
In Relativity aiR, the system stores audit records in SQL for a limited time before migrating them to the main data sink. The **PostMigrationPersistencePeriod** instance setting controls how long records remain in SQL:

- **Name:** PostMigrationPersistencePeriod
- **Section:** kCura.Audit
- **Default value:** 10 days

Note: Do not increase this value beyond 15 days. Doing so may cause system instability or unexpected behavior.

3.2 Permissions

Manage permissions for this feature on the Features tab. Grant the full feature for a group, or customize access with individual actions. For an overview of features and actions, see Feature permissions.



3.3 Supported Audit tab functionality

The following table lists supported and unsupported functionality on the Audit tab compared to the History tab.

Supported functionality	Currently unsupported functionality
• ARM – Archive & Restore • Dashboards • Group By/Pivot On functionality (limited number of fields) • Item list • Filtering • Views • Widgets • Reverting/mass revert document edits • Exporting data from lists • Exporting dashboard widgets as image	• Custom scripts • Export of dashboards • Exporting from the History tab

3.3.1 Audit agents

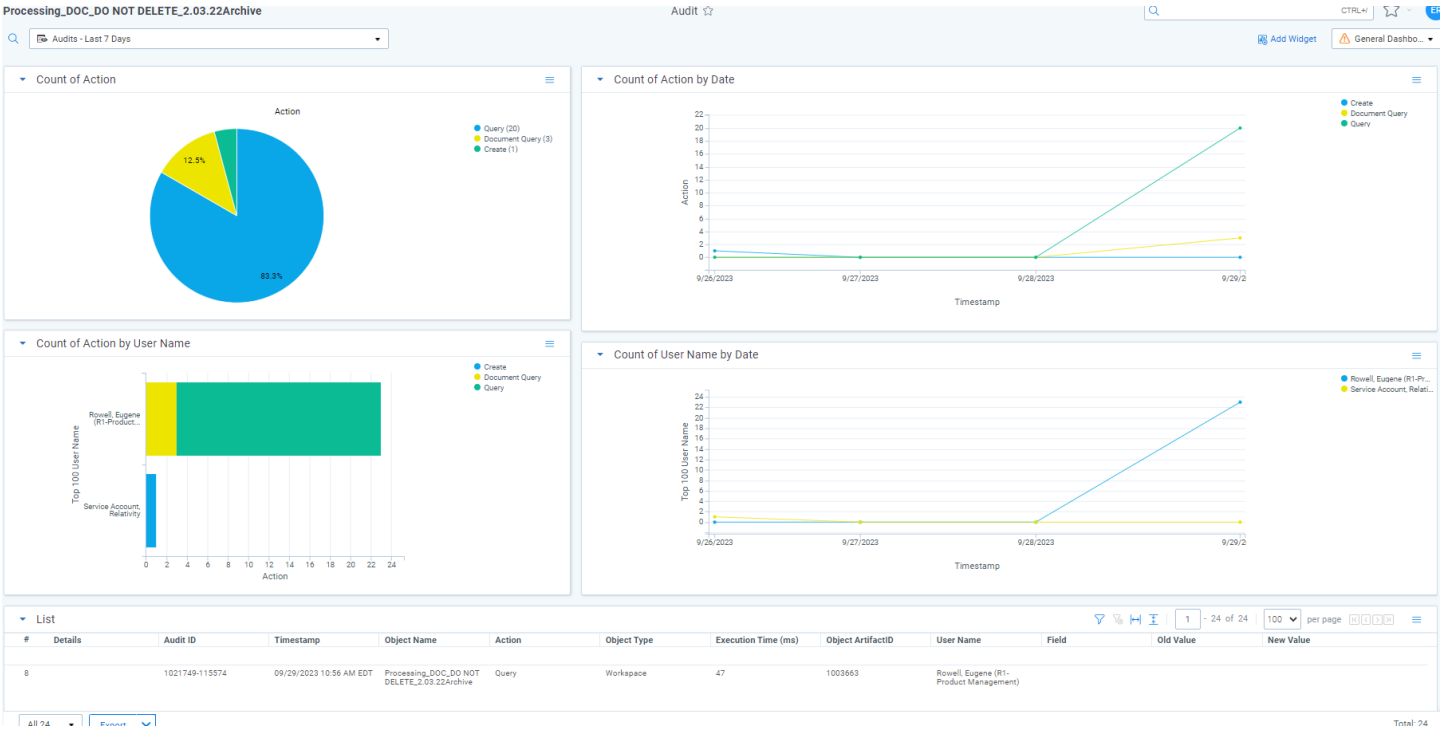
The Audit application includes the following agents:

Agent name	Function
Data Grid Audit Migrator	A Data Grid Audit Migrator agent migrates audit data from SQL to our main database.
Data Grid Audit Deleter	The Data Grid Audit Deleter agent is an off-hour agent that deletes all audits from SQL that have been successfully migrated. Along with un-migrated audits, it will leave other existing audits in SQL for a configurable number of days for billing purposes.
Data Grid Audit Reporter	The Data Grid Audit Reporter agent reviews the audit queue for errors that occurred during migration from SQL. This agent triggers a Relativity error based on the agent's run interval. This agent is set to an hourly run interval by default.
Data Grid Audit Manager	Populates filters in the Audit application.
Data Grid Manager	A Data Grid Manager agent is an off-hours agent responsible for Data Grid enabled workspace management, including deleting outdated search results cache tables and monitoring Data Grid index conditions.
Audit Export Agent	The Audit Export Agent is activated whenever a user exports data to CSV or XLSX in the Audit tab (Mass Export). This agent then retrieves data from a storage location and streams it into a file.
Audit Reviewer Statistics Agent	The Audit Reviewer Statistics Agent is activated whenever a user generates a Reviewer Statistics report (either by running the Reviewer Statistics script or by using the Case Metrics application). This agent retrieves data from a storage location, aggregates it, and saves it as a materialized view in the temporary tables of the workspace database.

3.4 Audit tab

Use the Audit tab to build custom widgets and design dashboards to meet workflow needs. You can use the same **Group By** and **Pivot On** functionality available in Relativity. The default view on the Audit dashboard shows the last 7 days of Audit activity.

Note: You cannot add the Security, Edit, Name, System Last Modified On, System Last Modified By, System Created By, or System Created On fields to an Audit list view. Additionally, avoid adding the **Artifact ID** field to any views from the Audit tab.



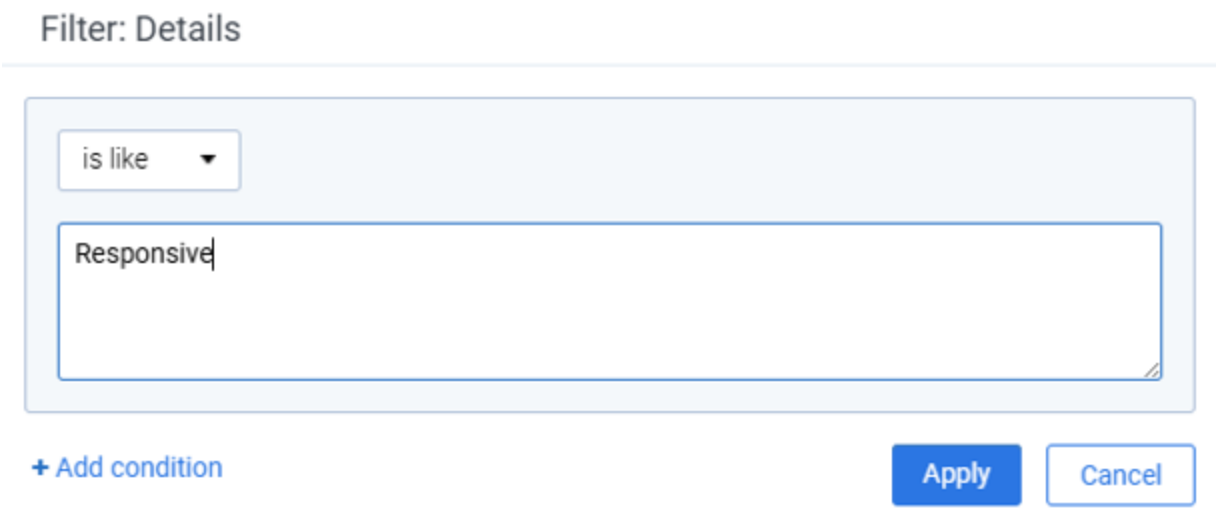
The Audit tab supports the following functionality:

- Creating and customizing views on the Audit tab.
- Applying filters and conditions to sort through audit records.
- Exporting audit data from list views and widgets.

3.4.1 Advanced Filtering Audit records

You can apply basic filtering to these list view fields: **Audit ID**, **Timestamp**, **Action**, **Object Type**, **Execution Time (ms)**, **Object ArtifactID**, and **User Name**. For the **Details** field, you can also use advanced filtering.

The list view does not currently support direct filtering on **Field**, **Old Value**, and **New Value**. Instead, you can use the **is like** and **is not like** operators to search for keywords within the Details field. This provides a rough filtering method for locating relevant records.



Note: Advanced filtering is available only for the **Details** field.

3.4.1.1 Advanced filtering example

the following is an example using **"is like"** and **"is not like"** operators:

Query	Result
Details is like Responsive	Returns records where “Responsive” text appears anywhere in the Details field
Details is not like Hot	Returns records where “Hot” text does not appear anywhere in the Details field

3.4.1.2 New value and old value filtering

If your workflow requires distinguishing between New Value and Old Value, we recommend the following steps:

1. Use **"is like"** filtering on Details to perform rough filtering within Relativity.
2. Export the filtered subset of records and apply further filtering outside the system.

This method supports more precise analysis using the available filtering options.

3.4.2 Details column

To display the query text of an audit record, click the expand details icon  in the Details column for that record. You can toggle between a table view and JSON view of audit details.

Audit Details

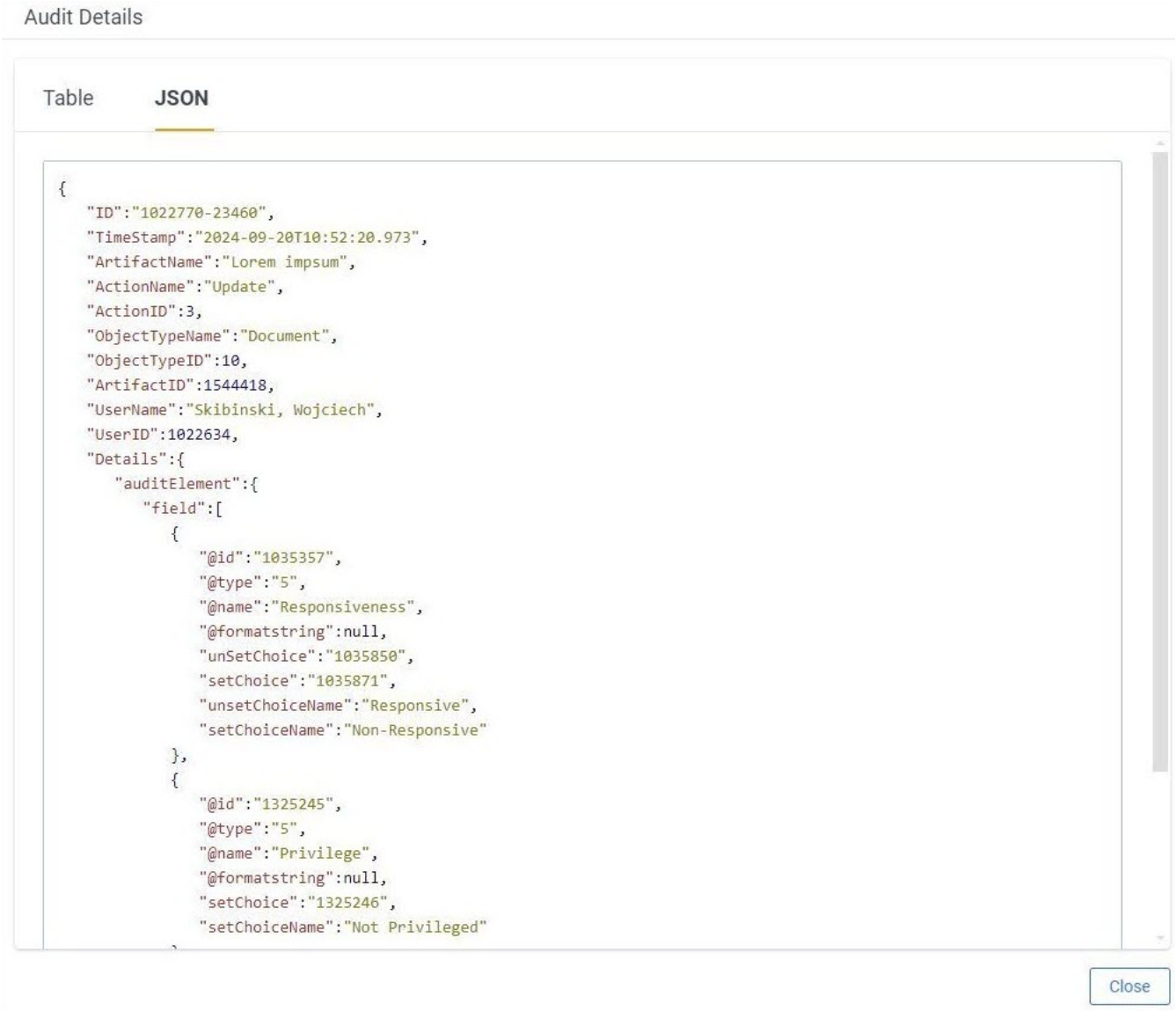
Table JSON

Name	Value
ID	1022770-23460
TimeStamp	2024-09-20T10:52:20.973
ArtifactName	Lorem impsum
ActionName	Update
ActionID	3
ObjectTypeName	Document
ObjectTypeID	10
ArtifactID	1544418
UserName	Skibinski, Wojciech
UserID	1022634
WorkspaceId	1022770
WorkspaceName	Wojtek Workspace

Field Changes

Name	Old Value	New Value
Responsiveness	Responsive (1035850)	Non-Responsive (1035871)
Privilege		Not Privileged (1325246)

Close



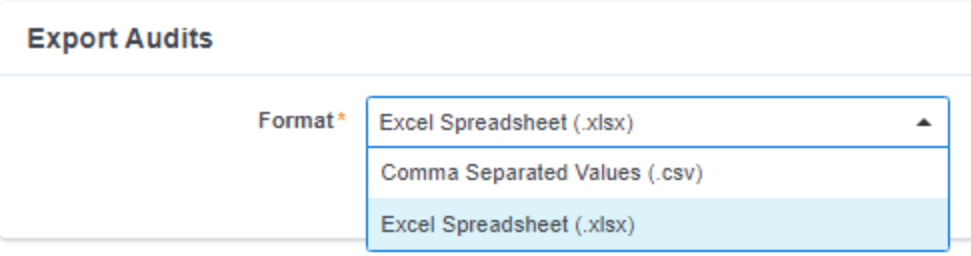
3.4.3 Exporting workspace audits

You can export audit data from list views and widgets. The export respects the data made on the filters in the list view, and the results are filterable.

Note: You currently cannot export audits at the instance level. When you export audit data, the Field, Old Value, and New Value are not displayed in separate columns but are preserved within the Details column. For the following field types, the choices names are included in the export in addition to IDs: **Single Choice Field**, **Multiple Choice Field**, **Single Object Field**, **Multiple Object Field**, and **User** Field.

To export audit data, complete the following:

1. From the mass operations bar, click **Export**.
2. Select the format you want to export your audits in (either .csv or .xlsx).

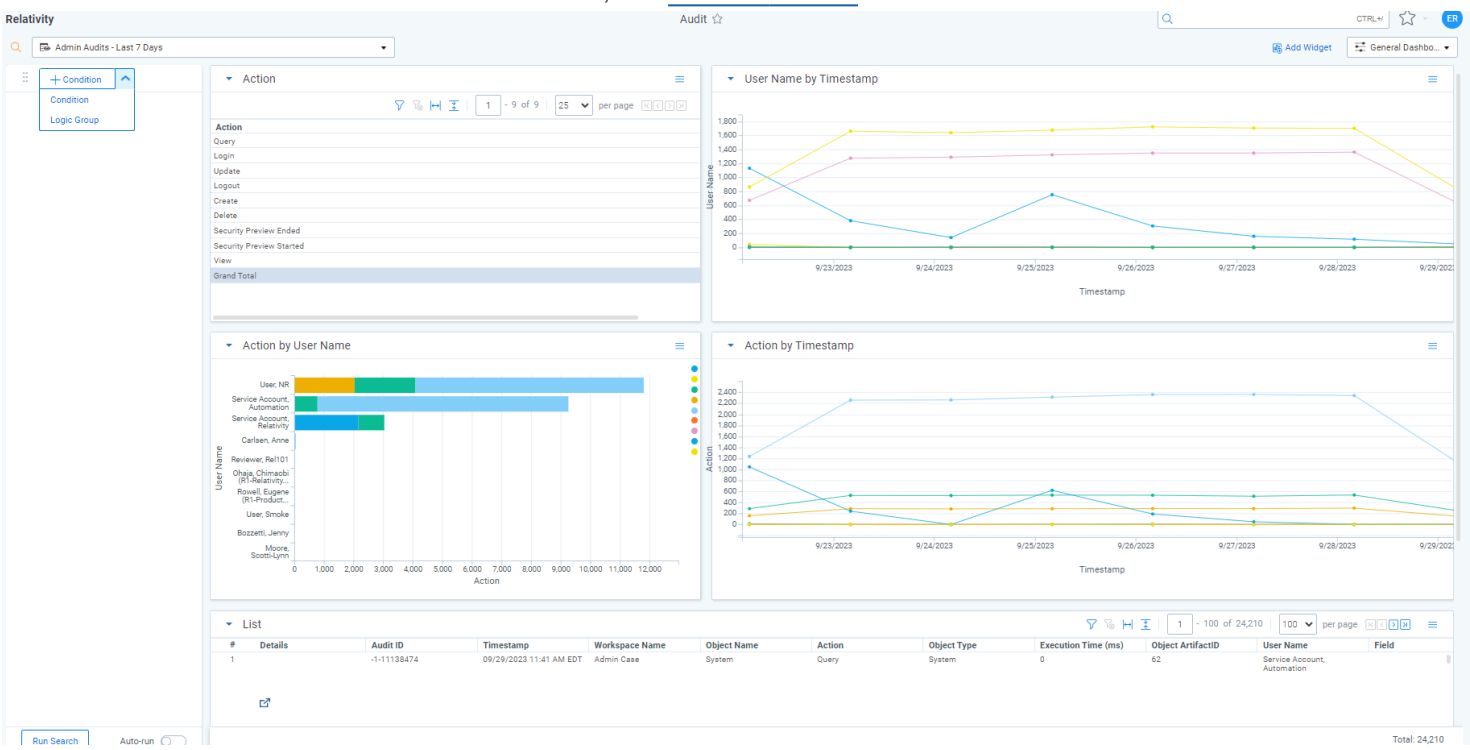


3. Click **Run**.

Note: Currently, when you sort on the Audit table and then export it, the sort order you specified is not retained. Only filter conditions are retained when you export.

3.5 Instance audits

The Audit tab functions the same at the instance level. You can build custom widgets and design dashboards by using the same Group By and Pivot On functionality available in workspace audits. However, exporting audits is not available. For a list of admin-level audited actions, see Audited actions.

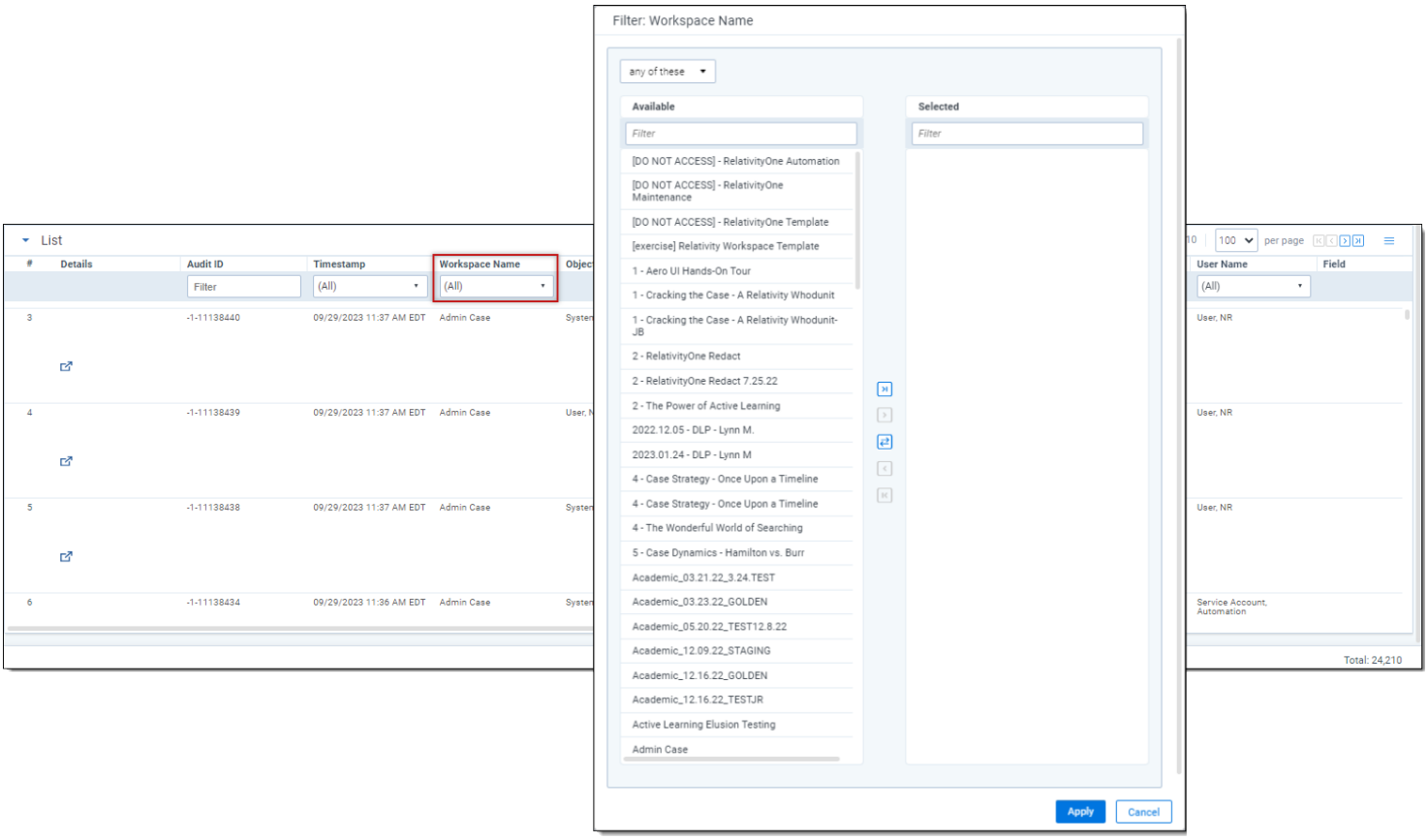


Note: You must be a system admin to view audits at the instance level.

3.5.1 Filtering on multi-workspace audits

System admins can view workspace audits at the instance level.

You can filter on the **Workspace Name** column to view audits for specific workspaces. By default, the Audit application displays audit information for the first 10 workspaces, sorted by Artifact ID. You can configure this number using the MaxAggregatedWorkspacesMaxAggregatedWorkspaces instance setting.



3.5.2 Reverting audited actions

System admins can revert a coding decision made by a user on a document from the Audit list. Reverting the coding decision will edit the choice back to the previous selection. This action can only be performed at the workspace level. You can revert the most recent Document Update, Mass Update, or Propagate action on the Document object.

Only the latest update action made to the following field types can be reverted:

- Currency
- Date
- Decimal
- Fixed Length Text
- Single choice
- Single object
- User
- Whole number
- Yes/No

Notes:

- You cannot revert a required field if it would result in returning that field to a blank (null) value. The system does not permit empty (null) values. For example, if a required field was blank at the time an update was applied and you then attempt to revert it, you will not able to do so.
- By default, the maximum number of audits you can run the mass revert operation on at one time is 5000. Attempting to run more than 5000 results in an error message. You can decrease the maximum number of audits using the instance setting. Do not increase this instance setting value past 5000.

Read a scenario
Let's assume that the Coding layout has two fields to edit: Responsiveness and Privilege. Neither of them is required. Below are the actions of two reviewers in order of execution:

1. *Reviewer1* updates **Document1** to set Responsiveness field to "Not Responsive."
2. *Reviewer1* updates **Document2** to set Responsiveness field to "Responsive" and Privilege field to "Privileged."
3. *Reviewer1* updates **Document3** to set Privilege field to "Privileged."
4. *Reviewer2* updates **Document1** to set Responsiveness field to "Responsive."
5. *Reviewer2* updates **Document2** to set Responsiveness field to "Not Responsive."

If you execute a mass revert on all actions above, then only actions 3, 4, and 5 will be reverted, because they are the last updates made to the documents.

Using the same example above, now let's assume that the Privilege field is required. In that case, only actions 4 and 5 will be revertible. Operation 3 cannot be reverted because it would result in a blank (null) value, which is not allowed by the system.

To revert a coding decision:

1. From the mass operations bar, select **Revert** in the drop-down menu.
2. Audit scans the list of audits in the current view to determine how many are revertible. Once it finishes, click **Run**.
3. Click **Close** to close the pop-up window.

Similar to reverting a single audit, each reverted audit generates a new audit record.

3.6 Audit Migration Reports tab

Use the Audit Migration Reports tab to generate migration error and migration status reports. These reports help you monitor the status of audit data as you migrate it into the main database. You can also run a migration error retry script.

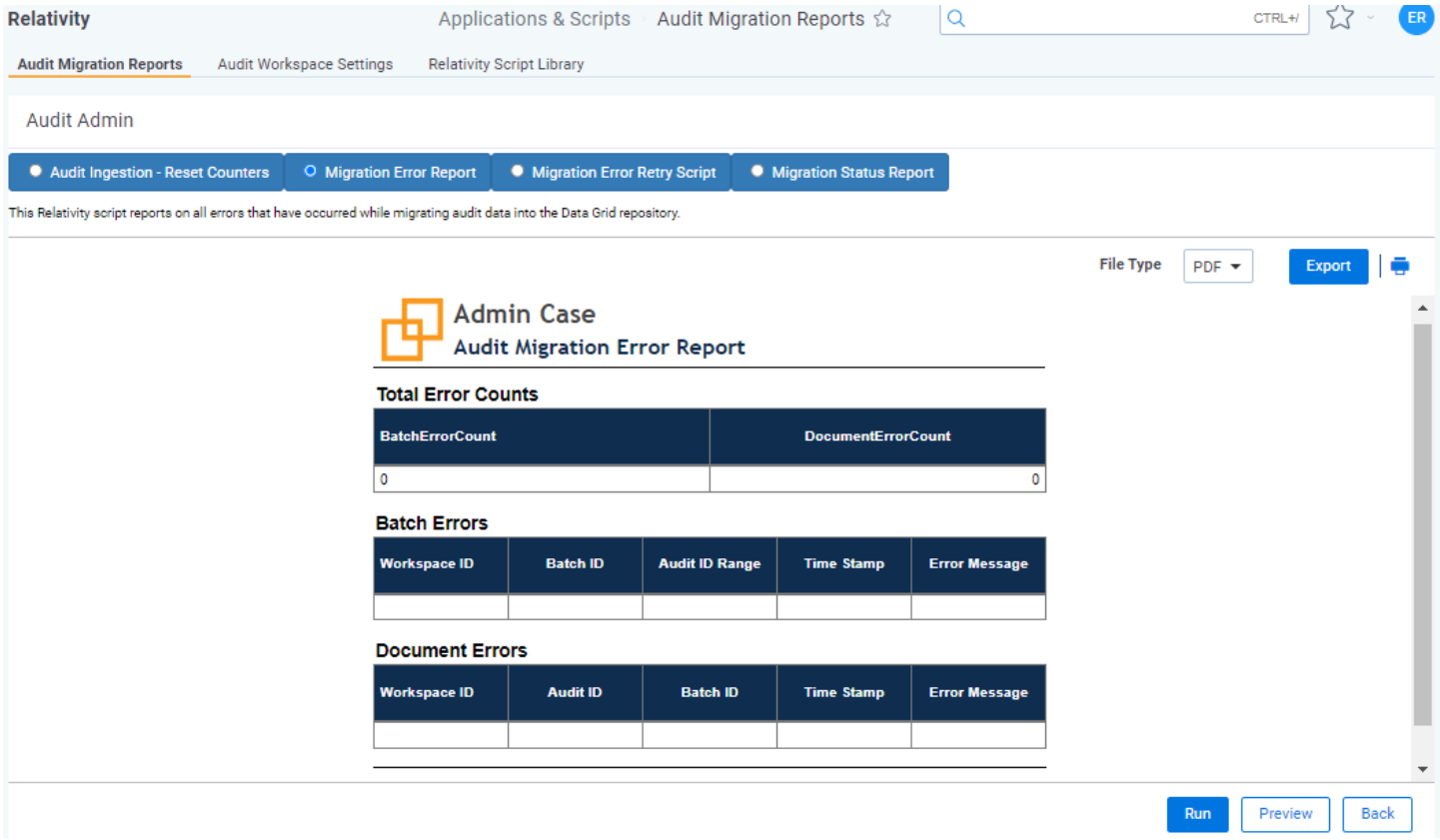
3.6.1 Migration Error Report

The Migration Error Report generates a report that provides information on all errors that have occurred while migrating audit data into the main database, including batch and document errors.

Note: You can also run this script on all environments in your workspace from the Relativity Script Library tab. Click the user drop-down menu in the upper-right corner of Relativity, and then click Home. Navigate to the **Applications & Scripts** > **Relativity Script Library** tab, and then search for the name of the script.

To preview the script, select the radio button for this script and click **Preview**. To run this report, click **Run**. The following results populate the bottom of the window.

Note: Audit automatically retries certain audit migration errors, like SQL timeouts, invalid XML, and inability to connect to the main database. With this improvement, the migration error report may display a total of 0 errors because the system automatically retried and resolved those common errors. In this situation, you do not need to run the Migration Error Retry Script.

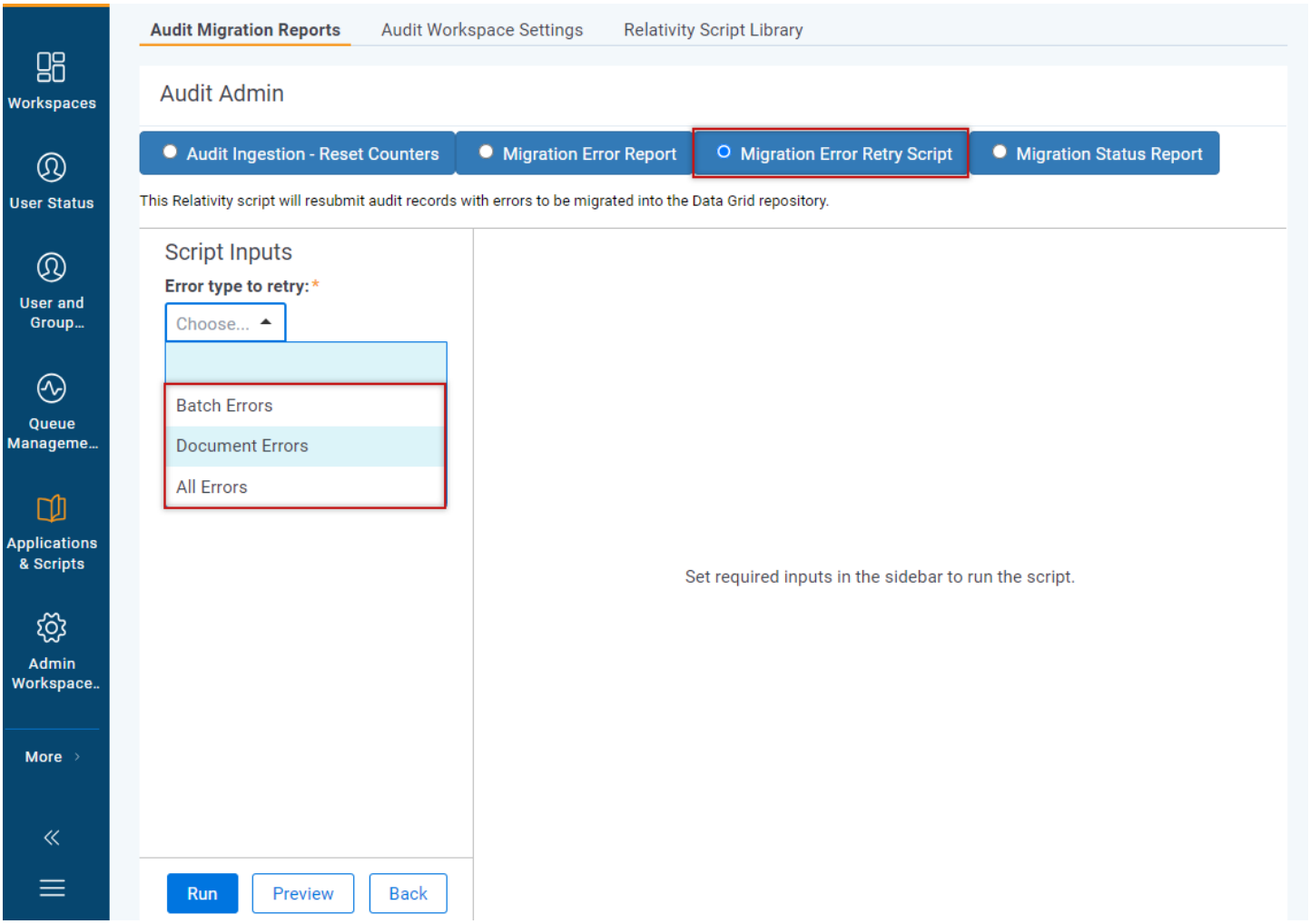


- **Total Error Counts**—this section provides a summary of all errors that occurred during migration.
  - **Batch Errors**—the total number of batch errors that occurred during migration.
  - **Document Errors**—the total number of document errors that occurred during migration.
- **Batch Errors**—this section provides a summary of all batch errors that occurred during migration.
  - **Batch ID**—the batch ID number of the batch that received an error.
  - **Audit ID Range**—the first and last Audit ID numbers contained in the batch that received an error.
  - **Time Stamp**—the time at which the error occurred.
  - **Error Message**—the text of the batch error.
- **Document Errors**—this section provides a summary of all document errors that occurred during migration.
  - **Audit ID**—the audit ID number of the document that received an error.
  - **Batch ID**—the batch ID number of the batch in which the document that received an error was contained.
  - **Time Stamp**—the time at which the error occurred.
  - **Error Message**—the text of the document error.

3.6.2 Migration Error Retry Script

After you identify errors with the Migration Error Report, investigate and fix specific audit issues. After you fix the issues, run this script to resubmit the audit records with errors for migration into the main database.

Note: You can also run this script on all environments in your workspace from the Relativity Script Library tab. Click the user drop-down menu in the upper-right corner of Relativity, and then click Home. Navigate to the **Applications & Scripts** > **Relativity Script Library** tab, and then search for the name of the script.



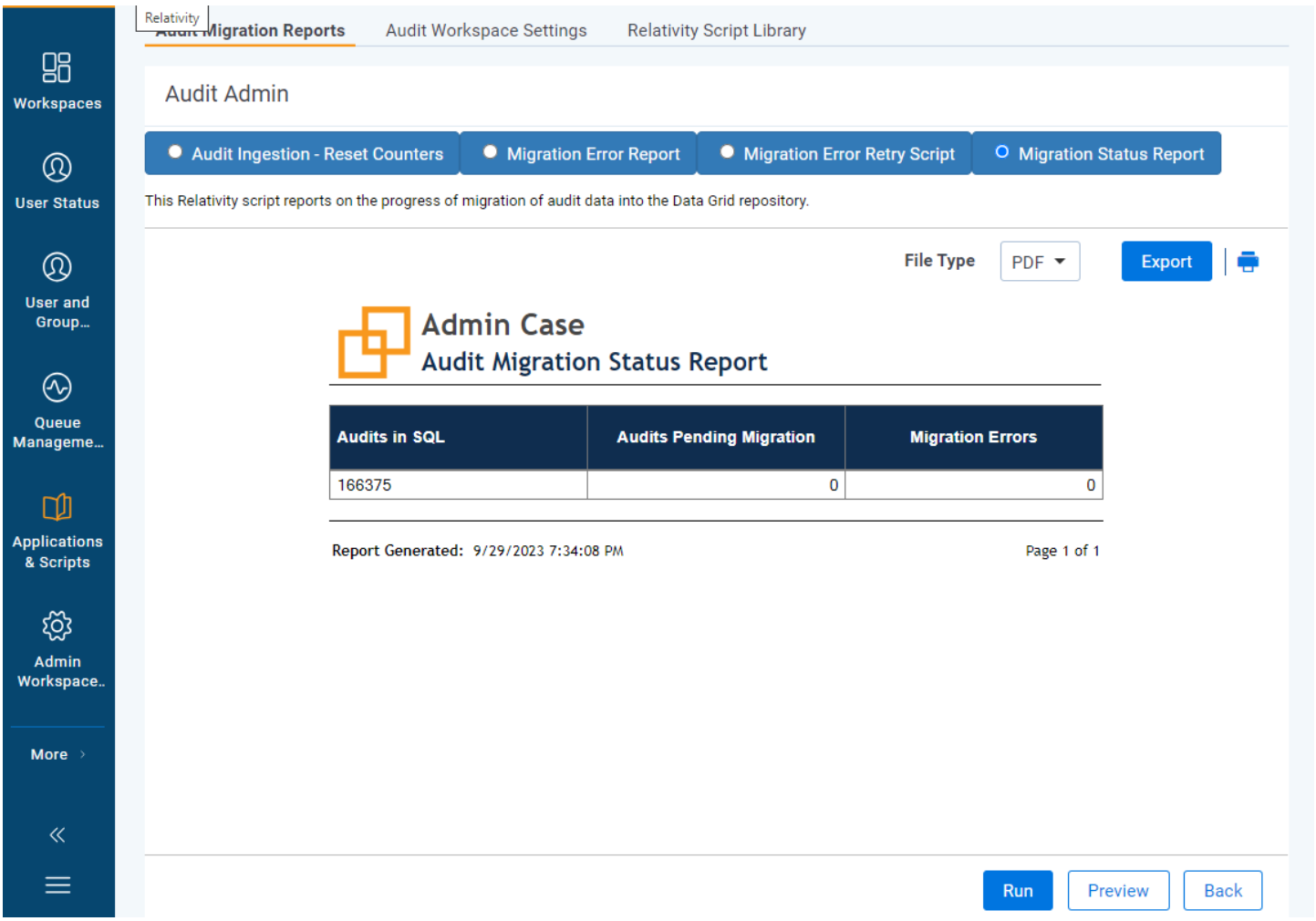
In the **Error type to retry** drop-down list, select from the following options:

- **Batch Errors**—retries all batches with errors as reported in the Migration Error Report.
- **Document Errors**—retries all documents with errors as reported in the Migration Error Report
- **All Errors**—retries all batch errors and document errors as reported in the Migration Error Report.

Click **Preview** to see a sample of the report, or select the appropriate option and click **Run** to execute the script.

3.6.3 Migration Status Report

The Migration Status Report shows the progress of migrating audit data into the main database. The includes audits in SQL, audits pending migrations, and migration errors. To preview the script, select the radio button for this script and click **Preview**.



Click **Run** to generate this report and display the following information:

- **Audits in SQL**—lists the number of audits in the SQL database.
- **Audits Pending Migration**—lists the number of audits in queue for migration into Data Grid.
- **Migration Errors**—lists the number of errors that occurred during migration.

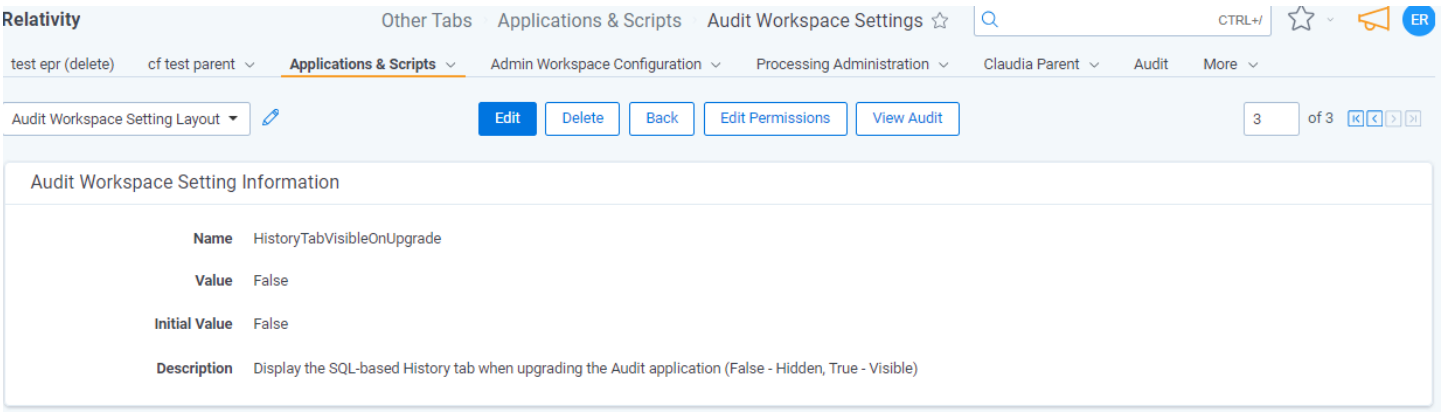
3.7 Audit Workspace Settings tab

Use the Audit Workspace Setting tab to configure settings specific to the Audit application. The Audit Workspace Setting tab contains one setting,**HistoryTabVisibleOnUpgrade**.

Note: You must have permission to view this tab in order to configure the setting.

3.7.1 HistoryTabVisibleOnUpgrade

The **HistoryTabVisibleOnUpgrade** tab configures whether the History tab is visible when upgrading the Audit application.



You can configure the **HistoryTabVisibleOnUpgrade** setting with one of two values:

- **True** - displays the History tab upon upgrade.
- **False** - hides the History tab upon upgrade.

By default, the HistoryTabVisibleOnUpgrade setting is set to hide the History tab when upgrading the Audit application. To configure HistoryTabVisibleOnUpgrade, click the **Edit** link and modify the **Value** field in the subsequent layout.

3.8 Audited actions

The following table lists audited actions in Relativity:

Note: If you perform a job while previewing a user's security settings, the audit action will be credited to your **username** and not to the user whose security you were previewing when you started the job.

Action name	Description of activity
CaseMap - Add Document	A document was sent to CaseMap.
CaseMap - Add Fact	A selection of text from the viewer was sent to CaseMap as a fact.
Conversion Complete	A file was converted by way of a user clicking on a file link in the document list, running an imaging set, imaging on the fly, running a mass image operation, or switching to text or production mode in the viewer.
Create	An item was created.
Delete	An item was deleted.
Document Query	A query was run on a list of documents, or a document query was canceled. (A message indicating that a query was canceled is displayed in the details and on the Query Text pop-up.)
Export	The contents of a production set, saved search, folder, or subfolder were exported.
Images - Created	Images were created.
File Download	A file was downloaded through the Single Simple File Upload application. For example, a user clicked Download File on the Error Actions console of an individual processing error layout.
File Upload	A file was uploaded through the Single SimpleFile Upload application. For example, a user clicked Upload Replacement File on the Error Actions console of an individual pro-

Action name	Description of activity
	cessing error layout.
Images - Created for Production	Images corresponding to a production outside of Relativity were imported into the system.
Images - Deleted	Images were deleted.
Import	Content associated with a load, production, or image file was imported.
Markup - Image - Created	Redactions or highlights were added to an image.
Markup - Image - Deleted	Redactions or highlights were removed from an image.
Markup - Image - Modified	Redactions or highlights were moved, resized or edited on an image.
Markup - Native - Created	Redactions or highlights were added. This audit entry applies to transcripts only.
Markup - Native - Deleted	Redactions or highlights were removed. This audit entry applies to transcripts only.
Markup - Native - Updated	Redactions or highlights were moved, resized or edited. This audit entry applies to transcripts only.
Move	A document was moved from one folder to another.
Native - Created	A native file was loaded into Relativity.
Native - Deleted	A native file was removed from Relativity.
Pivot Query	A Pivot report was run, or a Pivot report was canceled. (A message indicating that a query was canceled is displayed in the details and on the Query Text pop-up.)
Production - Add Document	A document was added to a production.
Production - Remove Document	A document was removed from a production.
Query	A process ran a query (such as categorization), or a query was canceled. (A message indicating that a query was canceled is displayed in the details and on the Query Text pop-up.)
RelativityScriptExecution	A Relativity script was run.
ReportQuery	A summary report was run.
Run	A file was imaged, saved as a PDF, or otherwise converted for viewing
Search Cache Table Creation	A search cache table was created. (Search cache tables are created the first time you search for a term or phrase using dtSearch or Relativity Analytics.)
Security	Security rights were assigned or changed
Tally/Sum/Average	The mass operation Tally/Sum/Average was run in the workspace.
Update	Document metadata was updated on a single-document basis. In addition, filters on information related to applications installed through the workspace or by an agent.
Update - Mass Edit	Document metadata was updated on a mass basis.
Update - Mass Replace	Document metadata was edited using a text mass replacement.
Update - Propagation	Document metadata was edited according to a propagation rule.
View	A document was viewed.

Action name	Description of activity
Workspace Upgrade	Details about scripts run on a workspace during an upgrade.

The following actions are audited at the admin-level. These admin-level actions are recorded against the Admin Case (workspace name). If you filter on the actual workspace name when searching for the Login action, you will not see any results.

Action name	Description of activity
Create	An item was created.
Update	An item was updated
Delete	An item was deleted.
Security	An owner of a saved search was set during creation or edit.
Login	A user logged in to Relativity.
Logout	A user logged out of Relativity.
Export	Data was exported from a tab at the instance level. For example, a workspace list, list of users, list of groups, etc.
RelativityScriptExecution	A Relativity script was executed.
Password Reset Request - Submitted	A password reset request was submitted.
Password Reset Request - Opened	A password reset request was opened.
Password Reset Request - Successful	A password reset request was successful.
Security Preview Started	A security preview started on a user or group.
Security Preview Ended	A security preview ended on a user or group.
Workspace Upgrade	Upgrade script run on the workspace (details can be viewed in the JSON tab of the Details).
Login - Failed	A login attempt to Relativity failed.

4 Authentication

RelativityOne uses several industry-standard technologies, enabling versatile authentication options. It supports local (such as password related) or external (such as external identification providers) authentication methods. You can add and enable each type individually, as well as assigning at least one, and in some instances multiple methods, for each user.

4.1 Choosing your authentication setup

Relativity aiR is moving to Centralized Authentication. Centralized Authentication is a unified system for managing user authentication and identities. Both setups are available during the transition, and the steps you follow depend on which one your instance uses.

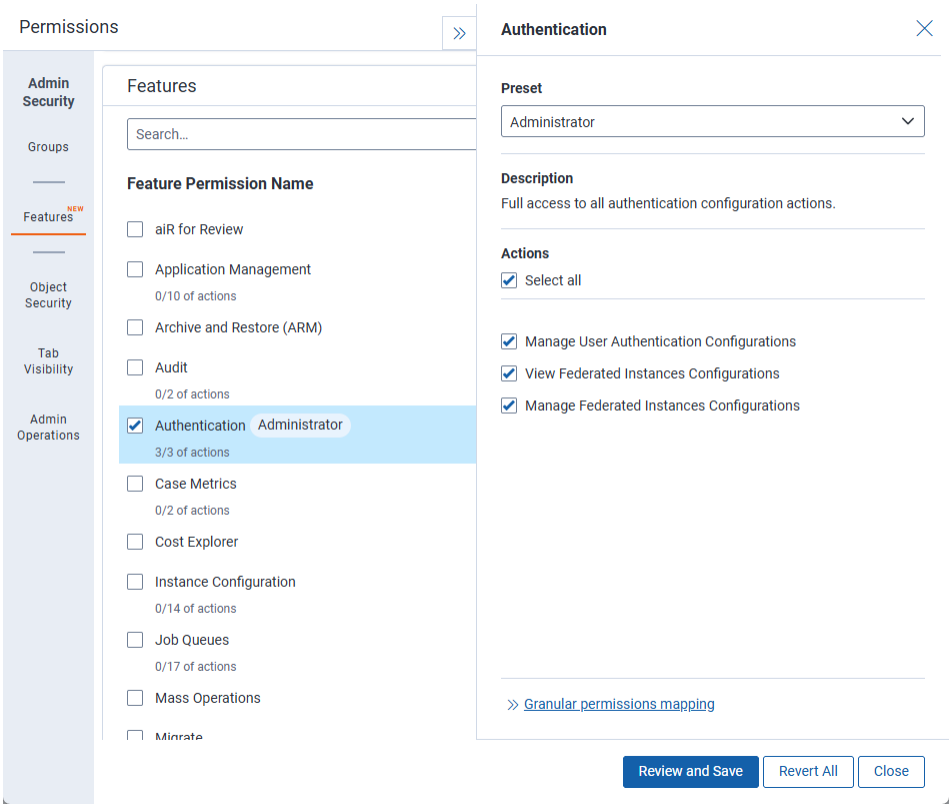
- **Centralized Authentication**—after onboarding, the Centralized Authentication tab appears in your instance. Users can then log in with it. For setup steps, see Centralized Authentication on page 94.

- **Authentication providers**—if your instance has not transitioned, you create providers from the Authentication Provider tab using the **New Authentication Provider** button. This topic and the provider topics it links to cover that setup.

Note: Both setups are supported until all instances complete the transition to Centralized Authentication. Customers who transitioned before the release should use the Community article for their onboarding wave. For more information, see Centralized Authentication on page 94.

4.2 Permissions

Manage permissions for this feature on the Features tab. Grant the full feature for a group, or customize access with individual actions. For an overview of features and actions, see Feature permissions.



4.3 Authentication overview

Review the following sections to learn more about the authentication methods, the object model, and the permissions model supported by Relativity:

4.3.1 Authentication methods

RelativityOne supports the following authentication mechanisms.

- **Password**—a method that includes a user name, the user's email address, and a password.
- **OpenID Connect**—a protocol for an external identity provider, authenticating against an external identity provider using the OpenID Connect protocol. OpenID Connect is a modern authentication protocol can be used to connect to providers such as Microsoft Entra ID. See OpenID Connect for more information.

- **SAML 2.0**—a method that authenticates against an external identity provider using the SAML 2.0 protocol. SAML 2.0 is an older authentication protocol that is still in widespread use. See SAML 2.0 for more information.

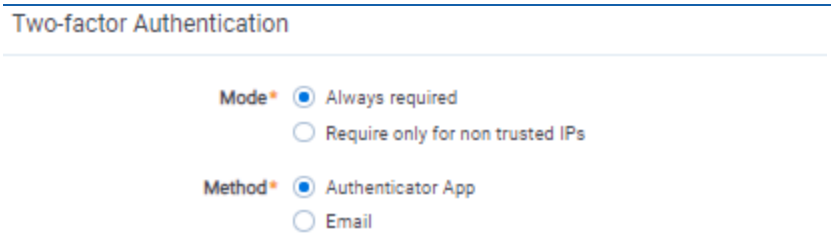
Notes:

- When implementing single sign-on (SSO) across Relativity instances, the following scenarios are supported:
  - Identity Provider-initiated SSO using SAML 2.0
  - ID provider and service provider-initiated SSO with OpenID Connect
- To log in using PIV/smartcard, configure Relativity aiR with an OpenID Connect or SAML provider that supports PIV/smartcard logins. PIV/smartcards are not directly supported in Relativity aiR.

In addition to the above protocols, Relativity has the following additional authentication features:

- **Two-factor Authentication**—when logging in with the Password method, you can require the user to pass an additional two-factor check based on an email or message sent to the user's phone, through a mobile email gateway.
  - **Mode**—always required or require only for non-trusted IPs
  - **Method**—Authenticator App or email. For more information, see the authenticator app's documentation.

  Note: Relativity recommends the Authenticator App as the preferred two-factor challenge method, because it offers enhanced security compared to email-based verification.

- **Trusted IP Range**—limit access to the Relativity application based on the user's source IP address.

4.3.2 Authentication object model

Relativity provides several tabs or object types that are used to configure authentication. By combining these object types, the system admin is able to control the Relativity login page and authentication options for the users in the environment.

Authentication Provider—an authentication provider holds the settings for one login protocol. For example, you can add the Password Provider to your environment to set minimum and maximum password length, password history settings, and more. Some protocols have several configuration options, and others have very few. On the Authentication Provider tab, every instance has a Default Password provider, and you cannot add a second provider of that type.

You can add OpenID Connect and SAML 2.0 external identity providers. You can have more than one provider of either type in an environment.

Login Method - Users can have one or more Login method objects that binds that user to a particular Authentication Provider. For example, if you have a Password Authentication Provider in the environment, the Password Login Method contains the specific password for a given user. If you have Azure Active Directory configured as a Provider, each user's AAD subject identifier would be stored in an associated Login method.

User—the User object holds the TrustedIPs setting. When you set a TrustedIP for a user, that user can authenticate with Relativity aiR only from that IP range. All other authentication-related fields sit on the Provider and Method objects.

Note: In Centralized Authentication, trusted IP addresses are managed on the authentication provider rather than on the individual user. For more information, see Centralized Authentication on page 94.

4.3.3 Authentication object permissions

These default object permissions are recommended for managing user authentication:

- **System admins only**—full permissions, including view, update, delete, secure, add
  - **Authentication Provider Type**
  - **Authentication Provider**
  - **Login Method**
  - **OAuth2 Clients**
- **Anyone with the ability to view a user**—view
  - **Authentication Provider Type**
  - **Authentication Provider**
  - **Login Method**
- **Anyone with the ability to edit a user**—update, delete, add
  - **Login Method**

4.4 Configuring authentication providers

These steps apply to instances that have not transitioned to Centralized Authentication. System admins must assign each user at least one authentication method before that user can log in.

Note: In Centralized Authentication, you set up password and SSO providers through the Authentication Provider tab. To assign users to these providers, use the Centralized Authentication page. For detailed steps on completing these actions, refer to the Centralized Authentication on page 94 documentation.

4.4.1 Creating authentication providers

Authentication providers are instances of authentication provider types. You create only the instances of the provider types you need. For example, if you plan to support only password methods, you only have to create an authentication provider for passwords, and not for any other provider types.

Note: Adding a new authentication provider of the same type overwrites an existing provider of that type.

You can have only one instance of each provider type. OpenID Connect and SAML 2.0 are the exceptions. You can have more than one instance of those types if each one has a different name.

To create an Authentication Provider:

1. Select the **Authentication Provider** tab.
2. Click the **New Authentication Provider** button.
3. Enter a **Name**. This is the friendly name of the provider instance.

4. Optionally select the **Enabled** status. By default, each authentication provider is enabled. If the provider is not enabled, users cannot log in with that method.
5. Select a **Provider Type**. You can select OpenID Connect or SAML2.
   The **Authentication Provider Settings** section appears.
6. Set the Authentication Provider Settings, if any. See Authentication provider settings below for the specific method.
7. Click **Save**.

Note: For help with error messages, see the SSO Troubleshooting console on page 153.

4.4.2 Assigning a login method to individual users

You assign an authentication method to each user for them to log in with. Each user must have at least one authentication method in order for them to log in but you may assign multiple methods. See Managing user authentication methods on page 123.

4.4.3 Enabling Relativity aiR Connect

Enable Relativity aiR Connect to connect two or more of your Relativity instances. Use a single identity to securely connect multiple instances and let users navigate between them securely with cross-authentication using a single sign-on provider (SSO). For more information, see Relativity aiR Connect on page 149.

4.5 Authentication provider settings

Authentication providers may have settings that you configure. These settings apply to all instances of that authentication provider.

Every provider instance has at least one setting, Enabled. When Enabled is set to **Yes**, the authentication provider is available. Both this setting and Enabled on the Authentication Provider must be set to **Yes** for a user to log in with that method. If either one is set to **No**, the method is not available.

Authentication providers that require additional settings:

- **Default Password provider** - additional settings for the Default Password provider include:
  - **Minimum Password Length** – sets the minimum number of characters for a password.
  - **Maximum Password Length** – sets the maximum number of characters for a password.
  - **Maximum Password Attempts Before Reset Required** – sets the maximum number of consecutive unsuccessful login attempts before being locked out. You must send the user a password reset request before they can attempt to log in again.
  - **Maximum Password Age (in days)** -sets the maximum number of days a password remains valid. The user will be prompted for a new password on a logon at the expiration date. If set to zero, the password does not expire.
  - **Users Can Change Password Default** – enables the user to change their password.
  - **Allow Password Recovery via Email** – enables the user to use email to recover a forgotten password. **Yes** displays the Forgot Password link on the user's login screen.
  - **Password Recovery Request Limit** – sets the maximum number of password resets before Relativity locks out the user. You must send the user a password reset request before they can attempt to log in again. This value resets to zero on each successful log in.

- **Maximum Password History** – sets the maximum number of previous passwords that users cannot use for a new password. The default value of zero enables any previous password.
- **Additional Work Factor** – increases the number of encryption hashes. Relativity already provides several built in hash levels represented by the default zero value. Changing this value to 1, 2, or 3 adds additional encryption protection but may significantly increase login time.

Note: The following non-alpha-numeric characters are not allowed: \, ", <, >, £ in passwords.

- **OpenID Connect with Microsoft Azure AD** - see OpenID Connect on page 137 authentication provider flows.
- **SAML 2.0 provider** - see SAML 2.0 provider on page 130.

4.6 Centralized Authentication

Centralized Authentication is a unified system for managing user authentication and identities across Relativity aiR. It is built on the Okta Customer Identity platform. By centralizing user authentication data, it helps to streamline administration. Users sign in with the same credentials across multiple Relativity aiR instances.

Centralized Authentication supports a variety of authentication methods, including standard password-based login and Single Sign-On (SSO). For SSO, it is compatible with both **Security Assertion Markup Language (SAML)** and **OpenID Connect (OIDC)** protocols, allowing organizations to integrate with their preferred identity providers and authentication standards.

Note: Did your instance onboard to Centralized Authentication before this release? Continue to use the Community article for your onboarding wave. Use this topic ***after*** Relativity transitions your instance to the current experience.

- **January–June 2025 (password only)**—see V1—Centralized Authentication.
- **June–December 2025 (SSO and password)**—see V2—Centralized Authentication.

4.6.1 Prerequisites

Confirm your browser allows traffic to and from the new login page: **login.relativity.one**, ***.okta.com**, and ***.oktacdn.com**.

4.6.2 Centralized Authentication workflow

1. The System Administrator sets up the authentication providers. This includes reviewing the password provider, creating new password providers, and registering an SSO provider.
2. Existing users log in to Relativity aiR using Centralized Authentication with their existing credentials.
3. The System Administrator invites only new users or newly enabled users to the Relativity instance through Centralized Authentication.

   Note: If a disabled user is enabled after the transition to Centralized Authentication, the System Administrator must send that user an invitation to set up their account and password.
4. Users accept the invitation and set up their account and password.

4.6.3 Setting up your Authentication Provider

The Authentication Provider page streamlines the management of authentication providers and allows you to create and edit password providers with ease.

System Administrators can set up one or both of the following types of authentication providers:

1. **Password–**a two-factor authentication (2FA) method that includes a username, (the user's email address), and a password. See Password Provider setup.

   Note: Simple password setup is currently permitted, however, disabling two-factor authentication is not recommended.

2. **SSO (Single Sign-On)**—an external authentication provider gives users one set of credentials for multiple applications, including Relativity. See SSO setup on page 108.

4.6.3.1 SSO setup

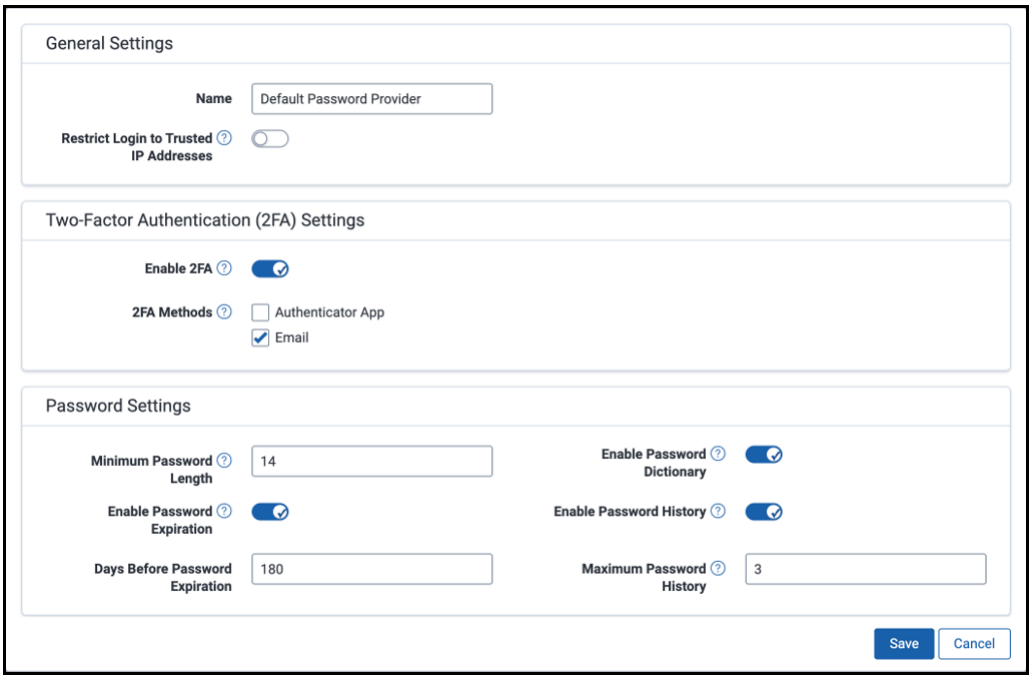
System administrators can configure SSO provider connections using the guided self-service wizard that walks them through configuring their Single Sign-On provider, including testing the connection at the end. Additional, detailed information will be added here prior to the rollout to SSO customers.

Notes: To use your existing SSO provider with Centralized Authentication, you will need to re-register the SSO connections in Relativity using the wizard. For best results, open your identity provider in a separate window and/or work with someone who has access to it.

You can update your existing application or create a new one in your identity provider to include the new redirect URL. For OIDC, you can simply add the second redirect URL to the existing application. For SAML, if you replace the redirect URL, users will be unable to log in until Centralized Authentication is enabled.

4.6.4 Password Provider setup

From the Authentication Provider tab, click the New Password Provider button and fill out the following fields:



1. Under **General Settings**, enter a Password Provider Name
2. In the Two-Factor Authentication (2FA) Settings section, confirm the settings in the following fields:
   - **Enable 2FA**–this toggle is enabled by default to use two-factor authentication for a more secure password experience. If you disable this toggle, a warning is displayed as it does not align with Relativity aiR

Security Best Practices.

- **2FA Methods**–select one or both two-factor authentication challenge methods: Email and Authenticator App. By default, the Authenticator App is selected and is the recommended option, because it offers stronger security than email-based MFA.
  - If both are selected, the user can select which one they want to use during the login process.
  - To learn more, see Two-factor authentication on page 45.

3. In the **Password Settings** section, set the following fields:
   - **Minimum Password Length**–enter the least number of characters permitted for user account passwords. Relativity aiR Security Best Practices recommends 10 or more characters.
   - **Enable Password Expiration**–this toggle is enabled by default with the **Days Before Password Expiration** set to 180. If disabled, passwords never expire.
     - You may update the desired number of days in the **Days Before Password Expiration** field.
     - This value is calculated per user account based on the date the user last reset their password.
   - **Enable Password Dictionary**–enable this toggle to prevent the most commonly used passwords from being used in password creation. If disabled, these passwords are permitted.
   - **Enable Password History**–enable this toggle to prevent reuse of passwords. Enter the maximum number of previous passwords to be tracked in history in the **Maximum Password History** field. If disabled, users are permitted reuse previous passwords.
4. Click **Save**.

4.6.4.1 Password requirements

Legacy Requirements	Centralized Authentication Requirements
Minimum character length – defined by customers (default 8)	Minimum character length - defined by customers (default 14)
4 of the 4 criteria: • 1 lower case letter • 1 upper case letter • 1 number • 1 non-alpha-numeric character	No change

Additional password considerations

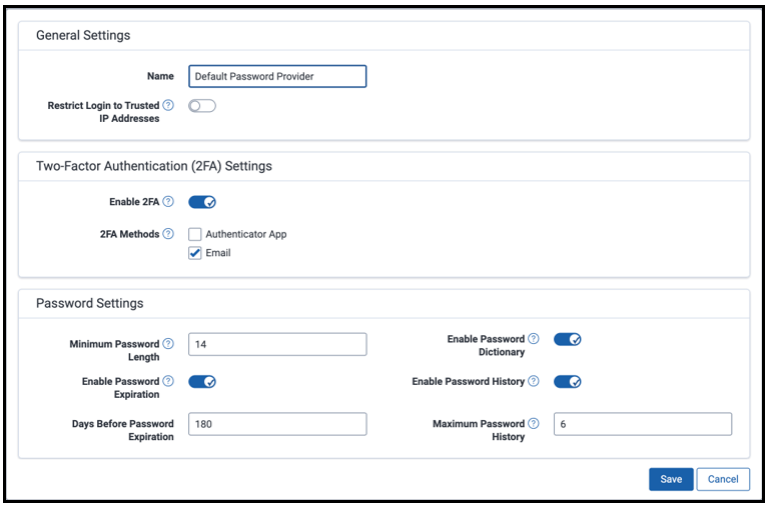
Feature	Legacy	Centralized Authentication
Maximum character length	X (default 50)	No enforced max (72 character evaluation limit)
Maximum failed password attempts before password reset required (Brute Force Protection)	X	X (10 failed attempts)
Maximum password age	X (default no	X (default 180 days)

Feature	Legacy	Centralized Authentication
	expiration)	
Maximum password history	X	X
Disallow commonly used passwords	Not supported	X
Set password for user	X	Not supported to mitigate risk of user account sharing.
Suspicious IP Throttling	Not supported	X
Breached Password Detection	Not supported	X

After you complete the password setup, you can confirm user eligibility or enrollment status from the Centralized Authentication tab.

4.6.4.2 Edit a Password Provider

1. In the Authentication Provider tab, select the **Edit** icon next to the Password Provider you want to update.
2. In the modal window, update any of the following:
   - **Provider Name**
   - **Two-Factor Authentication (2FA) Settings**
   - **Password Settings**
   - **Trusted IP usage**
3. To change the 2FA challenge method, select your preferred option (for example, switch from Email to Authenticator App).
4. To update Trusted IP addresses, add or remove addresses as needed.
5. Click Save to apply your changes.



4.6.4.3 Trusted IP Support

Trusted IP support allows you to restrict user logins to specified IP addresses or ranges to enhance the security posture of your environment.

Trusted IP Overview

Centralized Authentication support for trusted IPs will differ from legacy behavior in that they will be applied at the authentication provider level instead of the individual user level.

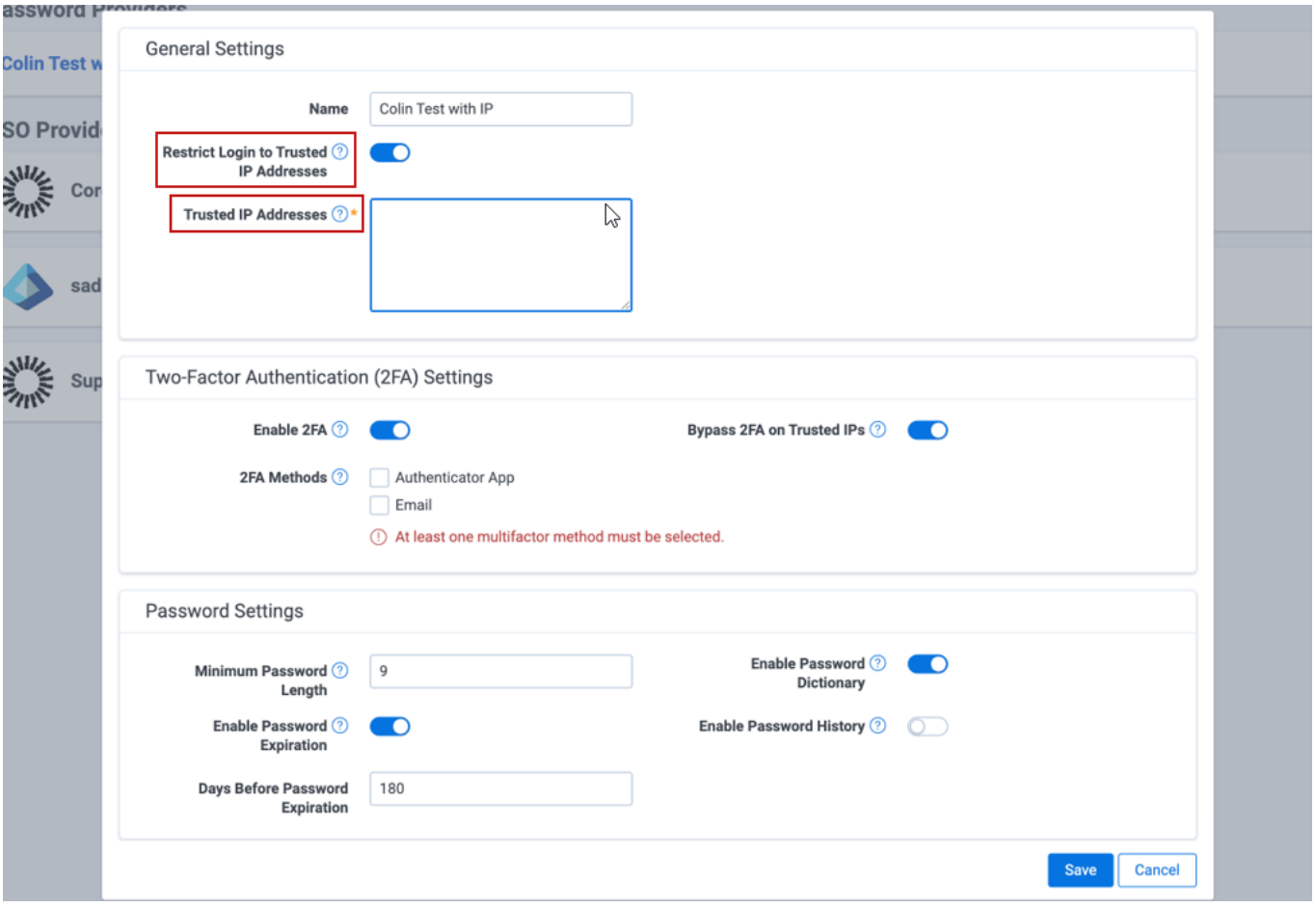
- **Password Providers** - trusted IPs are defined and managed at the password provider level.
- **SSO Providers** - trusted IPs on OIDC providers can no longer be managed within Relativity and should be configured on your Identity Provider.
- If a user attempts to log in from an unauthorized IP address, authentication will fail.
- The **Bypass MFA on Trusted IP** is no longer a supported workflow.

Note: If you previously configured trusted IP addresses with legacy authentication, remove them to avoid unintended interaction.

4.6.4.4 Setting up Trusted IP addresses

Follow these steps to configure trusted IP addresses for a password provider:

1. Navigate to the Authentication Provider tab.
2. Click the edit icon next to the password provider you want to configure.
3. Enable the **Restrict Login to Trusted IP Addresses** toggle.
4. In the Trusted IPs field, enter one or more IP addresses or ranges. Separate multiple entries with a comma, space, or new line.



5. Click **Save**.

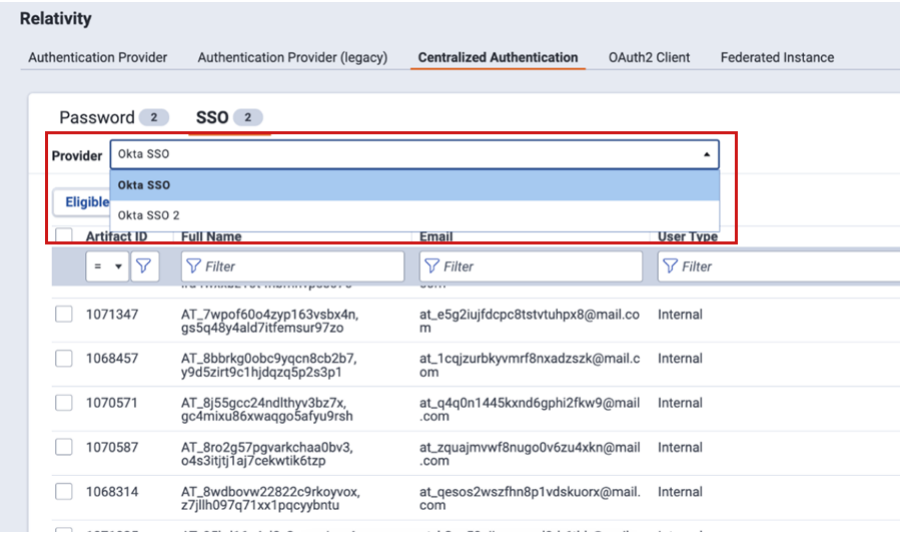
4.6.5 Inviting users

You can invite new users individually from their user record or in bulk from the Eligible tab on the Centralized Authentication page.

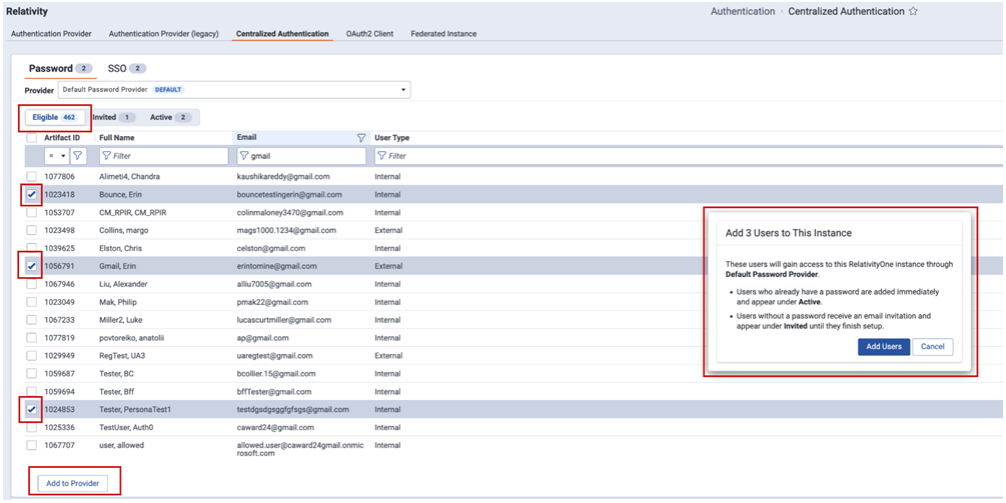
Note: The following invitation instructions apply only to users who authenticate with a password provider. By default, users who authenticate through an SSO provider will not need to accept an invitation to use Centralized Authentication. System administrators will still need to create the user account in Relativity, and grant access through their identity provider; however, users can sign in directly using Centralized Authentication, and the system will authenticate them through their SSO identity provider.

4.6.5.1 Centralized Authentication tab invitation

1. Navigate to the **Centralized Authentication** tab.
2. Select the **Authentication Provider Type** (Password or SSO) that you want to manage users for, and select the specific provider from the **Provider** dropdown.

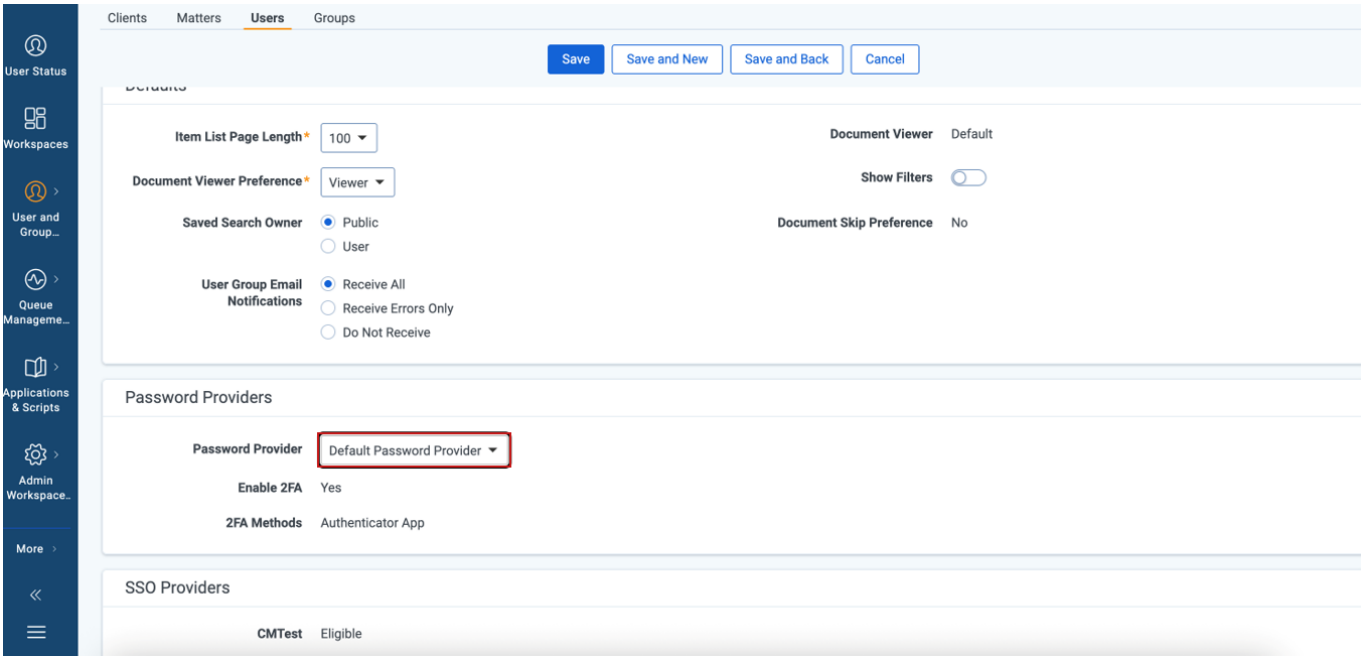


3. For **Password Providers**:
   a. Select **Eligible** to view users who can be added to this password provider.
   b. Select one or more users and click **Add to Provider** and **Add Users** in the Confirmation window.



4.6.5.2 User tab invitation

1. Navigate to the Users tab and click the **Edit** icon next to the user you want to invite.
2. Select the desired **password provider** from the drop-down menu.



> **Note:** After you select the password provider, the system displays the configured MFA settings.

3. Click **Save**.
4. Click **Save and Invite** to send the email invitation to the user to join this Relativity aiR instance via Centralized Authentication.



The user receives an email invitation from **support@relativity.one** with the subject, "Welcome to Relativity aiR." See User accepts the invitation. Once invited, the user appears on the **Pending list** until they accept the invitation, at which point they move to the **Enrolled list** within the tab for this specific password provider.

4.6.6 Managing user transition

Administrators can track user transitions to Centralized Authentication and manage invitations directly from the Centralized Authentication tab. This overview helps you see which users are assigned to each authentication provider and monitor their progress.

4.6.6.1 Monitor progress by Authentication Provider

Navigate to the Centralized Authentication tab, then choose the authentication provider you want to review. The information you see changes based on the provider type.

Password Providers

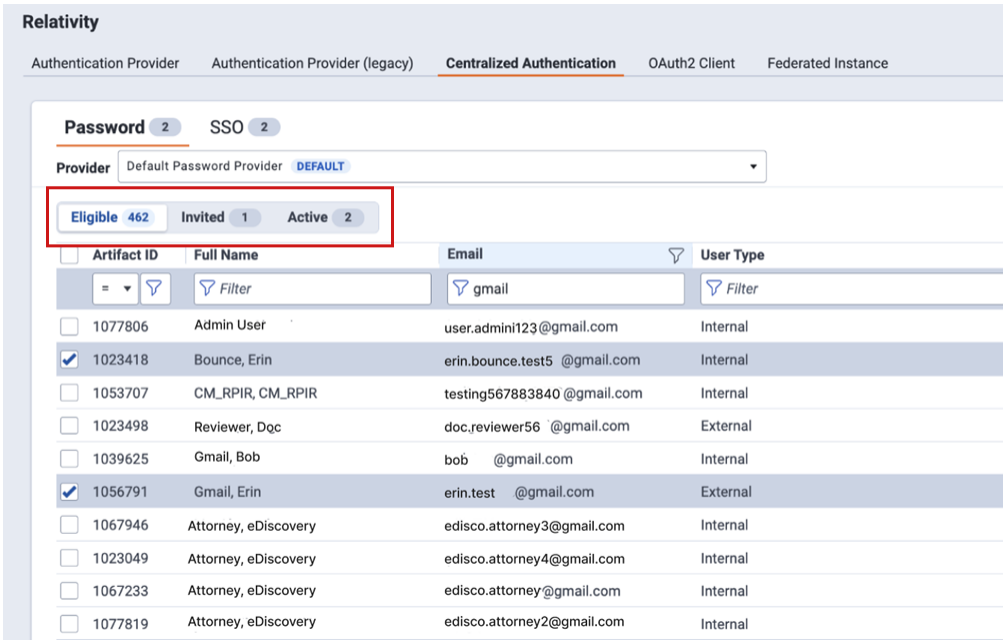
Eligible: Displays users not currently assigned to the provider. The list shows only enabled users and lets you filter by Artifact ID, Full Name, Email, or User Type.

Invited: Shows users who have been sent an invitation but haven't accepted it yet. The list displays Artifact ID, the Inviter's name, the Invitee's name, the invitation URL, when the invitation expires, and the creation date. Use the Invitation URL if a user can't receive the invitation email.

If an invitation expires, select the user and choose **Re-invite** at the bottom of the screen to send a new invitation.

Note: Users who already have a Centralized Authentication password do not appear in the Invited tab because they move directly to Active.

Active: Lists users who have been assigned to log in with this provider. You can view such details as Artifact ID, Full Name, Email, and User Type.



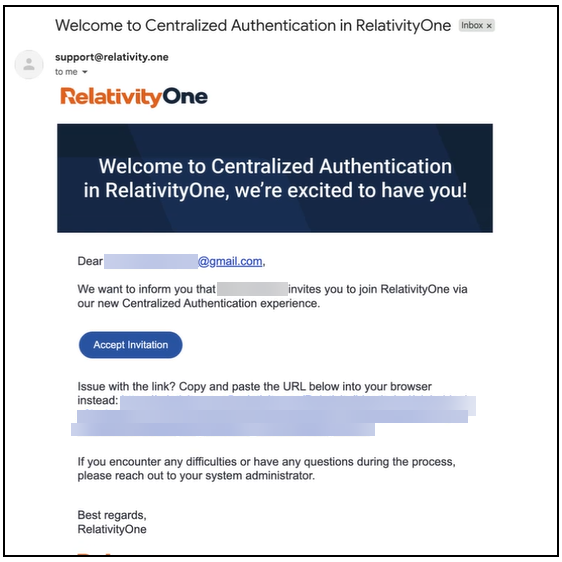
4.6.7 User accepts the invitation

With the transition to a global identity model, the login experience will differ slightly for new and existing Relativity users:

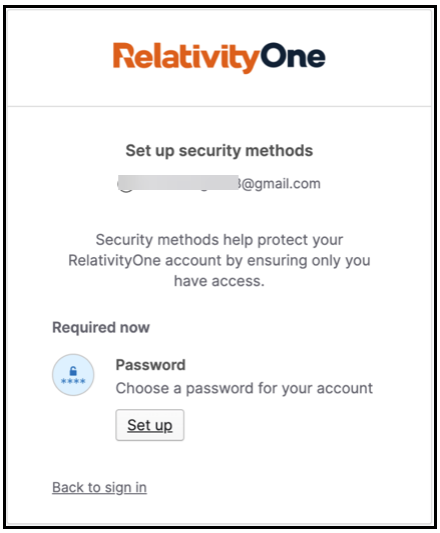
- **New users** will continue to receive an invitation to set up their password as part of the onboarding process.
- **Existing users** will receive a notification email and can access the new instance using their current credentials.

When the user receives the email invitation from **support@relativity.one** with the Subject, “Welcome to Centralized Authentication in Relativity aiR,” they need to accept it.

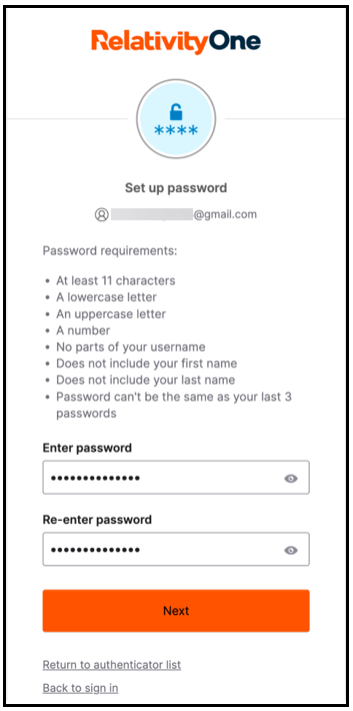
1. The user clicks the **Accept invitation** button or copies the hyperlink displayed into their browser which will take the user to the universal login page. The invitation expires after 7 days by default.



2. In the "Accept your invitation" dialog, follow these steps:
    a. Click Set up.



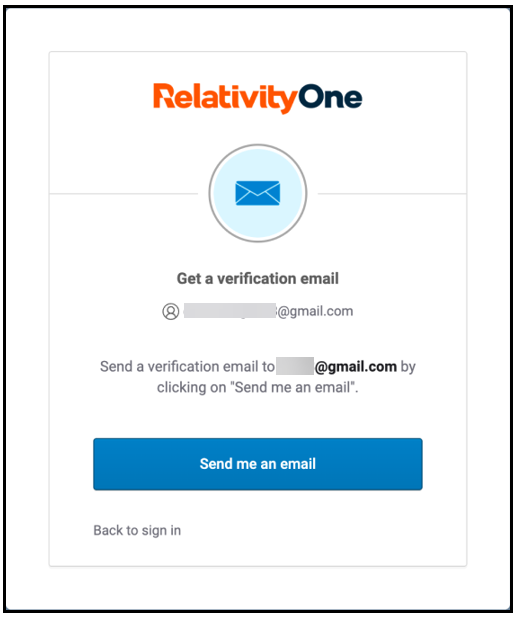
b. Set your password, re-enter your password, and click Next.



c. The user will be prompted to configure an optional MFA factor.

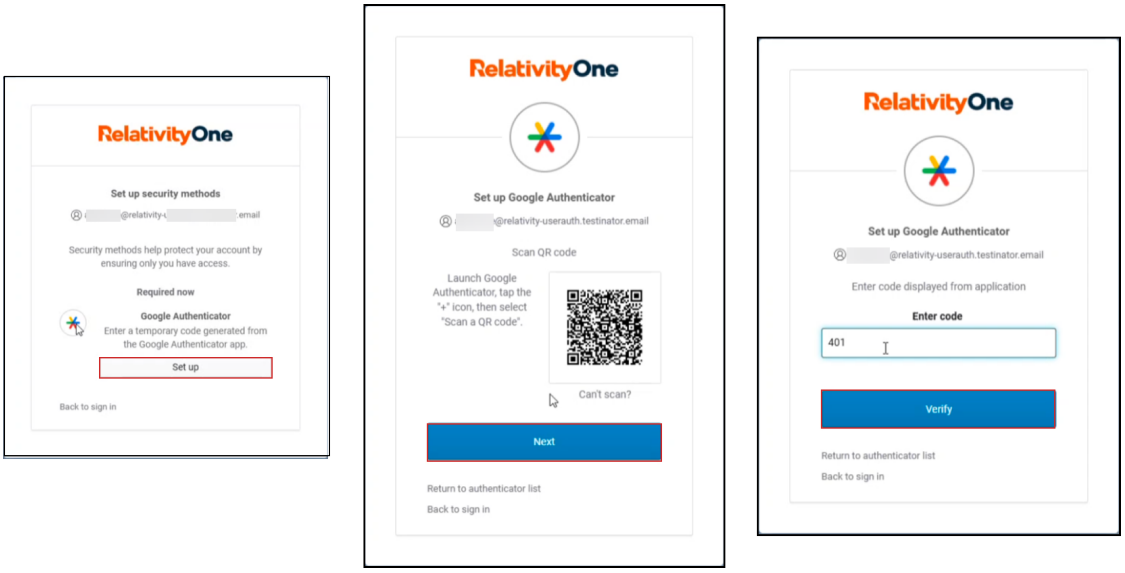
Note: This step is not required, and the user can simply click Continue to proceed.

d. If multi-factor authentication (MFA) is enabled, complete the MFA challenge based on the method configured:
    a. **Email**: Enter the one-time passcode sent to your email, then select "Send me an email".

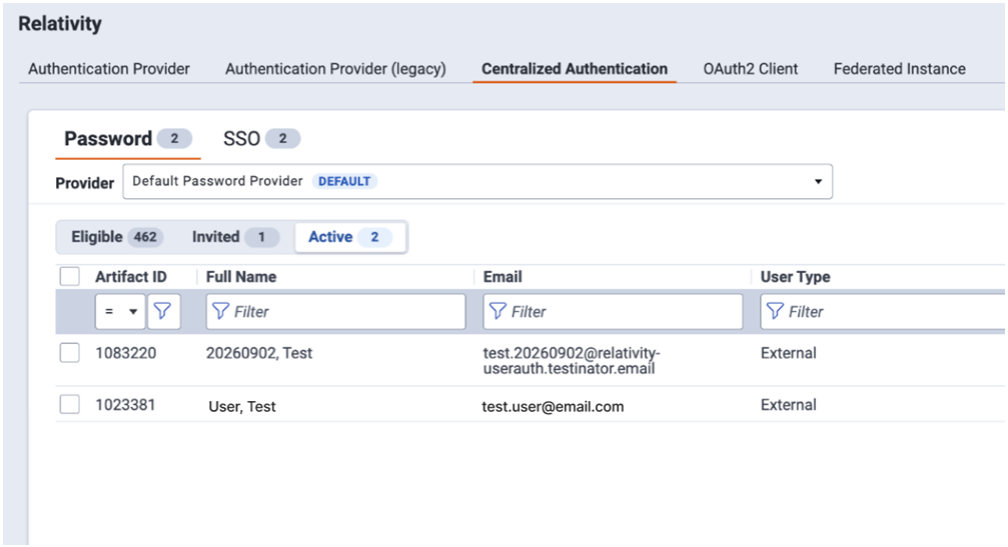


        i. **Authenticator app**: Select the Google Authenticator option, then use your preferred mobile authenticator app to scan the QR code displayed on the screen. Enter the one-time code

generated by the app in the provided field and click **Continue**.

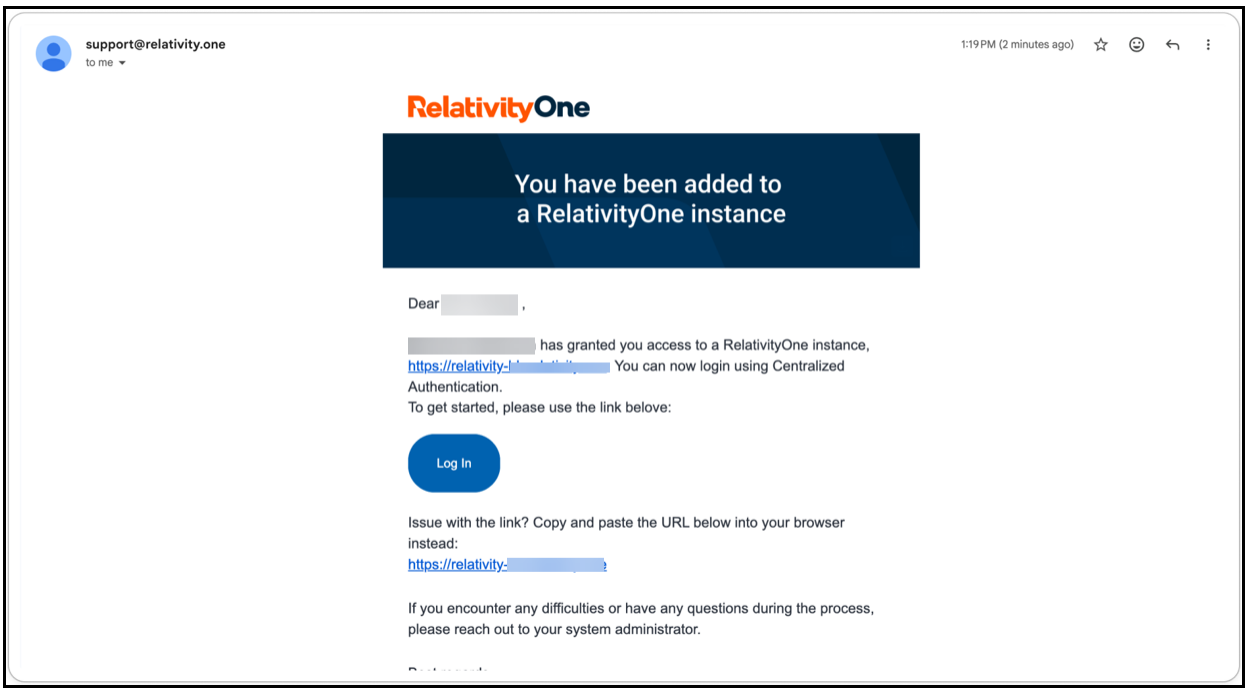


3. The user logs in to Relativity aiR using Centralized Authentication. Admins can verify the user's acceptance status by checking the **Active** list for the associated authentication provider in Centralized Authentication.



4.6.8 Existing Relativity aiR users

When an existing user is added to a new Relativity aiR instance, they receive a welcome email from **support@relativity.one** with the subject line "**Welcome to Relativity aiR.**" The email notifies the user that they have been added to another instance and confirms that they can log in using their current credentials.



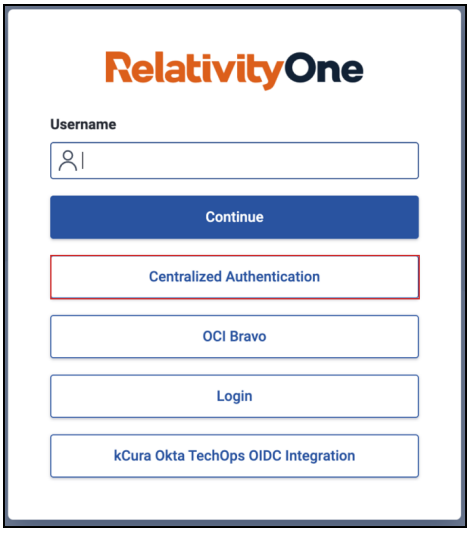
4.6.9 Logging in to Relativity aiR

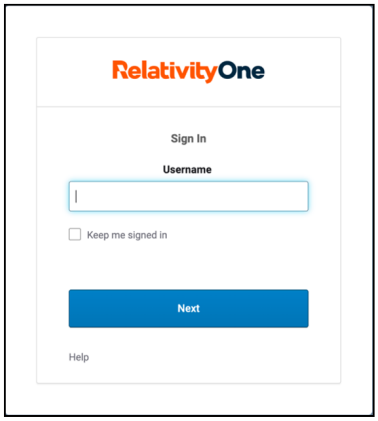
Your organization will notice a slight change in the login process as Centralized Authentication rolls out to users.

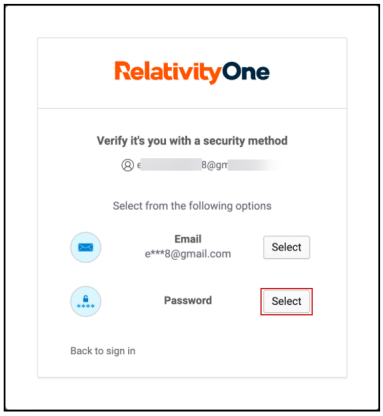
4.6.9.1 Transition period to Centralized Authentication

During the transition period, your organization will use both the legacy authentication and Centralized Authentication workflows to allow time for reviewing settings, registering SSO providers, and performing testing. During this time, the user login process works as follows:

1. Navigate to your Relativity aiR URL.
2. On the login page, click **Centralized Authentication**, then enter your **Username** and select **Password** as your method of verification.





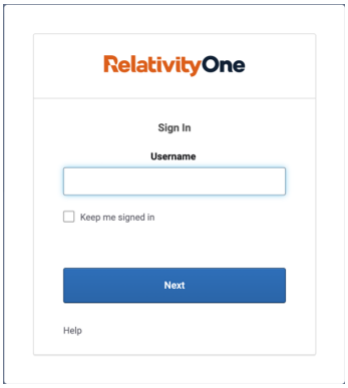


Note: Users should login with their existing Relativity aiR password. If MFA is enabled, you will be prompted either to send a verification email to receive a one-time code or to enter the code from your Authenticator app. You can enter your password or one time code first; the other option will be requested afterward.

4.6.9.2 Centralized Authentication login

Once the transition period ends and your organization is fully using Centralized Authentication, the user login process will work as follows:

1. Navigate to your Relativity aiR URL.



> **Notes: Relativity Support is not able to reset user passwords.**To reset your password, go to the Relativity aiR login page. After entering your email address (username) and clicking Next, the **Forgot your password?** link will appear. If you still do not see this option, please contact your Relativity aiR system administrator for assistance, as only they can reset your password. Relativity Support cannot perform password resets on behalf of users.

- **Using Password login**: Enter an email address and click Next, then select your verification method (password, email, or authenticator app) and follow prompts to complete the process.

4.6.9.3 Force Password Change

Use the **Force Password Change** option on a user's detail page when they need to create a new password.

When enabled:

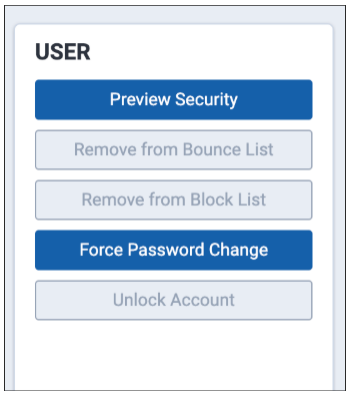
- The user's current password will expire immediately.
- At their next sign-in with a password provider, the user enters their current password, then sets a new one to continue.
- No password reset email is sent as part of this process.

Steps for the administrator

To force a password change, complete these steps:

1. Navigate to the Users tab and open the user's detail page.
2. In the console, select **Force Password Change**.

Note: This action may appear as **Force Password Reset** until the label update is fully rolled out.



3. Confirm the action when prompted.
4. Tell the user to sign in and set a new password.

What the user sees next

After you force the change, the user completes these steps:

1. The user signs in with their email address and current password.

Note: If MFA is required, the user completes it during sign-in.

2. Relativity prompts the user to change their password.
3. The user sets and confirms a new password. The password must meet the password provider requirements.
4. The user continues into Relativity aiR.

When to use Force Password Change vs. Forgot password

Use the following table to choose the right action:

Situation	Recommended action
The user knows their password, and you need them to set a new one.	Use **Force Password Change**.
The user does not know their password.	The user clicks the **Forgot your password?** link on the login page after entering their email address. Admins do not set passwords under Centralized Authentication.
The user cannot complete MFA with their authenticator app.	Reset the authenticator app, then have the user re-enroll at the next sign-in. See Reset a User's Authenticator App.

Note: Force Password Change is not the legacy **Send Password Reset Email** workflow. Under Centralized Authentication, the user handles password creation and self-service reset. Relativity Support cannot reset user passwords.

4.6.9.4 Reset a User's Authenticator App

Follow these steps to reset a user's Authenticator App:

Note: Users may need to reset their Authenticator app when switching phones or changing apps (for example, from Google Authenticator to Microsoft Authenticator).

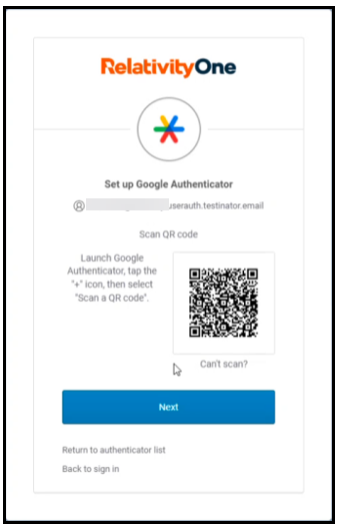
1. Navigate to the Users tab and open the user's detail page.
2. Select Reset Authenticator App.



3. After the reset, the system displays a success message.
4. Notify the user that they need to sign in again.

What the user sees next

1. The user signs in with their username and password.
2. After entering their password, the system prompts them to scan a QR code to set up their Authenticator app.



3. The user enters the one-time code generated by the app and signs in successfully.

4.7 SSO setup

Centralized Authentication supports single sign-on (SSO). A guided wizard on the **Authentication Provider** tab walks you through the setup. You can configure your identity provider, test the connection, and enable it for your users.

The wizard is the same for every provider. Each provider topic describes only the settings that differ, so start here first.

4.7.1 Supported identity providers

The wizard supports the following identity providers:

- **Okta (Org2Org)**—connects an Okta org-to-org integration using private key JWT authentication.
- **Microsoft Entra ID**—connects a Microsoft Entra ID application.
- **Google Workspace**—connects a Google Cloud client.
- **Custom SAML**—connects any SAML 2.0-compliant identity provider.
- **Custom OIDC**—connects any OpenID Connect (OIDC)-compliant identity provider.

Each provider uses the same wizard. The provider topics cover only the settings unique to that provider.

Note: To use your existing SSO provider with Centralized Authentication, re-register the connection in Relativity with the wizard. For best results, open your identity provider in a second window, or work with someone who has access to it.

4.7.2 Prerequisites

Complete these items before you register an SSO provider:

- Confirm your browser allows traffic to **login.relativity.one**, ***.okta.com**, and ***.oktacdn.com**.
- Open your identity provider in a separate browser window.
- Confirm you have administrator access to your identity provider, or work with someone in your organization who does.

4.7.3 Registration workflow

Registering an SSO provider requires you to move between Relativity and your identity provider (IdP). The following table shows where each part of the setup takes place.

Task	Where you do this
Start the wizard and select your identity provider type.	Relativity
Create or configure an application for Relativity.	Identity provider
Enter the connection values from your application.	Relativity
Add the redirect callback URI and grant user access.	Identity provider
Test the connection, then finish the wizard.	Relativity, then sign in to your identity provider

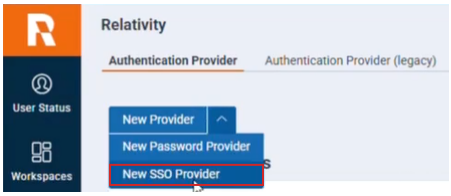
4.7.4 SSO setup wizard

The wizard walks through the same stages for every provider. You create an application in your identity provider, enter the connection settings, exchange a redirect URL, grant access, and test the connection. The connection settings differ by provider, so see your provider topic for the exact fields.

4.7.4.1 Registering an SSO provider

To register an SSO provider:

1. Navigate to the **Authentication Provider** tab.
2. Click **New SSO Provider**.



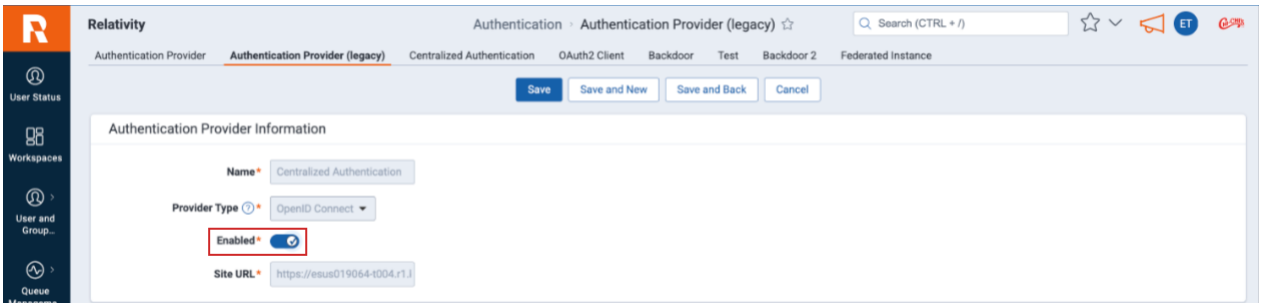
3. Enter a display name.
4. Select your identity provider, then click **Next**.
5. Create or configure an application in your identity provider. For the steps, see the topic for your provider.

6. Enter the connection settings the wizard requests. The fields vary by provider.
7. Copy the redirect URL from the wizard, and paste it into the sign-in redirect field in your identity provider.
8. Grant, or confirm access to the appropriate users or groups in your identity provider.
9. Click **Test Connection**. A window opens and prompts you to sign in to your identity provider.
10. Complete the sign-in prompt. A green check mark confirms success, and a red error indicates a problem to resolve.
11. Click **Finish**. The new provider appears on the **Authentication Provider** tab.

Note: If your identity provider requires multi-factor authentication (MFA), complete the MFA prompt during the connection test.

If your instance is currently migrating to Centralized Authentication, follow this step to complete the transition. After you test the connection, enable the Centralized Authentication provider.

On the **Authentication Provider (legacy)** tab, open the **Centralized Authentication** provider. Set the **Enabled** toggle to on, then click **Save**. This will update your login page to the Centralized Authentication login page, and you will no longer see your previous login options.



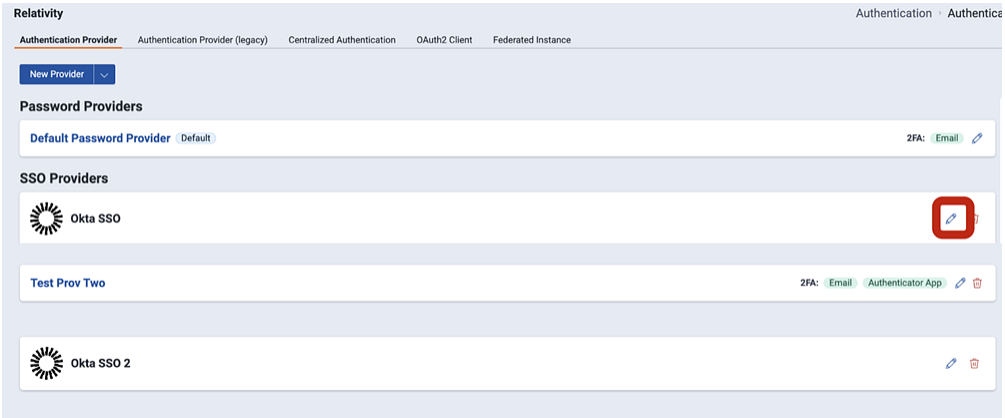
4.7.4.2 Editing an SSO provider

You may need to update an SSO provider to change its name or, more commonly, to rotate the certificate or secret. To do this, edit the SSO provider and then use **Test Connection** to confirm the configuration.

Note: You must update or rotate your own SSO certificate or client secret. Relativity support cannot perform this action for you.

To edit an SSO provider:

1. On the **Authentication Provider** tab, find the provider you want to change.
2. Click the **Edit** icon (pencil). The wizard reopens.



3. Update the values you want to change.
4. Complete the wizard to apply your changes.

4.7.5 Considerations

Review the following before and after setup:

- To use an existing SSO provider with Centralized Authentication, re-register the connection in the wizard.
- Trusted IPs for SSO providers are configured in your identity provider, not in Relativity.
- SSO users do not need to be sent nor accept an invitation from Relativity. You create the user in Relativity and grant access through your identity provider.
- Ensure the user email address is the same between the two
- The connection fields differ by provider. See your provider topic for the required fields.

4.7.6 Related topics

4.7.7 Okta (Org2Org)

Okta Org2Org connects an Okta org-to-org integration to Relativity as a single sign-on (SSO) provider. Okta Org2Org authenticates with a private key JWT, so it does not use a client secret.

This topic covers the settings specific to Okta Org2Org. For the shared wizard steps, see SSO setup on page 108.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

4.7.7.1 Before you begin

Complete these items before you configure the provider:

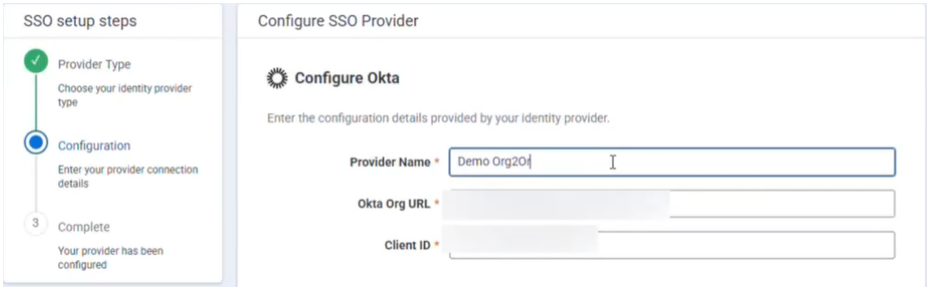
- Create an Okta org-to-org integration in your Okta org.
- Confirm you have administrator access to your Okta org.
- Review the prerequisites in Prerequisites on page 109.

4.7.7.2 Okta Org2Org settings in Relativity

When you reach the connection screen in the wizard, complete these fields:

- **Provider Name**—enter a name for the connection.
- **Okta Org URL**—enter your Okta org URL. Copy it from the browser address bar, and remove **admin** from the address.

- **Client ID**—enter the Client ID from your Okta org-to-org connection. To get this value, see Getting the Client ID from Okta below.



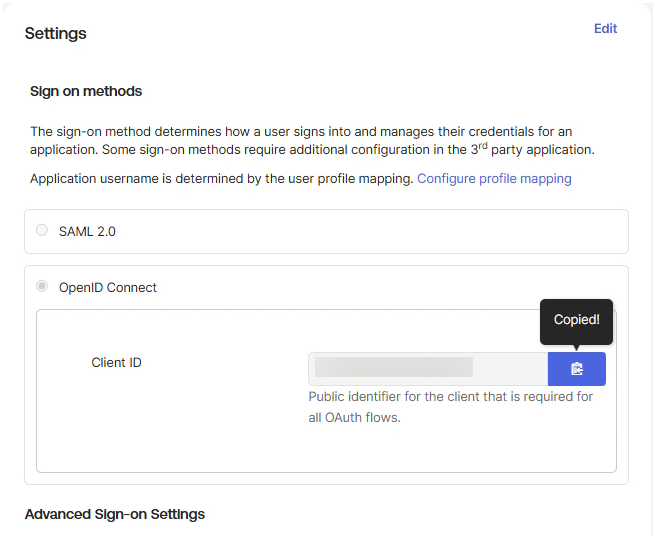
Note: Okta Org2Org uses private key JWT authentication. You do not enter a client secret for this provider.

4.7.7.3 Getting the Client ID from Okta

Generate the Client ID in your Okta org-to-org connection before you enter it in Relativity.

To get the Client ID:

1. In Okta, open your org-to-org connection.
2. On the **Sign On** tab, click **Edit**.
3. Select **OpenID Connect**.
4. Click **Save**. Okta generates a Client ID.
5. Copy the Client ID.

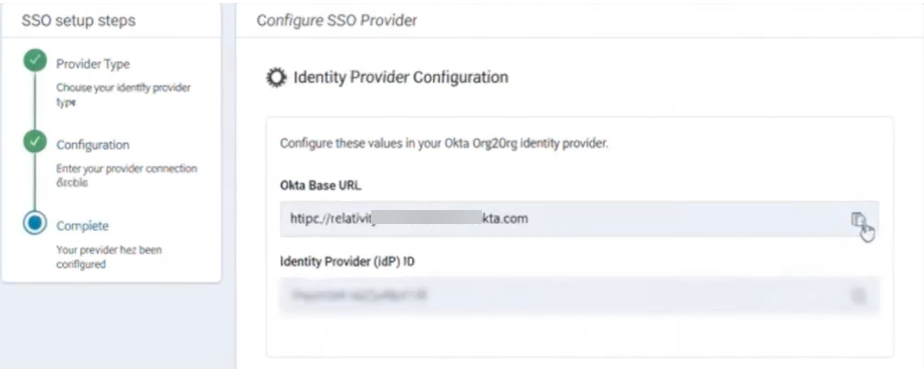


4.7.7.4 Completing the connection in Okta

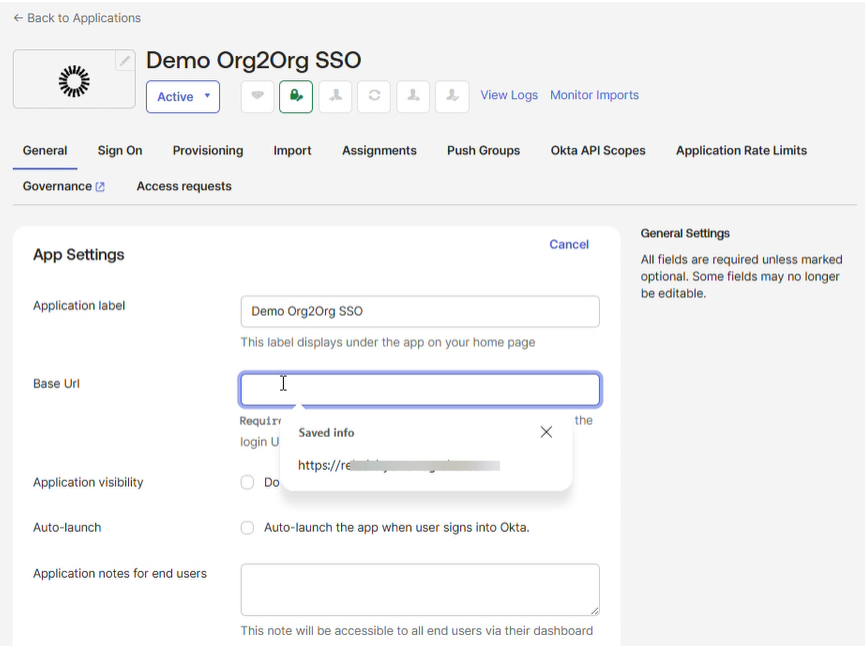
After you enter the Relativity settings and continue, the wizard generates two values. Copy each value into your Okta org-to-org connection.

To copy the Okta base URL value:

1. In the wizard, copy the Okta base URL value.



2. In Okta, open the org-to-org connection.
3. On the **General** tab, click **Edit**.
4. Paste the value into the **Base URL** field.

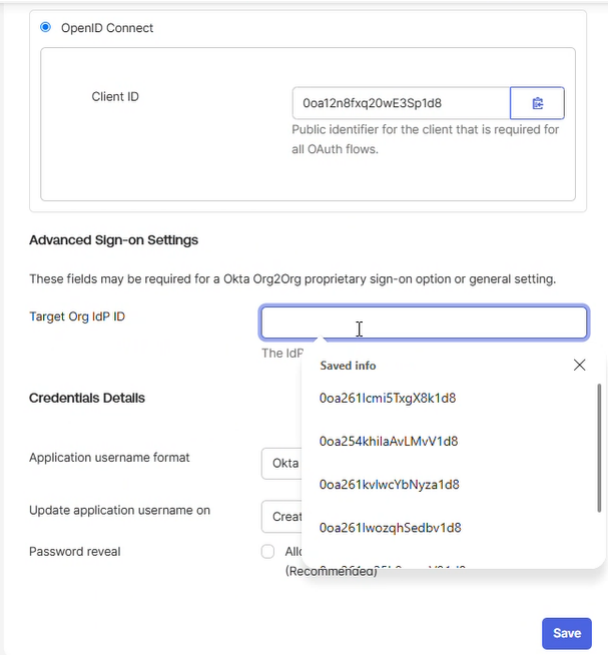


5. Click **Save**.

To copy the target org IdP value:

1. In the wizard, copy the target org IdP value.
2. In Okta, on the **Sign On** tab, click **Edit**.

3. Paste the value into the **Target org IdP** field.



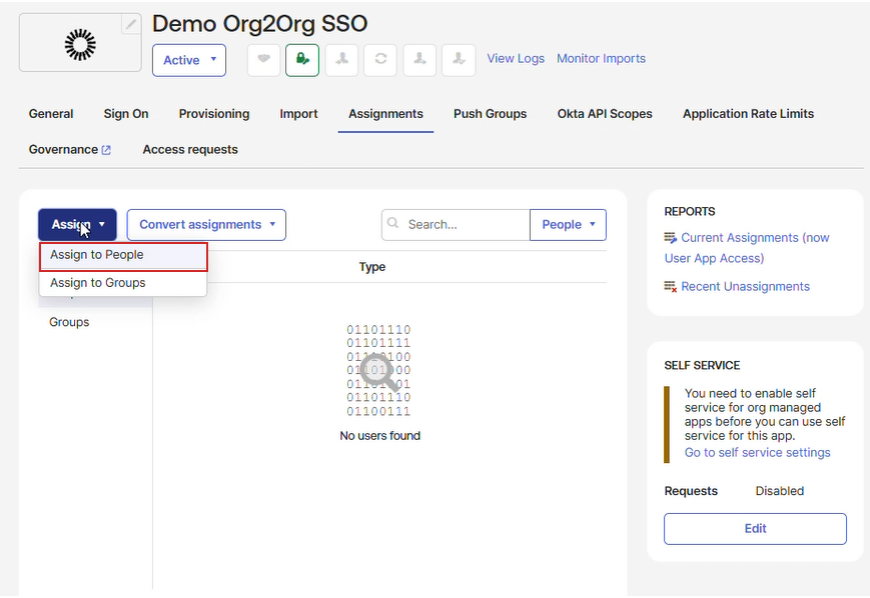
4. Click **Save**.

4.7.7.5 Assigning users in Okta

Before you test the connection, assign your users to the application in Okta.

To assign users to the application:

1. In Okta, navigate to the Assignments tab and click the Assign button.



2. Assign the user or group and click **save**.

Note: If you do not assign a user in Okta, the connection test fails for that user.

4.7.7.6 Testing and enabling the provider

To test the connection and finish setup, follow the shared steps in Registering an SSO provider on page 109. The test connection triggers a login to your Okta org using the configured settings. A green check mark confirms success, and a red error indicates a problem to resolve.

4.7.7.7 Related topics

4.7.8 Microsoft Entra ID

Microsoft Entra ID connects an Entra ID application to Relativity as a single sign-on (SSO) provider using OpenID Connect.

This topic covers the settings specific to Microsoft Entra ID. For the shared wizard steps, see SSO setup on page 108.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

4.7.8.1 Before you begin

Complete these items before you configure the provider:

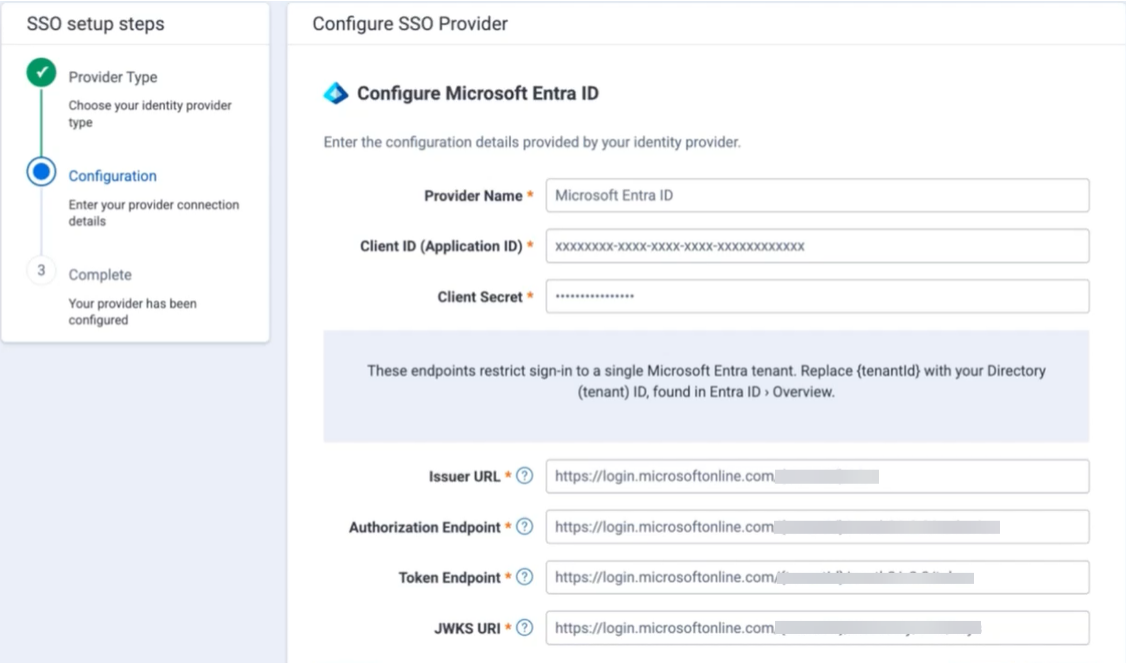
- Register an application for Relativity in Microsoft Entra ID.
- Confirm you have administrator access to the Azure portal.
- Review the prerequisites in Prerequisites on page 109.

4.7.8.2 Microsoft Entra ID settings in Relativity

When you reach the connection screen in the wizard, complete these fields:

- **Name**—enter a name for the connection.
- **Client ID**—enter the Application (client) ID from your Entra ID application.
- **Client Secret**—enter a client secret that you create in Entra ID.
- **Issuer URL**—enter the issuer from your application endpoints.
- **Authentication endpoint**—enter the OAuth 2.0 authorization endpoint (v2.0).
- **Token endpoint**—enter the OAuth 2.0 token endpoint (v2.0).

- **JWKS URI**—enter the JWKS URI from your application endpoints.



Note: If you have your Entra ID tenant ID, you can enter it to populate the endpoint values instead of entering each endpoint separately.

4.7.8.3 Getting the values from Entra ID

Collect these values from your application in the Azure portal before you enter them in Relativity.

To get the values:

1. In the Azure portal, open your application registration.
2. Copy the Application (client) ID.
3. Create a client secret.
4. Copy the client secret value.
5. Click **Endpoints**.
6. Copy the following values:
    - the issuer
    - the OAuth 2.0 authorization endpoint (v2.0)
    - the OAuth 2.0 token endpoint (v2.0)
    - the JWKS URI

4.7.8.4 Adding the redirect URL in Entra ID

After you enter the Relativity settings and continue, the wizard generates a redirect URL. Add it to your Entra ID application.

To add the redirect URL:

1. In the wizard, copy the redirect URL.
2. In the Azure portal, open your application registration.

3. Click **Authentication**.
4. Add the redirect URL under the **Web** platform.
5. Click **Save**.

Note: Assign your users to the application in Entra ID so they can sign in.

4.7.8.5 Granting admin consent

An administrator must grant consent for the **User.Read** permission. This consent lets Relativity read the resources it needs in Microsoft Entra ID.

4.7.8.6 Testing and enabling the provider

To test the connection and finish setup, follow the shared steps in Registering an SSO provider on page 109. The test connection triggers a login to your Okta org using the settings configured. If your organization requires multi-factor authentication (MFA), complete the MFA prompt.

4.7.8.7 Related topics

4.7.9 Google Workspace

Google Workspace connects a Google Cloud client to Relativity as a single sign-on (SSO) provider using OpenID Connect.

This topic covers the settings specific to Google Workspace. For the shared wizard steps, see SSO setup on page 108.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

4.7.9.1 Before you begin

Complete these items before you configure the provider:

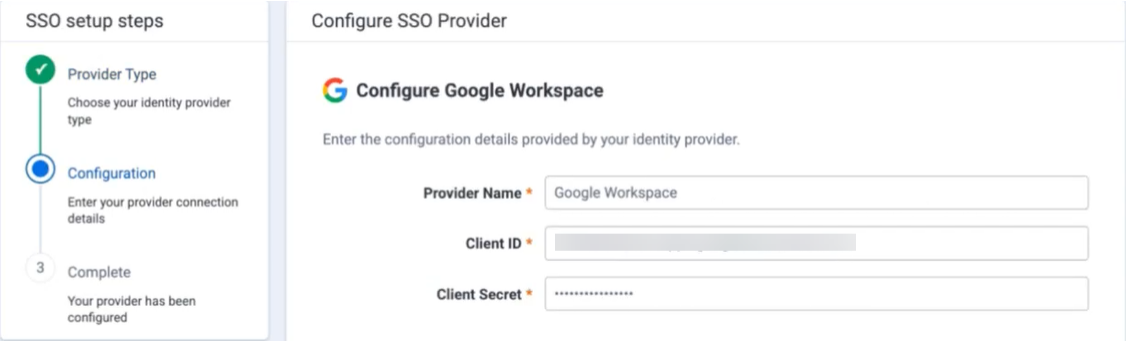
- Create a project in the Google Cloud console.
- Confirm you have administrator access to the project.
- Review the prerequisites in Prerequisites on page 109.

4.7.9.2 Google Workspace settings in Relativity

When you reach the connection screen in the wizard, complete these fields:

- **Name**—enter a name for the connection. The name must be unique, fewer than 120 characters, and cannot contain backslashes.
- **Client ID**—enter the Client ID from your Google Cloud client.

- **Client Secret**—enter the Client Secret from your Google Cloud client.



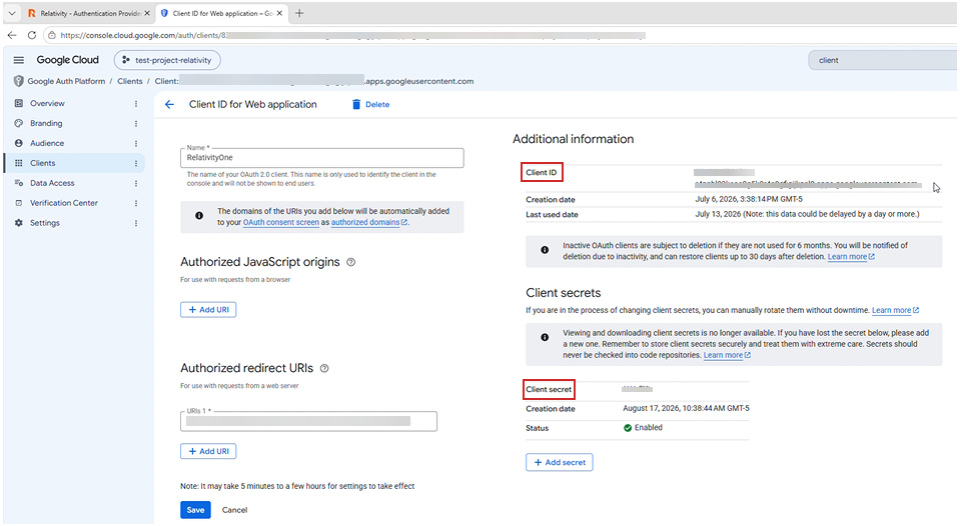
Note: Google displays the client secret only once. Copy and save it when you create the client.

4.7.9.3 Getting the values from Google Cloud

Create a client in the Google Cloud console and copy its credentials before you enter them in Relativity.

To get the values:

1. In the Google Cloud console, open your project.
2. Go to the **Clients** tab.
3. Create a client.
4. Select **Web application**.
5. Enter a name for the client.
6. Click **Create**. Google generates a Client ID and a Client Secret.
7. Copy the Client ID and the Client Secret.

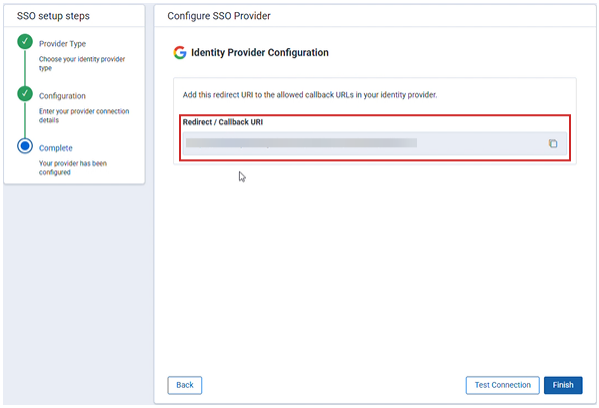


4.7.9.4 Adding the redirect URI in Google Cloud

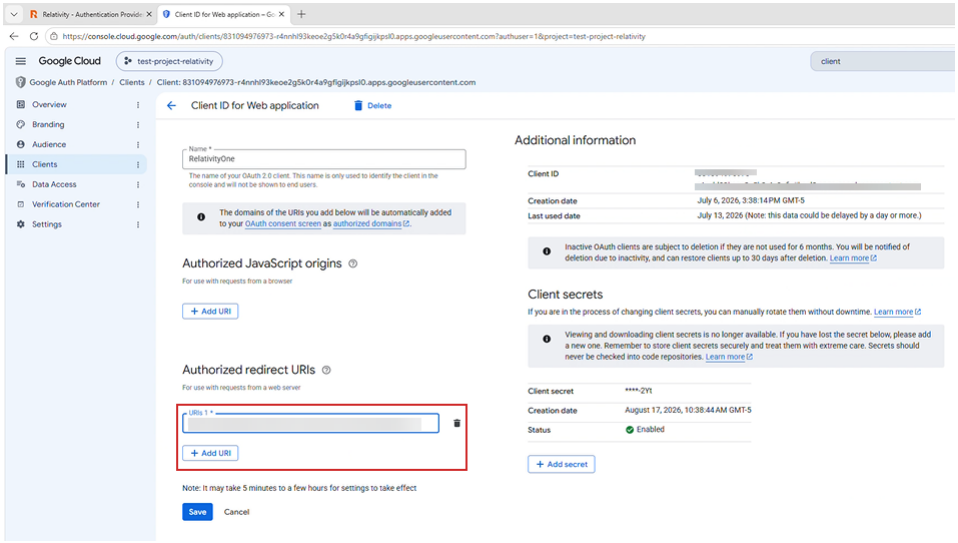
After you enter the Relativity settings and continue, the wizard generates a redirect URI. Add it to your Google Cloud client.

To add the redirect URI:

1. In the wizard, copy the redirect URI.



2. In your Google Cloud client, add the redirect URI to the authorized redirect URIs.



3. Click **Save**.

4.7.9.5 Testing and enabling the provider

To test the connection and finish setup, follow the shared steps in Registering an SSO provider on page 109. The connection test prompts you to sign in with your organization email address. If your organization requires multi-factor authentication (MFA), complete the MFA prompt.

4.7.9.6 Related topics

4.7.10 Custom SAML 2.0

Some identity providers do not have a dedicated option in the SSO setup wizard. For those providers, select **SAML 2.0** and enter the connection details yourself.

This topic covers the **SAML 2.0** settings only. For the shared wizard steps, see SSO setup on page 108.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

4.7.10.1 When to use SAML 2.0

Select **SAML 2.0** in the Provider Type step when both of the following are true:

- Your identity provider supports the SAML 2.0 protocol.
- Your identity provider does not have its own option in the Provider Type step.

Identity providers that commonly use this option include ADFS, Duo, Keycloak, and PingFederate.

Note: Some identity providers support both SAML 2.0 and OpenID Connect. Select the protocol your provider is configured for. For OpenID Connect, see Custom OpenID Connect on the next page.

4.7.10.2 Before you begin

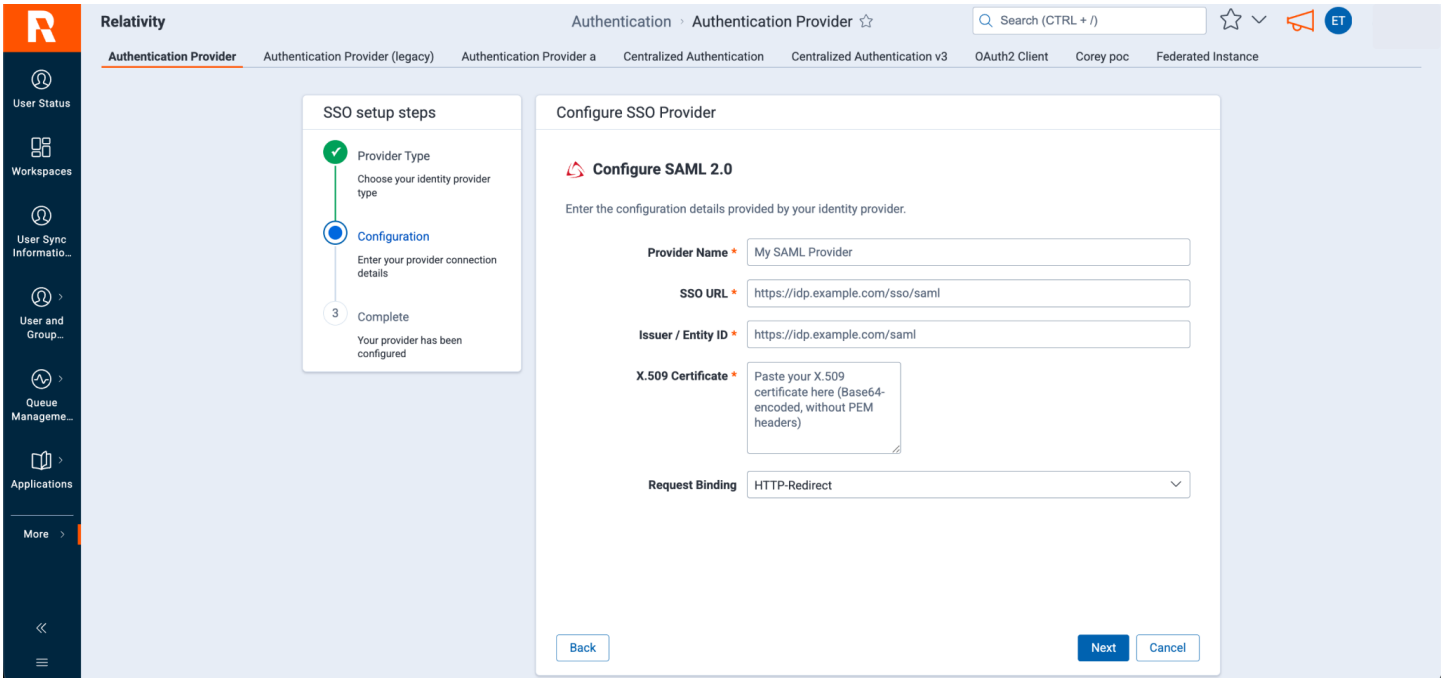
Complete these items before you start the wizard:

- Create an application for Relativity in your identity provider.
- Confirm you have administrator access to your identity provider.
- Review the prerequisites in Prerequisites on page 109.

Note: Open your identity provider in a separate browser window while you work through the wizard. You move values between the two systems.

4.7.10.3 SAML 2.0 settings in Relativity

Enter the configuration details from your identity provider on the Configure SSO Provider screen.



Complete these fields:

- **Provider Name**—enter a name for the connection. The login page shows this name on the SSO button.
- **SSO URL**—enter the single sign-on URL from your identity provider.
- **Issuer / Entity ID**—enter the unique identifier of your identity provider.
- **X.509 Certificate**—paste the Base64-encoded signing certificate from your identity provider. Remove the PEM header and footer lines.
- **Request Binding**—select the binding your identity provider expects. The default value is **HTTP-Redirect**.

Provider Name, **SSO URL**, **Issuer / Entity ID**, and **X.509 Certificate** are required.

Note: Relativity aiR supports only the RSA-SHA256 assertion signing algorithm. Configure your identity provider to sign assertions with that algorithm.

4.7.10.4 Getting the values from your identity provider

Collect these values in your identity provider before you start the wizard. Field labels differ by provider, so check your provider's documentation for the equivalent name.

- The single sign-on URL, sometimes called the SSO endpoint or the login URL.
- The issuer, sometimes called the entity ID or the IdP identifier.
- The signing certificate.

For the steps to create the application and locate these values, see your identity provider's documentation.

4.7.10.5 Testing and enabling the provider

After you enter the settings, the wizard generates a callback URL. Add it to your identity provider, then test the connection.

For these shared steps, see Registering an SSO provider on page 109.

Note: Assign your users to the application in your identity provider before you test the connection. The test simulates a login.

4.7.10.6 Related topics

4.7.11 Custom OpenID Connect

Some identity providers do not have a dedicated option in the SSO setup wizard. For those providers, select **OpenID Connect** and enter the connection details yourself.

This topic covers the **OpenID Connect** settings only. For the shared wizard steps, see SSO setup on page 108.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

4.7.11.1 When to use OpenID Connect

Select **OpenID Connect** in the Provider Type step when both of the following are true:

- Your identity provider supports the OpenID Connect (OIDC) protocol.
- Your identity provider does not have its own option in the Provider Type step.

Identity providers that commonly use this option include Duo, Keycloak, and PingFederate.

Note: Some identity providers support both OpenID Connect and SAML 2.0. Select the protocol your provider is configured for. For SAML 2.0, see Custom SAML 2.0 on page 119.

4.7.11.2 Before you begin

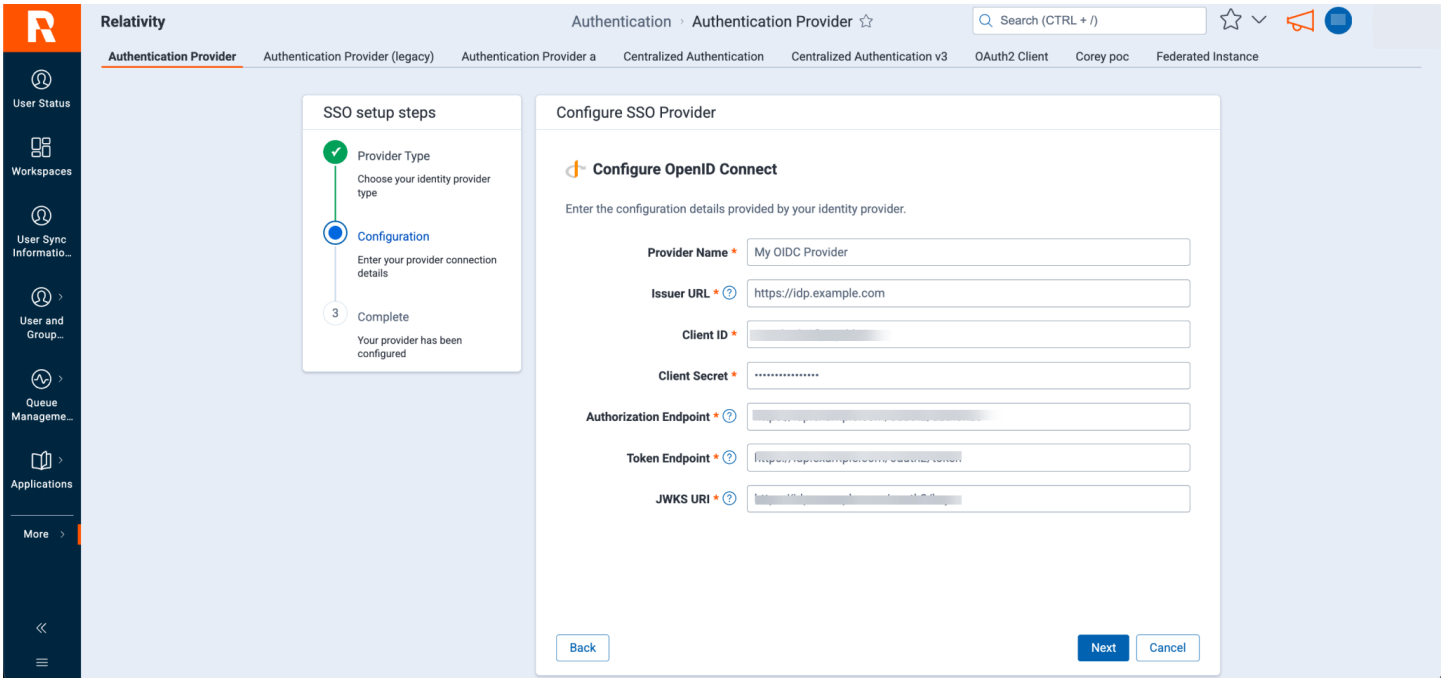
Complete these items before you start the wizard:

- Create an OIDC application for Relativity in your identity provider.
- Confirm you have administrator access to your identity provider.
- Review the prerequisites in Prerequisites on page 109.

Note: Open your identity provider in a separate browser window while you work through the wizard. You move values between the two systems.

4.7.11.3 OpenID Connect settings in Relativity

Enter the configuration details from your identity provider on the Configure SSO Provider screen.



All of these fields are required:

- **Provider Name**—enter a name for the connection. The login page shows this name on the SSO button.
- **Issuer URL**—enter the issuer from your identity provider.
- **Client ID**—enter the client ID from the application you created for Relativity.
- **Client Secret**—enter the client secret from that application.
- **Authorization Endpoint**—enter the authorization endpoint from your identity provider.
- **Token Endpoint**—enter the token endpoint from your identity provider.
- **JWKS URI**—enter the JSON Web Key Set (JWKS) URI from your identity provider.

Note: Many identity providers display the client secret only once. Copy and store it when you create the application.

4.7.11.4 Getting the values from your identity provider

Collect these values in your identity provider before you start the wizard. Field labels differ by provider, so check your provider's documentation for the equivalent name.

- The client ID and client secret from your OIDC application.
- The issuer.

- The authorization endpoint, the token endpoint, and the JWKS URI.

Many identity providers publish the issuer, the endpoints, and the JWKS URI together at their OpenID configuration endpoint.

For the steps to create the application and locate these values, see your identity provider's documentation.

4.7.11.5 Testing and enabling the provider

After you enter the settings, the wizard generates a callback URL. Add it to your identity provider, then test the connection.

For these shared steps, see Registering an SSO provider on page 109.

Note: Assign your users to the application in your identity provider before you test the connection. The test simulates a login.

4.7.11.6 Related topics

4.8 Managing user authentication methods

As a system admin, you must assign at least one authentication method to each user in order for them to log in. A user can have multiple login methods but only one Password.

Note: These steps apply to instances that have not transitioned to Centralized Authentication. In Centralized Authentication, password settings, two-factor authentication, and trusted IP addresses are managed on the authentication provider rather than on the individual user. For more information, see Centralized Authentication on page 94.

4.8.1 Invitation workflow

A significant security improvement to the Relativity authentication process is that the system admin no longer knows or can set user passwords. The invitation workflow, called that because you invite users to log in to Relativity, is the new mechanism for them to set and to manage their own passwords. Now, a system admin (when creating a new user), or a user (if they forget their password) initiates an email sent to them at their specified address, and they create or reset their password directly within Relativity.

Note: For help with single sign-on error messages, please see the SSO Troubleshooting console on page 153.

The invitation workflow applies to the following methods:

- Password below
- Two-factor authentication on the next page
- Password Outside Trusted IP on page 125

4.8.1.1 Password

The password option requires the user to enter only a password for authentication. It does not require an additional check or two-factor criterion.

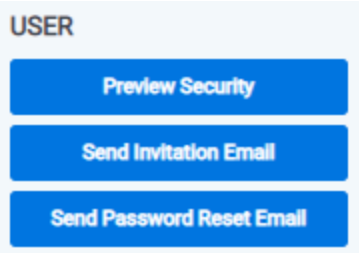
To assign and to configure this option for a user:

1. After creating a new user, edit their profile (**Users** tab, and click their full name).
2. In the **Login Method (User)** section, click **New**.

3. In the **Login Method Information** pop-up window, select the password provider method from the Provider drop-down list.
   The **Default Password Settings** section appears.
4. Disable the **Enable Two-factor Authentication** toggle. For more information, see Two-factor authentication below.
5. Set the **Default Password Settings**.
   - **Can Change Password** - Allows the user to change their password at any time.

     Note: End users can set their initial password when they receive their invite, regardless of this setting's value.

   - **Require Change Password on Next Login** - enable to prompt the user for a new password at their next login. The user must first log in with their current password. This setting does not recover a forgotten password.
   - **Maximum Password Age** - enable to set number of days a password can work. Set the number of days in the text box.
   - **Set Password for User** - enable to create a password for the user.
6. Click **Save**.
7. Click **Send Invitation Email**.



   This sends an invitation email to the user at the email address listed in their profile's User Information section. By default, the link in the email is valid for one week (10080 minutes).

   Note: You can use the InvitationLinkLifetimeInMin instance setting to increase the default invitation link expiration period.

   If the email can't be sent because your system email SMTP settings are not configured properly, a warning is displayed.

   You can also use the Invite mass action on the Users tab to send invitation email to multiple users.

4.8.1.2 Two-factor authentication

The two-factor authentication is a variation of the Password method that requires a passcode in addition to a password.

To assign and configure this option for a user,

1. Edit their profile (**Users** tab, and click their full name).
2. In the **Login Method (User)** section, click **New**.
3. In the **Login Method Information** pop-up window, select the password provider method from the Provider drop-down list.
   The **Default Password Settings** section appears.

4. Enable the **Enable Two-factor Authentication** toggle.
5. Select the **Mode**, "always provide passcode" or "ignore passcode for Trusted IPs."
6. Select the **Method**, use an "authenticator app" or "email" address.

   Note: Both the Email and Authenticator App challenge methods are supported. Relativity recommends the Authenticator App, and you should use it whenever possible, because it provides a more secure authentication experience than email-based verification.

7. Set the preferred **Default Password Settings**.
8. Click **Save**.

For authenticator app, the user will follow the instructions on the app or enter the app's passcode. For email two-factor authentication, the system emails a passcode to the user during logon, and it's different each time. For more information on signing in with an authenticator app, see the Admin Guide.

Note: The link in the email is valid for 5 minutes, and only the most recently-sent email can be used. The link expiration time is not configurable.

4.8.1.3 Password Outside Trusted IP

The Outside Trusted IP is a variation of the Password method that requires a passcode only if the user logs in outside of a specified IP range. If the log on is inside the trusted range, then only a password is required.

Note: Password reset emails are not generated for users logging in via 2FA from an untrusted IP address. To initiate a password reset in these cases, an administrator must send a reset link from a trusted IP address.

To assign and to configure this option for a user:

1. After creating a new user, edit their profile (**Users** tab, and click their full name).
2. In the **Login Method (User)** section, click **New**.
3. In the **Login Method Information** section, select the password provider method from the Provider drop-down list. The **Login Method Settings** section appears. You can assign only one instance from among Password RSA methods.
4. Select **Require only for non Trusted IPs** in the **Two-factor Authentication** section.
5. Enter the user's email address you want to send the password to in the Email Address field. This address can be different from the email in the user's profile.
6. Click **Save** and then **Back**.
7. Click **Send User Invitation Email**.

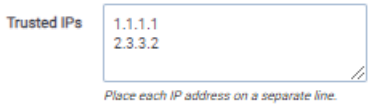
4.8.1.4 To define a Trusted IP range:

You define an IP address or addresses as valid locations from which users can log in from in a combination of two settings.

The second setting specifies a valid IP address or addresses for each user. This can be an individual address, a range of addresses, or combination of either. The specified range is called the Trusted IPs. Users outside of this range or ranges won't be able to login except by using Password authentication with the Two Factor Mode set to **Outside Trusted IPs**.

To set the user Trusted IP range:

1. Select the **Users** tab.
2. Click the user's name.
3. Click **Edit**.
4. Enter the IP range in the **Trusted IPs** field. If you have multiple trusted IPs, enter each IP range on a new line.



5. Click **Save**.

By default, no value is empty, which indicates any IP address is valid.

In case of setting the user's Trusted IP range, you can specify an individual address, a range of addresses, or a combination of either, separate each one with a carriage return.

Addresses use the "###.###.###.###" format. The following wildcards are available for both settings:

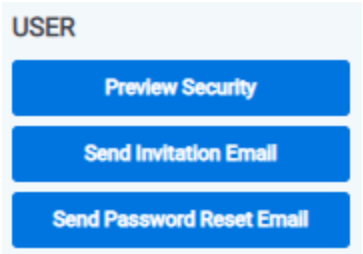
Type	Description	Example
Asterisk (*) (Asterisk wildcard)	Matches zero or more characters.	192.168.31.*. You can't use this notation with the match range of digits wildcard.
Hash (#) (Hash wildcard)	Matches any single digit 0-9.	192.168.31.**##**. You can't use this notation with the match range of digits wildcard.
[start-end] (Match range of digits wildcard)	Matches a range of digits.	192.168.31. **[0-255]**. You can't use this notation with the asterisk and/or hash wildcards.
16-bit mask	A 16-bit number that masks an IP address.	192.168.0.0/16 is the same as 192.168.0.0/255.255.0.0. Network address range is 192.168.0.0-192.168.255.255.
24-bit mask	A 24-bit number that masks an IP address.	192.168.31.0/24 is the same as 192.168.31.0/255.255.255.0. Network address range is 192.168.31.0 - 192.168.31.255.
25-bit mask	A 25-bit number that masks an IP address.	192.168.31.0/25 is the same as 192.168.31.0/255.255.255.128. Network address range is 192.168.31.0 - 192.168.31.127.

4.8.1.5 Password reset

To reset a user's password, send them an email with a reset link. Relativity Support does not reset passwords for end users.

To reset a user's password:

- Click **Send Password Reset Email**.



The link in the email is valid for 15 minutes. Use only the most recently sent email. You can use the **[confirm setting name]** instance setting to extend the reset link lifetime.

Note: Resetting a password is not the same as requiring a password change. To require a new password at next login, use **Require Change Password on Next Login**. That setting does not recover a forgotten password.

If the **Forgot your password?** link is unavailable in your environment, the user must contact you. You then send a password reset email.

4.8.2 Manually setting passwords

By default, system admins can't set or see user passwords. Instead, system admins can send a password reset email, and users create and manage their own passwords. However, there are some situations, such as for testing or project development, that may require system admins to explicitly and manually set passwords.

To set this option in your Relativity instance, add the **AdminsCanSetPasswords** instance setting to the **Relativity.Authentication** section and set it to **True**. You must manually enter this setting and value because it is not present from the default Relativity installation.

Note: When Centralized Authentication is enabled, administrators cannot manually set user passwords. The **AdminsCanSetPasswords** instance setting will have no effect in this mode. Password creation/reset is handled exclusively by the user via the Centralized Authentication workflow.

To set a password, use the following procedure.

1. After creating a new user, open their profile (Click the Users tab, and then click their full name).
2. In the **Login Method (User)** section, click **New**.
3. In the **Login Method Information** section, select the password provider method from the **Provider** drop-down list.
   The **Login Method Settings** section appears.You can assign only one instance from among Password and RSA methods.
4. Select **Set Password** to **True**.
   The password requirements appear.
5. Enter the password in the **Password** field.
6. Re-enter the password in the **Retype Password** field.
7. Click **Save** and then **Back**.

The password information doesn't appear except when you're editing it. If a current password exists, it doesn't appear either. Each new password overwrites the existing password.

4.8.3 OpenID Connect

1. After creating a new user, edit their profile (**Users** tab, and click their full name).
2. In the **Login Method (User)** section, click **New**.
3. In the **Login Method Information** section, select the OpenID Connect provider method from the **Provider** drop-down list. The **Login Method Settings** section appears.
4. Enter the subject identifier for the authentication provider as the **OpenID Connect Subject**.
5. Click **Save** and then **Back**.

4.8.4 SAML 2.0

1. After creating a new user, edit their profile (**Users** tab, and click their full name).
2. In the **Login Method (User)** section, click **New**.
3. In the **Login Method Information** section, select the SAML 2.0 provider method from the **Provider** drop-down list. The **Login Method Settings** section appears.
4. Enter the subject identifier for the authentication provider as the **SAML2 Subject**. For example, if you select Email as the application username in Okta, you must enter the Relativity user's email here.
5. Click **Save** and then **Back**.

4.9 Microsoft Entra ID - OpenID Connect

Microsoft Entra ID can be set up as an OpenID Connect authentication provider to log users into a different Relativity instance. You need to complete some steps within Microsoft Entra ID and Relativity to user Entra ID OpenID Connect.

Note: We support B2C (business-to-customer) SSO integration through the OIDC and SAML2 protocols. Customers whose provider supports either of these protocols can integrate with Relativity aiR. The following steps focus on registering an Azure application and credentials for Entra ID. If you're setting up Relativity with EntraID External ID (formerly known as AzureAD B2C), please refer to Microsoft's documentation.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

4.9.1 Registering an Azure application and credentials

Before you begin configuring Entra ID in Relativity, you will need to add Relativity as an application within Entra ID.

1. Log in to Azure Portal.
2. Navigate to **App registrations**for **Microsoft Entra ID** (formerly known as Azure Active Directory).
3. Click **New registration**.
4. Enter an application name in the **Name** field.
5. Accept the default setting, **Accounts in this organizational directory only**, as the supported account type.
6. Click **Register**.
7. Copy the **Application (client) ID** that was generated and past it to a safe location, as it will be used in a later step.
8. Click the **Endpoints** button.
9. Copy the **OAuth 2.0 authorization endpoint (v2) URL** that was generated and past it to a safe location, as it will be used in a later step.
10. Trim the oauth2/v2.0/authorize from the URL. For example:
    - *https://login.microsoftonline.com/8a3fa923-3223-4978-9d4d-fa012e19898b/oauth2/authorize*
    - *https://login.microsoftonline.com/8a3fa923-3223-4978-9d4d-fa012e19898b/*

4.9.2 Configuring Entra ID OpenID Connect

Review the following list of settings that display on the Authentication Provider form. You can configure or update these settings based on your authentication needs.

4.9.2.1 Authentication provider information

- **Name**—enter a user-friendly name for the authentication provider.
- **Provider Type**—select OpenID Connect.
- **Enabled**—the provider is enabled by default. However, you can disable it.
- **Site URL**—set the URL that users enter in the browser to access an instance of Relativity.

4.9.2.2 Authentication provider settings

- **OAuth2 Flow**—select either **Implicit** or **Code**.
- **Client ID**—enter the Entra ID's Application ID.
- **Display on Login Screen**—determines if the OpenID Connect button displays on the login page.
- **Login Screen Button Text**—determines the text that appears on the button displayed on the login page.
- **Authority URL**—enter the Authority from the trimmed **OAUTH 2.0 AUTHORIZATIONENDPOINT** from step 9 in Configuring your external identity provider.
- **Scopes**—the default value for this field is **openid**. The **openid** checkbox must be selected because it's a required setting. However, you can also select the email or profile option. The identity provider responds with the claims associated with the scopes that you request. In other words, the scopes translate into claims that you can use.
- **Subject Claim Type**—the default value for this field is **sub**. Enter one of the following values based on the scopes that you set:

  Notes: In Microsoft Entra ID, email is an optional claim and is not included in the OpenID token by default. Consider using upn instead. Consult with your Entra ID administrator to determine which claim type is best suited for your organization. For more information, see the Microsoft documentation on optional claims.

  - If you selected only OpenID in the Scopes field, this field must be set to **sub**.
  - If you selected OpenID and email in the Scopes field, set this field to **upn**.
  - If you selected OpenID and profile in the Scopes field, set this field to a property available from the identity provider. These properties differ for each provider.

  The identity provider sends an identity token to you, which contains the claims for your selected scopes. When you request only the openid scope, then sub is used as the claim type. It often represents a unique identifier for the user within your system. If you are using Entra ID, then see Microsoft identity platform ID tokens for a full list of token identifiers.

4.9.2.3 Completing your external identity provider set up

1. Log in to Azure Portal.
2. Navigate to the application you created earlier.
3. Click **Authentication**.
4. Add your **Redirect URL** from the Relativity Authentication Provider. Keep the Type field set to Web.

5. Complete the scenario that matches the value you selected for OAuth2 Flow.
    - Scenario: you selected **Implicit** for OAuth2 Flow.
        1. Check the **ID Tokens** box.
        2. Click **Save**.
    - Scenario: you selected **Code** for OAuth2 Flow.
        1. Click **Certificates & Secrets**.
        2. Click **New client secret**.
        3. Click **Add**.
        4. Copy the client secret value.
        5. Navigate back to the Authentication Provider in Relativity.
        6. Click **Edit**.
        7. Paste the value for **Client Secret** with the value from step 4.
        8. Click **Save**.

4.9.2.4 Adding users to the application in Azure

1. Click **Azure Active Directory**.
2. Click **Enterprise Applications**.
3. Click into the application that you created for Relativity authentication.
4. Click **Users and groups**.
5. Click **Add user**.
6. Select your users.
7. Click **Assign**.

4.10 SAML 2.0 provider

SAML is an open-standard format for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP).

Note: As a service provider, Relativity supports **SAML IdP-initiated single sign-on (SSO)**. However, it does not support **SP-initiated SSO.**

Relativity uses SAML assertions (tokens) to verify the users mapped to the identity provider. SAML assertions contain information on the identity of the individual who has logged in. Assertions also contain the identity provider issuing the assertion, known in Relativity as the Issuer URL. Each Assertion is typically prepared for a specific receiver, known as the Audience. Assertions protect this information by cryptography signing it. An Assertion is only valid if it is from a known Issuer URL to the expected Audience and correctly signed.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

4.10.1 Considerations

- SAML assertions must be cryptographically signed for Relativity to verify their authenticity. Make sure your SAML IdP is configured accordingly.
- You can use Relativity with any SAML 2.0-compliant IdP, such as Centrify, Okta, Microsoft Active Directory Federation Service (ADFS), or OneLogin.
- Relativity aiR only supports the **RSA-SHA256** assertion signing algorithm.
- After saving the Authentication provider for the first time, the system generates the Redirect URL. Placeholder values may need to be added to the third-party Authentication setup before obtaining this value.

4.10.2 Configuring a SAML 2.0 authentication provider

To add a SAML 2.0 authentication provider, complete the fields below.

Authentication Provider Information

- **Name**—enter a user-friendly name for the authentication provider.
- **Provider Type**—select SAML2.
- **Enabled**—the provider is enabled by default, but you can disable it.
- **Site URL**—set the URL that users enter in the browser to access an instance of Relativity.

Authentication Provider Settings

- **Audience**—the unique identifier of the service provider (SP). We recommend using the same value as your Site URL.
- **Issuer URL**—the unique identifier of the identity provider (IdP).
- **Certificate**—an x509 certificate provider by the identity provider.
- **Subject Claim Type** (Optional)—The attribute in the SAML subject used to validate the login. We recommend to leave this blank.

4.10.3 Configuring specific SAML providers

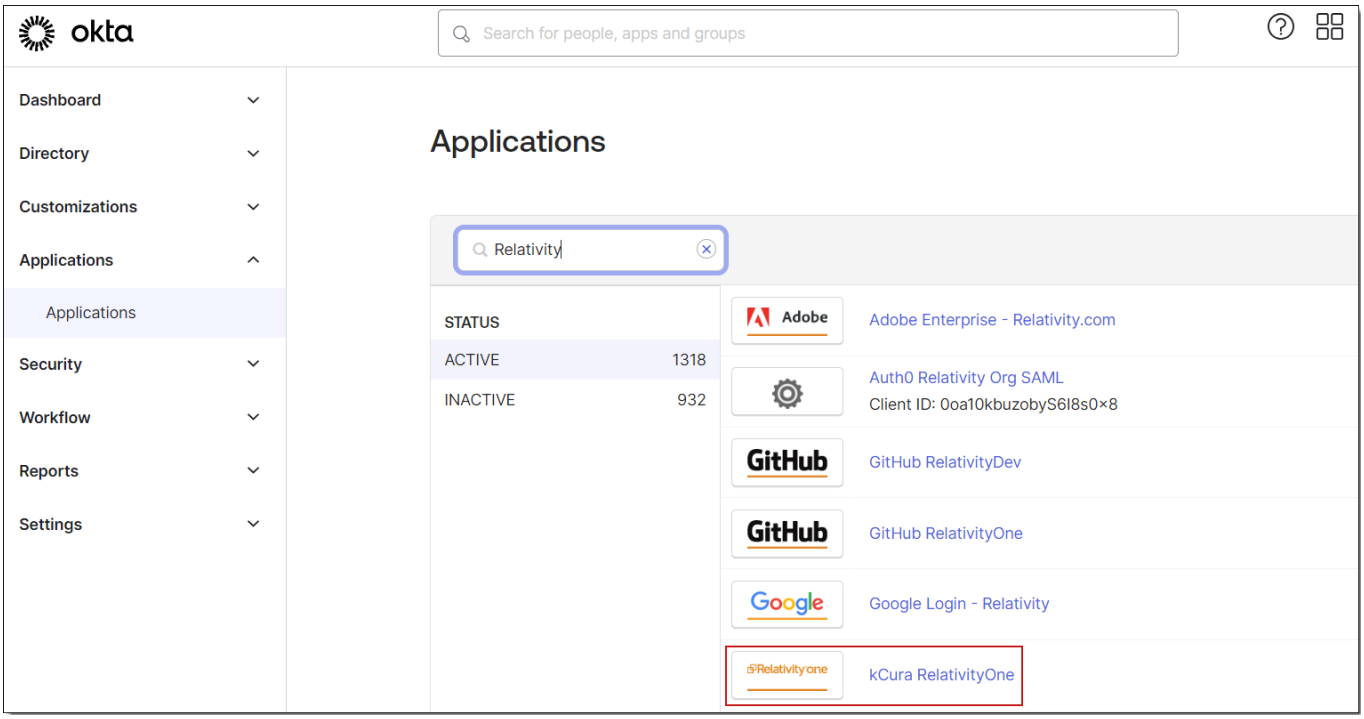
The following sections provides the guidelines for integrating Relativity with Okta and ADFS.

4.10.3.1 Configuring Okta as a SAML 2.0 identity provider

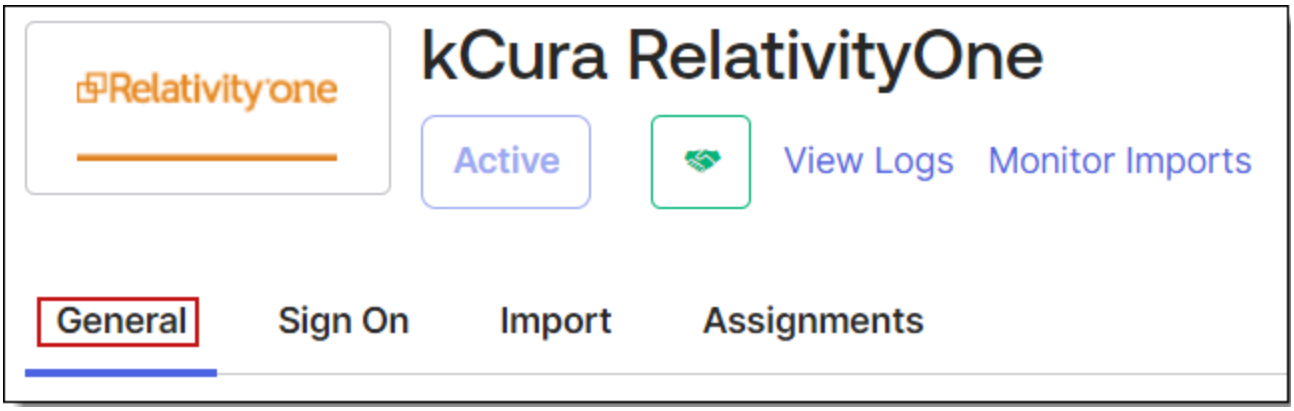
This is an example of configuring Okta.

Initial configuration:

1. In the Okta admin console, navigate to Applications and search for Relativity.



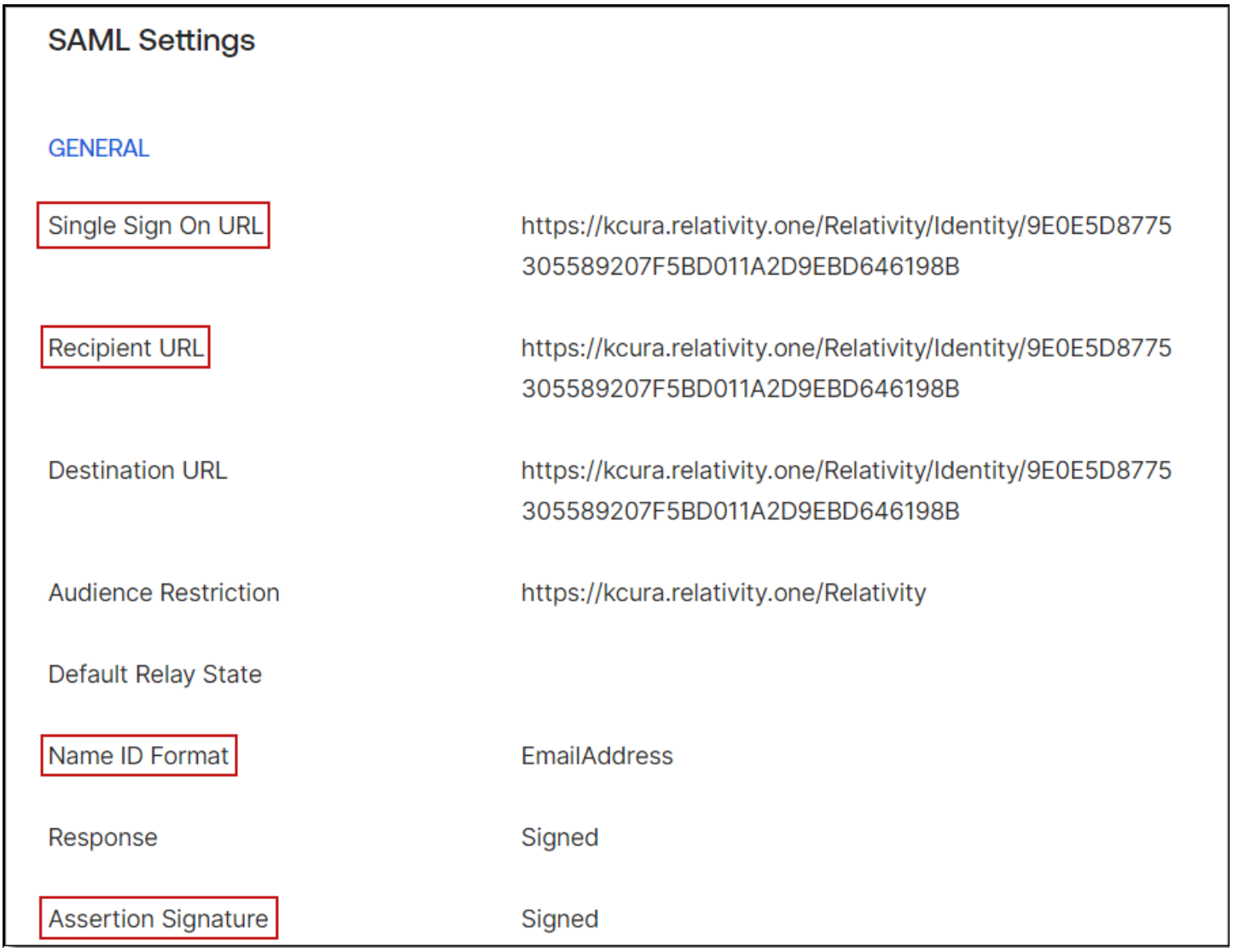
2. Navigate to the **General tab** and specify these SAML settings:



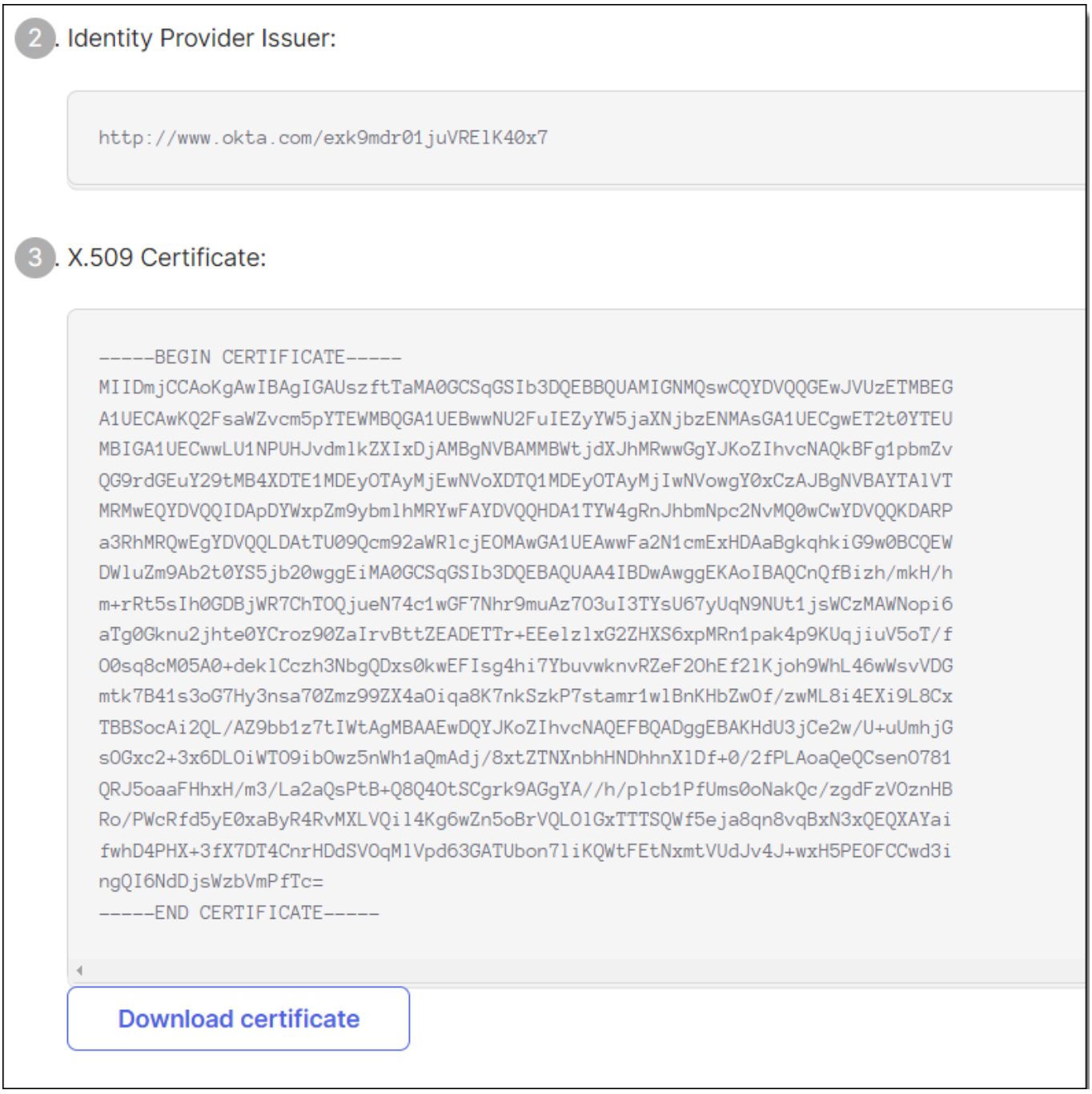
- For the single sign-on URL, for enter your Relativity Instance URL. This is the URL that is used for public access to go to your web servers.
- For Recipient URL, put in a unique identifier, such as the URL for your instance. Note this value for later.

  Note: Audience URI is case-sensitive. Specifying **/relativity** instead of **/Relativity** can break your authentication.

- For the Name ID Format you would like to use for logging in, select **Email**.
- For Assertion Signature, select Signed.



3. You have now partially configured you application in Okta to set up logging in to Relativity. You must now configure the SAML provider in Relativity. These Okta values can be found under the **Sign on** tab.
    - The Audience URI (SP Entity ID, from the previous step).
    - The Identity Provider Issuer (In Okta, click **View Setup Instructions** on the Sign On tab).
    - The X.509 Certificate (also in Setup Instructions).

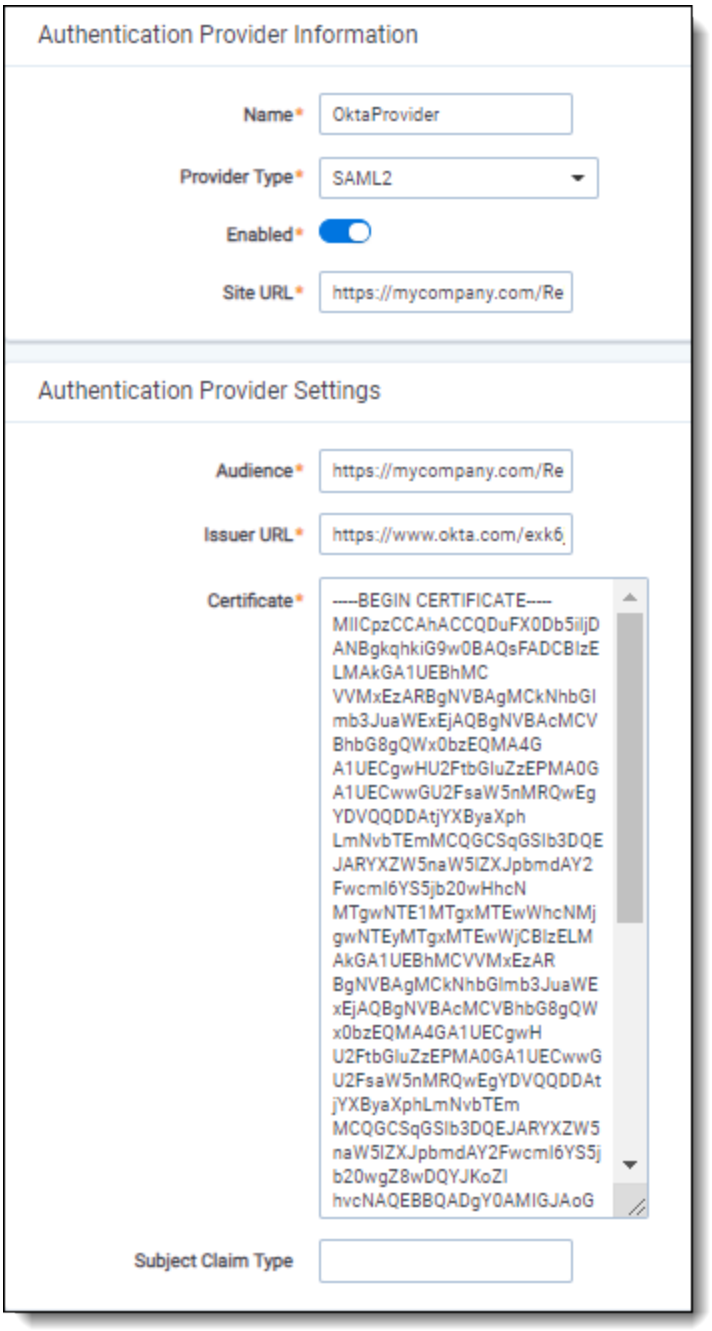


Note: Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

Next, set up the SAML 2.0 authentication provider in Relativity:

1. Log in to Relativity with system admin credentials.
2. Open the Authentication Provider tab.
3. Click **New Authentication Provider**. The Authentication Provider Information form opens.
4. Enter a name for your provider.

5. Select SAML2 from the Provider Type drop-down menu.



6. Enter the site URL. This is the URL users enter into the browser to access this instances of Relativity.
7. Enter the Audience URI (SP Entity ID) from Okta in the Audience field.
8. Enter the Identity Provider Issuer from Okta in the Issuer URL with.
9. Enter the X.509 certificate from in Okta in the Certificate field.
10. (Optional) If you are using a specific user identifier claim that is not the default claim, enter it as the Subject Claim Type.
11. Click **Save**.

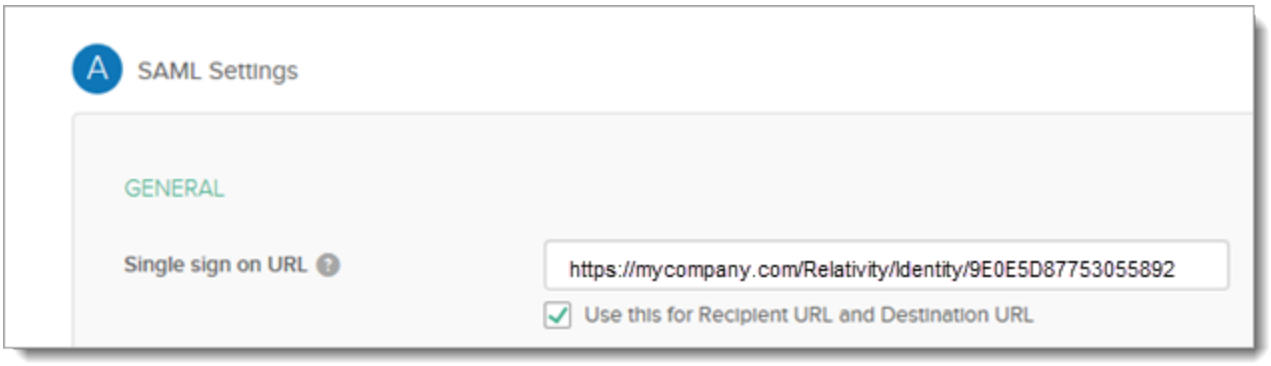
12. Note the Redirect URL on your new authentication provider.



You have now set up your Relativity instance to list for SAML 2.0 assertions at a given endpoint on your server (the Redirect URL).

Next, finish setting up the SAML IdP in Okta:

1. Log in to Okta and navigate to the application you created earlier.
2. Update the single sign-on URL to be the Redirect URL given to us by Relativity on the authentication provider you have created.



You have now configured Okta to send SAML 2.0 assertions to your Relativity instance, and Relativity is set up to verify the SAML assertions.

Note: You must also assign Okta users to the SAML application, and then map the users to SAML login method in Relativity. When configuring the login method, you must specify the user's email in the SAML2 Subject field (if you select Email as the application username in Okta). For more information, see Managing user authentication methods on page 123.

4.10.3.2 Configuring ADFS as a SAML 2.0 identity provider

You can also configure ADFS as a SAML 2.0 authentication provider for Relativity.

Note these terminology difference between Relativity and ADFS:

	ADFS	
Audience	Relying Party Identifier(s)	https://[company name].relativity.one/Relativity
Redirect URL	End-Point URL	https://[company name].relativity.one/Relativity/Identity/<random string>
Issuer URL	Services Trust End-Point (SAML)	http://<adfs-service>/adfs/services/trust
SAML Subject Name	Claim Type	Name ID, E-Mail Address, UPN (Leave blank in Relativity SAML Provider configuration)
n/a	Claim Rules	Incoming, Transformation, Outgoing Claim Rules (see below)

When setting up claim rules, you must send Name ID as default claim type for Relativity. Use these guidelines:

1. Add Send LDAP Attributes As Claims: Select Email Addresses or User-Principal-Name to E-Mail Address from the AD store.
2. Add Pass Thru Claim for E-Mail Address or a Transforming claim.
3. Add Transforming Claim (from E-Mail Address to Name ID).

4.11 OpenID Connect

OpenID Connect is an identity layer on top of the OAuth 2.0 protocol. You can verify the identity of the end user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end user. You can use any provider that supports the OpenID Connect protocol.

Note: FedRAMP requirements for Relativity aiR Gov instances mandate the customer's **Authority URL** must undergo a review by the Relativity Security team. Following a successful review, the URL will be added to the Relativity firewall allow list prior to setting up single sign-on authentication.

The following Authority URLs are already approved and do not require review:

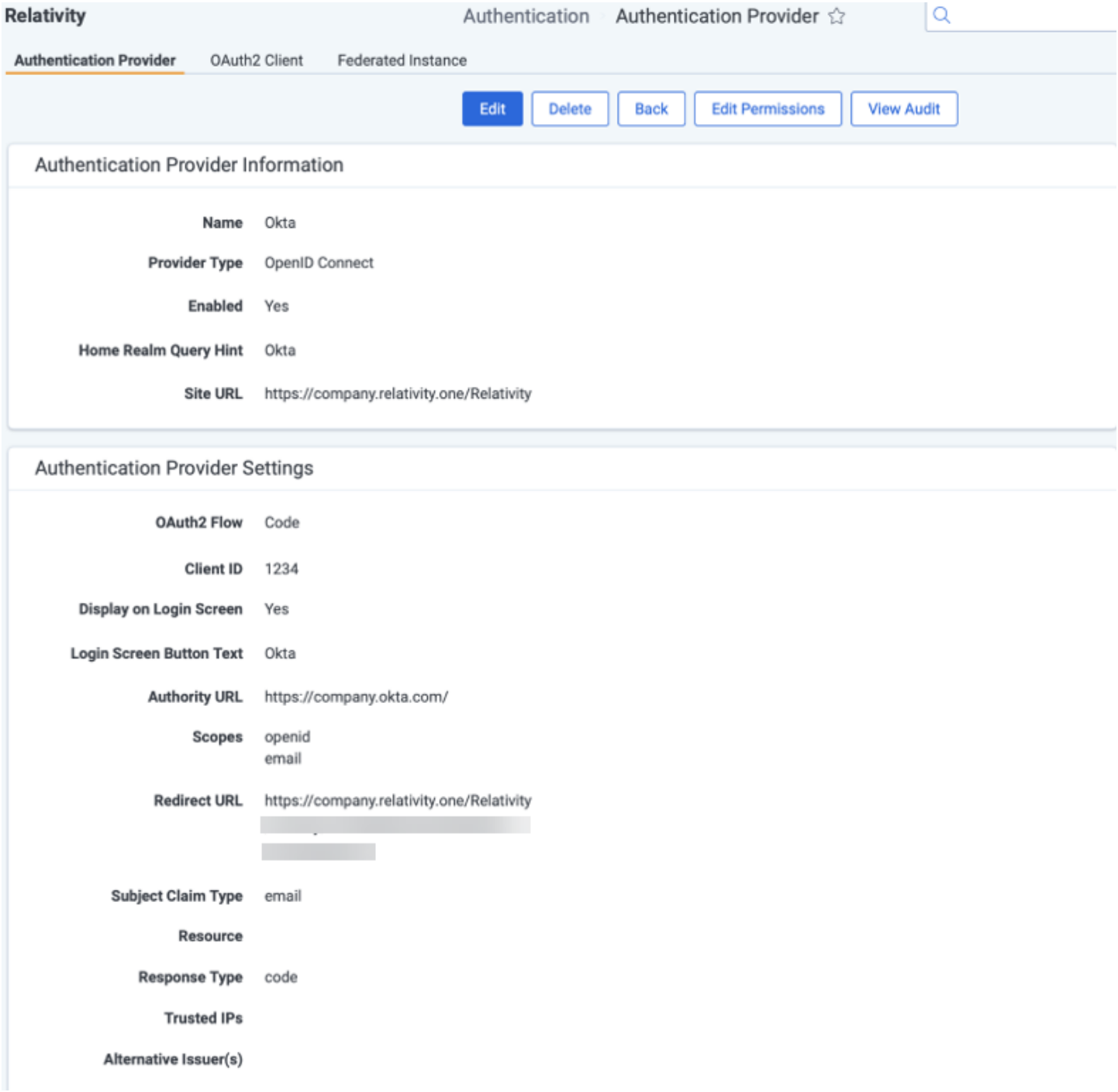
- okta.com
- login.microsoft.com
- login.microsoftonline.com
- login.microsoftonline.us
- login.windows.net

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

4.11.1 Configuring an OpenID Connect authentication provider

To add OpenID Connect on top of your OAuth2 configuration, enter the required information in the fields listed below.

Note: The Authentication Provider information (such as Client ID, Client Secret, and endpoints) should be generated by your Identity Provider (IdP), unless otherwise specified by your organization.



Authentication Provider Information

- **Name**—enter a user-friendly name for the authentication provider.
- **Provider Type**—select OpenID Connect.
- **Enabled**—the provider is enabled by default. However, you can disable it.
- **Site URL**—set the URL that users enter in the browser to access an instance of Relativity.

Authentication Provider Settings

- **OAuth2 Flow**—select either **Implicit** or **Code**.
- **Client ID**—enter your application's ID.

- **Display on Login Screen**—determines if the OpenID Connect button displays on the login page.
- **Login Screen Button Text**—determines the text that appears on the button displayed on the login page.
- **Authority URL**—enter the URL that hosts the OpenID configuration well-known endpoint.
- **Scopes**—the default value for this field is **openid**. The **openid** checkbox must be selected because it's a required setting. However, you can also select the email or profile option. The identity provider responds with the claims associated with the scopes that you request. In other words, the scopes translate into claims that you can use.
- **Redirect URL**—After saving the new Authentication Provider RDO (Relativity Dynamic Object), it will be shown in the settings.
    - **Example**—<https://company.relativity.one/Relativity/Identity D7158859-3355-46FB-96D1-78B1B0466AB1>
- **Subject Claim Type**—the default value for this field is **sub**. Enter one of the following values based on the scopes that you set:
    - If you selected only OpenID in the Scopes field, this field must be set to **sub**.
    - If you selected OpenID and email in the Scopes field, set this field to **upn**.
    - If you selected OpenID and profile in the Scopes field, set this field to a property available from the identity provider. These properties differ for each provider.

  The identity provider sends an identity token to you, which contains the claims for your selected scopes. When you request only the openid scope, then sub is used as the claim type. It often represents a unique identifier for the user within your system. If you are using Azure AD, then see Microsoft identity platform ID tokens for a full list of token identifiers.
- **Resource** — what is being accessed by your OIDC provider

  Note: This value should remain unchanged unless instructed otherwise by your IT department.
- **Response Type**—specifies how your provider responds to the authentication request. In this case, the response includes a code.

  Note: This value should remain unchanged unless instructed otherwise by your IT department.
- **Trusted IPs** — specifies a list of trusted IP addresses for a user. Authentication fails if a user attempts to log in to Relativity from an unauthorized OP address. This list of IPs is evaluated in conjunction with the individual user's trusted IP list.
- **Alternative Issuer(s)** - set this field to the issuer in your OpenID configuration if it does not match your authority URL. Refer to your IT department for guidance on if this field needs to be set

4.11.2 OpenID Connect authentication provider flows

There are two authentication provider flows used with Relativity: code flow and implicit flow. Below are two images showing a detailed OpenID Connect authentication flow for both.

4.11.3 Just-in-time provisioning

Just-in-time provisioning lets an admin control access Relativity environments through an external ID provider, such as Okta. Instead of creating groups in Relativity, they can be created in Okta or similar provider. When created in another provider and mapped in Relativity, the required login objects are automatically created in Relativity.

Note: JIT is only available with OpenID Connect and is not supported for SAML.

JIT provisioning takes user claims from the access token provided by the external ID provider and uses the claims to setup a User for login to Relativity.

JIT User Provisioning automatically creates the objects necessary for login, and the Required Claims feature restricts users from using JIT User Provisioning. For example, this feature can be used to restrict access to a tenant to users within a geographic region.

When a user logs in, Relativity checks to see if the client exists, then checks if the user exists. If both exist, Relativity then checks to see if the user group exists. If all these items exist, the user can log into Relativity. Personal group and Group claim mapping assignments are checked on every login. Users are assigned/removed to groups on every login, based on the Group Claim Mappings. For more information, see Group claim mapping below .

To set up just-in-time provisioning on the authentication provider page, complete the fields below.

- **Implement**—whether JIT Provisioning is enabled or disabled.
- **Client**—this sets the Relativity Client a user is assigned to when provisioned.
- **Username Claim Type**—the Claim Type used to set a user's username. This should be mapped the claim containing the email address.
- **First Name Claim Type**—the Claim Type used to set a user's first name.
- **Last Name Claim Type**—the Claim Type used to set a user's last name.
- **Personal Group**—toggle used to set if a Personal Group should be created for a user.
- **Personal Group Claim Type**—the Claim Type used to set the personal group's name.
- **Group Claim Type**—the Claim Type used with Group Claim Mappings when determining group assignments for a user.
- **Default Trusted IPs**—a list of IP address values that are automatically set to the user's TrustedIPs setting.

Note: The identity provider (IdP) must send the following claim types for just-in-time provisioning features to function correctly:

- User creation— the IdP must include the ***Username Claim Type***, ***First Name Claim Type***, and ***Last Name Claim Type*** in the token. If any of these claim types are not sent by the IdP, user creation does not take effect.
- Group mapping—the IdP must include the ***Group Claim Type*** in the token. If the Group Claim Type is not sent by the IdP, group mapping does not take effect.

4.11.3.1 Group claim mapping

This section will add the users to the specified group on login. The groups need to be existing in Relativity. A token can include two or more group mappings. Group assignments from Group Claim Mappings are performed on every login.

User Claims are provided by a client's identity provider. Relativity does not control the claims assigned to a user. Relativity only checks that the claims are present when provisioning a user. The claims are passed to Relativity in the access token from the client's identity provider during the login process.

Note: Group mapping claim values must be present in the token. Just-in-time user provisioning cannot query external endpoints (such as AzureAD's graph API) to determine group membership.

Any matching claims are then compared to the Group Claim Mappings. Claim values that match the Group Claim Mappings determine which group to assign a user as a member. If the user claims do not match any Group Claim Mappings, then the user is removed from that group.

Groups that users are added to outside of group claim mappings need to be administered manually.

4.11.3.2 Required claim

Required Claims is an optional setting that System Admins can configure on their authentication providers. Required claims is used to control what users gain access to a tenant. JIT user provisioning automatically creates the objects necessary for login, and the Required claims feature restricts users from using JIT user provisioning. For example, this feature can be used to restrict access to a tenant to users within a geographic region.

This setting is used with JIT-enabled authentication providers. Admins can set a list of claims that Relativity will check for when provisioning a user. A user must have at least one required claim to be a provisioned user. System Admins can set multiple claims as Required Claims, and a user must have at least one to pass the check.

The Required Claims check only works on the initial login. It will deny a user from being provisioned. If a user already exists in the system, then Required Claims does not affect login.

4.11.3.3 Personal claim group

The Personal Group feature allows for controlling permissions at the user level within Relativity. Normally, permissions in Relativity are set on the Group object. By creating a group for every user in Relativity (a user's personal group), you can effectively set permissions for individual users. This is an optional feature.

4.11.4 Okta OpenID Connect

Okta can be set up as an OpenID Connect authentication provider to log users into a different Relativity instance.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

4.11.4.1 Pre-requisites

- To configure Okta as an OpenID Connect provider for Relativity, you, or your Okta admin, will need to set up the Relativity app in Okta. To complete this part of the configuration, follow the steps in the Okta documentation. During the process, select Web as the platform and OpenID Connect as the sign-on method. After completing the steps provided by Okta and customizing the steps for Relativity, you will navigate back to Relativity.
- The Okta 'Initiate login URI' setting may need an HRD parameter. For more information, see Creating or editing a federated instance.

4.11.4.2 Configuring Okta OpenID Connect

In Relativity, navigate to the Authentication Provider tab. On the Authentication Provider, fill in the fields as follows:

Authentication provider information

- **Name**—enter a user-friendly name for the authentication provider.
- **Provider Type**—select **OpenID Connect**.
- **Enabled**—the provider is enabled by default. However, you can disable it.
- **Site URL**—set the URL that users enter in the browser to access an instance of Relativity.
  - **Example**—https://company.relativity.one/Relativity

Authentication provider settings

- **OAuth2 Flow**—select **Code**.
- **Client ID**—enter the Client ID from your Okta parameters Client ID.
- **Client Secret**—enter the Client Secret from your Okta parameters client secret.

- **Display on login screen**—determines if the OpenID Connect button displays on the login page.
- **Login Screen Button Text**—determines the text that appears on the button displayed on the login page.
- **Authority URL**—[the Okta domain parameter] (i.e. http://customer.okta.com). The Authority URL can be retrieved from the Sign On tab in Okta. If you go to the OpenID Connect ID Token section and in the Issuer area.
- **Scopes**—the default value for this field is **openid**. The **openid** checkbox must be selected because it's a required setting. However, you can also select the email or profile option.

  The identity provider responds with the claims associated with the scopes that you request. In other words, the scopes translate into claims that you can use.
- **Subject Claim Type**—the default value for this field is **sub**. Enter one of the following values based on the scopes that you set:
  - If you selected only OpenID in the Scopes field, this field must be set to **sub**.
  - If you selected OpenID and email in the Scopes field, set this field to **email**.
  - If you selected OpenID and profile in the Scopes field, set this field to a property available from the identity provider. These properties differ for each provider.

  The identity provider sends an identity token to you, which contains the claims for your selected scopes. When you request only the openid scope, then sub is used as the claim type. It often represents a unique identifier for the user within your system

Configure Okta

Once you configure the authentication provider, you'll need to assign it as a login method to your users. To complete the configuration in Relativity, navigate to the User and Group Management > Users tab. For complete steps on configuring an OpenID Connect login method, see OpenID Connect on page 127.

4.11.5 Relativity OpenID Connect

Relativity can be set up as an OpenID Connect authentication provider to log users into a different Relativity instance. For example you can set up a Relativity Server environment (primary instance) to act as authentication provider for a Relativity aiR cloud instance (secondary instance).

4.11.5.1 Pre-requisites

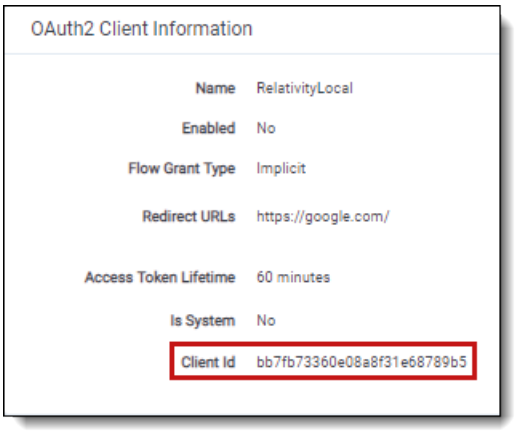
Before you begin you must have the following items completed.

- Ensure that the primary instance is set up to use HTTPS.
- Verify that the secondary instance can resolve the host address of the primary instance.
- Confirm that the authenticated users are defined in both systems.

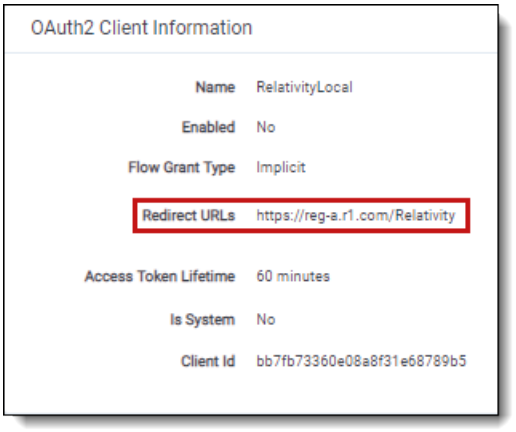
4.11.5.2 Configuring Relativity OpenID Connect

To configure an OpenID Connect provider for Relativity:

1. Navigate to the primary instance and set up an OAuth2 client. You must specify Implicit as the OAuth2 Flow. Note that initially you don't have the redirect URL value (you get it when you set up the Authentication Provider on the secondary instance), so specify any placeholder URL instead. For more information, see OAuth2 clients on page 144.After you save the OAuth2 client, note the generated value of the Client Id. This is required to set up the authentication provider in the secondary instance.

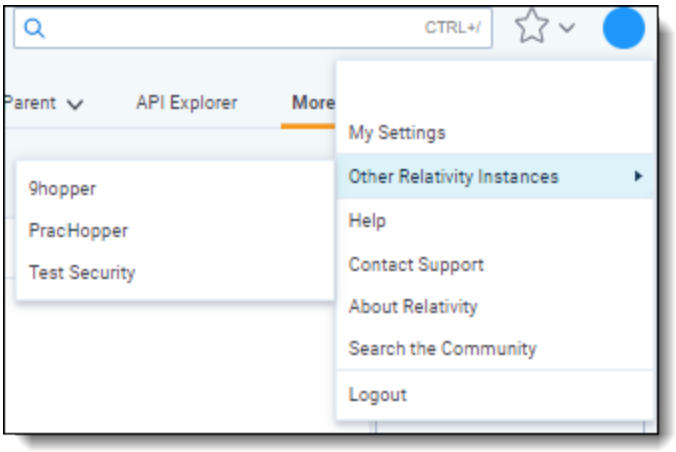


2. Navigate to the secondary instance and configure a new OpenID Connect authentication provider using the Client Id value from the previous step. Note that the OAuth2 Flow values must also be Implicit, and the Authority URL must point to the Relativity Identity service of the primary instance. An example of a Redirect URL is *https://mycompany.relativity.one/Relativity/Identity*.
3. After you save the provider, note the generated value of the Redirect URL. It is required to complete the OAuth2 client setup in the primary instance.
4. Set up the user(s) to use the Authentication Provider as the Login Method, specifying the user's email (Relativity user ID) as the **OpenID Connect Subject** field value. For more information, see Managing user authentication methods.
5. Navigate back to the primary instance and update the OAuth2 provider with the Redirect URL.



6. In the primary instance, set up a federated instance pointing to the secondary Relativity instance. Note the use of the Home Realm Discovery (HRD) URL parameter to provide a single sign-on experience. The Home Realm discovery URL is generated when the Authentication Provider is created and can be found in the Authentication Provider Information section of the Authentication Provider page. For more information, see Federated instances on page 154.
7. Navigate back to the secondary instance and set up a federated instance pointing to the primary Relativity instance. Don't set up the HRD redirect for that federated instance.
8. Log out of the secondary instance.

9. Use the federated instance link to log in to the secondary instance from the primary instance.



10. Use the federated instance link in the secondary instance to return to primary instance.

You have now configured a Relativity environment to serve as an authentication provider for another Relativity instance.

4.12 OAuth2 clients

The OAuth 2.0 authorization framework enables a third-party application to obtain access to an HTTP service. OAuth2 clients allow you to configure external services and applications to authenticate against Relativity in a secure manner. For example, a client application can present the user with the Relativity login page to get an access token to call Relativity APIs. The application can then call the APIs to perform tasks for customizing e-discovery workflows and automation. For background information on OAuth2, see OAuth2 Specification.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

OAuth2 clients can be used in conjunction with Relativity authentication providers and federated instances in different enterprise integration scenarios, including:

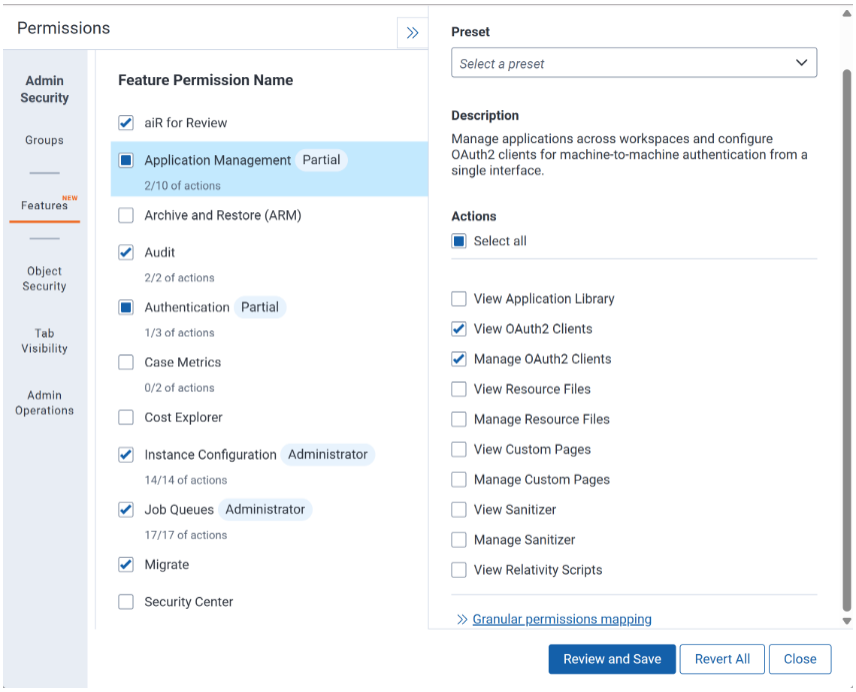
- Relativity as an authentication portal for another instance of Relativity
- Relativity as an authentication portal for another website
- Authenticating to Relativity's APIs from a standalone application without needing a Relativity user's username and password
- Embedding the Relativity login form in a native desktop application
- Embedding the Relativity login form in a mobile application

To set up an OAuth2 client in Relativity, you must correctly determine the grant type required for your application. The OAuth2 client setup information also includes a client ID, a redirect URI, and a client secret key. Relativity uses these details to validate your application and authorize the API calls.

Note: For security reasons, the client secret is only visible at the time of creation or reset. Be sure to copy and securely store the secret when it is first displayed, as it cannot be retrieved later. If the secret is lost, you must reset it to generate a new one.

4.12.1 Permissions

Manage these permissions on the Features tab, under the Application Management feature. Grant a group access by feature, or by individual action. For an overview of features and actions, see Feature permissions.



4.12.2 Creating or editing an OAuth2 client

To create OAuth2 clients or edit information for an existing OAuth2 client:

1. Open the **OAuth2 Client** tab.
2. Click **New OAuth2 Client** to create a new OAuth2 client, or click **Edit** next to the OAuth2 client you want to edit. The OAuth2 Client Information form appears.
3. Complete the fields on the form. Fields in orange are required.
    - **Name**—the descriptive name of the OAuth2 client. The name must be unique.
    - **Enabled**—yes/no value indicating whether the client will be given access to Relativity.
    - **Flow Grant Type**—the mechanism for acquiring an authentication token also known as OAuth2 grant type. Relativity supports the following grant types:
        - **Client Credential**—for applications such as background processes that may need to get an access token for their own account, outside the context of any specific user. This grant type requires a client secret.
        - **Code**—for apps running on a web server. The grant type is used to obtain both access tokens and refresh tokens and is optimized for server-side applications. The client must be capable of interacting with the resource owner's user-agent (typically a web browser) and capable of receiving incoming requests (via redirection) from the authorization server. This grant type requires a client secret.

        Note: You cannot change the flow value when editing an OAuth2 client.

- **Implicit**—for lightweight browser-based or mobile applications typically implemented using a scripting language such as JavaScript. The implicit grant type is used to obtain access tokens (it does not support the issuance of refresh tokens) and is optimized for public clients known to operate a particular redirection URI. The client receives the access token as the result of the authorization request. This grant type does not require a client secret.
- **Resource Owner**—suitable in cases where the resource owner has a trust relationship with the client, such as the device operating system or a highly privileged application. The authorization server should take special care when enabling this grant type and only allow it when other flows are not viable. This grant type can be used for clients capable of obtaining the resource owner's credentials (username and password, typically using a command line prompt). It is also used to migrate existing clients using direct authentication schemes such as HTTP Basic or Digest authentication to OAuth by converting the stored credentials to an access token. This grant type requires a client secret.

- **Redirect URLs**—the URLs that the user can be redirected back to after the request is authorized. Specify values only if Implicit or Code are selected in the Flow field. The URLs must include the *http* or *https* protocol prefix.
- **Context User**—Relativity user context for OAuth2 client authorization. This enables an administrator to restrict the access privileges on an OAuth2 client based on the user's permissions as well as audit. Context User is required if Client Credentials is selected as the OAuth2 flow, and cannot be specified for other flows.

  Note: An OAuth2 client continues to function even if the context user's Relativity account is disabled. The client remains operational as long as the OAuth2 client itself is enabled.

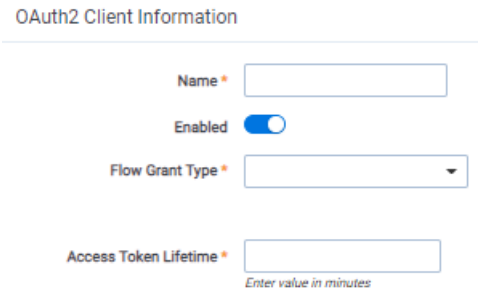
- **Access Token Lifetime**—the duration (in minutes) for which access tokens issued to the clients are valid. The recommended value varies depending on the specified OAuth2 flow:
  - Client Credentials and Code Flow must have a short lifetime. It is recommended that the value match the Identity Server default of 1 hour (60). For more information, see Identity Server documentation (https://docs.duendesoftware.com/identityserver/reference/models/client/).
  - Resource Owner access token must also have a lifetime of 1 hour because a client secret and a refresh token are available.
  - Implicit flow tokens must match Relativity's token lifetime of 10 hours (600), after which the user must log in again.
- **Allow Refresh Tokens** - Refresh tokens require updates to the application. You must test any changes in a sandbox instance before deploying to production.

  Note: To obtain a refresh token, it is necessary to use an Authorization Code with a Proof Key for Code Exchange (PKCE) flow.

- **Trusted IPs** - An optional feature for the OAuth2 client object. Enter each IP address on a new line, and use CIDR notation to specify a range of IP addresses. The system checks trusted IPs whenever a token is requested using the OAuth2 client's ID and secret. If the request comes from an IP address outside the specified range, the system returns a 400 error with the message **"invalid_client. IP address not allowed."**

  Note: Changes to Trusted IPs take up to 5 minutes to apply.

4. Click **Save**. The form displays the new OAuth2 client with these generated field values:
    - **Enabled**—yes/no value indicating whether the client will be given access to Relativity.
    - **Flow Grant Type**—the mechanism for acquiring an authentication token also known as OAuth2 grant type.
    - **Redirect URLs**—the URLs that the user can be redirected back to after the request is authorized.
    - **Access Token Lifetime**—the duration (in minutes) for which access tokens issued to the clients are valid.
    - **IsSystem**— specifies whether the OAuth2 client is part of an internal Relativity application.



    - **Client ID** – the unique identifier for the Client autogenerated by Relativity.
    - **Client Secret** – the unique secret used by the client. Also auto generated by Relativity if you select Client Credential, Resource Owner, or Code as the value of the Flow field.

    Note: The client secret is only displayed once, immediately after creation or reset. You will not be able to view it again. Be sure to copy and securely store the secret at that time. If you lose the secret, you must reset it to generate a new one.

4.12.3 Resetting a client secret

You can reset an OAuth2 client secret for the following Flow values (grant types):

- Client Credential
- Resource Owner
- Code

To reset an OAuth2 client secret:

1. From the **OAuth2 client** tab, locate and open the OAuth2 client whose secret you want to delete.
2. Click **Reset Secret** in the OAuth2 Client console.



3. From the confirmation dialog, click **Ok**. The OAuth2 client secret is reset.

Note: After resetting, the new client secret will be displayed only once. You must copy and store it securely, as it cannot be viewed again later.

4.12.4 Deleting an OAuth2 client

To delete an OAuth2 client:

1. From the **OAuth2 client** tab, locate and open the OAuth2 client you want to delete.
2. Click **Delete**.
3. From the confirmation dialog, click **Ok**. The OAuth2 client is removed.

Note: System clients cannot be deleted.

Viewing an OAuth2 client audit history

Use the OAuth2 client audit history to view all actions taken on a record. Use this information to view what the values were prior to a change.

To view an OAuth2 client's audit history:

1. From the OAuth2 client tab, locate and click the OAuth2 client for which you wish to view its history.
2. Click **View Audit**. A dialog appears, listing all actions taken on that OAuth2 client.
3. (Optional) Using the **Export to File** drop-down list at the bottom of the dialog, click **Go** to export the following audit history details in a .CSV file:
   - User Name
   - Action
   - Timestamp
4. Close the dialog when you have finished viewing the audit.

4.13 Authentication providers

An authentication provider holds the settings for one login protocol. In this workflow, you create and configure each authentication provider individually using the **New Authentication Provider** button on the Authentication Provider tab.

These topics apply to instances that have not transitioned to Centralized Authentication. Both workflows are supported during the transition, so the steps you follow depend on which one your instance uses. For help identifying which setup applies to you, see Choosing your authentication setup on page 89.

Note: If your instance uses Centralized Authentication, use Centralized Authentication on page 94 instead. The provider setup steps in these topics do not match the fields in the Centralized Authentication wizard.

4.13.1 Supported authentication providers

Review the topic for the identity provider you want to configure:

- OpenID Connect on page 137—configure any identity provider that supports the OpenID Connect protocol, and set up just-in-time provisioning.
- Okta OpenID Connect on page 141—configure Okta as an OpenID Connect identity provider.
- Microsoft Entra ID - OpenID Connect on page 128—register an Azure application and configure Microsoft Entra ID as an OpenID Connect identity provider.
- SAML 2.0 provider on page 130—configure a SAML 2.0 identity provider, including Okta and ADFS.

4.13.2 Assigning login methods

After you create an authentication provider, assign a login method to each user before that user can log in. For those steps, see Managing user authentication methods on page 123.

4.13.3 Related topics

4.14 Relativity aiR Connect

Use a single login to access all your Relativity aiR workspaces and instances with Connect. Securely connect multiple instances and let users navigate between them securely with cross-authentication using OpenID Connect as the single sign-on provider (SSO). With Connect you can log in to Relativity once and access workspaces across multiple instances that are connected as federated instances.

Once the connection between the instances is created, the Relativity users can sign in and navigate between workspaces in the different instances.

Caution: Relativity aiR Connect allows you to leverage another instance as a trusted identity provider for your environment. This functionality allows users within the connected instance to authenticate directly into yours. This eliminates the need for a single user to have multiple credentials within Relativity aiR. However, you must exercise caution when assigning the Connect login method. Granting this access effectively cedes control over user authentication to the external instance for users with the Connect login method. This means the connected instance verifies user identities and grants access to your environment. Therefore, it's critical to reserve the Connect login method exclusively for users whose identities you trust and whose access needs can be effectively managed by the external instance. Assigning Connect to your internal users could compromise your security posture, as unauthorized individuals from the connected instance could potentially gain access to your environment.

Note: Relativity aiR Connect cannot be used to connect two instances owned by the same customer (or their global entity). In order to connect two instances owned by the same customer, please see Linking additional Relativity instances

4.14.1 Enabling Relativity aiR Connect

To enable Connect and connect two or more Relativity instances, each party's Relativity aiR primary contact must complete a Relativity aiR Connect Request form. This applies unless the two instances are owned by the same customer (or their global entity).

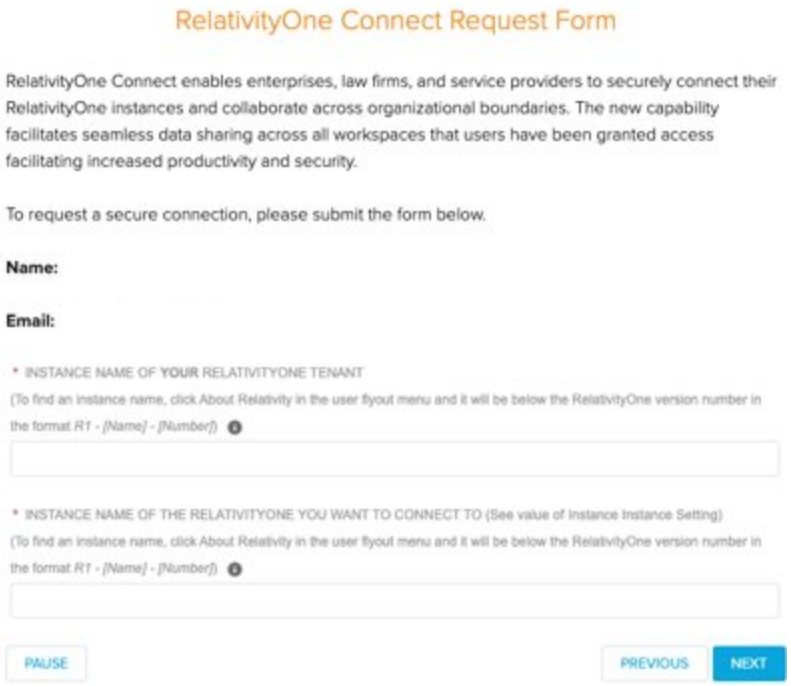
To begin using Relativity aiR Connect, the primary Relativity aiR contact at your organization needs to navigate to the Community site.

As your organization's primary Relativity aiR contact, navigate to the Community site. In the Community site, navigate to Relativity aiR Connect Request Form.

1. In the top navigation menu, click **Support**.
2. On the Support page, click the **Submit or resume** button under Relativity aiR Requests.

   Note: If you don't see the Relativity aiR Requests section, you are not the Relativity aiR Primary Contact. Please make sure you are logged in as the primary contact to move forward in requesting a form.
3. In the Relativity aiR Request page, click the **Choose Request Type** drop-down menu.
4. Select **Relativity aiR Connect**.
5. Click **Next**.

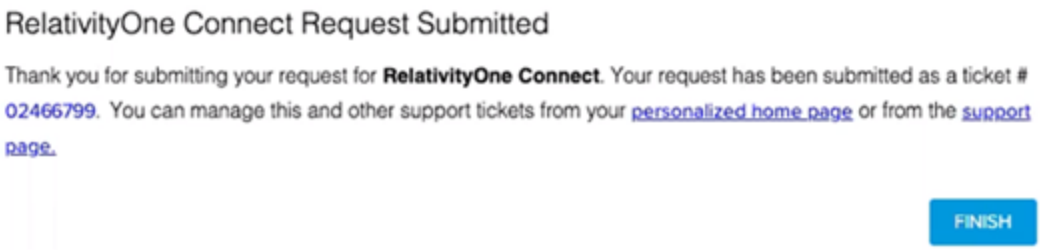
This opens the Relativity aiR Connect Request Form.



In the request form, confirm that the name and the email address match your information. Then continue filling out the form by entering the instance name of your Relativity aiR tenant and the instance name of the Relativity aiR instance that you want to connect to by completing the following fields:

- **Instance Name of your Relativity aiR tenant**—the name of your organization's instance.
- **Instance Name of the Relativity aiR tenant you want to connect to**—the name of the instance name that you want organization's instance to connect to.

Once entered, click **Next**. Confirm the request was submitted and click **Finish**.



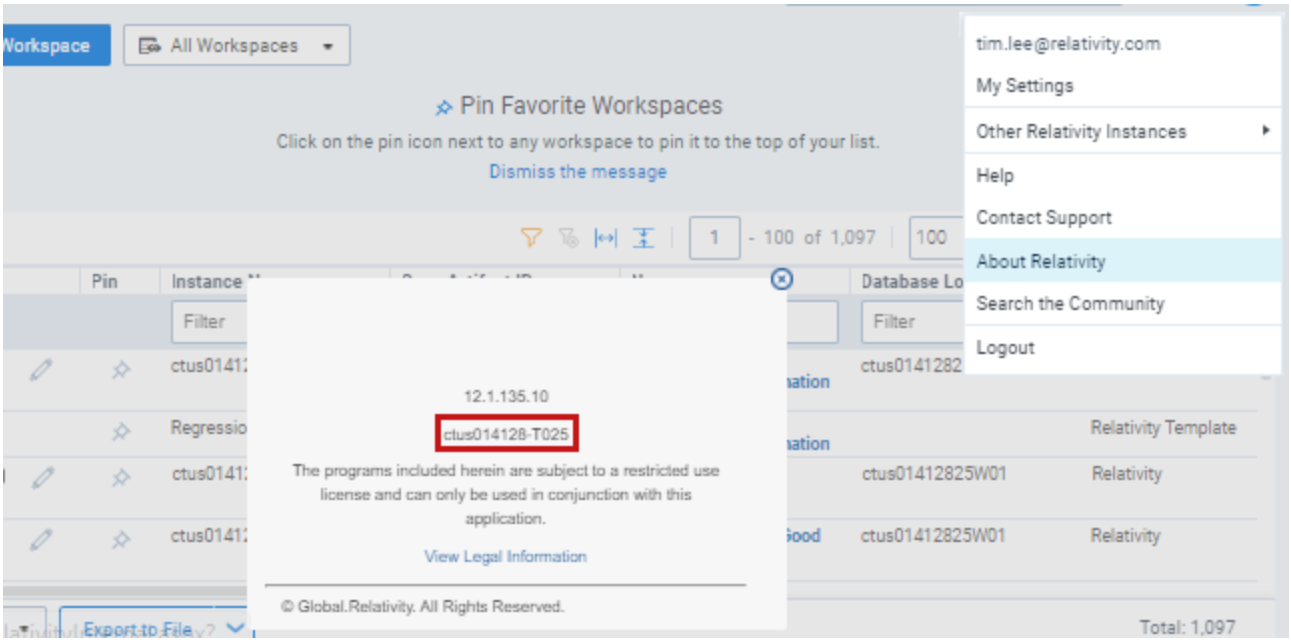
Once submitted, Relativity can confirm the Relativity aiR primary contacts email addresses and instance names. Once confirmed, a new authentication provider option is available when updating a user's login method.

Note: To connect to more than one Relativity aiR instance, you will need to submit multiple requests.

Once the request has been submitted, Relativity can confirm the Relativity aiR primary contacts email addresses and instance names. Once confirmed, a new authentication provider option is available when updating a user's login method.

4.14.1.1 Finding instance names

Find the instance names in the User options drop-down menu. Copy the instance name from your instance and retrieve the other instance name.



4.14.2 Connecting users to different instances

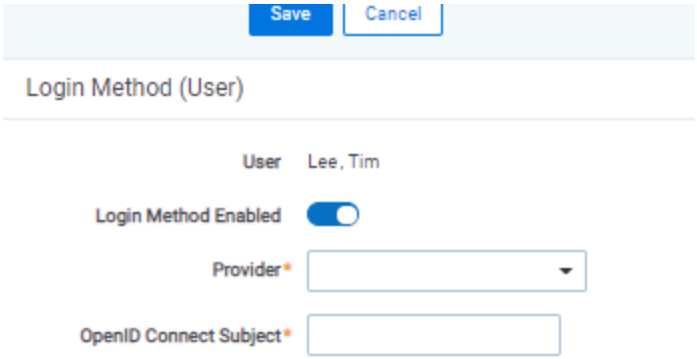
To connect users to multiple instances with their one set of login credentials, navigate to the Admin-level Users tab. Find the user that needs to be connected and select the user.

Once the user is selected and their user information page is available, add a new Login Method.

1. In the Login Method section, click **New**.
2. Click the **Provider** drop-down menu.
3. Select the instance name of the connected environment.
4. Enter the **OpenID Connect Subject**.

   Note: The OpenID Connect subject is the user email address in the other instance.

5. Click **Save**.



An already existing user also needs the default password provider login method removed.

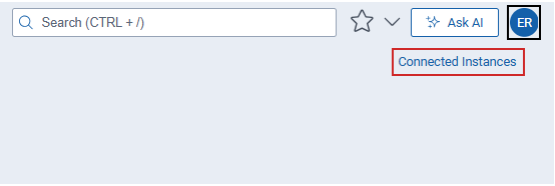
Each instance has that instance's group and security permissions. If the users already exist from previous engagements, no action is needed.

4.14.3 Navigating between instances

As a user, the links to the connected instances appear in the User drop-down menu. The available instance names are available in the **Other Relativity Instances** drop-down option. Hover over the Other Relativity Instances and click the name of any instance.

Note: By default, the connected instances in the Other Relativity Instances drop-down option are visible to all users. If you want to limit who can see the instances in the drop-down option, apply item-level security to the connected instance in the Federated Instances tab. For more information on individual item security, see Relativity object security.

Once clicked, you need to confirm your credentials with your SSO provider. Once confirmed, you can navigate within the newly opened instance.



4.14.4 Updating Relativity aiR Connect after a URL change

When a connected instance's URL changes, two records must be updated manually in the instance that holds the connection:

- The **Federated Instance** record that points to the changed instance
- The **Redirect URL** on the **OAuth2 client** configured for that connection

The authentication provider's redirect URL updates automatically, however, the OAuth2 client in the connected instance does not update automatically. A stale Redirect URL on the OAuth2 client causes login failures for users navigating between instances.

To update the OAuth2 client:

1. In the connected instance, open the **OAuth2 Client** tab.
2. Open the OAuth2 client associated with the connection.
3. Update the **Redirect URL** to reflect the new instance URL.
4. Click **Save**.

Also update the Federated Instance record for the changed instance.

4.14.5 Billing information

To avoid double billing, we look at the domain for the user's email. So if a user with the same email address exists in multiple instances, they will not be billed multiple times.

4.14.5.1 User type information

The User Type, is something that can be used to tag a user as someone coming from another instance. It is only for organizational uses, and doesn't affect billing.

As a user, you can use it to categorize users that we create. If you'd like a user to work with Relativity aiR Connect, they need to work on the two instances that are connected. It's important to make sure that the user exists in both instances, so you can use the user type to distinguish that this user was created, so you can log in.

4.14.6 Frequently asked questions

(If a user in my environment is already an administrator, will they keep their admin rights when using Connect to log in to the other instance?
No. Each Relativity aiR environment maintains its own groups and permissions. When you add a Connect login for a user, you can restrict their permissions in the target environment by placing them only in specific groups. If you do not assign them to a group with user- or workspace-management rights, they cannot add users or modify groups in the other instance.

Why does Relativity warn against giving Connect logins to internal users, and how can this risk be mitigated?
Assigning your internal users a Connect login method means they authenticate through the external environment. In that scenario, an administrator of the external instance could potentially take over your user's account and access your environment. **Relativity recommends reserving Connect logins for external collaborators only**. Additional safeguards include giving external users only the permissions they need, ensuring both instances enforce strong security controls (for example, MFA), and coordinating with the other administrator about account policies and deactivation procedures.

If I create a user in my environment, will Relativity aiR alert me if that person already exists in the connected instance?
No. Relativity aiR Connect does not automatically check whether the user exists in the other environment. Administrators need to coordinate with their counterparts in the connected instance to confirm and, if necessary, create the account on both sides.

Can I create a new user in my instance and immediately grant them access to the other connected environment?
You can add a Relativity aiR Connect login method to a user in your own instance, but the user must also exist (with the same email address) in the other instance for authentication to succeed. Connect does not automatically provision accounts across environments.

4.15 SSO Troubleshooting console

The **SSO Troubleshooting console** eliminates the need for third-party tools when gathering essential information for troubleshooting error messages. It offers administrators actionable error messages to help them address configuration issues.

4.15.1 Considerations

- This console should not be utilized for auditing purposes.
- You must have the ***Edit*** permission on the Authentication Provider object to view the console.>
- The error log will only show the 10 most recent error messages.

4.15.2 Viewing the SSO Troubleshooting console

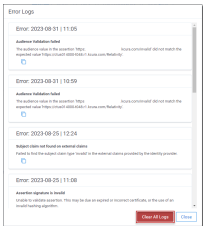
To view and manage the errors in the console:

1. Navigate and select your authentication provider



2. Click on the **Errors Log** button.

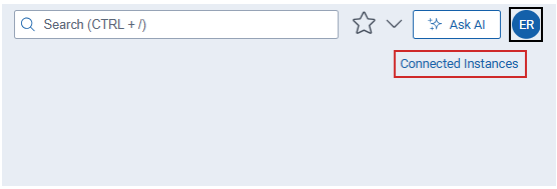
3. Review the errors and make the necessary updates to resolve the issue.
4. Once the errors have been resolved, clear the error log.



See this related pages:

4.16 Federated instances

Federated instances provide a way for reviewers to easily switch to other Relativity environments. In Relativity, links to federated instances appear in the User drop-down.



You can use federated instances in combination with OAuth2 clients and authentication providers to enable single sign-on for multiple environments in your Relativity ecosystem.

Note: Customers utilizing the same third-party OIDC provider (e.g., Okta, EntraID) in both instances can use the Authentication provider's HRD hint to streamline the connection process, eliminating the need for manual linking.

4.16.1 Creating or editing a federated instance

To create a federated instance or edit information for an existing federated instance:

1. Open the **Federated Instances** tab.
2. Click **New Federated Instance** to create a new federated instance, or click **Edit** next to the federated instance you want to edit. The Federated Instance Information form appears.
3. Complete the following fields:
    - **Name** – the name of the federated instance. Enter a name that makes the instance easy for users to recognize, like Relativity aiR Reviewer.

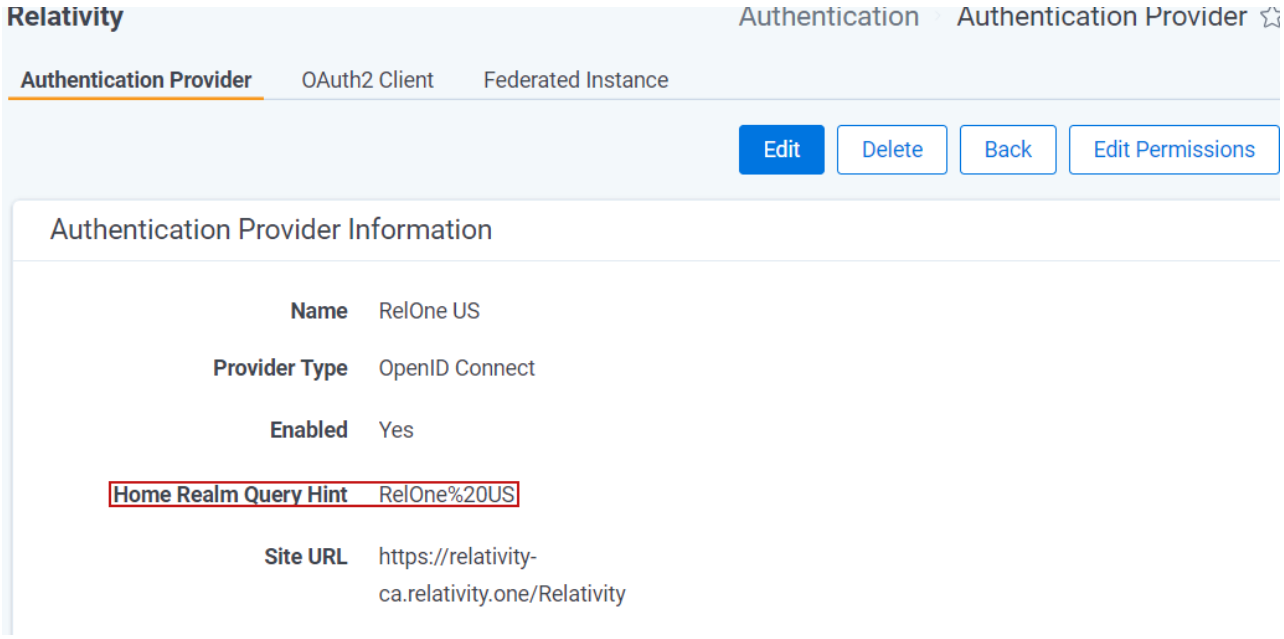
      Note: You can't change the name of an existing federated instance.

    - **Instance URL** – the URL address of the instance you want to create a link to. To obtain this URL, navigate to the Relativity instance you want to appear in the drop-down menu. Copy and paste the URL from that instance into this field.

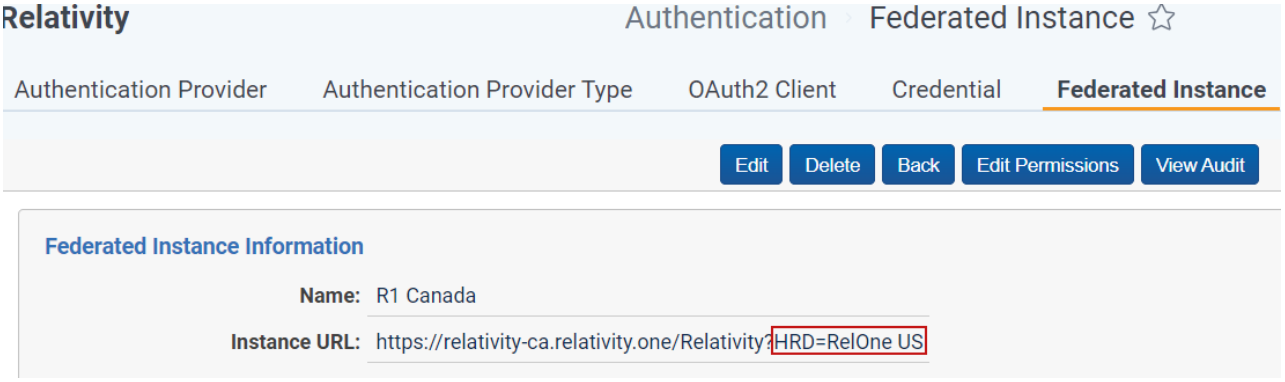
      You can also choose to add the Home Realm Discovery (HRD) parameter to mimic single sign-on experience inside your Relativity cluster. HRD is a redirect URL to a configured authentication provider for the federated instance. It is supported for OpenId Connect.

      Locate the **Home Realm Query Hint** (HRD parameter value) within the provider-specific details section

of the Authentication Provider tab.



To establish a link to a specific instance, return to that instance and input the **Home Realm Query Hint** (HRD parameter value) within the designated Instance URL field.



- *https://mycompany.com/Relativity?HRD=<Provider Name>*

> **Note:** You cannot connect more than one authentication provider using the Federated Instances feature. The authentication provider must be set up correctly for single sign-on to work. If the authentication by the provider fails, the user will be presented with the login screen of the Federated Instance.

4. Click **Save**.

The federated instance will appear in the User drop-down menu.

You can restrict access to the federated instances you create using the padlock icon and assigning the appropriate groups access to the instance. If you restrict access to a federated instance, it doesn't appear in the User drop-down menu.

4.16.2 Deleting a federated instance

To delete a federated instance:

1. Navigate to the **Federated Instance** tab.
2. Locate and open the federated instance you wish to delete.
3. Click **Delete**.
4. From the confirmation dialog, click **Ok**.

The federated instance is removed.

Updating a federated instance after an instance URL change

When a Relativity aiR instance URL changes, Relativity does not automatically update federated instance records in other instances that reference the old URL. You must update them manually.

After a URL change, complete these steps for each instance that has a federated instance record pointing to the changed instance:

1. Open the **Federated Instances** tab on the instance that contains the record.
2. Click **Edit** next to the federated instance that points to the changed URL.
3. Update the Instance URL field to the new URL.
4. Click **Save**.

If the connection uses Relativity aiR Connect, also update the Redirect URL on the OAuth2 client in the connected instance.

Note: Note: If multiple instances maintain federated links to the changed instance, update the federated instance record in each of those instances.

Viewing a federated instance audit history

Use the federated instance audit history to view all actions taken on a record. Use this information to view what the values were prior to a change.

To view a federated instance's audit history:

1. Navigate to the Federated Instance tab.
2. Locate and click the federated instance for which you wish to view its history.
3. Click **View Audit**. A dialog appears, listing all actions taken on that federated instance.
4. (Optional) Using the **Export to File** drop-down list at the bottom of the dialog, click **Go** to export the following audit history details in a .CSV file:
    - User Name
    - Action
    - Timestamp
5. Close the dialog when finished viewing the audit.

5 Batches

You can create batches in Relativity by splitting a static set of documents into multiple document sets based on criteria set by a system admin. With the appropriate permissions, users can then check out these batches and assign themselves documents.

Note: A member of the workspace's admin group will only be able to check out or be assigned batches if that user is also part of another group (not system admin) in the workspace that has the **View Batches** permission. Being a workspace admin alone is not sufficient to receive batch assignments.

Batching can bring structure to managing a large-scale document review with multiple reviewers. You can generate batches automatically or manually. Automatic document assignment reduces the chances of accidental redundancy in the review process.

Note: You may want to consider using Review Center as a streamlined alternative. For more information, see the Review Center guide.

5.1 Batch fields in Relativity

The fields in Relativity that store batch-related values are:

- **Batch Set**—the batch set to which the batch belongs.
- **Batch**—the name of the batch.
- **Batch Status**—the status of the batch. A batch may be:
  - **Blank**—the batch is not checked out.
  - **In progress**—the batch is checked out.
  - **Completed**—the batch is checked in as completed.
- **Batch Unit**—the optional grouping condition on the batch.
- **Assigned To**—the reviewer to whom the batch is checked out.
- **Reviewed**—specifies whether the batch is reviewed.
- **Batch Size**—the number of records in the batch.

5.2 Creating and editing batch sets

Documents are pre-converted for viewing upon the checkout of a batch set based on the NumberOfDocumentsToAutoPreconvert instance setting. This setting is set to 1000 by default and can be adjusted to suit your needs.

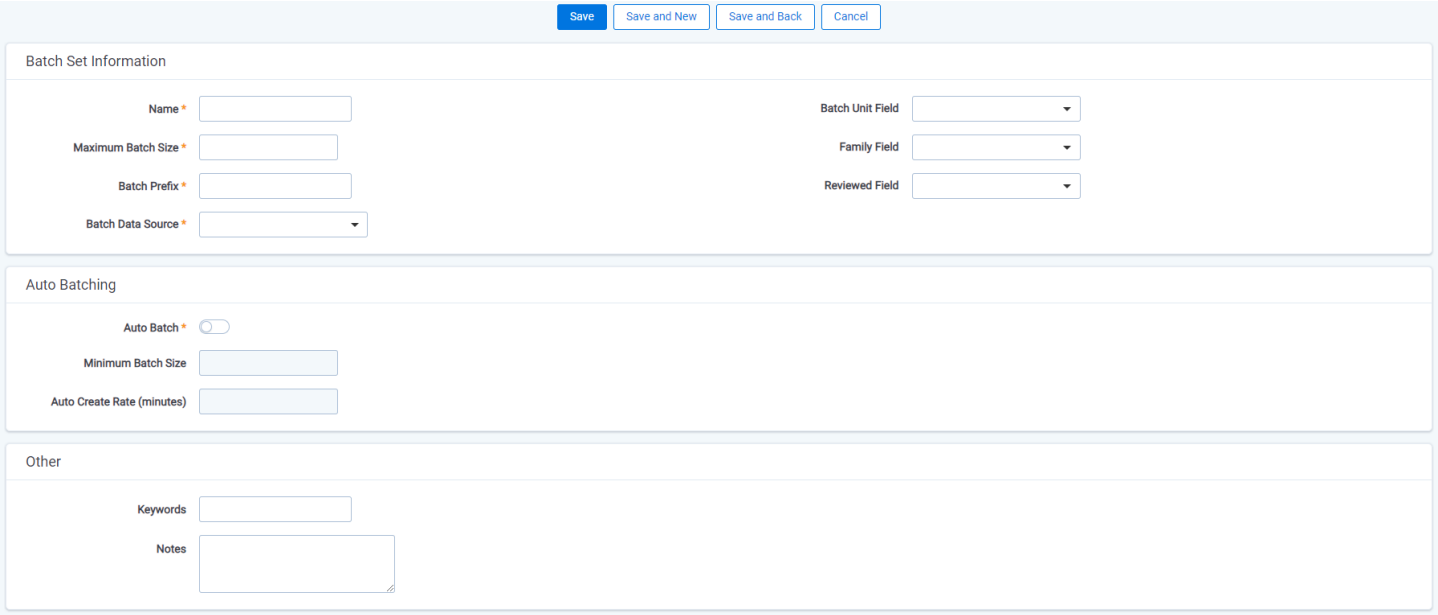
Note: If the value is set to 0, pre-conversion will be disabled.

To create or edit a batch set, perform the following steps:

1. Navigate to the **Batch Sets** tab.
2. Click **New Batch Set** to create a new batch set, or click **Edit** next to the batch you want to edit.

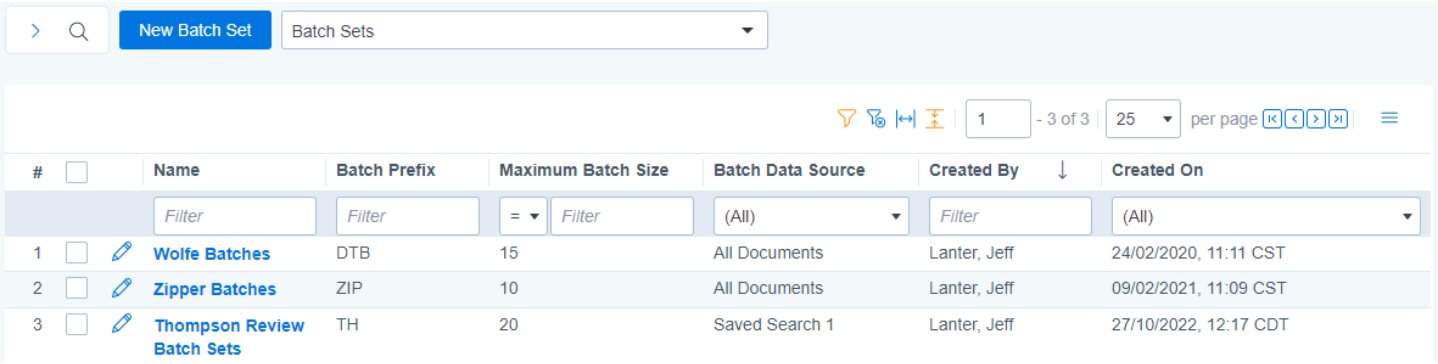
   Note: If you select a value in the **Family Field**, then the batch set will include family documents from that related group that are also included in the data source.

   The Batch Set Information form appears with required fields in orange.
   Complete the fields to create or edit the batch set. See Fields on the next page.
3. Click **Save**.



5.2.1 Batch Sets for Reviewers

Once you have created the batches, navigate to the **Batch Sets** tab using the quick search, CTRL + /, function. Here you will see a reviewer's view of the newly created batches.



5.2.2 Fields

The following fields display on the New Batch Set information form:

- **Name**—the name of the batch set.

  Note: If you are performing a multi-stage review with multiple batch sets per phase, be sure to include the phase name in the batch set name. We also do not recommend using the space bar before or after the name. This makes it easier to search for information within a specific phase.

- **Maximum Batch Size**—the maximum number of documents in one batch. If you also select a Family Field option, the Maximum Batch Size value may be exceeded.

  Note: Your batch may contain fewer documents than this value if there are no more documents to batch or no more documents with the current Batch Unit value.

- **Batch Prefix**—sets the prefix for the batch numbering.

- **Batch Data Source**—the saved search containing documents that you want to batch. If the saved search references a dtSearch or an Analytics index, that index must be active. The sort order of the data source can influence how documents are ordered in batches and how the documents are grouped for batching.
- **Batch Unit Field**—an optional grouping mechanism, enabling you to group similar documents in the same batch. Documents with different values in a batch unit field are not included in the same batch unless the Family Field would override this.

  Note: A common batch unit field is custodian. However, you can use any single choice, multi-choice, single object or non-relational and non-system fixed length text field.

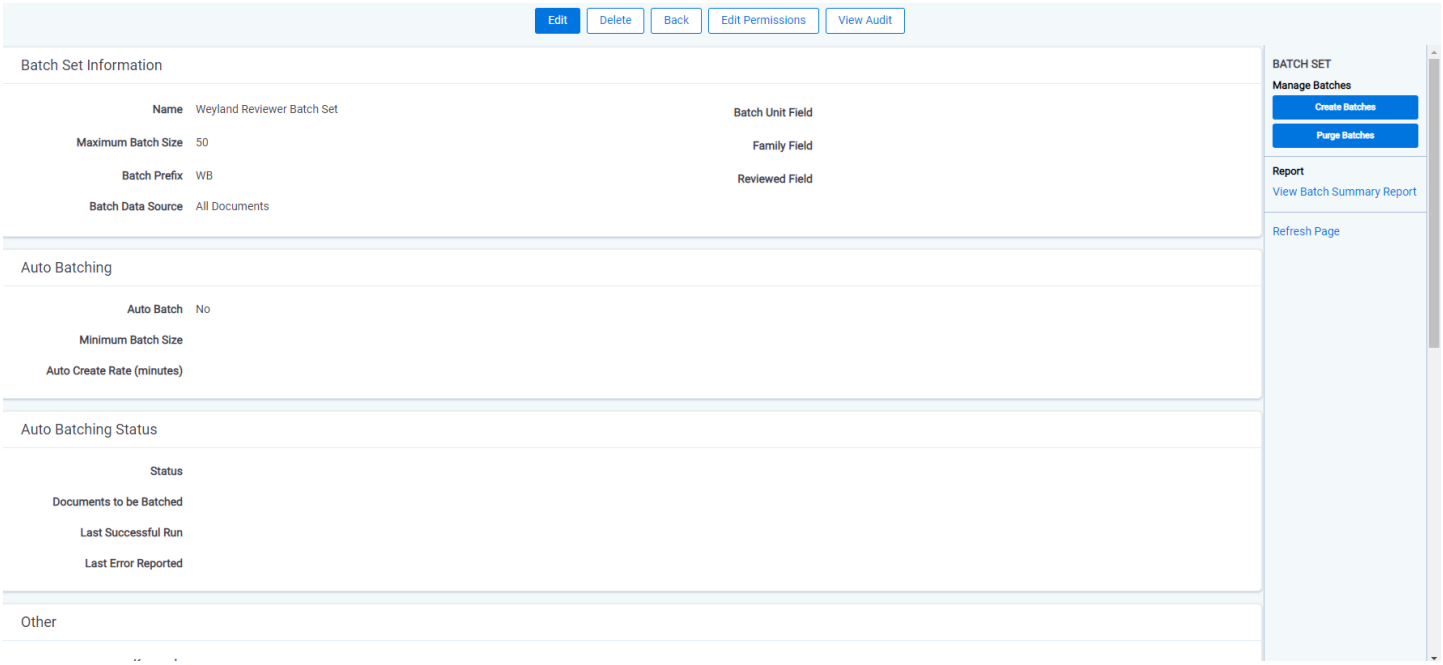
  When using multiple choice fields for the Batch Unit Field, the choice values must be the same in order for them to be grouped in a batch. If the combination of choices is unique enough for the choice values, Relativity batches the documents into separate batch groups.
- **Family Field**—you can select your workspace group identifier. Documents in a family group are not split across batches, even if their batch unit field differs.
  If you select an option for this field, the Maximum Batch Size may be exceeded.
- **Reviewed Field**—an optional field that you can select from any yes/no, single-choice, or multi-choice field from the drop-down menu. Based on your selection, a tally is kept of how many documents in the batch have been reviewed. The batch set monitors the field you specify as the Reviewed field. It also increments a count for each document in the batch that has been coded with a value for that field.
- **Auto Batch**—enables the system to automatically generate batches.
  - **Disabled**—the default, which enables standard manual batch processing.
  - **Enabled**—automatically generates batches according to the settings below.
- **Minimum Batch Size**—only available if Auto Batch is enabled. This is the smallest possible number of documents in a batch.
- **Auto Create Rate**—only available if Auto Batch is enabled. This represents how often, in minutes, the system attempts to create batches.
  Newly created batches appear on the Review Batches tab. Any users with access to the Review Batches tab will be able to see any batches that they have permissions for.

  Note: With auto batching enabled, the Relativity service account runs the saved search specified as your batch data source. The Relativity Service account is a system admin account.

5.2.3 Batch Set console

Once you save your batch set, the Batch Set console displays the following options:

- **Create Batches**—creates the batches based on the entered settings. Created batches display on the bottom half of the batch set details page.
- **Purge Batches**—deletes any batches associated with the entire batch set.
- **View Batch Summary Report**—displays the Batch Summary report. This field is only enabled after you have created batches.
- **Refresh Page**—refreshes the page.



Note: Previously created batches do not update to include new properties. For example, if you create batches with a batch size of 500 and then need to lower the size, you should purge the existing batches. You can then make any changes and recreate the batches. You will lose any existing data in the original batch set when you purge those batches.

5.2.4 Auto Batching Status

This section displays on a batch after it has been created to help you track the status of auto batching. The following options display:

- **Status**—displays the current status of the batch: Pending, Processing, Error or Finished
- **Documents to be Batched**—displays the remaining documents that do not meet the minimum batch size. You must manually create a batch for these remaining documents.
- **Last Successful Run**—the date and time stamp of the last successful batch run.
- **Last Error Reported**—the date and time stamp of the last error that occurred.

5.3 Deleting an individual batch

To delete an individual batch using the Delete mass operation, do the following:

1. Navigate to the **Review Batches** tab.
2. Select the individual batch you would like to delete from the list.
3. Select **Delete** from the mass operations drop-down menu in the bottom-left.
   A pop-up window displays.
4. Click **Delete** in the pop-up.
   The selected batch is removed.

5.4 Deleting a batch set

Use the following procedure to delete a batch set.

1. Navigate to the **Batch Set** tab.
2. Select the checkbox next to the batch you want to delete.
3. Select **Delete** in the mass operations drop-down menu, and click **Go**.
   A confirmation message appears.
4. Click **OK**.

For more information, see Mass delete on page 362.

5.5 Searching for documents not in existing batch sets

In some cases, you may need to search for all documents not included in a batch set. To properly search for documents not included in a batch set, use the following search criteria:

- Field: **Batch**
- Operator: **not these conditions**
- Value:
  - Field: **Batch::Batch Set**
  - Operator: **any of these**
  - Value: select all existing batch sets

Documents included in the batch sets you select for the **Batch::Batch Set** field value are excluded from your search results.

Note: If you want to run a search that excludes only certain batch sets select **these conditions** as the first operator. Select **none of these** as the second operator. Documents belonging to more than one batch set may return in your search results. Using this combination of search operators returns documents that belong to any batch set you don't specify in the **Batch::Batch Set** value.

5.6 Batching process overview

The batching process works in a loop which contains the following steps:

1. Identify the next set of documents to be placed into a batch, based on the batch set's configuration, the documents returned by the saved search, and the list of documents that have already been placed in batches in the batch set.

   Note: The process that this step follows can vary depending on whether the batch set is configured with a Batch Unit Field or Family Field. The potential variations are described in the sections below.

2. Create a new batch and assign those documents to the batch.
3. Determine if there are documents returned by the saved search that have yet to be placed into a batch associated with the batch set. If there are unassigned documents, this loop starts over again from the first step.

5.6.1 No Batch Unit Field or Family Field configured

- Relativity searches for the next set of document returned by the saved search that have not been placed into a batch yet. These documents are used to populate the next batch.
  - The number of documents in the next batch will be between 1 and the Maximum Batch Size field value.

5.6.2 Batch Unit Field configured; No Family Field configured

1. Relativity searches for the next single document returned by the saved search that has not been placed into a batch yet.
2. Relativity searches for the next set of documents returned by the saved search that have not been placed into a batch yet and have a Batch Unit Field value that matches the Batch Unit Field value of the document found in step 1. These documents are used to populate the next batch.
    - The number of documents in the next batch will be between 1 and the Maximum Batch Size field value.

5.6.3 Batch Unit Field and Family Field configured

1. Relativity searches for the next single document returned by the saved search that has not been placed into a batch yet.
2. Relativity searches for the next set of documents returned by the saved search that have not been placed into a batch yet and have a Batch Unit Field value that matches the Batch Unit Field value of the document found in step 1.
    - The number of documents will be between 1 and the Maximum Batch Size field value and these documents will include between 1 and Maximum Batch Size field value of unique Family Field values.
    - Each document with an empty Family Field value is treated as if it is in a unique family by itself.
3. Relativity searches for all documents returned by the saved search that have not been placed into a batch yet and have a Family Field value that matches the Family Field value of any of the documents found in step 2. These documents are used to populate the next batch.
    - This process does not take Batch Unit Field into consideration and at minimum, all documents that were identified in the previous step are included in the batch.
    - Each document with an empty Family Field value is treated as if it is in a unique family by itself. Even if one or more of the documents returned in the second step had an empty Family Field value, documents with empty Family Field values that have Batch Unit Field values that do not match the Batch Unit Field value of the document identified in step one will not be included in these results.

5.6.4 No Batch Unit Field configured; Family Field configured

1. Relativity searches for the next set of documents returned by the saved search that have not been placed into a batch yet.
    - The number of documents will be between 1 and the Maximum Batch Size field value and these documents will include between 1 and the Maximum Batch Size field value of unique Family Field values.
    - Each document with an empty Family Field values is treated as if it is in a unique family by itself.
2. Relativity searches for all documents returned by the saved search that have not been placed into a batch yet and have a Family Field value that matches the Family Field value of any of the documents found in step 1. These documents are used to populate the next batch.
    - Each document with an empty Family Field value is treated as if it is in a unique family by itself.

Note: The documents are evaluated in the order they are returned by the saved search, as configured by the sorting options applied to the saved search. When no sort options are applied to a saved search, the Document Artifact ID field is used as the default sort order.

5.6.5 Exceeding the maximum batch size

When a batch set has a Family Field value, it is possible for the number of documents in individual batches to exceed the Maximum Batch Size value. This is due to the fact that the batching process first identifies the next documents to be placed in a new batch based on the Maximum Batch Size and Batch Unit Field values before proceeding to include all documents returned by the saved search that have a Family Field value that matches the Family Field value of any document initially identified as a candidate for the new batch and have not yet been placed into any batches belonging to the relevant batch set.

Based on the document data set in the workspace, the selected saved search, and the batch set field values, it may not be possible to completely prevent this from happening. For example, a family that includes more documents than the Maximum Batch Size value, will always result in at least one batch within the batch set that exceeds the Maximum Batch Size limit.

Depending on the scenario, it may be possible to reduce the number of occurrences where the Maximum Batch Size is exceeded by adjusting the sort option on the saved search which is used as the Batch Set Data Source. Families that tend to be clustered together within the results of a saved search or within the results of a saved search as grouped by Batch Unit Field values will more often naturally fall into the same batch, based on the other batch set field values. Sort options that cause family documents to be split and spread out across the results of a saved search will increase the likelihood that these documents will end up being batched together in a way that they exceed the configured maximum batch size. Choosing saved search sort options that prioritize clustering families of documents together, can sometimes help reduce the occurrences of this issue.

5.7 Assigning batches and checking batches in and out

Any batches you or another user create for your account appear in the Review Batches tab. You can control which batches reviewers see by:

- Applying views to the batches tab, creating any list of batches you'd like to see. You can restrict these views.
- Securing batch sets, where you can then assign permissions to all batches in a batch set.
- Securing individual batches.

You can also restrict the Batches tab so only workspace managers and system admins can see it. In this model, a system admin or a user with Assign Batch permissions would need to check out batches to reviewers as needed.

Note: Reviewers can assign batches to other reviewers with the Assign Batches permission. Reviewers without this permission can only check out batches for themselves. By default, reviewers don't have this permission.

5.7.1 Assign a batch or check a batch out

To check out batches, perform the following steps:

1. Click the **Review Batches** tab.
2. Click **Edit** next to the batch you want to check out.
   Depending on permissions, you might see a drop-down menu where you can select other users to assign batches to. If the drop-down menu is not available, you can only check out batches for yourself. You can't check out batches that another user has checked out.

   Note: A user who belongs **only** to the Workspace Admin Group will not appear in the **Assign To** drop-down list for batch check-out. To be assignable as a batch reviewer, that user must also belong to at least one other group in the workspace (not the System Administrators or the Workspace Admin group) that has access to the workspace and the permission to **view** batches. A workspace admin with no additional reviewer group membership cannot be assigned batches.

3. Click **Check Out** to assign the documents in the batch to the selected reviewers. Once you assign batches, the **Batch::Assigned To** field contains the reviewer's name.

   Note: System admins can't check out batches using the **Me** link.

Reviewers can check out batches one at a time but they may assign multiple batches to themselves or others as needed. A batch may also be checked out for as long as desired. Reviewers need to check in the checked out batch as Completed or Pending before they can check out another. A batch that has been checked in as completed can still be checked out again.

5.7.2 Reassign a batch or check a batch in

A batch can be checked in at any time including when you have finished reviewing all of the documents in a batch. To check a batch in, perform the following steps:

1. Navigate to the **Review Batches** tab.
2. Click the **Edit** icon in the row of your desired batch.
3. Select one of the options on the Batch Edit pop-up. Depending on permissions, you might not see the **Reassign To** button.
   - **Check in as pending** - you can check in the batch as pending for the assigned user.
   - **Check in as completed** - you can check in the batch as completed for the assigned user.

     Note: You can select the Check in as completed option even if not all of the documents have been reviewed.

   - **Reassign** - you can assign the batch to another user.

5.8 Building views for checked-out documents

5.8.1 Build a checked-out documents view

You can build views for a reviewer to see only their checked-out documents that either have not been reviewed yet or have already been reviewed. We recommend creating or designating a field for coding documents before completing these steps.

1. Navigate to the **Views** tab.
2. Click **New View**.
3. Complete the required fields. See Views on page 702 for more information.
4. Click **Conditions**.
5. Click the **+ Condition** button.
6. On the Add Condition - Select Field modal, select **Batch** from the list.
7. Click the arrow next to the Batch button and select **Batch::Assigned To** from the list.
8. Click on the operators drop-down menu and select **is logged in user**.
9. Click **Apply**.
10. Click the arrow next to the Batch button and select **Batch::Status** from the list.
11. Click on the operators drop-down menu and select **any of these**.

12. Select the **In Progress** option from the list and click the **Move selected from left to right** icon.
13. Click **Apply**.
14. Click the **+ Condition** button.
15. On the Add Condition - Select Field modal, select the field you use for coding decisions from the list.
16. Select **is not set** from the operators drop-down menu to create a view of unreviewed documents or select **is set** from the operators drop-down menu for a view of reviewed documents.
17. Click **Apply**.
18. Click **Save**.
19. Optionally, repeat these steps and choose the alternate option for step 16 to create both an unreviewed and reviewed view for checked-out documents.

6 Choices

Choices are the predetermined values that you apply to single and multiple choice list fields. With the necessary permissions, you can create choices for workspace fields and admin fields.

In a workspace, you use choices in coding fields to allow users to record decisions on a document. For example, a Responsiveness field might have choices like Responsive, Not Responsive, and Not Sure. You can add and edit workspace choices directly within Field forms and the Choices tab. Within the Field forms, any saved single or multiple choice field contains the choice editor, so you can create and manage choices directly within the field. Within, the Choices tab you may also add single or multiple choices, reorder choices, and create parent and child choices.

From Home, choices are predetermined values applied to pre-workspace objects, such as workspaces, clients, and matters. These choices function the same as choices within a workspace.

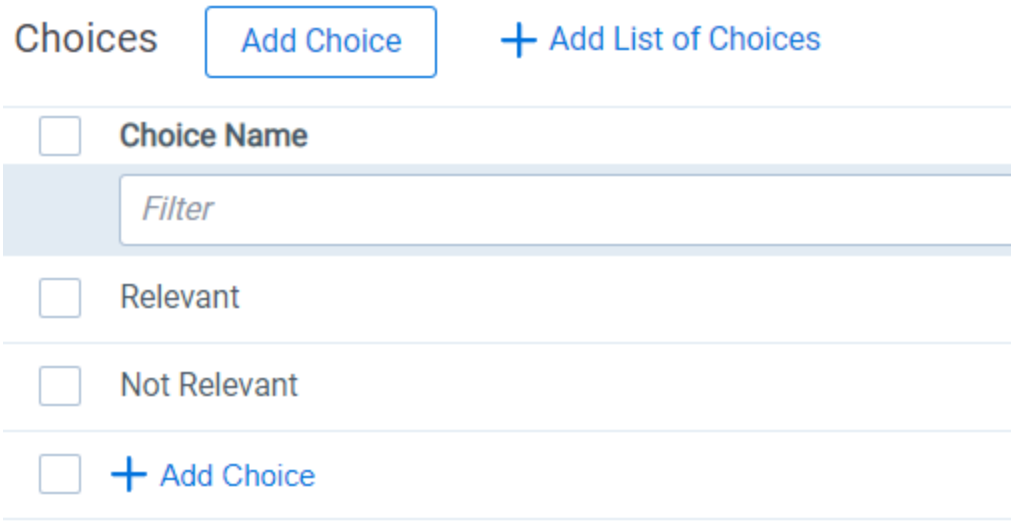
6.1 Accessing the Choice editor

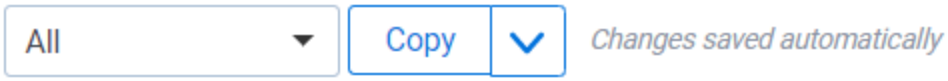
With the Choice Editor, you can add and edit choices from the Fields tab, the Choices tab, and layouts.

6.1.1 Accessing the Choice editor from the Fields tab

To access the Choice editor from the Fields tab:

1. Navigate to the **Fields** tab.
2. Click on the Name of an existing single or multiple choice field or create and save a new single or multiple choice field.
3. Locate the Choice editor in the **Choices** section on the Fields form.

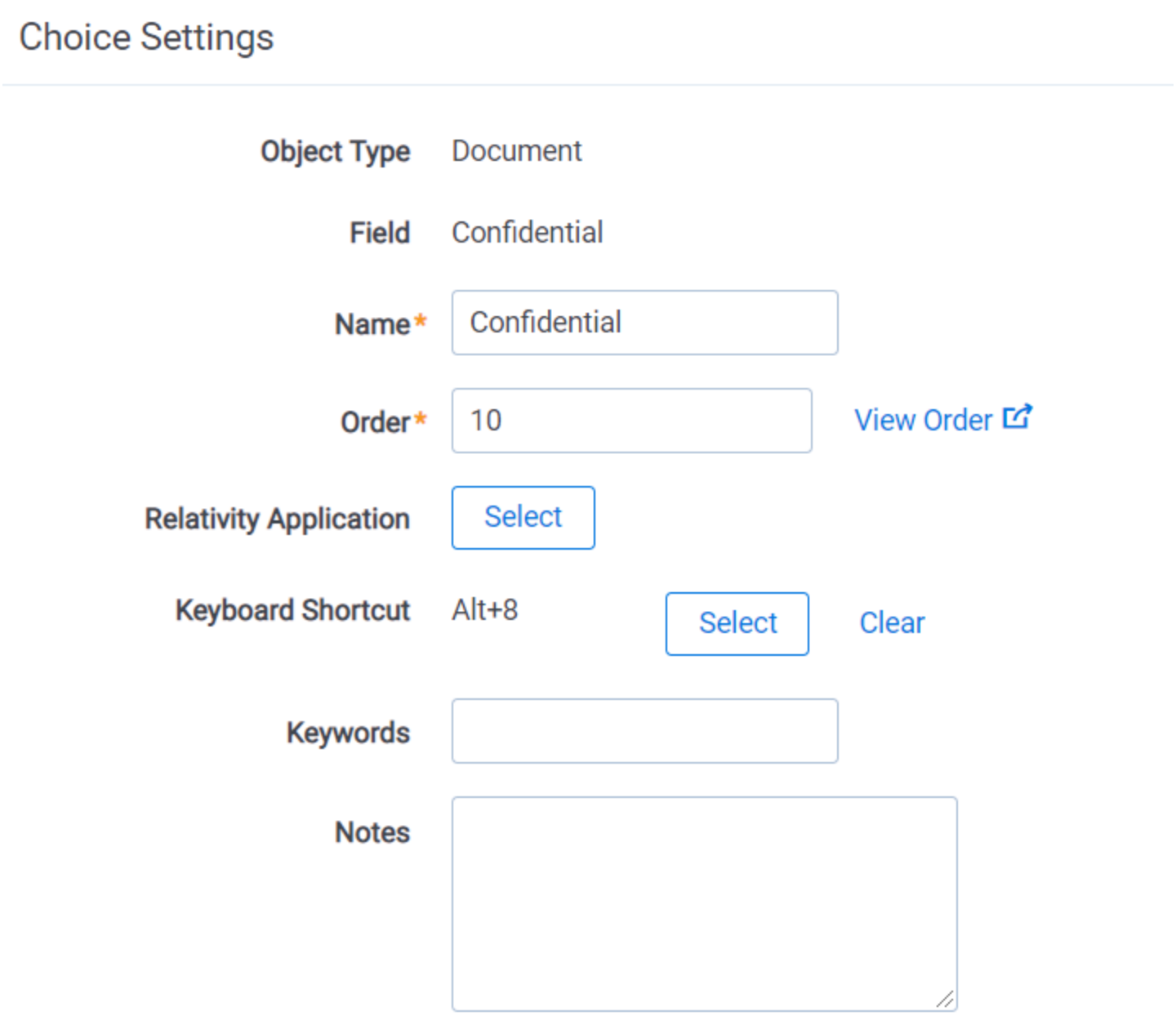




6.1.2 Accessing the Choice editor from the Choices tab

To access the Choice editor from the Choices tab:

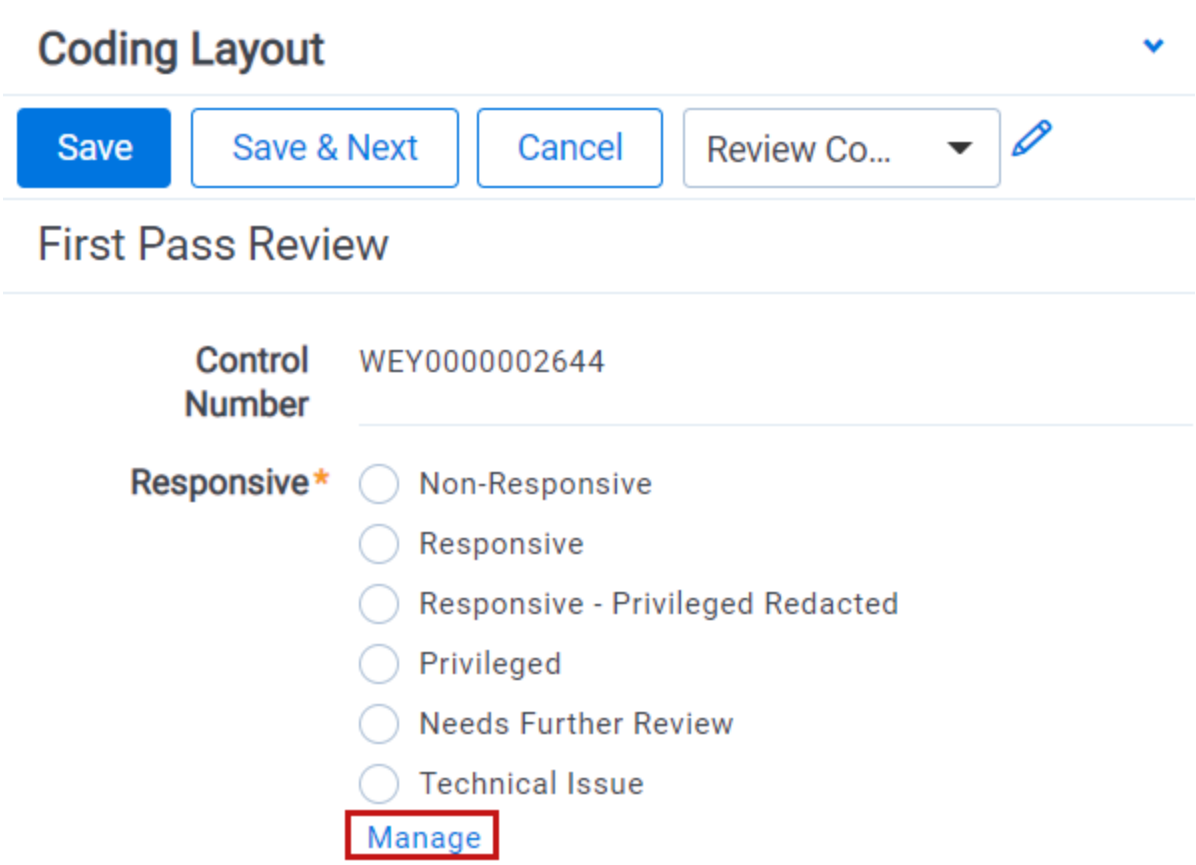
1. Navigate to the **Choices** tab.
2. Click **Edit** next to a choice.
3. The **Choice editor** opens.



6.1.3 Accessing the Choice editor from layouts

To access the Choice editor from layouts:

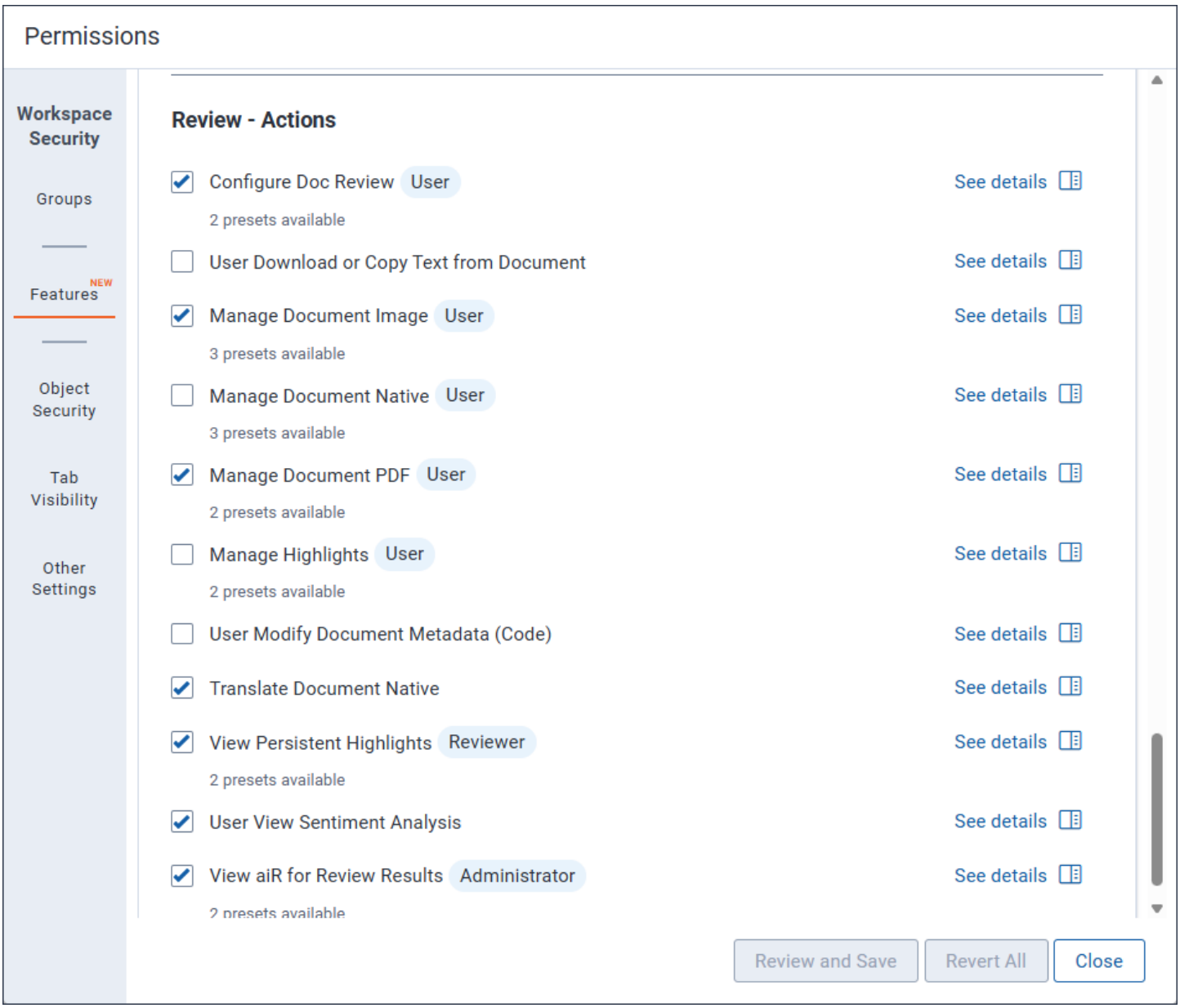
1. Open a document in the Viewer.
2. Click **Edit** on the layout.
3. Click **Manage** for the field that you want to add another choice.



The Choice Editor opens.

6.2 Permissions

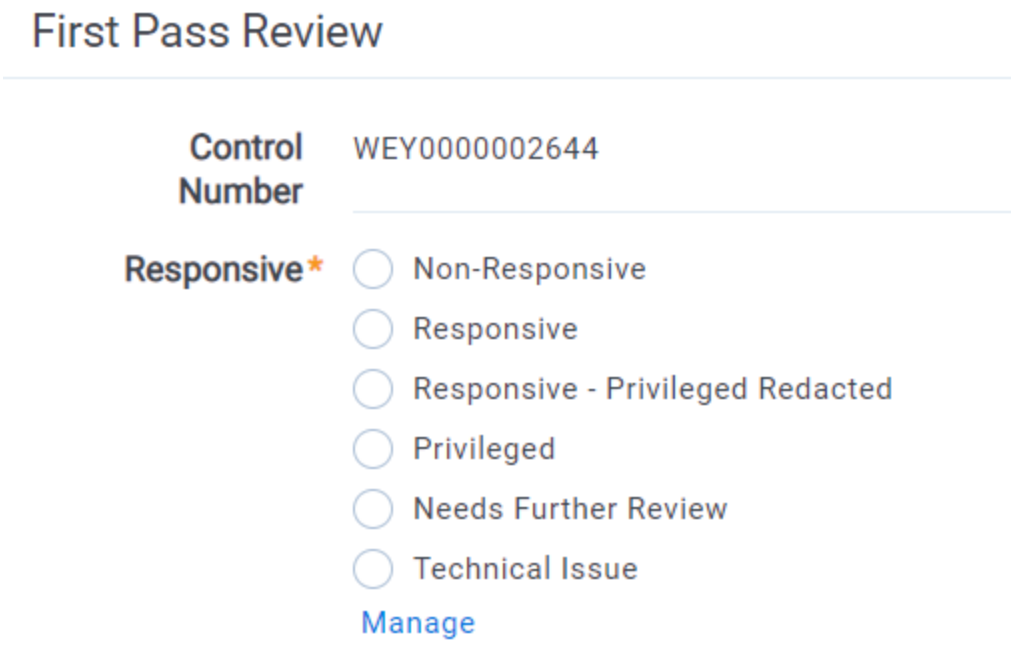
Manage permissions for this feature on the Features tab. Grant the full feature for a group, or customize access with individual actions. For an overview of features and actions, see Feature permissions.



In order for a group to be able to edit and add choices, you must grant them Edit and Add permissions on the Choice object.

If the **Add Field Choice By Link** box is checked, users can view the Choice editor through the **Manage** link on the layout, but they still cannot edit and add choices without those permissions.





6.3 Adding choices

Using the Choice editor, you can add a single or multiple choices to a field.

6.3.1 Adding a choice from the Fields tab

To add a choice from the Fields tab:

1. Navigate to the **Fields** tab.
2. Click on the Name of an existing field or create and save a new single or multiple choice field.
3. Locate the Choice editor in the **Choices** section on the Fields form.
4. Click **Add Choice** at the top or bottom of the Choice editor.
   Enter the name of the choice you want to add. The new choice is automatically saved.
5. (Optional) Click **Details** to customize the choice, and then click **Save**. See Choice detail fields on page 172.

6.3.2 Adding a choice from the Choices tab

To add a single choice from the Choices tab:

1. Navigate to the **Choices** tab.
2. Click **New Choice**.
3. In the Field section, select an **Object**.
4. In the Field section, select a **Field** that you want to associate the new choice with. The **Choices** section appears.
5. In the Choices section, click **Add Choice**.
6. Enter the name of the choice you want to add. The new choice is automatically saved.
7. (Optional) Click **Details** to customize the choice, and then click **Save**. See Choice detail fields on page 172.

6.3.3 Adding a choice from a layout

To add a choice from a layout:

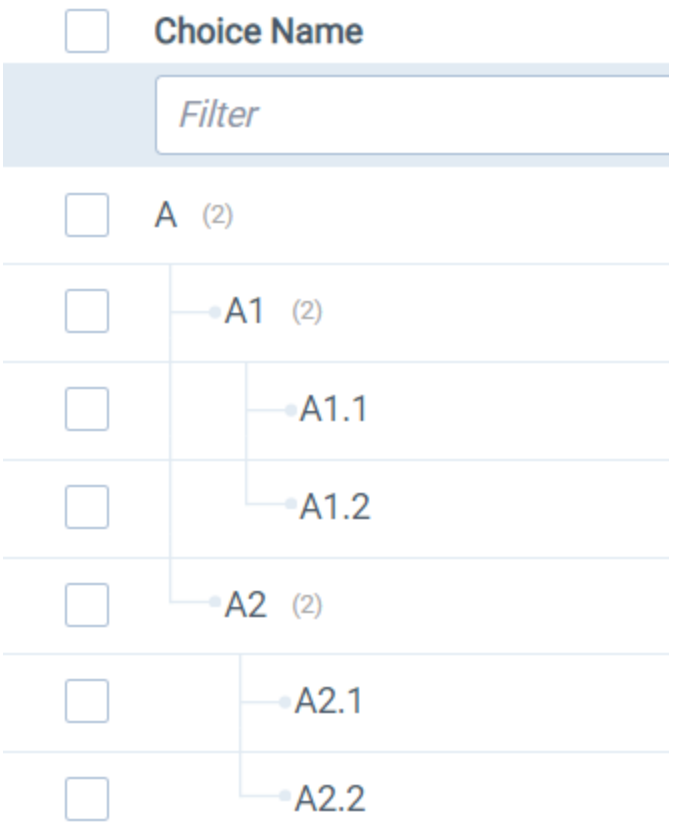
1. Under the field that you want to add a new choice, click **Manage**. The Manage Choices window opens.
2. Click **Add Choice** or **Click to add a choice**.
3. (Optional) Click **Options** to customize the choice, and then click **Apply**.
4. Click **Apply**.

6.3.4 Adding multiple choices

To add many choices:

Note: You can't create more than 300 choices at one time. If you attempt to create more than 300 choices at one time, then only the first 300 choices get created.

1. From the Choice editor, click **Add List of Choices**. The **Add List of Choices** textbox appears.
2. Enter each choice on a separate line. You can also copy and paste a large list of choices, but ensure each choice is entered on a separate line.
3. (Optional) To create families of choices, use hyphens at the beginning of each separate line. Each hyphen represents a level between parent and child choices. If a choice contains a hyphen, but there is no parent relation, a warning will display.
4. Click **Save**.



6.4 Editing choices

After you create a choice, you can edit the name and the details of the choice using the Choice editor.

6.4.1 Editing choice names

To edit the name of a choice:

1. Navigate to the **Choice editor**. See Accessing the Choice editor on page 165.
2. Click on the name of the choice that you want to rename.
3. Enter the new name of the choice. The new name is automatically saved.

6.4.2 Editing choice details

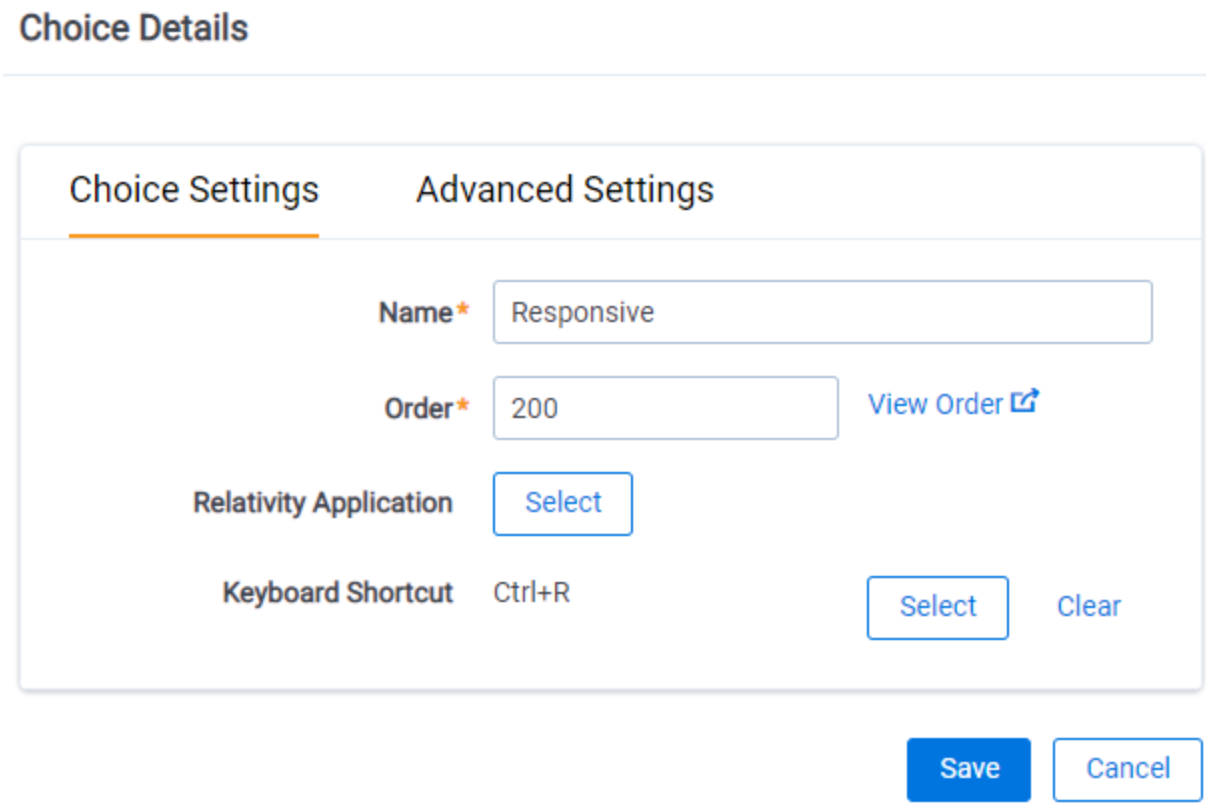
To edit the details of a choice:

1. Navigate to the **Choice editor**. See Accessing the Choice editor on page 165.
2. Hover over the name of the choice that you want to edit.
3. Click **Details**.
4. Modify the details of the choice. See Choice detail fields below.
5. Click **Save**.

6.5 Choice detail fields

The Choice Details editor has two tabs: Choice Settings and Advanced Settings.

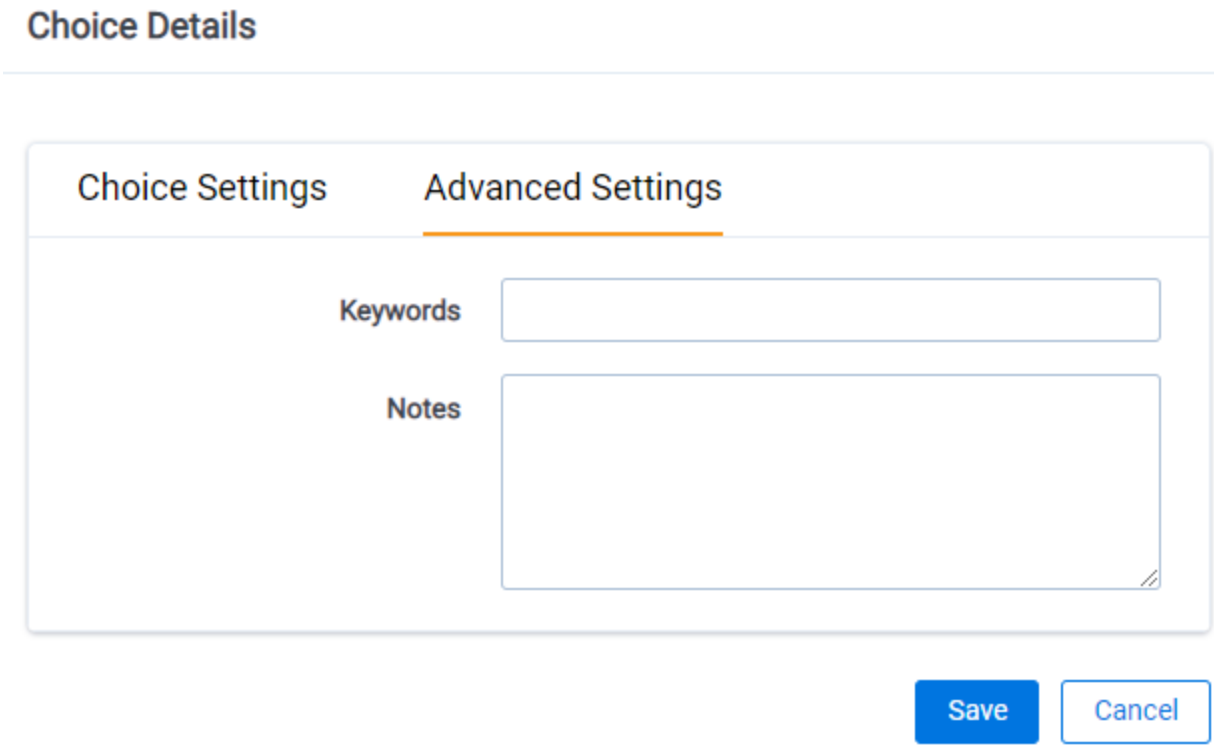
Choice Setting tab fields include:



- **Order** - a number that represents the position of the choice in relation to the field's other choices. The lower the number, the higher the position on the list. Pane order can be any positive or negative integer, but you can't use decimals.
- **Parent choice** - sets the parent choice.
- **Relativity Applications** - associates an existing application in your workspace to the new choice, in order to link to Relativity Dynamic Objects.See the Applications section in the Admin guide.
- **Keyboard Shortcut** - designates a keyboard shortcut for the document choice you're editing or creating. You can use the shortcut to code and edit documents in the Viewer. You need to be in edit mode before you can use keyboard shortcuts for choices. This setting is only available for document fields and consists of the following checkboxes. You have to use Ctrl and/or Alt or you get an <Invalid Keyboard Shortcut> warning next to the Key drop-down field:
  - **Ctrl** - sets the Control key as part of the combination used to trigger the keyboard shortcut.
  - **Alt** - sets the Alt key as part of the combination used to trigger the keyboard shortcut.
  - **Shift** - sets the shift key as part of the combination used to trigger the keyboard shortcut.
  - **Key** - sets the key you want to use in combination with the key specified in one or more of the check-boxes (Ctrl, Alt, and Shift).

  A pipe character and the keyboard shortcut appear next to the name of the choice when you create a keyboard shortcut.

Advanced Settings tab fields include:



- **Keywords** - keywords associated with the choice.
- **Notes** - any notes, such as a description, that you want associated with the choice.

6.6 Deleting choices

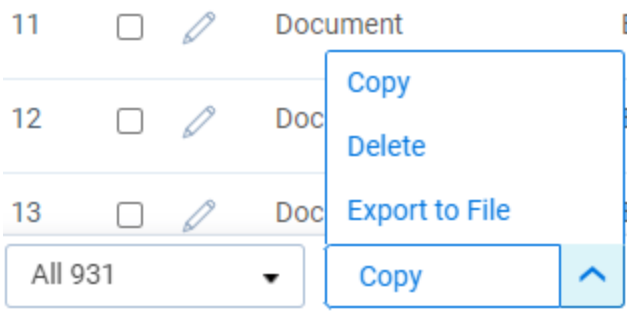
To delete a choice:

1. Navigate to the Choice editor. See Accessing the Choice editor on page 165.
2. Hover over the name of the choice that you want to delete.
3. Click **Delete**.

You can also delete multiple choices using the **Delete** mass operation from the **Choices** tab.

6.7 Performing mass operations on choices

You can perform mass Copy, Delete, and Export to File on choices from the **Choices** tab.



Notes:

- If you apply a mass operation on a parent choice, the mass operation is not automatically applied to the child choice.
- When deleting a parent choice in the Choice editor, Relativity also deletes the children.
- When using mass delete from a list page, you must delete all the children choices of a parent choice first before you can delete the parent choice.

6.8 Organizing choices

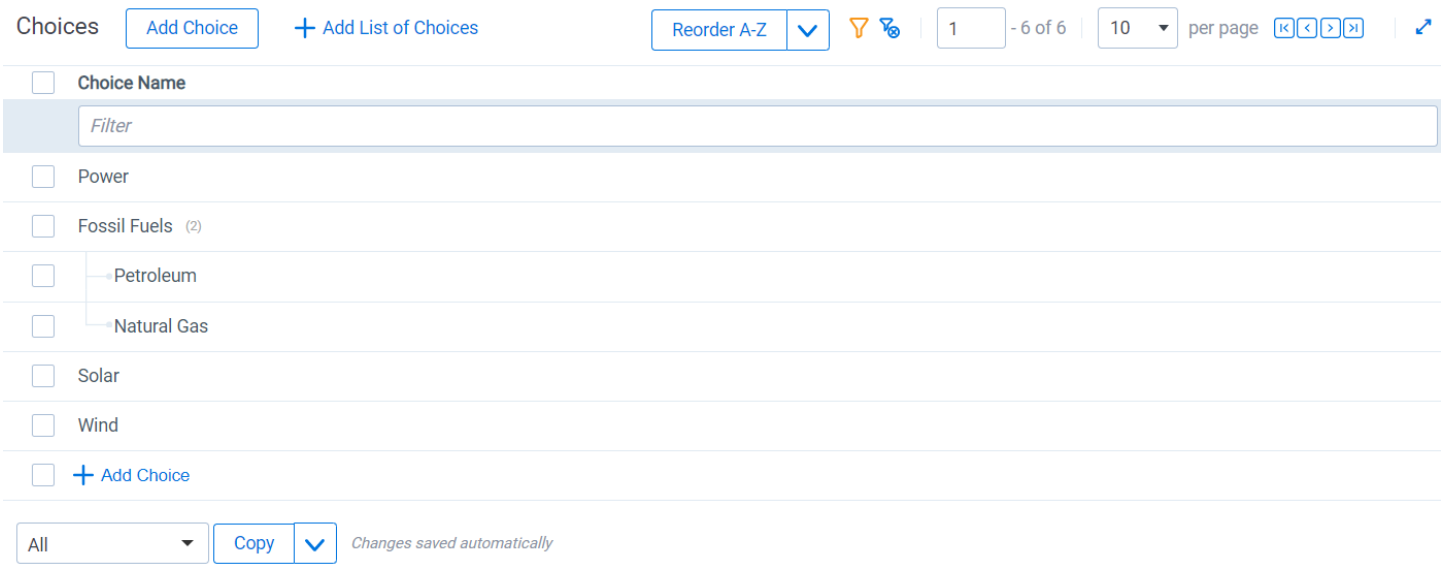
Using the Choice editor, you can reorder choices and create families of choices.

6.8.1 Dragging and dropping choices

To reorder choices, click the choice row you want to move and drag and drop the choice to the desired position. A blue bar appears in the position where the choice is moved to.

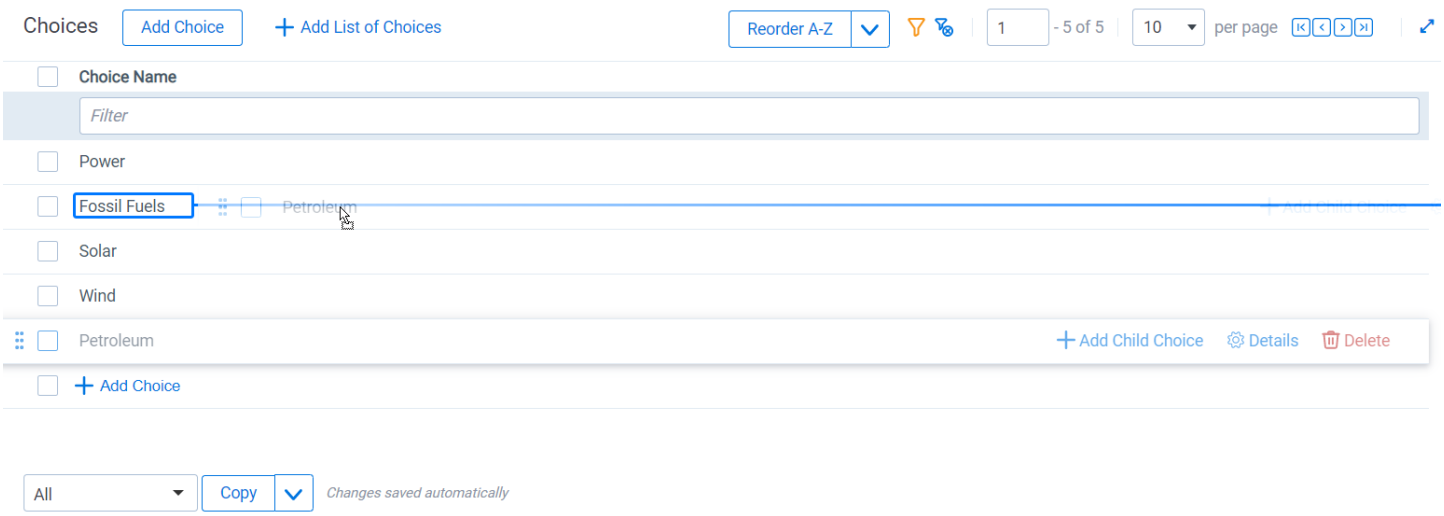
6.8.1.1 Creating choice families

Using the Choice editor, you can create choice families by nesting choices to create a parent choice. When a child choice is selected in a layout, the parent choice is automatically selected as well. A dotted gray line connects the parent choice to its children. In the screenshot below, **Fossil Fuels** is the parent choice of child choices, **Petroleum** and **Natural Gas**.



Note: You can only nest multiple choice field types.

To create a child choice, click the choice row and drag the choice into a preexisting choice. The preexisting choice becomes the parent choice. A double blue bar appears under the new parent tab where the child tab is moved to.



6.8.2 Alphabetizing choices

You can also alphabetize choices, parent choices, and child choices. To reorder choices in ascending alphabetical order, starting with A, click the Reorder drop-down menu and select **Reorder A-Z**. To reorder choices in descending order, starting with Z, click the drop-down on the reorder button and click **Reorder Z-A**.

Notes:

- You must have edit permissions for the field to reorder choices. If you don't have edit permissions for the field, the **Reorder A-Z** button will not appear in the Choice editor.
- Once you alphabetize the choices you can also rearrange choices within the sort. The alphabetize button will not automatically re-alphabetize the choices if you move choices individually.

6.8.3 Reordering top level choices

You can reorder top level choices in the Choices List using the Sort top level choices feature. You can use this method to edit the sort order of choices according to your preferences without manually editing each choice directly. This only reorders top level choices, not nested choices.

Follow these steps to Sort top level choices:

1. Click **Select All Choices**. The Choices List opens.
2. Click the **Sort Top Level Choices** link in the Sort Top Level Choices column for the field whose choices you want to reorder.
3. Select a choice in the **Order for codes of type** window.
4. Use the **Move Up** or **Move Down** buttons to order your choices.
5. Click **Save**.

Note: It is a suggested practice to order your choices in multiples of 10 so that it is easier to insert more choices in your intended order in the future. If you enter choices with orders that are not in multiples of 10 and use the Sort top level choices feature to reorder your choices, then Relativity automatically reorders all previously entered order numbers in multiples of 10.

6.9 Fields in workspaces

- **Field** - the single choice or multiple choice list field in which you want the choice to appear.
- **Name** - the choice value that appears to users. For example, if you want the choice to read "Responsive," name it "Responsive." Choice names can be up to 200 characters.
- **Order** - a number that represents the position of the choice in relation to the field's other choices. The lower the number, the higher the position on the list. Items that share the same value appear in alphanumeric order. Pane order can be any positive or negative integer, but you can't use decimals.

  Note: We recommend setting the tab order by 10's, starting with 10, then 20, 30, etc. Numbering in groups of 10 lets you later insert an item into any position without reordering all items (e.g., 10, 20, **25**, 30, 40).

- **Parent choice** - when you create a sub-choice, you can select a parent choice under which the current choice appears. Be aware that once you set your family of choices and tagged values, editing a parent choice causes inconsistencies.

  Note: If you need to change a parent choice, create a new choice family, mass edit the applicable documents, and then remove the old choice.

- **Relativity Applications** - associate an existing application in your workspace to the new choice, in order to link to Relativity Dynamic Objects. See the Applications section in the Admin guide.
- **Keyboard Shortcut** - designates a keyboard shortcut for the document choice you're editing or creating. You can use the shortcut to code and edit documents in the Review Interface. You need to be in edit mode before you can use keyboard shortcuts for choices. This setting is only available for document fields and consists of the following checkboxes. You have to use Ctrl and/or Alt or you get an <Invalid Keyboard Shortcut> warning next to the Key drop-down field:
  - **Ctrl** - sets the Control key as part of the combination used to trigger the keyboard shortcut.
  - **Alt** - sets the Alt key as part of the combination used to trigger the keyboard shortcut.
  - **Shift** - sets the shift key as part of the combination used to trigger the keyboard shortcut.
  - **Key** - sets the key you want to use in combination with the key specified in one or more of the checkboxes (Ctrl, Alt, and Shift).

6.10 Admin choices

From Home, choices are predetermined values applied to pre-workspace objects, such as workspaces, clients, and matters. These choices function the same as choices within a workspace.

To create or edit an admin choice:

1. Click your name in the upper right corner of Relativity and click **Home**.
2. Click the **Choices** tab.
3. Click **New Choice**. If you want to edit an existing choice, click the **Edit** link next to the Choice name.
4. Complete the fields on the form. See Admin fields on the next page.
5. Click **Save**.

6.10.1 Admin fields

- **Field** - sets the type of admin choice. You can select one of the following options:
  - **Case status** - choices available in the **Status** field on workspace objects.
  - **Client status** - choices available in the **Status** field on client objects.
  - **dtSearch Index Share Location** - choices available in the **Index share** field on dtSearch index objects.
  - **File location** - choices available in the **Default file repository** field on workspace objects.
  - **Matter status** - choices available in the **Status** field on matter objects.
  - **Processing Source Location** - choices available in the **Select source for files to process** field in processing set objects.
  - **User type** - choices available in the **Type** field under user information for user objects.
- **Name** - the choice value that appears to administrators. For example, if you want the choice to read "Internal," name it "Internal." Choice names can be up to 200 characters.
- **Order** - a number that represents the position of the choice in relation to the field's other choices. The lower the number, the higher the position on the list. Items that share the same value appear in alphanumeric order. Pane order can be any positive or negative integer, but you can't use decimals. You can click the View Order button to access the order of other choices.

Note: We recommend setting the tab order by 10's, starting with 10, then 20, 30, etc. Numbering in groups of 10 lets you later insert an item into any position without reordering all items (e.g., 10, 20, **25**, 30, 40).

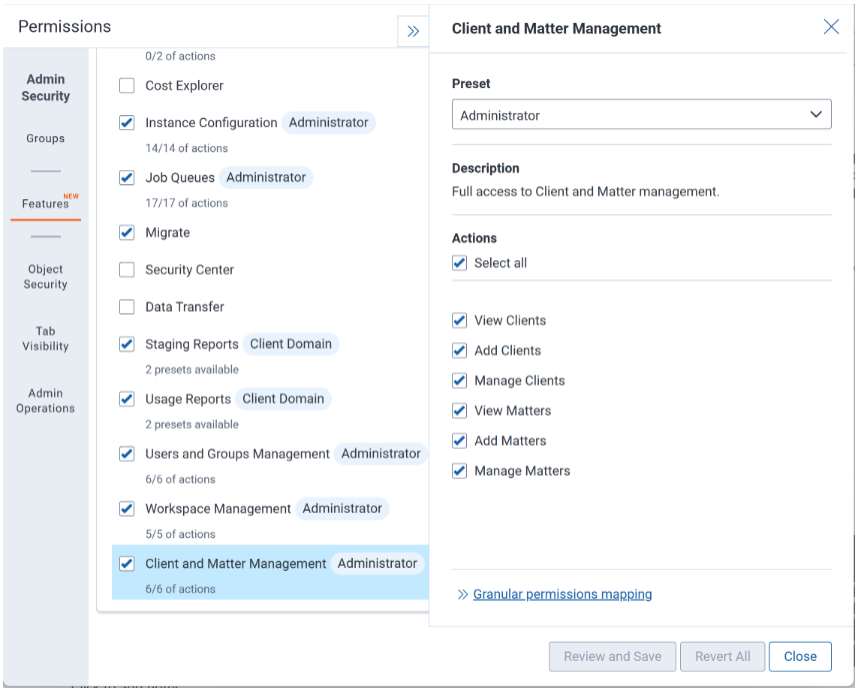
You can also add or edit an admin choice on the Choices tab. See Adding choices on page 170.

7 Clients

Clients are companies or organizations. In Relativity, link clients with associated users, matters, groups, and workspaces.

7.1 Permissions

Manage permissions for this feature on the Features tab. Grant the full feature for a group, or customize access with individual actions. For an overview of features and actions, see Feature permissions.



7.2 Creating or editing a client

To create a client or edit information for an existing client, perform the following steps:

1. Select the **Clients** tab and then click **New Client** to create a new client, or click **Edit** next to the client whose information you want to edit. The New Client form appears.

   Note: If your Clients tab view list does not contain the **Edit** field, you can add it.

2. Complete the fields on the form. See Fields below.
3. Click **Save**. You can optionally enable tenancy on the client.

7.2.1 Fields

The following fields display on the Client Information form. Fields in orange are required.

- **Name** - the name of the client. The name must be between 1 and 210 characters.
- **Client Number** - the billing number for the client. This value must be between 1 and 50 characters.
- **Status** - the current status of the client. The default options are active or inactive, but you can add any status value. Use the status value to organize and display lists of clients using Relativity views. See Views on page 702.

7.3 Enabling client domains on a client

Note: You cannot convert an existing client to a client domain.

To request a new client domain, you must submit a Relativity aiR request via the Community site by navigating to the Support tab and then Relativity aiR requests (as detailed in the following knowledge article). Please note that the Client Domain creation process takes 3 business days. If an Utility Server was requested, you will also be contacted with the following information:

- IP address to the new client domain Utility Server.
- Client domain user credentials to the new Utility Server.

The following things occur automatically after client domains are enabled:

- The system creates a new **Everyone - [Client's Name]** group and adds that group to the client domain. Only users whose client field is set to the client domain are included in the client domain everyone group. The system also removes those users from the default Relativity Everyone group. A system admin can add any users to any group regardless of client domain status.

  Note: The **Everyone - [Client's Name]** group should not be assigned as the workspace administrator group for a given workspace that is part of a Client Domain.

- The system creates a unique copy of all resource pools associated with any workspaces under the client domain.

  Note: Permissions assigned to groups override client domain isolation. If a non-client domain group has permissions to see a client domain's workspace or users, then those non-client domain users in the non-client domain group can still access client domain items. Enabling client domains does not change previously configured item level security settings applied to any objects within the client domain.

- The system creates a client domain admin group that permits its members to perform admin operations within the client domain.

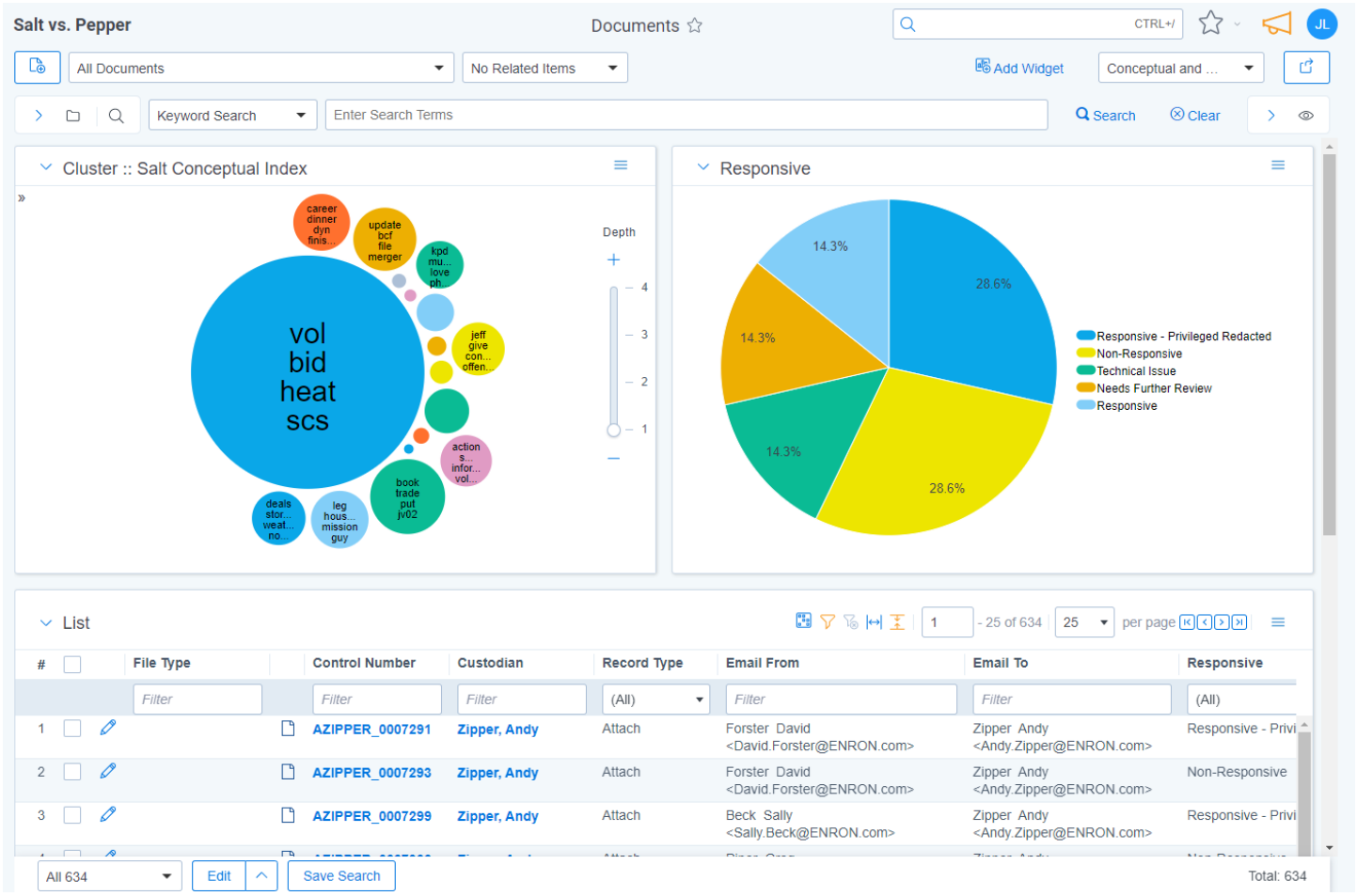
  Note: After enabling client domains, system administrators needing to make group or permission changes should be extra cautious and thoroughly investigate the potential impact to client domain separation before implementing any new group/permission changes.

- The newly created Client Domain Admin group is automatically granted admin permissions to the staging file share provisioned for that client domain, enabling full file share management (view, upload, download, edit, secure) within their domain's staging area.

8 Dashboards

When you've created a page configuration you'd like to preserve, you can create a customized dashboard. You can save multiple dashboards to quickly change the page configuration. The item list and any widgets on the dashboard will update automatically in response to filtering or searching. Dashboards only report on data within the workspace you are in.

Note: For a list of dashboards that provide an effective starting point for administrators to help review teams visualize their data set, see Common commonly-used dashboards in the Admin Guide.



The page initially appears with the folder browser on the top left, the search panel on the bottom left and the item list to the right. Within this new framework, you have multiple options for customizing your display.

You can resize, move, or collapse any panel on the page, including any widgets you create.

- To resize any panel, hover over the line separating the item list from the panel until you see the mouse pointer change to horizontal arrows, then click and drag.
- To move, hover over the top of the panel until you see the Multi-Direction Cursor icon. Then, click and drag the panel to the new location.
- To collapse the search panel or browser pane, click the Collapse icon. Once collapsed, click the **Show Browser Panel** icon to restore the browser pane or the **Show Search Panel** icon to restore the search panel.

Additionally, you can drag and drop panels to rearrange on the page. Click any panel and drag it to a new location. The other panels will automatically move to accommodate the panel you're dropping.

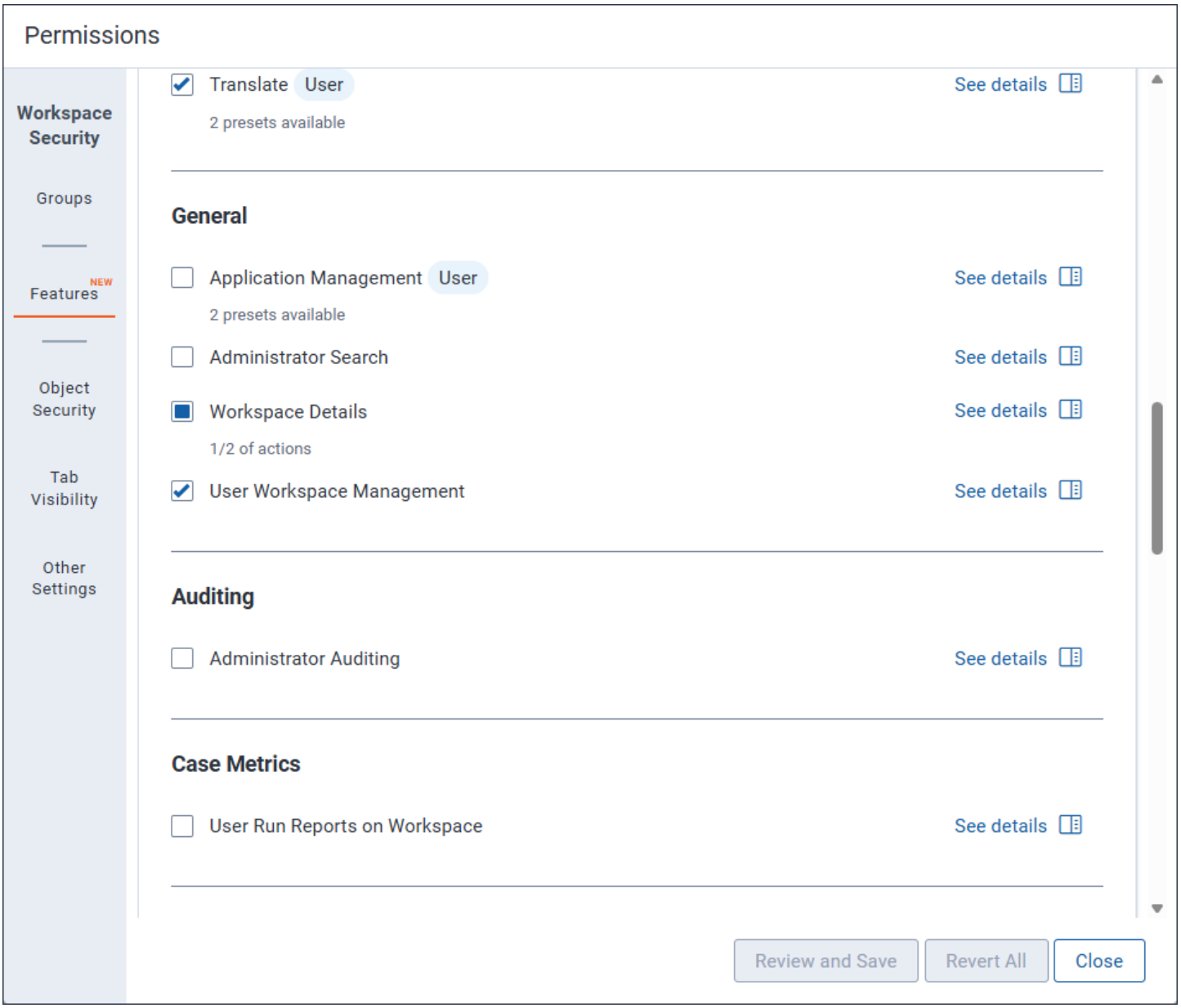
Dashboards and widgets can be copied over to newly created workspaces if they are part of a template. Dashboards only report on data within the workspace you are in if data is loaded in the workspace.

Note: You must have the correct workspace permissions to add, edit, or save a dashboard and to save pivot widgets to your dashboard.
You can also export individual Pivot widgets to Excel or to PNG format from each widget's context menu. See Exporting a Pivot widget in the Admin Guide for more information.

Note: To enable the Add Widgets button and Pivot functionality for an Relativity Dynamic Object (RDO), you must select Enabled for the **Pivot** property in the Object Type Information section for the object.

8.1 Permissions

Manage permissions for this feature on the Features tab. Grant the full feature for a group, or customize access with individual actions. For an overview of features and actions, see Feature permissions.



8.2 Creating a dashboard

To create a dashboard:

1. Click the **Dashboards** drop-down menu in the top right corner of the screen.

   Note: You can only access the drop-down if Pivot is Enabled for the given object type.

2. Click **New Dashboard** to save the current page configuration as a new dashboard.
3. Enter a name and an order number for the dashboard.

Note: The dashboard with the lowest order number will appear by default when you log in to Relativity.

8.3 Adding widgets to a dashboard

You can add the following widgets to customize your dashboard:

- **Pivot charts and tables**—you can use Pivot to summarize data in tables or charts to visually analyze trends in your data.
- **Cluster visualizations**—on the Documents tab, you can use Relativity Cluster Visualization to render your cluster data as an interactive visual map by adding a Cluster Visualization widget. This offers you a quick overview of your document cluster sets and quickly drill into each cluster set to view sub-clusters and conceptually-related clusters of documents. Please note that there may be only one cluster visualization widget per dashboard.
- **Communication Analysis**—after running the name normalization operation within structured analytics, you can use this widget to visualize communication frequencies, patterns, and networks between the entities linked to the documents in the view.

Note: When you reach the maximum number of widgets allowed on a dashboard, the **Add Widget** button will be grayed out and a tooltip displays when you hover over it that lets you know the reason you cannot add any additional widgets to your dashboard. This is controlled by the **MaxNumberDashboardWidgets** instance setting.

8.4 Saving changes to a dashboard

You can also make changes on the fly and save a dashboard with the changes. If a dashboard has not been saved, an orange notification displays in the Dashboard drop-down menu until it is saved.

1. Click the Dashboards drop-down menu in the top right corner of the screen to display the list of dashboards available on the current tab.
2. Click **Save** to save the changes to the existing dashboard. Click **Save As** to save the page configuration as a new dashboard, and then enter a **Name** and **Order** number.

Note: If a dashboard is part of a locked application, the option to save the dashboard is unavailable.

8.5 Deleting a dashboard

To delete a dashboard from the current tab you are in, click the **Delete** icon to the right of the dashboard you want to delete in the Dashboards drop-down menu.

Click **Delete** in the Delete Dashboard Confirmation pop-up window to delete the dashboard.

Note: If a dashboard is part of a locked application, the option to delete the dashboard is unavailable.

8.6 Renaming a dashboard

To rename a dashboard:

1. Click on the **Edit** icon next to the name of the dashboard in the Dashboard drop-down menu.
2. Enter a **Name** and an **Order** number for the dashboard. The order number controls the order in which the dashboard displays in the list.
3. Click **Save** to save your changes.

Note: If a dashboard is part of a locked application, the option to edit the dashboard is unavailable.

8.7 Filtering a dashboard

You can narrow the content in a dashboard so that only the results of a single field displays by double-clicking on a bar in a bar chart or a portion of a pie chart. Alternatively, you can narrow the content in a line graph by clicking on a node or to filter the results in a table, click on a field and then click **Accept**.

To clear the filters on a dashboard:

1. Ensure the search panel is expanded. If it is hidden, click on the **Show Search Panel** icon in the upper-left.
2. Ensure that the **Auto-run** field in the search panel is enabled.
3. Click **Clear All Conditions**.

8.8 Exporting a dashboard

You can export the pivot charts and cluster visualization images on your dashboard to Microsoft Excel. The charts can then be modified as needed in Excel. Cluster visualization images cannot be modified using Excel, however, since they are a PNG image of the visualization.

Note: Exporting to Excel functionality does *not* require Microsoft Excel to be installed (except for viewing of the exported file).

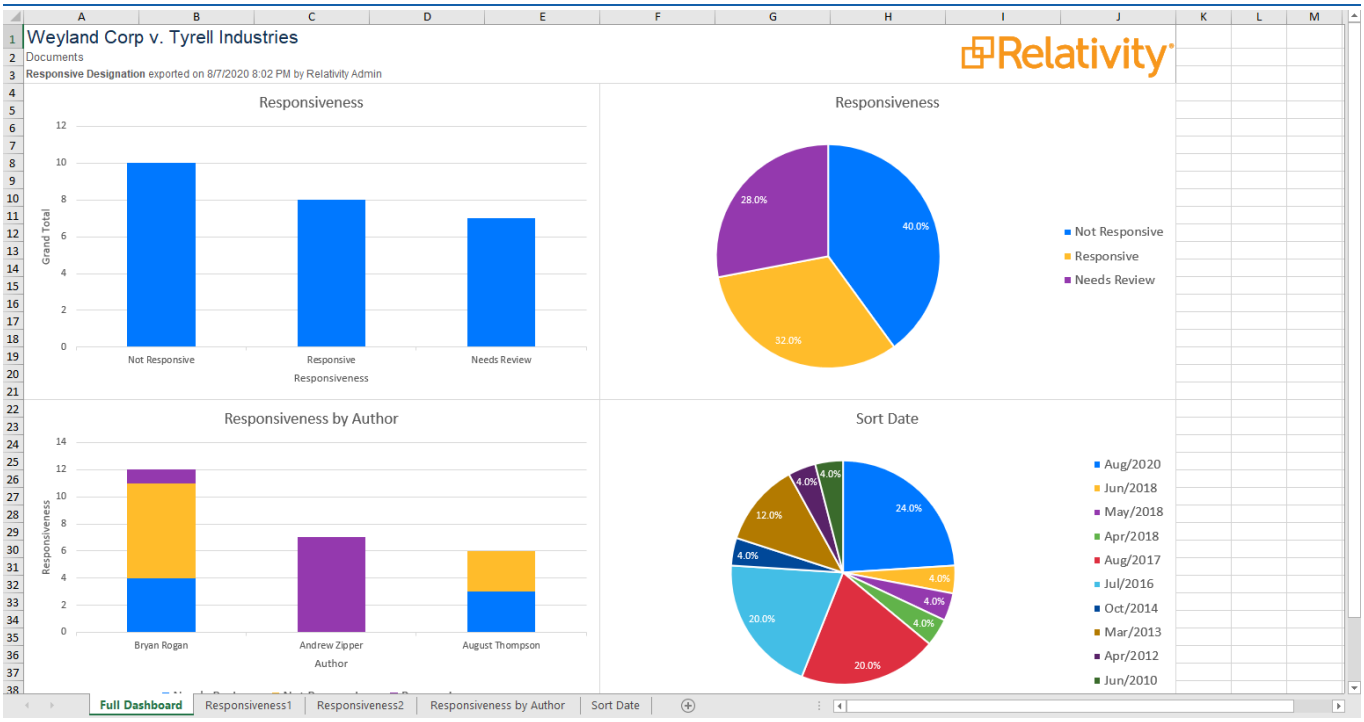
To export your dashboard to Excel:

1. On your current dashboard, click the **Export** button to the right of the Dashboard drop-down to export your dashboard with the currently selected export format settings.
   Alternatively, click the drop-down arrow to the right to make the following export format setting selections, and then click the **Export** button at the bottom of the drop-down menu. By default, all listed items are selected, but the individual selections that you make persist until you change them.
   - **Dashboard name** - selecting this means the name of the dashboard will be included in the export.
   - **Export date and time** - selecting this means the date and time of the export will be included in the export.
   - **Show data worksheets** - selecting this means the data for the individual widgets will be included in the export (and you can then modify this data).
   - **Relativity logo** - selecting this means the Relativity logo will be included in the export.
   - **User Name** - selecting this means the username that created the export will be included in the export.
   - **View Name** - selecting this means the name of the view from which the export was generated will be included in the export.
   - **Workspace Name -** selecting this means the name of the workspace will be included in the export.

   Relativity will automatically generate and download the new Excel workbook locally for you.

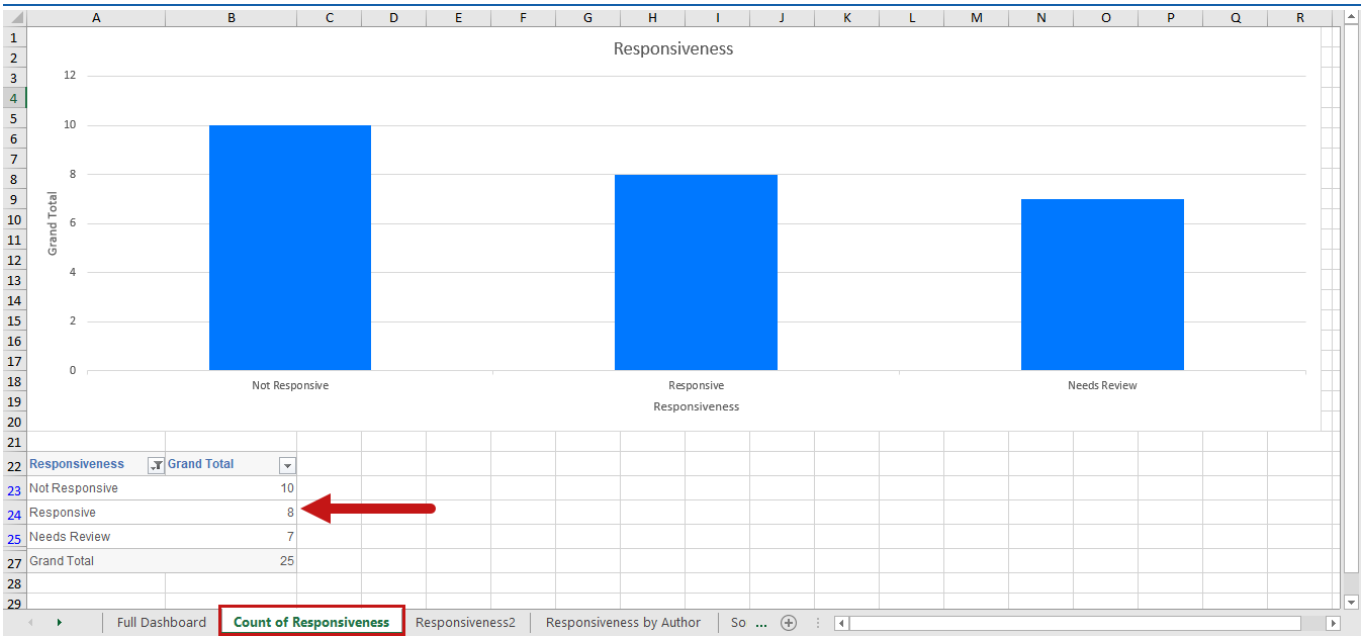
2. Click on the new Excel document that was downloaded locally to open it.

Note: If you export a scroll-able table widget, it will not be shown on the Full Dashboard worksheet tab.



3. You can modify the data on the relevant worksheet for the chart and all the charts including the Full Dashboard worksheet update to reflect the modified data using Excel's built in chart functionality. Furthermore, the data table is sortable and filterable—the chart will reflect the data listed in the table. You can refer to user documentation on how to use charts in Microsoft Excel for more information on modifying these charts for other purposes.

Note: You cannot modify any cluster visualization using Excel, since this is just a PNG image of the visualization.

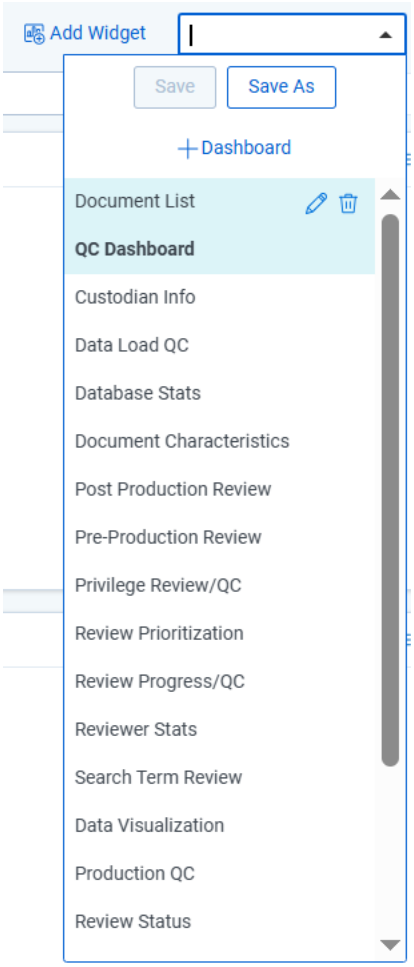


Note: You can also export individual Pivot widgets to Excel or to PNG format from each widget's context menu. See Exporting a Pivot widget in the Admin Guide for more information.

8.9 Commonly-used dashboards

This topic provides recommendations for the fields to group by and pivot on to create some commonly used dashboards in your case life cycle.

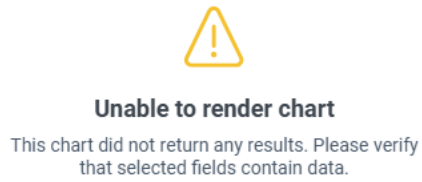
With these dashboards, you and your case team will be better equipped to explore and prioritize your review, identify patterns and trends across custodians, and develop better review strategies with real-time insight.



Use the examples described below to generate ideas for dashboards you may want to create in your cases.

Note the following:

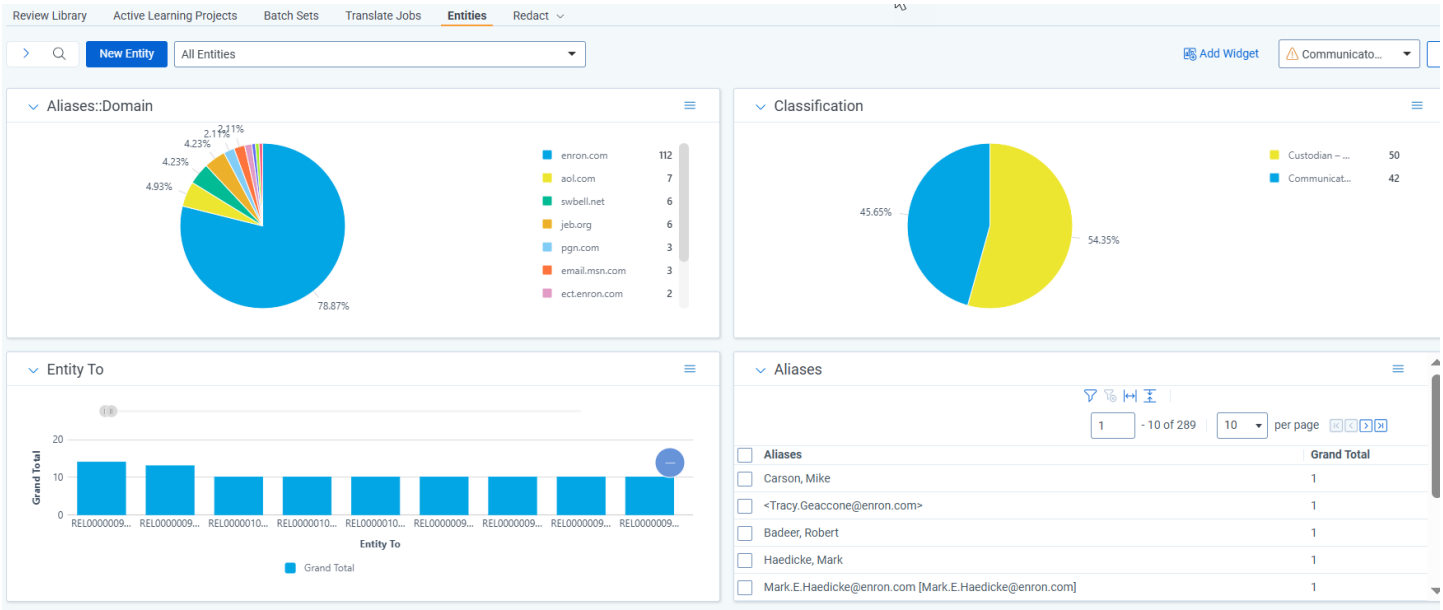
- The fields described here may differ in name than what you see in your workspace.
- When adding a widget, you cannot select fields that have not been enabled for pivot on or group by; you must manually enable those fields in order to select them. If those fields are part of a locked application, you must unlock it in order to edit them.
- A widget will not render if the included fields do not contain any data. For example, if you attempt to create an STR-based dashboard without having run STR on key terms, you will see the following:



8.9.1 Communicators

If you've run name normalization and want to create a Communicators dashboard within the Entities tab, group by and pivot on the following fields:

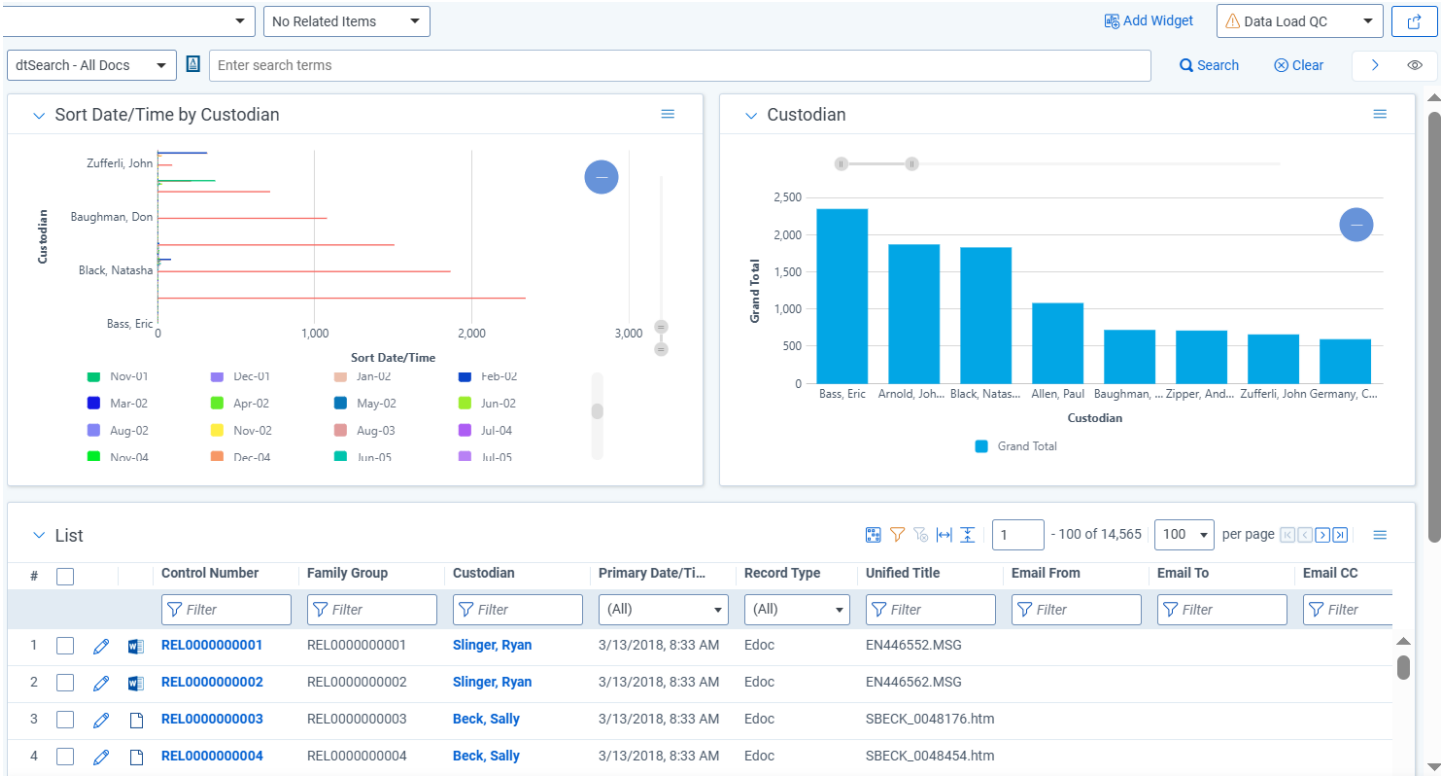
- Group by Aliases: Domain
- Group by Aliases
- Group by Classification
- Group by Entity To



8.9.2 Data Load QC

To create the Data Load QC dashboard, group by and pivot on the following fields:

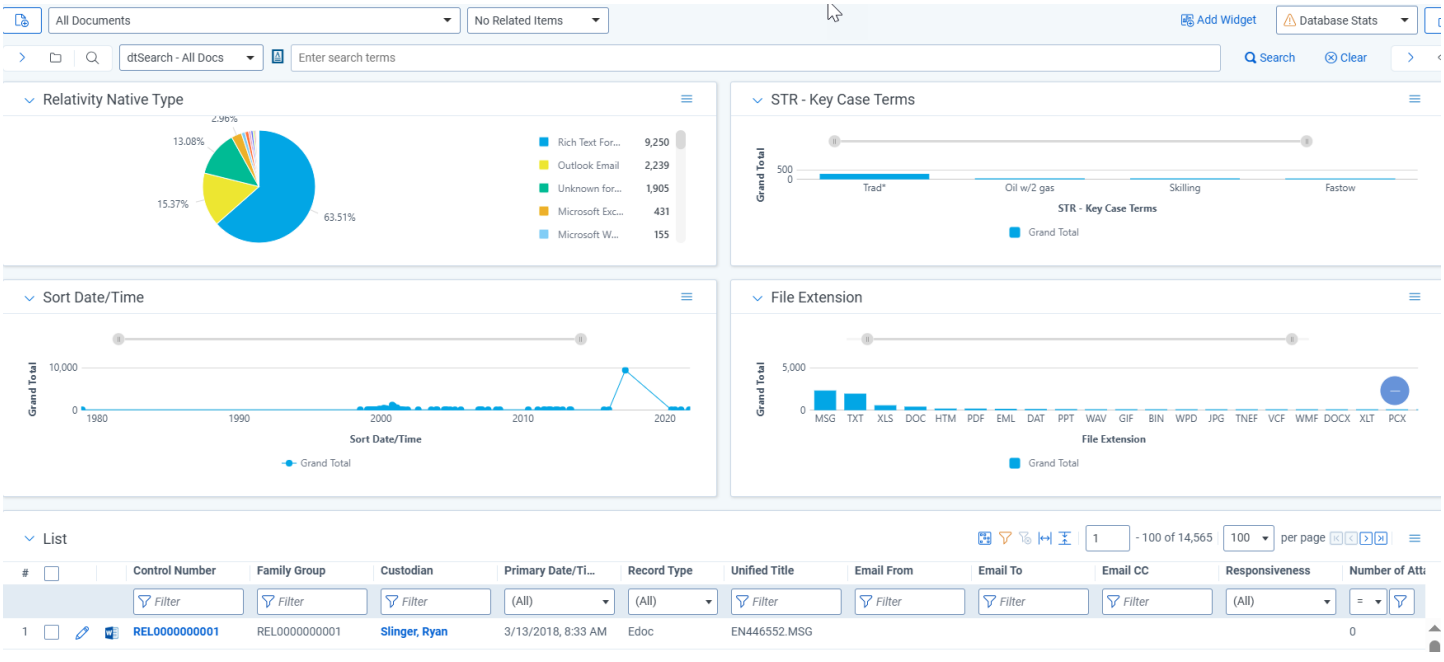
- Group by Custodian
- Group by Custodian and pivot on Sort Date (Year)



8.9.3 Database Stats

To create the Database Stats dashboard, group by and pivot on the following fields:

- Group by Native Type
- Group by Extension
- Group by Sort Date
- Group by Key Term STR

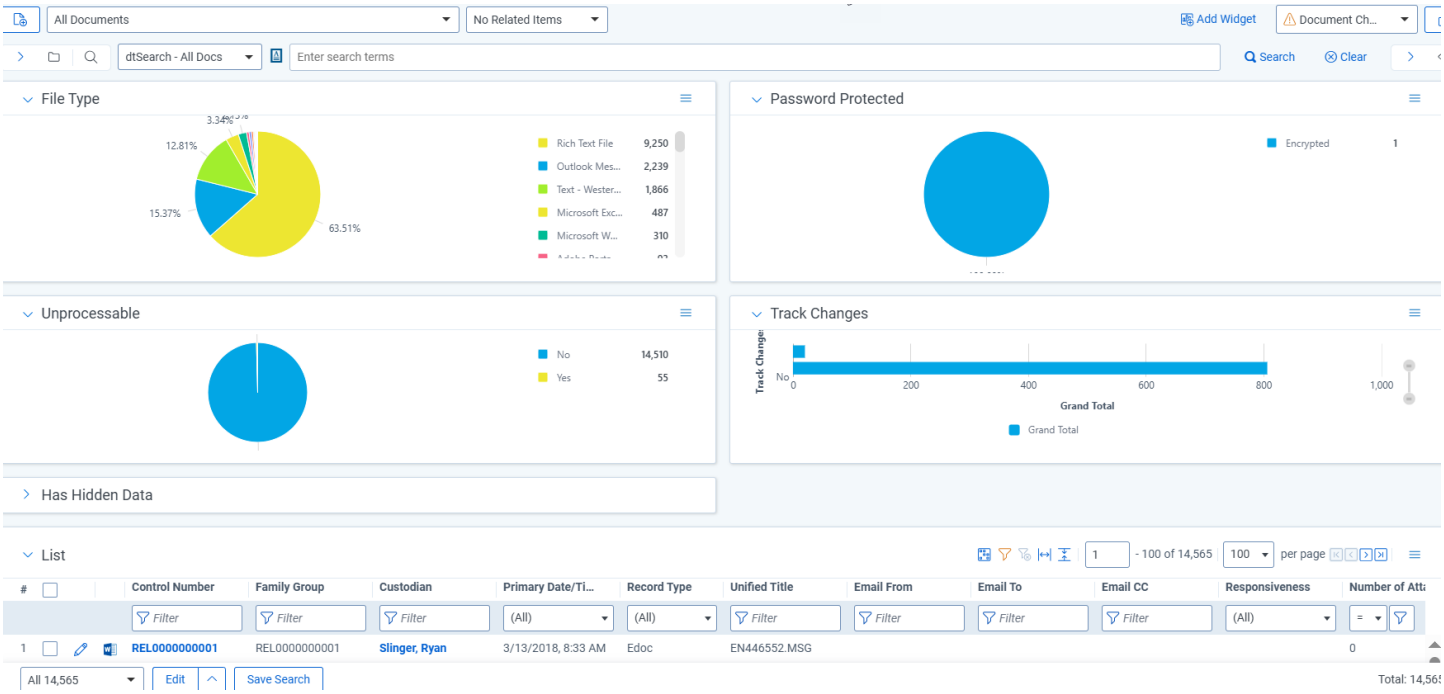


8.9.4 Document Characteristics

To create the Document Characteristics dashboard, group by and pivot on the following fields:

- Group by Unprocessable
- Group by Track Changes
- Group by Password Protected
- Group by File Type
- Group by Has Hidden Data - this widget is collapsed in the dashboard example below.

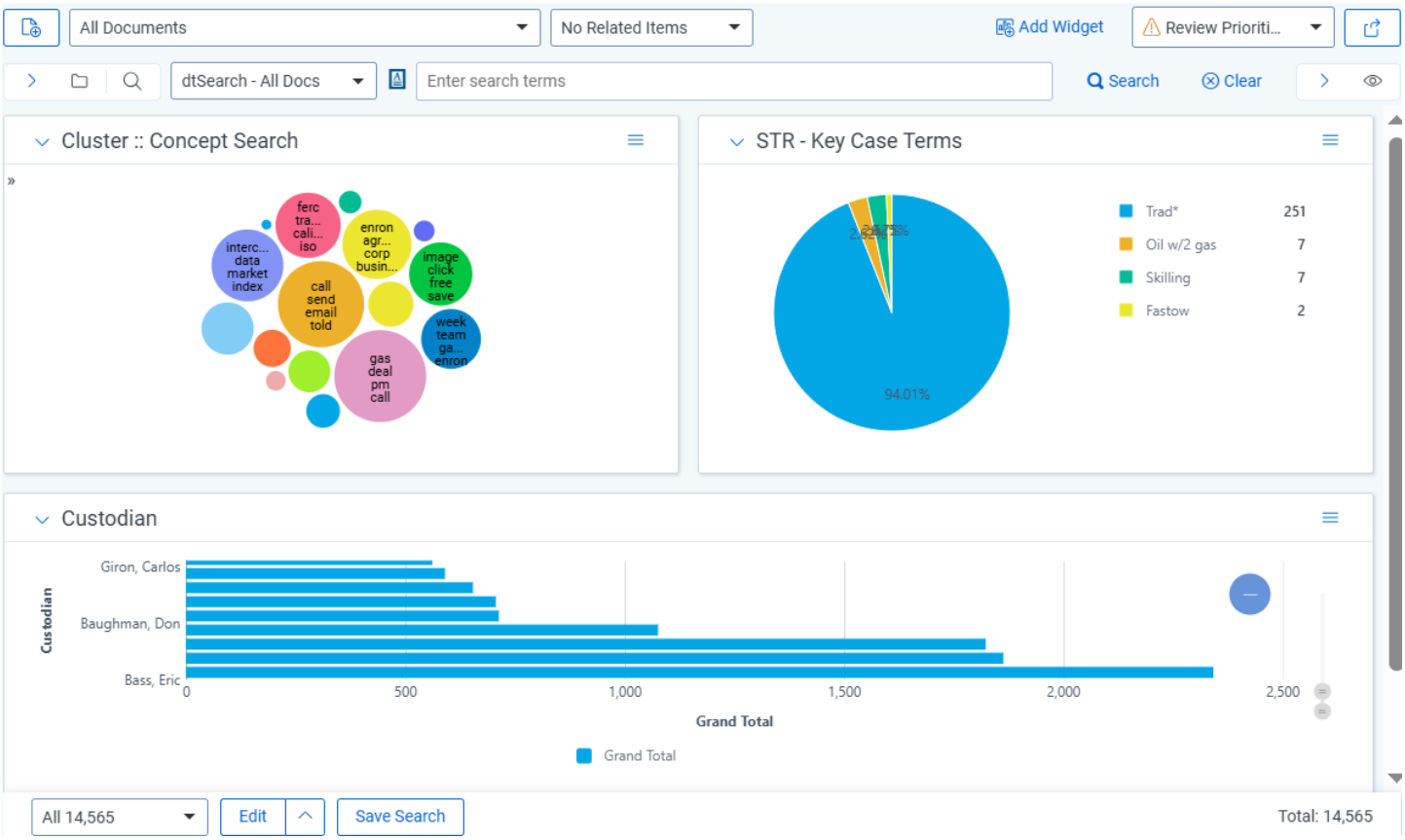
Note: You can collapse your widgets, as seen in Has Hidden Data below. If you save your dashboard with a widget collapsed, it will remain collapsed.



8.9.5 Review Prioritization

To create the Review Prioritization dashboard, group by and pivot on the following fields:

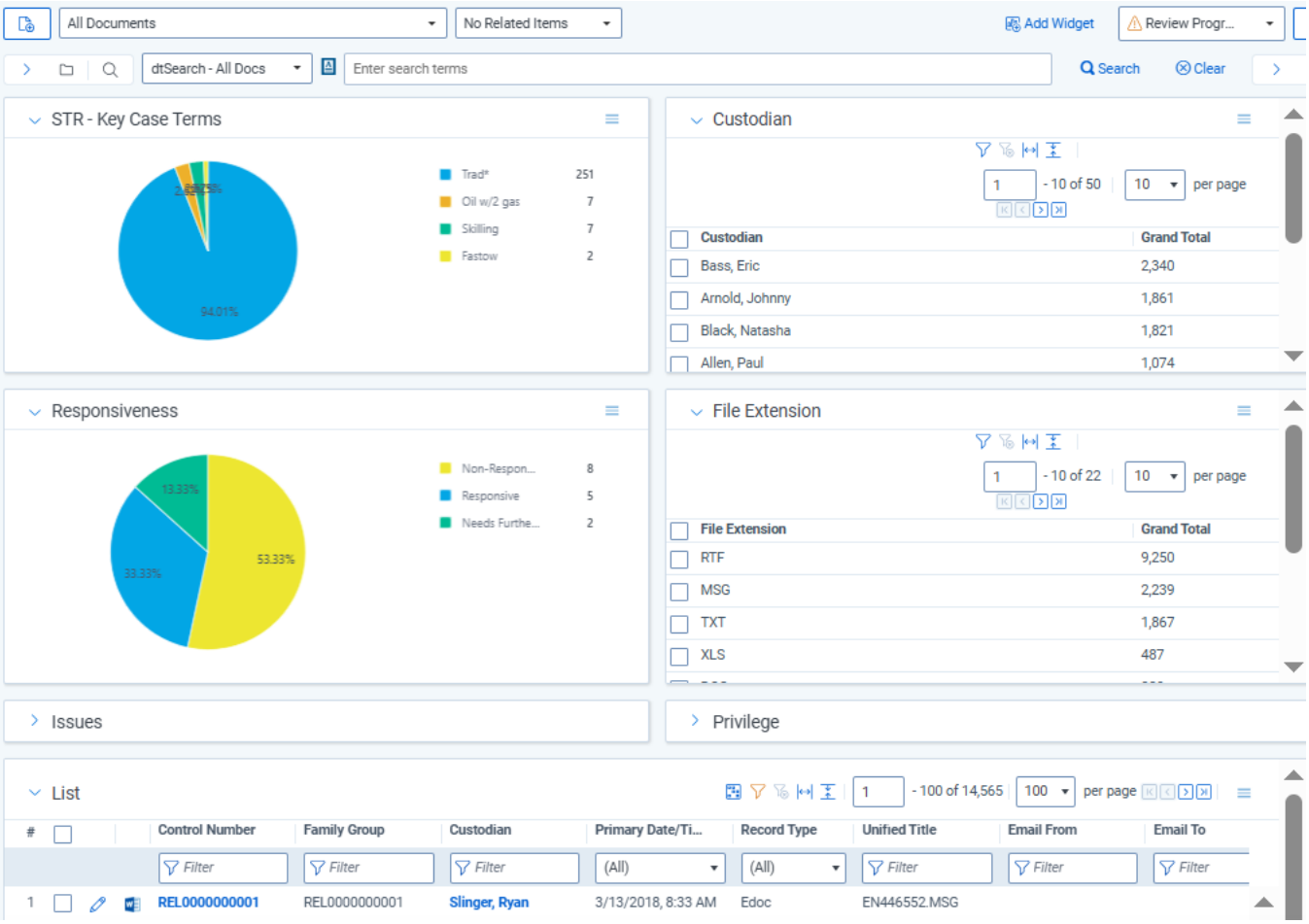
- Cluster Visualization Widget
- Group by Key Term STR
- Group by Custodian



8.9.6 Review Progress/QC

To create the Review Progress/QC dashboard, group by and pivot on the following fields:

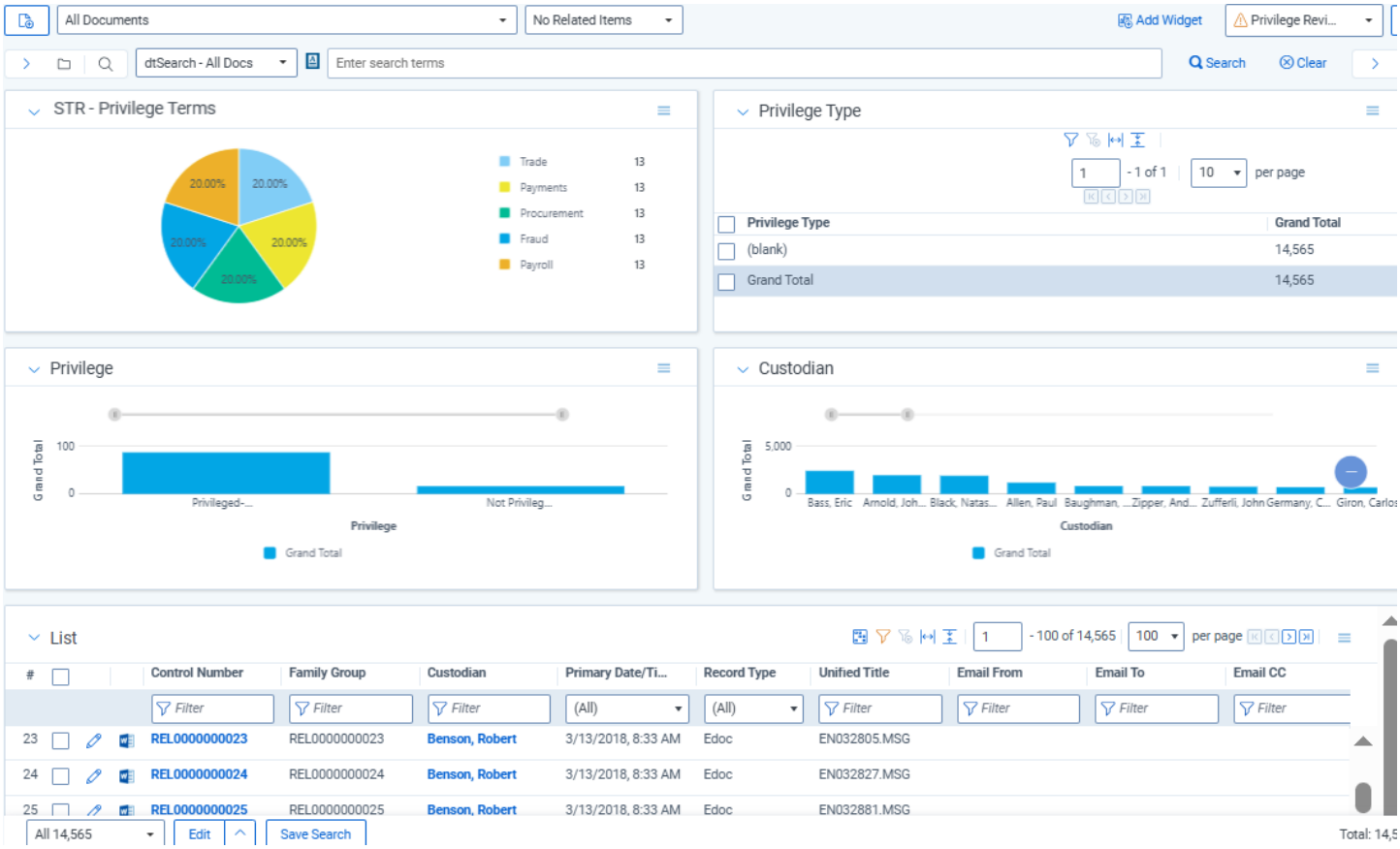
- Group by Responsive Designation
- Group by Privilege
- Group by Issues
- Group by Key Term STR
- Group by Custodian
- Group by File Extension



8.9.7 Privilege Review/QC

To create the Privilege Review/QC dashboard, group by and pivot on the following fields:

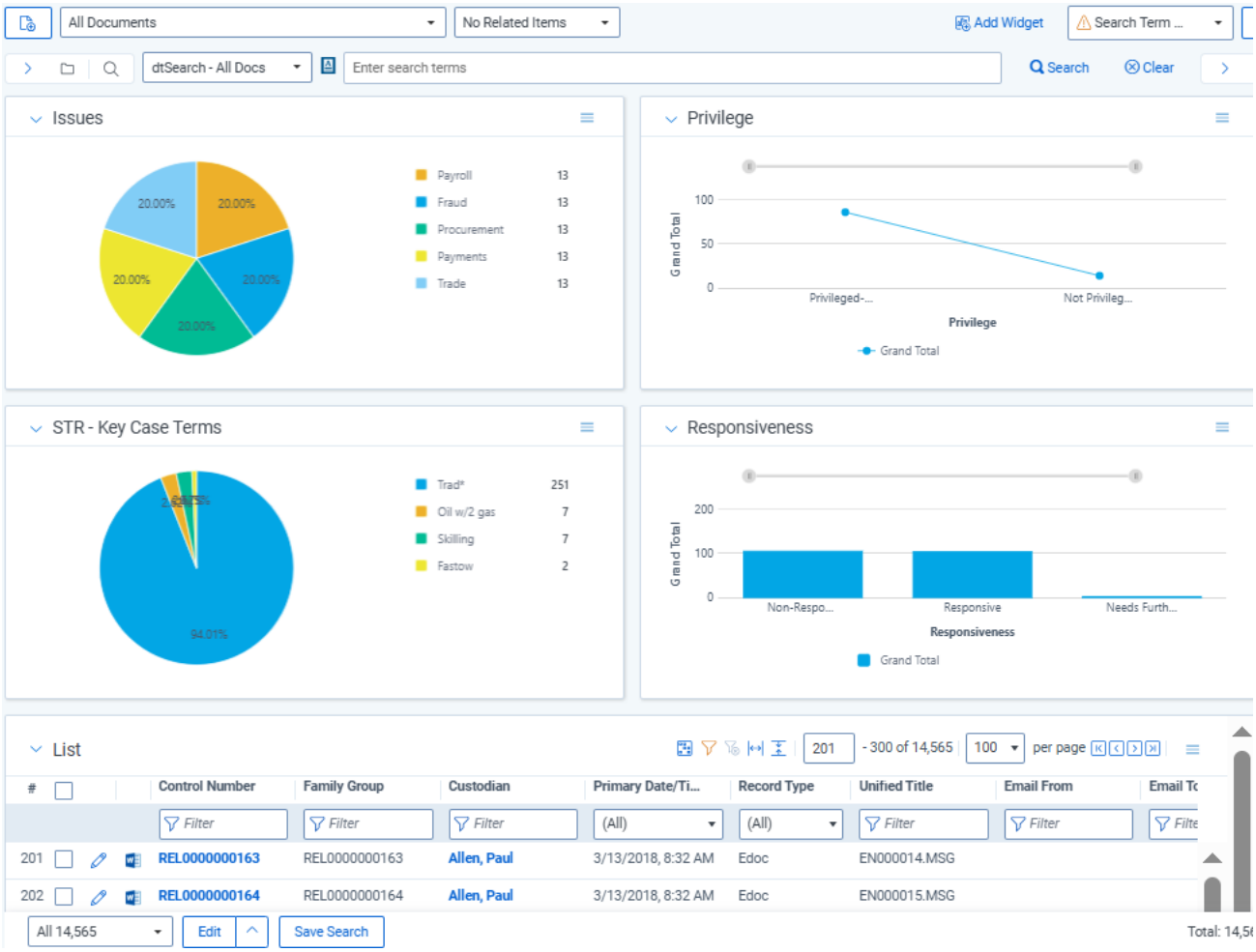
- Group by Privilege
- Group by Privilege Designation
- Group by Privilege Terms STR
- Group by Custodian



8.9.8 Search Term Review

To create the Search Term Review dashboard, group by and pivot on the following fields:

- Group by Responsive Designation
- Group by Key Term STR
- Group by Issue Coding STR
- Group by Issues
- Group by Privilege
- Group by Privilege Terms STR

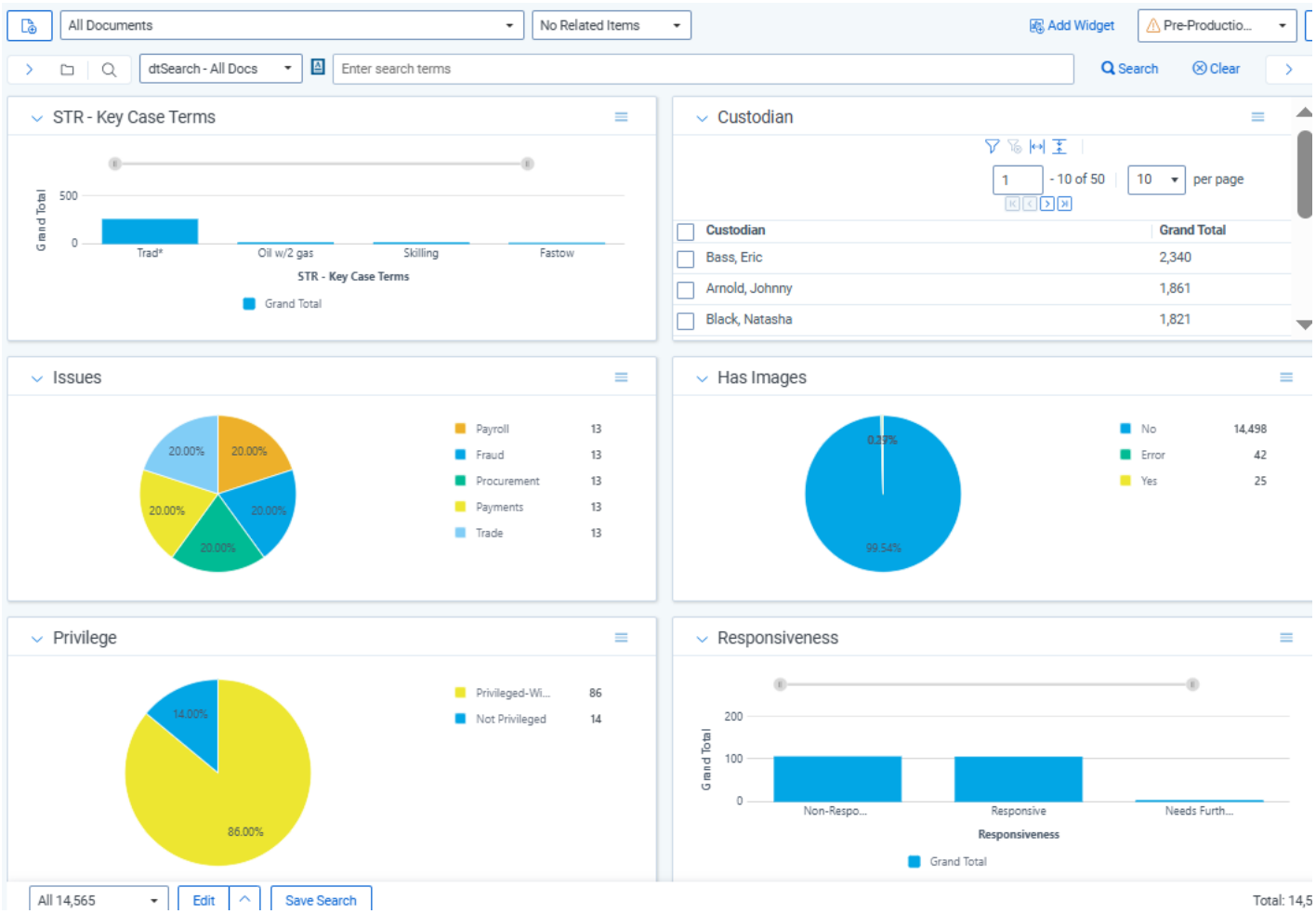


8.9.9 Pre-Production QC

Note: The production fields in your environment may not be enabled for group by/pivot on, and you may be unable to manually enable them if the application is locked.

To create the Pre-Production QC dashboard, group by and pivot on the following fields:

- Group by Custodian
- Group by Responsive Designation
- Group by Privilege
- Group by Key Term STR
- Group by Has Images
- Group by Issues

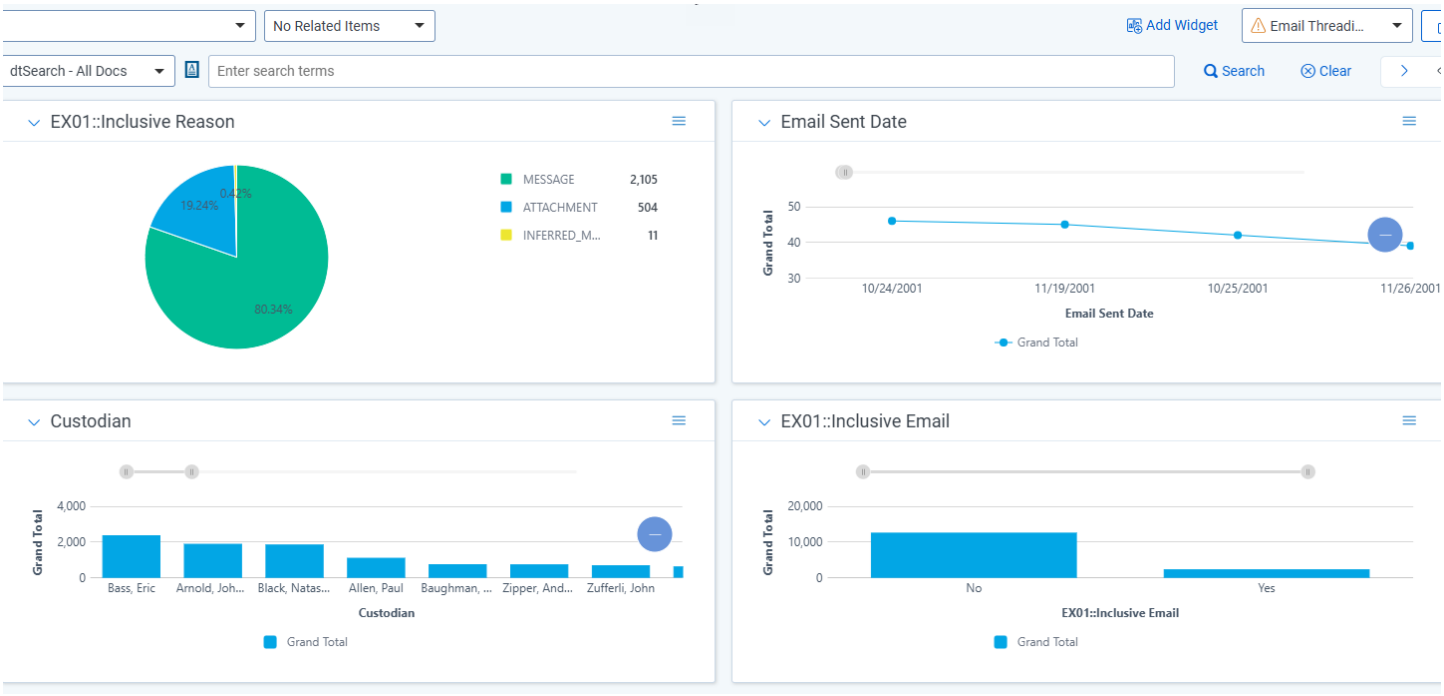


8.9.10 Email Threading

To create the Email Threading dashboard, group by and pivot on the following fields:

- Group by Inclusive Email
- Group by Inclusive Reason
- Group by Custodian
- Group by Date Sent (year)

Note: We recommend using your Email Threading view with this dashboard.

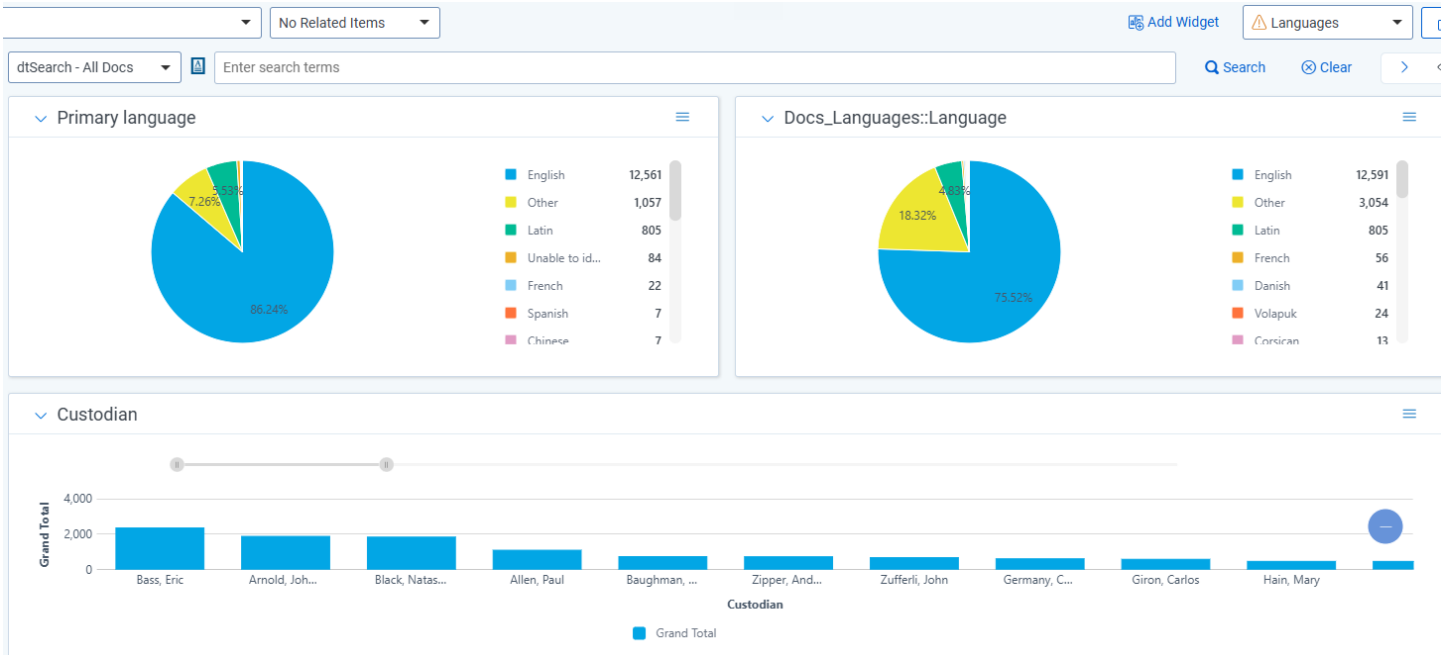


8.9.11 Language Identification

To create the Language Identification dashboard, group by and pivot on the following fields:

- Group by Primary Language
- Group by Docs_Languages::Language
- Group by Custodian

Note: We recommend using your Language Identification view with this dashboard.



8.9.12 Special considerations

- Create a default Document List dashboard (lowest order number) with only the item/document list, no additional widgets.
- You can only have one Cluster Visualization widget on a dashboard.
- You can create dashboards on other objects.
- Dashboards can be created in your template, so they carry over to your new workspaces. However, some dashboards, such as those with search term report widgets or cluster visualization, will need to be created in the individual workspace once you've created your clusters and/or STRs.

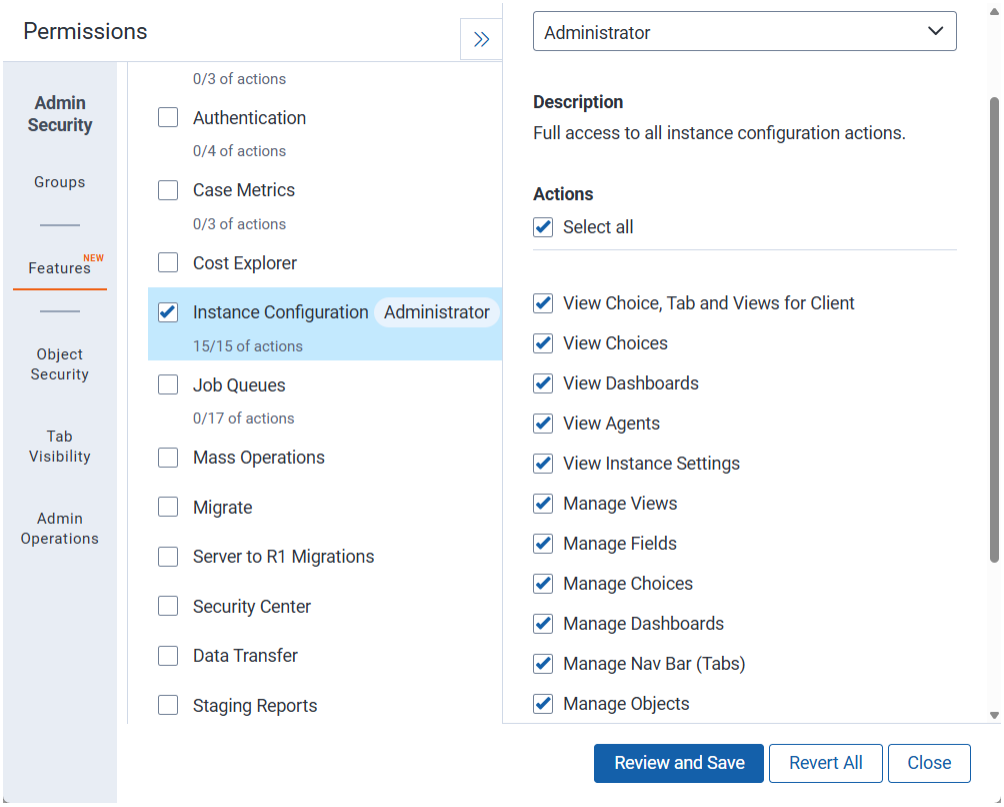
9 Fields

Fields store object information, document metadata, and coding choices within Relativity. You can use fields to display metadata on views and layouts. You can also use fields to create associations between different objects in Relativity.

9.1 Fields permissions

Manage permissions for this feature on the Features tab. Grant the full feature for a group, or customize access with individual actions. For an overview of features and actions, see Feature permissions.

Fields permissions are located within the Instance Configuration Feature permission, on the instance-level Features tab:



Granular permissions
The following granular permissions are designated for use of fields:

Object Security	Tab Visibility	Other Settings
• **Field** - View, Edit, Delete, Add • **Relativity Application** - View	• **Workspace Admin** • Fields	None

9.2 System fields

All Relativity workspaces contain the following system fields:

- **Artifact ID**—uniquely identifies all database objects in Relativity.
- **Batch, Batch::Assigned to, Batch::Batch Set, Batch::Status**—stores values related to any document batches.
- **Document Compare**—displays the Document Compare  icon. Use Document Compare to compare the extracted text of one document to another.

  Note: Document Compare is particularly useful when working with groups of near duplicates or conceptually similar documents.
- **Control Number**—the workspace identifier. You can rename this field.
- **Extracted Text**—stores any full text or OCR text loaded into Relativity. It is available for searching and as a radio button in the Viewer.
- **FileIcon**—an icon representing the document's Relativity Native File Type.
- **Folder Name**—the name of the folder where the document resides.

  Note: This is just the location folder, not the full folder path.
- **Has Images**—a single choice field indicating whether a document has images.
- **Has Natives**—a yes/no field indicating whether a document has natives.
- **Has Inline Tags**—a yes/no field indicating whether a document has a right-click tag markup.
- **Relativity Image Count**—the number of non-production images associated with a document.
- **Relativity Native Time Zone Offset**—This field adjusts how header dates and times appear in the Native Viewer for emails. If the field is blank or set to 0, the Viewer displays dates and times in Coordinated Universal Time (UTC).
  - When Relativity processes documents, it populates this field with the UTC offset of the time zone selected in the Processing profile. If applicable, it also includes the Daylight Saving Time (DST) adjustment.
    - For example, documents processed in Central Standard Time (CST) receive a value of -6.00 (UTC-6).
    - Documents processed in Central Daylight Time (CDT) receive a value of -5.00 (UTC-5).
  - You can manually update this field with a whole or fractional number—positive or negative—to offset the time from UTC to the desired time zone.
    - For example, to display UTC-processed documents in India Standard Time (IST), enter 5.50 because IST is UTC+5:30.
    - You can also mass edit this field

- This field only affects how header dates and times appear for email messages in the Viewer. It does not apply to images or extracted text, and it does not modify the actual metadata fields.
- If Relativity did not process the documents, the system calculates the time zone offset based on available metadata in the following order:
  1. **EmailSentOn**
  2. **EmailReceivedOn**
  3. **LastModified**
     If none of these fields exist, the Relativity Native Time Zone Offset field remains empty.

  Note: Relativity does not automatically account for DST adjustments for data processed outside of Relativity. To apply DST, use the Set Native Timezone Offset with DST script. Only Relativity administrators can deploy this script. For more information, see Set native time zone offset with DST .

- Relativity Native Time Zone Offset can be used with Basic Imaging and the Native Viewer.

  Note: The Native Time Zone Offset field and the Time Zone field serve different purposes. Make sure the correct field is populated for your imaging method.

- **Relativity Native Type**—the type of native file loaded into the system. The system assigns this value.
- **Supported by Viewer**—a yes/no field indicating whether the viewer supports the native document.
- **System Last Modified On**—the date and time at which the document was last modified.
- **System Last Modified By**—identifies the user who last modified the document.
- **System Created On**—the date and time when the document was created.
- **System Created By**—identifies the user who created the document.
- **<Markup Set Name>**—created when a user creates a markup set. Its values are:
  - Blank when the document has no highlighting or redactions for the markup set
  - **Has Redactions** when the document has redactions for the markup set.
  - **Has Highlights** when the document has highlights for the markup set.

  Note: If a highlight or redaction is created using a third-party application or script, this field may not automatically update.

- **<Production Name>**—created when a user creates a production. This field stores how the document was added to a production. It is either blank, contains Images Only, Natives Only, or Images and Natives.
- **Production Alerts**—a yes/no field to warn of any production execution problems

Note: You cannot edit the Source value for processing fields that are system mapped. For a list of processing system fields, see the Processing User Guide.

9.3 Creating and editing fields

To create a new field or edit an existing one:

1. Navigate to the **Fields** tab in your workspace.
2. Click **New Field**. To edit a field, click the **Edit** next to the field's name.

   Note: You can add an Edit link to your field list view if it does not already exist.

3. Input and modify field information on the field details page. If you are creating a new field, the Field Information section must be completed before the remaining sections will display. See Fields below.

   Note: You can not change a field's type after creating the field. See Field types on page 210.

4. Click **Save** to save the field details.
   If a field takes longer than ten seconds to be created, a modal appears with an option to cancel the field creation. This option can be used to limit performance issues in a very large workspace.

   Note: We recommend avoiding sensitive data in field names. Do not embed personal identifiers in field names (for example, use **QA Review** instead of **John Smith Review**).

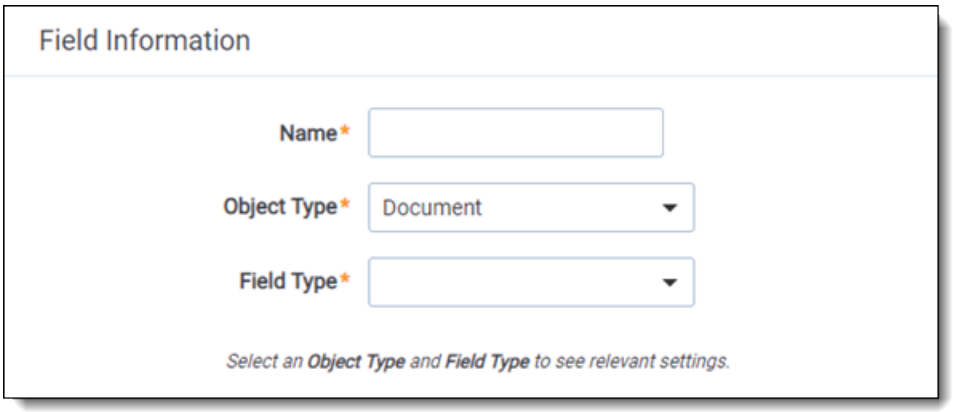
9.4 Fields

The fields object includes the following field sections:

- Field information
- Field settings
- Advanced settings
- List and dashboard settings
- Choices

9.4.1 Field information

Each field in the Field Information section must be completed before the fields in the remaining sections will display. The options you select in this section will determine what fields display in the Field Settings and Advanced Settings sections.

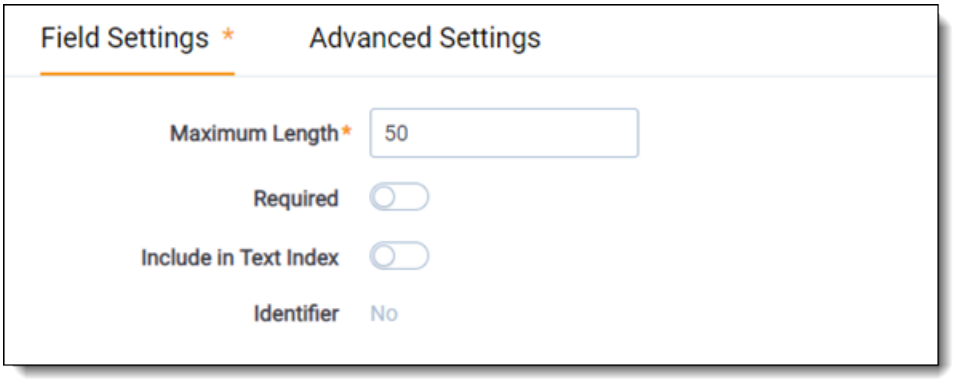


- **Name**—the field's name. This must be between 1-50 characters.
- **Object Type**—determines which object Relativity uses to classify the field.
  - You create object types in the Object Type tab.
  - If you are not sure which Object Type to select, ask "What object do I want to add information to?" The answer is your object type. For example, if you want your new field to store information about a document, select Document.

    Note: You can create new objects within Relativity. These dynamic objects are securable, non-document objects within your workspace. By connecting objects to each other you can create powerful custom applications within your workspace.
- **Field Type**—determines the field's functionality and presentation. For example, a Yes/No field type indicates that the reviewer must choose a value of either yes or no to edit the field.
- **Associative Object Type**—an object that the single object or multiple object field type uses to create a relationship. The objects selected in the Object Type and Field Type options determine the available associative object types.

9.4.2 Field settings

The fields in this section depend upon which options you selected in the Field Information section. You may see any of the following options in this section:



- **Available in Field Tree**—places the field and its choices in the Field Tree browser.
  - This field defaults to no.
  - This field is only editable for Document object type fields. The field type must be one of the following: single choice, multiple choice, single object, or multiple object.
- **Available in Viewer**—displays the field in the viewer. The user can then check text against the original document or image. This setting is only editable for long text fields with a Document object type. If set to Yes, the field is available in a drop-down menu on the Extracted Text setting in the viewer.

  Note: Copies of reflected fields are not available in this drop-down menu. If you select an empty long text field in the viewer, the viewer displays a blank page.
- **Default Overlay Behavior**—defines how Relativity handles multiple choice or multiple object fields when importing a load file.
  - **Merge Values**—merges previous values with load file values.
  - **Replace Values**—removes previous values and replaces them with the values in the load file.

  This field defaults to Merge Values and is only available for multiple choice and multiple object fields.

- **Formatting**—determines the field's format and only applies to the following fields:
  - **Date**—displays only the date.
  - **Date+Time**—displays the date and time.
  - **Use Thousands Separator**—if enabled, a comma displays between digits where appropriate for decimal and whole numbers fields.
  - **Whole Number**—none displays the value as a string of numbers. Integer displays the value with commas separating each group of three digits.
- **Identifier**—indicates if the field is the workspace's unique identifier with a value of yes or no. You are unable to edit this field.

  Note: Relativity does not enforce uniqueness.
- **Include in Text Index**—adds the field values to the workspace's SQL text index, making the field searchable via keyword search.
- **Maximum Length**—the value entered is the maximum number of characters permitted in the field. The value is set to 50 by default.
- **"No" Display Value**—determines how a "no" value displays in a list. No is the default value but you may edit it as desired.
- **Required**—determines whether the user must populate the field on a layout with information in order to continue coding documents. This does not apply when loading workspace data. Fields that are required on a coding layout display with a star next to them.
- **Storage**—determines how long text field data is stored. The available options are **Data Grid**, or **SQL**.
  - **Data Grid**— the optimized storage layer for long text fields. Data Grid enables greater workspace scale and stability.

    For workspaces created after April 13, 2026, and ARM restores performed after April 16, 2026, Extracted Text and OCR Text fields are automatically stored in Data Grid. Processing and OCR jobs in these workspaces can only target Data Grid–enabled fields for Extracted Text and OCR Text.
  - **SQL**— SQL storage can be used for dynamic text fields (such as the Notes field) or for fields that need sorting, filtering, or pivot functionality.

    SQL is not available as a storage option for Extracted Text or OCR Text fields in workspaces created after April 13, 2026, or in workspaces restored via ARM after April 16, 2026.

    Note: When storing in Data Grid, users will not be able to use bulk operations, filter on document pages, pivot and sort, or utilize fields in layouts (including on the document panel). For more information about storage in Data Grid, please see Processing to Data Grid

    Caution: If you have existing long text fields stored in SQL in workspaces created before April 13, 2026, you can use the Data Grid Text Migration Application to migrate those fields from SQL to Data Grid. For more information, see Data Grid Text Migration application.

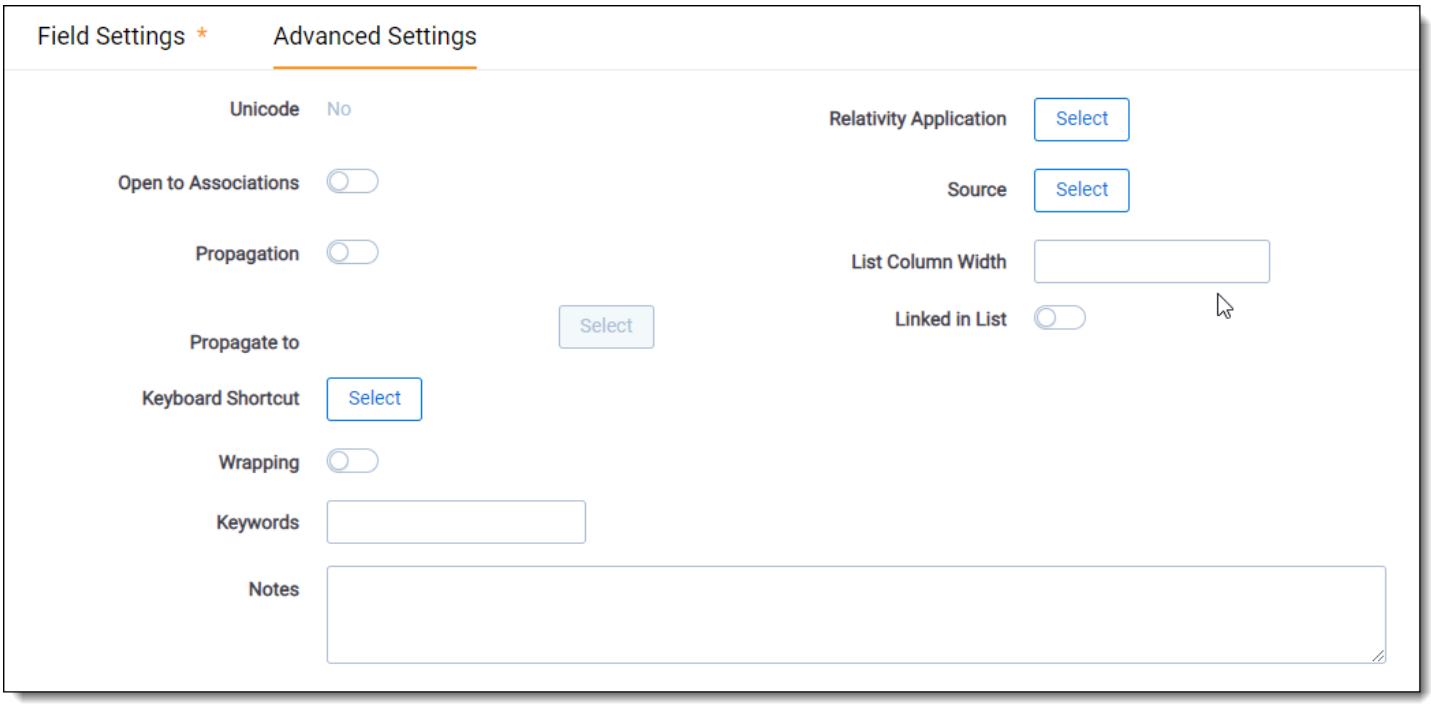
Note: Once you enable a field for Data Grid, you cannot disable it. The option to edit the field is unavailable after you save.



- **"Yes" Display Value**—determines how a "yes" value displays in a list. Yes is the default value but you may edit it as desired.

9.4.3 Advanced settings

The fields in this section depend upon which options were selected in the Field Information section. You may see any of the following options in this section:



- **Auto Add Choices**—adds all choices associated with a single or multiple choice field to an application. This property only applies to single and multiple choice fields.

  Note: If you are changing this property from No to Yes and you did not add the field to applications in your workspace, the choices are not added until you re-add the field to each application. The **Relativity Applications** property in this section lists each application to which this field is currently assigned.

- **Enable HTML**—indicates whether or not to allow HTML code to execute within the field.
  - **Enabled**—executes the code when the layout displays the field.
  - **Disabled**—displays the field as plain text.

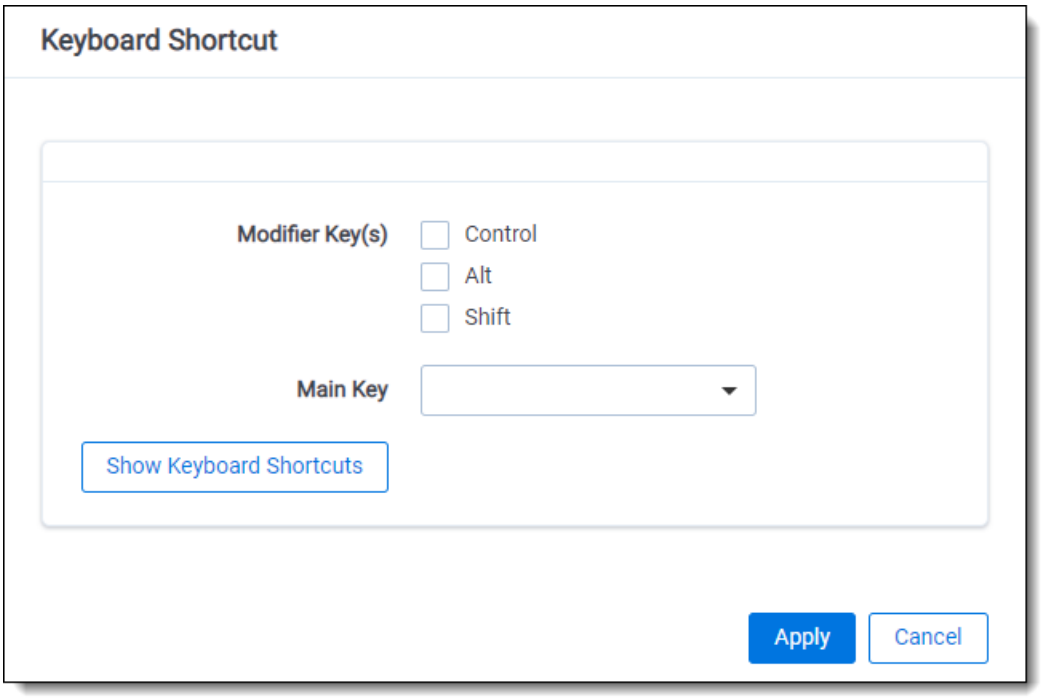
  Notes: Using allow HTML, you can configure Relativity to throw an alert when the field appears in a layout. HTML will always display as plain text in a view. The AllowHTMLVisible instance settings table value controls whether or not the Allow HTML value displays on the Field page.

- **Field Tree View**—determines the values and the order they appear in the field tree. It also determines the views that appear in the pickers when you set conditions for searches and views. To select a view, the field must be single object or multiple object.
  - When Available in Field Tree is No, this property is disabled. When Available in Field Tree is Yes, this property reflects the default value of <All Items>.
  - When you select a view for Field Tree View, Relativity respects the sort order of that view. If you do not define a sort order, it sorts by Artifact ID.
  - If you choose search terms reports as the associated object type and you are adding the field to the Field Tree View, only search term report items with a status of Completed appear in the field tree.

  Note: For Field Tree View, you can select any view you have rights to see. However, a warning appears when you attempt to save the field, if the selected view is personal. If you edit the view selected as the Field Tree View, you receive a warning when you attempt to save it as a personal view.

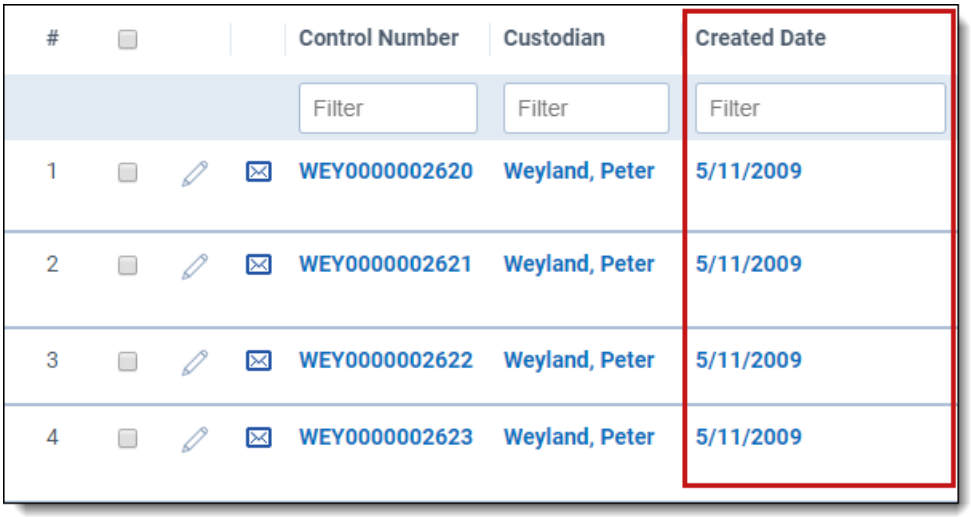
  The Field Tree View property includes two icons:
  -  edits the view by opening Conditions, step 3 of 4, in the view wizard.
  -  creates a new view from Basic Information, step 1 of 4, of the view wizard.
- **Field Type**—the type of the catalog field to which you are mapping. This must match the type of the field you are creating or editing.
- **Keyboard Shortcut**—you can define a keyboard shortcut for the document field you are editing or creating with keyboard shortcuts. You can then use this shortcut to code and edit documents in the Review Interface. This setting is available only for document fields.
  You can use the following key options to define the shortcut trigger. You must use Ctrl, Alt, and/or Shift, and the workspace cannot have duplicate keyboard shortcuts.
  - **Modifier Keys**—check the desired key option to define the shortcut trigger. You must use Ctrl, Alt, and/or Shift. The workspace cannot have duplicate keyboard shortcuts.
  - **Main Keys**—click on the drop list and click on the desired key to use in combination with the other specified keys.

- **Show Keyboard Shortcuts**—click to view a list of the current keyboard shortcuts.



Note: You can modify the key combinations for system keyboard shortcuts if you have the Modify System Keyboard Shortcuts security permission.

- **Keywords**—allows you to enter words that describe the field you are creating. There is a 50 character limit.
- **Length**—the length of a fixed-length text field.
  - Defaults to 255 characters.
  - Maximum length is 4,999 characters.
  - Maximum length is 4,000 if Unicode enabled.
- **Linked in List**—sets the field as a hyperlink. In the example below, the Date Sent field was set to Linked: Yes. As a result, Created Date appears as a hyperlink in the view. Clicking the date launches the related document in the viewer. Similarly, clicking any link in the document record also launches the document in the viewer.



Note: When you create a Yes or No field, set the width to 30 pixels for the optimum column size.

- **List Column Width**—the width, in pixels, of the column in the view. To accept Relativity's default, leave this field blank.
- **Notes**—allows you to enter words that describe the field you are creating. There is not a character limit.
- **Open to Associations**—determines whether an object field can display its information on an associated object field. Fields that are open to association are sometimes referred to as *reflected* fields. Reflected fields can be re-named and exported via the Export to File mass action.
    - When you open a field to association, that field's information is viewable and editable on an associative list found on the object with which you associate it.
    - For example, you have two associated objects: Entity and Company. You want to add a field called Address to hold addresses on the Company object and to display addresses on an Entity. To do this, create a new field with an object type of Company and set the Open to Associations field to Yes. This creates two fields: a Company object field called Address and a Company::Address field on the Entity object. If the generated reflected field name exceeds the maximum length of 100 characters, it is handled as follows:
        - Each field is allocated 50 characters, anything over that 50 character limit is truncated.
        - The field's ArtifactID is appended to the field's name part.
        - Additional space is truncated to allow room for the field's ArtifactID to become part of the new name.
        - The two field name parts are joined with "::", for example: "AAAAAAAAA BBBBBBBBB CCCCCCCCC DDDDDDDDD EEEEEEE (1000012)::GGGGGGGGG HHHHHHHHH IIIIIIIII JJJJJJJJJ KKKKKKK (1000013)".
- **Propagation**—forces a coding value to a specified group of related items. This value must be set to **Yes** before you can propagate to a related item.
- **Propagate To**—click the **Select** button to access the propagation options. The available options depend on the relational fields set for the workspace. Check the desired related items and click  to move the selected items to the right. Click **Apply**.
- **Relational**—you can make a fixed-length text field relational. A relational field is used to identify a group of related documents, such as families, duplicates, or near duplicates. For example, MD5 Hash is commonly used to identify duplicates. If set to Yes, identifies the field as relational. Once set to Yes, the Friendly Name, Import Behavior, and Order fields become required in order to save the field.

Note: You can only set relational field properties on fixed-length text fields that don't exceed 450 characters.

- **Relational Properties**—click the **Select** button to access the following relational options:
    - **Friendly Name**—a label for the relational field that users can easily understand. For example, you could change the relational MD5 Hash field to Duplicates, since it is used to group copies of the same document. This name displays in the Include Related Documents menu in workspaces and in the Related Items pane.
    - **Import Behavior**—controls how blank values are handled when importing through the Import/Export. Depending on how your vendor processes these group identifiers, the relational field on the parent document may be blank. Select an option to determine how blank fields are imported:

- **Leave blank values unchanged**—Relativity imports the fields with blank values.
- **Replace blank values with identifier**—Relativity updates the blank relational field with the document identifier.

  Note: When you append documents through Import/Export, with a relational field's Import Behavior set to **Replace blank values with identifier**, blank values are replaced on that relational field even if it is not mapped to a load file field. The same action occurs when you import blank values mapped to the relational value using an overlay.

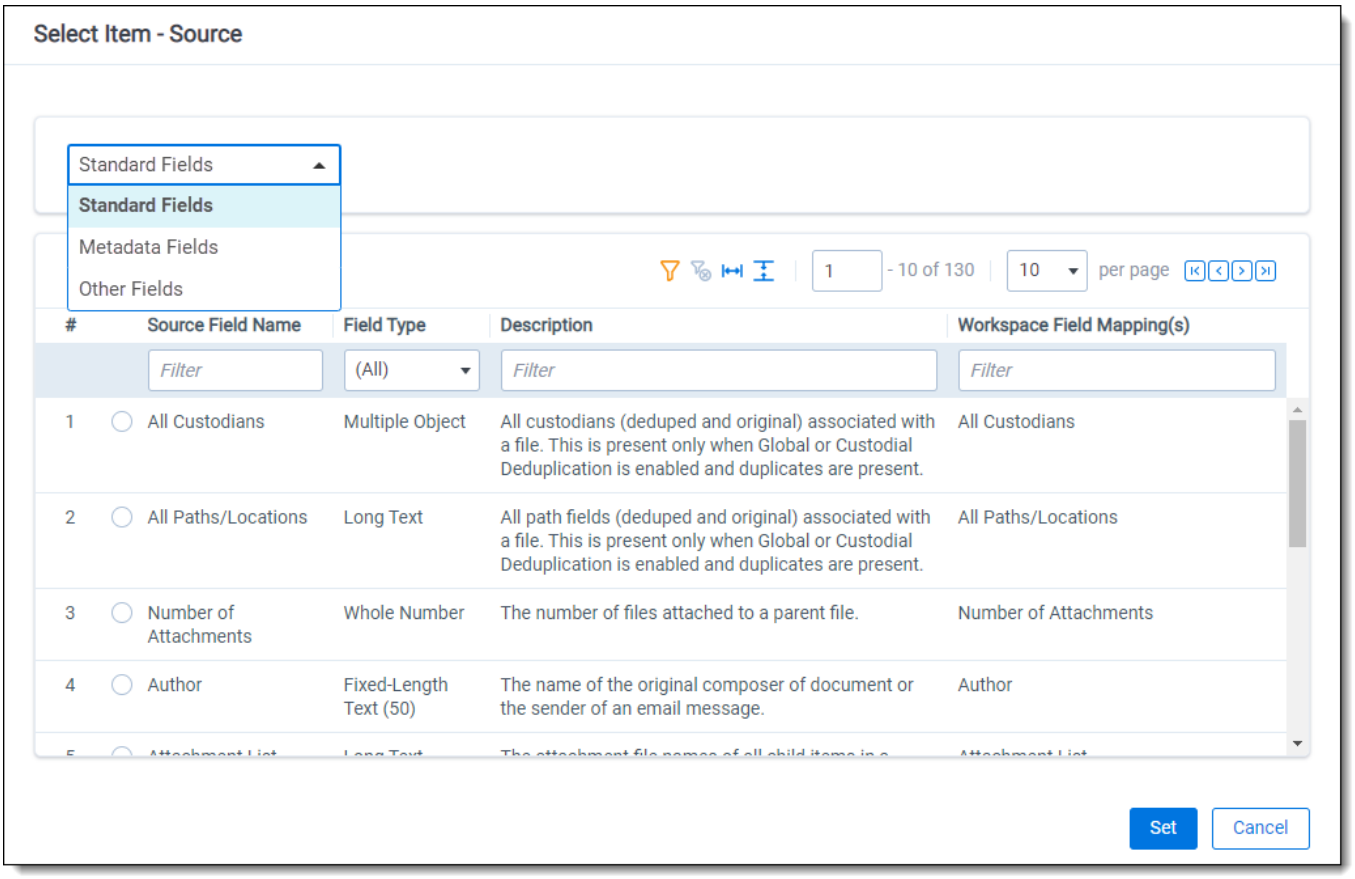
- **Pane Icon**—select and upload an icon for display in the Related Items pane of the Review Interface. Users can click on the icon to display a list of items grouped by this relational field. You can download the Relativity-provided Relational Field Icons.zip, or you can upload a custom icon. Icons shouldn't exceed 16 x 16 pixels.
- **Order**—controls the pane icon order on the bottom of the Related Items pane. Use the following guidelines:
  - Icons with low order numbers appear to the left.
  - Icons with the same order number are sorted alphanumerically.
  - The order number can be any positive or negative integer. We recommend using groups of 10, such as 10, 20, and 30, so you can easily insert a new icon without having to reorder existing ones. You can use the **View Order** button to see how icons are currently ordered in the Related Items pane. The Order Reference window displays the leftmost icon at the top of the list.
- **Relational View**—controls the view that appears in the Related Items pane. Shared values in this field determine the documents the view displays. This field contains  and  icons you can use to edit the selected view or create a new view.

  Note: You cannot select a view that contains conditions or add/edit conditions to a view referenced by a relational field. You also cannot make a relational view personal. This view will control the fields displayed and sort order.

- **Relativity Applications**—associates the field with a Relativity application. Click the **Select** button to select an existing application. Check the desired applications and click  to move the selected items to the right. Click **Apply**.
  This option is only available for those who have the Manage Relativity Applications permission.

  Note: Locked applications don't appear in the selection menu. To make an application available, unlock it first.

- **Source**—the list of fields that you can use when mapping processing fields. Click the **Select** button to access the available field sources, which contain the following options:
  - **Standard Fields**—contains a collection of fields from both the Metadata Fields and Other Fields options.
  - **Metadata Fields**—contains fields extracted from the actual file or file system.
  - **Other Fields**—contains static, or system fields such as control number, processing set name, custodian, and so forth.



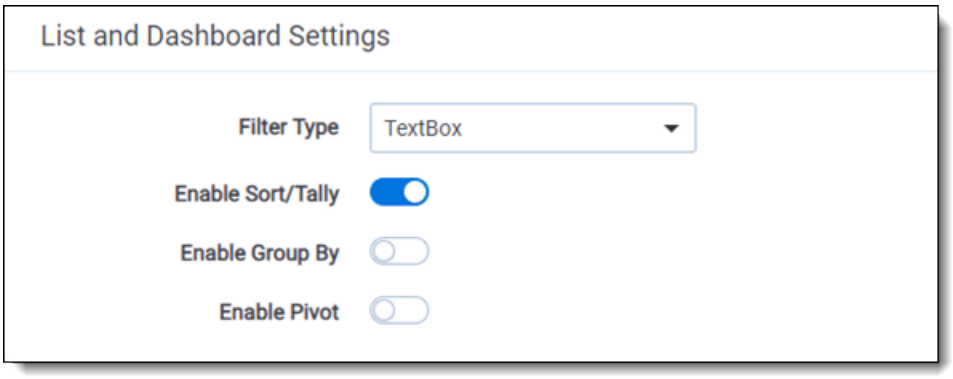
- **Source Field Name**—the name of the catalog field to which you are mapping the field you are creating or editing.
- **Field Type**—displays the category of each field.
- **Description**—the description of the catalog field.
- **Workspace Field Mapping(s)**—the name of the Relativity field to which the catalog field is mapped. This is blank if the field has not yet been mapped. Note the following about the field catalog:
  - If you want to display every field available for mapping, switch to the All Fields view from the Field Catalog view. All fields are accessible in the All Fields view, but the Field Catalog only provides the processing-related fields.
  - The Source field is disabled if you do not select Document as the Object Type.
  - The Source field is disabled for processing fields that are system-mapped, meaning processing system fields that were automatically mapped when you installed or upgraded the Processing application.
  - For more information on using the field catalog to map processing fields, see the Processing User Guide.

- **Unicode**—special characters are permitted. This option must be enabled before you can load any Unicode data into the field. We recommend keeping this option enabled.

Note: If Unicode data is loaded into a non-Unicode enabled field, then the data becomes unreadable.

- **Wrapping**—toggles text wrapping for the field.
  - **Enabled**—wraps all of a field's text, displaying the contents on multiple lines.
  - **Disabled**—the field extends as far right as necessary within the screen to display the text.

9.4.4 List and Dashboard Settings



- **Filter Type**—determines type of filter available for the field.

  Note: When using the new UI framework, Filter Type is not used except for the following scenarios: disabling filtering on the field by selecting None, selecting List filters for Fixed Length fields, or selecting a custom pop-up picker view for a multiple and single object fields.

  - **None**—disables filtering on the field.
  - **List**—displays a drop-down list of all the field's values in the workspace. Users can select only one of the values.

    Notes:
    - Fields that contain a large number of items may also cause the List filter to take longer to populate. We recommend you only select the List filter type for Single Choice and Yes/No fields. For fields that may contain a large number of choices, you can designate a pop-up filter instead.
    - **Fixed Length Text fields**—if the field contains more than 255 items, the List filter type you specify for the field will revert to the text box filter type and an error will be written to the Error Log when you visit a Document list view containing the field.
    - **Single Choice / Single Object fields**—if the field contains more than 255 items, the List filter type you specify for the field will revert to None (disabled) and an error will be written to the Error Log when you visit a Document list view containing the field.
  - **TextBox**—displays a text box that a user can query for text. You can use search operators in the filter box. See Filters in the Searching guide.
  - **Multi-list**—displays a list for a user to select one or more fields to filter.
  - **Boolean**—displays Boolean choices for the field. Users can select one option.
  - **CustomOnly** (Advanced)—searches with multiple search terms and operators. When you use this filter in a view, the operators that display are dependent upon the field type. The CustomOnly filter type is available for the following field types:

- Fixed Length
- Long Text
- Decimal
- Whole Number
- Currency
- Date

- For more information on how the CustomOnly filter works, see Filters in the Searching guide.
- **Popup**—displays a pop-up picker where you can select values to use while filtering a list, or modifying criteria in a saved search or view.
- You can access these pop-up pickers from layouts, field filters through a **Select...** button, view conditions, advanced search conditions, and the mass edit window. You can access this picker via the check and uncheck buttons next to the field name. For more information, see Mass edit on page 358.
- In the pop-up picker view drop-down field, you can select any view you have rights to see. However, a warning appears when you attempt to save the field, if the selected view is personal. If you edit the view selected as the Field Tree View, you receive a warning when you attempt to save it as a personal view.

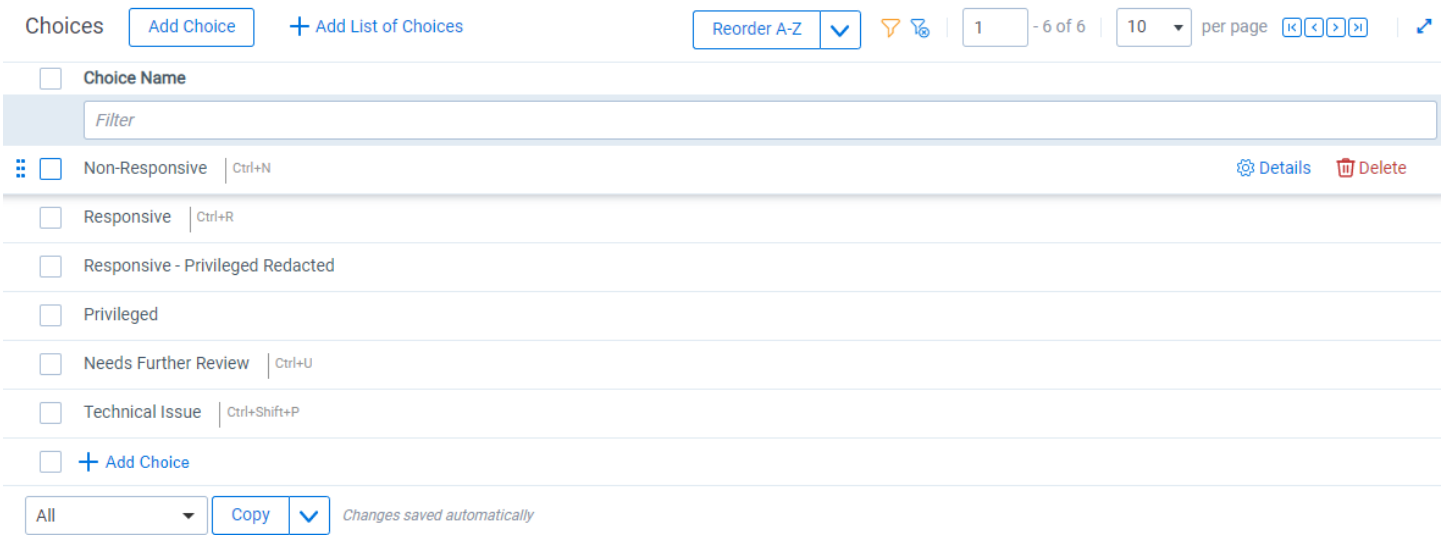
Depending on the type of field you're creating, only certain filters are available.

Filter	Field types
List	Fixed-length text, single choice, single object, user
TextBox	Fixed-length text, long text, date, whole number, decimal, currency, object
Multi-list	Single choice, multiple choice, multiple object
Boolean	Yes/No
Custom Only	Fixed-length text, date, whole number, decimal, and currency
Popup	Single object, multiple object, single choice, and multiple choice

- **Enable Sort/Tally**—if enabled, sorts document lists based on the field.
- **Enable Group By**—if enabled, makes the field available to group by when using Pivot. Relativity does not support Pivot On for Long Text fields due to the performance impact.
- **Enable Pivot**—if enabled, makes the field available to pivot on. Relativity does not support Pivot On for Long Text fields due to the performance impact.

9.4.5 Choices

The Choices section contains the Choice editor, which you can use to add and edit choices for a single or multiple choice field.



9.5 Field types

Relativity supports the following field types:

- Fixed-length text
- Long text
- Date
- Whole number
- Decimal
- Currency
- Yes/No
- Single choice
- Multiple choice
- User
- File
- Single object
- Multiple object

9.5.1 Fixed-length text

The fixed-length text field type is a text field with a limited length. You can use up to 4,999 characters. Unicode-enabled fixed-length text fields cannot exceed 4,000 characters.

- The sum of all fixed-length text fields for any individual object should be no larger than 8,060 bytes. To see how many of your 8,060 bytes remain, go to object you are checking. The control panel section displays remaining bytes in the usage field.
- Examples: Email from, Email subject, Conversation, Document extension, File Name, Parent Document ID, Subject.

9.5.2 Long text

You can add more than 4,999 characters in a long text field.

- The technical limitation of a long text field is 2 GB. Relativity usually defaults to streaming only files smaller than 50 MB.
- Examples: Full text, Conversation ID, Email BCC, Email To, Source File, Title

9.5.3 Date

The date field type stores the date or date and time. Dates must be in a valid format. For example, 01/00/2000 is not valid. Attempting to load an invalid date produces an error.

- Relativity accepts many formats, including SQL-accepted formats that match your SQL Server's regional settings. However, the date displays as mm/dd/yyyy for the US or dd/mm/yyyy for the UK. When entering a date field, you can use the picker to choose from a calendar or enter a date directly in the field.
- Example: Email sent date, Date Created, Date Last Modified, Date Received, Date Sent.

Note: When you search on a user-created date field using a relative date, Last 7 Days for example, you may see different results between a saved search and a search from the search panel if you are not in the same timezone as your Relativity instance.

9.5.4 Whole number

The whole number field type stores any natural numbers or their negatives.

- This value cannot exceed 2,147,483,647. In other words, 2,147,483,64**8** and higher is invalid.
- Example: Page count, Number of Attachments.

9.5.5 Decimal

The decimal field type stores numeric values that may include decimals.

- With this field you can have a maximum of 15 digits before the decimal and two digits after the decimal.
- Example: Percentage, File Size.

9.5.6 Currency

The currency field type stores numeric values in a currency format. Ten digits is the maximum for this field.

- Your currency symbol is set based on Windows regional currency settings in the server hosting Relativity. The formatting, such as decimal, commas, negative number sign, the position of currency symbol, are based on the browser's language. When using Relativity aiR, the settings of the regional server cannot be changed. They are set to the US currency symbol.
- Example: Amount sold.

9.5.7 Yes/No

The Yes/No field type accepts one of two values. The default values are Yes and No.

- You can edit the display values in the Yes/No display values section. See Fields on page 199.
- Example: Reviewed.

Note:

- Use **Single Choice** fields rather than **Yes/No** fields when possible - creating Single Choice fields will not impact reviews and may improve search performance. Before doing so however, check to confirm whether your workflow can support Single Choice fields.
- If you are exporting a Yes/No field type with Import/Export or Integration Points, the values will display as True/False in the exported files.

Yes/No fields are useful, but consider the following caveat:

Searching for yes/no fields can be difficult, especially if the field displays as a checkbox. The check box only displays as checked or unchecked; however, a yes/no field has three potential values. These values include yes, no, or null. Because of the searching difficulties, you may want to display yes/no fields as drop-down menus.

9.5.8 Single choice

The single choice field type provides a predetermined set of values called choices.

- You can choose only one value.
- Example: Responsiveness, Custodian

9.5.9 Multiple choice

The multiple choice field type provides a predetermined set of values called choices.

- You can choose multiple choices. You can also nest the choices in a hierarchy structure.
- Example: Issues, Deponent

Note: If Overlay Behavior is set to Replace Values on this field, a warning message appears stating that on import that the current values for this field will be deleted and replaced with the values included in the load file. The Overlay Behavior setting must be set to Merge Values in order to merge the values from the load file with the field's current values.

9.5.10 User

The user field type contains users with rights to the current workspace. Depending on the function of the field, Relativity filters the list of users to display only members of certain groups.

Note: A user field with a **[removed]** tag signifies that the user wasn't assigned to any of the workspace groups.

9.5.11 File

With the file field you can upload files for a non-document object. You can click on the **Select** button to choose a file to upload or drag-and-drop the file onto this field to upload it. When you add a file field, Relativity automatically creates file size, file icon, and text fields for the object. Once you upload a file, you can click on Pop Out icon to open the file in the Viewer.

The text field contains the extracted text of all files uploaded to the file field. The Text Extraction Manager agent must be running in the Relativity environment to populate the text field.

Note: Relativity prohibits users from uploading certain file types to file fields. The RestrictedNativeFileTypes instance setting value defines the prohibited file types. To receive assistance with this instance setting, contact our Support team through the Support page.

Note: You can create only one File field per object type. File fields are not available on the Document object type.

9.5.12 Single object

The single object field type defines a one-to-many relationship between two objects. You add a single object field on the selected object under the Object Type option. You can then create a one-to-many relationship with the selected object using the **Associative Object Type** option.

For example, you could use a single object field called Sender Domain to create a relationship between email messages and the domains of their senders. You add the Sender Domain field to a Document object and associate it with a Domain object. By doing so, you used a single object field to create a one-to-many relationship, since each email message can originate from only one domain, but many different domain options are available.

9.5.13 Multiple object

The multiple object field type defines a many-to-many relationship between two objects. You add the Multiple Object field on the selected object under the Object Type option. You can then create a many-to-many relationship with the object selected in the **Associative Object Type** option.

For example, you could use a multiple object field called Recipient Domains to create a relationship between available domains and the email recipient domains from email messages.

Note: If Overlay Behavior is set to Replace Values on this field, you will be prompted with a warning message on import that the current values for this field will be deleted and replaced with the values included in the load file. The Overlay Behavior setting must be set to Merge Values in order to merge the values from the load file with the field's current values.

You add the Recipient Domains field on a Document object and associate it with a Domain object. By doing so:

- You used a multiple object field to create a many-to-many relationship, since you can have multiple domains, and each recipient of an email message can have a different domain.
- Relativity automatically creates two fields when you define Multiple Object field type. The first Recipient Domains field has a Document object type. The second Recipient Domains field represents the relationship between the Recipient Domains object type and the Domain associative object type.

  Note: The **Assigned to** field displays user information in the format "last name, first name." You must use the user's email address when loading this field in Relativity. For example, you would load a user named John Smith as johnsmith@example.com.

9.5.14 Fields and performance

Field configuration can dramatically impact database performance. Use the following guidelines to improve field efficiency:

- Set fixed-length text fields to the minimum size needed and to no more than 400 characters.
- Store choice data in single or multiple choice fields if possible.
- Use separate objects to store repetitive content when possible.
- Set up fields as Unicode in advance because the system will have to re-index a field if you make the change following data load.
- Only include fields in the text index when it is truly necessary to do so.

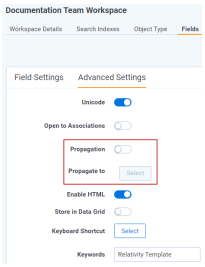
9.5.15 Linking Fields to Field Categories

Once a field has been created, you can link it to a field category to help you efficiently find that field and apply it when adding conditions in the search panel. To learn more about linking a field to a field category, visit Field categories.

9.6 Applying propagation to documents

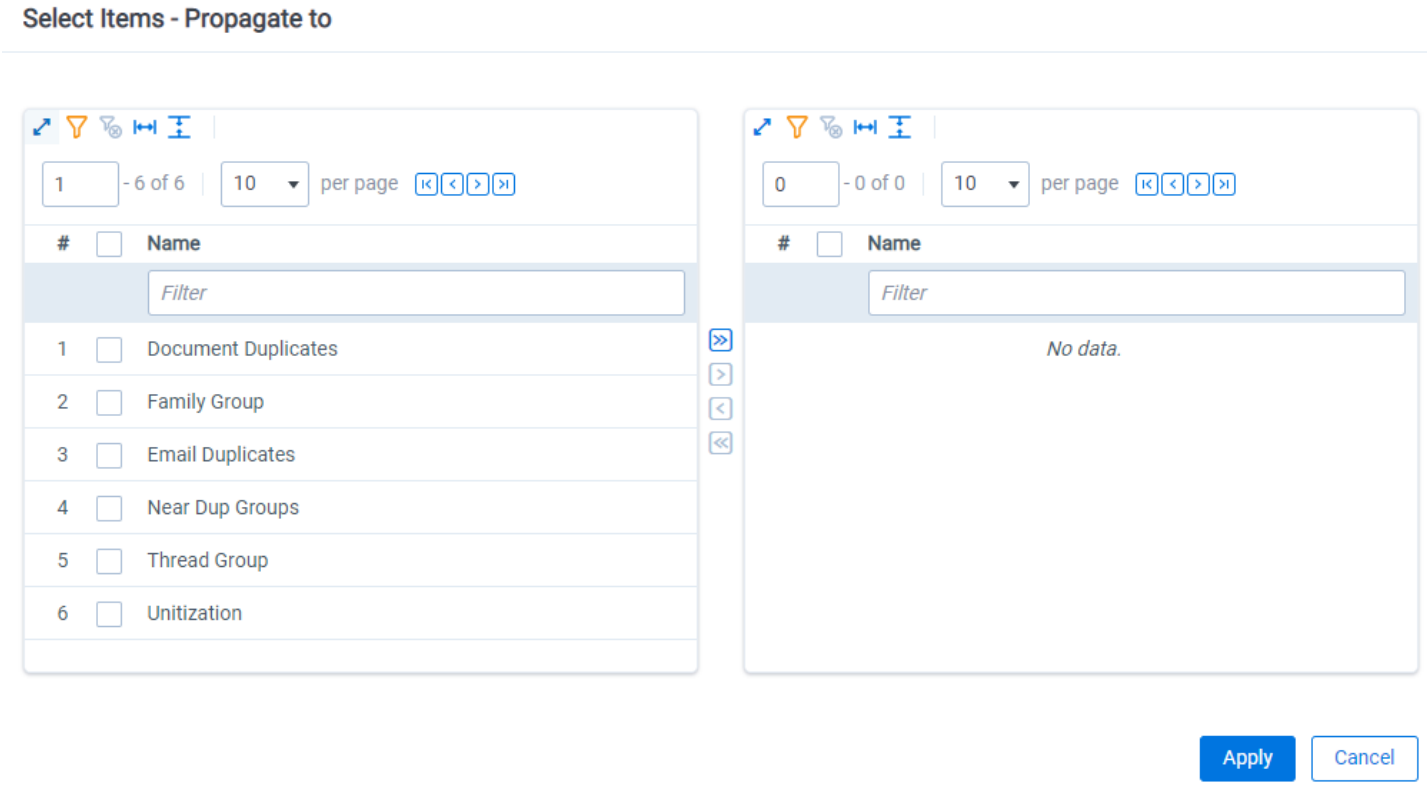
The propagation function can help enhance your document review workflow to save time spent coding documents. For example, you can tag a document as Responsive and have the value propagate to that document's family members.

To enable propagation, toggle **Propagation** on.



Click the  icon in the **Propagate To** row.

The available options depend on the relational fields set for the workspace.



When you code a document in a field on which propagation is enabled, the propagation function automatically codes related documents with the same value. Click **Save** or **Save & Next** in the layout to apply the field propagation rules.

Note: Propagation works on all document object field types. Associative Object Lists do not work with propagation.

Propagation doesn't cascade or cause chain reactions, meaning that only the documents in the saved document's groups receive the propagated values. For example, if you create a responsiveness field to propagate both family and duplicates, and you code a parent email as Responsive, these actions occur:

- **Family propagation** - codes child email attachments as responsive
- **Duplicate propagation** - codes duplicate emails of the parent as responsive

Duplicates of the child attachments aren't coded as responsive. This action would be a duplicate propagation triggered by family propagation.

9.6.1 Propagating to documents in multiple groups

When you code a document that's a member of multiple related groups – for example, Duplicates and Email Families – it's important to understand how coding decisions propagate in specific scenarios.

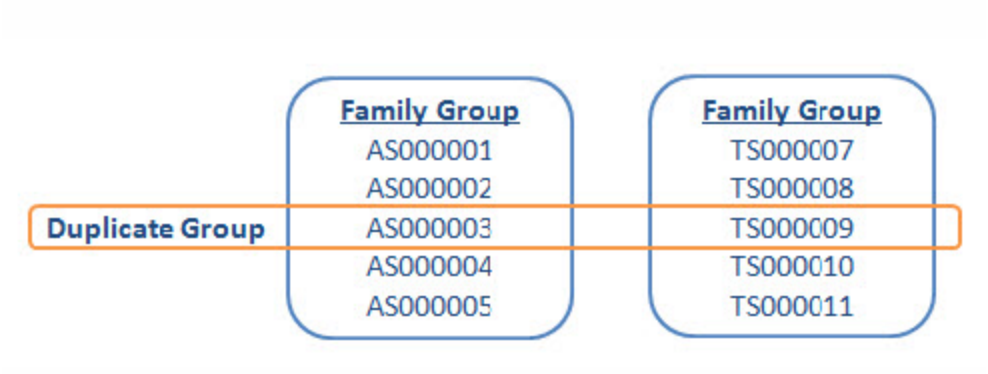
The following scenarios illustrate how propagation applies to a set of documents. Assume that propagation is active for both email families and duplicates.

There are two email families:

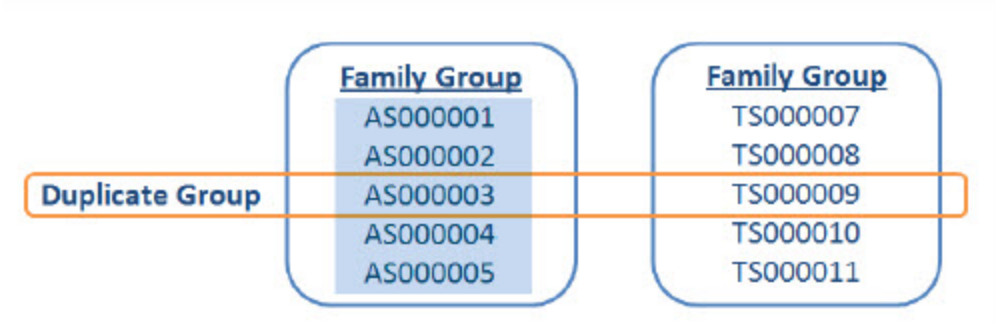
- AS000001 – AS000005
- TS000007 – TS000011

Within these families, two documents are duplicates:

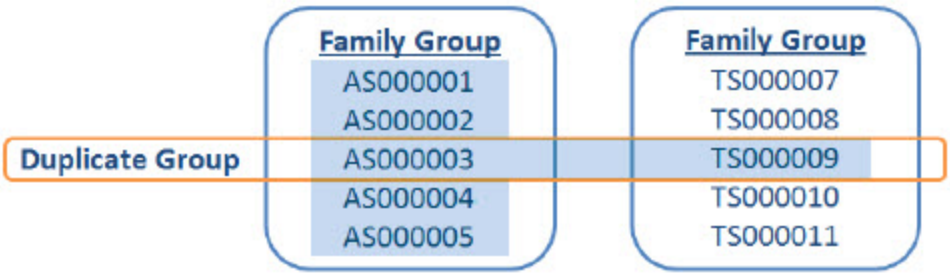
- AS000003
- TS000009



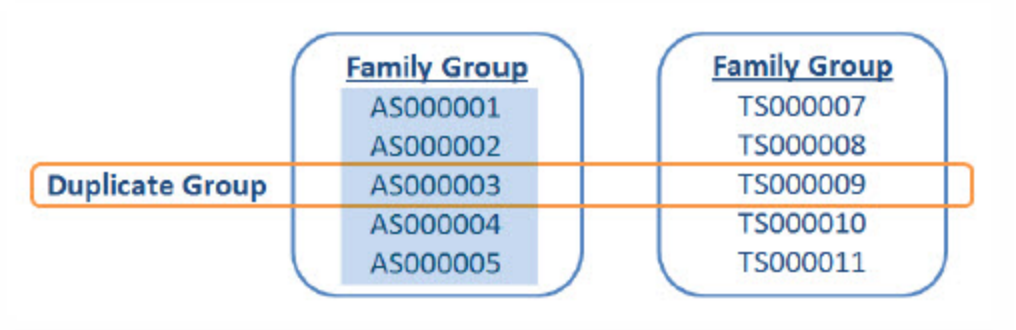
Coding **AS000001** as **Responsive** tags only the family, shown in blue.



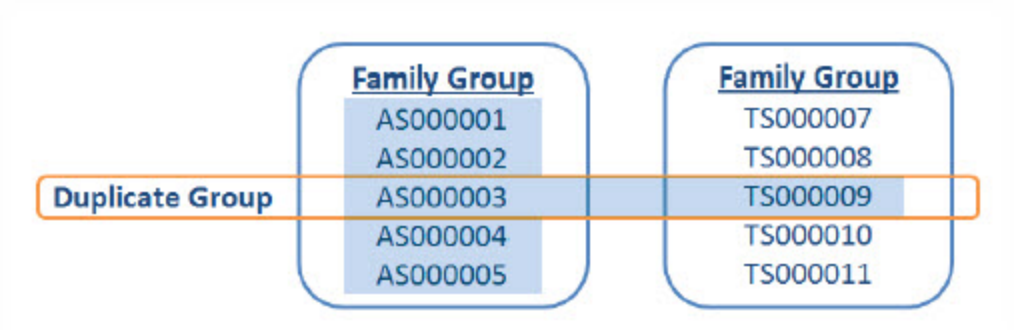
Coding **AS000003** as **Responsive** tags the family, and the duplicate, shown in blue.



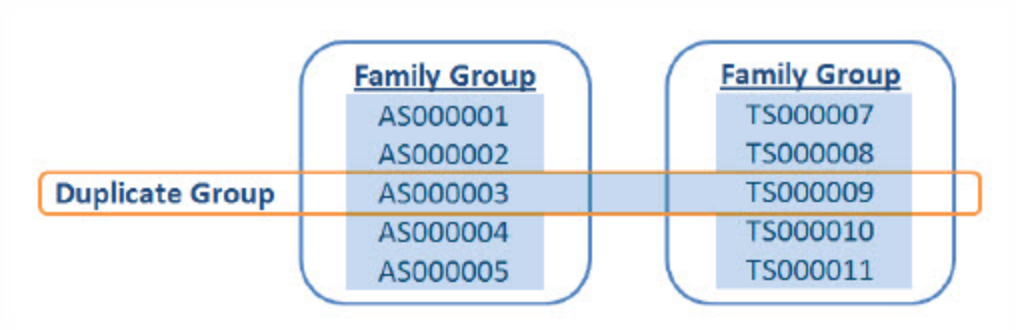
Mass editing **AS0000001** and **AS000002** as **Responsive** tags only the family, shown in blue.



Mass editing **AS000002** and **AS000003** as **Responsive** tags the family and the duplicate, shown in blue.



Mass editing **AS000003** and **TS000009** as **Responsive** tags all of the listed documents.



10 Field categories

Field categories allow you to quickly and accurately apply field conditions to the document list, a saved search, or a view. Once a field category has been created, it can be linked to as many fields as desired. The field category can then

be selected when adding fields or conditions in the search panel, a view, or a saved search to conveniently access and apply the linked fields.

All Fields is a system default field category that displays every non-secured field in your workspace. It cannot be edited or secured from other users and it will always display at the bottom of the Field Categories drop-list. All Fields allows you to conveniently switch between viewing all of the fields and the fields included in a particular field category.

Field categories have object permissions so that they can be created and limited to a specific group or workflow within in Relativity. Securing a field category only determines whether it is visible in the drop-list of field categories that can be selected when adding conditions in the search panel.

Note: Field categories that you create are carried over during workspace upgrades and when those cases are used as templates. The All Fields field category will also carry over after an upgrade, though it is currently a system default that cannot be configured by users.

10.1 Creating a field category

To create a new field category, do the following:

1. Navigate to the **Field Categories** tab.

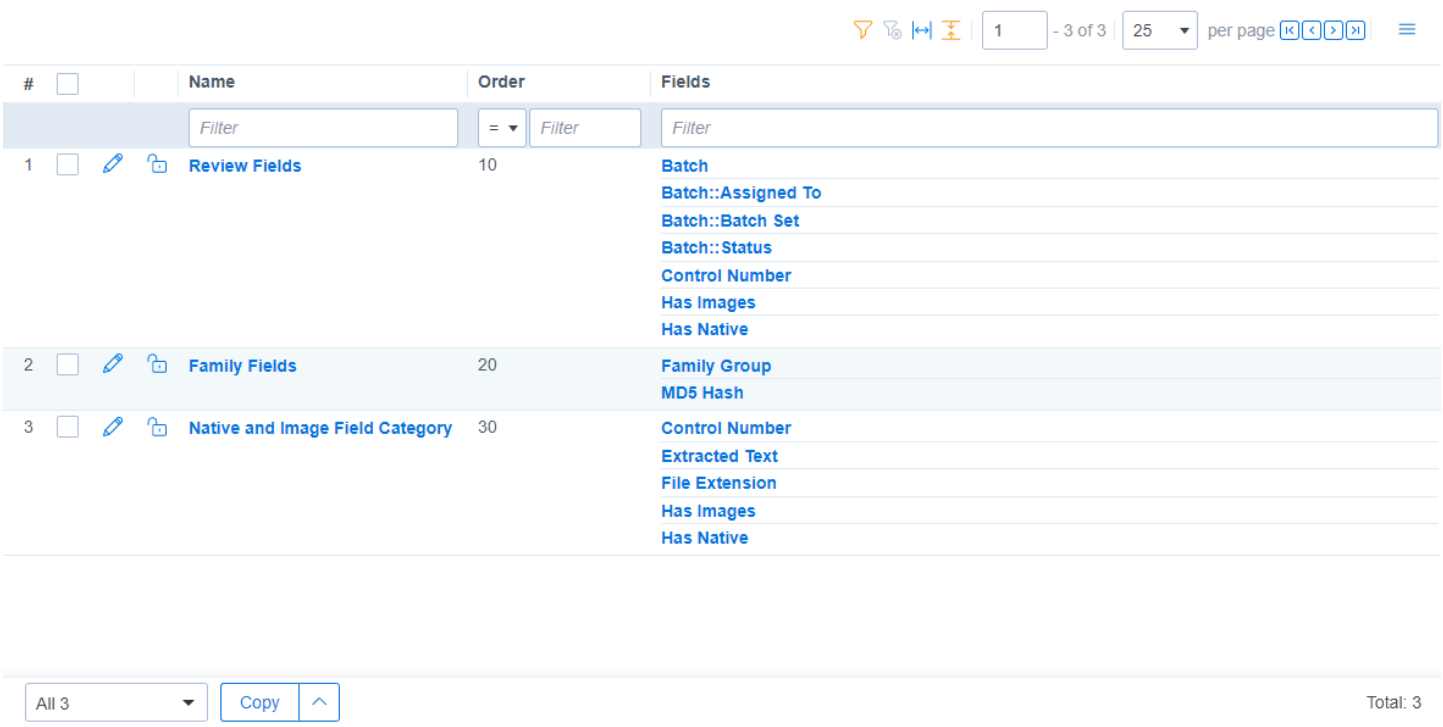
   Note: All Fields is a field category that is always present in Relativity but it does not display on the Field Categories tab since it cannot be edited.

2. Click **New Field Category**.
3. Enter the desired information for the following fields:
   - **Name** - the title of the field category
   - **Order** - determines where the field category appears within the view drop-down list. Items that share the same value are sorted in alphanumeric order.
     - Order can be any integer (positive or negative). No decimals are allowed. You can use the **View Order** button to see how items are currently ordered.

       Note: Ordering by 10's, starting with 10, then 20, then 30, etc. is recommended because you can insert an item into any position later in the workspace, without the need to reorder all items.
4. Click **Save** to create the new field category.

10.2 Viewing fields associated with a field category

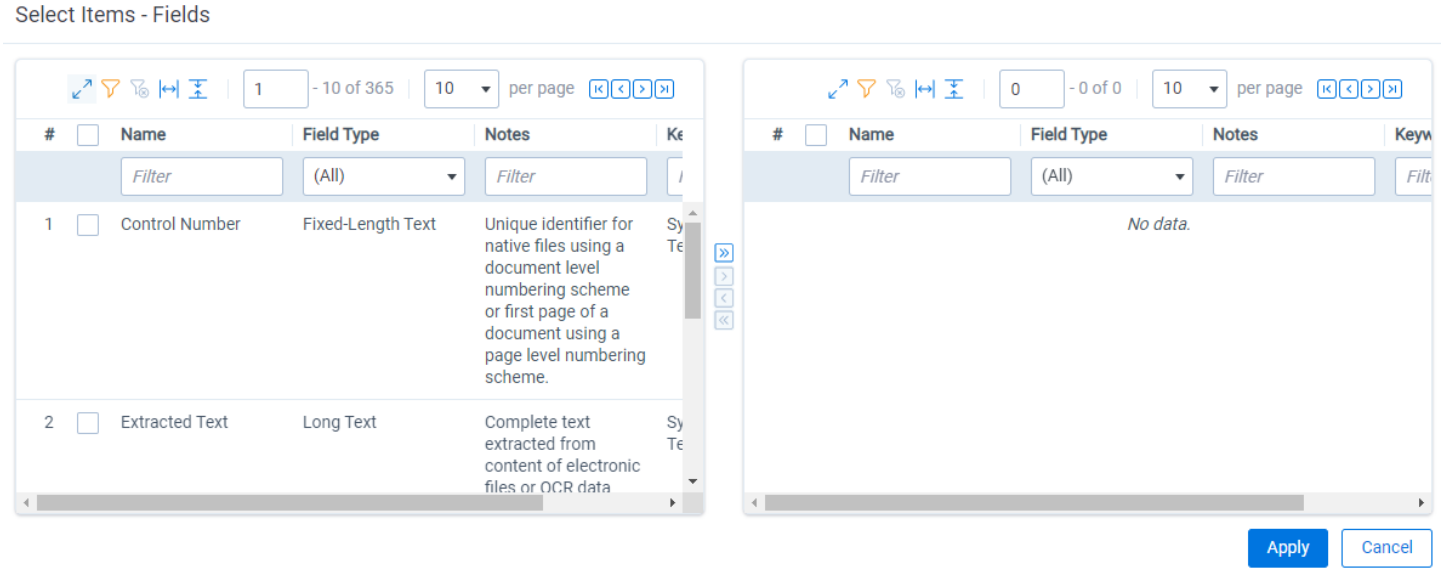
Before linking and unlinking fields to a field category, it can be helpful to see what fields are associated with each field category. To do this, add the Fields field to the desired field category view and select that view on the Field Categories tab.



10.3 Link a field or fields to a field category

To link a field or fields to a field category, do the following:

1. Navigate to the **Field Categories** tab.
2. Click on the desired field category in the list.
3. Click **Link**.



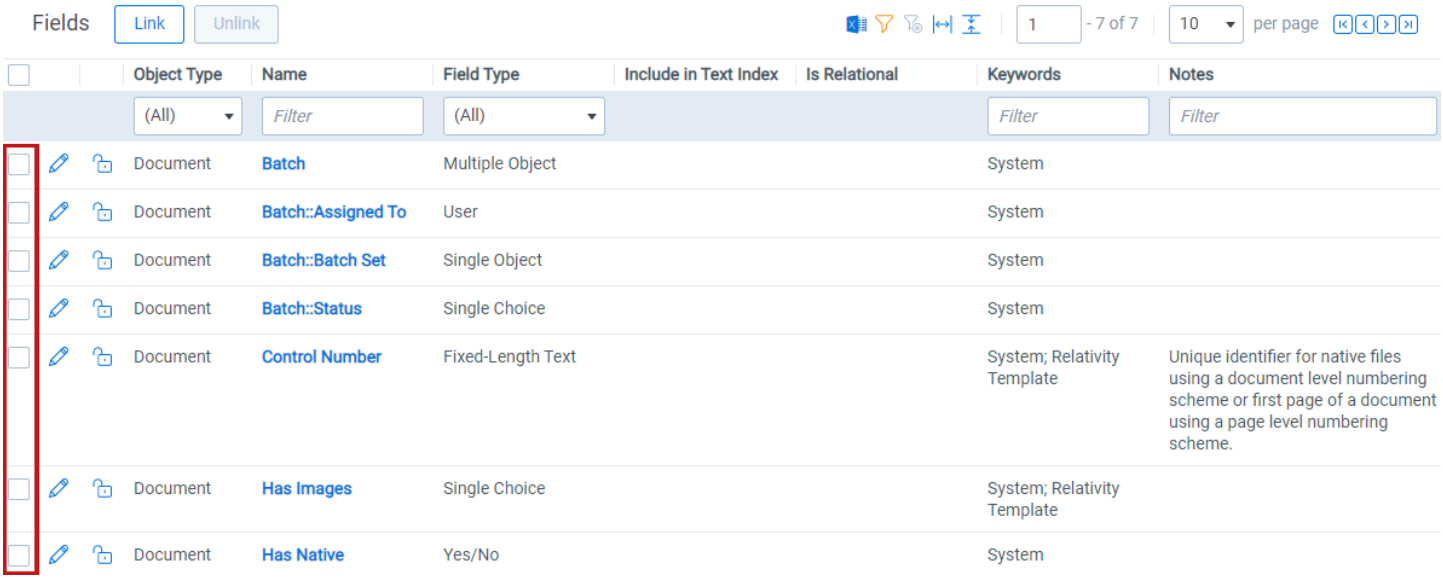
4. Filter the field list as needed and check any desired fields.
5. Once the desired fields have been selected, click the **Move selected left to right** icon.

6. Click **Apply**.
   The selected fields are linked to the field category and display in the Fields section.

10.4 Unlink a field or fields from a field category

To unlink a field or fields from a field category, do the following:

1. Navigate to the **Field Categories** tab.
2. Click on the desired field category in the list.
3. Click the checkbox on the left side of the row for any fields you wish to unlink.



4. Click **Unlink**.
5. Click **Unlink** again in the pop-up.
   The selected fields are no longer linked to the field category.

11 Filters

Filtering provides a fast and easy way to search for items in a list in Relativity. You can use filters to search for values in the fields on the active view, and across all records available in the searchable set. Filters are also available for item lists on tabs and pop-up windows.

The field type associated with each column determines the available filter types, such as text boxes, pop-up pickers, and drop-down lists. You do not need any specific security permissions to use filtering.

11.1 Showing and hiding filters in the item list

You enable filters by clicking an icon located at the top of the document list. You can:

- **Show/Hide filters** ()—to display the field filters at the top of each column. This icon turns orange when you activate a filter. Click the icon again to hide the filters. Your filter settings remain unchanged.
- **Clear all** ()—to remove the current filter settings. This option is only available after you set a filter.

The filter type determines the steps required to set the filtering criteria that it uses. See Filter types for details on filter types and their use.

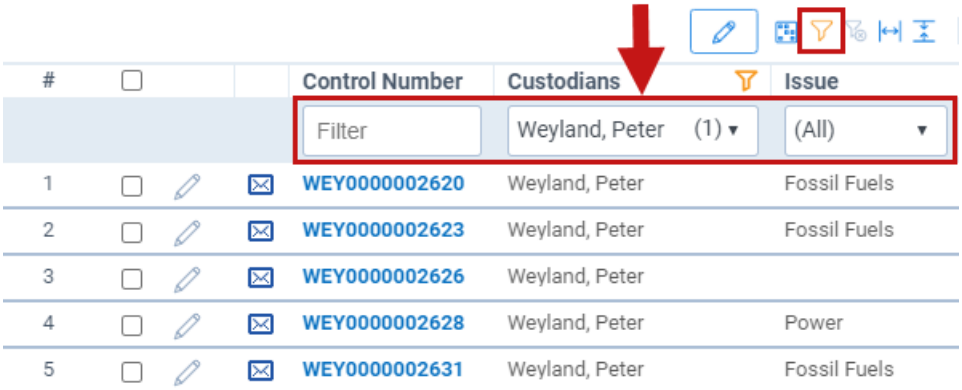
Note: When you create or edit a field, you can select its **Filter Type**. See Fields in the Admin guide.

After enabling filters, you are ready to enter criteria for the fields in your list.

Note: Before defining a new search filter, click the **Clear All** ( ) icon or the **Clear All Conditions** link in the Search Conditions panel to remove any filter settings. For example, say you create a filter on the Privileged field, but now want to search only by the Custodian field. If you do not clear the filter, Relativity filters your documents by both the Privileged and Custodian fields, and your results may include fewer documents than you expect.

To use a filter:

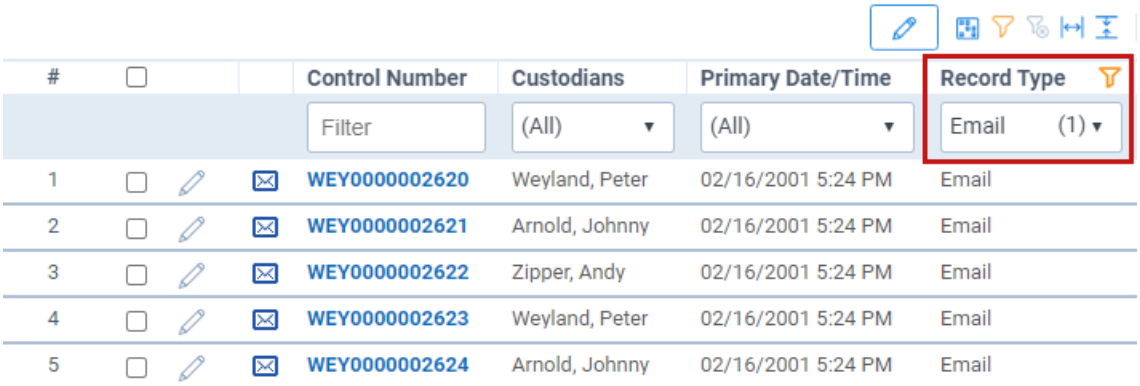
1. If filtering is not enabled, do so by clicking the filter icon to display the filtering fields below the column headings. The icon will change to orange.
2. Enter your filter criteria. The filter type determines how you enter the criteria and how to use operators to further define the filter. See Filter types for details on filter types and their use.



#			Control Number	Custodians	Issue
			Filter	Weyland, Peter (1)	(All)
1			WEY0000002620	Weyland, Peter	Fossil Fuels
2			WEY0000002623	Weyland, Peter	Fossil Fuels
3			WEY0000002626	Weyland, Peter	
4			WEY0000002628	Weyland, Peter	Power
5			WEY0000002631	Weyland, Peter	Fossil Fuels

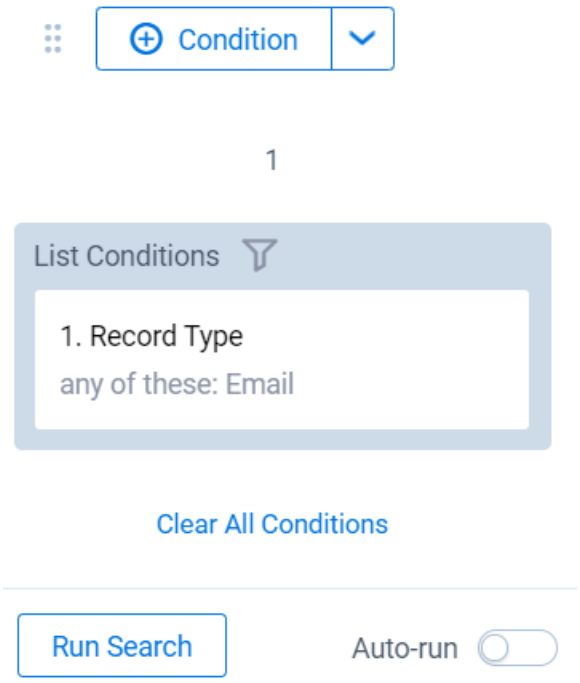
3. Press **Enter** to display the filter results.

The field column header displays the filter icon, letting you know which fields have filters applied. This persists whether you have the filters shown or hidden.



#			Control Number	Custodians	Primary Date/Time	Record Type
			Filter	(All)	(All)	Email (1)
1			WEY0000002620	Weyland, Peter	02/16/2001 5:24 PM	Email
2			WEY0000002621	Arnold, Johnny	02/16/2001 5:24 PM	Email
3			WEY0000002622	Zipper, Andy	02/16/2001 5:24 PM	Email
4			WEY0000002623	Weyland, Peter	02/16/2001 5:24 PM	Email
5			WEY0000002624	Arnold, Johnny	02/16/2001 5:24 PM	Email

The Search Conditions panel also shows the filtering conditions.



You cannot edit the Search Conditions cards by clicking on them. However, you can clear all the conditions by clicking the link at the bottom of the panel.

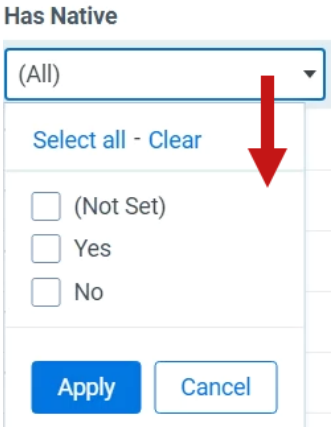
11.2 Filter types

Relativity contains the following filter types:

- Boolean—Yes/No fields.
- Numeric—decimal, whole number, and currency fields.
- List—single choice, single object, user, and fixed-length text fields.
- Date—date fields.
- Multi-list—multiple choice, multiple object, and single choice fields.
- Text box—fixed-length text, long text, date, whole number, decimal, currency, and object fields.

11.2.1 Using Boolean filters

Boolean filters are available for Yes/No field types. To use a Boolean filter, click the drop-down menu and select **Yes**, **No**, or **(Not Set)** from the list. Click **Apply** to set the conditions. Click **Select all** to select all the options. Click **Clear** to remove the filter settings.



11.2.2 Using numeric filters for numbers

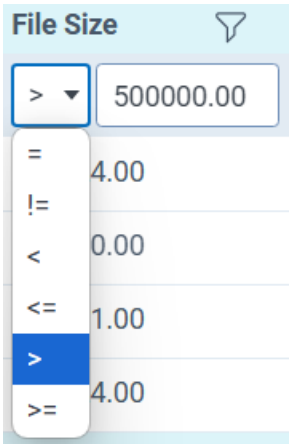
The numeric filter is available for the following field types:

- Decimal
- Whole Number
- Currency

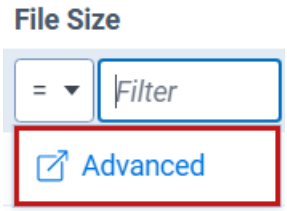
To use a numeric filter, click the drop-down menu and select an operator. Operators include:

- Equal to (=)
- Not equal to (!=)
- Greater than (>)
- Less than (<)
- Less than or equal to (<=)
- Greater than or equal to (>=)

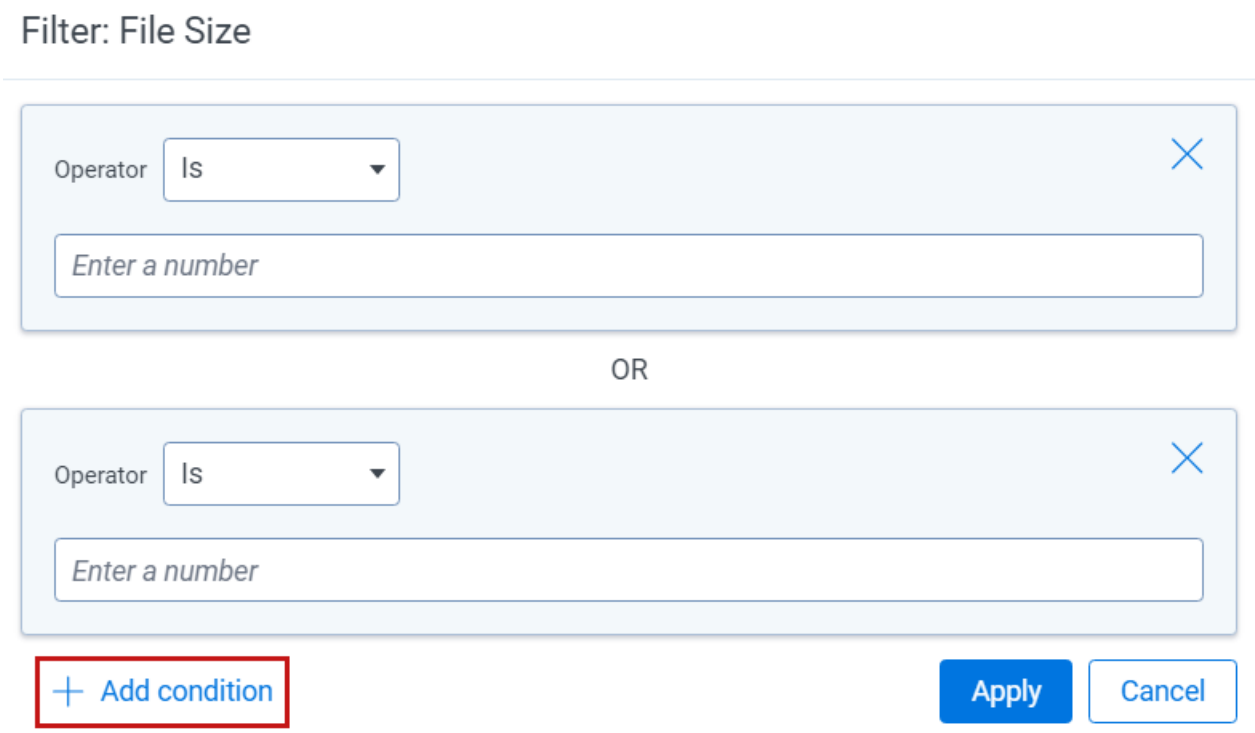
Enter a numerical value in the filter text box. After you enter the value in the text box, press **Enter** to apply the filter. For example, you might search for documents having a file size greater than 500000 bytes.



When you click inside a filter text box, the **Advanced** link appears. Clicking this link opens the advanced filters screen for the filter type.



Here, you can adjust the operator and add conditions to further define the filter. Click **Apply** to set the conditions.

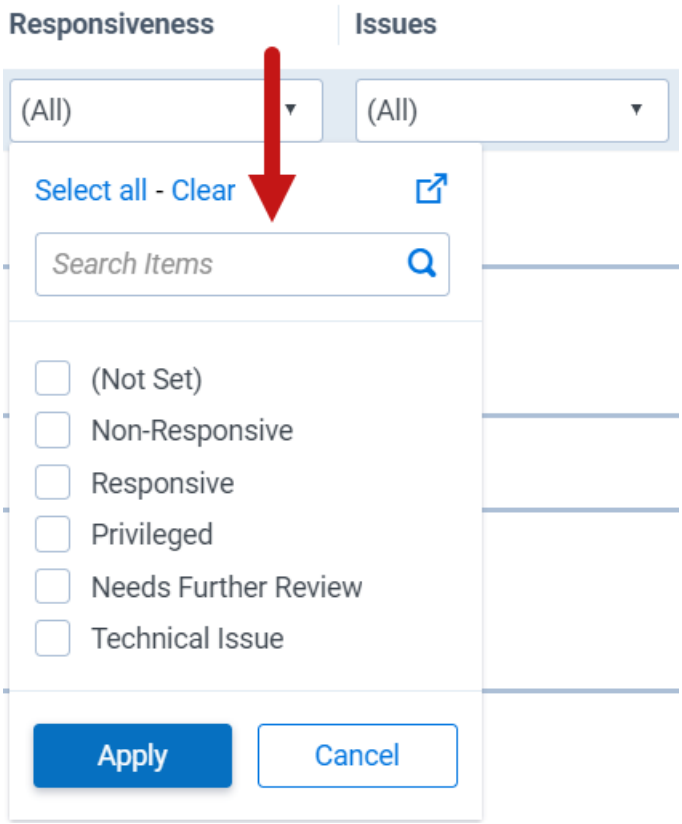


11.2.3 Using List filters

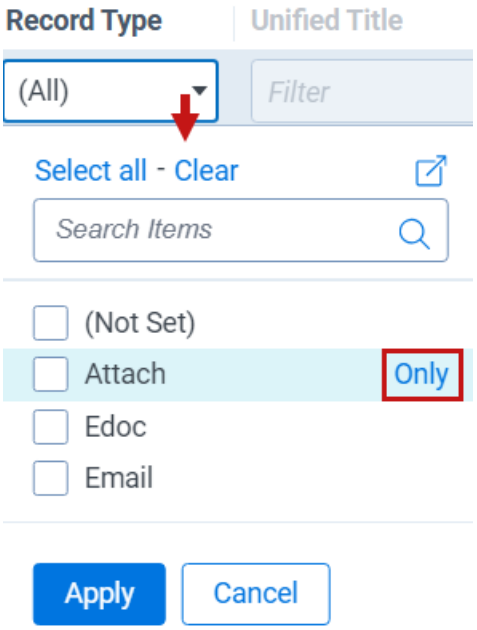
The List filter is available for the following field types:

- Single Choice
- Single Object
- User
- Fixed Length Text

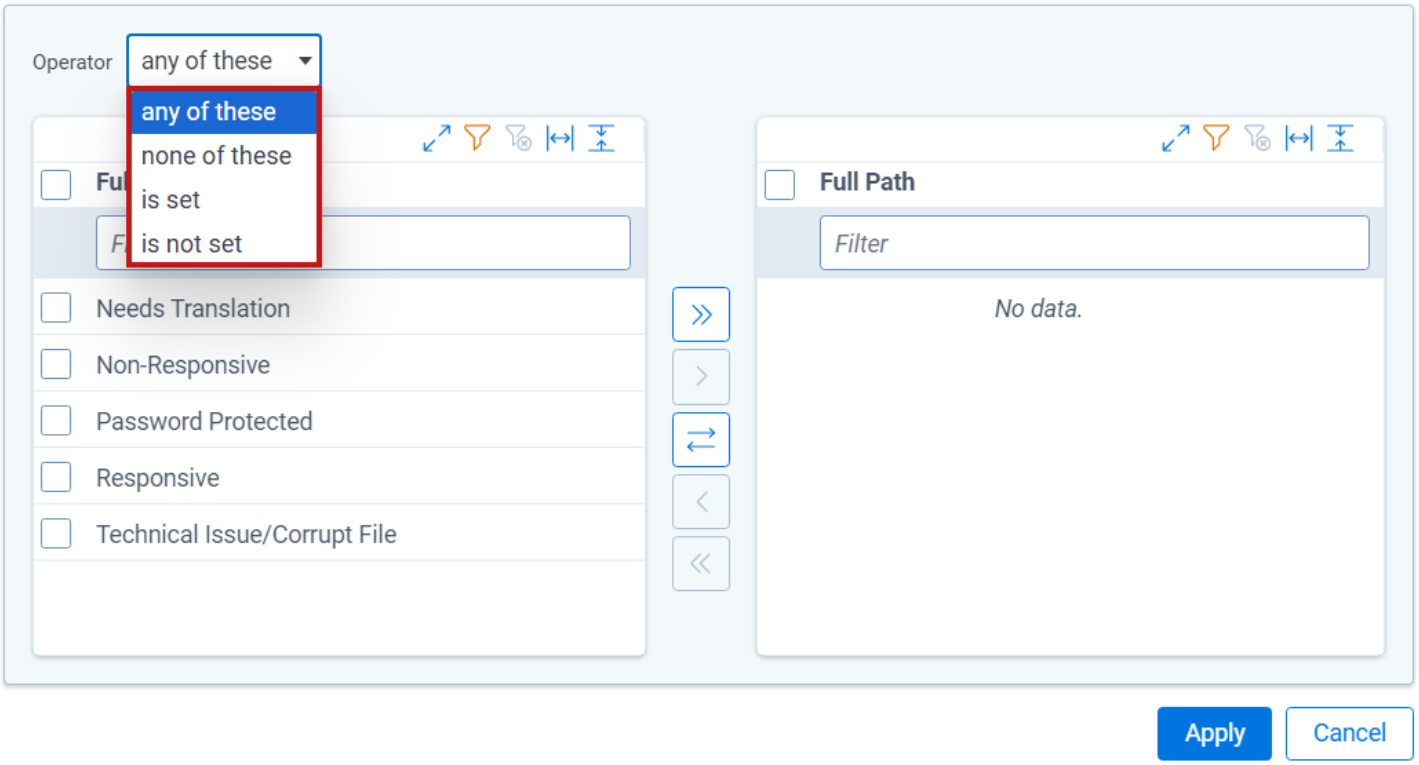
List filters are often associated with fields used for coding documents. The options displayed in the drop-down menu vary by the type and purpose of the associated field. For example, a field called Responsiveness might have the filter conditions of Responsive, Not Responsive, or Needs Further Review. Select the options that you want to filter for, and click **Apply**. Alternatively, you can click **Select all** to select all filters in the list. Click **Clear** to remove all selections. Click **(Not Set)** to show items where the field is empty (null).



If there is a single filter choice you want to apply immediately, hover over the item's row and click **Only** when it appears on the right side.



Click the **Advanced filters** ( ) icon to the right of the **Select all - Clear** options to launch the advanced filters dialog. This dialog has more operators and you can add or remove list items to the field's drop-down menu. Click **Apply** to set the conditions.



11.2.4 Using date filters

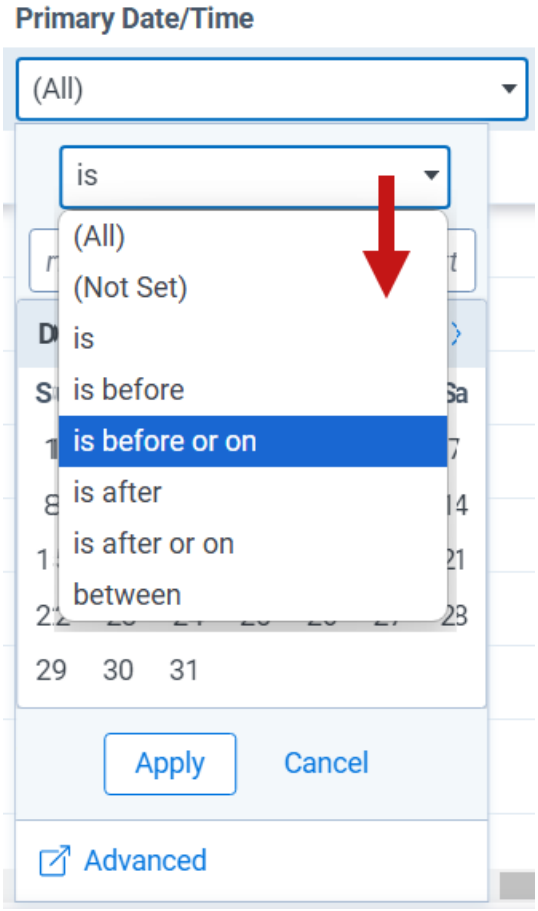
The date filter is available for Date field types to filter on dates and date ranges.

The following operators are available:

- (All)
- (Not Set)
- Is
- Is before
- Is before or on
- Is after
- Is after or on
- Between

For example, if you only want to view items sent before or on January 21, 2024 7 AM, do the following:

1. Select the **is before or on** operator.

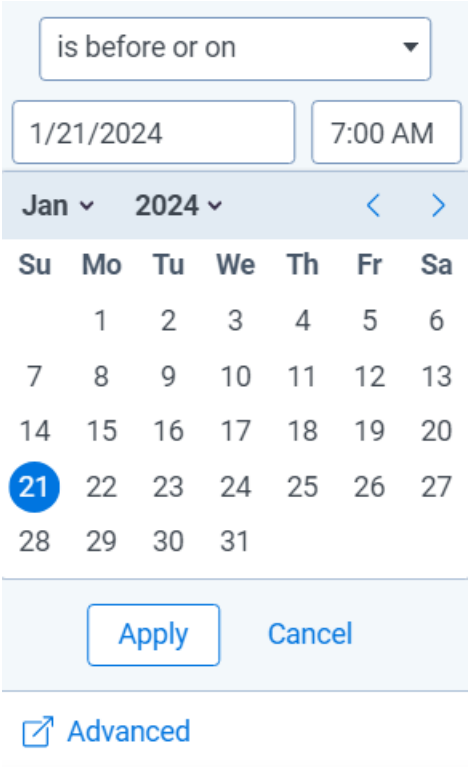


2. Use the calendar interface to select the date, *January 21, 2024*. You can enter the date directly into the text boxes, or use the forward and back arrows to scroll through the calendar months.

   Note: When you select the Between operator, two calendars display in the drop-down date filter, allowing you to pick the starting and ending dates and times.

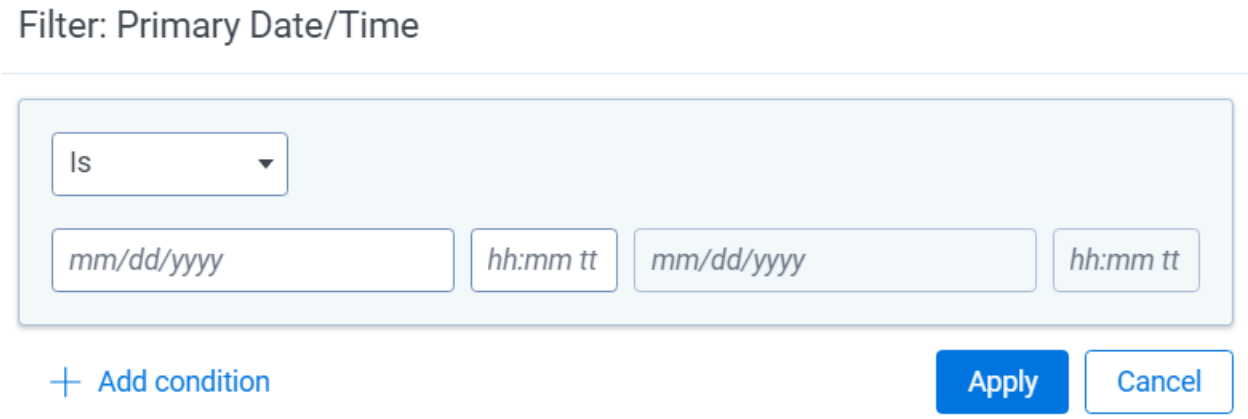
3. Enter the time of *7:00 AM*.

   Note: Filtering on fields using the date and time format does not support using @Today. If you do not enter a specific time, Relativity enters the default time of 12:00 AM.



4. Click **Apply** to set the conditions. Only items sent on or before 7 AM on January 21, 2024 appear in your document list.

Click the **Advanced** ( ) link at the bottom of the calendar interface to launch the advanced filters screen. This screen has more operators where you can add additional date and time conditions. Click **Apply** to set the conditions.



11.2.5 Using multi-list filters

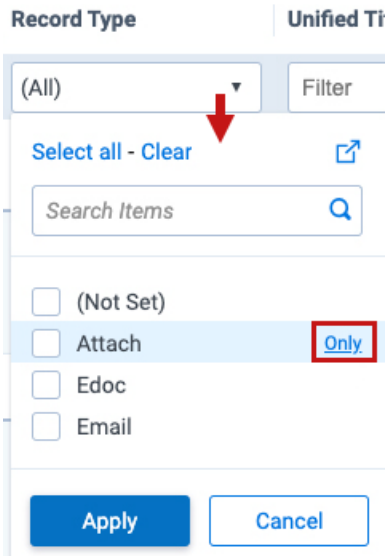
The multi-list filter is available for the following field types:

- Multiple Choice
- Multiple Object
- Single Choice

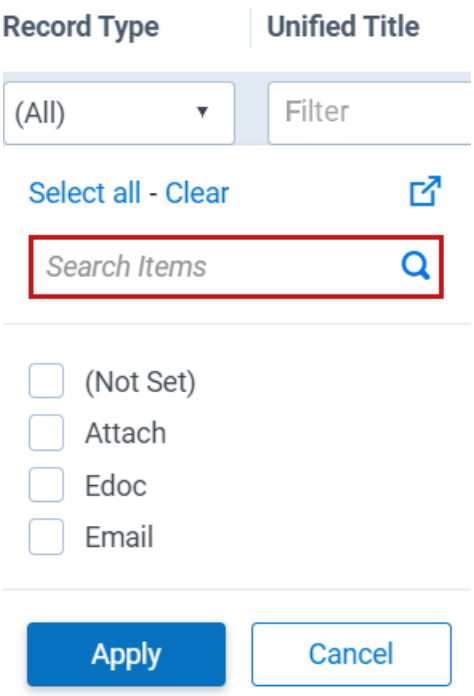
Using multi-list filters, you can select multiple conditions from a drop-down menu. These filters are often associated with fields used for coding documents.

To apply a multi-list filter, click the drop-down menu to display the conditions list. Select the conditions that you want to filter on. Click **Select all** to select all filters in the list. Click **Clear** to remove all selections. Select **(Not Set)** to show items where the field is empty (null). Click **Apply** to set the conditions.

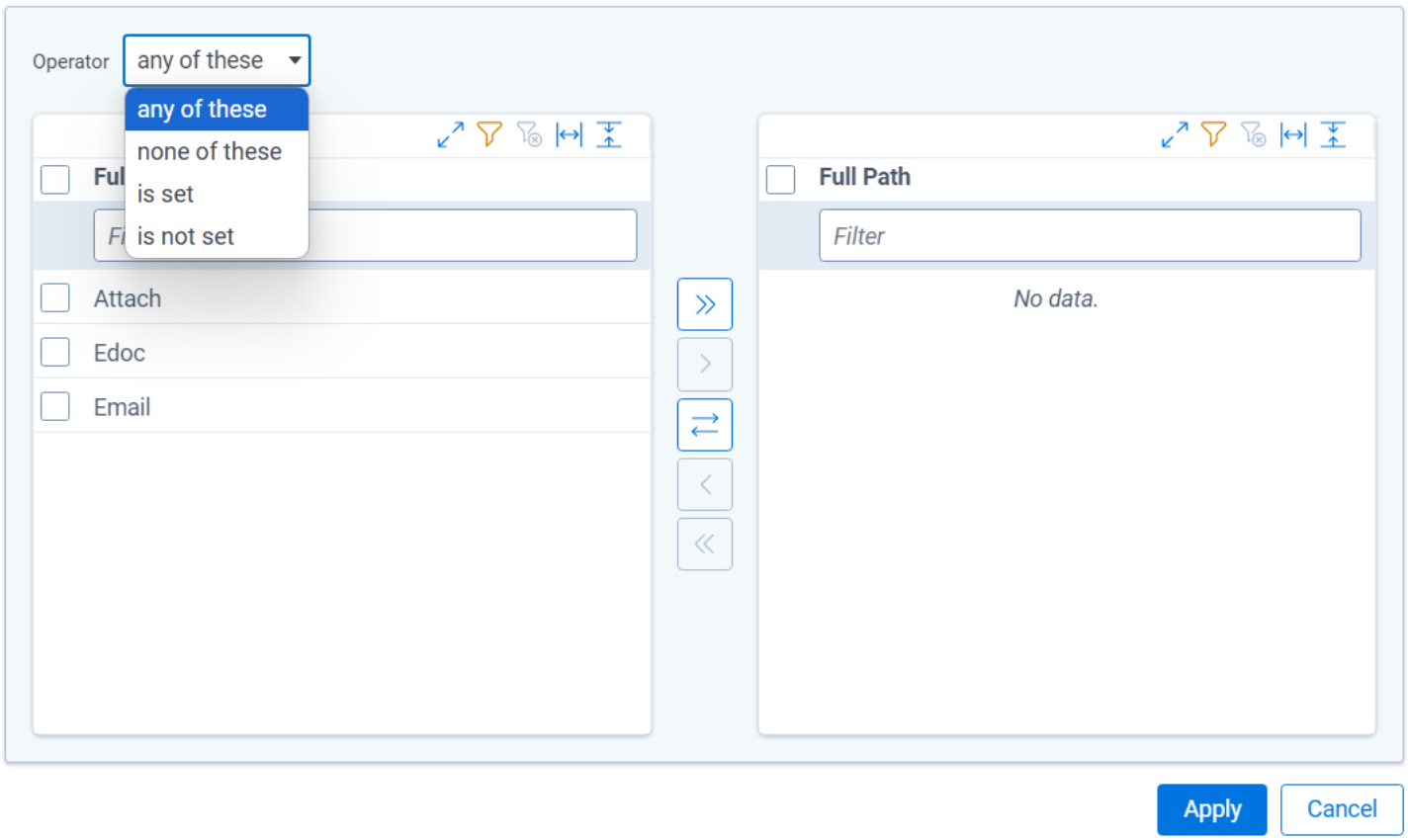
If there is a single filter choice you want to apply immediately, hover over the item's row and click **Only** when it appears on the right side.



To find a specific list item in a large list, use the search box to enter a term. The list filters automatically as you type.



Click the **Advanced filters** ( ) icon to the right of the **Select all - Clear** options to launch the advanced filters screen. This screen has more operators where you can add or remove list items to the field's drop-down menu. Click **Apply** to set the conditions.



11.2.6 Using text box filters

The text box filter is available for the following field types:

- Fixed-length Text
- Long Text
- Date
- Whole Number
- Decimal
- Currency
- Object

You can use text box filters to search on specific terms, numbers, and dates. Enter one or more terms in the filter text box. Connect multiple terms using the following operators:

- AND
- OR
- IS SET
- IS NOT SET
- BETWEEN
- = (equal)

- >= (greater than or equal to)
- <= (less than or equal to)

When entering terms and operators directly into a text box filter, you must use the proper syntax. See Text box filter search examples for more information.

You can also use the advanced text box filter feature to build more advanced filter queries on the selected text field. See Using advanced text box filtering.

11.2.7 Text box filter search examples

Using operators, you can perform text searches by entering search strings directly into the filter text box. Additionally, you can use the advanced filtering feature to build more detailed queries. See Using advanced text box filtering for more information.

11.2.7.1 Search operators

The following table lists examples of valid search strings using search operators.

Valid search strings	Description of search results
cubs OR sox	Matches either *cubs* or *sox* or both.
cubs AND sox	Matches both *cubs* and *sox*. Both terms must appear for a successful match.
cubs OR sox AND kcura	Matches either *cubs* or *sox* or both, and *kcura*.
percent sign (%)	Acts similar to a wildcard, or the *is like* operator in a query. *%chard* matches *Richard*, *Pritchard*.
underscore (_)	Acts as a wildcard for a missing character. Do not use the underscore to check a field's value. It is slower and more resource-intensive than using the percent sign (%).
= with term	Matches an exact phrase.
cubs sox	Matches an exact phrase, *cubs*(space)*sox*.
IS SET	Returns only items where the field has a value.
IS NOT SET	Returns only items where the field does not have a value (null).

The following table shows examples of invalid search strings.

Invalid search strings	Description of search results
cubs AND	The AND operator requires a right search term.
cubs OR	The OR operator requires a right search term.
AND cubs	The AND operator requires a left search term.
OR cubs	The OR operator requires a left search term.

11.2.7.2 Alphabetical filtering

The following table lists examples of valid search strings you can use to filter text alphabetically.

Alphabetical filtering	Description of search results
>= c	Matches any term or phrase where the first letter is *c* or later in the alphabet.
<= c	Matches any term or phrase where the first letter is *c* or earlier in the alphabet.

Alphabetical filtering	Description of search results
= cubs sox	Matches the exact phrase *cubs*(space)*sox*.
cubs BETWEEN sox	Matches terms or phrases where the first letter of the phrase falls between *c* and *s* in the alphabet.

11.2.7.3 Dates and numbers

The following table lists examples of valid date and number searches, and the expected result set. When entering dates, do not place a zero (0) in front of single-digit values. For example, use *7/24/2024* and not *07/24/2024*.

Valid search strings	Description of search results
>= 7/24/2024	Matches *7/24/2024* and later dates.
<= 7/24/2024	Matches *7/24/2024* and earlier dates.
= 7/24/2024	Matches the exact date of *7/24/2024*.
>= 7/24/2024 1:23 PM	Matches *7/24/2024 1:23 PM* and later dates and times.
<= 7/24/2024 1:23 PM	Matches *7/24/2024 1:23 PM* and earlier dates and times.
= 7/24/2024 1:23 PM	Matches the exact date and time of *7/24/2024 1:23 PM*.
7/24/2024 BETWEEN 8/24/2024	Matches dates that include and fall between *7/24/2024* and *8/24/2024*.
7/24/2024 1:23 PM BETWEEN 8/24/2024 3:45 PM	Matches dates and times that include and fall between *7/24/2024 1:23 PM* and *8/24/ 2024 3:45 PM*.
7/24/2024	Matches the exact date of *7/24/ 2024*.
>= 100	Matches numbers that are greater than or equal to *100*.
<= 100	Matches numbers that are less than or equal to *100*.
= 100	Matches *100* exactly.

The following table includes examples of invalid data and number search strings.

Invalid search strings	Description of search results
> 7/24/2024	You must use the equal sign with the greater than operator (>=).
< 7/24/2024	You must use the equal sign with the less than operator (<=).
>= 0/24/2024	The search string starts with 0 for the month. Instead of *01/24/2024*, use *1/24/2024*.
= 0/24/2024	The search string starts with 0 for the month. Instead of *01/24/2024*, use *1/24/2024*.
07/24/2024 BETWEEN 8/24/2024	The search string starts with 0 for the month in the starting date. Instead of *01/24/2024*, use *1/24/2024*.
7/24/2024 BETWEEN 08/24/2024	The search string starts with 0 for the month in the ending date. Instead of *01/24/2024*, use *1/24/2024*.

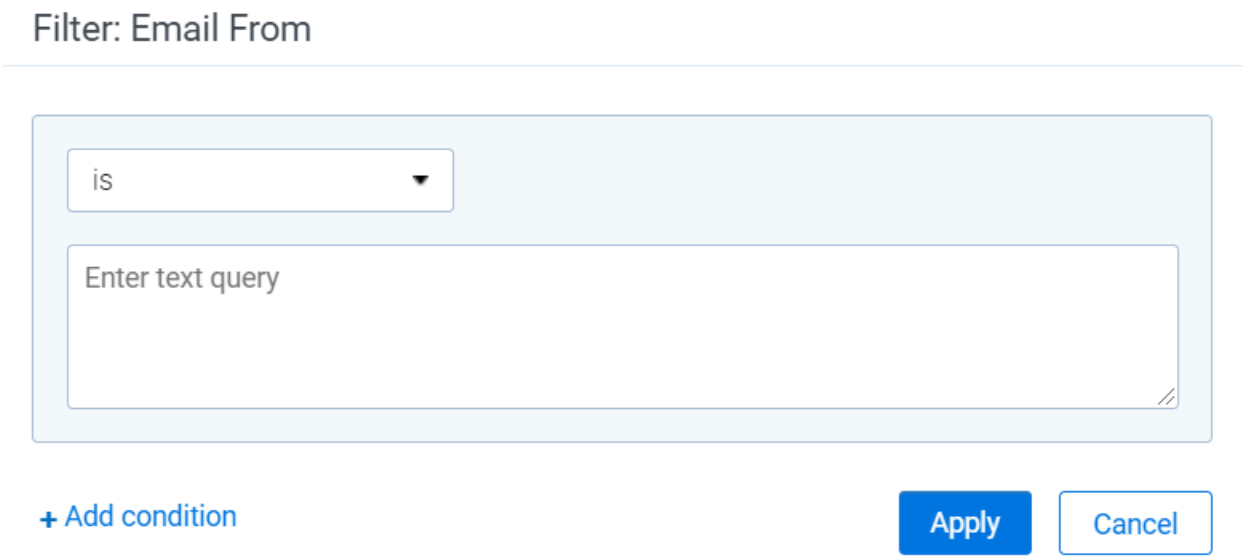
11.2.8 Using advanced text box filtering

You can use the following operators with advanced filtering:

- Is
- Is not
- Is set
- Is not set
- Is less than
- Is greater than
- Is like
- Is not like
- Contains
- Does not contain

To use advanced text box filtering:

1. Click inside the filter text box for a column. The **Advanced** link appears.
2. Click the **Advanced** link.
3. Choose an operator (such as is greater than.) See Fixed-length, long, or extracted text operators in the Searching guide for a list of definitions of the available operators.



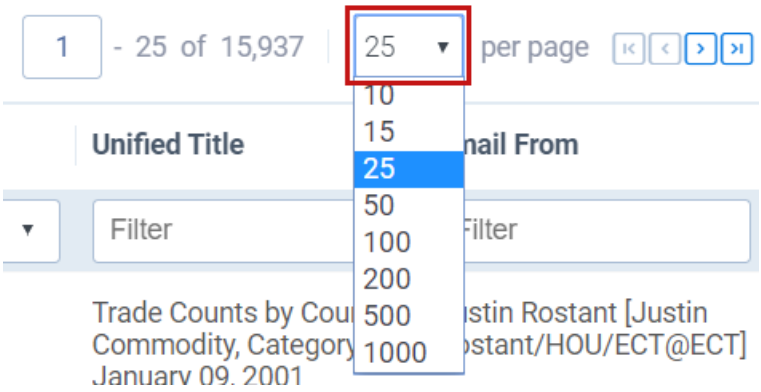
4. Enter a value into the query text box(such as 100.) The filter returns items where the value of the field is greater than 100.
5. (Optional) Click **Add condition** to add a new filter condition. For example, you may want to also return items where the text field contains the word privilege.

   Note: Multiple conditions are automatically connected with an OR operator.

6. Click **Apply** to set the conditions.

11.3 Changing item sets per page

You can use the set selector menu to change the number of items that appear per page. The set selector menu is at the top of the document list. The option you select remains the default setting during your session until you select another option.



11.4 Saving filters as a search

To save your filtered item set as a saved search:

1. Click the **Save Search** button located at the bottom of the screen.
2. Select or enter the following required information:
    - **Name**—enter a title for the search. The title appears in the saved searches browser.
    - **Owner**—select **Public** to make the search available to all users or choose a specific user from the list. Click **Me** to select your name from the list, making the search private. (You must have the appropriate privileges to view searches.) See Controlling the visibility of saved searches in the Searching guide.
    - **Search Folder**—click the **Select** button to launch a pop-up window where you can save the new search to a specific folder on the saved searches browser. Highlight the folder where you want to save the search, and click **OK** to select it.
3. Add to or change the search criteria as needed. See Create and edit a saved search.
4. Click **Save**.

12 Groups

With groups you can organize users in Relativity. A user can be a member of one or more groups. You can grant groups permission to view admin tabs from Home. You can also add groups to workspaces and set permissions per group on a workspace-by-workspace basis.

12.1 System groups

Relativity workspaces include the following default system groups:

- **Everyone** - All users are members of the Everyone group. System admins can manage the permissions all users have on system level views and scripts. You are unable to revoke certain permissions for the Everyone group.

- **System Administrators** - Relativity system admins have rights to see every item in a Relativity environment. System admins have full access to all admin tabs. System admins can then create and edit new clients, matters, users, groups and views, among other capabilities. System admins also have the following script and applications-related permissions: view, run, preview, create/write, edit (unlocked scripts only), link, and import applications.

  Note: Regardless of permissions, system admins can't edit locked scripts.

Note: Relativity Lockbox is enabled for all Relativity aiR customers. When the Relativity Lockbox feature is enabled (via the EnableCustomerLockbox instance setting), Relativity system admins must also belong to a group within a workspace in addition to the System Administrators group to access and administer security within that workspace. Refer to Support if you need more information on this feature.

Note: Feature Permissions provide an alternative to Relativity's security management by shifting the focus from Object Types and Tab Visibility to feature-based permissions. This method is an alternative option. Any feature-specific permissions information already in this and other topics is still applicable. The Feature Permissions interface enables administrators to manage permissions at the feature level, offering a more intuitive experience. By viewing granular permissions associated with each feature, administrators can ensure comprehensive control, ultimately reducing complexity and minimizing errors. For details see Instance-level permissions and Workspace-level permissions.

The following table shows script permissions for each group.

Role	View	Run	Edit (locked scripts)	Edit (unlocked scripts)	Preview	Write	Link
System Admin	✓	✓		✓	✓	✓	✓
Standard User	✓	✓					✓

12.2 Creating and editing groups

To create a new group or edit an existing group:

1. Click your name in the upper right corner of Relativity, and then click **Home**.
2. Click the **Groups** tab.
3. Click **New Group**. To edit group information, click the **Edit** link next to an existing group name.

   Note: If your groups list doesn't show Edit links, edit the All Groups view to display the Edit link.

4. Add or edit the fields on the group details page. See Fields for details.
5. Click **Save** to save the group information.

The group details page displays a list of users added to the group as well as group-accessible workspaces. For more information, see Managing security in the Admin guide.

12.3 Fields

The groups object contains the following fields:

Group Information

- **Name** - the group's name, which is a required field for creating a group.

  Note: As your Relativity environment grows, arbitrary group names like "Group 1" can produce a confusing administrative workflow. Name each group according to their purpose and permission level, such as "ACME Co. Reviewer" and "ABC Corp. Administrators."

- **Client** - a required field that makes the group a child object of the chosen client.
- **Group Type** - an uneditable field that displays one of the following categories:
  - System Admin
  - System Group
  - Personal
  - Everyone
  - Workspace Admin
- **Keywords** - an optional field where extra group information may be recorded.
- **Notes** - an optional field where extra group information may be recorded.

12.4 Adding users to groups

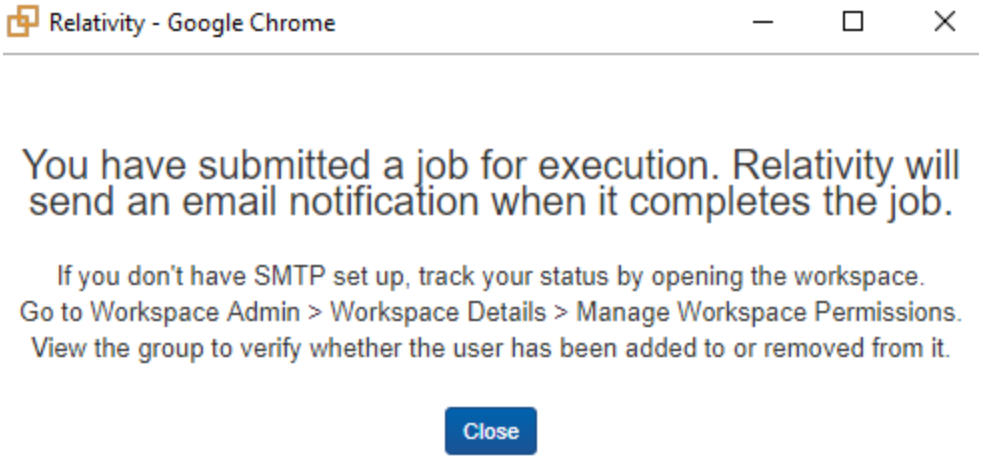
You can add and/or remove users from groups from either the group details page or the user details page. The procedure is the same for both.

Note: A job is executed when you add users to a group or when you remove them from one.

To add or remove users:

1. Click your name in the upper right corner of Relativity, and click **Home**.
2. Click the **User and Group Management** tab. You can complete the following steps from either the Users or Groups tabs:
   - From the **Users** tab, click the name of a user and scroll down to the Groups section on the form.
   - From the **Groups** tab, click the name of a group and scroll down to the Users section on the form.
3. To add a user to the group, click **Add** in the Users or Groups section depending on the tab.
4. Choose an item on the selection dialog, and click **OK**.

5. Click **Close** on the message indicating that you have submitted a job.



Note: Relativity sends an email message notifying you when the job is completed. If an error occurs, the email message contains a link that you can use to retry the job. You must be logged into Relativity before you click the retry link. The Errors tab also displays the retry link.

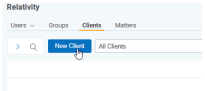
Note: The (Admin) Errors tab has been permanently removed from Relativity aiR, and the ability to read errors through the API has been disabled. Job-specific errors are now addressable directly within your workspaces. For more information, see Errors tab deprecation.

6. To remove a user from a group, click **Remove**. Click **OK** on the confirmation message, and then click **Close**.

Note: You can preview the security of a group to determine whether or not the appropriate permissions are granted to that group over particular workspaces. For more information about previewing group security see Preview security.

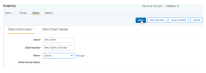
12.5 Adding external users through groups

1. At the instance-level, navigate to the Clients tab.
2. Click the **New Client** button.

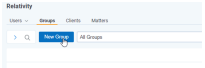


3. Create a new client to associate the external group to and click **Save.**

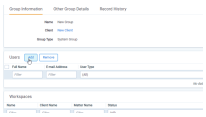
Note: The 'client number' field can either be the 'client name' value again, or a unique identifier.



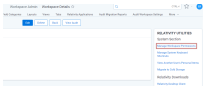
4. Once the new client has been created, navigate to the Group tab and select **New Group**.



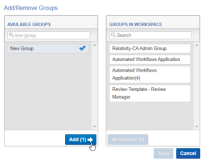
5. Enter a Group name to associate the external users to and connect it to the newly created client.



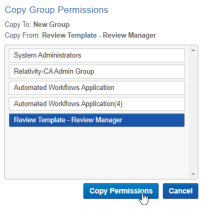
6. Add any users to this group who will need access to the workspace.
7. Next, navigate to the workspace you want to give them access to and click on Workspace Details on the right side of the screen.



8. Select Add/Remove Groups and filter to the newly created group. Select Add, then Save.



9. Click on the newly created group and select the Copy option. After copying permissions, you can select the **Preview** option to confirm what level of access they will have within the workspace.



10. Select the template group from which you want to assign permissions.

Note: Choices can vary depending on the workspace's template. Reviewer groups usually start with a Level 1, which grants the least permissions. More permissions are offered as the level increases. In contrast, Admin Groups often have most or all permissions within a workspace. If you are unsure, it is recommended to select the group with the lowest level of permissions. You can always copy a group with higher permissions later if you need to grant more capabilities.

12.6 Adding or removing groups from a client domain

You can add or remove objects from client domains if you activate the client domains feature.

Note: Moving a group into a client domains may cause the group to lose previously configured permissions.

Note: Relativity displays a warning message when a sys admin attempts to edit or copy permissions for any group in a client domain. This warning makes the sys admin aware that modifying permissions may have significant consequences. For example, changing permissions may allow client domain users to modify items outside their tenancy. The sys admin can click **Manage Permissions** to proceed with the update or **Cancel** to exit the pop-up window.

Use the following steps to add a group to a client domain:

1. Navigate to the **Groups** tab.
2. Select the group you want to add to the client domain from the list.
3. Click **Edit**.
4. Click **Select** next to the **Client** field in **Group Information** section.
5. Select the client with client domains enabled from the list.
6. A warning message requires you to confirm your decision by clicking **Save**.
7. Click **Save**.

Use the following steps to remove a group from a client domain:

1. Navigate to the **Groups** tab.
2. Select the group you want to remove from the client domains from the list.
3. Click **Edit**.
4. Click **Select** next to the **Client** field in **Group Information** section.
5. Select a client not associated with a client domain from the list.
6. Click **Save**.

13 Imaging

Imaging converts native documents into static image files (TIFF or JPEG) that you can review, redact, and produce. Use imaging profiles to control output settings like file format, DPI, and document-type-specific options. Then use imaging sets, mass image, or image on the fly to convert your documents.

There are three ways to image documents:

- **Imaging sets** — image a group of documents based on a saved search and a specific imaging profile. Imaging sets also provide error-handling functionality you can use to view error messages and rerun imaging on specific documents or jobs.
- **Mass image** — select multiple documents from a document list and image them at once using a specific imaging profile.
- **Image on the fly** — image a single document directly in the Viewer using any imaging profile you have permission to use.

13.1 Security permissions for imaging

The following security permissions are designated for imaging documents in Relativity aiR. These apply to all imaging options, including image-on-the-fly, mass image, and imaging sets, unless otherwise noted.

Object security	Tab visibility	Other settings
• **Document** – Add, View • **Imaging Profile** - View, Edit, Add • **Imaging Set** - View, Edit, Add	• Documents • Imaging Profiles • Imaging Sets	Mass Operations • Image System Field requirements

Object security	Tab visibility	Other settings
Note: You can still use mass imaging and image-on-the-fly even if you don't have the Edit permission on the Imaging Set object. • **Native Type** - View **Note:** View permission for the Native Type object is needed to create a new Basic and/or Native Imaging Profile.		• Has Images field

Note: When you run imaging on a specific saved search used in an imaging set, documents that don't have the "Add Image" permission will be skipped.

Note: Feature Permissions provide an alternative to Relativity's security management by shifting the focus from Object Types and Tab Visibility to feature-based permissions. This method is an alternative option. Any feature-specific permissions information already in this and other topics is still applicable. The Feature Permissions interface enables administrators to manage permissions at the feature level, offering a more intuitive experience. By viewing granular permissions associated with each feature, administrators can ensure comprehensive control, ultimately reducing complexity and minimizing errors. For details see Instance-level permissions and Workspace-level permissions.

13.2 Troubleshooting imaging

If Image commands are missing from the Viewer or mass operations menu, or the Run button on an imaging set is disabled, check the following:

Symptom	Possible cause	Resolution
Image commands missing from the Viewer or mass operations menu	The Imaging application is not installed in the workspace.	Reinstall the Imaging application from Relativity Applications.
Image commands missing from the Viewer or mass operations menu	The user's group does not have the Mass Images permission (under Mass Actions) or the Add Image document permission.	Grant the required permissions to the user's group. See the Security permissions section for details.
The Run button on an imaging set is disabled	The user's group does not have the required permissions.	Verify that the user has View, Edit, and Add permissions on the Imaging Set object, and the required document permissions.

13.3 Image on the fly

By using the Imaging option in the Viewer, you can image a single document on the fly with any imaging profile you have permissions to. For more information, see Imaging on the fly on page 740.

13.4 Mass image

You can image multiple documents at the same time by using the Mass Image operation in the document list. Select an Imaging Profile to use when imaging a group of documents. For more information on mass imaging, see Mass image on page 368.

13.5 Imaging profiles

An imaging profile controls the settings used to image a group of documents. You can convert documents to black and white TIFF files or colored JPEG files. After you create a profile, you can use it in multiple imaging sets, update the profile settings, and set permissions on it. Imaging profiles, as well as any updates to the default profile, are included in workspace templates.

Relativity includes a default imaging profile that has the recommended default settings preset. It's best practice to make a copy of this default profile and make changes as appropriate when creating additional profiles. The mass image and the image-on-the-fly functionality defaults to this profile, but you can select any other profile when converting documents to images.

Note: Base your imaging profile selection on your case needs, such as document type or production format requirements. Imaging profiles do not map directly to Relativity user roles—no single profile type is better suited for a case manager, reviewer, or litigation support specialist than any other.

There are two main options for creating an imaging profile:

- **Basic Imaging Engine Options**—provides a select number of simple settings for creating the profile.
- **Native Imaging Engine Options**—provides an expanded range of settings for creating a profile.

13.5.1 Creating and editing an imaging profile

To create or edit an imaging profile:

1. Navigate to the **Imaging Profiles** tab in a workspace.
2. Click **New Imaging Profile**.
3. Complete the required fields. See Fields for details.
4. Click **Save**.

Note: When you create a new profile from scratch, no default values exist for any profile fields. To start with default values already in place, copy the Default profile, assign it a unique name, and use it as a base for your imaging job.

Note: Relativity propagates native file types to imaging profiles only when the profile is created.

13.5.2 Fields

Expand the below drop-downs to view the fields and their descriptions associated with each section of the imaging profile.

Note: * indicates fields that are set automatically with default settings. You can change these settings as needed.

Imaging Profile Options

- **Name**—the name of the imaging profile.

  Note: You can not rename the default profile.

- **Imaging Method**—sets the type of imaging for the profile. The imaging engine options appear for the selected imaging method.

- **Basic**—uses a select number of user-specific settings to image documents using Oracle.
- **Native**—uses an expanded range of user-specific settings to image documents.

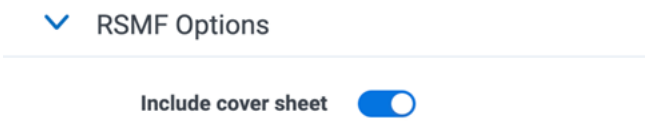
Note: A warning appears if you cannot perform native imaging.

Basic Imaging Engine Options

- **Basic Image Output Quality (DPI)***—controls the resolution and density of an image in dots per inch. A higher DPI value produces more image detail. The typical range is 200–600. The default value is 300, which matches the Default profile.
- **Basic Image Format***—sets the image format for files sent to the basic imaging engine for the profile, the default for this field is set to **TIFF**. The options are:
  - **JPEG**—renders the image as a color JPEG file. Selecting this can possibly decrease imaging performance because JPEGs have larger file sizes than TIFFs and therefore require more disk space.
  - **TIFF**—renders the image as a black and white TIFF file. This is recommended; this is the value in the Default profile.
- **Basic Image Size***—sets the image size for all images rendered with the basic imaging engine profile, the default for this field is set to **Original setting**. The options are:
  - **Original setting**—renders the image with the original document settings.
  - **Letter (8.5 in x 11 in)**—renders the image in standard letter size.
  - **A4 (8.27 in x 11.69 in)**—renders the image in A4 size.
  - **Legal (8.5 in x 14 in)**—renders the image in legal paper size.
  - **Custom**—sizes the image by using either or both values in the Maximum Image Width and Maximum Image Height fields. When you enter a value in either or both of these fields, Relativity converts the document to an image size that fits within these parameters, while maintaining the aspect ratio. If both of these fields are empty, Relativity displays an error message indicating that you must enter a value in one of them.
- **Maximum Image Height (Inches)** and **Maximum Image Width (Inches)** specify the largest allowable size for the generation of custom images. Relativity converts the document to an image size that fits within these parameters, while maintaining the aspect ratio. Only the Custom option references these fields, requiring you to enter a value in at least one of them.

RSMF Options

Select the **Include cover sheet** toggle to include or exclude a cover sheet.



Native Imaging Engine Options

- **Native Image Output Quality (DPI)***—controls the resolution and density of an image in dots per inch. A higher DPI value produces more image detail. The typical range is 200–600. The default value is 300, which matches the Default profile.
- **Native Image Format***—sets the image format for files sent to the native imaging engine for the profile, the default for this field is set to **TIFF**. The options are:

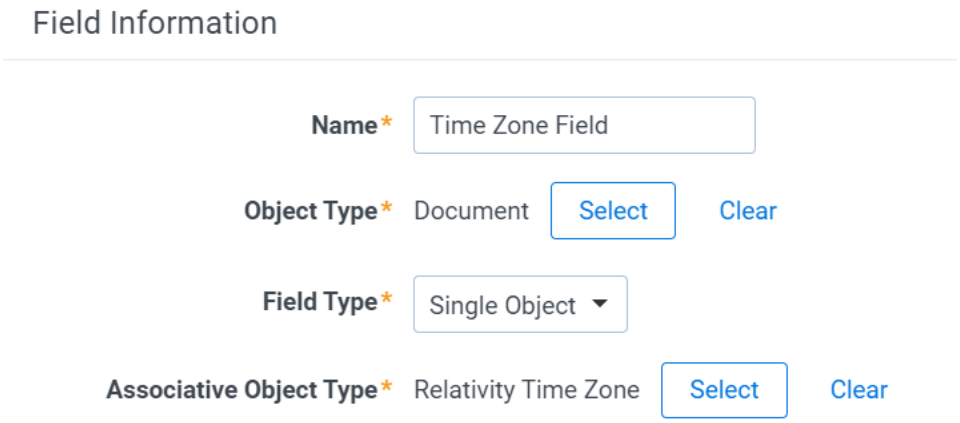
    - **JPEG**—renders the image as a color JPEG file. Selecting this can possibly decrease imaging performance because JPEGs have larger file sizes than TIFFs and therefore require more disk space.
    - **TIFF**—renders the image as a black and white TIFF file. This is recommended and is the value in the Default profile.
- **Automatically detect and render color pages to JPEG***—(Overrides 'Native Image Format' selection of TIFF) auto-detects and images color pages as JPEG files even if you selected TIFF as the Native Image Format. If you select Yes, Relativity overrides the TIFF Native Image Format for color pages only. If you select No, color pages remain as TIFFs. The default for this field is set to **No**.
- **Maximum pages imaged per file**—a native global setting for all document types that sets the maximum number of document pages that are imaged. For example, if you set this value to 50 and have a 100-page document, Relativity only images the first 50 pages of the document. Use this option to image only the number of pages entered in this box.
- **Dithering Algorithm***—the procedure the native imaging engine uses to convert images from color to black and white TIFFs. This setting is only used if Native Image Format is set to TIFF, the default for this field is set to **Floyd Steinberg**. The algorithm options are:
    - **Clustered 6x6**—groups pixels into clusters of 6x6.
    - **Clustered 8x8**—groups pixels into clusters of 8x8.
    - **Clustered 16x16**—groups pixels into clusters of 16x16.
    - **Dispersed 4x4**—disperses pixels in a 4x4 matrix.
    - **Dispersed 8x8**—disperses pixels in an 8x8 matrix.
    - **Dispersed 16x16**—disperses pixels in a 16x16 matrix.
    - **Floyd & Steinberg**—diffuses the difference between the actual analog value and quantized digital value of a pixel to its neighboring pixels.
    - **Threshold**—compares each pixel value against a fixed threshold. During this process, individual pixels in an image are marked as object pixels if their value is greater than the threshold value. If their value is less, they're marked as background pixels. If you select this, you must provide a value between 0-255 in the Dithering Threshold field.
- **Dithering Threshold**—sets the threshold against which all pixels are compared. This is required if you chose Threshold for the Dithering Algorithm field above. You can provide any value between 0 - 255. The recommended default threshold is 128. When the pixel RGB color model in an image is greater than the threshold, it's converted to black. When less, it's converted to white.
    - See Native imaging - dithering algorithm options on page 282 for details on the various dithering algorithms available within Relativity native imaging, as well as use cases for each algorithm, including the size and clarity of images you create.
- **Native Image Time Zone**—determines the time zone used to display dates and times in a document image. This field updates the date sent when native imaging an email, but the native document and metadata remain unchanged. Native Image Time Zone supports MSG and EML files only.

  Note: For Native Image Time Zone to apply, you must select Date Sent in the Native Image Date field. If you do not make a selection, Native Image Time Zone does not apply and defaults to the current date.

  To set the time zone value, click the drop-down next to Native Image Time Zone and select a time zone. If you do not select an option, the time zone defaults to Coordinated Universal Time (UTC).

To add an option to the Native Image Time Zone picker list:

1. Navigate to the **Fields** tab and click **New Field**.
2. Set these fields:



   - **Name**—type the name of the Native Image Time Zone option.
   - **Object Type**—select Document.
   - **Field Type**—select Single Object.
   - **Associative Object Type**—select Relativity Time Zone.
3. Click **Save**.

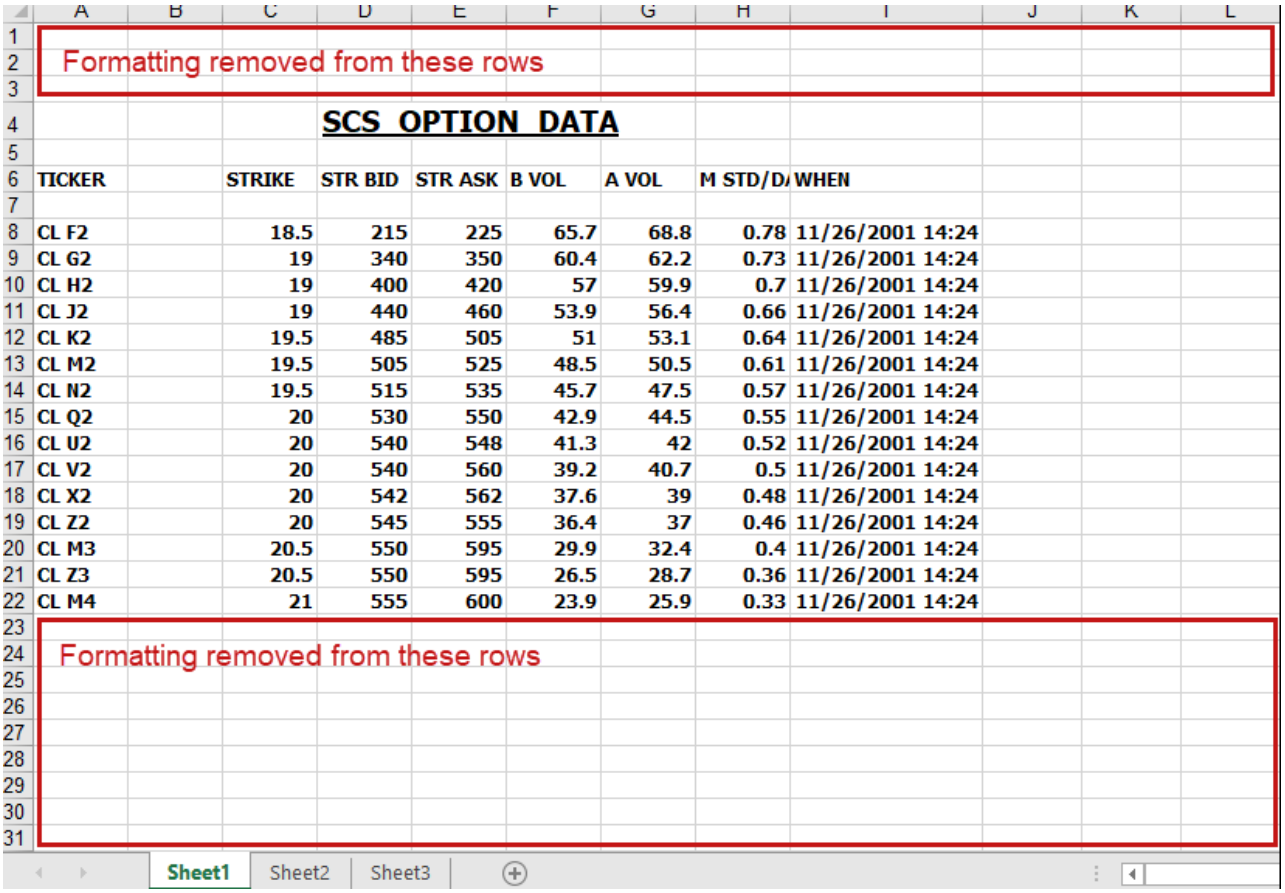
- **Native Image Date** - select any document-level date field available in the pop-up picker as the current date used when rendering date-related document field codes. If no selection is made here, the Native Image Date defaults to the current date (today's date). Microsoft Visio documents are incompatible with Native Image Date. If you configure this field on a profile that has linked time and date Application Field Codes, the linked Application Field Codes override the Native Image Date setting.

Spreadsheet Options (Native)

- **Paper size/orientation***—specify a paper size and orientation for your spreadsheet, the default for this field is set to **Original setting**. The options are:
  - **Original setting**
  - **Letter (8.5 in x 11 in)**
  - **Letter (11 in x 8.5 in)**
  - **Tabloid (11 in x 17 in)**
  - **Ledger (17 in x 11 in)**
- **Page Order***—determines the order used to render spreadsheets when data exceeds one page, the default for this field is set to **Original setting**. Options include:
  - **Original setting**—renders a spreadsheet based on the spreadsheet's original page setting.
  - **Down, then over**—renders a spreadsheet first from the top of the page to the bottom and then from the left to the right.
  - **Over, then down**—renders a spreadsheet first from the left of the page to the right and then from the top to the bottom.
- **Print Area***—override any pre-defined print area in an Excel file. When you select Ignore Print Area, Relativity images the entire document, the default for this field is set to **Ignore print area**. The options are:

    - **Original setting**—uses the original print area settings of the document.
    - **Ignore print area**—ignores the original print area settings of the document.
- **Hide and page break after _ consecutive blank rows and columns***—sets a maximum value for consecutive blank rows or columns. By default, the native imaging engine checks for a run of 10 blank rows or columns and compresses them to limit the number of pages rendered for a spreadsheet. The default for this field is set to **10**.
- **Show track changes in spreadsheet***—displays any modifications made to the document through the Track Changes option in Excel, the default for this field is set to **Yes**. The options are:
    - **Yes**—shows track changes.
    - **No**—doesn't show track changes.
- **Include row and column headings***—renders row and column headings (the number assigned to rows and the letters assigned to columns). The options are:
    - **Original setting** - uses the original row and column headings of the document.
    - **Yes** - renders the row and column headings.
    - **No** - doesn't render row and column headings.
- **Include comments***—determines whether Relativity renders comments found in the spreadsheet, the default for this field is set to **Yes**. The options are:
    - **Yes**—renders comment found in the spreadsheet. This is the value used in the Default profile.
    - **No**—doesn't render comments found in the spreadsheet.
- **Include headers and footers***—renders headers and footers in the spreadsheet. The printing of these items interferes with the ability of the native imaging engine to detect blank pages – for this reason, it's recommended that you leave this set to No, the default for this field is set to **Yes**. The options are:
    - **Original setting**—uses the original header and footer settings of the document.
    - **Yes**—renders the headers and footers of the document.
    - **No**—doesn't render the headers or footers of the document.
- **Include gridlines***—renders the gridlines between rows and columns in the spreadsheet, the default for this field is set to **Yes**. The options are:
    - **Original setting**—uses the original gridline settings of the document.
    - **Yes**—renders the gridlines between rows and columns in the spreadsheet.
    - **No**—doesn't render the gridlines between rows and columns in the spreadsheet.
- **Include borders***—renders the borders of the spreadsheet, the default for this field is set to **Yes**. The options are:
    - **Yes**—renders the borders of the spreadsheet.
    - **No**—doesn't render the borders of the spreadsheet.
- **Unhide hidden worksheets***—displays hidden worksheets, the default for this field is set to **Yes**.
- **Limit spreadsheet rendering to _ pages**—images only the whole number value of pages entered in this field's textbox. This value must be less than or equal to the maximum pages imaged per file value entered in the Native Imaging Options section above.

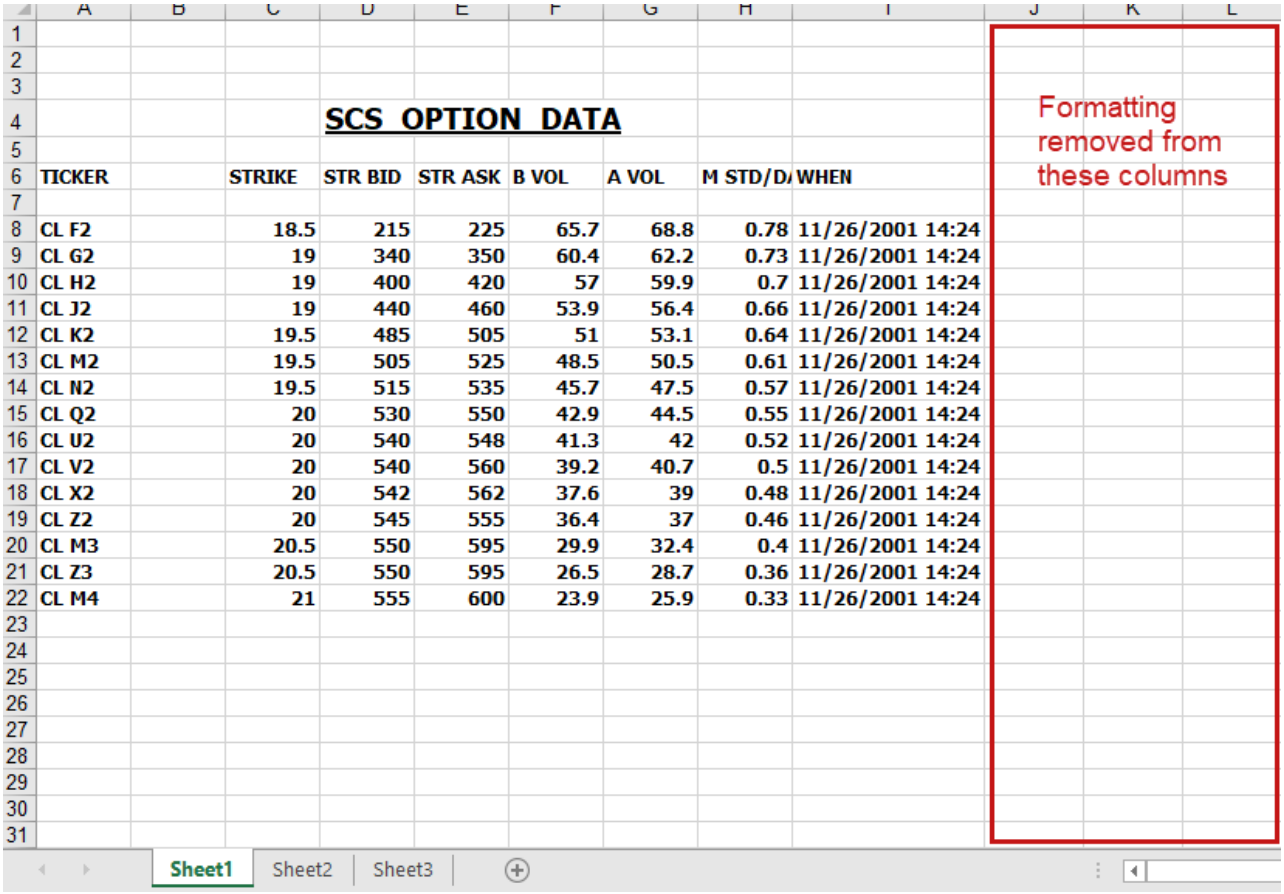
- **Zoom Level %** resets the zoom level for a spreadsheet. This value overrides the default settings internally stored in the file. The zoom level range is 10% - 400%.
- **Fit to _ pages wide**—resets the page width for a spreadsheet. This value overrides the default settings internally stored in the file.
- **Fit to _ pages tall**—reset the page height for a spreadsheet. This value overrides the default settings internally stored in the file.
- **Formatting**—determines the formatting of the spreadsheet with the following options:
  - **Auto-fit rows**—expands the dimensions of rows to accommodate their content. When you select these options, Relativity displays any hidden rows. This option is selected by default.
  - **Auto-fit columns**—expands the dimensions of columns to accommodate their content. When this option is selected, any hidden columns display. This option is selected by default.
  - **Clear formatting in empty rows**—clears the formatting from entire rows that do not have content in any of their cells and whose adjacent rows are both empty. This option does not remove the formatting from an empty cell that is a part of a row that has cells with content. With this option, the number of pages rendered is reduced.



TICKER	STRIKE	STR BID	STR ASK	B VOL	A VOL	M STD/D	WHEN
CL F2	18.5	215	225	65.7	68.8	0.78	11/26/2001 14:24
CL G2	19	340	350	60.4	62.2	0.73	11/26/2001 14:24
CL H2	19	400	420	57	59.9	0.7	11/26/2001 14:24
CL J2	19	440	460	53.9	56.4	0.66	11/26/2001 14:24
CL K2	19.5	485	505	51	53.1	0.64	11/26/2001 14:24
CL M2	19.5	505	525	48.5	50.5	0.61	11/26/2001 14:24
CL N2	19.5	515	535	45.7	47.5	0.57	11/26/2001 14:24
CL Q2	20	530	550	42.9	44.5	0.55	11/26/2001 14:24
CL U2	20	540	548	41.3	42	0.52	11/26/2001 14:24
CL V2	20	540	560	39.2	40.7	0.5	11/26/2001 14:24
CL X2	20	542	562	37.6	39	0.48	11/26/2001 14:24
CL Z2	20	545	555	36.4	37	0.46	11/26/2001 14:24
CL M3	20.5	550	595	29.9	32.4	0.4	11/26/2001 14:24
CL Z3	20.5	550	595	26.5	28.7	0.36	11/26/2001 14:24
CL M4	21	555	600	23.9	25.9	0.33	11/26/2001 14:24

  - **Clear formatting in empty columns**—clears the formatting from entire columns that do not have content in any of their cells and whose adjacent columns are both empty. This option does not remove the formatting from an empty cell that is a part of a column that has cells with content. With this option, the

number of pages rendered is reduced.



SCS OPTION DATA

TICKER	STRIKE	STR BID	STR ASK	B VOL	A VOL	M STD/D	WHEN
CL F2	18.5	215	225	65.7	68.8	0.78	11/26/2001 14:24
CL G2	19	340	350	60.4	62.2	0.73	11/26/2001 14:24
CL H2	19	400	420	57	59.9	0.7	11/26/2001 14:24
CL J2	19	440	460	53.9	56.4	0.66	11/26/2001 14:24
CL K2	19.5	485	505	51	53.1	0.64	11/26/2001 14:24
CL M2	19.5	505	525	48.5	50.5	0.61	11/26/2001 14:24
CL N2	19.5	515	535	45.7	47.5	0.57	11/26/2001 14:24
CL Q2	20	530	550	42.9	44.5	0.55	11/26/2001 14:24
CL U2	20	540	548	41.3	42	0.52	11/26/2001 14:24
CL V2	20	540	560	39.2	40.7	0.5	11/26/2001 14:24
CL X2	20	542	562	37.6	39	0.48	11/26/2001 14:24
CL Z2	20	545	555	36.4	37	0.46	11/26/2001 14:24
CL M3	20.5	550	595	29.9	32.4	0.4	11/26/2001 14:24
CL Z3	20.5	550	595	26.5	28.7	0.36	11/26/2001 14:24
CL M4	21	555	600	23.9	25.9	0.33	11/26/2001 14:24

- **Text Visibility**—determines the visibility of the text in a spreadsheet through the following options:
  - **Remove background fill colors**—removes background color and ensures that any hidden text or rows formatted to match the background color appear.
  - **Set text color to black**—displays the font color of text as black and ensures that any hidden text appears, such as text with a white font on a white background.

Note: If an Excel spreadsheet contains comments, those comments appear on a separate page after Relativity renders the spreadsheet. Also, native imaging clears any filters set in a spreadsheet.

Email Options (Native)

- **Orientation***—determines the orientation of the email when it's rendered, the default for this field is set to **Portrait**. The options are:
  - **Portrait**—selects a standard portrait display in which the height is greater than the width.
  - **Landscape**—selects a standard landscape display in which the width is greater than the height.
- **Resize images to fit page***—modifies the image sizes to make them compatible with the page size. Select Yes for resizing. Select No to prevent resizing. The default for this field is set to **Yes**.
- **Resize tables to fit page***—modifies the table sizes to make them compatible with the page size. Select Yes for resizing. Select No to prevent resizing. The default for this field is set to **Yes**.
- **Split tables to fit page***—wide tables are split and re-printed on a new line when they are imaged, so no content is lost. Select Yes to split tables. Select No to prevent table splitting. The default for this field is set to **Yes**.

- **Download images from Internet***—download images from the Internet. This option also applies for Word files. The default for this field is set to **Yes**.
- **Clear indentations***—removes the tabs from e-mail threads to improve their display. Select Yes to prevent the entries in the thread from aligning too far to the right. Select No to keep tabs in email threads. The default for this field is set to **No**.
- **Detect character encoding***—analyzes text in the email body to determine the best language encoding to use during imaging. Select Yes for the native imaging engine to determine the language encoding to use during imaging. Select No for the character encoding specified in the email header metadata to set the language encoding used during imaging. The default value is set to Yes.
- **Display SMTP addresses***—renders SMTP addresses for To, Cc, and Bcc fields instead of Microsoft Exchange information. Select Yes for rendering. Select No to prevent rendering. The default for this field is set to **No**.
- **Show message type in header***—adds text in the header identifying the image as a message, appointment, distribution list, etc. Select Yes for the addition of text. Select No to prevent the addition of text. The default for this field is set to **No**.

Note: MHT emails do not use Imaging Profile configurations. This is a known limitation of the format. MHT emails may not render correctly when imaged.

Word Processing Options (Native)

- **Show track changes***—renders any markups added to the document through the Track Changes feature in Word, the default for this field is set to **Yes**. The options are:
  - **Yes**—renders the document's markups.
  - **No**—doesn't render the document's markups. No is the default.
- **Page Orientation***—determines the rendered page orientation of Word files, the default for this field is set to **Original setting**.
  - **Original setting**—retains the original page orientation.
  - **Portrait**—renders the imaged Word file in portrait mode.
  - **Landscape**—renders the imaged Word file in landscape mode.
- **Show**—determines which additional document attributes to render. The options are:
  - **Full comments page** —appends an additional page at the end of the imaged document containing the complete list of all comments with their full text. Use this option to ensure no comment content is lost due to truncation in the side margin view. This option can be used alongside or instead of the Comments option.
  - **Comments**—renders any comments added to the document through the Review feature in Word. Comments appear in the side margin view.

    Note: Long comments may be shortened in the side margin view. To display complete comment text, enable the Full comments page option.
  - **Field codes**—renders the field that Microsoft Word used as a placeholder for potentially changing data rather than the actual data in the document. Selecting Show Field Codes shows all field codes when imaging Word documents with the native imaging profile. If any Word field codes associate with a rendering option other than Show Field Codes or Document Default are linked to the native imaging profile, that behavior overrides this setting. See Microsoft Word field code considerations.

- **Hidden text**—renders any comments or directions added to the text of a document through the Hidden text feature in Microsoft Word. Selecting this makes the hidden text specified in the Microsoft Word file visible in the same manner as the normally-entered text.

Note: Native imaging for Word documents generally replicates whatever Microsoft Word's Print Preview displays. This means that the imaged output may differ from what you see in the Native Viewer or Word's Print Layout view. For example, comments in Word documents may appear with full commenter names in the Native Viewer but display only initials or anonymized labels (such as "Comment") in the imaged output, depending on the document's internal privacy and metadata settings.
For some options, Relativity applies custom rendering logic rather than relying solely on Word's default Print Preview behavior. For example, when the Full comments page option is enabled in the native imaging profile, Relativity renders comments at the end of the document as separate pages.

For some imaging options, Relativity applies custom rendering logic rather than relying solely on Word's default Print Preview behavior. For example, when you enable the Full comments page option in Word Processing Options, Relativity renders comments at the end of the document as separate pages..

Microsoft Word Options (Basic)

- **Show Comments**—renders any comments added to the document through the Review feature in Word.
- **Show track changes**—renders any markups added to the document through the Track Changes feature in Word, the default for this field is set to **No**. The options are:
  - **Yes**—renders the document's markups.
  - **No**—doesn't render the document's markups.

Presentation Options (Native)

- **Show speaker notes***—renders the slide at the top of the page and the speaker's notes at the bottom. If you select Yes, the orientation of the presentation is portrait. If you select No, the orientation is landscape with the slide only. The default for this field is set to **Yes**.
- **Include PowerPoint Comments**—comments included in the original presentation will be rendered below each slide.
- **Slide Orientation***—determines the rendered page orientation of slide files. If you have "show speaker notes" selected, the image orientation is in portrait mode to accommodate the notes. The default for this field is set to **Original setting**.
- **Original setting**—retains the original page orientation.
  - **Portrait**—renders the imaged PowerPoint file in portrait mode.
  - **Landscape**—renders the imaged PowerPoint file in landscape mode.

Note: Native imaging unhides any hidden slides in a presentation.

PowerPoint Options (Basic)

- **Show speaker notes***—renders the slide at the top of the page and the speaker's notes at the bottom. If you select Yes, the orientation of the presentation is portrait. If you select No, the orientation is landscape with the slide only. The default for this field is set to **Yes**.
- **Comments**—renders any comments added to the document through the Review feature in PowerPoint.
- **Comments**—renders any comments added to the document through the Review feature in PowerPoint.

HTML Options (Native)

- **Remove non-breaking space (NBSP) codes***—removes long rows of non-breaking spaces (NBSP) codes. These prevent the text from wrapping properly. Native imaging automatically formats page breaks without cutting text or margins when rendering HTML as PDF. The default for this field is set to **No**.

PDF Options (Basic)

- **PDF Include Comments***— allows comments to be automatically captured during PDF imaging.

13.5.3 Native file imaging profile validation

Native imaging profiles must follow specific validation guidelines. Imaging profile validation reviews the following rules for all Native Imaging Engine Options:

- **Valid numerical values**—numerical values fit within a designated range based on individual numerical field requirements
- **Configuration specific to format type**—option selections and requirements vary based on the Native Image Format selection
- **Field dependencies**—specific fields require additional field configurations to satisfy groups of settings available for native imaging, and specific fields are ignored based on the configuration of a related field

Native File Imaging profile validation only runs when using the default **Native Imaging Profile Layout** for new imaging profiles.

13.5.3.1 Numerical Field Values

The following table provides valid numerical value ranges and recommended values for select numerical configuration fields. Valid value ranges include the minimum and maximum values provided.

Field	Minimum Value	Maximum Value	Recommended Value
Native Image Output Quality (DPI)	0	2400	300
Dithering Threshold	0	255	128

13.5.3.2 Format Specific Requirements

The following table states whether a field is set required or ignored based on the selected Native Image Format. If applicable, select the required field value.

Native Imaging Format	Field	Field Required/Ignore	Required Field Value (if applicable)
JPEG	Images/Dithering Algorithm	Ignored	
JPEG	Dithering Threshold	Ignored	
JPEG	Render color pages to JPEG	Ignored	
TIFF	Images/Dithering Algorithm	Required	
TIFF	Render color pages to JPEG	Required	Yes

13.5.3.3 Field Dependencies

The following table lists field dependencies and required field values if applicable. The Field 1 and Field 1 Value columns list fields and values that require you to configure the fields and values listed in the Required Field 2 and

Required Field 2 Value columns.

For example, if Images/Dithering Algorithm is set to Threshold, you must configure a value for the Dithering Threshold field.

Field 1	Field 1 Value	Required Field 2	Required Field 2 Value
Images/Dithering Algorithm	Threshold	Dithering Threshold	<any>
Dithering Threshold	<any>	Images/Dithering Algorithm	Threshold
Fit to ___ pages wide	<any>	Fit to ___ pages tall	<any>
Fit to ___ pages tall	<any>	Fit to ___ pages wide	<any>

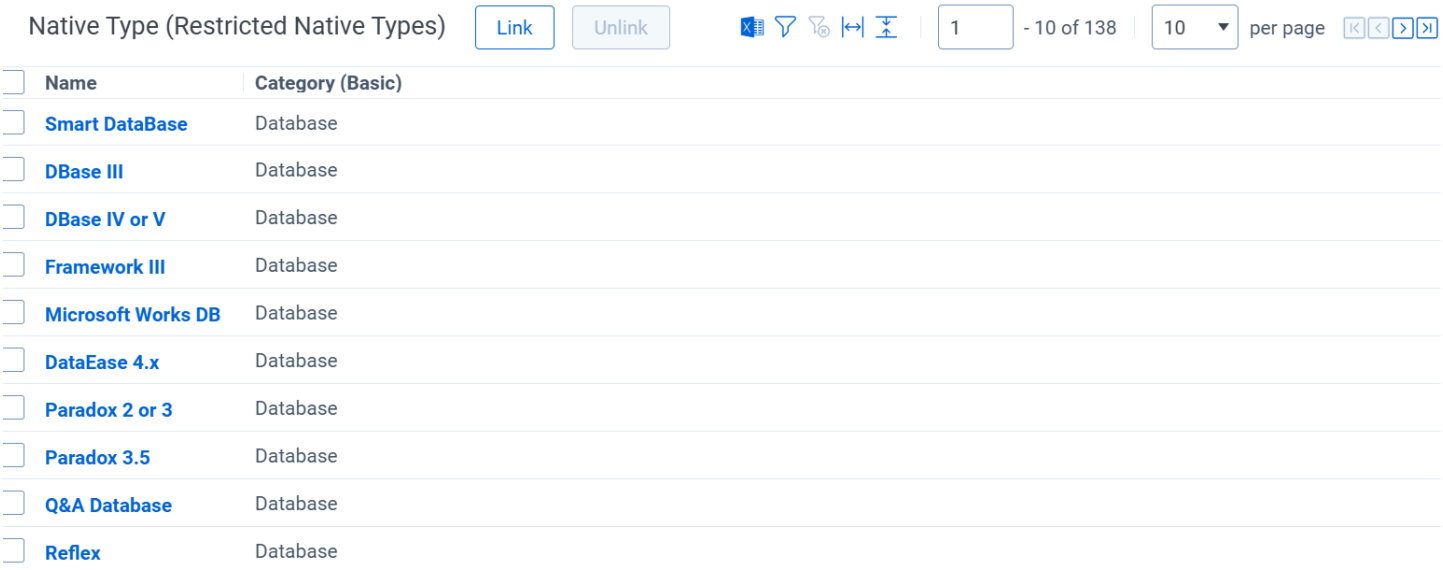
When fields in the Field Set column are configured, values set for fields listed in the Field Ignored column are ignored:

Field Set	Field Ignored
Zoom Level %	Fit to pages ___ wide
Zoom Level %	Fit to pages ___ tall
Fit to ___ pages wide	Zoom Level %
Fit to ___ pages tall	Zoom Level %

Note: With validation rules you can only configure Zoom Level % or the set of Fit to ___ pages fields. Don't set values for all three fields.

13.5.4 Viewing imaging profile details

On the Imaging Profile Details page, Relativity displays profile settings and a list of restricted native type files.



13.5.4.1 Restricted native types

The Restricted Native Types section lists the file formats that Relativity won't convert into images. It also includes features that you can use to modify this list. You see the following columns and options displayed in the Restricted Native Types section:

- **Name**—lists file formats.
- **Category (Basic)**—indicates a grouping of related file types or formats. For example, Word Processor is the category for common word processing formats such as Word, WordStar, WordPerfect, and others. (Additional super types are Database, Spreadsheet, Graphic, Multimedia, and Other.)
- **Link**—adds existing native types to the restricted list through the Select Items pop-up.
  Select one or more file types in the Available Items list, click **Add** to include them in the Select Items list, and then click **Set** to link them to the profile.

Note: You can't add new native file types to Relativity. For a list of native types that Relativity supports, see the Native Types tab or Viewer-supported file types on page 759. Contact Support if you have additional questions about supported native types.

- **Unlink**—removes restricted native types from the list. When you use this profile, Relativity images these documents.
  Select one or more file types, and click **Unlink**.
- **Resize, export, filter—**  —resize columns, export, and filter the list of restricted native types. These features function similarly to those available on views.
- **Export the list**  —creates a list of restricted native types in Excel.

13.5.4.2 Application field codes

Application Field Codes is how Relativity refers to fields that Microsoft documents use to store document data. For example, [Date] is a field code in Microsoft that shows the date of document creation. Excel and PowerPoint refer to these fields as header and footer, Word refers to them as field codes, and Visio refers to them as fields. But for simplicity, Relativity refers to them as field codes, regardless of which Microsoft application document you're viewing.

When imaging Microsoft application documents in Relativity, field codes embedded within a document can contain incorrect or irrelevant information. The imaged field code functions as it should, but instead of using the original Date, for example, the field code captures the date the document was imaged within Relativity instead of the date the document was actually created. By creating Application Field Codes in Relativity, however, you can determine how various field codes appear on imaged documents.

Relativity comes with 17 of the most commonly-used field codes automatically linked to the default native imaging profile with the most common rendering options supported. You can edit these linked field codes or remove them from the default native imaging profile based on your rendering preferences. You can also add additional field codes to Relativity beyond the 17 we include.

Note: Application Field Codes are only configurable with native imaging.

For more information on Application Field Codes and how to link them to native imaging profiles, see Application Field Codes.

13.6 Imaging sets

An imaging set consists of an imaging profile and a saved search containing the documents you want to image. You run the imaging job from the imaging set console. In addition, on the Imaging Set Details page, you can view document-level error messages and rerun an imaging job if it failed.

Note: The (Admin) Errors tab has been permanently removed from Relativity aiR, and the ability to read errors through the API has been disabled. Job-specific errors are now addressable directly within your workspaces. For more information, see Errors tab deprecation.

13.6.1 Imaging set workflow

To image a group of documents using an imaging set, complete the following steps in order:

1. Create a saved search containing the documents you want to image. You will select this saved search as the data source when creating the imaging set.
2. Create an imaging profile that defines how the images are generated, or use an existing profile.
3. Create an imaging set that references the saved search and the imaging profile.
4. Run the imaging job from the imaging set console.

After the imaging job is complete, reviewers can view, redact, and apply markups to the images in the viewer.

13.6.2 Creating and editing an imaging set

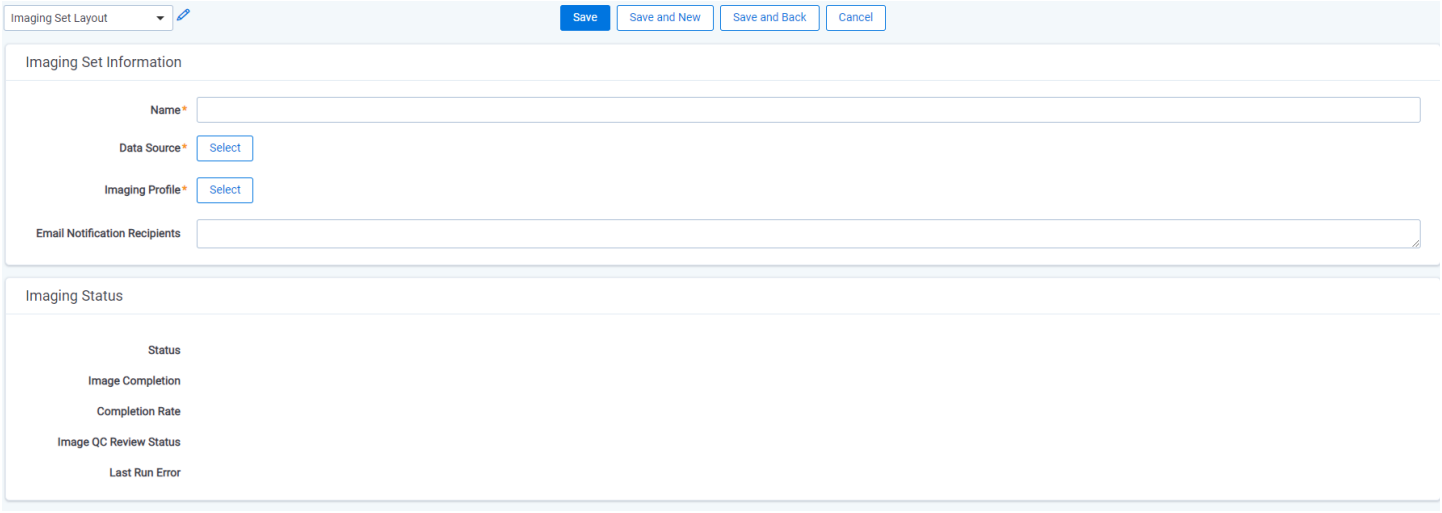
Note: To run an imaging set, you must install the Imaging Request and Imaging Response agents. The standard configuration is 4 Imaging Response agents. The maximum recommended number is 8; exceeding this limit can cause database issues. For installation and activation details, see Imaging.

To create or edit an imaging set:

1. Navigate to the **Imaging** tab, and then click **Imaging Sets** in a workspace.
2. Click **New Imaging Set**.
   The Imaging Set Form appears.
3. Complete all required fields. See Fields for details.
4. Click **Save.** The saved set layout provides the set details and the imaging set console, from which you run the imaging job.

13.6.3 Fields

The imaging set form contains the following fields:



Imaging Set Information

- **Name** — The name of the imaging set.
- **Data Source** — A saved search containing the documents to image. Only documents in the saved search are imaged.
- **Imaging Profile** — A predefined set of parameters that controls how images are generated. The list that appears when you click the ellipsis includes both Native and Basic profiles.
- **Email Notification Recipients** — The email addresses of users who should receive notification when the following processes complete within the imaging job. Separate multiple email addresses with a semicolon.
    - Imaging set completed successfully
    - Imaging set completed with errors

Imaging Status

- **Start Time** — Appears when either of the following conditions is met:
    - The imaging set is in the Submitting status.
    - The imaging set is in the Imaging status and the job has started.
- **Status** — The current state of the imaging job. This field refreshes automatically to show progress. The value changes based on issues encountered during the job. The possible values are:
    - **Staging** — The job has started, but no documents from the imaging set have been processed yet.
    - **Preparing files** — Relativity is preparing files for submission by splitting them into batches, creating data tables, and getting them ready for imaging. A percentage tracker reflects the progress of this status.
    - **Submitting** — Documents are being submitted to the queue and prepared for imaging. A percentage tracker reflects the progress of this status.
    - **Imaging** — The imaging job is currently running. A percentage tracker reflects the progress of this status.
    - **Completed** — The last document in the set has been processed and no job remains in the ImagingJob database table.
    - **Completed with Errors** — The last document in the set has been processed, errors occurred during the job, and no job remains in the ImagingJob database table. You can view document-level error details on the Imaging Set Details page.
    - **Skipped** — The document was not submitted for imaging. Documents may be skipped if they have unsupported file types that cannot be converted to images.

      Note: In Automated Workflows, documents with a Skipped status due to unsupported file type errors are automatically excluded from subsequent imaging runs. This prevents redundant processing attempts on files that cannot be imaged. Manual imaging sets include all documents from the saved search, allowing you to retry if needed.
    - **Stopped** — The imaging set was stopped by Relativity.
    - **Stopped by User** — The imaging set was manually stopped by the user through the Stop Imaging button on the console.
- **Image Completion** — Refreshes automatically to show progress. Lists the following information:
    - **# documents pending submission** — The number of documents from the imaging set that have not yet been submitted for imaging.
    - **# documents submitted** — The number of documents that have been submitted for imaging.

- **# documents remaining** — The number of documents that do not yet have a status of Imaged, Errored, or Skipped. This number starts at the total document count and decreases as the imaging job progresses.
- **# documents successfully imaged** — The number of documents imaged by the worker manager server without errors.
- **# documents with errors** — The number of documents that were submitted to the worker manager server and received an error during imaging.
- **# documents skipped** — The number of documents from the imaging set that were never submitted to the worker manager server for imaging.

- **Completion Rate** — Lists the following information:
  - **# documents submitted per hour** — During the submission phase, the average number of documents submitted to the worker manager server per hour. This value is calculated by normalizing the number of documents submitted over a 10-minute interval and scaling up to an hour.
- **Image QC Review Status** — The number of documents set to be hidden from QC review, based on your selection for the Hide Images for QC Review option after clicking Image Documents on the console. This field also lists the number of documents that currently have viewable images.
- **Last Run Error** — The date and time of the last error.

13.7 Image upload

Use the image upload feature to upload a single image for a document record directly in the viewer.

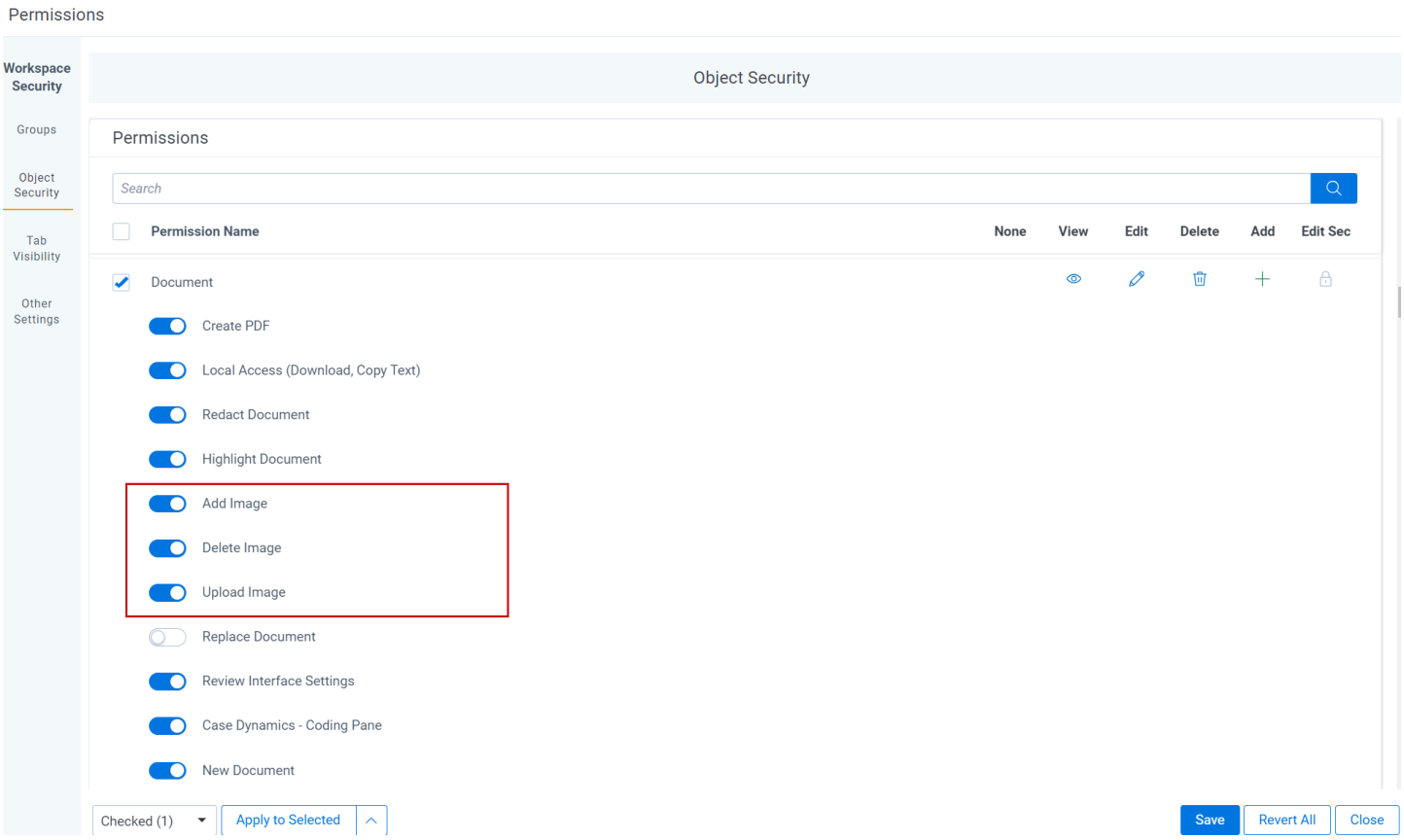
With this feature, you're able to upload the following file types:

- GroupIV TIFF
- JPEG
- PDF

13.7.1 Required security permissions

To use the image upload feature, you must have the following permissions enabled in the Object Security console:

- Upload Image
- Add Image
- Delete Image

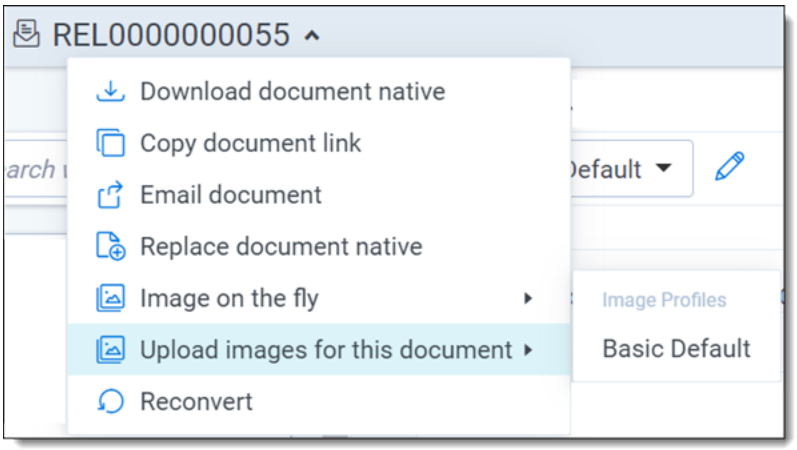


13.7.2 Uploading an image

You can upload a single image for a document record directly in the viewer.

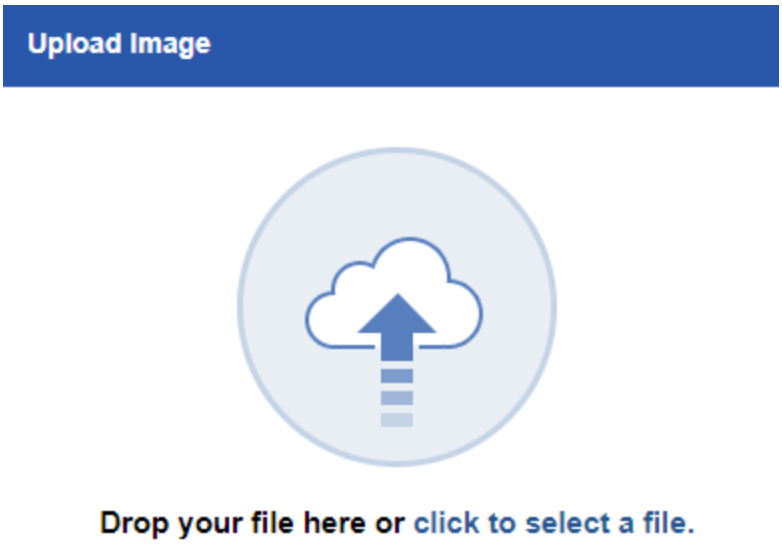
To upload an image:

1. In the viewer, click the file name.
2. Select **Upload images for this document**.



3. In the menu, select the imaging profile you want to use. For more information, see Imaging profiles on page 240

4. In the upload window, select **click to select a file** to browse for the image, or drag a file from your local machine and drop it into the upload window.



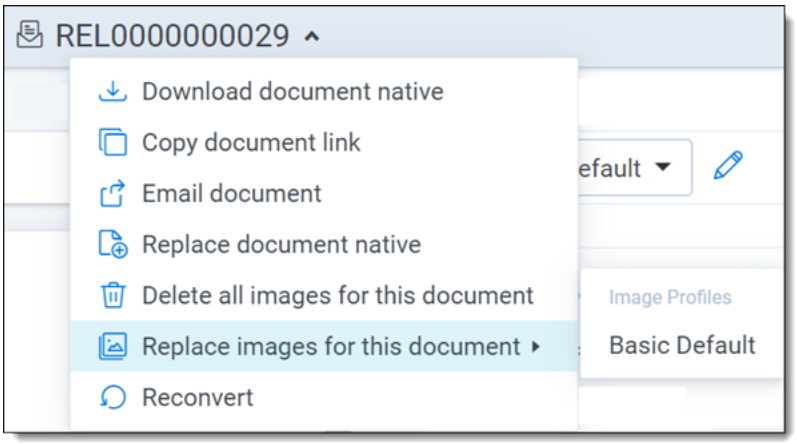
Relativity automatically begins to upload the file after you select it. When the upload is complete, the image appears in the viewer.

13.7.3 Replacing an image

If an image already exists for a document, you can replace it.

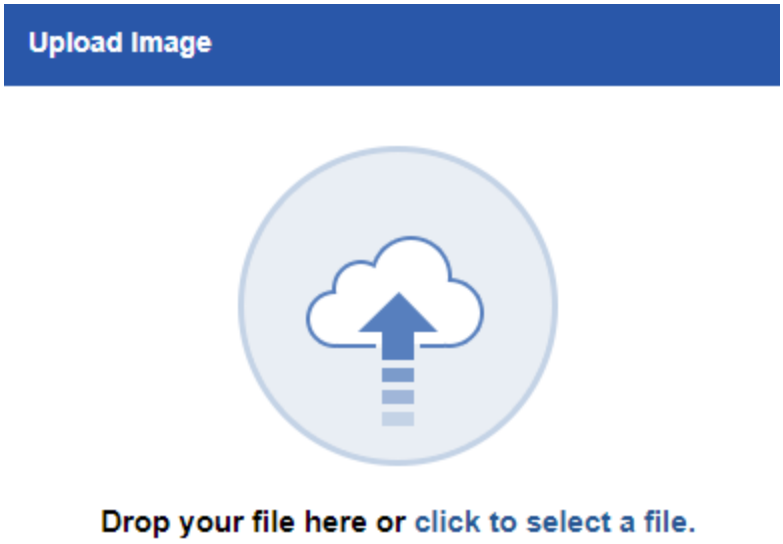
To replace an existing image:

1. In the viewer, click the document name.
2. Select **Replace images for this document**.



3. In the menu, select the imaging profile you want to use.
4. In the upload window, select **click to select a file** to browse for the image, or drag a file from your local

machine and drop it into the upload window.



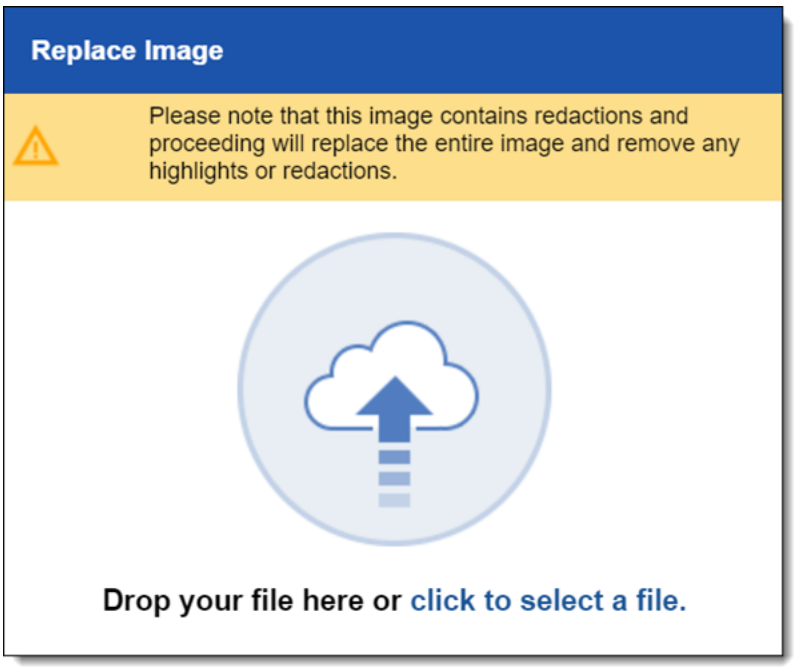
Note: Replacing an image replaces the entire document's images, not a single page. For example, uploading a JPG or TIFF file results in one image regardless of how many pages the original document had. Uploading a 5-page PDF file results in 5 images.

Relativity automatically begins to upload the file after you select it. When the upload is complete, the image appears in the viewer.

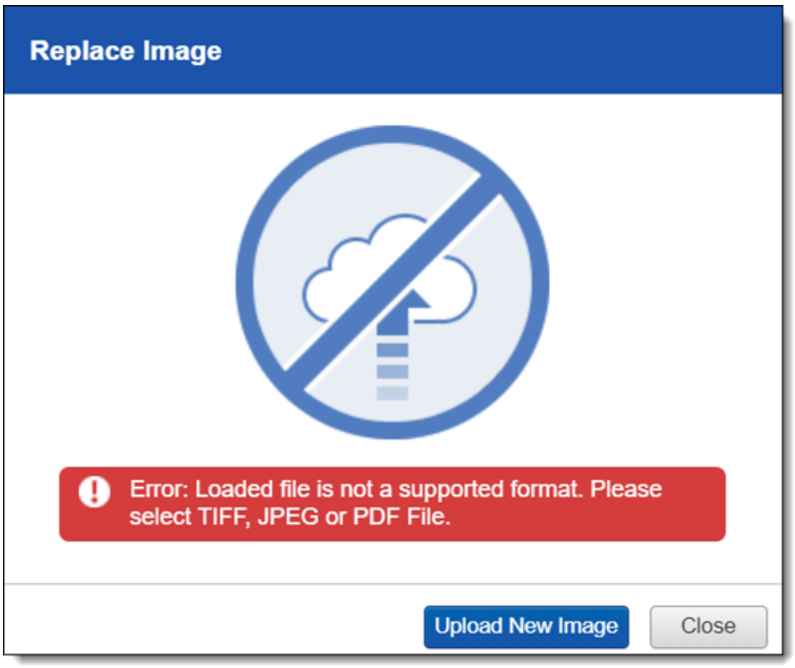
13.7.4 Warnings and error messages

If you have redacted or added highlights to an image in the viewer and then attempt to upload a new image, a message appears informing you that replacing the image will remove those redactions or highlights.

Note: Replacing an image that has redactions updates the Has Redactions field to No and removes all existing redactions and markup.



If you attempt to upload an unsupported file type, you'll receive an error message.



From here, you can click **Upload New Image** to select a new image to upload.

13.7.5 Audits for image upload

The following audit events are recorded when a user performs image upload actions in the viewer.

- **Images - Created** — The user uploaded an image for a document in the viewer.
- **Images - Deleted** — The user deleted an image from the viewer.

13.8 Application Field Codes

Application Field Codes is how Relativity refers to fields that Microsoft documents use to store document data. For example, [Date] is a field code in Microsoft that shows the date of document creation. Excel and PowerPoint refer to these fields as header and footer, Word refers to them as field codes, and Visio refers to them as fields. But for simplicity, Relativity refers to them as field codes, regardless of which Microsoft application document you're viewing.

When imaging Microsoft application documents in Relativity, field codes embedded within a document can contain incorrect or irrelevant information. The imaged field code functions as it should, but instead of using the original Date, for example, the field code captures the date the document was imaged within Relativity instead of the date the document was actually created. By creating Application Field Codes in Relativity, however, you can determine how various field codes appear on imaged documents.

Relativity comes with 17 of the most commonly-used field codes automatically linked to the default native imaging profile with the most common rendering options supported. You can edit these linked field codes or remove them from the default native imaging profile based on your rendering preferences. You can also add additional field codes to Relativity beyond the 17 we include.

Note: Application Field Codes are only configurable with native imaging.

13.8.1 Application Field Codes in Relativity

Use the following table to view the 17 Application Field Codes that come with Relativity. An asterisk denotes the default rendering behavior.

Field Code	Supported Rendering Options			
	Show Field Code	**Show Nothing**	**Document Default**	**Replace with Relativity Field**
Microsoft Word				
Date	✓*	✓	✓	✓
FileName	✓	✓	✓*	✓
NumPages	✓	✓	✓*	✓
Pages	✓	✓	✓*	✓
Time	✓*	✓	✓	✓
Microsoft Excel				
Date	✓*	✓	✓	✓
File	✓*	✓	✓	✓
Page	✓	✓	✓*	✓
Pages	✓	✓	✓*	✓
Path	✓*	✓	✓	✓
Time	✓*	✓	✓	✓
Microsoft Powerpoint				
DateTime	✓*	✓	✓	✓
Footer	✓	✓	✓*	✓

Field Code	Supported Rendering Options			
	Show Field Code	Show Nothing	Document Default	Replace with Relativity Field
Slide Number	✓	✓	✓*	✓
Microsoft Visio				
Directory	✓*	✓	✓	✓
FileName	✓*	✓	✓	✓
Now	✓	✓	✓*	✓

Note: For PowerPoint, Relativity only supports field codes for headers and footers. Field codes for speaker notes and text boxes are not supported.

If you need to add field codes beyond the 17 that come pre-loaded, Relativity provides additional field codes you can select via a pop-up picker or enter manually. Those field codes are:

Field Code	Supported Rendering Options				Relativity Availability	
	Show Field Code	Show Nothing	Document Default	Replace with Relativity Field	*Popup Picker*	*Manual Entry*
Microsoft Word						
Author	✓	✓	✓	✓	✓	✓
Citation		✓	✓			✓
CreateDate	✓	✓	✓	✓	✓	✓
Embed			✓			✓
Link			✓			✓
PrintDate	✓	✓	✓	✓	✓	✓
SaveDate	✓	✓	✓	✓	✓	✓
Microsoft Excel						
Picture	✓	✓	✓	✓	✓	✓
Tab	✓	✓	✓	✓	✓	✓
Microsoft Visio						
DocCreation	✓	✓	✓	✓	✓	✓
DocLastEdit	✓	✓	✓	✓	✓	✓
DocLastPrint	✓	✓	✓	✓	✓	✓
PageCount	✓	✓	✓	✓	✓	✓
PageNumber	✓	✓	✓	✓	✓	✓

Please note that Relativity currently does not support the following Microsoft Word field codes:

- AutoNum
- AutoNumLgl Time

- AutoNumOut
- Custom
- GoToButton
- IncludePicture
- MacroButton
- PageRef
- Seq

13.8.2 Application Field Code formats

If you want to add field codes beyond the 17 that come with Relativity or the field codes available in the pop-up picker, you can manually enter the field code for each Microsoft application. Code means any string of non-special characters, for example, DateTime.

Microsoft Word format
Acceptable formats are {Code}, [Code], and Code.

Microsoft Excel format
Acceptable formats are [Code], Code, &Code, &[Code].

Microsoft PowerPoint format
Acceptable formats are [Code] and Code.

Microsoft Visio format
Acceptable formats are [Code] and Code.

13.8.3 Creating or editing an Application Field Code

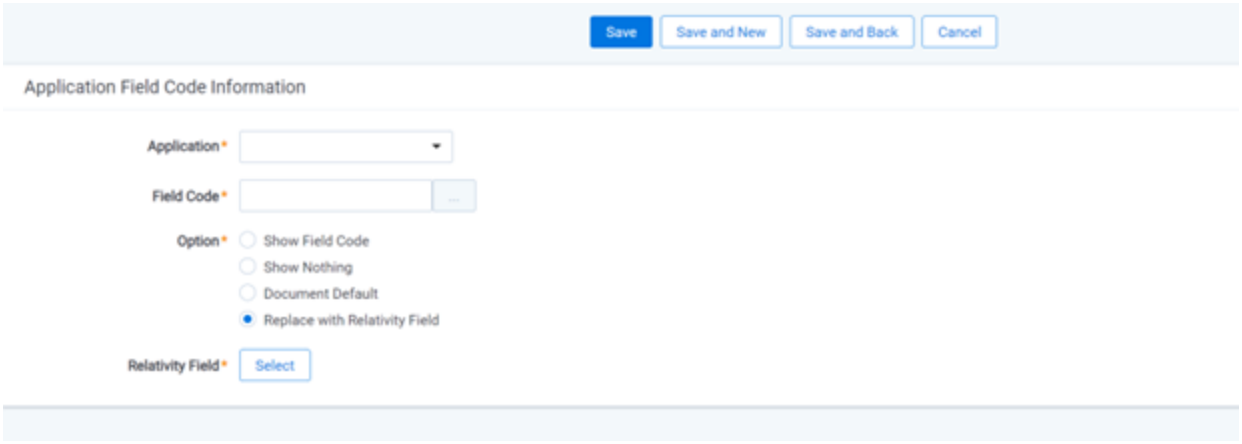
You can create a field that's available in the pop-up picker, create a field code that isn't available already in Relativity, or edit one of the pre-loaded 17 field codes or a field code you've already created. To create a new Application Field Code:

Note: When creating Application Field Code RDOs, when the option is Relativity Field, you cannot use the following system fields: System Modified By, System Created By, or Folder Name.

1. In a workspace, navigate to the **Job Admin** tab and select the **Application Field Code** tab.
2. Click **New Application Field Code**, or click the **Edit** link of an existing Application Field Code. The Application Field Code Information layout opens.
3. Complete all required fields. See Fields below for details.
4. Click **Save**.

13.8.4 Fields

The Application Field Code Information fields are:



- **Field Code** - The field code that appears on your document set. Click ... to see a full list of available field codes. See Application Field Codes on page 259 for details.

  Note: You can add a field code to your imaging profile even if the field code isn't a part of the default or available lists. See Application Field Code formats on the previous page for details.

- **Application** - The application used to create the documents. This field automatically populates once a field code is selected.
- **Option** - The way field codes render on the imaged document set.
  - Select from the following options:
    - **Show Field Code** - This option displays the field code in the imaged document.
    - **Show Nothing** - This option hides the selected field code in the imaged document.
    - **Document Default** - This option applies the default setting of the document to the field code in the imaged document.
    - **Replace with Relativity Field** - This option replaces the selected field code text with a Relativity date, fixed-length, or whole number field value that you choose in the imaged document.
- **Relativity Field** - The Relativity field value to replace the selected field code text. This option is required when Replace with Relativity Field is selected.

13.8.5 Linking an Application Field Code to a native imaging profile

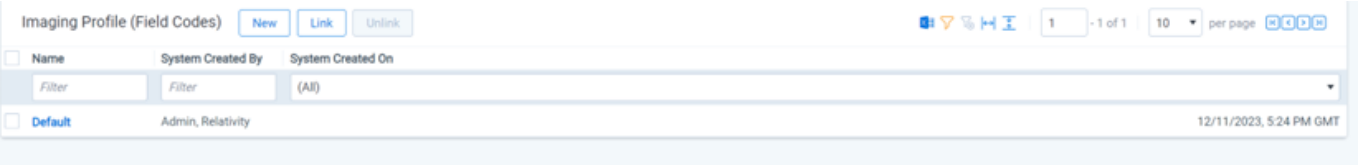
Note: View permission needs to be selected on Application Field Code for the Application Field Code layout to display in the imaging profile page.

Once you create your Application Field Code, link the field code to the appropriate native imaging profile. This is only required if you create a new Application Field Code that isn't linked to a native imaging profile by default. The Imaging Profile (Field Codes) section lists the available native imaging profiles in a workspace.

To link an Application Field Code to an existing native imaging profile:

1. Click **Link**. The Select Items - Imaging Profile (Field Codes) popup picker opens.
2. Select the imaging profile where you want to link the Application Field Code.
3. Click **Add**.

4. Click **Set**.



13.9 Running an imaging set

To run an imaging set, click **Image Documents** on the imaging set console. This kicks off the conversion of documents to images. While the job is running, this button toggles to **Stop Imaging**. Use the Stop Imaging button to stop the imaging job. With the Image Documents Options prompt you can Hide Images for QC Review. See QC Review on page 278 for more information.

13.9.1 Special considerations

Keep in mind the following special considerations:

- A single imaging set can support up to 1,000,000,000 documents. Exceeding this limit will result in job failure.
- You can't delete an imaging set while it is running.
- Imaging Sets will not re-image documents that already have an image.
- Frequent worker updates can result in minor inconsistencies if files are imaged days apart using Native Imaging.

13.9.1.1 Extracted text validation

When you run native imaging, Relativity performs an extracted text validation step after imaging completes. This validation compares the extracted text from the source document with the text extracted from the intermediate PDF to identify possible missing text.

If the validation detects potentially missing text, a document-level warning is generated with the message "Possible missing extracted text on images." This warning is informational only and does not cause the imaging job to fail.

Keep the following in mind:

- The validation is limited to the first 50,000 characters of extracted text.
- False positives can occur when words merge in the intermediate PDF due to low-contrast formatting in the source file.

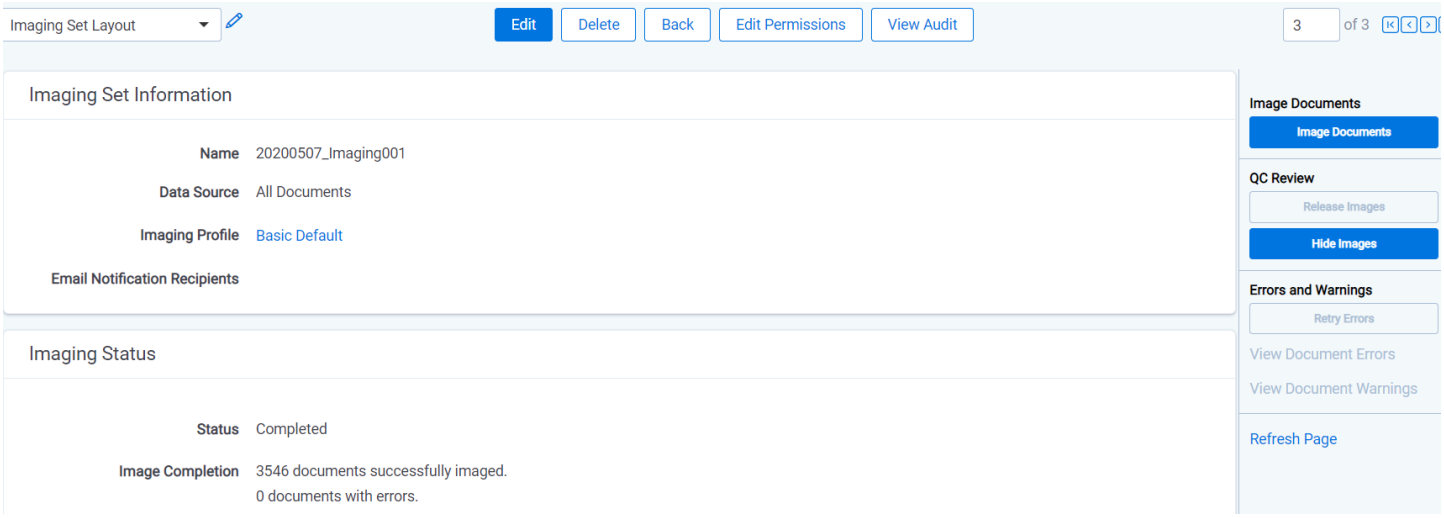
To view warnings generated during the imaging job, click View Document Warnings on the imaging set console. For more information, see Imaging warnings.

Note: When you run native imaging on files, Relativity validates extracted text by comparing the source document text with text from the intermediate PDF. If text appears missing, a document-level warning ("Possible missing extracted text on images") is generated. This warning is informational only and does not fail the imaging job. The validation is limited to the first 50,000 characters. For details, see Imaging Warnings.

13.9.2 Unsupported file types

Documents with unsupported file types receive a *Skipped* status and will not be imaged. When using Automated Workflows, these documents are automatically excluded from subsequent imaging runs to optimize processing efficiency.

13.9.3 Imaging Set console



Depending on the progress of the job, the following options are available on the console:

- **Image Documents** - begins the imaging job.
- **Release Images** - allows users to see the images after the QC review process is complete.
- **Hide Images** - prevents users from viewing the images until the QC review process is complete.
- **Retry Errors** - reruns documents with imaging errors. This is only enabled if errors have occurred during the imaging job.

  Note: Retry Errors will use the same imaging profile the documents with imaging errors were created with, even if the imaging profile is changed.

- **View Document Errors** - redirects you to the Imaging Document Error tab, where the results are filtered by all imaging errors associated with the documents in the imaging set. You can expand the results by modifying the filters.
- **View Document Warnings** - redirects you to the Imaging Warnings tab, where the results are filtered by all Imaging Warnings associated with the documents in the imaging set. You can expand the results by modifying the filters.
- **Show Errors** - provides the option to view document-level errors for an imaging set run prior to September 2018. When you click this button, a pop-up displays a filterable list of documents and fields. The fields include:
  - **Control Number** - the control number of the item in error.
  - **Artifact ID** - the artifact ID of the item in error.
  - **File Type Identification (Native)** - the file type of the item in error as identified by the native imaging engine. This is only populated if the native imaging engine runs the imaging set.
  - **File Type Identification (Basic)** - the file type of the item in error as identified by the basic imaging engine. This value is populated when the basic engine identified the document when you import the document into Relativity.
  - **Imaging Method** - the method selected in the Native Types table for the identified file type in error – Basic or Native.
  - **Actual Imaging Method** - the method that was used to image the item in error – Basic or Native.

- **Message** - the description of the cause of the error.
- **Full Text** - the complete error text string the system provides, including stack trace.

- **Refresh Page** - refreshes the page and see the current state of the imaging job.

Note: When you mass image, image on the fly, run an imaging set, and retry an imaging set, the list of passwords specified in the password bank accompanies the imaging job so that password-protected files are imaged in that job. For more information see Password Bank in the Processing User Guide.

13.9.4 Imaging profile caching

Relativity caches all imaging profile settings until the imaging job you kick off through the imaging set console completes. The only exceptions to this are the following scenarios:

- In the case of fatal errors, the imaging profile information remains cached until you delete the set or you delete the job record associated with that set from the ProcessingQueue table.
- In the case of non-fatal errors, Relativity no longer caches all profile information except for the Time Zone and Last Modified Date information.

13.9.5 Password Bank

The Password Bank stores passwords used to protect certain files. When you process or image files protected by the passwords in this bank, Relativity sends the passwords to the respective engine, which then uses them to unlock the corresponding file.

Notes:

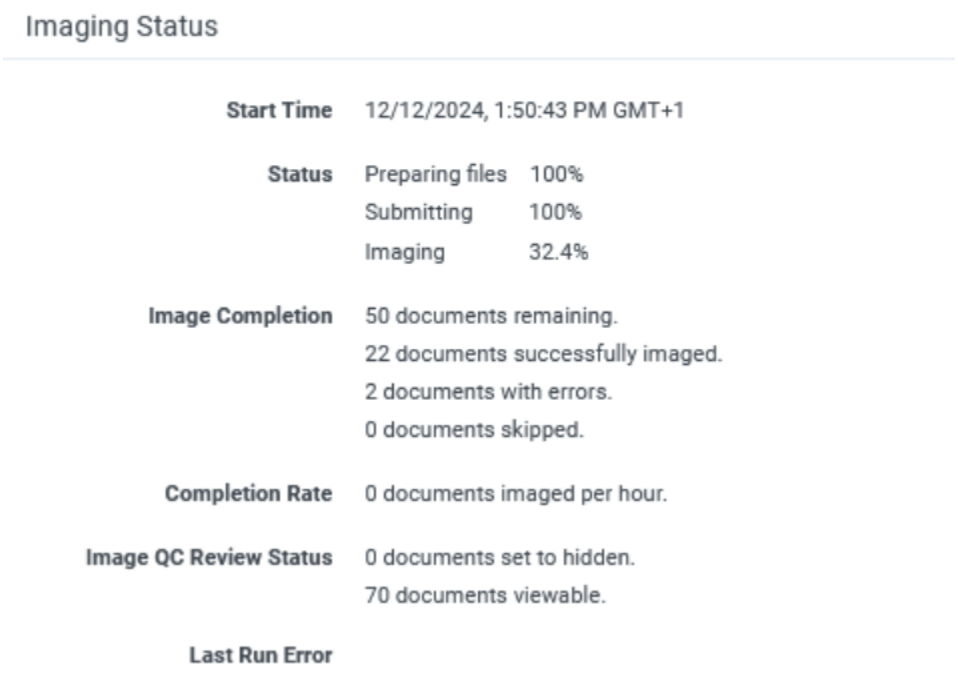
- The Password Bank tab appears under both the Imaging and the Processing applications and is updated in each to reflect the most current entries are added, deleted, or edited.
- Save as PDF does not integrate with the Password bank. If you select Save as PDF when imaging a native document that is password protected, an error occurs.

For more information see Password Bank in the Processing User Guide.

13.10 Monitoring imaging status

Use the Imaging Status section to monitor the progress of an imaging job. To update the status information, click Refresh Page on the imaging set console. Status information is also available in the default Imaging Set view.

The Imaging Status section provides the following fields:



- **Start Time** — Displays the start time and date of the imaging set. This field is visible only when the imaging set is in Submitting or Imaging status.
- **Status** — Provides any of the following values, depending on the imaging job in the imaging status section and in the default Imaging Set view:

Status	What happened	What it means
Staging	User clicked Image Documents.	The job is in the queue. The imaging set is awaiting execution.
Preparing files	The Imaging Request Agent began preparing files.	Relativity is splitting files into batches and preparing them for the imaging job. A percentage tracker displays the progress.
Submitting	The Imaging Request Agent began submitting documents to the Imaging Queue.	Relativity is creating the imaging job and submitting documents to the queue. A percentage tracker displays the progress.
Imaging	All documents have been submitted to the Imaging Queue.	Relativity is creating images of the documents. A percentage tracker displays the progress.
Completed	The job completed.	All documents were imaged successfully.
Completed with errors	The job completed with imaging errors.	One or more documents encountered an error during imaging.
Error - Job Failed	The job manager encountered an exception.	The job manager terminated the imaging job.
Stopping	User clicked Stop.	The Imaging Queue is stopping worker jobs. Documents are being updated so that Has Images is set to No.
Stopped by user	The job stopped.	All worker agents have stopped imaging documents. The job manager has stopped the job.

- **Image Completion** — Displays the number of remaining documents, successfully imaged documents, documents with errors, and skipped documents.
- **Completion Rate** — Displays the rate at which documents are submitted or imaged, expressed as documents per hour.
- **Last Run Error** — Displays the error from the most recently completed job that ended with errors.

Note: During imaging, Relativity skips documents that already have images, documents with restricted native types, and documents with images in a pending state (that is, documents with the Has Images field set to Yes). These documents are included in the skipped documents count.

Note: Delete an imaging set only when it has one of the following statuses:

- Stopped by user
- Error - Job Failed
- Completed with errors
- Completed

13.11 Imaging errors

This topic describes document-level imaging errors, where they appear, and how to resolve them.

13.11.1 Viewing imaging errors

To view document level imaging errors, go to the **Imaging Document Errors** tab. The Imaging Document Error tab contains all imaging error history, including errors that are resolved.

The tab includes the following error names:

- Document Type is not supported.
- OI EXOpenExport failed - 11: file is password protected or encrypted.
- OI EXOpenExport failed - 4: no filter available for this file type.
- OI EXOpenExport failed - 9: file is corrupt.
- OI EXOpenExport failed - 10: file is empty.

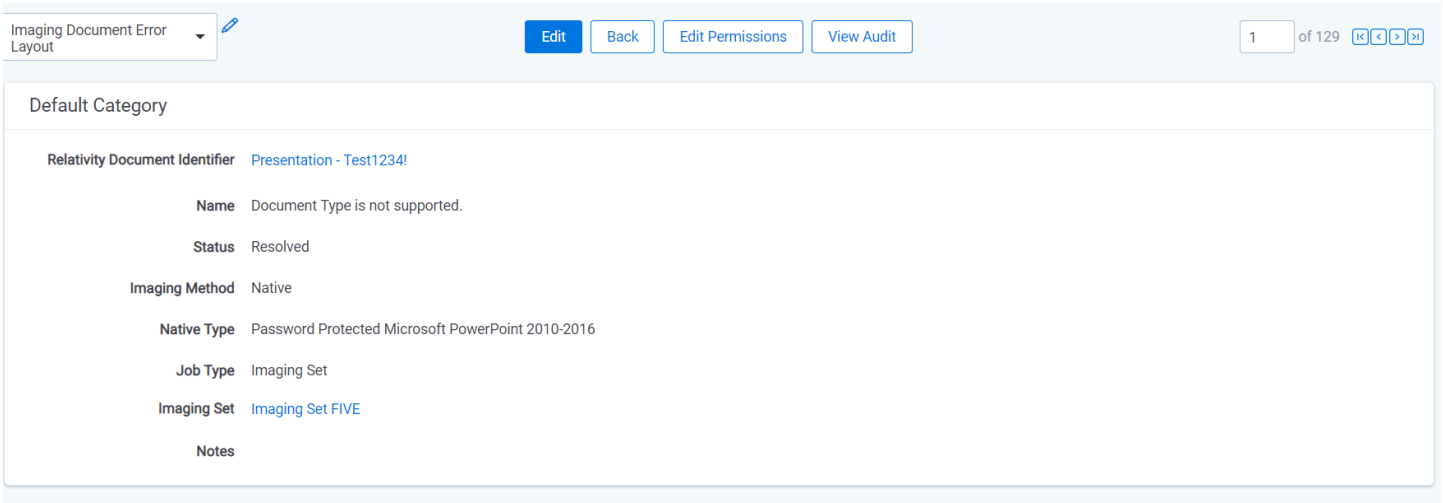
#	Relativity Document I...	Name	Status	Job Type	Imaging Set	Imaging Method	Native Type
	Filter	Filter	(All)	(All)	Filter	(All)	Filter
1	Presentation - Test1234!	Document Type is not s...	Resolved	Imaging Set	Imaging Set FIVE	Native	Password Protected Microsoft PowerPoint 2010-2016
2	PasswordProtectedExcel2007preSP1 - Test1234!	Document Type is not s...	Resolved	Imaging Set	Imaging Set FIVE	Native	Password Protected Microsoft Excel 2007/2008
3	Word Sheet - Test1234!	Document Type is not s...	Resolved	Imaging Set	Imaging Set FIVE	Native	Password Protected Microsoft Word 2010-2016
4	PWPre2007MultiPageLongTextHeaderFooter - Test1234!	Error occurred when at...	Resolved	Imaging Set	Imaging Set FIVE	Native	Microsoft Excel 2000
5	PDF Sheet - Test1234!	Error occurred when at...	Resolved	Imaging Set	Imaging Set FIVE	Native	Adobe Acrobat (PDF)

Note: Imaging errors recorded before upgrading to 9.7.229.5 remain in the Show Errors dialog box and are not migrated to the Imaging Document Errors tab.

To learn more about an imaging error, click the **Name** field for a document on the Imaging Document Error tab. The Imaging Document Error Layout will open.

Layout fields include:

- **Relativity Document Identifier** — The unique identifier for the document.
- **Status** — The current status of the imaging error: Ready to retry, Retried, or Resolved.
- **Imaging Method** — The method used to image the document: Basic or Native.
- **Native Type** — The file type of the document in error, as identified by the native imaging engine.
- **Job Type** — The method used to run the imaging job: Imaging Set, Mass Imaging, or Image on the Fly.
- **Imaging Set** — The imaging set the document belongs to, when the Job Type is Imaging Set. Click the imaging set name to open the Imaging Set Layout.
- **Notes** — A space to record notes about the imaging error.



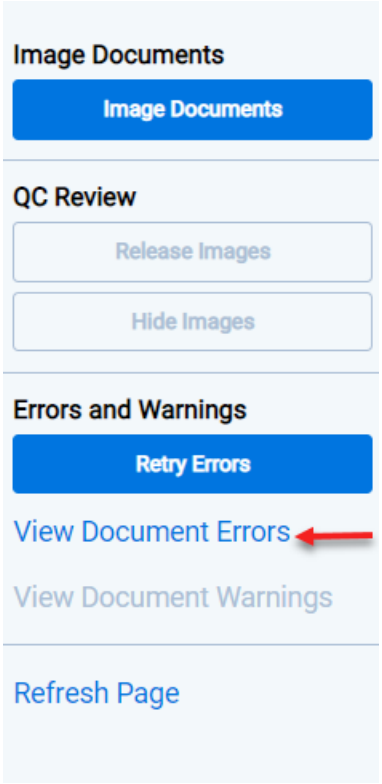
You can also open the Imaging Document Error Layout from the following locations:

- Imaging Sets tab below
- Documents tab on the next page
- Review Interface on the next page

13.11.1.1 Imaging Sets tab

To see imaging errors via the Imaging Sets tab:

1. Go to the **Imaging Sets** tab.
2. Click an imaging set. The Imaging Set Layout opens.
3. Click the **Name** field for a document to view more details about the error. The Imaging Document Error Layout opens.
4. Click **View Document Errors** on the Imaging Set console. This brings up the Imaging Document Error tab with a list of the errors that occurred during the job. By default, this action will add a filter to the Imaging Document Error tab to show only errors with a status of Ready to retry.



5. Click on the **Name** field for a document to obtain more information about the error. The Imaging Document Error Layout will open.

13.11.1.2 Documents tab

To see documents with imaging errors via the Documents tab:

1. Go to the **Documents** tab.
2. Create a new view.

Fields	Conditions	Sort
• Originating Imaging Document Error	• Has Images, any of these: Error	• NA

3. Select the view you just created from the View bar.
4. In the Document list, click on the **Originating Imaging Document Error** link for a document. The Imaging Document Error layout will open.

13.11.1.3 Review Interface

To see imaging errors on the Review Interface layout:

1. Click on the Layout.
2. Add the **Originating Imaging Document Error** field to the Layout.
3. Click **Save and Close**.

4. In the layout, click on the **Originating Imaging Document Error** link for a document that has an imaging error. The Imaging Document Error layout will open.

13.11.2 Imaging error scenarios

Errors will occur in your imaging job in any of the following scenarios:

- The Native Imaging engine attempts to render a corrupted native file.
- The Native Imaging engine attempts to render a password-protected native file that does not have a valid corresponding entry in the Password Bank. For more information, see Password Bank in imaging workflow on the next page.
- The Native Imaging engine attempts to render a document when the native file for that document is deleted from the repository.
- The Native Imaging engine attempts to render a native file when the FileShare repository is unavailable (access is denied).
- The Native Imaging queue service is stopped when the user attempts to run an imaging job.
- The Native Imaging queue service is disabled during an imaging job.
- The Native Imaging engine attempts to render a native file when there is no hard drive space in the file share repository.
- The Native Imaging engine is installed but the imaging job is not pointing to a valid server because the Native Imaging URL in the instance setting table is incorrect or invalid.
- The conversion request failed.
- The imaging request is no longer tracked. This occurs when a request key is removed from the server, typically as a result of an Internet Information Services (IIS) reset. This error appears only in the population table and not in the Errors tab. This scenario applies to imaging set, mass imaging, and image-on-the-fly jobs.
- The request key is no longer valid. This occurs when Relativity receives a status report for a conversion or imaging job that it is no longer tracking, typically because the job timed out. An IIS reset may cause this. This scenario applies to imaging set, mass imaging, and image-on-the-fly jobs.

When Relativity Native Imaging encounters an error, it retries the imaging job one time. Relativity logs additional errors in the error report.

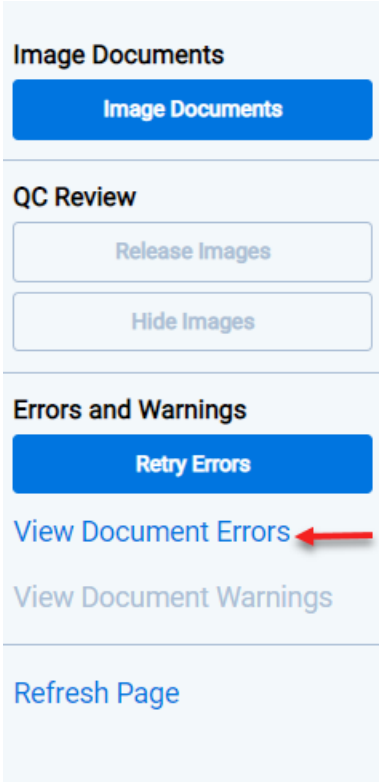
13.11.3 Error email notification

When errors occur during an imaging job, Relativity sends an email to all users listed in the Email Notification Recipients field for that imaging set. The email summarizes the errors and includes a link to the Imaging Document Errors tab.

13.11.4 Retrying imaging errors

To retry imaging errors:

1. Click **View Document Errors** on the imaging set console. The Imaging Document Errors tab opens, filtered to errors with a status of Ready to retry.



2. Click **Retry Errors**.

Retrying imaging errors re-images the documents that previously resulted in errors. When the retry job reaches a status of Initializing, the Retry Errors button changes to Stop Imaging. Click **Stop Imaging** to cancel the retry job.

13.11.5 Password Bank in imaging workflow

The following steps depict how the Password Bank typically fits into the imaging cycle.

1. You create a password bank that includes a list of passwords that correspond with the files you intend to image.
2. You create an imaging set with the data source that contains the encrypted documents.
3. You start imaging the documents in the imaging set by clicking **Image Documents** in the Imaging Set console.
4. All passwords you supplied to the password bank become synced via an agent and accompany the job as it goes to the imaging engine.
5. The imaging engine images the files in the imaging set and refers to the passwords provided in the password bank. It then sends the imaged files back to Relativity.
6. Once the imaging status changes to Completed, you review and release images from QC review.
7. The imaged documents become available for review in the workspace, along with all the other previously-encrypted documents whose passwords you provided.

Note: The Password Bank works with both Native and Basic imaging.

To view and resolve password-protection errors:

1. After running an imaging set, click View Document Errors in the imaging set console.
2. In Relativity, go to the Password Bank and create entries for every password that corresponds with the files that resulted in errors.

3. Click Retry Errors in the imaging set console to re-image the files that previously resulted in password-protection errors.

The imaged documents, along with other documents that were previously encrypted, become available for review in the workspace.

For more information, see Password bank in the Processing User Guide.

13.12 Imaging Warnings

The Imaging Warnings object identifies possible cut-off content in imaged MSG and EML files and stores that information for review.

Note: Relativity supports the following email file types for imaging: MSG, P7M, P7S, ICS, VCF, EML, EMLX, and TNEF. However, imaging warnings are only generated for EML and MSG file types.

To view a list of documents that have imaging warnings, go to the Imaging Warnings tab. You can also add imaging warning fields to a Core Reviewer layout or a document view.

13.12.1 Special considerations

Note the following when working with imaging warnings:

- If you delete an image, the imaging warnings associated with that image remain.
- If you delete a document that has associated imaging warnings, the warnings are no longer visible and cannot be searched.
- Relativity does not perform warning detection on images uploaded using the image replacement feature in the Document viewer.
- Relativity does not perform warning detection on documents longer than 25 pages.
- Documents longer than 25 pages are marked as Cut-off Detection Not Performed in the Warning Type field.

13.12.2 Imaging Warnings tab

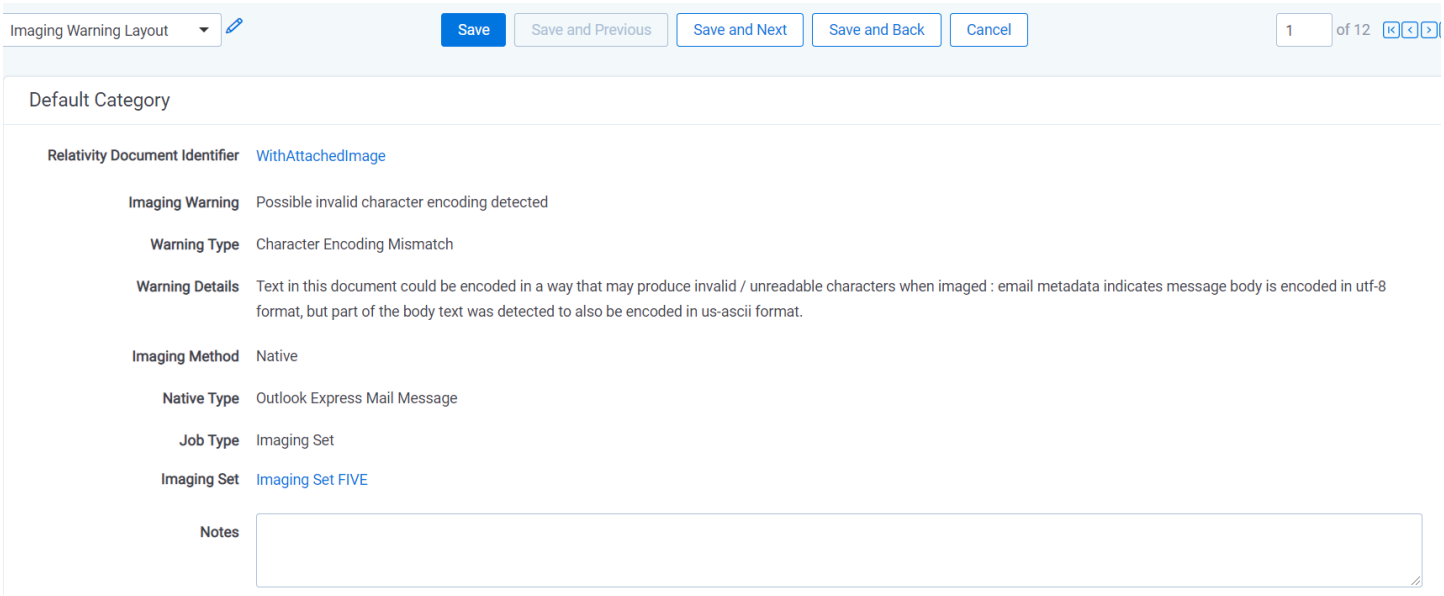
The Imaging Warnings tab displays information related to current Imaging Warnings.

#		Relativity Document I...	Imaging Warning	Warning Type	Warning Details	Imaging Method	Native Type	Job Type
		Filter	Filter	(All)	Filter	(All)	Filter	(All)
1		WithAttachedImage	Possible invalid charac...	Character Encoding Mismatch	Text in this document could be encoded in a way that may produce invalid / unreadable characters when imaged : email metadata indicates message body is encoded in utf-8 format, but part of the body text was detected to also be encoded in us-ascii format.	Native	Outlook Express Mail Message	Imaging Set
2		29350	Possible invalid charac...	Character Encoding Mismatch	Text in this document could be encoded in a way that may produce invalid / unreadable characters when imaged : email metadata	Native	Outlook Email	Imaging Set

Note: Previous imaging warning information is not preserved. If a document with an imaging warning is re-imaged, the prior imaging warning is deleted.

13.12.2.1 Imaging Warning layout

When you click the **Imaging Warning** field for a document, the Imaging Warning layout opens.



Note: You cannot access the Imaging Warning layout from the **Documents** tab. To open the Imaging Warning layout, go to the **Imaging Warnings** tab or the **Core Reviewer** layout, then click the **Imaging Warning** field for a document.

The Imaging Warning layout has the following fields:

- **Relativity Document Identifier** — The control number of the document, with a link to the document in the Viewer.
- **Imaging Warning** — A description of the problem detected. Description options are:
  - Possible cut-off embedded image detected.
  - Possible cut-off text detected.
  - Cut-off detection not performed.
  - Split performed on table larger than page width.
  - Possible missing or invalid Rich Text Format content detected in the email body.
  - Possible invalid character coding detected.
  - Possible missing extracted text on images

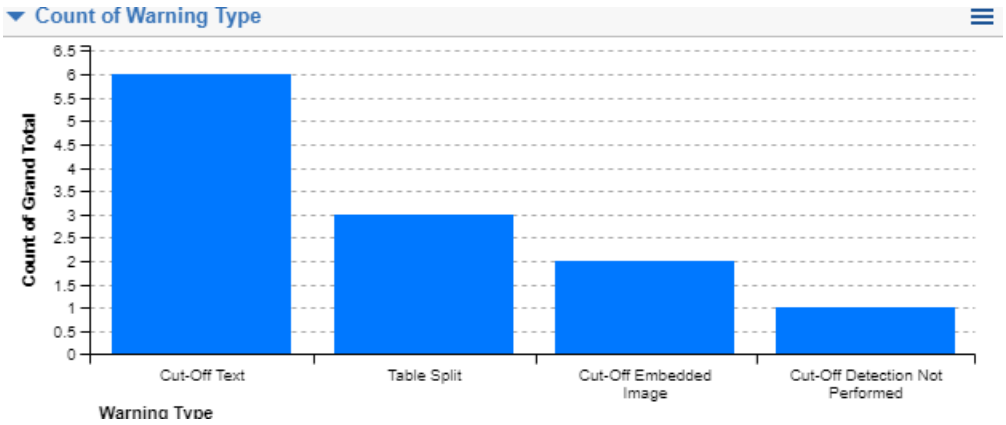
  For more information, see All imaging warnings on the next page.
- **Warning Type** — A predefined list of options for grouping and searching warnings. This field has better search performance than a text-based field such as Imaging Warning. Warning types include:
  - Cut-Off Embedded Image
  - Cut-Off Detection Not Performed
  - Table Split
  - Missing or Invalid Rich Text Format Content

    - Character Encoding Mismatch
    - Missing Text
- **Warning Details** — Additional information about the problem, such as the page range where issues are detected.
- **Imaging Method** — The method used to image the document: Basic or Native.
- **Native Type** — The file type of the document before imaging.
- **Job Type**— The method used to create the image. Job types include:
    - On-the-fly
    - Mass imaging
    - Imaging Set
- **Imaging Set** — The imaging set used to produce the image, when the job type is Imaging Set. Click the imaging set name to open the Imaging Set Layout.
- **Notes** — A space to enter notes about the imaging warning.

Note: Except for the Notes field, you cannot modify the Imaging Warning fields, and you cannot link or unlink Imaging Warnings to documents.

13.12.2.2 Warning Type pivot table

In the Imaging Warnings tab, you can create a pivot table based on the Warning Type field and then export the pivot or dashboard. See the Admin Guide.



Note: You can only create the Warning Type pivot in the Imaging Warnings tab. The Warning Type field is not available for widgets on the Documents tab.

13.12.3 All imaging warnings

The following table lists the all the imaging warnings:

Imaging Warning Type	Why this warning occurred	Recommended action
Character Encoding Mismatch	The text in this document may be encoded in a way that produces invalid or unreadable characters when imaged. The email metadata indicates the message body uses one character encoding, but part of	Create a saved search with this warning type as a search condition and

Imaging Warning Type	Why this warning occurred	Recommended action
	the body text uses a different encoding. Example formats include: • UTF-8 • Windows-1252 • us-ascii	manually QC the returned documents.
Cut-Off Detection Not Performed	Email that is greater than 25 pages cannot have cut-off detection performed on it.	Create a saved search with this warning type as a search condition and manually QC the returned documents.
Cut-Off Embedded Image	Embedded images within a table go beyond the boundaries of the page.	Use different imaging profile options, such as landscape, auto-fit tables, split tables and auto-fit images.
Cut-Off Text	Text within a table goes beyond the boundaries of the page.	Use different imaging profile options, such as landscape, auto-fit tables, and split tables.
Missing or Invalid Rich Text Format Content	The rich text data in the email body may be missing or incorrect. As a result, text in the email body may be missing from the generated image.	Create a saved search with this warning type as a search condition and manually QC the returned files.
Table Split	Tables that go beyond the boundaries of the page have been split and re-printed on a new line.	Create a saved search with this warning type as a search condition and manually QC the returned files.
Table Split Not Completed	Tables that are beyond boundaries of the page could not be split. Reasons for this include an abnormally wide first column, when there are rows that span across multiple columns, or a table within a table. The exact page where the table begins will be reported.	Use different Imaging Profile options, such as landscape, auto-fit tables, and split tables.

13.12.4 Core Reviewer layouts

To facilitate the QC of documents, you can link the Imaging Warnings layout to a Review layout. See the Admin Guide.

You can also add Imaging Warnings fields to a Core Reviewer layout. The Core Reviewer layout can be configured to show Imaging Warning details or create pop-ups with that information. See the Admin Guide.

Imaging Warnings fields that you can add to a layout include:

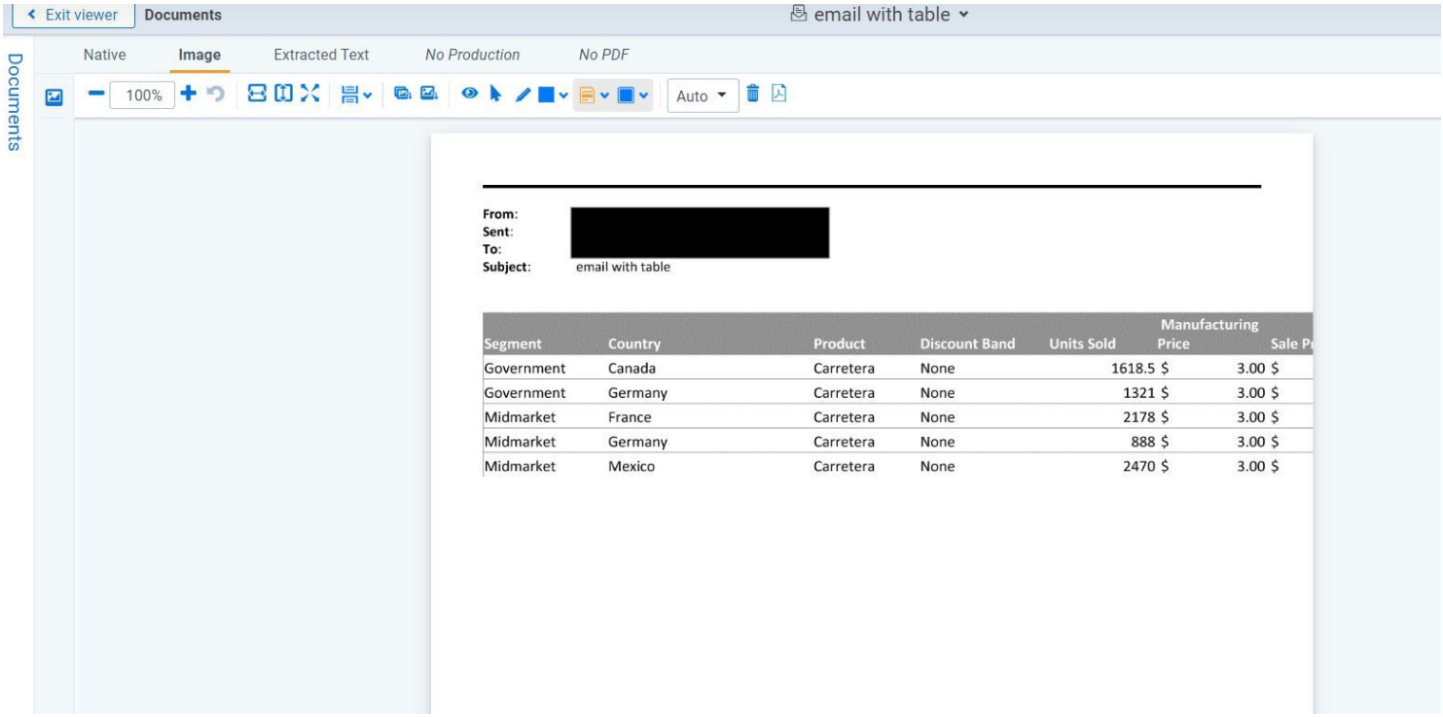
- Imaging Warning
- Warning Type
- Warning Details

For field descriptions, see Imaging Warning layout on page 273.

13.12.5 Re-imaging emails with tables

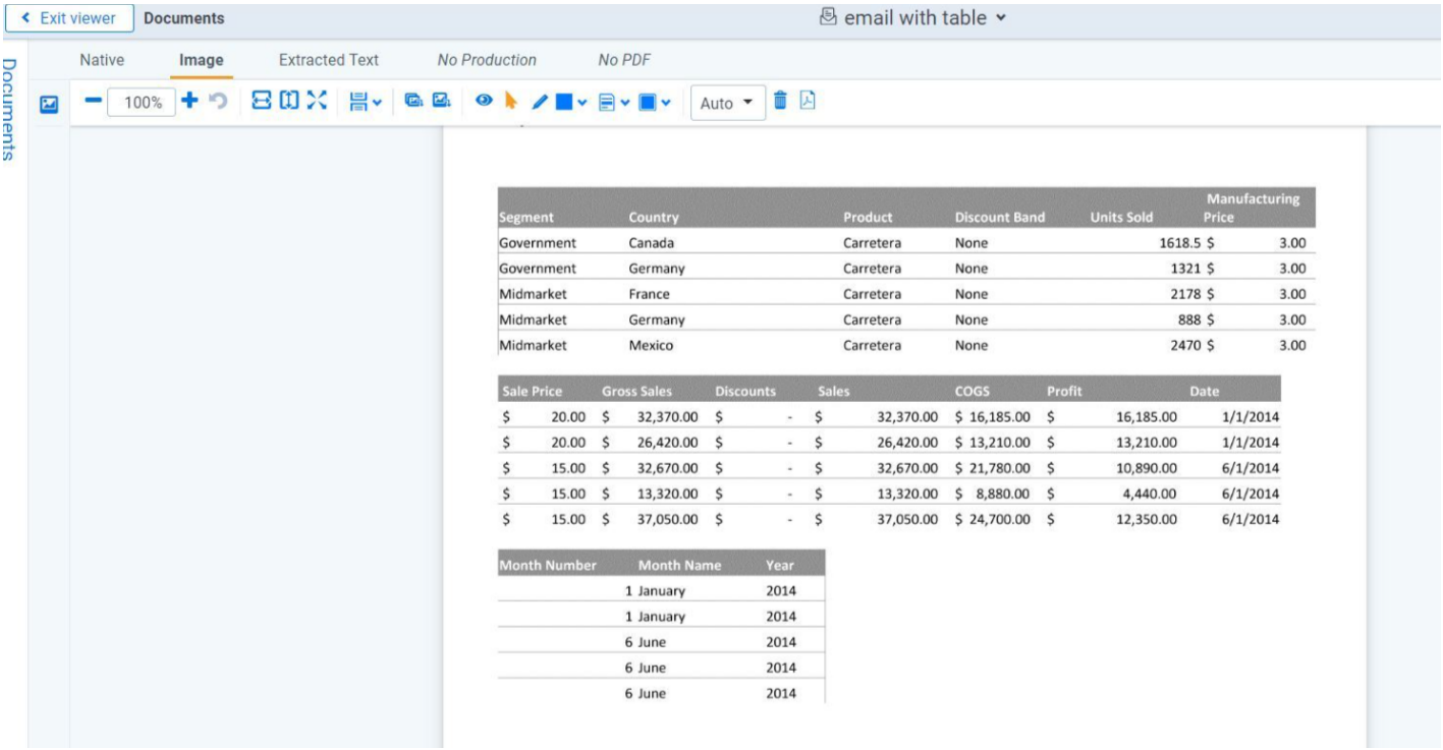
You can image large tables in emails without the table being cut-off in the resulting image by setting the Split tables to fit page width field in the Native imaging profile to Yes. When this field is set to Yes, wide tables are split and re-printed on a new line when they are imaged with no content lost.

The following screen shot shows an imaged email where the Split tables to fit page width field was set to No on the imaging profile.



Segment	Country	Product	Discount Band	Units Sold	Manufacturing Price	Sale P
Government	Canada	Carretera	None	1618.5 $	3.00 $	
Government	Germany	Carretera	None	1321 $	3.00 $	
Midmarket	France	Carretera	None	2178 $	3.00 $	
Midmarket	Germany	Carretera	None	888 $	3.00 $	
Midmarket	Mexico	Carretera	None	2470 $	3.00 $	

This screen shot shows an imaged email where the Split tables to fit page width field was set to Yes on the imaging profile.



Segment	Country	Product	Discount Band	Units Sold	Manufacturing Price
Government	Canada	Carretera	None	1618.5 $	3.00
Government	Germany	Carretera	None	1321 $	3.00
Midmarket	France	Carretera	None	2178 $	3.00
Midmarket	Germany	Carretera	None	888 $	3.00
Midmarket	Mexico	Carretera	None	2470 $	3.00

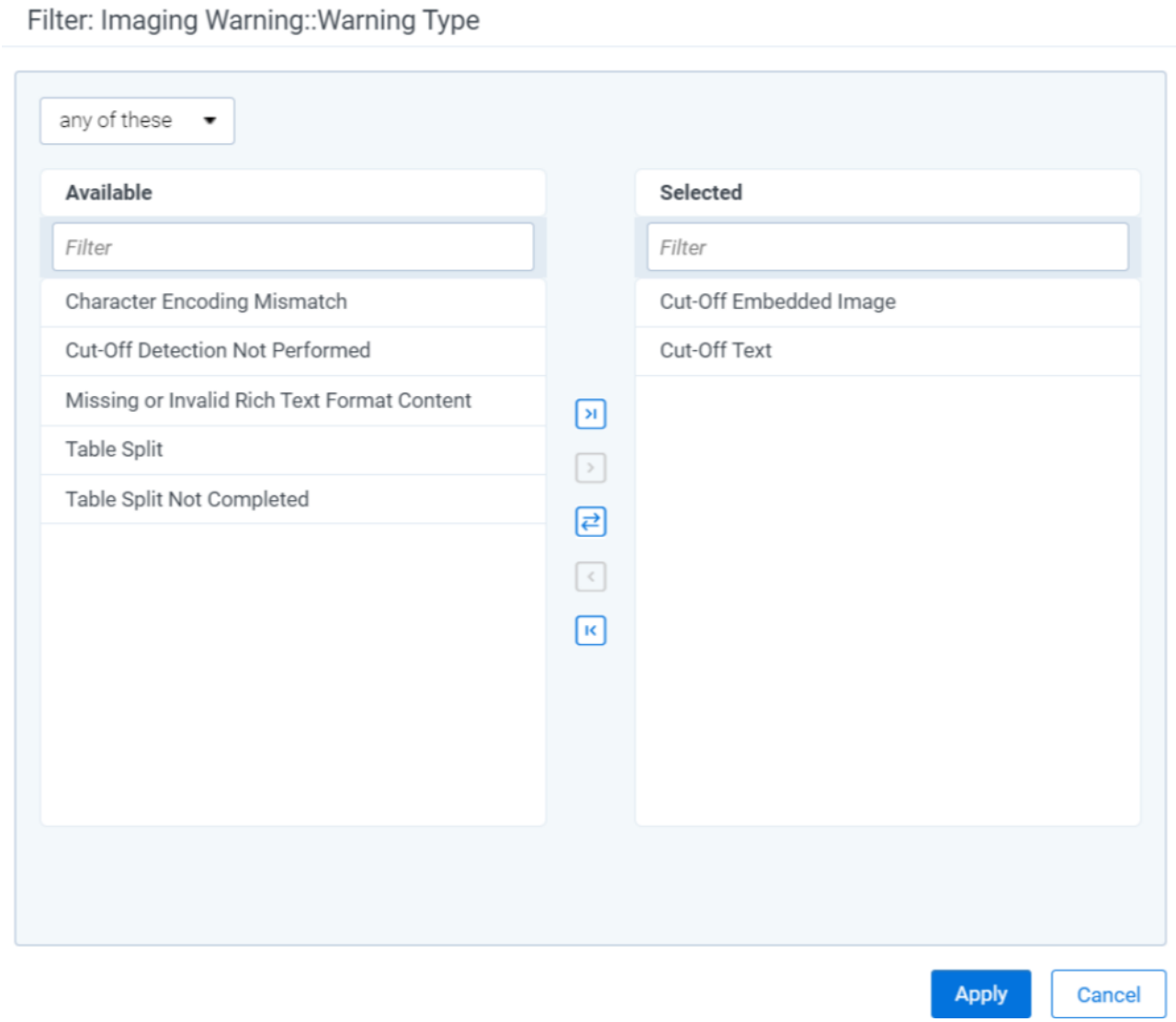
Sale Price	Gross Sales	Discounts	Sales	COGS	Profit	Date
$ 20.00	$ 32,370.00	$ -	$ 32,370.00	$ 16,185.00	$ 16,185.00	1/1/2014
$ 20.00	$ 26,420.00	$ -	$ 26,420.00	$ 13,210.00	$ 13,210.00	1/1/2014
$ 15.00	$ 32,670.00	$ -	$ 32,670.00	$ 21,780.00	$ 10,890.00	6/1/2014
$ 15.00	$ 13,320.00	$ -	$ 13,320.00	$ 8,880.00	$ 4,440.00	6/1/2014
$ 15.00	$ 37,050.00	$ -	$ 37,050.00	$ 24,700.00	$ 12,350.00	6/1/2014

Month Number	Month Name	Year
1	January	2014
1	January	2014
6	June	2014
6	June	2014
6	June	2014

Setting the Split tables to fit page width field to Yes slows down imaging time. Consider imaging documents without this setting first, then re-imaging documents that receive an imaging warning.

To re-image documents that have an imaging warning:

1. Create a saved search that brings back documents with Imaging Warnings.
    - Select **Imaging Warning** from the **Add Condition** drop-down menu. A dialog box opens.
    - Select **these conditions** from the Operator.
    - Click **Add Condition** and select **Imaging Warning::Warning Type**.
    - Select **any of these** from the Operator drop down.
    - Move **Cut-Off Embedded Image** and **Cut-Off Text** from Available to Selected and click **Apply**. (Click to expand image)

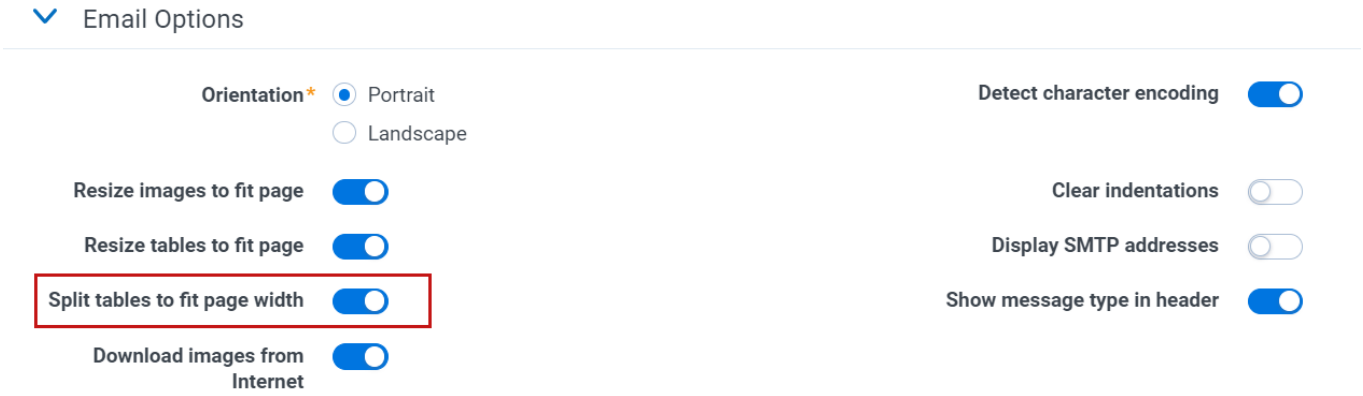


    - Click **Apply**.

    For more information, see the Admin Guide.
2. Delete the images in documents that have Imaging Warnings.
    - Filter on the saved search you created.
    - Select **Delete** from Mass Operations.

- Select **Delete only images from selected documents**.
- Click **Delete**.

3. Create a Native Imaging Profile, and in the Email Options tab, set the Split tables to fit page width field to **Yes**. For more information, see the Admin Guide.



4. Create an Imaging Set.
   - Select the saved search you created for **Data Source**.
   - Select the native imaging profile you just created for Imaging Profile.
   - Click **Save**.

   For more information, see the Admin Guide.
5. Open the Imaging Set.
6. Click **Image Documents** from the Imaging Sets console.

13.13 QC Review

QC Review lets you hide images in an Imaging Set from most users until a QC reviewer approves them. The QC reviewer can view the images, but other groups cannot see them until you release the set. A permission setting in the Admin Operations section of the Workspace Details tab controls whether members of a group can view images held for QC Review. If a user does not have sufficient permissions, the Image radio button is unavailable in the Viewer until you release the Imaging Set.

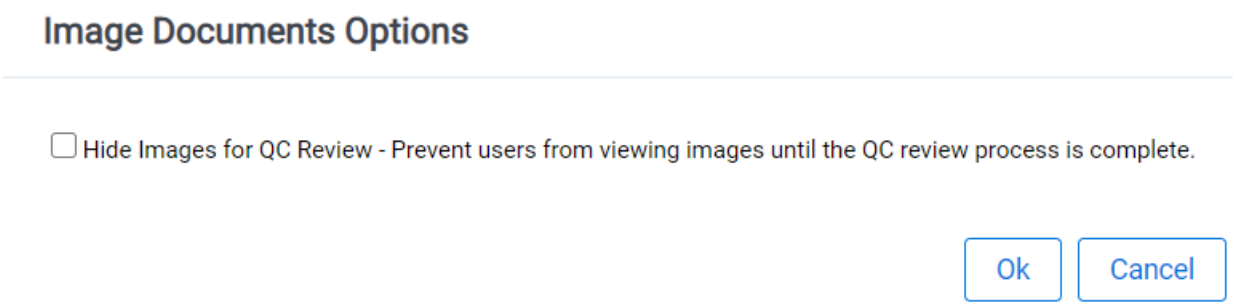
Use QC Review when you need one team to review images before releasing them to a larger group. You can restrict access to images in an Imaging Set while another group performs quality checks, then release the images when the review is complete.

Note: QC Review of Imaging Sets that contain large volumes of documents can be optimized with Random Sampling. See Sampling on page 587

13.13.1 Hiding images for QC

To hide images for QC Review:

1. Click the **Imaging Set** tab.
2. Select an Imaging Set.
3. Click **Image Documents**.
4. Select the **Hide Images** checkbox. This prevents users without the View Images Hidden for QC Review permission from viewing images in this Imaging Set.



5. Click **OK**.

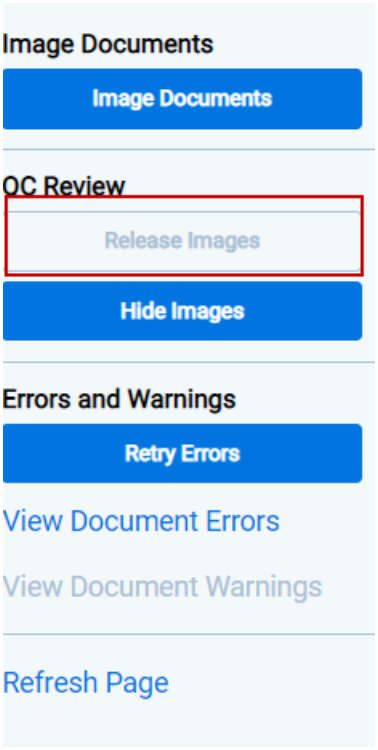
> **Note:** The ImageQCOnByDefault instance setting value makes this checkbox default to checked. See the Instance setting guide.

Only users in groups with the View Images Hidden for QC Review permission can view the images. You can apply this permission to any group from the **Workspace Details** tab.

13.13.2 Releasing images

When the QC review is complete, follow these steps to release images to other groups:

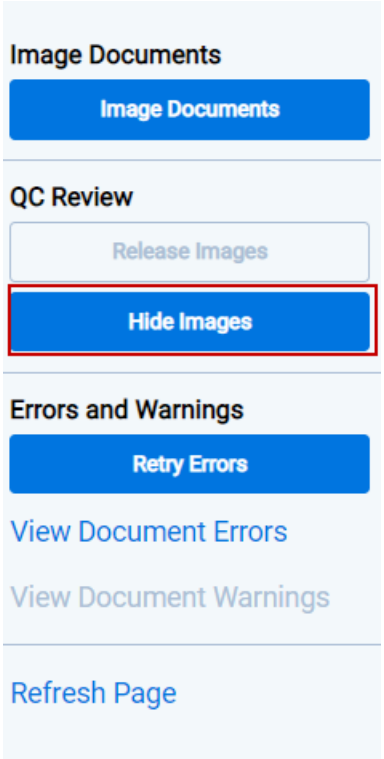
1. Click the **Imaging Set** tab.
2. Select the Imaging Set.
3. Click **Release Images**. A confirmation window appears asking you to confirm that you want to release all images in this Imaging Set.



4. Click **OK**.

If documents in an Imaging Set already have images when you set it up for QC Review, use the following steps to hide them.

1. Click the **Imaging Set** tab.
2. Select an Imaging Set.
3. In the QC Review section, click **Hide Images**.



13.13.2.1 QC Review fields

The following two fields are used in QC Review. If you image a document in more than one Imaging Set, the Imaging Set field displays only the most recent one.

- **Image QC Status** — This choice field indicates whether the document image is **Hidden for QC**. If the image is not hidden, this field is null.
- **Imaging Set** — This field displays the most recent Imaging Set associated with the document. This field is null if the document image comes from outside Relativity or from the Image on the fly feature.

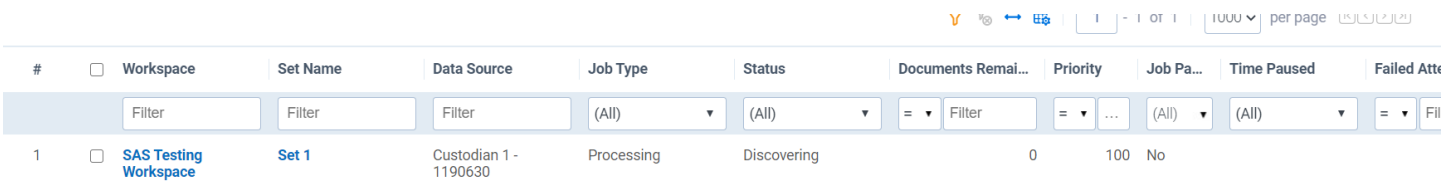
13.13.2.2 Image QC Review Status

The Image QC Review Status section of the Imaging Set console displays the following fields.

- **Documents set to hidden** — Displays the number of images hidden during the imaging process.
- **Documents viewable** — Displays the number of documents with viewable images.

13.14 Imaging jobs in the Imaging Queue

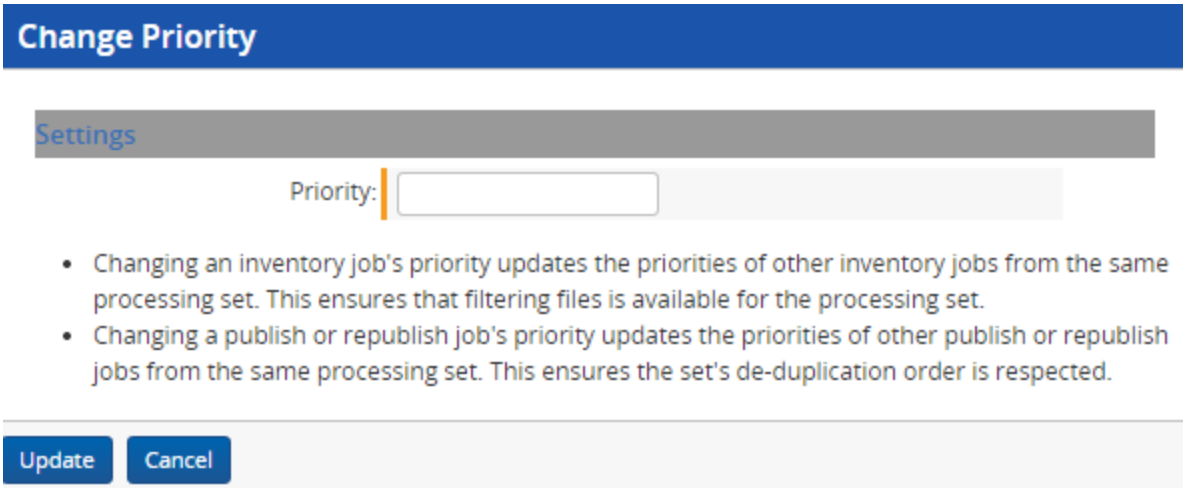
The Imaging Queue displays all current imaging jobs running in your environment. You can view the queue if you have system admin rights to see the tab. Select the **Queue Management** tab, and click**Imaging Queue**.



The Imaging Queue view displays the following fields:

- **Workspace**—Indicates the workspace associated with the imaging set, Mass Image, or Image-on-the-fly job.
- **Imaging Set Name**—Indicates the imaging set, Mass Image, or Image-on-the-fly operation used for the job. Mass Image and Image-on-the-fly jobs are named and auto-incremented when they are added to the queue.
- **Data Source** —The data source associated with the job. This field is populated only for processing jobs and is blank for imaging jobs.
- **Job Type**—Indicates the job being run, will say "Imaging" for all types of Imaging jobs.
- **Imaging Set Artifact ID**—The unique identifier for the imaging set. The artifact ID will be set to blank for Image-on-the-fly or Mass Image jobs because these operations do not have imaging sets.
- **Imaging Profile** —Lists the name of profile used to create the document images.
- **Documents Remaining**—Lists the number of documents waiting to be imaged.
- **Status**—Displays the current stage of the imaging job. Image-on-the-fly or Mass Image operations have only Waiting and Processing statuses.
- **Priority**—Indicates the order in which the imaging job will be run. Jobs initiated through image sets or Mass Image operations have default values of 100, while jobs initiated by Image-on-the-fly have default values of 1 (which means they will be worked on before mass image operations).
- **Submitted Date**—Indicates the date and time when an imaging job was submitted, or an attempt was made to resolve errors in a job through the Imaging Set Console.
- **Submitted By**—Lists the name of the user who initiated the imaging job.

Relativity sends jobs to the imaging engine by priority, and then orders them by submitted date. To change the priority of a job, click **Change Priority** at the bottom of the view. Enter a new integer value in the **Priority** field, and then click **Update**. Jobs assigned a lower value have a higher priority.



To cancel imaging jobs, select one or more jobs, and click **Cancel Imaging Job**. You can cancel a job at any point while it is active, including during the Preparing files, Submitting, and Imaging phases.

Note: If you cancel an imaging job or delete an imaging set during an imaging job, all images from imaged documents within that set remain in the database.

Note: To change the priority of a job where **Customer lockbox** is enabled, you must be in a permission group having access to the workspace where the job originated, along with the System Administrator's group. For more information, see Customer lockbox.

13.15 Native imaging - dithering algorithm options

Relativity native imaging offers multiple dithering algorithms you can apply when imaging your documents. Use the comparison tables below to evaluate image size and quality across algorithm types for text-rich and image-rich documents.

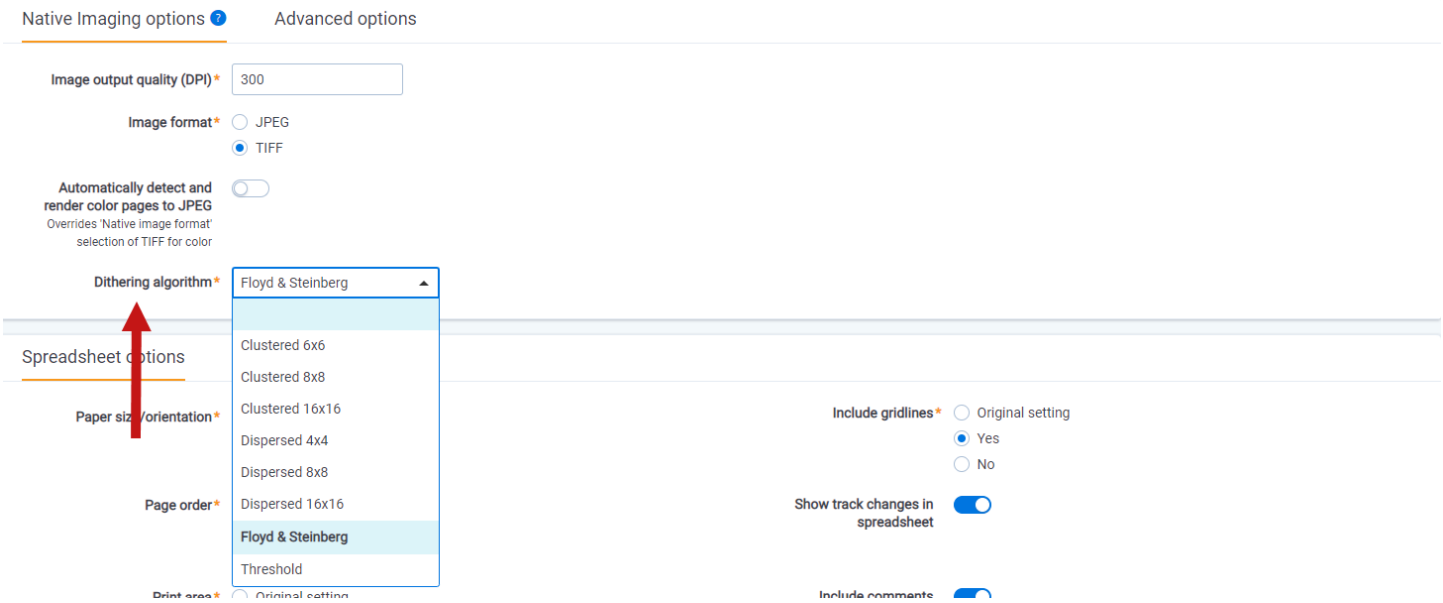
13.15.1 Dithering algorithm details

When configuring native imaging, system admins can select from eight dithering algorithms:

Consider grouping the eight options under four algorithm families and providing a one-sentence description of each family, for example:

- **Clustered 6x6, 8x8, 16x16** — groups pixels into clusters. Larger cluster sizes produce smaller file sizes but lower image detail.
- **Dispersed 4x4, 8x8, 16x16** — disperses pixels across a matrix pattern. Produces a finer, more even grain than clustered dithering.
- **Floyd & Steinberg** — diffuses the difference between a pixel's color value and its quantized equivalent to neighboring pixels. Produces high-quality results for image-rich documents.
- **Threshold** — compares each pixel value against a fixed threshold (0–255). Values above the threshold convert to black; values below convert to white. Requires a threshold value in the Dithering Threshold field.

  Note: If you select Threshold, you must also enter a value (0–255) in the Dithering Threshold field. The recommended default is 128.



13.15.1.1 Dithering results for text-rich documents

The following table shows dithering results for text-rich documents. Each image in the table shows a document sample magnified to 150% to illustrate visual differences between algorithms. All samples are 300 DPI, black and white.

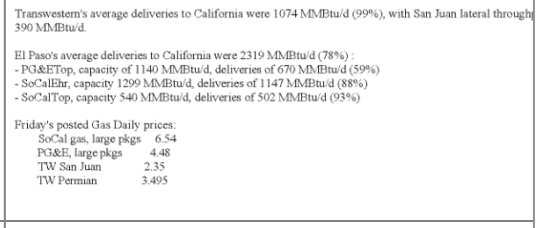
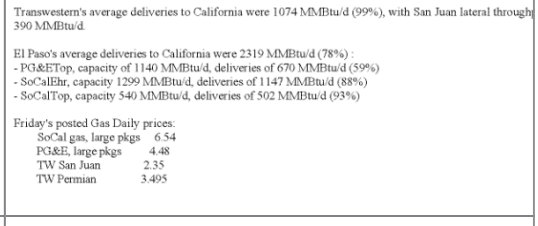
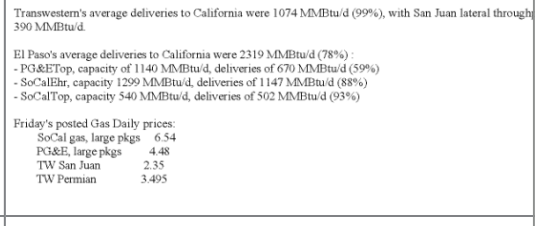
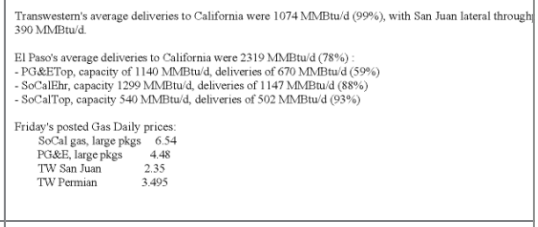
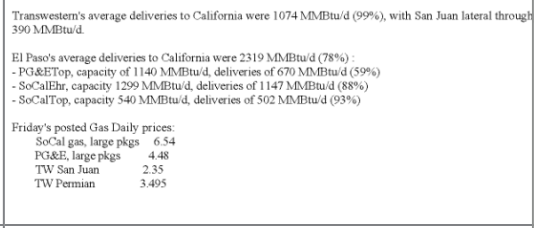
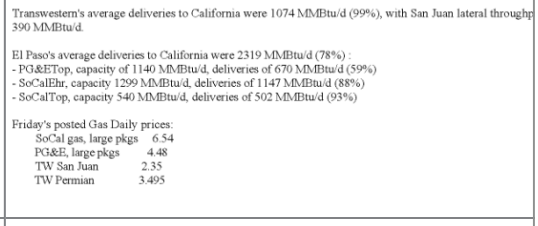
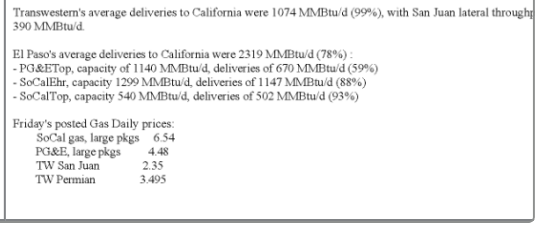
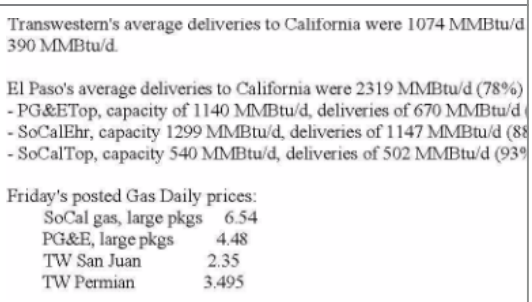
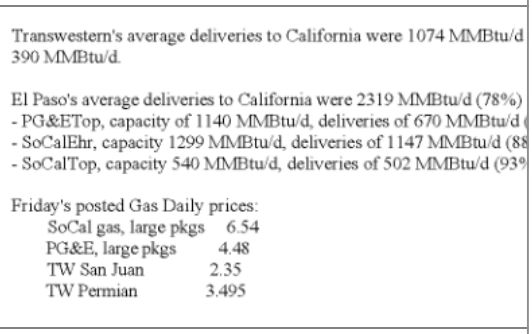
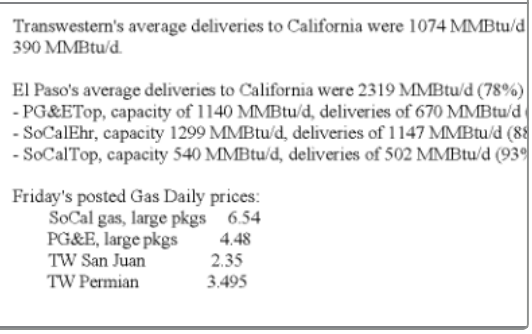
Image dithering type	Size	Image sample magnified (150% scale)
Clustered 6x6	27 KB	
Clustered 8x8	25 KB	
Clustered 16x16	23 KB	
Floyd & Steinberg	24 KB	
Dispersed 4x4	24 KB	
Dispersed 8x8	24 KB	
Dispersed 16x16	24 KB	

Image dithering type	Size	Image sample magnified (150% scale)
Threshold 0	2 KB	
Threshold 127	22 KB	
Threshold 215	22 KB	
Threshold 255	22 KB	

13.15.1.2 Dithering results for image-rich documents

The following table shows dithering results for image-rich documents. Each image in the table shows a document sample magnified to 150% to illustrate visual differences between algorithms. All samples are 300 DPI, black and white.

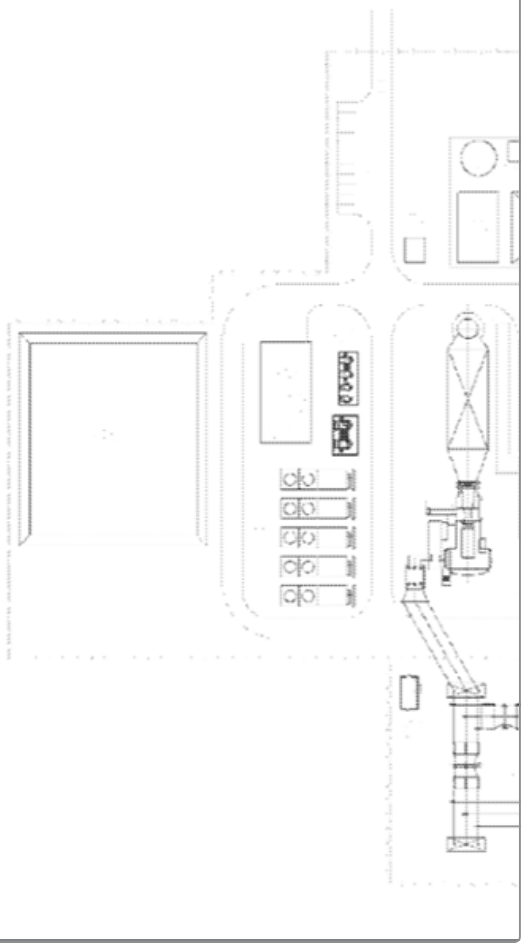
Image dithering type	Size	Image sample magnified (150% scale)
Clustered 6x6	45 KB	

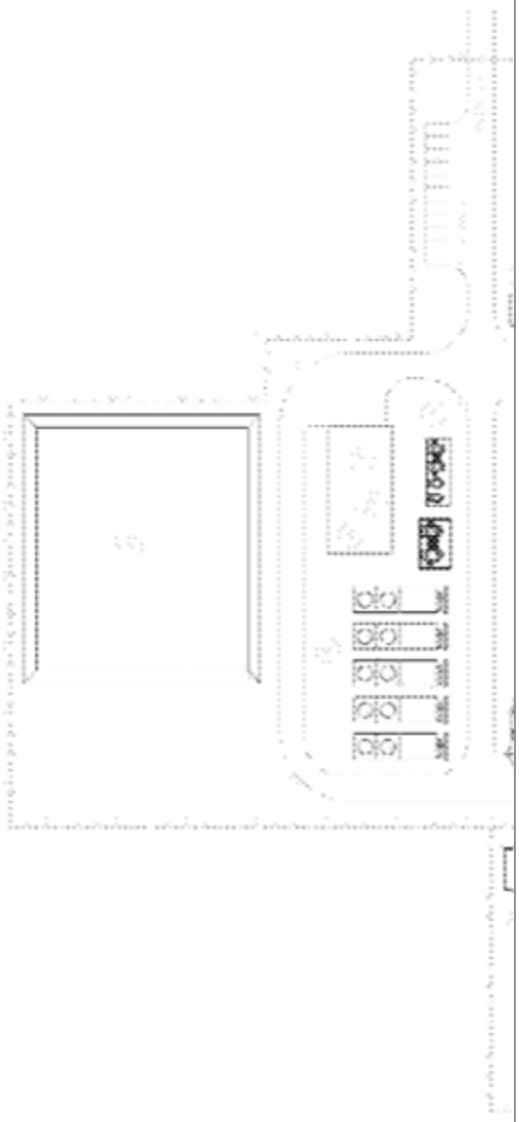
Image dithering type	Size	Image sample magnified (150% scale)
Clustered 8x8	39 KB	

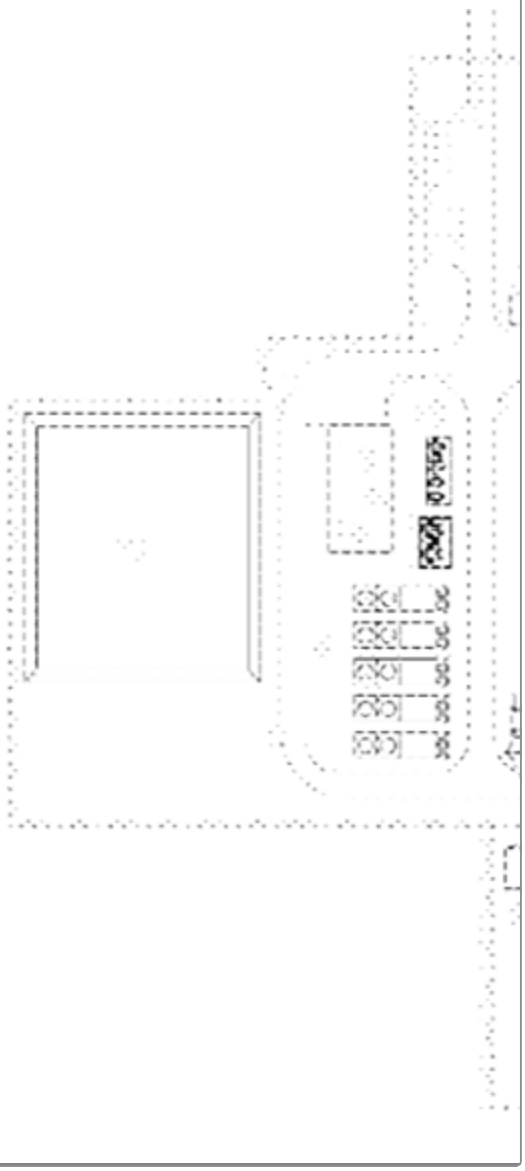
Image dithering type	Size	Image sample magnified (150% scale)
Clustered 16x16	33 KB	

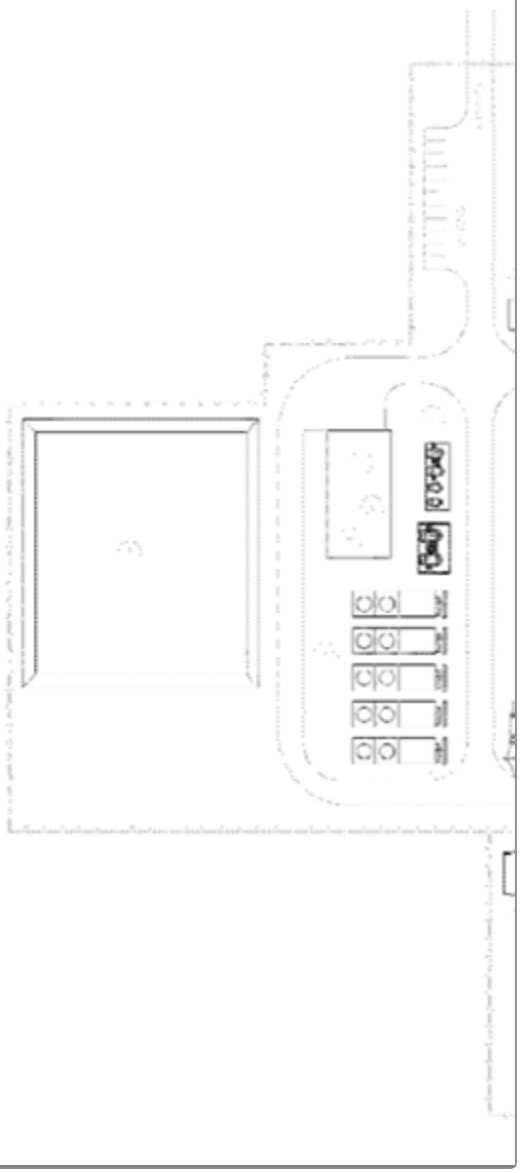
Image dithering type	Size	Image sample magnified (150% scale)
Floyd & Steinberg	70 KB	

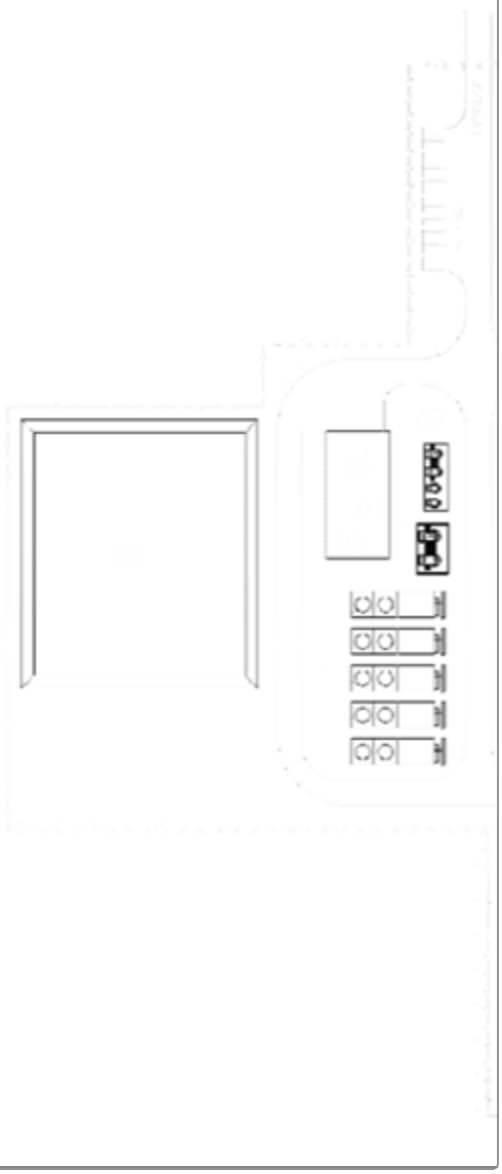
Image dithering type	Size	Image sample magnified (150% scale)
Dispersed 4x4	64 KB	

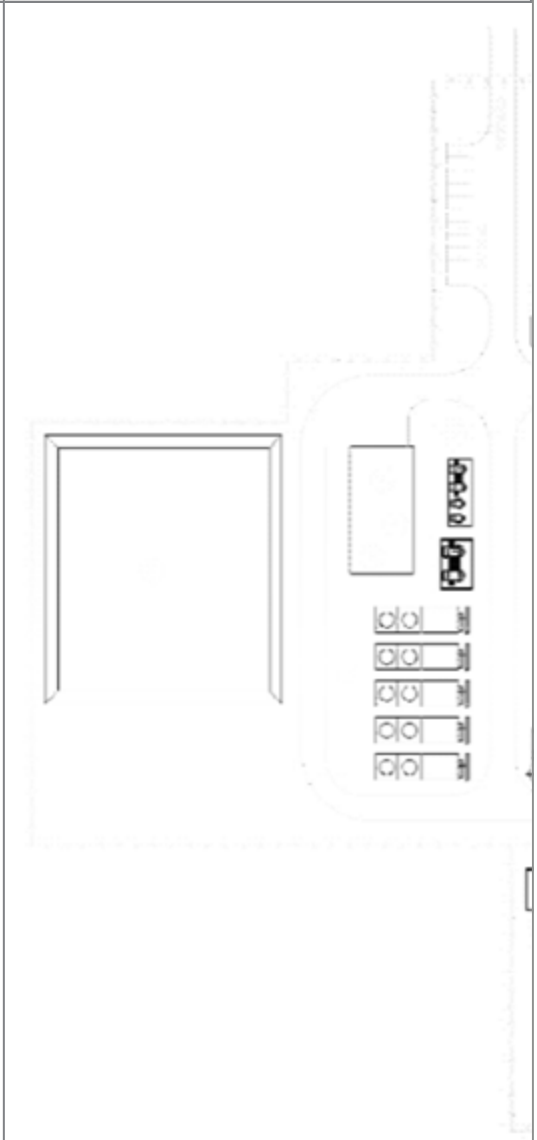
Image dithering type	Size	Image sample magnified (150% scale)
Dispersed 8x8	52 KB	

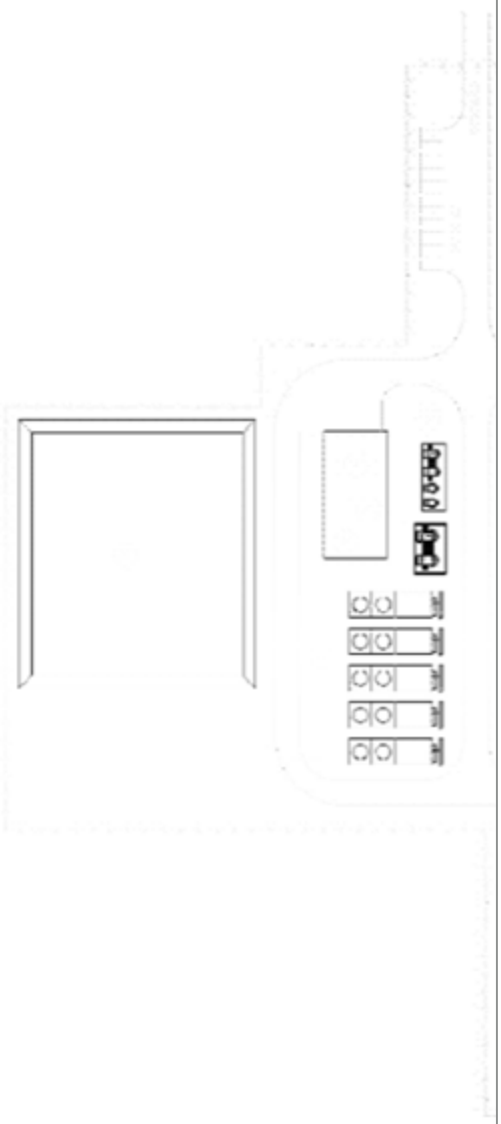
Image dithering type	Size	Image sample magnified (150% scale)
Dispersed 16x16	69 KB	

Image dithering type	Size	Image sample magnified (150% scale)
Threshold 0	2 KB	

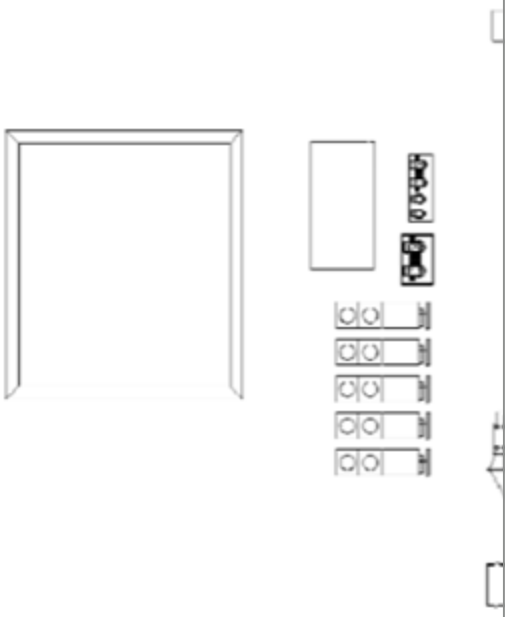
Image dithering type	Size	Image sample magnified (150% scale)
Threshold 127	79 KB	

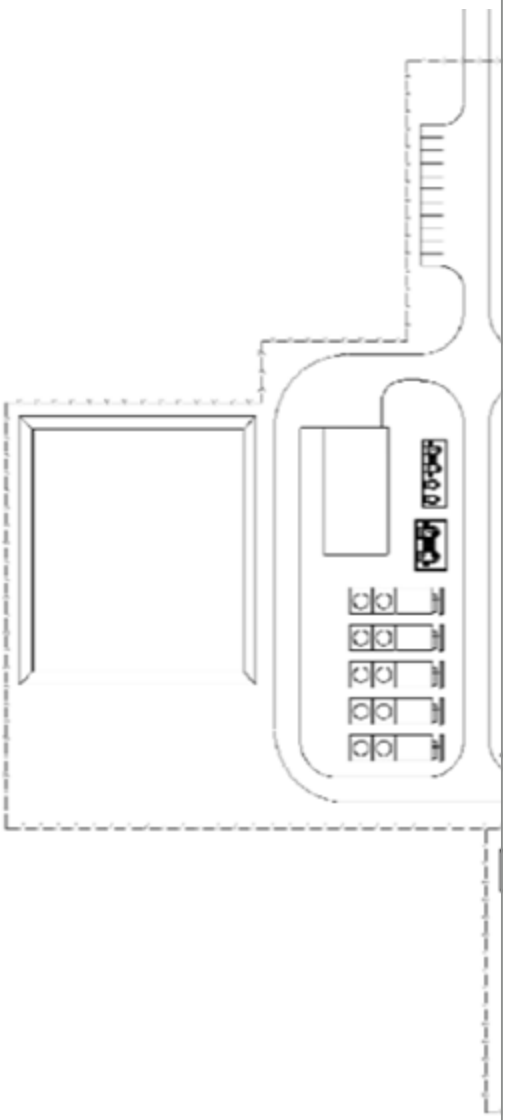
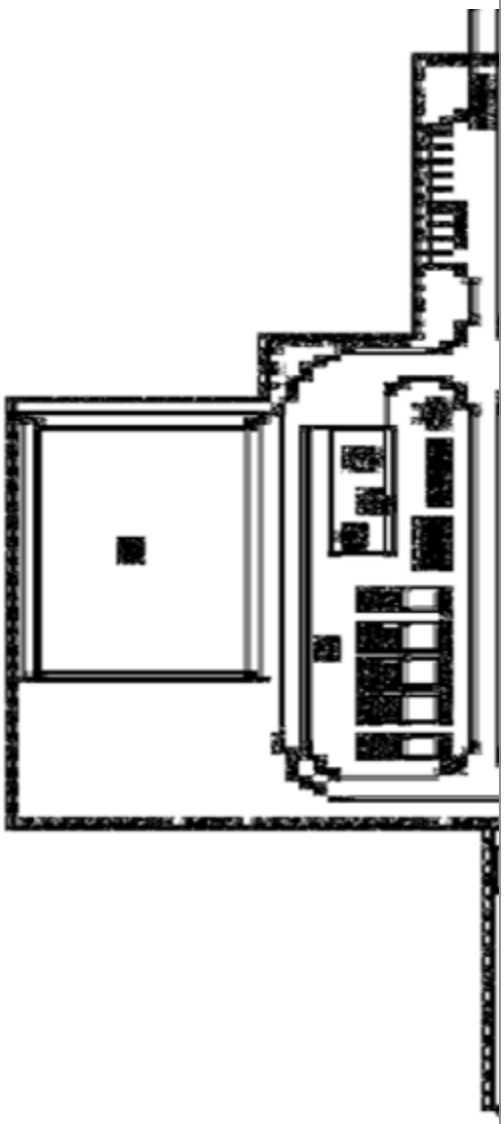
Image dithering type	Size	Image sample magnified (150% scale)
Threshold 215	27 KB	

Image dithering type	Size	Image sample magnified (150% scale)
Threshold 255	20 KB	

13.16 Imaging native types

The Native Types tab lists the file types that Relativity supports. Use this tab to identify and restrict file types from imaging. Import/Export supports the same file types.

#		Name	Imaging Method	Category (Basic)	Restricted From Imagi...	Prevent Native Download
		Filter	(All)	(All)	(All)	(All)
1		Word for DOS 4.x	Basic	Word Processor	No	No
2		Word for DOS 5.x	Basic	Word Processor	No	No
3		Wordstar 5.0	Basic	Word Processor	No	No
4		Wordstar 4.0	Basic	Word Processor	No	No
5		Wordstar 2000	Basic	Word Processor	No	No
6		WordPerfect 5.0	Basic	Word Processor	No	No
7		MultiMate 3.6	Basic	Word Processor	No	No
8		MultiMate Advantage 2	Basic	Word Processor	No	No

To locate specific file types, use the **Show Filters** option. You can also create a new view to customize what appears on the tab. Default restricted file types propagate to new imaging profiles. To edit these settings, click the **Edit** link for a file type. You can change the default restriction from imaging and the native download prevention setting.

If you restrict a particular file type, Relativity does not apply that restriction to existing Imaging Profiles. The restriction applies only to Imaging Profiles you create after editing the setting.

13.16.1 Editing a native type

1. Click the **Edit** link for a file type. You can also click the **Edit** button on the details page.
2. On the edit form, select the Yes or No radio button for the **Restricted From Imaging By Default** option. This value is set to No by default.
3. Select the Yes or No radio button for the **Prevent Native Download** option. This value is set to No by default.

   Note: If **Prevent Native Download** is set to **Yes**, the Native button does not appear in the Viewer for files of that type for any user in the workspace.

4. Click **Save.**

13.16.2 Generating a complete list of native types and their respective imaging engines

To generate a .CSV file listing all native types and their imaging methods, categories, restriction status, and native download prevention status:

1. Navigate to the **Native Types** tab.
2. In the mass action drop-down menu in the lower left, select **All**.
3. From the same menu, select **Export to File**.
4. Click **Go**.

Note: Relativity does not support Framesets in MHT files.

13.17 Supported file types for imaging

Relativity imaging supports many different file types. The following table lists supported and unsupported file types for Native and Basic imaging.

Other supported file type pages: Processing | Viewer

13.17.1 Categories

Container files | Database, spreadsheets | Document, text, word processors | Email, messaging, chat | Graphics, images | Other

File type	File extension	Supported	
Container files		Native	Basic
Compressed files	7z, .zip, .tar, .gz, .bz2, .rar, Z, .cab, .alzip		✓
Relativity Collection Container	.rcc		
File type	**File extension**	**Supported**	
Database, spreadsheets		Native	Basic
Database files	.dbf		
Excel	.xlsx, .xlsm, .xlsb, .xlam, .xltx, .xltm, .xls, .xlt, .xla, .xlm, .xlw, .uxdc	✓	✓
File type	**File extension**	**Supported**	
Document, text, word processors		Native	Basic
Adobe files	.pdf, .fm, .ps, .eps	✓	✓
Hangul Word Processor	.hwp		✓
HTML	.html, .mht, .htm, .mhtml, .xhtm, .xhtml **Note:** While Relativity native imaging supports MHT files, it does not support MHT framesets.	✓	✓
JungUm Global	.gul	✓	✓
Text files	.txt, .csv, and others	✓	✓
Word	.docx, .docm, .dotx, .dotm, .doc, .dot, .rtf	✓	✓
WordPerfect	.wpd, .wps	✓	✓
File type	**File extension**	**Supported**	
Email, messaging, chat		Native	Basic
AppleDouble	AppleDouble-encoded attachments in e-mails		✓
Email	.msg, .p7m, .p7s, .ics, .vcf, .eml, .emlx, .tnef	✓	✓

File type	File extension	Supported	
Email containers	.pst, .ost, .dbx, .mbox, .nsf, and Bloomberg .xml		✓
Short message	.rsmf		✓

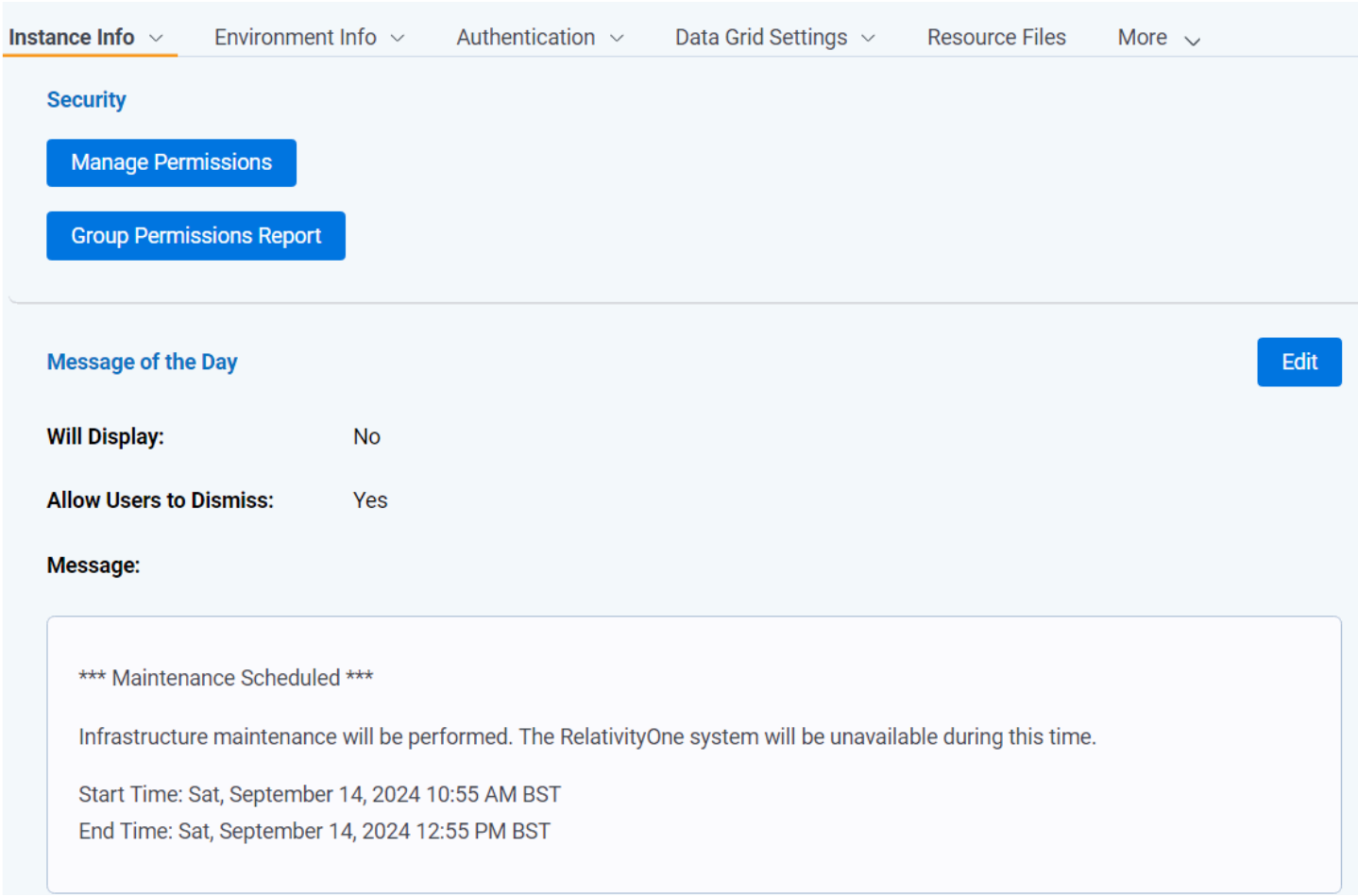
File type	File extension	Supported	
Graphics, images		Native	Basic
CAD files	.dxf, .dwg, .slddrw, .sldprt, .3dxml, .sldasm, .prtdot, .asmdot, .drwdot, .stl, .eprt, .easm, .edrw, .eprtx, .edrwx, .easmx		✓
EnCase	.e01, .ex01, .l01, .lx01		
Image files	.jpg, .jpeg, .ico, .bmp, .gif, .tiff, .tif, .jng, .koala, .lbm, .pbm, .iff, .pcd, .pcx, .pgm, .ppm, .ras, .targa, .tga, .wbmp, .psd, .cut, .xbm, .dds, .fax, .sgi, .png, .exf, .exif, .wdp	✓	✓
Image files	.webp **Note:** This extension can be imaged using the native imaging method on Server 2022, Server 2023, Server 2024 and Relativity aiR. It cannot be imaged on Server 2021.	✓	
Image files	.heic		✓
Vector files	.svg, .svgz, .wmf, .plt, .emf, .snp, .hpgl, .hpg, .plo, .prn, .emz, .wmz **Note:** Relativity only supports the text within .svg files. Any images within .svg files will not be displayed. An .svg file with only images will be completely blank.	✓	✓
Visio	.vsd, .vdx, .vss, .vsx, .vst, .vsw, .vsdx, .vsdm	✓	✓

File type	File extension	Supported	
Other		Native	Basic
Apple iWork suite (Pages, Numbers, Keynote)	.pages .numbers .key **Note:** Encrypted iWork files are not supported.		✓
OpenOffice	.odc, .ods, .odt, .odp, .xps	✓	✓
OneNote	.one	✓	✓
Microsoft Project 2013 **Note:** Microsoft Project 2016 is not supported	.mpp	✓	

File type	File extension	Supported	
PowerPoint	.pptx, .pptm, .ppsx, .ppsm, .potx, .potm, .ppt, .pps, .pot	✓	✓

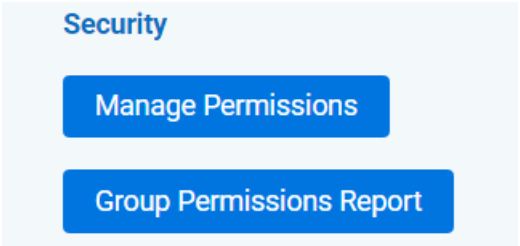
14 Instance Details tab

The Instance Details tab provides basic information for managing instance security and any messages you want users to see after they log into the environment.



14.1 Security

In the Security section, you can manage group permissions and generate a group permissions report.



14.1.1 Manage Permissions

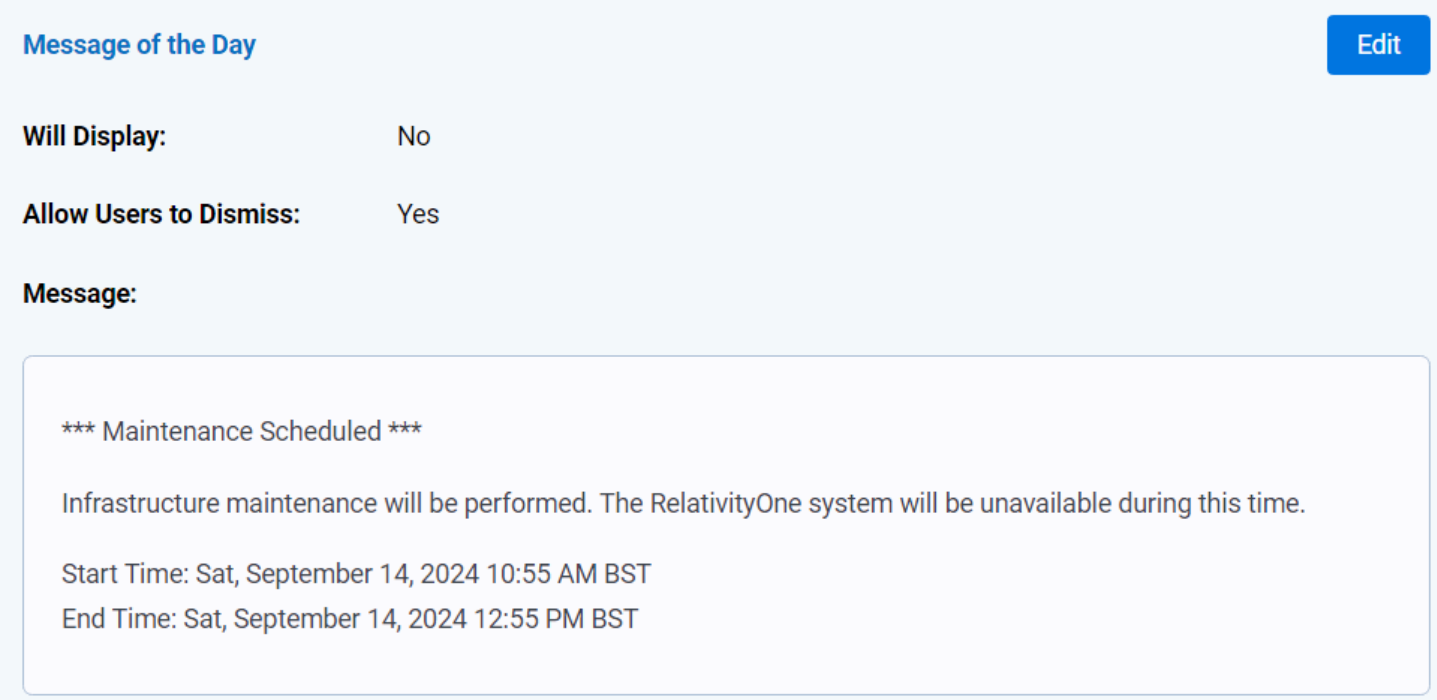
Click **Manage Permissions** to open the Admin Security console. See Instance security for more information on how to manage group permissions.

14.1.2 Group Permissions Report

Click **Group Permissions Report** to open the Script: Admin Group Permissions console. See Instance security for more information on how to run a group permissions report.

14.2 Message of the Day

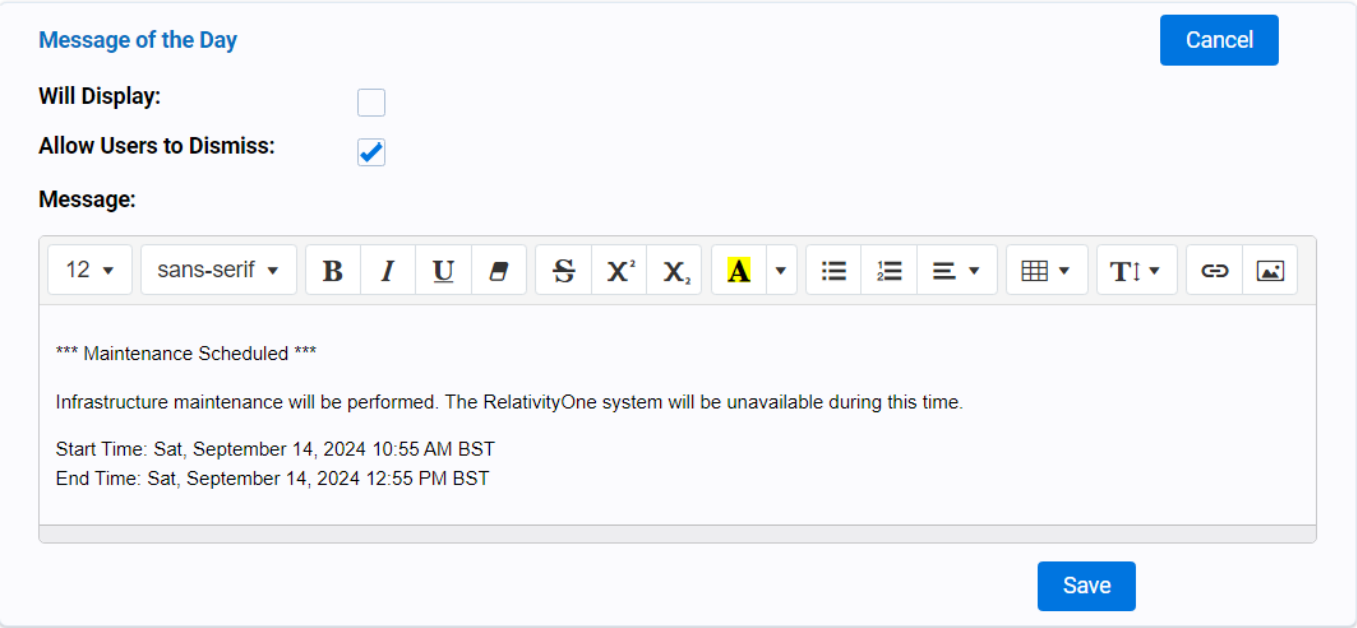
The Message of the Day is a message that appears to all users when they log in to Relativity. This is most commonly used to inform users of planned system maintenance, but you can use this feature to display any content you want. Only System Administrators can modify the Message of the Day.



To activate or edit the Message of the Day:

1. Click **Edit** in the Message of the Day section. The button is in the upper right corner of the section.

2. Enter a new message or edit an existing message. Use the text editor controls to customize the look and feel of your message.



3. Select the **Will Display** checkbox to activate the message for users when they log into Relativity.
4. Select the **Allow Users to Dismiss** checkbox to allow users to hide the message.
    - If you enable this setting, users will see a checkbox in the message stating **Do not show me this message next time.** Users will not see the message again, including when they log back in to Relativity, unless it is changed to a new one.
    - If you disable this setting, users will see the message every time they login.
5. Click **Save**.

15 Keyboard shortcuts

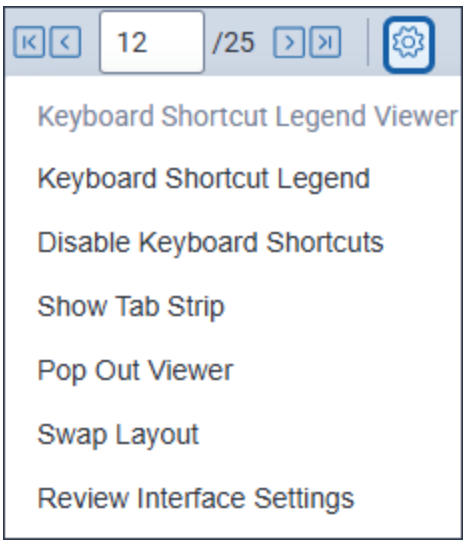
With keyboard shortcuts you can edit and navigate in the Review Interface. Using keyboard shortcuts, you can change Viewers, populate choices, save edits, cancel edits, and move between and within documents. Keyboard shortcuts are enabled by default. To disable shortcuts while using the Review Interface, click on the Viewer Settings menu in the upper-right and select the **Disable Keyboard Shortcuts** option.

Users with permissions to edit fields and choices can create additional shortcuts using the Keyboard Shortcuts property on the choice.

You can modify the key combinations for system keyboard shortcuts if you have security permission for the Admin Operation called **Modify System Keyboard Shortcuts**. For more information about this permission see workspace security in the Admin guide.

15.1 Keyboard shortcuts legend

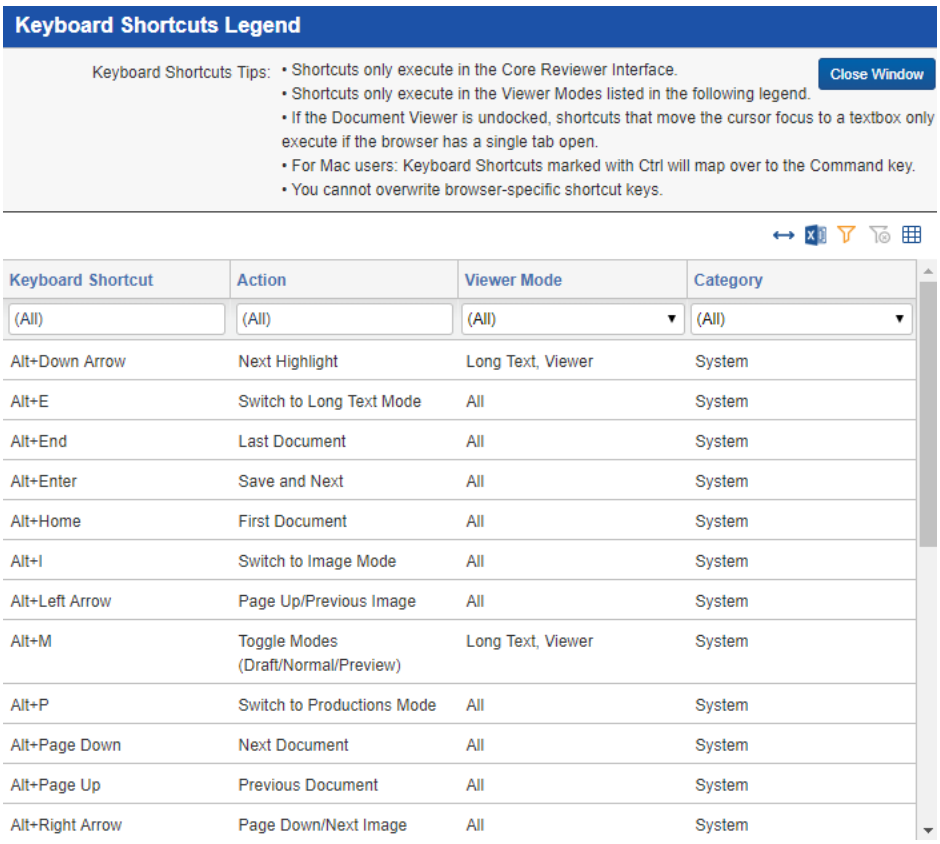
By default, standard user actions use system keyboard shortcuts. Keyboard shortcuts are listed in the Keyboard Shortcut Legend along with those used by the browser. You can access the legend by clicking on the Viewer Settings menu in the upper-right of the Review Interface and selecting the **Keyboard Shortcut Legend** option.



Within the legend, you can sort, filter, Export to Excel, and print. You can print by right-clicking and choosing the browser's print option.

The Keyboard Shortcuts Legend includes the following sortable columns:

- **Keyboard Shortcut** - the key combination used to execute the shortcut during document review.
- **Action** - the action that results from using the keyboard shortcut.
- **Viewer Mode** - the type of Viewer for which each shortcut is available. You can use most of the system category shortcuts in all viewer modes.
- **Category** - the shortcut type. Below, the legend displays only those shortcuts designated by the System and the browser. This column also lists all field and choice shortcuts that your system admin configured via field and choice properties.



Keyboard Shortcut	Action	Viewer Mode	Category
(All)	(All)	(All)	(All)
Alt+Down Arrow	Next Highlight	Long Text, Viewer	System
Alt+E	Switch to Long Text Mode	All	System
Alt+End	Last Document	All	System
Alt+Enter	Save and Next	All	System
Alt+Home	First Document	All	System
Alt+I	Switch to Image Mode	All	System
Alt+Left Arrow	Page Up/Previous Image	All	System
Alt+M	Toggle Modes (Draft/Normal/Preview)	Long Text, Viewer	System
Alt+P	Switch to Productions Mode	All	System
Alt+Page Down	Next Document	All	System
Alt+Page Up	Previous Document	All	System
Alt+Right Arrow	Page Down/Next Image	All	System

15.2 Special considerations for keyboard shortcuts

Keep in mind the following when working with Relativity's keyboard shortcuts feature:

- For Mac users, keyboard shortcuts marked with Ctrl map over to the Command key.
- Keyboard shortcuts are active when:
  - Keyboard shortcuts are enabled.
  - Focus is in the Review Interface.
  - The Viewer is either docked or undocked while the browser only has one tab open.
  - If the shortcut overlaps with a Windows shortcut, both shortcuts are triggered. For example, if a program installed on a user's computer uses the Ctrl + Alt + R shortcut, clicking Ctrl + Alt + R triggers that action regardless of whether a user is in any of Relativity's supported browsers.
- Keyboard shortcuts aren't triggered when:
  - Keyboard shortcuts are disabled.
  - Focus is not in the Review Interface.
  - The Viewer is undocked or in standalone mode, and the browser has more than one tab open.
- When the numbers 0-9 are used as shortcuts, they only fire when you press these digits in the main section of the keyboard. The shortcut doesn't fire if you press those digits found in the keypad.
- Keyboard shortcuts only execute in the Review Interface.
- Keyboard shortcuts only execute in the Viewer Modes listed in the legend.

- If the document viewer is undocked, shortcuts that move the cursor focus to a text box only execute if the browser has a single tab open.

15.3 Document field type shortcuts

The following table outlines what document field types users can define shortcuts for and what behavior the shortcuts trigger. You can also define keyboard shortcuts on individual choices for single & multiple choice fields, rather than the field itself. See the Document choice shortcuts table below for information on setting keyboard shortcuts for individual choices.

Field Type	Can define shortcut?	Layout Display Type	Behavior
Fixed Length Text	Yes	Text	Focus jumps to textbox
Long Text	Yes	Text Only	Focus jumps to textbox
		Rich Text	NO ACTION
Date	Yes	Date	Focus jumps to textbox
Whole Number	Yes	Integer	Focus jumps to textbox
Decimal	Yes	Decimal	
Currency	Yes	Currency	
User	Yes	Drop-down menu	Drop-down menu choices are toggled
		Picker	NO ACTION
Boolean	Yes	Checkbox	Checkbox state is toggled
		Drop-down menu	Drop-down menu choices are toggled
		Radiobutton	Radio button selected
Single Choice	No		
Multiple Choice	No		
Single Object	No		
Multiple Object	No		
File	No		

15.4 Document choice shortcuts

The following table outlines what document individual choices users can define shortcuts for and what behavior the shortcuts trigger:

Choice Type	Can define short-cut?	Layout Display Type	Behavior
Choice associated with Document Single Choice Field	Yes	Radio button	Choice is selec-ted/deselected
		Drop-down menu	Choice is selec-ted/deselected
Choice associated with Document Multiple Choice Field	Yes	Checkbox	Choice is selec-ted/deselected

Choice Type	Can define short-cut?	Layout Display Type	Behavior
		Popup Picker	NO ACTION

15.5 Creating keyboard shortcuts

Any user with permissions to create or edit a choice can create keyboard shortcuts.

The action that a shortcut triggers depends on the layout display type selected for the fields and choices. See Document field type shortcuts on the previous page and Document choice shortcuts on the previous page.

You can't define shortcuts for system actions or browser-defined shortcuts. See Keyboard shortcuts on page 301 and Keyboard shortcuts on page 301 for details.

You can configure user defined keyboard shortcuts on the Choices tab. These properties are identical to each other. To configure a choice shortcut, perform the following steps:

1. Navigate to the **Choices** tab.

   Note: You can also edit an existing Document field in this manner. See Fields on page 196.

2. Click the **Edit** icon in the row of the choice you would like to edit.
3. Click the **Select** button next to the Keyboard Shortcut field.
4. Select the desired key for the **Modifier Key(s)** field.
5. Choose the desired key from the **Main Key** drop-down menu.
6. Click **Apply**.
   If this shortcut is valid, you receive a message saying **<Valid Keyboard Shortcut>**
7. Click **Save**.
8. Navigate to the **Documents** tab and open a document.
9. Click on the Viewer Settings menu in the upper-right and select the **Keyboard Shortcut Legend** option.
10. Edit any layout and add a field that contains the choice that you assigned a keyboard shortcut to.
11. Using your keyboard, verify that the keyboard shortcut is working by holding down and pressing the assigned keys.

16 Layouts

Layouts are web-based coding forms that give you the ability to view and edit document fields. You can use layouts to develop workflows specific to the needs of your case. You can develop layouts that contain only the fields required to complete specific review tasks, making the review process clean and intuitive. You can also use object-level permissions to turn layouts on and off as necessary.

16.1 Layouts permissions

The following permissions are needed to use layouts:

Object Security	Tab Visibility	Other Settings
• Layout - View, Edit,	• Workspace	None

Object Security	Tab Visibility	Other Settings
Delete, Add • Relativity Application - View	Admin • Layouts	

16.2 Creating and editing layouts

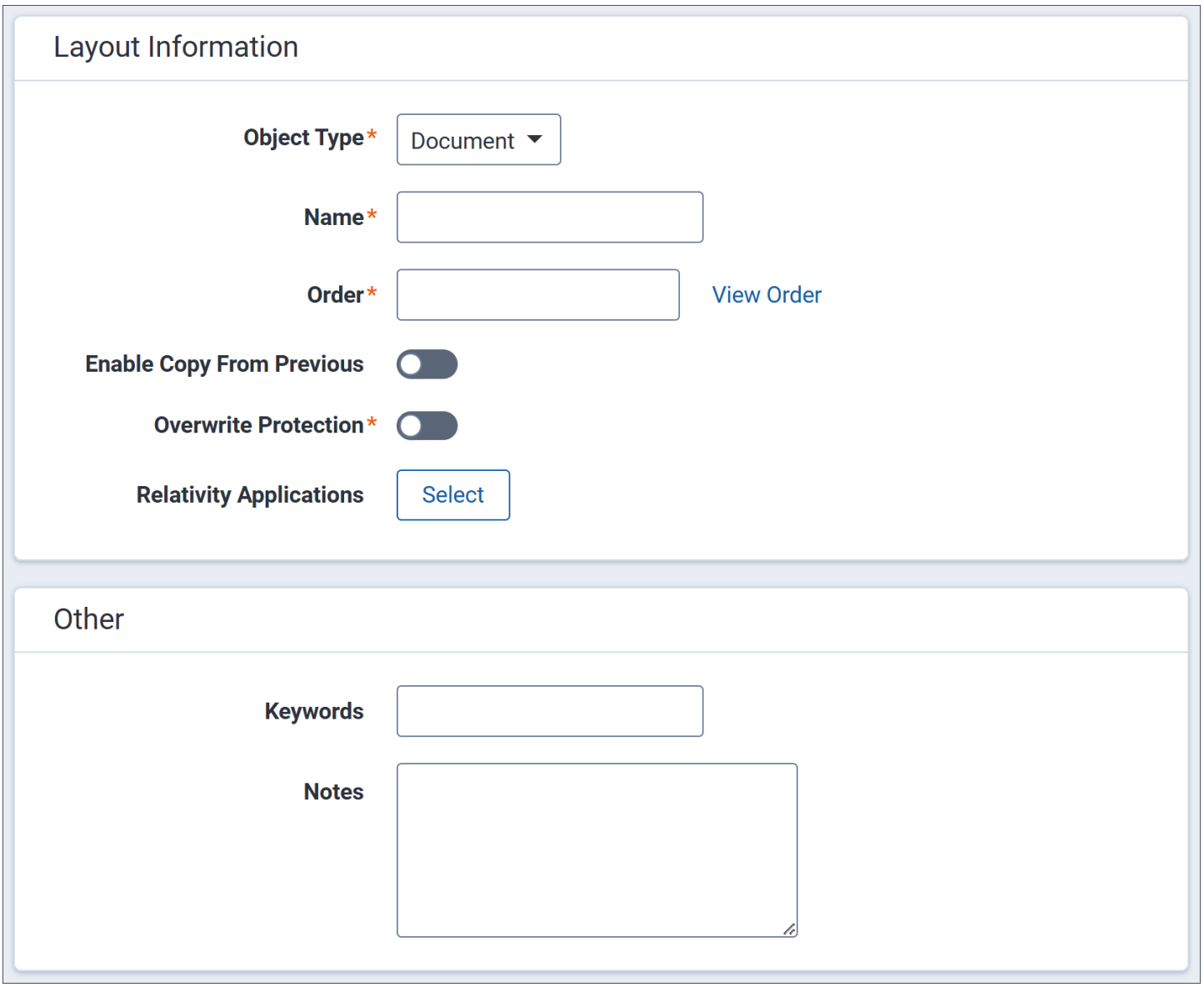
To create a new layout or edit an existing one:

1. Navigate to the **Layouts** tab.
2. Click **New Layout**. To edit a layout, click the **Edit** link next to the layout's name. The Layout Information details layout opens.
3. Complete the required fields on the Layout Information layout. An orange bar to the right of the field name indicates that it is required. See Layout Information fields below
4. Click **Save**.
5. From the Layout console, click **Build Layout** to open the layout builder. See Using the layout builder on page 309.

Note: We recommend avoiding sensitive data in Layout names. Do not embed personal identifiers in Layout names (for example, use **QA Review** instead of **John Smith Review**).

16.3 Layout Information fields

The Layout Information contains the following fields:



Layout Information

- **Owner** drop-down—determines which users can view the layout. Select from the following options:
  - **Public**—all users can see the layout. This is the default selection.
  - **Specific User**—limits the visibility of the layout to the selected user in the drop-down.
  - **Me**—limits visibility to the logged in user.

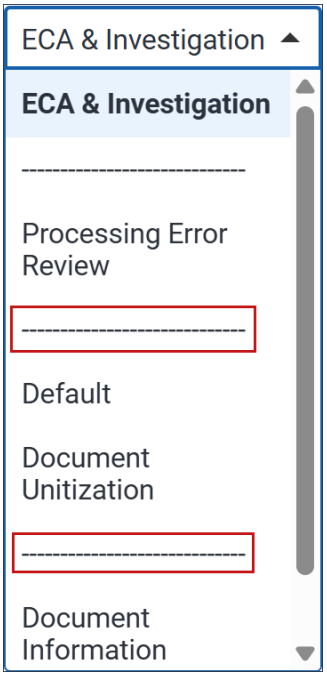
  Note: System admins can view layouts and other securable items that users have made private.

- **Object Type**—the object type that the layout uses to modify or code. For example, select Document as the object type if you were creating a layout for coding documents.

  - **Note:** The Document layout is the only layout that contains the Enable Copy From Previous field. See Copy from Previous on page 319

- **Name**—the name of the layout. There is a 50-character limit for this field.

- **Order**—the number that represents the position of the layout in relation to the other layouts. The lower the number, the higher the position on the list. Layout order can be any positive or negative integer, but you can't use decimals.
    - **View Order**—click to open up a pop-up window displaying the order of existing views.
- **Overwrite Protection**—prevents a user from saving changes to an item that another process has modified since the user opened or edited the layout. By default, this field is set to **Disabled**.
    - You can edit this field only when the instance setting **AllowChangesToOverwriteProtection** is set to **True** in the instance setting table in SQL. By default, this value is False. See AllowChangesToOverwriteProtection instance setting in the Instance setting guide. Contact Relativity Support if you would like to edit this instance setting in your environment.
    - If you disable Overwrite Protection, we recommend that you avoid using **Save & Next** while coding documents because there is a possibility that your coding decisions may not be saved if another user is editing the same document at the same time. Instead, as a best practice, we recommend clicking **Save** and then carefully reviewing the layout to ensure your coding selections have been saved before navigating to the next document.
- **Relativity Applications**—associates the layout with an application created in the Relativity Applications tab. Click **Select** to display the Select Items pop-up, and choose an application. To set this option, you must have the permission Manage Relativity Applications, available under Admin Operations on the Security page. If users have many layouts that they use during document review, you can add a new layout with dashes in the Name field, (----------) and an appropriate order number to serve as a separator. This assists in organizing layouts and building the workflow.



Other

- **Keywords**—include any key words to associate with the layout.
- **Notes**—contains any notes regarding the layout.

16.3.1 Changing layouts

The layout with the lowest order number displays by default when a user opens a document. Depending on your screen resolution and the length of the current layout's name, it may appear truncated in the layouts drop-down menu.

To display a tool-tip with the layout's full name, hover your cursor over the layouts drop-down menu.

You can change layouts before or while you are reviewing documents by doing the following:

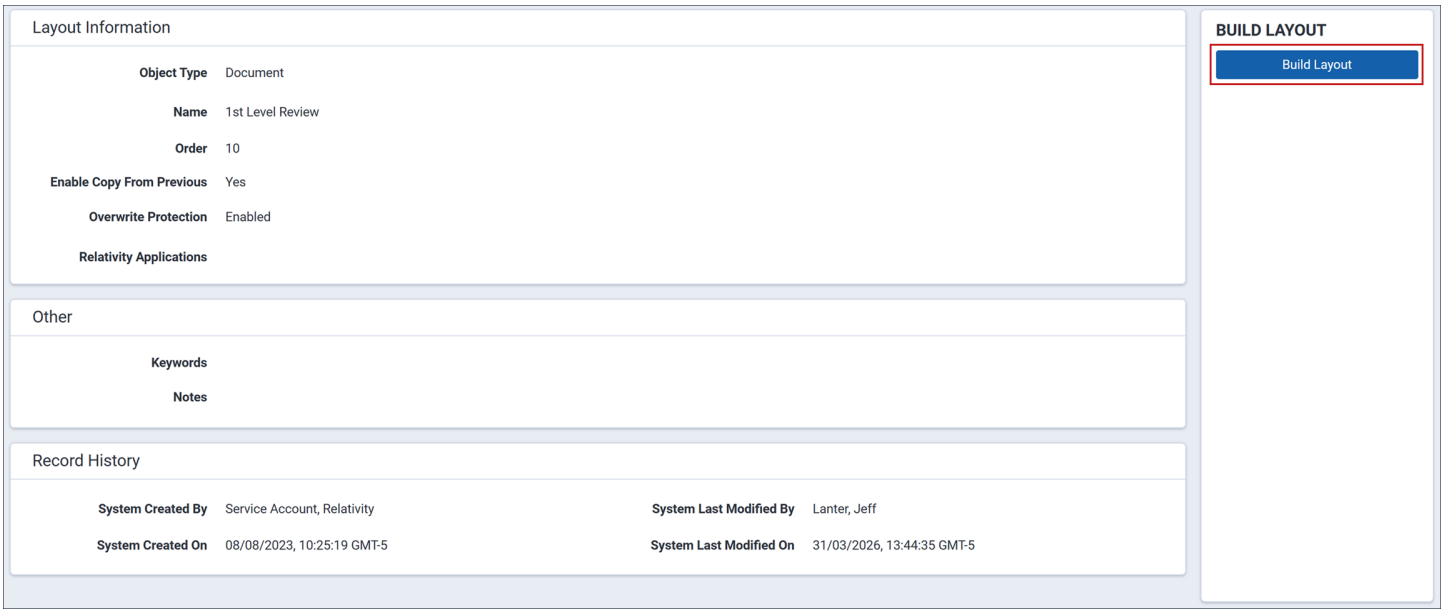
1. Click on the layouts drop-down menu.
2. Select the desired layout.

> **Note:** If you have entered a coding decision and have not saved it before selecting a new layout, a pop-up will display. Click **Cancel** to go back and save the coding decision before changing layouts or click **OK** to discard the coding decision and proceed to the new layout.

16.4 Using the layout builder

The layout builder is a customizable screen where users can create a layout. The layout console exists within the layout builder, which is available once you save a layout or when you select an existing layout from the Layout List page.

To build a layout, click **Build Layout** in the **Layout console**. The layout builder appears.



The layout builder contains the following components:

- **Edit Layout Information: [Layout Name]**—click this link to navigate back to edit mode for the layout you are currently updating. See Creating and editing layouts on page 306.
- **Category**—contains fields on the layout. See Adding and editing categories on page 318.
- **Layout group**—consists of one or more categories or object lists in a tabular format. See Creating and editing a layout group on the next page.

16.4.1 Layout Options console

Use the Layout Options console to build your layout. Clicking an item to the left of the console displays that item's properties for you to interact with.

The Layout Options console contains the following items:

- **Properties**—depending on the selected item in the layout, that item's properties appear here. See Field properties on page 317 or Object list properties on page 313.

  Note: From the Properties section, click to collapse the properties or click to expand an item's properties.

- **Add Category/Add Object List** drop-down—use these buttons to add a category or an object list to the layout.
  - **Add Category**—adds a new category to the layout. See Adding and editing categories on page 318.
  - **Add Object List**—adds a new object list to the layout. See Adding and editing an object list on page 312.
- **Fields**—drag and drop available fields onto the layout category or object list. See Adding fields and text on page 314.

  Note: You cannot add fields stored in Data Grid to layouts.

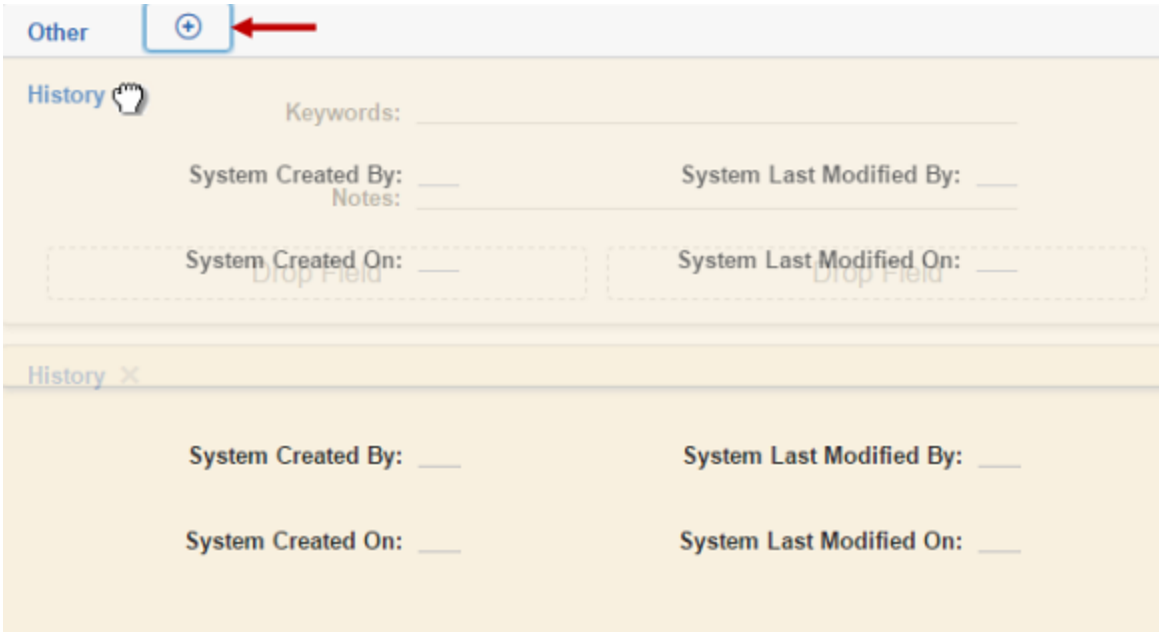
16.4.2 Creating and editing a layout group

A layout group consists of one or more categories or object lists that display in a tabular format to maximize screen space and eliminate scrolling in the layout. Use layout groups on the Document or RDO layout.

Note: A layout group may consist of both categories and objects.

To create a layout group:

1. From the layout builder, click and drag a category/object list over another category/object list, then let go of your cursor click. A plus sign appears to the right of the category that you're dragging the other category onto.

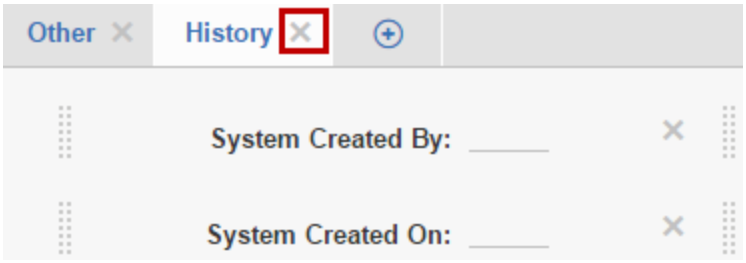


   The category/object list appears in a new tab.



2. Click ⊕ or drag another existing category/object list onto the layout group to add more items to the group.
3. Click **Save** or **Save and Close**.

To delete a category/object list, click ✕ next to the item. If the category/object list contains fields, a warning appears before deletion.

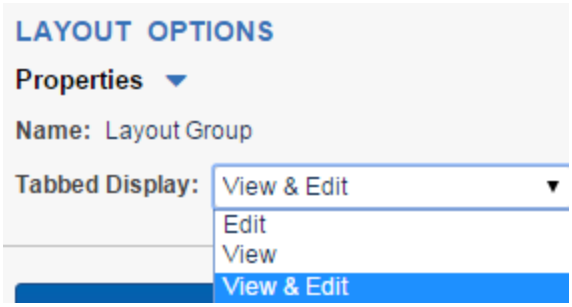


To move a category/object list outside of a layout group, click and drag that item out of the group and place anywhere on the layout.

16.4.2.1 Layout Group properties

When you select a layout group, the Layout group properties appear in the Layout Options console.

Note: From the Properties section, click ▼ to collapse the properties or click ▲ to expand an item's properties.



The layout group properties contain the following items:

- **Name**—the name of the layout group property.
- **Tabbed Display**—this option determines when to render the layout group as tabs. When the layout group does not display as tabs, it displays in a sequential, vertical list.
  - **Edit**—displays the tabbed layout group only when a user is in edit mode. Once the user saves and views the layout, the categories render in a list.

- **View**—displays the tabbed layout group only when a user is in view mode. When the user is editing the layout, the categories render in a list.
- **View & Edit**—displays the tabbed layout group when a user is in view and edit mode.

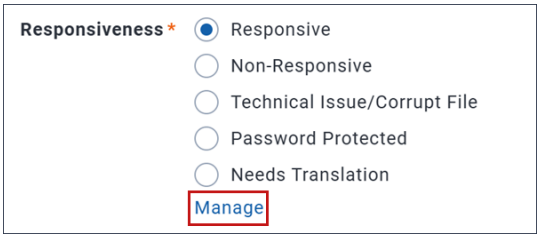
16.4.3 Saving the layout

Changes made to a layout are applied when you click **Save**. The next time a user loads the layout when editing or selecting to go to the next document, the changes are visible.

If a user is in the process of editing a document when a change is made to the layout, the Overwrite Protection setting determines whether the user can successfully save those edits, or if they need to re-open the layout and make their selections again before saving.

16.5 Adding a choice to a layout

To add a choice to a layout in edit mode:



1. Click the **Manage** link on a single choice or multiple choice field on the layout. The Choice editor modal opens.
2. Click **Add Choice**,**Add Many Choices**, or **Click to add a choice**.
3. Enter a name for the choice or many choices.
4. (Optional) Click **Details** to further customize the choice.
5. Modify the details of the choice.
6. Click **Close**.

New choices appear at the bottom of the list of choices. New choices also appear in the Choices tab and Field forms.

Note: If you have edit permissions, you can reorder the choice.

16.6 Pop-ups on the layout

In most instances, choices and objects appear as check boxes and radio buttons. Occasionally there are too many options to reasonably display on the layout, such as in a large list of issues. In these cases, you can display the choices in a pop-up picker. To add a field with a pop-up display, select **Popup Picker** on the **Display Type** field on the Add or Edit Field to Layout form.

To access the pop-up display for a field, click **Select**. You can filter the choices in the pop-up to locate the desired one.

16.7 Adding and editing an object list

You can add a list of child objects to layouts for the parent object type, and you can add associative object lists to objects related by a single or multiple object field. Use the Layout Options console to add these lists to layouts when child or associative objects exist for the current object type.

Note: Child and associative objects frequently refer to user-created objects in Relativity. These Dynamic Objects are securable, non-document objects that you can add to a workspace. You can link Dynamic Objects to documents and to other object types to create powerful custom applications within your workspace.

16.7.1 Adding and editing an object list

To add an object list:

1. From the Layout Options console, click the **Add Category** drop-down > **Add Object List**. A new Object List appears in the layout builder and its corresponding properties appear in the Layout Options console. To edit an existing object list, click the object list.
2. Make changes to the properties as applicable. See Object list properties below.
3. Click **Save** or **Save and Close**.

To delete an object list, click next to the item. If the object list contains fields, a warning appears before deletion.



To move an object list, click and drag the item to anywhere on the layout.

16.7.1.1 Child and associative object lists

Once you add an object list to a layout, the child object layout details includes a child list of all items. The list provides the following option for working with the child objects:

- **New** - creates a new object of the type represented in the list.
- **Delete** - removes objects from Relativity.

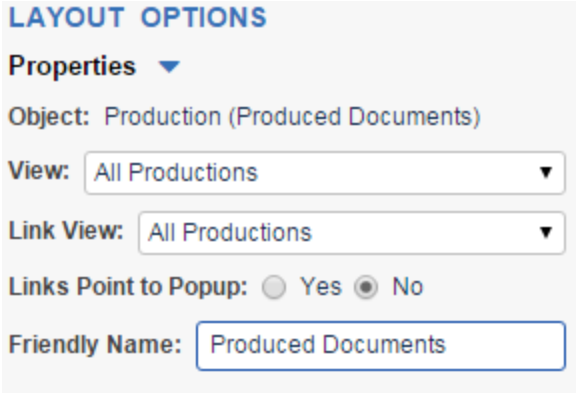
The associative object list provides the following options:

- **New** - creates a new object of the type represented in the list.
- **Link** - displays a pop-up for adding objects of the same type to list.
- **Unlink** - removes objects from the list.

16.7.1.2 Object list properties

Note: From the Properties section, click to collapse the properties or click to expand an item's properties.

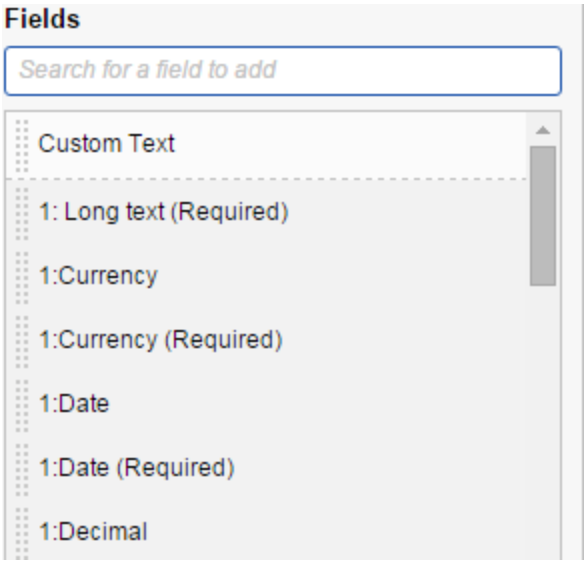
The object list properties contain the following items:



- **Object** - displays available object types (child or associative). Your selection determines the type of objects that appear in the list. If there are no available linked objects, a warning appears.
- **View** - displays views available for the selected child or associative object.
- **Link View** - determines which fields are available when clicking the Link button to link to an existing object to the current layout's object.
- **Links Point to Popup** - creates a hyperlink that displays object details in a pop-up. Select **Yes** to create the link or **No** if you do not want the link available.
- **Friendly Name** - re-name the object list to a more user-friendly name.

16.8 Adding fields and text

Use the fields in the Layout Options console to create your layout. Search for available fields in the search box. Relativity automatically places wild cards at the beginning and end of the entered characters. The list of available fields is dependent on the layout Object Type and any fields created with the same Object Type.



16.8.1 Layout options

The Layout Options contain the following fields:

- **Field** - displays the name of the field that is added. You can select any available workspace field. You can add a specific field only once to the layout.

Note: You can't add fields stored in Data Grid to layouts.

- **Display Type** - controls how the field appears on the layout. The field type determines the available display options:
  - **Fixed length** - text appears as text.
  - **Whole number** - appears as an integer.
  - **Date** - appears as a date.
  - **Yes/no** - has three values - blank, yes, or no. This field can be displayed as a drop-down menu, check-box, or radio button list.
  - **Long text** - appears as text.

    Note: If a field with long text is selected and it contains enough text, the long text field may affect the display of other fields in the layout that are beneath it.

  - **Rich text** - appears as text with bold and italics. This option is only available if the field has the Allow HTML property set to Yes.

    Note: The Sanitizer object controls whether HTML attributes are sanitized and how specific HTML content is sanitized from fields on page render. You can modify the sanitizer object to add HTML alerts and links. We recommend not modifying the default setting.

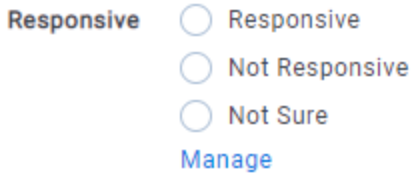
  - **Single-choice list** - appears as a drop-down menu or radio button.
  - **Decimal** - appears as a decimal.
  - **Currency** - appears as currency.
  - **Multiple-choice** - list can appear as a checkbox list or pop-up picker. A pop-up picker displays the field label and a box containing the current field values. Reviewers click 

, which displays a filterable list of field choices. Filtering can be applied to pop-up picker views to find choices. For more information on the pop-up picker, see Pop-ups on the layout.

    Note: If a coding layout becomes long and cumbersome, change the field display from checkbox list to pop-up picker. This unclutters the layout by effectively hiding the field's choices and presenting them only if necessary. Displaying a large number of choices with check boxes, drop-down menus, or radio buttons on a layout can also slow performance. The display type automatically flips to a pop-up picker if the number of choices exceeds the configurable choice display limit.

  - **User** can appear as a drop-down menu or a picker.
- **Repeat Columns** controls how single and multiple-choice lists appear on a layout. When you select this option for a multiple-choice field, choices are ordered left to right, and top to bottom.

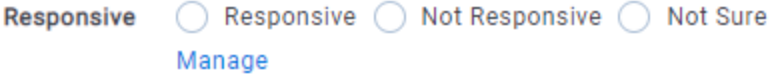
- **Single Column Display:** Enter 0, 1, or leave the option blank.



- **Multiple Column Display:** Enter any value higher than 1 to set the number of columns. A value of 2 results in a two column display.



A value of 3 results in a three column display.



- **Custom label** is used to display your own text instead of the field name. Click  button to enter your custom label.

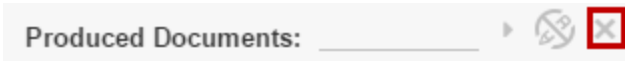
16.8.2 Adding fields to a category

To add fields to a category, drag and drop a field from the Fields section to the category. *Drop Field* placeholder text appears to indicate where you can place fields on the category.



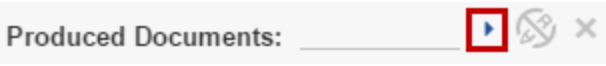
16.8.3 Removing fields from a category

To remove a field from a category, click  next to the field. The layout builder moves that field back to the Fields list for future use.

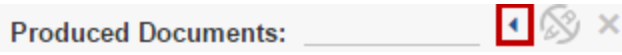


16.8.4 Making a field one or two column

To make a one column field two columns, click .

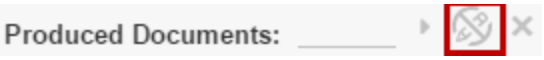


To make a two column field one column, click .



16.8.5 Making a field read-only

To make a field read-only, click .



Note: The option **Allow Copy from Previous** is disabled for fields that have their **Read-Only** option set to **Yes**, as well as for system and relational fields such as MD5 HASH. See Copy from Previous on page 319.

16.8.6 Other fields considerations

- You can drag and drop fields from one category to another.
- You can drag and drop fields from one column to another.
- Add custom text by dragging and dropping the Custom Text field to a layout. To edit, select the Custom Text field and edit the Custom Text in the text box or the rich text editor. If you enter rich text, the message *Rich text added* appears. See Using the rich text editor on page 322.
- Certain HTML-enabled text fields such as Email Threading Display may not display correctly if you add them to a layout.

16.8.7 Field properties

Depending on the field selected in the layout builder, different properties appear. Below is a list of the following field properties:

Display Type - controls how the field appears on the layout. The field type determines the available display options:

- **Fixed length** - text appears as text.
- **Whole number** - appears as an integer.
- **Date** - appears as a date.
- **Yes/no** - has three values - blank, yes, or no. This field can be displayed as a drop-down menu, checkbox, or radio button list.
- **Long text** - appears as text.

Note: If a field with long text is selected and it contains enough text, the long text field may affect the display of other fields in the layout that are beneath it.

- **Rich text** - appears as text with bold and italics. This option is only available if the field has the Allow HTML property set to Yes.
- **Single-choice list** - appears as a drop-down menu or radio button.
- **Decimal** - appears as a decimal.
- **Currency** - appears as currency.
- **Multiple-choice** - list can appear as a checkbox list or pop-up picker. A pop-up picker displays the field label and a box containing the current field values. Reviewers click  , which displays a filterable list of field choices. Filtering can be applied to pop-up picker views to find choices. For more information on the pop-up picker, see Pop-ups on the layout.

  Note: If a coding layout becomes long and cumbersome, change the field display from checkbox list to pop-up picker. This unclutters the layout by effectively hiding the field's choices and presenting them only if necessary. Displaying a large number of choices with check boxes, drop-down menus, or radio buttons on a layout can also slow performance. The display type automatically flips to a pop-up picker if the number of choices exceeds the configurable choice display limit.

- **User** can appear as a drop-down menu or a picker.
- **Show Name Column** displays the field name as label when you select this checkbox. Clear the checkbox to hide the label.
- **Rows (long text only)** is used to set the number of visible lines in a long text box, such as attorney comments.
- **Custom label** is used to display your own text instead of the field name. Edit the Custom Text in the text box or click  to open the rich text editor. See Using the rich text editor on page 322. If you enter rich text, the message *Rich text added* appears.

16.9 Creating a new category

Categories act as headers that visually divide the layout into different sections. You can create a category for each sub-task in a review.

For each layout, Relativity automatically creates a default category. The category contains a default name field that Relativity assigned to it based on the layout's object type. For example, the default category contains the document identifier when the object type of the layout is document and a Name field when the object type is OCR Set or Analytics Profile.

16.9.1 Adding and editing categories

A category contains fields on your layout. Use categories to organize layout content.

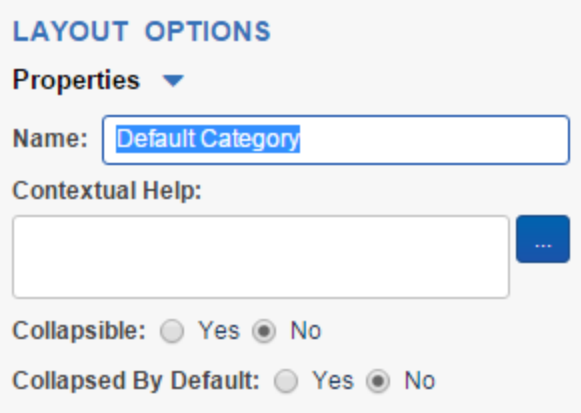
To add a new category:

1. From the Layout Options console, click **Add Category**. A new Default Category appears in the layout builder and its corresponding properties appear in the Layout Options console. To edit an existing category, click the category.
2. Make changes to the properties as applicable. See Category properties on the next page.
3. Click **Save** or **Save and Close**.

16.9.2 Category properties

Note: From the Properties section, click to collapse the properties or click to expand an item's properties.

The category properties contain the following items:



- **Name** - the name of the category. This name appears as a section header in the layout.
- **Contextual Help** - add contextual help text to the layout to further guide users as they are interacting with the fields in this category.
  - Enter text in the field to add plain text contextual help.
  - Click the **Rich Text Editor** icon to load a web-based rich text editor where you can enter and edit rich text contextual help. See Using the rich text editor on page 322. If you enter rich text, the message *Rich text added* appears.
  - Contextual Help appears as the **Additional information** icon in the layout. Users can click this icon to display the contextual help message.
- **Collapsible** - Determines whether the category can be collapsed or not in a layout. If **Yes** is selected, the category can be collapsed by the user. If **No** is selected, the category cannot be collapsed by the user even if Collapsed By Default is set to **Yes**.
- **Collapsed By Default** - Determines whether the category is collapsed when each document is loaded in the Viewer or not. If Collapsible is set to **Yes** and **Yes** is selected for this option, the category will be collapsed by default whenever a document is opened in the Viewer. If **No** is selected, the category will be expanded whenever a document is opened in the Viewer.

16.10 Copy from Previous

You can design a layout to include the **Copy from Previous** toolbar. This enhances review by providing the ability to copy coding values from one document to another within a review session. The **Enable Copy From Previous** and **Allow Copy From Previous** options have to be enabled on both the layout and field respectively to use this feature.

After you've coded and saved a document as part of the review process, an icon displays in the layout next to any fields that are eligible for Copy from Previous. A value for each eligible field has to be selected and then saved before you can use Copy from Previous. If there is a field where no value was selected, then it is not eligible for Copy from Previous and the icon does not display to denote this.

Copy from Previous is not available for the following fields:

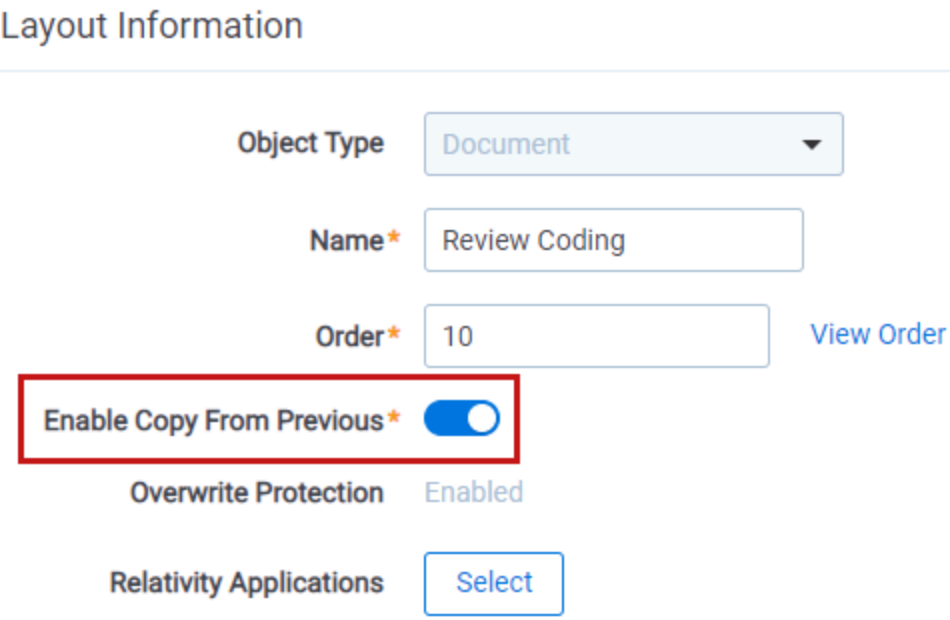
- Single object fields
- Multi-object fields
- Read only fields
- System fields
- Relational fields
- Control Number (Document ID)

Note: Copy from Previous always mirrors the parent document's current field values at the time the action is triggered. It does not reference any historical state. If fields have been added to or removed from the parent document since a prior review, the child document remains eligible for Copy from Previous. Only the parent's currently configured fields and values are copied. Any choice that no longer exists on the parent will not be carried forward to the child.

16.10.1 Adding the Copy from Previous toolbar

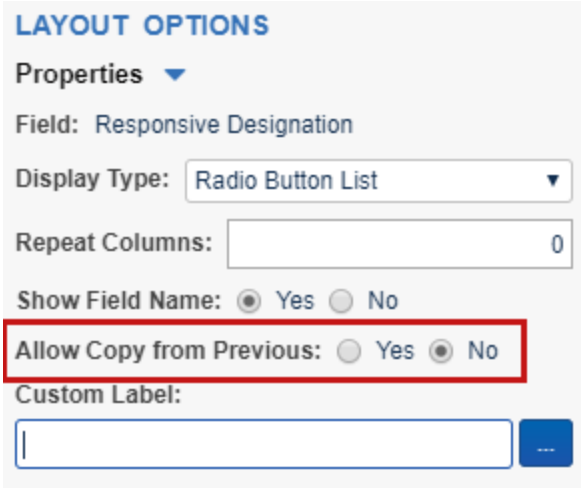
You can add the Copy from Previous toolbar to any layout with a Document object type. To add this toolbar:

1. Navigate to the **Layouts**, click the layout on which you want to enable Copy from Previous.
2. Click **Edit**.
3. On the layout, click on the desired field and set **Enable Copy from Previous** to **Yes**.



4. Ensure that all applicable fields on the layout have the option **Allow Copy from Previous** set to **Yes**. If those fields are set to No and you want their values to be copied during review, set the Allow Copy from Previous option to **Yes**. If you need to remove the Copy from Previous option from a layout click **Disable Copy from Pre-**

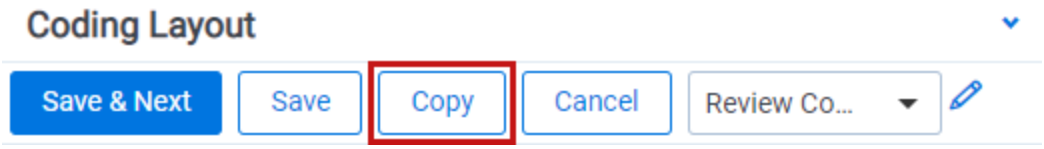
vious. This button only becomes available after you add the toolbar to a layout.



5. Click **Save** or **Save and Close**.

16.10.2 Using Copy from Previous

When the toolbar appears in the Coding card, it provides the following options:



- **Copy** - applies the coding values to fields that have the option **Enable Copy from Previous** set to **Yes**. The coding values from the copyable fields are applied to the document currently displayed in the Viewer. The reviewer can modify the values as necessary, and then save these changes.
- **Previous icon** - displays to the left of any fields that were previously saved. The copyable coding values assigned to this document are applied to current document, when the reviewer clicks the Copy button.

Note: Copy from previous is not available for system fields.

After you copy the value into the field, a green check mark displays near the field to indicate that its been copied.

To use Copy from Previous:

1. When you start a review session, code the values for the first document and click **Save & Next**. This enables the **Copy** option on the document layout. The Previous field is updated with the document identifier of this first document.
2. Click **Copy** when you want to copy the coding values of the designated fields from the previously-saved document to the current one. After Relativity populates the layout with these coding values, you can continue to modify them.
3. Click the **Save & Next** button to save your changes, and continue the review process.
    - If you click **Save** or **Cancel**, the layout appears as read-only and the Copy is disabled. You can click **Edit** to restart the review. You must then code the first document, and click **Save & Next** before the Copy button is enabled. Whenever you leave Edit mode or select a different layout, you need to repeat this process.

- In the layout, the Previous icon displays to the left of the field that you previously saved.

Note: The default keyboard shortcut for the Copy from Previous button is **Alt + Shift + Z**. However, your workspace may be configured with a custom keyboard shortcut. Contact your system admin for additional information.

16.11 Using the rich text editor

The rich text editor provides support for hyperlinks, images, and tables.

It also features the following:

- Supports both inline and pop-up display type for a more seamless experience. See Adding fields and text on page 314.
- You can configure the maximum text values for long text fields using the instance setting *MaximumNumberOfCharactersSupportedByLongText* in the Instance setting guide.

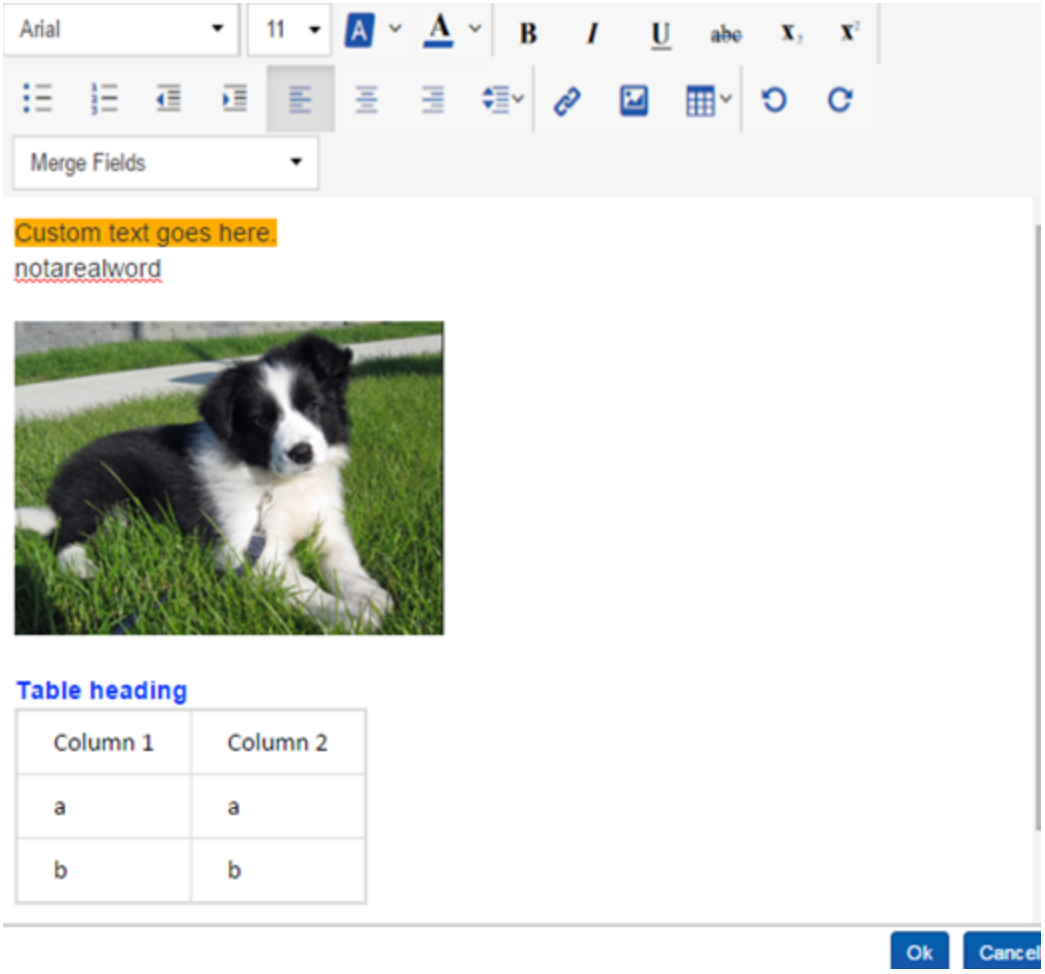
The rich text editor is available in several circumstances:

- **Long Text field**—the Enable HTML field option is enabled on a long text field which is added to a layout. See Enable HTML in Field information on page 199.
  - Set the long text field with the Display Type: Inline Rich Text.
  - On the layout builder, make the long text field two column. This will render the inline text editor as a two column width in an RDO layout. See Adding fields and text on page 314.
- **Contextual help or Custom text**—when adding contextual help or custom text to a layout. See Layouts on page 305.
- **Custom Label**—when adding a custom label to a field.

Note: The Sanitizer object controls whether HTML attributes are sanitized and how specific HTML content is sanitized from fields on page render. You can modify the sanitizer object to add HTML alerts and links. We recommend not modifying the default setting.

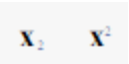
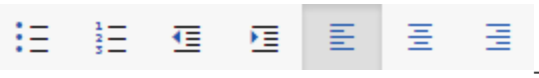
16.11.1 Rich text editor features

The rich text editor contains the following features:



- Arial —change the font type. Arial is the default font type.
  - You can configure the default font using the instance setting, RichTextEditorFontDefault.
  - See *RichTextEditorFontDefault* in the Instance setting guide.

  Note: In Microsoft Internet Explorer and Edge, the font type drop-down menu does not appear. You can, however, change the default font face in IE using the RichTextEditorFontDefault instance setting. See RichTextEditorFontDefault in the Instance setting guide.
- 14 —change text font size.
- —changes selected text background highlight color.
- —changes selected text color.
- **B** —bolds selected text.
- *I* —italicizes selected text.

-  —underlines selected text.
-  —adds a strikethrough to selected text.
-  —add subscript or superscript to selected text.
-  —arrange content in a bulleted or numbered list, outdent or indent text, and align text left, center, or right.
-  —customize the space between each line of text.
-  —insert hyperlink. Here, you can specify the URL, link text, and whether the link opens in a new tab.
  - Relativity requires HTTPS links only.
    - Links need to follow the following format: start with *https://*, and can include forward slashes, periods, and alphanumeric characters.
    - For example, *Relativity Customers*.
  - To add a link, you must be in the *Legal Hold admin* group, or a group that has view permission for the Object security permission *InstanceSettings*. For more information, see the Admin guide.
  - To add a link, you must update the *DomainNameWhiteListUrls* instance setting. It's a semicolon-delimited list of allowed domains. For example, "google.com;mozilla.org".
-  —insert an image from a URL.

Complete the following steps before inserting an image:

1. Host the image at a public accessible HTTPS URL.
   - Relativity does not upload the image file. Relativity references the URL directly.
   - The URL must start with https:// and contain no trailing spaces or special characters. A trailing space alone breaks the image.
   - Test the URL in a private browsing window on a machine that is not signed in to your network. If the image does not load without a login, it does not render in Relativity.
   - URLs that require authentication, such as SharePoint, OneDrive, or an intranet, do not work.
2. Add the domain to the Sanitizer safeURL allowlist.

   Notes: Adding a domain to *DomainNameWhiteListUrls* does not safelist it for images. If you insert links and images from the same domain, you need both settings.

   - If you are not a system admin or are unsuccessful in adding to the safeURL allow list, submit a ticket to add your image domain, contact Relativity Support.

        - Include the full image URL, the workspace name, the Artifiact ID.
        - State that it is for a Legal Hold communication.
    - The Sanitizer strips image URLs from domains not on its safeURL allowlist.
    - For system admins, if you have access to the Sanitizer object, you can append a safeURL regex rule yourself.
        - Back up the current value first. Edit in a local text editor.
        - Hide the Sanitizer tab afterward to prevent unintended changes.
        - For more information, see Sanitizer object documentation.
3. Insert the image by selecting the image icon in the rich text editor.
4. Paste the URL.
5. Verify the image before saving.
    - If the image appears as a blank square, the URL is not publicly accessible or the domain is not safelisted.
    - The editor does not display an error message. A blank square is the only signal.
6. Resize the image when you first insert it.
    - Resize the image when you first insert it.
    - Resizing an image on a communication you are re-editing may not save.

Note: For more information about inserting an image, see the Relativity Community:

- Troubleshooting Inserting Images into Legal Hold Communications
- Sanitizer, HTML and Javascript not functioning as expected

-  —insert a table.
-  —use to undo or redo actions taken in the rich text editor.

16.11.1.1 Copying and pasting

You can copy and paste from Microsoft Word with most formatting staying intact. Always double-check formatting before saving the communication because formatting from another application may not be carried over.

Copying and pasting bullet or numbered lists from MS Word, Chrome, and Firefox convert into HTML lists in the rich text editor. The HTML lists will consist of and tags in the editor. These pasted lists can then be edited in like other lists in the editor.

Note: Copying and pasting into the rich text editor only works when copying from MS Word, Chrome, and Firefox. This is currently not possible for Internet Explorer 11.

17 Lists

Lists provide a simple way to save a list of objects, such as documents, without specifying the types of conditions you do for a saved search. Since lists aren't based on conditions, they remain constant unless you replace an existing list.

Lists are especially useful when saving a list of sampled items. When using Sampling, you can save a random sample set of documents as a list in order to access the same sample set again later. See Sampling on page 587. When saving a list of documents, you can view the list later by creating a saved search with the list set as search criteria. The Lists console includes a command to automate the creation of a saved search from a list.

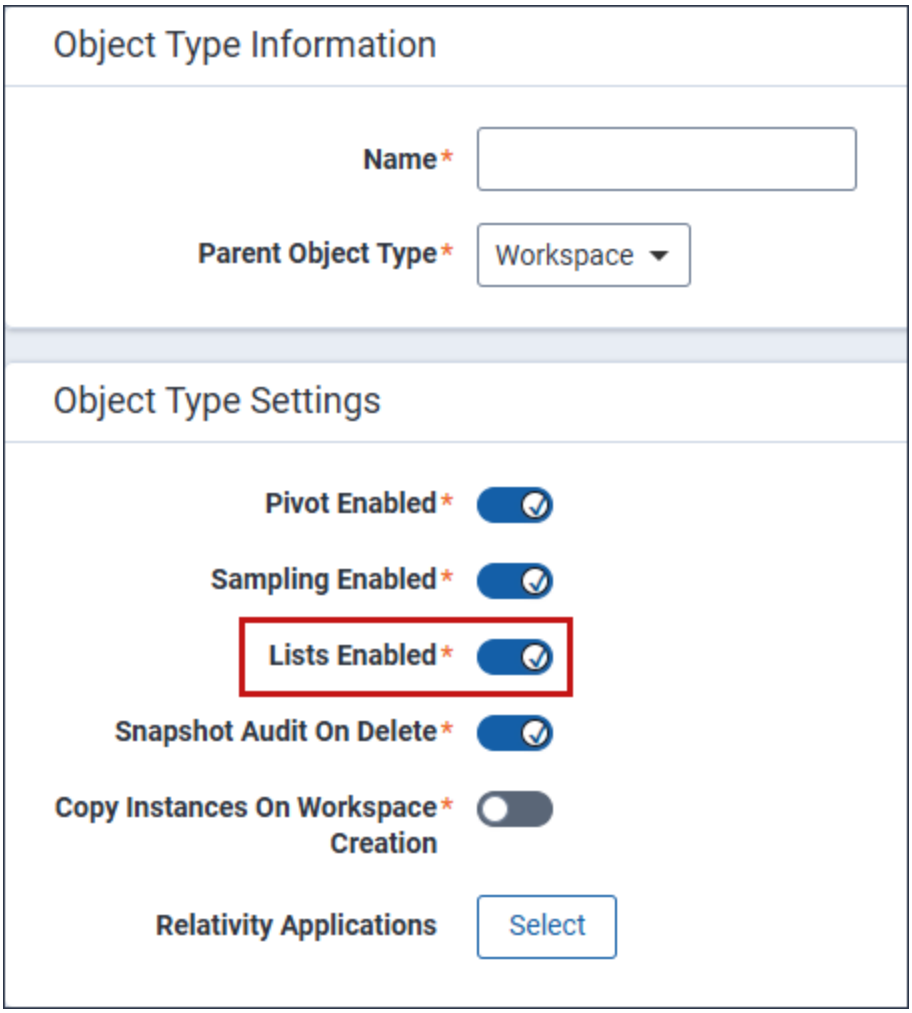
Auditing is performed when a user creates or deletes a list. Individual documents are not audited when added to a list.

17.1 Enabling lists on an object

The option to save items to a list is available on any object type that has the **Lists** field enabled.

To enable an object to be saved to a list:

1. Navigate to the **Object Type** tab.
2. Click **Edit** on an object type.
3. Toggle the **Lists Enabled** field on..



4. Click **Save**.

After enabling **Lists** for an object, you can perform a Mass Save as List operation to save a search as a list. For more information, see Mass Save as List in the Admin guide.

17.2 Viewing items in a list

To view items in a saved list, create a new saved search or view based on the list.

Note: The Create Search from List button has been deprecated. To create a search from a list, create a new saved search that includes the desired list as a condition.

17.2.1 Incorporating a list of documents as a search criterion in a saved search

Follow these steps to create a new saved search using a saved list of documents as the search criteria:

1. On the **Documents** tab, click the **Saved Searches browser** icon.
2. Click **Create New Search**.
3. Type a name for the saved search in the **Name** field.
4. Add a condition with the following column settings:
    - **Field**—select **Lists**.
    - **Operator**—select **these conditions**.
    - **Value**—select the following value criteria:
        - **Field**—select **Lists**.
        - **Operator**—select **any of these**.
        - **Value**—select one or more saved lists to include in the search criteria.
5. In the **Fields** category, select the fields you want to include when viewing your saved search results. Select the **Lists** field to show the list(s) with which an object is associated.
6. Click **Save** to save the search. Or, click **Save & Search** to save and execute the search.

For more information on creating a saved search, see the Searching guide.

17.2.2 Creating a view from a saved list

To view the items saved as an object list, create a view with a field condition using the Lists field. Follow these steps to create a new view that displays the items saved in a list for any object type.

1. Click the object's tab in your workspace. For example, if the name of the object type for which you saved a list of items is Media, click the Media tab.
2. Click the **Create View** icon.
3. Type a name for the new view in the **Name** field.
4. Verify **Object Type** is set to the object type for which you saved a list.
5. Click **Next**.
6. Add the fields you want to include in your view to the **Selected Fields** box.
7. Click **Next**.

8. Add a condition with the following settings:
    - **Field** - select **Lists**.
    - **Operator** - select **these conditions**.
    - **Value** - click the ellipsis and select the following Lists criteria:
        - **Field** - select **Lists**.
        - **Operator** - select **any of these**.
        - **Value** - select and add one or more saved lists to include in your view.
9. Click **Next**.
10. (Optional) Select one or more fields with ascending or descending sort order for your view.
11. Click **Save**.
12. Select your new view from the view drop-down menu on your object tab to display the saved list of items.

Note: For more information on creating a view, see Creating a view with field categories on page 706.

18 Relativity Script Library

The following is a list of standard scripts available in Relativity. This list may vary per version of Relativity.

These scripts are available in the Relativity Script Library. To access the script library:

1. Navigate to **Home**.
2. Click the **Relativity Script Library** tab.

To add library scripts to your Script tab in a workspace for your users to run, refer to the Relativity Admin Guide.

Caution: Changes to SQL fields executed by Relativity Scripts do not produce Audit logs.

Script	Description
Case permission audit	Reports on all users, workspaces, groups, and each group's permissions in a Relativity environment.
Choice field stratified sampling	Selects a specified number of sample documents across categories chosen by the user, ensuring that each category is represented equally.
Create Cluster Upgrade Jobs	Creates job entries in the EDDS database to upgrade Analytics clusters for CAAT 3.17.2.
Globally administer keyboard shortcuts	Forcibly assigns a keyboard shortcut to a specific system function; this script runs against all workspaces.
Monitor Cluster Upgrade Jobs	Checks and reports the status of all Analytics cluster upgrade jobs recorded in the EDDS database.
Lockbox report	The Lockbox Report script will list out all workspaces where anyone at Relativity ODA LLC has current access to along with the name of the group that the Relativity ODC LLC user is linked to.
Lockbox Bypass report	The Lockbox Bypass Report script provides audit history of changes to the Lockbox instance setting, by whom, and when.
Populate parent to	Populate parent to child is a workspace-level script propagates the Document ID of the parent

Script	Description
child	document to any children of that document.
Propagate sent date to family documents	Sets all email families' documents to the same sent date as their parent documents in a case.
Report sample-based statistics	Generates reports for the deprecated sample-based learning feature.
Reviewer statistics	Reports on the efficiency of reviewers over the specified date range; the returned statistics provide a count on how many documents were reviewed over a certain period of time.
Saved search gap and overlap check	Identifies documents with gaps in Bates numbers or overlapping Bates numbers in a workspace.
Set duplicate flag field	Identifies and sets a Yes/No field on all case documents to indicate it as a duplicate or primary.
Set native file size field	Stores the native file size (in KB), for each case document in a decimal field.
Set Relativity folder path field	Stores the current Relativity folder path of each document in a long text field.
Total Automated Workflows in Instance	Reports on the number of automated workflows in your instance.
Upgrade legacy applications	Upgrades a legacy application (v 6.8 and earlier) to a Relativity Application object

The Relativity Script Library includes all scripts installed with your version of Relativity. To request additional scripts, contact Relativity Customer Support.

The following scripts are available outside the script library:

Script	Description
Australian Document ID	Renumbers your Relativity documents and Host/Family fields into a standard Prefix, Box, and Document format.
Get database size	Displays size and location information for all database files in a specific workspace. Use the following SQL command to run this script: `exec sp_helpdb <databaseName>`

18.1 Australian Document ID

The Australian Document ID Relativity script gives you the flexibility to renumber your Relativity documents and Host/Family fields into a standard Prefix, Box, Folder and Document format. For example, ABC.001.001.0001.

The script will maintain an audit of all changes.

18.1.1 Special considerations

- The Australian Document ID Relativity script allows you to renumber your Relativity documents and Host/Family fields into a standard Prefix, Box, Folder, and Document format (e.g., ABC.001.001.0001). When running the script, you must specify a required Identifier field, such as DocumentID or Control Number. This means the script can overwrite the Control Number field with the new format you define.

- If you process additional documents into the workspace after renumbering with the Australian Document ID script, de-duplication may not work as expected against copies that have been renumbered. This is because de-duplication in Relativity typically relies on the Control Number or Document Identifier field. If the original Control Number is overwritten, the system will not recognize previously processed documents as duplicates based on the new identifier. Therefore, renumbering changes the key field used for de-duplication, and subsequent imports will not de-duplicate against the renumbered copies.

18.1.2 Downloading the script from the Community

The Australian Document ID script is not included by default in the Relativity Script Library. Click here to download it from the Community. You must have valid Community credentials to do so.

18.1.3 Installing to the Relativity Script Library

Note: Upload the RAP first to the Application Library, which then produces the script.

Perform the following steps to install Australian Document ID to Relativity's Application Library:

1. Log into Relativity as a system admin.
2. Navigate to the **Applications & Scripts** tab and click **New Relativity Script**.
3. Paste the contents of the script file in the provided Script Body field.
4. Click **Save**. The script is now added to the Script Library.

18.1.4 Installing Australian Document ID application to a workspace

You can install the Australian Document ID application to your workspace from the Application Library tab from Home or from the Relativity Applications tab within the workspace.

Follow these steps to install the application from within the workspace:

1. Access your workspace and navigate to the **Scripts** tab.
2. Click **New Relativity Script**.
3. Under the Script Type section, select the radio button next to **Select from Script Library**.
4. Click the **Select** button to browse the script library.
5. Select the Australian Document ID script and click **Set**.
6. Click **Save**.

18.1.5 Running the solution

You can run the solution by completing the following steps:

1. Access your workspace and navigate to the **Scripts** tab.
2. Click the **Australian Document ID Format** script.
3. Click **Run Script**.
4. Complete the following required fields:
    - **Saved Search** – a required list of documents to renumber
    - **Document Identifier** – a required Identifier field, e.g. "DocumentID" or "Control Number"

- **Document Group** – an optional family host/field, e.g. “Document Host”
- **Prefix** - a required alphanumeric field (3-6 characters), e.g. “ABC”
- **Box** - an optional numeric field (3-6 characters), e.g. “001”
- **Folder** - a required numeric field (3-6 characters), e.g. “001”
- **Document** - an optional numeric field (3-6 characters), e.g. “0001”

5. Click **Run**.

18.2 Billing statistics - case rollup

Note: Relativity has deprecated this script for Relativity aiR commercial customers. We recommend that you create custom reports via Usage Reports within the Management Console.

18.3 Billing statistics - users

Note: Relativity has deprecated this script for Relativity aiR commercial customers. We recommend that you create custom reports via Usage Reports within the Management Console.

18.4 Choice field stratified sampling

This script selects a specified number of sample documents across categories chosen by the user, ensuring that each category is represented equally. These documents can then be reviewed or set aside for any process which benefits from sampling a broad variety of documents.

Examples of how to use this script include:

- Sampling documents with different coding tags
- Sampling documents across different folders
- Sampling across clusters
- Sampling documents coded by different reviewers for quality checks

The most common use of this script is sampling documents from each cluster in a conceptual cluster, then pre-coding those documents before starting a prioritized review queue in Review Center. The variety of content in the sample gives the AI classifier a strong foundation for its relevance predictions, and it can increase the accuracy of those predictions early in the queue.

18.4.1 Special considerations

Consider the following when running this script:

- If you plan to sample documents across clusters, you must create the clusters first. For more information, see Clustering in the Analytics guide.
- You can use any single-choice or multiple-choice field to define the categories for the script.
- When used on a multiple choice field with parent and child choices, this script only considers the child choices. In a cluster visualization, these are represented as the outermost ring of clusters.

18.4.2 Inputs

1. Before running the script, create a Yes/No field to track which documents have been selected by the script. If you use a previously created Yes/No field, the script will overwrite any existing values.
2. Create a saved search which includes documents from all categories you want to sample. If you are sampling from a specific set of clusters, make sure only the desired clusters are selected when creating your saved search.
3. Navigate to the **Scripts** tab.
4. Select the Choice Field Stratified Sampling script. If the script is not present in the workspace's Script tab, you must add it.
5. Click **Run**.
6. In the pop-up window, fill out the following fields:
    1. **Choice to sample from** - select the choice field containing the categories you want to sample.
    2. **Saved Search** - select the saved search created in step 2.
    3. **Number from each choice** - enter the number of documents you want to sample from each category.
    4. **Is Sampled Field (Yes/No)** - select the Yes/No field created in step 1.
7. Click **Run**.

18.4.3 Results

Once run, this script updates the Yes/No field to Yes for the sampled documents. To view all sampled documents, go to the Document List view and search for a Yes value in that field. You can then code the documents or create a saved search to set them aside for later.

18.5 Copy To Legacy Document Fields

The Copy To Legacy Document Fields script has been deprecated. The functionality it provided is now available as a built-in feature in Production Sets. No script installation or Community download is required.

For more information, see Production sets.

18.6 Create sample set

This script is no longer supported.

18.7 Forgotten password reset audit

This script is no longer supported in Relativity aiR.

18.8 Globally administer keyboard shortcuts

The Relativity script for globally administering keyboard shortcuts forces the assignment of a keyboard shortcut for a specific system function across all workspaces. The script overwrites existing keyboard shortcuts currently assigned to other system functions, fields, or choices. After the script runs, the updated keyboard shortcut is available for use in the Review Interface. For more information about these shortcuts, see the Admin Guide.

18.8.1 Category

System Functionality

18.8.2 Special considerations

This script overwrites an existing keyboard shortcut combination assigned to a system function, field, or choice across all Relativity workspaces. You may want to review your current review workflows to determine how they are affected by modifications to the shortcut combinations.

18.8.3 Inputs

Use the following steps to run the script Globally Administer Keyboard Shortcuts:

1. Navigate to the **Relativity Script Library** tab.
2. Use the **Name** column to filter on the script Globally Administer Keyboard Shortcuts.
3. Click on **Globally Administer Keyboard Shortcuts** in the list.
4. Click **Run Script** to display the Script: Globally Administer Keyboard Shortcuts modal.
5. Select options in the following boxes:
    - **Shift**, **Alt**, and **Ctrl** list the options **On** or **Off** for enabling or disabling these keys. You must select a value for each of these options.
    - **Key** lists alphanumeric values from 0-9, and A-Z. It also lists options for the keys: End, Home, Space, Return, Down Arrow, Up Arrow, Left Arrow, Right Arrow, Page Down, and Page Up.
    - **System Action** lists the system keyboard shortcuts used in the Review Interface, and Keyboard Shortcut Legend. For more information about these shortcuts, see the Admin Guide.
6. Click **Preview** to view the script that runs across the workspaces.
7. Click **Run** to display a confirmation message.
8. Click **OK** to display the results of the update.

Note: If you later want to modify this keyboard shortcut, you need to rerun the script with the new settings. You cannot rollback the changes.

18.8.4 Results

In the Results section, you can review the list of workspaces updated with the new keyboard shortcut combination. A list of parameters used by the script to perform the update appears. To download a list of workspaces with the updated shortcut, click the **Go** button next to the **Export to File** option.

18.9 Propagate sent date to family documents

This Relativity script sets all email families documents to the same sent date as their parent documents in a case. This allows for chronological sorting within all documents.

This is a case functionality script to be run at a case level.

18.9.1 Special considerations

Consider the following when running this script.

- This script cannot be undone.
- The script may run for some time without reporting any progress.
- This script updates the Document table.

18.9.2 Inputs

Before running the script, complete the following inputs:

- **Date Field - Original** - the field from which you want the date to be propagated, such as Sent Date.
- **Date Field Sort** - the field you created to be the destination to which you want the date to be propagated, such as Parent/Family Date.
- **Family Identifier** - the relational field used to identify which documents are grouped together.
- **Date Propagated** - a Yes/No field you created to indicate which documents the script updates, which also indicates where data is changed. If you add additional data to the workspace at a later date, and need to run the script again, this flag ensures the script runs only on the newly added documents.
- **Document Sort Field** - instead of using ArtifactID to order documents in each family, use this input to select your choice field in which to order documents by. This accounts for some document families where the lowest ArtifactID isn't the parent.

Note: This script uses the Group Identifier to identify email families. Because this field is not populated for documents without families, it will not run on them. In order to get it to run on them, populate the Group ID field by running Mass Replace on the empty Group ID field, replacing it with another field such as Control Number. Once this is complete, rerun the script. All the documents should then have the destination field populated.

18.9.3 Results

Once this script has been run, the Sent Date field will be updated so all family documents in a case have the same value as their parent document. The parent must be the record with the lowest ArtifactID.

Note: This script ignores records where the field assigned to Date Propagated field is set to Yes. As a result, this script will only affect documents where this field is empty or set to No.

18.10 Billing statistics - Relativity aiR - case rollup

Note: Relativity has deprecated this script for Relativity aiR commercial customers. We recommend that you create custom reports via Usage Reports within the Management Console.

18.11 Report sample-based statistics

This script generates reports for the deprecated sample-based learning feature. If you have legacy sample-based learning projects in your workspace, you can select one and generate several types of reports based on its contents.

Because the sample-based learning feature is now deprecated, you cannot modify the data within the projects or create new ones. These reports show each legacy project as-is, regardless of whether the project was completed.

18.11.1 Report types

The available reports are:

- **Project Summary**—this provides a consolidated set of quality metrics from the entire project so that you can see the state of the project based on the last round completed. It includes manually coded documents, project categorization results, project overturn results, and control set statistics.
- **Overturn Summary**—this provides a high-level view of a project's overturn percentages and tallies from round to round. The accompanying table gives even greater detail, including a breakdown of responsive and non-responsive overturn rates.
- **Round Summary**—this report is split into two graphs. The first graph provides a categorization breakdown of each category per round, allowing you to track categorization results as the project progressed. The second graph displays the volatility of each category per round, while accompanying tables provide additional information such as document tallies and population size changes.
- **Issue Summary**—this provides a breakdown of issue coding categorization results. The table version of the report also displays document tallies and previous round information.
- **Designation Issue Comparison**—this provides insight into designation and issue coding categorization results and how they relate to one another.
- **Rank Distribution**—this provides insight into categorization results according to their rank score. The accompanying table also provides document tallies.
- **Control Set Statistics**—this displays a project's accuracy trends from round to round. The report displays precision, recall, and F1 scores for each round in a single line chart.

18.11.2 Inputs

1. Navigate to the **Scripts** tab.
2. Select the Report Sample-Based Statistics script. If the script is not present in the workspace's Script tab, you must add it.
3. Click **Run**.
4. In the pop-up window, fill out:
    1. **Project**—select the legacy project you want the report based on.
    2. **Report Type**—select the type of report.
5. Click **Run**.
6. Click **Accept** on the pop-up confirmation.

This script may take a few minutes to process.

18.11.3 Results

After the script finishes, a custom URL will appear in the Script Output pane. To view the report, copy and paste the URL into a new browser tab.

This report can be exported into a variety of formats using the drop-down menu in the upper right corner.



18.12 Reviewer statistics

Note: If the workspace has a large amount of audit data, we recommend breaking up the date ranges to smaller data sets to be able to retrieve the data efficiently. If a data set becomes too large, the report performance begins to degrade and may result in an error.

The Relativity Reviewer Statistics scripts report on the efficiency of reviewers over the specified date range. The returned statistics provide a count on how many documents were reviewed over a certain period of time. Time zone of the reviewers must be specified in order for the report to accurately account for reviewers in different time zones.

The returned statistics provide a count of how many documents were reviewed over a certain period of time. For simple coding fields like textbox, radio button, drop down, etc., edit tracking occurs when a user clicks Save, or Save and Next. For example, when a user commits coding changes.

You can use the following scripts to generate this information:

- **Reviewer Statistics** - use this script to generate a report that lists the system admins.
- **Reviewer Statistics** - **No System Administrators** - use this script to generate a report that does not include system admins.

Note: Ensure that users running this script have both the Relativity Script Object Security > View permission enabled and View All Audits checked in the Admin Operations section of Other Settings.

18.12.1 Inputs

Enter the following field information:

- **Reviewer Time Zone** - The reviewer time zone for which you wish to report on.
- **Start Date** - the start date for which you wish to report on.
- **End Date** - the end date for which you wish the report on.
- **Include Additional Action** - set this field to add statistics for Mass Edits and Propagation.
- **Downtime threshold (minutes)** - this field helps to calculate the Total Usage Time metric and determines whether two audits belong to the same group of action. The default value for this field is 60 minutes. If the time difference between the two actions is less than the Downtime threshold, that time will be included to add up to the Total Usage metric; if it's greater than the Downtime threshold, only two minutes will count for these two actions (one minute for each action).

Note: If the Audit application is installed in your workspace, the script pulls audit data from Elasticsearch.

18.12.2 Results

Once you run this script, the Reviewer Statistics report displays.

The report includes the following columns:

Note: By default, the following columns are not included in the output. To include these columns, in the **Include Additional Action** drop-down list, select **Mass Edits and Propagation**.
Propagations
Distinct Propagations
Propagations Per Hour
Propagations Per Day
Distinct Propagations Per Hour
Distinct Propagations Per Day

Column	Definition
Full Name	The reviewer's full name.
Total Usage Time	The total usage time is calculated as the difference between the time the user first views or edits any document in the workspace and the time the user last views or edits any document in the workspace per session. A session is anytime the user has logged in to Relativity. All sessions for the selected date range are then totaled per user. The Total Usage Time is affected by the Downtime threshold (minutes) value. Any idle time that is less than the Downtime threshold value is counted for the Total Usage Time but any value greater than the Downtime threshold is not counted. Usage time is calculated this way to avoid counting long periods of idle time as part of the Total Usage Time. For example, if a Reviewer logs into Relativity at 9:00 AM and reviews documents from 9:00-12:00 and then takes lunch from 12:00-1:00 PM but never logs out of Relativity, their Total Usage Time would only be for three hours because the idle lunch hour is not counted since they were not viewing or editing documents in Relativity and that time is greater than the Downtime threshold (minutes) value. When audits are stored in Elasticsearch, the session ID is used to calculate the total usage time for the session.
Views	The total number of documents a reviewer looked at over the reported period.
Distinct Views	The number of unique documents a reviewer looked at over the reported period.
Edits	The total number of editing/coding decisions made over the reported time period.
Distinct Edits	The total number of documents edited, excluding repeated edits of the same document. The "distinct" classification is meant to account for duplicate actions performed against unique documents.
Edits Per Hour	The number of edits per hour based on the reviewer's total usage time.
Edits Per Day	The number of edits performed per day over the period reported on.
Distinct Edits Per Hour	The number of distinct edits per hour based on the reviewer's total usage time.
Distinct Edits Per Day	The number of unique edits performed per day over the period reported on.
Mass Edits	The total number of document edits using the Mass Edit action.
Distinct Mass Edits	The total number of unique document edits using the Mass Edit action.
Mass Edits Per Hour	The number of Mass Edits per hour based on the reviewer's total usage time.
Mass Edits Per Day	The number of Mass Edits per day over the period reported on.
Distinct Mass	The number of distinct Mass Edits per hour based on the reviewer's total usage time.

Column	Definition
Edits Per Hour	
Distinct Mass Edits Per Day	The number of distinct Mass Edits per day over the period reported on.
Propagations	The total number of documents that were updated via propagation.
Distinct Propagations	The total number of unique documents that were updated via propagation.
Propagations Per Hour	The number of propagations applied per hour based on the reviewer's total usage time.
Propagations Per Day	The number of propagations applied per day based on the period reported on.
Distinct Propagations Per Hour	The number of unique documents that had propagations applied per hour based on the reviewer's total usage time.
Distinct Propagations Per Day	The number of unique documents that had propagations applied per day based on the period reported on.

18.13 Set duplicate flag field

This Relativity script identifies and sets a Yes/No field on all case documents to indicate them as original or duplicate.

This is a case functionality script to be run at a case level.

18.13.1 Special considerations

Consider the following when running this script:

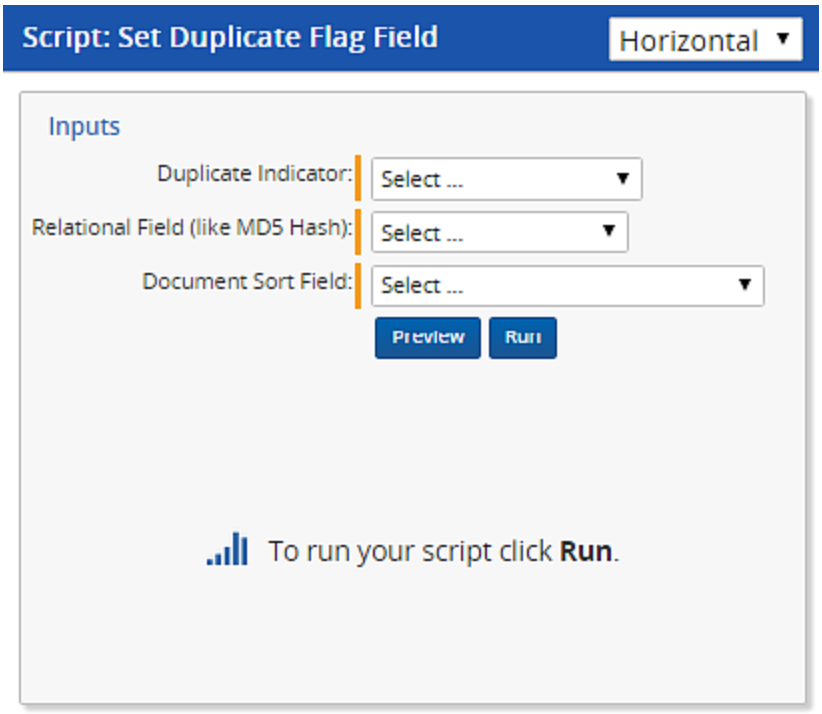
- This script cannot be undone.
- The script may run for some time without reporting any progress.
- The script skips any documents which already have their duplicate flag field already set to Yes. (It updates only documents on which this field isn't set.)

18.13.2 Inputs

Note: Before running this script, you must create a Yes/No field to act as the Duplicate Indicator.

- **Duplicate Indicator** - the Yes/No field that determines whether documents are duplicates.
- **Relational Field** - the field that shows document relationship (such as MD5 Hash).
- **Document Sort Field** - the sort order field for duplicate documents. For example, if MD5 Hash is specified as the Relational Field and Control Number as the Document Sort Field, the document with the lowest Control Number will be flagged as original; the other documents with the same MD5 Hash field value will be flagged as

duplicates.



18.13.3 Results

When you run this script, all documents that are duplicates are marked **Yes** and all documents that are original are marked **No**.

18.14 Set extracted text size field

Note: This script is no longer supported. You can use the Set long text size mass operation in place of this script. For more information, see the Admin Guide.

18.15 Set native file size field v4

This Relativity script stores the native file size for each document in the workspace in a decimal field.

18.15.1 Special considerations

Consider the following when running this script:

- The script cannot be undone.
- The script may run for some time without reporting any progress.
- The script updates the Document object. If you create a new field for the native file size, you must manually add it to your views to see the script results.
- The script will only set the field if it is blank. It does not update or change existing file size field values.
- When running this script against documents that do not have the file size field set, the file size value will be in kilobytes.

- When running this script against documents imported through the Processing New Document option, the file size value will be in bytes.
- Depending on the method used to upload or import files, you may see different file size formats (bytes or kilobytes.)
- This script populates the file size field for any files, including third party documents not processed in Relativity. This script also include files that were transferred into the workspace as *Links only* Natives via Integration Points.

18.15.2 Inputs

Before running the script, create a decimal field to store the script's native file size output. You can map to this field in the script. Be sure to add the field to your views to see the results.

18.15.3 Results

Once run, this script updates the Native File Size field with the file size for any document in the workspace. Note that there could be a mix of file size values in bytes and kilobytes.

18.16 Set production beg/end attach fields

The Set production beg/end attach fields script has been deprecated. The functionality it provided is now available as a built-in feature in Production Sets. No script installation or Community download is required.

For more information, see Production sets.

18.17 Set Relativity folder path field

This Relativity case script stores the current Relativity folder path of each document in a long text field. A document cannot be in more than one folder path. See the full path structure of a folder for example, Custodian / J Smith / Inbox.

This script populates the new long text field with the current case folder structure.

This is a case functionality script to be run at a case level.

Note: The script will not work on long text fields stored in data grid. You must disable the Stored in Data Grid option when creating the long text field.

18.17.1 Special considerations

The risks outlined below must be considered when running this script:

- This script cannot be undone.
- The script may run for some time without reporting any progress.
- This script updates the Document table.
- If, at any time, a folder is renamed or a document is moved, the folder path value is inaccurate.

Note: For workflows where you need to run this script on a document that had a previously populated folder path, the Set Relativity Folder Path field may not populate fields on one workspace. For more information and a solution, see Set Relativity Folder Path Field not populating fields on one workspace.

18.17.2 Inputs

By default, this script will only update documents that do not have an existing folder path. To update the folder path of documents with existing folder paths, ensure the following are in place before running the script:

- Create a long text field to store the folder path.
- Ensure the Folder Path field is not populated. Otherwise, the script won't return results.

> **Note:** If you want to able to search the original folder path after running the script, save the original folder path in a separate field before you clear the existing folder path.

18.17.3 Results

Once the script has run, it reports on each distinct folder path in the case, returning the number of documents per path, and the execution time of the script. It also updates the Folder Path field with the Relativity folder path of that document.

A table with the following is returned:

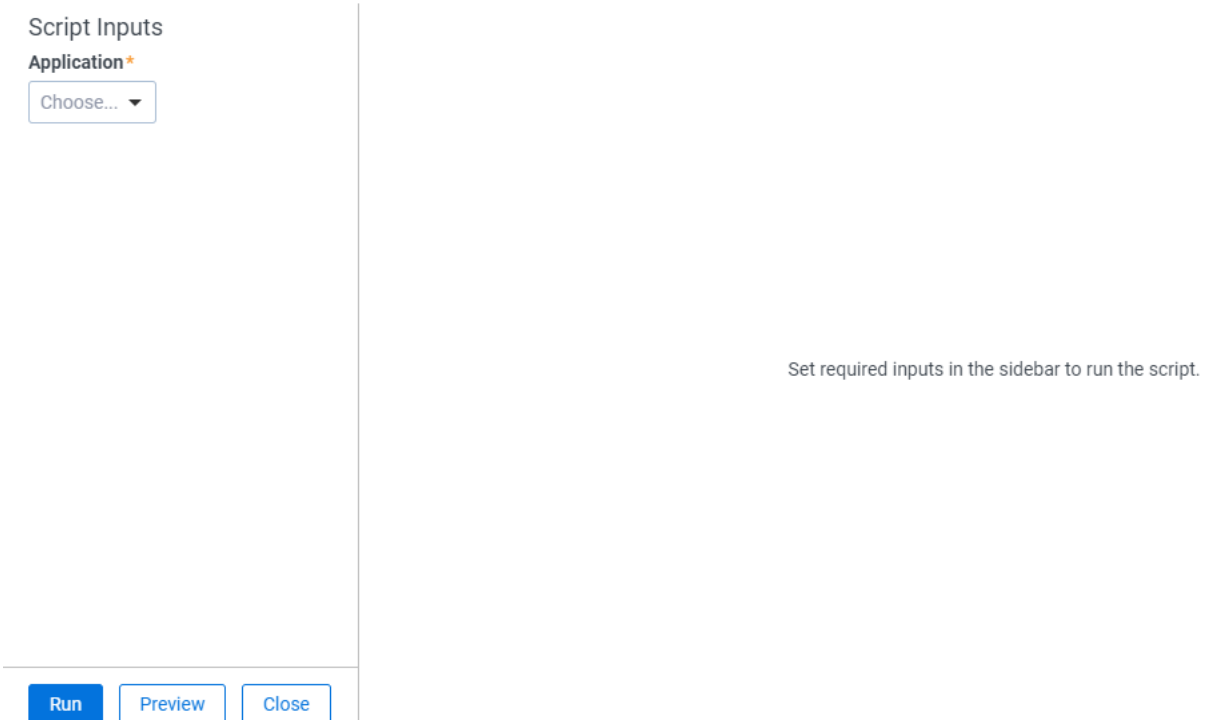
Column	Definition
Timestamp	An indication of when the step or path finished processing.
Message	The name of a distinct Relativity folder path or an execution step in the script.
DocCount	The count of documents for a folder path or, if -1, the execution step of the script.

18.18 Upgrade legacy applications

This Relativity script performs an upgrade of version 6.8 Relativity applications and earlier. It can also be used to upgrade a 6.9 or 6.10 Relativity application if it was exported with the ADS Utility.

18.18.1 Inputs

Choose an application from the **Application** field. Only applications from Relativity 6.8 or earlier and 6.9 or 6.10 applications that were exported with the ADS utility are available in this drop-down menu.



18.18.2 Results

Once this script is run, a Completed message appears.

After running, this script the application is available in the Relativity Applications tab. Use this to export the application and import/upgrade the application using the Relativity Desktop application.

19 Markups

Highlights and redactions are two different types of markups. Highlights function similar to a highlighter and help draw attention to information within a document as part of your internal review process. Highlights are drawn by the user and persist on a document until removed. Highlights cannot be produced and should not be used to protect sensitive information. You can manage highlights that originate from persistent highlight sets, searches, and aiR Review in the left panel in the Viewer.

Redactions do obscure the content they are placed over and can be produced. You can place markups either manually or automatically as part of a project using Redact.

You can add markups to documents that contain an image using the Image Viewer. When you open a document in the Native Viewer that has not been imaged, select **Image on the Fly** from the Document actions menu to image the document which can then be opened in the Image Viewer.

Note: If two people edit a markup at the same time, an error occurs.

19.1 Permissions

The following permissions are required to use each part of markups:

Object Security	Tab Visibility
Document: View, Edit	Documents

Object Security	Tab Visibility
• Redact Document • Highlight Document	

Note: The Redact Document and Highlight Document allow a user to apply any redaction and any highlight respectively. For example, if the user has the Redact Document permission and not the Highlight Document permission, they can apply any type of redaction but they cannot apply any highlights.

19.2 Highlights

When you create a highlight, a colored box appears in the area you select, just like using a highlighter.

19.2.1 Creating highlights

To create a highlight:

1. Click the **Highlight Color** icon.
   Blue is the default color. Click the drop-down menu to select a different color.
2. Draw the highlight across the sections of text you want to highlight.

When you create a highlight, it appears in the Markup Navigation Pane. See Using the Markup Navigation pane on page 350.

19.3 Redactions

A redaction hides text on a page. In Relativity, you can create several different types of redactions:

- Creating basic redactions below
- Creating inverse redactions on the next page
- Creating full-page redactions on the next page
- Creating mass redactions on page 345

When you create a redaction, it appears in the Markup Navigation Pane. See Using the Markup Navigation pane on page 350.

19.3.1 Creating basic redactions

To apply a basic redaction to a document:

1. Click the **Redaction Type** icon.
   The black redaction tool is the default. Click the drop-down menu to select a different tool. You can select from the following:
   - **Black Redaction**—creates a solid black box, like using a black marker. While you draw the box, a gray translucent fill appears.
   - **Cross Redaction**—creates a white redaction box black border and a black X from corner to corner.

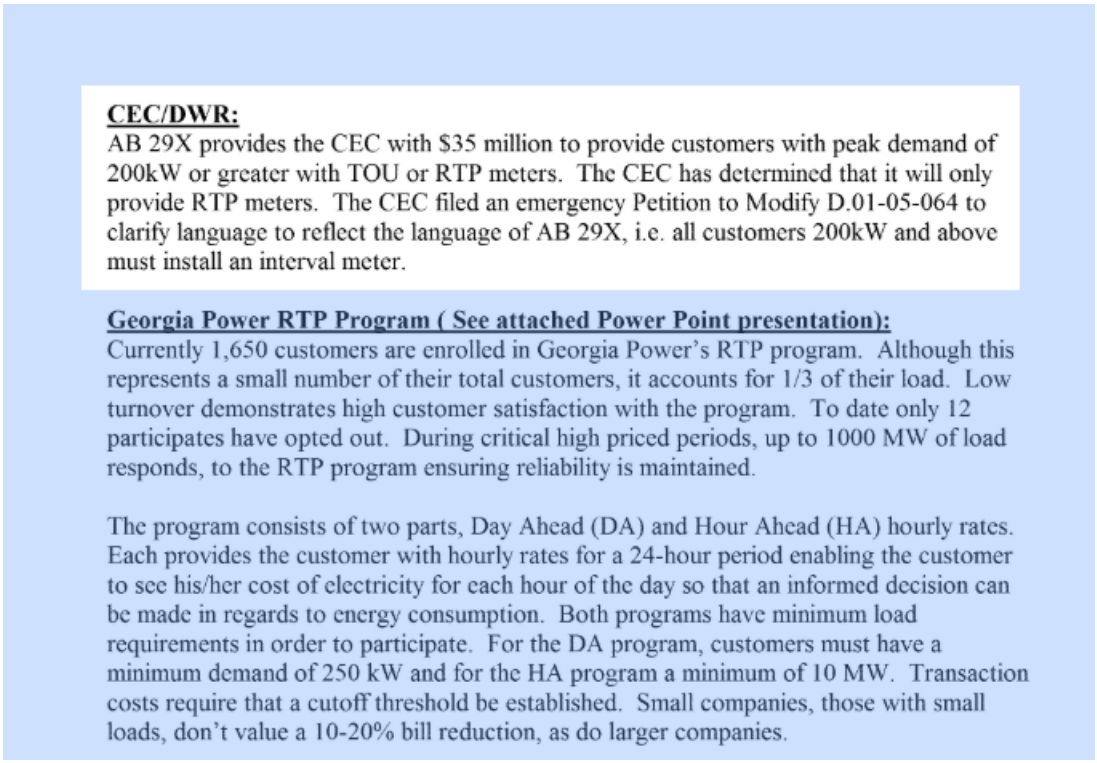
- **Text Redaction**—creates a white redaction box with black text. The text will fill the box by default. To change the font size, keep the redaction box selected and click **Font Size**, and then select a new font size from the drop-down menu. You can right-click a textbox redaction to apply different text. See Editing redaction text on page 348. The system admin determines which text options are available.
- **White Redaction**—creates a solid white box with a gray border. The gray border does not print or produce.

2. Draw the redaction boxes across the sections of the page you want to redact. You can draw in any direction.

19.3.2 Creating inverse redactions

An inverse redaction creates a black redaction across the full page except on the locations where you draw boxes. To create an inverse redaction, perform the following steps:

1. Click the Redaction Mode icon and select **Inverse Redact** from the drop-down menu.
2. Draw the inverse redaction boxes across the sections of the page you do not want to redact.
   A blue cast indicates where you will add the black redaction, and the white box indicates the area that is not redacted. You can move or re-size the white box using the controls. You can also highlight text that is not redacted.



CEC/DWR:
AB 29X provides the CEC with $35 million to provide customers with peak demand of 200kW or greater with TOU or RTP meters. The CEC has determined that it will only provide RTP meters. The CEC filed an emergency Petition to Modify D.01-05-064 to clarify language to reflect the language of AB 29X, i.e. all customers 200kW and above must install an interval meter.

Georgia Power RTP Program (See attached Power Point presentation):
Currently 1,650 customers are enrolled in Georgia Power's RTP program. Although this represents a small number of their total customers, it accounts for 1/3 of their load. Low turnover demonstrates high customer satisfaction with the program. To date only 12 participates have opted out. During critical high priced periods, up to 1000 MW of load responds, to the RTP program ensuring reliability is maintained.

The program consists of two parts, Day Ahead (DA) and Hour Ahead (HA) hourly rates. Each provides the customer with hourly rates for a 24-hour period enabling the customer to see his/her cost of electricity for each hour of the day so that an informed decision can be made in regards to energy consumption. Both programs have minimum load requirements in order to participate. For the DA program, customers must have a minimum demand of 250 kW and for the HA program a minimum of 10 MW. Transaction costs require that a cutoff threshold be established. Small companies, those with small loads, don't value a 10-20% bill reduction, as do larger companies.

19.3.3 Creating full-page redactions

A full-page redaction creates a redaction across the entire page. To apply a full-page redaction, click the **Redaction Mode** icon and select **Full-Page Redact** from the drop-down menu. The black full page redaction tool is the default. Click the Redaction Type drop-down menu to select a different tool. You can select from the following:

- **Black Redaction**—creates a solid black box, like using a black marker.
- **Cross Redaction**—creates a white redaction box with a black border and a black X from corner to corner.

- **Text Redaction**—creates a white redaction box with black text. You can right-click a text box redaction to apply different text. See Editing redaction text on page 348. The system admin determines which text options are available.
- **White Redaction**—creates a solid white box with a gray border. The gray border will not be printed or produced.

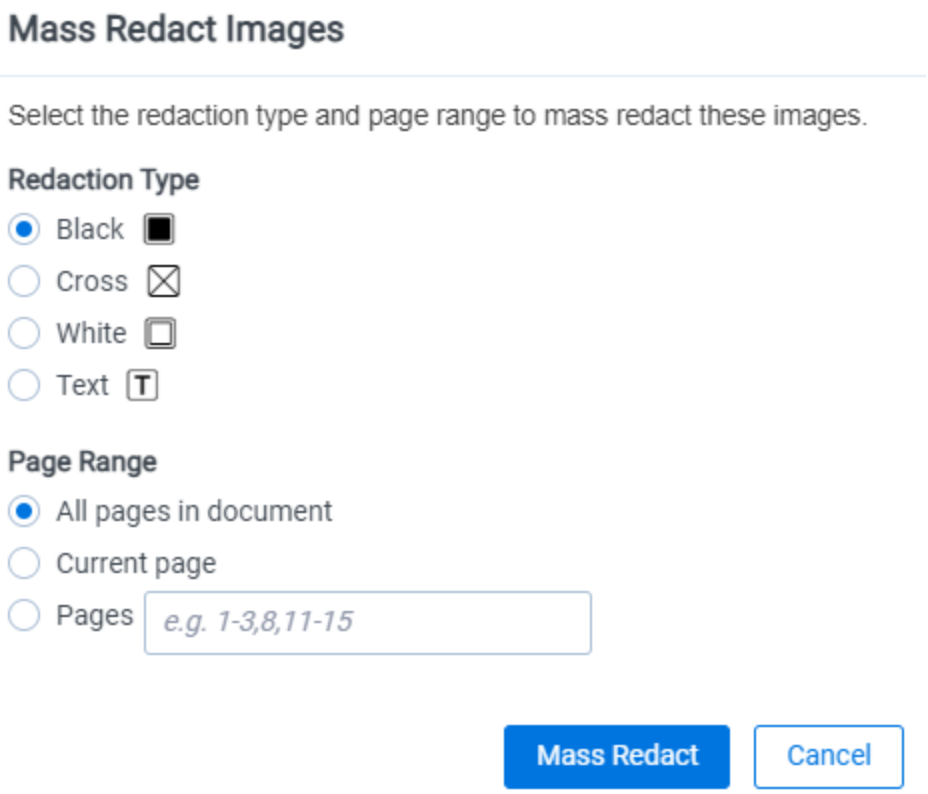
You can also create a keyboard shortcut to apply a full-page redaction. See Creating keyboard shortcuts on page 305.

After you apply a full-page redaction, you can resize it to make it smaller than the full page and then work with it like a normal redaction. Additionally, you can create new redactions on top of a full-page redaction if desired.

19.3.4 Creating mass redactions

You can use the mass redact option to apply full-page redactions of any type to a set of pages in your document. To apply mass redactions:

1. Click the **Redaction Mode** icon and select **Mass Redact** from the drop-down menu.
   The Mass Redact Options pop-up appears.
2. Select the type of redaction to apply. You can select from the following:



   - **Black**—creates a solid black box, like using a black marker.
   - **Cross**—creates a white redaction box with a black border and a black X from corner to corner.
   - **Text**—creates a white redaction box with black text. In the Text Options section, you can select the font size and text to apply to the redactions. To apply custom text, select **<Enter Custom Text>** from the **Text** drop-down menu, then enter the text in the **Text** field.
   - **White**—creates a solid white box with a gray border. The gray border will not print or produce.
3. Specify a range of images to apply the redaction to. Select **Pages** and enter a set of pages or select **All pages in document** to apply the full-page redactions to the entire document.
4. Click **OK**. The redactions apply to the set of pages you specify.

19.4 Editing markups

To re-size a single markup,

1. Click inside the markup shape.
   Blue dot controls appear on the corners and edges of the markup.
2. Select any control and drag to re-size the markup.
3. Optionally, you can also re-size markups using the arrow keys.
   - To re-size a markup in a larger increment, press **Shift** + the arrow key on your keyboard that points in the direction you would like to expand the markup.
   - To re-size a markup in a smaller increment, press **Ctrl** + **Shift** + the arrow key on your keyboard that points in the direction you would like to expand the markup.

You can move markups individually or as a set. To select multiple markups on a page,

click the **Selector** icon and drag across the markups. Alternatively, press **Shift** or **Ctrl** and click to select individual markups, or click **Ctrl + A** to select all markups on an image. Controls appear on the corners and edges of all selected markups.

To move, click and drag the selected markups to a new location. You can also move selected markups using the arrow keys. To move a markup in a larger increment, press the arrow key on your keyboard that points in the direction you would like to move the markup. To move a markup in a smaller increment, press **Ctrl** + the arrow key on your keyboard that points in the direction you would like to move the markup.

19.5 Deleting markups

You can delete markups individually or as a set. To delete a single markup, right-click a markup and click **Delete**. You can also press the **Delete** key with a markup selected and click **Yes** on the Confirm Delete pop-up. For Mac users, press **Fn + Delete**.

To delete multiple markups:

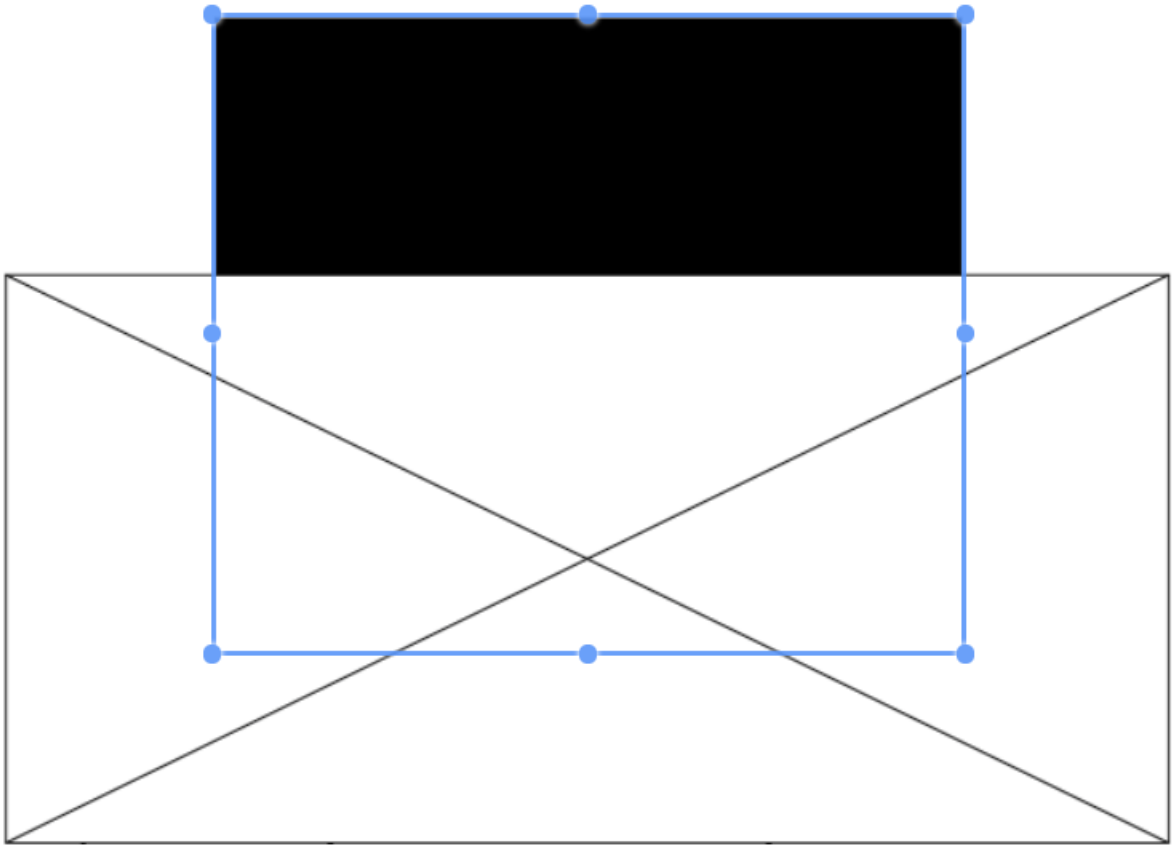
1. You can use any of the following methods to select markups for deletion:
   - Left-click and drag the selection box over the markups you wish to delete.
   - Hold down on **Ctrl** on your keyboard, and left-click on each markup you wish to delete.
   - Right-click on a markup after selecting any other markups you would like to delete.
2. Select **Delete** from the right-click menu.
   The Delete Markups modal displays.
3. Verify that you wish to delete the number of markups displayed in the modal and click the **Delete X Markups** button.
   The selected markups are deleted.

Note: If you have a full-page redaction applied to an image, then you apply an additional full-page redaction, the most recently applied full-page redaction appears on top. If you then delete the second redaction, the first full-page redaction persists.

19.5.1 Working with overlapping markups

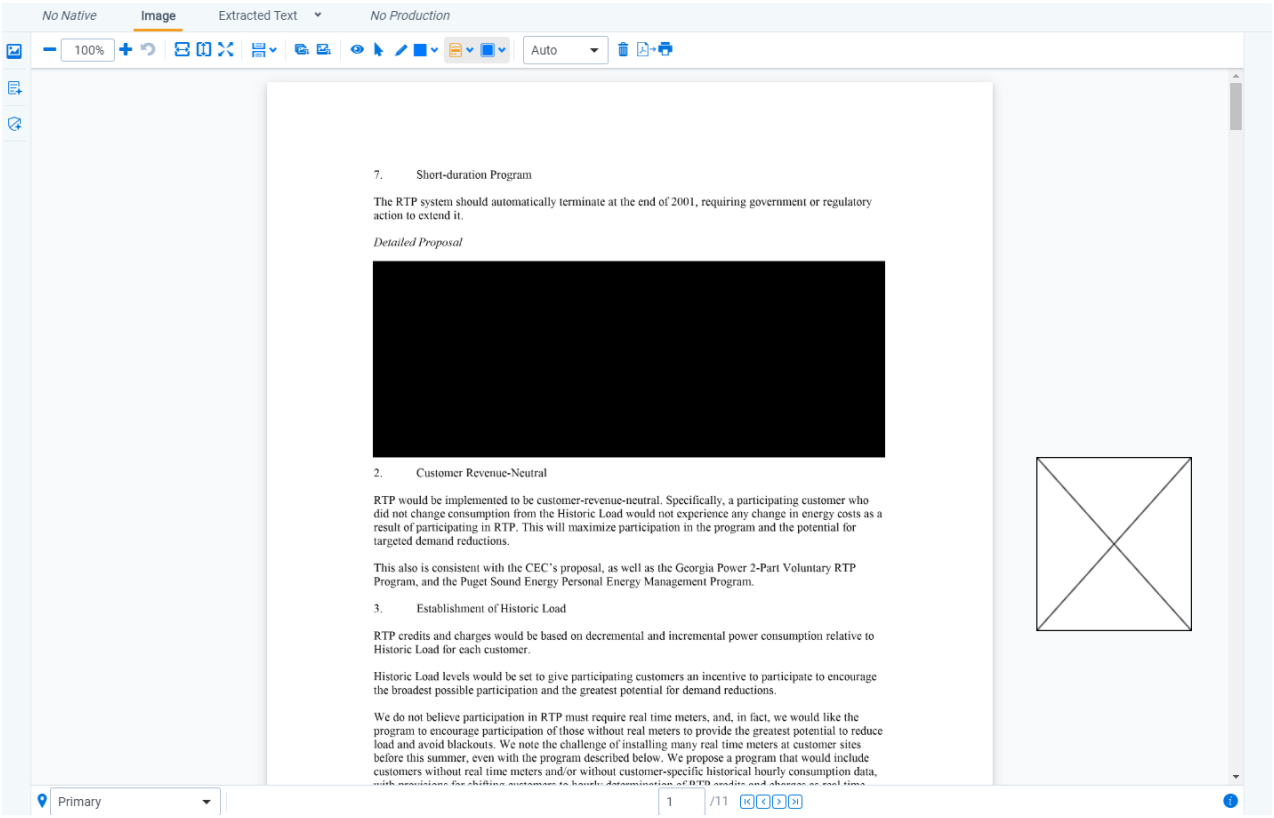
If you have multiple markups on a page that overlap each other, when you hover over the markups, translucent controls appear. Click the markup you want to work with, and the controls become active to indicate which markup is

active. In the following example, the black box redaction is active.



19.5.2 Working with markups outside of page boundaries

If you have markups that exist outside the boundaries of an image, such as those created by custom applications, they will render in their currently saved coordinates in the Viewer. Interacting with the markup by attempting to move or select it will move the markup within the page boundaries. This change is saved and audited in the workspace.



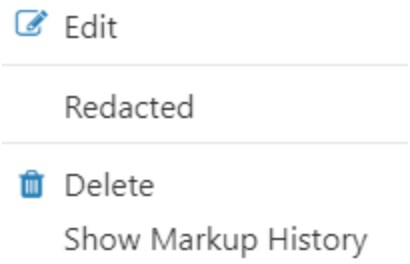
19.5.3 Editing redaction text with a markup set

When you create a text redaction, it will display the most recent word or phrase you entered while editing a redaction. If you have never edited or created a text redaction before, it will display **Redacted** instead.

To perform this task you need the permissions for the markup sets object as well as the individual markup set you wish to use.

To edit the text in a text box redaction using the default text for a markup set:

1. Choose the desired markup set from the drop-down list in the bottom-left corner of the Viewer.
2. Right-click the redaction and select the default redaction text from the markup set.



19.5.4 Editing redaction text

To edit the text in a text box redaction, perform the following steps:

1. Right-click the redaction and select **Edit**.
   The Edit Redaction Text pop-up opens.

2. Enter the new redaction text in the field and click **Edit Redaction**.
   The new text appears in the redaction. Any new redactions you create will display the same text until you edit a redaction or use the default Redacted option.

19.5.5 Editing font size in text box redactions

The font size for text box redactions defaults to fill the entire text box. To edit the font size, perform the following steps:

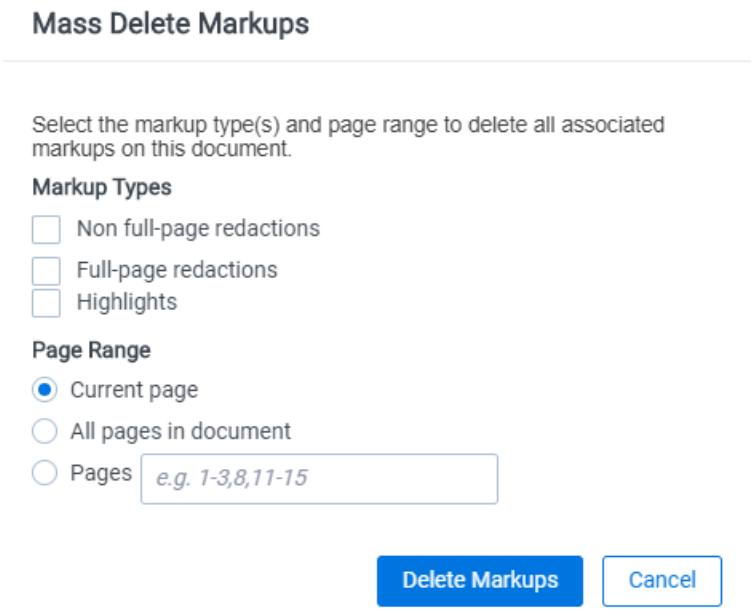
1. Select the text box redactions.
   You can press **Ctrl** or **Shift** and click to select multiple text box redactions.
2. Click the Font Size drop-down menu and select a font size.
   The font size applies to the text in all selected text box redactions.

When you create a new text box redaction, the last selected font size automatically applies to the text.

19.6 Mass deleting markups

You can mass delete markups from a single page, from a range of pages, or from your entire document at once using the delete redactions and highlights option. To mass delete markups:

1. Click the **Delete Highlights** icon.



2. Select the markup types you want to delete. You can select **Non full-page redactions**, **Full-page redactions**, **Highlights**, or any combination of these.
3. Select the range of pages from which to delete the selected markups. You can select **Current page**, **Pages**, enter a set of pages, or **All pages in document**.
4. Click **Delete Markups**. The selected markup types are deleted from the range of pages you selected.

19.7 Controlling markup visibility

You can toggle redaction visibility between visible, transparent, and invisible. Markup visibility only affects how markups display in the Viewer until they are burned in during production. Use the **Change Markup Visibility** icon to change the setting.

- Click once to set the markups to transparent.
- Click a second time to set the markups to invisible. The redactions are not deleted, just temporarily hidden.
- Click a third time to return the markups to full visibility.

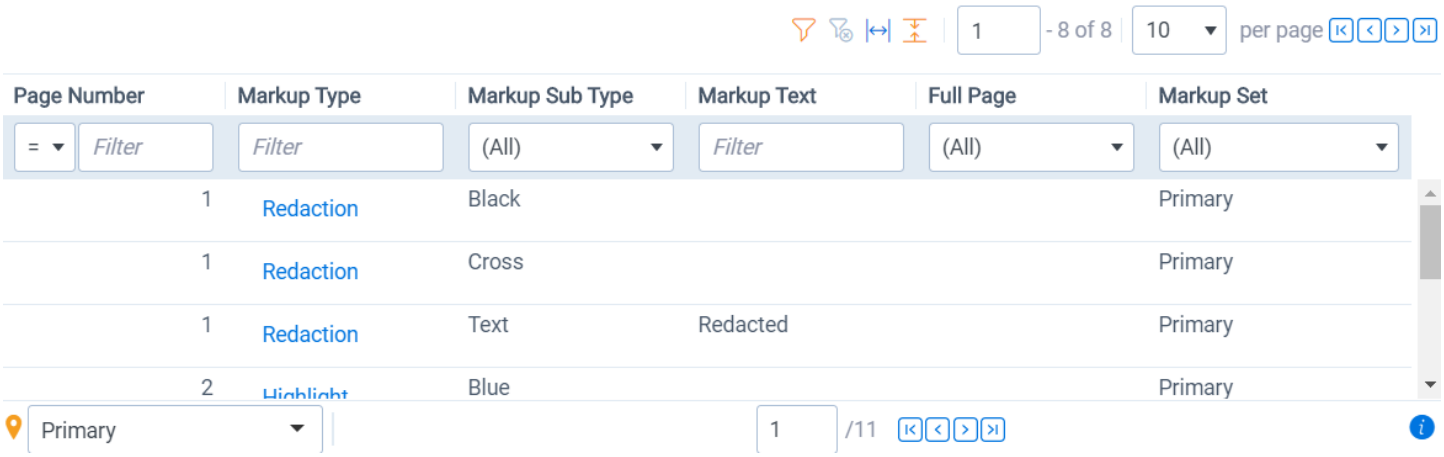
19.8 Viewing markup history

To view the history of any highlight or redaction, right-click on the markup in the Viewer and select **Show Markup History** from the menu. The Markup Information pop-up appears with information identifying each action, the user who performed the action, and the date and time at which the user performed the action.

19.9 Using the Markup Navigation pane

In the Viewer, you can locate markups in a document using the Markup Navigation pane. This pane has different functionality than the Redact navigation card.

To open Markup Navigation pane, click the **Markup Sets** icon in the lower left corner of the Viewer. The Markup Navigation pane displays a list of all redactions and highlights that reviewers created in the document, as well as references to their page numbers and parent markup sets.



You can click anywhere on the markup row to jump to the page where the markup occurs. In addition, Relativity updates the active markup set to the one associated with your row selection in the Markup Navigation pane.

20 Markup sets

A markup set contains highlights and redactions grouped together so that they can conveniently be applied to documents in the Viewer.

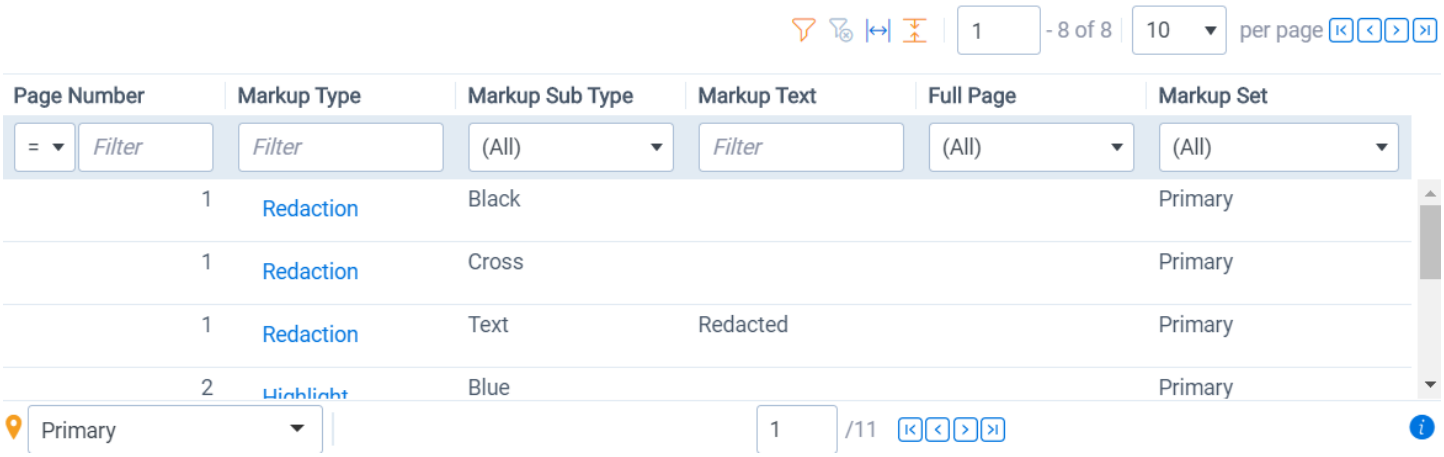
For example, if you want to mark certain redactions as Confidential and others as Private, you can create a markup set containing the words Confidential and Private and apply them to your document set without manually entering the words for each textbox redaction.

Note: The only proper way to secure the text behind a redaction is to the produce the document that contains the redacted text. If a group has View rights only to a markup set (not Edit or Delete rights) and a reviewer in that group loads a document in the Viewer because they have no other way to view that document, they can actually see the text behind the redaction.

While viewing a document, you can change markup sets in the drop-down menu and see different highlights and redactions in the document. Multiple reviewers can redact the same document at the same time using different markup sets.

In the Viewer, you can locate markups in a document using the Markup Navigation pane. This pane has different functionality than the Redact navigation card.

To open Markup Navigation pane, click the **Markup Sets** icon in the lower left corner of the Viewer. The Markup Navigation pane displays a list of all redactions and highlights that reviewers created in the document, as well as references to their page numbers and parent markup sets.



You can click anywhere on the markup row to jump to the page where the markup occurs. In addition, Relativity updates the active markup set to the one associated with your row selection in the Markup Navigation pane.

Note: Before you apply markup to a document, note that the Native Time Zone Offset field controls the date and time that displays on redacted and highlighted images. You may want to review and adjust the UTC value to avoid placing incorrect time designations on documents you intend to produce.

20.1 Permissions

The following permissions are needed to use each part of markup sets:

Object Security	Tab Visibility
• Markup Set - View, Edit, Delete, Add	• Markup Sets

20.2 Creating and editing a markup set

To create or edit a markup set:

1. Navigate to the **Markup Sets** tab.
2. Click **New Markup Set**. If you want to edit an existing markup set, click the **Edit** link next to the markup set name.
3. Complete the fields on the markup set form. See Fields on the next page.

4. Click **Save**.
   The markup set is created and can be selected on the Image Viewer. With a markup set selected, you can apply markups to a document.

20.3 Fields

Markup sets contain the following fields:

- **Name** - the name of the markup set.
- **Order** - indicates the placement of the markup set in the markup set drop-down menu in the viewer. Use the following guidelines when ordering markup sets:
  - The **Markup Set** drop-down menu displays markup sets with low order numbers near the top of the list. (The default markup set has the lowest order number.)
  - Sets with the same order number sort alphanumerically.
  - You can use any positive or negative integer for the order number. You can't use a decimal as an order number.

  Note: We recommend ordering markup sets by groups of 10, such as 10, 20, 30, and so on. Using this numbering scheme you can easily insert another markup set without having to reorder the existing ones.
- **Redaction text** - enter the words or phrases that you want to set as textbox redaction options on native images, native PDF, and stored PDF documents. To access the textbox redaction options, right-click on a selected text redaction in the Native or PDF Viewer. To set multiple redaction options, enter each term on a separate line.

  Note: There is a limit of 15 text redaction options in a markup set. If there are more than 15 options in a markup set, they are not displayed in the right-click menu.

20.4 Copying markup sets

On the markup set list, you can use the Copy mass operation to duplicate a markup set. When you copy a markup set, you also copy any existing redactions that have been applied to documents.

For example, you redact documents with the markup set Attorney, and then you copy this markup set, and rename it Expert. In the viewer, you open a document previously redacted with the Attorney markup set, but now you select the Expert markup set. The viewer displays the document with the redactions previously applied with the Attorney markup set.

To copy a markup set, follow these steps:

1. Navigate to the **Markup Sets** tab.
2. Select the checkbox next to the markup set(s) you want to copy.
3. Select **Copy** from the mass operation drop-down list, and click **Go**.
   The markup set automatically copies and appears in the markup set list. To edit the name of the new markup set, click the **Edit** link, enter a new name, and click **Save**.

   Note: When copying a Markup Set, any existing associated redactions on documents are also copied to the new Markup Set.

21 Mass operations

Using mass operations, you can perform actions on a set of documents at once instead of performing the same action for each individual document. Some mass operations are available to reviewers, while other mass operations will only display in the mass operations bar if you are a system administrator. Access to each mass operation can be granted individually.

For details on how to monitor the status of a mass operation that you've started, see Mass operation jobs.

Notes:

- Some mass operations like Edit, Replace, and Delete can temporarily lock down the document table while executing. In a workspace with a large number of records and users, the table may be locked for an extended period of time and prevent users from performing standard edits. In such cases, we recommend carrying out mass operations at night or an off-peak time.
- You can't use mass operations on Data Grid-enabled fields.
- Custom mass operations may also appear in the list. These include operations added to Relativity by your team or those provided by installed applications in your environment.

21.1 List of standard mass operations

The following table provides a list of the most standard mass operations, specifically those available on the Document object. Click any of the links below for more details.

There are other feature-specific mass operations that occur only on a limited number of objects. These are not listed below, but instead are found in their corresponding feature topics. For example, the Republish operation is available only on the Files tab within the Processing feature.

Mass operation	Description	Additional Required Permissions (Workspace-level)
Edit	You can use the mass edit operation to modify fields and coding values for multiple documents or objects at the same time.	Document: Edit permission on the document object (so the user can modify field values). The fields to be edited must be on a layout the user can access.
Copy	Use Mass copy to copy items within Relativity. By using mass copy you can easily copy and rename items to improve workflows.	Object-specific: Rights to create the given object being copied. For example, to mass-copy views or layouts, the user needs Add (and likely Edit) permission on the View or Layout object respectively, since new copies will be created. (The Mass Copy permission alone is not sufficient without create rights on those objects.)
Move	You can use the mass move operation to move selected documents from their current folder to another existing folder. If you mass move any documents, any custom security applied to those documents is lost.	Document: Add and Delete permissions on the document object. (This combination effectively allows removing the doc from its current folder and adding it to the target folder.) The user also needs rights to the destination folder(usually via having access to the folder structure).
Delete	You can use the Mass delete operation to remove a group of documents or objects from Relativity in a single operation. When	Document: Delete permission on the document object (to remove those documents).Note: if deleting document images/natives as part of the

Mass operation	Description	Additional Required Permissions (Workspace-level)
	you delete documents, you can also remove their images and natives from the file servers.	operation, ensure the group also has rights to delete those files if applicable.
PDF	With the Mass PDF operation you can create PDF files from natives, images, and produced documents, and save those PDFs on your computer. The Mass PDF operation also allows you to store PDFs created from native files or original images in Relativity and review them in the PDF Viewer.	Document: at least View permission on documents to read them. To store PDFs in Relativity, the group needs Add rights on the Relativity Dynamic Object (RDO) that holds stored PDFs (the system manages this).If including produced images in the PDF, the user must have View rights on the "Production Data Source" object (to access produced versions).
Replace	You can use the mass replace operation to replace existing long or fixed-length field text with new content.	Document: Edit permission on the document object (to modify the field content).Essentially the same rights as Mass Edit, on the fields being replaced.
Image	Mass imaging creates TIFF or JPEG images for a document set based on the settings in the imaging profile you select. Relativity also provides a default imaging profile that you can use out-of-the-box.	Document: Add permission on Document (to add new images to documents) and typically View on Document (to read them). Also, the user needs access to an Imaging Profile and an installed Imaging application.Note: In practice, having Add rights on documents and on the Imaging Set/Profile objects is required for imaging operations.
Tally/sum/average	You can use the tally/sum/average operation to tally, sum, or average the values of fields associated with documents or objects. This operation is commonly used to determine the number of pages in a print job or production.	Field: View permission on the fields to be tallied. (The user must be able to see the field values on the documents. No special "edit" needed since it's a read/report action.)If tallying numeric fields for sum/avg, view rights on those fields suffice.
Export to file	Use the Export to file option from the Mass Operations bar to export the current View to a file (e.g., .xls, .cvs, .dat). If no individual records are selected, Relativity will export all records in the current view, regardless of how many records are displayed per page.	Document: View permission on the object(s) being exported (e.g. documents for a document list export).The user must be able to see all fields in the view. No special object rights beyond read access are needed for a basic export.
Convert	Use Mass convert to pre-convert a large set of documents into HTML5 format before review. By using mass convert you can eliminate document load time in the viewer.	Document: View permission on documents (to read and convert them). No additional rights required to convert, aside from an active viewer / conversion agent. (Mass Convert just automates viewer pre-render; if "Mass convert" is enabled for the group, and they can view the docs, they can perform it.)
Save as List	Use this to save a group of documents as a list, follow this procedure. The same steps apply to other objects with **Lists**	Lists: Add permission on the List object (to create a new list of documents). The user also needs rights to view the documents.(In Relativity

Mass operation	Description	Additional Required Permissions (Workspace-level)
	enabled.	aiR, if a user has rights to create Lists, the "Save as List" option will be available on the mass operations bar when appropriate.)
Detect Sentiment	Use this to score documents on the likelihood that they contain specific emotions. For more information, see Sentiment analysis in the Analytics guide.	Analytics/AI: Likely requires the Analytics classification feature to be installed. No explicit separate object permission documented – if the feature is enabled, granting this mass operation should suffice along with View on documents. (Ensure the user can see the sentiment results field if one is used.)

21.2 Mass operations permissions

- **Assign to Entity**—gives group members the rights to select and re-assign an alias to a different entity when using name normalization in Analytics.
- **Cluster**—gives group members the rights to cluster documents using Analytics clustering.
- **Convert**—gives group members the ability to convert a large set of documents into HTML5 format for faster document load times within the viewer.

  Note: Mass convert is not available in repository workspaces.

- **Copy**—gives group members the rights to copy securable objects such as views and layouts.
- **Delete**—group members can mass-delete documents. Mass delete also requires the rights to delete documents.
- **Edit**—gives group members the rights to use their layouts to simultaneously edit document field values for multiple documents.
- **Export**—gives group members the rights to export audit data via Audit.

  Note: This permission only appears if Audit is installed and configured.

- **Export to File**—gives group members the right to export the contents of a view to a .csv, .xls or .dat file.
- **Image**—group members can simultaneously send image requests for multiple native files.
- **Move**—gives group members the right to simultaneously move documents from one or more folders to one target folder. Mass Move also requires add and delete document rights.
- **Merge**—gives group members the rights to select and merge multiple entities into a single entity when using name normalization in Analytics.
- **PDF Actions**—gives group members the ability to download, create, store, or number PDFs. For more information, see Mass PDF permissions
- **Produce**—gives group members the right to simultaneously add multiple documents to a production set.

- **Replace**—group members can perform a replace operation on multiple documents. Examples include:
  - Copying the contents of one text field to another.
  - Adding a set string to the beginning or end of an existing field.
  - Merging the values of a source field with the values of a target field.
- **Process Transcript**—group members can process imported transcripts for viewing in Relativity.
- **Send To Case Map**—group members can send multiple documents to CaseMap.

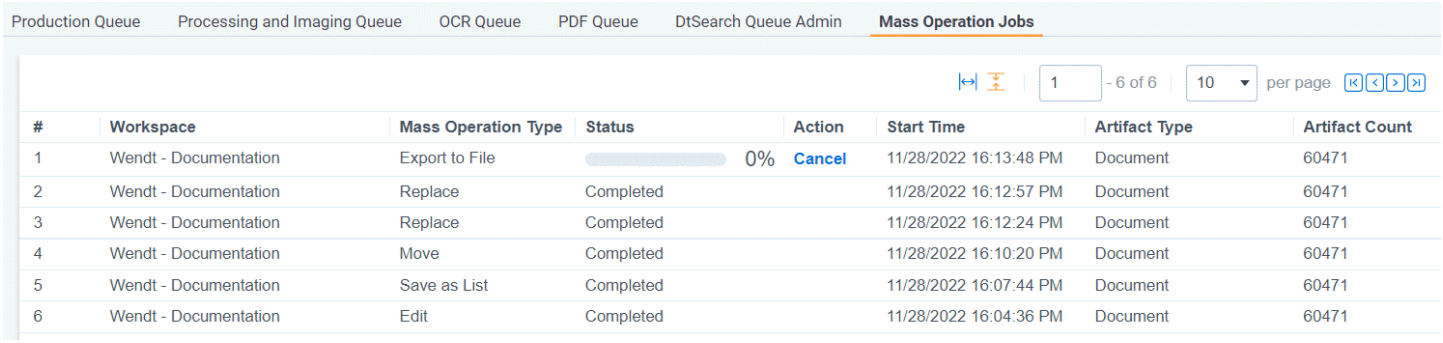
  Note: CaseMap is not compatible with Windows 8.

- **Tally/Sum/Average**—group members can tally, sum and average the values of any numeric fields. This action is recorded under the document history.
- **Custom mass operations**—may appear in this list. They include mass operations that you added to Relativity or that are available in applications currently installed in your environment.

21.3 Mass Operation Jobs status

The Mass Operation Jobs page shows in-progress and recently completed mass operations from the last 5 days across your Relativity aiR instance that don't have a dedicated queue. This page only displays jobs submitted by the current signed-in user.

Note: Users with permissions for the Queue Management tab in the Tab Visibility section of the Admin Security console automatically gain access to the Mass Operation Jobs tab.



#	Workspace	Mass Operation Type	Status	Action	Start Time	Artifact Type	Artifact Count
1	Wendt - Documentation	Export to File	0%	Cancel	11/28/2022 16:13:48 PM	Document	60471
2	Wendt - Documentation	Replace	Completed		11/28/2022 16:12:57 PM	Document	60471
3	Wendt - Documentation	Replace	Completed		11/28/2022 16:12:24 PM	Document	60471
4	Wendt - Documentation	Move	Completed		11/28/2022 16:10:20 PM	Document	60471
5	Wendt - Documentation	Save as List	Completed		11/28/2022 16:07:44 PM	Document	60471
6	Wendt - Documentation	Edit	Completed		11/28/2022 16:04:36 PM	Document	60471

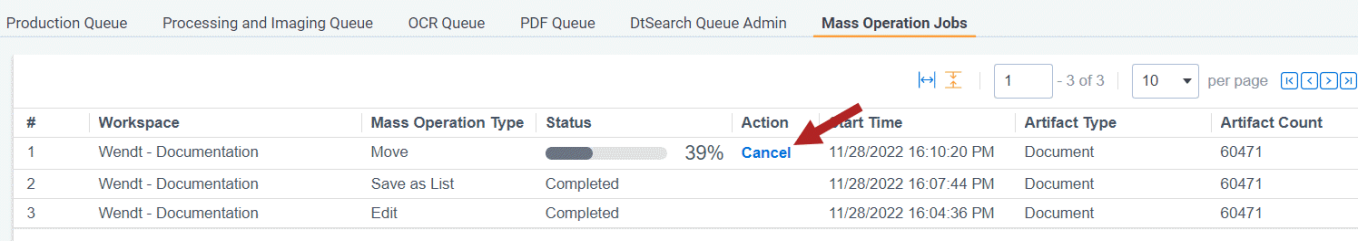
An Edit mass operation job appears on this page. However, a mass Save as PDF job doesn't appear here because it's already included in the PDF Queue. For more details, see the Mass Operation Type list below.

The Mass Operation Jobs page contains the following fields:

- **Workspace**—the name of the workspace in which the mass operation was started.
- **Mass Operation Type**—the specific mass operation that was kicked off. This could include any job for which there is not a dedicated queue, such as:
  - Edit
  - Replace
  - Move

- Save as List
- Export to file

- **Status**—the current state of the job. This will display one of the following:
  - **Idle**—the job has not yet been picked up by an agent and is not yet in progress.
  - **Percent complete**—the job is in progress at the displayed percentage of completeness. During this time, you can click **Cancel** to cancel the job.
  - **Completed**—the job has completed without errors.
  - **Canceled**—the job has been canceled.
- **Action**—any mass operation that is in progress and displays a completion percentage is also eligible to be canceled. To cancel a mass operation, click **Cancel** on the job in the Action column. To confirm the cancellation, click **Cancel job**. The mass operation remains in progress until you confirm its cancellation, which means it is possible for the job to complete before you are able to completely cancel it. If you want to return to the jobs page and allow the job to proceed, click **Go back**.



- **Start Time**—the date and time at which the mass operation was started.
- **Artifact Type**—the object on which the mass operation was run. For example, if you started a mass Edit job on any number of items from the Document list in your workspace, this will display **Document**.
- **Artifact Count**—the number of artifacts returned from the job.

21.4 Cancel production job

To cancel multiple production jobs from the Production Queue tab, use the Cancel Production Job mass operation.

21.4.1 Security configuration

You must configure certain instance level permissions to use Cancel Production Job.

To configure the security permissions:

- Navigate to the **Instance Details** tab.
- Click **Manage Permissions**.
- Click **Edit Permissions** for a group on the Group Management tab.
- Enable the following security permissions:

Object Security	Tab Visibility	Admin Operations
• N/A	• Queue Management (parent) • Production	• Change Queue Priority • View Admin

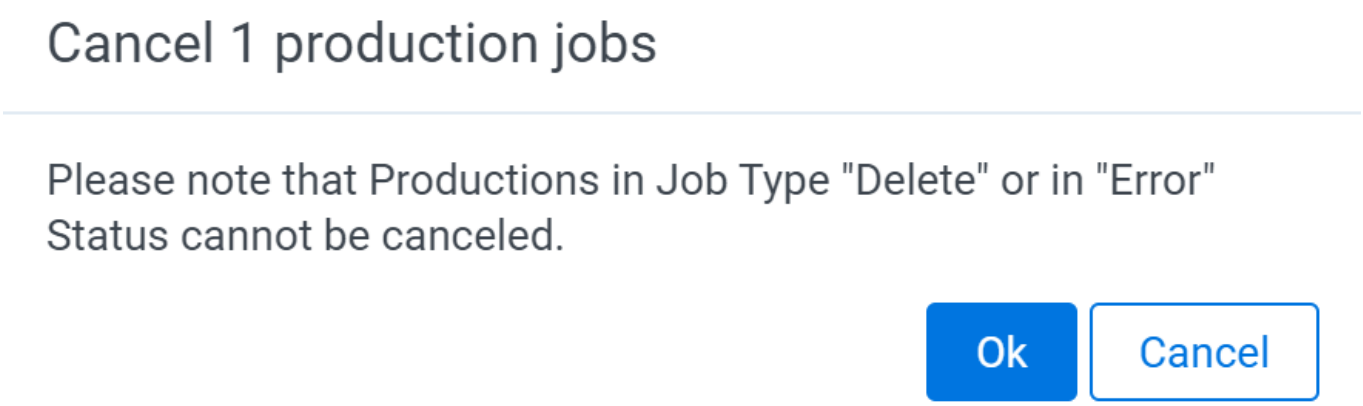
Object Security	Tab Visibility	Admin Operations
	Queue (child)	Repository

Note: As long as users have the listed security permissions, they do not need view permissions to the workspaces or the production jobs to use Cancel Production Job.

21.4.2 Using Cancel Production Job

To cancel multiple production jobs from the Production Queue tab:

- Navigate to the **Production Queue** tab.
- Select the productions jobs that you want to cancel.
- Click **Cancel Production Job** from the mass operations bar. The Cancel production job window opens.



- Click **Ok**.

For more information about the Production queue, see Production queue.

21.5 Mass edit

You can use the mass edit operation to modify fields and coding values for multiple documents or objects at the same time. You can use any layout that you have rights to.

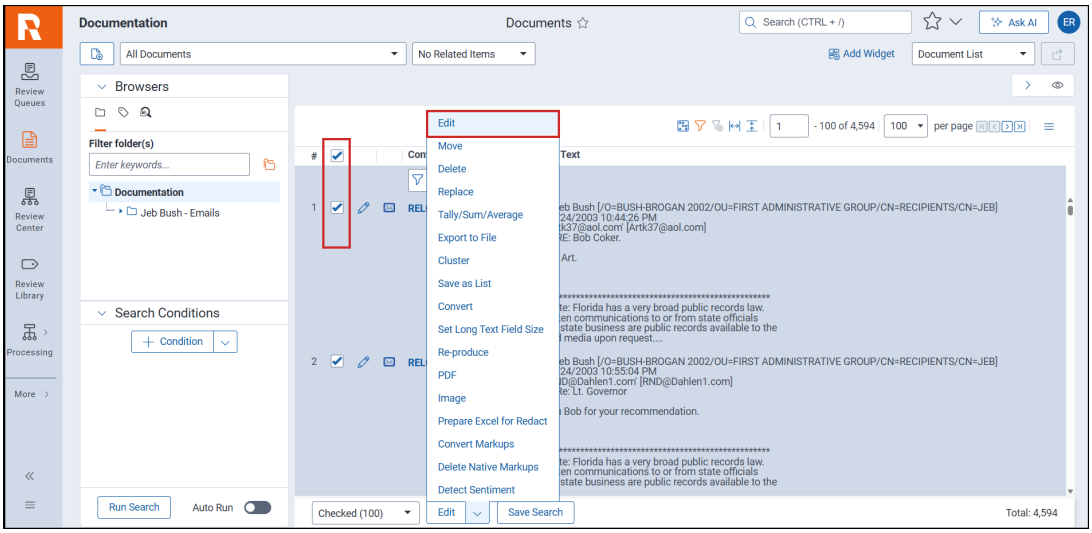
Note: You cannot use mass operations on Data Grid-enabled fields.

Note: To perform mass operations on an object type, ensure that the **'Use Relativity Forms'** setting is enabled for that specific object type.

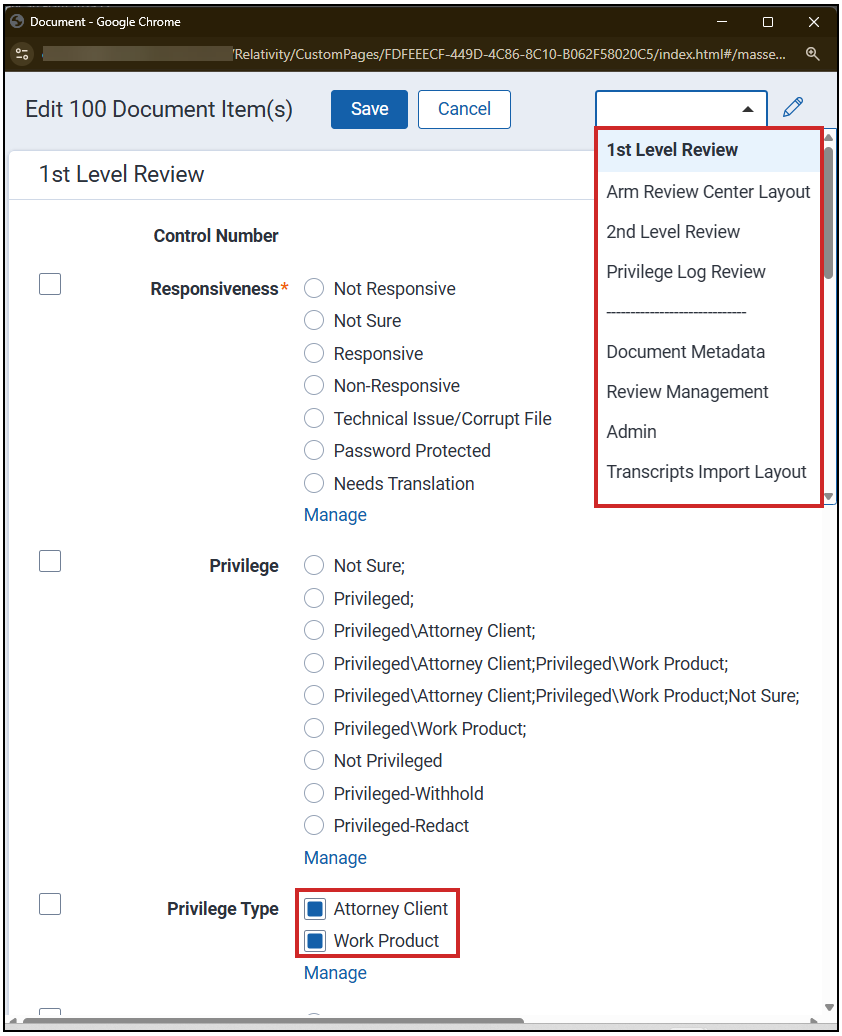
To perform a mass edit operation:

1. From the mass operations bar on the document list, choose whether to edit **All** searchable items or **Checked** items.

2. Select **Edit** in the drop-down menu.



The Mass Edit form displays. Using the drop-down menu, you can select from all layouts you have rights to see.



3. Select the layout and fields. There are three options for multiple-choice field values, known as a tri-state check box:

- Blank removes the value from any of the selected documents.
- Shaded leaves any values on the selected documents as-is.

  Note: When mass editing Yes/No fields, the shaded check box sets the value to null.

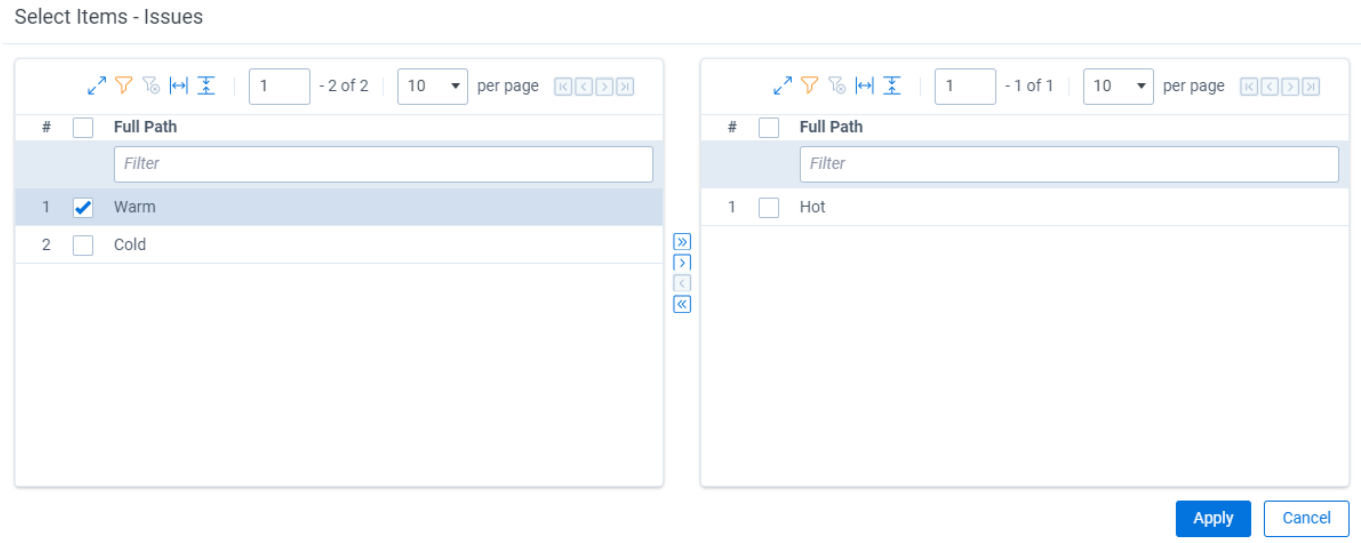
- Checked applies the option to all selected documents.

4. Click **Save** to apply your changes.

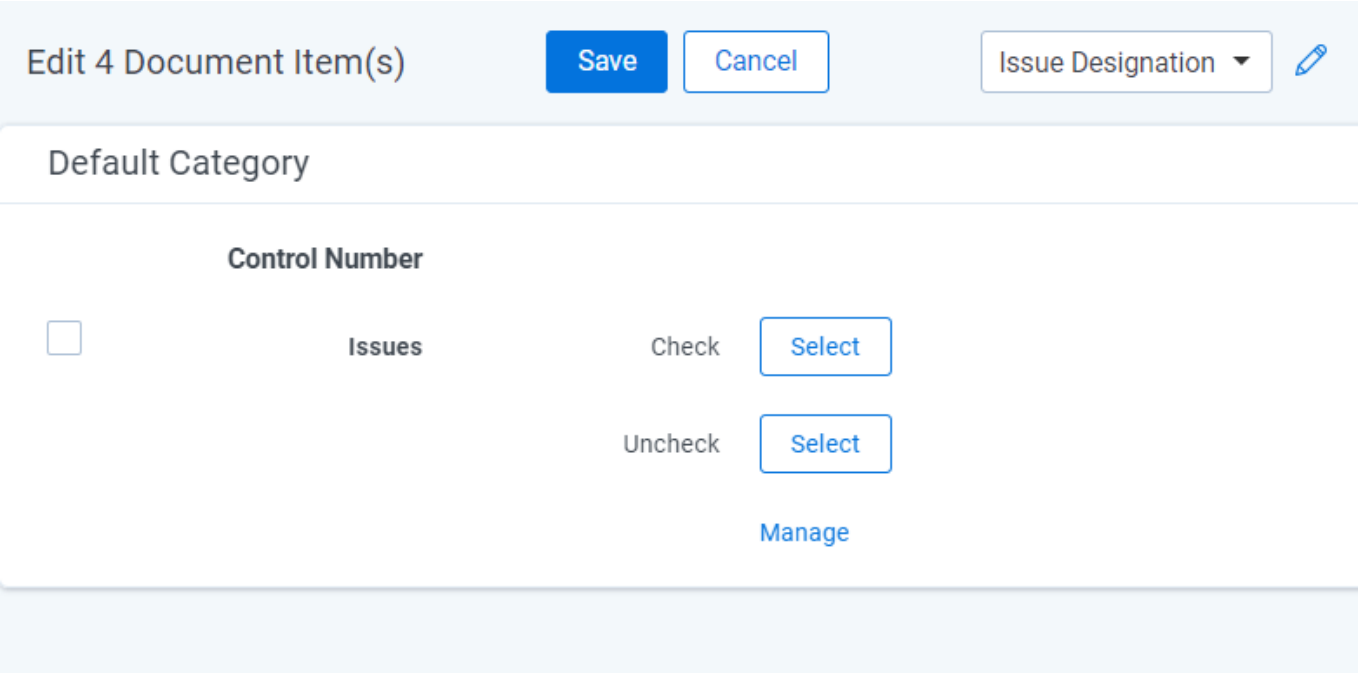
21.5.1 Working with multi-choice fields on the mass edit form

In the mass edit form, there are two options for editing multi-choice fields: a checkbox or a pop-up picker. When you select the pop-up picker as the display type during the layout build, there are two options to edit the field: **Check** and **Uncheck**.

1. Click **Check** to create a list of items to add to the field or click **Uncheck** to create a list of items to remove from the field. Items not selected remain unchanged. Clicking either **Check** or **Uncheck** opens the Available Items window.
2. From the **Available Items** window, you can move choices and objects into the Selected Items list. Select the check box next to the desired selection, and move it to the right panel. This builds a list in the bottom window of selected items. To remove something from this list, select it and move it to the left panel.
3. Click **Apply** to proceed with the action to **Check** or **Uncheck** the items from the field. Clicking **Cancel** stops any action.



On the sample screen below, the mass edit form reflects checked and unchecked objects and choices.



4. Once values have been set, a **Clear** link displays next to the Check and/or Un-Check buttons. You can then clear the set values without returning to the Items to Check window to remove them. You can add a new choice to a multi-choice field using the Add link.
5. Click **Save** to apply your updates and redisplay the item list. If the item list loads slowly, and you cancel the request, your updates to the documents remain saved.

Note: When you attempt to mass edit documents in the Related Items pane while there are unsaved changes in the current layout, Relativity displays a message indicating that your changes will be lost. If you continue, the coding values in the layout are updated to match those selected for the mass edit.

21.6 Mass copy

Use Mass copy to copy items within Relativity. By using mass copy you can easily copy and rename items to improve workflows. Mass copy is not available on the Document object.

Note: Large mass copy jobs may reduce performance for other users in the workspace. We recommend running them during off-peak hours. For search terms reports, schedule the copy job and any report runs separately.

Note: You cannot use mass operations on Data Grid-enabled fields.

To perform a mass copy:

1. From the mass operations bar on the document list, choose whether to copy **All** searchable items, **Checked** items, or **These** items in the current returned set.
2. Select **Copy** in the drop-down menu.
   The Copy window displays.
3. Click **Ok** to copy the items.

21.7 Mass move

You can use the mass move operation to move selected documents from their current folder to another existing folder. If you mass move any documents, any custom security applied to those documents is lost. The document inherits the rights of the new parent folder.

If documents are moved in error, you have two options to reverse the action:

- **Manual Reversion:** Move each document back to its original sub-folder individually.
- **Database Restore:** Restore the workspace database to a backup from before the mass move occurred. This option may require assistance from your system administrator and could impact other recent changes in the workspace.

Note: You cannot use mass operations on Data Grid-enabled fields.

From the mass operations bar on the document list, choose whether to move **All** searchable items, **Checked items** or **These** items in the current returned set.

1. Select **Move** in the drop-down menu.
   The mass move select folder form displays.
2. Select the target location and click **OK**. Note that all documents move to the target directory. The subdirectory structure of the source folder is maintained.



21.8 Mass delete

Remove documents and objects efficiently with **Mass delete**. This feature lets you delete a group of documents or objects from Relativity in one go. You can even choose to remove their associated images and native files from the file servers for a more comprehensive cleanup.

Access Mass delete from the Mass operations toolbar. If you have the necessary permissions, you can even execute a **force delete**, which permanently removes documents and certain objects, including unlinked associative entities and child objects. This option requires the **Delete Object Dependencies** permission within the Admin Operations section of the security settings.

Note: Mass delete is a permanent action, so ensure you **double-check your selections before proceeding**, as this operation cannot be undone. Additionally, Mass operations are **not** supported for Data Grid-enabled fields.

21.8.1 Mass delete permissions

Users need the following permissions to successfully mass delete documents:

Object Security	Other Settings	
Document	Mass Operations	Admin Operations
• View (Eye icon) • Edit (Pencil icon) • Delete (Trash can icon) • Add Image • Delete Image	• Delete • Edit • Image	• Delete Object Dependencies

21.8.1.1 Deleting documents that were published through Processing has two key effects:

- **Marking deleting:** The deleted documents get flagged as "Yes" in the "Processing Deletion" field on the Discovered Files page. This helps track which documents no longer exist after being published.
- **Recalculating deduplication and publishing new primaries:** Relativity automatically analyzes the remaining data to identify duplicates and adjust its understanding of the primary documents. If applicable, new primary documents may be published to replace the deleted ones. This ensures an exact data representation and avoids issues with missing information. For more details on this behavior and its implications, refer to the documentation section on Post-publish delete.

To mass delete documents after publishing, follow the steps in the Processing topic, Post-publish delete > Running a post-publish delete.

21.8.1.2 Special considerations

Deleting Documents:

- **Full deletion:** By default, this removes everything - documents, duplicates, and associated files. You can choose to preserve the document record by keeping it in place and only deleting images or native files.
- **Force delete:** When performing a full deletion, this permanently removes the selected data. For image and native file deletions, you can disable force delete as immediate or permanent removal might be necessary.
- **Create audit snapshot:** Enable this option to create an extra audit record for every deleted document, helping you track changes and keep a detailed history.

Best Practices to Avoid Slow Mass Deletes

Large mass delete operations can strain system resources, causing long job runtimes and potential timeouts.

Follow these best practices to ensure efficient deletions:

Disable Snapshot Auditing

Snapshot Auditing on Delete creates a copy of every field for each document before deletion. This significantly slows large mass deletes.

In order to improve performance:

- Turn off snapshot auditing on the Document object type before running large deletes.
- Standard audit events (edits, deletions) are still logged—you retain a full audit trail of actions taken on documents.
- Only enable snapshot auditing if your data governance policies require a complete copy of each deleted record. See Enabling or disabling snapshot auditing on delete on the next page.

Remove Pre-Delete Event Handlers

Custom Pre-Delete event handlers execute additional logic before each deletion, adding overhead to every item being deleted.

Note: Pre-Delete handlers are different from Pre-Mass-Delete handlers. Check your workspace for any Pre-Delete handlers attached to the Document object and remove or disable them before running large mass deletes.

Manage Extracted Text Storage

If extracted text is stored in SQL rather than Data Grid and the extracted text is very large, it can significantly slow mass delete times.

We recommend running a mass edit to clear extracted text from the documents before deleting. While the edit operation will take time, it makes the subsequent delete much faster.

Simplify Delete Dependencies

If the delete dependencies list is very long, the deletion will take longer to process.

We recommend using a mass edit to clear out multi-object fields before deleting. This reduces the number of relationships the system must handle during deletion.

Batch Large Deletions

Deleting millions of documents in a single operation can overwhelm the system.

We recommend deleting no more than 500,000 documents at a time.

Smaller batches:

- Reduce the risk of timeouts
- Make it easier to monitor progress
- Allow for recovery if issues occur

Schedule Deletes During Off-Peak Hours

If the workspace is under heavy use (such as during active document review), schedule mass deletes during off-peak times—nights or weekends. This minimizes impact on other users and reduces system contention.

Note: If deletions continue to fail or run excessively long after following these practices, contact support for additional assistance.

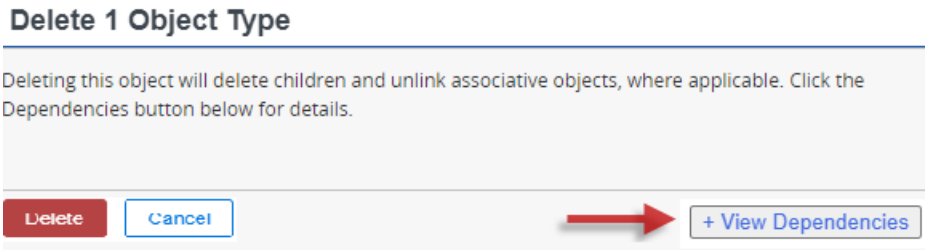
21.8.2 Performing a mass delete on other objects

To perform a mass delete operation on other objects, execute the following steps:

1. Navigate to the tab for the object that you want to delete.
2. Select **Checked items** or **All items** in the current returned set.
3. Select **Delete**. The Delete Details form prompts you to confirm the deletion.

- **Note:** Depending on your access level, you may see a warning on the Delete Details Form when deleting certain objects. This means that removing these objects will also automatically delete their associated objects (like child items) and unlink related objects (like associative links).

- This is only applicable when deleting specific types of , such as:
  Analytics Categorization Sets: Categories and associated data will be deleted.
  Search Terms Reports: Reports and associated data will be deleted.
  OCR Sets: OCR data and associated documents will be deleted.
  Image Sets: Images and associated documents will be deleted.



4. Click **Delete** to delete the object and its children, as well as unlink associative objects. This message displays when you have the security permission **Delete Object Dependencies** listed in the Admin Operations section of the Security page.
5. (Optional) To view a report showing affected objects, click **View Dependencies**. When the current object doesn't have any children or associative objects, the **View Dependencies** toggle is turned off.

To improve mass delete performance when deleting large numbers of documents, turn snapshot auditing off. See Enabling or disabling snapshot auditing on delete below.

21.8.3 Enabling or disabling snapshot auditing on delete

- Enabling the "snapshot audit" creates a full copy of the current value of every field for every deleted document. This means you retain a full historical record of their contents even after deletion, enabling you to track document changes over time. However, be aware that it can considerably expand the audit table size and potentially add some delay to mass deletions.
- Even with "snapshot audit" turned off, the system meticulously tracks every field change for every document, creating a detailed record. So, even when you delete a document, its audit trail remains preserved, capturing all alterations made before its deletion. This effectively meets the need to document coding decisions on deleted documents, as they were finalized and registered before the document's removal.
- While enabling "snapshot audit" offers valuable historical documentation, it comes at a cost: a noticeably larger audit table and potentially sluggish mass deletions. This occurs because the system meticulously captures every deleted document, replicating its entirety. This can be resource-intensive and delay your deletion tasks.
- For a quicker and more efficient mass delete experience, consider these two optimizations:
  - Disable the "snapshot audit" setting. This eliminates the need to create and store complete copies of every deleted document, significantly reducing the size of the audit table and the overall resource

demands of the deletion process.

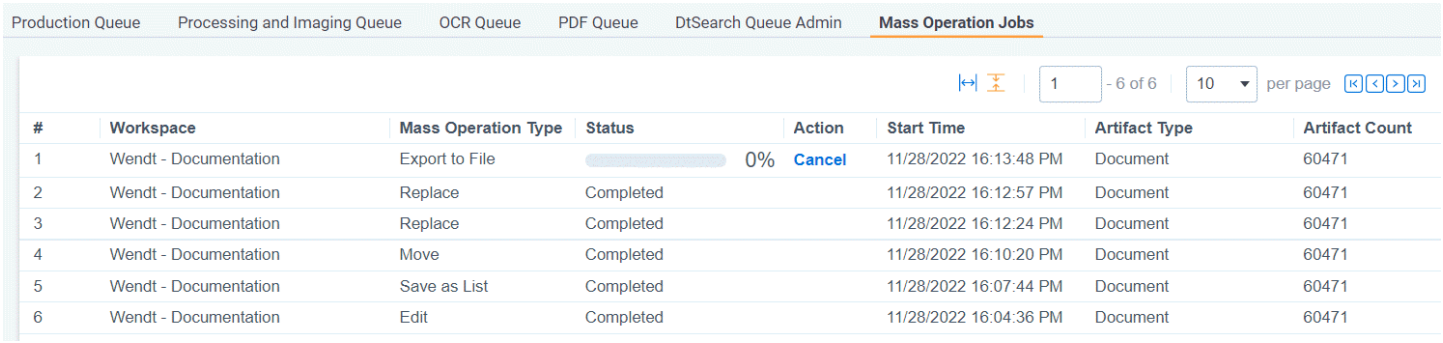
- Remove any "PreDeleteHandlers" attached to the document object. These custom pre-deletion scripts can add unnecessary steps and delays to the process. By removing them, you allow documents to be deleted directly, streamlining the workflow and improving performance. For information on PreDeleteHandlers, see Pre Mass Delete event handlers.

Feature	Description	Impact on Mass delete performance
Snapshot audit	Creates a full copy of every deleted document	Significantly increases the size of the audit table and slows down the Mass deletion process
PreDeleteHandlers	Custom code that runs before deleting a document	Can slow down the Mass deletion process

21.9 Mass Operation Jobs status

The Mass Operation Jobs page shows in-progress and recently completed mass operations from the last 5 days across your Relativity aiR instance that don't have a dedicated queue. This page only displays jobs submitted by the current signed-in user.

Note: Users with permissions for the Queue Management tab in the Tab Visibility section of the Admin Security console automatically gain access to the Mass Operation Jobs tab.



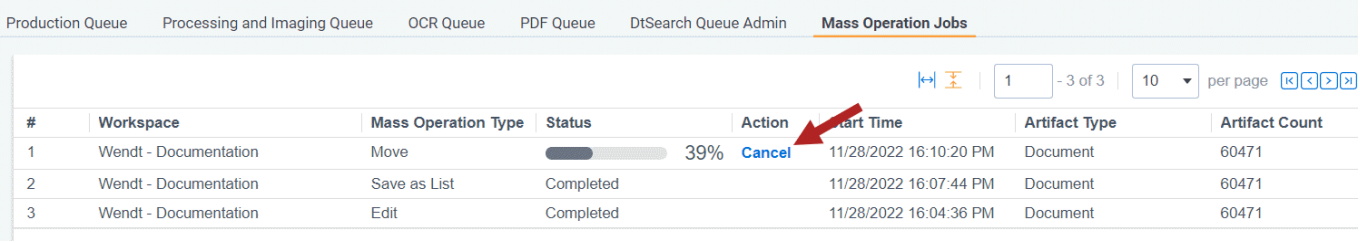
#	Workspace	Mass Operation Type	Status	Action	Start Time	Artifact Type	Artifact Count
1	Wendt - Documentation	Export to File	0%	Cancel	11/28/2022 16:13:48 PM	Document	60471
2	Wendt - Documentation	Replace	Completed		11/28/2022 16:12:57 PM	Document	60471
3	Wendt - Documentation	Replace	Completed		11/28/2022 16:12:24 PM	Document	60471
4	Wendt - Documentation	Move	Completed		11/28/2022 16:10:20 PM	Document	60471
5	Wendt - Documentation	Save as List	Completed		11/28/2022 16:07:44 PM	Document	60471
6	Wendt - Documentation	Edit	Completed		11/28/2022 16:04:36 PM	Document	60471

An Edit mass operation job appears on this page. However, a mass Save as PDF job doesn't appear here because it's already included in the PDF Queue. For more details, see the Mass Operation Type list below.

The Mass Operation Jobs page contains the following fields:

- **Workspace**—the name of the workspace in which the mass operation was started.
- **Mass Operation Type**—the specific mass operation that was kicked off. This could include any job for which there is not a dedicated queue, such as:
  - Edit
  - Replace
  - Move
  - Save as List
  - Export to file

- **Status**—the current state of the job. This will display one of the following:
  - **Idle**—the job has not yet been picked up by an agent and is not yet in progress.
  - **Percent complete**—the job is in progress at the displayed percentage of completeness. During this time, you can click **Cancel** to cancel the job.
  - **Completed**—the job has completed without errors.
  - **Canceled**—the job has been canceled.
- **Action**—any mass operation that is in progress and displays a completion percentage is also eligible to be canceled. To cancel a mass operation, click **Cancel** on the job in the Action column. To confirm the cancellation, click **Cancel job**. The mass operation remains in progress until you confirm its cancellation, which means it is possible for the job to complete before you are able to completely cancel it. If you want to return to the jobs page and allow the job to proceed, click **Go back**.



- **Start Time**—the date and time at which the mass operation was started.
- **Artifact Type**—the object on which the mass operation was run. For example, if you started a mass Edit job on any number of items from the Document list in your workspace, this will display **Document**.
- **Artifact Count**—the number of artifacts returned from the job.

21.10 Mass replace

You can use the mass replace operation to replace existing long or fixed-length field text with new content.

Note: You cannot use mass operations on Data Grid-enabled fields.

To perform a mass replace operation, perform the following steps:

1. From the mass operations bar on the document list, choose whether to replace text in **Checked items** or **All items** in the current returned set.
2. Select **Replace** in the drop-down menu.

   The Replace Documents form displays.
3. Complete the fields on the Replace Documents form.
   - **Field** - the field you want to update. Select from workspace fixed length or long text fields.
   - **Action** - determines the action to be performed:
     - **Replace Entire Field** - replaces the field entirely.
     - **Append to End** - adds the new value to the end of the field. A delimiter option appears. Enter a character to separate the existing and appended values.
     - **Insert at Beginning** - adds the new value to the beginning of the field. A delimiter option appears. Enter a character to separate the existing and prepended values.

- **Search For** - use to search (and thus replace) only selected text in the field instead of the entire field. A new text option displays, where you can enter the text you want to replace.

- **Update With** - determines what is applied to the field.
  - **Text** - adds text to the field.
  - **Field** - adds another field's value to the field set above.
- Click **Add Another Field** at the top of the form to add an additional replacement action to the form.

21.11 Mass image

Mass imaging creates TIFF or JPEG images for a document set based on the settings in the imaging profile you select. Relativity also provides a default imaging profile that you can use out-of-the-box. You can customize profiles to create color JPEG images, adjust image size, and leverage other formatting options.

The mass image operation uses the same technology as the Relativity native file viewer.

Note: The mass image operation is disabled if the Imaging application isn't installed.

To perform a mass image operation, perform the following steps:

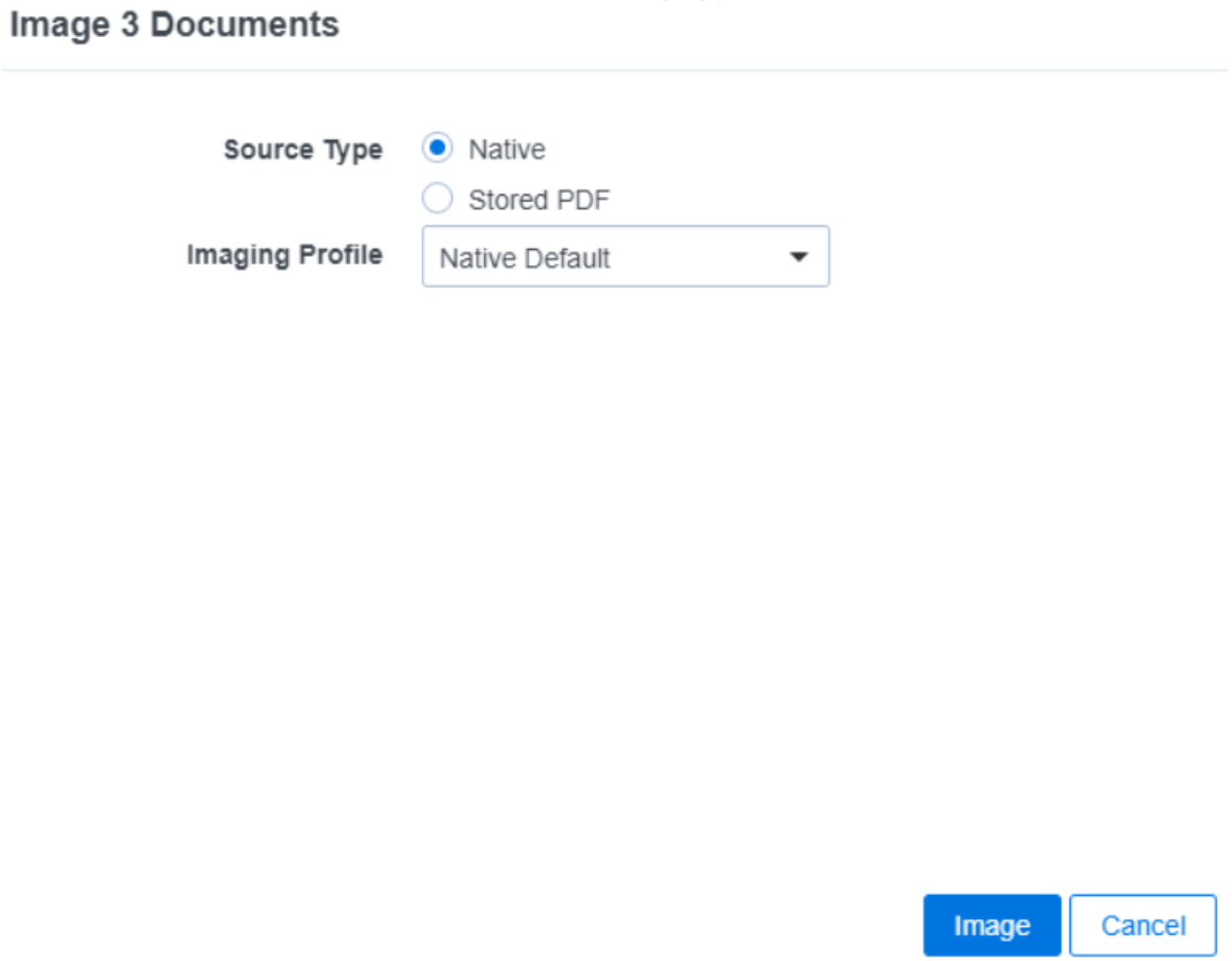
Note: You cannot use mass operations on Data Grid-enabled fields.

- From the mass operations bar on the document list, choose whether to image **Checked items** or **All items** in the current returned set.

  Note: The maximum number of documents you can select at one time for the mass image action is 10,000 documents. If the number of documents selected exceeds this value, a warning appears and prevents the job from running. If you want to image more than 10,000 documents, create and run an imaging set.

- Select **Image** in the drop-down menu.
  The Image Documents pop-up displays.
- Select a **Source Type**.

- Select an option in the **Imaging Profile** drop-down menu. Only profiles that you have permissions to use appear. You can also use the **Default** profile for the imaging job.



- Click **OK** to create the images. Depending on the number of documents you submit, this may take some time. Image-on-the-fly jobs take precedence over batch image jobs.

Note: If any of the documents you selected to image is of a type that is included in the Restricted Native Types object on the imaging profile you selected for the mass image job, that document can't be imaged and you receive a corresponding error message.

21.12 Tally/sum/average

You can use the tally/sum/average operation to tally, sum, or average the values of fields associated with documents or objects.

This operation is commonly used to determine the number of pages in a print job or production. For documents, it's recorded under the document history.

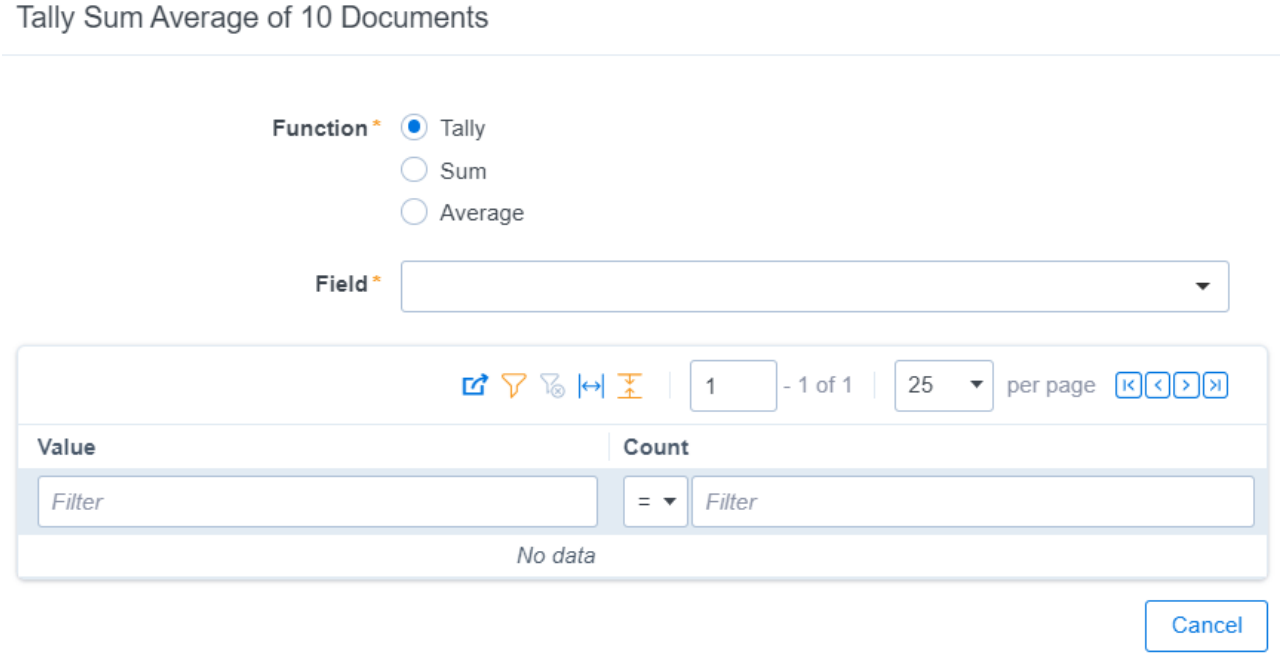
21.12.1 Considerations

- You can only use tally/sum/average on **fixed-length text**, **choice**, **user**, and **number** fields.
- You can't use mass operations on Data Grid-enabled fields.

- Tally/Sum/Average calculates the mean of a column without counting null as 0. When a column contains null values, the operation yields a different result from an average calculated by summing the column and dividing the total document count. To include null values in the denominator of a Tally/Sum/Average calculation, you must change the null value to **0** to ensure the inclusion of those documents.

To perform a tally/sum/average operation, perform the following steps:

1. Choose whether to tally/sum/average **Checked items** or **All items** in the current returned set
2. Select **Tally/Sum/Average** in the drop-down menu. The Tally/Sum/Average pop-up displays with options for the following fields:
    - **Field** - used as the basis of the calculation. For example, you could select a custodian field if you want a tally of these entries.
    - **Function** - the option performed on the field:
        - **Tally** - lists a count for each item type in the specified fields of all selected documents or objects.
        - **Sum** - adds the values in the specified numeric fields of all selected documents or objects.
        - **Average** - calculates mean value of the specified numeric fields for all selected documents or objects.



The result of a tally is similar to a summary report; it outlines the values of a field and the count for each. The tally runs across the entire section, but only reports the top 100,000 values. After your results appear, you can perform the following actions:

- Filter the results.
- Clear All filter text.
- Browse through the results using the blue arrows.
- Sort the results.
- Export results to an external file.

21.13 Mass export to file

Use the Export to file option from the Mass Operations bar to export the current View to a file (such as, .xls, .cvs, .dat). If no individual records are selected, Relativity will export all records in the current view, regardless of how many records are displayed per page. For example, if a saved search returns 1,000 records and you 'Export to File' the view without selecting individual records, Relativity will export 1,000 records.

All fields in the current view and its content are exported, including unicode characters.

21.13.1 Considerations

- Mass exports do not guarantee any sort order in the exported data, nor does mass export to file necessarily save data in the same order as it is displayed in the interface.
- The Mass export to file option displays in the mass operations bar on the Views, Tabs, and Relativity Scripts Library tabs.
- You cannot use mass operations on Data Grid-enabled fields.

21.13.2 Using mass export to file

To perform the Export to file mass operation:

1. Select the records you want to export from the view. Do not select any records if you would like to export all of them.
2. Select **Export to File** in the drop-down menu.
   The Exporting form displays.
3. Select values for the fields on the Exporting Documents form. See Fields below.
4. Click **Run** to export the file or **Cancel** to cancel the export.

21.13.3 Fields

- **Format**
  - Excel spreadsheet via HTML (.xls) creates an Excel file. Fields are placed into separate cells in the .xls file. Fields are placed into separate cells in the .xls file.
  - Comma Separated Values (.csv) creates a comma delimited text file. Fields are separated by semi-colons. Fields are separated by semicolons in the .csv file.
  - Concordance DAT format (.dat) creates a DAT text file with the standard concordance delimiters. Fields are separated by semicolons in the .dat file.

    Note: The names of exported files include the word *export*, the date (YYYYMMDD), the time (HHMMSS in UTC), and a file extension. For example, the name of an exported file might be export_20131119_16073.xls.
- **Encoding**—select the desired encoding for the output file.
- **Escape Formulas**—select Yes or No. When you select Yes, any line starts with the following special characters: =,@,+,-, or if the line starts with any combination of spaces before those characters, Relativity prepends a single quote to the beginning of the line.

21.14 Move to folder path

Note: The Document Utilities application is required to use the move to folder path mass operation.

You can use the move to folder path mass operation to move documents to a new folder that you specify in a text field on the document object. Relativity automatically creates the new folder when you run this mass operation. You can also specify a default folder that Relativity uses when the destination folder path isn't set on a document. You must install the Document Utilities application to add the Move to folder path mass operation to your workspace.

A sample use case for this mass operation involves updating the folder path for documents loaded into the wrong folder on a workspace. For example, you may have inadvertently selected file path as the folder path when importing documents via Import/Export.

In addition, the move to folder path mass operation provides you with the ability to move multiple documents to different folders simultaneously. Unlike the mass move operation, where you can only select a single folder when moving documents. For more information, see Mass move on page 362.

21.14.1 Prerequisites for the move to folder path mass operation

You must complete the following prerequisites before you can use the move to folder path mass operation:

21.14.1.1 Installing the Document Utilities application

You must install the Document Utilities application to add the Move to folder path mass operation to your workspace. The installation process follows the same steps used to install other Relativity applications. For more information, see Installing applications on the Relativity RelativityaiR Documentation site.

You must have system admin permissions to install an application. See Workspace security on page 622.

Complete these steps to install the application:

1. Log in to the Relativity Community (https://community.relativity.com/s/files), and search on Document Utilities. When the search results appear, locate the Relativity.DocumentUtilities.rap in the Files section.

   Note: You need to register to access the Relativity Community if you don't currently have an account. You also must have an Admin Contact account type in the Relativity Community to download applications. If you don't currently have this account type, contact an Admin Contact in your organization, who can then request that Customer Support assign this account type to you. For more information, contact Customer Support via the Community site.

2. Download the Relativity.DocumentUtilities.rap file.
3. Install the Document Utilities application in a workspace or add it to the Application Library tabs making it available for installation in workspaces across your environment. For more information, see Installing applications on the Relativity RelativityaiR Documentation site.

After installing the application, Relativity displays the **Move to folder path** option in the drop-down menu on the mass operations bar.

21.14.1.2 Setting required security permissions

You must have the following security permissions to run the move to folder mass operation:

- **Mass operations** - Under the Mass Operations section of the Other Settings Tab in Workspace Security, you need permissions to the following:
  - **Move**
  - **Move to folder path**

- **Object security** - you need to have the following permissions on these objects in the Object Security tab under Workspace Security:
  - **Document** - requires **Add** and **Delete** permissions.
  - **Folder** - requires **Add** and **Edit** permissions. If you want to remove empty folders, you also need **Delete** permissions.
- **Layout security** - you need to have **View** permissions on the **Move Documents to Folder Path Layout** in the Layouts tab.
- **Folders security** - you need permissions to **Folders** in the **Browsers** section of the **Other Settings** tab.

21.14.1.3 Creating a destination folder path field

Before you can run this mass operation, create a fixed-length or long text field type for storing a destination folder path on the document object.

Use these guidelines for formatting your folder path:

- Separate nested folders in the path with forward slashes (/) or backward slashes (\).
- Don't use a slash as the initial character in your folder path. A final slash isn't required in the folder path.
- Don’t use these special characters (/ \ : ? " * < > |) in your folder names. If your folder names include these characters, Relativity strips them out, except for back and forward slashes used as delimiters. For example, a path with folders named *Custodians|<>/Revie\wed/Ja*?ne* would become *Custodians/Reviewed/Jane*.
- Folder paths may include Unicode characters.
- Folder paths may include the workspace name, but it isn't required. For example, if you have a document with a destination path of *<WorkspaceName>\Custodian* and another one with the path of *Custodian*, this mass operation moves both documents to the *Custodian* folder under the workspace root.

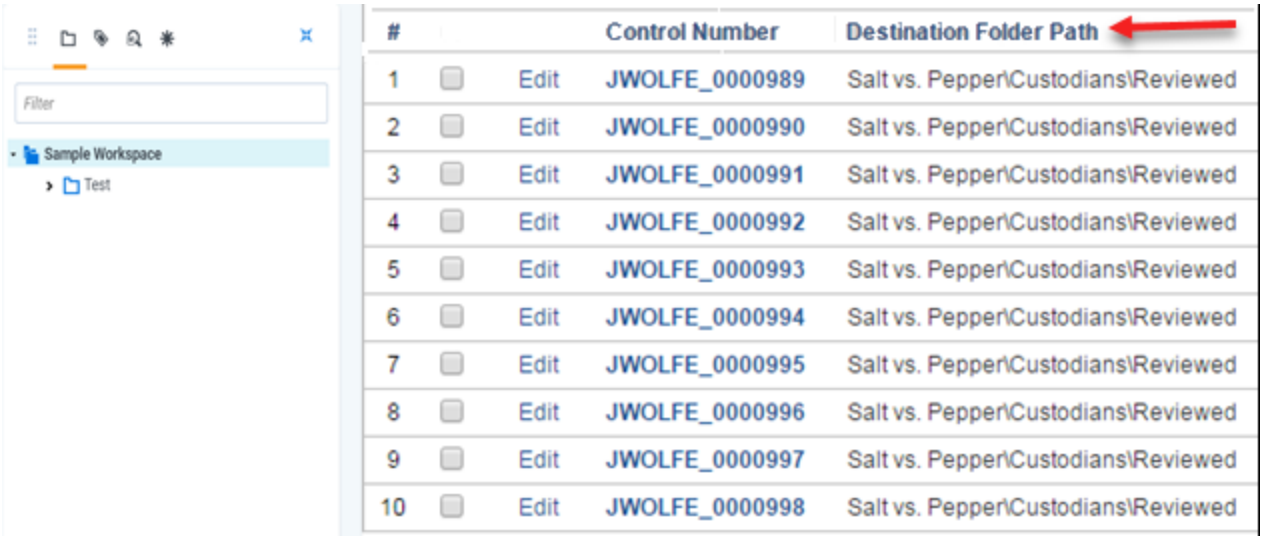
21.14.1.4 Populating the folder path field on the document object

After creating a folder path field on the document object, you must populate it with a destination folder path for the documents that you want to move.

Perform one of the following tasks to populate this field with the destination folder path:

- **Edit the field** - click the **Edit** link that appears on the Documents tab, and update this field on the document when Relativity displays the layout containing it.
- **Run a mass edit operation** - see Mass edit on the Relativity Documentation site.
- **Overlay the destination folder fields on documents** - see Import/Export on the Relativity Documentation site.

The following screen shot illustrates a list of documents with a folder path field set to a specific destination:



21.14.2 Running the move to folder path mass operation

When you run the move to folder mass operation, Relativity moves all the documents with the same destination folder in a single batch. While the Move to folder path mass operation batches documents moving to the same folder, the MassCustomBatchAmount and the MassMoveBatchAmount instance settings control the batching process. The MassCustomBatchAmount instance setting controls the number of documents per batch for each unique destination folder. The MassMoveBatchAmount value controls the number of documents for each batch size. See Instance settings on the Relativity Documentation site.

For optimum performance, use these guidelines when running this mass operation:

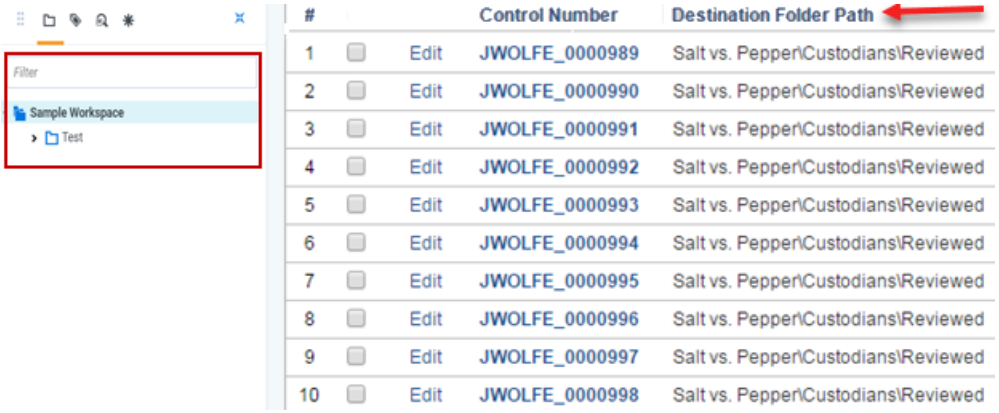
- Perform a test on a small sample set of documents before moving a large number of them.
- Execute only one move to folder path mass operation at a time.

Use these steps to move documents to a new folder:

1. Navigate to the **Documents** tab in your workspace.
2. Select the documents that you want to move to the destination folder path.
3. In the first drop-down menu in the mass operations bar, choose **Checked** or **All** based on your selections from the current document set.
4. Select **Move to folder path** in the second drop-down menu, and then click **Go**.
5. Complete the fields in the Folder path settings dialog. See Fields for move to folder path mass operation on the next page.
6. Click **OK** to run the mass operation. Relativity creates any destination folders that don't currently exist, and moves the documents to their specified destination folders. It also moves any documents with an empty folder path field to the location specified in the **Empty folder path placeholder** field. See Fields for move to folder path mass operation on the next page.

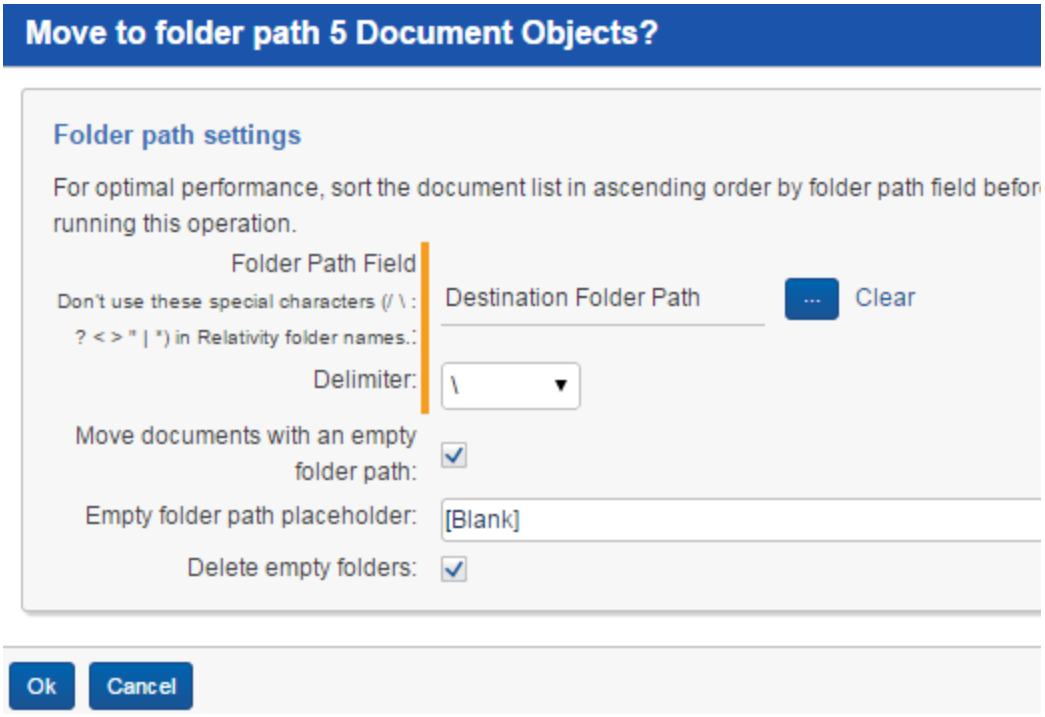
Note: To stop the mass operation, click **Cancel**. The mass operation finishes moving the current batch of documents before it stops. Relativity then displays a message indicating the percent of documents that were moved.

7. Optionally, refresh the page to see the newly created folders. See the following screen shot for an example of a new folder structure:



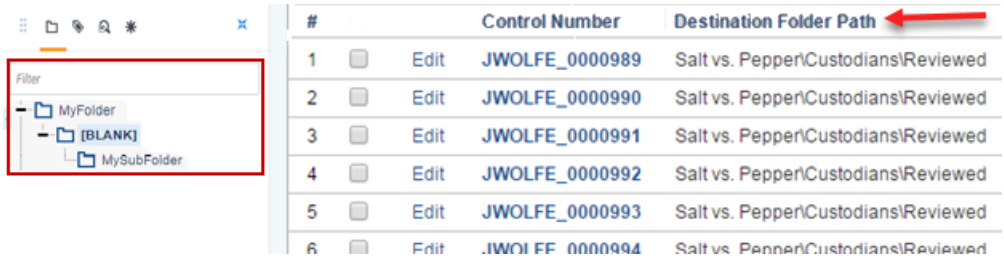
21.14.2.1 Fields for move to folder path mass operation

The Folder path settings dialog includes the following fields:



- **Folder Path Field** - click ... to select the field that you populated with the destination folder path. See Move to folder path on page 372.
- **Delimiter** - select forward slash (/) or back slash (\) as the delimiter for any nested folders.
- **Move documents with empty folder path** - select this checkbox if you want to move documents with empty folder path fields to the location specified in the **Empty folder path placeholder** option. If you don't select this checkbox, Relativity doesn't move documents with empty folder path fields.
- **Empty folder path placeholder** - enter the name of a folder where you want to move documents that don't have a destination specified in their folder path field. If the path contains subfolders, separate the folders with the same delimiter as you selected in the **Delimiter** field. This folder path may include Unicode characters.The following list describes how Relativity handles empty folders:

- If a folder path contains one or more empty folders, then Relativity replaces the blank location with the name in the **Empty folder path placeholder** field. For example, it updates the folder path **MyFolder-\\MySubfolder** to **MyFolder\[BLANK]\MySubfolder**, if the name in this field is [BLANK].



- If a folder path contains consecutive empty directories, Relativity consolidates them into a single directory, so that **MyFolder\\ \\\MySubfolder** becomes **MyFolder\[BLANK]\MySubfolder** when the name in this field is [BLANK].
- If a folder path contains two consecutive delimiters separated by a space, Relativity sets the name of the newly created folder to blank.

- **Delete empty folders** - select this checkbox to delete any folders within the entire workspace that are empty after you move the documents. Relativity doesn't delete empty folders when they have dependencies.

  Note: If an error occurs during the deletion of empty folders, Relativity stops this process and displays an error message. Please reach out to your Relativity administrator for further assistance.

21.15 Mass Save as List

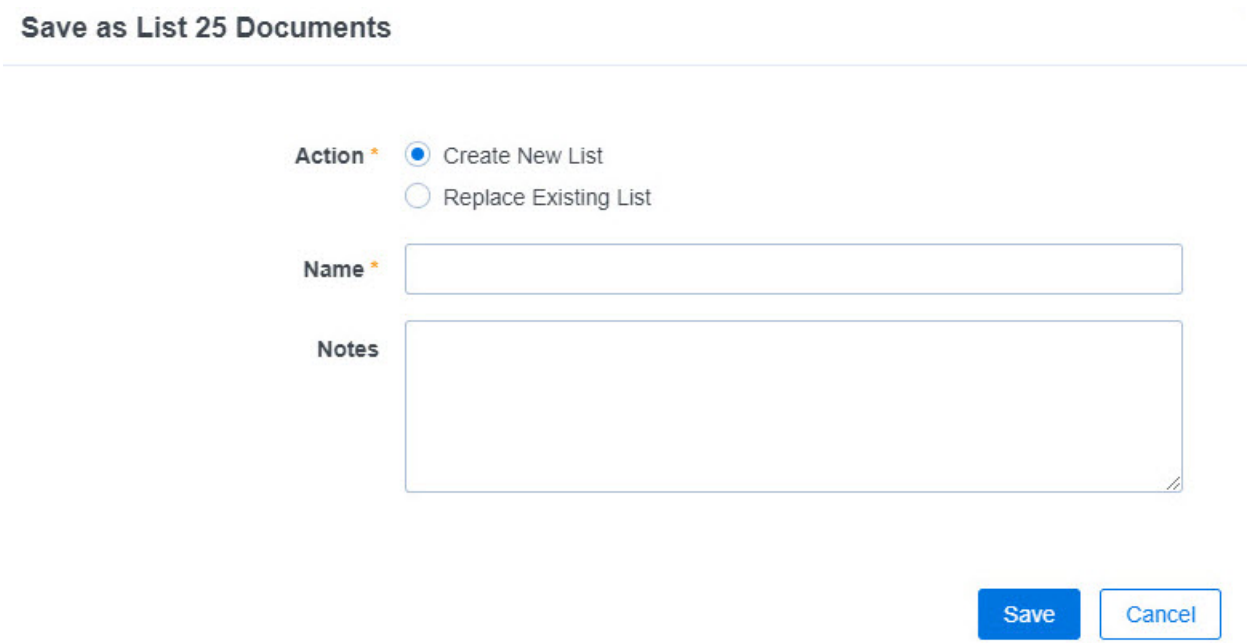
To save a group of documents as a list, follow this procedure. The same steps apply to other objects with **Lists** enabled. Always begin by clicking the tab of the object for which you want to save a new list. Mass Save as List is available from the mass operations bar.

Note: You cannot use mass operations on Data Grid-enabled fields.

To save a group of documents as a new list or replace an existing list:

1. Navigate to the **Documents** tab.
2. Display the documents you want to save to a list by selecting a folder, view, saved search, or performing a document search.
3. From the mass operations bar on the document list, choose whether to save **Checked items** or **All items** in the current returned set.

4. Select **Save as List**. The Save as List pop-up window opens.



5. Complete all required fields.
    - **Action** - creates a new list or replace the contents of an existing list. Select one of the following options:
        - **Create new list** - creates a new list with the list name specified in the **Name** field.
        - **Replace existing list** - replaces an existing list with the currently selected objects. Select an existing list from the Select Item - List window.
    - **Name** - stores the name of a new list. Type the new list name.
6. Click **Save**.

21.16 Mass PDF

With the Mass PDF operation you can create PDF files from natives, images, and produced documents, and save those PDFs on your computer. The mass PDF operation also allows you to store PDFs created from native files or original images in Relativity and review them in the PDF Viewer. The Mass PDF application is available from the mass operations bar on the document list.

21.16.1 Considerations

- We do **not** support downloading produced PDFs or produced native files. You can create and download PDFs from **natives**, **original images**, and **produced images**.
- The mass PDF operation support jobs up to 10,000 documents or 1,000,000 images.
- For large or recurring PDF jobs, consider using PDF Sets withAutomated Workflows. This is ideal for nightly PDF generation or sets larger than the Mass PDF limits (10,000 documents). See PDF Sets documentation for details.
- You cannot use mass operations on Data Grid-enabled fields.
- The PDF application is not available in workspaces created from the Relativity aiR ECA Template or in workspaces where the Repository Workspace application is installed.
- The PDF application needs to be manually installed on any workspace that was restored using ARM.

- You cannot use the PDF Portfolio functionality if you select more than 2,500 documents.
- Make Text Searchable applies only to the **Store** action. Downloading PDFs on the fly does not produce searchable PDFs. To download a searchable PDF, first store the PDF with Make Text Searchable enabled, and then download the stored PDF.
- OCR effectiveness depends on image quality. Poor results may occur with blurry images or low-contrast text. For OCR constraints and best practices, see OCR.

21.16.2 PDF permissions

The PDF application has the following associated permissions:

- System administrators can configure the **PDF Actions** permission for individual users or groups by restricting download, create, store, and numbering operations.
- The **PDF** permission within "Tab Visibility" settings manages access to the PDF and PDF Profile tabs.
- The **PDF Profile** permission within "Object Security" settings controls access and operations over the PDF Profile object.

In order to PDF production images, the user group needs View rights to “Production Data Source.”

Note: System administrators with the correct permissions setup for **Save as PDF** are unable to test this in **Preview Security** mode. This is done to prevent downloading documents that haven't been authorized.

Relativity Dynamic Object (RDO) Permission	Mass PDF Action
View	
Edit	Overwrite PDFs
Delete	Delete PDFs
Add	Store PDFs
Download PDF (custom permission)	Download PDF
Brand PDF (custom permission)	Brand PDF
Count PDF (custom permission)	Count PDF

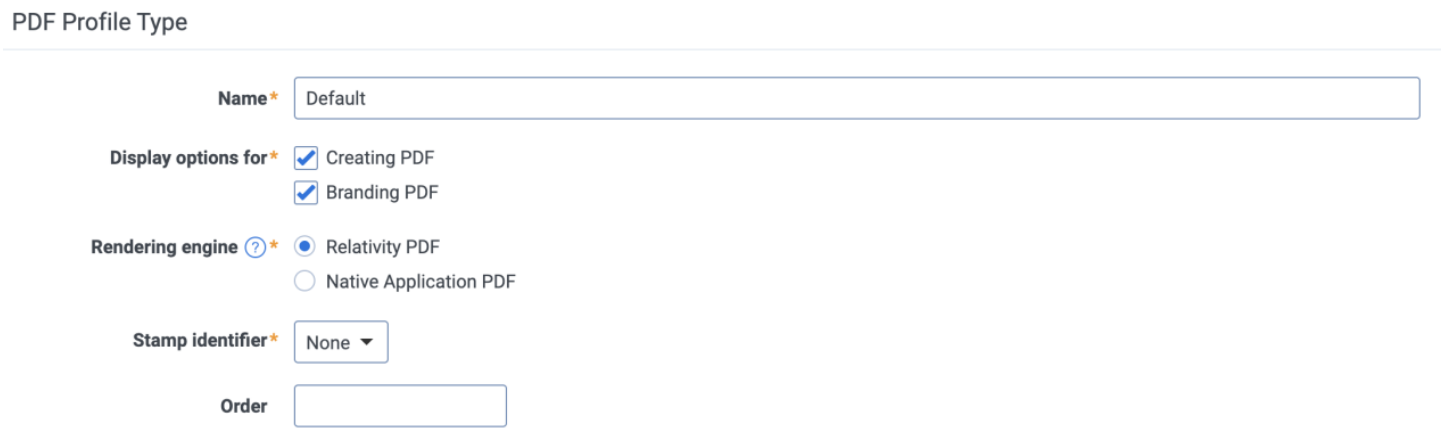
21.16.3 PDF profile

Use the PDF profile to customize how to create your PDFs when using the following actions from the PDF Mass Operation: Store, Download and Brand.

To create a new PDF profile:

1. Navigate to the **PDF Profile** tab.
2. Click **New PDF Profile** and enter a name.

Note: The settings defined in the PDF profile do not apply to the following actions from the PDF Mass Operations: Count and Delete.



21.16.3.1 PDF Profile Types

Note: Choose the PDF Profile type that matches your objective. Relativity doesn't require the PDF app. If you uninstall the app, Relativity deletes all PDF profiles and any launched PDF sets. Reinstalling the app doesn't restore previously created profiles or sets.

- **Creating PDF below**—Select “Creating PDF” to display options associated with the “Store” and “Download” action from the PDF Mass Operation. When selecting this option, the Select Identifier option will enable you to stamp your PDFs with the content of a *single* field in a *single* location: bottom, top, left, right, center.
- **Branding PDF on page 385**—Select “Branding PDF” to display options associated with the “Brand” action from the PDF Mass Operation. Select this option to add different branding fields on *any* of the available locations: bottom, top, left, right, center. To apply Branding PDF to a PDF, you need to first create your stored PDFs and then run the Mass PDF operation to add the new branding.
- Stored PDF—Select Stored PDF to apply PDF profile settings when using the Download action in the Mass PDF operation. This option enables you to download PDFs that have already been stored in Relativity, while preserving visual markup elements such as transparent redactions and highlights, if those were configured in the selected PDF profile. This ensures that the downloaded version reflects the markup behavior defined in the profile, such as including highlights and redactions tied to a markup set. The stored PDF itself remains unchanged.

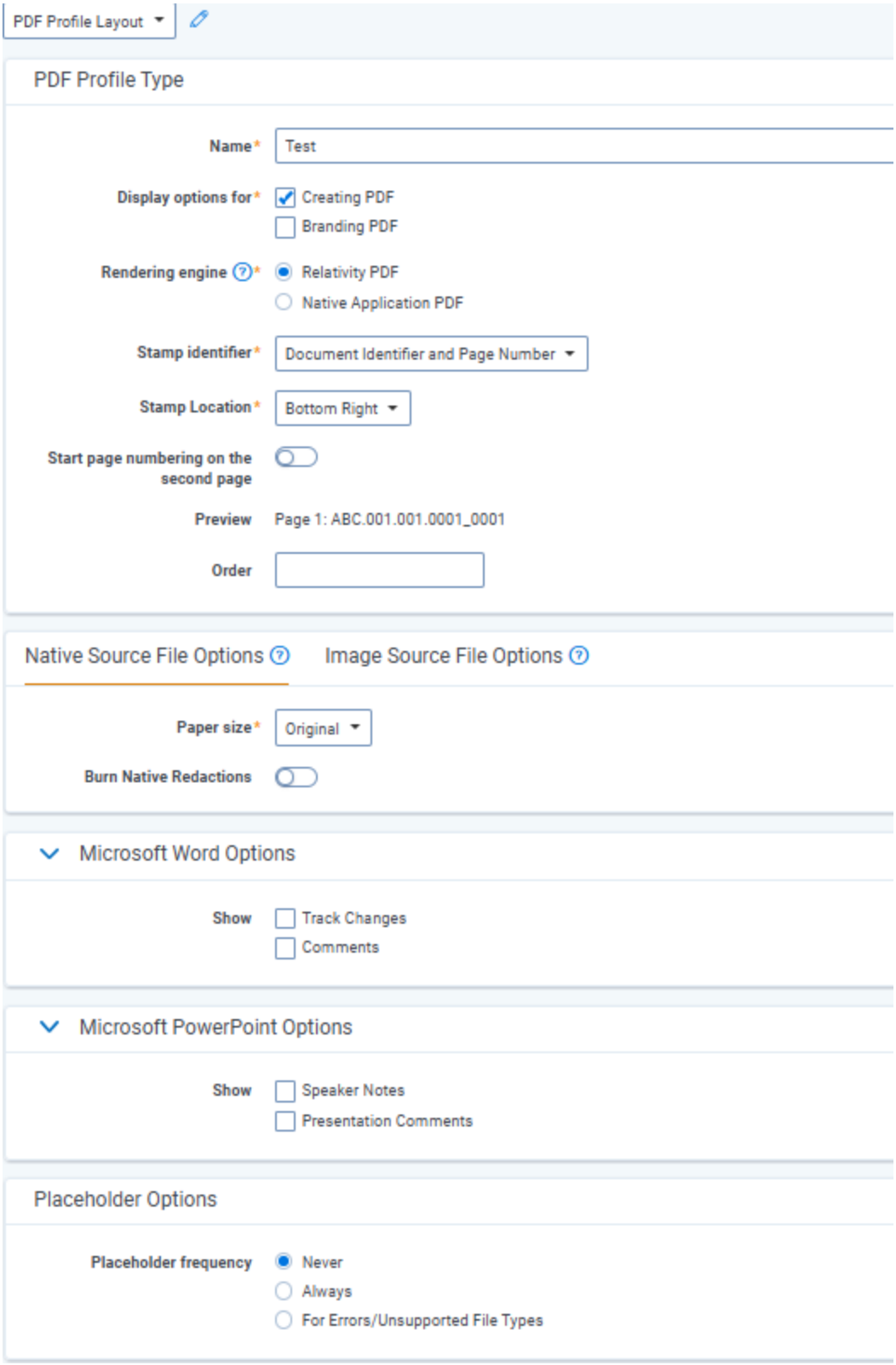
21.16.4 Creating PDF

When selecting “Creating PDF,” the system will give you the option to select the rendering engine of your preference to create your PDFs. A rendering engine is the component that converts the original documents into PDF format. Relativity provides two rendering engine options:

- **Relativity PDF**—Select this option to create a PDF profile that will generate PDFs using Relativity’s proprietary PDF engine.
- **Native Application PDF**—Select this option to create a PDF profile that will generate PDFs using the Native applications. This is equivalent to how imaging works in Relativity. Basic imaging is equal to relativity PDF and native imaging is equal to native application PDF.

21.16.4.1 Rendering options for Relativity PDF engine

These options apply to every file type: natives, original images, and produced images.



- **Stamp Identifier**—select this option to add a single identifier on each page of the resulting PDF in a specific page location. You can choose to stamp your PDFs which one of the following options:
  - **Document Identifier**—choose this option to stamp each page of the PDF with the document identifier. For example: REL_00001.

- **Document Identifier and Page Number**—this option will stamp [Document Identifier]_[page number]. You can choose among three options:
  - **Add the page number to every page of the PDF**
    - Page 1: REL_00001_0001
    - Page 2: REL_00001_0002
  - **Start the page numbering on the second page**
    - Page 1: REL_00001
    - Page 2: REL_00001_0001
  - **Start the page numbering on the second page with 2**
    - Page 1: REL_00001
    - Page 2: REL_00001_0002
- **Field**—choose this option to stamp the PDFs with a field value, then select the desired Field Name.
- **Free Text**—choose this option to stamp the PDFs with the text of your choice as entered in the Text field.

  Note: There is a 100 character limit.

- **Stamp Location**—select the area of the page where you want to add your stamping from the drop-down list.
- **Order**—enter a value in the order field to determine the position of the newly created PDF profile in the drop-down selection from the Mass PDF function.
  - If there is a numeric value in the order field, the PDF profiles will be ordered in ascending order of those values.
  - If there is no value in the order field, the PDF profiles will be ordered by name in ascending order.

File naming behavior for downloaded PDFs:

When you download PDFs using the Mass PDF operation, Relativity uses the document identifier of the value of a custom field (as configured in the PDF profile) to name the exported file.
If a file name contains any unsupported characters such as **/ \ : * ? " < >**, Relativity automatically appends the document's **Artifact ID** (a unique numeric identifier) to the end of the file name. This ensures the exported file has a valid and unique name that the operating system can process.

Example:

Source field value	Exported file name
2025-02-16 14:30 0066501.eml_FTI_000076647	0205-02-19 1430 0066501.eml_FTI_000076647_**51930132**

In this example, the colon(:) in 14:30 is an unsupported character, so Relativity removes it and appends the **Artifact ID 51930130** to the file name.

Native Source Files Options

The options on this tab are available when the “File Type” selected in the Mass PDF operation is “Natives.”

- **Paper Size**—select the size for both the PDFs that you create to download and the PDFs you store in Relativity. The paper size option only applies when the source file type of the PDF job is natives. The paper sizes available are: Letter, Legal, A5, A4, A3, and original. The original option will maintain both the original paper size and orientation of each page on the native file. The Letter, Legal, A5, A4, and A3 options will create a PDF with portrait orientation in the selected paper size.

- **Burn Native Redactions**—indicates that you want to include redacted natives as part of the PDF job. Toggling this field on makes the Native Options Markup Set field required below.
- **Native Options Markup Set**—this field is only visible if you selected to Burn Native Redactions above. It indicates which markup set is used to apply native redactions to the documents you are about to convert to PDF. Select the desired markup set from the drop-down.
- **Make Text Searchable** — select this option to create searchable stored PDFs from non-searchable native files. When enabled, Relativity automatically uses OCR to extract text from non-searchable elements during PDF creation. This includes:
  - Text contained in image-based native files
  - Text embedded within images inside native documents (for example, a screenshot included in a Word document that contains text). The resulting stored PDF is searchable, allowing users to find text directly within the PDF using standard PDF search tools.
    This setting is shared with the Image Source Files Options tab. Enabling Make Text Searchable on the Native tab automatically enables it on the Image tab, and the reverse is also true. Both options control the same underlying setting.

    Note: Make Text Searchable applies only to the Store action. Direct downloads of PDFs from native files do not produce searchable PDFs, regardless of PDF Profile configuration. See Store vs. download behavior for details.
- **OCR Profile** — select the OCR profile to use when extracting text from non-searchable elements. If no OCR profiles have been created in the workspace, Relativity uses a default OCR profile. For information on OCR profile settings, including language, accuracy, and preprocessing options, see OCR.

Image Source Files Options

The options on this tab are available when the "File Type" selected in the Mass PDF operation is "Original Images."

- **Make Text Searchable**—select this option to translate images of text, such as scanned and redacted documents, into actual searchable text characters in the resulting PDF.

  Note: This function applies only to Original Image and Produced Image file types.
- **OCR Profile**—select the OCR profile to be used to translate images of text into actual searchable text characters.

  Note: If there are not OCR profiles created in the workspace, Relativity will use a default OCR profile.
- **Include highlights**—select this option to include highlights in the resulting PDFs. This option applies only when converting original images to PDF, and is only for highlights which are associated with a markup set. You will be required to specify the markup set to use.
- **Include redactions**—select this option to include redactions in the resulting PDFs. This option applies only when converting original images to PDF, and is only for redactions which are associated with a markup set. You will be required to specify the markup set profile to use.
- **Include Slip Sheet**—select this option to include a slip sheet on the first page of the generated PDF. Available options are: Blank Page, identifier only, and coding layouts. The slip sheet character limit is 98.

Microsoft Word Options

When converting native file types that are MS Word Documents into PDFs using Relativity PDF Engine, the following options can be configured in the PDF Profile:

- **Show Track Changes**—if the native MS Word document has track changes, this option will include those track changes in the resulting PDF.
- **Show Comments**—if the native MS Word document has comments, this option will include those comments in the resulting PDF.

Microsoft PowerPoint Options

When converting native file types that are MS PowerPoint Documents into PDFs using the Relativity PDF Engine, the following options can be configure in the PDF Profile:

- **Show Speaker Notes**—if the native MS PowerPoint document has track speaker notes, this option will include those speaker notes in the resulting PDF.
- **Show Presentation Comments**—if the native MS PowerPoint document has Presentation Comments, this option will include those comments in the resulting PDF.

Placeholder Options

Select **Never**, **Always**, or **For Errors/Unsupported File Types** when assigning a PDF placeholder for a document during PDF Rendering.

21.16.4.2 Rendering options for Native Application PDF

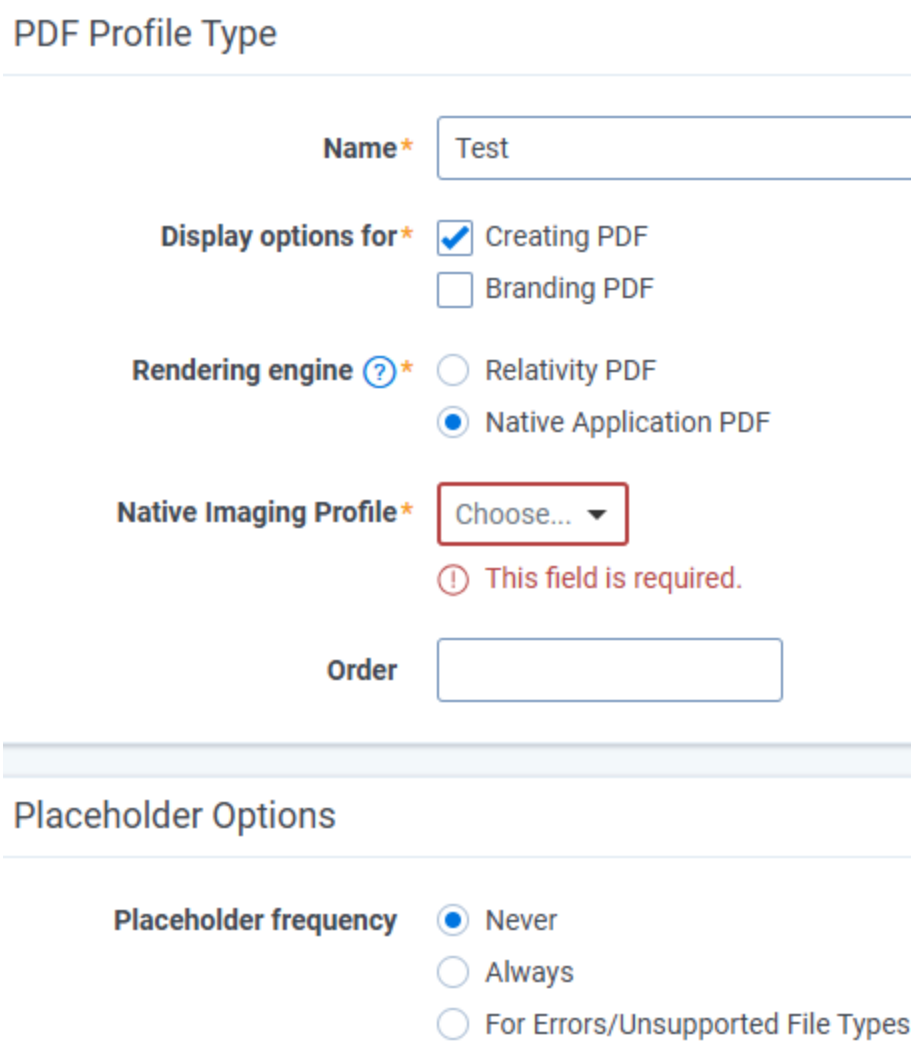
The “Native Application PDF” engine uses the following options available in a Native Imaging Profile:

- Spreadsheet Options with their corresponding Advance Options
- Email Options
- Word Processing Options
- Presentation Options

To use the Native Application Engine when creating Stored PDFs, first create an Imaging Profile with the desired configuration.

Note: The PDF profile supports the following options from the selected Imaging Profile: **Email**, **Word**, **PowerPoint**, and **Excel** files. However, any options in the Imaging Profile related to HTML files are **not** supported by the PDF profile.

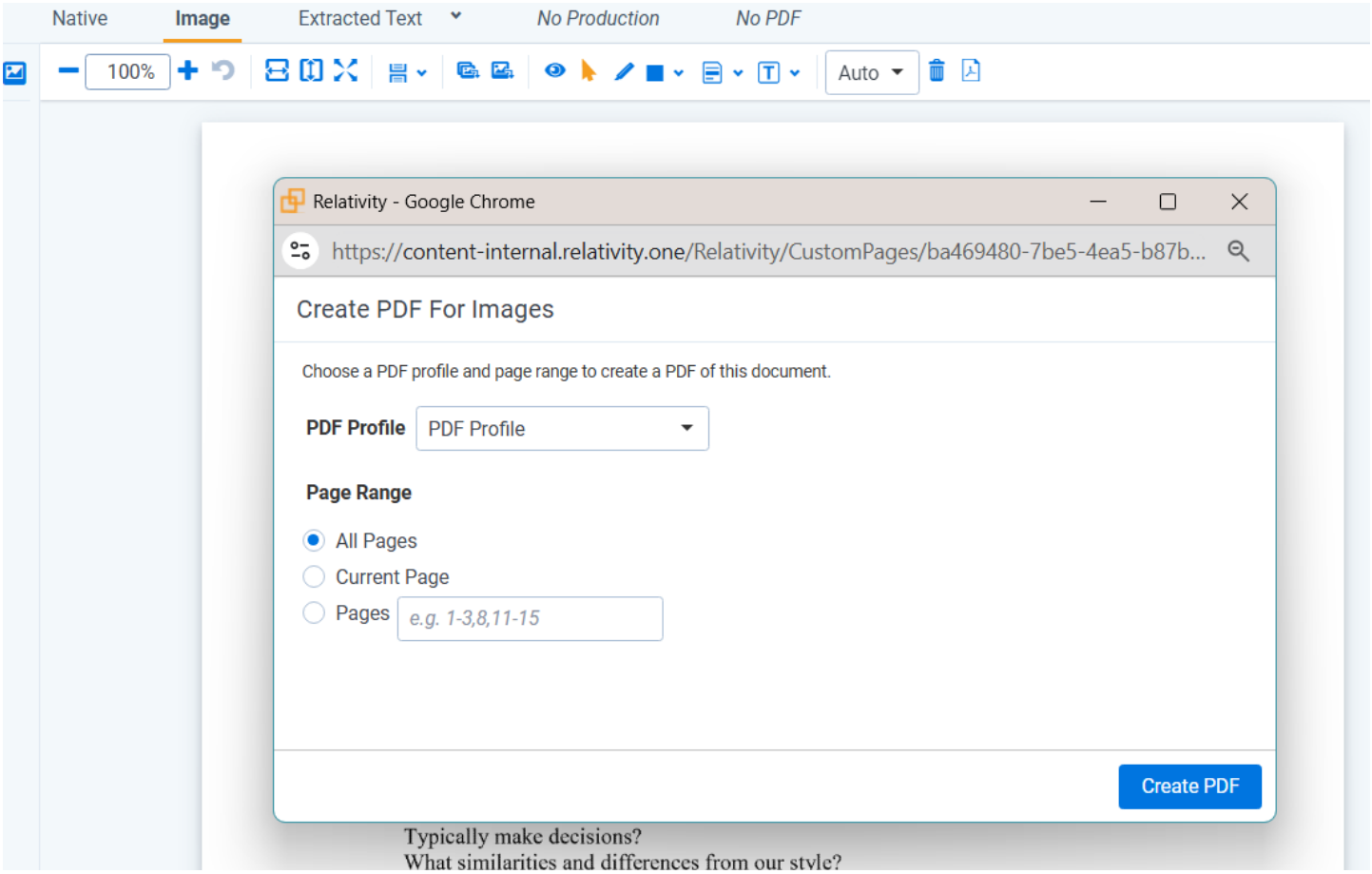
Then, you can select it from the **Native Imaging Profile** drop-down menu.



Placeholder Options

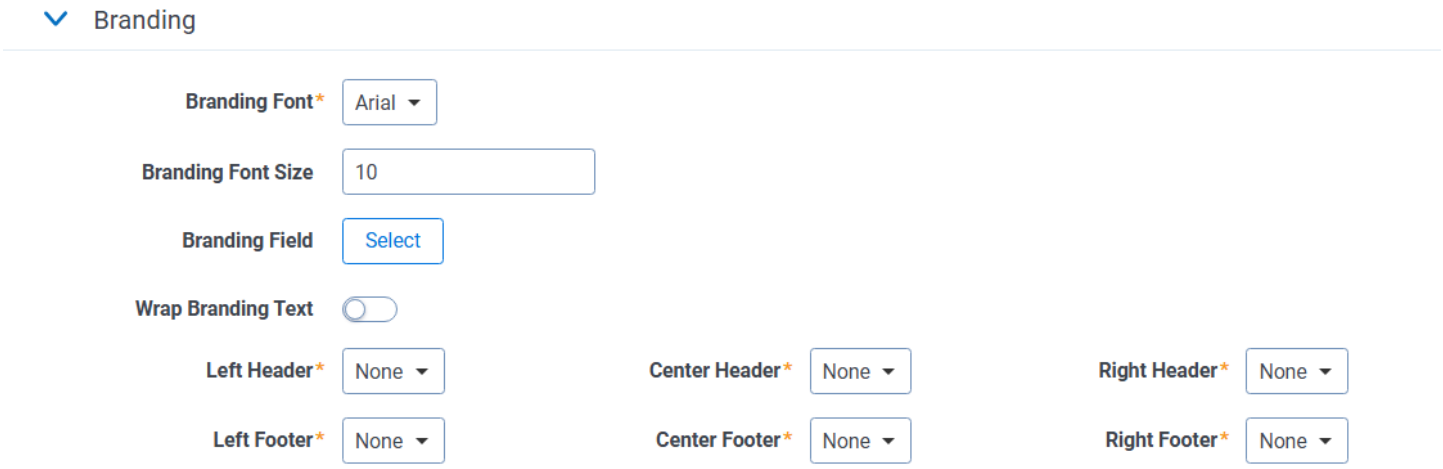
Select **Never**, **Always**, or **For Errors/Unsupported File Types** when assigning a PDF placeholder for a document during PDF Rendering.

Once a PDF profile is created, it is available on the Mass PDF action and from the Viewer.



21.16.5 Branding PDF

When adding branding to produced PDFs, the following options can be configured in the PDF Profile.



Branding options

- **Branding Font**—select a font for branding.
- **Branding Font Size**—select a font size.
- **Branding Field**—select a field for branding. You can only select and use one branding field.

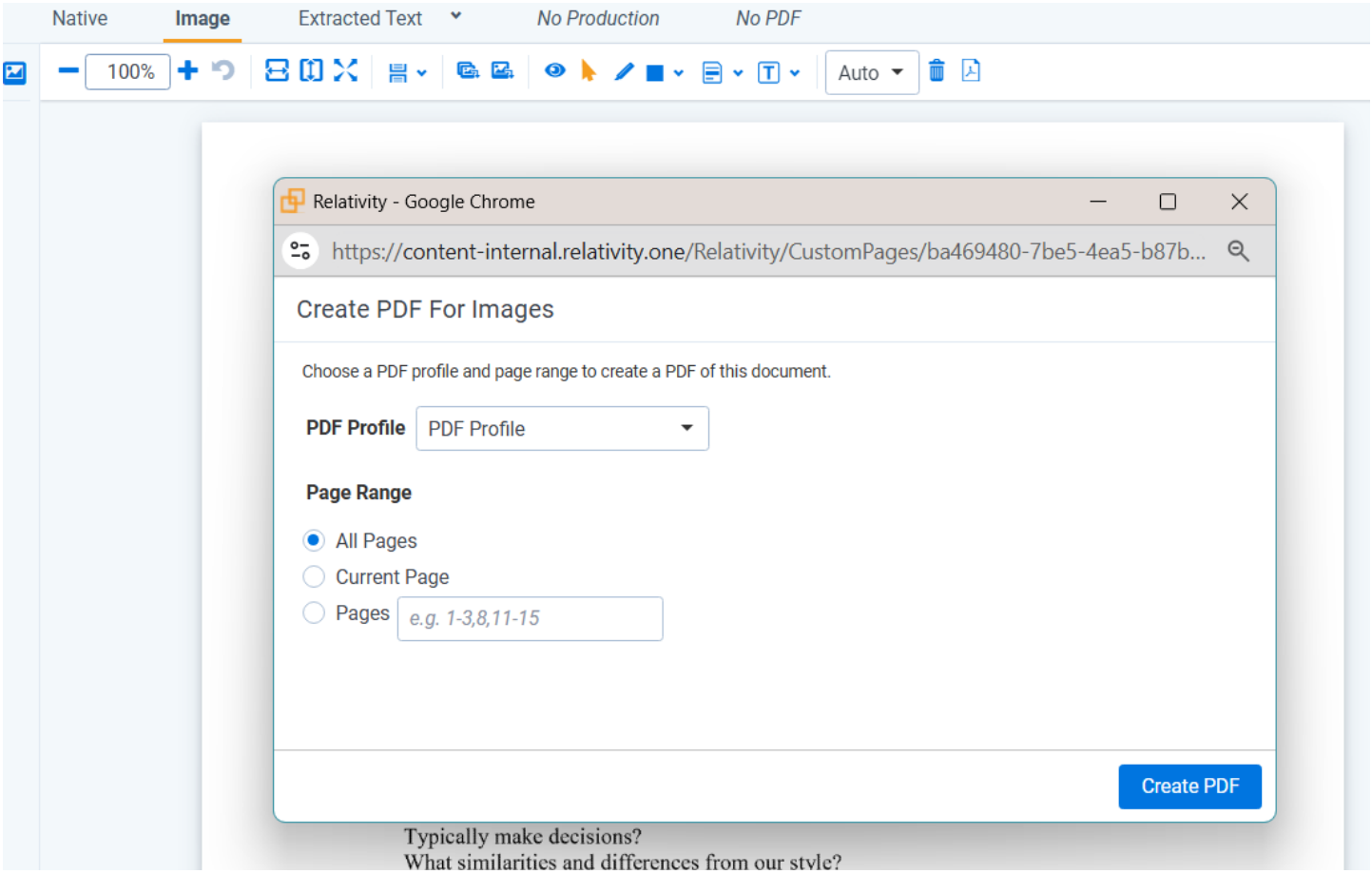
- **Wrap Branding Text**—if the text being stamped is too long, wrap the text to fit multiple lines. Flip this option to true to wrap text within the allotted field.
- **Left Header**—select a left header. Choose Document Identifier, Document Identifier + Page Number, Field, Free Text, or Level Numbering.
- **Left Footer**—select a left footer. Choose Document Identifier, Document Identifier + Page Number, Field, Free Text, or Level Numbering.
- **Center Header**—select a center header. Choose Document Identifier, Document Identifier + Page Number, Field, Free Text, or Level Numbering.
- **Center Footer**—select a center footer. Choose Document Identifier, Document Identifier + Page Number, Field, Free Text, or Level Numbering.
- **Right Header**—select a right header. Choose Document Identifier, Document Identifier + Page Number, Field, Free Text, or Level Numbering.
- **Right Footer**—select a right footer. Choose Document Identifier, Document Identifier + Page Number, Field, Free Text, or Level Numbering.

Level Numbering options

When selecting "Level Numbering" as a Branding option, the following Level Numbering options became available in the PDF Profile. These options allow you to add new sequential numbers to rendered PDFs:

- **Numbering type**—select Page Level or Document Level numbering.
- **Prefix**—enter a prefix to be used for numbering.
- **Minimum Box Number**—enter a minimum box number. This is set to 1 by default and indicates the Start Number.
- **Minimum Folder Number**—enter a minimum folder number. This is set to 1 by default.
- **Minimum Page Number**—enter a minimum page number. This is set to 1 by default.
- **Delimiter**—select period, hyphen, or underscore.
- **Relational Field Behavior**—select none or keep in same folder
- **Relational Field Behavior**—select a relational field such as Family Group or
- **Maximum Box Number**—enter a maximum box number. This is set to 9999 by default.
- **Maximum Folder Number**—enter a maximum folder number. This is set to 9999 by default.
- **Maximum Page Number**—enter a maximum page number. This is set to 9999 by default.

Once a PDF profile is created, it is available on the Mass PDF action and from the Viewer.



The PDF application comes with a default profile that is not listed on the PDF profile tab and that cannot be modified. This is a basic profile that creates non-searchable PDFs without highlights, redactions, slip sheet or stamp identifier.

The default PDF profile is only available if there are no other PDF profiles created in the workspace. Once a system administrator creates a new PDF profile, the default Profile is no longer available for the users.

21.16.6 Creating PDFs via mass operation

Note: If you are creating PDFs to open in the Viewer, it is important to note that the Viewer displays PDF text by mapping the character codes to Unicode in most cases. To check whether PDF text has been properly encoded and will display correctly in the Viewer, copy the text in the original PDF file and paste it into another application like Microsoft Word or Notepad. If the pasted text does not display correctly, the PDF is not properly encoded. If the pasted text displays correctly in another application but not in the Viewer, contact Support for assistance.

To convert multiple documents into PDFs:

1. From the mass operations bar on the document list, select either **Checked items** or **All items** in the current returned set.
2. Select **PDF** in the mass operations drop-down menu. The PDF options window displays.

3. Select the appropriate settings:

Notes:

- The settings available depend on the file type selected. Natives, original images, or produced images. For example, production options are available if you select Produced Images. Likewise, if you are going to save all your documents in a single PDF, then there are no options on how to name the individual PDF.
- When saving your PDF as a zip or PDF portfolio you can choose to name your individual PDFs using just the control number or the control number plus a field.
- You also have the option to decide whether to include a numbering prefix on the file name. In the past that prefix was always added.

Action

- **Download**—download your PDFs. When selecting multiple documents, a toggle option is available to "Combine PDFs by Document Family." Once selected and downloaded, users will receive a single combined PDF for documents that share the same ID for the chosen relational field.

  Note: This option is available only when you select **Individual PDFs in a Zip** under the PDF Option setting.

  Note: The **Make Text Searchable** setting in the PDF Profile does **not** apply when using the Download action. PDFs created through the Download action are generated on the fly and do not include OCR-based text extraction. To download a fully searchable PDF, you must run a Mass PDF or PDF Set using the Store action with Make Text Searchable **enabled**. After the stored PDF is created, download it. The downloaded stored PDF retains the searchable text.

- **Store**—creates a PDF from the native or imaged version of the documents. Those PDFs will be stored in Relativity and can be reviewed using Relativity's PDF Viewer.
- **Brand**—sequentially numbers documents with a structured Document ID and stamps the Document ID on each page of a PDF. Only profiles that have branding options set can be leveraged for this action.

  Note: Selecting the **Brand** option when using a PDF profile that has Level Numbering configured could conflict with the control number.

- **Count**—calculates and updates the PDF Page Count field when document page counts need to be updated in the database. This only works for counting rendered PDF documents.
- **Delete**—deletes the stored PDFs associated with the selected natives.

  Note: If you import PDF Images and the PDF Page Count is not set, you cannot brand the documents. You must run the Count action beforehand to make sure the field is populated.

File Types

- **Natives**—saves the native of the documents.
- **Original Images**—saves the imaged versions of the documents.
- **Produced Images**—saves the produced versions of the documents.
- **Stored PDF**—saves the PDFs that are currently stored in Relativity and can be reviewed using Relativity's PDF Viewer. Single file Stored PDFs will be downloaded as a Zip file.

Note: Produced images are supported only when you download to PDF. Produced PDFs and produced native files are not supported.

PDF Options

- **Individual PDFs In A Zip**—saves resulting PDFs as a zipped file.
- **Single PDF**—creates one PDF with all documents.
- **PDF Portfolio**—creates one PDF Portfolio with all documents.

Note: You cannot use the PDF Portfolio functionality if you select more than 2,500 documents.

Note: When you Mass Save as PDF a group of documents, the documents retain their sort order based on the order in which they appear within your document list.

When saving a PDF as a .zip or PDF portfolio you can:

- choose to name your individual PDFs using the control number, the control number plus a field, or just a field.
- decide whether to include a numbering prefix on the file name. In the past, that prefix was always added.

Naming Options

This option defines the name of the individual PDFs created when documents are saved as **Individual PDFs In A Zip** or **PDF Portfolio**. The zip file or the portfolio file itself that contains the PDF files is always named **result.[extension]**.

- **Control Number**—choose this option to name the PDFs after the control number of the original document.
- **Control Number And Field**—this option appends value of a field to the original control number name. When using this option, the resulting name of the document is [control number]_[field value].
- **Field**—choose this option to name the PDFs after a field value.
- **Append File Type**—appends native, image, or production at the end of the file name based on the type of documents used to create the PDF.
- **Prefix Sequential Number**—this option appends a numeric prefix based on the sort order in which they appear within your document list. For example, 01_FirstDocument.pdf.

Note: If the length of file name is longer than 251 characters, the system will use the first 251 characters.

Production Options

- **Include original images for documents that haven't been produced**—if a document has not been produced, you can check this option to create PDFs from the images associated with that document instead.
- **Modify Production Order**—select which produced version of the document to include in the PDF set.
  - The save job first looks at the production set at the top of the list. If the document is included in this production that version is saved. If not, the save job checks if the document is in the next production. Only one production per document is saved.

- The list includes only the productions related to the documents selected, those productions are sorted by recent to oldest. For example, if there are 8000 productions in your workspace, but the selected documents are produced across only 100 productions, the list will show only those 100 productions.

PDF Profile Options

The PDF Profile section displays the selected profile and all the corresponding values set on that profile. For details, see PDF profile on page 378.

4. Once you have applied all the desired settings, click **Download**, **Store**, or **Delete**, depending on the action you specified at the top of the layout. The system submits your PDF job. Once completed, the browser automatically downloads the resulting file. You also receive a confirmation email with a link to your PDFs to download.

21.16.6.1 RSMF and short message files

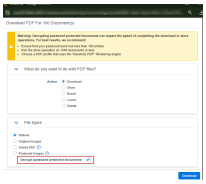
RSMF (Relativity Short Message Format) files render to PDF through imaging. To create a PDF of a conversation, image the RSMF file first. Then run the Mass PDF job on the original images. The imaged version mirrors the Short Message Viewer. Relativity aiR adds a Summary Report to the first page of the imaged RSMF. For more on imaging these files, see Short Message Viewer.

21.16.6.2 Using the Password Bank to Create PDFs from Password-Protected Natives

Note: Ensure you have a set of password banks uploaded to your workspace.

Documents that have been password encrypted and/or have a .pfx certificate can successfully undergo download and/or store PDF operations as long as the passwords and certificates in the password bank are correct. Only native file types that are downloaded or stored are supported.

Select the checkbox option to Decrypt password protected documents. When you select this checkbox, a warning will appear, providing best practices and cautioning about potential performance issues if those practices are not followed.



Note: Using a PDF profile with the Native Application Engine may result in slow performance. The operation's speed depends on the size of the password bank (more than 100 entries) and the position of correct passwords within the bank (if the correct password is the last one). This can lead to slow performance, potentially taking several hours and possibly timing out.

21.16.6.3 Best practices for large jobs

For large jobs, output size matters more than the number of documents or images. A job within the enforced maximums can still fail if the output is too large. This can happen in two ways. A single document with many pages or images can be too large to convert or package up.

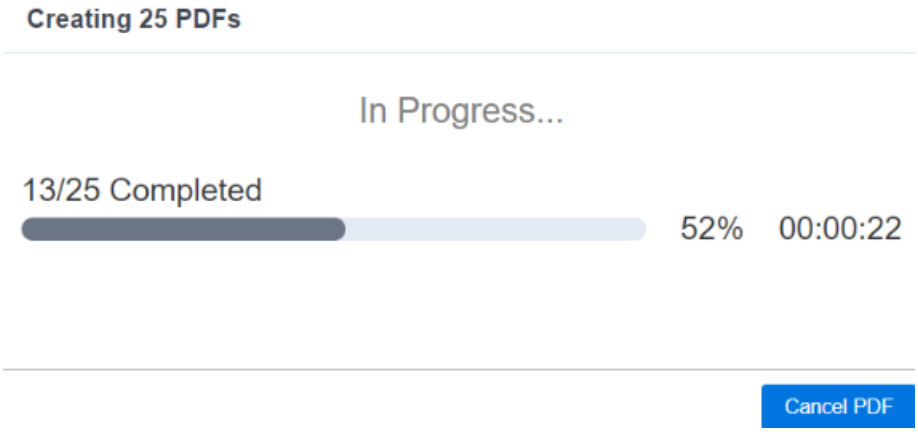
For large or complex jobs, we recommend the following:

- **Start with a small job.** Use it to gauge output size for your data, then increase the job size gradually.
- **Run high-volume documents separately.** Place documents with very high page or image counts in their own smaller jobs.
- **Expect lower limits with searchable PDFs.** The Make Text Searchable option increases the memory each document requires.

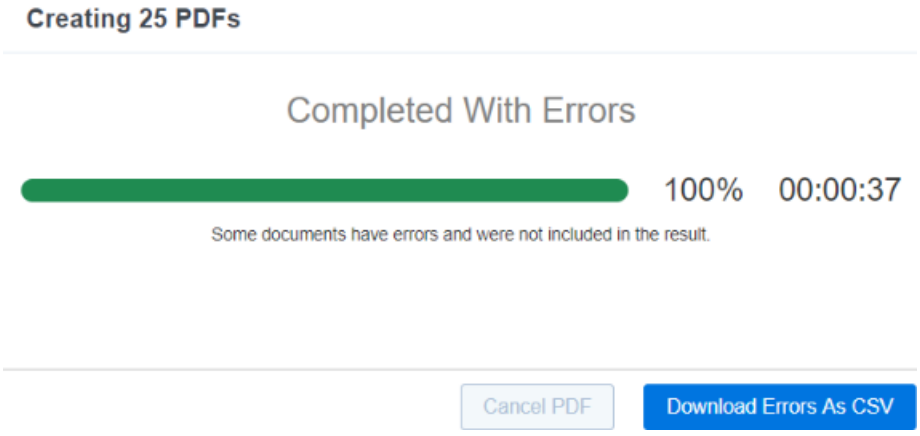
21.16.6.4 Mass PDF progress bar

The PDF application has a progress bar where you can see the status of your job, the number of documents completed, percentage completed, and the total duration of the job from start to completion. The progress bar will show the following status:

- **Creating**—your PDF job is being created and added to the queue.
- **Picked up**—your PDF has been picked up from the queue.
- **In Progress**—your PDFs are being created.
- **Packaging**—all PDF were created and now the ZIP file, or the Portfolio file is being created.
- **Completed**—job is complete.

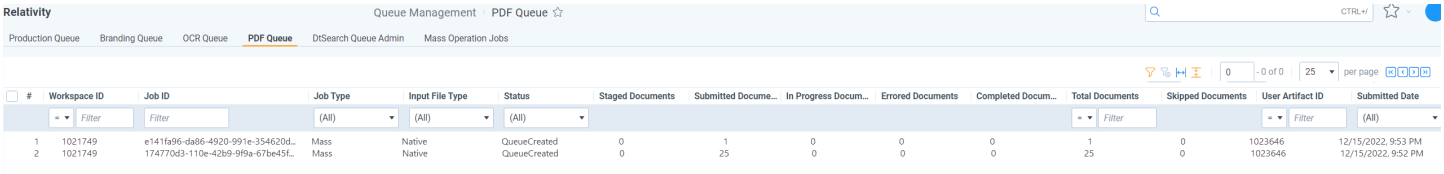


If the job completes with errors, you have the option to download a .csv file with the list of errors. For example, if you try to create a PDF for a native file that is password protected, or if you try to create a PDF from images and a document doesn't have images, those PDFs will not be created and those documents are included in the .csv error file.



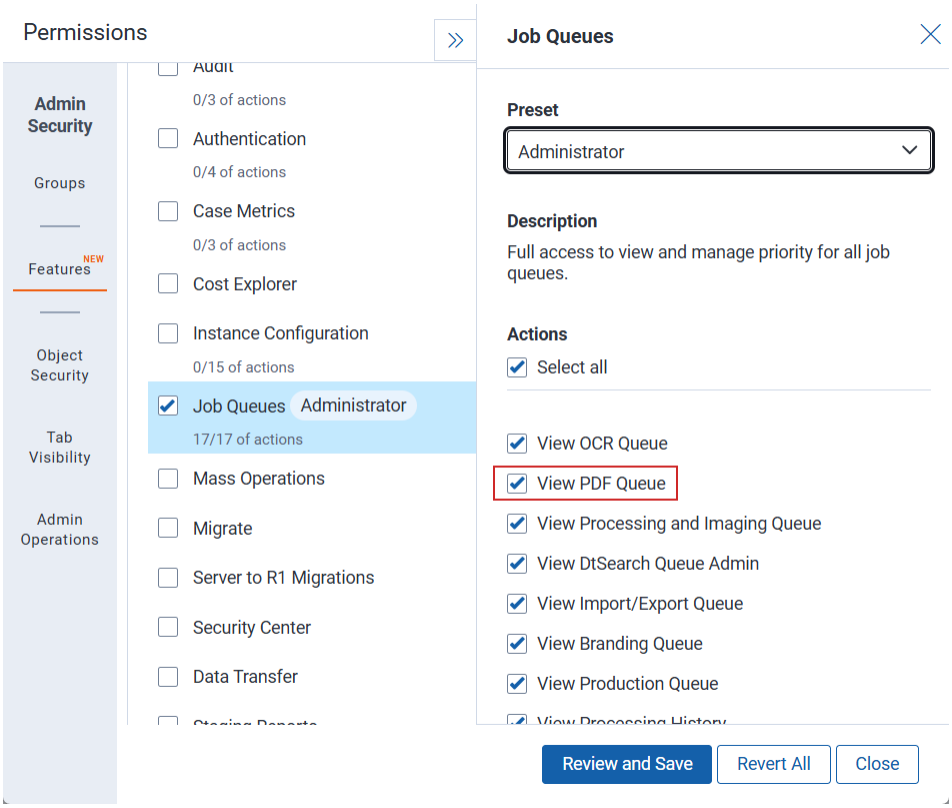
21.17 PDF Queue

PDF Queue is a sub-tab of Queue Management. From this screen, you can monitor all PDF jobs across an instance of Relativity that are not yet complete.



21.17.1 Permissions

Manage permissions for this feature on the Features tab. Grant the full feature for a group, or customize access with individual actions. For an overview of features and actions, see Feature permissions.



21.17.2 PDF Queue columns

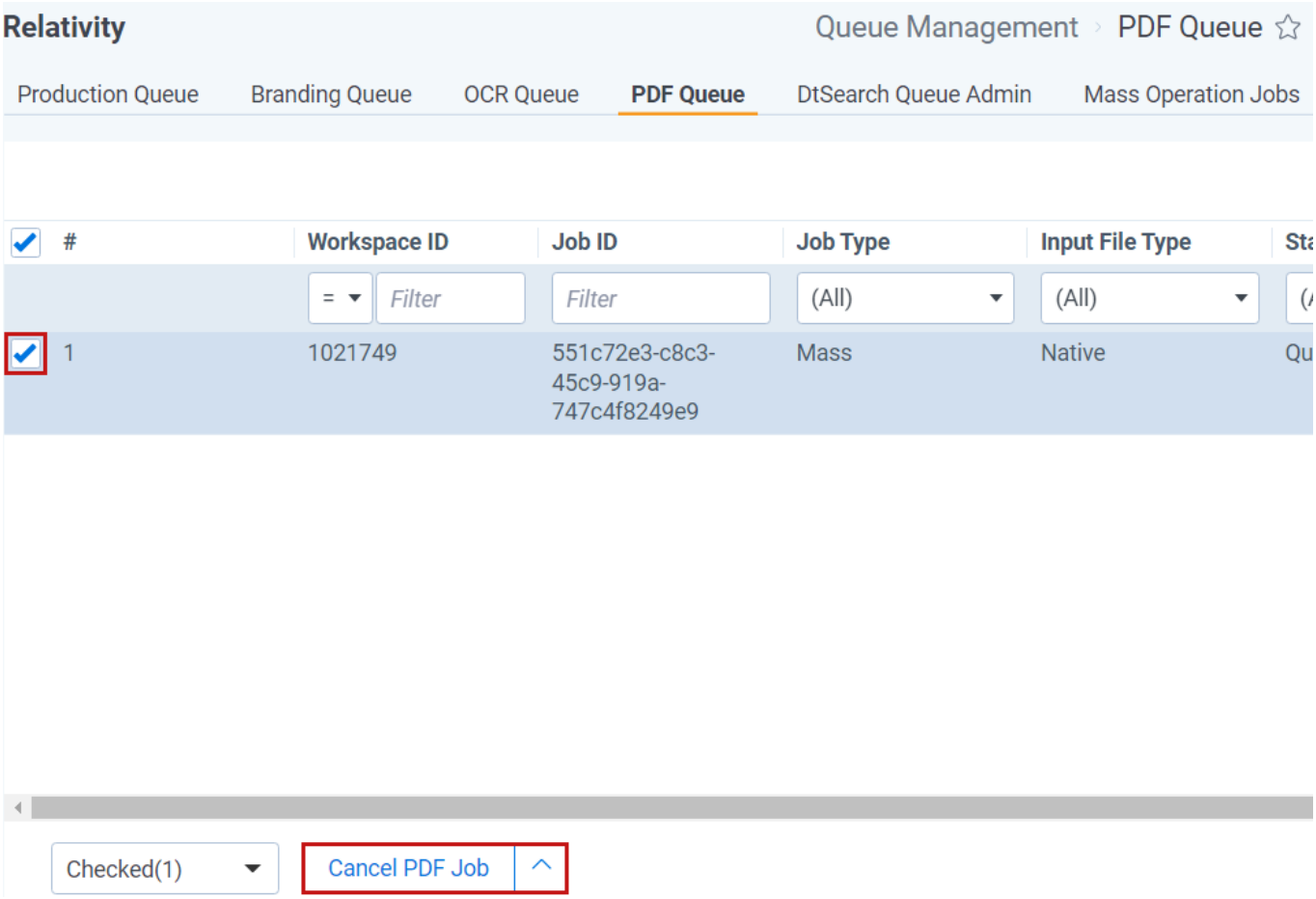
- **Workspace ID**—the ID of the workspace that contains the products set used for the job.
- **Job ID**—the unique ID assigned the job.
- **Job Type**—the type of job submitted. For example, Single, Mass, or Delete.
- **Input File Type**—the type of file submitted. For example, Native, Image, or Production.
- **Status**—the current stage of the production job.
    - **Created** - the system has created the PDF job but it has not yet been picked up by an agent.
    - **PickedUpByAgent** - an agent has picked up the PDF job.
    - **QueueCreated** - the backing queue in the system has captured all the documents within the PDF job that need to be worked on.
    - **InProgress** - an agent is currently working on the PDF job, specifically by converting documents to PDFs.

    - **JobError** - the job has stopped due to an error.
    - **FinalizingInitiated** - an agent has converted all the documents within the PDF job; the final step of zipping all the PDFs has been queued up.
    - **FinalizingInProgress** - finalization of the PDF job is in progress, in that an agent is now zipping all the PDFs.
    - **Cancelled** - a user has cancelled the PDF job.
- **Staged Documents**—the number of staged documents.
- **Submitted Documents**—the number of documents that were originally submitted.
- **In Progress Documents**—the number of documents in progress.
- **Errored Documents**—the number of documents that errored during the process.
- **Completed Documents**—the number of completed documents during the process.
- **Total Documents**—the total number of documents processed.
- **Skipped Documents**—the number of documents skipped.
- **User Artifact ID**—the unique ID of the user starting the job.
- **Submitted Date**—the date and time when a PDF job was run.

21.17.3 Cancel a PDF job

To cancel a PDF job:

1. Select the job(s).
2. Click the **Cancel PDF Job** button.



3. Click **Yes, Cancel PDF Job** on the confirmation modal.



21.18 Mass convert

Use the Mass Convert operation to pre-convert a large set of documents into HTML5 format before review. This process reduces document load time in the viewer and improves performance during document review.

You can access Mass Convert from the mass operations bar on the document list. Choose whether to convert checked items or all items in the current result set. Then, select Convert from the drop-down menu and complete the fields on the Convert Documents layout.

21.18.1 Conversion options

- **Natives**: Convert native files.
- **Images**: Convert embedded images.
- **Productions**: If selected documents belong to a production set, the set appears here.
- **Re-convert if previously converted**: Select this to convert documents again, even if they've already been converted. The system stores newly converted documents in the cache.

After you click **Run**, you can't cancel the job. Converting a large number of documents may reduce available disk space on the file server.

Note: Relativity aiR uses browser-based technology to render PDF and audio/video files. These file types do not go through the Mass Convert process. You don't need to run Mass Convert operations on them.

21.18.2 Limitations

- Mass Convert is only available for the Document object.
- It's not available in repository workspaces.
- You can't use Mass Convert on Data Grid-enabled fields.

21.19 Retry Production Job

To retry multiple production jobs from the Production Queue tab, use the Retry Production Job mass operation.

21.19.1 Security configuration

You must configure certain instance level permissions to use Retry Production Job.

To configure the security permissions:

1. Navigate to the **Instance Details** tab.
2. Click **Manage Permissions**.
3. Click **Edit Permissions** for a group on the Group Management tab.
4. Enable the following security permissions:

Object Security	Tab Visibility	Admin Operations
• N/A	• Queue Management (parent)	• Change Queue Priority

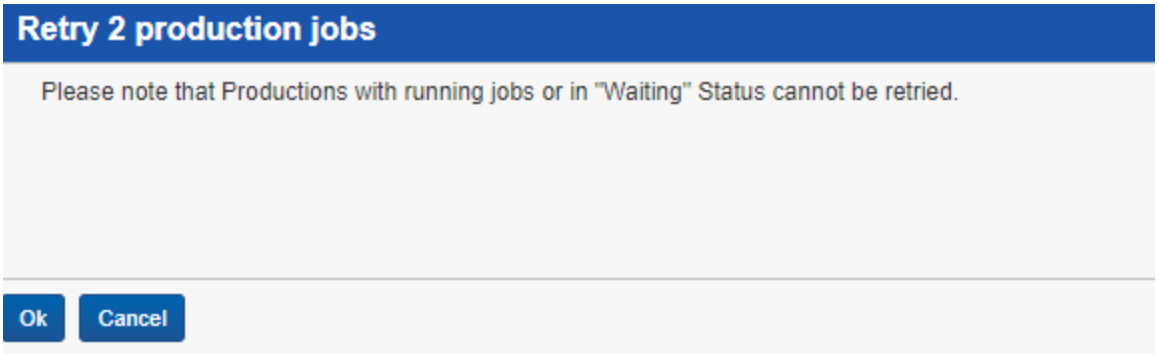
Object Security	Tab Visibility	Admin Operations
	• Production Queue (child)	• View Admin Repository

Note: As long as you have the listed security permissions, you do not need view permissions to the workspaces or the production jobs to use Retry Production Job.

21.19.2 Retrying production jobs

To retry production jobs from the Production Queue tab:

1. Navigate to the **Production Queue** tab.
2. Select the productions jobs that you want to cancel.
3. Click **Retry Production Job** from the mass operations bar. The Retry production job window opens.



4. Click **Ok**.

21.20 Set long text field size

You can use the set long text field size operation to calculate long text size and save the value in a decimal field for each selected document. You can use the mass operation with Data Grid-enabled or SQL extracted text fields. This feature is useful when creating views and saved searches of documents based on long text size. In Relativity, long text is declared as an uncompressed nvarchar(max). This means it will always hold each character as 2 bytes in terms of how this operation calculates the size of the long text field.

Note: The Set Long Text Field Size operation measures the size of the selected field using UTF-16 encoding. The sizes it estimates may be double the UTF-8 value used by some features, such as structured analytics.

21.20.1 Before you begin

To enable the mass operation in your Relativity instance, you must import the Long Text Size application from the application library. To do this, you must have the appropriate admin rights.

To install the Set Long Text Field Size application in your workspace:

1. Navigate to the **Relativity Applications** tab.
2. Click **New Relativity Application**.
3. Select **Select from Application Library**.

4. Click  on **Choose from Application Library**.
5. Select **Set LongText Field Size**, and click **OK**.
6. Click **Import**.

Note: After the application is installed, review the workspace permissions and remove the Set Long Text Field Size permission for the groups that should not have access to the mass operation.

21.20.1.1 Set long text field size considerations

- There's no hard limit on the number of documents you can update with the Set Long Text Fields Size script.
- Because this is a mass operation, run it during a maintenance window or other low-usage hours to minimize performance impact.
- Run time varies by document size and total volume. Larger documents take longer, and benchmark metrics aren't available to predict duration for very large sets (for example, 1,000,000 documents). To plan, run a small test batch, review results, and then scale up.

21.20.2 Using the mass operation

To set long text size:

1. Create a decimal field for saving the extracted text size. For more information, see Fields on page 196.
2. From the mass operations bar on the document list, choose whether to select **Checked items** or **All items** in the current returned set.

   Note: The set long text size mass operation permits the user to edit documents even if they have read-only permissions.
3. Select **Set long text field size** in the mass operations drop-down menu.
   The Set LongText Size form displays.
4. Select a source field to calculate long text size. The drop-down menu includes all long text fields you have permissions to see.
5. Select a decimal field to store the calculated long text size. The drop-down menu includes all decimal fields you have permissions to see.
6. Click **Run** to apply your changes.

Note: The mass operation stores the size of the text, in kilobytes, in the decimal field.

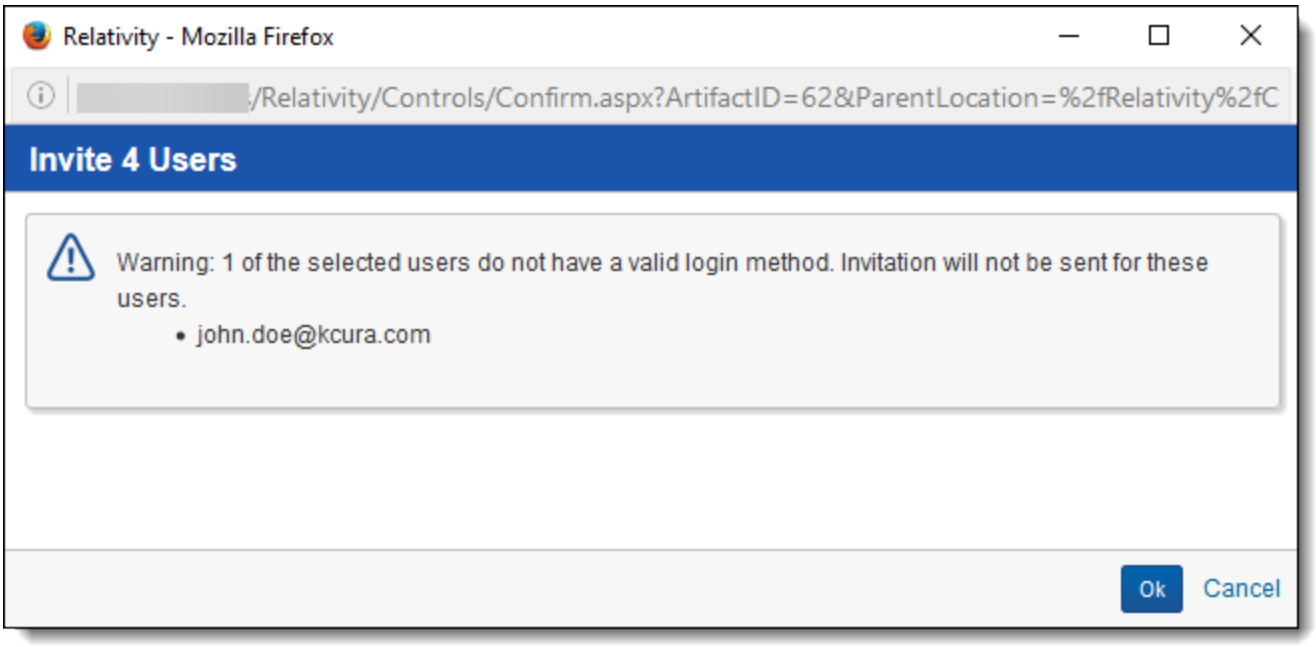
21.21 Invite users

You can use the Invite operation to send out invitation to newly-created users to log in to Relativity and set their passwords. This feature is useful when you setting up a large number of reviewers in a new case.

Note: You cannot use mass operations on Data Grid-enabled fields.

To send invitations to multiple users:

- Navigate to the Users tab.
- From the mass operations bar, choose whether to select **Checked items** or **All items** in the current returned set.
- Select **Invite** in the mass operations drop-down menu.
- The Invite Users dialog opens.



If any of the users can't be invited, they are listed in the dialog. The reasons may include:

- The user you are inviting doesn't have a valid login method. To correct this, assign the user a login method.
- You don't have edit permissions to the user(s) that you are inviting. Make sure you have edit permissions to the users.

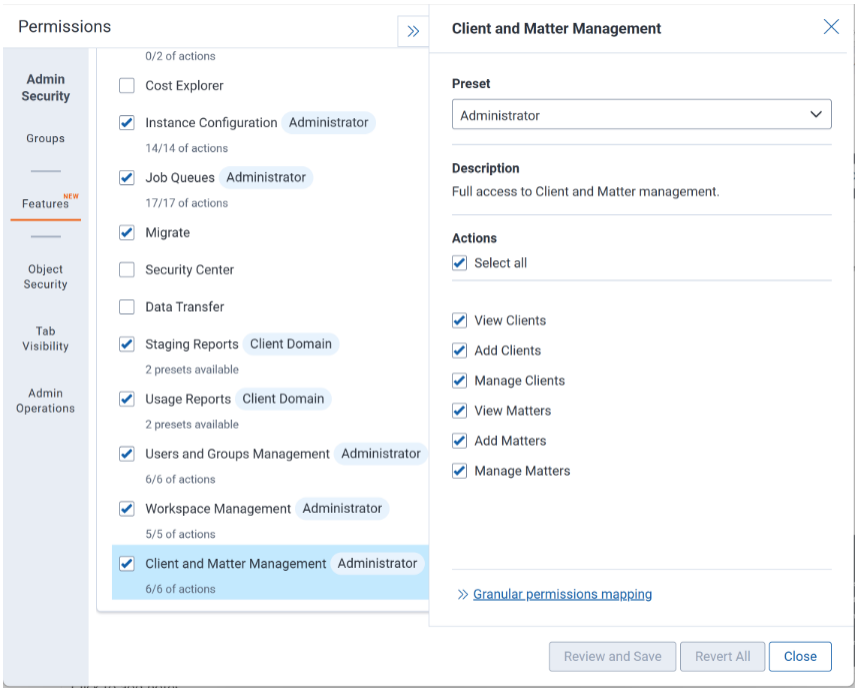
- Click **Ok**. The invitation emails are sent to the users.

22 Matters

Clients in Relativity are associated with one or more matters. Matters are used to define the different cases, disputes or advising that a firm may be involved with for a client. Within Relativity, a matter must be associated with an existing client. A matter can also be associated with one or more workspaces, but it's not required.

22.1 Permissions

Manage permissions for this feature on the Features tab. Grant the full feature for a group, or customize access with individual actions. For an overview of features and actions, see Feature permissions.



22.2 Creating or editing a matter

Note: Once a workspace is created, only System Administrators and Client Domain Administrators can make updates to the Matter object. Even users with full permissions for Matters and Clients will not have the ability to modify this object unless they are System Administrators or Client Domain Administrators.

To create or edit a matter, perform the following steps:

1. Select the **Matters** tab.
2. Click **New Matter** to create a new matter, or click **Edit** next to the matter whose information you want to edit. The Matter Information form displays with required fields in orange.
3. Complete the fields on the Matter Information form.
    - **Name** is the matter's name. This field must be between 1 and 210 characters.
    - **Matter Number** is a unique number that identifies the matter. Use this number internally to organize your matters.
    - **Status** is the matter's current status. The default options are Active or Inactive, but you can click **Manage** to add any value. This field is useful when organizing and displaying lists of matters using Relativity views. For information about using the Status field as an organizational tool, see Views on page 702.
    - **Client** is the matter's associated client. Click  to select from all available clients.

      Note: If your client list is too large, click **Show Filters** to quickly narrow the list by any available field criteria. Items in the client list are set by a system view. Therefore, it is possible to only see a subset of items.

22.3 Adding or removing matters from a client domain

You can add or remove objects from client domains if you have the client domains feature activated.

Use the following steps to add a matter to a client domain:

1. Navigate to the **Matters** tab.
2. Select the matter you want to add to the client domain from the list.
3. Click **Edit**.
4. Access the **Client** field in **Matter Information** section.
5. Select the client with client domain enabled from the list.
6. Click **Save**.

Use the following steps to remove a matter from a client domain:

1. Navigate to the **Matters** tab.
2. Select the matter you want to remove from the client domain from the list.
3. Click **Edit**.
4. Access the **Client** field in **Matter Information** section.
5. Select a client not associated with a client domain from the list.
6. Click **Save**.

Note: Before you delete a matter, make sure all associated workspaces are permanently deleted from the Recycle Bin. If an associated workspace is queued for deletion in the Recycle Bin, this disables matter deletion.

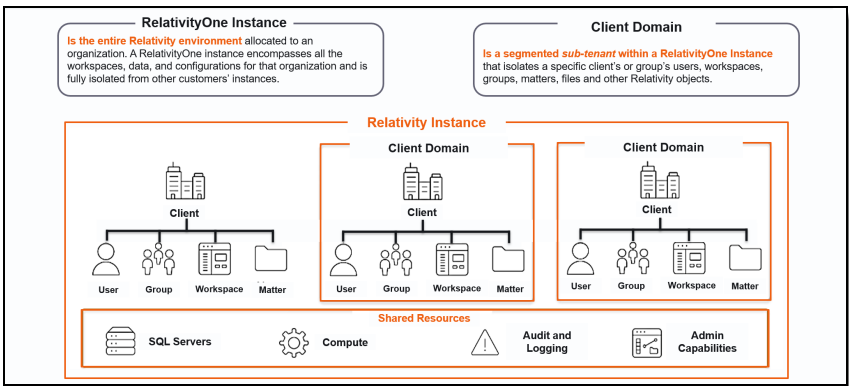
23 Client domains

The client domains feature enables Relativity to deliver more powerful managed service offerings for service providers in a single RelativityOne instance by providing an easier way to securely isolate users, workspaces, groups, and matters by clients.

Using client domains, system admins can empower a user group that is not part of the System Administrator group, client domain admins, to perform common administrative tasks within their own client domain while limiting their visibility into the Relativity environment as a whole. The client domain admins can customize the permission settings to various objects according to their preferences within their own domain, but cannot access any permissions outside of that. This resource isolation functionality grants your enterprise clients more administrative control over their own portions of the environment while preventing back-end visibility and unauthorized changes to your RelativityOne instance as a whole.

Note: Client domains are targeted for the above use case only and it is important to consider all the limitations outlined in Client domain limitations and considerations.

Implementing client domains requires an additional license from Relativity ODA LLC. Each client domain license is unique, and client domains can have different terms encoded on their license keys. The license for a client domain is unrelated to any other license for Relativity (e.g., number of seats). Client domain licenses are not transferable from one client to another. To request a new client domain, you must submit a Relativity aiR request via the Community site as detailed in the following knowledge article.



23.1 Client domains software architecture

The following describes the basic software architecture for client domains.

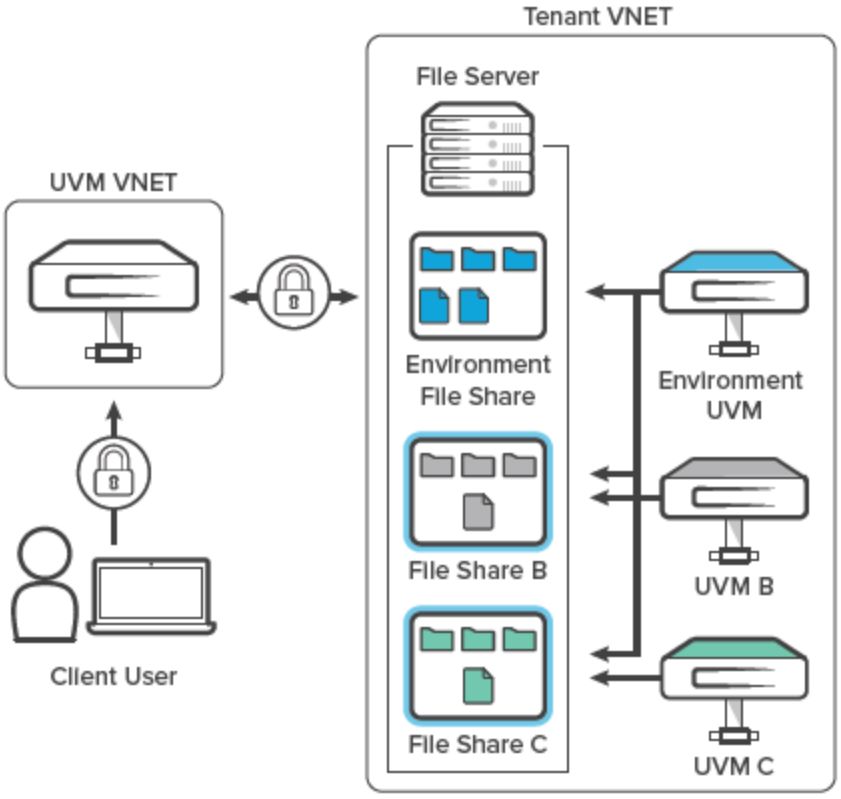
- **Permissions** - the root object of a client domain is the client object in the administrative workspace. By default, groups associated with a given client only have permission to perform actions on users, groups, matters, and workspaces associated with that client, unless a system administrator has given special permission across client domain boundaries. Additionally, each client domain has an associated group known as the client administrator group. By default, members of this group can create administrative objects (users, groups, matters, and workspaces) associated with the client. This group does not have permission to interact with or view objects of these types associated with other clients.
- **Credentials** - many services in Relativity aiR, such as HTML5 conversion and Staging Explorer, utilize custom credentials to access resources on the client domain's behalf. For example, a credential stored in Relativity aiR is used by the conversion service to access the Relativity file repository in a secure manner.

23.2 Client domains cloud infrastructure

The following information describes the architecture of the cloud infrastructure for client domains:

- **Utility Server** - each Relativity aiR tenant can have a Utility Server, which accesses the fileshare for each client domain. In addition, a dedicated Utility Server may be requested for a client domain within the tenant. Please note that there is a maximum of 11 client domain utility servers allowed per Relativity instance.
- **File server** - each client domain has a separate staging fileshare provisioned in the system. The Client Domain Admin group for that domain is automatically granted admin permissions to their respective staging fileshare, giving them full access to manage fileshare operations (view, upload, download, edit, secure). For additional details, see User access permissions to fileshares. For details on configuring fileshare permissions for Client Domains, see User access permissions to fileshares.
- **VPN Access** - All access to the Relativity aiR infrastructure is performed over a VPN. Within a tenant, all clients use the same VPN client); access is limited through the credentials of the Utility Server.

The following diagram shows how the above components interact.



23.3 Considerations before enabling client domains

Consider the following before enabling client domains:

- If you enable client domains on a client:
  - You can't disable it on that client later.
  - You can't edit the name of the client, but you can edit the Client ID number.
- You can add objects to a client domain after the client has client domains enabled, but it's best to verify that all objects you want to isolate within the client domain are child objects of the client.
- If you have client domains enabled, we recommend locking down System Administrator access to only those absolutely necessary.

23.4 Enabling client domains on a client

Note: You cannot convert an existing client to a client domain.

To request a new client domain, you must submit a Relativity aiR request via the Community site by navigating to the Support tab and then Relativity aiR requests (as detailed in the following knowledge article). Please note that the Client Domain creation process takes 3 business days. If an Utility Server was requested, you will also be contacted with the following information:

- IP address to the new client domain Utility Server.
- Client domain user credentials to the new Utility Server.

The following things occur automatically after client domains are enabled:

- The system creates a new **Everyone - [Client's Name]** group and adds that group to the client domain. Only users whose client field is set to the client domain are included in the client domain everyone group. The system also removes those users from the default Relativity Everyone group. A system admin can add any users to any group regardless of client domain status.

  Note: The **Everyone - [Client's Name]** group should not be assigned as the workspace administrator group for a given workspace that is part of a Client Domain.

- The system creates a unique copy of all resource pools associated with any workspaces under the client domain.

  Note: Permissions assigned to groups override client domain isolation. If a non-client domain group has permissions to see a client domain's workspace or users, then those non-client domain users in the non-client domain group can still access client domain items. Enabling client domains does not change previously configured item level security settings applied to any objects within the client domain.

- The system creates a client domain admin group that permits its members to perform admin operations within the client domain.

  Note: After enabling client domains, system administrators needing to make group or permission changes should be extra cautious and thoroughly investigate the potential impact to client domain separation before implementing any new group/permission changes.

- The newly created Client Domain Admin group is automatically granted admin permissions to the staging file share provisioned for that client domain, enabling full file share management (view, upload, download, edit, secure) within their domain's staging area.

Once client domains functionality is enabled for the client, you must assign a client domain admin.

23.5 Client domain admins

Client domain admins are essentially workspace admins for workspaces within the client domain. Any limitations are based on the permissions you set for the user group in Relativity that the client domain admin belongs to. The administrative actions available to client domain admins are only in the scope of the client domain. For example, client domain admins can edit or delete users belonging to that client domain, but they cannot do the same action for users part of a different client domain or users not associated with a client domain.

Client domain admins can do things like:

- Modify, add, and remove groups, users, and workspaces.
- Create all workspace and admin objects across the Relativity Framework, such as matters, fields, layouts, choices, and views.
- Start jobs like processing, imaging, and productions.
  - Tenants have access to the full complement of the Processing features, including inventory, discovery, and publish.
- Import data.

23.5.1 Client domain admin considerations

Consider the following when assigning a client domain admin:

- Client domain admins:
  - can access the Security Center with the correct permissions. For more information, see Client domain administrators.
  - cannot perform tasks that are exclusive to Relativity System Administrators.
  - do not have access to Mass Operations on the Users tab.
- Client domain admins cannot add themselves to any group (even groups tied to their own client domain). Only a System Administrator can change a user's group memberships.
- We recommend users review Client Domain and other Administrative type permissions for item-level security based on the workflow within your instance. Relativity recommends applying item-level security to all views for the following types within the Admin landing page, removing access from all non-administrative users:
  - Authentication Provider

    Note: Client Domain specific views can be used and configured to enable Client Domain administrators to configure and view their own users more easily. Ensure you have properly reviewed and tested all relevant permissions before doing so.
  - Authentication Provider Type
  - Code
  - Fields
  - Resource Pools
  - Resource Servers
- **Permissions assigned to groups override client domain isolation**. If a non-client domain group has permissions to see a client domain's workspace or users, then those non-client domain users in the non-client domain group can still access client domain items. Enabling client domains does not change previously configured item level security settings applied to any objects within the client domain.
- Users with the **Manage Cold Storage** Admin permission and access to the workspace can move it to or from Cold Storage.
- Transferring data via Integration Points uses a standard Relativity permissions check. If a client domain admin has access to a source and destination workspace and has permissions for importing and exporting data, they can transfer data to the workspace even if it's outside the client domain.
- Relativity displays a warning message when a system admin attempts to edit or copy permissions for any group in a client domain. This warning makes the system admin aware that modifying permissions may have significant consequences. For example, changing permissions may allow client domain users to modify items outside their tenancy. The system admin can click Manage Permissions to proceed with the update or Cancel to exit the pop-up window.
- If a system admin assigns additional permissions for other Admin objects to a client domain admin (such as, Queues), the client domain admin may be able to see information for other client domains.
- System Administrators should be aware of the following behavior to prevent unintentionally providing users with access to data outside their domain: If you add a user who is already a member of a domain admin group to another group that holds the Relativity Script system permission, the user will gain access to all users and groups across the entire Relativity instance. This could pose a major security concern; this is why the View Relativity Script permission is not granted by default to the Client Domain Admin for <Client> group. Once the user is removed from the new group, access will be restricted again to users and groups associated with their specific client.

- When importing a Client Domain Admin using the Relativity User Import Application, the application automatically includes the new user in the Everyone group by default. This action can disrupt the Client Domain security settings in your Relativity instance. To address this issue, follow these steps: remove the user from the Everyone group and assign them to the client-specific Everyone group. Achieve this by temporarily switching the user to any client not linked to a domain, and then back to the desired domain client.
- You can grant workspace admins within the client domain permission to edit security settings for groups within the client domain, but they can't edit permissions on groups outside of the client domain.
- Workspace Admin and Client Domain Admin permissions are not copied from the workspace template when a new workspace is created. They are taken from the Sys Admin permissions.

Feature	Action	Object Permissions	Tab Visibility	Other Settings	Presets
Authentication	View Federated Instance in User Menu	Federated Instances: View	None	View Admin Repository	Client Domain
Client and Matter Management	Add Matter to Client	Matter: Add (no view) Client: View	Matters	View Admin Repository	Client Domain
Instance Configuration	View Choice, Tabs, and Views for Client	View: View Choice: View Tab: View	None	View Admin Repository	Client Domain
Users and Groups Management	Add Users and Groups to Client	User: Add (no view) Group: Add (no view) Login Method: View, Add, Edit Auth Provider: View Auth Provider Type: View	User and Group Management, Users, Groups	View Admin Repository	Client Domain
Workspace Management	Add Workspaces to Client	Workspace: View, Add	Workspaces	View Admin Repository	Client Domain

Optionally, Client Domains may also have these permissions assigned.

Feature	Action	Object Permissions	Tab Visibility	Other Settings	Presets
Staging Reports	View Client Reports	None	Staging Reports Management Console	View Client Domain Staging Reports View Admin Repository	Client Domain
Usage Reports	View Client Reports	None	Matters	View Client Domain Usage Reports View Admin Repository	Client Domain

23.5.2 Default instance permissions

The following table provides a breakdown of the default instance permissions for a client domain admin:

Group	Permission	Type
Client Domain Admin for <Client>	View Admin Repository	Admin Operations
Client Domain Admin for <Client>	Add Matter	Add
Client Domain Admin for <Client>	Add User	Add
Client Domain Admin for <Client>	View View	View
Client Domain Admin for <Client>	View Choice	View
Client Domain Admin for <Client>	Add Group	Add
Client Domain Admin for <Client>	Add Workspace	Add
Client Domain Admin for <Client>	Add Error	Add
Client Domain Admin for <Client>	View Server	View
Client Domain Admin for <Client>	View Tab Type	View
Client Domain Admin for <Client>	Authentication Provider*	View
Client Domain Admin for <Client>	Login Method	View, Edit, Delete, Add
Client Domain Admin for <Client>	Staging Fileshare — View	Fileshare Operations
Client Domain	Staging Fileshare — Upload	Fileshare

Group	Permission	Type
Admin for <Client>		Operations
Client Domain Admin for <Client>	Staging Fileshare — Download	Fileshare Operations
Client Domain Admin for <Client>	Staging Fileshare — Edit	Fileshare Operations
Client Domain Admin for <Client>	Staging Fileshare — Secure	Fileshare Operations

* The View Authentication Provider permission is required for Client Domain admins to add login methods to their users. Because the Authentication Provider object is not client-bound, it is highly recommended that you apply item-level security to ensure that Client Domain admins can see only the necessary Authentication Providers.

23.5.3 Assigning a client domain admin

Once you enable client domains on a client, you must assign a client domain admin.

Caution: While a system administrator can assign users to the client domain admin group and adjust its permissions, Relativity strongly advises against changing Client Domain Admin permissions without explicit guidance from Relativity Support. Modifying these permissions may allow client domain admins to access objects outside their domain, compromising security.

Use the following steps to assign a client domain admin.

1. Navigate to the **Groups** tab.
2. Select the client domain admin group.
3. Click the **Add** button in the **Users** section.
4. Select the user you want to be the client domain admin.
5. Click **OK**.

A system admin can make any user a client domain admin by adding them to the client domain admin group. You can tailor the permission settings of a client domain admin group the same way you manage permissions for all other groups. See Setting instance permissions on page 610 for more information. See Client domain admin considerations on page 403 for more information on default permissions.

23.6 Client domain limitations and considerations

The following items are features and operations that are not available when using client domains (if a feature or operation isn't listed, it is available when using client domains):

- Client Domain Administrators do not have access to the Errors tab, which may impact their workflows.

Note: The (Admin) Errors tab has been permanently removed from Relativity aiR, and the ability to read errors through the API has been disabled. Job-specific errors are now addressable directly within your workspaces. For more information, see Errors tab deprecation.

- UVM (Utility Virtual Machine) is not available for Relativity aiR Government clients.
- The *What's New* feature is not available to Client Domain Administrators or Users.
- Multi-tiered client domains - an enabled Client Domain cannot have their own sub/child client domains.
- Cost Explorer isn't accessible within a Client Domain.
- Unique logos or URLs per client domain.
- Customer-managed keys (CMK)
- Self-provisioning / enabling of client domains requires a request to Relativity Customer Support.

The following items are features and operations that are have limitations in client domains or can only be used or performed by top-level system admins or a Relativity staff resource.

Note: If a feature, capability, or operation isn't listed, then there are no limitations on them when using client domains. For example, Legal Hold isn't listed and has full functionality when operating client domains.

Item	Limitation	Client domain admin	System admin
Client domains setup and configuration			
SSO setup	If the SSO provider is configured correctly, a system administrator can set up client domain user accounts to use it.	No access	Yes
Client domain setup	• Cannot be setup on a Client record that already has a workspace association. • There are no custom URLs created for Client Domain users. • Cannot disable client domain on client once enabled. • Cannot rename client once enabled. • The maximum number of client domains that can be created for an instance of Relativity is 100 without a utility server (or 11 if a utility server is required for all individual client domains within a Relativity aiR instance). **Note:** Performance may vary as you increase the number of client domains in your environment.	No access	No access
Instance settings	Not available per client domain.	No access	No access
Feature access			
aiR	Client Domain admins cannot access the instane-level aiR Review Jobs tab.	No access	Has access
ARM	Not available to Client Domain Admins. **Note:** ARM archives can be restored directly to a client domain.	No access	Has access
Creating / editing Relativity scripts	Not available to Client Domain Admin. • Admins can run scripts that have already been added to the workspace from the library.	No access	Has access

Item	Limitation	Client domain admin	System admin
	• Admin scripts are not supposed to be run by client domain admins. These scripts should not be part of the template workspace.		
Direct SQL access	Not available to Client Domain Admin.	No access	Has access
Migrate	Migrate (similar to ARM) is supported for client domains, but migrations can only be performed by a Relativity System Admin. Migrate cannot be used by a Client Domain Administrator due to security restrictions.	N/A	Has access
Cost Explorer	System Admins have access to the Cost Explorer, but client domain admins do not.	No access	Has access
Case Metrics	By default, the Client Domain Admin permission set does not include Case Metrics instance-level reporting, including the Scheduler. **We do not recommend** granting Client Domain Admins instance permissions beyond the defaults, because doing so can break down domain isolation. The Reviewer Metrics tab is the only Case Metrics component that accounts for client domains, and it shows only data for the admin's own client domain.	Has limited access	Has access
Relativity applications	• Client Domain Admin is not able to install or upgrade Relativity applications. • No support of multiple app versions. • Case Dynamics, and Transcripts applications have been tested and work without issue in environments with client domains. • Most applications are typically not built or tested with client domain structure or concerns in mind.	No access	Has access
Tabs	We recommend avoiding sensitive data in tab names. You can secure new tabs by overriding inherited security settings and applying .item-level security.	Has limited access	Has access
User and Group Synchronization application	The User and Group Synchronization application is not compatible with Client Domains.	No access	Has access
View, edit or cancel jobs / queues	Jobs / queue status not available to Client Domain Admins. Since client domain admins can't see or modify jobs in the queue, a system admin may need to inform client domain admins of the status of jobs they've start or if the job is still waiting in the queue.	No access	Has access
Views	We recommend avoiding sensitive data in view names. You can secure new views by overriding inherited security settings and applying .item-level security.	Has limited access	Has access
Preview Security	The Preview Security feature is only available to System admins.	No access	Has access

23.7 Adding or removing objects from a client domain

Any workspaces, users, groups, matters, or resource pools associated with a client domain during creation become automatically governed by that client's domain settings. When you move an object into a client domain, you're making it a child object of the client domain.

You can remove a Resource Pool and its associated servers if no other dependencies use them. Before removing these resources, verify that no active dependencies or references exist in the system.

The tenant admin group is tightly linked to the Client Domain. While you can revoke access or remove members from the group, Relativity does not support deleting the group.

See the following pages for more information on moving objects to and from client domains:

- ARM
- Workspaces on page 776
- Adding or removing users from a client domain on page 700
- Adding or removing groups from a client domain on page 237
- Adding or removing matters from a client domain on page 400

23.8 Deleting a client domain

In certain cases, you may need to completely remove (decommission) a client domain. Because Relativity does not allow you to simply delete a client once client domains are enabled, deletion requires a careful, manual process followed by a Relativity support request.

Use the following procedure to delete a client domain:

1. **Gather client domain details:** Note the **Client Domain Name**, **Client Domain ArtifactID**, and the **File Repository Location** for the client domain.
    - You can find the File Repository path by navigating to the client domain's Resource Pools tab in the admin workspace. Click on the client domain's resource pool, then go to the File Repositories tab. Expand the file repository field to see the entire URI path for that client domain's data.
2. **Delete all workspaces in the client domain:** Identify all workspaces associated with the client domain (including any template workspaces) and delete them. Ensure that no workspaces remain active under that client.
3. **Empty the Recycle Bin:** Make sure all deleted workspaces from step 2 are removed from the Relativity Recycle Bin as well. (In Relativity, deleting a workspace moves it to a Recycle Bin; you must permanently delete or restore items from the Recycle Bin. In this case, permanently remove those workspace artifacts.)
4. **Reassign or remove users, groups, and matters:** Identify all users, groups, and matters associated with the client domain, and then do the following:
    - For each user, group, or matter you want to keep, change its **Client** field to a client that isn't associated with a client domain. For instructions, see Adding or removing users from a client domain on page 700, Adding or removing groups from a client domain on page 237, and Adding or removing matters from a client domain on page 400.
    - Remove client domain groups from any workspaces outside the client domain.
    - Remove all users from the groups that remain in the client domain, including the client domain admin group. You can't delete these groups yourself. Relativity deletes them as part of the client domain deletion.

5. **Contact Relativity Support to request client domain deletion:** Open a support ticket with Relativity requesting a "Client Domain Deletion". In the ticket, provide the Client Domain Name, Client Domain ArtifactID, and the File Repository Location you gathered in step 1. Relativity's internal deletion pipeline will then proceed to delete all data inside the client domain's file repository and remove the client domain from the system.

   Note: You do not need to manually delete the physical files on disk for the client domain. The Relativity deletion pipeline will securely erase all data in the client domain's repository path as part of this process.

Note: Before you submit the deletion request, make sure that all workspaces in the client domain are deleted and that no client domain groups are assigned to workspaces outside the client domain. When Relativity deletes the client domain, it also deletes all groups, matters, and users that are still associated with the client. To keep any of these objects, reassign them to a client that isn't associated with a client domain before you submit the request.

Important: Deleting a client domain is irreversible. Make absolutely sure that the client domain's workspaces are no longer needed or have been migrated elsewhere, and that you have backups of any data if necessary, before proceeding with a deletion request.

24 OCR

Optical Character Recognition (OCR) translates images of text, such as scanned and redacted documents, into text characters. There are three main steps involved in OCR-ing documents:

Notes: All documents, including native files, must be imaged before using OCR.

1. Define a **production** or **saved search** that contains the documents you want to OCR. See Creating a saved search in the Searching guide or Creating and editing a production set.
2. Create an **OCR profile**. See Creating and editing an OCR profile on the next page.
3. Create an **OCR set** that references your OCR profile. See Creating and editing an OCR set on page 414.

With OCR you can view and search on text that's normally locked inside images. It uses pattern recognition to identify individual text characters on a page, such as letters, numbers, punctuation marks, spaces, and ends of lines.

Note: Relativity aiR scales automatically for OCR.

Note: See OCR on redacted production documents for information on running OCR on redacted production documents.

24.1 Document characteristics that affect OCR quality

The quality of your OCR results depends on the characteristics of the source document images. Documents with clear, high-contrast text generally produce the most accurate results, while documents with visual noise, complex layouts, or non-standard text produce less reliable results.

Use the following table to understand which characteristics lead to the best and poorest text extraction.

Characteristics that produce the best results	Characteristics that produce poor results
Native Office-to-PDF conversion	Mirror-flipped images
Dark text on a plain, light background	Text embedded inside charts or graphics
Standard fonts at body size or larger	Screenshots with overlapping UI elements

Characteristics that produce the best results	Characteristics that produce poor results
300 DPI or higher resolution (for scanned documents)	Dark or patterned backgrounds with sparse text
Simple layout with clear content separation	Handwriting or signatures
Text as standalone elements, not inside graphics	Text cropped at the image boundary
Correct, non-mirrored page orientation	Small caption or label text
Single content layer with no overlapping elements	

Note: If your documents contain characteristics from the poor results column, consider enabling the Preprocess Images option in your OCR profile. If you set Preprocess Images to Yes, preprocessing occurs before the OCR engine attempts to recognize characters. This improves the accuracy of the results at the expense of optimal job throughput.

24.2 Creating and editing an OCR profile

An OCR profile is a saved, reusable set of parameters that you use when creating an OCR set. To run an OCR job, you must first create an OCR profile.

You do not have to create a profile for every OCR set you create. You can use only one profile for all sets. However, you may want to have multiple profiles saved with different accuracy or language settings to use for different document sets you plan to OCR.

To create an OCR profile, follow these steps:

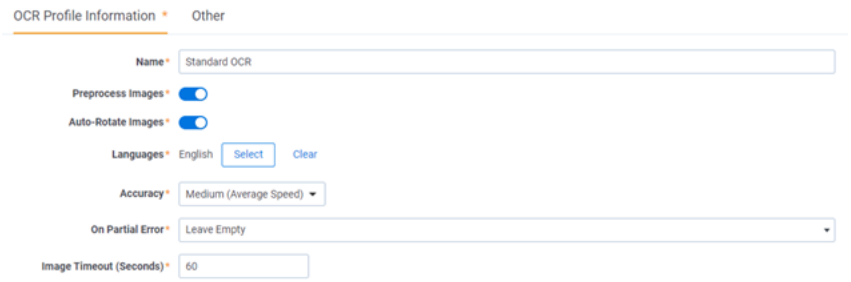
1. Click the **OCR Profiles** tab under the **OCR** tab.
2. Click **New OCR Profile**.
3. Complete the OCR Profile fields.
4. Click **Save**.

Notes: Special considerations when using Arabic as a recognition language:

- When Arabic is selected as a recognition language, the OCR engine also recognizes English by default. You do not need to select English as an additional recognition language.
- Running OCR with an OCR profile that combines Arabic with other languages is not supported. This configuration may lead to OCR Image Errors. As a result, you may not be able to recognize any text from the image, regardless of whether there was an actual recognizable text in the image.

24.2.1 OCR profile fields

Complete the following OCR profile fields:



- **Name** - the name of the OCR set. The following characters are not allowed: <,>,:,",/,\,|,?,*
- **Preprocess Images** - enhances the images to get rid of distortions before OCRing. If you set this to Yes, pre-processing occurs before the OCR engine attempts to recognize characters. This improves the accuracy of the results while significantly slowing down job completion. Setting preprocess images to Yes also arranges for any or all of the following sub-processes:
  - To improve visibility, resolution enhancement increases pixel density to 1.5 to 2 times of that of the original image.
  - Text line straightening removes the distortion that occurs when capturing curved book pages.
  - Removing parallax distortion assists in situations in which the camera is not perpendicular to the page and the image is flawed as a result; for best results, the image should contain at least six lines of justified text.
  - Deskewing corrects documents that became slanted during scanning.
- **Auto-Rotate Images** - makes the OCR engine detect page positioning, and then reposition the page accordingly. This can potentially impact the accuracy of OCR results. The rotated image is not saved back to Relativity in rotated position.

  Note: The OCR engine will only rotate the image if both preprocess and auto-rotate options are enabled.

- **Languages** - the language(s) you want the OCR engine to recognize while running the job. Click ... to choose from a list of languages. If the saved search or production you plan to use as your document set contains multiple languages, you may want to select more than one from this list. See the Supported languages matrix on the Documentation site.

  Note: If the saved search or production you use contains multiple languages and you only select one language from the list, the OCR uses the individual characters of the selected language to OCR all the text.

- **Accuracy** - determines the desired accuracy of your OCR results and the speed with which you want the job completed. This drop-down menu contains three options:
  - **High (Slowest Speed)** - runs the OCR job with the highest accuracy and the slowest speed.
  - **Medium (Average Speed)** - runs the OCR job with medium accuracy and average speed.
  - **Low (Fastest Speed)** - runs the OCR job with the lowest accuracy and fastest speed.

  Note: If an OCR job is not extracting text from redactions as expected and is instead displaying a blank space where text should be, change the Accuracy field from High to Low. In addition, if there are no images in the set that need rotating, turn off the Auto-Rotate Images option. Making these adjustments should improve data extraction.

- **On Partial Error** - determines the behavior when the OCR engine encounters an error on an image:
  - **Leave Empty** - records no results if an error is encountered in a document; even images without errors are excluded from being written. For example, if one document contains five images and one of the images errors, no results are written for that document.
  - **Write Partial Results** - records all successfully OCRed text while excluding text from errored images. With this option you can see potentially relevant text that would not be visible if you chose to leave the results of documents containing errored images empty. This option runs the risk of excluding potentially relevant text.
- **Image Timeout (Seconds)** - determines the maximum number of seconds per image before the OCR engine times out. If the job doesn't complete in this amount of time, it errors on that image. The default value is 60 seconds.

To further distinguish the profile, click the **Other** tab and enter information in the Keywords or Notes fields.



24.3 Creating and editing an OCR set

Using the OCR Sets tab you can submit groups of documents defined by a saved search or production to be OCRed based on the settings defined by the OCR profile. Relativity writes the results to the destination field that you specify.

To create an OCR set, you can copy an existing OCR set. If you copy an OCR set, every current setting in that set copies over.

Before you create an OCR set, you need to create an OCR profile. To create an OCR set, follow these steps:

1. Click the **OCR Sets** tab under the **OCR** tab.
2. Click **New OCR Set**. If you want to edit an existing OCR set, click the **Edit** link next to the OCR set name.
3. Complete the OCR Set fields.
4. Click **Save**. The OCR Set Console appears and you can Run the OCR set.

24.3.1 OCR set fields

Complete the following OCR set fields:

- **OCR Set Information**
  - **Name** - the name of the OCR set.
  - **Email notification recipients** - list all email addresses you want to receive email notification upon OCR completion. Separate each email address with a semicolon.

- **OCR status**-The following fields are read-only:
  - **Status** - view where the OCR set is in the process of running. When you save the set, this field shows a value of Staging until you click the **Run** button in the OCR Set Console. The following statuses occur after you click Run in the console:
    - Pending - awaiting pickup by the OCR Job Manager Agent
    - Building
    - Waiting - awaiting work by an OCR Job Worker Agent
    - In progress - OCR Job Worker Agents are recognizing images
    - Assembling text - The final remaining Documents are getting their text assembled
    - Finalizing
    - Completed (if no errors occurred)
  - If errors occurs or the job is canceled for any reason, the following statuses are possible:
    - Failure
    - Completed with errors (can be retried)
    - Stopping
    - Stopped
  - **Image Completion** - view the count of images completed in the OCR set, the number of images with errors, and the number of images left to be OCRed. Any errors appear in red.
  - **Document Completion** - view the count of documents completed in the OCR set, the number of documents with errors, and the number of documents left to have text assembled. After documents are completed, it is possible to view their OCR'd text. Any errors appear in red.
  - **Last Run Error** - view the last job error that occurred in the running of the OCR set.
- **OCR settings**
  - **OCR Profile** - select the OCR Profile that contains the parameters you want to run when you execute the OCR Set.

    Click 

    to bring up the OCR Profile Picker on OCR Set view, which lists Profiles that have already been created in the OCR Profiles tab.
  - **Destination Field** - specifies the field where you want the OCR text to reside after you run the OCR. This includes Data Grid-enabled long text fields and the extracted text field.

    Note: Any new workspaces created after April 13, 2026, as well as ARM restores performed after that date, will have Extracted Text and OCR Text automatically migrated to Data Grid. In these workspaces, any processing or OCR jobs involving Extracted Text and OCR Text fields will only be able to use fields that are enabled for Data Grid.

    Click 

    to bring up the Field Picker on OCR Set view, which lists all document long text fields you have access to. If you selected non-Western European languages in your OCR Profile, the destination field should be Unicode-enabled. This field is overwritten each time a document is OCRed with that destination field selected.

- **OCR Document Set**
  - **Saved Search** - if you're OCRing documents using a saved search, select the saved search containing the appropriate set of documents you plan to OCR.
    Choosing a saved search only OCRs the original image. If a document on the selected saved search does not have an associated image, that document will not be OCRed. Likewise, the OCR engine will not account for redactions added to the image unless there are redactions on the image itself.
  - **Production** - if you're OCRing documents using a production set, select the production set containing the documents you plan to OCR.

    Click 

    to open the Production Picker on OCR Set view, which displays all production sets with a status of Produced that you have access to. The engine OCRs all burned-in redactions, branding, headers and footers, and text. All documents with images in the production are OCRed, not only those with redactions. This includes placeholders.
  - **Only OCR Production Documents Containing Redactions** - you can OCR only produced documents with redactions. You can set this to Yes only if you selected a production set in the production field for the OCR Document Set. However, this setting does not check the selected production to see if there are images with redactions before running the OCR set. By default, this is set to No.

Note: The OCR engine does not support OCRing content that represents handwritten text.

24.4 Running an OCR set

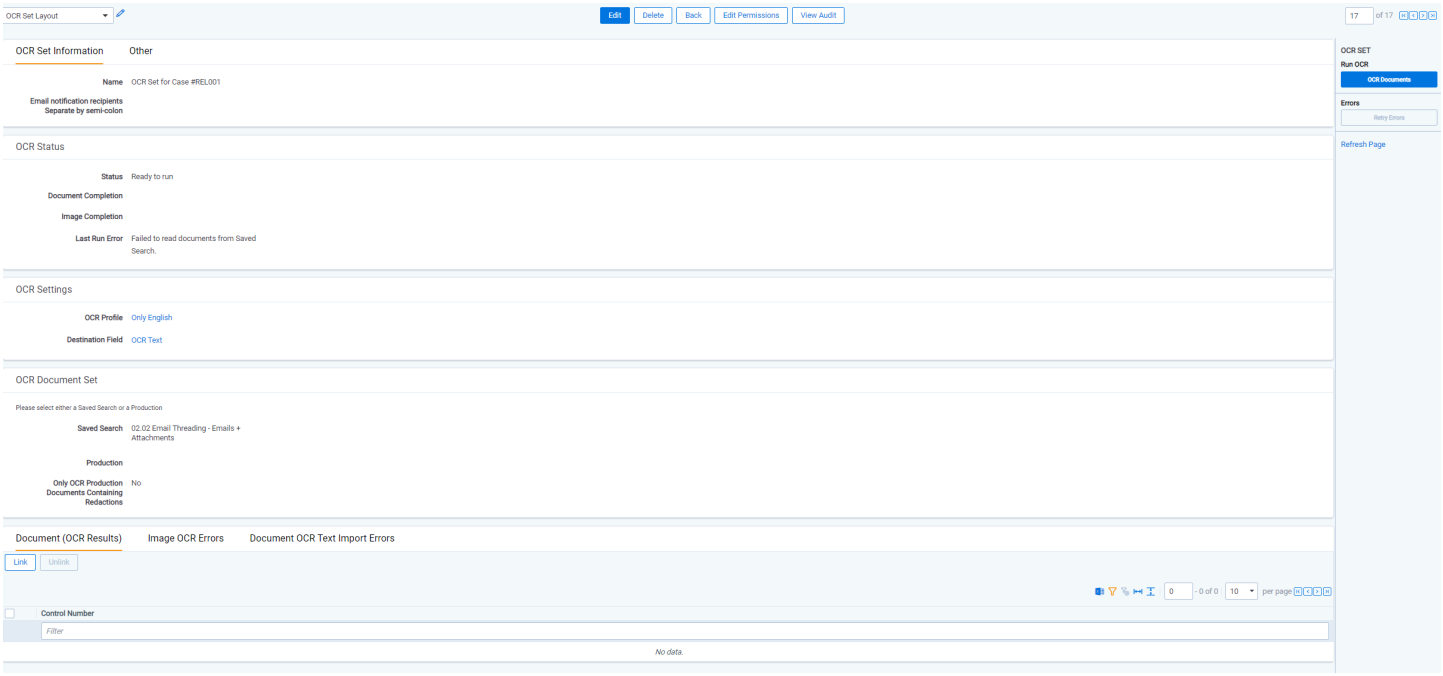
To run an OCR set, you need the following permissions.

Object	Permission
OCR Set	View
OCR Profile	View
Production	View
Saved Search	View
OCR Set Tab	View

Note: These permissions are required only to run an existing OCR set. To create a new OCR set or OCR profile, a user also needs Add permissions.

Note: Feature Permissions provide an alternative to Relativity's security management by shifting the focus from Object Types and Tab Visibility to feature-based permissions. This method is an alternative option. Any feature-specific permissions information already in this and other topics is still applicable. The Feature Permissions interface enables administrators to manage permissions at the feature level, offering a more intuitive experience. By viewing granular permissions associated with each feature, administrators can ensure comprehensive control, ultimately reducing complexity and minimizing errors. For details see Instance-level permissions and Workspace-level permissions.

When you save an OCR set, the OCR Set console appears that you use to run the OCR job.



The OCR Set console provides the following action buttons:

- **OCR Documents** - starts the OCR job. This processes all images in the selected data source or production. If a user stops the job, it completes with errors, or it fails. Click **OCR Documents** to start the job again. If there are documents in the Document (OCR Results) section of the OCR Set Layout form, these are not immediately cleared when you click OCR Documents on the console. These are only cleared when the job goes into processing, which is reflected in the Status when you click the **Refresh Page** link.

  Note: When you click **OCR Documents**, only existing images are OCRed. Images added after you click **OCR Documents** are not OCRed. Changes to an OCR profile are not reflected in the OCR set until you click **OCR Documents**.

- **Stop OCR** - terminates the running OCR job. This button enables after you click **OCR Documents**. When you stop a job, the text that was already OCRed is not saved, and you cannot resume the job from the point it stopped. You have to click **OCR Documents** to begin the job over again.
- **Retry Errors** - attempts to re-run a job with errors.

  Note: If an OCR set is in a status of **Completed with errors** and the data source is modified (i.e. the OCR set is updated from a Saved Search to a Production Set), the OCR set will reset to a status of Ready to run and cannot be retried.

  Retry is only possible when an OCR set is in **Completed with errors**. Retrying an OCR set runs only the images or documents that previously resulted in errors.

- **Refresh Page** - updates the Status, Image Completion, and Document Completion fields while the set is running. Clicking this button reloads the page and may reflect different values in those fields depending on what happened during the OCR job.

Note: During the **In progress** state, while the OCR Job Worker Agents are OCR'ing text, the OCR Job Manager Agent will find documents that have all of their images complete, and will export the text to the selected Destination Text field for that document. This means that OCR'ed text in the Destination Field of the Document will be updated as the OCR Set is progressing, and not at the end of the job.

After the OCR job completes, the Document (OCR Results) section of the OCR Set Layout form displays all documents successfully OCRed. The fields in this view are Control Number and File Icon.

You can also view Image OCR Errors and Document OCR Text Import Errors in the same tabbed display as Document (OCR Results).

These errors can be exported.

Note: Only the first 1000 image errors and first 1000 document errors are shown. These errors cannot be filtered.

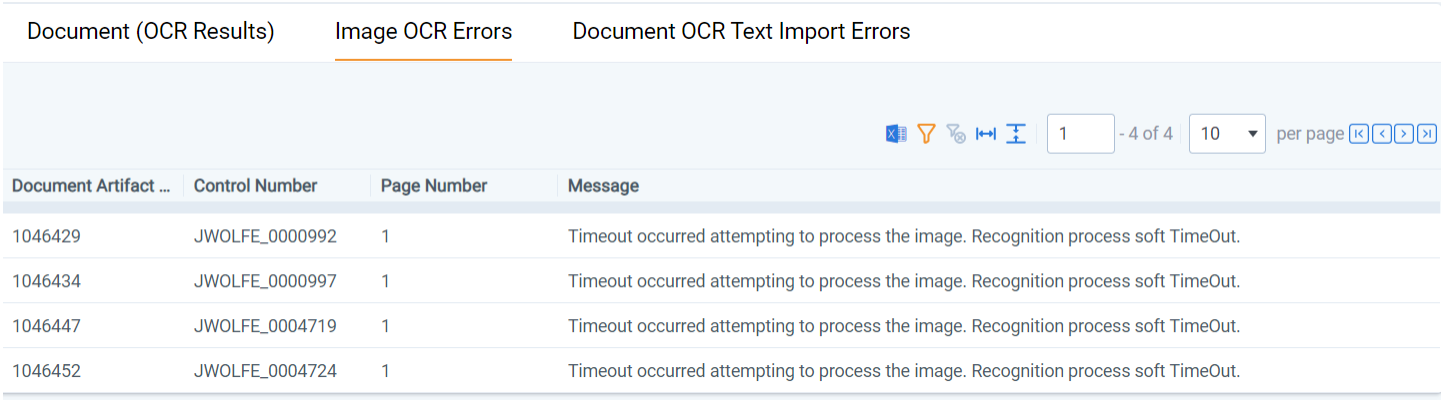


Image OCR Errors shows:

- Document Artifact ID
- Document Identifier
- Page Number
- Message

Document OCR Text Import Errors shows

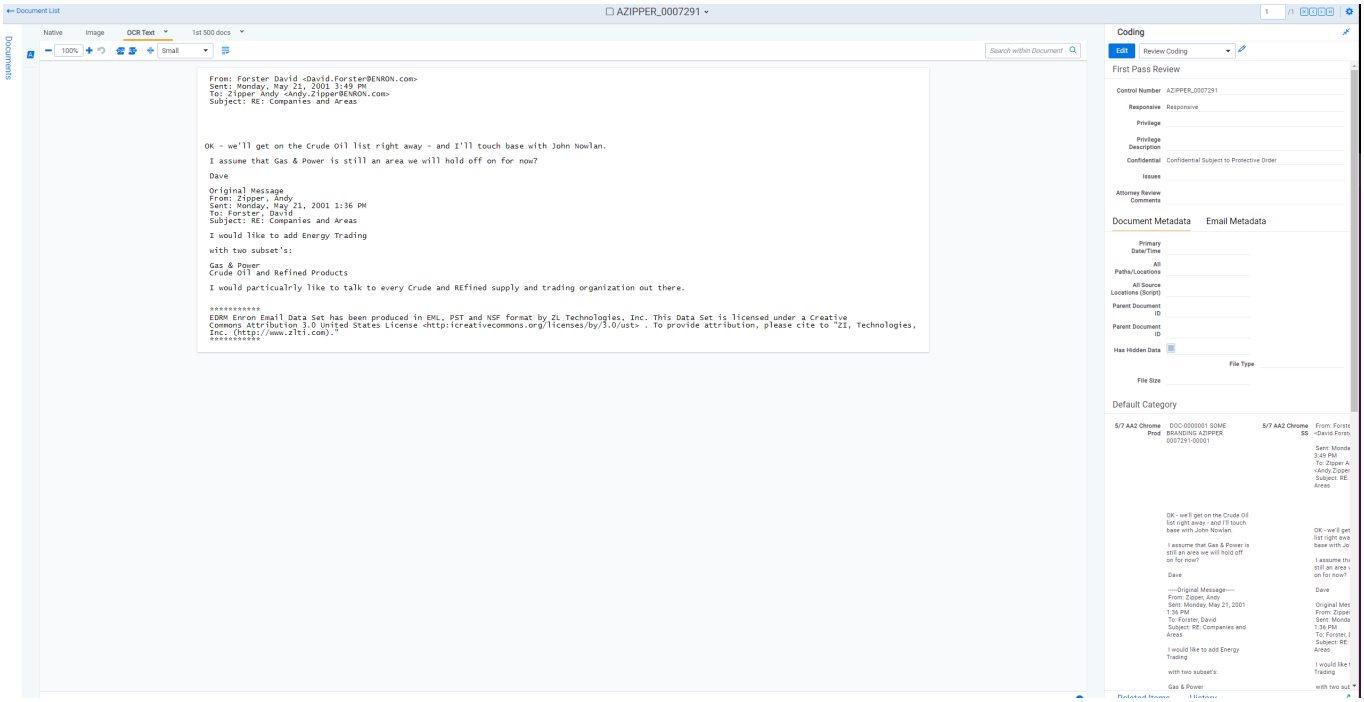
- Document Artifact ID
- Document Identifier
- Message

24.5 Viewing OCR text

After you run the OCR set, you can review your OCRed text. The most effective way of viewing your OCR text is by following these steps:

1. To launch the Review Interface, click the control number of a document.

2. Select the field where you stored the OCR text. If the document has text in multiple fields, select the field from the drop-down menu that appears.

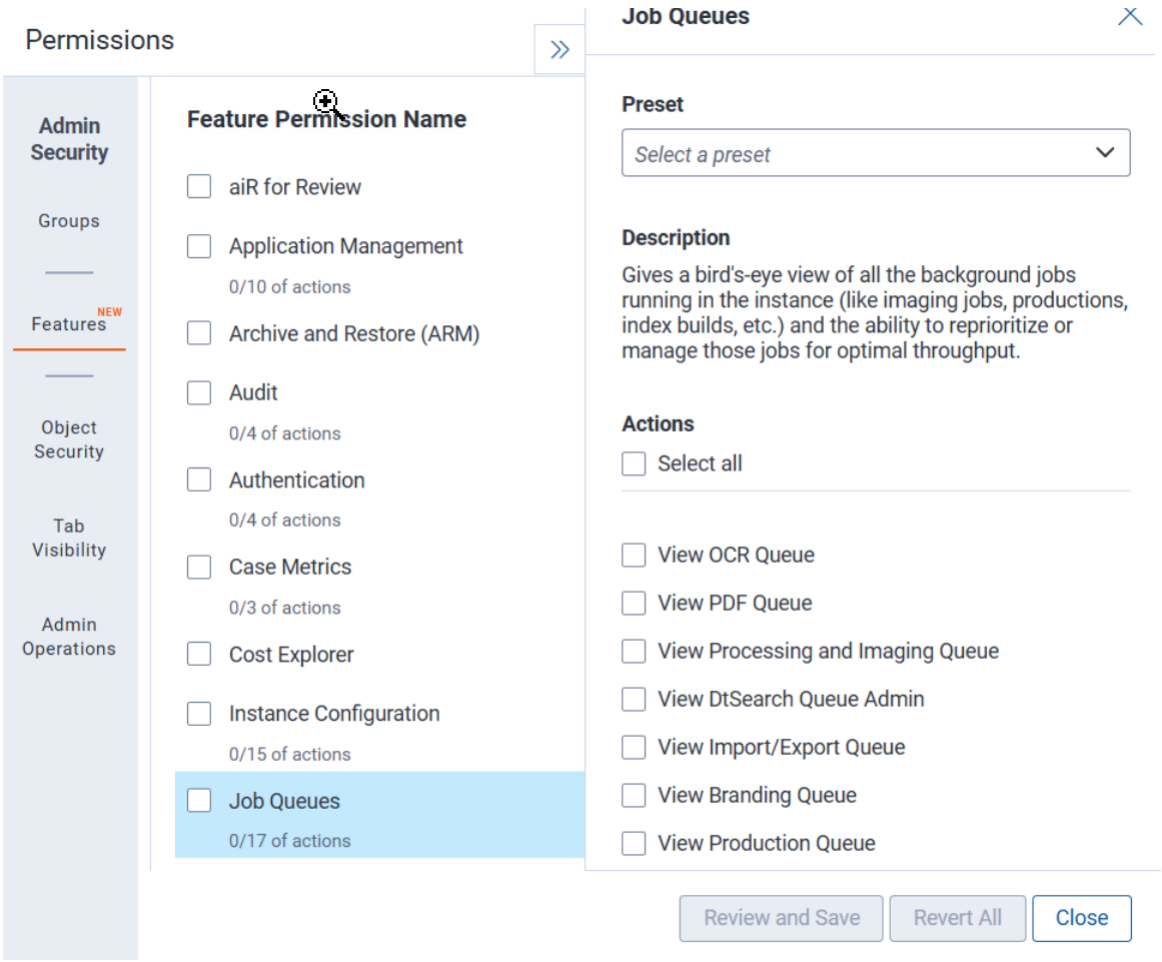


24.6 OCR queue

The OCR Queue tab displays all submitted OCR jobs in your environment, including their status, priority, and the workspace each job belongs to.

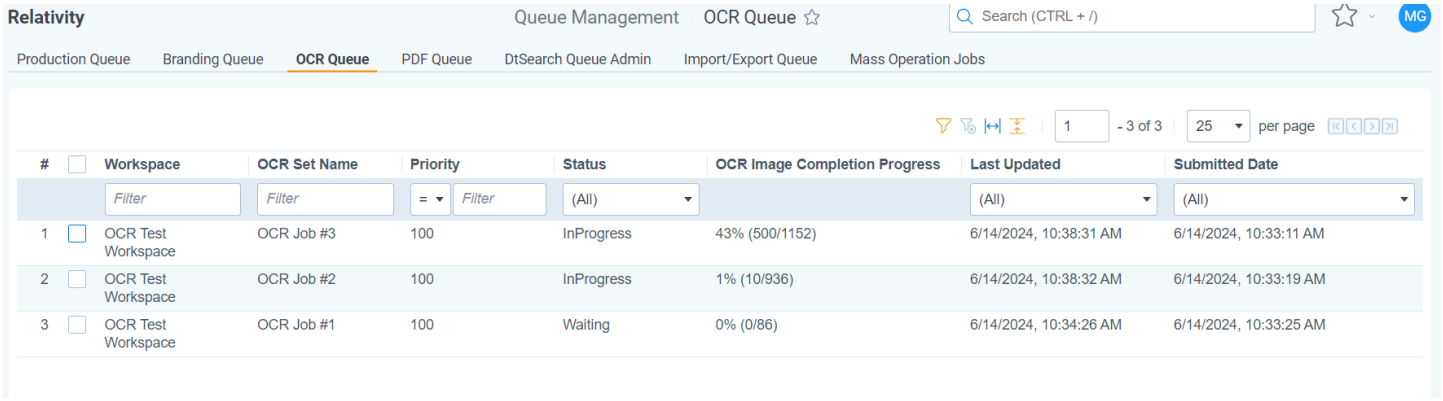
24.6.1 Permissions

Manage permissions for this feature on the Features tab. Grant the full feature for a group, or customize access with individual actions. For an overview of features and actions, see Feature permissions.



24.6.2 OCR queue fields

To display the default OCR Queue view, select the **Queue Management** tab, and then click **OCR Queue**. This list displays all OCR jobs submitted by users in your instance that have not yet successfully completed.



OCR queue columns

- **Workspace** - the name of the workspace containing the OCR set.
- **OCR Set Name** - the name of the OCR set that has a job running.
- **Priority** - the priority of the OCR set job. This value defaults to 100.
- **Status** - displays the status of the submitted job; this field updates as the OCR job progresses.

- **OCR Image Completion Progress** – displays the percentage and number of images OCRed so far and the total number of images to be OCRed in the OCR set.
- **Last Updated** - the date and time at which the OCR Set was last updated.
- **Submitted Date** - the date and time at which one of two actions occurred:
  - A user clicked **Run** on the OCR Set console.
  - A user clicked **Retry Errors** on the OCR Set console when the set was completed with errors.

24.6.3 Change job priority

To change the priority of an OCR job:

1. Click **Change Priority** in the lower-left of the view.
2. Enter a new value in the **Priority** field.
3. Click **Update**.

24.7 OCR on redacted production documents

Preparing redacted documents for production is a common challenge in eDiscovery. This topic provides details on completing OCR on redacted documents and exporting the text.

24.7.1 Before you begin

Run OCR after you complete the production but before you perform the final export:

- The production must have a status of Produced before you can select it in an OCR set.
- Create an OCR profile with your preferred settings.
- Create a long text field to hold your OCR results. You cannot OCR directly into the Extracted Text field.

24.7.2 Running the OCR job

1. Create an OCR Set.
2. In the **OCR Document Set** field, select the completed production.
   - To OCR only redacted documents, select **Yes** next to **Only OCR Production Documents Containing Redactions**.

   Note: OCR processes original images and production images, including burned-in redactions from the production process. OCR does not run on native files. Productions where redactions were applied directly to a PDF are not processed.
3. Click **Save** on the OCR Set.
4. On the OCR console, click **OCR Documents** to start the job.
5. When the OCR job is complete, the OCR text becomes ready to export.

24.7.3 Exporting a production

You can use Import/Export to export a production set load file out of Relativity aiR. For details, see the Admin Guide.

25 Pivot

Using Pivot, you can quickly analyze your workspace data to identify trends or patterns. You can use Pivot to summarize data in tables or charts, simplifying the analysis process. You can also create ad hoc Pivot reports using the options available on the Pivot menu.

To generate a Pivot report, you specify a field for grouping data totals and further characterize this data by selecting a secondary field. The Pivot grid displays your results in a table format that you can customize for more convenient viewing. See Running Pivot reports.

System admins or users with the appropriate permissions can create custom Pivot profiles that you can reuse on multiple data sets. You can configure these profiles with field information and formatting for charts, including line, pie, and bar graphs.

Note: Relativity does not support Pivot On or Group By for Long Text fields due to the performance impact. However, you can create a Pivot on any Relativity field that is enabled for Group By or Pivot On even if that field doesn't appear in the current view.

25.1 Pivot profiles

Using pivot profiles, you can create, save, and edit custom pivot settings to use at any time. Once saved, these profiles are accessible via a drop-down menu in the upper-right corner of the item list.

Pivot profiles include configured settings for the Group By, Pivot On, and Date fields, as well as the chart formats. When you select a profile, the fields in the Pivot menu automatically populate with predefined values. You can modify these values to run additional pivot reports. Use the Save button to save any updates to the preexisting profile or use the Save As button to create a new pivot profile.

If you create a pivot without selecting a profile, you can click **Save** to make the active settings into a profile. The pivot profile does not save the documents associated with it.

Note: You can't create or edit pivot profiles unless you have the required permissions.

25.1.1 Creating or editing a pivot profile

Perform the following steps to create or edit a pivot profile.

1. Navigate to the **Pivot Profiles** tab.
2. Click **New Pivot Profile**.
   The Pivot Profile Information form appears with required fields in orange.

   Note: Only fields that have been Pivot-enabled will be available to select in this form.
3. Complete the fields on the Pivot Profile Information section.
   - **Name**—the name of the profile. You may want the name to reflect fields on which you pivoted.
   - **Object Type**—click **Select** and choose the object type you would like this profile to appear under.
     - **Display**—select which of the three possible Pivot display types you want to be used to represent your profile in the item list:
       - **Pivot Grid**—designates the grid as part of the profile display.
       - **Pivot Chart**—designates the chart as part of the profile display.
       - **List**—designates the list as part of the profile display.

- **Group By**—click **Select** and choose the field you want to act as your Group By value in your profile. Only fields that are Pivot-enabled on the Field page are available in this list.

  Note: We do not recommend selecting long text fields with the Group By field due to the performance impact. For more information, see Pivot.

  - **Group By Date**—choose a method for providing the date values for the Group By field:
    - **Date**—displays the date with day, month, and year.
    - **Year**—displays only a year value.
    - **YearMonth**—displays the year and month values.
    - **Week**—displays week values.
    - **TwoWeeks**—displays every two weeks values.
- **Pivot On**—click **Select** and choose the Pivot On field in this profile. Only fields that are Pivot-enabled on the Field page are available in this list.

  Note: We do not recommend selecting long text fields with the Group By field due to the performance impact. For more information, see Pivot.

- **Pivot On Date**—provides the same dates for the Pivot On field as found above on Group By, with the addition of the following:
  - **Month**—displays only a month value. This option is only available in Pivot On if your Group By field is also a date.
- **Page Size**—determines the number of sets per page in a pivot chart or graph. Depending on the display specifications you set, you may want to enter a low value.

4. Complete the fields on the Chart Options section.
   - **Chart Type**—determines what kind of chart is used to represent the profile in the item list:
     - **Bar**—represents values in bar form.
     - **Pie**—represents values in pie form.
     - **Line**—represents values in line form.
     - **Table**—represents values in table form.
   - **Chart Orientation**—determines how the chart is positioned. There are two options:
     - **Horizontal**—arranges values horizontally.
     - **Vertical**—arranges values vertically.
   - **Sort On**—determines the basis on which the chart information is sorted. There are two options:
     - **Grand Total**—sorts by the total.
     - **Group By Field**—sorts by the Group By field you specified.
   - **Sort Order**—determines the order in which records are sorted. There are two options:
     - **Ascending**—sorts starting with the last record and ending with the first.
     - **Descending**—sorts starting with the first record and ending with the last.
   - **Switch Series**—switches the Group By and Pivot On fields' positions.

- **Toggles**—configure additional chart instructions. The options are:
  - **Show Grand Total**—toggles the display of grand total in the pivot chart. This value can help add context, but may throw off the scale of the pivot chart and reduce readability.
  - **Show Legend**—toggles the display of the Pivot Chart legend. This information can often be intuited from looking at the chart. If not, it can be added.
  - **Show Blank Values**—toggles the display of blank values in the chart.
  - **Show Labels**—toggles the value count labels on pivot charts.
  - **Rotate Labels**—rotates the group by labels at a 45 degree angle. This can help readability in fields with many values.
  - **Stagger Labels**—another option to improve readability of group by values. Stagger labels varies the horizontal position of the labels to improve readability.
  - **Show Sub-Chart**—toggles the display of sub-chart in bar chart, stacked bar chart, and line chart.

5. Click **Save**.

25.2 Running Pivot reports

Note: To enable the Add Widgets button and Pivot functionality for an Relativity Dynamic Object (RDO), you must select Enabled for the **Pivot** property in the Object Type Information section for the object.

The Pivot menu displays options to run reports on pivot-enabled fields in views and saved searches.

25.2.1 Pivot color map

The Pivot color map has been expanded to include 14 colors. When a chart is created, the color map checks to see if there are already colors assigned to a value in the chart. If there are assigned colors, the chart will maintain those colors. If not, a new color will be assigned for that value to help maintain color consistency.

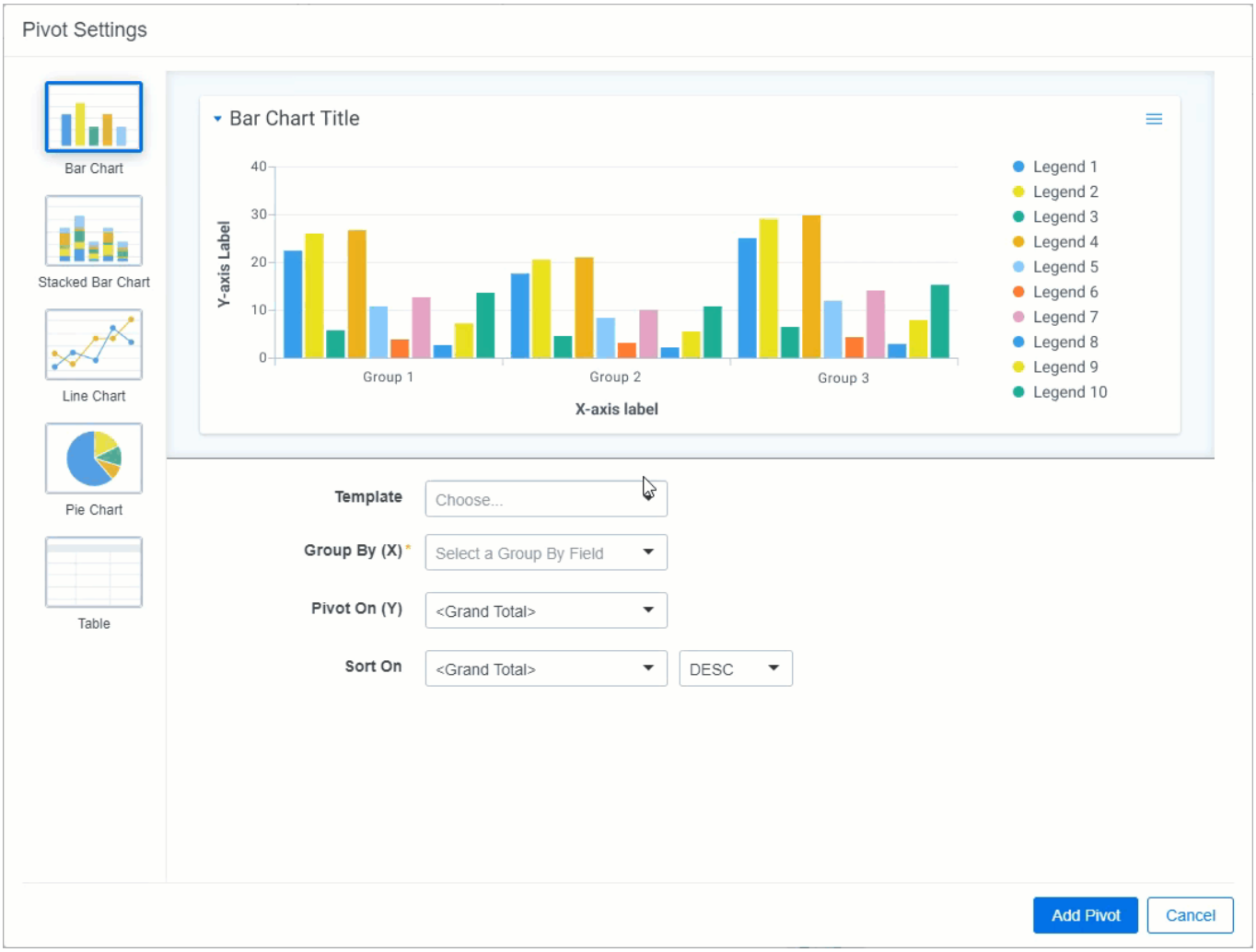
The following colors are in the color map:

#0AA7E8	#5F6EF7
#EDE500	#A3EE02
#0ABB94	#F66084
#EDAF02	#02C539
#82CEF8	#8294F8
#FF702E	#ECAAAA
#E09BC4	#0383CB

25.2.2 Adding a Pivot widget

To add a new pivot chart to a dashboard:

1. Click **Add Widget**, and then select **Pivot** from the drop-down menu.
2. Select the desired chart type by clicking on its thumbnail.



3. Perform one of the following to define settings for your Pivot widget:

Note: If you would like to select a Group by (X) or Pivot On (Y) field that does not have the Enable By option enabled, click on either **Group by (X)** or **Pivot On (Y)**, hover your cursor over desired field in the list, and click the **Enable** icon on the right side of the row. Click **Yes** to allow the field to be used in pivots and select that option for either Group by (X) or Pivot On (Y).

a. Select an existing Pivot profile from the **Template** drop-down menu. The Group By (X) and Pivot On (Y) fields populate with the settings defined by that Pivot profile.

Note: You can select an existing Pivot profile, then modify the settings in the Group By (X) and Pivot On fields. None of your changes are saved to the Pivot profile unless you save your new profile. See Pivot options on the next page.

OR

b. Select a field from the **Group By (X)** drop-down menu to define the horizontal axis of the pivot report.

c. (Optional) Select a field from the **Pivot On (Y)** drop-down menu to break down the totals that appear in each row. This acts as the vertical axis of the Pivot report.
If you select a date field in either the Group By (X) or Pivot On (Y) field, the **Date** drop-down menu displays in the same row as that field.
Select the desired date option:

- **Every Day** - summarizes on each day.
- **Every Week** - summarizes every week.
- **Every Two Weeks** - summarizes every two weeks.

  Note: If **Every Week** or **Every Two Weeks** is selected, the results are displayed from Sunday through Saturday.

- **Every Year** - summarizes on each year.
- **Every Month** - summarizes on each month.

d. (Optional) When you select a Group By (X) or Pivot On (Y) field, the Group By Results Returned field displays underneath. The Group By Results Returned field allows you to specify the number of results that will be returned. From the drop-down menu, select All, Top, or Bottom and in the field to right of the drop-down menu, enter the number of results you'd like to see displayed in the Pivot. For example, you can set the Pivot to display the top ten responsive designations for each custodian.

e. (Optional) After setting the Group By (X) and Pivot On (Y) fields, you can select a field from the **Sort On** drop-down menu and then select a sorting method, which determines how the displayed values for the selected field will be sorted on the screen.

4. Click **Add Pivot**.

The Pivot widget now appears on your Dashboard. Each other panel on the page is automatically re-sized or moved to accommodate the new widget.

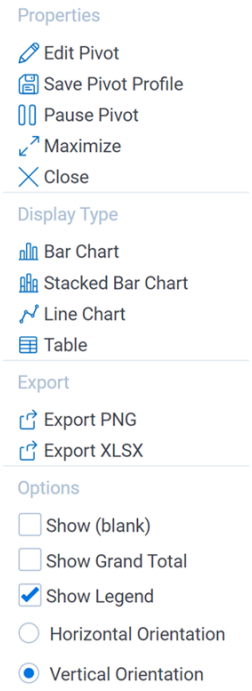
You can size and move panels to create the configuration you prefer. Click and drag to zoom in on the Pivot display. You can hover over any item to get a specific count for that item or click any item to drill down and view more information for that specific item.

Note: Click the value name in the legend to toggle it on and off.

25.2.3 Pivot options

Once you've added a Pivot widget to your Document list page, you can configure settings for the Pivot. Click the **Toggle widget menu** icon at the top right of the Pivot widget to display the Pivot options pane.

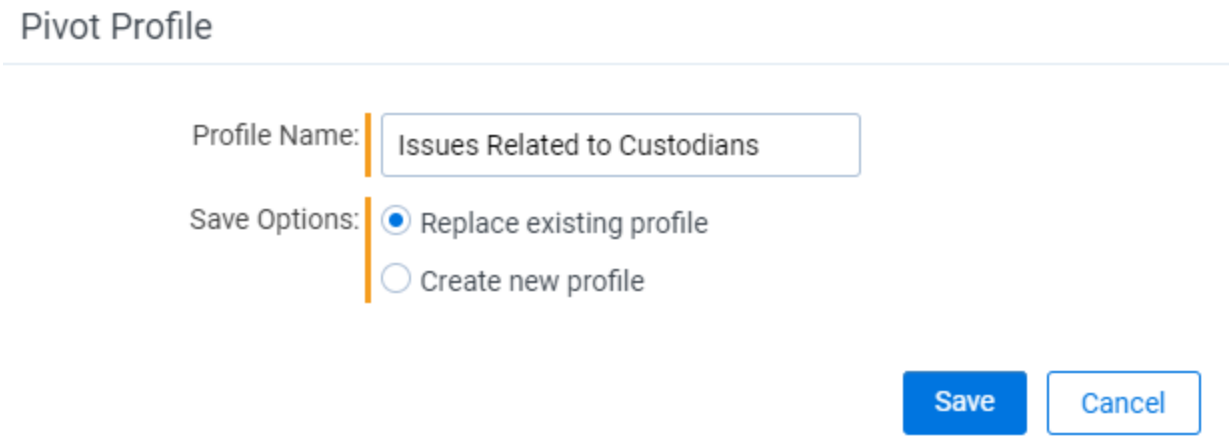
The Pivot options pane has 4 sections: Properties, Display Type, Export, and Options.



25.2.3.1 Properties

From the Properties section, you can edit the Pivot, save a Pivot profile, maximize the Pivot widget, or remove the widget.

- **Edit Pivot** - Displays the Pivot Settings window in which you can edit the Pivot settings.
- **Save Pivot Profile** - Displays the Pivot Profile window in which you can replace or create a new profile.
  - To replace the selected Pivot profile with the current settings, leave the default name in the Profile Name field and select **Replace existing profile**.
  - To create a new Pivot profile with the current settings, enter a new name in the Profile Name field and select **Create new profile**.



- **Pause Pivot** - Select to freeze the content in this pivot so that the information displayed is not affected by searching or filtering the document list. When a pivot is frozen, a paused message displays in the widget to help you track its status. You can unfreeze a pivot by clicking the **Resume Pivot** button in the widget. Once a widget is resumed, a search or filter must be applied to update the information displayed in the pivot.

- **Maximize** - When you maximize a widget, it takes over the whole Document list screen. To restore a maximized widget to the size it was before you maximized it, click the icon in the upper right and select **Restore**.
- **Remove** - Click **Remove** to delete the widget.

25.2.3.2 Display type

From the Display Type section on the Pivot options pane, you can change the display type for the Pivot. Select from the following:

- Bar Chart
- Pie Chart (available when you select only a Group By (X) value)
- Stacked Bar Chart (available when you select both a Group By (X) and Pivot On (Y) value)
- Line Chart
- Table

25.2.3.3 Export

From the Export section on the Pivot options pane, you can export the Pivot to one of the following formats:

- **Export PNG** - exports the chart as a PNG image file and automatically downloads it locally.
- **Export XLSX** - exports the chart as a Microsoft Excel Document where you can modify and configure the chart using Excel's built in chart functionality.

25.2.3.4 Options

From the Options section on the Pivot options pane, select the checkboxes to display blank values, show grand total, display the chart horizontally or vertically (for bar and stacked bar charts), choose whether to display the legend.

25.2.4 Working with Pivot chart results

By default, the Pivot chart displays your results as a graph using the Group By (X) field as the horizontal axis and the Pivot On (Y) field as the vertical axis. To change between different chart or choose different options, click the **Toggle widget menu** icon at the top right of the pane, then select a chart type from the Display Type section.

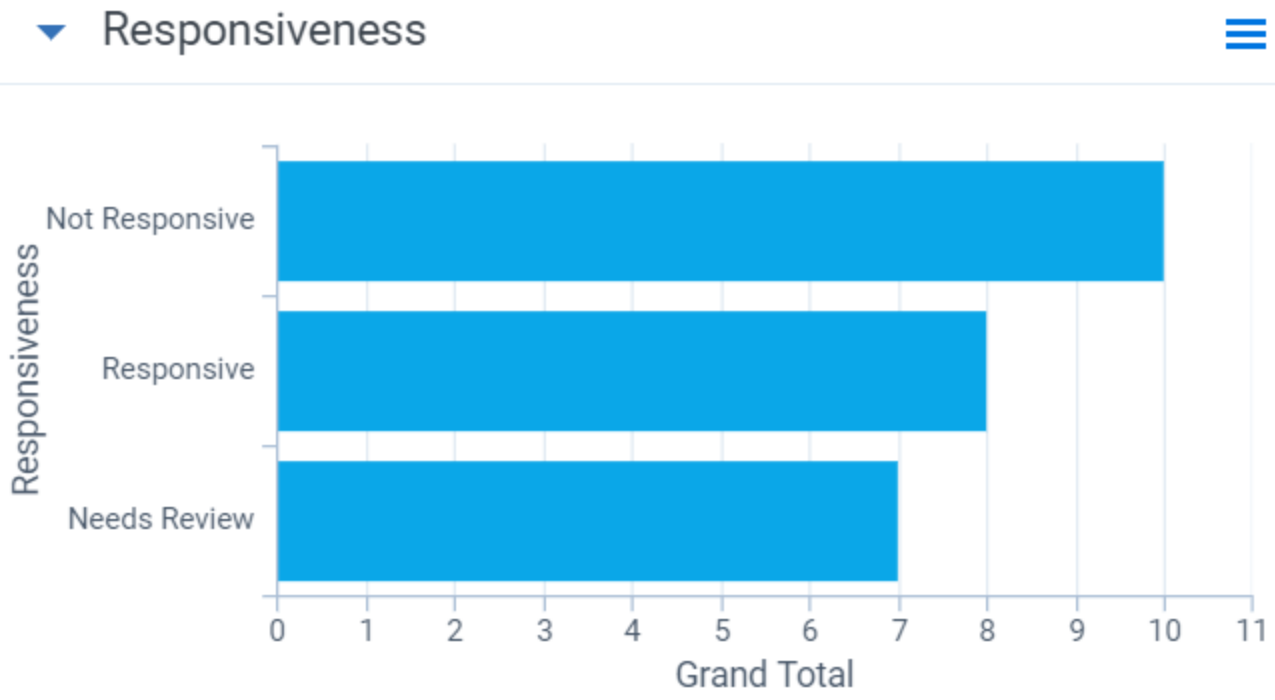
You have the following options:

- Using bar charts below
- Using pie charts on the next page
- Using stacked bar charts on the next page
- Using line charts on page 430
- Filtering the Document list from a Pivot chart on page 431
- Exporting a Pivot or cluster visualization widget on page 431

25.2.4.1 Using bar charts

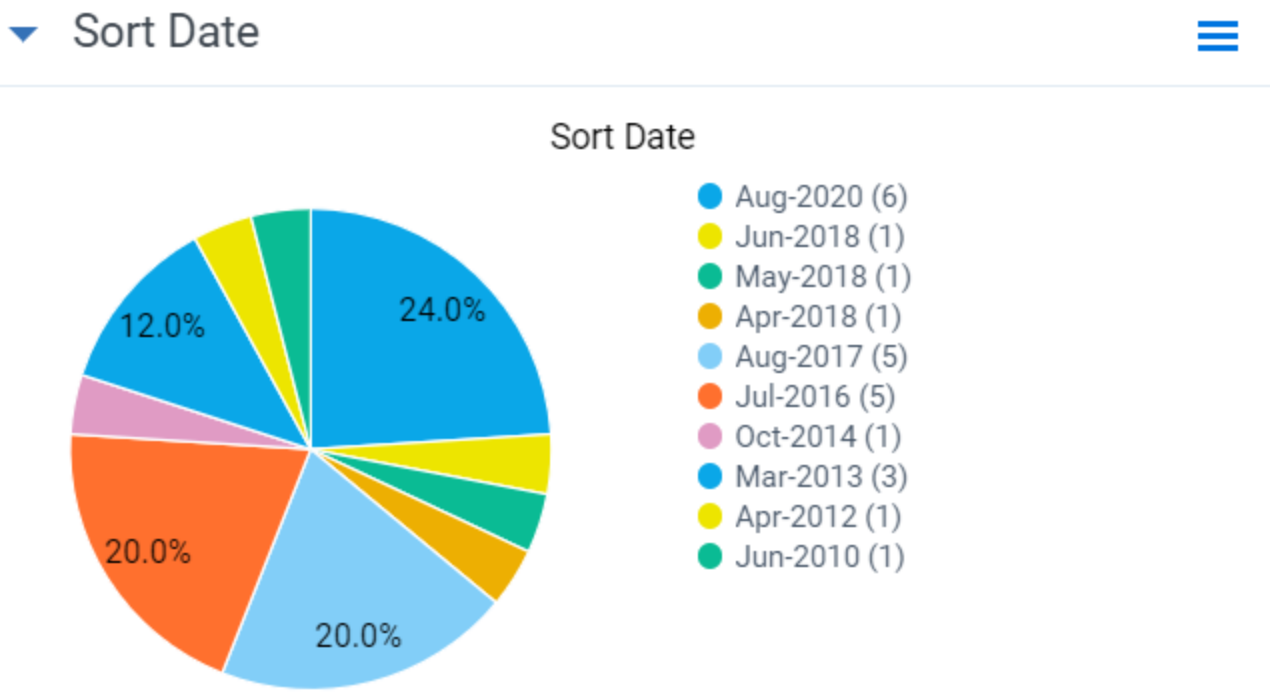
The bar chart displays results in a standard bar format. If you have multiple Pivot On (Y) results for your Group By values, the chart displays those results next to each other. Hover over a specific item to view details about that item. Using the Pivot options pane, you can select whether to display the chart vertically or horizontally.

You can click on the circle on either end of the slider to determine how zoomed in or out the bar chart is. Click on the circle within the chart to zoom back out.



25.2.4.2 Using pie charts

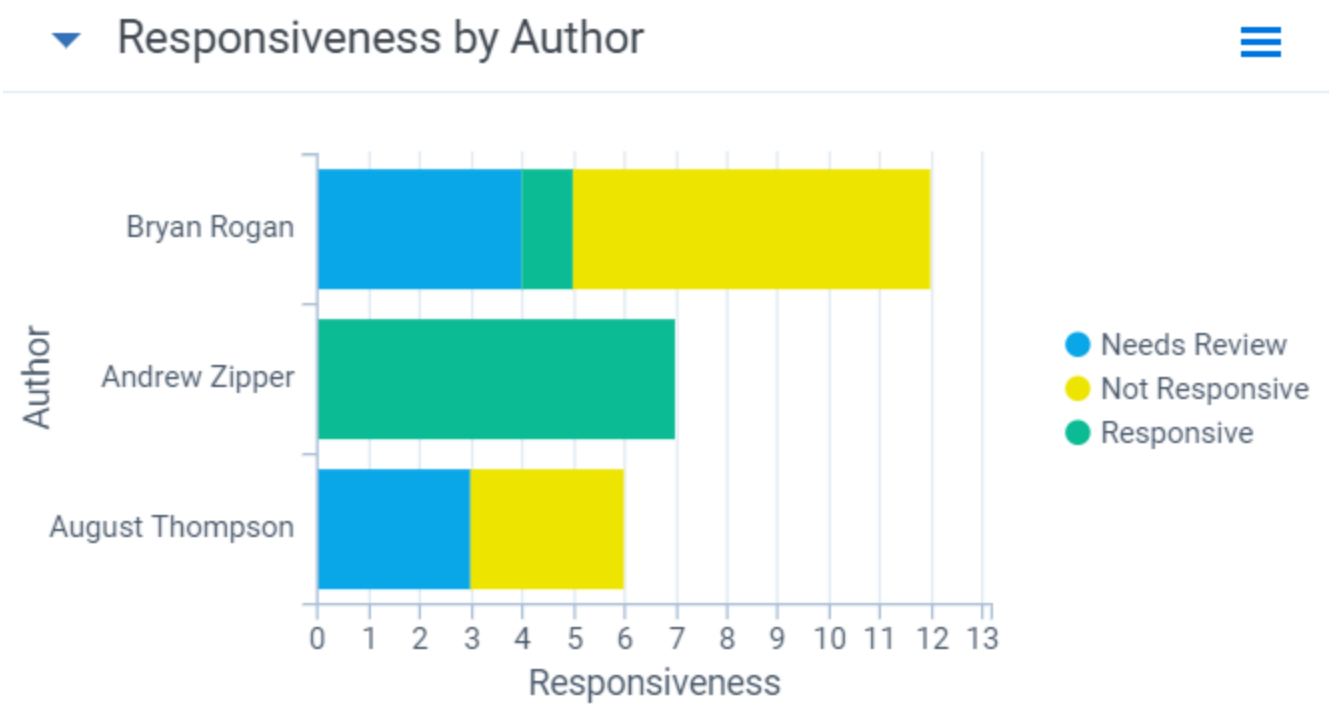
The pie chart displays results in a standard pie format. Hover over a specific item to view details about that item.



25.2.4.3 Using stacked bar charts

If you have multiple Pivot On (Y) results for your Group By (X) values, the stacked bar chart displays those results in a streamlined, comprehensive bar. Hover over a specific item to view details about that item. Using the Pivot options pane, you can select whether to display the chart vertically or horizontally.

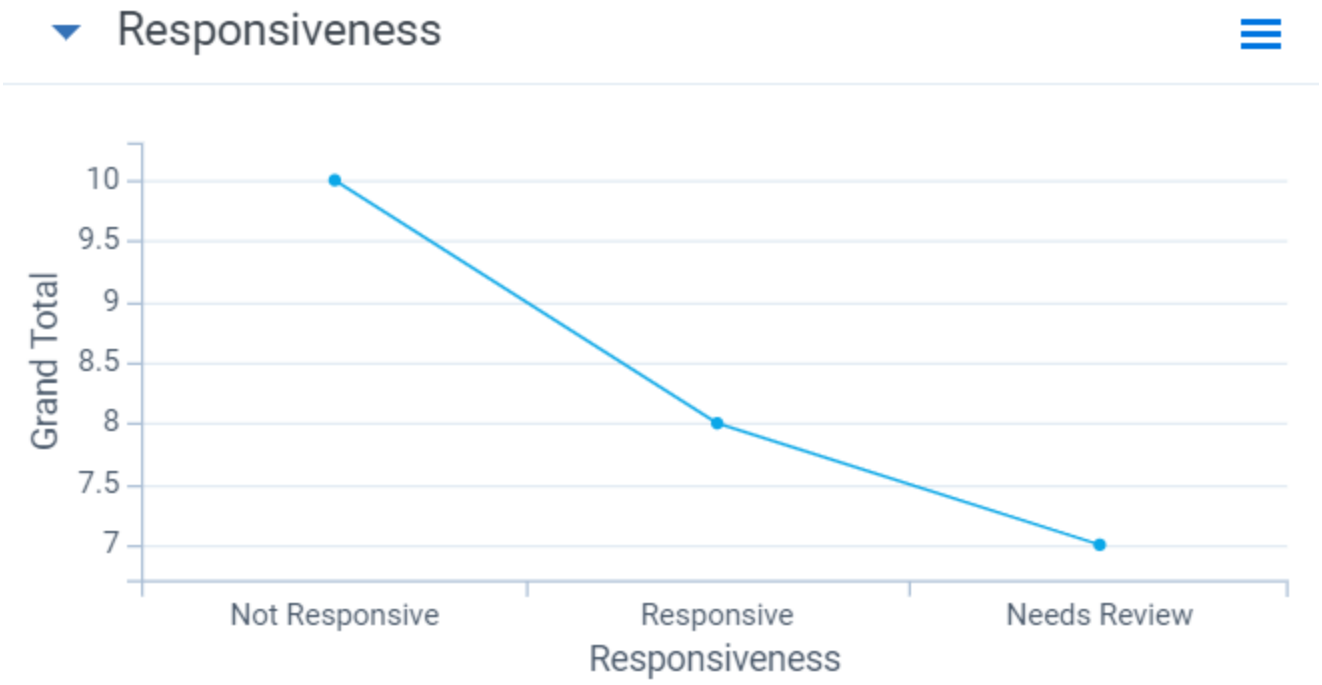
You can click on the circle on either end of the slider to determine how zoomed in or out the stacked bar chart is. Click on the circle within the chart to zoom back out.



25.2.4.4 Using line charts

The line chart displays results in a standard line format. Hover over a specific item to view details about that item. You can also drag and drop a gray box on the smaller version of the line chart above the legend to zoom in on particular areas of interest on the chart.

You can click on the circle on either end of the slider to determine how zoomed in or out the line chart is. Click on the circle within the chart to zoom back out.



25.2.4.5 Filtering the Document list from a Pivot chart

Using any chart type, you can click any item to view more information. From this modal, you can select Mass Edit to launch the mass edit operation for the related object. You can double-click on an item to filter the Document list so it only displays the results from that item. To activate multi-select mode and select multiple ranges of values for bar and pie charts, use **Ctrl + Click**. To select a range of points on a line chart, click and drag.

25.2.4.6 Exporting a Pivot or cluster visualization widget

Use the Pivot Options pane for the widget to save the information outside of Relativity. You can select from the following options:

- **Export PNG** - exports the widget as a PNG image file and automatically downloads it locally.
- **Export XLSX** - exports the widget as a Microsoft Excel Document where you can modify and configure the chart using Excel's built in chart functionality

> **Note:** Exporting to Excel functionality does *not* require Microsoft Excel to be installed (except for viewing of the exported file).

To export a widget:

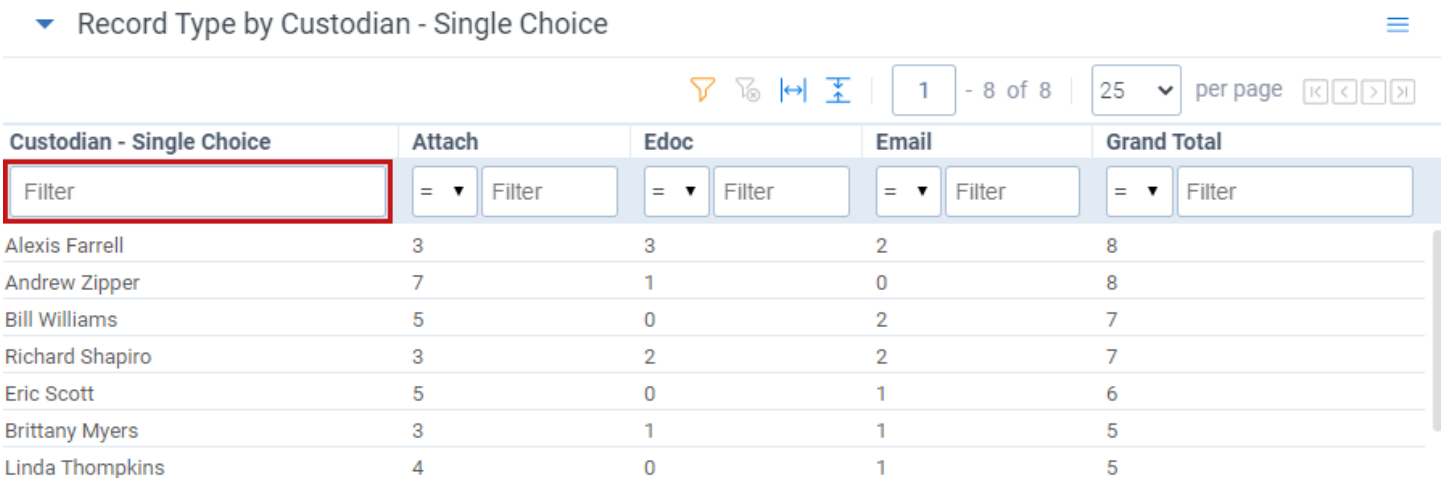
1. Click the **Toggle widget menu** icon at the top right of the relevant widget to display the options pane.
2. Select **Export PNG** or **Export XLSX**. The generated filed is automatically downloaded locally to your computer.
3. Open the file on your computer to view the result.
4. If you exported the widget to Microsoft Excel, you may use Excel's built in chart functionality to edit the chart and its data as needed.

> **Note:** Please note that you cannot modify cluster visualization widget data in Excel.

Note: If you want to export all the widgets on your dashboard to an Excel file, refer to Exporting a dashboard in the Admin Guide.

25.2.5 Working with Pivot table results

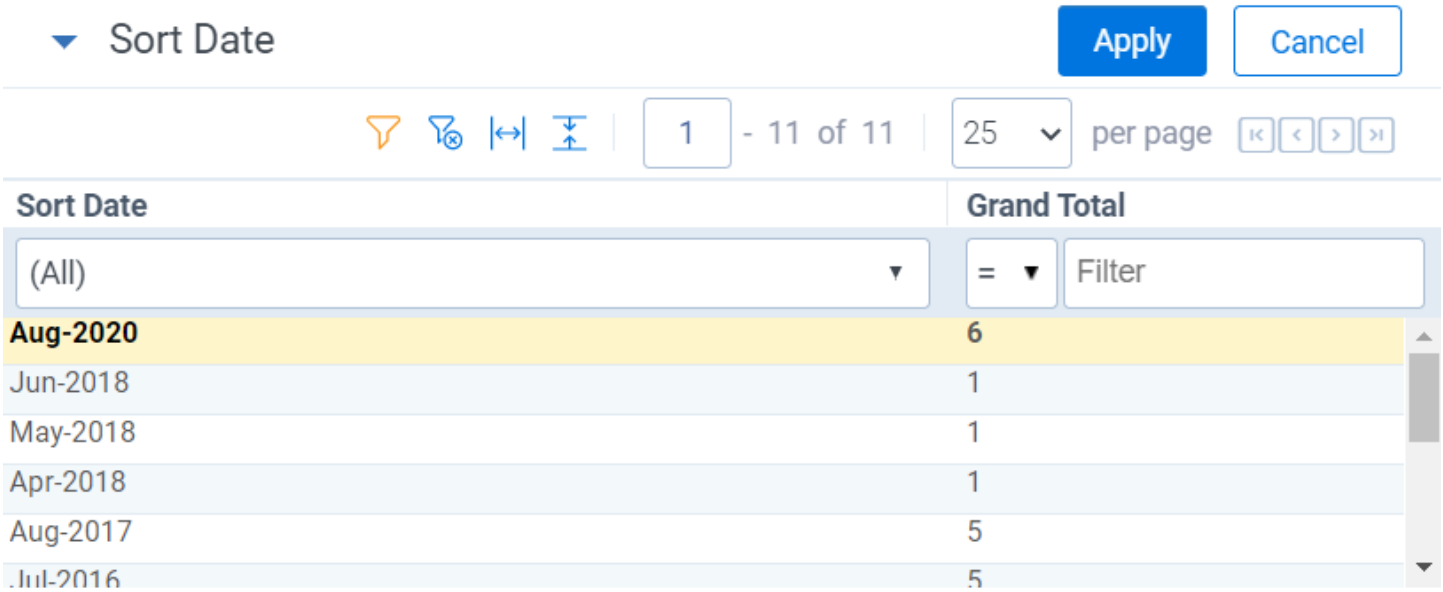
The Pivot table displays your results using the Group By (X) field as rows (horizontal axis) and the Pivot On (Y) field as columns (vertical axis). In the example below, the grid displays rows for each custodian and columns for each record type designation.



From the table results, you can modify the sort order of the results. By default, your Pivot results are sorted in descending order based on the **Group By (X)** field. You can modify the sort order by clicking on any of the column headers. Click once for a descending sort, and twice for ascending.

25.2.5.1 Filtering the Document list from a Pivot table

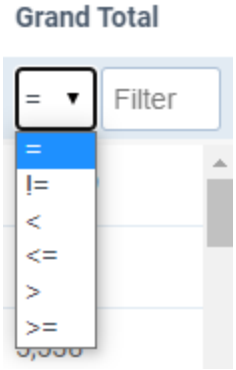
In the Pivot table, click any cell once to highlight it. Click **Apply** to confirm. The Document list refreshes to display only the results from the cell you selected.



To clear the filter, click **Clear All Conditions** in the Search Panel.

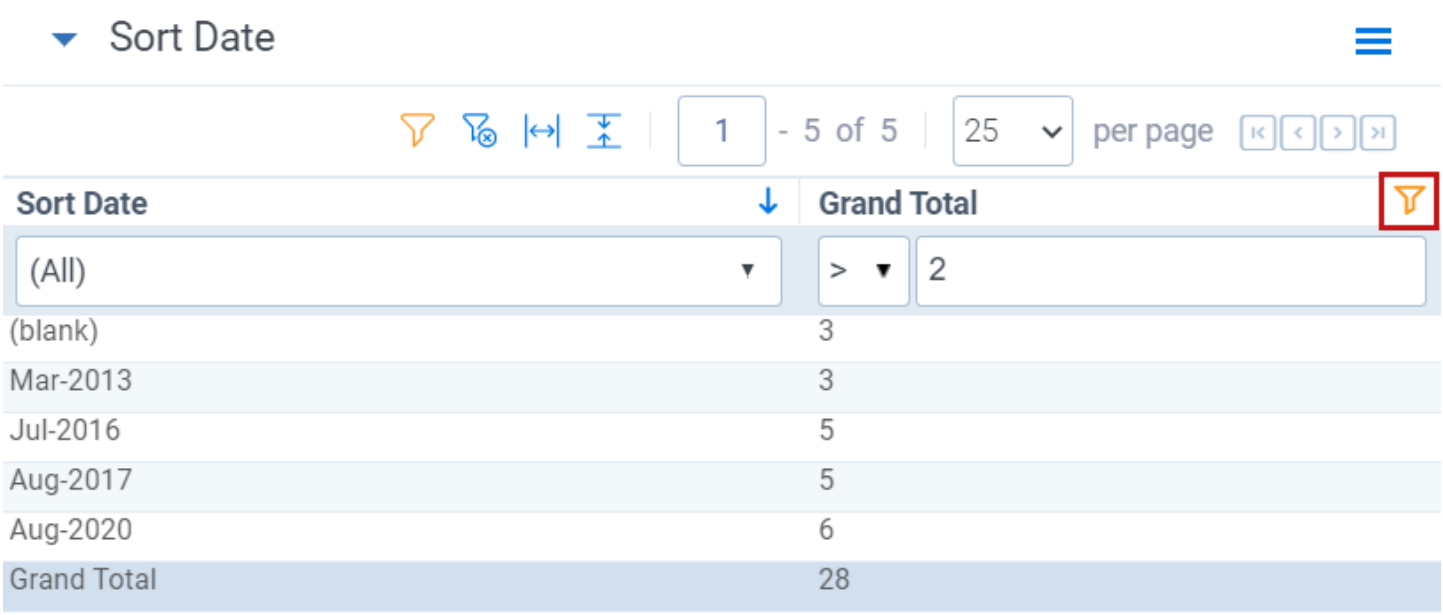
25.2.5.2 Filtering on numeric fields in a Pivot table

In a Pivot table, you can filter on any numeric field to return results that match a certain operator. In the Pivot table display, click the filter icon to apply a filter on a numeric field. From the drop down shown in that field, select an operator:



- = (equal to)
- != (not equal to)
- < (less than)
- <= (less than or equal to)
- > (greater than)
- >= (greater than or equal to)

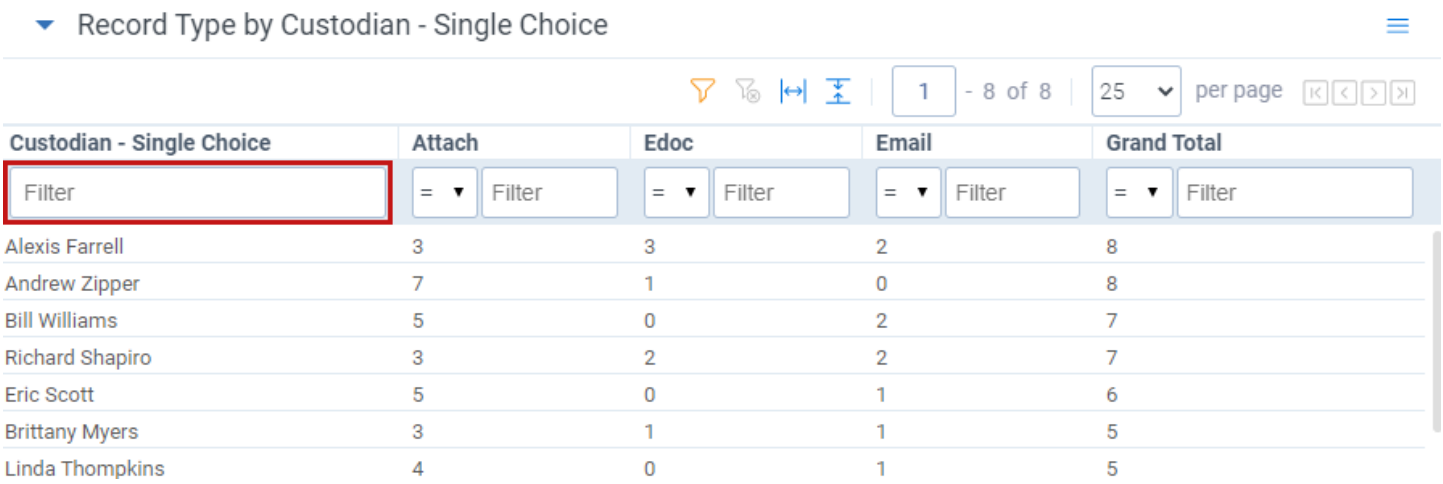
Once you've selected an operator, enter a numerical value in the filter textbox, then click **Enter** to apply the filter. When a filter is applied, the Hide Filter icon appears in the heading of the column.



To clear the filter, click the **Clear Filter** icon.

25.2.5.3 Filtering on the Group By (X) field in a Pivot table

In the Pivot table, you can filter on results from the Group By (X) field. You can limit results to a specific value or range for the field you've selected as the Group By (X) field (in this example, the field Custodian - Single Choice is the Group By (X) field). To filter for specific results on the Group By (X) field, enter a numerical value in the text field at the top of the column.



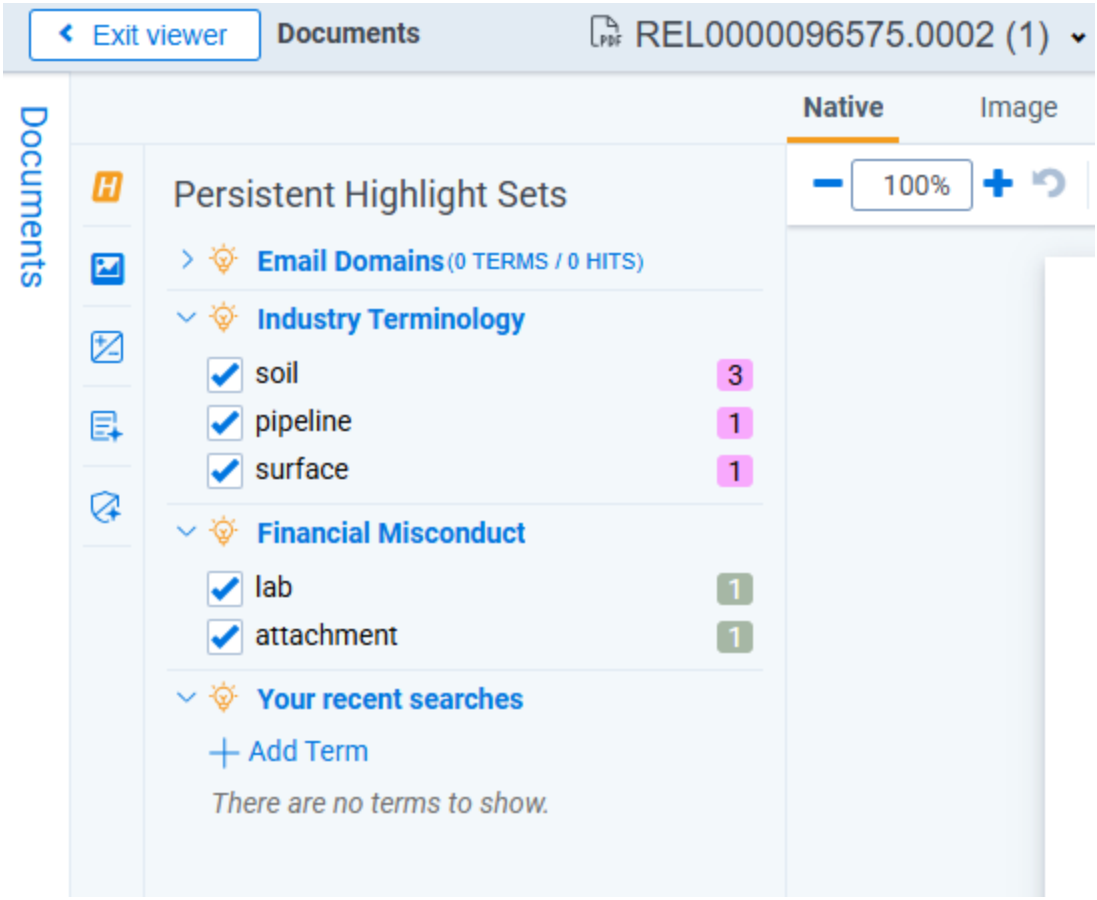
To clear the filter, click the **Clear Filter** icon.

26 Persistent highlight sets

With persistent highlight sets you can configure and apply term highlighting to assist with document review in the Viewer. In the Persistent Highlight Sets pane of the Viewer, you can see all sets saved in a workspace and apply or hide term highlights in the document you are reviewing.

If a document you are reviewing contains any of the terms specified in a set, the list of terms and the number of times they appear in the document appear under the set. If a document contains no terms from the set, you can not expand

or collapse the set in the tree. If the document contains some terms in the set, only the terms that exist in the document appear below the set name.



System admins can control which highlight sets different users see when working within a document. See Workspace security on page 622 Workspace security in the Admin guide.

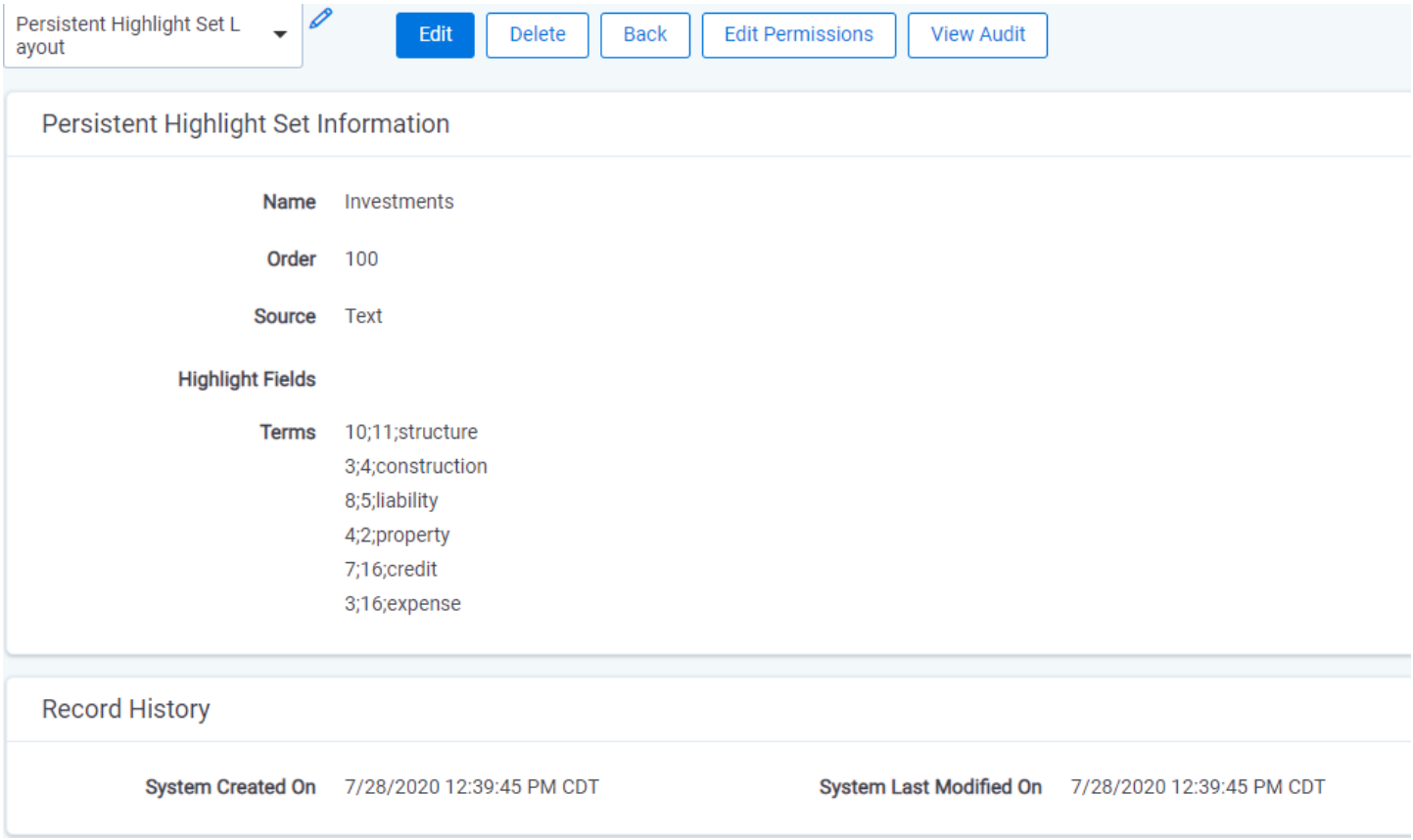
Persistent highlight sets are independent of markup sets. See Markup sets on page 350 Markup sets in the Admin guide.

26.1 Getting started with persistent highlight sets

You create persistent highlight sets in the **Persistent Highlight Sets** tab of a workspace. Each set includes a list of terms populated manually or from a source field in the set configuration. After you create a persistent highlight set, the set and its terms are available in the Persistent Highlight Sets pane of the Viewer.

The following persistent highlight set includes several terms with highlight color-coding. See Color-coding persistent highlights on page 446 for more information.

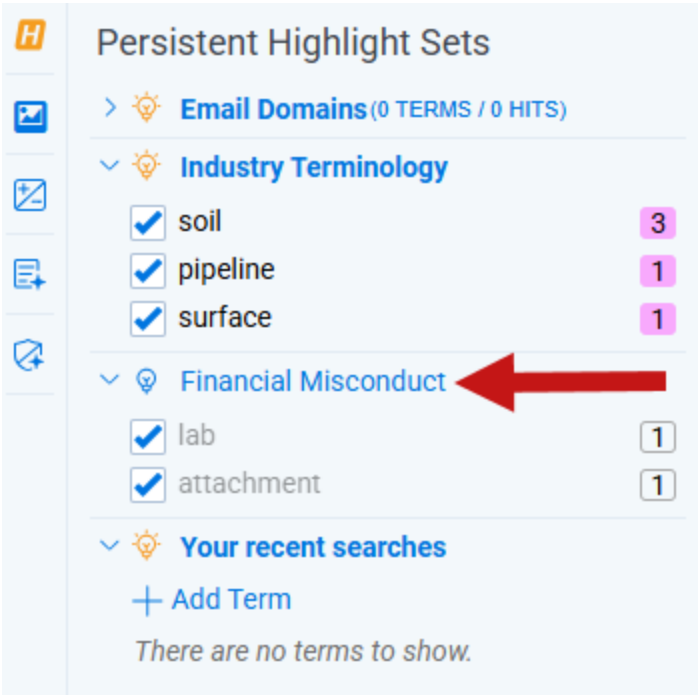
This set is available when a user opens the viewer and any edits made to this set are reflected immediately.



26.1.1 Showing and hiding persistent highlight sets in the Viewer

To view the list of available persistent highlights sets and related terms in the Persistent Highlight Sets pane, click the **Persistent Highlighting** icon in the left drawer.

Click the **Expand** icon next to a persistent highlight set to expand it and show the list of terms from that set found in the document. By default, all persistent highlight sets are enabled in the Viewer, and terms found in a document are selected in the Persistent Highlight Sets pane and highlighted in the document. Click a persistent highlight set's name or the icon to hide all term highlights from the set in the Viewer. When a persistent highlight set's icon is and the terms appear partially transparent in the Persistent Highlight Sets pane, the term highlights for the set are hidden in the Viewer.



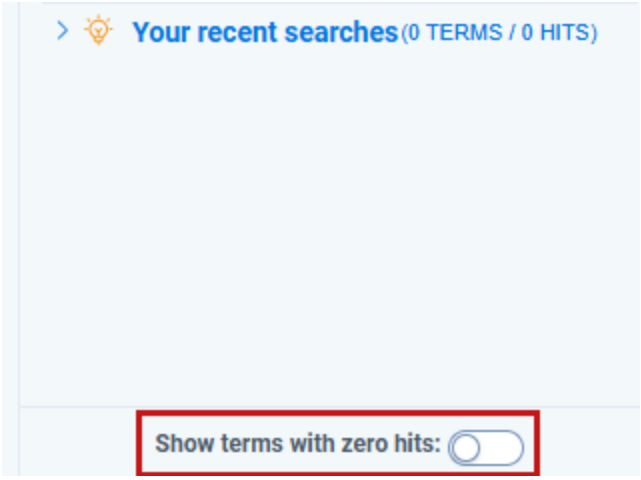
Clear a term's check box to hide its highlights in the Viewer. Select its check box to apply highlighting for the term in the Viewer again.

While using persistent highlight sets, you can determine whether terms that do not have any hits display in the Persistent Highlight Sets pane or not. If the Show terms with zero hits option is enabled, all terms in a persistent highlight set, including those with zero hits display in the Persistent Highlight Sets pane. However, if a field has hits for some Viewers and no hits in others, in the Viewers where there are no hits, the field will display as having zero hits.

If the Show terms with zero hits option is disabled, then any terms in a persistent highlight set that are not present in the current document will not display in the Persistent Highlights Set pane.

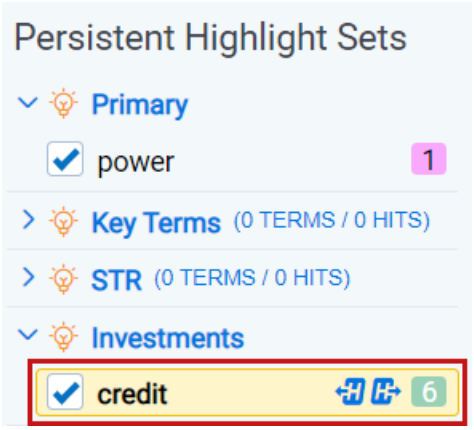
For example, if you created a set named Investments that contains five highlight terms and have the Show terms with zero hits option disabled, only three of the terms show in the pane for a particular document, because the other two terms have no hits and thus, are not present in the document.

Note: The Show terms with zero hits option does not support highlight fields that are based on search term reports. While the persistent highlight set displays in the Persistent Highlight Sets pane, the highlight field terms do not display unless there is at least one search hit regardless of whether Show terms with zero hits option is enabled or disabled.



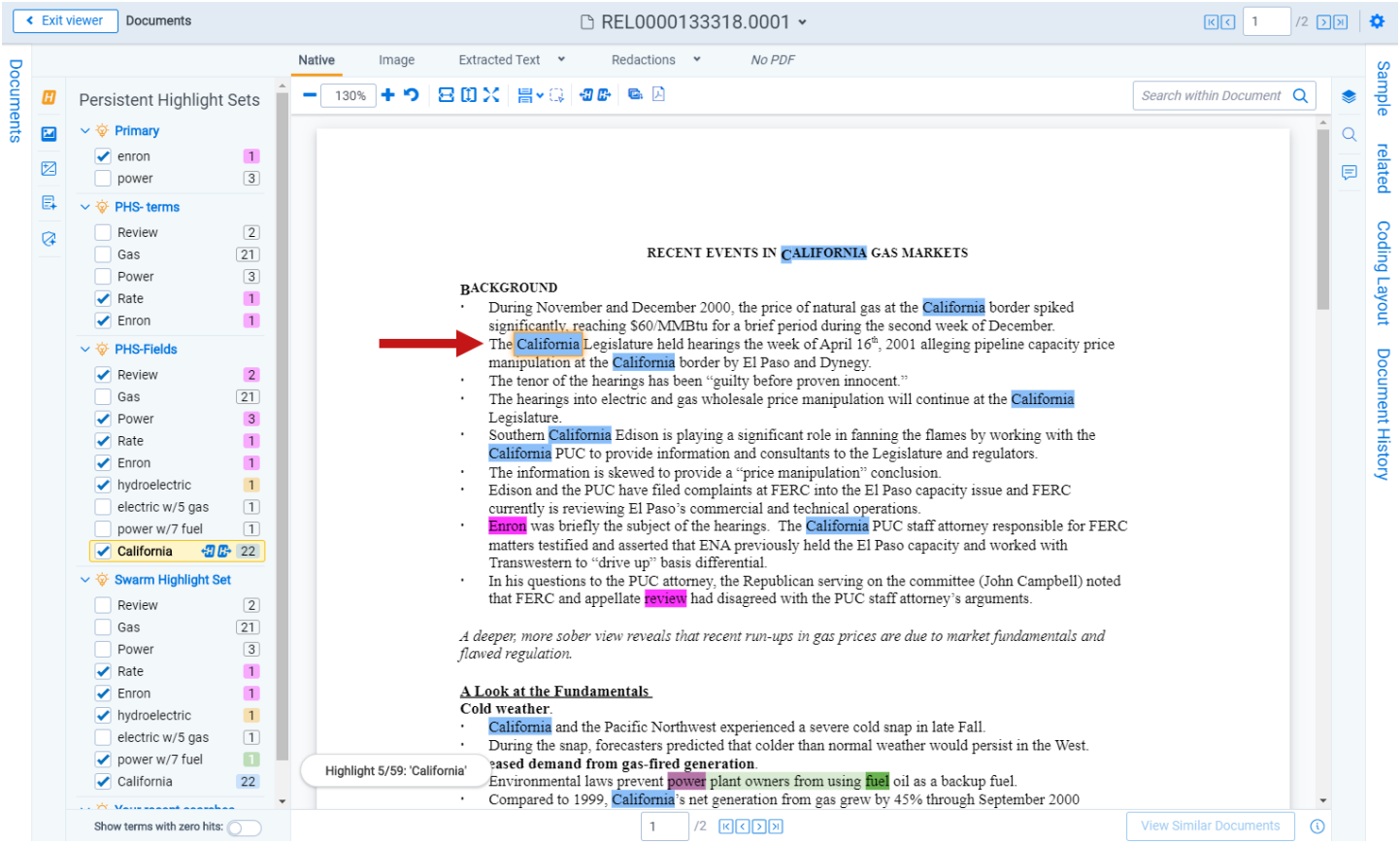
26.1.2 Navigating persistent highlight hits in the Viewer

You can navigate through the hits for a persistent highlight set or for a term while viewing a document in the Viewer. Click on either the persistent highlight set or the desired term in the Persistent Highlight Sets pane and the **Go to Next/Previous Highlights** icons display in the row.

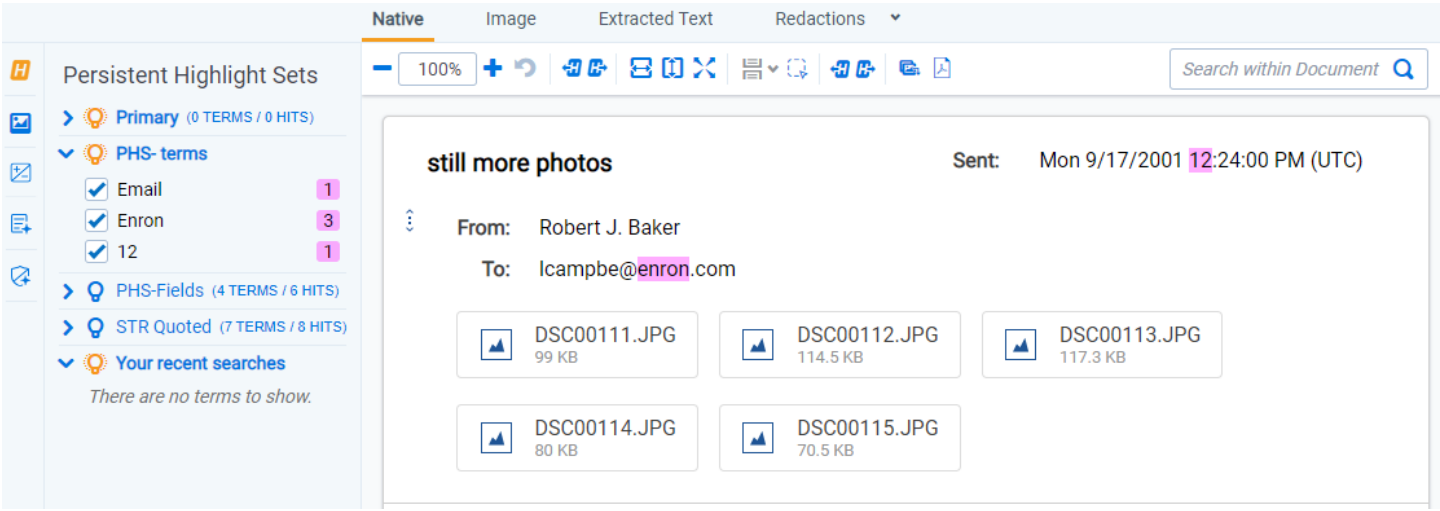


You can use the Next/Previous icons to cycle through the hits for either the persistent highlight set or the highlighted term. Regardless of where you are in a document, when you click the Next icon for the first time, you will be taken to the first highlight in the document for that persistent highlight set or term. Even if you have moved past it while browsing the document.

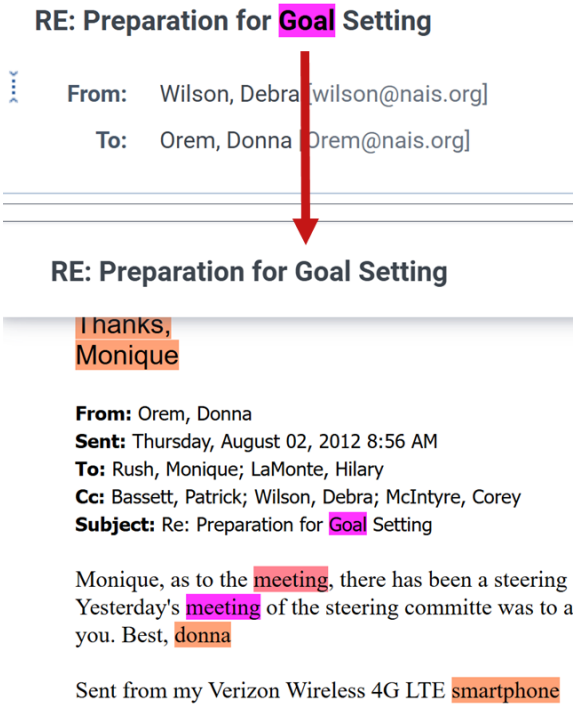
Clicking the Next/Previous icons also emphasizes the actively navigated highlight with an orange glow to help you track which one is active.



When you select a persistent highlight term in the Persistent Highlight Sets pane, in addition to highlighting all instances of that term in the body of an email, the Viewer also highlights instances of the term in the email header.



Note: If there is a highlight in the email header including the email subject, From:, To:, or Date:, the highlight will only display when you are at the top of the document, even though the fixed header continues to display at the top as you scroll down the page.



The number of terms and hits is listed to the left of the persistent highlight set's name. It is possible to have many highlight sets enabled but no highlights appear in a document.

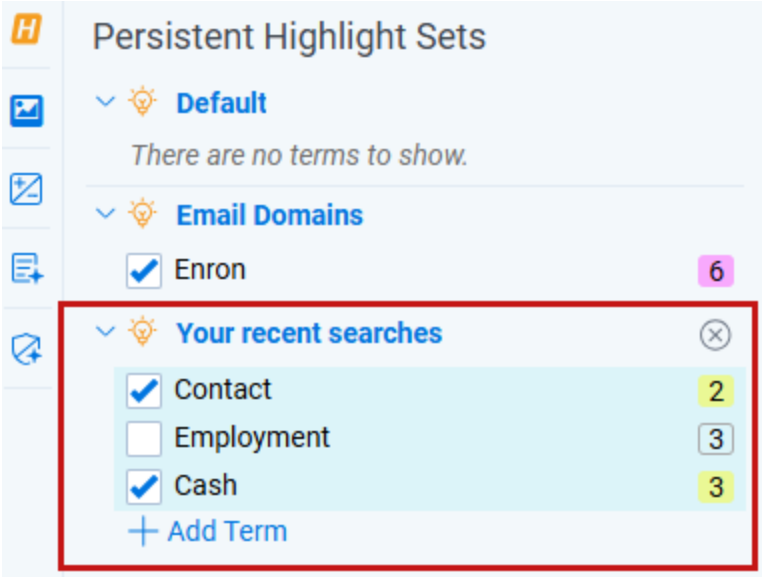
Selections made in the Persistent Highlight Sets pane persist throughout a user's session in Relativity. This includes any of the following changes related to the Persistent Highlight Sets pane in the Viewer:

- Showing or hiding the Persistent Highlight Sets pane.
- Enabling or disabling a persistent highlight set.

- Expanding or collapsing the term list for a persistent highlight set.
- Checking or clearing terms check boxes in a persistent highlight set.

26.1.3 Recent searches in the Persistent Highlight Sets pane

In addition to accessing persistent highlight sets, you can also search for terms and highlight any matches temporarily using the Your recent searches section. You can perform either dtSearch or Keyword searches from this section. dtSearch with persistent highlights does not ignore characters like dtSearch typically does.



You can also search using the search bar on the document list. The search bar lets you choose a search index, find search term matches, and then view matches in the Your recent searches section across different documents. The search term matches stay highlighted while navigating between documents as long as you do not remove the search condition from the search panel or log out of Relativity.



To perform either a dtSearch or Keyword search in the Your recent searches section:

1. Optionally, click on the **Persistent Highlighting** icon to expand the Persistent Highlight Sets pane.
2. Click the **+ Add Term** button.
3. Enter the desired dtSearch or Keyword search terms in the textbox.
4. Click the **Confirm** icon or press **Enter** on your keyboard.
   The Your recent searches section updates with the number of matches and any matches are highlighted in yellow in the current document.

Optionally, you can select a search in the Your recent searches section and use the Next/Previous icons to cycle through the matches. Regardless of where you are in a document, when you click the Next icon for the first time, you will be taken to the first highlight in the document for that persistent highlight set or term. Even if you have moved past it while browsing the document.

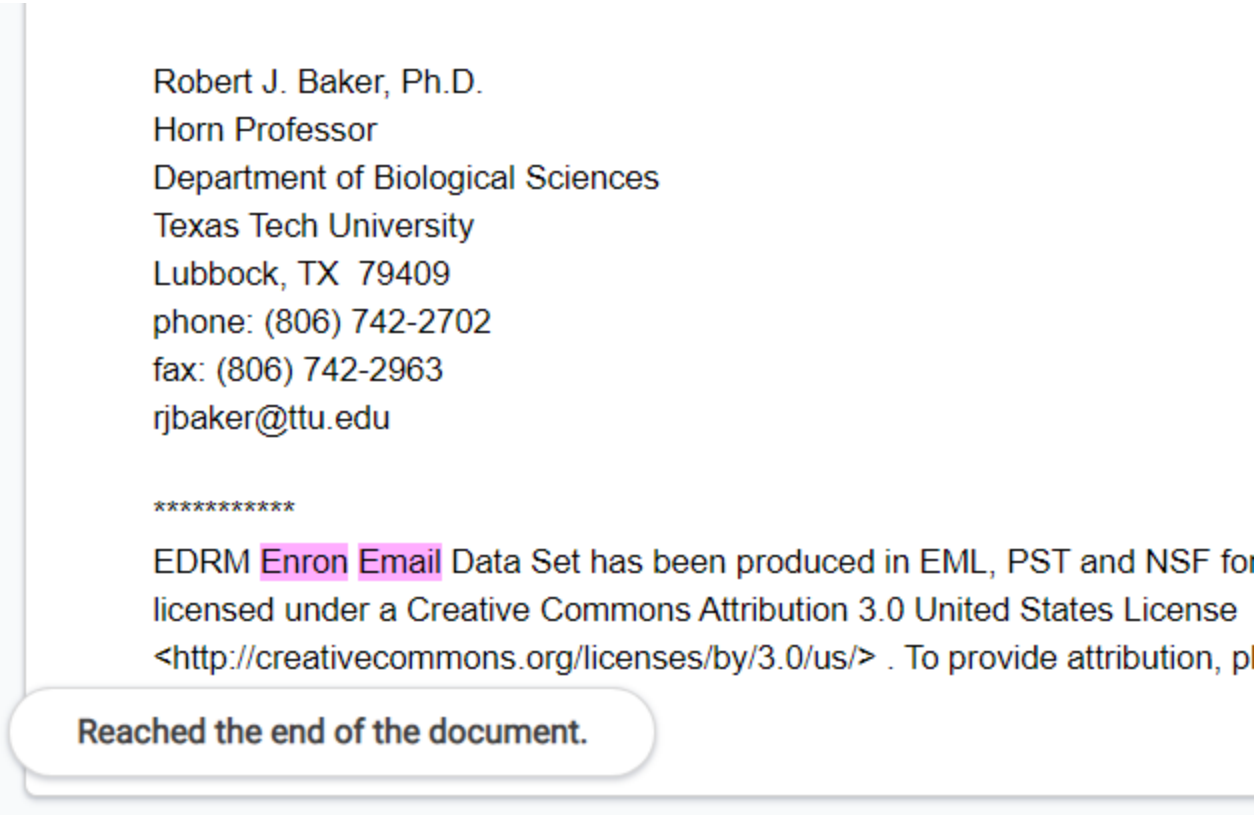
26.1.4 Navigating highlighted terms in the Viewer

To navigate between terms highlighted on a document in the Viewer, use the **Go to Previous Highlight** and **Go to Next Highlight**

icons on the Viewer toolbar.

The **Go to Previous Highlight** and **Go to Next Highlight** icons only navigate between terms enabled in the Persistent Highlight Sets pane.

When navigating through a document's highlighted terms, the following notification displays in the bottom-left to inform you that you have reached the beginning or end of the document and there are no more highlights.



26.1.4.1 Actively navigated and inactive highlights

To support advanced highlights within persistent highlight sets, two types colors can be available in the Viewer - actively navigated and inactive highlights. The colors are the same, but have a different level of opacity. Active highlights are the highlights that the Viewer is focused on. Active highlights are at full opacity and inactive highlights are at a lower opacity level. See Color-coding persistent highlights for more information.

Note: The auto-contrast feature automatically determines the text color based off the background color you select to ensure readability no matter which colors are selected. For example, if the background color is closer to black, the text will automatically be white or if the background color is closer to white, the text will automatically be black.

Note: The opacity level of the highlights for proximity searching and inactive terms can be adjusted by editing the value of the **ViewerHighlightStyleDefault** instance setting.

Color name	Highlight Color	Number
[Default]		0
Black		1
Dark red		2
Dark green		3

Color name	Highlight Color	Number
Dark yellow		4
Dark blue		5
Dark magenta		6
Dark cyan		7
Light gray		8
Gray		9
Red		10
Green		11
Yellow		12
Blue		13
Magenta		14
Cyan		15
White		16
Light green		17
Light blue		18
Light yellow		19
Light purple		20
Light red		21
Light orange		22
Purple		23
Orange		24
Dark purple		25
Dark orange		26

26.1.5 Persistent highlight set behavior across Viewers

Note the following regarding persistent highlight set behavior as the reviewer moves from document to document, changes Viewers, and uses pane toggles:

- Any changes made to a persistent highlight set tree in the panel when the Viewer is undocked, such as terms selected or unselected, will display when the Viewer is docked again.
- A synced standalone Viewer will not display changes made to a persistent highlight set, such as terms selected or unselected, in the pane of the main Viewer. However, Persistent Highlight Sets pane settings remain the same in the standalone Viewer as the reviewer goes from doc-to-doc.
- The Persistent Highlight Sets pane maintains its current state when you swap Viewer panes.
- The Persistent Highlight Sets pane in the Extracted Text Viewer and Native Viewer are independent of each other. A change made to the pane in the Extracted Text Viewer is not automatically reflected when the reviewer switches to the Native Viewer and back.

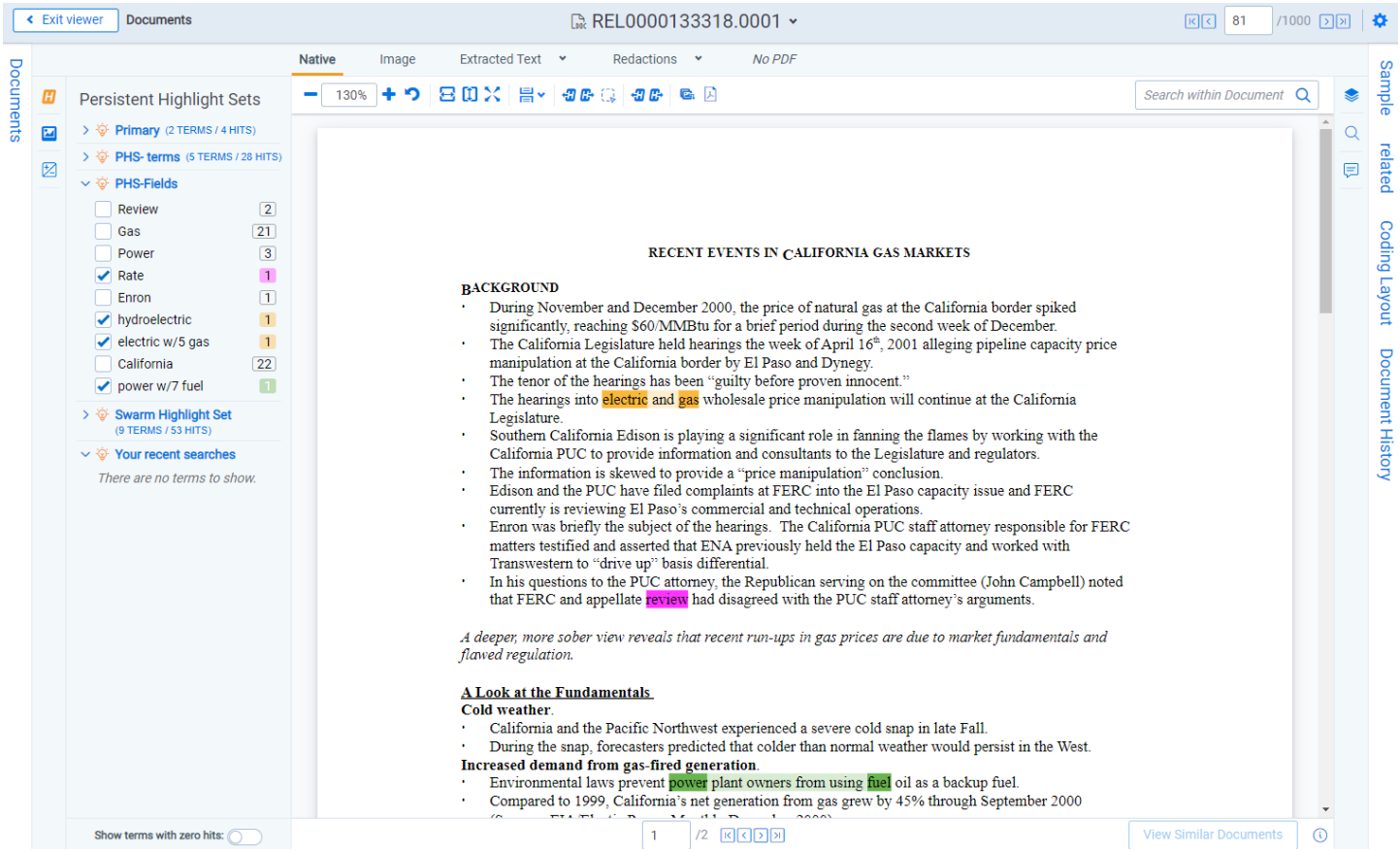
- Advanced persistent highlighting, available when using a search term report as a highlight field source, is only available in the Native and Extracted Text Viewer. See Using the highlight fields source on page 448.

See the Viewer documentation in the Admin Guide.

26.1.6 Persistent highlight behavior

When using a search term report that includes search syntax as a highlights source field, the highlight behavior is more inclusive than using persistent highlight terms. See Using the highlight fields source on page 448.

The different levels of opacity occur on a key term and interval term level. The key terms in the search are high opacity level highlights. The other interval terms picked up with search syntax are highlighted at a lower opacity level. For example, if you use the search "account w/5 cap" the words "account" and "cap" are highlighted with the full opacity highlight. The words between "account" and "cap" will have the lower opacity level highlight.



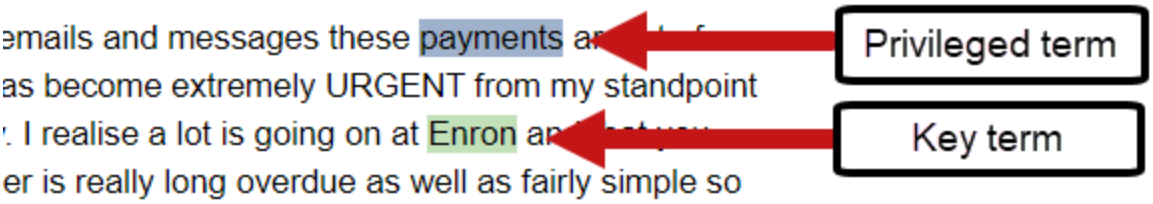
26.2 Using multiple persistent highlight sets

During the course of a review, the number of terms can grow as legal teams learn more about the case and the documents in it. In these cases, it may be beneficial to create multiple highlight sets.

With multiple highlight sets you'll have better organization and control over highlighted terms. For example, you may want to create highlight sets for:

- Key Terms
- Privilege Terms
- Specific Issue Terms, unique terms

You can visually group related terms by assigning a different highlight color to the terms in each highlight set.

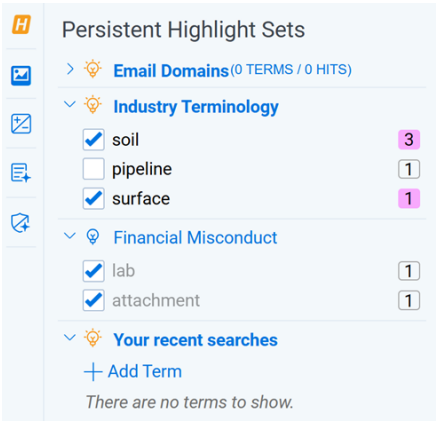


When multiple highlight sets include the same term the colors used in each set will mix together. For example, if a highlight set includes the term "apple" highlighted in blue and another highlight set includes the term "apple" highlighted in red, the highlight color will combine and display as purple in the Viewer. This only applies if both highlight sets are active for the same term.

Persistent highlighting sets and individual terms can be toggled on or off depending on reviewers' preferences or needs. A reviewer can control which sets or terms they have highlighted during review.

Clicking on the light bulb icon for a persistent highlight set enables or disables highlighting for the entire set. The icon indicates a persistent highlight set is enabled in the Persistent Highlight Sets pane. The icon indicates a persistent highlight set is disabled in the Persistent Highlight Sets pane. When disabling a persistent highlight set in the Viewer, terms included in the set aren't highlighted in documents until the set is enabled again.

Clicking a check box activates or deactivates highlighting for an individual term.



Security is another way to control persistent highlight sets. System admins can use object-level security to display only the persistent highlights sets necessary for users to complete their reviews. Limiting the visibility of persistent highlight sets also provides a cleaner interface for reviewers. See Relativity object security on page 671 for more information.

26.3 Performance considerations

Several factors can affect the performance of persistent highlight sets. These factors include individual document size, the number of terms, the types of operators used, and the performance of the local machine. For more information about how to create high performance searches, visit Creating efficient searches for persistent highlighting.

26.3.1 Individual document size

The size of individual documents affects persistent highlighting performance, not the workspace's document count. The larger the document, the longer it takes for persistent highlighting to compare and highlight each term in the document against the term list.

For example, Excel files with many tabs require more time to load. Persistent highlighting searches the contents of each tab, compares each term against the term list, highlights any term matches, then moves to the next tab until it has gone through the entire document. A 500-page document takes much longer to render highlights than a one-page email.

26.3.2 Number of terms

When using the Terms Search option as your source for persistent highlighting, performance can slow down as the list of terms grows. Performance degradation can occur once the list reaches 100 terms, and significant slowness occurs at 500 terms depending on the resources of your local machine. If you have a large list of terms, using Highlight Fields through search terms reports is a better solution.

26.3.3 Types of operators used

Creating efficient searches improves the performance of persistent highlighting whether working with a Terms Search or Highlight Fields. See Creating efficient searches for persistent highlighting on page 451.

26.3.4 Local machine

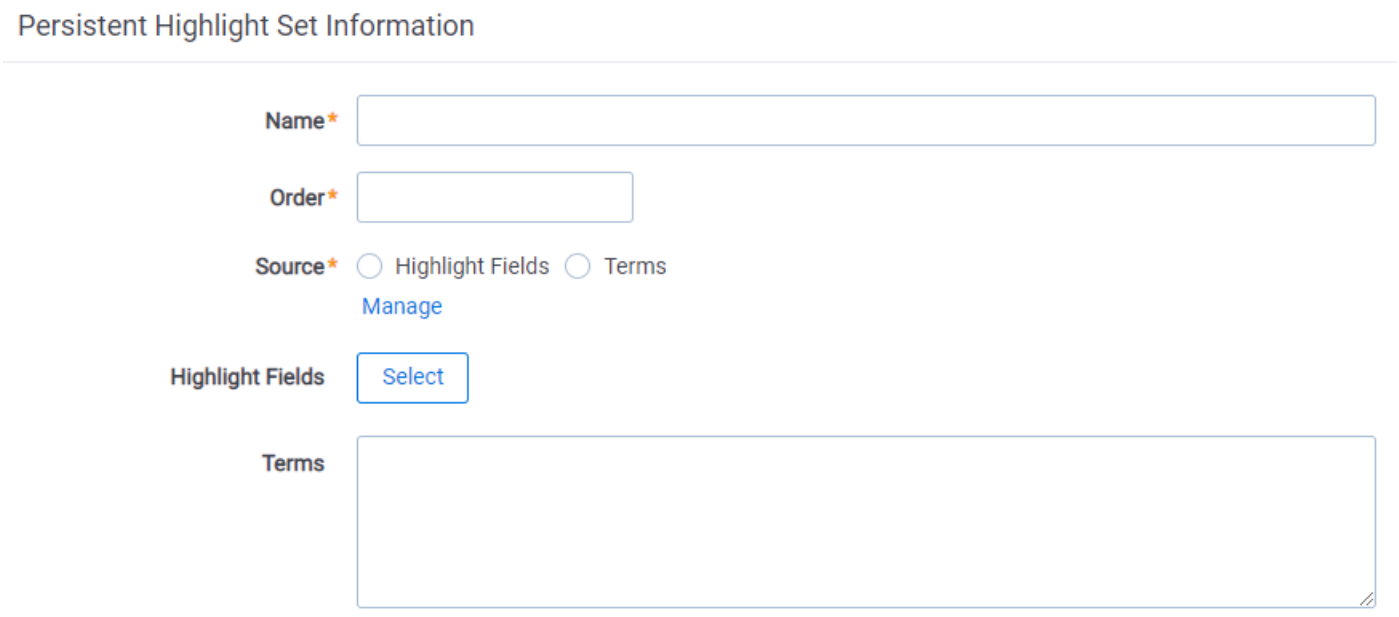
Persistent highlighting is rendered by the local machine, not by the Relativity server. If the resources for the local machine are strained, it will also affect performance.

26.4 Creating persistent highlight sets

To create a new persistent highlight set, follow these steps.

Note: If you plan to use the Source: Highlight Fields, you may need to create a search terms report. For more information, see Using the highlight fields source on page 448.

1. Navigate to the **Persistent Highlight Sets** tab.
2. Click **New Persistent Highlight Set**.
3. Complete all required fields in the Persistent Highlight Set Information section. See Fields on the next page for details.



4. Click **Save**.

Note: Verify that reviewers are not actively reviewing documents when creating persistent highlight sets. Creating persistent highlight sets while reviewers are actively reviewing documents can cause errors.

26.4.1 Fields

Persistent highlight sets include the following fields.

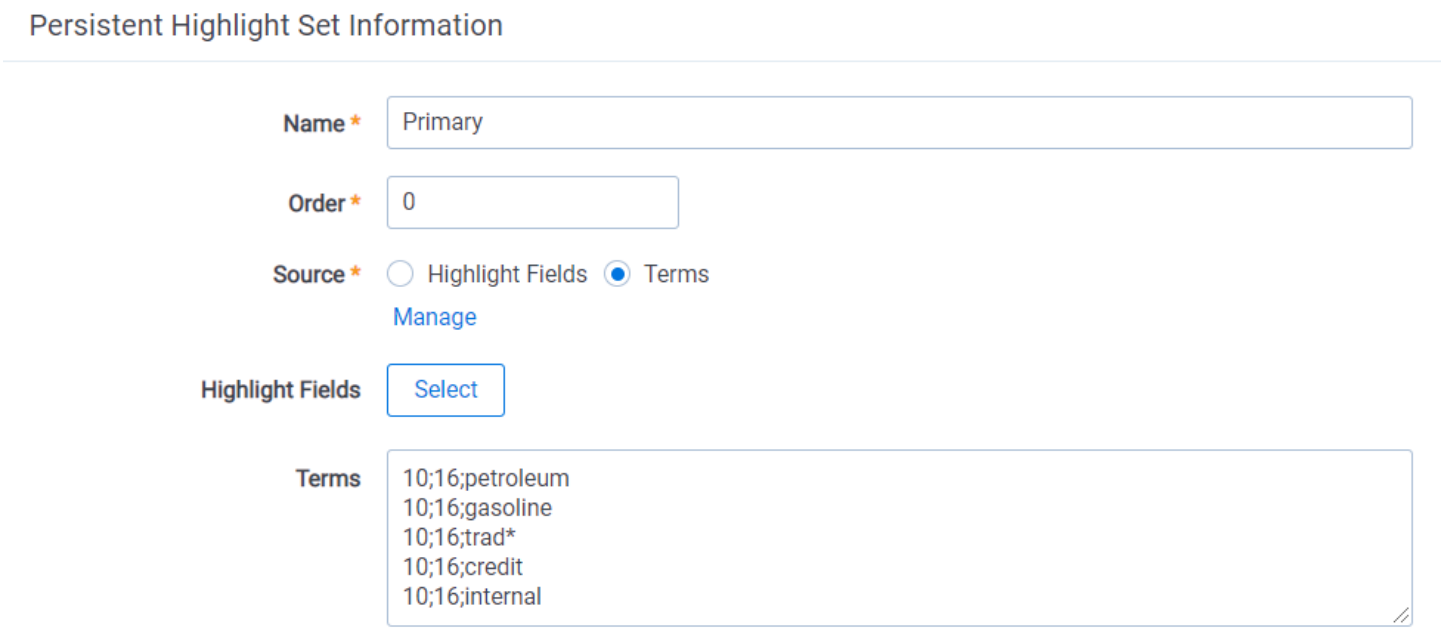
- **Name**—the descriptive name under which you want this set to appear in the Viewer and item list.
- **Order**—the order in which you want this set to appear.
- **Source**—determines the area the set draws from when designating characters to be highlighted and displayed in the Viewer. There are two options:
  - **Highlight Fields**—designates fields as the source of highlighting. Highlight Fields is capable of using dtSearch functionality. Selecting this radio button means you must select a Highlight Field in order to save this set.
  - **Terms**—designates terms as the source of highlighting. Selecting this radio button means you must enter terms into the Terms field below to save this set.
- **Highlight Fields**—choose the field referencing the list of terms to be highlighted. Click the **Select** button to bring up the system view called Field Picker on Persistent Highlight Sets, which displays the Name and Object Type for applicable multiple object fields. It also includes those created by search terms reports. To select the desired Highlight Field, check the field's box, click Add, and click Set. The field displays on the layout. See Using the highlight fields source on page 448.

  Note: If your search terms report is run against a dtSearch index with a customized alphabet file, the hits on the STR may not match the highlights rendered in the Viewer. Depending on how the alphabet file has been customized, you may see fewer highlight hits rendered in the Review Interface.

- **Terms**—enter terms you wish to highlight and select the color code to distinguish them in the Viewer. See Entering highlight terms below.

26.5 Entering highlight terms

If you choose **Terms** as the source of your highlighting, you have to enter the terms in the Terms field text box to save the new highlight set. You also have the option of applying color-coding to these terms in the Viewer.



26.5.1 Color-coding persistent highlights

When you enter a term in the Highlight Terms box, you can also specify the color for both the text and the background. Use the following format to color-code your persistently highlighted text:

[background color];[text color];[term to be highlighted]

For example, enter "3;16;Relativity" to highlight Relativity with dark green background and white text.

Note: The auto-contrast feature automatically determines the text color based off the background color you select to ensure readability no matter which colors are selected. For example, if the background color is closer to black, the text will automatically be white or if the background color is closer to white, the text will automatically be black.

Highlights are rendered at full opacity (using the original highlight color) when they are active. When they are not active, they will be rendered in a lighter shade of the original highlight color.

Note: The opacity level of the highlights can be adjusted by editing the value of the **ViewerHighlightStyleDefault** instance setting.

The following table includes available color codes.

Color name	Highlight Color	Number
[Default]		0
Black		1
Dark red		2
Dark green		3
Dark yellow		4
Dark blue		5
Dark magenta		6
Dark cyan		7
Light gray		8
Gray		9
Red		10
Green		11
Yellow		12
Blue		13
Magenta		14
Cyan		15
White		16
Light green		17
Light blue		18
Light yellow		19
Light purple		20

Color name	Highlight Color	Number
Light red		21
Light orange		22
Purple		23
Orange		24
Dark purple		25
Dark orange		26

If you enter terms with no color-coding, the background defaults to magenta and black text.

Note: Default has different implications for text and background. The default background color is white and the default text color is black.

26.5.2 Guidelines for adding terms or phrases

Use the following guidelines when adding terms or phrases into the Terms text box:

- Enter a term that you want highlighted and press **Enter**. You can enter multiple terms but each one must be on a separate line.
- Enter terms for persistent highlighting exactly as they appear in the document. Don't use quotation marks and connectors.

  Note: Quotation marks are not compatible with persistent highlighting with terms as a source, which automatically searches for an exact phrase. Quotation marks are compatible when using highlight fields as a source however. Using highlight fields as a source can result in slower document loading speeds.

- Keep lists simple. Do not use punctuation, special characters, or operators. Do not use dtSearch syntax when entering a list of terms as the source for the set. You may use dtSearch index terms in a search terms report, then use Fields as the Persistent Highlight Source instead to support highlights for dtSearch syntax.
  - AND or OR operators are not used in keyword searching. If used, Relativity looks for the exact phrase including AND or OR. For example, you entered these search terms: Apple AND Banana. Relativity highlights the entire phrase apple and banana in the document. Separate occurrences of apple, and occurrences of banana, are not highlighted.
  - Persistent highlight set terms do support wildcards. You can view highlighted terms that contain an * (asterisk) character, including a wildcard in the middle of a term. For example:
    - term* matches and highlights any word that starts with term with zero or more following characters.
    - *term matches and highlights any word that ends with term with zero or more preceding characters.
    - *term* matches and highlights any word that has term in it with zero or more preceding or following characters.
- Do not enter duplicate terms.
- Identify and remove terms with large hit counts.
- List variations of a term first and enter the root term last.
- If the list of terms is large (>100 terms), use Highlight Fields with a Search Terms Report.

26.6 Using the highlight fields source

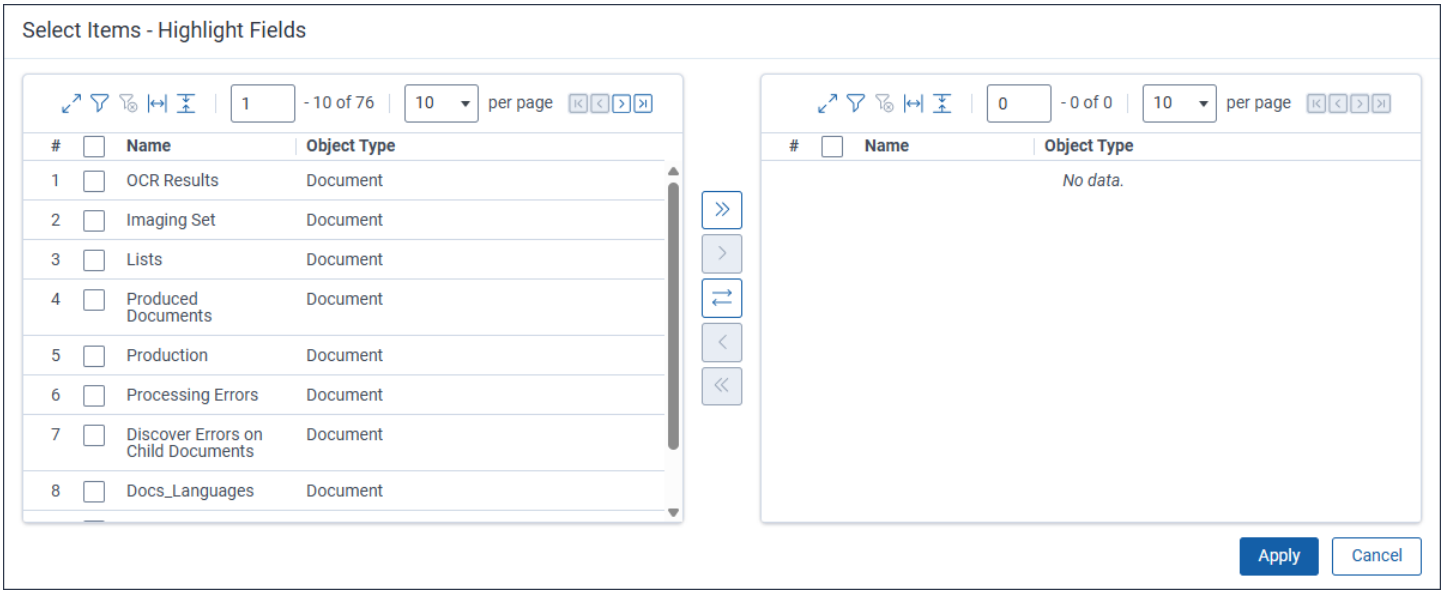
Using the Highlight Fields source in a persistent highlight set you can choose a field referencing a list of terms to highlight.

Select the **Highlight Fields** option, and then click the **Select** button to open the Select items - Highlight Fields modal. This system view displays the Name and Object Type for applicable multiple object fields, including those created by Search Terms Reports.

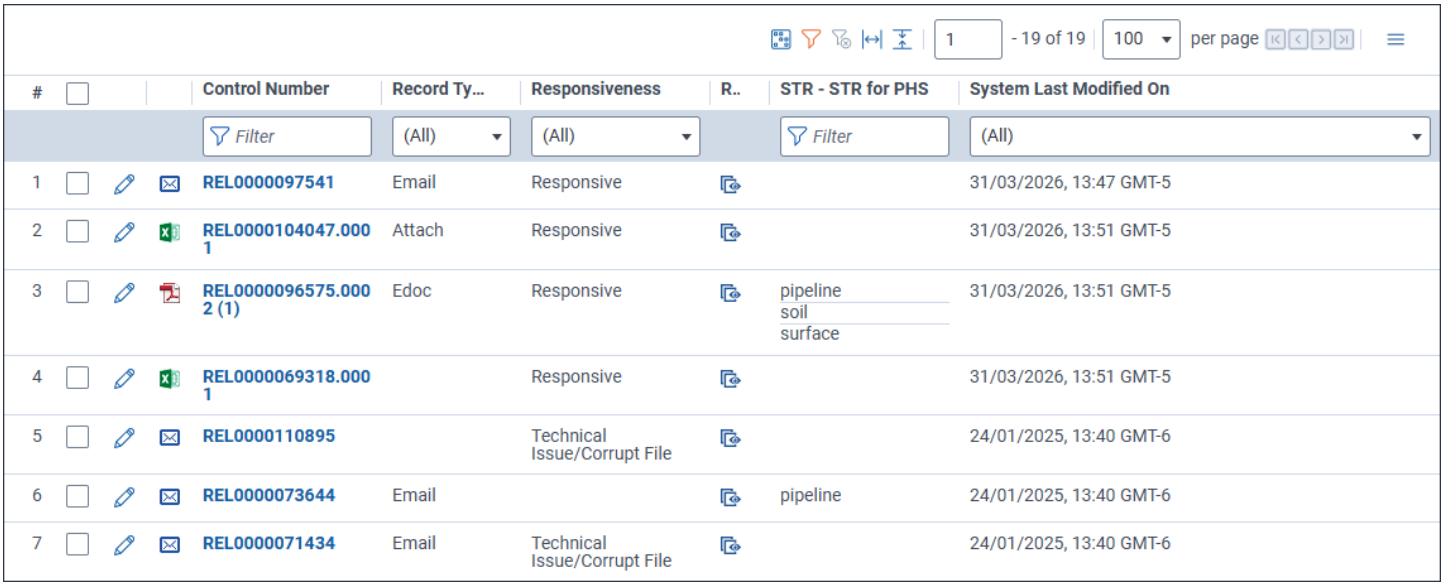
Note: Persistent highlights generated by a search terms report don't automatically update after you load new data into a workspace. To incorporate the text from new documents, perform either a full or incremental build on the dtSearch Index, then a full or incremental build on the search terms report.

To select a Highlight Field, check the field's box, click right arrow to move it the right section. Once all of the desired fields have been selected, click **Apply**. The field appears on the layout.

Note: We recommend selecting a search terms report or the Domains field as your highlight fields source.



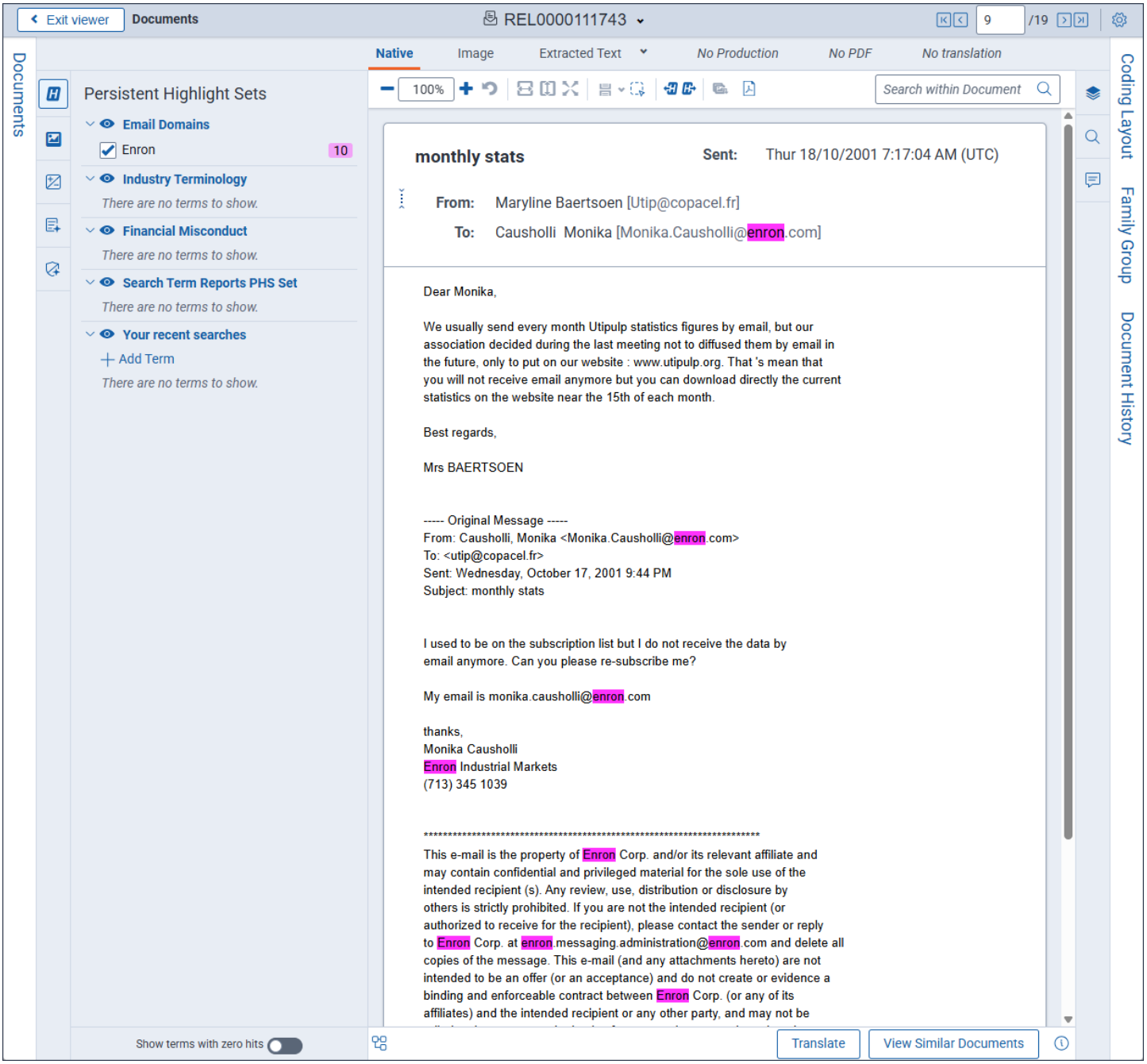
When using a Search Terms Report as the highlight fields source, the number of terms that Relativity searches for will vary among different records. Relativity only looks for the terms listed in the Search Terms Report for that document.



1 - 19 of 19 | 100 per page

#	Control Number	Record Ty...	Responsiveness	R..	STR - STR for PHS	System Last Modified On
	Filter	(All)	(All)		Filter	(All)
1	REL0000097541	Email	Responsive			31/03/2026, 13:47 GMT-5
2	REL0000104047.0001	Attach	Responsive			31/03/2026, 13:51 GMT-5
3	REL0000096575.0002 (1)	Edoc	Responsive		pipeline soil surface	31/03/2026, 13:51 GMT-5
4	REL0000069318.0001		Responsive			31/03/2026, 13:51 GMT-5
5	REL0000110895		Technical Issue/Corrupt File			24/01/2025, 13:40 GMT-6
6	REL0000073644	Email			pipeline	24/01/2025, 13:40 GMT-6
7	REL0000071434	Email	Technical Issue/Corrupt File			24/01/2025, 13:40 GMT-6

Relativity exhibits similar behavior when using an email Domains field as the highlight fields source. Relativity only looks for the email domains listed in the field for that document.



26.6.1 Best practices

Consider the following guidelines when creating or adding terms using Search Terms Reports as the highlight fields source:

- Enter terms exactly as they appear in the document.
- You can use operators such as AND and OR. For example, if you enter these search terms: Apple AND Banana, Relativity would highlight the two terms “apple" and "banana” in the document. See Search terms reports on page 599 for more information.

- Wildcards are useful in some cases. For example, the search term appl* highlights apple, application, applies, and so on. An excessive use of wildcards affects performance. Leading wildcards such as *itting, are not recommended. Using asterisks in the middle of a term don't count as wildcards.
- dtSearch operators can be used to highlight searches when used for a Persistent Highlight Sets in the Native Viewer. You must use a Highlight Fields source (such as a Search Terms Report results field) to use dtSearch syntax. Relativity dtSearch operators are not supported in the Extracted Text Viewer. The highlights for these searches use the active and inactive highlighting functionality. Actively navigated highlights are the highlights that the Viewer is focused on and display with full opacity. Inactive highlights display at a lower opacity level.

  Note: The increase of dtSearch operators does decrease performance.

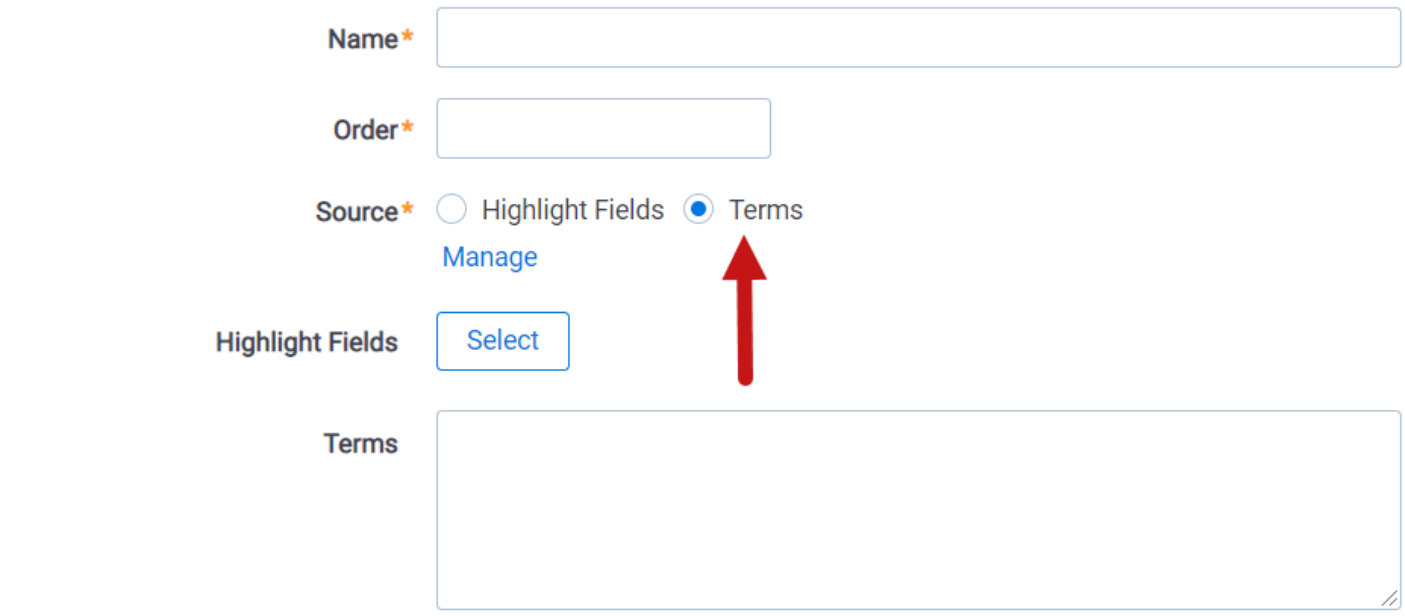
  - Persistent highlight does understand proximity searching. If you enter the phrase Relativity w/5 software as a search term, the search term report uses a dtSearch to find and tag all documents that meet the criteria. When viewed in the Viewer, the persistent highlighting functions as a dtSearch.
  - Persistent highlights does understand the stemming character (~). If you enter the term apply~ as a search term, the search term report finds and tags all documents with the word apply, or any document that stems from apply; including applied, applies, application, and so on. When looking at the document in the Viewer, the persistent highlight functions as a dtSearch. See Search terms reports on page 599 for information on supported syntax.
  - Any operator in quotes will be treated as literal by the Viewer search. For example, stemming “~” and wildcard “*” operators. However, dtSearch will treat stemming and wild card operators in quotes not as literal, but as the operator itself. For example, "run~” in the Viewer will find the exact phrase “run~” and "run~” in dtSearch will return hits for run, runner, running, etc.

26.7 Creating efficient searches for persistent highlighting

Creating efficient searches improves the performance of persistent highlighting, whether you're working with a Terms Search or Highlight Fields. Use the following guidelines to create efficient searches.

26.7.1 Using terms search

Avoid the following when writing searches for persistent highlighting:



- Do not use "AND" or "OR" connectors. Persistent highlighting looks for the exact phrase, trade and complete, instead of the word, trade, and the word, complete.
- Proximity, fuzziness, and stemming logic cannot be used in a Terms Search. Consider using Highlight Fields to access these search features as described below. The system ignores the dtSearch syntax. Terms receive no highlight if you use these advanced searching features. The search terms report Count column still lists the number of matching terms. For example:
  - The search term, oil w/10 water, searches for the exact phrase oil w/10 water.
  - If you enter the term apply~ as a search term, persistent highlighting technology looks for the term apply followed by any special character.
- Avoid using terms with a large number of hits per document. Persistent highlighting highlights each hit. For example, it takes longer to load a Word document containing 1,000 instances of a single term.
- Avoid using terms that only occur once in a document. Use search terms reports for those terms instead.
- Avoid long lists of numbers, such as Bates numbers or account numbers.
- Do not use duplicate terms.

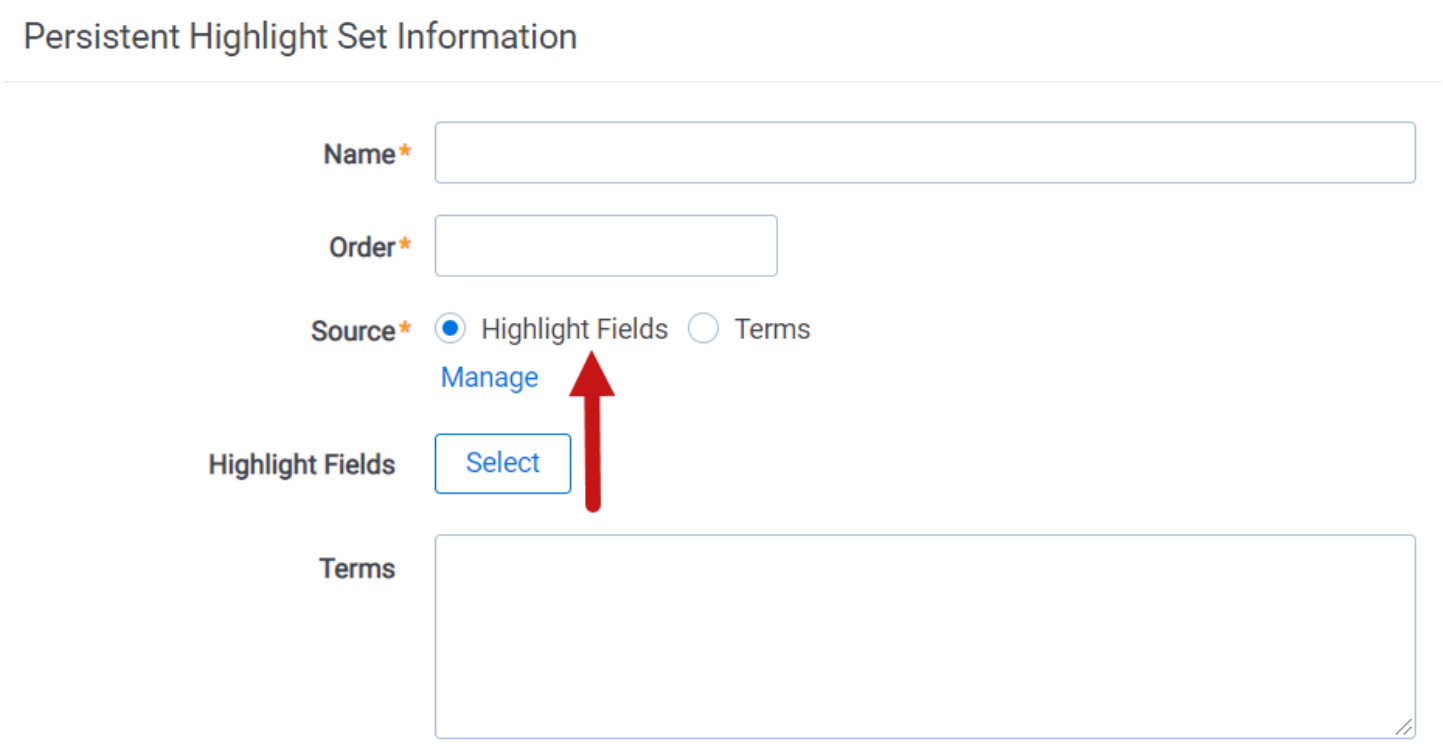
Use the following techniques to optimize your searches:

- Use the dtSearch Dictionary to identify variations of a term instead of using wildcards.
  - Identify which terms should be in the highlight set and which terms are not necessary.
  - You may want to avoid highlighting terms with high word counts.

Note: To highlight terms using objects, create a fixed-length text field for your object called Highlight Colors. You can enter color-coding in this field using the format: **[highlight color];[text color].**

26.7.2 Using highlight fields

Consider the following guidelines when creating or adding terms using Search Terms Reports as the highlight fields source:



- Enter terms exactly as they appear in the document.
- You can use operators such as AND and OR. For example, if you enter these search terms: Apple AND Banana, Relativity would highlight the two terms “apple" and "banana” in the document. See Search terms reports on page 599 for more information.
- Wildcards are useful in some cases. For example, the search term appl* highlights apple, application, applies, and so on. An excessive use of wildcards affects performance. Leading wildcards such as *itting, are not recommended. Using asterisks in the middle of a term don't count as wildcards.
- dtSearch operators can be used to highlight searches when used for a Persistent Highlight Sets in the Native Viewer. You must use a Highlight Fields source (such as a Search Terms Report results field) to use dtSearch syntax. Relativity dtSearch operators are not supported in the Extracted Text Viewer. The highlights for these searches use the active and inactive highlighting functionality. Actively navigated highlights are the highlights that the Viewer is focused on and display with full opacity. Inactive highlights display at a lower opacity level.

  Note: The increase of dtSearch operators does decrease performance.

  - Proximity searching logic can be used with Highlight Fields. If you enter the phrase "Relativity w/5 software" as a search term, the search term report uses a dtSearch to find and tag all documents that meet the criteria. When viewed in the Viewer, the persistent highlighting functions as a dtSearch. See Search terms reports on page 599 for information.
  - Stemming, including the stemming character (~), can also be used with Highlight Fields. If you enter the term "apply~" as a search term, the search term report finds and tags all documents with the word apply, or any document that stems from apply; including applied, applies, application, and so on. When looking

at the document in the Viewer, the persistent highlight functions as a dtSearch. See Search terms reports on page 599 for information.

- In Search Terms Reports, you can also use the Dictionary Search function to identify search terms using stemming or fuzziness. Copy the list of terms returned in this search. Paste them in the Add Terms box on the Search Terms Report form. Doing this enhances your search term list, while avoiding errors caused by special characters.
- Use the dtSearch Dictionary to identify variations of a term instead of using wildcards.
  - Identify which terms should be in the highlight set and which terms are not necessary.
  - You may want to avoid highlighting terms with high word counts.

27 Printing in Relativity

Relativity includes a few options that you can employ when you need to print natives or images of documents in Relativity. The following easily accessible features support printing a large group of documents or a single document at a time.

27.1 Save as PDF

Single Save as PDF is an option within the Viewer in Relativity. With this option you can save the native of the current open document as a PDF file. Once you save the PDF of the file, you can open the PDF and print it to your designated printing location. For more information, see Single Save as PDF.

27.2 Mass PDF

Mass PDF is a mass operation you can run from the mass operations bar in the case workspace interface. With Mass PDF you can save a group of documents and customize the way the documents render when you save or print them. After you download the .zip file of the PDFs, you can then print the group of PDFs to your designated printing location. For more information, see Mass Save as PDF.

28 Production

With the Production application, you can prepare documents for production—selecting non-privileged documents and turning them over to opposing counsel after review. You can customize productions with placeholders, branding, and other options.

28.1 Security permissions to run productions

The following security permissions are required to run productions in Relativity.

Object security	Tab visibility	Other settings
• **Production** – View, Edit, Add • **Production Data Source** - View, Edit, Add, Delete • **Production Information** - View, Edit, Add • **Production Placeholder** - View, Edit, Add	• Production Sets • Production Placeholder • Production	Mass Operations • Re-Produce Admin Operations • Override Production Restrictions

28.2 Upgrading production

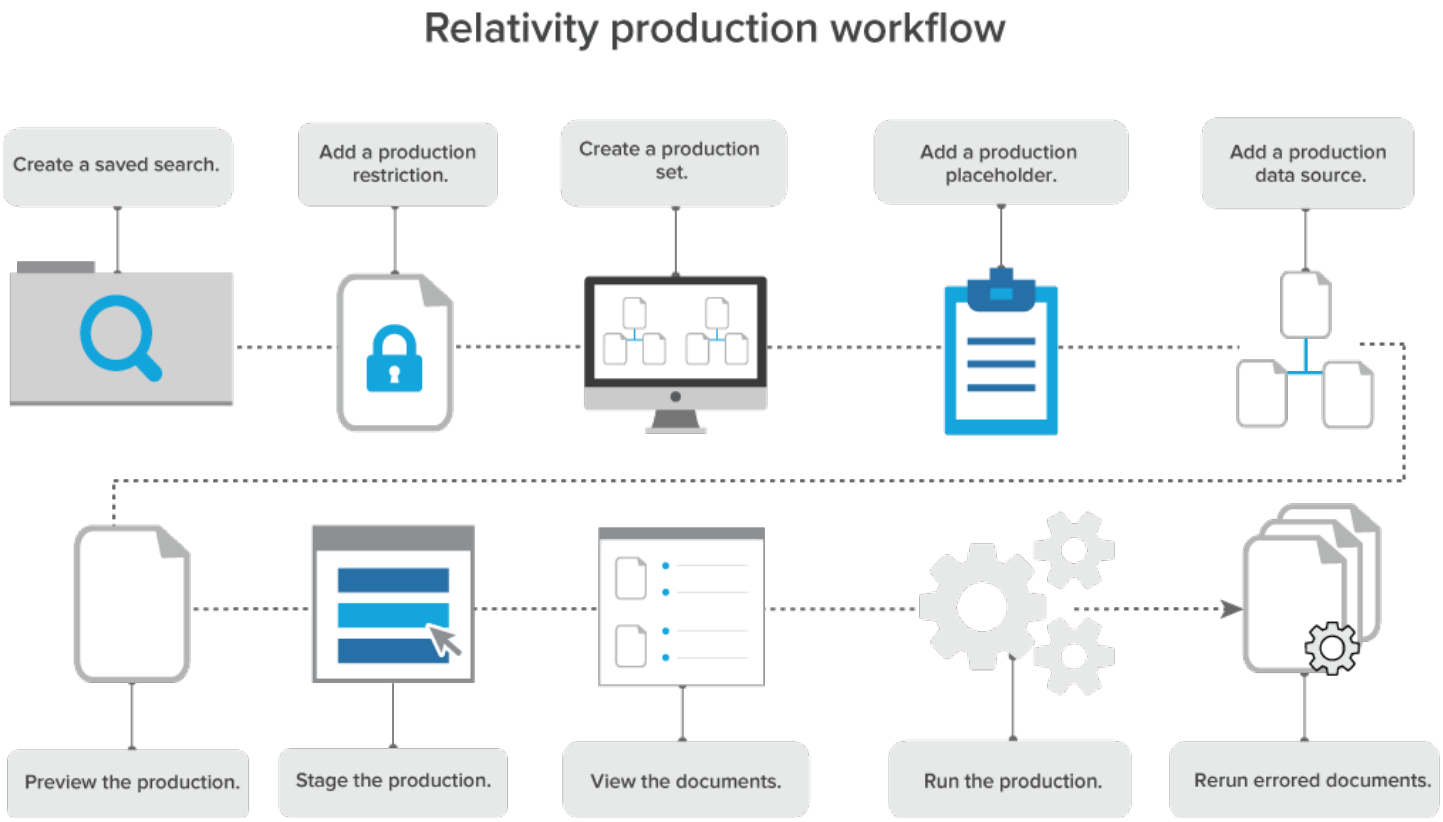
Production application upgrades occur concurrently with Relativity product updates. You can find information about production updates in the Relativity release notes and What's new.

To upgrade the application, use one of the following methods:

1. **Upgrade to the latest Relativity product update** - Upgrading to the latest Relativity update automatically upgrades production to the latest version.
2. **Upgrade production only** - Download the newly released RAP file from the Relativity Community and import it into the Application Library.

28.3 Basic production workflow

To produce documents, use the following workflow to create the required production components. Use the links in the image below for more information on each part of the production workflow.



28.4 Production information

The production information object stores important information about your production. Staging a production populates this object in your workspace. For example, you can use the production information object to check:

- The number of documents with redactions
- The control numbers of documents in your production
- Which documents were produced with a placeholder
- Which documents were produced as a native

The production information object also stores the Bates numbers associated with the production. When you delete a production, the Bates number fields clear automatically.

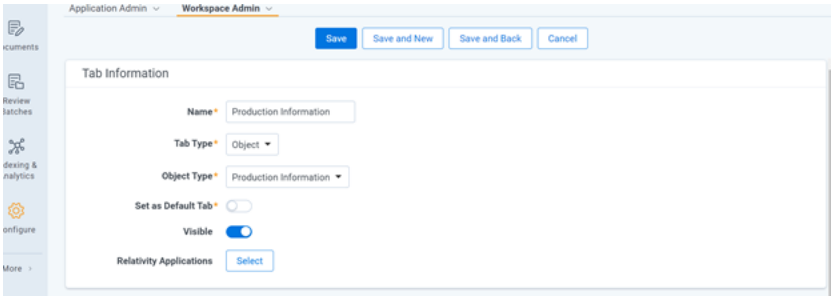
To view the information stored on this object, click **View Documents** in the production console. The View Documents pop-up displays information about documents and individual pages. You can also view document information in the saved search that is created automatically when the production job finishes.

After you run a production, you can view this information on the documents list for each produced document. Add the fields to a view, then create a tab from that view. See Views and Tabs in the Admin guide for more information.

28.4.1 Production information tab

To view detailed production information, create a production information tab and associate it with the production information object.

1. Navigate to Tabs.
2. Click **New Tab**.
3. Enter *Production Information* as the name for the tab.
4. Select **Object** as the tab type.
5. Select **Production Information** as the object type.



6. Configure the tab location.
7. Click **Save.**
8. Navigate to the Production Information tab to view information about your production set.

The following fields are stored on the production information object. You can view them on the production information tab:

- Artifact id
- Begin attachment
- Begin bates
- Data source
- Document
- Document id
- Edit
- End attachment
- End bates
- Has redactions
- Identifier

- Image count
- Name
- Production type
- Production set
- Security
- Sort order
- System created by
- System created on
- System last modified by
- System last modified on
- With images
- With natives
- With pdf
- With placeholder

28.5 Production sets

When you want to produce documents in a case workspace, you can create a production set that defines the markup set for redactions, the document numbering, the appearance of the numbering, and other settings that Relativity uses when you run the production.

You can then view the produced images in the Review Interface by selecting Production mode and the production set.

28.5.1 Creating and editing a production set

Before you can run a production, you must create a production set and add documents to it through a saved search. Use the following steps to create or edit a production set:

1. Navigate to the **Production** tab.
2. Click the **Production Sets** tab.
3. Click **New Production**.
4. To edit an existing production set, click the edit link next to the production set name.

   Note: You can change the name of a production at any point in the production process.

5. Add or edit the fields in each section as necessary. Required fields are orange.
   - Basic Settings on the next page
   - Numbering on page 459
   - Branding on page 465
   - Sorting on page 467

- Post Production on page 468
- Other on page 470

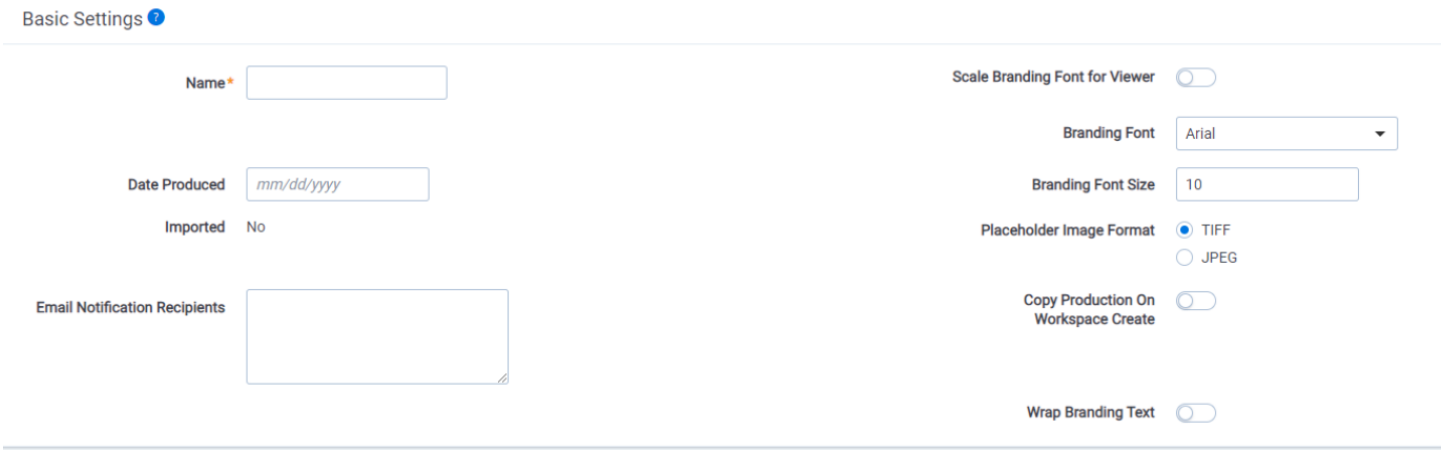
6. Save the additions or updates.

Note: If you imported a production, the imported Opticon file controls the page numbering. Relativity ignores any markup set, branding, or other settings on the Production Set form and produces the images exactly as imported.

28.5.2 Basic Settings

When you add or edit a production set, you can begin by modifying the settings in the Basic Settings section of the Production Set form.

The Basic Settings section contains the following fields:



- **Name**—(required) The name of the production set you are creating.
- **Date Produced**—The date the documents were produced. You can select any date. If you do not select a date, Relativity uses the date the production completed.
- **Email Notification Recipients**—Enter one or more email addresses to receive notifications when a production fails or completes. Separate multiple addresses with a semicolon.
- **Imported**—Indicates whether the production is open to receive imported production documents.
- **Scale Branding Font for Viewer**—(required) Scales up the branding text size to be consistent with Relativity 7.5 behavior for optimal viewing of images in the Viewer when set to **Yes**. Set this field to **No** to use the default font scaling when printing images. This field is read-only after you run a production set.
- **Branding Font**—(required) The font type applied to branded text. To set a default branding font for productions, adjust the DefaultBrandingFont instance setting.
- **Branding Font Size**—(required) The font size for branding added to a page. To set a default branding font size for productions, adjust the DefaultBrandingFontSize instance setting.
- **Copy Production on Workspace Create**—(required) When set to Yes, Relativity copies this production and its associated data sources into any new workspace created from this workspace template.
- **Wraps Branding Text**—Controls whether branding text wraps when the content of two adjacent headers or footers would otherwise overlap. Set to Yes to allow wrapping. Set to No to keep text from wrapping.

28.5.3 Numbering

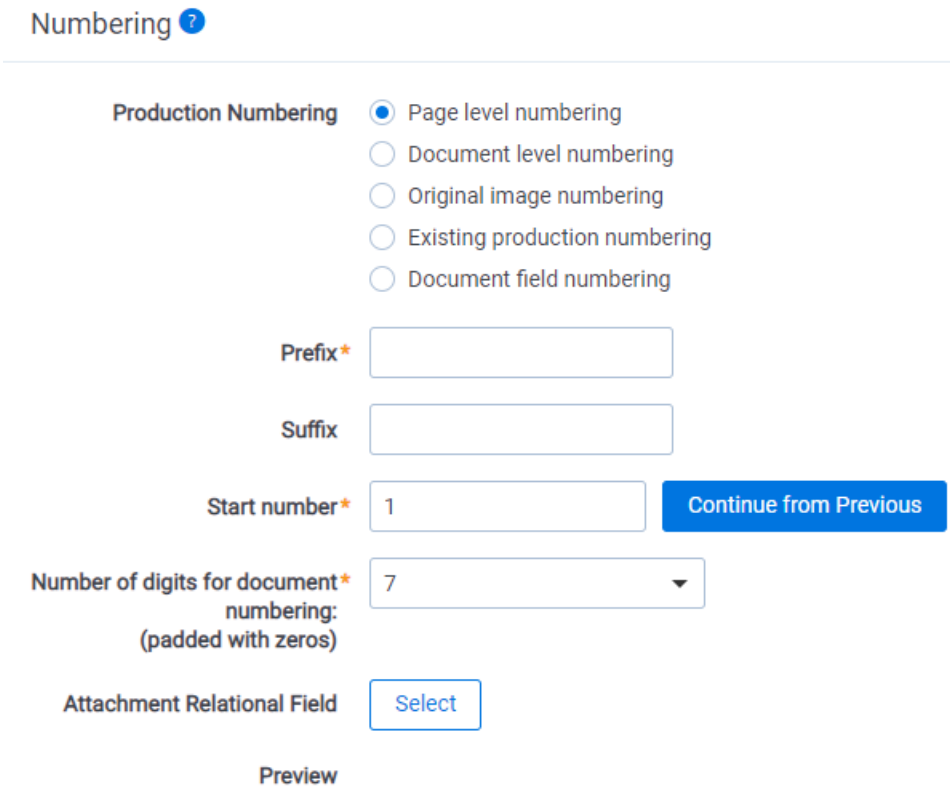
On the Production Set form, you can define multiple options that control how numbering is applied to images in your production.

Relativity provides the following numbering types for productions:

- Page level numbering
- Document level numbering
- Original image numbering
- Existing production numbering
- Document field numbering

Page level numbering
Select **Page level numbering** to generate a new incremental number (also known as a Bates number) on every page across your production documents. This number is branded on the images and PDFs in your production.

The form fields available when you select **Page level numbering** include:



- **Prefix**—(required) The characters added to the beginning of each Bates number. This is limited to 50 characters.
- **Suffix**—Optional characters applied to the end of each Bates number. This is a static, non-incremental text string, limited to 50 characters.
- **Start number**—(required) The first number used in a sequence of Bates numbers.To continue numbering from a previous production, click **Continue from Previous**.

Note: Continue from Previous is unavailable for productions that use original image numbering, existing production numbering, or document field numbering.

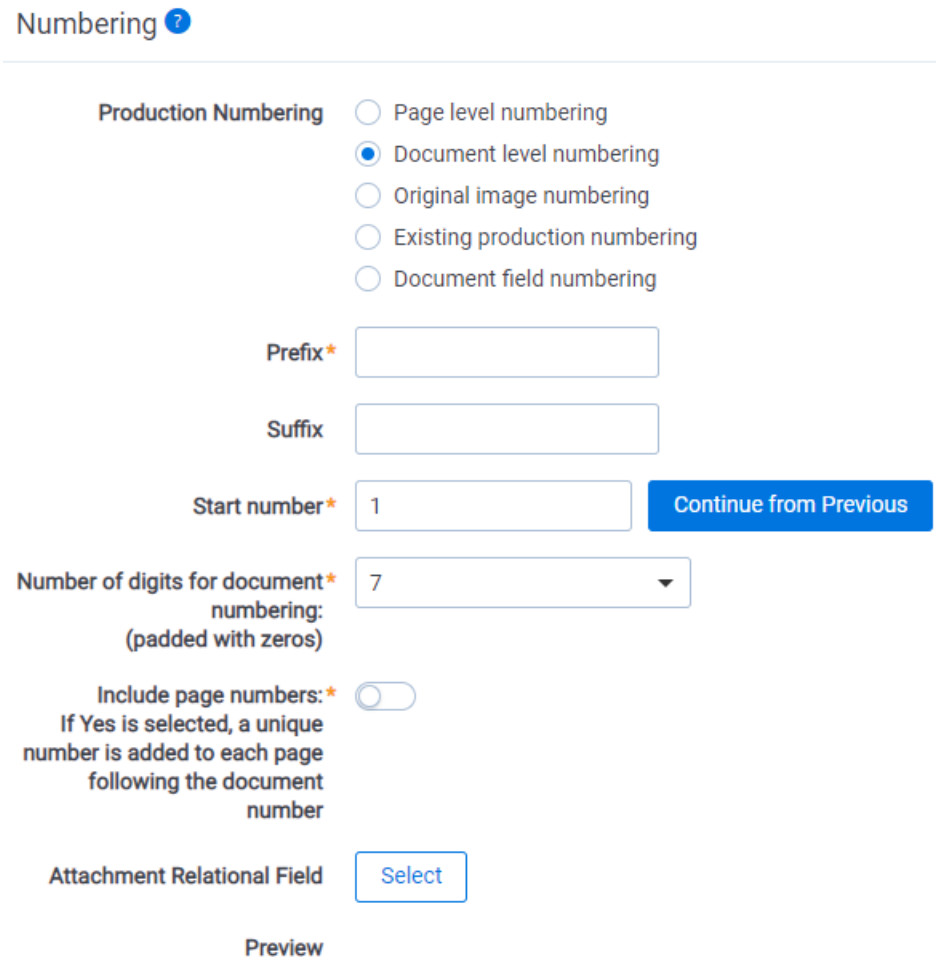
Relativity automatically populates the **Start number** field with the value that displays for the **Next doc number**.

- **Number of digits for document numbering**—(required) Determines how many digits the Bates number contains. The range of available values is 1–10. The default is 7 digits.
- **Attachment relational field**—Selects a relational field indicating a family group such as group identifier.
- **Preview**—Displays sample text illustrating how the Bates number appears in the images.

Note: Relativity does not support the combined length of the Prefix and Suffix exceeding 255 characters when using Page level numbering.

Document level numbering
Select **Document level numbering** to generate a new document number for each document, which is branded on the images in your production.

The form fields available when you select **Document level numbering** include:



- **Prefix**—(required) Lists the characters added to the beginning of each document number. This is limited to 50 characters.

- **Suffix**—Lists optional characters applied to the end of each document number. The suffix is added after the document number but before the page number when the **Include page number** option is selected. This is a static, non-incremental text string, limited to 50 characters.
- **Start number**—(required) Indicates the first number used in a sequence of document numbers. To select a previous production and continue with its numbering sequence, click **Continue from Previous**.

  Note: Continue from Previous will not work for productions using original image numbering, existing production numbering, or document field numbering.

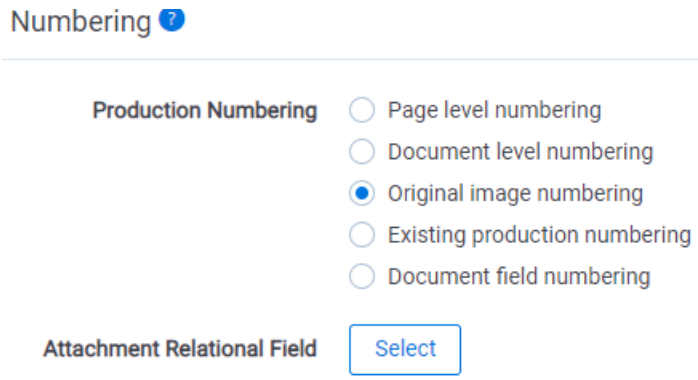
  Relativity automatically populates the **Start number** field with the value that displays for the **Next doc number**.
- **Number of digits for document numbering**—(required) Determines how many digits the document number contains. The range of available values is between 1 and 10. By default, this option is set to 7 characters.
- **Include page numbers**—(required) Adds a unique page number after the document number on each page in a document, when it is set to **Yes**. By default, this option is set to **No**.

  Note: If you export a production with document level numbering as single-page TIFF, and it does not include page numbering, Relativity automatically adds page numbers to identify each page uniquely.
- **Document Page Separator**—Displays when you select the Include page number option. The following separators are available:
  - _ (underscore, selected by default)
  - - (hyphen)
  - . (period)
- **Number of digits for page numbering**—Determines how many digits the page number contains. The range of available values is between 1 and 6. By default, this option is set to 4 characters.
- **Start numbering on second page**—Determines where the document level numbering begins.
  - **Yes**—Starts numbering on the second page of the production documents.
  - **No**—Starts numbering on the first page of the production documents.
- **Attachment relational field**—Selects a relational field indicating a family group such as group identifier.

Note: The combined length of the Prefix and Suffix cannot exceed 255 characters when using Document level numbering.

Original image numbering
Select the **Original image numbering** to retain the identifiers originally associated with your images. For example, you may want to retain the Bates or other numbers already assigned to images uploaded to Relativity. Relativity utilizes these values to create the production and attachment numbers.

The form fields available when you select **Original image numbering** include:



- **Attachment relational field**—Selects a relational field indicating a family group such as group identifier.

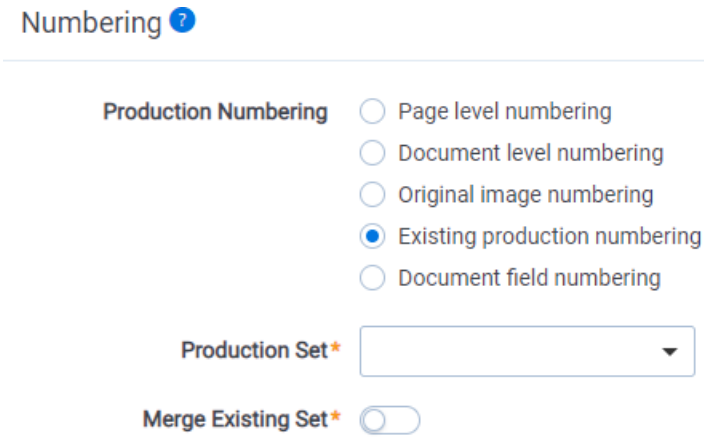
The following table provides several original image numbering scenarios:

Document has	Produced with	Generated Bates numbers with
Natives + imported images	Images and natives	The Image identifiers defined in the Image Load File.
Natives + images	Natives only	The Document Identifier.
Natives + Oracle images	Images only	The Images number created by the TIFF native manager: Document Identifier + <Page Number> + <Hash Value>. For example: Stel_Img_0_272ec3bf-9287-4862-be34-bbb230274a86
Images only (imported)	Images only	The Image identifiers defined in the Image Load File.
Natives only	Natives only	The Document Identifier.
Natives only	Images and natives	The created image place holder, using the Document Identifier field. For Example: e2f448d6-6e19-4d7c-9e50-7fccbf9c5c6b
Natives only	Images only	The created image place holder, using the Document Identifier field. For Example: e2f448d6-6e19-4d7c-9e50-7fccbf9c5c6b

Existing production numbering
Select **Existing production numbering** to reuse the Bates numbering fields from a previously run production set, change the images of the documents produced, or produce a subset of documents from the existing production. More specifically, you may want to select this option if, for example, a court order requires that your documents be produced without an already-applied confidential branding or if you need to redact already-produced documents for privilege.

Notes:

- When creating a production set with Existing production numbering, you cannot add documents not contained in the existing set, change page counts, or change whether or not a document previously produced as native only is produced with a placeholder. You can replace a document produced as an image with a placeholder, as long as it is a single-page document.
- When you choose a production set with more documents than the existing set, Relativity generates a warning to inform you that it auto-removed the extra documents. If the new production set contains a subset of the documents in the existing set, Relativity runs it without warnings.



The following required fields appear when you select the Existing production numbering choice:

- **Production Set**—(required) Select the production set containing the numbers you'd like to use for the set you're creating. Only completed production sets are available to select from this drop-down list.
- **Merge Existing Set**—(required) When you merge a new production with an existing production, the new production images replace the images in the previously existing production. The new production still exists for export. Relativity updates the Has Redaction field in the Production Information record in cases where redactions were added or removed. From the viewer, if you compare the existing production and the new production, the images look the same if the images from the existing production set are not in the cache. If existing production images are in the cache, you still see the original produced version of the image when you select the existing production set radio button. For more information on merging, see Production sets on page 457.

  Note: The Merge Existing Set functionality does not merge produced or redacted natives.

Selecting this option fully replaces the original production's produced image inside Relativity. You cannot export the original produced image if you merge the sets.

Note: If you have an existing production set with document level numbering, no page-level markers, and the existing production is migrated into the environment, you cannot merge the productions together with existing production numbering.

If one production references an already produced production in the **Production Set** field, you cannot delete the referenced production. You can resolve the error by referencing an existing production or modifying the parameters of the production to eliminate the reference to the deleted production.

Numbering merge conflicts

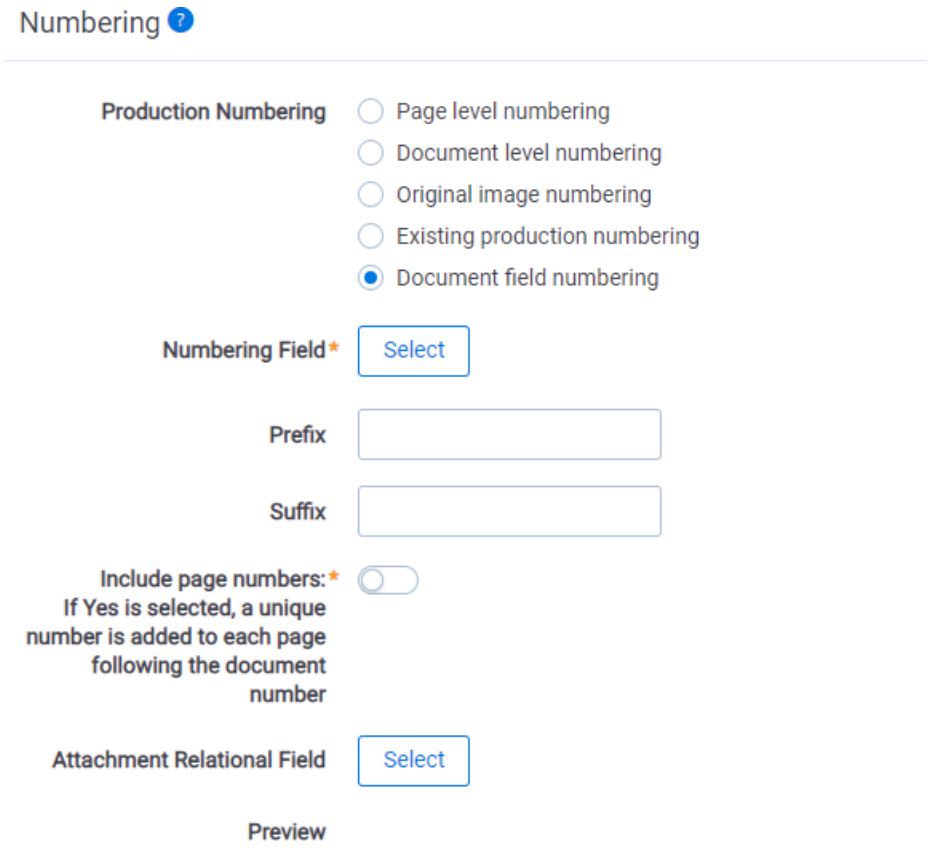
When electing to use an existing production's numbering and then merging that numbering, consider the following conflict scenarios. These scenarios result in errors when you attempt to run a new production set:

- The production set you are creating contains documents that were not included in the existing production set. Remove these documents from the new production before running it.
- The page counts of the documents in the production set you're creating differs from the page counts in the existing production set.
- If documents in a production set are also in the production restriction for that production, you must remove the documents from either the production set or the production restriction.
- You attempt to perform any action on a production set while it is merging with another.

Document field numbering

Select Document field numbering to use any fixed-length text field on the Document object for numbering. Reflective fields are not available for this numbering option.

For example, select this option if you import a set of documents into Relativity and want to maintain the original document numbering. You could choose control number as the field and produce documents using the control number as the bates field.



The following required fields appear when you select the Document field numbering choice:

- **Numbering Field**—(required) Select the field you'd like to use for numbering from this drop-down list. Only fixed-length text fields are available to select from this drop-down list.

  Note: The content of the numbering field, prefix, and suffix cannot exceed 255 characters.

- **Include page numbers**—(required) Adds a unique page number after the document number on each page in a document, when it is set to **Yes**. By default, this option is set to **No**.

  Note: If you export a production with document level numbering as single-page TIFF, and it does not include page numbering, Relativity automatically adds page numbers to identify each page uniquely.

  - **Document Page Separator**—(required) Displays when you select the Include page number option. The following separators are available:
    - _ (underscore, selected by default)
    - - (hyphen)
    - . (period)
  - **Number of digits for page numbering**—(required) Determines how many digits the page number contains. The range of available values is between 1 and 6. By default, this option is set to 4 characters.

- **Start numbering on second page**—(required) Determines where the document level numbering begins.
  - **Yes**—Starts numbering on the second page of the production documents.
  - **No**—Starts numbering on the first page of the production documents.
- **Attachment relational field**—Selects a relational field indicating a family group such as group identifier.

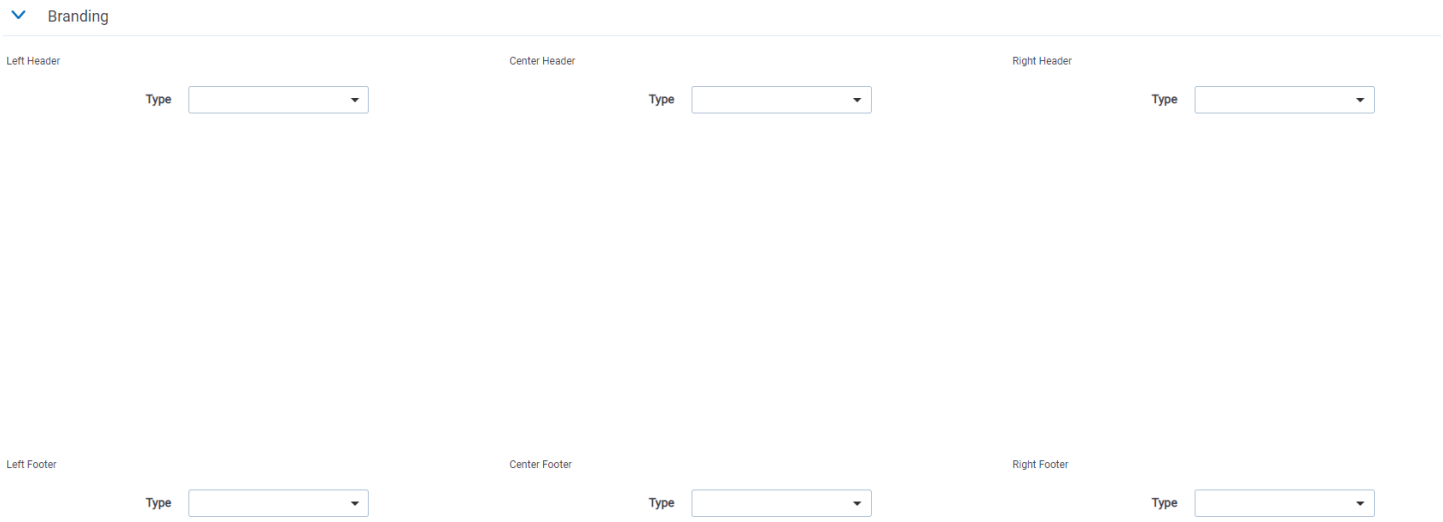
28.5.4 Branding

In the Branding section of the production set form, you can set branding options for headers and footers. You can position headers and footers to the left, center, and right on the images in your production.

Note: If this page loads slowly, reduce the ChoiceLimitForUI instance setting until the drop-down lists become popup pickers. This setting affects all workspaces in the environment.

Select a **Type** for each header or footer position where you want information branded in the image.

The following **Types** are available:



- **Production Bates Number**—Displays the Bates number associated with each document page.
- **Production Number**—Displays the document number associated with each page. (Available for **Document level numbering** and **Original image numbering** only)
- **Field**—Uses the value in the selected document field for branding on each image created for a document.

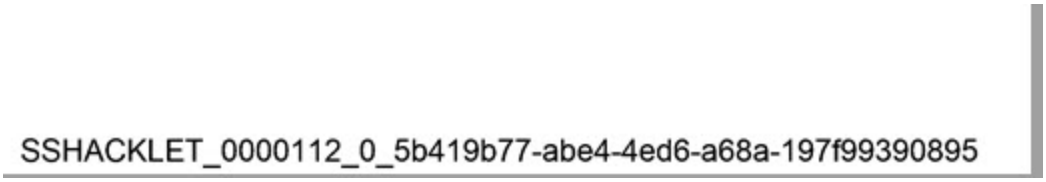
  Note: Relativity restricts the following field types from branding for document images in a production: user, multiple object, and reflective field types.

- **Free Text**—Uses any combination of text, tokens, and carriage returns that you define. Relativity does not support multi-reflected, multi-object, relational, file, user, and system fields for branding. You can use carriage returns to position the header or the footer closer to the top and bottom margins respectively. Use tokens to include field data as follows:

  Note: If you enter a field ID that represents a field that doesn't exist or is not a document field you cannot produce the production.

- **Production Number:** {!PRODNUM!}
- **Any Data Field:** {!FIELD:ARTIFACTID!} as in the example {!FIELD:1040549!}. You can brand multiple fields by separating the entries with carriage returns.

- **Original Image Number**—Uses the original page ID assigned by Relativity as follows:
  - When an image load file was used to import data, the numbering defined in the load file is applied. If you run a production with image placeholders, the original image number is replaced with the Document Identifier field.
  - Document ID, page ID, and a hash value are applied in combination when images were created using the Image-on-the-fly functionality.

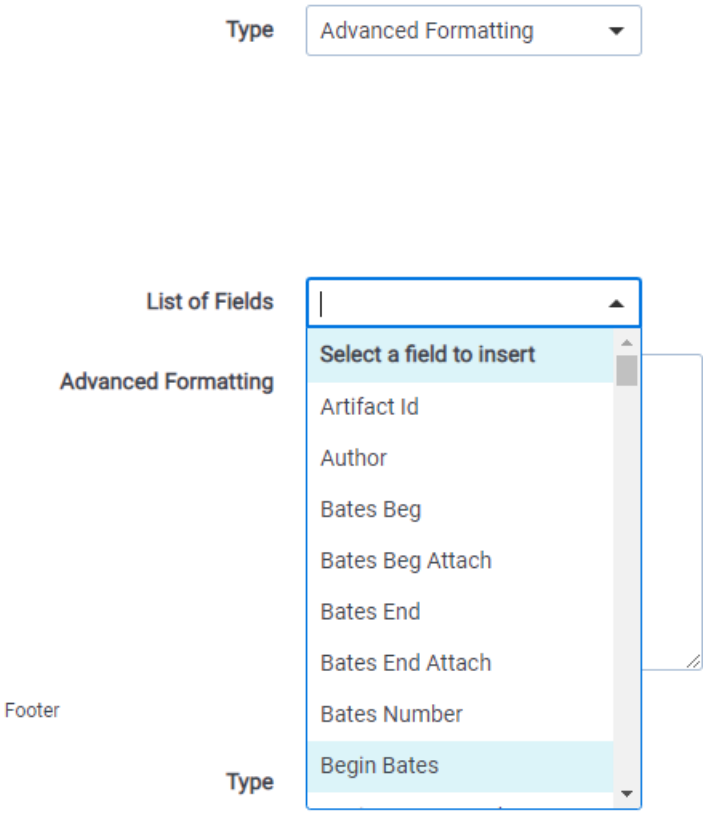
    In this example, SSHACKLET_0000112 is the Document ID, 0 is the page ID, and 5b419b77-abe4-4ed6-a68a-197f99390895 is the hash value.
- **Document Identifier + Page Number**—Uses the document identifier with the page number appended to it. This option sets the first page number to 1 even when the document contains only a single page. The following pages are numbered incrementally. In addition, the page number is padded with up to four digits as illustrated below.

  Note: Depending on the settings for the header and footer, Relativity prevents the image from being cut off by adding approximately five extra pixels to its edges.

- **Advanced Formatting**—Uses any combination of fields from the **Advanced Formatting** drop-down list, free-form text, and carriage returns. The Advanced Formatting option also supports a scripting language that you

can use to create conditional branding based on production, document, and page fields.



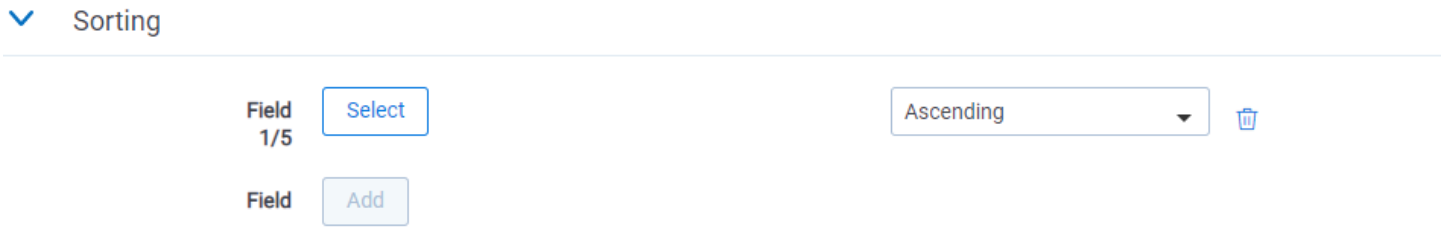
Branding text wraps by default if the content of two adjacent footers or headers are likely to overlap with each other. To keep text from wrapping by default across your entire Relativity instance, contact Support.

28.5.5 Sorting

In Sorting, you can select a field that determines how your production is sorted. You can sort a production set by more than one field at a time. You can also use a descending or ascending sort order. By default, the sort order is Artifact ID, which is the load order of the documents. When you perform a sort, family groups are not kept together. The sorting applies to all data sources added to the production set. Sorting is only applicable when Production Numbering is set to the following:

- Page level numbering
- Document level numbering
- Original image numbering
- Document field numbering

Note: If this page loads slowly, reduce the ChoiceLimitForUI instance setting until the drop-down lists become popup pickers. This setting affects all workspaces in the environment.



Note: If you do not specify a sort order, Relativity stamps documents in ascending Artifact ID order. The production numbering sort order doesn't determine the order of documents in the document list view.

Note: To keep family groups together in sort order, set the first sort field to Family Group, then add any additional sort criteria.

28.5.5.1 Sort order limitations

Existing production numbering does not support custom sort order.

When using Existing production numbering, documents are automatically sorted by Artifact ID (ascending). This is the internal document identifier assigned when documents are loaded into the workspace.

Family group splitting with Existing production numbering

If you are using the Attachment relational field to keep family groups together, be aware that families may be split when:

1. Using Existing production numbering, AND
2. Documents within a family have non-consecutive Artifact IDs, AND
3. Other documents in the production have Artifact IDs that fall between family members

In this scenario, the Begin Attachment and End Attachment fields may not correctly reflect the full family range.

Use Page level or Document level numbering with Sort Order set to your family grouping field (e.g., Group Identifier) as the first sort criterion to avoid errors.

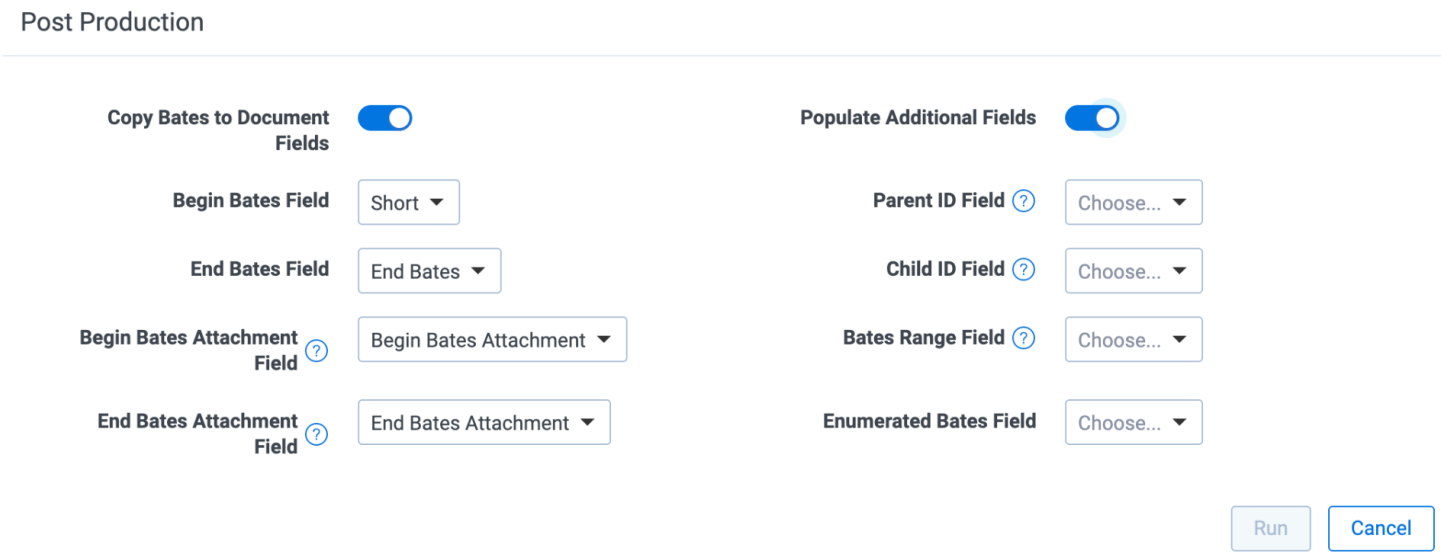
The following table lists sort order limitations for each numbering type:

Numbering type	Sort order support	Default sort
Page level numbering	Supported	User-defined
Document level numbering	Supported	User-defined
Original image numbering	Supported	User-defined
Document field numbering	Supported	User-defined
Existing production numbering	Not supported	Artifact ID

28.5.6 Post Production

In Post Production, you can select additional actions to run automatically after production completes. Post Production allows for better progress tracking, runs automatically, and provides visibility on the Production Set Console.

The **Copy Bates to Document Fields** action is supported in Post Production.



Note:
Post Production workflow replaces the need to run scripts after production. The functions of now deprecated legacy scripts are available in Post Production using the following fields:

- **Begin Bates Field** and **End Bates Field** replace the Assign Legacy Documents Bates Field
- **Begin Bates Attachment Field** and **End Bates Attachment Field** replace Set Beg Attach/End Attach Field
- **Parent ID Field** and **Child ID Field** replace Populate Parent ID and Child ID per Document

After a production completes, Relativity copies the stored production information to the fields you configured.

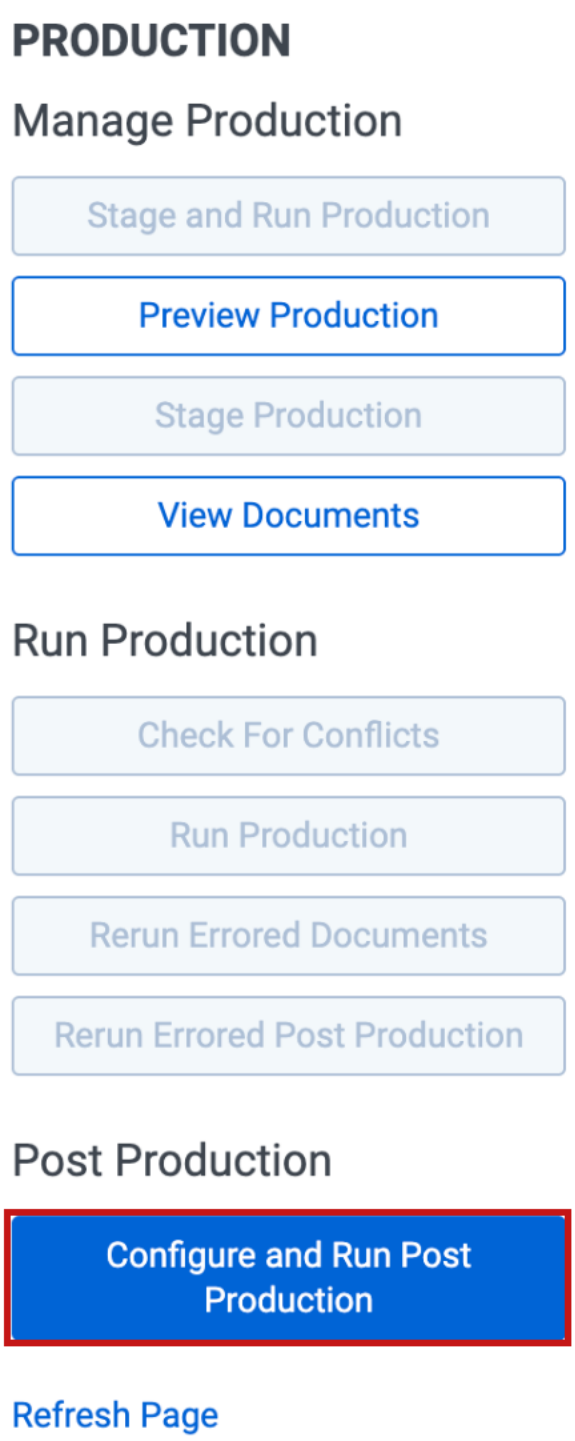
- **Begin Bates Field**—Choose the field that you want to copy from Production:BeginBates
- **End Bates Field**—Choose the field that you want to copy from Production:EndBates
- **Begin Bates Attachment Field**—Enabled only when Attachment Relational Field has been selected. Choose the field that you want to copy from Production:BegAttach
- **End Bates Attachment Field**—Enabled only when Attachment Relational Field has been selected. Choose the field that you want to copy from Production:EndAttach
- **Parent ID Field**—Populates a field with the Begin Bates number of the parent for each child in a document family. Attachment Relational Field is required to use Parent ID field.
- **Child ID Field**—Populates a field with a list of Begin Bates numbers of all children for a parent in a document family. Attachment Relational Field is required to use Child ID field.
- **Bates Range Field**—Populates a field with beg attach and end attach range separated by hyphen. Attachment Relational Field is required to use Bates Range field.
- **Enumerated bates Field**—Populates a field with a list of all bates numbers within a range of document.

Note: Create dedicated Fixed-Length Text fields for this operation or select fields with the purpose of having bates populated. Selecting one of the template fields may result in production failure.

28.5.6.1 Rerun Post Production

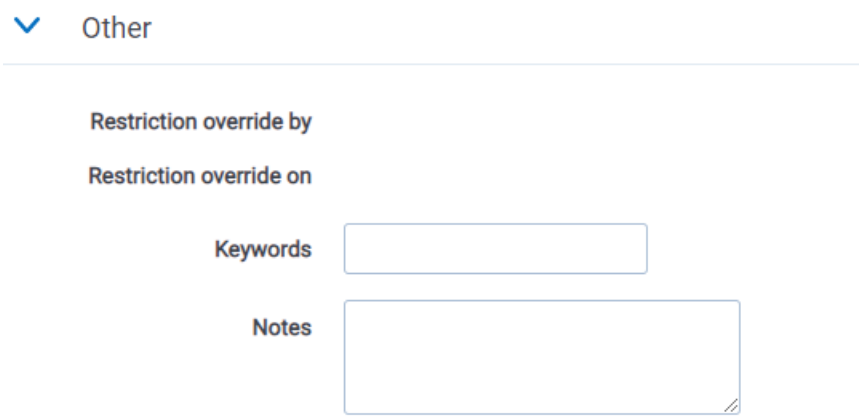
Post Production can be rerun for already completed production sets.

To rerun Post Production, navigate to a completed Production Set and click the **Configure and run post production** option.



28.5.7 Other

The Other section displays additional fields added to the form after the production set was saved:



- **Restriction override by**—Displays the name of the user who clicked the **Override and Continue** button when running the production without removing conflicts. This user must have the Override Production Restrictions permission.
- **Restriction override on**—Lists the date and time when the production restrictions were overridden.

28.5.8 Viewing production set details

28.5.8.1 Production set details options

You can use the options available on the detail view for production sets to edit permissions, view audit information, preview the production, and perform other tasks. You can access these options through the buttons at the top of the page.

Use the following buttons to complete tasks as necessary:

- **Edit**—Re-displays the production set form so you can update values in the fields. See Creating and editing a production set on page 457.
- **Delete**—Removes the production set from Relativity. When you delete a production, it is immediately removed from the Production Sets tab. Bates numbers might still appear in the Documents tab until Relativity removes them during off-hours maintenance, along with the production data source and any remaining production information.
  To retain the previously recorded Bates numbers, run the Assign Legacy Document Bates Fields script from the Relativity Script Library. After you click **Delete**, a confirmation message displays with the **Dependencies** button. See the Admin guide for more information on the dependencies report.

  Note: When deleting a production the production images are deleted, not the original images.

  Note: If you delete a production set in Relativity aiR, the documents themselves are not deleted. Any tagging or coding on those documents is retained. Only the production set and its produced images and Bates numbers are removed.
- **Back**—Redirects you to the item list on the Production Sets tab
- **Edit Permissions**—Displays a security page where you can set user permissions on a production set. You can edit rights only on the current production set. By default, the Production Set tab is secured according to the workspace-level rights. See the Admin guide for more information on setting permissions on objects.
- **View Audit**—Displays the history for the production.

The Production Set details options view also shows Production Status Information, Basic Settings, Numbering, Branding, Sorting, Other, and the Production Data Source. After you run the production, you can also view the first and last Bates values associated with it.

28.5.8.2 Previewing a production

In the Production console, click **Preview Production** to review your settings before running the production. Confirm that the basic settings, numbering, branding, sorting, and any other options are correct. For more information, see Production console on page 484.

(Click to expand the image)



28.5.9 Tracking multiple redaction sets

To track multiple redaction sets on the same document, complete these steps:

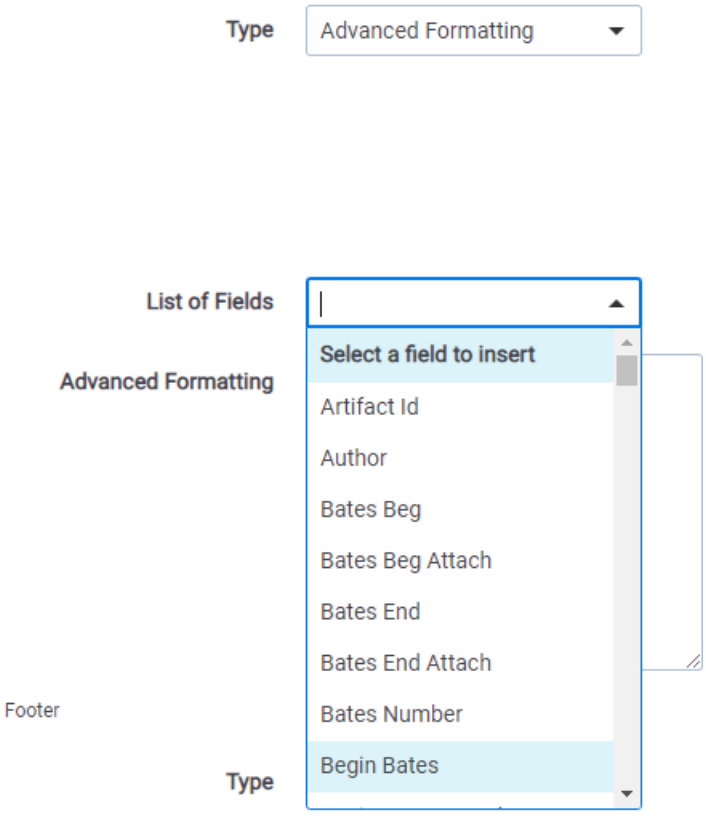
- Create multiple redaction sets by defining different markups. See Markups on page 342.
- Use each markup to redact the same document.
- Create a production and select a specific markup.

When you select the markup, it controls the redactions branded during production, so you can track multiple redaction sets on the same document, and generate different productions.

28.5.10 Advanced Formatting for Branding

Advanced Formatting is a type of branding available on the Production Set form.

With Advanced Formatting, you can brand headers and footers with a combination of fields from the Advanced Formatting drop-down list, free-form text, and carriage returns. It also supports a scripting language for creating conditional branding based on production, document, and page fields.



Conditional statements use three root context objects: Production, Document, and Page. Each object is described in the tables below.

- Production object below
- Document object on page 475
- Page object on page 477

Note: If you add a field to a conditional statement incorrectly, you can still save and run the production set. However, the branding produces incorrect results without generating an error.

28.5.10.1 Production object

The production object stores information about the production. It is the same for every item branded in the production.

Name	Data type	Description	Name in Advanced Formatting drop-down list
Document	DocumentDrop	The current document being branded.	N/A
ProductionId	int	The ID of the production.	Production Id
ProductionName	string	The name of the production.	Production Name
TotalDocuments	int	The total number of documents in the production.	Total Documents
TotalImages	int	The total number of images in the production.	Total Images

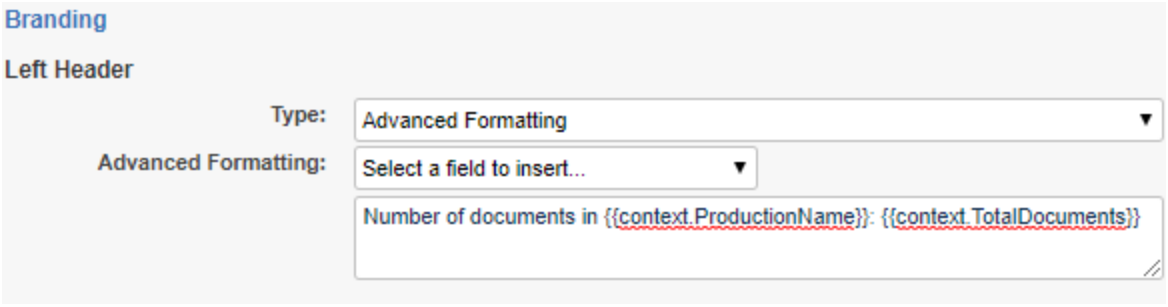
Name	Data type	Description	Name in Advanced Formatting drop-down list
WorkspaceId	int	The ID of the workspace.	Workspace Id

Example of Advanced Formatting with the production object

Example of Advanced Formatting with the production object

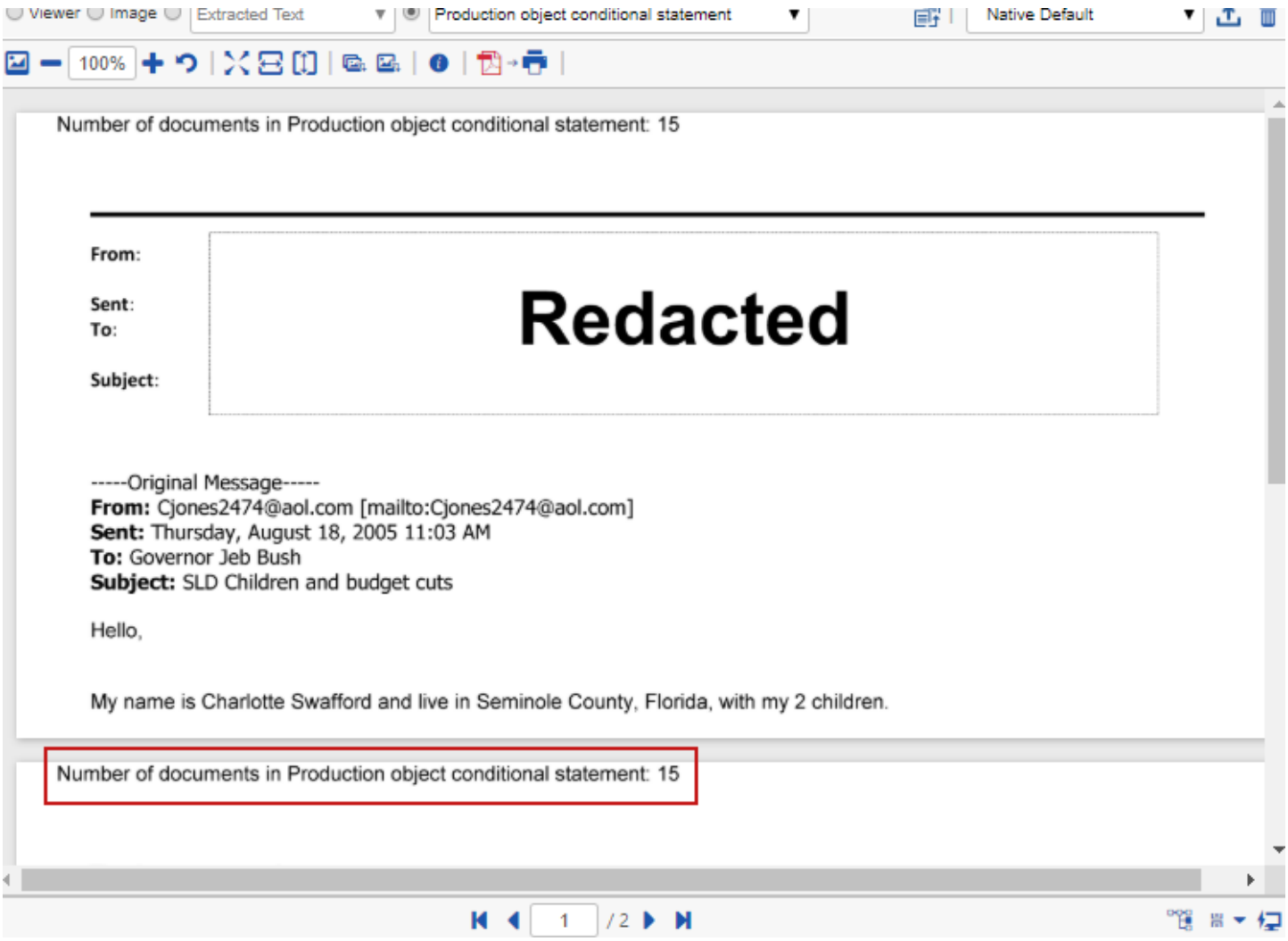
Note: The example in this section does not demonstrate everything that you can do with the production object.

As shown in the screen shot below, you can combine free-form text with productions objects.




```
Number of documents in {{context.ProductionName}}: {{context.TotalDocuments}}
```

The screen shot below shows a document that was branded per the command in the screen shot above. In this example, the ProductionName is Production object conditional statement, and the TotalDocuments is 15.



28.5.10.2 Document object

This object stores information about the document and changes for each document.

Name	Data type	Description	Name in Advanced Formatting drop-down list
ArtifactId	int	The ArtifactId of the document in the production.	Artifact Id
HasRedactions	bool	If set, the current document contains redactions on at least one page.	Document Has Redactions
HasPlaceholder	bool	If set, the current document is a placeholder.	Has Placeholder
BeginBates	string	The first bates number in this document.	Begin Bates
EndBates	string	The last bates number in this document.	End Bates
BeginBatesAttachment	string	The first attachment bates number in this document.	Begin Bates Attachment
EndBatesAttachment	string	The last attachment bates number in this document.	End Bates Attachment

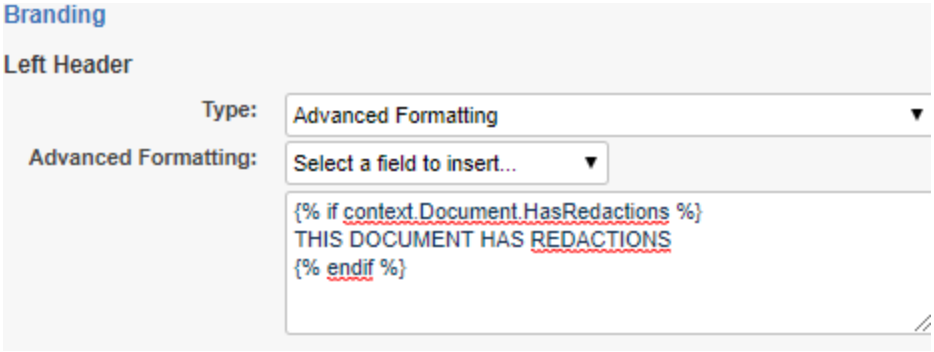
Name	Data type	Description	Name in Advanced Formatting drop-down list
Page	PageDrop	The current page being branded.	N/A
["Field Name"]	FieldDrop	Returns the field value for the specified document field. Returns null if the field does not exist or is not a supported field type. For example, context.Document["Control Number"].Value Only the following field types are supported: **Notes:** These values are in string format as done in object manager. Custom Placeholders also supports these field types. Reflected fields are not supported. • case FieldType.Date • case FieldType.Decimal • case FieldType.FixedLengthText • case FieldType.WholeNumber • case FieldType.YesNo • case FieldType.SingleChoice • case FieldType.MultipleChoice	N/A

Example of Advanced Formatting with the document object

Example of Advanced Formatting with the document object

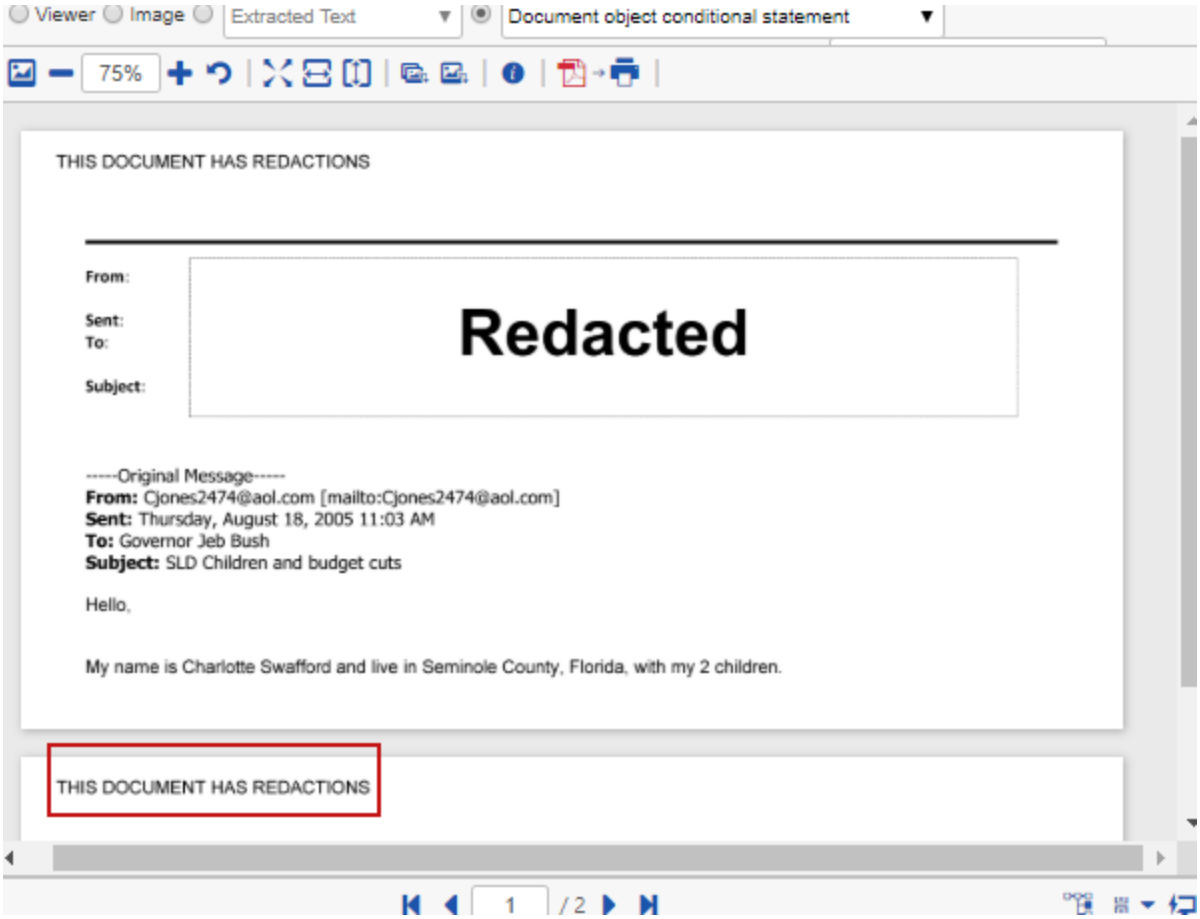
Note: The example in this section does not demonstrate everything that you can do with the document object.

As shown in the screen shot below, you can create conditional statements with the document object.




```
{% if context.Document.HasRedactions %}
THIS DOCUMENT HAS REDACTIONS
{% endif %}
```

The document in the screen shot below is branded per the command in the screen shot above. Since the document has a redaction, it meets the requirements of the conditional statement, so the free-form text is branded on this document.



28.5.10.3 Page object

The page object stores information about the page and will change for each page.

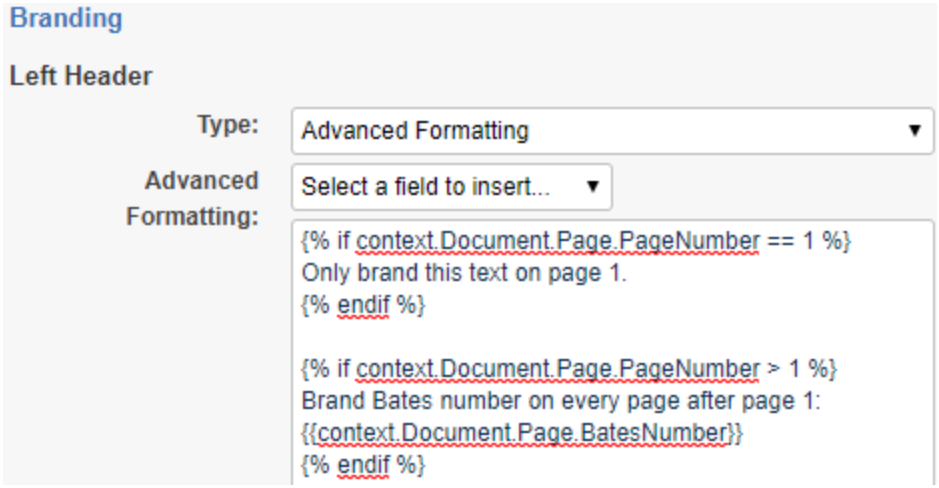
Name	Data type	Description	Name in Advanced Formatting drop-down list
BatesNumber	string	The bates number of the current page.	Bates Number
FileName	string	The name of the file.	File Name
HasRedactions	bool	If set, this page has redactions.	Page Has Redactions
IsPlaceholder	bool	If true, this page is a placeholder page.	Is Placeholder
PageNumber	int	The current page.	Page Number

Example of Advanced Formatting with the page object

Example of Advanced Formatting with the page object

Note: The example in this section does not demonstrate everything that you can do with the page object.

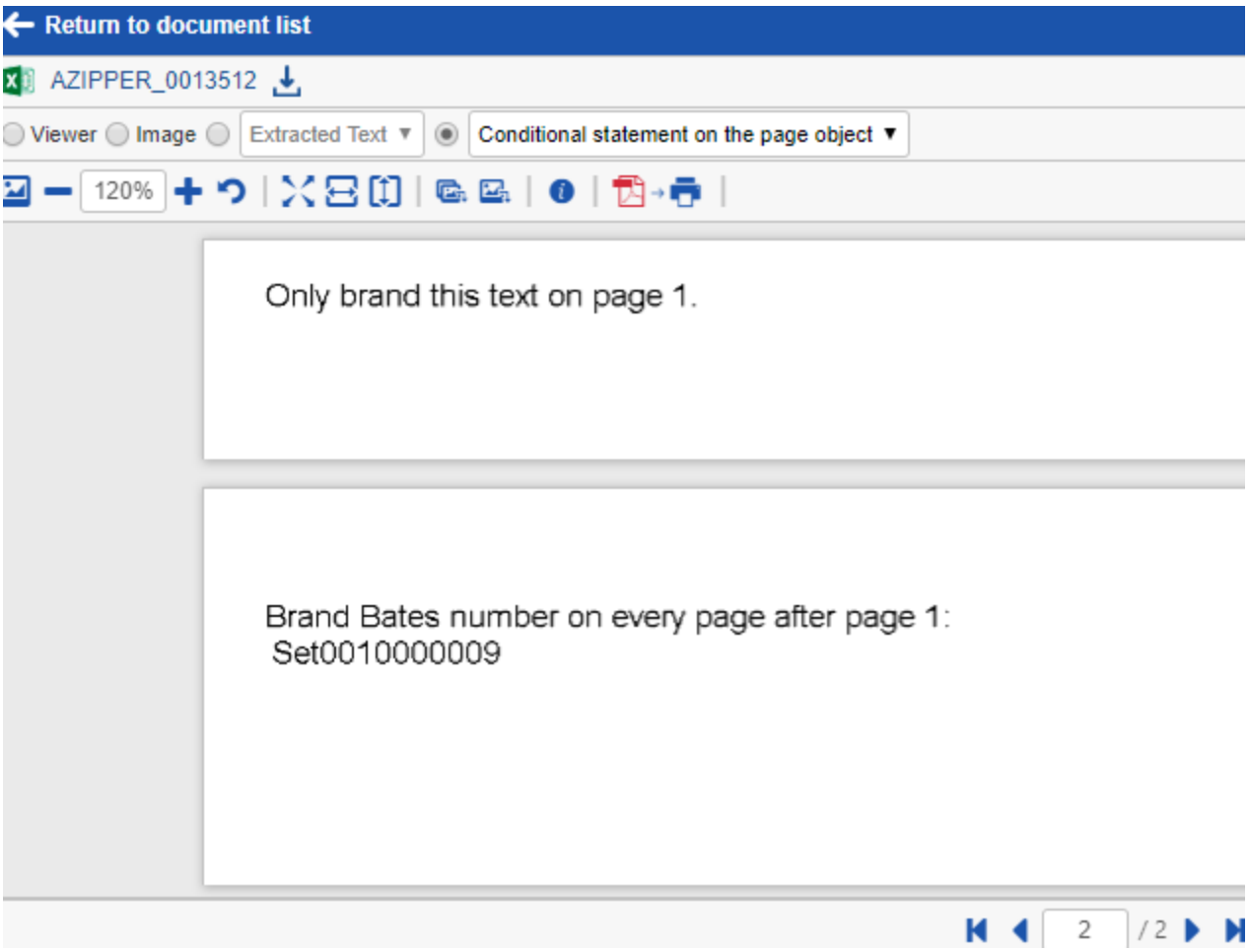
As shown in the screen shot below, you can use page objects in conditional statements.




```
{% if context.Document.Page.PageNumber == 1 %}
Only brand this text on page 1.
{% endif %}

{% if context.Document.Page.PageNumber > 1 %}
Brand Bates number on every page after page 1:
{{context.Document.Page.BatesNumber}}
{% endif %}
```

The document in the screen shot below is branded per the commands in the screen shot above. The free-form text from the first conditional statement is only printed on the first page. The free-form text from the second conditional statement is only printed on the second page.



28.5.10.4 Script examples

The following examples show common Advanced Formatting scripts:

- Brand the free-text, Production Name, and Page Number on every page.

```
Production Name: {{context.ProductionName}}
Page # {{context.Document.Page.PageNumber}}
```

- Brand the free-text on pages that have redactions.

```
{% if context.Document.Page.HasRedactions%}
THIS PAGE CONTAINS REDACTIONS
{% endif %}
```

- Brand the free-text on pages that have a specific page number.

```
{% if context.Document.Page.PageNumber == 1 %}
This text will be branded only on page 1
{% endif %}
```

- Brand the Bates Number on every page after page number 1.

```
{% if context.Document.Page.PageNumber > 1 %}
{{context.Document.Page.BatesNumber}}
{% endif %}
```

- Brand the free-text on the pages that fall between a page range.

```
{% if context.Document.Page.PageNumber > 1 and context.Document.Page.PageNumber
< 11%}
Confidential
{% endif %}

{% if context.Document.Page.PageNumber > 11 and context.Document.Page.PageNumber
< 21%}
Attorneys' Eyes Only
{% endif %}
```

- Brand the document that has a document field with specific value.

```
{% if context.Document["Confidentiality"].Value == "Attorneys' Eyes Only" %}

Confidential - Attorneys' Eyes Only

{% endif %}
```

28.6 Production data source

The production data source attaches saved searches to your production set. With the production data source you can specify the type of production and select placeholders from your placeholder library to customize your production. By setting the placeholder on the data source you can include multiple placeholders within a single production. The placeholder is based on the saved search attached to the production data source.

Note: You must have view, add, and edit permissions for the Production Data Source object in order to successfully create a data set. We also recommend the delete permission.

28.6.1 Adding a production data source

To add a production data source to your production:

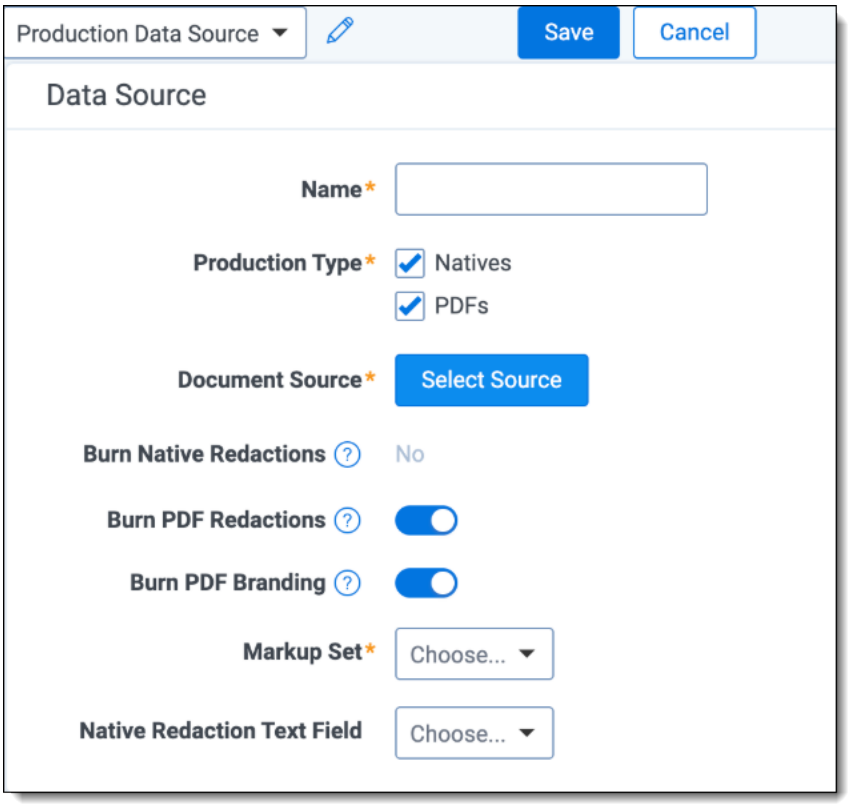
1. Navigate to the **Production** tab.
2. Select the **Production Sets** tab.
3. Click the name of the production where you want to add a data source.
4. Scroll down to the **Production Data Source** card.
5. Click **New**. The Add Production Data Source window opens.
6. Enter a **Name** for the production.
7. Select a **Production Type**.

Note: The PDF option is for rendered PDFs i.e., natives which were converted to PDFs and stored.

8. Select a **Document Source** from the available saved searches to use as a data source for the production.

Note: You must create public saved searches in order for your searches to populate another Relativity user's Available Items list.

9. Complete the following fields. Available fields depend on the Production Type selected.



- **Use Placeholder**—a single-choice field to add image or PDF placeholders to the data source. Documents without images or PDFs receive a placeholder (slip-sheet) in their place. The placeholder receives the same branding as the rest of the produced images. This option is only available if you produce images or PDFs.
  - **When No Image/PDF Exists**—inserts a placeholder only when no image or PDF exists for a document.
  - **Always Use Placeholder**—always inserts an image or PDF placeholder even when an image exists for a document.

- **Never Use Placeholder**—this is the default option. Never inserts an image or PDF placeholder for any document.

- **Placeholder Image Format**—(required) brands the Placeholder image as the file type selected. This field is set to TIFF by default, but users have the option to brand placeholder images as JPEG files too.
- **Burn Redactions**—indicates that redactions are applied to the documents when this field is enabled. Toggle On to apply redactions to documents. Toggle Off to not apply redactions. If you select to burn native redactions with the Burn Native Redactions field, this automatically displays a value of **No**.
- **Burn Native Redactions**—toggle on to include redacted natives as part of the production set. This automatically sets to **No** if you've enabled the Burn PDF Redactions field. Toggling this field on makes the Markup Set and Native Redaction Text Field settings required below.
- **Burn PDF Redactions**—toggle on to include redacted PDFs as part of the production set. This automatically sets to **No** if you've enabled the Burn Native Redactions field. Toggling this field on makes the Markup Set and Native Redaction Text Field settings required.
- **Burn PDF Branding**—toggle on to brand PDFs during Production with the configured settings. This field automatically appears when you select PDF as a Production Type.
- **Markup Set**—indicates which markup set is used to apply standard or native redactions to the production images. This field is only visible if you toggled on burn redactions or native redactions.

Notes:

- You cannot have the same document in more than one production data source.
- The Native Time Zone Offset field controls the date and time displayed on redacted and highlighted images. If necessary, you may want to review and adjust the UTC value to avoid incorrect time designations on documents and inaccurate productions.
- You cannot select more than one Burn Redaction option in a single data source.

- **Native Redaction Text Field**—select the field you want to use when burning native redactions. This field is only visible if you enabled the Burn Native Redactions field.

Note: There is an expected delay between a Production Set being marked as completed, and the designated Native Redaction Text field being populated.

- **Placeholder Text Destination Field**—long-text field on the Document object where placeholder text is written during production. This field is available when Use Placeholder is set to When No Image/PDF Exists or Always Use Placeholder.

Note: Placeholder Text Destination Field defaults to None. When a field is selected, the system copies the Placeholder Text value from each placeholder to the designated field for every document that receives that placeholder during production. If a placeholder's Placeholder Text is empty, the system writes null to the selected field.

10. Click **Save**.

28.7 Placeholders

You can create your own unique placeholders for productions using images or custom text. Once you create the placeholders, you can attach the placeholders to the production data source. You can also produce the same

document in multiple productions with different placeholders. The Placeholder library automatically includes a default image placeholder.

Note: When creating a template workspace using production, Relativity automatically copies Placeholders.

28.7.1 Creating an image placeholder

You can create an image placeholder using saved image files on your machine. Relativity supports uploading of TIF, JPEG, PNG, BMP, and GIF files for image placeholders. When saving the image placeholder, it is saved as a JPG file. To create and save an image placeholder for your productions, follow these steps:

Note: It's recommended image placeholders image size should be 2,550 pixels by 3,300 pixels at 300 DPI.

1. Navigate to the **Production** tab.
2. Click the **Placeholder** tab.
3. Click **New Placeholder**. To edit an existing image placeholder, click **Edit** next to the placeholder name.
4. Add or edit the following fields as necessary. Required fields are orange.
    - **Name**—the name of your Placeholder. Give your placeholder a descriptive name based on the image.
    - **Type**—the type of placeholder. Select **Image**.
    - **Placeholder**—the location of the image on your computer. Click **Choose File** and browse to the location of the image you want to use.
    - **Placeholder Text**—the value written to a document field during production when this placeholder is applied. Independent of the placeholder's visual content (image, custom text, or PDF).

      Note: The Placeholder Text field is optional. Leave it blank to write null to the destination field for any document that receives this placeholder. To specify which document field receives this value, set Placeholder Text Destination Field on the production data source.
5. Click **Save**.

28.7.2 Creating a custom placeholder

You can create a custom placeholder with your own text using the custom text editor within Relativity. To create a custom placeholder for your productions, follow these steps:

Note: If you add a large amount of text or upload large images to your custom placeholders there can be an increase in the staging and producing time of your productions.

1. Navigate to the Production tab.
2. Click the **Placeholder** tab.
3. Click **New Placeholder**. To edit an existing custom placeholder, click **Edit** next to the placeholder name.
4. Add or edit the following fields as necessary. Required fields are orange.
    - **Name**—the name of your Placeholder. Give your placeholder a descriptive name based on the custom text.
    - **Type**—the type of placeholder. Select **Custom**.
    - **Custom Text**—using the custom text editor enter the text you want to appear on your placeholder. You can also change your entered text using the options in the text editor.

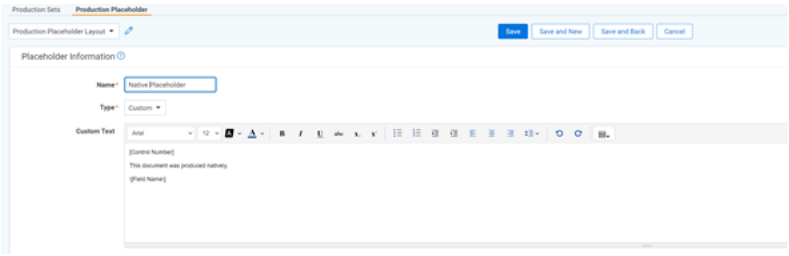
- The rich text editor for Placeholders contains a plugin you can use to add any document field or Bates number field to stamp on the placeholder. The field name inserts into your custom placeholder, but when you kick off the production, the field name dynamically updates per document. For example, [ControlNumber] updates with the control number field for the document the placeholder corresponds to. Custom type placeholders support document fields using the field name surrounded by brackets: [**Document Field Name**]. To include a square bracket in the plain text of the placeholder, escape it with a backslash: \[bracketed phrase\].

  Note: You can only use the date, decimal, fixed-length text, whole number, yes/no, single and multiple choice fields as a token for your placeholder. You must have permissions to the document fields to use them as a token for your placeholder.

- **Placeholder Text**—the value written to a document field during production when this placeholder is applied. Independent of the placeholder's visual content (image, custom text, or PDF).

  Note: The Placeholder Text field is optional. Leave it blank to write null to the destination field for any document that receives this placeholder. To specify which document field receives this value, set Placeholder Text Destination Field on the production data source.

5. Click **Save**.



28.7.3 Creating a PDF placeholder

You can create a PDF placeholder using saved PDF files on your machine. To create and save a PDF placeholder for your productions, follow these steps:

1. Navigate to the Production tab.
2. Click the **Placeholder** tab.
3. Click **New Placeholder**. To edit an existing placeholder, click **Edit** next to the placeholder name.
4. Add or edit the following fields as necessary. Required fields are orange.
   - **Name**—the name of your Placeholder. Give your placeholder a descriptive name.
   - **Type**—the type of placeholder. Select PDF.
   - **Placeholder**—the location of the PDF file on your computer. Click Choose File and browse to the location of the PDF file you want to use.
   - **Placeholder Text**—the value written to a document field during production when this placeholder is applied. Independent of the placeholder's visual content (image, custom text, or PDF).

     Note: The Placeholder Text field is optional. Leave it blank to write null to the destination field for any document that receives this placeholder. To specify which document field receives this value, set Placeholder Text Destination Field on the production data source.

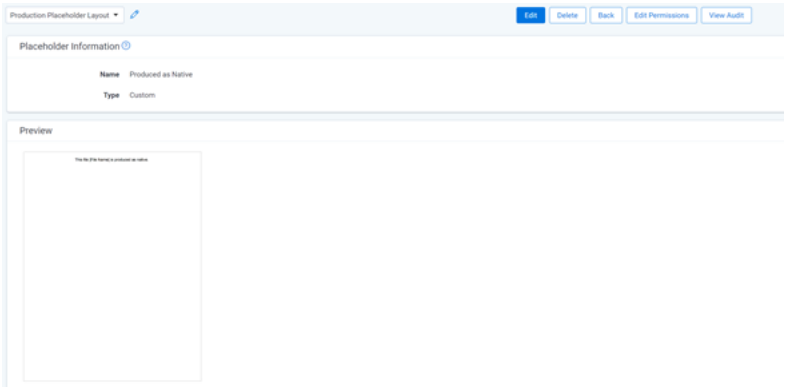
5. Click **Save**.

28.7.4 Previewing placeholders

You can preview your image and custom placeholders via the Placeholder Library before you attach the placeholder to your production data source. To preview your placeholders:

1. Select the **Placeholder** tab.
2. Click the name of the placeholder you want to preview. The placeholder opens in the Placeholder Layout displaying placeholder information and a preview.
3. Navigate through your placeholder library using the navigational arrows in the upper right of the Placeholder layout.

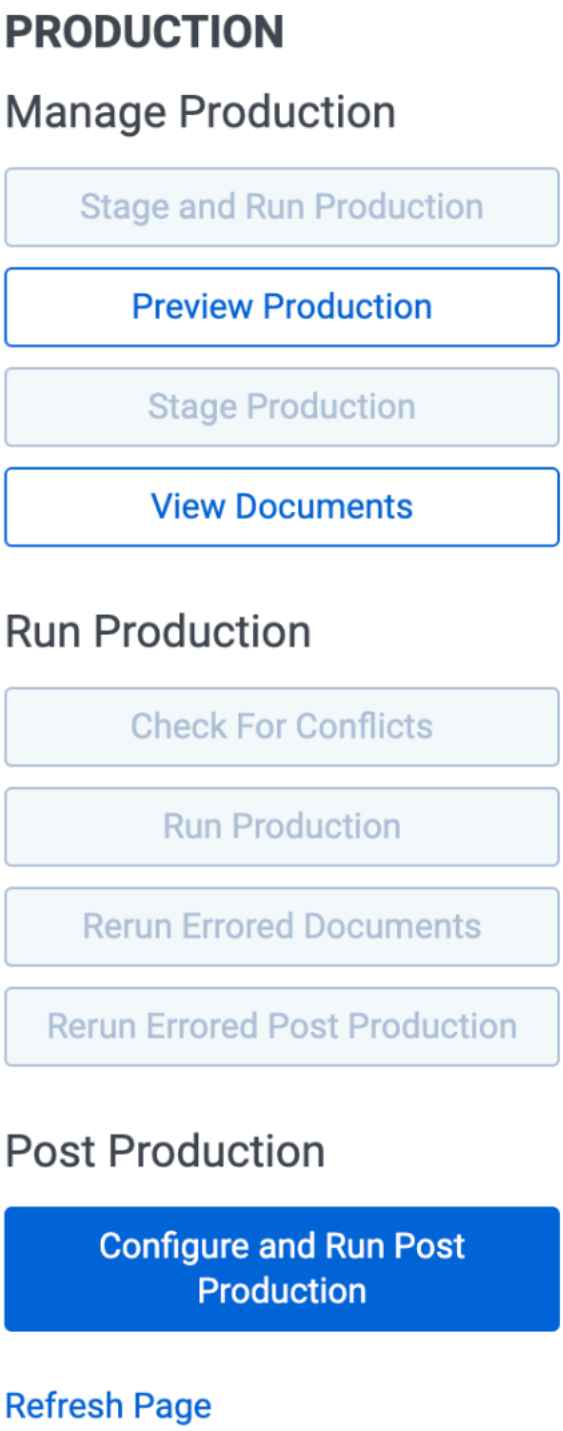
If a placeholder does not generate the way you want it to, click **Edit** to open the placeholder and make any necessary changes.



28.8 Production console

After you complete your production set and add your data sources, you can access the Production console to stage, run, and monitor your production. The Production console also includes a progress bar that updates production status in real time.

To access the production console, click the name of the production set.



28.8.1 Manage Production

The Manage Production section of the Production console displays the following options:

- **Stage and Run Production**—Takes a snapshot of the data sources and then automatically begins producing the staged documents. For more information, see Stage and run a production.
    - **Cancel**—Stops the stage and run job.
- **Preview Production**—Displays a sample image showing how Relativity applies branding to documents in the production.

- **Stage Production**—Takes a snapshot of the data sources for the production. For more information, see Stage a production.
- **View Documents**—Displays all documents included in the production set. For more information, see View documents.
- **Note:** You must have View Production and View Data Source permissions to view the document list. Documents you do not have access to are excluded from the list.
- **Cancel Staging**—Cancels a staging production. This is a dynamic button that appears once you click Stage Production.

  Note: Canceling a production may take time to complete, depending on the size of the production or the number of documents in scope.
- **View Staging Errors** —Displays problematic documents causing staging errors.

28.8.2 Run Production

The Run Production section of the Production console displays the following options:

- **Check for Conflicts**—Checks whether the production set includes any documents that conflict with existing production restrictions..For more information, see Check for production conflicts.
- **Run Production**—Runs the production for staged documents and automatically creates a saved search. If the production set includes documents with conflicts, the Production Restrictions dialog appears. If you are a system admin, you can resolve this using the following options:
  - **Override and Continue**—Proceeds with the production without removing the conflicts based on the Override Production Restrictions permission.
  - **Cancel**—Stops the production from running.

  For more information, see Run a production.
- **Rerun Errored Documents**—Produces documents that previously errored, after you make corrections. This button becomes active only after the production completes. If any documents resulted in errors or alerts, click this button to rerun them.
- **Rerun Errored Post Production**—Retries Post Production steps that resulted in errors. This button is active only when one or more Post Production steps completed with an error.
- **Cancel Production**—Cancels a staging production. This button appears after you click Stage Production.
- **View Branding Errors**—Displays a dialog with all documents and their branding error messages. Click a document in the dialog to open it and investigate the error. This button appears only when branding errors occur during a production run.
- **View Production Errors and Warnings**—Displays a dialog listing the validation and production errors and warnings that occurred.

28.8.3 Post Production

The Post Production section of the Production console displays the following options:

- **Configure and Run Post Production** - initiates Post Production after production completion.

28.8.4 Advanced Options

The Advanced Options section of the Production console displays the following option:

- **Copy To Legacy Document Fields**—Opens the script window for the Copy to Legacy Document Fields script. Use this script to update Bates fields on the Document object with Bates numbering information from a selected production's Production Information RDO. For more information, see Copy To Legacy Document fields in the admin guide.

28.8.5 Stage and run a production

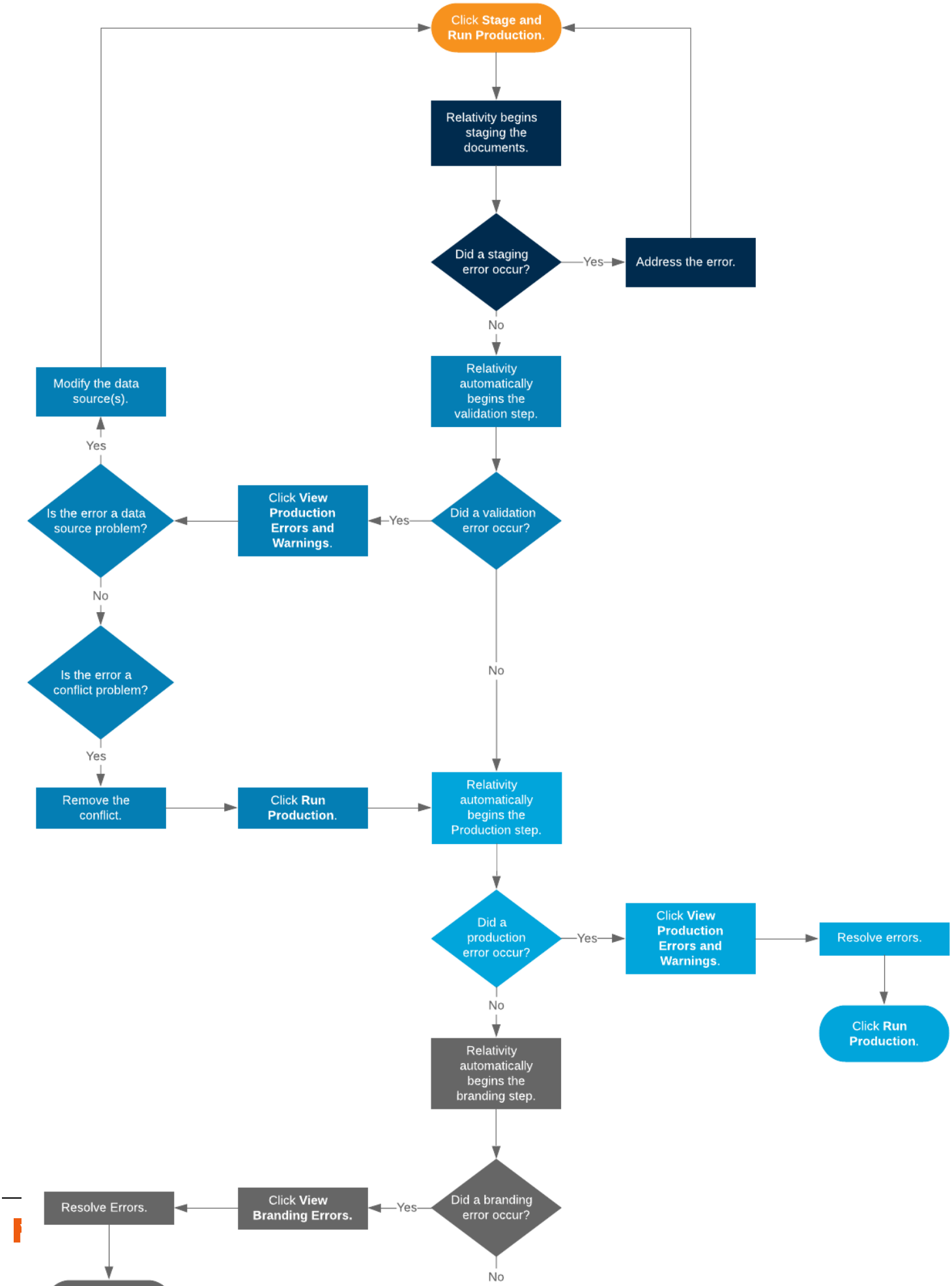
To stage and run a production in a single step, click **Stage and Run a Production** on the Production console.

28.8.5.1 Staging and running a production

A stage and run production job goes through 4 steps:

1. Staging on page 489
2. Validation on page 489
3. Production on page 490
4. Branding on page 490

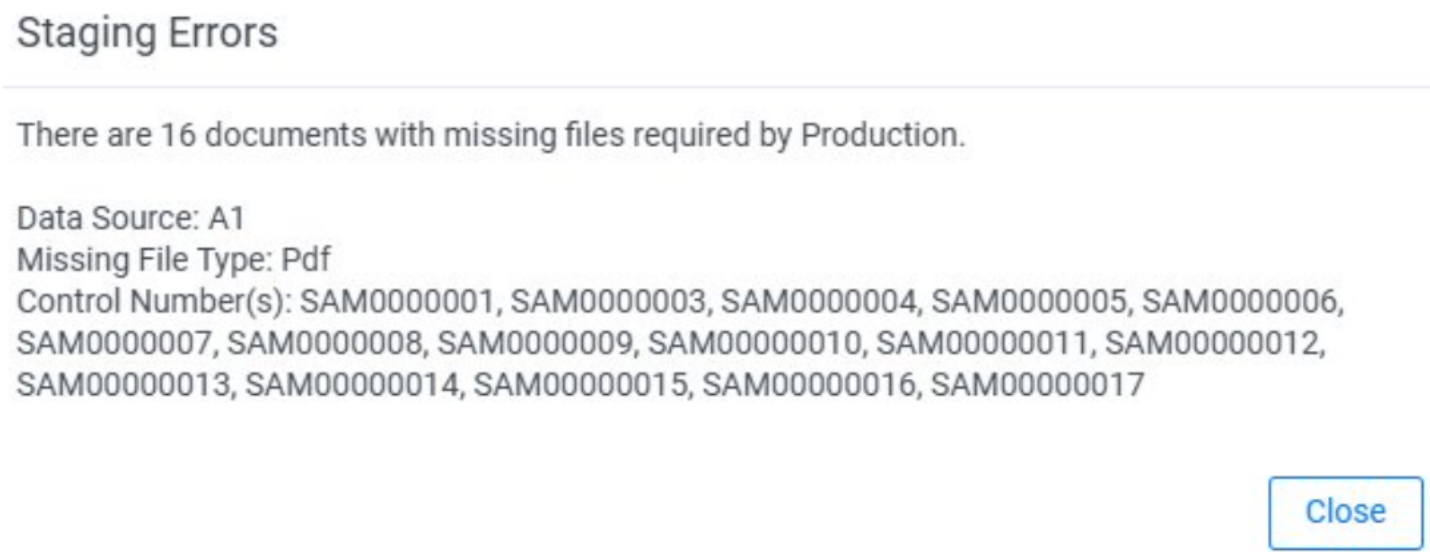
Stage and Run Production



Staging

During the staging step, Relativity takes a snapshot of the data sources. After staging finishes, Relativity automatically begins the validation step.
Staging errors occur when:

- **The same document is found in multiple data sources.**
  When the same document appears in multiple data sources, an error message appears. The error message identifies the data sources that returned the same document and which document they returned. To resolve the error, modify the saved searches you selected as your data sources so they do not return any of the same documents.
- **There are no documents in the data sources.**
  When no documents are found in the data sources, an error message appears. To resolve the error, make sure the saved searches you selected as your data sources are returning documents.
- **There are missing files in the data source.**
  When documents in the data source do not have images, natives, or PDFs, an error message appears. To resolve the error, modify the data sources, then click Stage and Run Production.



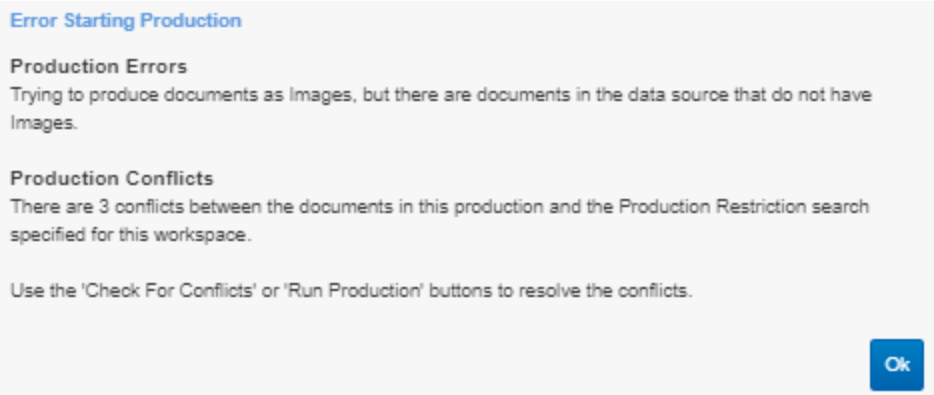
When an error occurs, click **View Production Errors and Warnings** on the Production console to open the Error Starting Production pop-up. The Error Starting Production pop-up lists the errors that occurred.

Conflicts occur when the data sources have documents that are also in the saved search selected in the Production Restriction field.

If a staging error occurs, address the error and then click **Stage and Run Production**.

Validation

During validation, Relativity performs a conflict check and data source validation. After validation finishes, production begins.
When a validation error occurs, click **View Production Errors and Warnings** on the Production console to open the Error Starting Production pop-up. The Error Starting Production pop-up lists the errors that occurred.



Conflicts occur when the production data sources contain documents that the saved search in the Production Restriction field also contains.

Conflict resolution option	Fix
Remove the conflict	Remove documents from the production set that are also in the saved search selected in the Production Restriction field. To remove the conflict: 1. Click **Check for Conflicts** on the Production console. The Production Restrictions pop-up will open. 2. Click **Remove Conflict** on the Production Restrictions pop-up. 3. Click **Run Production** on the Production console.
Override the conflict	Keep the documents in the production set that are also in the saved search selected in the Production Restriction field. To override the conflict: 1. Click **Run Production** on the Production console. The Production Warnings pop-up will open. 2. Click **Override and Continue** on the Production Warnings pop-up. The production job will continue without removing the conflict documents.
Modify the production restriction	Modify the Production Restriction field so none of the documents in the production restriction saved search are also in the production set. For information on modifying a production restriction, see Adding and editing production restrictions. After modifying the production restriction, click **Stage and Run Production** on the Production console.

Production

During production, Relativity produces the staged documents. After production finishes, branding begins.
If a production error occurs, click **View Production Errors and Warnings** on the Production console to see why the error occurred. After addressing the error, click **Run Production** on the Production console.

Branding

During branding, Relativity applies redactions and the specified header and footer to the images. After this step finishes, your production job is complete.

To resolve branding errors:

1. Click **View Branding Errors** on the Production console to open the Branding Errors pop-up.



2. In the **Branding Error Message** column, find the error and apply the fix:

Branding Error Message	Fix
Could not find file <file path>.	Because the system can not find the file path to the image, make sure the image exists at the file path mentioned in the Branding Error Message. Image or re-import the document.
The file at <file path> could not be opened or is not a valid image file.	• If the document is encrypted, add the document's password to the Password Bank. For more information, see Password Bank. • Make sure Relativity supports the file type of the image. You may need to image or import the document again.
The process cannot access the file <file path> because it is being used by another process.	Click **Rerun Errored Documents** on the Production console.
The number of images for document has changed after this production was initially run.	After reimaging, the number of images related to this particular document has changed. This may be related to issues with imaging or applied redactions. To ensure Bates numbering is correct for the entire production, recreate the production set.

3. Click **Rerun Errored Documents** to finish the production job.

To cancel the job, click **Cancel** on the Production console.

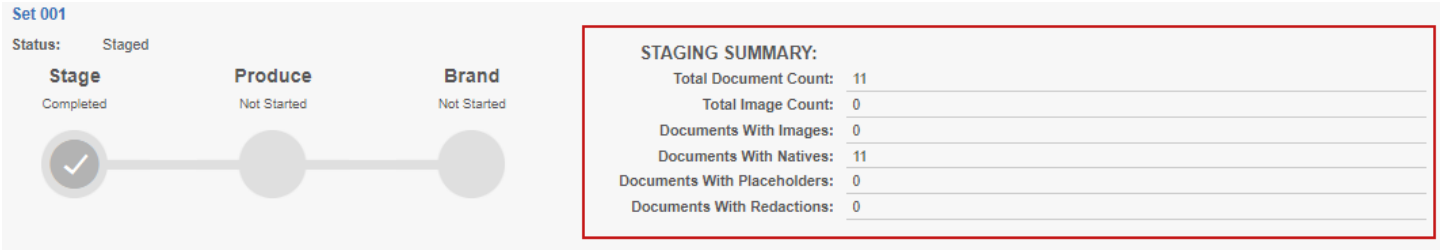
Post Production

This step is available on the Production console only if you enabled Post Production when creating the production set. During this step, Relativity runs automated post-production tasks, such as copying Bates numbers to document fields.

28.8.5.2 Checking production status

During each part of the production, a report is available in the Status section. The Stage, Produce, and Brand steps each have their own report. Use these reports to identify the number of documents, images, redacted documents, etc.

Staging Summary fields

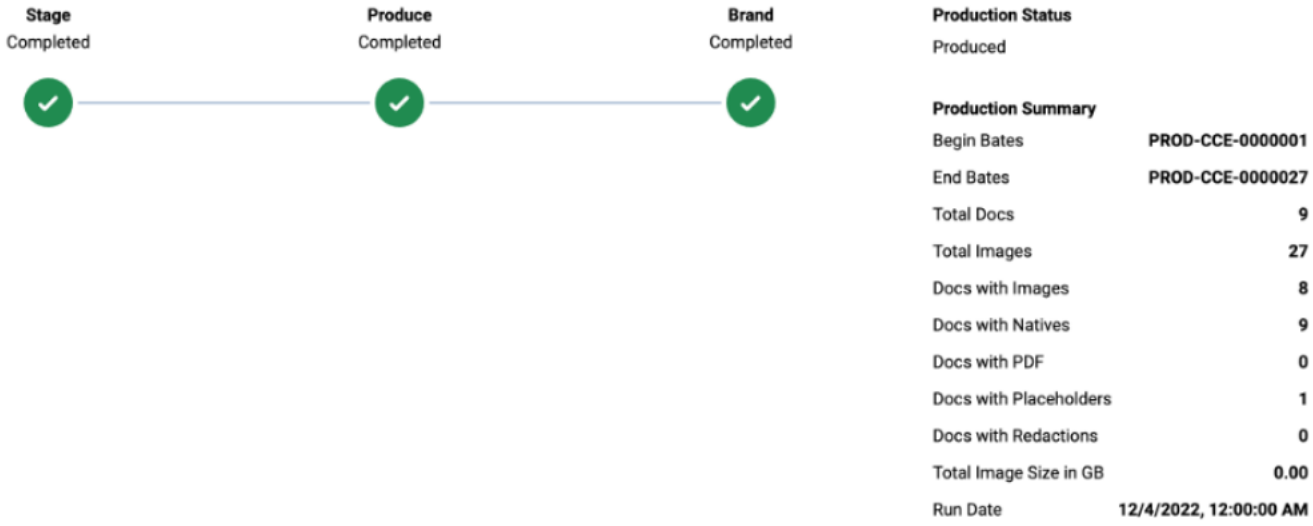


Staging Summary fields include:

- **Total Documents Count**—Lists the number of documents found during staging.
- **Total Images Count**—Lists the number of images found during staging.

- **Documents With Images**—Lists the number of documents that include images found during staging
- **Documents With Natives**—Lists the number of documents that include native files found during staging.
- **Documents With Placeholders**—Lists the number of documents that include Placeholders found during staging.
- **Documents With Redactions**—Lists the number of documents that include redacted images found during staging.

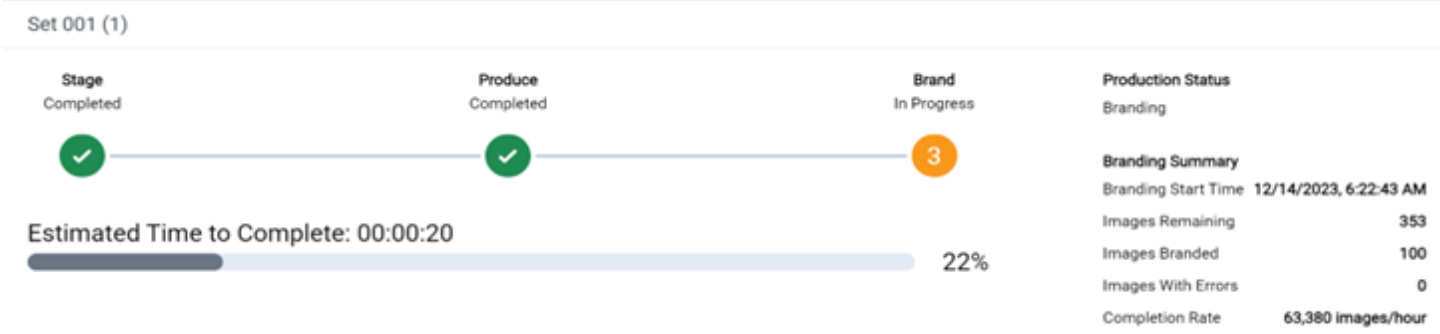
Production Summary fields



Production Summary fields include:

- **Begin Bates**—Lists the Bates number of the first document in the production set.
- **End Bates**—Lists the Bates number of the last document in the production set.
- **Total Docs**—Lists the number of documents included in the production set.
- **Total Images**—Lists the number of images included in the production set.
- **Docs With Images**—Lists the number of documents that include images included in the production set.
- **Docs With Natives**—Lists the number of documents that include natives included in the production set.
- **Docs With PDFs**—Lists the number of documents that include stored PDFs in the production set.
- **Docs With Placeholders**—Lists the number of documents that include placeholders included in the production set.
- **Documents With Redactions**—Lists the number of documents that include redacted images and redacted natives included in the production set.
- **Total Image size in GB**—Lists the size of images in GB.
- **Run Date**—Lists the date of when the production was run.

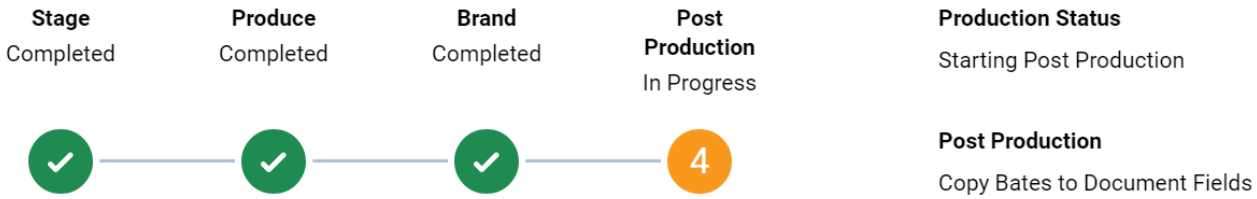
Branding Summary fields



Branding Summary fields include:

- **Start Time**—Lists the start time of branding.
- **Branding Completion**—Lists the time of completion for branding.
- **Completion Rate**—Lists the progress of branding.
- **Estimated Time Remaining**—Lists the amount of time left in branding.

Post Production Summary fields



Post Production Summary fields include:

- **Copy Bates to Document Fields**—Lists the progress of the step.

28.8.6 Stage a production

Before you can run a production, you must stage it. During staging, Relativity takes a snapshot of the data sources and prepares the documents. After you assign your data sources, placeholders, and production set, you are ready to stage.

28.8.6.1 Stage a production

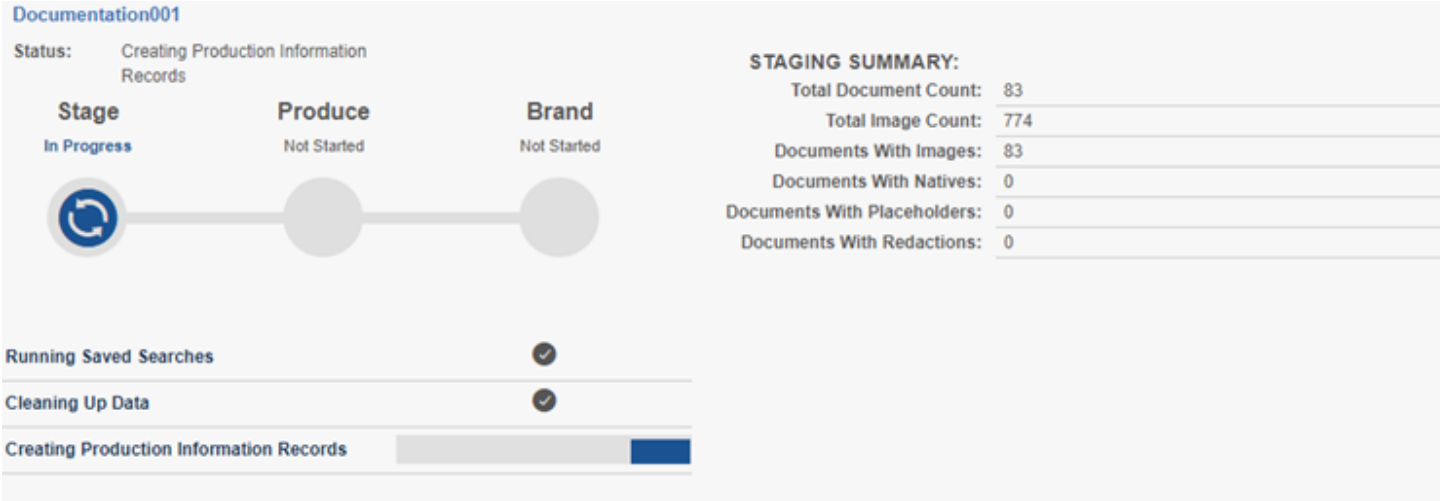
To stage a production:

- On the Production console, click **Stage**.

To stage and run a production in a single step:

- On the Production console, click **Stage and Run Production**.
  For more information, see Stage and run a production.

The progress bar displays the following:

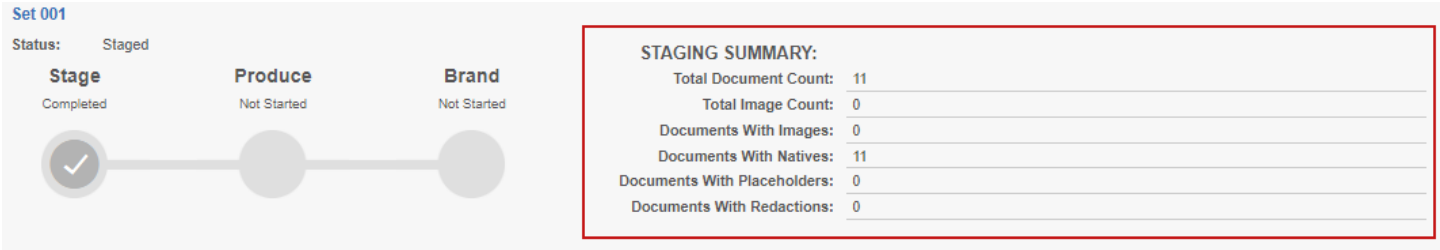


- **Staging**—Relativity is staging the production.
- **Running Saved Searches**—Relativity is running the saved searches associated with the production data sources.
- **Cleaning Up Data**—Relativity pre-sorts the documents and deletes any Production Information objects that may already exist if the production is being restaged.
- **Creating Production Information Records**—Relativity is creating the Production Information records associated with the production.

Relativity captures only the data sources from the most recent staging snapshot. If you modify a data source after staging, those changes do not appear in the production run. Examples of changes include modifying the conditions of a saved search for a data source and adding or deleting a data source from the production. To capture data source changes, restage the production immediately before you run it.

28.8.6.2 Staging Summary fields

During staging, a report appears in the Status section. Use this report to identify document and image counts, redacted documents, and other staging details.



Staging Summary fields include:

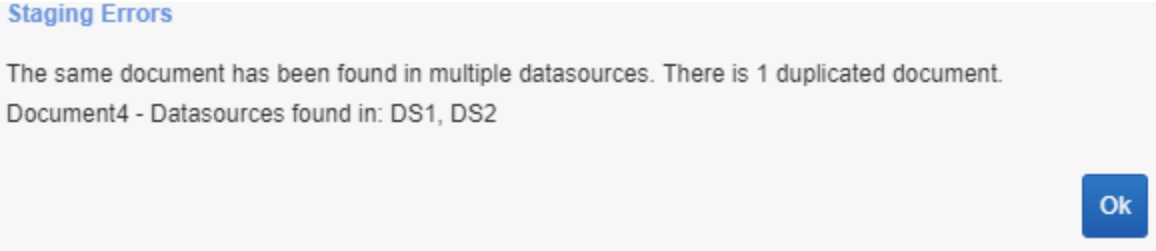
- **Total Documents Count**—Lists the number of documents found during staging.
- **Total Images Count**—Lists the number of images found during staging.
- **Documents With Images**—Lists the number of documents that include images found during staging
- **Documents With Natives**—Lists the number of documents that include native files found during staging.
- **Documents With Placeholders**—Lists the number of documents that include Placeholders found during staging.

- **Documents With Redactions**—Lists the number of documents that include redacted images found during staging.

28.8.6.3 Staging errors

Staging errors occur when

- **The same document is found in multiple data sources.**
  When the same document appears in multiple data sources, an error message identifies the affected data sources and document. To resolve this error, modify the saved searches for your data sources so that they do not return the same document.



- **There are no documents in the data sources.**
  When no documents are found in the data sources, an error message appears. To resolve this error, confirm that the saved searches for your data sources return documents.

28.8.7 View documents

You can view the total number of image and native files to produce and other specific information about each document included in a production.

To view documents in a production:

- On the Production console, click **View Documents**.

The View Documents window displays the following fields for each production document:

- Document Identifier
- Data Source Name
- Production Option
- Begin Bates
- End Bates
- Has Native
- Has Images
- Has Redactions

You can also find this information on the Production Information object.

View Documents

1 - 15 of 221 15 per page

Document	Data Source	Production Option	Begin Bates	End Bates	Has Native	Has Images	Has Redactions
Filter	Filter	Filter	Filter	Filter	(All)	(All)	(All)
REL0000005105	20191210_PROD001	Images	kCura00000001	kCura00000001	True	True	False
REL0000005105.0001	20191210_PROD001	Images	kCura00000002	kCura00000002	True	False	False
REL0000005105.0002	20191210_PROD001	Images	kCura00000003	kCura00000007	True	True	False
REL0000005105.0003	20191210_PROD001	Images	kCura00000008	kCura00000008	True	False	False
REL0000005105.0004	20191210_PROD001	Images	kCura00000009	kCura00000009	True	False	False
REL0000005105.0005	20191210_PROD001	Images	kCura00000010	kCura00000010	True	False	False
REL0000005105.0006	20191210_PROD001	Images	kCura00000011	kCura00000011	True	False	False
REL0000005105.0007	20191210_PROD001	Images	kCura00000012	kCura00000012	True	False	False
REL0000005105.0008	20191210_PROD001	Images	kCura00000013	kCura00000013	True	False	False
REL0000005105.0009	20191210_PROD001	Images	kCura00000014	kCura00000014	True	False	False
REL0000005105.0010	20191210_PROD001	Images	kCura00000015	kCura00000015	True	False	False
REL0000005105.0011	20191210_PROD001	Images	kCura00000016	kCura00000016	True	False	False
REL0000005105.0012	20191210_PROD001	Images	kCura00000017	kCura00000017	True	False	False
REL0000005105.0013	20191210_PROD001	Images	kCura00000018	kCura00000018	True	False	False
REL0000005105.0014	20191210_PROD001	Images	kCura00000019	kCura00000019	True	False	False

Close

28.8.8 Check for production conflicts

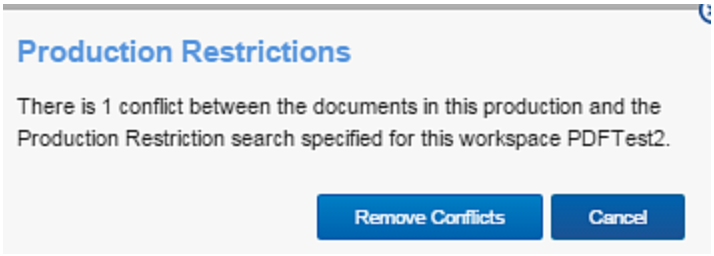
A conflict check compares the documents in your production against those in a saved search set in the **Production Restrictions** field on the workspace details page. For example, the saved search may contain conditions that identify privileged documents and their families — documents that should be excluded from production. See Production restrictions for more information.

Note: You must have permissions to the documents included in a production to remove production restrictions.

To check for production conflicts:

- On the Production console, click **Check for Conflicts**.

If a saved search is restricting the production, a Production Restrictions warning appears.



The warning includes the following options:

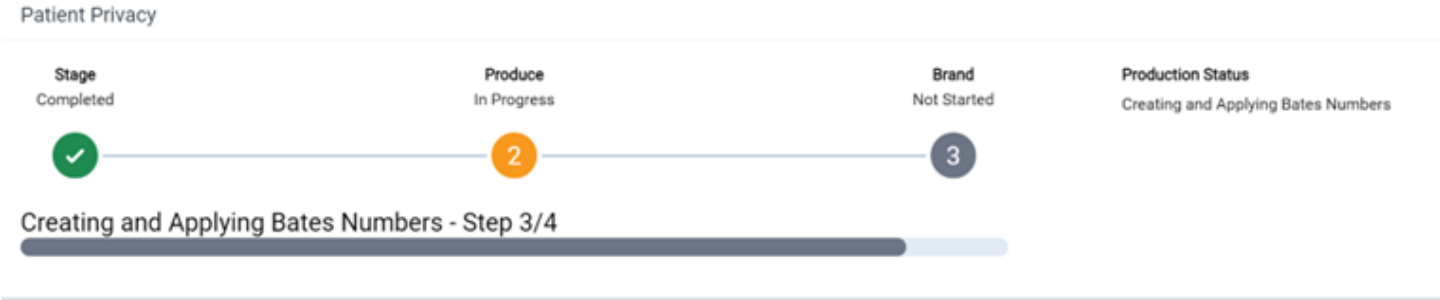
- **Remove Conflicts**—Deletes documents identified as conflicts from the production set (based on the Production Restrictions setting). If all the documents are conflicts, they are removed from the production set.

  Note: To view a list of removed documents, click the **History** tab and filter by the **Production - Remove Document** action.

- **Cancel**—Stops the conflict check and displays the production page.

28.9 Run a production

To run a production, click **Run Production** in the production console. After you click Run Production, the status bar updates with the following stages and fields as the documents produce:



- **Cleaning Existing Files** - deletes placeholder files (slip sheets) and any produced image files from a prior run production, if necessary.
- **Creating Placeholder Images** - creates placeholder images based on the production data source.
- **Creating and Applying Bates numbers** - creates and applies Bates numbers based on your production numbering.
- **Creating Branding Queue Records** - creates branding queue records for later review.

Note: In the viewer, you can view the produced images by selecting the Production mode. You can view the images exactly as they were produced.

28.9.1 Checking production status

During the production step, a report is available in the Status section. Use this report to quickly identify the number of documents, images, redacted documents, etc.

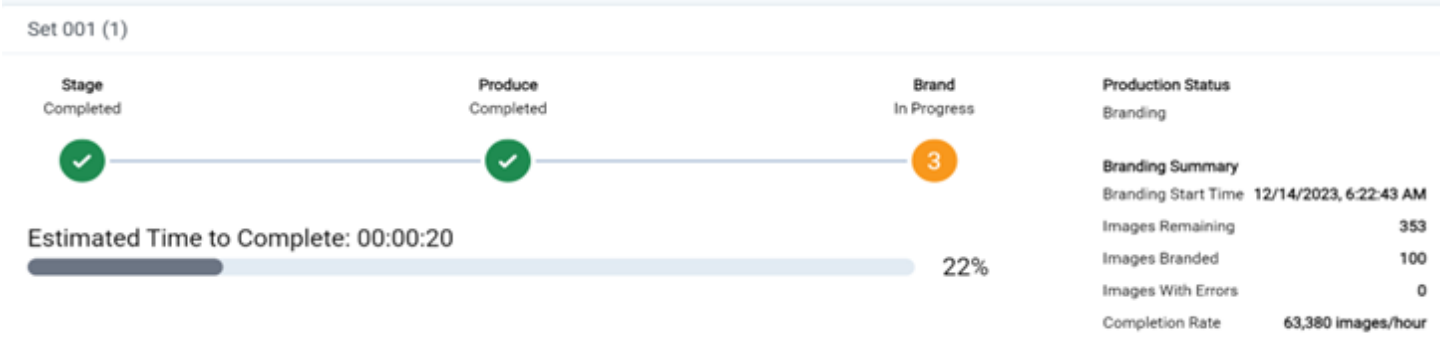
28.9.1.1 Production Summary fields



Production Summary fields include:

- **Begin Bates**—Lists the Bates number of the first document in the production set.
- **End Bates**—Lists the Bates number of the last document in the production set.
- **Total Docs**—Lists the number of documents included in the production set.
- **Total Images**—Lists the number of images included in the production set.
- **Docs With Images**—Lists the number of documents that include images included in the production set.
- **Docs With Natives**—Lists the number of documents that include natives included in the production set.
- **Docs With PDFs**—Lists the number of documents that include stored PDFs in the production set.
- **Docs With Placeholders**—Lists the number of documents that include placeholders included in the production set.
- **Documents With Redactions**—Lists the number of documents that include redacted images and redacted natives included in the production set.
- **Total Image size in GB**—Lists the size of images in GB.
- **Run Date**—Lists the date of when the production was run.

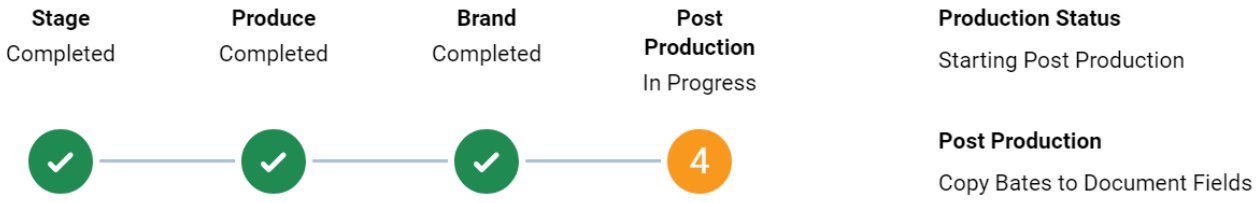
28.9.1.2 Branding Summary fields



Branding Summary fields include:

- **Start Time**—Lists the start time of branding.
- **Branding Completion**—Lists the time of completion for branding.
- **Completion Rate**—Lists the progress of branding.
- **Estimated Time Remaining**—Lists the amount of time left in branding.

28.9.1.3 Post Production Summary fields



Post Production Summary fields include:

- **Copy Bates to Document Fields** - lists the progress of the step.

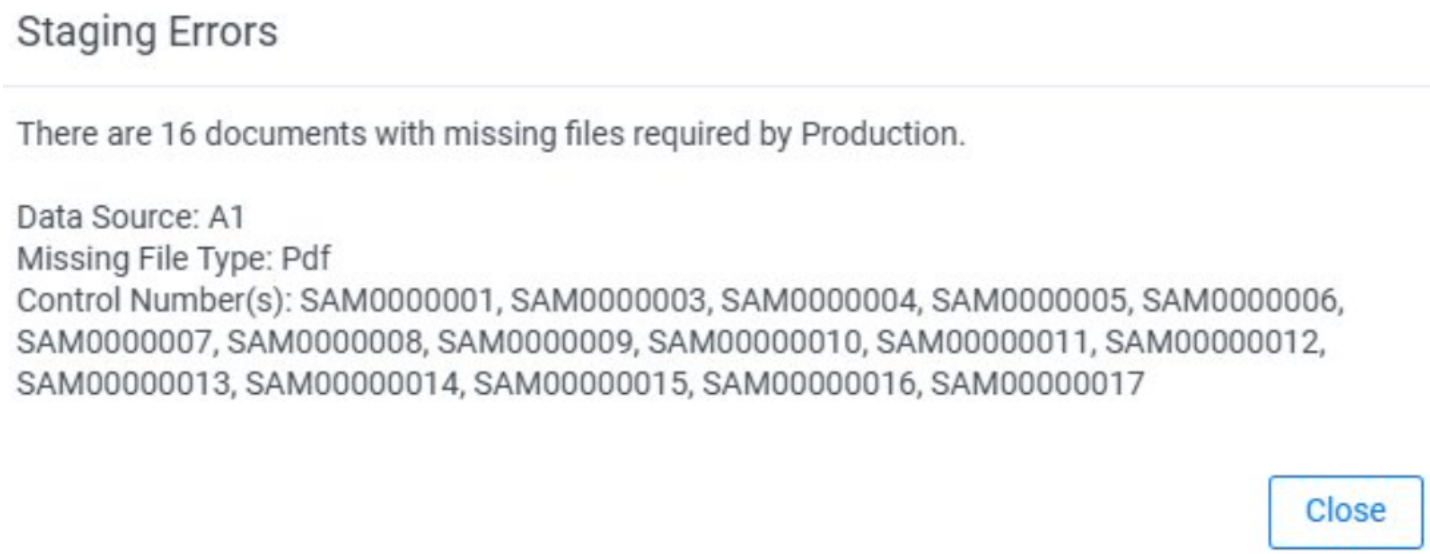
28.10 Production errors

When staging and running a production job, staging, validation, branding, and post production errors can occur.

28.10.1 Staging errors

Staging errors occur when:

- **The same document is found in multiple data sources.**
  When the same document appears in multiple data sources, an error message appears. The error message identifies the data sources that returned the same document and which document they returned. To resolve the error, modify the saved searches you selected as your data sources so they do not return any of the same documents.
- **There are no documents in the data sources.**
  When no documents are found in the data sources, an error message appears. To resolve the error, make sure the saved searches you selected as your data sources are returning documents.
- **There are missing files in the data source.**
  When documents in the data source do not have images, natives, or PDFs, an error message appears. To resolve the error, modify the data sources, then click Stage and Run Production.

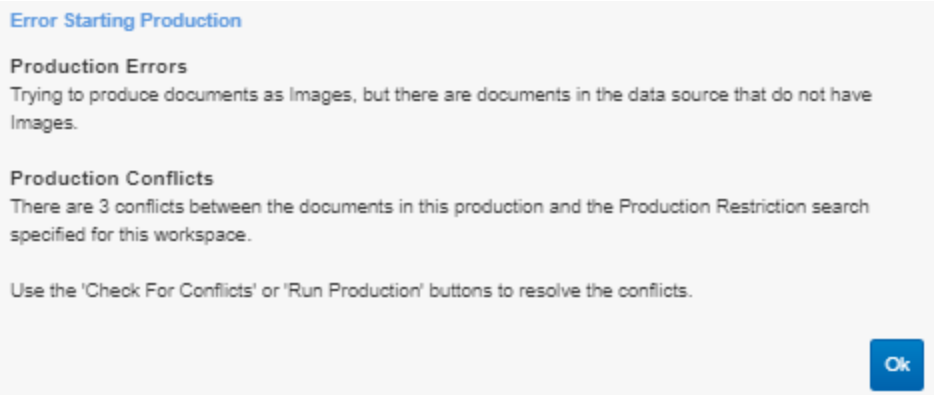


When an error occurs, click **View Production Errors and Warnings** on the Production console to open the Error Starting Production pop-up. The Error Starting Production pop-up lists the errors that occurred.

Conflicts occur when the data sources have documents that are also in the saved search selected in the Production Restriction field.

28.10.2 Validation errors

When a validation error occurs, click **View Production Errors and Warnings** on the Production console to open the Error Starting Production pop-up. The Error Starting Production pop-up lists the errors that occurred.



Conflicts occur when the production data sources contain documents that the saved search in the Production Restriction field also contains.

Conflict resolution option	Fix
Remove the conflict	Remove documents from the production set that are also in the saved search selected in the Production Restriction field. To remove the conflict: 1. Click **Check for Conflicts** on the Production console. The Production Restrictions pop-up will open. 2. Click **Remove Conflict** on the Production Restrictions pop-up. 3. Click **Run Production** on the Production console.
Override the conflict	Keep the documents in the production set that are also in the saved search selected in the Production Restriction field. To override the conflict: 1. Click **Run Production** on the Production console. The Production Warnings pop-up will open. 2. Click **Override and Continue** on the Production Warnings pop-up. The production job will continue without removing the conflict documents.
Modify the production restriction	Modify the Production Restriction field so none of the documents in the production restriction saved search are also in the production set. For information on modifying a production restriction, see Adding and editing production restrictions. After modifying the production restriction, click **Stage and Run Production** on the Production console.

28.10.3 Branding errors

To resolve branding errors:

1. Click **View Branding Errors** on the Production console to open the Branding Errors pop-up.



2. In the **Branding Error Message** column, find the error and apply the fix:

Branding Error Message	Fix
Could not find file <file path>.	Because the system can not find the file path to the image, make sure the image exists at the file path mentioned in the Branding Error Message. Image or re-import the document.
The file at <file path> could not be opened or is not a valid image file.	• If the document is encrypted, add the document's password to the Password Bank. For more information, see Password Bank. • Make sure Relativity supports the file type of the image. You may need to image or import the document again.
The process cannot access the file <file path> because it is being used by another process.	Click **Rerun Errored Documents** on the Production console.
The number of images for document has changed after this production was initially run.	After reimaging, the number of images related to this particular document has changed. This may be related to issues with imaging or applied redactions. To ensure Bates numbering is correct for the entire production, recreate the production set.

3. Click **Rerun Errored Documents** to finish the production job.

28.10.3.1 Post Production errors

These errors are usually related to transient issues. To resolve Post Production errors:

1. Click **Rerun Post Production errors** on the Production console.

28.11 Re-production

You can use the Re-produce mass operation to re-produce select documents from a produced production without having to run the whole production again. For each production that is modified, Relativity creates a new production job, which is a re-production job. Re-production jobs store the modified documents and reuse the numbering format, bates numbers, and branding options from the original productions.

Once a re-production job finishes running, the modified documents merge into the existing, original production set; they overwrite the documents that were previously produced. The previously produced version of the document will no longer display in the Viewer and will not be available for export.

Re-production jobs are stored as regular productions in the system and are not deleted after they are complete. If you want to export just the documents that were modified, use Import/Export to export the re-production job.

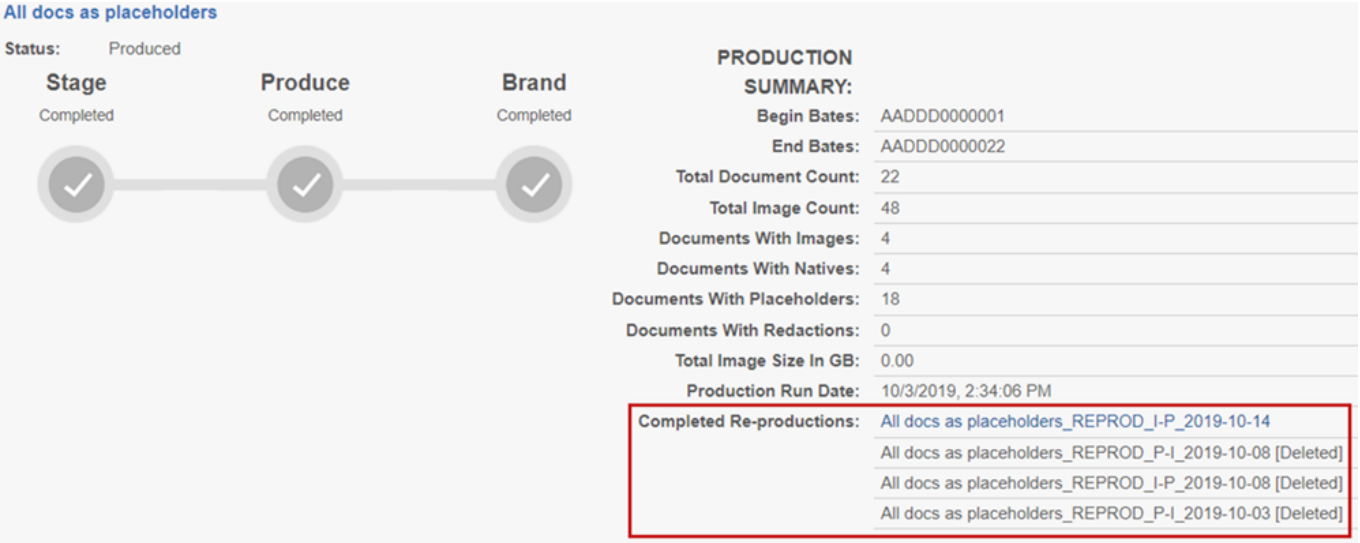
28.11.1 Special considerations

Special considerations for the re-production feature include:

- The re-production feature only works with productions that have been run in Relativity. It will not work with outside productions that have been loaded in.
- You can re-produce documents from multiple production sets with a single mass operation. However, you can only apply one re-production type at a time. Relativity recommends using saved searches to group documents that need the same type of re-production. See Re-production types on the next page.
- Placeholder text handling varies by re-production type: I-P writes placeholder text to the destination field, P-I can clear that field with the Clear Placeholder Text option, and I-I leaves the field unchanged. See Re-production types on the next page.
- Re-production checks for documents that have changed images. Changes to native documents will not be reflected.
- A re-production job is named after the original production that is modified and uses this naming convention: [original production name]_REPROD_[re-production type]_[date of the re-production job]. The re-production type in the name is abbreviated. Re-production type abbreviations include:

Re-production type	Abbreviation
Replace produced images with placeholder	I-P
Replace placeholder with images	P-I
Re-produce documents (same number of pages)	I-I

  For example, if on September 30, 2019, you ran a re-production job to replace documents that were produced as placeholders with images from a production set named "Production", the re-production name would be Production_REPROD_P-I_2019-09-30.
- Every time a production set is modified via the Re-production mass action, a new entry is added to the Completed Re-productions field in the Production Summary section of the original production set. Click on the name of a completed re-production to go to the production set for that re-production job. If you delete a re-production job or do not have access to that re-production set, the name of the set will still appear on the list, but you will not be able to click on it.



28.11.2 Security configuration

You must configure certain workspace level permissions to use the Re-production mass operation.

To configure the required security permissions:

1. Navigate to the **Workspace Details** tab.
2. Click **Manage Permissions**.
3. Click **Edit Permissions** for a group on the **Group Management** tab.
4. Enable the following security permissions:

Object security	Tab visibility	Other settings
• Production - View/Edit/Add • Production Data Source - View/Edit/Add • Placeholder - View	NA	Mass operations • Re-produce

28.11.3 Re-production types

Relativity supported and unsupported re-production types include:

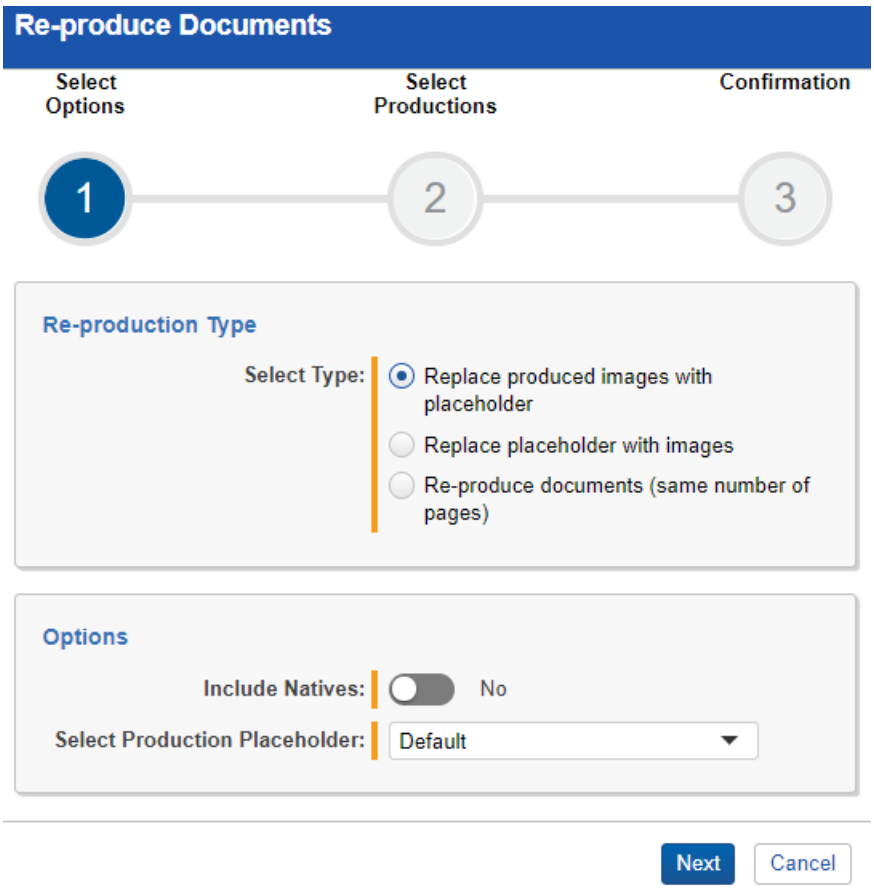
Supported re-production types	Unsupported re-production types
• Replace produced images with placeholder (I-P) below • Replace placeholder with images (P-I) on the next page • Re-produce documents (same number of pages) (I-I) on page 506	• Replace a document that was produced as a placeholder with another placeholder. • Replace a document that was produced as native only with produced images or a placeholder. • Re-produce the same document as images but with a different number of images.

While you can re-produce documents from multiple production sets with a single mass operation, you can only apply one re-production type at a time. For example, if you want to re-produce 100 documents, and you want to replace 60 with produced images and replace 40 with a placeholder, you would need to run two mass operations.

If none of the documents selected meet the re-production type you choose, when you move to the next step you will receive this error: “No productions match the re-production criteria. Please verify all selected documents are included in a production and match the original production type of the re-production options.” For example, you will receive this error if you selected five documents that were produced only as Natives and if you selected "Replace produced images with placeholder" as the Re-production type. To resolve the error, exit the module and remove the documents that do not meet the selected re-production type criteria from the group of documents you selected for re-production. To avoid this error, Relativity recommends using saved searches to group documents that need the same type of re-production.

28.11.3.1 Replace produced images with placeholder (I-P)

In the Re-produce Documents module, select **Replace produced images with placeholder** if you need to replace images in a production with a placeholder. With this re-production type, each page of an imaged document is replaced with a placeholder. For example, if an imaged document is 50 pages, each of the 50 pages would be replaced with a placeholder; the re-produced document would contain 50 placeholders. This preserves the original bates numbering. When you run an I-P re-production, Relativity writes the placeholder text configured for the selected placeholder to the destination field for every document that receives a placeholder in the batch. This matches how the original production run populates the field.

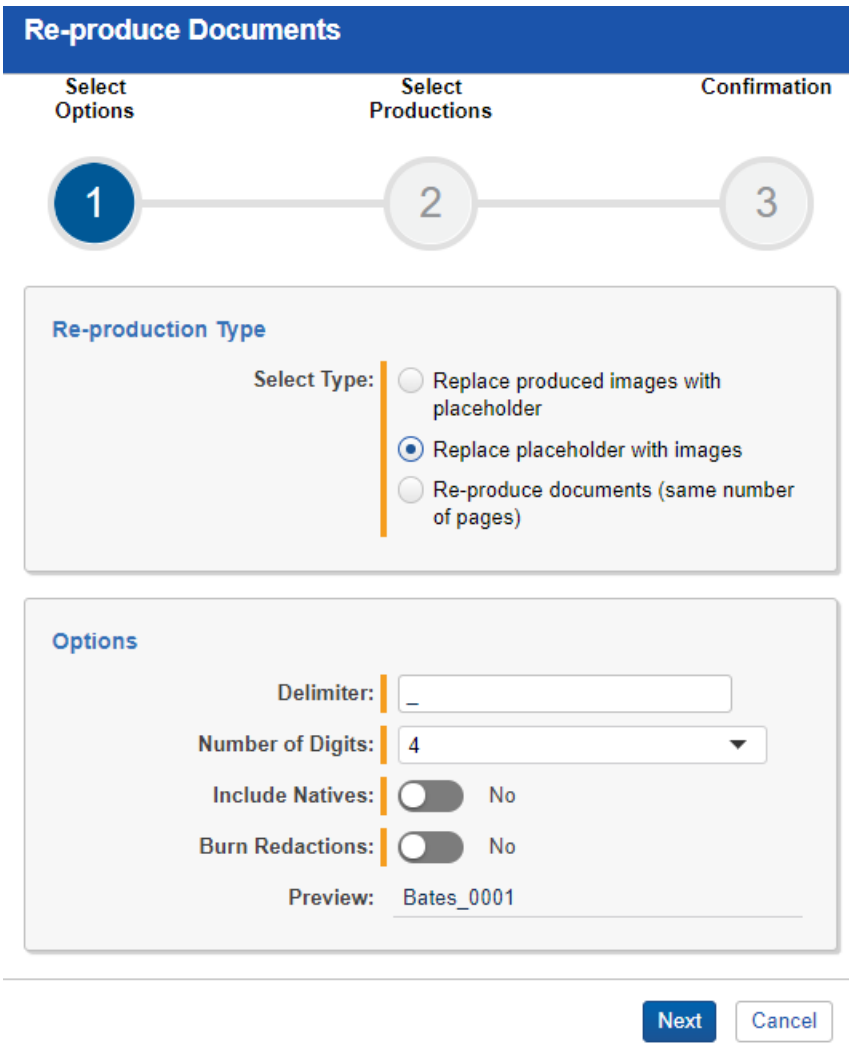


- **Include Natives** - a boolean field. Select **Yes** to include the natives of the documents you selected for re-production. Set this field to **No** if you only want to include a placeholder for the documents. This option overrides the option on the original production. If the document was originally produced with natives, but the user does not select "Include Natives", the document will be merged to the original production with no natives.
- **Select Placeholder** - select a Placeholder for the documents you selected for re-production.

28.11.3.2 Replace placeholder with images (P-I)

In the Re-produce Documents module, select **Replace placeholder with images** if you need to replace documents that were produced as placeholders with produced images.

Note: The documents must already be imaged before you run the mass operation, or an error will occur with the mass operation.



- **Delimiter** - given that you are replacing a placeholder (1-page image) with produced images, it is possible that the new document may have more than 1 page. This option allow you to use a character to suffix the original production bates number from the number of pages in re-produced image. The suffix will start on the second page with number #1. The following separators can be used:
  - _ (underscore, selected by default)
  - - (hyphen)
  - . (period)
- **Number of Digits** - determines how many digits the suffix number contains.. The range of available values is between 1 and 6. By default, this option is set to 4 characters.
- **Include Natives** - a boolean field. Select **Yes** to include the natives of the documents you selected for re-production. Set this field to **No** if you only want to include a placeholder for the documents. This option overrides the option on the original production. If the document was originally produced with natives, but the user does not select "Include Natives", the document will be merged to the original production with no natives.
- **Burn Redactions** - a boolean field. Select **Yes** to apply redactions to the documents you selected for re-production. Set this field to **No** if you do not want redactions applied to the documents.
  - **Select Markup Set** - indicates which markup set is used to apply redactions to the production images.
- **Clear Placeholder Text** - a boolean field, on by default. Select Yes to clear the destination field for documents whose field was populated by the original production run. Select No to keep the existing field value when the

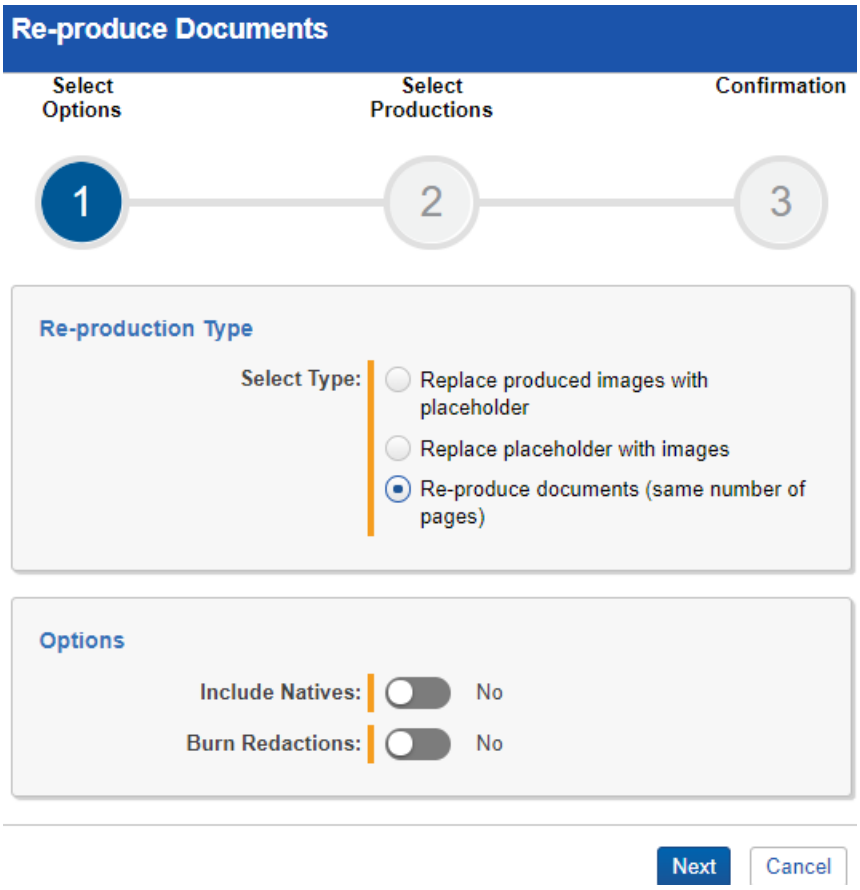
document moves from a placeholder to produced images.

- **Preview** - displays what the bates number will look like based on your selections.

28.11.3.3 Re-produce documents (same number of pages) (I-I)

In the Re-produce Documents module, select **Re-produce documents (same number of pages)** if you need to replace documents in a production. I-I re-productions do not change the destination field that the original production populated.

Note: The documents that you are using to replace the documents in the production must be the same number of pages as the documents in the production that you are replacing.



- **Include Natives** - a boolean field. Select **Yes** to include the natives of the documents you selected for re-production. Set this field to **No** if you only want to include a placeholder for the documents. This option overrides the option on the original production. If the document was originally produced with natives, but the user does not select "Include Natives", the document will be merged to the original production with no natives.
- **Burn redactions** - a boolean field. Select **Yes** to apply redactions to the documents you selected for re-production. Set this field to **No** if you do not want redactions applied to the documents.
    - **Select Markup Set** - indicates which markup set is used to apply redactions to the production images.

28.11.4 Re-production scenarios

Re-production scenarios include:

Documents selected	Re-production type selected	Productions available for modification	Number of documents to be modified in each production	Outcome
Doc A was produced as placeholder in Prod_1 Doc B was produced as placeholder in Prod_2	Replace Placeholders with images	Prod_1 Prod_2	Prod_1 | 1 out of the total of 2 documents selected will be modified in this production Prod_2 | 1 out of the total of 2 documents selected will be modified in this production	Doc A is re-produced in Prod_1 Doc B is re-produced in Prod_2
Doc A was produced as placeholder in Prod_1 Doc B was produced as Images in Prod_1	Replace Placeholders with images	Prod_1	Prod_1 | 1 out of the total of 2 documents selected will be modify in this production.	Doc A is re-produced in Prod_1
Doc A was produced as placeholder in Prod_1 Doc B was produced as images in Prod_1 Doc A was produced as images in Prod_2 Doc B was produced as placeholder in Prod_2	Replace Placeholders with images	Prod_1 Prod_2	Prod_1 | 1 out of the total of 2 documents selected will be modify in this production. Prod_2 | 1 out of the total of 2 documents selected will be modify in this production.	Doc A is re-produced in Prod_1 Doc B is re-produced in Prod_2
Doc A was produced as placeholder in Prod_1 Doc A was produced as images in Prod_2 Doc B was produced as images in	Replace Placeholders with images	Prod_1 **Note:** Prod_2 is not displayed because Doc A and Doc B were not produced as placeholder in Prod_2.	Prod_1 | 1 out of the total of 2 documents selected will be modify in this production.	Doc A is re-produced in Prod_1

Documents selected	Re-production type selected	Productions available for modification	Number of documents to be modified in each production	Outcome
Prod_2				
Doc A was produced as placeholder in Prod_1 Doc B was produced as placeholder in Prod_1 Doc A was produced as placeholder in Prod_2 Doc B was produced as images in Prod_2	Replace Placeholders with images	Prod_1 Prod_2	Prod_1 | 2 out of the total of 2 documents selected will be modify in this production. Prod_2 | 1 out of the total of 2 documents selected will be modify in this production.	Doc A is re-produced in Prod_1 Doc B is re-produced in Prod_1 Doc A is re-produced in Prod_2
Doc A was produced as placeholder in Prod_1 Doc B was produced as placeholder in Prod_1 Doc A was produced as placeholder in Prod_2 Doc B was produced as placeholder in Prod_2	Replace Placeholders with images Need to replace Doc A and Doc B in Prod_1. Need to replace Doc A only in Prod_2. Doc B should not be replaced in Prod_2.	Prod_1 Prod_2	Prod_1 | 2 out of the total of 2 documents selected will be modify in this production. Prod_2 | 2 out of the total of 2 documents selected will be modify in this production.	Doc A and Doc B are both modified in Prod_1 and Prod_2.

28.11.5 Re-produce documents

To re-produce documents:

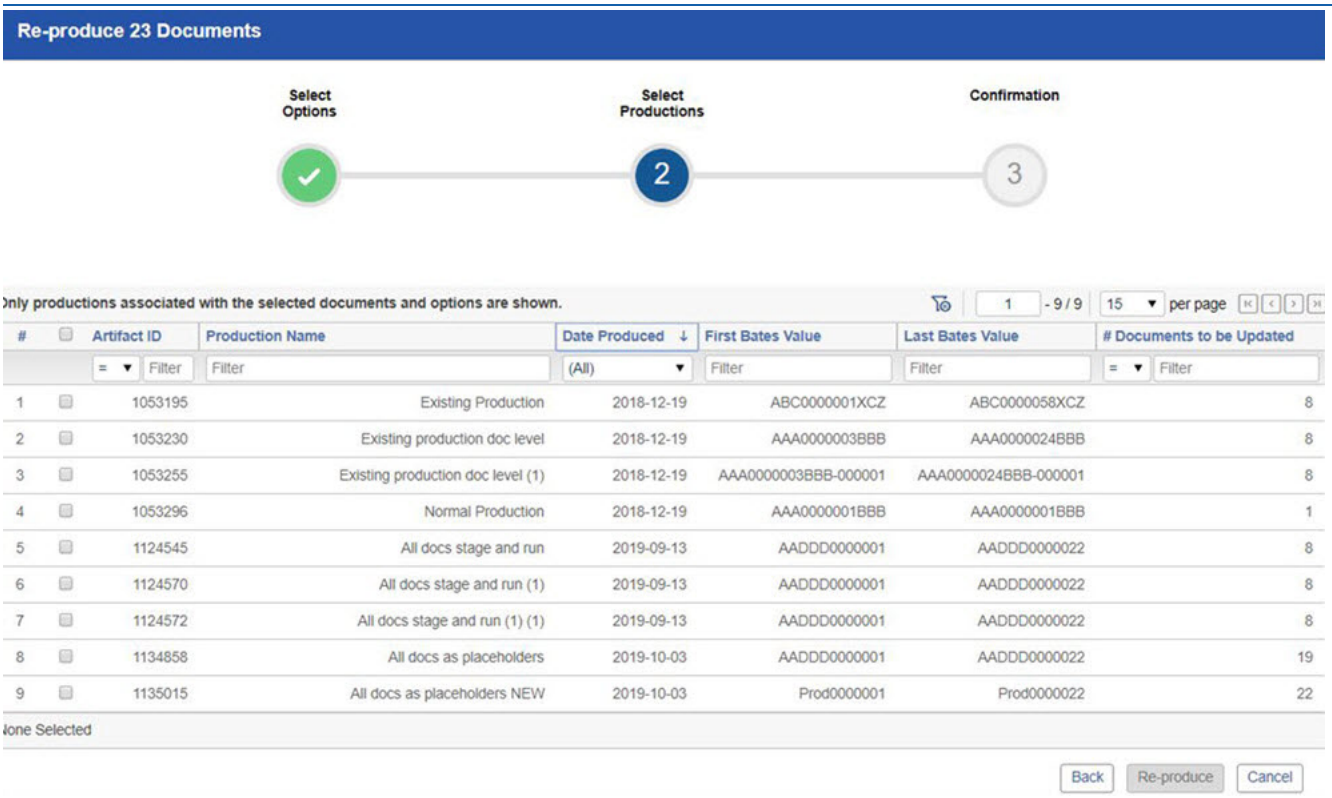
1. Navigate to the **Documents** tab in a workspace.
2. Select the documents that you want to re-produce from a document view, folder, field tree, saved search, or dashboard.
3. Click **Re-produce** from the mass operations menu. The **Re-produce Documents** module opens.

4. Select a Re-production Type, and complete the required fields. See Re-production types on page 503.

Note: If you are modifying multiple productions at the time, the options that you select on this step will apply to all the productions you are modifying, including the placeholder selected in this step, burn redactions, and the options of whether the documents will be produced with natives.

5. Click **Next**.
6. Select the productions that you want modify.

Note: Only productions associated with the selected documents and options display. Productions with a status different to "Produced" or Productions that used Existing numbering will not be available here.



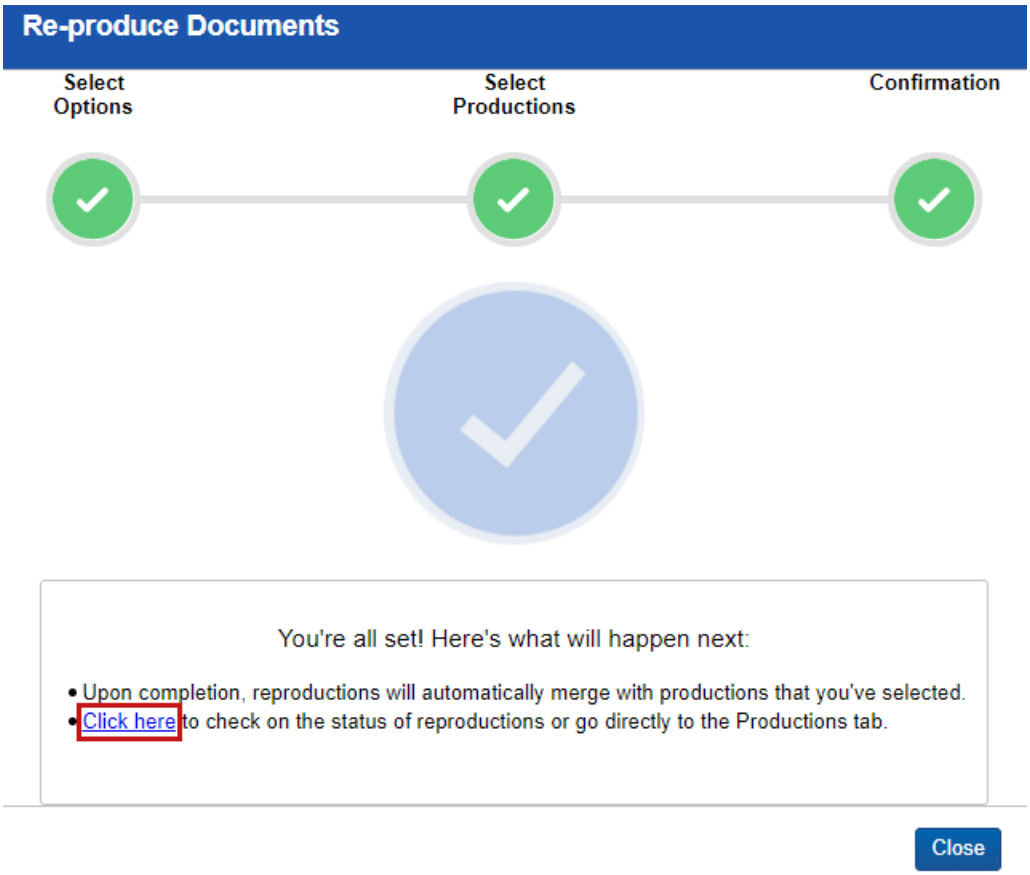
7. Click **Re-produce**.

Note: Do not close the Re-produce Documents module until the Confirmation checkmark appears. Once the Confirmation checkmark appears, the re-production sets have been created and added to the Production queue.

28.11.6 Re-production job status

To see the status of a re-production job:

- Click **Click here** in the Re-produce Documents module. This will take you to the Re-production view. See Re-production views on the next page.



- Navigate to the **Production Sets** tab, and select the **Re-production** view. See Re-production views below.

28.11.7 Re-production views

Two views on the Production Sets tab display information regarding re-productions:

- **Re-productions** - a view that lists every re-production jobs. Fields in the view include:
  - **Name** - the name of the re-production job.
  - **Status** - the status of the re-production job.
  - **First Bates Value** - the first bates number in the production.
  - **Last Bates Value** - the last bates number in the production.
  - **Prefix** - the characters added to the beginning of each Bates number.
  - **Production Set** - the name of and link to the original production set.
- **Original Productions** - a view that lists every production set that have been modified by a re-production job. Fields in the view include:
  - **Name** - the name of the original production.
  - **Status** - the status of the production job.
  - **First Bates Value** - the first bates number in the production.
  - **Last Bates Value** - the last bates number in the production.

- **Prefix** - the characters added to the beginning of each Bates number.
- **Start Number** - the first number used in a sequence of Bates numbers.

28.12 Branding queue

The Branding Queue displays production jobs receiving branding of redactions, header, footer, or other modifications. A production job displays in this queue only while it has a status of branding. The production job remains in the production queue until all branding is complete.

You can view the branding queue from Home. Select the **Queue Management** tab, and then click **Branding Queue**. See Branding queue fields on the next page for details.

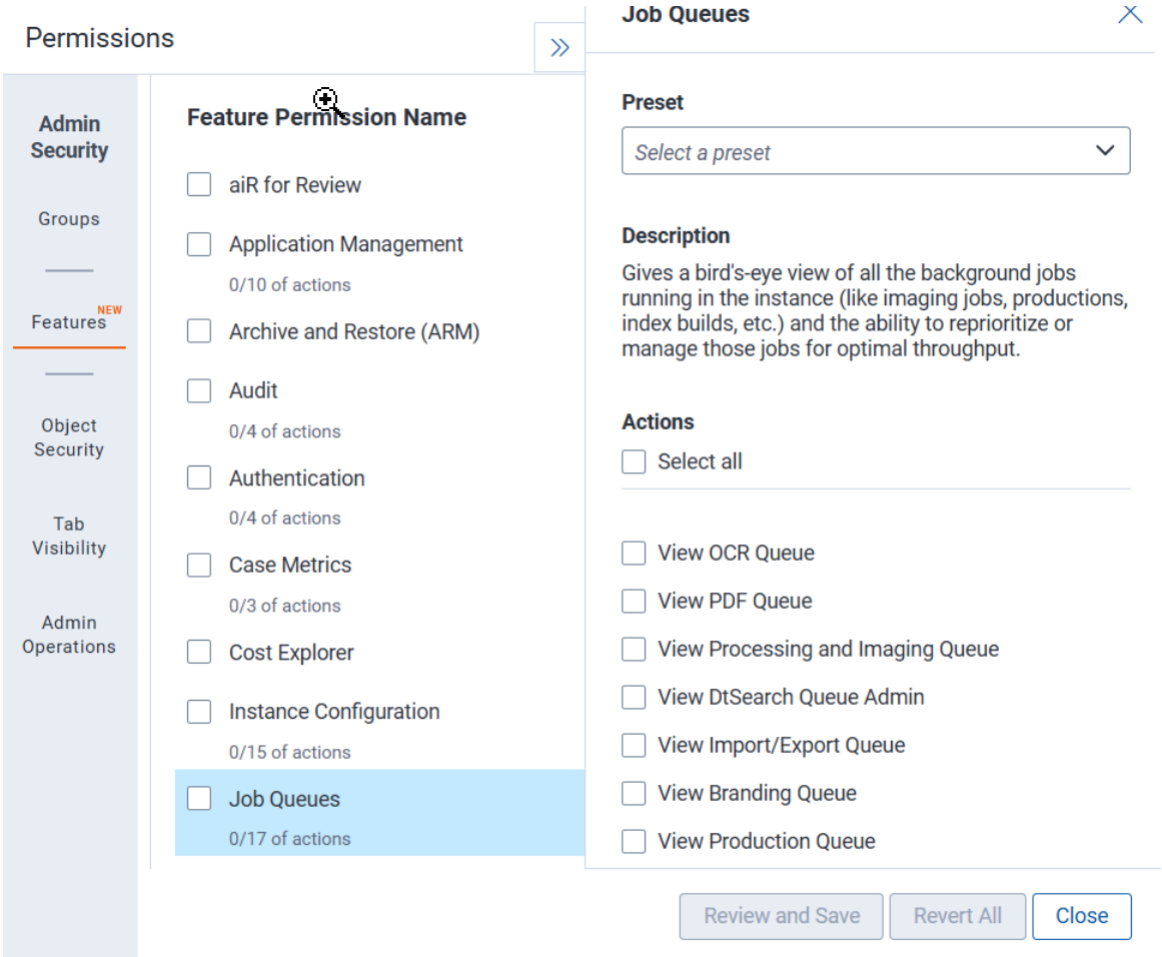
Note: Branding agents scale automatically in Relativity aiR based on the total size of all jobs in queue. All agents will be assigned to the highest priority Production, one at a time.

To change the priority of a job, click the **Change Priority** button at the bottom of the view. Enter a new integer value in the **Priority** field, and then click **Update**. Only one job runs at a time, the lower numbered job runs first and the higher numbered job runs last.

Note: Any change to the priority of a job in the branding queue also changes its priority in the production queue.

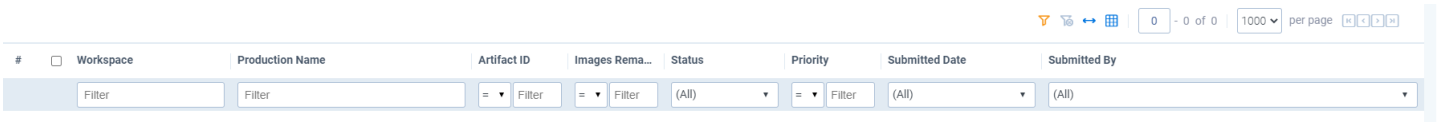
28.12.1 Permissions

Manage permissions for this feature on the Features tab. Grant the full feature for a group, or customize access with individual actions. For an overview of features and actions, see Feature permissions.



28.12.2 Branding queue fields

The Branding Queue view displays the following fields:



- **Workspace** - the workspace that contains the production set receiving branding
- **Production Name** - the production set receiving branding
- **Artifact ID** - the unique identifier for the production set
- **Images Remaining** - the number of images that require branding
- **Status** - the current stage of the branding job
- **Priority** - the order in which the branding job is run. Relativity completes branding jobs by priority. The default value is 100.
- **Submitted By** - the user who initiated the job. You can use this information to prioritize branding jobs by user.

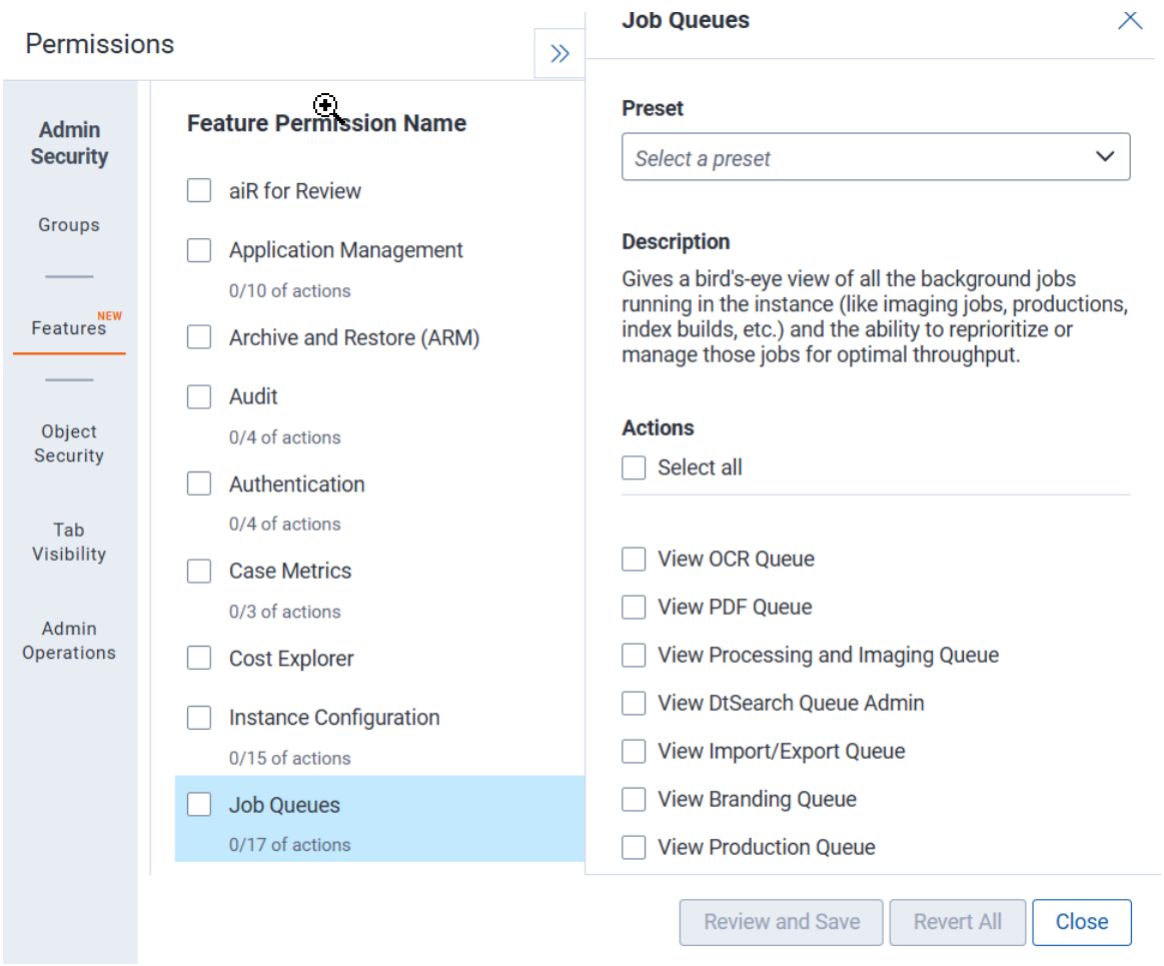
28.13 Production queue

The Production Queue tab displays all current production jobs running in your environment, and any jobs in error status. A job remains in this queue until the completion of branding and other processing.

You can view the production queue from Home. Select the **Queue Management** tab, and then click **Production Queue**.

28.13.1 Permissions

Manage permissions for this feature on the Features tab. Grant the full feature for a group, or customize access with individual actions. For an overview of features and actions, see Feature permissions.



28.13.1.1 Instance level permissions

You must configure certain instance level permissions to use Production Queue.

To configure the security permissions:

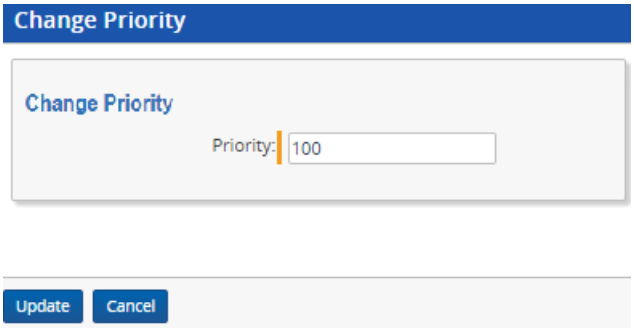
1. Navigate to the **Instance Details** tab.
2. Click **Manage Permissions**.
3. Click **Edit Permissions** for a group on the Group Management tab.
4. Enable the following security permissions:

Object Security	Tab Visibility	Admin Operations
• N/A	• Queue Management (parent) • Production Queue (child)	• Change Queue Priority • View Admin Repository

Note: As long as you have the listed security permissions, you do not need view permissions to the workspaces or the production jobs to use Retry Production Job.

28.13.2 Change job priority

To change the priority of a job, click **Change Priority** at the bottom of the view. Enter a new integer value in the **Priority** field, and then click **Update**. Only one job runs at a time, the lower numbered job runs first and the higher numbered job runs last.

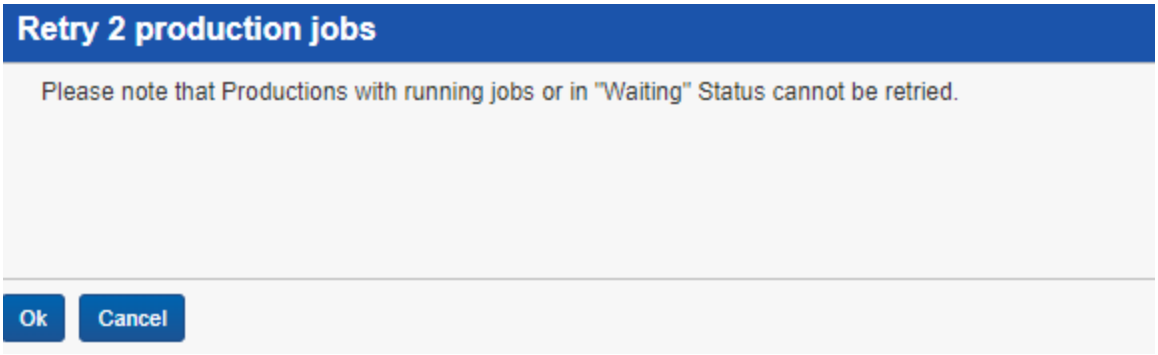


Note: During a production job, Relativity sends a job to the branding queue for the stamping of redactions, headers, or other modifications. Any change to the priority of a job in the production queue changes its priority in the branding queue.

28.13.3 Retry Production Job mass operation

To retry production jobs from the Production Queue tab:

1. Navigate to the **Production Queue** tab.
2. Select the productions jobs that you want to cancel.
3. Click **Retry Production Job** from the mass operations bar. The Retry production job window opens.



4. Click **Ok**.

28.13.4 Cancel Production Job mass operation

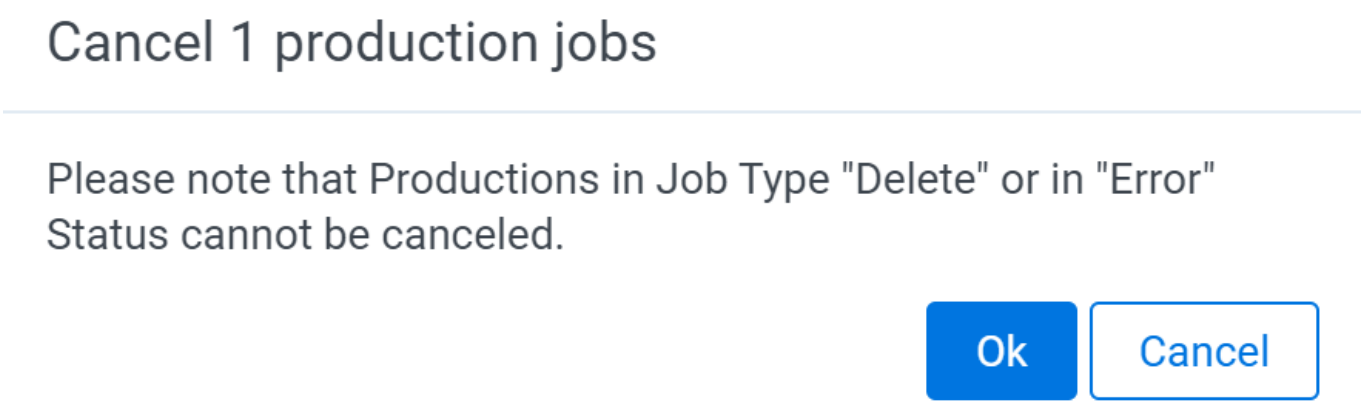
To cancel productions jobs from the Production Queue tab, use the Cancel Production Job mass operation.

28.13.4.1 Canceling multiple production jobs

To cancel multiple production jobs from the Production Queue tab:

- Navigate to the **Production Queue** tab.
- Select the productions jobs that you want to cancel.

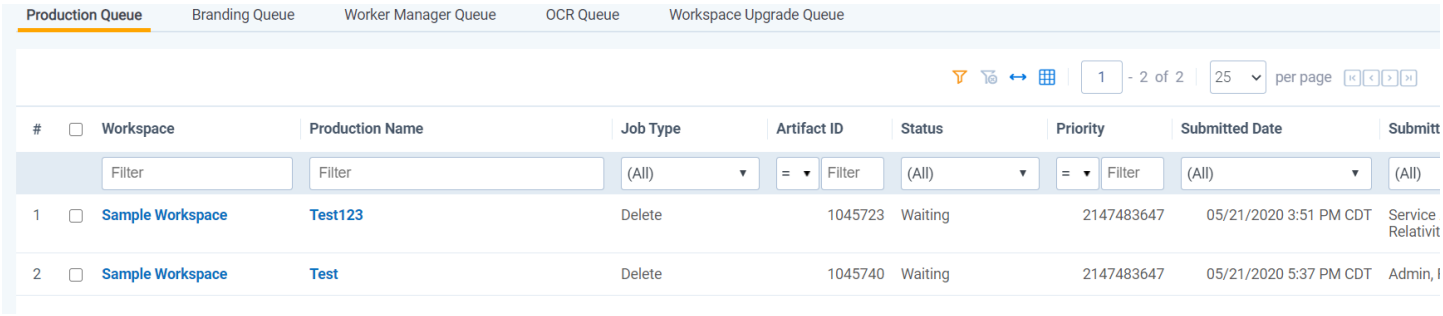
- Click **Cancel Production Job** from the mass operations bar. The Cancel production job window opens.



- Click **Ok**.

28.13.5 Production queue fields

The Production Queue displays the following fields:



- **Workspace** - the workspace that contains the production set used for a job.
- **Production Name** - the production set used for the job.
- **Artifact ID** - the unique identifier for the production set.
- **Status** - the current stage of the production job.
- **Priority** - the order in which the production job is run. Relativity sends jobs to the production engine by priority, and then orders them by submitted date and time. The default value is 100.
- **Submitted Date** - the date and time when a production job was submitted, or an attempt was made to resolve errors in a job. (In the Production Set Console, the user clicked **Run**, or **Resolve Errors**.)
- **Submitted By** - the user who initiated the job. You can use this information to prioritize production jobs by user.

29 Redact

With Redact, you can apply markups to imaged documents, spreadsheet files, and PDF files either manually or automatically as part of a project. You determine how a project applies markups by creating rules that establish what words, terms, or regular expressions will receive markups. You also determine which markup set is used by a project to apply markups. To learn more about markup sets, see Markup sets. Once a project has been run, Redact also provides tools to make reviewing markups easy.

29.1 Example workflow

While Redact is flexible enough to support different workflows, the following is a typical workflow:

1. Identify a set of spreadsheet or PDF files that require markups.
2. Do any of the following to apply markups to the set of documents:
    - Apply markups manually to the documents. To learn more, visit Manual markups with spreadsheet files, Manual markups with PDF files, and Redacting PDF annotations and attachments.
    - Search for terms in spreadsheet files and apply markups to them. To learn more, visit Using Find and Redact.
    - Apply markups automatically using project automation. To learn more, visit Automated spreadsheet markup project, Automated spreadsheet propagation project, Automated PDF markup project, Automated image markup project, and Automated image template project.
3. Review the markups to ensure quality control before production. To learn more, visit Reviewing markups to ensure accuracy.
4. Create a saved search of marked-up documents to assist you in producing them. To learn more, visit Searching for documents with Redact fields.

29.2 Installing Redact to a workspace

Optionally, you can create the following Redact fields before beginning the application installation process:

- **Redact Document Warnings**—Multiple choice
- **Redact Has Unresolved Markups**—Yes/No
- **Redact Needs Quality Review**—Yes/No
- **Redact Production Lock**—Yes/No

To install the Redact application to a workspace of your choice:

1. In the workspace, navigate to the **Relativity Applications** tab.
2. Select the **Select from Application Library** option.
3. Click on the **Select** icon.
   The Select Library application pop-up displays.
4. Filter the applications and select the **Relativity aiR Redact** application.
5. Click **Ok**.
6. Optionally, map the application fields to fields in the workspace as desired.
7. Click **Import**.

The Redact application is installed and ready for use in the workspace.

Note: All Redact permissions, including Redact mass operations, are granted to system and workspace administrators upon the initial workspace install. After installation, it is up to the system and workspace administrators to grant additional Redact permissions to user groups per workspace.

29.3 Before you begin

If you are going to use Redact with spreadsheet files, we recommend running the Prepare Excel for Redact mass operation, formerly known as the Unhide Excel Content mass operation, on all Excel documents beforehand. To learn more, see Manual markups with spreadsheet files, Automated spreadsheet markup project, and Automated spreadsheet propagation project.

Note: Workspaces using Blackout 5.2 or below can be migrated from Server to Relativity aiR. To learn more about Blackout migration, see Blackout migration.

29.4 File size considerations

To ensure high performance, there is a 4 GB file size limit for native files. This limit cannot be overwritten by entering a value higher than 4 GB in the *MaximumNativeSizeForViewerInBytes* instance setting. Any native files that are 4 GB or above will not receive markups using Redact.

29.5 Redact supported file types

Note: Redact does not support Excel 5.0 files or below.
Redact also does not support any of the following sheet types: Visual Basic module, Macro, or Dialog.

While occasionally files can be become corrupted and not work in Redact, the following file types are supported:

- **.pdf**—any standard
- **.csv**
- **.xls**—Excel 97 - 2003 workbook.
- **.xlsb**—Excel binary workbook.
- **.xlsx**—Office Open XML spreadsheet, ML workbook or template file, with or without macros.
- **.xlsm**—Excel macro-enabled workbook.
- **.xltx**—Excel template.
- **.xltm**—Excel macro-enabled template.
- **.xlam**—An Excel macro-enabled add-In file that's used to add new functions to Excel.

29.6 Permissions

Redact has permissions that you can give users that determine the actions they can take using this feature. To understand what permissions do and what permissions you may want to assign to users, read the list of all Redact permissions below and then groups of permissions that you may want to assign to allow a user to perform specific types of workflows.

When assigning Redact permissions, it is important to note that the Native PDF Redactions, Native Excel Redactions, and Image Redactions permissions let you apply markups across a set of documents or apply markups manually in the Viewer for their respective file types.

To understand what happens if these permissions are not granted to a user, a description of what a user cannot do without each permission is included. Without:

- **Native PDF Redactions**—users will not see PDF markup projects or Redact Markup Navigator features in the Viewer for native PDFs without this permission. Additionally, users will not be able to automatically or manually apply markups on native PDF documents.
- **Native Excel Redactions**—users will not see spreadsheet markup projects or spreadsheet propagation projects without this permission. Additionally, users will not see Redact Markup Navigator features in the Viewer for native spreadsheet documents without this permission. They will also not be able to automatically or manually apply markups on native spreadsheet documents.
- **Image Redactions**—users will not see the image markup project or image template projects without this permission. Additionally users will not see Redact cards in the Viewer for images without this permission. They will also not be able to apply redactions and/or highlights on the Document object.

29.6.1 All Redact permissions

Note: Feature Permissions provide an alternative to Relativity's security management by shifting the focus from Object Types and Tab Visibility to feature-based permissions. This method is an alternative option. Any feature-specific permissions information already in this and other topics is still applicable. The Feature Permissions interface enables administrators to manage permissions at the feature level, offering a more intuitive experience. By viewing granular permissions associated with each feature, administrators can ensure comprehensive control, ultimately reducing complexity and minimizing errors. For details see Instance-level permissions and Workspace-level permissions.

The following permissions are needed to use each part of Redact:

Object Security	Tab Visibility	Other Settings
• **Redact** - View, Edit, Delete, Add • Place/Edit Manual Redaction • Place/Edit Manual Highlight • Clear Markups • Unhide Excel Content • Viewer Quality Control Panel • View Quality Control Entries • Accept/Reject Quality Control Entries • Input Custom Redaction Text • Native PDF Redactions • Native Excel Redactions • Image Redactions • Stored PDF Redactions • **Redact Externally Redacted Native** - Add, Edit, Delete • **Redact Fields** - Add , Edit, Delete • **Redact Original Native** - Add, Edit, Delete • **Redact Produced Document** - Add, Edit,	• Redact • Redact Projects • Redact External Markups • Redact Audits • Redact Reports • Redact Settings • Redact Redacted File • Redact Original Native • Redact Externally Redacted Native • Redact Fields	• Convert Markups • Delete Native Markups • Prepare Excel for Redact

Object Security	Tab Visibility	Other Settings
Delete • **Redact Redacted File** - Add, Edit, Delete		

29.6.2 Native PDF Redactions permissions

To enable a user to complete the following tasks:

- Create and run PDF markup projects.
- Manually apply markups on native PDF documents in the Viewer.
- QC markups that were applied automatically by Redact projects.
- Edit the redaction text that has been applied to native PDF documents.

Assign them the following permissions:

- Native PDF Redactions
- Place/Edit Manual Redaction
- Place/Edit Manual Highlight
- Clear Markups
- Accept/Reject Quality Control Entries
- Input Custom Redaction Text
- Redact Produced Document

29.6.3 Native Excel Redactions permissions

To enable a user to complete the following tasks:

- Create and run spreadsheet markup projects and automated spreadsheet propagation projects.
- Manually apply markups to native spreadsheet documents in the Viewer.
- QC markups that were applied automatically by Redact projects.
- Edit the redaction text that has been applied to native spreadsheet documents.

Assign them the following permissions:

- Native Excel Redactions
- Place/Edit Manual Redaction
- Place/Edit Manual Highlight
- Clear Markups
- Prepare Excel for Redact
- View Quality Control Panel
- Accept/Reject Quality Control Entries

- Input Custom Redaction Text
- Redact Produced Document

29.6.4 Image Redactions permissions

To enable a user to complete the following tasks:

- Create and run image markup projects and image template projects.
- Manually apply markups to imaged documents in the Viewer.
- QC markups that were applied automatically by Redact projects.
- Edit the redaction text that has been applied to native imaged documents.

Assign them the following permissions:

- Redact permissions
  - Image Redactions
  - Place/Edit Manual Redaction
  - Place/Edit Manual Highlight
  - View Quality Control Panel
  - Accept/Reject Quality Control Entries
  - Input Custom Redaction Text
  - Redact Produced Document
- Document object permissions
  - Redact Document
  - Highlight Document

29.6.5 Redact Mass Operations permissions

If enabled, the mass operations permissions allow a user to do the following:

- **Convert SMarkups**—view and use the Convert Spreadsheet Markups mass operation. To learn more, visit Convert Spreadsheet Markups.
- **Delete Native Markups**—view and use the Delete Native Markups mass operation.
- **Prepare Excel Content**—view and use the Prepare Excel Content mass operation.

29.6.6 Markup set permissions

Individual markup sets are securable using permissions. Therefore, a user will be able to take the following actions with each permission that has been enabled for them:

- **View**—the ability to view a given markup set.
- **Edit**—the ability to edit a given markup set's properties. This does not allow a user to edit an actual markup.
- **Delete**—the ability to delete a given markup set. This does not allow a user to edit an actual markup.
- **Add**—the ability to create a new markup set. This does not allow a user to edit an actual markup.
- **Edit Security**—the ability to change the permissions for a given markup set.

29.6.7 Permissions for redacting documents outside of Relativity

The following Document object permissions are needed to redact documents outside of Relativity:

- **Upload/Add/Delete Image**—a user should be granted these permissions if they are redacting images outside of Relativity.
- **Replace Document**—a user should be granted this permission if they are redacting native documents outside of Relativity. This permission allows users to replace native documents.
- **Create PDF**—a user should be granted this permission if they have a workflow to redact a PDF of a native document.
- **Local Access (Download, Copy Text)**—a user should be granted this permission if they want to download the native document, redact the copied native document, and then re-upload that document to Relativity.

29.7 Automated spreadsheet markup project

Creating a spreadsheet markup project can save you time over manually redacting by applying markups to Excel spreadsheet and .csv files automatically. You can create a project by entering words, terms, phrases, or regular expressions that you would like Redact to apply markups to. Alternatively, you can enter project rules into a .csv file and upload it to the project page that will populate the rules for a spreadsheet markup project. Once the project is created and run, markups will be applied automatically based on the rules you create.

29.7.1 Supported file types

To learn more about which file types are compatible with Redact, see Redact supported file types.

29.7.2 Preparing Excel documents

We recommend running the Prepare Excel for Redact mass operation, formerly known as the Unhide Excel Content mass operation, on all Excel documents before applying markups with Redact. This preparation is done to ensure data is not lost after the markups are applied and also to prevent information that is covered by markups from being restored by third parties.

To prepare Excel documents:

1. Navigate to the **Documents** tab.
2. Select the desired Excel documents from the list.
3. Click on the mass operations menu and select the **Prepare Excel for Redact** option.
4. Click **Confirm**.
   The selected Excel documents are ready to receive markups using Redact.

29.7.3 Before you begin

Consider creating a saved search with the documents you wish to apply markups to and a markup set that contains the markups you wish to apply to the Excel and .csv files before starting the spreadsheet markup project creation process.

29.7.3.1 Considerations

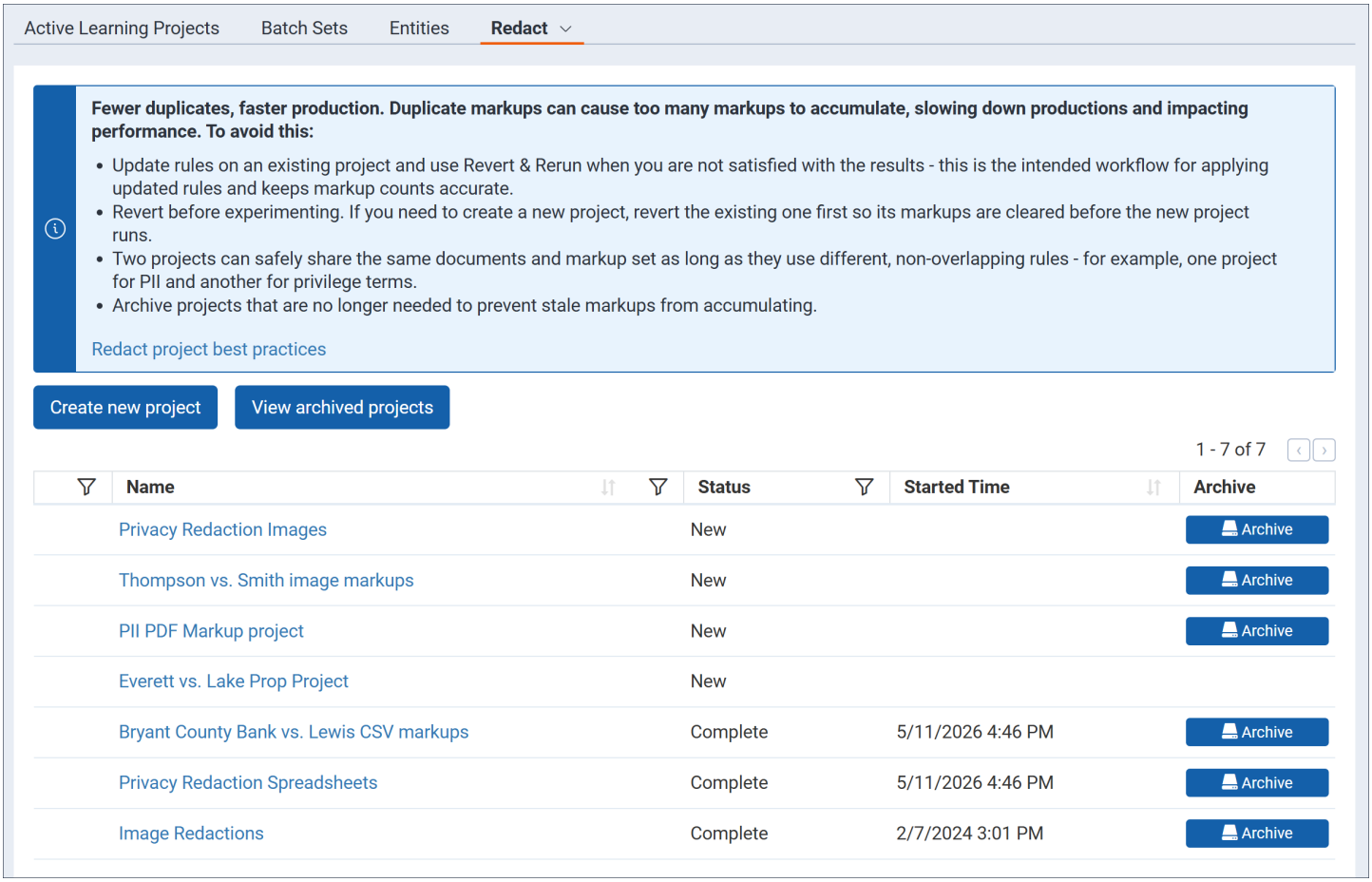
- If you apply a markup to a cell where the text overflows into empty neighboring cells, just as in the native application, the markup does not overflow into empty neighboring cells. However, when the document is produced and the markup is burned in, the text from the original cell no longer overflows and is completely hidden by the markup.

- Due to a limitation in the Excel file format, a cell cannot contain more than 32,000 characters. If you try to apply a text redaction to a cell and it already contains 32,000 characters, the redaction may not be applied and you will see a notification about the character limit.

29.7.4 Creating a spreadsheet markup project manually

To create a spreadsheet markup project using rules that you manually set:

1. Navigate to the **Redact Projects** tab.



2. Click **Create new project**.
3. Select the **Spreadsheet** project option.
4. Complete the **Create spreadsheet markup project** section fields. To learn more, visit Fields below.

Note: Using the same or similar documents, the same or similar rules, and the same markup sets in more than one project can lead to duplicate markups being applied.

5. Complete the **Rules** section fields. This section is optional and if you complete these fields, they will determine how the spreadsheet markup project applies markups. To learn more, visit Fields. Alternatively, you can leave these fields blank and upload a .csv file. To learn more, visit Creating a spreadsheet markup project using .csv rules.
6. Click **Save**.

29.7.5 Creating a spreadsheet markup project using .csv or .xlsm rules

While a project can be created manually, if you plan on running multiple kinds of projects with similar rules and terms, you can save time by using the same copy of .csv or .xlsm rules for each project. Please note that you may still need to adjust the scope in the rules based on which project you are running.

You can upload up to 100,000 rules in a .csv file though it is worth noting that the more rules are included in a .csv or .xlsm file, the longer a project will take to run. Rules that are uploaded with a .csv file cannot be viewed in the Redact interface and instead, you will need to download a copy of the .csv file and view it outside of Relativity.

Once you have entered the desired rules, save this file as a .csv before uploading to Relativity.

To create a spreadsheet markup project using rules generated by a .csv file, do the following:

1. Navigate to the **Redact Projects** tab.
2. Click **Create new project** .
3. Select the **Spreadsheet** project option.
4. Enter a **Project Name** and select a **Saved Search** and **Markup Set**. Leave all other fields blank. For more information on these fields, visit Fields below.
5. Click **Save**.
6. Click **Upload rules csv**.
7. Select the desired .csv or .xlsm file from your workstation and click **Open**.
   The file is uploaded and the rules will be created and added to the project.

29.7.5.1 .csv or .xlsm rules

Guidance for how to configure rules using a .csv or .xlsm file is provided below. To learn more about the functionality of the rules, visit Rules section below.

- **Word/Phrase**—Enter the desired word or phrase. There are no formatting requirements.
- **RegEx Name**—Enter name of the regular expression. There are no formatting requirements.
- **RegEx**—Enter the regular expression syntax. There are no formatting requirements.
- **Markup Type**—Enter one of the following options: Redaction, Highlight, Inverse, or Inverse Highlight. The options are case sensitive.

  Note: If the Inverse option is selected, the entire sheet is redacted unless there is data in the rules below that affect how markups are applied.

- **Markup Subtype**—Enter one of the following options: Redactions, Black, Text, or White. The options are case sensitive. If **Highlight** or **Inverse Highlight** is selected for Markup Type, you can select Yellow, Green, Blue, Orange, Pink, or Purple as highlight colors. These options are also case sensitive.

  Note: If **Inverse** is selected for the Markup Type, you do not need to select an option for the Markup Subtype.

- **Markup Text**—Enter the desired redaction text. This rule is only needed if **Text** is selected as the Markup Sub-type. There are no formatting requirements.
- **Markup Scope**—Enter one of the following options: Character, Cell, Word, Row, Column, or Sheet. The options are case sensitive.
- **Markup Reason**—Enter text to describe the reason for a markup's application. The text you enter is stored in the Markup Navigator. There are no formatting requirements.

- **DtSearch**—Enter the desired DtSearch style syntax. This rule is case sensitive.
- **InverseRedactsEntireWorkbook**—Enter either True or False. The options are case sensitive. If True is entered, the entire workbook is redacted. If False is entered, the initial redaction is limited to Sheet scope instead of the entire workbook.
- **ExpandSheetMarkupScope**—Determines whether a markup is created for the sheet name whenever a sheet is redacted or not. If this is left blank, the sheet name will not receive markups. Enter text to use as the sheet name redaction. The entered text must follow Excel sheet naming rules to be valid.

29.7.6 Fields

The following sections and fields display while creating a spreadsheet project:

29.7.6.1 Create spreadsheet markup project section

The following fields display in this section:

- **Project Name**—enter the name for this new project.
- **Saved Search**—click on the drop-down menu and select the saved search that contains the Excel spreadsheet and .csv files you wish to apply markups to. Optionally, you can enter a term or terms into search box at the top of the menu to help narrow results and find the desired saved search.

  Note: Selecting a nested search can cause performance issues with Redact and may result in a project that does not successfully complete.

- **Markup Set**—click on the drop-down menu and select the markup set that you wish to use to apply markups.

The following options work separately from the project rules. To learn more, visit Rules section. Depending on which of these options you select and what rules you include in a project, it is possible that one or more of these selected options will override at least some matches that the rules would otherwise find and apply markups to.

- **Redact all headers and footers**—select to replace the content in each header and footer with the default redaction text.
- **Redact all Excel objects**—select to apply a black redaction on all objects in the Excel documents included in this project. Excel objects include: WordArt, SmartArt, and embedded documents (email and Powerpoint), images equations, text-boxes, and shapes.

  Note: Selecting this option does not cause markups to be applied on charts. You can apply redactions to charts manually. To learn more, visit Manual markups with spreadsheet files.

- **Redact all Comments**—select and choose one of the following options to apply markups to comments in Excel documents:
  - **Remove comments**—select to remove any comments on spreadsheet files.
  - **Remove comment text**—select to replace comments with either **[Redacted]** or the text you enter in the box below this option.
- **Fallback text**—If you select redact options that are not valid and the project finds a match in a document, the text entered in this field will be used instead. For example, attempting to apply a black redaction to a .csv file is invalid and so the text entered in this field is applied as a redaction instead.
- **Ignore certain rows or columns**—select this option to prevent markups from being applied to specified rows or columns. This option can be used to ensure headers and footers display in Excel documents. Once this

option is selected, the rows and columns to be excluded from markup section displays underneath. Enter the rows or columns separated by commas that should not have markups applied.

29.7.6.2 Rules section

The Rules section is optional and these fields determine how the spreadsheet project will apply markups once it is run. After completing the fields in this section, a new group of fields will appear below it so that you can create multiple rules in a spreadsheet project if desired.

Note: If you are uploading a .csv file, this section should be left blank. To learn more, visit Creating a spreadsheet markup project using .csv rules.

The following fields display in this section:

- **Redaction/Highlight/Inverse/Inverse Highlight** toggle—if **Place redactions on sheets without matches** is selected, a workbook scope markup is applied if a match is found anywhere on the document. If **Place redactions on sheets without matches** is not checked, a sheet scope markup is applied on sheets where a match is found. Redact also creates Inverse markups on each match, following the Scope specified by the rule group.

  Note: Highlights are not compatible with .csv files. If you select either highlight option and run a project, it will result in errors and markups will not be applied to terms that match this rule.

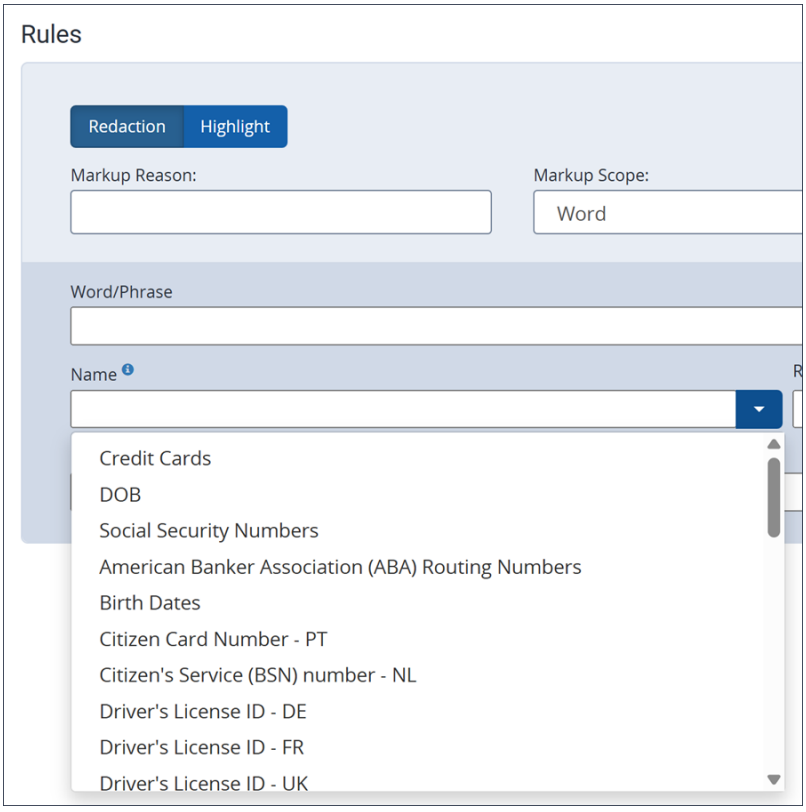
- **Markup Reason**—enter a description of why the markup for this rule will be applied to make it easy to track when reviewing markups using the Redact Navigation card.
- **Markup Scope**—determines the markup behavior when the project matches content in a document with a rule. Select one of the following options:
  - **Character**—places the markup on each cell where the entered characters match or on any non-cell character matches. This option can be used to redact information that is not a word such as an email handle or a social security number. Inverse redactions are not compatible with character markups. Markups applied using this option are not compatible with Convert Spreadsheet Markups.
  - **Word**—places the markup only on the exact matched text inside each cell that fits this rule. This option is only available if *Redaction* is selected.
  - **Cell**—places the markup on each cell that matches this rule. All of the content in the cell where a match is made will be covered by the markup.
  - **Row**—places the markup on the entire row where a cell matches this rule.
  - **Column**—places the markup on the entire column where a cell matches this rule.
  - **Sheet** — places a markup on the entire sheet where a cell matches this rule. If a match is found in the sheet name and not any other cells in the sheet, only the sheet name will receive a markup.
    - **Include Sheet name & content** — this option only displays when Sheet is selected. Select this option to apply a markup to both the sheet name and the sheet when a match is found. If this option is not selected and a match is found in the sheet name and not any other cells in the sheet, only the sheet name will receive a markup.
- **Markup SubType**—select the style of markup you would like to place for this rule. The options available in this drop-down menu are determined by the Redaction/Highlight/Inverse/Inverse Highlight toggle.

Note: Certain fields and file formats only support Text redactions. If you select a Markup SubType other than Text, and the project applies markups to a location that only supports Text redactions, those redactions will be changed to show the project's specified Fallback text. Areas where this applies include:
- All locations within a CSV
- Excel sheet names
- Excel headers & footers
- Excel comments
- Excel chart labels

- **Place redactions on sheets without matches**—select to place inverse redactions or highlights on any sheets that do not have content that matches this rule. This option best used when you want the majority of the documents to be redacted except for key information determined by this rule. This option can only be selected if Inverse or Inverse Highlight are selected above.
- **Word/Phrase**—enter the words, phrases, and text that you would like to apply a markup to for this rule. Multiple words or phrases can be added to a single rule group. The words, phrases, and text you enter are case sensitive.

Note: This field does not support dtSearch or wildcard syntax.

- **Name**—enter a name for this rule. Optionally, click on the drop-down menu to view a list of commonly used regular expressions as well as custom regular expressions users have created and select one to populate both the **Name** and **Regex** fields. These commonly used regular expressions are a starting point and not intended be all-inclusive of every variation of these patterns. Variations in document type, text quality, and pattern variability should be considered when using regular expressions.



- **Regex**—enter a regular expression which can be used to identify important patterns like email addresses, social security numbers, credit card numbers, and any other content that may appear in a regular pattern

throughout the documents in the selected saved search. Regular expressions require a name and the expression to be valid. After saving the spreadsheet markup project, the regular expressions you entered can be selected by name on other Redact automated projects within the same workspace. To see examples of commonly used regular expression terms, see Regular expression examples.

Note: If you use regex101.com to help form regular expressions to enter in Redact, ensure that you set it to /gmi (global, multi-line, case insensitive) to help you better achieve the desired results in Relativity.

When using regular expressions, the scope of markups applied is based on word. When a regular expression matches the word, it uses spaces to determine where to start and stop applying the markup. So if a set of words do not have spaces between them, a markup will be applied to the entire set and not just the word that matches your entered terms.
The following table includes potential terms that can be searched using regular expressions and an example of a word or phrase that will be completely covered by a markup to illustrate this behavior:

Regular Expression Terms	Marked up content
jane, smith, relativity	jane.smith@relativity.com
police, woman	policewoman
mother, in, law	mother-in-law

- **DtSearch**—Enter a DtSearch syntax where you would like to apply markups to any matches based on the Markup Scope and Markup SubType options selected. By default, Redact will apply markups to every term in a search syntax. DtSearch matches are evaluated within individual cells. If a match would span multiple cells, markups are not applied and only matches contained entirely within a single cell are redacted.
  Optionally, you can apply markups to part of a DtSearch syntax. For example, apple w/2 pear causes both apple and pear to receive markups. If you would like to apply a markup to one of the terms, in this case, apple, use the following syntax: (?<redact>apple) w/2 pear.
  Noise words and the alphabet list are not compatible with this field. We recommend using W/N operator for proximity matches instead.

  Note: Combining special characters or operators may lead to inaccurate results. We recommend using Regex in these situations instead

  The following syntax options are available with this field:

Special characters or operators	DtSearch functionality
AND, OR, NOT	Boolean operators
?,*	Wildcards
W/N (or WI)	W/N operators
PRE	Proximity with terms order
xfirstword, xlastword	Built-in search words
()	Operator precedence
""	Search words that are operators
%	Fuzzy searching
~	Stemming
(<?redact> {term})	Partial redaction

Special characters or operators	DtSearch functionality
!"#$&'()*+,./:;<=>?@{|}^{|}~˜	Special characters recognized as spaces that cause word breaks
#	Phonic searching
=	Numerical patterns

29.7.7 Running the project

Once you have created a project, you can run it to apply markups. To learn more, visit Running and reverting a Redact project.

Note: If a document that is too large is included in a project, it may not receive markups. The maximum file size for documents that can be opened in the Viewer and receive markups is determined by the *MaximumNativeSizeForViewerInBytes* instance setting. Increasing this instance setting's value can negatively impact Relativity's performance.

29.7.8 Reviewing markups

After markups have been placed, it is a best practice to perform quality control on documents before they are produced. To learn more about how to do this using Redact, visit Reviewing markups to ensure accuracy.

29.7.9 Reviewing the original native document

When a spreadsheet document is prepared by Redact, there are changes made to the native file to facilitate markup application. The changes include unhiding hidden columns, rows, and sheets. By the end of the preparation process, the original document is backed up to an RDO and the native is replaced with the flattened document.

If you would like to validate what content was previously hidden in a spreadsheet file, you can use the Open Original Native button to compare the document both before and after Redact preparation.

To access the original native file directly from the Viewer:

1. Navigate to the **Documents** tab and select a spreadsheet document from the list that has already been prepared for Redact.
2. Click on the **Open Original Native** button.
   A new browser window opens where you can click **Native** to view the native spreadsheet document or click **Original Native Text** to see the document before it was prepared for Redact.

29.8 Automated image markup project

Creating an image markup project allows you to apply markups to a group of imaged documents automatically saving you time. You can create a project by entering words, terms, phrases, or regular expressions that you would like Redact to apply markups to. Alternatively, you can enter the rules in a .csv file and upload it to Relativity to create the rules for the image markup project. Once the project is created and run, markups will be applied automatically based on the rules you create.

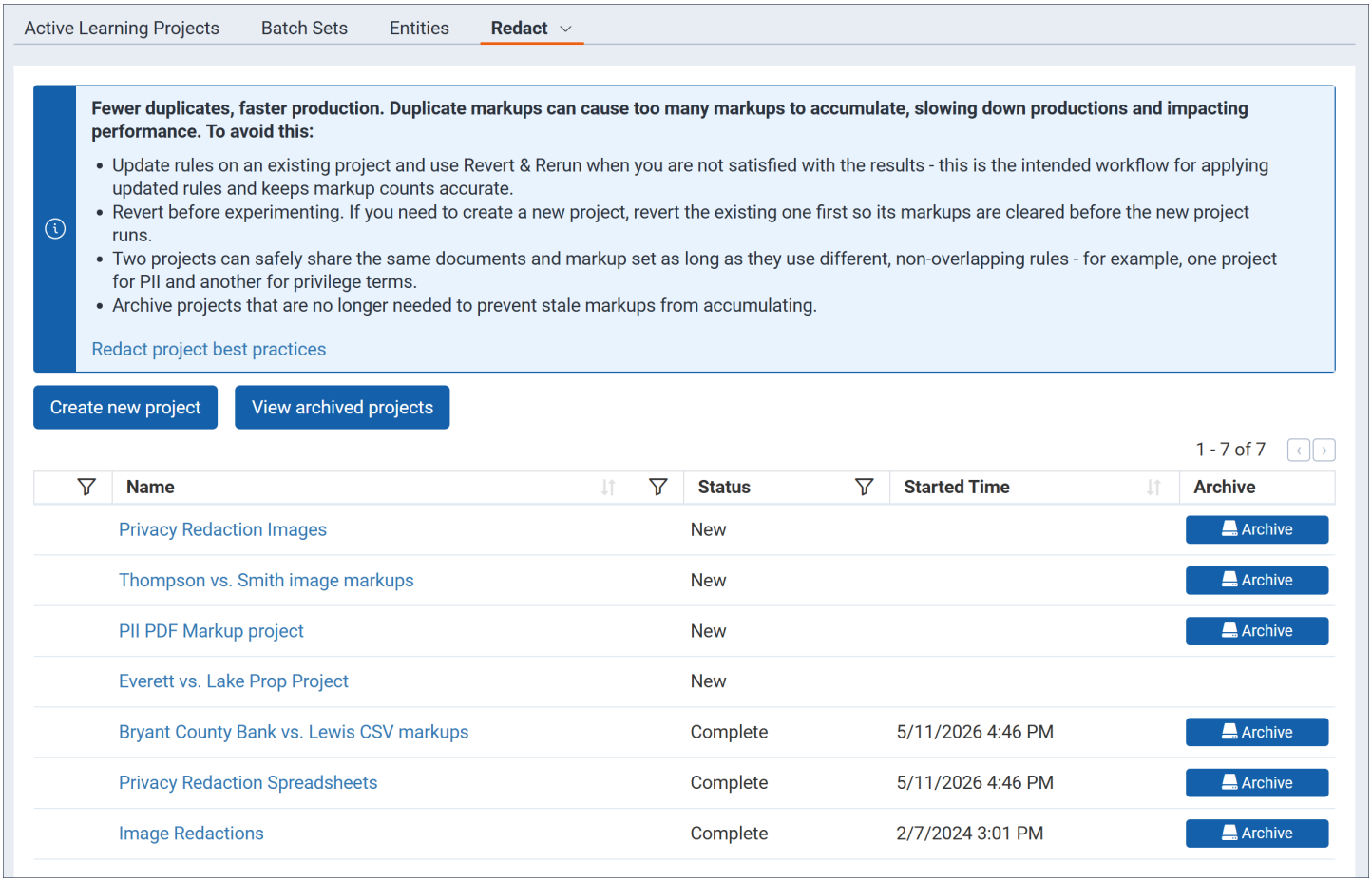
29.8.1 Before you begin

Consider creating a saved search with the documents you wish to apply markups to and a markup set that contains the markups you wish to apply to your imaged documents before starting the image markup project creation process.

29.8.2 Creating an image markup project manually

To create an image markup project using rules that you manually set, do the following:

1. Navigate to the **Redact Projects** tab.



2. Click **Create new project** button.
3. Select the **Image** project option.
4. Complete the **Create image markup project** section fields. To learn more, visit Fields below.

Note: Using the same or similar documents, the same or similar rules, and the same markup sets in more than one project can lead to duplicate markups being applied.

5. Complete the **Rules** section fields. This section is optional and if you complete these fields, they will determine how the image project applies markups. To learn more, visit Fields below. Alternatively, you can leave these fields blank and upload a .csv file. To learn more, visit the Creating an image markup project using .CSV rules below.
6. Click **Save**.

29.8.3 Creating an image markup project using .csv or .xlsm rules

While a project can be created manually, if you plan on running multiple kinds of projects with similar rules and terms, you can save time by using the same copy of .csv or .xlsm rules for each project. Please note that you may still need to adjust the scope in the rules based on which project you are running.

You can upload up to 100,000 rules in a .csv file though it is worth noting that the more rules are included in a .csv or .xlsm file, the longer a project will take to run. Rules that are uploaded with a .csv file cannot be viewed in the Redact interface and instead, you will need to download a copy of the .csv file and view it outside of Relativity.

Once you have entered the desired rules, save this file as a .csv before uploading to Relativity.

To create an image markup project using rules generated by a .csv file, do the following:

1. Navigate to the **Redact Projects** tab.
2. Click **Create new project** button.
3. Select the **Image** project option.
4. Enter a **Project Name** and select a **Saved Search** and **Markup Set**. Leave all other fields blank. For more information on these fields, visit Fields below.
5. Click **Save**.
6. Click on **Upload rules csv**.
7. Select the desired .csv or .xlsm file from your workstation and click **Open**.
   The file is uploaded and the rules will be created and added to the project.

29.8.3.1 .csv or .xlsm rules

Guidance for how to configure rules using a .csv or .xlsm file is provided below. To learn more about the functionality of the rules, visit Rules section below.

- **Word/Phrase**—Enter the desired word or phrase. There are no formatting requirements.
- **RegEx Name**—Enter name of the regular expression. There are no formatting requirements.
- **RegEx**—Enter the regular expression syntax. There are no formatting requirements.
- **Markup Type**—Enter one of the following options: Redaction or Highlight. The options are case sensitive.
- **Markup Subtype**—Enter one of the following options: Redactions, Black, Text, Cross, White, or Inverse. The options are case sensitive. If **Highlight** is selected for the Markup Type, you can select Yellow, Green, Blue, Orange, Pink, or Purple. These options are also case sensitive.

  Note: If **Inverse** is selected for the Markup Type, you do not need to select an option for the Markup Subtype.

- **Markup Text**—Enter the desired redaction text. This rule is only needed if **Text** is selected as the Markup Subtype. There are no formatting requirements.
- **Markup Scope**—Enter one of the following options: Character, Word, Line, Paragraph, Page, or Document. The options are case sensitive.
- **Expand Markup to Full Width of Page**—Enter either True or False. The options are case sensitive. If True is entered, markups are expanded to the width of the page. If False is entered, markups are not resized.
- **DtSearch**—Enter the desired DtSearch style syntax. This rule is case sensitive

29.8.4 Fields

The following sections and fields display while creating an image markup project:

29.8.4.1 Create image markup project section

The following fields display in this section:

- **Project Name**—enter the name for this new project.
- **Language Code**—enter the desired language code or codes if you wish to specify a non-English language for OCR. English is selected by default and you do not need to alter this option if the documents should remain in English. To learn more about how to enable non-English languages and enter codes, visit Redact Language Support.

- **Saved Search**—click on the drop-down menu and select the saved search that you wish to apply markups to. Optionally, you can enter a term or terms into search box at the top of the menu to help narrow results and find the desired saved search.

  Note: Selecting a nested search can cause performance issues with Redact and may result in a project that does not successfully complete.

- **Markup Set**—click on the drop-down menu and select the markup set that you wish to use to apply markups.

29.8.4.2 Rules section

The Rules section is optional and these fields determine how the image project will apply markups once it is run. After completing the fields in this section, a new group of fields will appear below it so that you can create multiple rules in an image project if desired.

Note: If you are uploading a .csv file, this section should be left blank. To learn more, visit Creating an image markup project using .CSV rules.

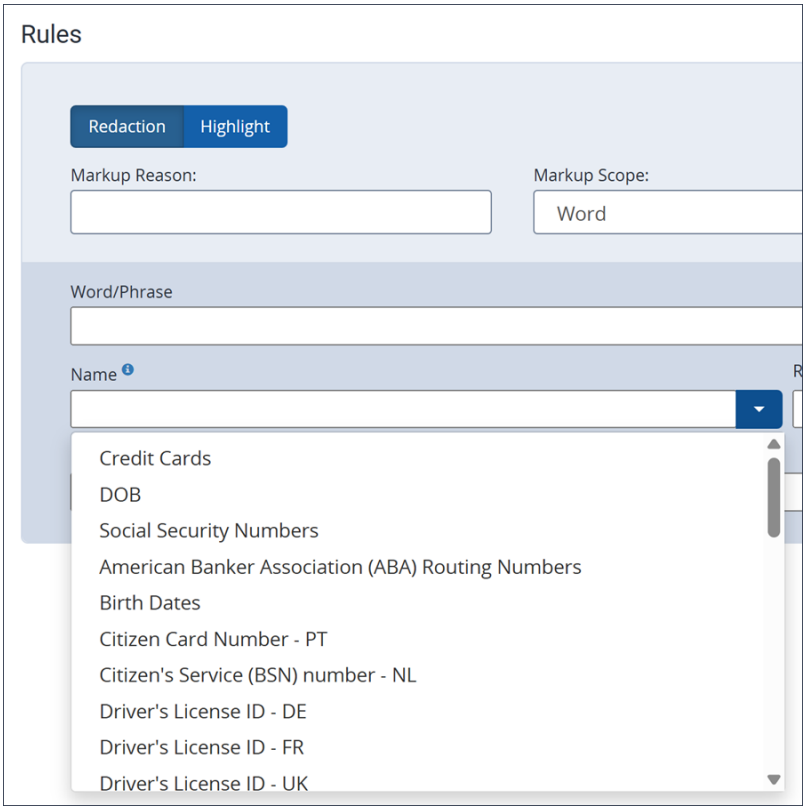
The following fields display in this section:

- **Redaction/Highlight** toggle—determines which type of markup you will be applying for this rule.
- **Markup Reason**—enter a description of why the markup for this rule will be applied to make it easy to track when reviewing markups using the Redact Navigation card.
- **Markup Scope**—determines the markup behavior when the project matches content in a document with a rule. Select one of the following options:
  - **Character**—places the markup on the exact match even if the match is part of a word. When this option is selected, new OCR text is generated before markups are applied. This option can also be used to redact information that is not a word such as an email handle or a social security number
  - **Word**—places the markup on the entire word that matches this rule.
  - **Line**—places the markup on the entire line of text where a word matches this rule.
  - **Paragraph**—places the markup between the most recent previous carriage return and the next carriage return where there is a word that matches this rule.
  - **Page**—places a markup on the entire page where there is a word that matches this rule.
  - **Document**—places a full-page markup on the entire document if there is a word that matches this rule.
- **Markup SubType**—select the style of markup you would like to place for this rule. The options available in this drop-down menu are determined by the Redaction/Highlight toggle.
- **Expand markup to full width of page**—select to apply a markup that spans the entire width of the page when a match is found. This option is intended for use with the Line, Paragraph, Page, or Document option in the Markup Scope drop-down menu.
- **Word/Phrase**—enter the words, phrases, and text that you would like to apply a markup to for this rule. Multiple words or phrases can be added to a single rule group. The words, phrases, and text you enter are case sensitive.

  Note: This field does not support dtSearch or wildcard syntax.

- **Name**—enter a name for this rule. Optionally, click on the drop-down menu to view a list of commonly used regular expressions as well as custom regular expressions users have created and select one to populate both the **Name** and **Regex** fields. These commonly used regular expressions are a starting point and not intended be all-

inclusive of every variation of these patterns. Variations in document type, text quality, and pattern variability should be considered when using regular expressions.



- **Regex**—enter a regular expression which can be used to identify important patterns like email addresses, social security numbers, credit card numbers, and any other content that may appear in a regular pattern throughout the documents in the selected saved search. Regular expressions require a name and the expression to be valid.
  Regular expressions can make false matches with image markup projects. Markup placement is dependent on the quality of HOCR produced from the source image. As a result, we recommend being defensive against common OCR mistakes. Each instance of any digit match can be replaced with a character replacement pattern that will evaluate numbers as common alphanumeric characters. To do so simply replace the \d pattern with [\dOIlZEASB].
  After saving the image markup project, the regular expressions you entered can be selected by name on other Redact projects within the same workspace. To see examples of commonly used regular expression terms, see Regular expression examples.

  Note: If you use regex101.com to help form regular expressions to enter in Redact, ensure that you set it to /gmi, global, multi-line, case insensitive, to help you better achieve the desired results in Relativity.

  When using regular expressions, the scope of markups applied is based on word. When a regular expression matches the word, it uses spaces to determine where to start and stop applying the markup. So if a set of words do not have spaces between them, a markup will be applied to the entire set and not just the word that matches your entered terms.
  The following table includes potential terms that can be searched using regular expressions and an example of a word or phrase that will be completely covered by a markup to illustrate this behavior:

Regular Expression Terms	Marked up content
jane, smith, relativity	jane.smith@relativity.com
police, woman	policewoman
mother, in, law	mother-in-law

- **DtSearch**—enter a dtSearch syntax where you would like to apply markups to any matches based on the Markup Scope and Markup SubType options selected. By default, Redact will apply markups to every term in a search syntax. dtSearch uses cross-cell matching so if a rule has text that would span multiple cells, all cells that contain a match will be redacted.
  Optionally, you can apply markups to part of a dtSearch syntax. For example, apple w/2 pear causes both apple and pear to receive markups. If you would like to apply a markup to one of the terms, in this case, apple, use the following syntax: (?<redact>apple) w/2 pear.
  Noise words and the alphabet list are not compatible with this field. We recommend using W/N operator for proximity matches instead.

  Note: Combining special characters or operators may lead to inaccurate results. We recommend using Regex in these situations instead.

  The following syntax options are available with this field:

Special characters or operators	DtSearch functionality
AND, OR, NOT	Boolean operators
?,*	Wildcards
W/N (or WI)	W/N operators
PRE	Proximity with terms order
xfirstword, xlastword	Built-in search words
()	Operator precedence
""	Search words that are operators
%	Fuzzy searching
~	Stemming
(<?redact> {term})	Partial redaction
!"#$&'()*+,./:;<=>?@{|}^{|}~˜	Special characters recognized as spaces that cause word breaks
#	Phonic searching
=	Numerical patterns

29.8.5 Running the project

Once you have created a project, you can run it to apply markups. To learn more, visit Running and reverting a Redact project.

Note: If you run a project and would like to edit the rules to get different results, we recommend reverting the project before editing the rules and rerunning it to prevent duplicate markups. To learn more, see Redact project best practices.

29.8.6 Reviewing markups

After markups have been placed, it is a best practice to perform quality control on documents before they are produced. To learn more about how to do this using Redact, visit Reviewing markups to ensure accuracy. If markups were placed on OCR text, we recommend using the **View hocr** button to validate project rule hit results. To learn more, visit Using the Redact navigation card in the Image Viewer.

29.9 Automated image template markup project

An image template project can be used to propagate all of the markups applied to a single, imaged document to each of the documents in a saved search. This is an effective way to apply markups in the same location for a group of documents. For example, if there is sensitive information in a series of tax forms that you want to obscure, you can run an image template project to apply the markups to each document.

29.9.1 Before you begin

To use this project, you will need to choose an imaged document and create a saved search.

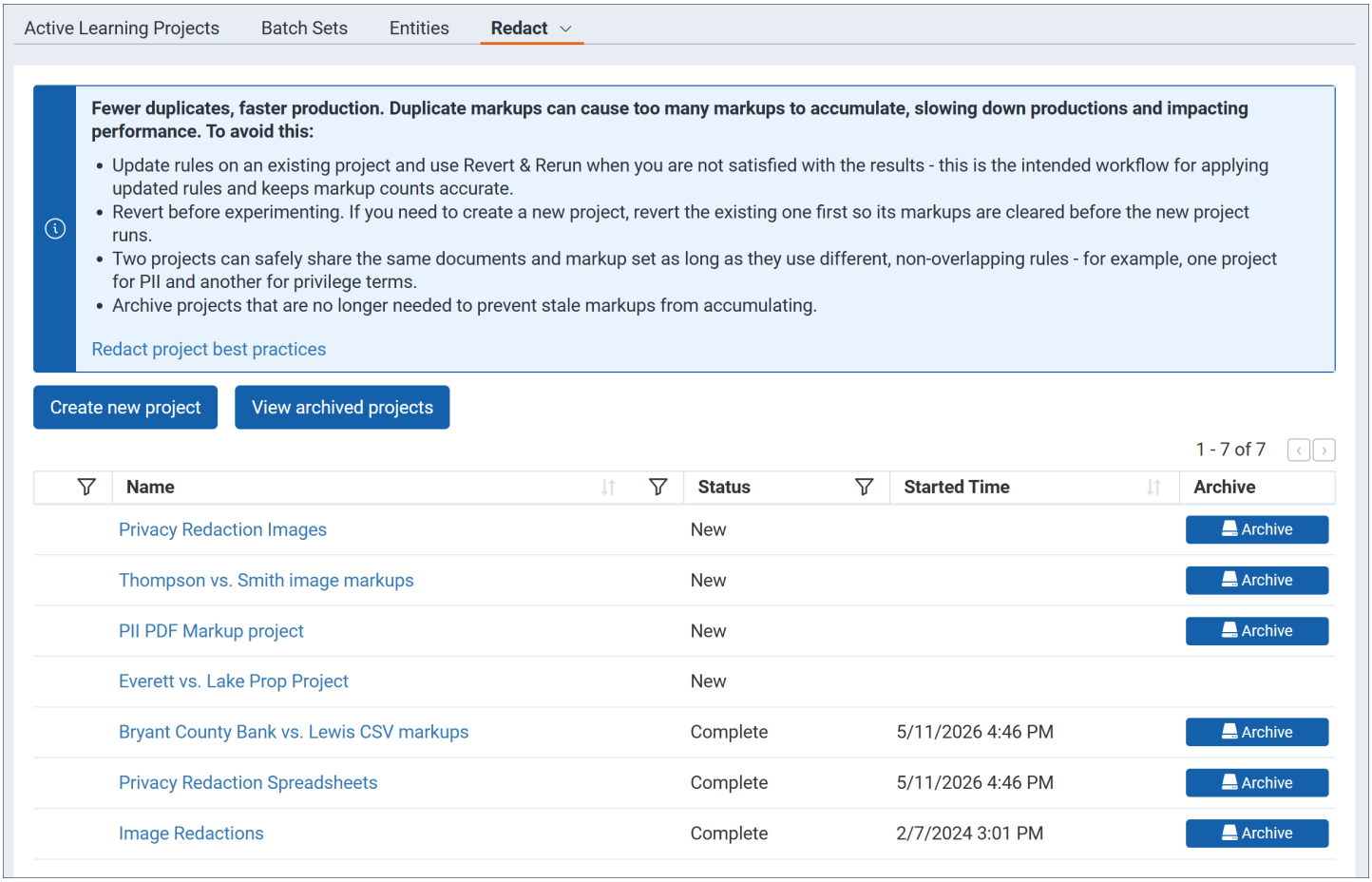
The chosen document should contain markups in the locations where you want to apply markups to the documents in your saved search. It is helpful to record the Control Number of this document because it will be entered in the Template Document Control Number field when creating the project.

The saved search should contain the set of documents that will receive the markups in the same locations as the chosen document.

29.9.2 Creating an image template markup project

To create an image template markup project, do the following:

1. Navigate to the **Redact Projects** tab.



2. Click **Create new project** in the upper-left.
3. Select the **Image Template** project option.
4. Complete the Create image template project section fields. To learn more, visit Fields below.

Note: Using the same or similar documents, the same or similar rules, and the same markup sets in more than one project can lead to duplicate markups being applied.

5. Click **Save**.

29.9.3 Fields

The following fields display in the Create image template project section:

- **Project Name** - Enter the name for this new project.
- **Saved Search** - Click on the drop-down menu and select the saved search that contains the documents you wish to apply markups to. Optionally, you can enter a term or terms into search box at the top of the menu to help narrow results and find the desired saved search.

  Note: Selecting a nested search can cause performance issues with Redact and may result in a project that does not successfully complete.

- **Markup Set** - Click on the drop-down menu and select the markup set that you wish to use to apply markups.

- **Template Document Control Number** - Enter the control number of the document that you wish to use as the source for markups and then propagate those markups to the documents in the saved search.

  Note: The document you use for this field applies markups to documents in the saved search based on the number of pages it has. For example, if you enter the control number for a document that only has one page, when you run the project, it will only apply markups to the first page of all the documents in the saved search, even if some of those documents contain two or more pages.

29.9.4 Running the project

Once you have created a project, you can run it to apply markups. To learn more, visit Running and reverting a Redact project.

Note: If you run a project and would like to edit the rules to get different results, we recommend reverting the project before editing the rules and rerunning it to prevent duplicate markups. To learn more, see Redact project best practices.

29.9.5 Reviewing markups

After markups have been placed, it is a best practice to perform quality control on documents before they are produced. To learn more about how to do this using Redact, visit Reviewing markups to ensure accuracy.

29.10 Automated PDF markup project

Creating a PDF markup project allows you to apply markups to the text of PDF files automatically saving you time. Redact can apply markups to any part of a PDF file that has searchable text including: page text, headers, footers, text-based annotations, form data, and field properties. You can create a project manually by entering words, terms, phrases, or regular expressions that you would like Redact to apply markups to. Alternatively, you can enter the rules in a .csv file and upload it to Relativity to create the rules for the PDF markup project. Once the project is created and run, markups will be applied automatically based on your selected options.

29.10.1 Before you begin

Consider creating a saved search with the documents you wish to apply markups to and a markup set that contains the markups you wish to apply to your PDF files before starting the PDF markup project creation process.

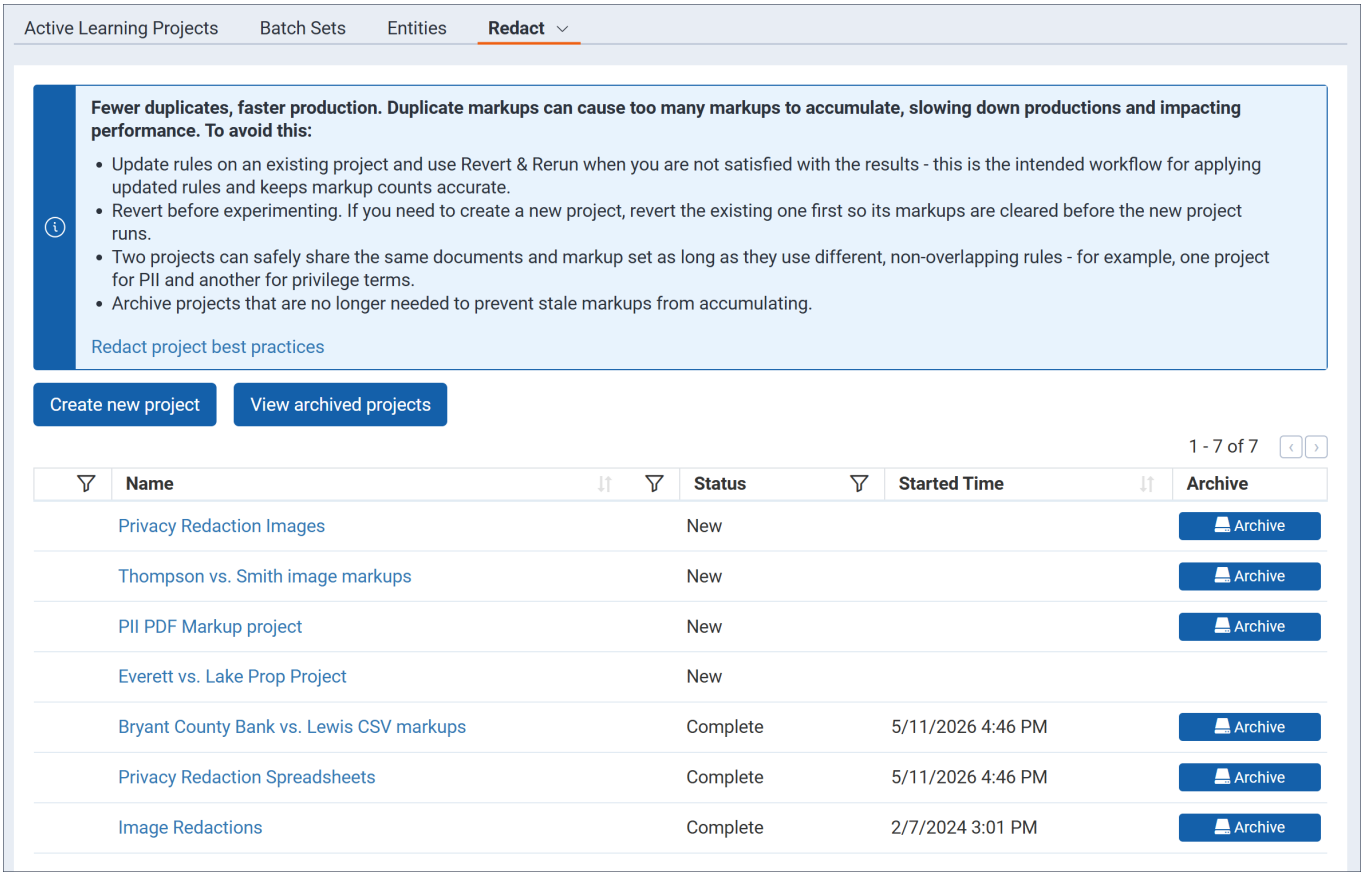
29.10.2 Supported file types

To learn more about which file types are compatible with Redact, see Redact supported file types.

29.10.3 Creating a PDF markup project manually

To create a PDF markup project using rules that you manually set, do the following:

1. Navigate to the **Redact Projects** tab.



2. Click **Create new project** in the upper-left.
3. Select the **PDF** project option.
4. Complete the Create PDF markup project section fields. To learn more, visit Fields below.

Note: Using the same or similar documents, the same or similar rules, and the same markup sets in more than one project can lead to duplicate markups being applied.

5. Complete the Rules section fields. This section is optional and if you complete these fields, they will determine how the PDF project applies markups. To learn more, visit Fields below. Alternatively, you can leave these fields blank and upload a .csv file. To learn more, visit the Creating a PDF markup project using .csv rules section below.
6. Click **Save**.

29.10.4 Creating a PDF markup project using .csv or .xlsm rules

While a project can be created manually, if you plan on running multiple kinds of projects with similar rules and terms, you can save time by using the same copy of .csv or .xlsm rules for each project. Please note that you may still need to adjust the scope in the rules based on which project you are running.

You can upload up to 100,000 rules in a .csv file though it is worth noting that the more rules are included in a .csv or .xlsm file, the longer a project will take to run. Rules that are uploaded with a .csv file cannot be viewed in the Redact interface and instead, you will need to download a copy of the .csv file and view it outside of Relativity.

Once you have entered the desired rules, save this file as a .csv before uploading to Relativity.

To create a PDF markup project using rules generated by a .csv file, do the following:

1. Navigate to the **Redact Projects** tab.
2. Click **Create new project** in the upper-left.
3. Select the **PDF** project option.
4. Enter a **Project Name** and select a **Saved Search** and **Markup Set**. Leave all other fields blank. For more information on these fields, visit Fields below.
5. Click **Save**.
6. Click on **Upload rules csv**.
7. Select the desired .csv or .xlsm file from your workstation and click **Open**.
   The file is uploaded and the rules will be created and added to the project.

29.10.4.1 .csv or .xlsm rules

Guidance for how to configure rules using a .csv or .xlsm file is provided below. To learn more about the functionality of the rules, visit Rules section below.

- **Word/Phrase**—Enter the desired word or phrase. There are no formatting requirements.
- **RegEx Name**—Enter name of the regular expression. There are no formatting requirements.
- **RegEx**—Enter the regular expression syntax. There are no formatting requirements.
- **Markup Type**—Enter one of the following options: Redaction or Highlight. The options are case sensitive.
- **Markup Subtype**—Enter one of the following options: Redactions, Black, Text, or White. The options are case sensitive. If **Highlight** is selected for the Markup Type, you can select Yellow, Green, Blue, Orange, Pink, or Purple. These options are also case sensitive.
- **Markup Text**—Enter the desired redaction text. This rule is only needed if **Text** is selected as the Markup Sub-type. There are no formatting requirements.
- **Markup Scope**—Enter one of the following options: Character, Word, or Line. The options are case sensitive.
- **Markup Reason**—Enter text to describe the reason for a markup's application. The text you enter is stored in the Markup Navigator. There are no formatting requirements.
- **DtSearch**—Enter the desired DtSearch style syntax. This rule is case sensitive.

29.10.5 Fields

The following sections and fields display while creating a PDF project:

29.10.5.1 Create PDF markup project section

The following fields display in this section:

- **Project Name**—enter the name for this new project.
- **Saved Search**—click on the drop-down menu and select the saved search that contains the documents you wish to apply markups to. Optionally, you can enter a term or terms into search box at the top of the menu to help narrow results and find the desired saved search.

  Note: Selecting a nested search can cause performance issues with Redact and may result in a project that does not successfully complete.

- **Markup Set**—click on the drop-down menu and select the markup set that you wish to use to apply markups.

- **PDF Version**—select an option to determine which type of PDF file to apply markups to.
  - **Native**—if selected, markups are applied to the original document and they are visible in the Native Viewer.
  - **Stored**—is selected, markups are applied to the stored PDF generated by the PDF application and the markups are visible in the PDF Viewer.
- **Remove All Attachments**—check to remove all attachments from each document in your selected saved search.

29.10.5.2 Rules section

The Rules section is optional and these fields determine how the PDF project will apply markups once it is run. After completing the fields in this section, a new group of fields will appear below it so that you can create multiple rules in a PDF project if desired.

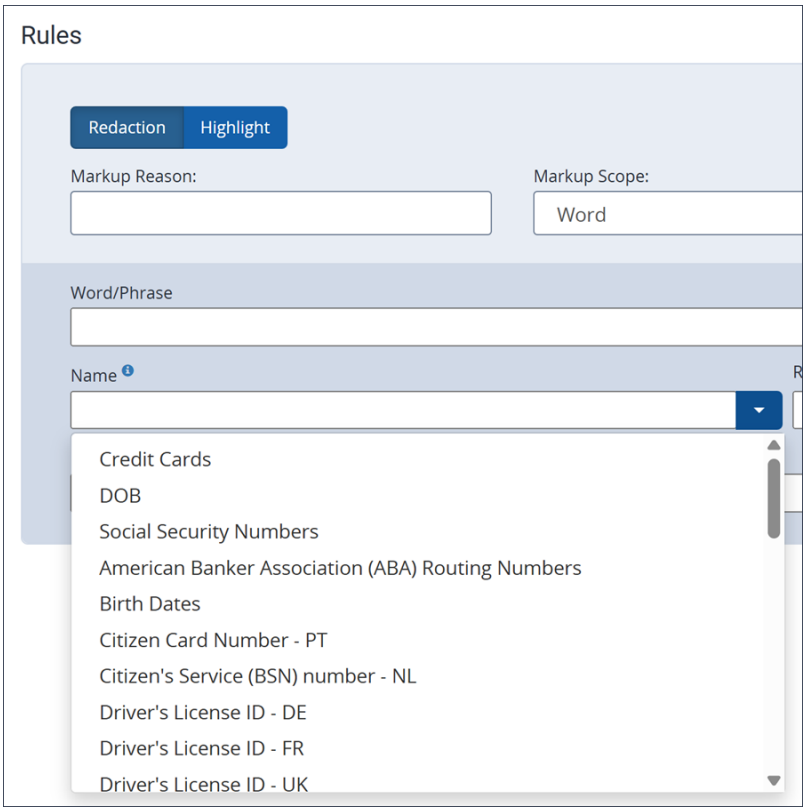
Note: If you are uploading a .csv file, this section should be left blank. To learn more, visit Creating a PDF markup project using .csv rules.

The following fields display in this section:

- **Redaction/Highlight** toggle—determines which type of markup you will be applying for this rule.
- **Markup Reason**—enter a description of why the markup in this group will be applied to make it easy to track when reviewing markups in the Redact Navigation card.
- **Markup Scope**—determines the markup behavior when the project matches content in a document with a rule. Select one of the following options:
  - **Character**—places the markup on the exact match even if the match is part of a word. For example, if Character is selected and you enter jane.smith for the rule, the project will match and apply a markup to Jane's name in jane.smith@domain.com, however, it will not apply a markup to @domain.com.
  - **Word**—places the markup on the entire word, even if only part of the word is matched. For example, if Word is selected and you enter jane.smith for the rule, the project would apply a markup to the entire email address when it matches jane.smith@domain.com.
  - **Line**—places a redaction that spans the entire horizontal line for the given match.
- **Markup SubType**—select the style of markup you would like to place for this rule. The options available in this drop-down menu are determined by the Redaction/Highlight toggle.
- **Word/Phrase**—enter the words, phrases, and text that you would like to apply a markup to for this rule. Multiple words or phrases can be added to a single rule group. The words, phrases, and text you enter are case sensitive.

  Note: This field does not support dtSearch or wildcard syntax.
- **Name**—enter a name for this rule. Optionally, click on the drop-down menu to view a list of commonly used regular expressions as well as custom regular expressions users have created and select one to populate both the **Name** and **Regex** fields. These commonly used regular expressions are a starting point and not intended be all-inclusive of every variation of these patterns. Variations in document type, text quality, and pattern variability

should be considered when using regular expressions.



- **Regex**—enter a regular expression which can be used to identify important patterns like email addresses, social security numbers, credit card numbers, and any other content that may appear in a regular pattern throughout the documents in the selected saved search. Regular expressions require a name and the expression to be valid. After saving the PDF project, the regular expressions you entered can be selected by name on other Redact projects within the same workspace. To see examples of commonly used regular expression terms, see Regular expression examples.

  Note: If you use regex101.com to help form regular expressions to enter in Redact, ensure that you set it to /gmi (global, multi-line, case insensitive) to help you better achieve the desired results in Relativity.

  When using regular expressions, the scope of markups applied is based on word. When a regular expression matches the word, it uses spaces to determine where to start and stop applying the markup. So if a set of words do not have spaces between them, a markup will be applied to the entire set and not just the word that matches your entered term(s).
  The following table includes potential terms that can be searched using regular expressions and an example of a word or phrase that will be completely covered by a markup to illustrate this behavior:

Regular Expression Terms	Marked up content
jane, smith, relativity	jane.smith@relativity.com
police, woman	policewoman
mother, in, law	mother-in-law

- **DtSearch**—enter a dtSearch syntax where you would like to apply markups to any matches based on the Markup Scope and Markup SubType options selected. By default, Redact will apply markups to every term in a search syntax. dtSearch matches are applied across the full document text. If a match spans multiple text lines or pages, each relevant line segment receives a markup.
  Optionally, you can apply markups to part of a dtSearch syntax. For example, apple w/2 pear causes both apple

and pear to receive markups. If you would like to apply a markup to one of the terms, in this case, apple, use the following syntax: (?<redact>apple) w/2 pear.
Noise words and the alphabet list are not compatible with this field. We recommend using W/N operator for proximity matches instead.

Note: Combining special characters or operators may lead to inaccurate results. We recommend using Regex in these situations instead.

The following syntax options are available with this field:

Special characters or operators	DtSearch functionality
AND, OR, NOT	Boolean operators
?,*	Wildcards
W/N (or WI)	W/N operators
PRE	Proximity with terms order
xfirstword, xlastword	Built-in search words
()	Operator precedence
""	Search words that are operators
%	Fuzzy searching
~	Stemming
(<?redact> {term})	Partial redaction
!"#$&'()*+,./:;<=>?@{|}^{|}~˜	Special characters recognized as spaces that cause word breaks
#	Phonic searching
=	Numerical patterns

29.10.6 Running the project

Once you have created a project, you can run it to apply markups. To learn more, visit Running and reverting a Redact project.

Note: If you run a project and would like to edit the rules to get different results, we recommend reverting the project before editing the rules and rerunning it to prevent duplicate markups. To learn more, see Redact project best practices.

Note: If a document that is too large is included in a project, it may not receive markups. The maximum file size for documents that can be opened in the Viewer and receive markups is determined by the *MaximumNativeSizeForViewerInBytes* instance setting. Increasing this instance setting's value can negatively impact Relativity's performance.

29.10.7 Removing a markup applied by a project

To remove a markup that was automatically applied to a PDF document, do the following:

1. Open the desired document in the Viewer.
2. Click on the **Redact PDF Markup Navigator** icon to expand it.
3. Ensure the **Annotations** icon is selected.

4. Hover your cursor over the **Redact** button in the row of the markup you wish to remove and select **Undo**. The selected markup is removed.

29.10.8 Reviewing markups

After markups have been placed, it is a best practice to perform quality control on documents before they are produced. To learn more about how to do this using Redact, visit Reviewing markups to ensure accuracy.

29.11 Automated production preparation project

Note: The production preparation project has been deprecated and as a result, this project should no longer be used as part of your Redact workflow.

If you have documents that were locked by a production preparation project and you need to produce and export them, we recommend using Import/Export. Any unlocked documents can also be exported using Import/Export but the newly unlocked documents must be run or re-run as part of a production so that the markups are burned in before the export.

To learn more about how to handle documents that were locked by a production preparation project in Blackout or Redact, see Blackout migration.

29.12 Automated spreadsheet propagation project

The spreadsheet propagation project can be used to take the markups applied to an Excel spreadsheet and apply them to another group of Excel documents that require similar markups. You can also take markups applied to a .csv document and apply them to a different group of .csv documents. This project uses a saved search that contains the source documents and a saved search with documents you wish to apply markups to and it propagates the markups based on a duplicate identifier such as MD5 Hash.

29.12.1 Preparing Excel documents

We recommend running the Prepare Excel for Redact mass operation, formerly known as the Unhide Excel Content mass operation, on all Excel documents before applying markups with Redact. This preparation is done to ensure data is not lost after the markups are applied and also to prevent information that is covered by markups from being restored by third parties.

To prepare Excel documents:

1. Navigate to the **Documents** tab.
2. Select the desired Excel documents from the list.
3. Click on the mass operations menu and select the **Prepare Excel for Redact** option.
4. Click **Confirm**.
   The selected Excel documents are ready to receive markups using Redact.

29.12.2 Before you begin

To run this project, you will need a *source* saved search that contains only the Excel or .csv documents with markups that you wish to apply to other documents. Additionally, every document in this search should have a duplicate identifier field selected. This saved search should not include any duplicate documents.

You will also need a *destination* saved search that contains all of the Excel or .csv documents that you wish to receive markups. Both saved searches should only contain either Excel documents or .csv documents. These documents should not contain any redactions, regardless of QC status, otherwise, they will be skipped by the project. Documents

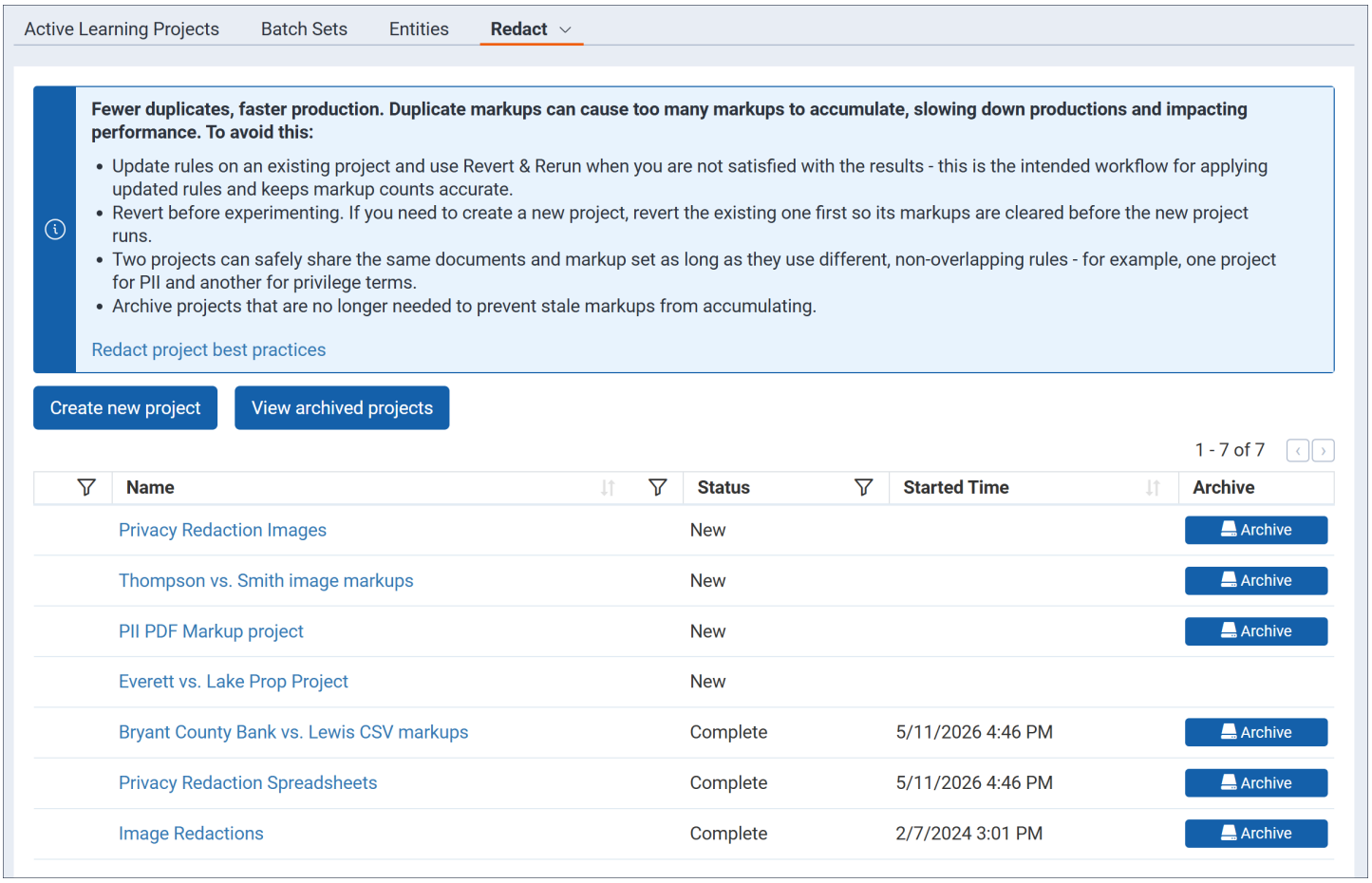
in the previous, *source* saved search should not be included in this destination saved search. Document duplicates are identified by the project based on the selected duplicate identifier field.

Note: Selecting a nested search can cause performance issues with Redact and may result in a project that does not successfully complete.

29.12.3 Creating a spreadsheet propagation markup project

To create a spreadsheet propagation markup project, do the following:

1. Navigate to the **Redact Projects** tab.



2. Click the **Create new project** button.
3. Select the **Spreadsheet propagation** project option.
4. Complete the **Create spreadsheet propagation project** section fields. To learn more, visit Fields.

Note: Using the same or similar documents, the same or similar rules, and the same markup sets in more than one project can lead to duplicate markups being applied.

5. Click **Save**.

29.12.4 Fields

The following fields display in the Create spreadsheet propagation project section:

- **Project Name**—enter the name for this new project.
- **Duplicate Identifier**—select the identifier that is assigned to the documents in the *source* saved search.

Source Documents

- **Saved Search**—click on the drop-down menu and select the saved search that contains either only Excel or .csv documents with markups that you wish to use as the source to be applied to another group of Excel or .csv documents. Optionally, you can enter a term or terms into search box at the top of the menu to help narrow results and find the desired saved search.

  Note: Selecting a nested search can cause performance issues with Redact and may result in a project that does not successfully complete.

- **Markup Set**—click on the drop-down menu and select the markup set that contains markups used on the documents in the *source* saved search.

Destination Documents

- **Saved Search**—click on the drop-down menu and select the saved search that contains either only the Excel or .csv documents that you wish to receive markups from the source documents. Optionally, you can enter a term or terms into search box at the top of the menu to help narrow results and find the desired saved search.

  Note: Selecting a nested search can cause performance issues with Redact and may result in a project that does not successfully complete.

- **Markup Set**—click on the drop-down menu and select the markup set that you wish to use to apply markups to the destination Excel or .csv documents.
- **Clear Markup Set**—If this option is selected, any markups or external redactions placed on a spreadsheet document in the destination documents are removed so that they receive new markups from the spreadsheet propagation project. If this option is not selected, documents with markups or external redactions are skipped by the project.

29.12.5 Running the project

Once you have created a project, you can run it to apply markups. To learn more, visit Running and reverting a Redact project.

Note: If a document is skipped but does not appear to have markups associated with it, try clearing the markup set and re-running the project.

Note: If a document that is too large is included in a project, it may not receive markups. The maximum file size for documents that can be opened in the Viewer and receive markups is determined by the *MaximumNativeSizeForViewerInBytes* instance setting. Increasing this instance setting's value can negatively impact Relativity's performance.

29.12.6 Reviewing markups

After markups have been placed, it is a best practice to perform quality control on documents before they are produced. To learn more about how to do this using Redact, visit Reviewing markups to ensure accuracy.

Note: If you run a project and would like to edit the rules to get different results, we recommend reverting the project before editing the rules and rerunning it to prevent duplicate markups. To learn more, see Redact project best practices.

29.12.7 Reviewing the original native document

When a spreadsheet document is prepared by Redact, there are changes made to the native file to facilitate markup application. The changes include unhiding hidden columns, rows, and sheets. By the end of the preparation process, the original document is backed up to an RDO and the native is replaced with the flattened document.

If you would like to validate what content was previously hidden in a spreadsheet file, you can use the Open Original Native button to compare the document both before and after Redact preparation.

To access the original native file directly from the Viewer:

1. Navigate to the **Documents** tab and select a spreadsheet document from the list that has already been prepared for Redact.
2. Click on the **Open Original Native** button.
   A new browser window opens where you can click **Native** to view the native spreadsheet document or click **Original Native Text** to see the document before it was prepared for Redact.

29.13 Blackout migration

Relativity now supports Blackout when using ARM to restore a workspace from Relativity Server to Relativity aiR. Native and image markups, Redact projects, and Redact reports are migrated from Blackout to Redact using this process. The event handlers run when updating to the next version of Redact post-installation. The event handlers do not need to be configured and they will automatically update previously migrated Blackout workspaces.

You can now migrate documents that were included in the Redact External Markups workflow. To learn more about this workflow, see Redact External Markups. If you have used this workflow to upload documents with external markups, they are now be supported in the archive and restore of the workspace.

Note: Before starting the archive or restore process, ensure that you have upgraded to Server 2025 Patch 1 and Server 2024 Patch 3 and are using Blackout 5.0, 5.1, or 5.2 and the most recent version of Relativity aiR Redact.

29.13.1 Limitations

- If you run an image markup project, you will need to re-HOCR each of the documents included in the project.
- There are no longer any limitations related to the CorrelationId column.
- If a user attempts to export an audit report from a server-migrated workspace and the table contains entries which map to Audit types that do not exist in Redact, the resulting audit will report the type as **Unknown**. The following audit types are marked as Unknown:
  - Image Markup Created using Find & Redact
  - Image Markup Created using Suggestions
  - Native Document Downloaded
  - Document Unlocked
  - Document Locked

29.13.2 Production preparation

The following considerations should be used for documents redacted in Blackout with the production preparation project. The production preparation project has been deprecated in Redact and native spreadsheet and PDF redactions are now burned in at the time of production.

29.13.2.1 For native spreadsheets and PDFs before the migration

These documents should be unlocked using the production preparation project as soon as possible, preferably by using Blackout before the migration. If you want to modify native redactions in Redact, you must also revert the production preparation project in Blackout before migration. If you want to produce the native redactions in Redact and the production preparation project has already been run in Blackout, you only need to run production in Relativity aiR and then export the documents using Import/Export.

Some other considerations for these document types include:

- To edit a markup in Redact that was burned in using Blackout, the markup must be reverted using the production prep project in Blackout or Redact.
- Any markup burned in using Blackout will be produced in Relativity aiR during production whether it was locked by production prep or not.
- Locking a document does not affect anything in Relativity aiR other than preventing a user from editing the markups. Locked documents have to be unlocked in either Blackout or Redact to edit the markups.

29.13.2.2 Unlocking documents in Redact or Blackout before migration

Documents are locked by production preparation projects to ensure that once the documents are produced, the desired markups are maintained. However, sometimes the circumstances in a case change and you are required to update previously produced documents. When needed, you can unlock documents to allow any user to edit or apply new markups to them.

Note: The original native that has markups is no longer accessible after you unlock the project. As a result, we recommend creating a copy of the marked up native before unlocking the project.

Note: If you unlock a production preparation project in Redact, the production preparation project will no longer be available.

To unlock documents that were previously produced by a project:

1. Navigate to the **Redact Projects** tab and click on the project which contains the produced documents you wish to unlock.
2. Click **Unlock Project**.
   The Unlock Project modal displays.
3. Click **OK**.
   The unlock documents task is added to the queue and will begin running when agents are available. Once the task is complete, a message will display at the top of the screen when viewing a production preparation project indicating that the documents are unlocked.

Note: If you run the project a second time, it will regenerate the extracted text over whatever was added to the field in the first run. Additionally, if you selected **Retain a copy of the redacted file**, an additional copy will be created during the second run.

29.14 Convert Markups

You can use the Convert Markups mass operation, formerly known as Convert Spreadsheets Markup, to change the highlights to redactions or vice versa, regardless of whether the markups were created manually or by an automated project. The Convert Markups mass operation works with native spreadsheets, native PDFs, and stored PDF documents. Alternatively, you can use this mass operation to change the redactions from one type in a document to another.

Note: Only text or cell content redactions can be applied to .csv files.

29.14.1 Changing markup types

To switch markup types in a document or series of documents, do the following:

1. Navigate to the **Documents** tab and select any documents you wish to convert.
2. Select the **Convert Markups** option from the mass operations bar.
3. For the Files to Convert field, select either **Natives (PDF & Spreadsheets)** or **Stored PDFs** to determine which type of documents are affected.
4. Select the **Markup Set** you wish to convert and then select the **Markup Type** and **Markup Subtype** you wish to convert from and to.
5. Click **Submit**.
   The selected documents have the applied highlights converted to redactions or the applied redactions converted to highlights and an email is sent to the user's email address that summarizes the results of the mass operation.

29.14.2 Reviewing converted markups

There are some special considerations when reviewing converted markups or re-running Redact projects that involve converted markups. Once a document has had markups converted, using the Accept/Reject column in the Redact Navigation card will remove and replace the converted markup. To learn more about the Redact Navigation card, visit Reviewing markups to ensure accuracy.

However, if a project is reverted and run again, that project's rules will be reapplied and the conversions applied by the Convert Markups mass operation are lost.

29.15 Manual markups with spreadsheet files

Redact allows you to apply manual markups to Excel or .csv files in the Viewer. You can apply markups to specific parts of an Excel file including the sheet names, charts, objects, and headers and footers. An audit of the markups applied to each document can be viewed at any time to make tracking markups easy. You can also quickly locate any markups in a document and approve or reject them as part of your quality control process by using the Redaction Navigation card.

Note: Placing a markup on a document causes the coding layout to refresh. If you are editing a layout and place a markup, any unsaved edits to the layout fields will be lost. We recommend editing the fields on a layout and saving your changes before applying manual markups to a document.

If you would prefer to have markups applied automatically, see Automated spreadsheet markup project and Automated spreadsheet propagation.

29.15.1 Preparing Excel documents

We recommend running the Prepare Excel for Redact mass operation, formerly known as the Unhide Excel Content mass operation, on all Excel documents before applying markups with Redact. This preparation is done to ensure data is not lost after the markups are applied and also to prevent information that is covered by markups from being restored by third parties.

To prepare Excel documents:

1. Navigate to the **Documents** tab.
2. Select the desired Excel documents from the list.
3. Click on the mass operations menu and select the **Prepare Excel for Redact** option.
4. Click **Confirm**.
   The selected Excel documents are ready to receive markups using Redact.

29.15.2 Excel file markup considerations

Note: If a cell in a spreadsheet file contains more than 32,767 characters, applying a redaction causes the text in the cell to be truncated.

Excel files must be prepared for redaction prior to markup application. This preparation is done to ensure data is not lost after the markups are applied and also to prevent information that is covered by markups from being restored by third parties.

When you apply the first markup to an Excel file, the following will occur:

- All calculated fields are replaced with their original calculated values.
- All formulas are replaced with their calculated values.
- All pivot tables are replaced with their original calculated values.
- All change-history is removed from documents.
- All hidden and very-hidden rows, columns, and sheets are unhidden.
- All merged cells are un-merged.

29.15.3 Supported file types

To learn more about which file types are compatible with Redact, see Redact supported file types.

29.15.4 .csv file markup considerations

Since .csv files are text-based, they function differently than Excel files. A .csv file must display in table format in the Native Viewer before redaction options appear in the right-click menu. Only text or cell content redactions can be applied to .csv files.

Redact supports single and double quote characters as qualifiers.

The following delimiters are supported for .csv files, in order of highest to lowest priority:

- Comma
- Tab
- Semicolon

- Colon
- Space

If no delimiter is found, the .csv file will display in a single column. Redact provides warning messages that indicate which .csv files failed to match a delimiter to help you troubleshoot.

29.15.5 Applying markups to .csv files

Note: If you apply a markup to a cell where the text overflows into empty neighboring cells, just as in the native application, the markup does not also overflow into empty neighboring cells. However, when the document is produced and the markup is burned in, the text from the original cell no longer overflows and is completely hidden by the markup.

You can apply redactions to a single cell or multiple cells by doing the following:

1. Open the desired .csv file in the Native Viewer.
2. Select the desired markup set in the bottom-left drop-drown menu. If **None** is selected, you will not be able to apply markups.
3. Select the desired cell or click and drag your cursor to select multiple cells.
4. Right-click on the highlighted area, hover your cursor over **Relativity Redact** in the right click-menu and then hover your cursor over **Redact** again, and select the desired redaction type.
   A redaction is applied to the selected area.

29.15.6 Applying markups to Excel files

Markups can be applied to many different elements of an Excel file as needed.

29.15.6.1 Manually applying markups

Note: If you apply a markup to a cell where the text overflows into empty neighboring cells, just as in the native application, the markup does not also overflow into empty neighboring cells. However, when the document is produced and the markup is burned in, the text from the original cell no longer overflows and is completely hidden by the markup.

You can apply markups to a single cell or a series of rows or columns by doing the following:

1. Open the desired Excel file in the Native Viewer.
2. Select the desired markup set in the bottom-left drop-drown menu. If **None** is selected, you will not be able to apply markups.
3. Select either the desired cell, the desired row or column, or click and drag your cursor to select the area you wish to apply a markup to.
4. Right-click on the highlighted area, hover your cursor over **Relativity Redact** in the right-click menu, and select the desired markup option from the menu.
   A redaction or highlight is applied to the selected area.

29.15.6.2 Applying the same markup repeatedly

For your convenience, you can rapidly apply the same markup to a single cell or a series of rows or columns by doing the following:

1. Select and apply a markup to the Excel document. See Manually applying markups for more information.
2. Select the desired cell, row, or column that you wish to apply the same type of markup to.

3. Right-click and select the **Redact - name of the previously applied markup** option. During a session, the name of this option updates to display the name of the markup type that was most recently applied.
   A markup of the same type as was most recently applied is added to the currently selected cells, rows, or columns.

29.15.6.3 Cell Content redactions

You can also edit the text of a single cell on-the-fly with this markup option. When a cell content redaction is applied, background colors, patterns, and borders from the selected cell will be maintained. Additionally, the font, font size, and color of the first word in the cell will be maintained in the redaction and any other fonts, font size, or colors in additional words will not.

To edit the contents of a single cell using a cell content redaction, do the following:

1. Open the desired Excel file in the Native Viewer.
2. Select the desired markup set in the bottom-left drop-drown menu. If **None** is selected, you will not be able to apply markups.
3. Select the cell you wish to apply a redaction to.
4. Right-click on the highlighted cell and hover your cursor over **Relativity Redact** and then **Redact**, and finally, select **Cell Content**.
   The Redact Cell Text modal displays.
5. Edit the cell's text as desired to create the redaction.
6. Click **Update Cell Content**.
   The Cell Content redaction is applied to the selected cell.

29.15.6.4 Sheet Name redactions

The name of a sheet within an Excel file can be redacted if it contains sensitive information.

To redact the name of a sheet, do the following:

1. Open the desired Excel file in the Native Viewer.
2. Select the desired markup set in the bottom-left drop-drown menu. If **None** is selected, you will not be able to apply markups.
3. Click on the **Sheet Names** icon.
4. Click **Redact** in the row of the sheet name you wish to apply a redaction to.
   The Redact Current Sheet Name modal displays.
5. Edit the sheet's name as desired to create the redaction.

   Note: Due to software requirements in Excel, each sheet name redaction you enter must be unique compared to the other sheet names. Additionally, the name cannot be blank, contain the following characters: / \ ? * : [ ], and cannot begin or end with an apostrophe.

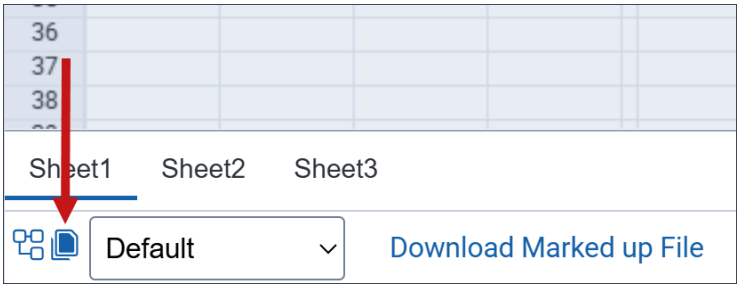
6. Click **Redact**.
   The Sheet Name redaction is applied to the sheet.

29.15.6.5 Chart redactions

Note: Due to limitations of the .xls file format, the Review Interface is unable to visually represent markups applied to either the full sheet chart or full sheet chart components. This does not impact Redact's ability to create markups for these components or the branding process. The Download Marked Up File button can be used to verify markup application.

To apply a redaction to a chart, do the following:

1. Open the desired Excel file in the Native Viewer.
2. In the bottom toolbar, click on the **Redact Spreadsheet Markup Navigator** icon to expand it.

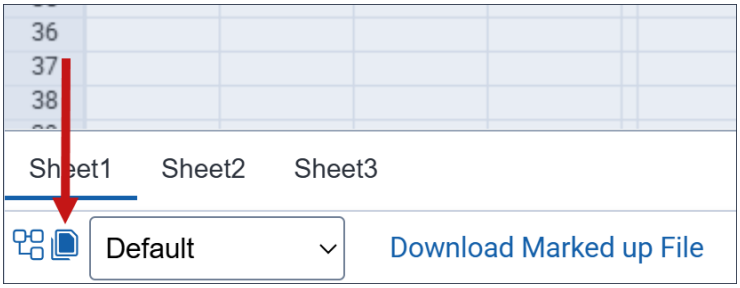


3. Click on the **Chart** icon to display a list of all the charts in the document.
4. Click the **Redact** button on the right side of the chart's row you wish to redact.
   A black box redaction is applied to the chart.
5. Optionally, to apply a redaction to either the chart title or labels, click on the name of the chart and then click on the **Redact** button on the right side of any chart contents' row you wish to redact.

29.15.6.6 Comment redactions

To apply a redaction to a comment, do the following:

1. Open the desired Excel file in the Native Viewer.
2. In the bottom toolbar, click on the **Redact Spreadsheet Markup Navigator** icon to expand it.

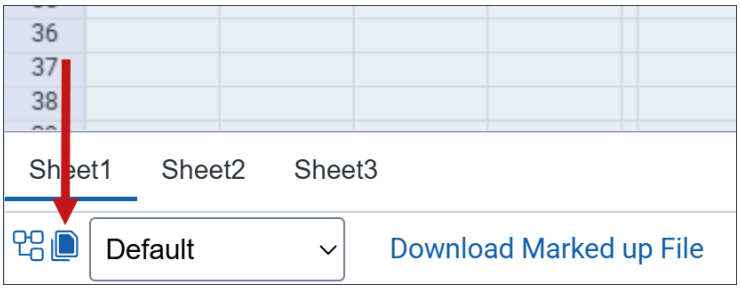


3. Click on the **Comment** icon to display a list of all the comments in the document.
4. Click on the comment you wish to redact.
   The Redact Comment modal displays.
5. Edit the comment as desired to create the text redaction.
6. Click **Save**.
   The redaction is applied to the comment.

29.15.6.7 Header and footer redactions

Headers and footers in Excel files are not visible in the Viewer. However, you can apply redactions to them by doing the following:

1. Open the desired Excel file in the Native Viewer.
2. In the bottom toolbar, click on the **Redact Spreadsheet Markup Navigator** icon to expand it.



3. Click on the **Headers** icon to display a list of headers in the document.
4. Optionally, you can navigate to the header or footer you wish to redact by clicking the drop-down menu and selecting the desired option or clicking the Next or Prev links in the card.
5. Click on the header or footer you wish to redact.
   The Redact Header/Footer modal displays.
6. Edit the header or footer as desired to create the redaction.
7. Click **Save**.
   The redaction is applied to the header or footer.

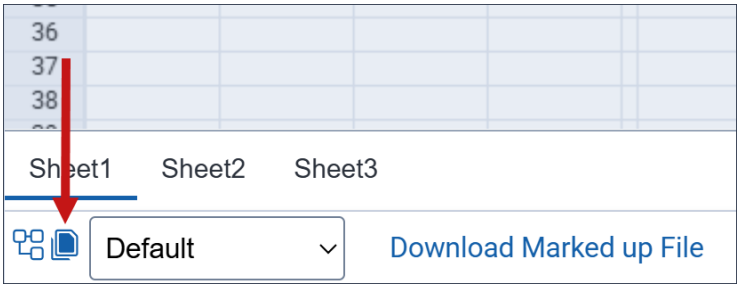
29.15.6.8 Object redactions

Excel files may contain a variety of objects including:

- WordArt
- SmartArt
- Embedded documents (email, PowerPoint), images, equations, text boxes, and shapes

You can apply a black redaction to these objects, by doing the following:

1. Open the desired Excel file in the Native Viewer.
2. In the bottom toolbar, click on the **Redact Spreadsheet Markup Navigator** icon to expand it.



3. Click on the **Objects** icon to display a list of objects in the document.
4. Click the **Redact** button on the right side of the object's row you wish to redact.
   A black redaction is applied to the object you selected.

29.15.7 Convert Spreadsheets Markup

If markups have been applied to one or more documents, you can change all of the redactions to highlights or vice versa using the Convert Spreadsheets Markup mass operation. To learn more visit, Convert Spreadsheets Markup.

29.15.8 Inverting markups

You can either select an entire markup or portions of a markup to remove it and restore the data that was hidden underneath the markup. Inverted markups only removes markups from the selected areas, it does not apply any markups to other portions of a document. Inverting markups also excludes areas of the document from branding. The ability to invert markups replaces the revert markups feature.

Inversions are recorded in the Redact Spreadsheet Markup Navigator as having the **Inverse** value for the Markup Type field. This makes inverted markups easy to find within a document. Alternatively, you can also apply inverted markups automatically using a Redact project.

To apply an inverted markup:

1. Open the desired spreadsheet file in the Native Viewer.
2. Select either the desired cell, the desired row or column, or click and drag your cursor to select the area with a markup that you would like to redact. Only cells that have markups will be inverted and cells without markups will be unaffected by this process.
3. Right-click on the highlighted area and hover your cursor over **Redact** in the right-click menu and select **Invert Selection**.
   The selected markups, whether applied manually or by a Redact project, are removed from the document.
4. Optionally, you can review inverted markups in the Redact Spreadsheet Markup Navigator. You can also remove an inverted markup to restore the previous markup by clicking the **Reject** icon in the Accept/Reject column.

29.15.9 Excel document keyboard shortcuts

The following options are available to help you conveniently navigate Excel documents using your keyboard:

Keyboard Shortcut	Action
Page up / Page down	Scroll up or down one screen length in the document.
CTRL+End	Select the bottom-right cell and move it into view.
CTRL+SHIFT+End	Extend the current selection of cells to the bottom-right cell.
CTRL+Home	Select the top-left cell and move it into view.
CTRL+SHIFT+Home	Extend the current selection of cells to the top-left cell.
Arrow left / up / right / down	Move the current selection left / up / right / down by one cell.
CTRL+Arrow left / up / right / down	Move the current selection left / up / right / down by one cell.
CTRL+SHIFT+Arrow left / up / right / down	Extend the current selection left / up / right / down.
Tab	Move the current selection to the right by one cell.
Shift+Tab	Move the current selection to the left by one cell.
CTRL+A	Select the entire spreadsheet.
CTRL+Shift+Space	Select the entire spreadsheet.

Keyboard Shortcut	Action
CTRL+Space	Extend the current selection to include the full columns.
Shift+Space	Extend the current selection to include the foll rows.

29.15.10 Reviewing markups

After markups have been placed, perform quality control on documents before they are produced. To learn more about how to do this using Redact, visit Reviewing markups to ensure accuracy.

29.15.11 Reviewing the original native document

When a spreadsheet document is prepared by Redact, there are changes made to the native file to facilitate markup application. The changes include unhiding hidden columns, rows, and sheets. By the end of the preparation process, the original document is backed up to an RDO and the native is replaced with the flattened document.

If you would like to validate what content was previously hidden in a spreadsheet file, you can use the Open Original Native button to compare the document both before and after Redact preparation.

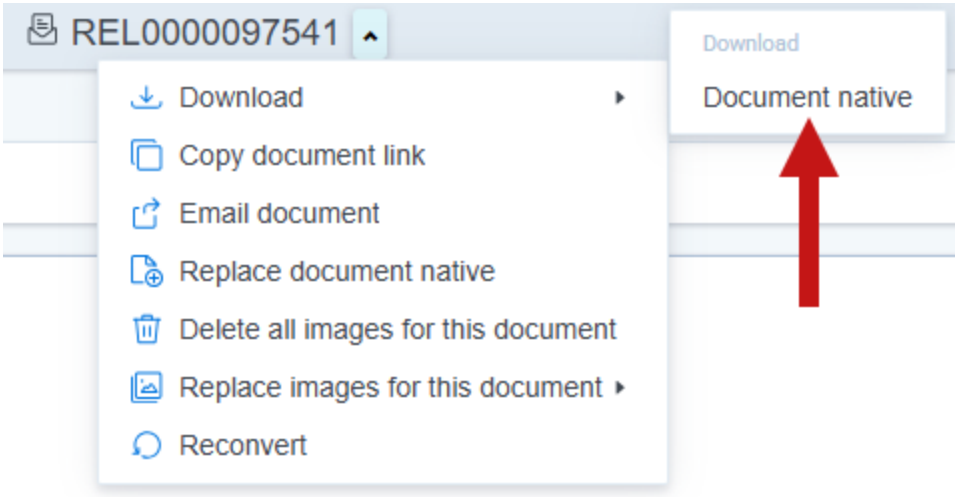
To access the original native file directly from the Viewer:

1. Navigate to the **Documents** tab and select a spreadsheet document from the list that has already been prepared for Redact.
2. Click on the **Open Original Native** button.
   A new browser window opens where you can click **Native** to view the native spreadsheet document or click **Original Native Text** to see the document before it was prepared for Redact.

29.15.12 Downloading and exporting marked up documents

You can download or export documents in the following ways:

- To download a copy of the native file without any markups, click on the document actions menu in the Viewer, hover your cursor over the **Download** option, and then select **Document native**.



- To download a copy of a native spreadsheet file with the markups applied in the Native Viewer, click on the **Download Marked Up File** button.
- To export multiple documents that have markups applied, run a production that includes these documents and then export the production set using Import/Export.

29.16 Manual markups with PDF files

Redact allows you to apply markups to PDF files in the Viewer. An audit of the markups applied to each document can be viewed at any time to make tracking markups easy. You can also quickly locate any markups in a document and approve or reject them as part of your quality control process by using the Redaction Navigation card. Additionally, the Original Text field in the Redaction Navigation card is now supported with PDF documents so that you can see what text each markup covers.

Note: Placing a markup on a document causes the coding layout to refresh. If you are editing a layout and place a markup, any unsaved edits to the layout fields will be lost. We recommend editing the fields on a layout and saving your changes before applying manual markups to a document.

If you would prefer to have markups applied automatically, see Automated PDF markup project.

29.16.1 PDF markup considerations

You can see a preview of what markups will look like on a PDF file by using the Download Marked Up File button in the toolbar at the bottom of the Viewer.

29.16.2 Supported file types

To learn more about which file types are compatible with Redact, see Redact supported file types.

29.16.3 PDF basic redactions

To apply a black, text, or white redaction to a PDF, do the following:

1. Select the desired markup set in the bottom-left drop-drown menu. If **None** is selected, you will not be able to apply markups.
2. Click the **Redaction Mode** icon. The black redaction tool is the default. Click the drop-down menu to select a different tool. You can select from the following:
    - **Black** - creates a solid black box, like using a black marker. While you draw the box, a gray translucent fill appears.
    - **Text** - creates a white redaction box with black text. The text will fill the box by default. You can right-click a text box redaction and select **Edit** to change the text redaction as desired. Alternatively, you can right-click a text box redaction and select either most recent word or phrase you entered while editing a redaction or if you have never edited or created a text redaction before, you can select **Redacted** instead. The system admin determines which text options are available.
    - **White** - creates a solid white box with a gray border. The gray border won't be printed or produced.
3. Draw the redaction boxes across the sections of the page you want to redact. You can draw in any direction. The redaction is applied to the PDF file.

29.16.4 PDF highlights

To apply an highlight to a PDF, do the following:

1. Select the desired markup set in the bottom-left drop-drown menu. If **None** is selected, you will not be able to apply markups.
2. Click the **Highlight Mode** icon and select a color from the drop-down menu. Blue is the default color.
3. Draw the highlight across the sections of text you want to highlight.
   The highlight is applied to the PDF file.

29.16.5 Rejecting highlights or markups

To reject a markup or highlight so that it isn't included in production, do the following:

1. You can use either of the following methods to select highlights or markups:
    - Hold down on **Ctrl** on your keyboard, and left-click on each highlight or markup you wish to reject.
    - Right-click on a markup after selecting any other highlight or markup you would like to reject.
2. Do either of the following to reject the selected markups:
    - If you right-clicked on a markup, select **Reject** from the right-click menu.
      The selected markups are rejected.
    - Otherwise, press the **Delete** key on your keyboard and click **Reject** in the modal.
      The selected markups are rejected.

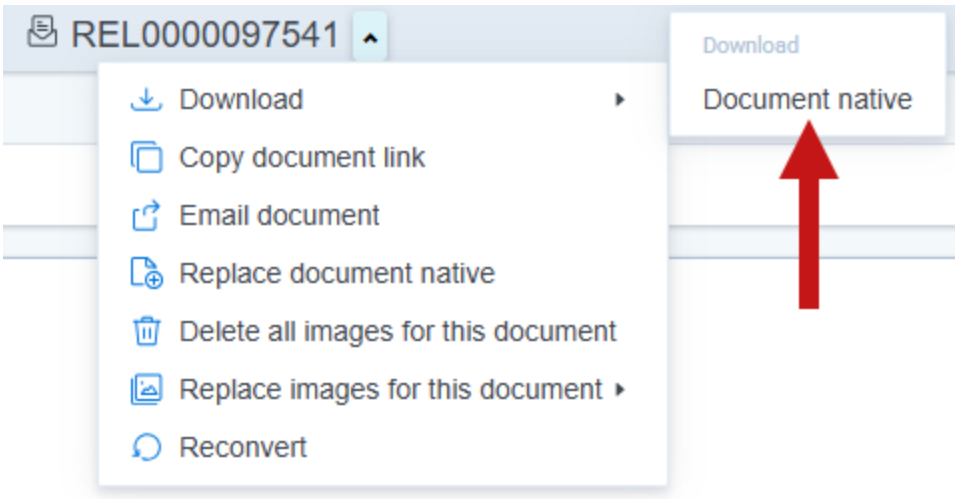
29.16.6 Reviewing markups

After markups have been placed, it is a best practice to perform quality control on documents before they are produced. To learn more about how to do this using Redact, visit Reviewing markups to ensure accuracy.

29.16.7 Downloading and exporting marked up documents

You can download or export documents in the following ways:

- To download a copy of the native file without any markups, click on the document actions menu in the Viewer, hover your cursor over the **Download** option, and then select **Document native**.



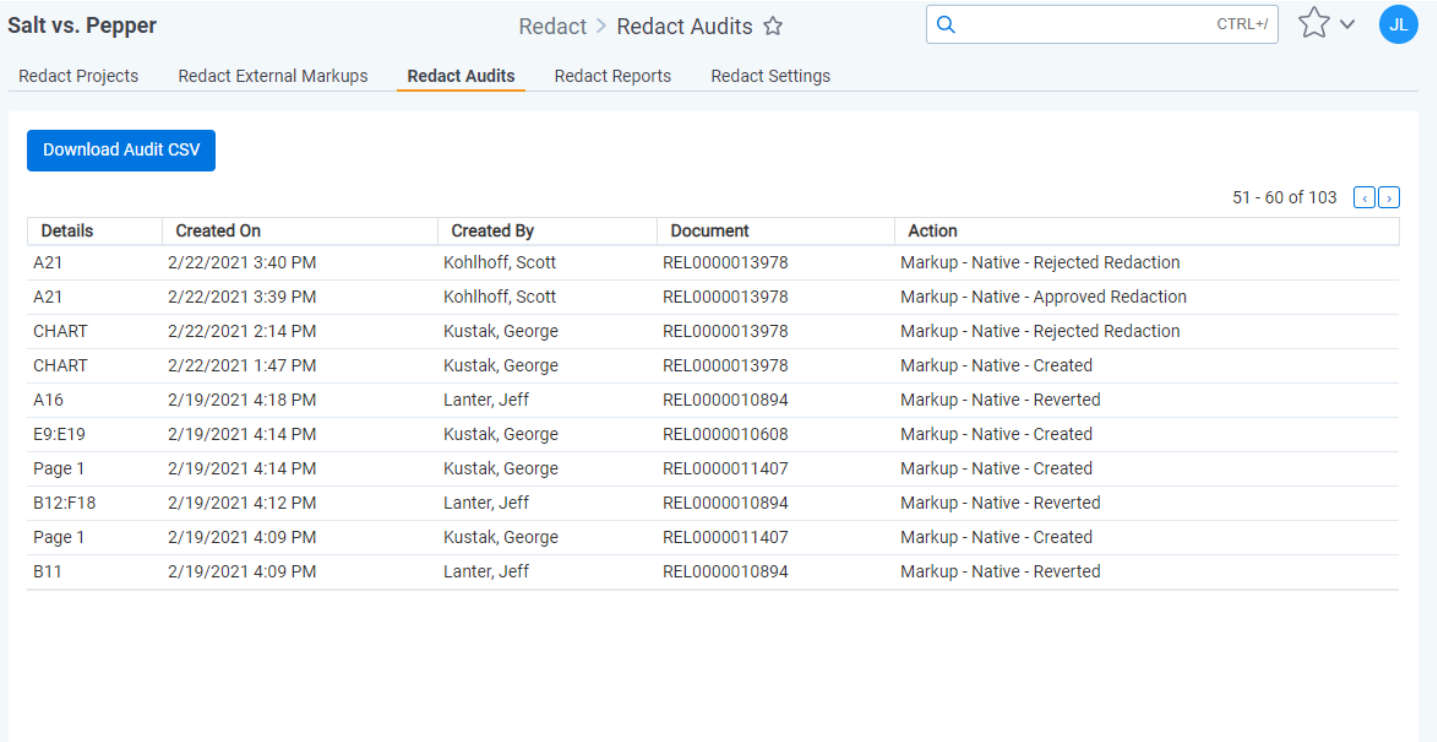
- To download a copy of a native PDF file with the markups applied in the Native Viewer, click on the **Download Marked Up File** button.
- To export multiple documents that have markups applied, run a production that includes these documents and then export the production set using Import/Export.

29.17 Redact Audits

As users interact with markups in Redact, an audit of each action is maintained. You can use this audit to track who applied markups, reverted them, and/or who approved/rejected each markup.

The ten most recent markup actions display in the Redact Audits tab. You can view additional markup actions by clicking the left or right icons in the upper-right.

To download a .csv file that contains information on all markup actions to your workstation, click **Download Audit CSV**.



Details	Created On	Created By	Document	Action
A21	2/22/2021 3:40 PM	Kohlhoff, Scott	REL0000013978	Markup - Native - Rejected Redaction
A21	2/22/2021 3:39 PM	Kohlhoff, Scott	REL0000013978	Markup - Native - Approved Redaction
CHART	2/22/2021 2:14 PM	Kustak, George	REL0000013978	Markup - Native - Rejected Redaction
CHART	2/22/2021 1:47 PM	Kustak, George	REL0000013978	Markup - Native - Created
A16	2/19/2021 4:18 PM	Lanter, Jeff	REL0000010894	Markup - Native - Reverted
E9:E19	2/19/2021 4:14 PM	Kustak, George	REL0000010608	Markup - Native - Created
Page 1	2/19/2021 4:14 PM	Kustak, George	REL0000011407	Markup - Native - Created
B12:F18	2/19/2021 4:12 PM	Lanter, Jeff	REL0000010894	Markup - Native - Reverted
Page 1	2/19/2021 4:09 PM	Kustak, George	REL0000011407	Markup - Native - Created
B11	2/19/2021 4:09 PM	Lanter, Jeff	REL0000010894	Markup - Native - Reverted

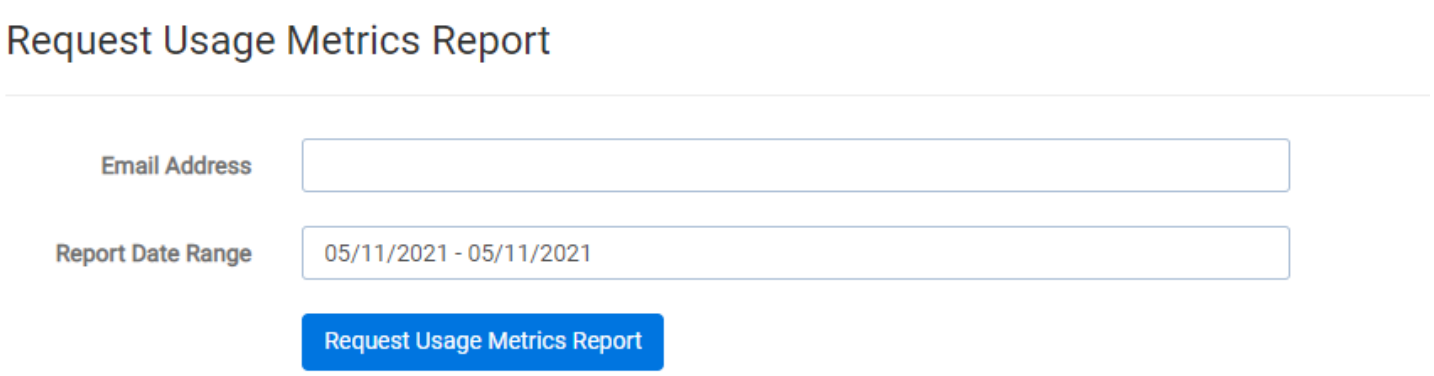
The following columns display in the Redact Audits tab:

Name	Description
Details	Displays the location (page number for PDF files or cell name for spreadsheet files) of the markup that was created, reverted, or accepted/rejected. If the markup was applied to a chart, CHART displays instead of the location.
Created On	Displays the date and time that the action took place.
Created By	Displays the name of the user who took the action.
Document	Displays the name of the document where the action took place.
Action	Displays the type of action taken by the user.

29.18 Redact Client Usage Report

Redact offers the Client Usage Report to help you track data and billing information.

You can generate a usage report to help you track how much you have used Redact for billing and/or data tracking purposes. A usage report can be generated for a specific date range and it provides detailed usage statistics for each workspace.



To generate a Redact Client Usage Report, do the following:

1. Navigate to the **Redact Client Usage Report** tab.
2. Enter the **Email Address** where you would like to receive the usage report.
3. Click on the **Report Date Range** field and select or enter the desired range.
4. Click **Request Usage Metrics Report**.
   After a short time, the email address you entered will receive an email with a CSV file attachment containing the report.

Note: The placed markups in each report are calculated by taking the total number of markups placed within the selected date range and subtracting the number of markups were both created and reverted within that date range.

29.19 Redact External Markups

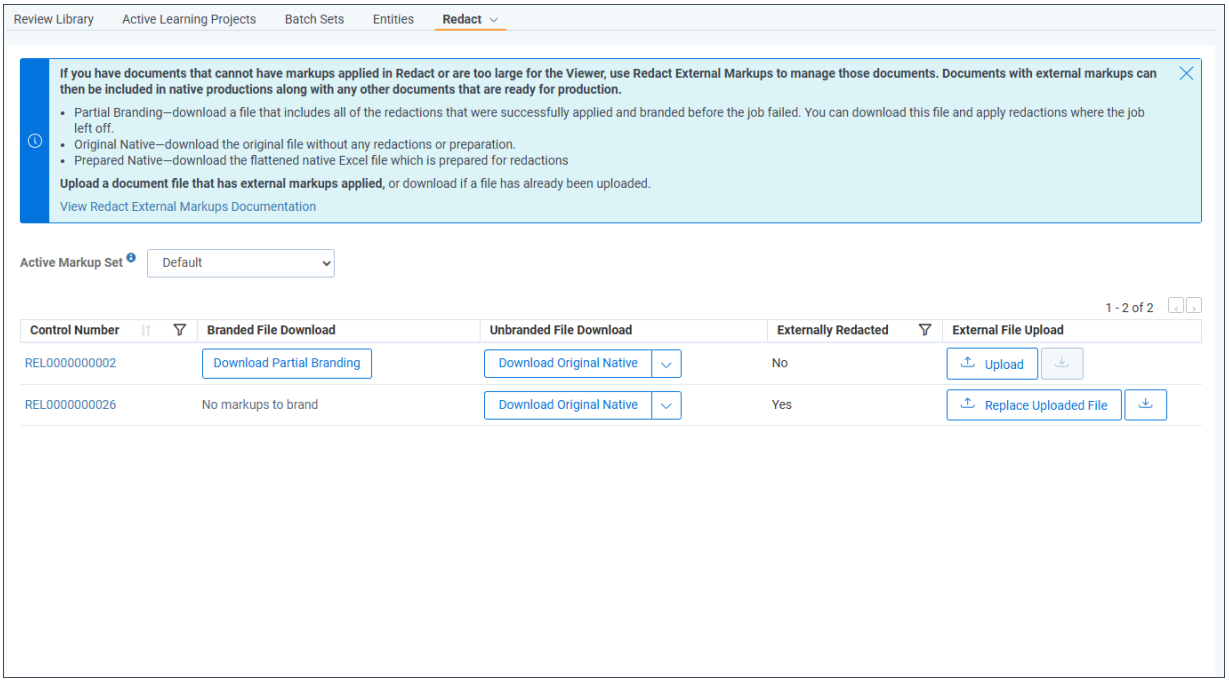
Some documents cannot receive markups using Redact and if you open a document like this in the Viewer, a notification displays. For documents that cannot have markups applied in Redact or are too large for the Viewer, we recommend using Redact External Markups.

External Markups only supports native files. Stored PDFs are not compatible with this feature.

After adding documents to the External Markups tab by selecting the Redact Document Warnings field, you can download each document, apply markups externally, and then re-upload them. Documents with external markups can then be included in native productions along with any other documents that are ready for production.

Uploaded documents with external markups must maintain the same file type extension or you may experience an error.

Note: We do not recommend applying external markups to a document unless it will only receive external markups. If a document has external markups, it can no longer receive any other kinds of markups in Relativity to prevent production errors.



29.19.1 Example workflow

This workflow illustrates how External Markups can prevent reviewers from being disrupted while performing manual redactions using Redact in the Viewer.

1. The case team identifies a set of PDF and spreadsheet files that are too big to display in the Viewer.
2. A saved search that includes only these large document files is created.
3. Add the documents to the Redact External Markup tab by checking the **Redact Document Warnings** and **Cannot be Redacted in Native Viewer** field options. To learn more, see Adding documents to External Markups tab.
4. Reviewers are granted access to the Redact External Markups tab.
5. Reviewers select the markup set that they used to apply any redactions to the documents.
6. Reviewers download documents to apply markups to externally.
7. Markups are placed using your tool of choice such as Microsoft Excel or Adobe Acrobat. If you are applying markups using Excel, please note that applying a Fill Color over data does not safely redact that information. Instead, any data in the cells you wish to redact should be removed:
    a. Click on the cell you wish to redact.
    b. Press **Delete** on your keyboard.
    c. Right-click the cell and select **Fill Color** with Black selected.
8. The documents with external markups are re-uploaded to Relativity and ready for production.

29.19.2 File size considerations

To ensure high performance, there is a 4 GB file size limit for native files. Any native files that are 4 GB or above will not receive markups using Redact.

29.19.3 Adding documents to External Markups tab

Once you have identified documents that need to have markups applied externally and placed them in a saved search, do the following to add the documents to the External Markups tab:

1. Either edit an existing layout or create a new one and ensure that the layout includes the **Redact Document Warnings** field.
2. Navigate to the **Documents** tab and open the saved search that contains the documents that you wish to apply external markups to.
3. Select the documents you wish to add to the External Markups tab.
4. Select Edit in the mass operations toolbar.
   The Edit X Document Item(s) pop-up displays.
5. Select the layout that contains the Redact Document Warnings field that you created for step 1 from the drop-down menu in the upper-right.
6. Select **Redact Document Warnings** and then select **Cannot be Redacted in Native Viewer**.
7. Click **Save**.
   The selected documents are added to the External Markups tab.

29.19.4 Recommended uses of External Markups

The following are examples of situations where we recommend using External Markups instead of the normal Redact workflow:

File Type	Description
PDF	If a PDF file contains corrupted content, the PDF will not properly brand unless External Markups is used.
PDF	Large PDF files that are 1 GB or larger will potentially not brand correctly without using External Markups.
Spreadsheet	Macros in spreadsheet files can cause issues with burning in markups unless External Markups is used.
Spreadsheet	Documents containing an individual table of 7,500,000 cells or more are not supported for performance reasons. We recommend using External Markups to ensure markups are applied correctly.
Spreadsheet	A large spreadsheet that is either 4 GB or larger or it contains 1,000 columns or more can cause errors when applying markups. Files of this size typically experience reduced performance as well.
Spreadsheet	Redacting entire rows or columns may lead to different behavior in the Viewer versus you download to your workstation. It is expected that the redacted row will only display where there is text in the Viewer, but when you download the file, you will see text in each cell spanning the entire row or column. Before preparing documents for production, consider whether this behavior suits your needs and if not, you can use External Markups.
Spreadsheet	If columns are hidden in the original, spreadsheet document, there might be formatting issues during production. We recommend QC'ing spreadsheets with hidden content before production and if there are formatting issues, using External Markups instead.

29.19.5 External Markups tab columns

The following columns display in the External Markups tab:

Column Name	Description
Control Number	Displays the control number for each document. Click on the control number to open the document in the Native Viewer.
Branded File Download	Displays either the Download Partial Branding button or No markups to brand. Click on the **Download Partial Branding** button to download a file that includes all of the redactions that were successfully applied and branded before the job failed. You can download this file and apply redactions where the job left off.
Unbranded File Download	The drop-down menu may contain one or both of the following options: Download Original Native or Download Prepared Native. • **Download Original Native**—Click on the drop-down menu and select this option to download the original file without any redactions or preparation. • **Download Prepared Native**—Click on the drop-down menu and select this option to download the flattened native file which is prepared for redactions.
Externally Redacted	Displays Yes if the document has already had external markups applied or No if none have been applied.
External File Upload	Displays either the Upload button or the Replace Uploaded File button. A download button is also available if an external file was previously uploaded. • **Upload**—Click to select a document file that you wish to upload to Relativity and apply external markups to. • **Replace Uploaded File**—Click to select a document file that has external markups applied and upload it to replace the current file. • **Download**—Click to download a copy of the document that has external markups already applied.

29.20 Redact Language Support

While Redact only supports English when it is initially installed, it can support over 100 languages. If you are interested in having non-English languages added to Redact, please contact Relativity Support.

Language packs can be included in an image project either individually or mixed together to cover multiple languages. In some cases you may find that the results are more accurate if you use a single language pack even if there are words in English in the documents. Since results can vary, we recommend testing non-English language support on a set of documents before doing a full project run.

29.20.1 Language settings in Relativity

Documents should be loaded into Relativity with the proper language settings. This is an important component of interacting with images for non-English languages and a critical requirement for non-Romance languages.

For example, if documents with Japanese text are being run using Redact, they will need to be loaded from a processing engine that supports processing Japanese documents with the appropriate language settings.

If using Relativity Processing, select the Japanese language in either the processing set or processing profile. This ensures that the extracted text is encoded correctly and can be used for comparison when determining how much quality control is needed.

29.20.2 Entering Language Codes in an image markup project

If non-English languages have been enabled, please note the following:

- By default, projects will run with the eng code which causes English to be the only supported language.
- If there is a chance that multiple languages could be combined together in the documents, you can ensure the languages receive the appropriate markups by adding a + between each language code. For example, entering **spa+eng** causes Spanish and English to receive markups by a project.
- Language codes are prioritized from left to right so the left-most code will be given the highest priority.
- The Redact application only supports three character length for supported language codes. For example, if a user entered **chi_sim_vert** as the language code for the trained data file **chi_sim_vert.traineddata** in an image project, the project fails.
  Instead, you should rename the trained data file to three characters like csv before uploading it to Relativity in order to successfully use that trained data file.

29.21 Redact project best practices

Duplicate markups can slow down your review workflow, inflate markup counts, and cause unexpected behavior during production. You can use the following tips to prevent duplicate markups and ensure that your Redact projects run smoothly.

29.21.1 Use the minimum number of projects

The fewer projects you have running against the same documents and markup set, the lower the risk of duplicates. Before creating a new project, ask whether you can instead update the rules on an existing project. In most cases it can.

29.21.2 Revert before experimenting with a new project

Creating and running too many projects is a common cause of duplicate markups. Instead of creating a new project that is potentially similar to others to try out a different rule configuration, revert the existing project. This clears the markups from the old project so that they do not accumulate alongside the results from the new one.

29.21.3 Update rules in an existing project rather than creating a new one

If you run a project and are not happy with the results, edit the rules, revert the project to clear any previously applied markups, and then rerun the project to test the edited rules. We recommend this workflow because it ensures that no markups from the initial project run are left on the documents and so you can see exactly how the edited rules work.

Creating a new project for every rule change and running it alongside the old projects accumulates markups from multiple projects on the same documents. Over time this leads to duplicate markups that are difficult to untangle.

29.21.4 Maintain one data source per project

To prevent duplicate markups, we recommend using one unique saved search per project and avoid using either the same or similar rules across projects, particularly with the same markup set. If documents appear in multiple projects with overlapping rules and the same markup set, duplicate markups are almost certain once you run the projects.

For example, the following setup is recommended because there are no shared documents, there is a low chance of duplicate markups:

- Project A - Saved Search A - Markup Set 1
- Project B - Saved Search B which has no documents shared with Saved Search A - Markup Set 1

The following setup is not recommended because the overlap between documents and rules in Project A and Project B in this example has a much higher chance of causing duplicate markups when both projects are run:

- Project A - Saved Search which includes documents 1-500 - Markup Set 1 - PII rules
- Project B - Saved Search which includes documents 400-800 - Markup Set 1 - same PII rules

29.21.5 Use separate markup sets if multiple projects must cover the same documents with the same rules

If your workflow requires multiple projects to process the same documents with similar or the same rules, we recommend assigning each one of these projects its own unique markup set. This makes it easy to track the markups that are applied by the different projects.

29.21.6 Other overlapping scenarios

You can run projects that use unique rules, even if they share documents and the same markup set because the markups will be applied to different content and in different locations within the documents.

If you have projects that use unique rules- for example, one project for PII and another for privilege terms - they can safely share both the same documents and the same markup set, since their markups will cover different content and locations.

For example, the following setup has different rules but the same markup set and because the rules are unique, there is little concern over duplicate markups:

- Project A - PII rules - All Redactions markup set
- Project B - Privileged terms rules - All Redactions markup set

The following setup is not recommended because it uses the same rules and the same documents which is likely to cause duplicate markups:

- Project A - PII rules - first batch documents - PII Redactions - Batch 1 markup set
- Project B - PII rules - second batch documents which contains the same ones as first batch - PII Redactions - Batch 2 markup set

29.21.7 Audit your projects before running

Before running a project that contains a lot of documents, verify that:

- No two active projects share the same documents, the same markup set, and the same or similar rules.
- Projects that were used for testing or earlier rule iterations have been archived or deactivated so that none of their markups persist.
- Any previously applied markups from deprecated projects have been removed.

29.22 Redact Project Status

The Redact Project Status tab lets you view all of the projects in an instance to track their status. This is useful when there are multiple projects queued across an instance and you want to see when a particular project might begin. Additionally, you can change the priority of projects that have been queued and have not been completed yet from this tab. This allows you to prioritize key Redact projects when several have been queued. Only users who have the system admin permission can access this tab.

To view the status of every project in an instance, do the following:

1. Navigate to the **Redact Project Status** tab.Projects are sorted from newest to oldest based upon when they were created.

   Note: Projects are sorted from newest to oldest based upon when they were created.

2. Optionally, apply filters to the Project Type, Name, and/or Current Status column to determine what project information displays.
3. Optionally, you can click on the name of a workspace to navigate there and edit a project as needed.

29.22.1 Redact queue priority

Redact projects in the Default queue are ordered based on when a run begins. If one or more project is added to the Priority queue, it will take precedence over any projects in the Default queue. To learn more about adding a project to the Priority queue, see Redact project Priority queue below. Stopping a project will pause it until it is restarted. Pausing a project will cause the next queued project to begin. Once a project is restarted, it is moved to the bottom of its respective queue.

29.22.2 Redact project Priority queue

If there is more than Redact project queued, you can assign priority to one or more of those projects so that they will be completed sooner than the projects in the Default queue. If multiple projects are in the priority queue at any given time, those projects will be prioritized based on their start time. For example, if two projects are in the Priority queue, the project that was started first will be run first and the project that was started second will be run second.

To add one or more Redact projects to the Priority queue, do the following:

1. Navigate to the **Redact Project Status** tab.
2. Select each queued projects that you would like to add to the Priority queue.
3. Click on the **Change Queue** button in the bottom-left.
4. Ensure **Priority queue** is selected and then click **Change**.
   The selected Redact projects are added to the Priority queue and will begin running before projects in the Default queue.

29.22.3 Removing a project from the Priority queue

If a Redact project has been added to the Priority queue and you no longer want it to have priority status, you can move it back to the Default queue. To accomplish this task, do the following:

1. Navigate to the **Redact Project Status** tab.
2. Select each queued projects that is in the Priority queue that you wish to move to the Default queue.
3. Click on the **Change Queue** button in the bottom-left.
4. Select **Default queue** and then click **Change**.
   The selected Redact projects are moved to the Default queue and the next project in the Priority queue will begin immediately. If there are no projects in the Priority queue, the project with the earliest start time in the Default queue will begin running.

29.23 Redact Reports

Redact Reports allow you to create a custom report that contains markup and/or document field information for all of the documents in a saved search. A Markup Report contains a row for each markup applied to documents in the

selected saved search. A Document Report contains a single row for each document in the saved search so you can efficiently view document field information. The user that generates the report receives a .csv copy via email.

Note: Audits for image redactions are moved from SQL to data grid after ten days. Once this occurs, those audits no longer provide as much information in Redact Reports and instead, display the following message: "Audit is in data grid and can not be read."

29.23.1 Available report fields

Redact can report on any field that is currently associated with the document object, Redact specific fields, and fields from the Viewer redaction table. This flexibility allows the creation of many different types of reports.

Note: Avoid using long text fields for Redact reports because they may result in a malfunctioning .csv file.

After choosing the fields for the report, they can re-ordered. The first field selected will be the left-most column in the report, while the bottom will be the right-most column.

29.23.2 Generate a Markup or Document Report

To generate a Markup or Document Report and receive it via email, do the following:

1. Navigate to the **Redact Reports** tab.
2. Click the **Markup Report** button to create a report that contains a row for each markup in the included documents or click **Document Report** button to create a report that contains a single row of information for each included document.
3. From the **Saved search** drop-down menu, select a saved search that contains the documents you wish to generate a report about. Optionally, you can enter a term or terms into search box at the top of the menu to help narrow results and find the desired saved search.
4. Select the desired fields you wish to be included in the report in the Available Report Fields section and click on the right arrow icon to add them to the Fields Included in Report section.

   Note: Regardless of which report you select, markup and document fields are available to be added to the report. The selected fields may display differently depending on which report you select.

5. Once all of the desired fields have been added to the Fields Included in Report section, click **Generate Report**. The user that generated the report receives a copy via email. A Markup Report will have the following naming convention: RedactionLog_<WorkspaceArtifactID>_<YYYY-MM-DD> and a Document Report will have the following naming convention: DocumentLog_<WorkspaceArtifactID>_<YYYY-MM-DD>.

29.23.3 Redact specific fields

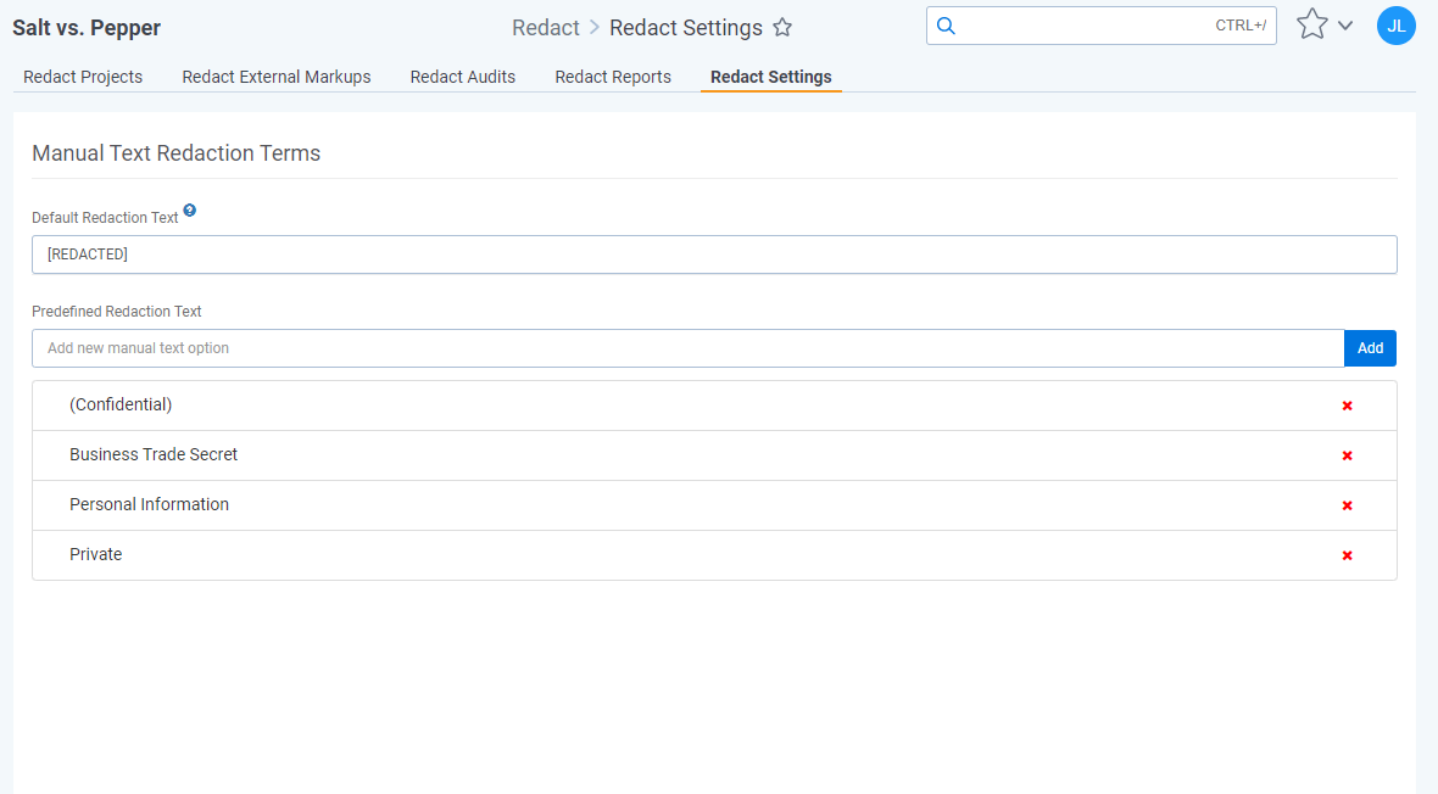
The following fields in the table below are populated by Redact or the Viewer Redaction table. In some cases, the data may be collected from both Redact and the Viewer Redaction table simultaneously such as Markup Scope which can be provided by Redact for spreadsheet redactions, but the Viewer redaction table for image redactions.

Field	Description	Additional Results
Markup Approved	Displays TRUE if the markup has been approved in the Redact Navigator card.	
Markup Location	Displays the cell name where the markup is located in a spreadsheet document.	
Markup	The type of redaction placed.	Redaction or highlight

Field	Description	Additional Results
Type		
Markup Scope	The markup scope selected when placing the markup. This value is provided for both Redact and Viewer created markups.	• Images: Word / Line / Paragraph / Page / Document / • Native Spread-sheet: Cell / Sheet / Row / Column
Markup SubType	The markup subtype selected when placing the markup. This value is provided for both Redact and Viewer created markups.	• Redaction: Black / Text / White / Cross / Inverse • Highlights: Yellow / Green / Blue / Orange / Pink / Purple
Markup Text	The text entered when placing a redaction. This value is provided for both Redact and Viewer created text redactions.	
Markup Set	The markup set that a redaction is associated with. This value is provided for both Redact and Viewer created redactions.	
Markup Reason	The reason that was specified when creating the Redact rule groups. This field is exclusive to Redact.	
Markup Page Num-ber	The page number where the markup is placed.	
Markup Cell	The cell location where a native spreadsheet markup is placed.	
Markup Sheet	The spreadsheet file that was redacted during an automated spreadsheet job.	
Markup Automated	Displays if the markup was created by a Redact automated project or not. This field can display both True and False when generating the privilege log report type.	
Markup Created By	Displays the user who created the markup. If the markup was the result of a Redact project, it will display the user who executed the job.	
Markup Timestamp	Displays the date and time when a markup was applied.	
Original Text	Displays the text that is obscured by each markup. If the text is longer than the character limit, an abbreviated version of the word(s) will display in the report.	
Project Name	Displays the name of the Redact project that applied each markup.	
Rule Name	Displays the name of the rule that resulted in the match and caused a markup to be applied by the Redact project.	

29.24 Redact Settings

The Redact Settings tab lets you determine what text displays in the text redaction options when you access the right-click menu in a spreadsheet document.



The Default Redaction Text field can be edited to determine the contents of the text redaction that is applied when the Custom Redaction Text option is selected from the right-click menu.

Additionally, you can create convenient text redaction options by entering them in the **Predefined Redaction Text** field and clicking **Add**. These options will be displayed in the Text Redaction modal when the Text option is selected in the right-click menu.

If it is no longer needed, a Predefined Redaction Text option can be removed by clicking the red X in that option's row.

29.25 PDF annotation and attachment markups

Markups can be applied to PDF annotations and attachments. The different types of annotations and attachments are described below as well as how to apply markups to them.

29.25.1 PDF annotation redactions

Annotations are commonly used in PDFs and with Redact you can apply markups to any annotations you desire. There are two different kinds of annotations used in PDF files including annotations that are used to mark up the PDF file and annotations that consist of interactive forms or multimedia. To learn more about the different annotations, see PDF annotation types below.

29.25.1.1 PDF annotation types

There are two types of PDF annotations: markups and non-markup annotations.

Markup annotations

There are three types of markup annotations:

- Free text annotations which placed on text in a PDF file.
- Pop-up associated annotations include Text, Line, Square, Circle, Highlight, Underline, Strikeout, RubberStamp, Caret, Ink, and File Attachments.
    - Text Markup annotations are a subtype of pop-up associated annotations and contain one or more words in a document upon which the pop-up is associated with. They also include markup annotations such as Underline, Strikeout, Caret, Squiggly, etc.
- Sounds annotations do not have a pop-up window but may have associated text specified by the Contents entry.

Non-markup annotations

Pop-up annotations typically do not appear by themselves and have a parent property which is associated to a markup annotation.

If no parent association is defined for a pop-up annotation, the Viewer may use the pop-up annotation's content as the text for the annotation.

29.25.1.2 Applying redactions to PDF annotations

If you apply a redaction to a PDF annotation, once they are produced the entire annotation will be removed and not redacted.

To apply a redaction to a PDF file with annotations do the following:

1. Select the desired markup set in the bottom-left drop-drown menu. If **None** is selected, you will not be able to apply markups.
2. Click the Redaction Mode icon. The black redaction tool is the default. Click the drop-down menu to select a different tool.
3. Draw the redaction boxes across the annotation you want to redact. You can draw in any direction.

    Note: You cannot redact part of an annotation. If a redaction is applied to an annotation, the entire annotation will be redacted.

    The redaction is applied to the PDF file.

29.25.2 Redacting PDF attachments

PDF files that contain embedded files can also be redacted with Redact. Embedded files often contain multimedia content but they can also be a means of retaining an external file reference when the PDF file is archived or transmitted. PDF attachments can be manually redacted in the Redact Navigation card. Alternatively, if you would like PDF files to be redacted through automation, see Automated PDF markup project.

29.25.2.1 Applying markups to PDF attachments

To apply a markup to a PDF file with attachments do the following:

1. Select the desired markup set in the bottom-left drop-drown menu. If **None** is selected, you will not be able to apply markups.
2. Click the Redaction Mode icon. The black redaction tool is the default. Click the drop-down menu to select a different tool. You can select from the following:
    - **Black** - creates a solid black box, like using a black marker. While you draw the box, a gray translucent fill appears.
    - **Text** - creates a white redaction box with black text. The text will fill the box by default. To change the font size, keep the redaction box selected and click the Font Size drop-down menu, and then select a new font size from the drop-down menu. You can right-click a text box redaction and select **Edit** to change the

text redaction as desired. Alternatively, you can right-click a text box redaction and select either most recent word or phrase you entered while editing a redaction or if you have never edited or created a text redaction before, you can select **Redacted** instead. The system admin determines which text options are available.

- **White** - creates a solid white box with a gray border. The gray border won't be printed or produced.

3. Draw the redaction boxes across the annotation you want to redact. You can draw in any direction.

Note: Attachments that are redacted will be removed completely from the document. If you would like to view the file with the attachment removed, click on the **Download Marked Up File** button or run a production that includes the PDF document.

The redaction is applied to the PDF file.

29.26 Regular expression examples

Regular expressions can be used to help locate sensitive information including contact information, credit card numbers, and personal identification numbers. Examples of regular expressions that can be used to create rules are provided below.

Note: The provided examples are meant to be a starting point for your Redact projects. They are not guaranteed to find and apply markups to every piece of sensitive information. We recommend double-checking documents before production to ensure that all sensitive information is properly redacted.

29.26.1 Before you begin

29.26.1.1 Image markup considerations

If you are using regular expressions for an automated image markup project, results may be improved by being defensive against common OCR mistakes. Each instance of any digit match can be replaced with a character replacement pattern that will evaluate numbers as common alphanumeric characters.

To do so replace the \d pattern with [\dOIlZEASB]. This type of defensive matching is not typically needed for spreadsheets.

29.26.1.2 Named groups

To specify that only part of a regular expression match should be redacted, use the <redact> named group. Only one named group can be used per rule.

For example, the regular expression TFN(:|:\s|\s|)(?<redact>(\d{8,9}) will match **TFN: 12345678** but will only apply a markup on the 12345678.

29.26.2 Email addresses and phone numbers regular expressions

Name	Description	Example
France Phone Numbers	This regular expression can be used to redact french phone numbers that include the country code but do not have delimiters.	\b([0O]?[1Il][1Il])?[3E][3E][0O]?[\dOIlZEASB]{9}\b

Name	Description	Example
Germany Phone Numbers	This regular expression can be used to redact German phone numbers.	\b[\d\w]\d{2}[\d\w]{6}\d[\d\w]\b
UK Phone Numbers	This regular expression can be used to redact UK phone numbers that include country code but does not have delimiters.	\b([0O]?[1Il][1Il])?[4A][4A][\dOIlZEASB]{10,11}\b
US Phone Numbers	This regular expression can be used to redact US phone numbers. It is recommended to test this regex on a website like regex 101 with the phone numbers that appear in your document set before running it in a project to validate that it will match. This regular expression may be overly aggressive so sampling is recommended.	\b((\+|\b)[1I][\-\.])?\(?\b[\dOIZSB]{3,5}([\-\.]|\) ?)[\dOIZSB]{3}[\-\.][\dOIZSB]{4}\b
US Street Address	This regular expression uses a multi-state conditional hint to redact street addresses. Similar to phone numbers, this regular expression should be sampled for desired results before running against the full document set.	\b\d{1,8}\b[\s\S]{10,100}?\b(AK|AL|AR|AZ|CA|CO|CT|DC|DE|FL|GA|HI|IA|ID|IL|IN|KS|KY|LA|MA|MD|ME|MI|MN|MO|MS|MT|NC|ND|NE|NH|NJ|NM|NV|NY|OH|OK|OR|PA|RI|SC|SD|TN|TX|UT|VA|VT|WA|WI|WV|WY)\b\s\d{5}\b

29.26.3 Universal regular expressions

Name	Description	Example
Dates	This regular expression will match dates.	\b([0-3]?\d(st)?(th)?|jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)[/\-]([0-3]?\d(st)?(th)?|-jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)[/\-]\d{2,4}\b
Email Addresses	This regular expression will match and redact full email addresses.	\b[a-z0-9._%\+\-—|]+@[a-z0-9.\-—|]+\.[a-z|]{2,6}\b
Redact specific email domains		\b[a-z0-9._%\+\-—|]+@(gmail|Relativity)\.[a-z|]{2,6}\b
Exclude specific email domains		\b[a-z0-9._%\+\-—|]+@[a-z0-9.\-—|]+\.[a-z|]{2,6}(?<!Relativity.com|gmail.com)\b
Partial text (redact local email)		(?<redact>[a-z0-9._%\+\-—|]+)@[a-z0-9.\-—|]+\.[a-z|]{2,6}
Birth Dates	This regular expression uses contextual hints to locate and redact dates that are in proximity to words that typically denote birth dates. It's important to understand that while dates are regular patterns, birth dates are not. If a non-birth date exists within close proximity of our contextual hits, it will be redacted. The contextual hint words in this regular expression are: • birth • birth date • birthday • date of birth • born	\b(birth|birthdate|birthday|dob|born)\W+(?:\w+\W+){0,5}?(?<REDACT>(\d{4}|\d{1,2})[\/\-]\d{1,2}[\/\-](\d{4}|\d{1,2}))\b
IPv4	This regular expression will match and general IPv4 addresses.	\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b
IPv6	This regular expression will match and general IPv6 addresses.	\b([\d\w]{4}|0)(\:([\d\w]{4}|0)){7}\b
Pre-OCR or HOCR images without any redaction rules	This regular expression does not find matches or apply markups. Instead, you can use this regular expression to begin running OCR for a large project without needing to create other rules first. You can then add the rules for matching terms while the OCR is run-	\A

Name	Description	Example
	ning at your convenience.	
Redact text after key term		\bTerm\s?(?<redact>[\d]{9})

29.26.4 Financial accounts regular expressions

29.26.4.1 Credit cards

If using the regular expressions below for an automated image markup project, results may be improved by being defensive against common OCR mistakes. Each instance of any digit match can be replaced with a character replacement pattern that will evaluate numbers as common alphanumeric characters.

To do so simply replace the \d pattern with [\dOIlZEASB]. This type of defensive matching is not typically needed for spreadsheets.

Visa, MasterCard, AmEx

```
\b((4\d{3}|5[1-5]\d{2}|2\d{3}|3[47]\d{1,2})[\s\-]?\d{4,6}[\s\-]?\d{4,6}?([\s\-]\d{3,4})?(\d{3})?)\b
```

This regular expression matches the following samples.

Visa

- 4532613257548007
- 4716563756075937
- 4929038415234561233
- 4718 4123 4142 4124
- 4716-5637-5607-5937

MasterCard

- 2720-9928-3988-7281
- 2720992839887281
- 5461718001676921
- 5489790994470834
- 5489 7909 9447 0834
- 5489-7909-9447-0834

American Express

- 372714876128394
- 346781676352683
- 376506566639896
- 3765 065666 39896
- 3467 816763 52683
- 3400 0000 0000 009

Individual brand credit cards

Card name	Regular Expressions
American Express card	\b3[47][0-9]{13}\b
BCGlobal	\b(6541|6556)[0-9]{12}\b
Carte Blanche card	\b389[0-9]{11}\b
Diners Club card	\b3(?:0[0-5]|[68][0-9])[0-9]{11}\b
Discover card	\b65[4-9][0-9]{13}|64[4-9][0-9]{13}|6011[0-9]{12}|(622(?:12[6-9]|1[3-9][0-9]|[2-8][0-9][0-9]|9[01][0-9]|92[0-5])[0-9]{10})\b
Insta Payment card	\b63[7-9][0-9]{13}\b
JCB card	\b(?:2131|1800|35\d{3})\d{11}\b
Korean Local card	\b9[0-9]{15}\b
Laser card	\b(6304|6706|6709|6771)[0-9]{12,15}\b
Maestro card	\b(5018|5020|5038|6304|6759|6761|6763)[0-9]{8,15}\b
Mastercard	\b(?:4[0-9]{12}(?:[0-9]{3})?|[25][1-7][0-9]{14}|6(?:011|5[0-9][0-9])[0-9]{12}|3[47][0-9]{13}|3(?:0[0-5]|[68][0-9])[0-9]{11}|(?:2131|1800|35\d{3})\d{11})\b
Solo card	\b(6334|6767)[0-9]{12}|(6334|6767)[0-9]{14}|(6334|6767)[0-9]{15}\b
Switch card	\b(4903|4905|4911|4936|6333|6759)[0-9]{12}|(4903|4905|4911|4936|6333|6759)[0-9]{14}|(4903|4905|4911|4936|6333|6759)[0-9]{15}|564182[0-9]{10}|564182[0-9]{12}|564182[0-9]{13}|633110[0-9]{10}|633110[0-9]{12}|633110[0-9]{13}\b
Union Pay card	\b(62[0-9]{14,17})\b
Visa card	\b4[0-9]{12}(?:[0-9]{3})?\b
Visa Mastercard	\b(?:4[0-9]{12}(?:[0-9]{3})?|5[1-5][0-9]{14})\b

Other financial accounts

Name	Description	Example
American Banker Association (ABA) transit routing numbers	This regular expression matches the following ABA routing numbers: • 011103093 • Florida 067014822	\b((0[0-9])|(1[0-2])|(2[1-9])|(3[0-2])|(6[1-9])|(7[0-2])|80)([0-9]{7})\b

Name	Description	Example
	• Maine 211274450 • Massachusetts/Rhode Island 211370545 • Metro DC/Maryland/Virginia 054001725 • New Hampshire 011400071 • New Jersey/Delaware 031201360 • New York – Metro NYC or former Commerce customers 026013673 • New York – Upstate NY or former Banknorth customers 021302567 • North Carolina/South Carolina 05390219 • Pennsylvania 036001808 • Vermont 011600033	
US ABA Routing Transit Number	This regular expression can be used to apply markups to an ABA routing number.	\b(0[0-9]|1[0-2]|2[1-9]|3[0-2]|6[1-9]|7[0-2]|80)\d{7}\b
SWIFT Code	This regular expression can be used to redact SWIFT codes for payment instruction information.	\b[A-Z]{6}[A-Z0-9]{2}([A-Z0-9]{3})?\b
IBAN Codes	This regular expression can be used to redact IBAN codes for payment instruction information.	(?:(?:IT|SM)\d{2}[\w]\d{22}|CY\d{2}[\w]\d{23}|NL\d{2}[\w]{4}\d{10}|LV\d{2}[\w]{4}\d{13}|(?:BG|BH|GB|IE)\d{2}[\w]{4}\d{14}|GI\d{2}[\w]{4}\d{15}|RO\d{2}[\w]{4}\d{16}|KW\d{2}[\w]{4}\d{22}|MT\d{2}[\w]{4}\d{23}|NO\d{13}|(?:DK|FI|GL|FO)\d{16}|MK\d{17}|(?:AT|EE|KZ|LU|XK)\d{18}|(?:BA|HR|LI|CH|CR)\d{19}|(?:GE|DE|LT|ME|RS)\d{20}|IL\d{21}|(?:AD|CZ|ES|MD|SA)\d{22}|PT\d{23}|(?:BE|IS)\d{24}|(?:FR|MR|MC)\d{25}|(?:AL|DO|LB|PL)\d{26}|(?:AZ|HU)\d{27}|(?:GR|MU)\d{28})

29.26.5 Government identification numbers regular expressions

These regular expressions can be used to help you apply markups to personally identifiable information related to government records such as tax IDs, government issued IDs, and more.

Name	Description	Example
Argentina National Identity (DNI) Number	This regular expression matches the following examples: • 34.960.099 • 63.889.141 • 40.571.278 • 45.855.200 • 80.933.831	\d{2}\.\d{3}\.\d{3}
Australia Tax File Number	The Australian tax file number is typically 8-9 digit numbers preceded by TFN. Other indicators in the government website may say things like payee's tax file number or tax file number. Typically, you can use these indicators to confirm that the 8-9 digits are a TFN. To apply markups, you will need to select the **Character** option for the Markup Scope field as well. For example, when the TFN appears like TFN: 12345678, you can search for TFN: and then use the Redact named group redaction hint to only redact the numbers. TFN(:|:\s|\s|)(?<redact>(\d{8,9}) This regular expression will match TFN: 12345678 but will only place a redaction on the 12345678.	
Canada Passport ID	This regular expression will match Canadian passport IDs.	\b[\w]{2}[\d]{6}\b
Canada Postal code	This regular expression will match Canadian postal codes.	\b[a-z]\d[a-z][-]?\d[a-z]\d\b
Canada Social Insurance Number	This regular expression will match Canadian insurance numbers.	\b(\d{3}[\—\-_]\d{3}[\—\-_]\d{3})|(\d{9})\b
Croatia Vat ID card number	This regular expression will match Croatian VAT ID card number.	\bHR\d{11}\b
Czech Republic Vat ID card number	This regular expression will match Czech Republic VAT ID card number.	\bCZ\d{8,10}\b
Denmark Personal ID number	This regular expression will match Denmark Personal ID number.	\b\d{10}|\d{6}[-\s]\d{4}\b
France National ID card (CNI)	This regular expression will match France's National ID card (CNI).	\b\b\d{12}\b\b
France Social Security Number (INSEE)	This regular expression will match France's Social Security Number (INSEE).	\b\d{13}|\d{13}\s\d{2}\b
France Driver's	This regular expression will match France's Driver's license ID.	\b\d{12}\b

Name	Description	Example
License ID		
France Passport ID	This regular expression will match France's Passport ID.	\b\d{2}11\d{5}\b
Germany ID card number	This regular expression will match Germany's ID card number.	\bl\d{8}\b
Germany Passport ID	This regular expression will match Germany's Passport ID.	\b[cfghjk]\d{3}\w{5}\d\b
Germany Driver's License ID	This regular expression will match Germany's Driver's License ID.	\b[\d\w]\d{2}[\d\w]{6}\d[\d\w]\b
Ireland Personal Public Service (PPS) Number	This regular expression will match Personal Public Service (PPS) Number.	\b\d{7}\w{1,2}\b
Netherlands Citizen's Service (BSN) number	This regular expression will match Citizen's Service (BSN) number.	\b\d{8}|\d{3}[-\.\s]\d{3}[-\.\s]\d{3}\b
Poland National ID (PESEL)	This regular expression will match Poland's National ID (PESEL).	\b\d{11}\b
Portugal Citizen Card Number	This regular expression will match Portugal's Citizen Card Number.	\d{9}[\w\d]{2}|\d{8}-\d[\d\w]{2}\d
Spain Social Security Number (SSN)	This regular expression will match Spain's Social Security Number.	\b\d{2}\/?\d{8}\/?\d{2}\b
Sweden Passport ID	This regular expression will match Sweden's Passport ID.	\b\d{8}\b
United Kingdom Passport ID	This regular expression will match United Kingdom's Passport ID.	\b\d{9}\b
United Kingdom Driver's License ID	This regular expression will match United Kingdom's Driver's License ID.	\b[\w9]{5}\d{6}[\w9]{2}\d{5}\b
United Kingdom National Health Service (NHS) number	This regular expression will match United Kingdom's National Health Service (NHS) number.	\b\d{3}\s\d{3}\s\d{4}\b
United States Social Security Number	These regular expressions are optimized for image and spreadsheet documents respectively. The image version of the SSN Regex is specifically created to be defensive against common	Image Projects \b[\dIZEASBO]{3} [\dIZEASBO]{2} [\dIZEASBO]{4}|([\dIZEASBO] ?)

Name	Description	Example
(SSN)	OCR mistakes such as 1 being read as l, i, or I.	{3}[\—\-_] ?([\dlZEASBO] ?){2}[\—\-_] ?([\dlZEASBO] ?){4}\b Spreadsheet Projects \b[\d]{3} [\d]{2} [\d]{4}|([\d] ?){3}[\—\-_] ?([\d] ?){2}[\—\-_] ?([\d] ?){4}\b Spreadsheet and PDF projects redact all but the last four digits of SSN with spaces (?<redact>\b[\d]{3} [\d]{2}) [\d]{4} Spreadsheet and PDF projects redact all but the last four digits of SSN with hyphens (?<redact>([\d] ?){3}[\—\-_] ?([\d] ?){2}[\—\-_]) ?([\d] ?){4}\b
US Federal Employer Identification Number	This regular expression will match the Federal Employer ID number.	\b[0-9]{2}[—\-][0-9]{7}\b

29.27 Reviewing markups to ensure accuracy

After markups have been applied, whether it be manually or automatically by a project, it is important to review them for quality control purposes. The Redact Navigation card allows you to track whether a markup has been reviewed and remove any markups that are no longer needed. Alternatively, to ensure that automated projects applied markups correctly, you can use Quality Review to compare the number of matches found in the extracted text of a document versus the number of markups that were applied by the project(s) to help you identify discrepancies before producing documents.

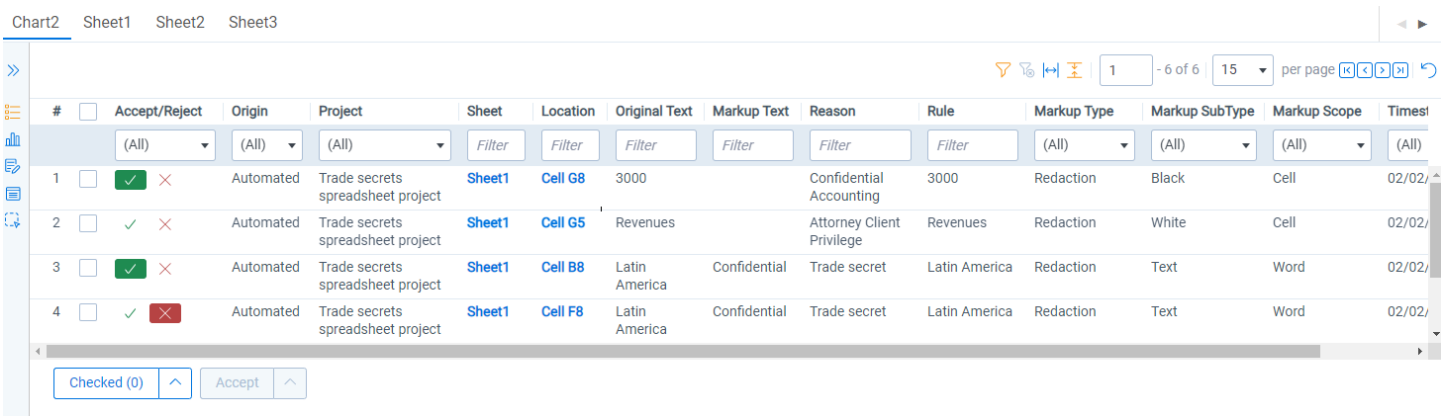
29.27.1 Using the Redact Navigation card to review markups

The Redact Navigation card offers you the ability to indicate that a markup has been approved or you can remove any markups that are no longer needed as you perform quality control. After a markup has been applied to a document, the **Redact - Has Native Redactions** field updates to display the name of any markup sets used to apply markups to that document. You can then create a saved search using that field to organize a set of documents that have had markups applied in Redact. For more information on this, see Searching for documents with Redact fields.

After opening a document in the Viewer, click the **Redact Markup Navigator** icon in the bottom-left to expand the Redact Navigation card. Each markup is displayed in its own row that provides additional information described below. Optionally, you can click the Approve icon to approve a markup or click the Reject icon to remove the markup from the document as part of your quality control process.

If you want to approve or reject several markups at once, select the desired markups manually or choose **All** from the Checked drop-down menu, and then click **Accept** or if you want to reject all markups, click **Reject**.

While viewing the Redact Navigation card in the Image Viewer, you can download a .csv report to your workstation that includes Redact related information by clicking the **Export to CSV** icon.



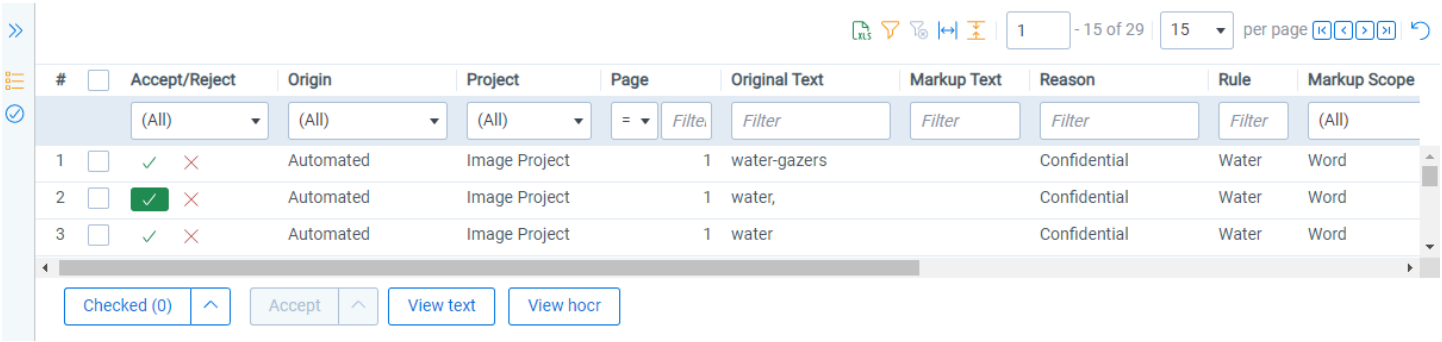
The following columns display in the Redact Navigation card:

Column Name	Description
Accept/Reject	This optional column allows you to review markups that have already been applied. The Accept/Reject column can be in one of the following states depending on which icons have been selected: • Not Set - Neither approved or rejected have been selected for this markup. The applied markup function normally. • Approved - If selected, the applied markup has been approved for production and will function normally. • Rejected - If selected, the applied markup will be removed.
Location	Displays the cell name where the markup is located. Optionally, you can click on the cell name to navigate to the location of this markup.
Markup Scope	Displays what each markup obscures as selected when creating the project.
Markup Subtype	If the markup is a highlight, this column displays the name of the color used in the highlight. If the markup is a redaction, this column display the name of the redaction type.
Markup Text	Displays the text in the markup for text redactions.
Markup Type	Displays whether the markup is a highlight or redaction. Optionally, you can click on the **Markup Type** to navigate to the markup within the document.
Origin	Displays one of the following options to indicate where a markup came from: • Manual - indicates that the markup was applied manually. • Automated - indicates that the markup was applied through automation by running a project.
Original Text	Displays the text that is obscured by each markup. If multiple cells are obscured by a single markup, this column will display the name of each cell that is covered by the markup and the text that is obscured by the markup.
Project	Displays the name of the project that applied each markup in the document.
Reason	Displays the rationale you entered when creating the project for each markup.
Rule	Displays the name of the rule that resulted in the match and caused a markup to be applied by the Redact project.
Sheet	Displays the name of the sheet where the markup is located. Optionally, you can click on the sheet

Column Name	Description
	name to navigate to the location of this markup.
Timestamp	Displays the date and time when a markup was created.

29.27.2 Using the Redact navigation card in the Image Viewer

In addition to the functionality described above, the Redact navigation card offers additional options in the Image Viewer to help you better understand how markups were applied to an OCR document that has extracted text. Applying markups to OCR documents has some fuzziness and if there are similar characters in the document to your search terms it can lead to false matches. As a result, we recommend QC'ing markups that are applied to an OCR document to ensure accuracy. You can view both the extracted text of the document and the text recognized as part of an OCR job and compare the two to better understand why a markup was or was not applied to certain terms.



Click **View text** to see the extracted text from the current document in a pop-up window.

Click **View hocr** to see the text from the OCR document in a pop-up window.

29.27.3 Review image markups using Quality Review

After running an automated image markup project, it is a best practice to review documents and ensure that all sensitive information has been properly redacted or highlighted. To aid you in this process, the Image Viewer has Quality Review. Click on the **Redact Image Markup Navigator** icon and ensure that the **Quality Review** icon is selected.

Quality Review contains a view, Image Quality Review, that allows you to compare the number of matches in the extracted text of a document as determined by the rules in the project you ran versus the number of markups applied to the document. You can use this view to find discrepancies and ensure that markups are applied to all of the correct information before production.

The following columns display in Quality Review:

Column Name	Description
Type	Displays whether each rule was a regular expression or word/phrase.
Rule	Displays the name of the rule in a previously ran project that has a match either in the normal text or extracted text of the document.
Placed	Displays the total number of markups applied to this document.
Expected	Displays the total number of matches in the extracted text of the document. If this number is higher than in the Placed column, carefully review the document to ensure that there is not any sensitive information that could be exposed after production.

29.27.4 Delete Native Markups

Markups that have been applied to a native document can be removed from one or more documents at a time using the Delete Native Markups mass operation. Delete Native Markups allows you to remove either all markups applied to the documents or all of the markups from a single markup set.

To remove markups on native documents, do the following:

1. Navigate to the **Documents** tab.
2. Select each document that you wish to remove markups from.
3. Select **Delete Native Markups** from the mass operations toolbar.
   The Delete Native Markups pop-up displays.
4. Select either **All Markup Sets** to remove all markups from the selected documents or the desired markup set to remove only markups applied using that markup set.
5. On the **Remove From** field, select one of the document types to remove markups from.
6. Click **Save**.
   The markups are removed from the selected documents and an email is sent to the user's email address that summarizes the results of the mass operation.

29.28 Running and reverting a Redact project

A project can be run once it has a Project Name, Saved Search, Markup Set, and rules. To help you track a project's readiness, a status message that indicates whether it is ready to be run or not displays when viewing a project. If there are multiple projects that have been queued to run, they will be completed in order of when they were queued. Once a spreadsheet or PDF markup project finishes running, it generates a report that contains a list of any documents where Redact could not apply a markup for quality control purposes.

Note: If you run a project and would like to edit the rules to get different results, we recommend reverting the project before editing the rules and rerunning it to prevent duplicate markups. To learn more, see Redact project best practices.

Note: By default, each document pair in a spreadsheet propagation project has up to 30 minutes to finish processing. If a pair does not complete in that time, Redact stops waiting on the pair of documents, marks that pair as failed, and continues processing the remaining pairs in the project. The length of time before a document pair times out can be adjusted with the **ExcelPropagationPairTimeOut** instance setting. To learn more, see Adjusting the spreadsheet propagation time out length.

29.28.1 Running a project

To begin running a project, do the following:

1. Navigate to the **Redact Projects** tab.
2. Click on the project you wish to run.
3. Click on the **Run** button.
   The project is added to the queue and will begin running when agents are available. To view rough estimates on a project's run-time, visit Redact project performance expectations.

Note: By default, a document has up to 55 minutes to finish processing before Redact skips that document and tries to run the remaining documents in the project. The length of time before a document times out can be adjusted with the **RedactProjectDocumentProcessingTimeOut** instance setting. To learn more about this instance setting, see Adjusting Redact time out length.

29.28.2 Redact project performance expectations

Note: As part of the release of Redact, Viewer performance has been upgraded so that document load time has decreased.

We are providing directional estimates on project performance to help you gauge the duration of a project run. Consider these project estimates more as directional rather than precise because project performance may vary across other variables (file size, number of rules, pages per document, etc).

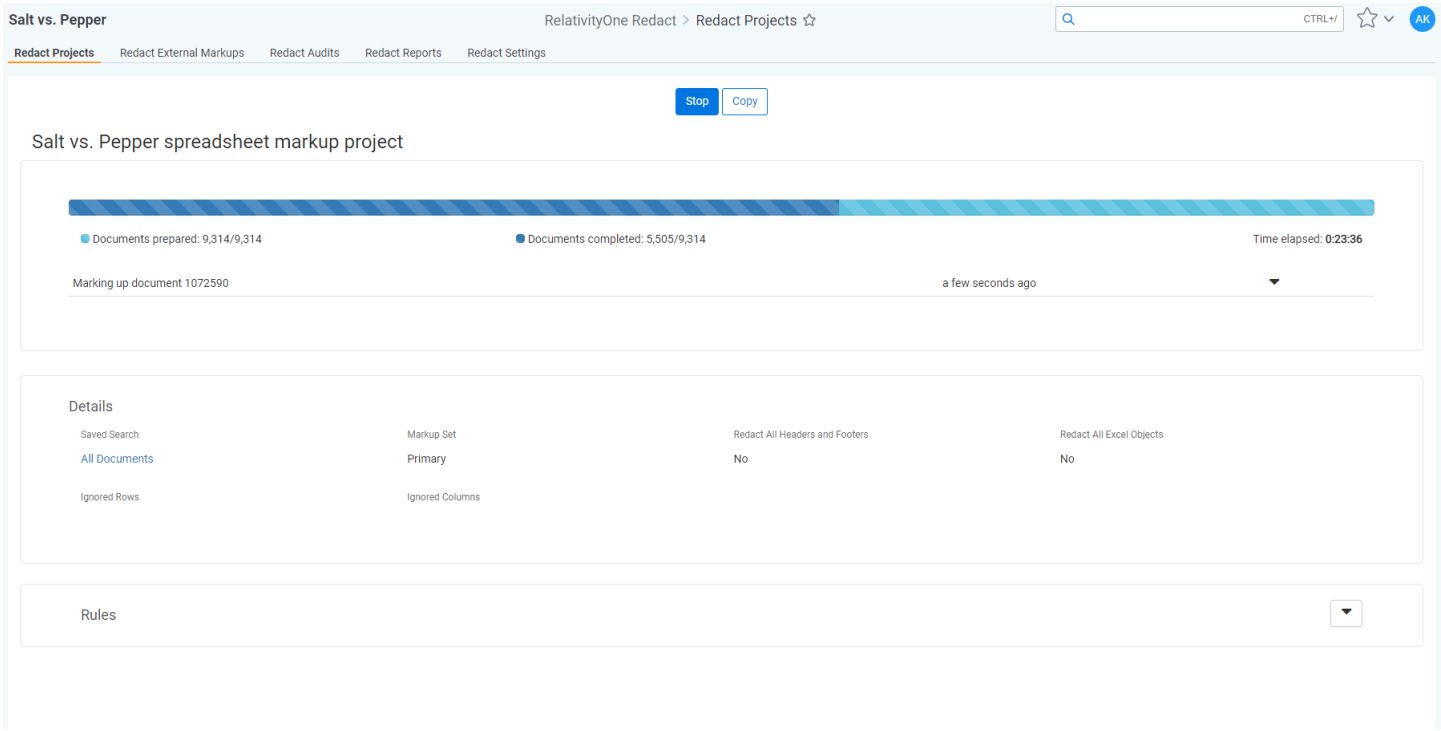
To help you determine the size of a project, you can use the Tally/sum/average mass operation. Select the Relativity Image Count field for the mass operation and include all of the documents in the saved search that the project will utilize to generate an estimate. To learn more, visit Tally/sum/average.

- Default agent configuration (1 high resource agent)
- Vertical scaling (additional agents on the same server)
- Horizontal scaling (additional agents on the different servers)

Project Type	Number of Agents	Pages/Minute
Image	1	32
	2	71
	3	105
Spreadsheet	1	700
	2	1,089
PDF	1	170
	2	250

29.28.2.1 Viewing a project's run status

If you view a project that is running, you can see information about the progress of the run.

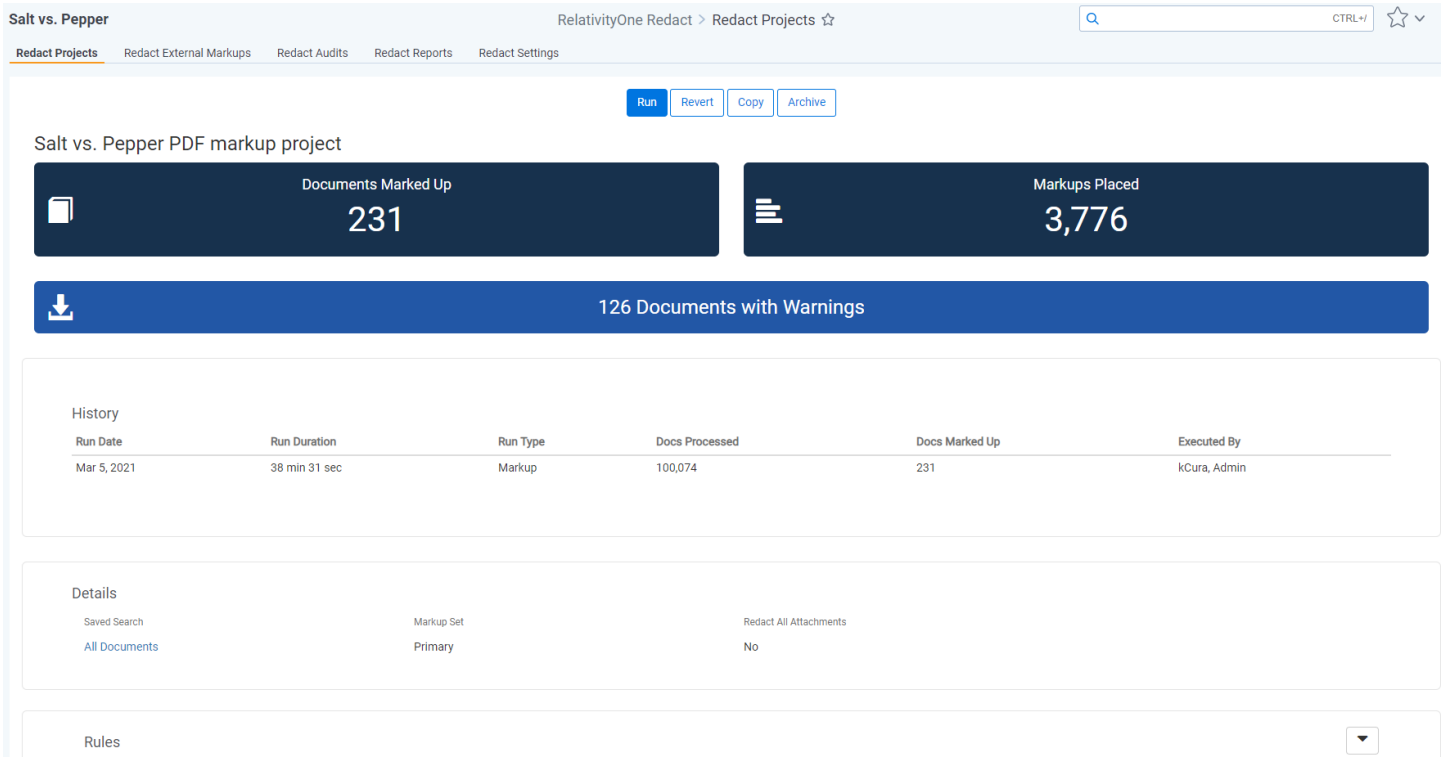


The following information displays:

- **Documents prepared**—Displays the number of documents that have been added to the project run for potential markup.
- **Documents completed**—Displays the number of documents that have been reviewed and had markups applied according to the project rules.
- **Progress bar**—Displays the progress of the run. The light blue bar represents the amount of Documents prepared and the dark blue bar represents the amount of Documents completed.
- **Time elapsed**—Tracks the amount of time that has passed while the project is running.
- **Current status**—Once a project begins running, a status bar will display to show what task is being completed. Once multiple tasks are completed, you can click on the bar to view previous tasks.

29.28.2.2 Viewing completed project's results

Once a project has finished running, you can find information about the results by viewing the job.



The following information may display depending on which type of project you ran:

- **Documents Marked Up**—Displays the total number of documents that have had markups applied to them by this project's run. Clicking this tile will navigate you to the Documents tab where a saved search that contains all of the documents that have had markups applied by this project.
- **Markups Placed**—Displays the total number of markups that have been applied to documents by this project's run. Clicking this tile will navigate you to the Documents tab where a saved search that contains all of the documents that have had markups applied to them.
- **Documents to review**—To help you quality control the automation process, Redact will compare the number of matches in the extracted text of a document to the number of markups applied to it and if there are more matches than markups applied, the document will be flagged. This tile tracks the number of flagged documents where there is a discrepancy between those two tallies. Clicking on this tile will navigate you to the Documents tab where a saved search that contains all of the documents that have less markups than there are matches in the extracted text.
- **Documents with warnings**—Displays the number of documents that encountered a warning. These warnings do not affect the project's run or prevent other documents from having markups applied. Clicking this tile will download a .CSV file to your workstation that contains a list of document warnings and any error messages.
- **History**—This section contains information and statistics about the most recent project run.
  - **Docs Processed**—The number of documents in the saved search that meet the project type and are eligible to receive markups. For example, if you are running a spreadsheet markup project, only spreadsheet documents would be tallied for this field even if other document types are included in the saved search.
  - **Docs Marked Up**—The number of documents in the saved search that contain at least one hit based on the project rules.

29.28.3 Stopping a project that is running

You can halt a project that is currently running by doing the following:

1. Navigate to the **Redact Projects** tab.
2. Click on the project you wish to stop.
3. Click **Stop**.
   The project's run is stopped. Any documents that were processed as part of the project's run will have markups applied. The number of documents that were marked up by the project is displayed when viewing the project.

29.28.4 Reverting a project

If you have run a project that applied markups to documents and those markups need to be removed, you can revert the project's run. To revert a project, do the following:

1. Navigate to the **Redact Projects** tab.
2. Click on the project you wish to revert.
3. Click **Revert**.
   The Revert Project modal displays.
4. Click **Revert** again.
   The reversion task will be added to your queue will begin running when agents are available. To view rough estimates on a project reversion's run-time, visit Redact project performance expectations. While the project is being reverted, a status bar will display the reversion's progress. Once completed, the project will display a message indicating that the project was reverted.

29.28.4.1 Adjusting Redact time out length

You can adjust the length of time a document has to complete processing before it is skipped by the project by creating an instance setting in your environment. To add the **RedactProjectDocumentProcessingTimeOut** instance setting:

1. Navigate to the **Instance Settings** tab.
2. Click **New Instance Setting**.
3. Enter the following information:
   - **Name**—RedactProjectDocumentProcessingTimeOut
   - **Section**—Relativity.Redact
   - **ValueType**—Integer 32-Bit
   - **Value**—Enter the maximum length of time in minutes that a document can be processed before it is skipped by the project. The default value is 55 minutes if you have not created or edited this instance setting previously.
4. Click **Save**.
   The instance setting is created and the processing of documents in a project will time out based on the Value you entered.

29.28.4.2 Adjusting the spreadsheet propagation time out length

You can adjust the length of time a document pair has to complete processing before it fails and the Redact project moves onto the next documents by creating an instance setting in your environment.

To create the **ExcelPropagationPairTimeOut** instance setting:

1. Navigate to the **Instance Settings** tab.
2. Click **New Instance Setting**.

3. Enter the following information:
    - **Name**—ExcelPropagationPairTimeOut
    - **Section**—Relativity.Redact
    - **ValueType**—Integer 32-Bit
    - **Value**—Enter the maximum length of time, in minutes, that a single document pair can be processed before it is failed by the project. The default value is 30 minutes if you have not created or edited this instance setting previously.
4. Click **Save**.
   The instance setting is created and the processing of document pairs in a spreadsheet propagation project time out based on the Value you entered.

Note: If you set a value that is not valid, a negative number, for example, Redact ignores the entered value and reverts back to the instance setting default of 30 minutes.

29.29 Searching for documents with Redact fields

Redact comes with several fields to help make tracking markups applied both inside and outside of Redact easy. You can use these fields in a saved search to view documents that have certain types of markups applied with Redact.

The following fields can be used to track markups:

Field Name	Description
Redact - Has External Markups	A multi-object field associated with the Markup Set Relativity field. You can use this field to determine if a document was externally redacted and associated with one or more markup sets.
Redact - Has Native Highlights	A multi-object field associated with the Markup Set Relativity field. You can use this field to determine if one or many markup sets have spreadsheet or PDF highlights.
Redact - Has Manual Native Markups	A multi-object field associated with the Markup Set Relativity field. You can use this field to determine if one or many markup sets have documents with manually placed markups.
Redact - Has Native Redactions	A multi-object field associated with the Markup Set Relativity field. You can use this field to determine if one or many markup sets have spreadsheet or PDF redactions.

29.29.1 Creating a saved search using Redact fields

Before creating a saved search, ensure that you are a System or Case Administrator with permission to create Relativity searches and then do the following:

1. Navigate to the **Documents** tab, click on the **Saved Searches** browser icon, and click **Create New Search**.
2. Click **Add Condition**.
3. In the field list, select the desired Blackout field.
4. Click the **Add Condition** button and select the same Blackout field.
   The filter modal displays.
5. Select the desired markup set options to determine which documents will display in the results of the saved search.
6. Click the right arrow icon to move the selected markup set options to the right table and click **Apply**.

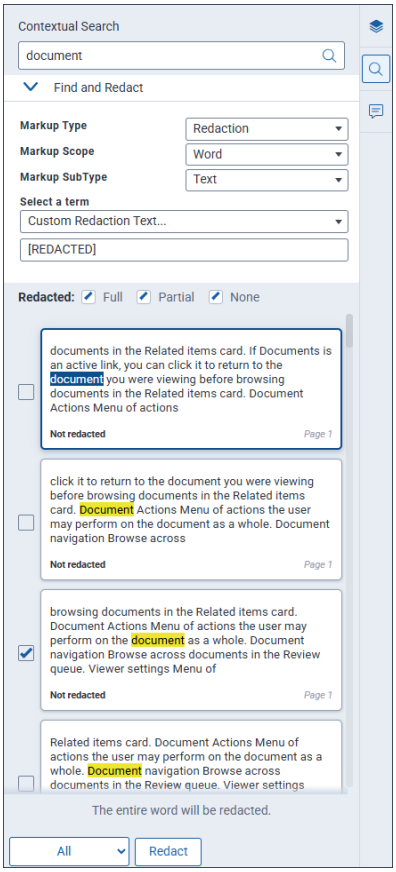
7. Click **Apply** again.
8. Optionally, repeat steps 2-7 to add additional fields as needed.
9. Click **Save & Search** or **Search**.
   The Document list is updated to show only documents that fit the condition criteria.

29.30 Using Find and Redact

You can apply markups to a spreadsheet, native PDF, or stored PDF in the Viewer while using the search capabilities of the Contextual Search card. To create a stored PDF, use Mass PDF.

This feature finds terms in a spreadsheet, native PDF, or stored PDF document and applies a markup to the desired terms without having to run a Redact project or manually apply markups.

Note: The contextual search returns hits on comments and chart labels content in spreadsheet documents. These content types cannot receive markups using Find and Redact. To apply a markup to a comment or chart label, see Manual markups with spreadsheet files.



To search for terms and apply markups:

1. Click the **Contextual Search** card icon.
2. Enter the desired search terms.
3. Click the **Find and Redact** section to view the markup options.
4. Edit the markup options to determine the type and appearance of the applied markups.
   A message displays at the bottom of the Contextual Search card to help you track the Markup Scope option that is selected.

5. Press **Enter** on your keyboard or click the **Search** icon in the Contextual Search textbox to search the document for matching terms.
6. Optionally, you can filter the results with the following options:
    - **Full**—Select to display any terms that match the search terms and are fully redacted. If unselected, these terms will not display in the results.
    - **Partial**—Select to display any terms that match the search terms and are partially redacted. If unselected, these terms will not display in the results.
    - **None**—Select to display any terms that match the search terms and have not been redacted. If unselected, these terms will not display in the results.
7. Either select each search term result that you would like to apply a markup to or click on the **Checked (X)** button and select **All** to apply a markup to all search term results.
8. Click the **Redact/Highlight** button.
   A modal displays while the markups are applied. Once the job is done, **Redactions complete** displays at the bottom of the card. If you complete a new search using either the term or the term within a search string, the results will display their markup status to help you track whether each term match is not redacted, partially redacted, or fully redacted.

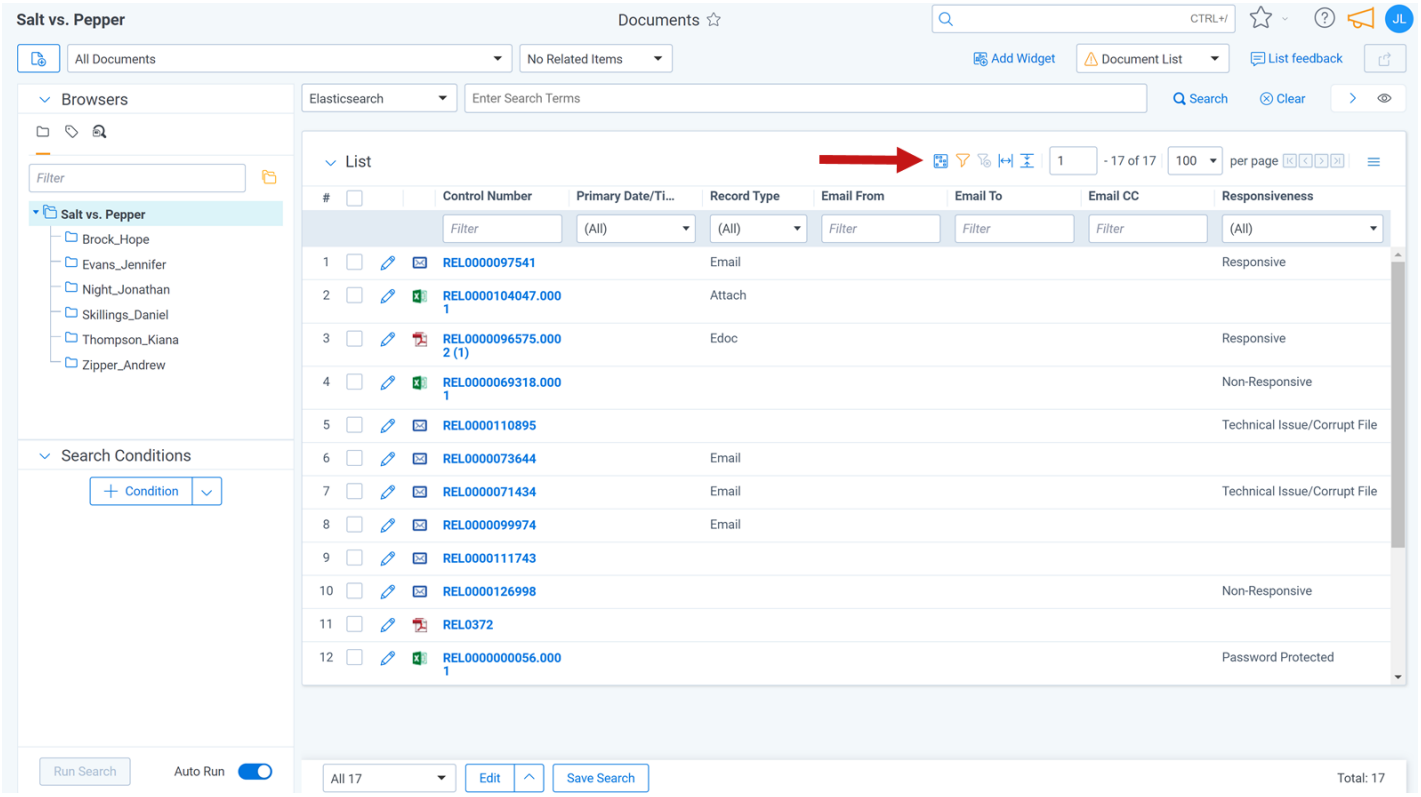
Note: A message displays when markups could not be applied to any results because it is either a comment or chart label. Locate results that did not receive a markup by refreshing the document and then searching for the same term again. Any terms that were previously selected and did not receive a markup are returned in the results.

30 Sampling

With sampling you can generate a randomized subset of items from a larger population. You can use that randomized sample to QC the list items or to identify characteristics of the whole population. To execute sampling, Relativity uses a randomization algorithm which guarantees an efficient and unbiased result.

You can enable any object to use Relativity's sampling. By default, sampling is enabled on the Document object.

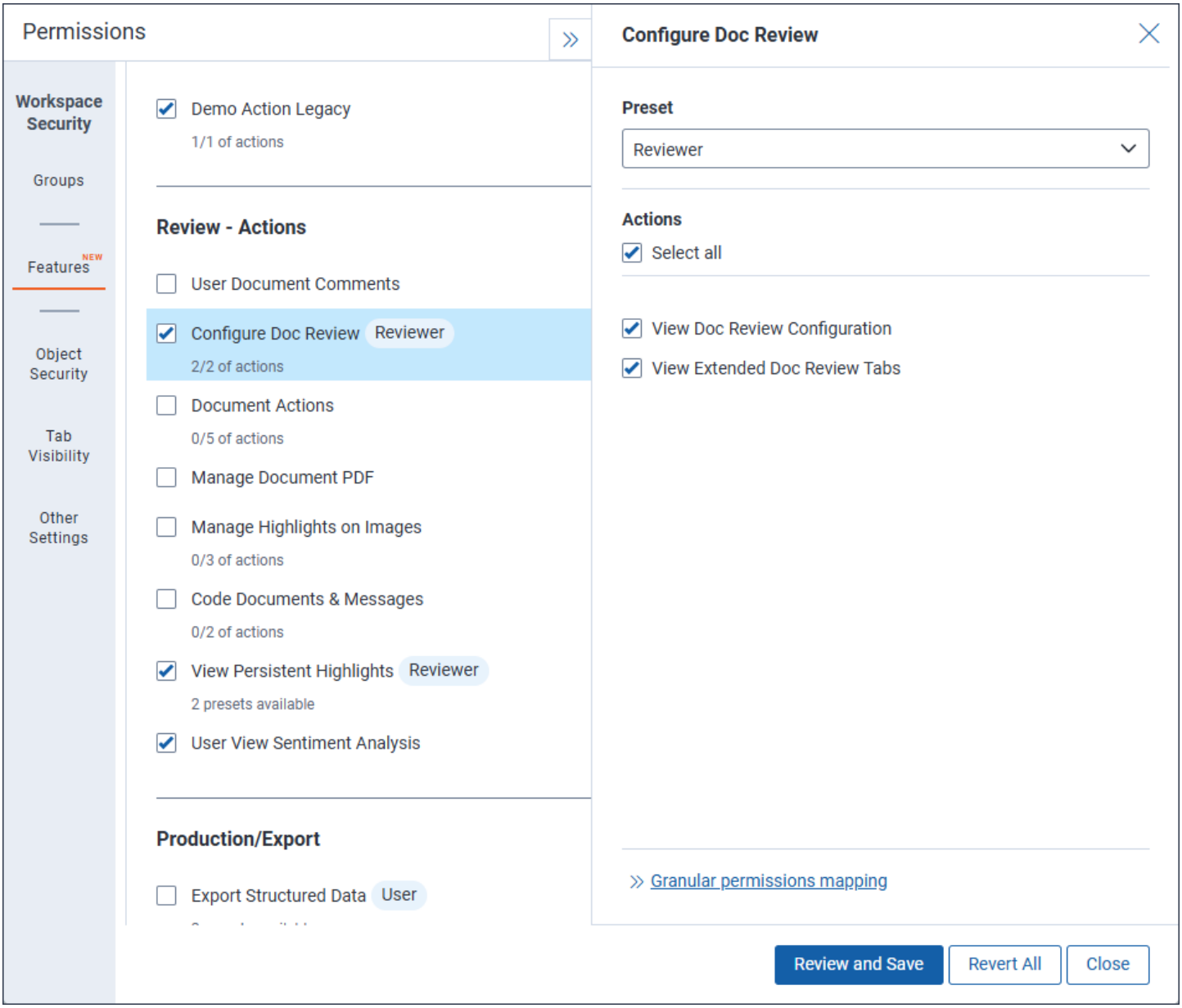
Once you've enabled sampling for an object, the sampling icon is available in the List section.



Note: The sampling feature requires the **Use Sampling** Admin Operations permission. See Workspace security on page 622.

30.1 Permissions

Note: This feature supports feature permission actions. Each action grants access to a specific task within the feature. You can grant groups access to individual actions, allowing them to perform only the tasks they need. To grant access to the entire feature, select all of its actions. Manage feature actions on the Features tab in a group's workspace permissions. For instructions, see Setting workspace permissions. For more information about feature permissions, see Feature permissions.



30.2 Enabling sampling on an object

To enable an object for sampling:

1. Navigate to the **Object Type** tab.
2. In the Object Type Information section, enter a name and select the object for which you want to enable sampling.
3. Ensure that **Sampling Enabled** is enabled. If you are creating a new object, this is enabled by default.
4. Ensure that **Lists Enabled** is enabled. If this field is disabled, you can't save the list of sampled items without creating a separate field, and then using mass edit to tag all of the sampled items. This field is disabled by default for new object types.

> **Note:** You can't save a list of sampled items as a saved search because the sample results are generated randomly.

5. Click **Save**. The sampling icon is now available on the object as long as you are assigned the Use Sampling Admin operation permission.

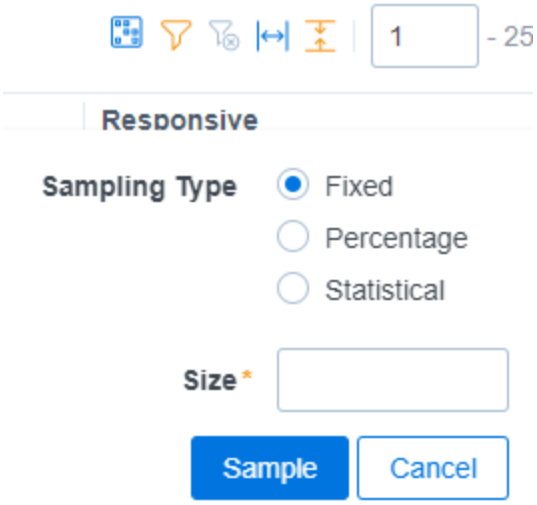
30.3 Generating a sample

The sampling drop-down menu provides three options for setting the sampling type (size):

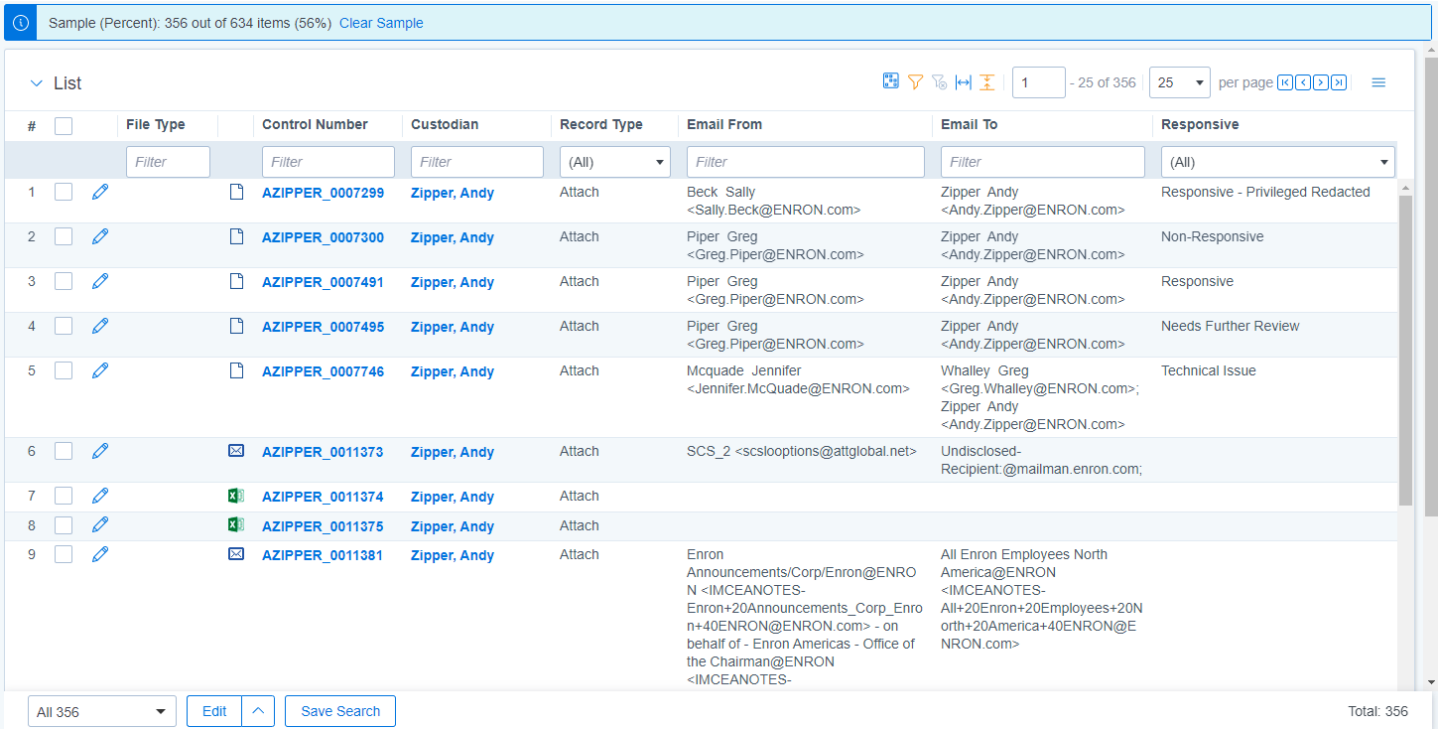
- **Fixed size** - creates a randomized sample set of a specific number of items from the entire item list. See Creating a fixed size sample set on the next page.
- **Percentage** - creates a randomized sample set of a specific percentage of items from the entire item list. See Creating a percentage sample set on the next page.
- **Statistical** - creates a randomized sample set of a size based on statistical sample calculations, which determines how many items reviewers need to address in order to get results that reflect the entire data set as precisely as needed. See Creating a statistical sample set on page 592.

Note: If you select a sampling type you previously applied in the same workspace, Relativity automatically populates the related settings field(s) with your last value(s).

Clicking **Sample** on the sampling drop-down menu applies your sampling settings to the item list and creates the randomized sample set.



The sample summary bar displays the sampling type you applied and a count of the sample set out of the total number of items.



Once you've applied the desired sampling settings, you can save the sampling results as a list using the Save as List mass operation. Then open the list as a saved search. For more information on lists, including creating and viewing lists, see Lists.

Note the following:

- Click **Clear Sample** on the sample summary bar menu to clear the sample. The sample set you create persists on the list of items until a user clears it. This includes while updating search conditions, switching and navigating within browser panels, including adding in relational items, and navigating to other tabs.
- The Sampling button is disabled when a related items option is selected from the Related Items drop-down menu or a search. If you have applied sampling and select a related items option from the Related Items drop-down menu, the sampling is removed from the list.

Note: The Save Search icon is also disabled for sampling results because the sample results are generated randomly. Clearing a sampled list of items re-enables the Save Search icon.

30.3.1 Creating a fixed size sample set

To create a sample set of a fixed size:

1. Navigate to the **Documents** tab.
2. Display the documents you want create a randomized sample of by selecting a folder, view, saved search, or performing a document search.
3. Click the **Sampling** icon to display the sampling drop-down menu.
4. Select **Fixed size** and provide a value greater than 0 in the **Size** field.
5. Click **Sample**.

30.3.2 Creating a percentage sample set

To create sample set of a specified percentage of total documents:

1. Navigate to the **Documents** tab.
2. Display the documents you want to create a randomized sample of by selecting a folder, view, saved search, or performing a document search.
3. Click the **Sampling** icon to display the sampling drop-down menu.
4. Select **Percentage** and provide a percentage value greater than 0% in the **Percentage** field.
5. Click **Sample**.

30.3.3 Creating a statistical sample set

Note: We recommend that you only use the statistical sampling type on data sets that are large enough to return a reliable statistical sample. If a data set contains fewer than 300 items, you may want to consider using a different sampling type.

To create a sample set size based on statistical confidence and margin of error specifications:

1. Navigate to the **Documents** tab.
2. Display the documents you want to create a randomized sample of by selecting a folder, view, saved search, or performing a document search.
3. Click the **Sampling** icon to display the sampling drop-down menu.
4. Select **Statistical**.
5. Select **99%**, **95%**, or **90%** for the **Confidence Level** field.
6. Select a value for the **Margin of Error** field. This is the room for error you want to allow in your sample results when you select a sampling type of statistical. Selecting a lower margin of error requires a larger sample size.
7. Click **Sample**.

31 Scripts

Scripts are Relativity artifacts. This means they have the same features as standard Relativity objects, allowing them to be secured and audited.

Note: Relativity Scripts are a tool to access and modify data stored in Relativity SQL databases. Not all data is available in SQL, and data currently in SQL may be migrated to other storage systems. The recommended integration mechanism is to use APIs/Services instead of scripts to avoid future migration or interruption. You should only use scripts when an appropriate API is not available. Relativity will add new and updated APIs over time - review the available APIs periodically to determine if you can replace a script with an API or REST service call.

Caution: Changes to SQL fields executed by Relativity Scripts do not produce Audit logs.

Only users who are members of groups with the appropriate permissions can write scripts. System admins have permissions to preview, edit, and create scripts.

If a script is locked, it appears as read only, and you can't edit it. If a script is unlocked it's available for editing.

The following table represents the script permissions allowed for each group.

			Locked Script		Unlocked Script			
	View	Run	Edit	Preview	Edit	Preview	Write	Link
System Admin	x	x		x	x	x	x	x
Standard User	x*	x*						x**

* With view rights
** With add rights

31.1 Script compatibility and updates

To improve system performance, architecture improvements are often applied to Relativity's SQL tables for new versions.

When upgrading, your personally-created scripts must be tested and revalidated before you run them. Remember that the recommended integration mechanism is to use APIs instead of scripts to avoid potential disruption if the data schema or storage mechanism changes.

Note: If you use a Relativity script in a custom development project, it is recommended to make a copy of the script and use the copied script in your project. Software updates may modify the scripts provided by Relativity, which could cause unintended results if you use the Relativity-provided scripts directly in your custom development projects.

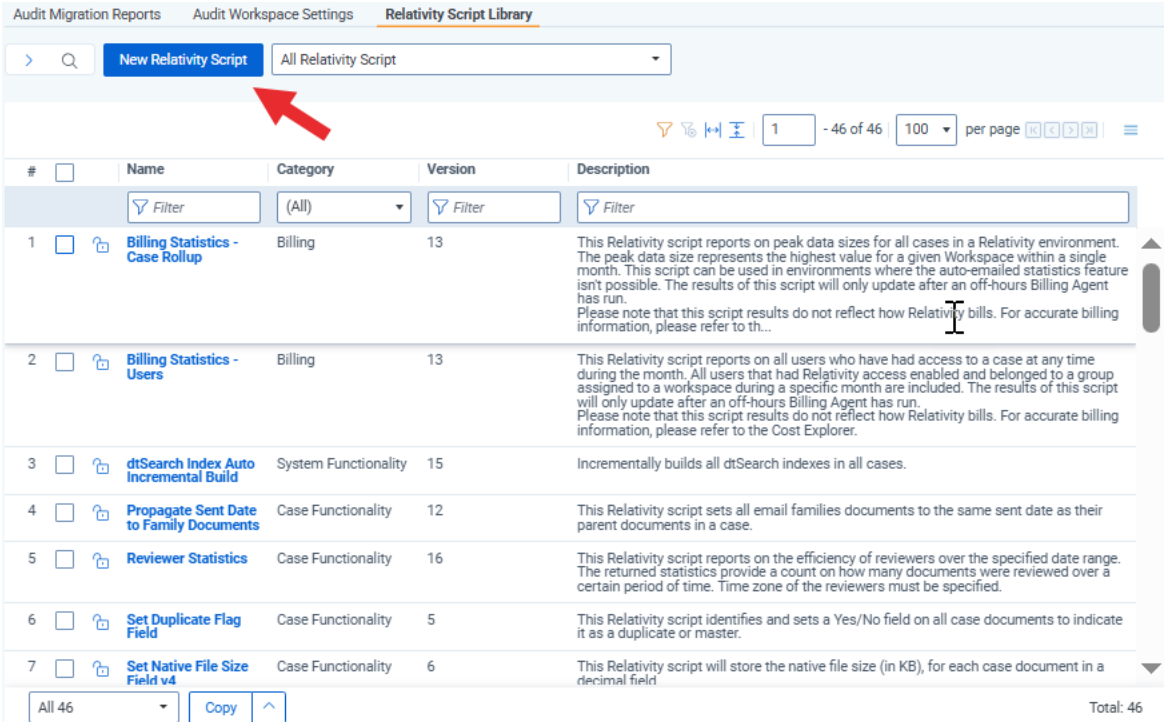
When upgrading your environment, the unique script key is referenced to determine if an update is required. If so, this is performed automatically.

31.2 Creating a new library script

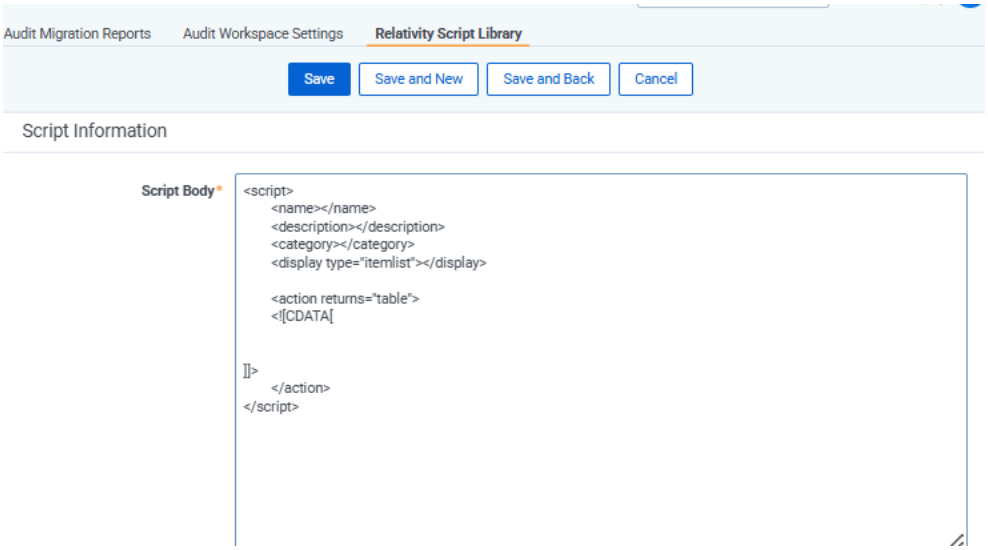
You can create a new library script in Admin to then be available for selection from the Scripts tab in any workspace in which the Scripts tab is visible.

To do this:

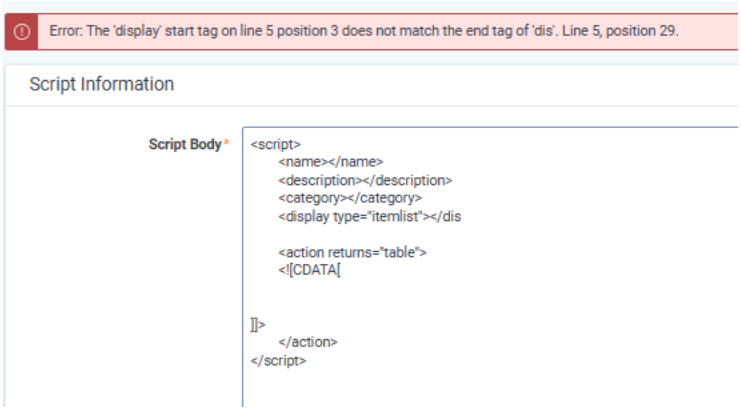
1. Navigate to the **Relativity Library Scripts** tab in Admin.
2. Click **New Relativity Script**.



3. In the **Script Body** field, enter values for each script component and click **Save**.



If any errors occurred in the script body, you will see an error message identifying the line and position of the problematic text. Relativity will not save the new script until you address the errors.



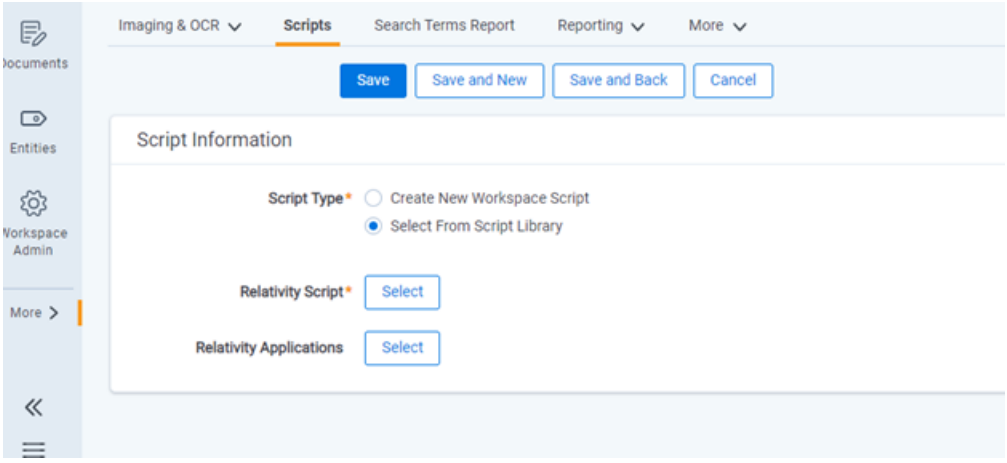
If no errors occur, Relativity saves the new script, and it is available for selection from the Scripts tab.

31.3 Selecting an existing library script

Due to the complexity and impact a script can have, only Relativity, SQL, and XML expert users should create and run them.

To select a library script and add it to your workspace, perform the following steps:

1. Navigate to and select the **Scripts** tab.
2. Click **New Relativity Script**. If you want to edit an existing script, click the **Edit** link next to the script name.
3. Complete the following fields:



   - **Script Type** - select **Select from Script Library** to choose from a list of predefined Relativity scripts. The Script Library tab is created when Relativity is deployed. Note that this is the only option available for the Script Type field if the AllowAddOrEditScripts instance setting is set to its default value of False.
   - **Relativity Script** - select the script from the script library.
   - **Relativity Applications** - associates the script with an application created on the Relativity Applications tab. All existing applications are available when you click the ellipsis. This is only available for those who have the **Manage Relativity Applications** permission under Admin Operations. For information on applications, see the Applications Guide.
4. Click **Save**.

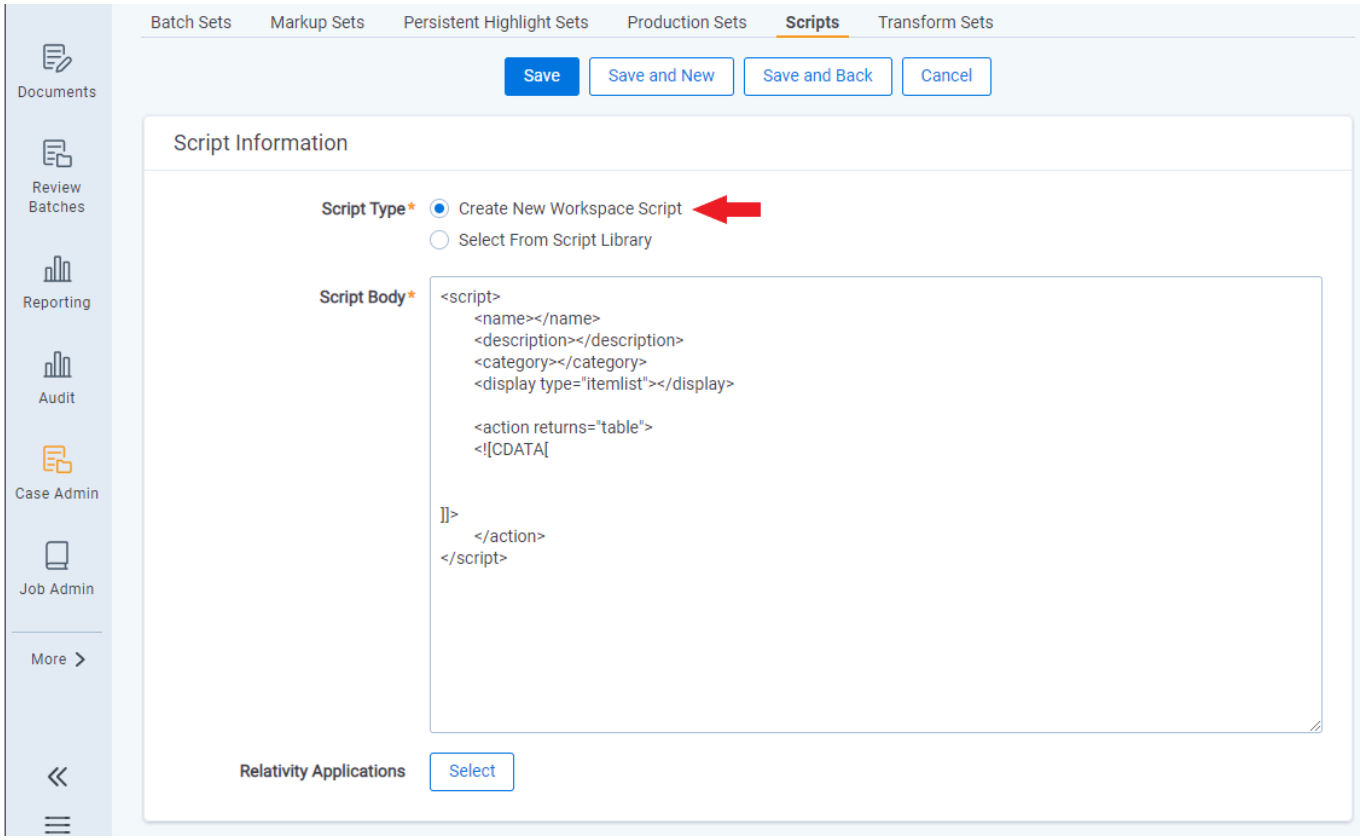
31.4 Creating a new workspace script

You must set the AllowAddOrEditScripts instance setting to True to make the Create New Workspace Script option available. In order to enable this instance setting in Relativity aiR, contact Customer Support.

Due to the complexity and impact a script can have, only Relativity, SQL, and XML expert users should create and run them.

To create a new workspace script, follow these steps:

1. Navigate to and select the **Scripts** tab.
2. Click **New Relativity Script**. If you want to edit an existing script, click the **Edit** link next to the script name.
3. Complete the following fields:



   - **Script Type** - select **Create New Workspace Script**.
   - **Relativity Applications** - associates the script with an application created on the Relativity Applications tab. All existing applications are available when you click the ellipsis. This is only available for those who have the **Manage Relativity Applications** permission under Admin Operations. For information on applications, see the Applications Guide.
   - **Script Body** - enter the script code into this area. For information on how to format a Relativity script, . see the Script Development guide.
4. Click **Save**.

31.5 Adding a library script to the script tab

In order for scripts to appear in your Script tab for your users to run, you must add them. To add a library script to the Script tab, follow these steps:

1. Navigate to and select the **Scripts** tab.
2. Click **New Relativity Script**.
3. Choose **Select from Script Library** on the **Script Type** field.
4. In the **Relativity Script** field, click **Select**, and choose the library script you want to add.
5. Click **Save**.
   The script information screen appears.
6. In the Script console, click **Run Script**.
   The script appears in your Script tab. In addition, Relativity adds the Is Link column to the view and sets it to Yes. When you add a library script to a workspace, it remains linked to the Script Library as indicated in the Is Link column. This column displays No if you add your own custom script to the workspace.

31.6 Running a library script

To run a script, follow these steps:

1. Navigate to and select the **Scripts** tab.
2. Click **Run** next to the script you want to run or open the script and click **Run Script** on the Actions console.
3. Configure the required fields on the script layout.
4. Click **Preview** to display a pop-up of the SQL script, or click **Run** to execute the script.

32 Script groups

You can use script groups in Relativity to create a dashboard view into your scripting activities. Script groups are an extension of the Relativity script page where you can dynamically create script dashboards based on the category specified in the Relativity script XML. These dashboards provide you with a radio button list of all scripts, and they provide a centralized location to run your similar scripts.

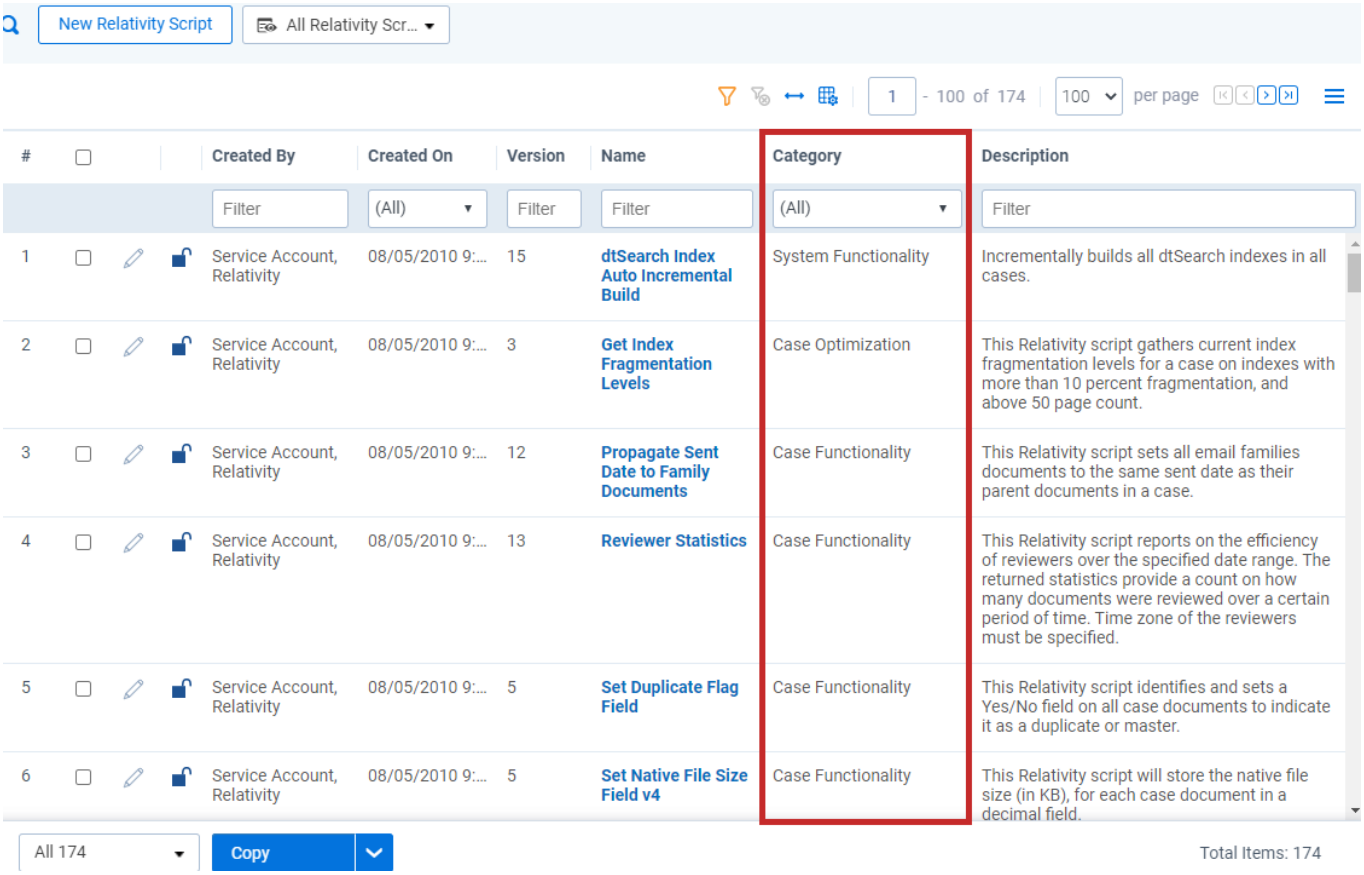
Caution: Changes to SQL fields executed by Relativity Scripts do not produce Audit logs.

See Scripts on page 592 for more information.

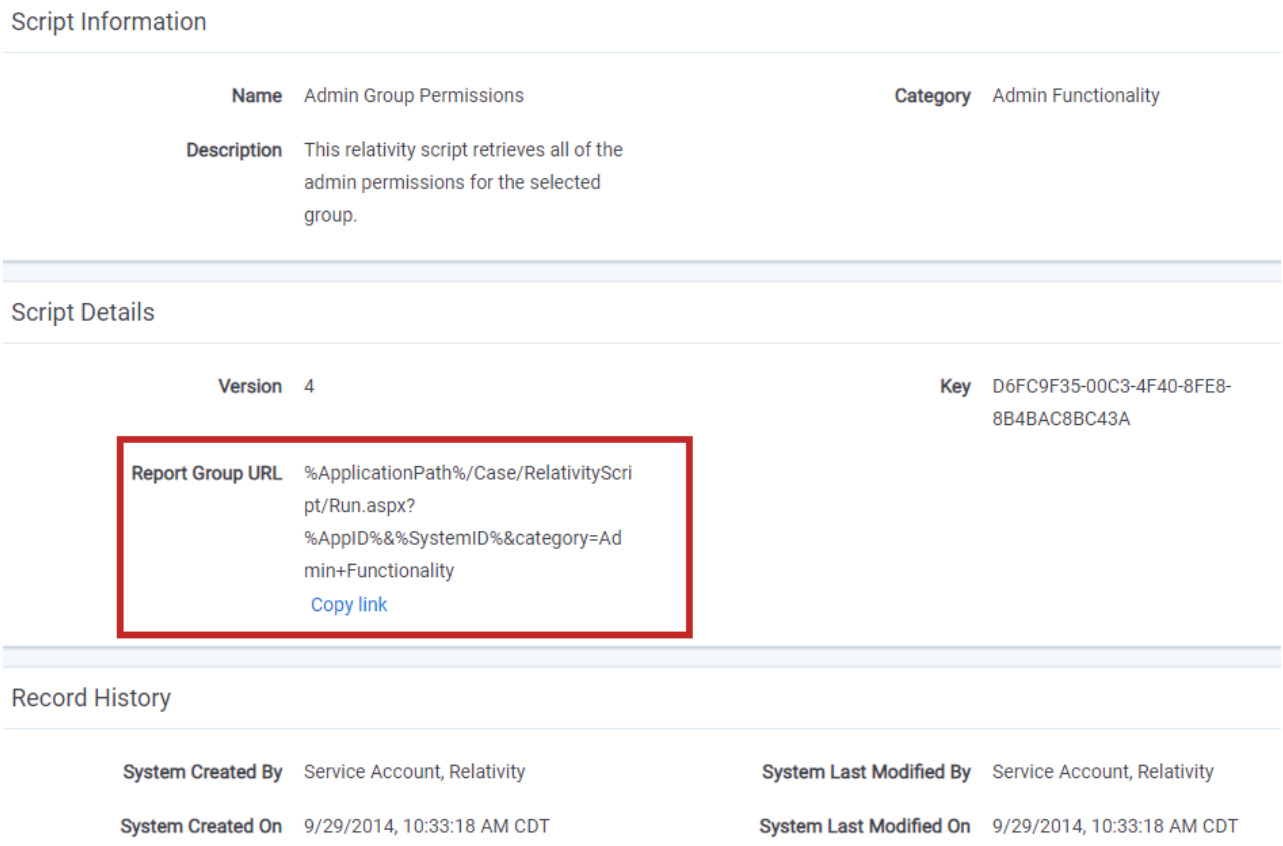
32.1 Setting up a script group

Follow these steps to set up a script group:

1. Create or select a group of Relativity scripts that you would like to add to a script group . They must all share the same Category. You can also create new categories. See Creating a new workspace script on the previous page.



2. Create a new external tab that links to your script group. See Creating and editing tabs on page 689. If the category name contains spaces, replace the spaces with the + sign.
    a. Copy the script category's Report Group URL to your clipboard or Notepad. For example, if you are creating a script group for all scripts whose category is Case Functionality, open any script belonging to this category. Then, copy the entire path listed in Report Group URL.



b. Navigate to **Workspace admin** > **Tabs**, and then select **New Tab**.

c. Enter the following:

- **Link Type** - External
- **Link**- Paste the entire Report Group URL path. It should look similar to the following:
- %ApplicationPath%/*Case/RelativityScript/Run.aspx?%AppID%&%SystemID%&category=Case+Functionality*
- Leave all other fields at default settings.

3. Navigate to the new tab you created for your script group.

Note: Linked scripts can only be members of a script group as an admin tab. You can't create script groups of linked scripts within a workspace.

33 Search terms reports

33.1 Search terms reports

You have reached an outdated topic. See https://help.relativity.com/RelativityaiR/Content/Relativity/Search_term_reports/STR.htm for information on search term reports.

34 Searching

Relativity includes flexible search features designed to facilitate the document review process. These features support a range of searching needs from filtering on fields and simple keyword searches to the development of complex

queries. The following list summarizes the searching features available in Relativity.

34.1 Filters

You can use filters to limit the documents or items that appear in item lists on Relativity tabs and pop-ups. When you enable the filters for an item list, you can set criteria on single or multiple fields so that only matching documents or items appear in the view.

Filters query across the searchable set of documents in the active view to return your results. Relativity supports multiple filter types so that you can choose the best format for different field types. See the Searching Guide for more information.

34.2 Search panel

The search panel is available for the Document list and for many other tabs in Relativity. It allows you to build complex searches by rearranging and visualizing nested conditions by dragging and dropping them. Conditions can be easily set and organized into logic groups, with the logic display at the top of the panel updating automatically to reflect any changes made. You can access your dtSearch and keyword search indexes and fields within the workspace when creating a search.

With the search panel, the search conditions tool allows you to refine searches by selecting fields, operators, and values to customize queries. This tool can be used independently or in conjunction with keyword searches, dtSearches, Analytics, or Cluster visualization. See the Searching Guide for more information.

34.3 Keyword searches

You can run keyword searches from the Documents tab and from Dynamic Object tabs. With these searches, you can leverage the basic functionality for querying the SQL full-text index populated with data from extracted text fields. The keyword search engine supports the use of Boolean operators and wildcards. See the Searching Guide for more information.

34.4 Saved searches

Saved searches give you the functionality to define and store queries for repeated use. With flexible settings, you can create a saved search based on any Relativity search engine, assign security permissions to it, and define specific columns to display your search results. Saved searches support the development of complex queries that you build using a form with search condition options. These queries run dynamically to ensure that updated results appear when you access a saved search. See the Searching Guide for more information.

34.5 dtSearch

Available on the Documents tab, you can use dtSearch's advanced searching functionality to run queries with proximity, stemming, and fuzziness operators, along with basic features such as Boolean operators and wildcards.

System administrators can create a dtSearch index for a specific subset of documents in a workspace, and then assign security to it. They must manually update indexes when you modify the document search sets used to create them. See the Searching Guide for more information.

34.6 Analytics

Supporting conceptual searching, Analytics includes documents in a result set when they contain similar ideas or conceptual relationships, rather than matching specific search terms or conditions.

You can create searches with Analytics that categorize your documents based on the concepts contained in a sample document set. Instead of categorizing documents, you can also perform clustering, which uses specific algorithms, system-defined rules, to identify conceptually related documents. See the Searching Guide for more information.

34.7 Regular expressions

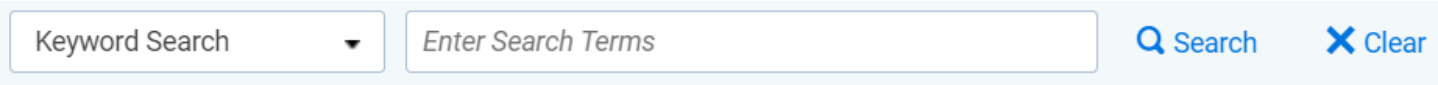
Regular Expressions (RegEx) is a form of advanced searching that looks for specific patterns, as opposed to certain terms and phrases. With RegEx you can use pattern matching to search for particular strings of characters rather than constructing multiple, literal search queries. You can use RegEx with a dtSearch index using dtSearch syntax options to construct complex queries. See the Searching Guide for more information.

34.8 Assist

Assist uses generative AI to help you quickly analyze and understand your document data. Simply ask questions in conversational language to find relevant information in Relativity, such as documents related to specific people, keywords, or topics like bribes or corruption. This helps you identify key documents, clarify communications, and map out relationships and roles among actors. See the Searching Guide for more information.

34.9 Additional features

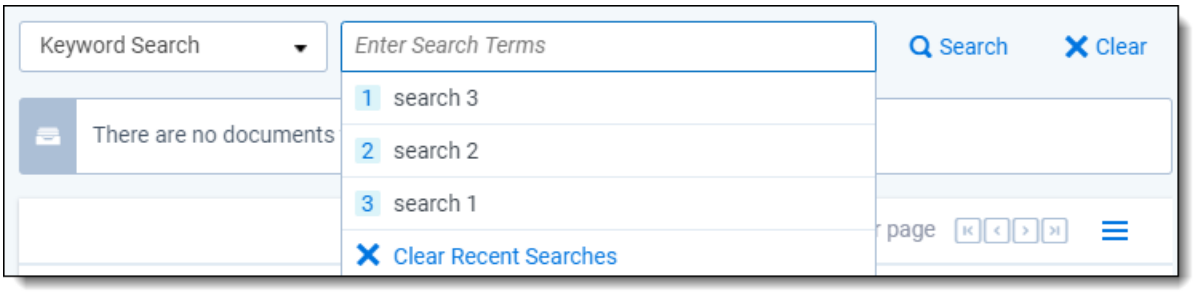
Relativity provides additional features that makes searching easy to use from the Documents tab. Use the **search bar** to run a keyword search query, or click the drop-down list to select another search index you created.



With the *search condition* option, you can build queries using the same condition options available for saved searches.

You can click **Save as Search** on the Documents tab to create saved searches based on the criteria defined for keyword searches, dtSearches, Analytics, or the search conditions option. See the Searching Guide for more information.

You can also use the search bar to view recent searches. Click in the search bar to see up to 10 of the most recent searches from any index in descending order, with the most recently run search first.



Select any search from the list to run that search. To clear the list, click **Clear Recent Searches**.

35 Security and permissions

In Relativity, you can manage security levels for users and system admins, as well as individual objects like views, tabs, and fields. You can assign permissions at the group level and preview effective security rights by impersonating a member of the group or a specific user. If a user belongs to multiple security groups, they'll receive the highest permissions from the combination of groups.

Feature Permission modernization **Feature Permissions modernization:** Learn how modernized Feature Permissions streamline permissions management by making the Features tab the primary way to grant or revoke access for supported features. Includes migration tooling and alignment guidance.

Consider the following:

Note: It's recommended to update security permissions for document folders with a large number of documents during non-business hours to avoid delays in your document review project.

- If the Lockbox feature is enabled via the **EnableCustomerLockbox** instance setting, Relativity system admins must also belong to a group within a workspace in addition to the System Administrators group to access and administer security within that workspace. If you need more information on this feature, please contact Support.

35.1 Levels of Security in Relativity

In Relativity, there are two primary levels of security for assigning permissions: **Object-level** and **Item-level** security. These levels of security control access to either entire sets of Objects or specific Items, depending on their configuration.

Object-level permissions – Serve as a comprehensive setting that applies to all items within a specific Object type.

These permissions are categorized into two main groups:

- **Instance permissions** - these permissions pertain to system admin groups and are used to control access to designated system admin objects.
- **Workspace permissions** - these permissions are associated with user groups added to a particular workspace. If a user group is not added to a workspace, it implies that users within that group have no access to that workspace.

You can employ object-level security to restrict entry to specific documents or items within the workspace. These objects encompass various components such as workspaces, documents, fields, and other elements within the system.

Tailoring access to these objects can be done on an individual user or group basis. User access determines the extent of permissions and actions a specific user can perform. Group access simplifies the management of permissions for a set of users in the same category. By managing user or group access, you can determine who is authorized to view, edit, or carry out specific actions on the objects within the system.

Furthermore, objects can have document-level or field-level permission configurations. Document-level permissions allow you to control access to individual documents based on user roles or specific criteria. Similarly, field-level permissions offer the ability to regulate access to particular fields within a document. You can set restrictions on who is permitted to view or modify specific fields based on user or group permissions.

Note:
The **Manage Object Types** permission grants group members the ability to:

- Create a new tab for a new object type when adding the new object type.
- Automatically gain view, add, edit, delete, and secure permissions for all newly created object types.
- Automatically gain tab visibility for newly created tabs.

Item-level permissions control access to a single item in a workspace, such as one document, view, or OCR set, instead of relying on the permissions set for its object type across the workspace. With item-level permissions, you can:

- restrict an item to specific groups. When you turn on **Override Inherited Security** for an item, only the groups on that item's security list can access it.

- define what each of those groups can do with the item, such as view, edit, delete, or edit its security. Item-level permissions are most often used to give a group less access to an item than it has across the workspace, but you can also give a group more access.

When you turn on **Override Inherited Security** for an item, the item starts with the same permissions as the workspace-level settings for its object type. You can then change the permissions for that item. From then on, the system uses the item-level permissions for that item and ignores the workspace-level settings. For example, if a group has **None** for the OCR Set object at the workspace level, but you add that group to the item-level security of a specific OCR set, users in that group can view that OCR set.

Note: To remove a group's access to an item completely, remove the group from the item using the **Add/Remove Groups** button. You can't set a group's access to **None** on an item. If a group is added to an item, the lowest level of access it can have is **View**.

To change item-level permission settings, you must navigate to the specific document or object and make changes individually.

Note: For examples of scenarios, see Permissions scenarios on page 676

For most object types it is possible to grant to one of six permissions on the Item or Object level.

- **None** - user does not have any access to the object.
- **View** - user has access to view the object. This is the lowest object permission.
- **Edit** - user has access to edit and view the object.
- **Delete** - user has access to delete, edit, and view the object.
- **Add** - user has access to add new objects.
- **Edit Security** - grants users the ability to edit the security of objects.

  Note: For some object types, options will be missing from the above list of permissions. For example, administrators cannot set permissions to 'None' for the 'Users' or 'Views' objects, because it will make Relativity unusable.

  Note: You can't set a group's access to **None** on an item. To remove a group's access to an item completely, remove the group from the item's security instead.

35.2 Instance security

Relativity is modernizing how you manage permissions. The Features tab is becoming the primary way to grant access. As each feature modernizes, Relativity manages its granular permissions from the Features tab. These changes roll out feature by feature over time. The Feature permissions topic explains the model and lists which features are modernized.

With instance security you can apply permissions to system admin groups to limit or grant access to particular system admin objects. You can access the Admin Security dialog from the Instance Details tab on page 299.

Note: Users must be assigned to the following two groups in order to have full system administration access:
1. **System Administrators** - This grants access to all admin-level permissions, such as ARM, queue management, users, and groups tabs.
2. **<Customer Name> Admin Group** - This gives the user permissions to access all workspaces in the instance, unless the workspace was migrated through **ARM** or **Migrate** without the group being properly mapped first.

See the following related pages:

35.2.1 Features

The Features tab lists all features and the permissions they include. For a feature that uses actions, you grant access by selecting actions. An action is the smallest permission unit. For the full model, see Feature permissions.

35.2.1.1 Feature states

A feature shows one of three states for the selected group. The state reflects how many of the feature's actions you select.

- **Disabled** — none of the feature's actions are selected. 
- **Partially Enabled** — some, but not all, of the feature's actions are selected. 
- **Enabled** — all of the feature's actions are selected. 

35.2.2 Granular permissions

Granular permissions
Object Security tab

The Object Security tab lists all system admin objects with their related item-level permissions.

Item-level rights include:

- **None**  —denies users access to the object.
- **View**  —view the object. This is the lowest level object permission.
- **Edit**  —edit and view the object.
- **Delete**  —delete, edit, and view the object.
- **Add**  —add new objects. This icon turns blue when the setting is unsaved; once you click Save, the blue icon becomes grey. This icon turns green when you give users this permission both when the setting is unsaved and saved.
- **Edit Security**  —grants users the ability to edit the security of objects. This icon turns blue if you click twice indicating a not applicable status.

Object Security tab
These are the granular admin objects you can secure for a group.

You can apply system admin permission settings to any of the following objects in the Object Security tab:

Note: Only system administrators can edit the Client and Matter for a workspace. In addition, the **Errors tab** is only available to system administrators.

- **Client** - access to the Clients tab.
- **Group** - access to the Groups tab.
- **Matter** - access to the Matters tab.
- **Relativity Script** - access to the Relativity Script Library tab.
- **Tab Type** - access to the Tabs tab.
- **User** - access to the Users tab.
- **View** - access to the Views tab.
- **Workspaces** - access to the Workspaces tab.
- **Workspace Application** - access to Workspace Applications.
- **Workspace Portal Services**
- **Workspace Portal Services Permission** - allows you to view the workspace names from other instances in Workspace Portal.

Note: The following objects are secured by default and should not be modified. Please contact Relativity Supportif you need to modify these objects.

- **Agent** - access to the Agents tab.
- **Agent Type** - access to the Agent Types page when creating a new agent.
- **Choice** - access to the Choice tab.
- **Error** - access to the Errors tab.

The (Admin) Errors tab has been permanently removed from Relativity aiR, and the ability to read errors through the API has been disabled. Job-specific errors are now addressable directly within your workspaces. For more information, see Errors tab deprecation.

- **License** - access to the License tab. Only full system admins can edit license information.
- **Resource File** - access to the Resource files tab.
- **Resource Pool** - access to the Resource pools tab.
- **Servers** - access to the Server tab.

Note: If you see the Workspace Processing Settings item listed in the object security section of your console, note that this represents an RDO for which there is no front-end implementation. It stores the Invariant StoreID and Data Grid settings for the workspace, but it provides no functionality, and it controls nothing.

35.2.3 Tab Visibility tab

In Relativity, the Tab Visibility setting lets you determine which tabs within the user interface are accessible to specific user groups. This encompasses both parent and child tabs that can be configured for access by these groups. You can enhance user efficiency by combining object security permissions with tab visibility settings. It's essential to understand that tab visibility settings don't alter the permission rights for objects presented on each tab. Instead, they solely govern whether the tab is visible in the navigational menu.

You can make a tab visible to a user even if they lack the necessary permissions to view objects listed on that tab. Nevertheless, it's crucial to understand that tab visibility settings don't restrict access to the objects featured on a particular tab. Users can still access these objects through direct URLs or via the API, even if the tab isn't visible to them in the navigational menu.

Note: Granting tab visibility to a group without view permissions for the object allows users to view the tab but prevents them from taking action. Granting object permissions to a group without tab permissions for the object restricts users from completing required tasks.

Tab Visibility tab list
These are the granular admin tabs you can make visible to a group.

- **Workspaces** - visibility of the Workspaces tab.
- **Administration** - visibility of the Administration tab.
    - **Clients** - visibility of the Clients sub-tab.
    - **Users** - visibility of the Users sub-tab.
    - **Groups** - visibility of the Groups sub-tab.
    - **User Status** - visibility of the User Status sub-tab.
    - **Matters** - visibility of the Matters sub-tab.
    - **Views** - visibility of the Views sub-tab.
    - **Tabs** - visibility of the Tabs sub-tab.
    - **Application Library** - visibility of the Application Library sub-tab.
- **Queue Management** - visibility of the Queue Management tab.
    - **Production Queue** - visibility of the Production Queue sub-tab.
    - **OCR Queue** - visibility of the OCR Queue sub-tab.
    - **Branding Queue** - visibility of the Branding Queue sub-tab.
- **Instance Details** - visibility of the Instance Details tab.
- **Relativity Script Library** - visibility of the Relativity Script Library tab.

  Note: The following tabs are secured by default and should not be modified. Please contact Relativity Support if you need to modify these tabs.

- **Choices** - visibility of the Choices sub-tab.
- **Resource Files** - visibility of the Resource Files sub-tab.
- **License** - visibility of the License sub-tab. Only full system admins can edit license information.
- **Servers** - visibility of the Servers tab.
- **Agents** - visibility of the Agents tab.
- **Resource Pools** - visibility of the Resource Pools tab.
- **Performance Dashboard** - visibility of the Performance Dashboard tab.
    - **Application Performance** - visibility of the Application Performance sub-tab.
    - **Server Health** - visibility of the Server Health sub-tab.

35.2.4 Admin Operations tab

You can alter the following permission settings from the Admin Operations tab of the Admin Security page.

Admin Operations tab
These are the granular admin operations you can grant a group.

- **Access Staging Explorer**- access to Staging Explorer.
- **Change Queue Priority** - access to priority of queues.
- **Force Logout on User Status** - access to the ability to bump users out of Relativity.
- **Manage Object Types** —permission that grants group members the ability to:
  - Create a new tab for a new object type when adding the new object type.
  - Automatically gain view, add, edit, delete, and secure permissions for all newly created object types.
  - Automatically gain tab visibility for newly created tabs.
- **Manage Cold Storage** - grants group members permission to migrate and retrieve workspaces to and from Cold Storage.
- **Send Message** - access to send messages to users in Relativity.
- **Use Quick Nav** - access to the quick nav button.
- **View Admin Repository** - required in order to access tabs and objects from home.

  Note: Users will have access to the Workspaces tab even without the View Admin Repository permission.

- **View Audits** - access to the ability to view audit records on the View Audits tab.

  Note: If you are using Relativity aiR, the following admin operations are secured by default and should not be modified. Please contact Relativity Support if you think you need to access this functionality.

- **Agent Operations** - access to agent operations.

35.2.4.1 A Note on View Admin Repository

The "View Admin Repository" permission is essential for certain features and supported applications to operate correctly. Apart from the specific features that require this permission, it can also be granted to enable users to generate reports and apply filters to Workspace, Client, Matter, User, and Group objects during report setup.

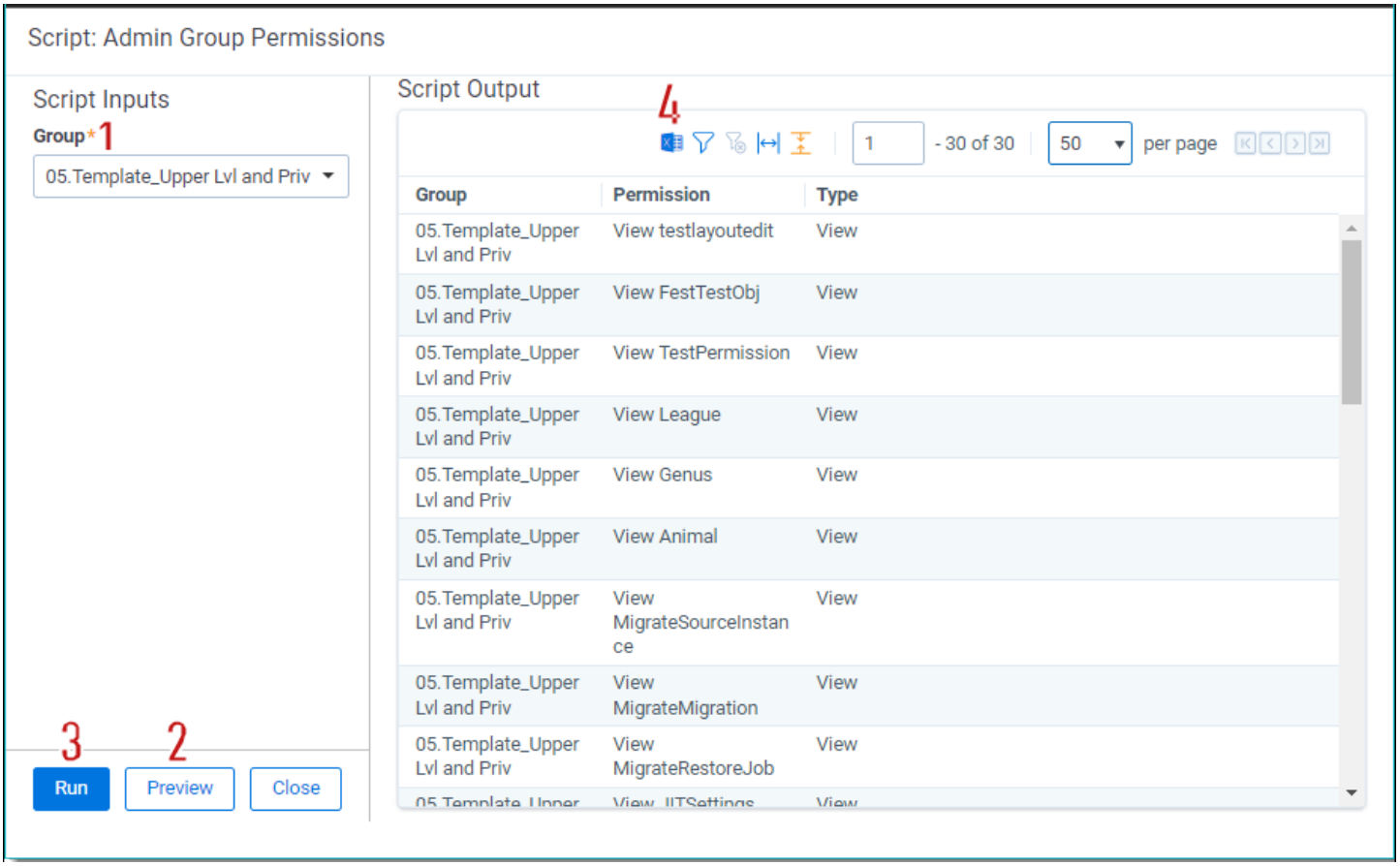
Granting "View Admin Repository" permission to a user provides access to User and Group objects within the platform. This means that these users can retrieve User and Group information, regardless of whether they are using the mobile app.

The following features and supported applications necessitate the "View Admin Repository" permission:

- Case Metrics
- Staging Explorer
- Workspace Portal
- Processing Administration
- Production/Branding Queue
- ARM

35.2.5 Group Permissions report

With the Group Permissions Report you can easily assess all permission settings applied to any group. Navigate to the Instance Details tab and click **Group Permissions Report**.



You can perform the following actions from this console:

1. **Group** - select any group in your Relativity environment from the Group drop-down menu. Click Run to see a list of all system admin permission settings for that group.
2. **Preview** - displays the Script Body that defines the selected group's permission settings.
3. **Run** - generates Group Permissions Report on the selected group.
4. **Export to File** - click Go to export a .CSV file of all the selected group's system admin permission settings.

35.2.5.1 Reading the Group Permissions Report

- **Group** - displays the selected group's name.
- **Permission** - displays the name of the system admin object on which system admin rights are granted for the selected group.
- **Type** - displays the group's permission level on the object listed in the Permission column.

35.2.6 Uneditable admin permission settings for the Everyone group

All users in any instance of Relativity are members of the Everyone group. The following admin permissions apply to the Everyone group by default, and this permission setting configuration is necessary for your Relativity environment to function properly. You can't add or revoke any of the following permission settings on the Everyone group.

Uneditable admin permissions
These admin permissions are fixed for the Everyone group.

- **View User** - visibility of user.
- **View View** - visibility of views.
- **View Code** - visibility of code.
- **View Group** - visibility of groups.
- **View**, **Edit**,and **Add Error** - visibility, edit rights, and add rights to errors.
- **View Relativity Script** - visibility of Relativity script.
- **View Resource Server** - visibility of resource servers.
- **View Tab Type** - visibility of tab types.

35.2.7 Script and application library permissions

System admins are the only users able to access the following items:

Script and application library permissions
These permissions apply to the script and application libraries, for system admins only.

Application Library View:

- **Upload Application button** - access to the button that uploads applications into workspaces.

Application Library Details:

- **Install** - access to the Install button on the Application details screen.
- **Upgrade** - access to the upgrade applications button. This button only appears if an upgrade to the application is available.
- **Cancel** - access to the Cancel button. This button only displays during installation.
- **Push to Library button** - access to the Push to library button.

Relativity Script Library view:

- **New Script button** - access to the New Relativity Script button on the Relativity Script Library tab.

New Script page:

- **Edit button** - access to the Edit button on scripts.
- **Delete button** - access to the Delete button on scripts.
- **Script Header** - access to the Script Header in the XML editor.
- **XML Editor** - access to the XML editor on the New Script page.

Edit Script page:

- **Script Header** - access to the Script header on the Edit Script page.
- **XML Editor** - access to the XML editor on the Edit Script page.

Run Script page:

- **Preview button** - access to the Preview button on the Run Script page.

35.2.8 System administrator privileges

The following actions are exclusive to System Administrators and don't require additional permissions:

- Perform Mass Operations on admin. level objects
- Permanently delete or recover workspaces from the Recycle Bin
- Access to the Errors tab on the Admin. level
- Manage group permissions within Instance details

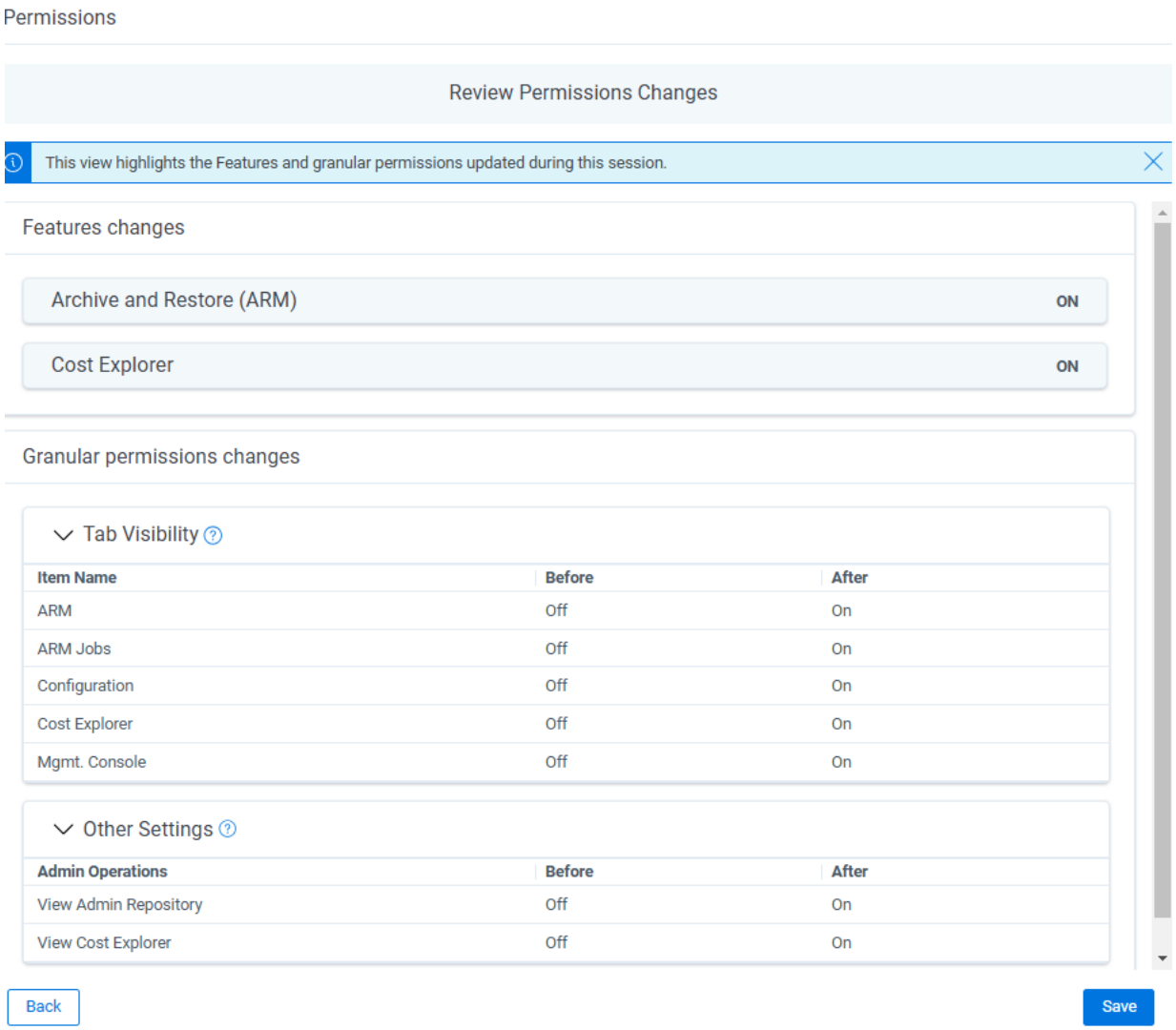
35.3 Setting instance permissions

Permissions can be set based on the features using the Features tab on page 615 or by using the granular settings on the Object Security tab on page 619, Tab Visibility tab on page 620, or Admin Operations tab on page 621.

Edit instance permission settings from the **Instance Details** tab. Access Admin security with the following steps:

1. Click the Relativity logo in the upper left corner or navigate to **Home** with the user drop-down menu.
2. Navigate to **Instance Details**.
3. Click **Manage Permissions**.
4. Click **Edit Permissions** next to the group whose permissions you want to manage.
5. Modify the settings on the tabs as needed. Refer to the Features tab on page 615, Object Security tab on page 619, Tab Visibility tab on page 620, or Admin Operations tab on page 621 sections for specific information of each tab.
6. Click **Revert All** to undo all unsaved changes. Each feature returns to its last saved selections.
7. Click **Review and Save** after modifying settings.

8. Review the unsaved changes displayed on the Review Permissions Changes modal.



   - **Features changes**—lists the features that were changed and how they were changed. Changes at the granular level may affect the status of the feature setting, so review this information carefully.
   - **Granular permissions changes**—lists the changes made at the granular permissions level, including those resulting from feature changes or direct edits at the granular permission level.

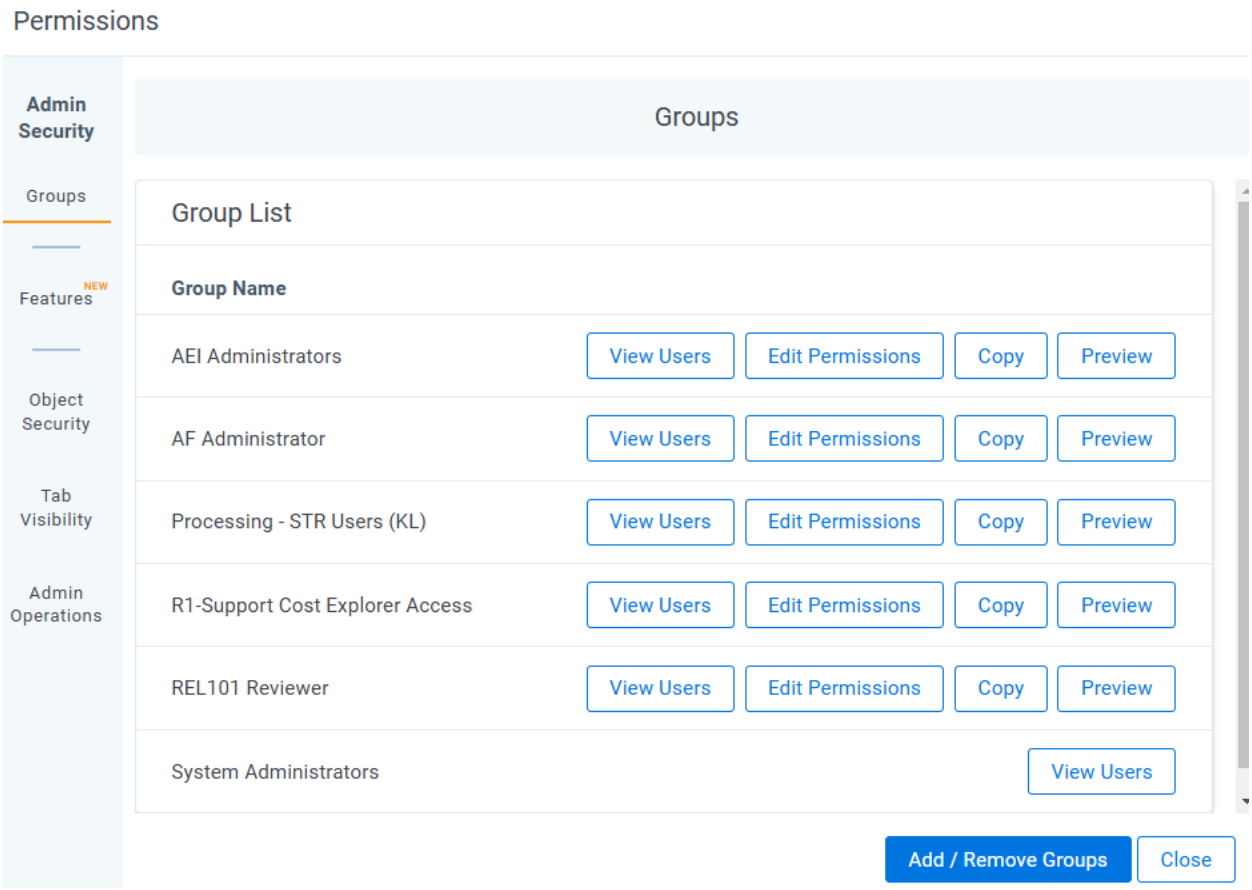
9. Click **Save** to finalize the changes.

From here you can edit the admin permissions of groups.

35.3.1 Groups Management tab

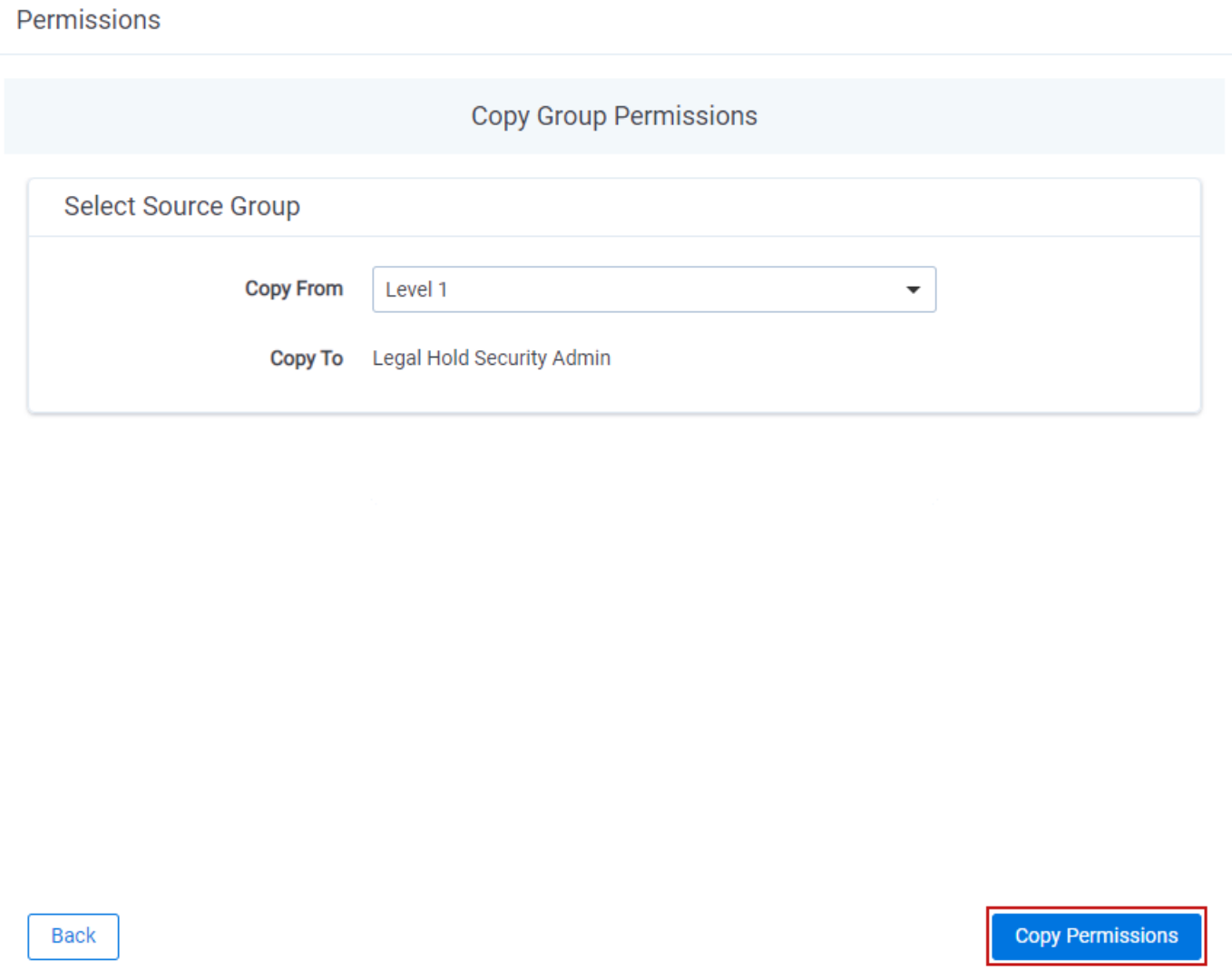
The Group Management tab displays all groups that have admin security privileges.

In the Group Management tab you can view all users in a group, edit the permissions of any group, transfer a group's permissions to another group, or preview a group's current permission settings. The Group Management tab displays all groups that have Admin Security access in Relativity. The following actions are available for groups added to a workspace other than system admins:



- **View Users**—displays a list of users in a group.
- **Edit Permissions**—opens the Object Security tab for editing the admin permissions of a group.

- **Copy**—opens a list of groups whose permission settings you can transfer to the group. Click **Copy Permissions** at the bottom of the list to complete the transfer.

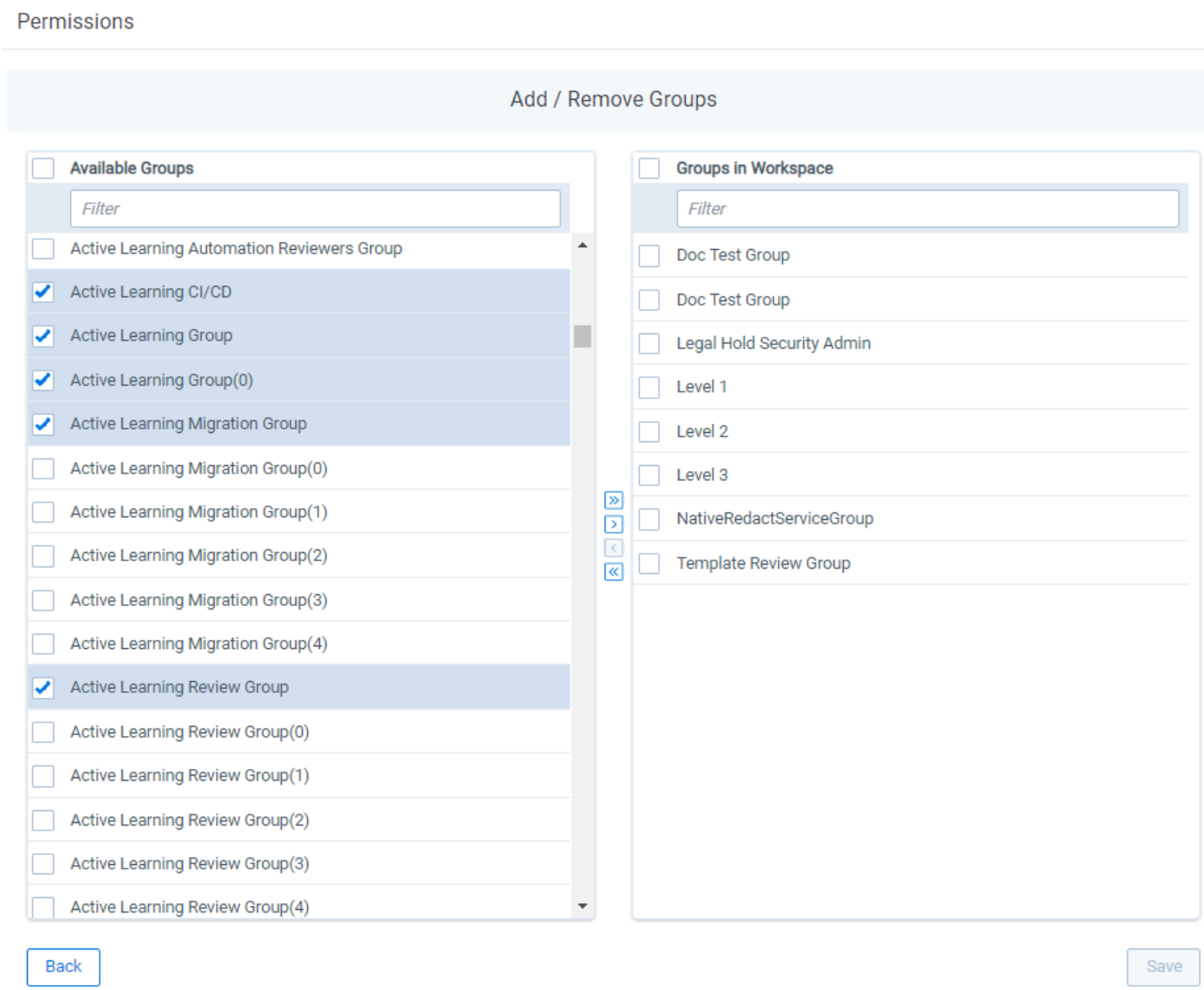


- **Preview**—preview currently applied security settings for a group. See Preview Security for more information.
- **Add/Remove Groups**—opens the Add/Remove Groups dialog to grant admin access to groups. See Add/Remove Groups below for more information.

Note: A system admin is the only user able to grant other users membership into the System Administrators group. Any user who is not a member of the System Administrators group is unable to add themselves to any group.

35.3.1.1 Add/Remove Groups

Click the Add/Remove Groups button on the Group Management tab of the Admin Security window to access the Add/Remove Groups window. The Group Management page displays all groups that exist in your Relativity environment.



The Add/Remove Groups window displays the following lists:

- **Available Groups**—lists groups in your Relativity environment not yet granted access to the workspace.
- **Groups with Admin Permissions**—lists groups granted access to admin permissions.

You must add a group to the Groups with Admin Permissions column to grant the group admin security privileges.

Adding groups to the Groups with Admin Permissions column

To add admin permissions to a group, follow these steps:

1. Navigate to **Instance Details**.
2. Click **Manage Permissions**.
3. Click **Add/Remove Groups**.
4. Scroll through the Available Groups list or search for a specific group using the search bar.
5. Select one or more groups from the Available Groups list in any order.

6. Click **Add**.
7. Click **Save**.

Removing groups from the Groups with Admin Permissions column

To remove admin permissions from a group, follow these steps:

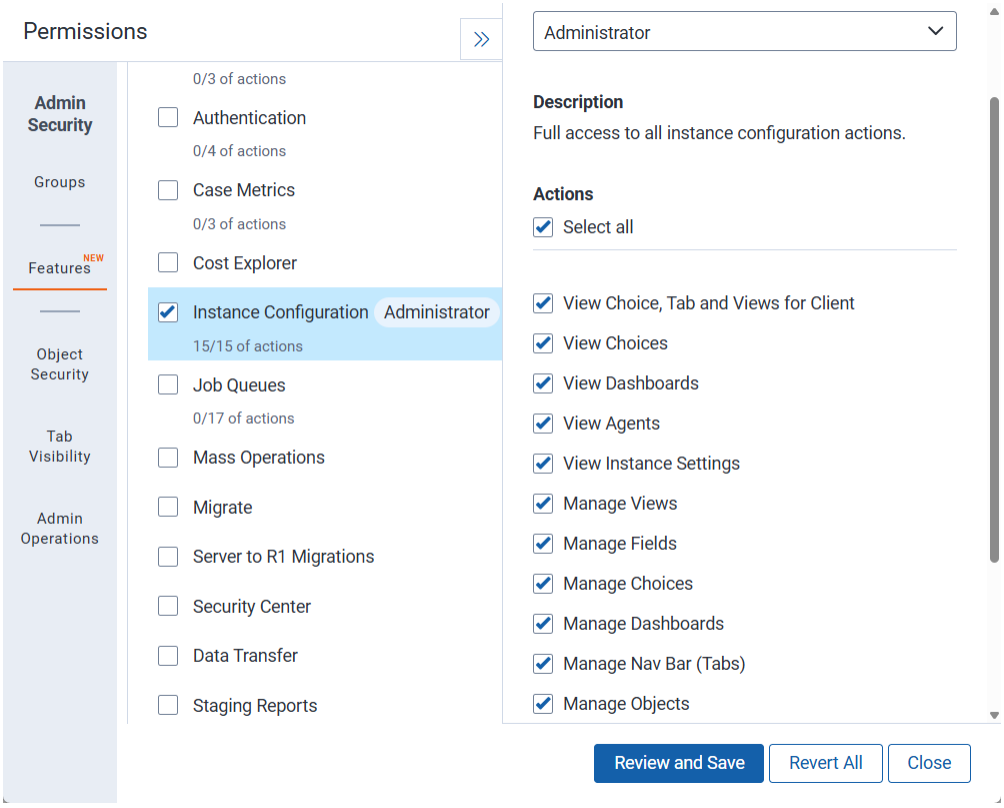
1. Navigate to **Instance Details**.
2. Click **Manage Permissions**.
3. Click **Add/Remove Groups**.
4. Scroll through the Groups with Admin Permissions list or search for a specific group using the search bar.
5. Select one or more groups from the Groups with Admin Permissions list in any order.
6. Click **Remove**.
7. Click **Save**.

35.3.2 Features tab

The Features tab groups related permissions into features. You can grant a whole feature, or grant specific actions within it, without setting each permission on the Object Security, Tab Visibility, and Admin Operations tabs.

Each feature includes specific actions, which represent individual tasks users can perform within that feature. Granting access to actions lets you control permissions more precisely, allowing a group to perform certain tasks without providing full access to the entire feature.

A feature or action combines the required permissions drawn from the other three tabs. When you select a feature, Relativity applies the permissions its actions require. For an overview of features and actions, see Feature permissions, Feature actions.

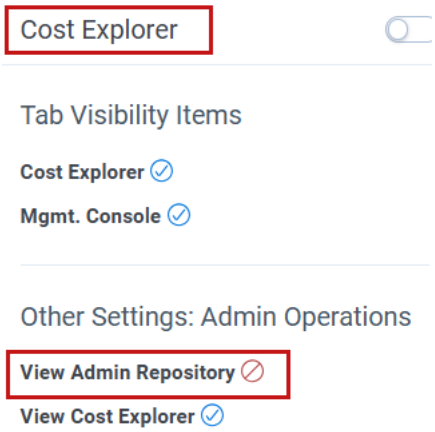


35.3.2.1 Considerations

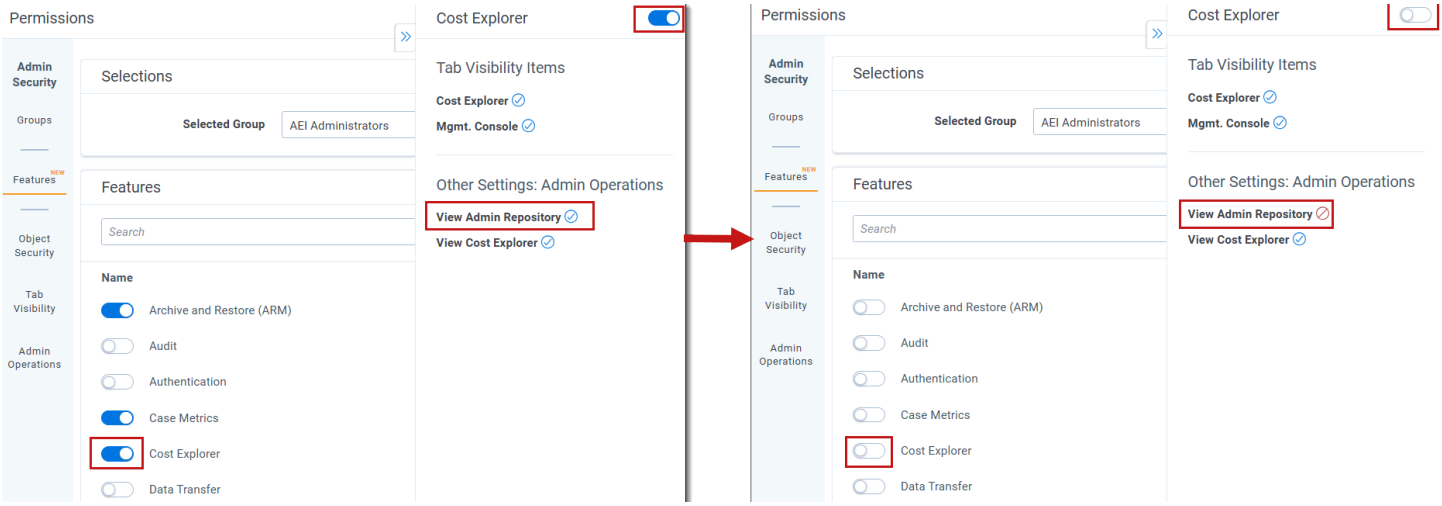
Keep these factors in mind when setting Feature permissions:

Granular permission settings on the Object Security, Tab Visibility, and Admin Operations tabs are the primary source of truth and propagate to features listed on the Features tab. Changes to these permissions from those tabs will also update in the corresponding features.

Scenario:
Changing a specific permission under the Object Security, Tab Visibility, and Admin Operations tab associated with an enabled feature will result in the feature being disabled.
If you remove the View Admin Repository capability on the Admin Operations tab, it will be disabled within its corresponding Cost Explorer feature on the Features tab.



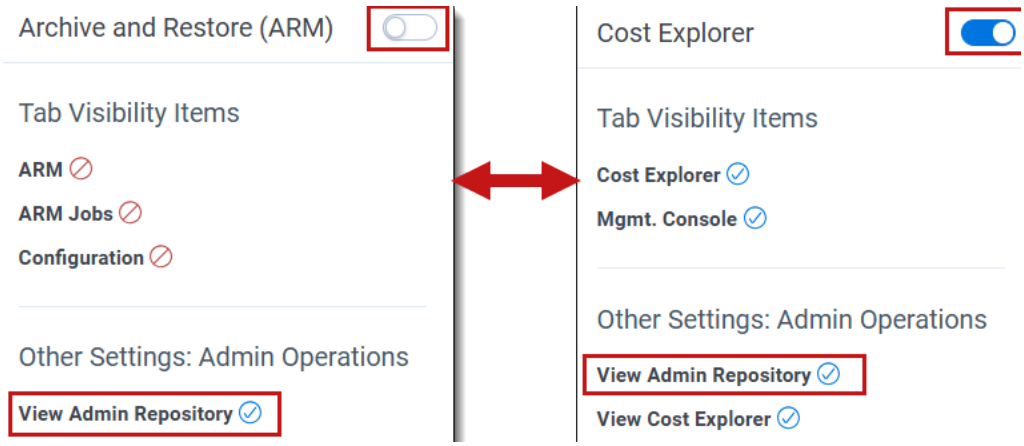
Scenario:
Disabling a feature on the Features tab disables its associated granular permissions for that feature. However, if a granular feature is part of another enabled feature, then it will remain enabled (blue check mark) on the disabled feature's See Details panel.
If the Cost Explorer feature is enabled on the Features tab and you disable View Admin Repository on the Admin Operations tab, the Cost Explorer feature on the Features tab is automatically disabled. Additionally, any other feature that included the View Admin Repository capability is also disabled.



Therefore, if all granular permissions are enabled for a feature, the feature's toggle is enabled. If any of the granular permissions is disabled for a feature, the feature's toggle is automatically disabled.

Scenario:
Disabling a feature revokes access to all granular permissions associated with the feature that are not currently granted as part of a different enabled feature. Therefore, enabling and then disabling a feature will not necessarily return the group to the state it was previously in. Be sure to examine the Review Permissions Changes dialog to

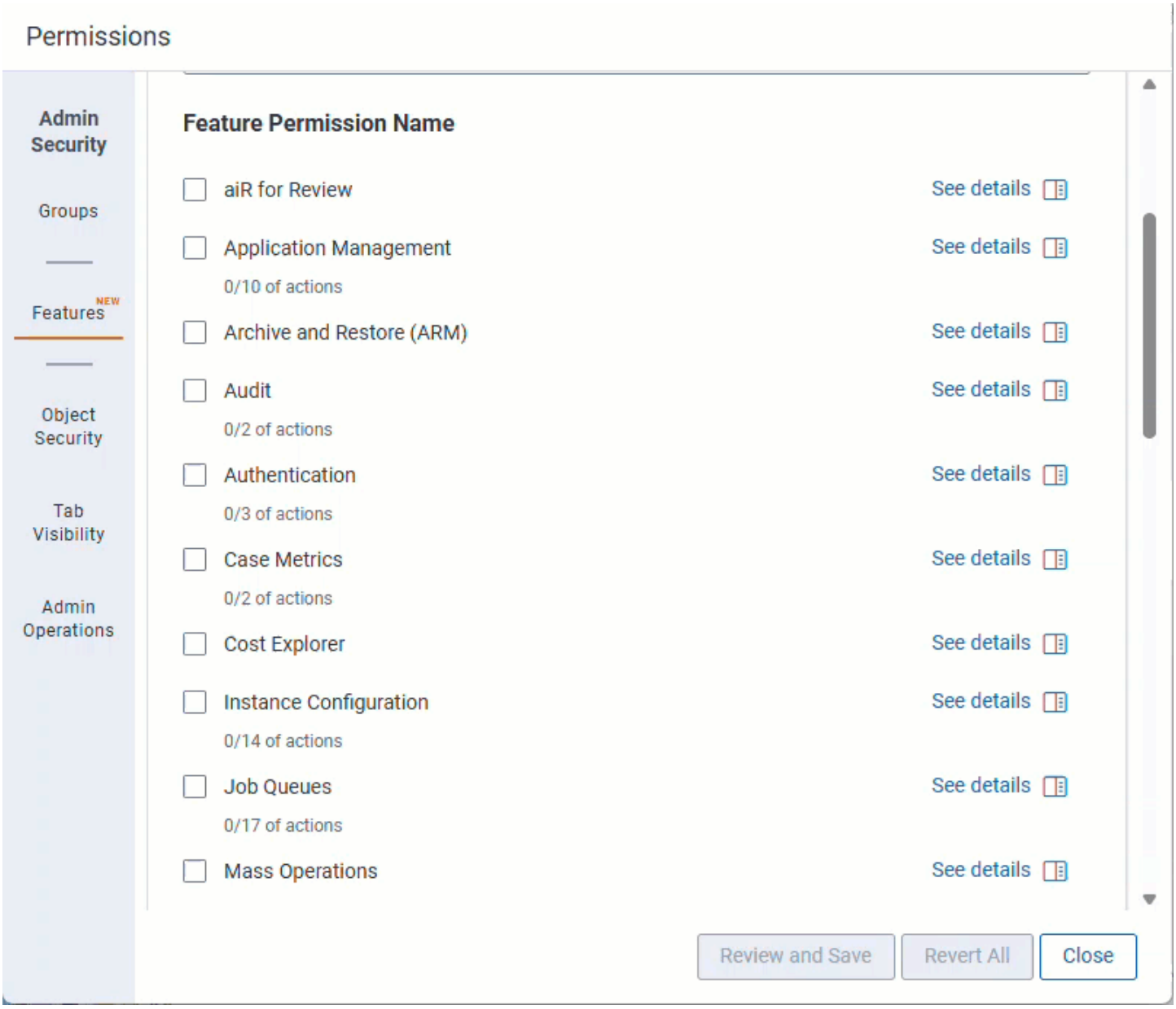
confirm all permissions changes are as expected.
The Archive and Restore (ARM) and Cost Explorer features are enabled, and they share the granular permission of View Admin Repository. If you disable the Archive and Restore (ARM) feature, the View Admin Repository setting remains enabled (blue check mark) on the See Details panel of Cost Explorer because they are included in the enabled Cost Explorer feature.



Scenario:
A group has access to two permissions. If you enable a feature for that group which includes those two permissions as well as two additional permissions, the group will then have access to all four permissions.
Subsequently, if you disable the feature for the group, all four permissions will be disabled for the group (assuming none of the permissions are part of another enabled feature). The group will not revert to having access to the original two permissions.

35.3.2.2 Using the Features tab

The Features tab lists the features available for the selected group. Select a feature's checkbox to grant all of its actions. Clear the checkbox to remove them. To grant specific tasks, select individual actions, or apply a preset from the Preset list. You can also do the following:

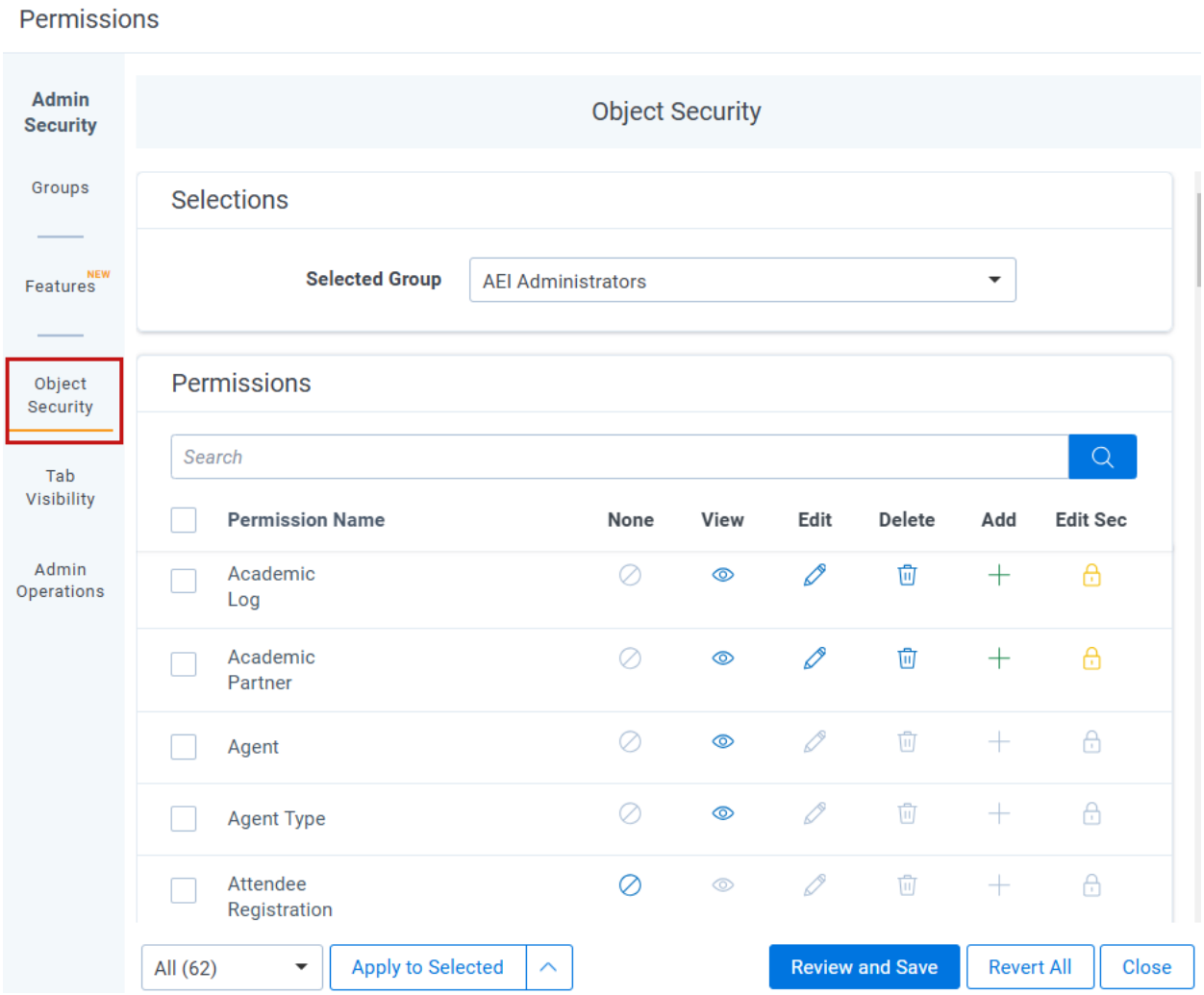


- Use the **Search** bar to locate a particular permission in the list.
- Click **See Details** for a feature to open its details panel. The panel includes:
  - **Preset—** an optional starting set of actions, such as Viewer or Administrator. Select a preset, then select or clear individual actions before you save. Not all features have a preset.
  - **Description —** appears under the preset and summarizes the access the selected preset grants. It changes when you select a different preset.
  - **Actions —** the individual tasks in the feature. Select Select all to include every action, or select actions individually.
  - **Granular permissions mapping —** a read-only reference to the permissions behind the feature. Click Granular permissions mapping at the bottom of the panel to open it. Expand an action to see the permissions it maps to. These come from the Object Security, Tab Visibility, and Admin Operations tabs. Icons show whether each permission is granted, not granted, or shared across features.

35.3.3 Granular permissions

Granular permissions
Object Security tab

With the Object Security tab you can grant admin permissions to Relativity objects.



You can apply the following group permission settings to any Relativity object in the Object Security window:

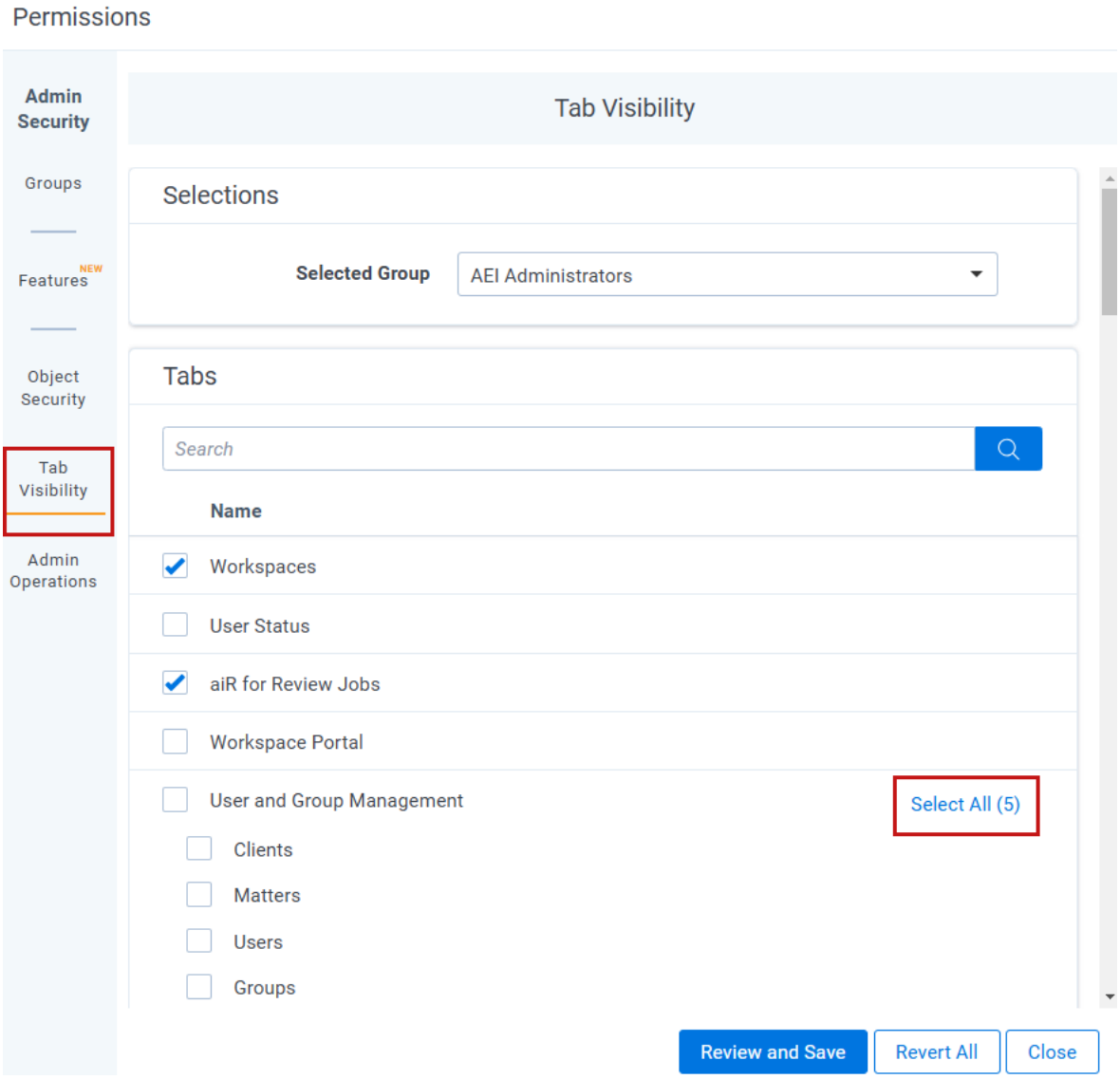
- **None**  —denies users access to the object.
- **View**  —view the object. This is the lowest level object permission.
- **Edit**  —edit and view the object.
- **Delete**  —delete, edit, and view the object.

- **Add** —add new objects. This icon turns blue when the setting is unsaved; once you click Save, the blue icon becomes grey. This icon turns green when you give users this permission both when the setting is unsaved and saved.
- **Edit Security** —grants users the ability to edit the security of objects. This icon turns blue if you click twice indicating a not applicable status.

See Workspace security on page 622 for a complete list of objects and the impact of each assignable security permission.

35.3.4 Tab Visibility tab

With the Tab Visibility tab you can grant a group permission to view admin tabs.

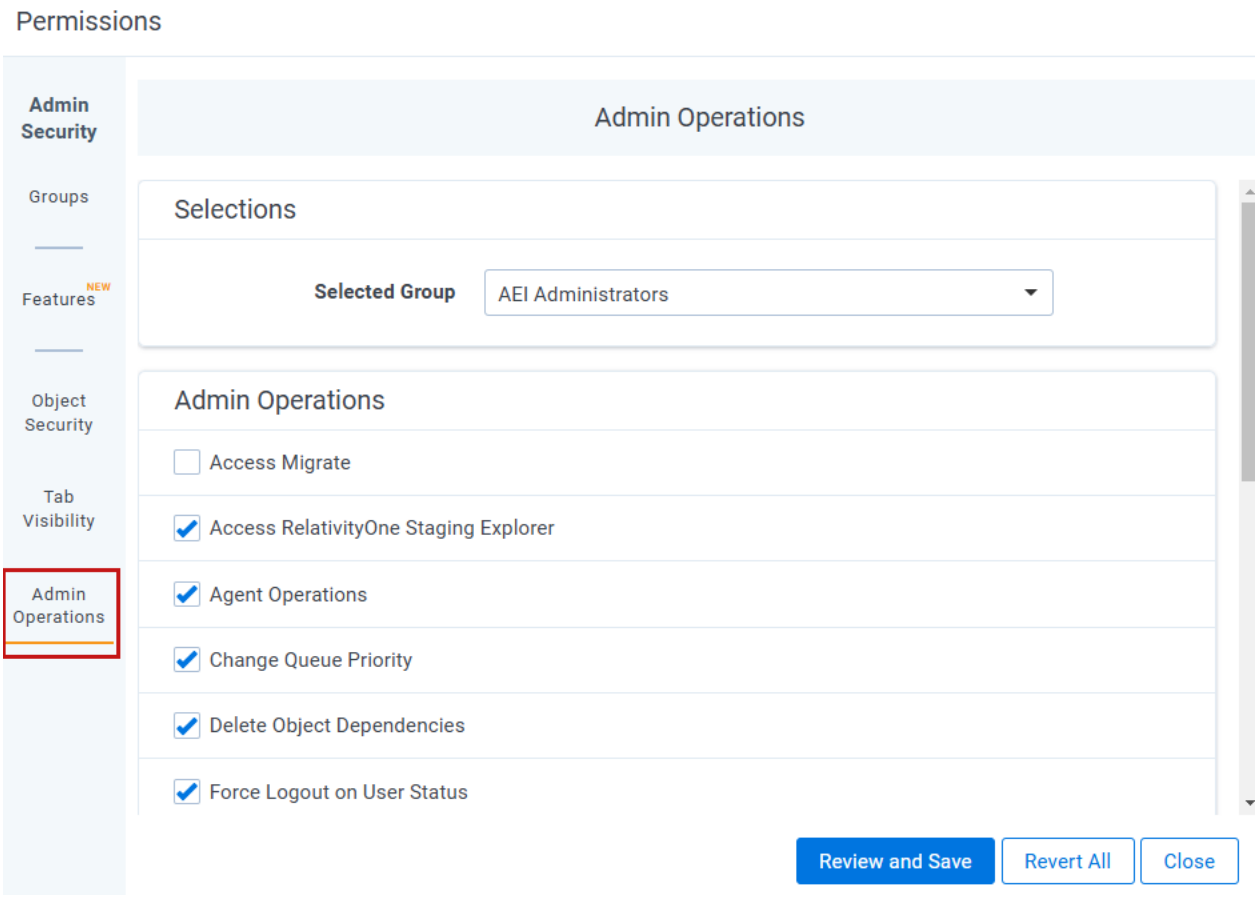


You must grant tab visibility independent of permission settings for users in a group to access a permitted tab. You can make any tab visible by selecting the checkbox in the list. To make all sub tabs visible, click on the parent tab and click **Select all (#)**.

Note: Do not use tab visibility as a sole method of preventing security permissions.

35.3.5 Admin Operations tab

With the Admin Operations tab you can grant admin action permissions to particular groups. See Admin Operations tab on page 607 for a complete list of actions you can grant through this tab.



Note: For more scenario examples, see Permissions scenarios

35.3.5.1 Frequently asked questions

Will I be able to continue to use granular permissions for certain use cases?
Yes, you will be able to continue to use granular permissions. While Feature Permissions is designed to eliminate the need to manage permissions at the granular level via the Object Security, Tab Visibility, and Admin Operations tabs, we understand that there may be unique situations which require the use of the more granular method. Therefore, that functionality will remain in Relativity aiR for the time being.

Why is the user not seeing a tab that should be available as part of the enabled feature?
First, ensure the user has Tab Visibility by looking for a blue check mark next to the tab name in the See Details pane of the feature. If confirmed and still not visible:

1. Check item-level Security: if the tab is secured against the selected group, it will not be available in the application.
2. Check the tab configuration: if the tab's parent is not visible, it will not appear in the side panel or hamburger menu, but it will still be accessible via Quick Nav.

Why are certain features not available in my instance?

Feature availability is determined by your instance configuration. Features will only show when the relevant applications are installed in the instance. If any necessary components are missing, the feature will not be available.

I had enabled a Feature for a specific group earlier, but now it appears as disabled for that same group. What could have caused this?

Although this situation should be rare, it can occasionally arise. This typically occurs when the feature definition is changed to include a permission that the group does not have, often because a new permission has been introduced to the system. To resolve this issue, re-enable the feature for the affected group.

35.4 Workspace security

Relativity is modernizing how you manage permissions. The Features tab is becoming the primary way to grant access. As each feature modernizes, Relativity manages its granular permissions from the Features tab. These changes roll out feature by feature over time. The Feature permissions topic explains the model and lists which features are modernized.

Relativity's security rights are highly customizable. Each group you add to a workspace can have vastly different permissions than others. You can also copy an existing group's permissions to save time on configuring them.

You set group permissions when adding a group to workspace, but you can change these permissions at any time from the Workspace Details page.

Note: If you assign admin permissions to a user group by copying permissions from system admins, you must unset and reset the View Workspace permission to allow the user group to edit the workspace.

Note: When the Customer lockbox feature is enabled, Relativity system admins must also belong to a group within a workspace in addition to the System Administrators group to access and administer security within that workspace. Refer to Support if you need more information on this feature.

35.4.1 Features

For the list of features available at the workspace level and the permissions each one includes, see Workspace-level permissions in Feature permissions.

35.4.2 Legacy granular permissions

Legacy granular permissions

35.4.2.1 Object security

The Object Security tab lists all workspace objects with their related item-level permissions. Item-level rights include:

- **None**  —denies users access to the object.
- **View**  —view the object. This is the lowest level object permission.
- **Edit**  —edit and view the object.
- **Delete**  —delete, edit, and view the object.

- **Add**  —add new objects. This icon turns blue when the setting is unsaved; once you click Save, the blue icon becomes grey. This icon turns green when you give users this permission both when the setting is unsaved and saved.
- **Edit Security**  —grants users the ability to edit the security of objects. This icon turns blue if you click twice indicating a not applicable status.

Not all item-level rights apply to select objects. Some object permissions require corresponding tab visibility or browser permission. For example, a group with all item-level rights assigned for the Field object can only add, edit, delete, or edit security for fields with access to the Fields tab.

Note: When **Override Inherited Security** is on for an item, the system uses that item's item-level permissions instead of the object-level permissions. For more information, see Item-level permissions on page 679.

Note: Once a workspace is created, only System Administrators and Client Domain Administrators can make updates to the Matter object. Even users with full permissions for Matters and Clients will not have the ability to modify this object unless they are System Administrators or Client Domain Administrators.

35.4.3 Object list

The following is a list of common securable objects in a Relativity workspace. Objects with sub-options, related tab visibility permissions, or specific effective rights state the related requirements and rights.

Note: This list contains objects related to core functionality, and additional objects may be described in the documentation for individual features. This list also does not include custom objects you may find in your environment.

These are the granular objects you can secure for a workspace group.

- **Alias**—a textual representation of an author. Aliases are identified during the Analytics name normalization operation.
- **Analytics Categorization Result**—an object that displays the results of an Analytics categorization set.
- **Analytics Categorization Set**—a group of parameters used for gathering example documents that Analytics uses as the basis for identifying and grouping other conceptually-similar documents.
    - Viewing, editing, deleting, or adding Analytics categorization sets, or editing security of Analytics categorization sets requires access to the **Analytics Categorization Set** tab.
- **Analytics Categorization Set Build History**—a record of the historical actions and changes made during the process of creating or updating a categorization set for use in analytics. This history may include information about changes to categories, mappings, and other settings related to the categorization set.
- **Analytics Category**—an object in Analytics that define the categories specific to your analytics set.
    - Viewing, editing, deleting, or adding Analytics categories for Analytics categorization sets, or editing security of Analytics categories requires access to the **Analytics Categorization Set** tab.
- **Analytics Example**—a document that Analytics uses to run the Analytics set against to set a baseline.
- **Analytics Index**
    - Search index permissions must be kept in sync with permissions on the Analytics Index object. If a user has view permissions to Search Index, but no permissions to Analytics Index, they can still access Index Search functionality in the item list and in the viewer. If a user has full View/Edit/Add/Delete

security permissions to an Analytics Index, but does not have permissions for Search Index, they will not be able to View/Edit/Add/Delete Analytics indexes.

- **Analytics Profile**—a group of parameters used for specifying an Analytics Index's dimensions, concept noise words, dtSearch noise words, and filter configurations.
    - Editing, deleting, or adding Analytics profiles, or editing security of Analytics profiles requires access to the **Analytics Profiles** tab.
- **Application Field Code**—an identifier assigned to a specific field within an application. The field code is used to reference and manipulate the field's data.
- **Audit Dashboard**—a visual display that provides an overview of audit-related information, including tracked activities, user actions, and system changes. The audit dashboard allows users to monitor and analyze audit data for compliance and security purposes.
- **Audit Workspace Setting**—a configuration within a Relativity workspace that defines how audit-related activities and changes are tracked and recorded. This setting determines which actions are logged and the level of detail captured in the audit trail.
- **Batch**—a group of documents assembled based on criteria that an admin sets and then assigns to a reviewer for review.
    - Edit—group members can view, check out, and edit batches.
    - Delete—group members can view, edit, and delete batches.
    - Viewing and checking out, editing, available batches requires access to the **Review Batches** or **Batch Sets** tab.
    - Adding batches requires access to the Batch Sets tab.
    - Editing security on batches requires access to the **Review Batches** or **Batch Sets** tab.
- **Batch Set**—the set to which the batch belongs.
    - Using any Batch Set permissions requires access to the **Batch Sets** tab.
- **Batch Set Cleanup**—the process of removing or cleaning up residual data, jobs, or elements associated with batch sets. This cleanup ensures that unused or outdated batch-related information is removed from the system, optimizing performance and resource usage.
- **Catalog Field**—a field within a catalog that contains metadata or attributes associated with a specific item, document, or data entry. Catalog fields are used to organize, categorize, and manage information within catalogs.
- **Choice**—a value applied to a single or multi-choice list field that is used in coding fields to allow reviewers to record decisions on a document.
    - Editing, deleting, or adding choices, or editing the security for choices requires access to the **Choices** tab.
- **Cluster Set**
    - Permissions for Cluster Set and the multiple choice fields that hold cluster data should be kept in sync. If a group has the None permission set on the Cluster Set object, but View/Edit/Add/Delete permissions to the Multiple Choice fields that hold cluster data, users in that group will still see Analytics clusters in the cluster browser and will be able to visualize clusters. To prevent the group from viewing the clusters in the cluster browser, or visualizing clusters, you must item-level secure the multiple choice fields that hold the cluster data for the group.
- **Color Map**
    - Email thread visualization requires View permissions or higher for the Color Map object.

- **Custom Page**—a custom web page created that enhances the flexibility of application development by supporting the creation of custom layouts and the display of dynamic content, such as unique graphics, dynamic date, and report results.
- **Data Grid Audit**—the recording and tracking of changes made to data grid fields within a Relativity workspace. Data grid audits capture modifications to data entries in data grids, providing an audit trail of changes for compliance and accountability purposes.
- **Data Grid Audit Field Mapping**—a configuration that defines the relationship between data grid fields and their corresponding audit fields. This mapping ensures that changes made to data grid fields are accurately captured and recorded in the audit trail.
- **Dashboard**—a page configuration made up of widgets and item lists.
- **Destination Workspace**—the Destination Workspaces tab in the Integration Points object, which provides information on the workspaces to which users have exported data through Integration Points. Note that this setting has no impact on the Destination Workspace field on the Connect to Source layout of the Integration Point you are creating or editing. This means that you can still select a workspace from that field drop-down list even if you do not have permission to this object.
- **Document**—a record within a workspace.
    - **Upload Image**—group members can use the image upload functionality in the viewer to upload a single image.
    - **Replace Document**—group members can replace a single document in the viewer.
    - **Create PDF**—group members can print and save as PDF individual documents from Relativity.
    - **Local Access** (Download; Copy Text)—group members can open the file in its native application or to copy text from the viewer. This permission does not prevent users from being able to download the native file on an RDO using the Document actions menu in the Viewer.
    - **Redact Document**—group members can place stamp or text box redactions on a document.
    - **Highlight Document**—group members can place a highlight on a document.
    - **Add Image**—group members can use Relativity's image-on-the-fly functionality.
    - **Delete Image**—group members can delete images in Relativity.
    - **New Document**—group members can upload a new document.
    - **Case Dynamics - Coding Pane**—group members can use the Case Dynamics coding pane.
    - **Review Interface Settings** —The section within a document's settings that pertains to configuration options specific to the review interface. This subsection allows users to define how the document behaves and appears during the review process.

      Note: Use the document **Edit** permission to tag documents with workspace coding values using layouts. Do not assign coding users rights to edit fields or edit layouts. Use the **Field** edit permission, along with access to the **Fields** tab, to edit field properties such as changing a fixed length text field from 255 to 320 characters.
- **Domain**—the name of the business or organization on the internet. For example, "@company.com" in the email address "jsmith@company.com" is the domain for that company email address.
- **Entity**—the individuals or entities who own or facilitate the data found in the data sources.
    - Group members can view, add, edit, and delete the entities used for Relativity Processing, Legal Hold, and Collection, and Analytics.

- **Event Handler**—the name of the assembly that helps facilitate the completion of document review and various other functions in Relativity by applying custom business logic to corresponding user actions.
- **Field**—the Relativity entity used to store document metadata and coding values within Relativity.
    - **Add Field Choice By Link**—exposes the **Manage** link option on choice fields, allowing group members to add new choices to a field on a layout.
    - Editing, deleting, sorting, or adding fields, or editing the security of fields requires access to the **Fields** tab.
- **Field Category**—a grouping or classification of related fields within a workspace. Field categories help organize fields based on their purpose or functionality, making it easier to manage and work with a large number of fields.
- **Filter Set**—a predefined set of criteria used to filter and narrow down data displayed in views and reports. Filter sets allow users to quickly apply specific filters to focus on relevant information.
- **Folder**—the name of the container of documents in Relativity that are arranged in a hierarchy in the folder browser.
    - Using any Folder permissions requires access to the **Folder** browser.

    Note: You can customize permissions for individual child folders. This does not change the permissions of a folder's parent, but it can change the behavior of a folder's children, if you configure the children folders to inherit permissions from their parent.

    Note: Changing root folder permissions during import is not a supported workflow.
- **Job History**—the Job History tab in the Integration Points object, which provides information the history of import and export jobs run through Integration Points.
- **Job History Error**—the Job History Errors tab in the Integration Points object, which provides information errors that occurred during import and export jobs run through Integration Points.
- **Imaging Profile**—the name of the profile that controls the settings used to image a group of documents.
    - Editing, deleting, or adding imaging profiles, or editing security of imaging profiles requires access to the **Imaging Profiles** tab.
- **Imaging Set**—the profile and saved search containing the documents you want to image.
    - Editing, deleting, or adding imaging sets, or editing security of imaging sets requires access to the **Imaging Sets** tab.
- **Imaging Warning**—a notification or alert generated during the imaging process that indicates potential issues or discrepancies that may affect the quality or accuracy of the imaged documents.
- **Import/Export Extraction Job**—a task that involves extracting and transforming data during the import or export process. Import/export extraction jobs ensure that data is correctly formatted and mapped for successful transfer.
- **Import/Export Job**—an automated task that facilitates the import or export of data between different instances or systems. Import/export jobs enable efficient data transfer while maintaining data integrity.
- **Install Event Handler**—the name of the pre or post-install event handler, which is an assembly that runs when you install them to configure your Relativity environment to support your applications.
    - Viewing, adding, or deleting event handlers requires access to the **Object Type** tab.

- **Inventory Filter**—the filter applied when inventorying files to view how inventories data affects data in your processing set using the Processing application.
- **Integration Point**—the entity that you create to configure data integrations from third-party systems to Relativity objects using the Integration Points application.
- **Integration Point Profile**—the profile that you create and save for future use when running future data import or export jobs through the Integration Points application.
- **Integration Point Type**—the integration point type, import or export, that you specify when you create an integration point to configure data integrations from third-party systems to Relativity objects using the Integration Points application.
- **Layout**—the name of the web-based coding form that gives reviewers access to view and edit document fields and complete specific review tasks.
    - Editing, deleting, or adding layouts, or editing security of layouts requires access to the **Layouts** tab.
- **Legacy Sentiment Result**—an outcome or classification generated by a sentiment analysis process using previous sentiment analysis models or methods.
- **Lists**—an option for saving a group of items without having to specify the types of conditions required for a saved search, which means they remain constant unless someone replaces them with an existing list.
    - Editing, deleting, or adding lists, or editing security of lists requires access to the **Lists** tab.
- **Markup Set**—a securable sets of annotations and redactions available to reviewers for applying text redactions to documents in the Viewer.
    - Editing, deleting, or adding lists, or editing security of markup sets requires access to the **Markup Sets** tab.

    Note: The only proper way to secure the text behind a redaction is to the produce the document that contains the redacted text. If a group has View rights only to a markup set, not Edit or Delete rights, and a reviewer in that group loads a document in the Viewer because they have no other way to view that document, they can actually see the text behind the redaction, in which case that text is not totally secured.
- **Mass Operation**—single actions performed on multiple documents or objects at the same time, such as mass edit, move delete, produce, replace, image, print image, send to CaseMap export file, cluster, and process transcripts.
    - Viewing, adding, or deleting mass operations requires access to the **Object Type** tab.
- **Native Type**—a Relativity-supported file type that an admin can import and image; Native Type pertains to the Native Types tab and list, which an admin references when selecting file types to restrict from imaging.
    - Edit—group members to edit the **Restricted From Imaging By Default** checkbox for native types.
    - Delete—group members to remove native types from the restricted list.
    - Add—group members to add existing native types to the restricted list.

    Note: Even with all Native Type permissions assigned, a user cannot add new native file types. Relativity is already configured with the native file types that it recognizes.
- **Object Rule**—permits special or additional functions with user-configurable options. For example, a New Button Override that redirects an object's new button action to another Relativity page or other URL as directed by the user.
    - Viewing, adding, or deleting object rules requires access to the **Object Type** tab.

- **Object Type**—the type of object specified when creating a Relativity Dynamic Object. For example, Document and Workspace are object types.
    - Editing, deleting, or adding object types, or editing security of object types requires access to the **Object Type** tab.
- **OCR Language**—determines what language is used to OCR files where text extraction isn't possible, such as for image files containing text.
    - Viewing, editing, deleting, or adding OCR languages, or editing security of OCR languages requires access to the **Processing** tab.
- **OCR Profile**—a saved, reusable set of parameters that you use when creating an OCR set.
    - Viewing, editing, deleting, or adding OCR profiles, or editing security of OCR profiles requires access to the **OCR Profiles** tab.
- **OCR Set**—a group of documents defined by a saved search or production to be OCRed based on the settings defined by the OCR profile.
    - Viewing, editing, deleting, or adding OCR sets, or editing security of OCR sets requires access to the **OCR Sets** tab.
- **Password Bank**—a password repository used to decrypt certain password-protected files during inventory, discovery, and native imaging.
- **Password Entry**—a password you enter into the password bank to decrypt password-protected files.
    - Viewing, editing, deleting, or adding password entries in the Password Bank, or editing security of password entries requires access to the **Password Bank** tab.
- **Persistent Highlight Set**—a reusable, transferable set of persistent highlight specifications a reviewer can select in the Viewer to assist in document review.
- **Pivot Profile**—a saved, reusable group of pivot setting that you apply to pivots to quickly analyze case data.
- **Quick Create Sets**—the Quick Create Sets tab, formerly Processing Assistant, lets you create multiple data sources, entities, and processing sets based on a specific file structure from a single object.
- **PDF Profile**—a configuration that defines settings and parameters for generating PDF documents, including formatting, layout, and content options.
- **Processing Data Source**—all data sources associated with all processing sets in the workspace.
- **Processing Error**—a list of errors related to your processing job.
    - **Download and Upload files with processing sets**—group members can download error files and upload replacements for them through the Error Actions console on the error details layout.
- **Processing Set**—an object to which you attach a processing profile and at least one data source and then use as the basis for a processing job.
- **Production**—an application that prepares relevant and non-privileged documents to turn over to opposing counsel after review.
    - Viewing, editing, deleting, or adding production sets, or editing security of production sets requires access to the **Production Sets** tab.

    Note: Productions appear in the viewer by default. There are no permissions for specific viewer options. To restrict productions from appearing in the viewer for a certain group, set the Production permission to **None**  .
- **Production Data Source**—saved set of parameters that Relativity uses when running a production.

- **Production Information**—information records associated with a production during the Staging process of running a production.
- **Placeholder**—text or images you can include in a production as a placeholder for removed or forthcoming information.
- **Queue Refresh Trigger**—a mechanism within Relativity's Review Center that initiates a process to update the review queue with the latest information.
- **Relativity Application**—a customizable collection of Relativity objects that provides improved case and matter management.
    - Viewing, editing, deleting, or adding Relativity applications , or editing security of applications requires access to the **Relativity Applications** tab.
- **Relativity Export Service Job**—a task initiated to export data from the system using the Relativity Export Service. This job ensures the accurate and secure transfer of data to external destinations.
- **Relativity Import Data Source**—the source of data that is being imported. This can include various file types, databases, or other external sources of information.
- **Relativity Import Job**—an automated process used to import data from external sources into the system. Import jobs facilitate the seamless integration of data for various purposes.
- **Relativity Script**—a SQL-based command that admins can use to customize and augment Relativity functionality. Scripts are deployed with Relativity and reside in the Relativity script library.
    - Viewing, editing, deleting, or adding Relativity scripts, or editing security of scripts requires access to the **Scripts** tab.
- **Relativity Time Zone**—the time zone for which the Relativity environment adheres to.
- **Repeated Content Filter**—a filter that finds the text in each document that matches your configuration parameters and suppresses it from the Analytics index.
    - Viewing, editing, deleting, or adding repeated content filters, or editing security of repeated content filters requires access to the **Repeated Content Filters** tab.
- **Report**—flexible reporting features designed to facilitate roll-ups of information about your case review.
    - Viewing, editing, deleting, or adding summary reports, or editing security of summary reports requires access to the **Summary Reports** tab.
- **Review Center Queue**—a collection of documents within Relativity's Review Center functionality that serve as a central location for reviewers to access and analyze documents relevant to a specific case or investigation.
- **Search**—flexible search features designed to facilitate document review process.
    - Security settings for the Search object apply to saved searches.
    - Editing, deleting, or adding saved searches, or editing security of saved searches requires access to the **Saved Searches** browser.
- **Search Container**—the search folder object, which applies to all saved search folders.
    - Security settings for the Search Folder object apply to saved search folders.
    - Editing, deleting, or adding saved search folders, or editing security of saved search folders requires access to the **Saved Searches** browser.
- **Search Index**—access to searching features, such as dtSearch and other searches available from the Documents tab.
    - Search index permissions must be kept in sync with permissions on the Analytics Index object. If a user has view permissions to Search Index, but no permissions to Analytics Index, they can still

access Index Search functionality in the item list and in the viewer. If a user has full View/Edit/Add/Delete security permissions to an Analytics Index, but does not have permissions for Search Index, they will not be able to View/Edit/Add/Delete Analytics indexes.

  - **Dictionary Access**—group member can see the dictionary function when searching with a dtSearch index.
  - Using available search indexes with dictionary search requires access to the **Documents** tab.
  - Selecting and using available search indexes requires access to the **Documents** tab.
  - Editing, deleting, or adding search indexes, or editing security of search indexes requires access to the **Search Indexes** tab.

- **Search Terms Report**—a tool an admin can use to enter a list of terms or phrases and generate a report listing those words' frequencies in a set of documents.
  - Viewing, editing, deleting, or adding search terms reports, or editing security of search terms reports requires access to the **Search Terms Reports** tab.
- **Search Terms Result**—a list of results from the search terms report.
- **Sentiment Analysis Job**—a task that involves analyzing text data to determine sentiment or emotional tone. Sentiment analysis jobs provide insights into the emotional context of text content.
- **Sentiment Result**—the outcome or classification generated by a sentiment analysis process that indicates the sentiment or emotional tone detected in a text document.
- **Source Provider**—group members can see all available source providers when creating an integration point; for example LDAP, FTP, Import Load file, and Relativity.
- **Structured Analytics Errors**—a list of errors related to your Structured Analytics job.
  Structured Analytics Set—a saved, reusable group of settings that Structured Analytics uses to shorten your review time, improve coding consistency, optimize batch set creation, and improve your Analytics indexes.
- **Tab**—an interface component that gives the admin or reviewer access to an assortment of Relativity functionality.
  - Editing, deleting, or adding tabs, or editing security of tabs requires access to the **Tabs** tab.
- **Tab Sync Backup**—a backup mechanism that ensures the consistency and synchronization of data across different tabs or sections within the user interface.
- **Trained Model**—a machine learning model that has been trained using specific data to make predictions or classifications based on new input.
- **Transform Set**—a feature that uses handlers to analyze and extract the contents of one field and copy them to another.
  - Viewing, editing, deleting, or adding transform sets, or editing security of transform sets requires access to the **Transform Sets** tab.
- **View**—a customizable list of items in Relativity from which a user can sort and filter to locate specific items.
  - Editing, deleting, or adding views, or editing security of views requires access to the **Views** tab.
- **Workspace**—a securable document repository used to facilitate productions, witness testimony, and other documents in which admins and reviewers conduct searches for relevant materials and set up views to organize that material.
  - Editing or deleting a workspace, or editing security of a workspace requires access to the **Workspace Details** tab. When the edit security permission is selected, it grants the group the ability to manage permission and the Add/Remove Groups button will display.

    - The Workspace Details feature grants these permissions through its actions. The View Workspace Details action grants View, and the Manage Workspace action grants View, Edit, Delete, and Edit Security. See Feature permissions.
- **Workspace Processing Settings**—Represents an RDO for which there is no front-end implementation. It stores the Invariant StoreID and Data Grid settings for the workspace, but it provides no functionality, and it controls nothing.
- **Note:** If you are using Relativity aiR, the following objects are secured by default and should not be modified. Please contact Relativity Support if you need to modify these objects.
- **Agent Type**
- **Event Handler**
- **Install Event Handler**
    - Viewing, adding, or deleting event handlers requires access to the **Object Type** tab.
- **Processing Error**

35.4.3.1 Tab visibility

These are the granular tabs you can make visible to a group. The following list shows common Relativity parent and child tabs, in alphabetical order by parent tab name.

- **Workspace Admin**
    - **Workspace Details**

      Note: If a user has view access or greater, edit, delete rights, to the workspace object and has view access to the Workspace Details tab, but does not have permission to View Workspace Details, the admin operation, the user cannot view the Workspace Details tab.
    - **Search Indexes**
    - **Object Type**
    - **Fields**
    - **Choices**
    - **Layouts**
    - **Views**
    - **Tabs**
    - **Relativity Applications**
    - **Custom Pages**
    - **History**

      Note: If a user has view access or greater to the History tab, but does not have permission to View All Audits , the user cannot view the **History** tab.
    - **User Status**
- **Worker Status**
- **Processing > Errors**

- These are the granular tabs you can make visible to a group.
- The following is a list of common Relativity parent and child tabs in alphabetical order by parent tab name:
- **Case Admin**
  - **Batch Sets**
  - **Markup Sets**
  - **Persistent Highlight Sets**
  - **Production Sets**
  - **Scripts**
- **Case Metrics**
  - **Reports**
  - **Reviewer Metrics**
- **Dashboard**
- **Documents**
- **Entities**
  - **Entities**
  - **Aliases**
- **Indexing & Analytics**
  - **Structured Analytics Set**
  - **Analytics Profiles**
  - **Repeated Content Filters**
  - **Search Indexes**
  - **Analytics Categorization Set**
- **Imaging**
  - **Imaging Profiles**
  - **Imaging Sets**
  - **Native Types**
  - **Password Bank**
- **Lists**
- **OCR**
  - **Profiles**
  - **OCR Sets**
- **Processing**
  - **Processing Sets**
  - **Quick Create Sets**
  - **Processing Data Sources**

    - **Processing Profile**
    - **Password Bank**
    - **Inventory**
    - **Reports**
- **Processing Administration**
    - **Worker Monitoring**
    - **Processing History**
- **Reporting**
    - **Search Terms Reports**
    - **Summary Reports**
    - **Pivot Profiles**
    - **Domain**
    - **Search Terms Results**
- **Review Batches**

35.4.4 Browsers

35.4.4.1 Browsers

In the Browsers section, you control which browsers are visible to a group. Select a browser type to make it visible for the group.

The following is a list of Relativity browsers:

- Folders

  Note: For more information on securing folders, see Relativity object security on page 671.

- Field Tree
- Advanced & Saved Searches
- Clusters

See the Browsers panel on page 790 section for complete details regarding each browser type.

Groups not granted access to any of the available browsers in a workspace see their document list spanning the whole screen.

35.4.5 Mass operations

35.4.5.1 Mass operations

In the Mass Operations section, you control which types of mass action rights the group can access. This section also lists any custom mass operations that you have added to Relativity or that are available in applications currently installed in your environment.

Select the check mark next to the mass action you want group members to have access to.

These are the granular mass operations you can grant a group.

- **Assign to Entity**—gives group members the rights to select and re-assign an alias to a different entity when using name normalization in Analytics.
- **Cluster**—gives group members the rights to cluster documents using Analytics clustering.
- **Convert**—gives group members the ability to convert a large set of documents into HTML5 format for faster document load times within the viewer.

  Note: Mass convert is not available in repository workspaces.

- **Copy**—gives group members the rights to copy securable objects such as views and layouts.
- **Delete**—group members can mass-delete documents. Mass delete also requires the rights to delete documents.
- **Edit**—gives group members the rights to use their layouts to simultaneously edit document field values for multiple documents.
- **Export**—gives group members the rights to export audit data via Audit.

  Note: This permission only appears if Audit is installed and configured.

- **Export to File**—gives group members the right to export the contents of a view to a .csv, .xls or .dat file.
- **Image**—group members can simultaneously send image requests for multiple native files.
- **Move**—gives group members the right to simultaneously move documents from one or more folders to one target folder. Mass Move also requires add and delete document rights.
- **Merge**—gives group members the rights to select and merge multiple entities into a single entity when using name normalization in Analytics.
- **PDF Actions**—gives group members the ability to download, create, store, or number PDFs. For more information, see Mass PDF permissions
- **Produce**—gives group members the right to simultaneously add multiple documents to a production set.
- **Replace**—group members can perform a replace operation on multiple documents. Examples include:
  - Copying the contents of one text field to another.
  - Adding a set string to the beginning or end of an existing field.
  - Merging the values of a source field with the values of a target field.
- **Process Transcript**—group members can process imported transcripts for viewing in Relativity.
- **Send To Case Map**—group members can send multiple documents to CaseMap.

  Note: CaseMap is not compatible with Windows 8.

- **Tally/Sum/Average**—group members can tally, sum and average the values of any numeric fields. This action is recorded under the document history.
- **Custom mass operations**—may appear in this list. They include mass operations that you added to Relativity or that are available in applications currently installed in your environment.

For more information about mass operations, see Mass operations on page 353.

35.4.6 Admin operations

You can secure several admin operations separately. To assign permissions to a group, select check boxes for any combination of these operations.

These are the granular admin operations you can grant a group.

- **Allow dtSearch Index Swap**—grants group members the ability to execute the Index Swap function from the dtSearch console. For more information, see the Searching Guide.
- **Allow Export**—grants group members the ability to export files through the export functionality found in Integration Points.
- **Allow Import**—grants group members the ability to import load files through import functionality found in Integration Points.
- **Assign Batches**—grants group members permissions to check out batches to other reviewers.
- **Communication Analysis Widget**—grants group members permission to add the Communication Analysis widget to a dashboard via the **Add Widget** drop-down menu.

  Note: Groups without this permission can still view and interact with the Communication Analysis widget assuming they have access to the dashboard the widget is part of.

- **Delete Object Dependencies**—grants group members permission to force the deletion of an object, which includes unlinking associative objects and deleting child objects. The group members must also have permissions to delete any dependent child and/or modify associative objects.
- **Email Thread Visualization**—grants group members permissions to access email thread visualization.
- **Export Dashboard**—grants group members permission to download a saved dashboard.
- **Manage Object Types**—permission that grants group members the ability to:
  - Create a new tab for a new object type when adding the new object type.
  - Automatically gain view, add, edit, delete, and secure permissions for all newly created object types.
  - Automatically gain tab visibility for newly created tabs.
- **Manage Relativity Applications**—group members can associate objects with applications by making the **Relativity Applications** field available on create and edit pages for Field, Layout, View, Script, Object Types, and all other objects compatible with applications. Users with this and Edit permissions for applications are allowed to lock and unlock an application from editing.
- **Modify System Keyboard Shortcuts**—grants group members permission to the **Manage System Keyboard Shortcuts** button. User groups must also have permissions to see the Workspace Admin and Workspace Details tab along with the View Workspace Details permissions. This button is located in the Relativity Utilities console on the Workspace Details page. See Keyboard shortcuts on page 301

  Note: If a user group is given this permission they can modify and delete keyboard shortcuts for their group within a workspace.

- **Override Production Restrictions**—grants group members permissions to override the setting in the Production Restrictions option on the Workspace Details page. The group members will be able to produce documents that contain conflicts based on these restrictions. See Adding and editing production restrictions on page 785.
- **Use Pivot/Chart**—grants group members permissions to use the Pivot grid and chart functions.

- **Use Quick Nav**—grants group members the ability to search tabs in a workspace using the quick nav feature. See Quick nav on page 43.
- **Use Sampling**—grants group members permission to the sampling menu on any object that has the Sampling field set to Enabled. The sampling menu users can create sample sets of items using a sampling methodology of their choice. For example, a user can make a sample set of documents to review for QC purposes. For more information, see Sampling on page 587.
- **View All Audits**—grants group members permission to view the history of a document in the Viewer through the Document History icon, as well as workspace objects, such as markup sets, Dynamic Objects, fields, and others, through the View Audit option on those objects' layouts.

  Note: If a user has view access or greater to the History tab, but does not have permission to View All Audits, the user cannot view the History tab.

- **View Batch Pane**—grants group members permission to view the batches associated with a document in the related items pane.
- **View Images Hidden for QC Review**—grants group members permission to view all images in an imaging set with a QC status set to hide images. For more information, see QC Review on page 278.
- **View User Status**—grants group members permissions to access the User Status tab.
- **View User's Personal Items**—grants group members permission to click the View Another User's Personal Items link on the Workspace Details page and modify the View Other's Personal Items console.
- **View Workspace Details**—grants group members permissions to access the Workspace Details page and the Relativity Utilities console. The Workspace Details feature grants this tab through either of its actions. See Feature Permissions.

  Note: If a user has view access or greater to the Workspace Details tab, but does not have permission to View Workspace Details, the user cannot view the Workspace Details tab.

  Note: If you are using Relativity aiR, the following admin operations are secured by default and should not be modified. Please contact Relativity Support if you think you need to access this functionality.

35.4.7 Customer lockbox

See Relativity aiR lockbox on the next page.

35.4.8 Workspace admin group

A system admin can assign any group in Relativity to have full admin rights over a particular workspace. A workspace admin has near-complete control over all objects within the workspace, but members of the group do not have the script permissions available only to system admins.

Note: While Workspace Administrators have extensive control over their respective workspaces, they do not automatically inherit the full range of system administrator privileges. Non-standard permissions like "**New Document**" must be added. Additionally, the "**Workspace**" permission is initially set only to "**View**" status.

Use the following steps to set a designate a workspace admin group:

1. Click **Edit** on the **Workspace Details** tab.
2. Click **Select** in the **Workspace Admin Group** field.

3. Select the group you want to set as the workspace admin group.
4. Click **Ok**.

Note: You can only designate one group per workspace as a workspace admin group.

Note: Being in a workspace's Admin Group alone does not permit a user to be assigned review batches. The user must also belong to at least one other group in that workspace (not the System Administrators group or the Workspace Admin group) that has access to the workspace and the **View Batches** permission. In other words, a Workspace Administrator with no additional group memberships will not appear as an available reviewer for batch checkout.

You can also grant workspace admins permission to alter the security settings of any group.

To grant workspace admins permission to alter the security settings of any group:

1. Click **Manage Workspace Permissions** from the Workspace Details tab.
   The Workspace Security window opens.
2. Select **Object Security**.
3. Select the desired group from the **Select a Group** dropdown.
4. Click the **Edit Security** padlock for the **Workspace** object permission.
5. Click **Save**.

35.4.9 Relativity aiR lockbox

Relativity aiR's Lockbox feature gives you greater control over data access in your workspace. It helps protect sensitive information from unauthorized access by System Administrators, while still enabling authorized users to access data for valid legitimate purposes.

Lockbox also offers built-in alerting, providing notifications whenever access changes occur. This ensures you have full visibility into your tenant's security posture.

Configuration details:

Lockbox includes two separate controls, managed through the EnableRelativityLockbox and EnableCustomerLockbox instance settings. This separation allows precise configuration based on your specific requirements. **By default, EnableCustomerLockbox is disabled**, but you can turn it on when your organization needs additional oversight for System Administrator access.

35.4.9.1 Instance settings:

Instance setting name	Description	Default Value	Impact
EnableRelativityLockbox	Controls access to workspaces for all Relativity employees, except those explicitly granted access by the customer.	True	Prevents all Relativity employees from accessing workspaces unless they are added to workspace groups. This requires manual intervention by the

Instance setting name	Description	Default Value	Impact
			customer to grant access to Relativity employees.
EnableCustomerLockbox	Controls access to workspaces for System Administrators.	False	Prevents System Administrators from accessing workspaces unless they are added to workspace groups. This requires System Administrators to disable Lockbox to access workspaces, which triggers alerts to be generated.

- You can view and manage security permissions for Relativity Support team users on the security permissions page unless you choose to lock them out entirely.
- When the **EnableCustomerLockbox** instance setting is enabled or disabled, a Security Alert is automatically generated. This built-in alerting helps you maintain full visibility into any changes to your workspace's security settings and ensures you are always informed when access controls are adjusted.
- To allow your System Administrators to access workspaces, set the EnableCustomerLockbox instance setting to "False".
- To grant Relativity support temporary access to a workspace, you can either add Relativity support to a group that belongs to the workspace, or set the **EnableRelativityLockbox** instance setting to "False".

When you contact Relativity Support for troubleshooting, the following high-level steps are performed if access to customer workspace is required to resolve an issue:

1. Support is requested through the usual means.
2. The Relativity Customer Support technician will request that you add a Relativity aiR Support group to the workspace in question.
3. The Relativity Customer Support technician will troubleshoot your case per standard protocol.
4. Upon resolution, the Relativity Customer Support technician will advise you that the issue is resolved.
5. You should then remove the Relativity aiR Support group from the workspace you added them to.

Refer to Support if you need more information on this feature.

35.4.9.2 Lockbox reports

To help you monitor and audit the use of the Customer Lockbox feature in Relativity, we provide two scripts:

- Lockbox Bypass report - This script provides an audit trail of any changes made to the **EnableCustomerLockbox** instance setting, including details such as who made the change and when it occurred.
- Lockbox report - This script provides a list of all workspaces to which an employee of Relativity ODA LLC currently has access, as well as the name of the group to which the user is linked.

> **Note:** The report does not include the actual names of users. This report may reference Maintenance workspaces ("[DO NOT ACCESS]...") to which Relativity maintains access. While this script is focused on auditing "Relativity ODA LLC" employees, you can create a similar custom script to audit your own employees if desired.

> **Note:** The Security Center – Lockbox Access tab provides an in-application view of all workspaces where Relativity employees have or had access (with user names, groups, and timestamps), which can be used as an alternative to running the Lockbox report script for on-demand transparency into Relativity aiR support access.

35.4.9.3 Lockbox security notifications

In Relativity aiR, system administrators can be added to the **Security Notifications** group for a given instance to receive notifications whenever any of the following events occur:

- A member of Relativity staff is granted access to a customer workspace while Lockbox is enabled.
- The **EnableCustomerLockbox** instance setting is enabled or disabled.
- A user is added or removed from the Security Notifications group. Note that only the person who was added or removed will receive the email notification - other group members will not be notified.

> **Note:** If the Security Notifications group is accidentally deleted, you can re-add it.

Additionally, if any person with a Relativity email address is added to a group with associated workspaces, the email address will receive notifications whenever a user is added to or removed from the group.

When any of these conditions are met, members of the Security Notifications group will receive an email notification. The notification email includes a link to the Security Center, where Relativity workspace access can be revoked if needed.

35.5 Feature permissions

You can manage permissions more efficiently using the Features tab. Instead of adjusting individual settings across Object Security, Tab Visibility, and Other Settings, you can enable permissions by feature.

Features represent key system capabilities such as Preservation, Production, Imaging, and Configure Doc Review. Each feature groups together the necessary permissions from the three tabs. When you enable a feature, all related permissions are automatically applied.

To achieve this, all permission changes must now be made through Feature Permissions instead of the older granular settings in Object Security, Tab Visibility, and Other Settings/Admin Operations. The modernization of Feature Permissions simplifies permissions management and creates consistency across workflows. This update ensures that feature behavior is standardized and easier for end users to understand and use.

Feature Permissions are rolling out through a phased modernization. Migration tooling supports controlled adoption with full audit visibility.

During migration, each feature exists in one of two states:

- **Modernized—** Feature Permissions controls all permissions for the feature. Granular permissions are locked, and the feature toggle governs them. You cannot directly edit permissions in Object Security, Tab Visibility, or

Other Settings.

- **Non-modernized—** Legacy behavior remains. You can continue to modify granular permissions in Object Security, Tab Visibility, and Other Settings, and those changes appear on the Features tab.

When you enable or disable a feature, Feature Permissions applies or revokes the entire set of dependent permissions in a single action. This simplifies configuration and reduces the risk of misaligned settings.

35.5.1 Currently modernized features

Below you will find the current Feature Permissions that are modernized. When a feature is modernized, its associated Object Security, Tab Visibility, and Admin Operations permissions are locked and can only be modified through the Feature Permission toggle. For more information, see Modernized features on page 647.

Note: Shared granular permissions cannot be disabled via the Feature Permission toggle if another Feature Permission that includes the same permission is currently enabled. For more information, see Modernized features on page 647.

* = Shared granular permission

Modernized Feature Permission	Level	Object Security	Tab Visibility	Admin Operations / Other
aiR Review	Instance	None	aiR Review Jobs	* **View Admin Repository**
Application Management	Instance	Library Application – View OAuth2 Client – View, Add, Edit, Delete, Secure Resource File – View, Add, Edit, Delete, Secure Custom Page – View, Add, Edit, Delete, Secure Sanitizer – View, Add, Edit, Delete, Secure * **Relativity Script – View**	Application Library * **Authentication** OAuth2 Client Resource Files Custom Pages Sanitizer * **Applications & Scripts** Relativity Script Library	* **View Admin Repository**
Archive and Restore (ARM)	Instance	None	ARM ARM Jobs Configuration	* **View Admin Repository**
Audit	Instance	Data Grid Audit – View * **Relativity Script – View**	Audit * **Applications & Scripts** Audit Migration Reports	View Audits * **View Admin Repository**
Authentication	Instance	* **Authentication Provider – View, Edit, Add, Delete, Secure**	* **Authentication**	* **View Admin Repository**

Modernized Feature Permission	Level	Object Security	Tab Visibility	Admin Operations / Other
		* **Authentication Provider Type – View** * **Login Method – View, Edit, Add, Delete, Secure** Group Claim Mapping – View, Edit, Add, Delete, Secure Required Claim – View, Edit, Add, Delete, Secure JIT Settings – View, Edit, Add, Delete, Secure Federated Instance – View, Edit, Add, Delete, Secure	Authentication Provider Authentication Provider (legacy) Authentication Provider Type Federated Instance	
Case Metrics	Instance	Schedule – View, Edit, Add ScheduleReport – View, Edit, Add ScheduleReportField – View, Edit, Add ScheduleReportFilter – View, Edit, Add	Case Metrics Reports Scheduler	* **View Admin Repository**
Client and Matter Management	Instance	Client – View, Edit, Add, Delete, Secure Matter – View, Edit, Add, Delete, Secure	Clients Matters	* **View Admin Repository**
Cost Explorer	Instance	None	Cost Explorer * **Management Console**	* **View Admin Repository** View Cost Explorer
Data Transfer	Instance	None	Staging Explorer	* **View Admin Repository** Access Staging Explorer Send Email Notification
Instance Configuration	Instance	View – View, Edit, Add, Delete, Secure Field – View, Edit, Add, Delete, Secure + Add Field Choice By Link Object Type – View, Edit, Add, Delete, Secure Object Rule – View, Edit, Add, Delete, Secure Layout – View, Edit, Add, Delete, Secure Tab – View, Edit, Add, Delete, Secure Choice – View, Edit, Add, Delete, Secure Dashboard – View, Edit, Add, Delete, Secure Agent – View, Edit, Add, Delete, Secure Agent Type – View, Edit, Add, Delete, Secure InstanceSetting – View, Edit, Add, Delete,	Admin Workspace Configuration Views Fields Object Type Choices Dashboards Tabs Tab Sync Agents Server & Agent	* **View Admin Repository** Delete Object Dependencies Manage Object Types Agent Operations

Modernized Feature Permission	Level	Object Security	Tab Visibility	Admin Operations / Other
		Secure	Management Instance Settings	
Job Queues	Instance	None	Queue Management OCR Queue PDF Queue Processing and Imaging Queue DtSearch Queue Admin Import/Export Queue Branding Queue Branding Queue Legacy Production Queue Production Queue Legacy Processing Administration Processing History Translate Jobs kCura Admin Workspace Upgrade Queue Text Migration Jobs Text Migration Reports Transcription Queue	* **View Admin Repository** Change Queue Priority
Migrate	Instance	Migrate Migration – View, Edit, Add, Delete, Secure Migrate Restore Job – View, Edit, Add, Delete, Secure Migrate Source Instance – View, Edit, Add, Delete, Secure	Migrate	* **View Admin Repository** Access Migrate

Modernized Feature Permission	Level	Object Security	Tab Visibility	Admin Operations / Other
Security Center	Instance	None	Security Center	None
Staging Reports	Instance	None	Staging Reports * **Management Console**	* **View Admin Repository** View Instance-wide Staging Reports View Client Domain Staging Reports
Usage Reports	Instance	None	* **Management Console**	* **View Admin Repository** View Instance-wide Usage Reports View Client Domain Usage Reports
Users and Groups Management	Instance	User – View, Edit, Add, Delete, Secure Group – View, Edit, Add, Delete, Secure * **Client – View** * **Authentication Provider – View** * **Authentication Provider Type – View** * **Login Method – View, Edit, Add, Delete**	Groups Users * **User and Group Management** Centralized Authentication User Status	* **View Admin Repository** Send Message Force Logout on User Status
Workspace Management	Instance	Workspace – View, Edit, Add, Delete, Secure * **Client – View** Matter – View, Add Resource Pool – View	Workspaces	* **View Admin Repository** Manage Cold Storage

This table is updated as additional features move to the modernized state. Check back regularly or review the release notes for the latest changes.

35.5.2 Considerations

Keep these factors in mind when setting Feature permissions:

- For **modernized** features, the Feature Permission becomes its own unique entity and is no longer simply a stateless collection of the granular permissions associated with that feature. Once modernized, the Feature Permission can only be granted or revoked by modifying the value of the Feature Permission directly and will never be changed based on modification of the granular permissions.

- For **non-modernized** features, any change modifications should happen in the Feature tab, but are still available for granular permission settings on the Object Security, Tab Visibility, and Other Settings tabs.

35.5.3 Using the Features tab

The Features tab lists the features available for the selected group. Each feature shows its current state for that group.

To apply a preset to a feature:

1. Find the feature in the list.
2. Click **See details**. A panel opens on the right.
3. Select a **preset**.
4. Click **Review and Save**.
5. Review the changes, then click **Save**.

Some features control only a few permissions and do not offer presets. Select the checkbox next to the feature to grant access. Clear the checkbox to remove access.

You can also do the following from the Features tab:

- Use the Search bar to find a feature in the list.
- In a feature's **See details** panel, click Granular permissions mapping. A read-only reference shows the granular permissions behind each preset.

35.5.3.1 Feature actions

Actions are available within Feature Permissions. An action represents a specific task that users can perform within a feature. Actions allow administrators to customize access for a group by granting only the tasks they need instead of granting access to the entire feature.

Example: the Audit feature includes two actions: **View Audit** and **View Audit Migration Reports**.

Key details about actions:

- Each action maps to one or more granular permissions, managed by Relativity.
- Actions are additive. Selecting an action grants access to its task. It does not remove access granted by other actions or features.
- Each action belongs to one feature. The same action does not appear in another feature.

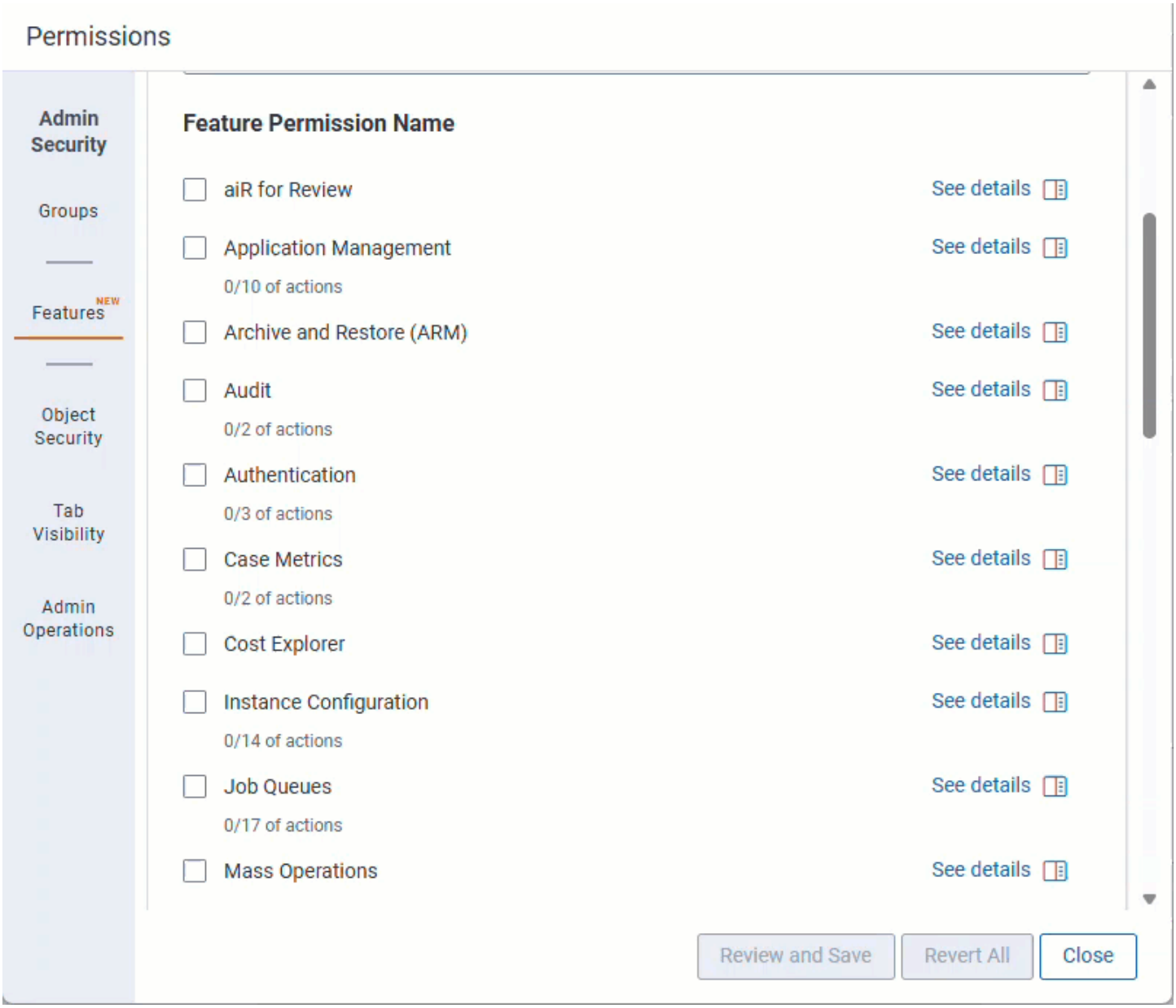
35.5.3.2 Presets

A preset is an optional group of related actions. It gives you a starting point for a feature. When you select a preset, Relativity selects the actions defined for that preset. You can then select or clear individual actions before you save.

Notes:

- The preset itself does not define access, however, the actions you save do.
- Presets appear in the feature's See details panel.
- A label on the feature shows which preset is applied.

Most features with presets offer Viewer and Administrator. Staging Reports and Usage Reports offer Client Domain and Instance-wide. Some features have no preset. For those, select all actions, or select individual actions.



35.5.3.3 Feature states

A feature's state for a selected group depends on how many actions are enabled:

- **Disabled:** None of the feature's actions are selected.
- **Partially Enabled:** Some, but not all, actions are selected.
- **Enabled:** All of the feature's actions are selected.

A feature with no actions has only two states: **Disabled** or **Enabled**.

35.5.3.4 Viewing the legacy permissions mapping

Some features map their actions to granular permissions. To see this mapping, open the feature's See details panel. Click Granular permissions mapping. The mapping is a read-only reference. It shows the granular permissions behind

each preset or action.

The mapping uses these icons:

- **Enabled permission** — the group has this granular permission.
- **Disabled permission** — the group does not have this granular permission.
- **Permission used by multiple Features** — more than one feature includes this permission.
- **Permission not found by name** — a tab permission was renamed. Relativity cannot identify it by the new name, so Relativity does not modify this permission.

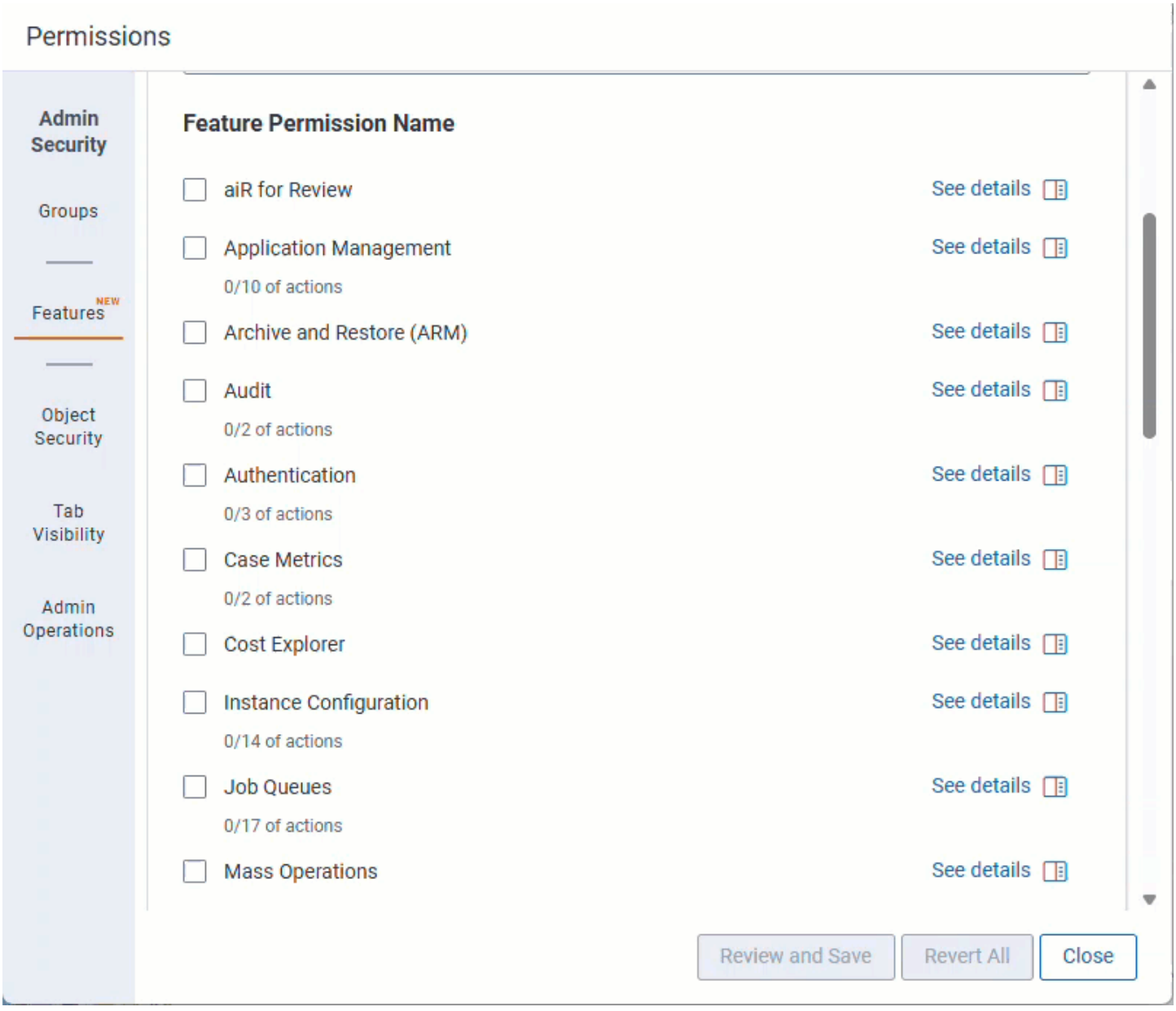
Icon Guide

Enabled permission

Disabled permission

Permission used by multiple Features

Permission not found by name



35.5.3.5 Configuring feature actions for a group

1. Open permissions for the group. For steps, see Setting instance permissions.
2. In the Features list, find the feature.
3. Click **see details**.
4. Select a preset, or select individual actions
5. Click **Review and Save**.
6. Review the listed changes, then click **Save**.

35.5.4 Feature permission behavior

Feature permissions and granular permissions represent the same access from different perspectives. How changes are applied depends on whether the feature has been modernized.

35.5.4.1 Behavior for all features

These behaviors apply to every feature, whether or not it is modernized:

- **A selected feature checkbox**—grants every granular permission the feature includes.
- **A selected action**—grants only the granular permissions mapped to that action. Other actions and features keep the access they already grant.
- **A cleared feature checkbox**—revokes the feature's granular permissions, except any that another enabled feature also includes.

A modernized feature locks its granular permissions, so you cannot change them directly. Changing a granular permission is therefore the one behavior that applies only to features that are not modernized.

35.5.4.2 Non-modernized features

For non-modernized features, access can be managed from either the Features tab or the **Object Security**, **Tab Visibility**, and **Other Settings** tabs. The standard feature behaviors described above still apply. You can also enable or disable granular permissions directly. When you do, the state of every enabled feature that includes that permission is updated. A feature is considered enabled only when all of its associated permissions are enabled.

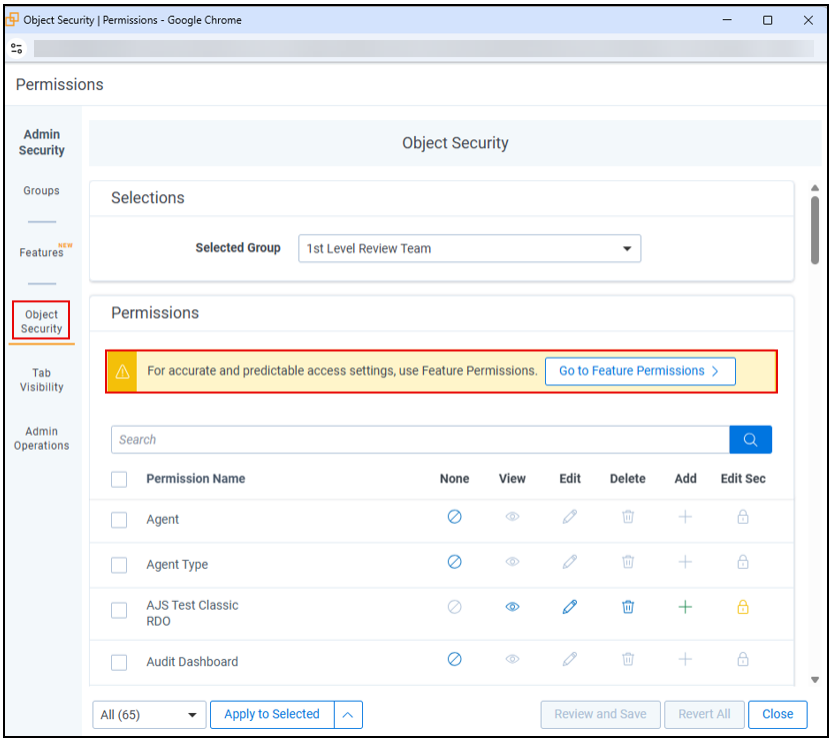
Keep the following behaviors in mind:

- **Shared permissions may remain enabled after a feature is disabled.**
  A granular permission can belong to multiple features. If you disable one feature, but another enabled feature still includes the same permission, that permission remains enabled.
- **Disabling a feature does not restore previous access levels.**
  Enabling a feature grants all permissions included in that feature, including permissions the group may not have had previously. When the feature is later disabled, all of those permissions are revoked, not just the ones added by enabling the feature. Review the Review Permissions Changes dialog carefully before saving your changes.

35.5.4.3 Modernized features

As features move to the modernized state, the way you manage permissions for them changes. The Features tab becomes the only way to change access. The feature permission is its own entity rather than a collection of the granular permissions behind it. Relativity locks those granular permissions and manages them, so you **cannot** change them on the Object Security, Tab Visibility, or Other Settings tabs. Only the behaviors for all features apply.

Legacy granular permission pages, such as Object Security, show a banner directing you to make permission changes on the Features tab.

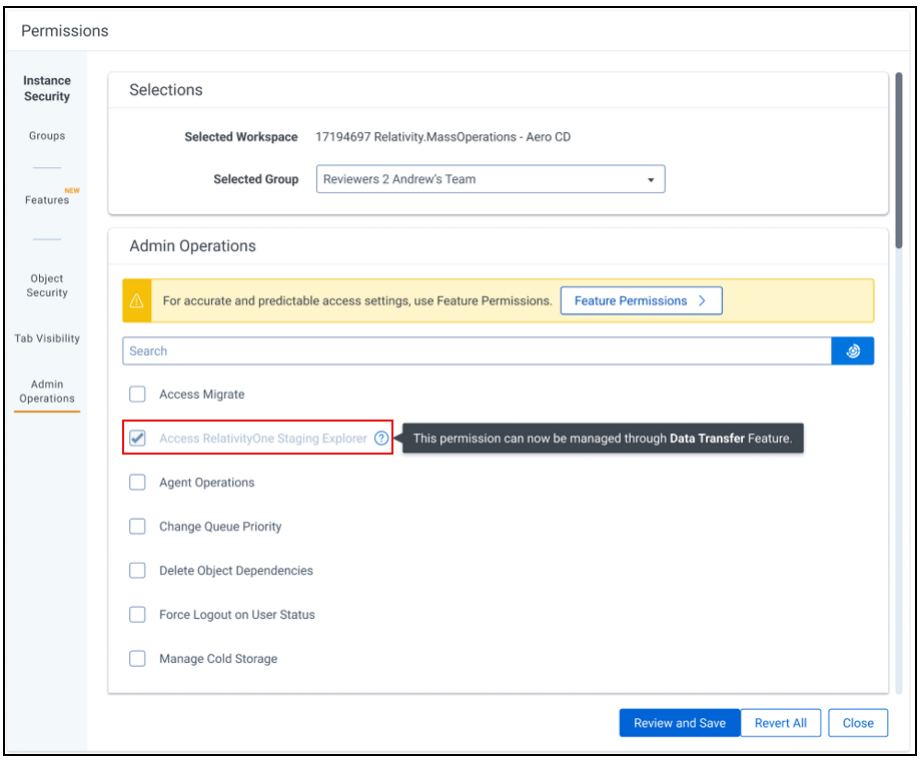


Granular permissions you can change

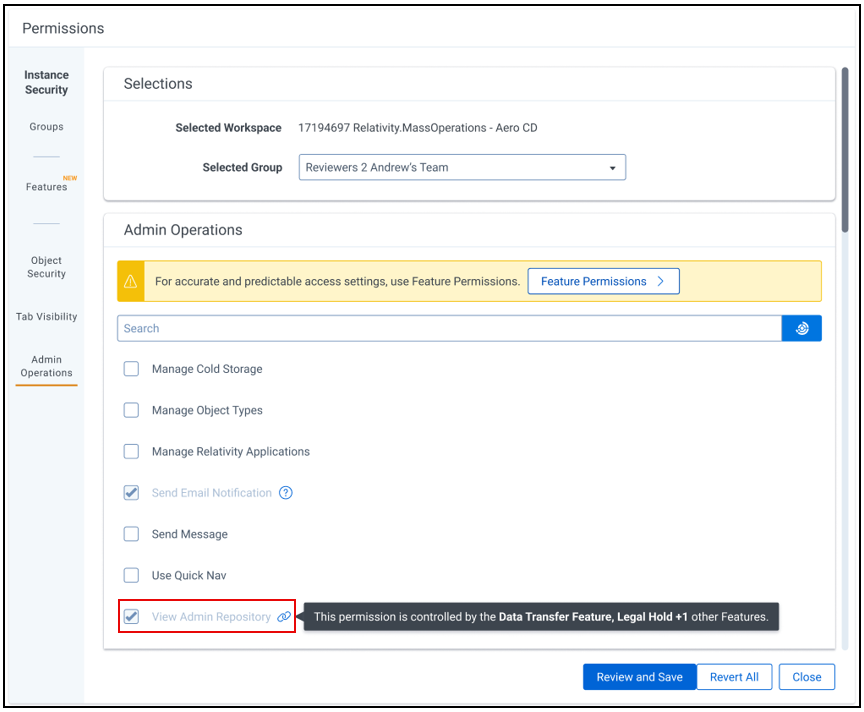
Whether you can change a granular permission depends on the features it belongs to:

Granular permission	Feature state	Can you change it
Not modernized—belongs to no modernized feature	Any	Yes
Fully modernized—belongs only to modernized features	Any	No
Partially modernized—belongs to both modernized and non-modernized features	At least one modernized feature is enabled	No
	All modernized features are disabled	Yes

A fully modernized granular permission is read-only. A tooltip names the feature permission to use instead.

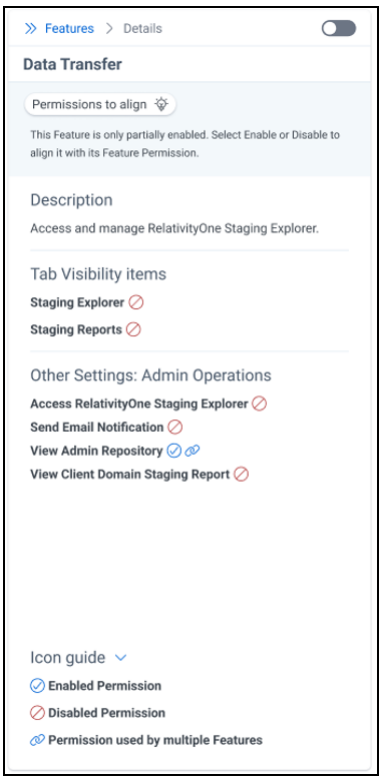


A partially modernized granular permission is read-only while at least one of its modernized features is enabled. A message names the feature permissions that require it.



Shared granular permissions

A granular permission shared across multiple features does not always reflect the state of any one of them. The **See details** panel lists every granular permission a feature includes, and a blue link icon marks the shared ones.



35.5.5 Frequently asked questions

Will I be able to continue to use granular permissions for certain use cases?
No, if the feature is modernized, management can only be done via the feature permission. If the feature has not been modernized granular permissions can be leveraged to manage the permissions.

What is the difference between a modernized and non-modernized Feature Permission?
A modernized Feature Permission is the sole control point for granting or revoking access to that feature. The underlying granular permissions are locked and managed automatically. A non-modernized Feature Permission works as it does today. You can still edit granular permissions directly on the Object Security, Tab Visibility, and Other Settings tabs.

What does the blue lightbulb icon mean?
The blue lightbulb icon indicates that a group's current permissions configuration is out of alignment with a modernized Feature Permission. You should enable or disable the feature to bring the group into alignment. See Aligning permissions with modernized features for steps.

Do I need to take action immediately when a feature is modernized?
Existing groups and their permissions configurations are not impacted at the time of modernization. However, it is highly encouraged to align each group's permissions as soon as possible so that they are prepared for the future state of permissions.

Why is the user not seeing a tab that should be available as part of the enabled feature?
First, ensure the user has Tab Visibility by looking for a blue check mark next to the tab name in the See Details pane of the feature. If confirmed and still not visible:

1. Check item-level Security: if the tab is secured against the selected group, it will not be available in the application.
2. Check the tab configuration: if the tab's parent is not visible, it will not appear in the side panel or hamburger menu, but it will still be accessible via Quick Nav.

Why are certain features not available in my workspace?
Feature availability is determined by your workspace configuration. Features will only show when the relevant applications are installed in the workspace. If any necessary components are missing, the feature will not be available.

I had enabled a Feature for a specific group earlier, but now it appears as disabled for that same group. What could have caused this?
Although this situation should be rare, it can occasionally arise. This typically occurs when the feature definition is changed to include a permission that the group does not have, often because a new permission has been introduced to the system. To resolve this issue, re-enable the feature for the affected group.

35.5.6 Workspace-level permissions

Set administrator or user permissions at the feature level. The tables below show the specific permission settings included in each feature at the workspace-level.

For more details on setting feature permissions, refer to Setting workspace permissions.

Note: None stands for Not Applicable

Automated workflows
Purpose: Automates multi-step processes in a workspace. For example, running searches, imaging sets, or productions in sequence without manual intervention. With this feature enabled, a group can create and manage Automated Workflow objects (the definitions of the workflows) and access the Automated Workflows tab.

Permissions: The feature grants full rights to the Automated Workflows object (Add, Edit, Delete, etc., including "Copy to Workspaces" and "Sync to Workspaces") so users (typically admins or power users) can design workflows. It also ensures the group has any needed rights for actions the workflows might perform. For example, rights to run imaging sets, OCR sets, dtSearch indexes, search term reports, and structured analytics sets if those are part of a workflow. The feature toggle also exposes the Automated Workflows tab in the workspace UI and enables special mass operations (like "Set Long Text Field Size") that certain automated actions require.

Considerations: Only administrative users should typically have this feature, since designing workflows requires broad access to many objects. When the feature is enabled, the system adds a dedicated backend "Workflow Agent" user to run workflow actions. The designing user must have all necessary rights, but the actions execute under that agent account.

The feature permissions designated for Automated workflows are:

Role (Admin or User)	Object Security	Tab Visibility	Other settings
Administrator	**Automated workflows** - Add, Edit, Delete, View, Secure, Copy to Workspaces, Sync to Workspaces	Admin	None

Case metrics
The feature permissions designated for Case metrics are:

Role (Admin or User)	Object Security	Tab Visibility	Other settings
User	**Reviewer Metrics** - View, Add, Edit, Delete, Secure	Case Metrics	View All Audits
		Reports	
		Reviewer Metrics	

Collect
The feature permissions designated for Collect are:

Role (Admin or User)	Object Security	Tab Visibility	Other settings
User	**Collection** - Add, Edit, View	Advanced	N/A
	Collection Detail Custodian - Add, Edit, Delete, View	Collect	

	Collection Detail Custodian Target - Add, Edit, Delete, View	Collections	
	Collection Detail Custodian Target Result – Add, Edit, Delete, View	Custodial Target Status	
	Collection Detail Noncustodial Source – Add, Edit, Delete, View	Custodian Targets	
	Collection Detail Noncustodial Source – Add, Edit, Delete, View Entities	Entities	
	Collection Detail Request – Add, Edit, Delete, View	Matters	
	Collection Detail Source Instance – Add, Edit, Delete, View	Monitor	
	Collection Detail Source Type – Add, Edit, Delete, View	Non-Custodial Target Status	
	Collection Detail Summary – Add, Edit, Delete, View	Status Summary	
	Collection Matter – Add, Edit, View		
	Collection Run – Add, Edit, View		
	Collection Source Instance - View		
	Collection Source Instance Parameter - View		
	Collection Source Target Parameter Instance - View		
	Collection Source Target Parameter Type - View		
	Collection Source Type - View		
	Collection Source Type Parameter Type - View		
	CollectionSourceTypeCriteria - View		
	Collection Source Type Criteria Validator - View		
	Collection Source Type OAuth Definition - View		
	Custodian Target – Add, Edit, Delete, View		
	Custodian Target Generation Error – Add, Edit, Delete, View		
	Entity - View		
	Relativity Time Zone – Add, Edit, View		
	Processing Data Source – Add, Edit, View		
	Processing Error – Add, Edit, View		
	Processing Profile – Add, Edit, View		
	Processing Set – Add, Edit, View		
	Folder – Add, Edit, View		
Administrator	**CollectionSourceTypeCriteria** – Edit, Delete, Secure, Add, View	Advanced	N/A
	Custodian Target – Edit, Delete, Secure, Add, View	Collect	

	Noncustodial Target Generation Error – Edit, Delete, Secure, Add, View	Collection Admin	
	Collection Source Instance Parameter – Edit, Delete, Secure, Add, View	Collections	
	Collection Source Type Criteria Validator – Edit, Delete, Secure, Add, View	Custodial Target Status	
	Collection Detail Request – Edit, Delete, Secure, Add, View	Custodian Targets	
	Entity – Edit, Delete, Secure, Add, View	Entities	
	Collection Source Type Parameter Type – Edit, Delete, Secure, Add, View	Matters	
	Collection Source Type – Edit, Delete, Secure, Add, View	Monitor	
	Collection – Edit, Delete, Secure, Add, View	Non-Custodial Target Status	
	Collection Run – Edit, Delete, Secure, Add, View	Status Summary	
	Processing Error – Edit, Delete, Secure, Add, View		
	Collection Detail Custodian – Edit, Delete, Secure, Add, View		
	Processing Data Source – Edit, Delete, Secure, Add, View		
	Relativity Time Zone – Edit, Delete, Secure, Add, View		
	Collection Detail Custodian Target Result – Edit, Delete, Secure, Add, View		
	Collection Source Type OAuth Definition – Edit, Delete, Secure, Add, View		
	Processing Profile – Edit, Delete, Secure, Add, View		
	Collection Source Target Parameter Type – Edit, Delete, Secure, Add, View		
	Noncustodial Data Source Instance – Edit, Delete, Secure, Add, View		
	Collection Detail Custodian Target – Edit, Delete, Secure, Add, View		
	Collection Detail Source Type – Edit, Delete, Secure, Add, View		
	Collection Detail Source Instance – Edit, Delete, Secure, Add, View		
	Processing Set – Edit, Delete, Secure, Add, View		
	Collection Source Instance – Edit, Delete, Secure, Add, View		
	Custodian Target Generation Error – Edit, Delete, Secure, Add, View		
	Collection Detail Summary – Edit, Delete, Secure, Add,		

	View		
	Collection Source Target Parameter Instance – Edit, Delete, Secure, Add, View		
	Collection Matter – Edit, Delete, Secure, Add, View		
	Collection Detail Noncustodial Target – Edit, Delete, Secure, Add, View		
	Folder – Edit, Delete, Secure, Add, View		
	Collection Detail Noncustodial Source – Edit, Delete, Secure, Add, View		

Export structured data
The feature permissions designated for Export structured data are:

Role (Admin or User)	Object Security	Tab Visibility	Other set-tings
User	**Document** – Add, Edit, View	Documents	Allow Export
	Folder – Add, Edit, View	Import/Export Job	
	Import/Export Extraction Job – Add, Edit, View		
	Import/Export Job – Add, Edit, View		
	Production - View		
	Relativity Export Service Job – Add, Edit, View		
	Relativity Time Zone - View		
Administrator	**Document** – Add, Edit, View, Secure, Delete	Documents	Allow Export
	Folder – Add, Edit, View, Secure, Delete	Import/Export Job	
	Import/Export Extraction Job – Add, Edit, View, Secure, Delete		
	Import/Export Job – Add, Edit, View, Secure, Delete		
	Relativity Time Zone – View, Secure, Edit, Delete		
	Production – View, Secure, Edit, Delete		
	Relativity Export Service Job – Add, View, Edit, Secure, Delete		

Imaging
The feature permissions designated for Imaging are:

Role (Admin or User)	Object Security	Tab Visibility	Other settings
User	**Document** – Add, View	Documents	Image - mass
	Imaging Profile – Add, View, Edit	Imaging Profiles	

Role (Admin or User)	Object Security	Tab Visibility	Other settings
	Imaging Set – Add, View, Edit	Imaging Sets	
	Native Type - View		
Administrator	**Document** – Add, View, Edit, Secure, Delete	Documents	None
	Imaging Profile – Add, View, Edit, Delete, Secure	Imaging Profiles	
	Imaging Set – Add, View, Edit, Delete, Secure	Imaging Sets	
	Native Type – View, Secure, Edit, Delete		

Legal hold
The feature permissions designated for Legal hold are:

Role (Admin or User)	Object Security	Tab Visibility	Other settings
Administrator	**Custodian Role** – Add, View, Edit, Delete	Legal Hold	Manage Object Types
	Custodian Status – Add, View, Edit, Delete	Projects	Use Pivot/Chart
	Entity – Add, View	Communications	View All Audits
	Field – Add, View, Add Field Choice By Link	Reports	
	JobSchedule – Add, View, Edit, Delete	Question Responses	
	Legal Hold Application Permissions: • View • Assign Custodian(s) • Release Custodian(s) • Remove Custodian(s) • Open Project / Close Project • Preservation Hold • Send Communication(s) • Send Communication Preview • Send Communication Reminder • Send Escalation • View Portal As Custodian • Act On Behalf of Custodian • Respond To Message • Send Global Reminder Now • Send Test Global Reminder	Mailbox	

Role (Admin or User)	Object Security	Tab Visibility	Other settings
	• Test Outgoing Email Settings • Send Project Reminder Now • Send Test Project Reminder • Approve Communications		
	Legal Hold Selector Communications – Add, View, Edit, Delete	Project Reminder	
	Legal Hold Selectors – View	Custodian Status Dashboard	
	Preservation Case – Add, View, Edit	Tasks	
	Preservation Case Source – Add, View, Edit, Delete	Legal Hold Libraries	
	Preservation Custodian Status – Add, View, Edit, Delete	Questionnaires	
	Preservation Custodian Target – Add, View, Edit, Delete	Questions	
	Preservation Hold Settings – Add, View, Edit, Delete	Attachments	
	Preservation Source – Add, View, Edit, Delete	Scheduled Reports	
	Preservation Target Discovery Status – Add, View, Edit, Delete	Legal Hold Admin	
	Preservation Target Filter – Add, View, Edit, Delete	Legal Hold Settings	
	Preserve Product – Add, View, Edit, Delete	Global Reminder	
	Preserve Product Source – Add, View, Edit, Delete	Preservation Hold Settings	
	Project – Add, View, Edit, Delete	Role	
	Project Health – Add, View, Edit, Delete	Custodian Portal Authentic-ation Provider	
	Project Questionnaires – Add, View, Edit, Delete	Item Selectors	
	Project Questionnaires Report Sub View - View	Entities	
	Roles – Add, View, Edit, Delete		
	Scheduled Report – Add, View		

OCR
The feature permissions designated for OCR are:

Role (Admin or User)	Object Security	Tab Visibility	Other settings
User	**OCR Set** – Add, View	OCR Sets	Advanced & Saved Searches
	OCR Profile - View	OCR Profiles	
	Production - View		
	Search - View		
Administrator	**OCR Set** – Add, View, Secure, Edit, Delete	OCR Sets	Advanced & Saved Searches
	OCR Profile – View, Add, Edit, Secure, Delete	OCR Profiles	
	Production – View, Secure, Edit, Delete		
	Search – View, Secure, Edit, Delete		

Preservation
The feature permissions designated for Preservation are:

Role (Admin or User)	Object Security	Tab Visibility	Other set-tings
User	**Preservation** – View, Edit, Delete	Data Preservation	
	Preservation Data Service - View		
	Preservation Data Source - View	Preservation Hold Entity Status	
	Preservation Error – View, Edit, Delete	Preservation Hold Job	
	Preservation Hold Entity Status – View, Edit, Delete	Preservation Error	
	Preservation Hold – View, Edit, Delete	Preservation	
	Preservation Hold Job – View, Edit, Delete	Preservation Hold	
Administrator	**Custodian Role** – View, Secure, Edit, Delete		None
	Custodian Status – View, Secure, Edit, Delete		
	Entity – View, Secure, Edit, Delete		
	Field – View, Secure, Edit, Delete		
	JobSchedule – View, Secure, Edit, Delete		
	Legal Hold Application Permissions – View, Secure, Edit, Delete		
	Legal Hold Selector Configurations – View, Secure, Edit, Delete		
	Legal Hold Selectors – View, Secure, Edit, Delete		
	Preserve Product – View, Secure, Edit, Delete		
	Preserve Product Source – View, Secure, Edit, Delete		
	Preservation – View, Edit, Delete, Secure	Data Preservation	

Role (Admin or User)	Object Security	Tab Visibility	Other settings
	Preservation Case – View, Secure, Edit, Delete		
	Preservation Case Source – View, Secure, Edit, Delete		
	Preservation Custodian Status – View, Secure, Edit, Delete		
	Preservation Custodian Target – View, Secure, Edit, Delete		
	Preservation Data Service – View, Edit, Delete, Secure	Preservation Error	
	Preservation Data Source – View, Edit, Delete, Secure	Preservation Hold Job	
	Preservation Error – View, Edit, Delete, Secure	Preservation Data Source	
	Preservation Hold – View, Edit, Delete, Secure	Preservation	
	Preservation Hold Entity Status – View, Edit, Delete, Secure	Preservation Data Service	
	Preservation Hold Job – View, Edit, Delete, Secure	Preservation Hold	
	Preservation Hold Settings – View, Secure, Edit, Delete		
	Preservation Source – View, Secure, Edit, Delete		
	Preservation Target Discovery Status – View, Secure, Edit, Delete		
	Preservation Target Filter – View, Secure, Edit, Delete		
	Project – View, Secure, Edit, Delete		
	Project Health – View, Secure, Edit, Delete		
	Project Questionnaires – View, Secure, Edit, Delete		
	Project Questionnaires Report Sub View – View, Secure, Edit, Delete	Preservation Hold Entity Status	
	Roles – View, Secure, Edit, Delete		
	Scheduled Report – View, Secure, Edit, Delete		

Production
The feature permissions designated for Production are:

Role (Admin or User)	Object Security	Tab Visibility	Other settings
User	**Production** – Add, View, Edit	Production Sets	Copy
	Production Data Source – Add, View, Edit, Delete	Production Placeholder	Re-produce
	Production Information – Add, View, Edit	Production	
	Production Placeholder – Add, View, Edit	Case Admin	

Role (Admin or User)	Object Security	Tab Visibility	Other settings
Administrator	**Production** – Add, View, Edit, Secure, Delete	Production Sets	View All Audits
	Production Data Source – Add, View, Edit, Delete, Secure	Production Placeholder	Override Production Restrictions
	Production Information – Add, View, Edit, Secure, Delete	Production	Copy
	Production Placeholder – Add, View, Edit, Secure, Delete	Case Admin	Re-produce

Redact
The feature permissions designated for Redact are:

Role (Admin or User)	Object Security	Tab Visibility	Other settings
User	**Document** – View, Redact Document, Highlight Document, Local Access (Download, Copy Text)	None	None
	Markup Set – Add, View		
	Redact – Add, Edit, Delete, View, Place/Edit Manual Redaction, Place/Edit Manual Highlight, Clear Markups, Unhide Excel Content, View Quality Control Panel, Accept/Reject Quality Control Entries, Native PDF Redactions, Native Excel Redactions, Image Restrictions		
	Redact Externally Redacted Native – Add, Edit, View		
	Redact Original Native – Add, Edit, View		
	Redact Produced Document – Add, Edit, View		
Administrator	**Document** – View, Delete, Edit, Secure, Redact Document, Highlight Document, Local Access (Download, Copy Text)	Redact Projects	Convert Spreadsheet Markups
	Markup Set – Add, View, Delete, Edit, Secure	Redact Original Native	
	Redact – Add, Edit, Delete, View, Secure, Place/Edit Manual Redaction, Place/Edit Manual Highlight, Clear Markups, Unhide Excel Content, View Quality Control Panel, Accept/Reject Quality Control Entries, Input Custom Redaction Text, Native PDF Redactions, Native Excel Redactions, Image Redactions	Redact External Markups	Revert Native Redactions
	Redact Externally Redacted Native – Add, Edit, View, Delete, Secure	Redact Settings	
	Redact Original Native – Add, Edit, View, Delete, Secure	Redact Redacted File	

Role (Admin or User)	Object Security	Tab Visibility	Other settings
	Redact Produced Document – Add, Edit, View, Delete, Secure	Redact Audits	Prepare Excel for Redact
		Redact Externally Redacted Native	
		Redact	

Sentiment analysis
The feature permissions designated for Sentiment analysis are:

Role	Object Security	Tab Visibility	Other settings
Administrator	**Sentiment Analysis Job** – Add, Edit, View, Delete, Secure	Sentiment Analysis Jobs	Detect Sentiment
	Sentiment Result – Add, Edit, View, Delete, Secure	Sentiment Results	
		Documents	

Structured analytics
The feature permissions designated for Structured analytics are:

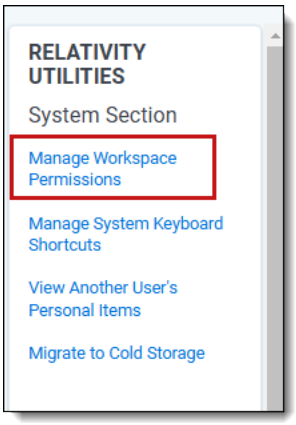
Role	Object Security	Tab Visibility	Other settings
User	**Alias** - View	Structured Analytics Results	
	Alias Domain - View	Documents	
	Analytics Profile - Add, Edit, View	Aliases	
	Entity - View	Repeated Content Filters	
	Repeated Content Filter – Add, Edit, View	Analytics Profiles	
	Structured Analytics Errors - View	Alias Domains	
	Structured Analytics Results – Add, Edit, View	Structured Analytics Set	Communication Analysis Widget
	Structured Analytics Set – Add, Edit, View	Entities	Email Thread Visualization
Administrator	**Alias** – Add, Edit, View, Delete, Secure	Structured Analytics Results	
	Alias Domain – Add, Edit, View, Delete, Secure	Documents	
	Field – View, Edit	Alias Domains	
	Analytics Profile – Add, Edit, View, Delete, Secure	Aliases	Email Thread Visualization

Role	Object Security	Tab Visibility	Other settings
	Repeated Content Filter – Add, Edit, View, Delete, Secure	Analytics Profiles	
	Structured Analytics Errors - View	Entities	Communication Analysis Widget
	Structured Analytics Results – Add, Edit, View, Delete, Secure	Indexing & Analytics	Assign to Entity
	Structured Analytics Set – Add, Edit, View, Delete, Secure	Structured Analytics Set	Merge

35.6 Setting workspace permissions

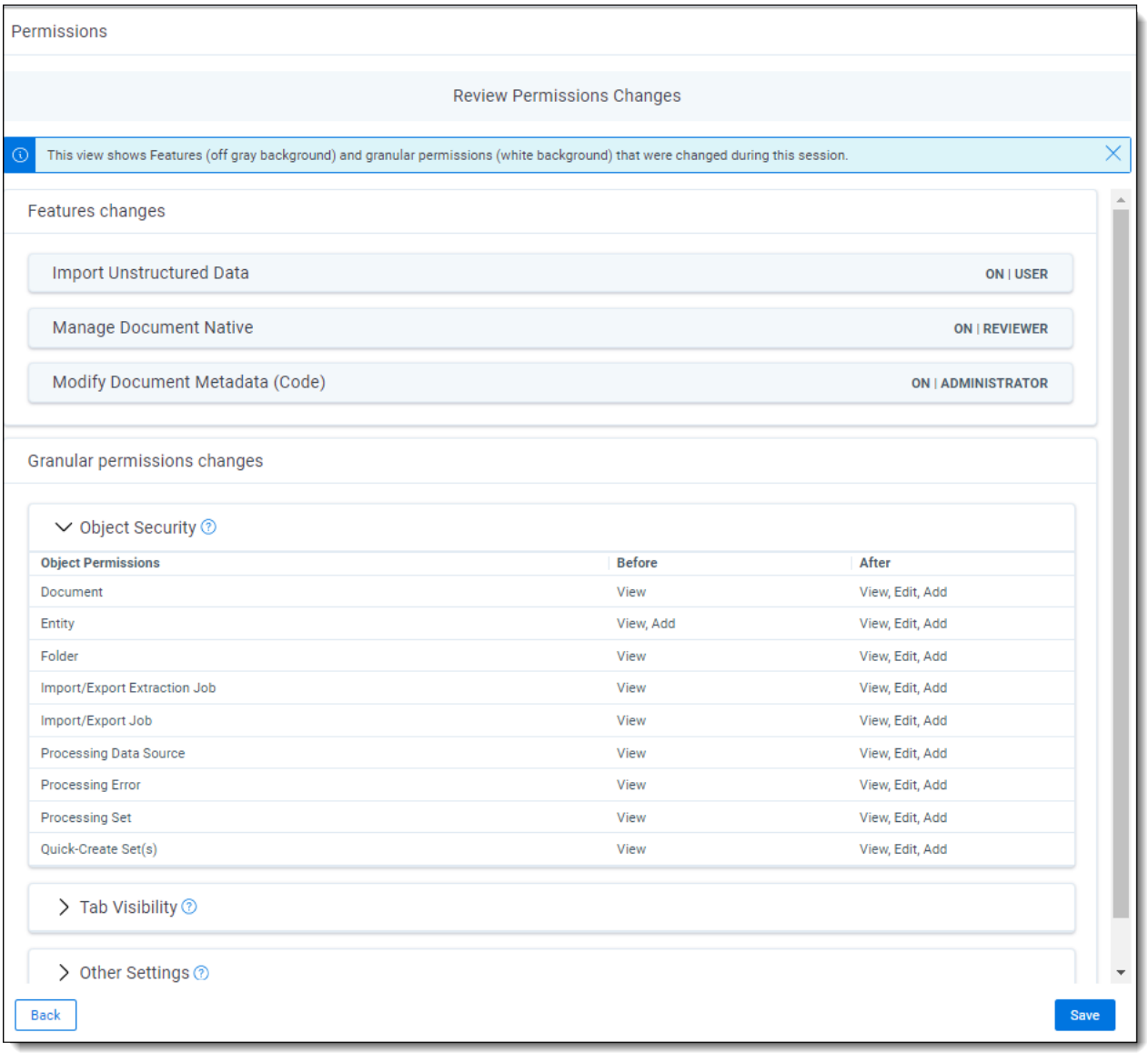
Permissions can be set based on features using the Features tab on page 665. Edit workspace permissions using the Workspace Security dialog accessible from the **Workspace Details** tab. Access the dialog using the following steps in a workspace:

1. Click the **Administration** tab followed by **Workspace Details**.
2. Click **Manage Workspace Permissions** in the Relativity Utilities console to open the Workspace Security dialog.



3. Do any of the following:
   - Perform group management. Refer to Group Management on the next page for more information.
   - Modify the settings on the tabs as needed. Refer to the Features tab on page 665, Object Security tab on page 667, Tab Visibility tab on page 668, or Other Settings tab on page 670 sections for specific information of each tab.
4. Click **Revert All** to undo all unsaved changes. The features return to their previous settings.
5. Click **Review and Save** after modifying settings.

6. Review the unsaved changes displayed on the Review Permissions Changes modal.



- **Features changes**—lists the features that were changed and how they were changed. Changes at the granular level may affect the status of the feature setting, so review this information carefully.
- **Granular permissions changes**—lists the changes made at the granular permissions level, including those resulting from feature changes or direct edits at the granular permission level.

7. Click **Save** to finalize the changes.

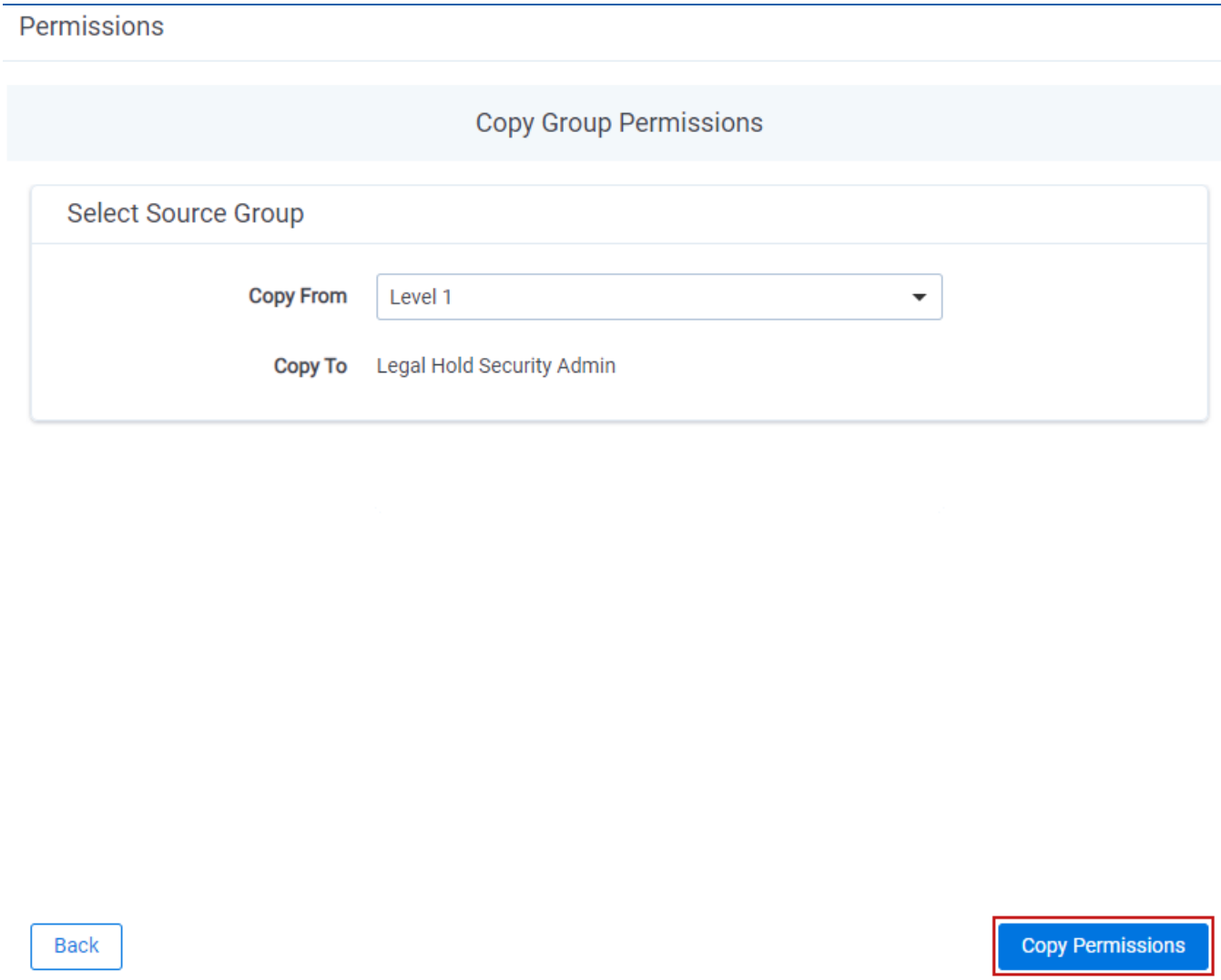
Note: To add and remove groups, you must have the Edit Security permission set for the Workspace object and the Add and Delete permissions set for the Groups object (instance level security).

35.6.1 Group Management

The Group Management tab displays all groups added to a workspace. The following actions are available for groups added to a workspace other than System Admins:

- **View Users**—displays a list of users in a group.
- **Edit Permissions**—opens the Object Security tab for you to begin editing the workspace permissions for a group.
- **Copy**—opens a list of groups whose permission settings you can transfer to the group. Select a group and click **Copy Permissions** at the bottom of the list to complete the transfer.

Note: Copying permissions from one group to another will cause **all** permissions to be overwritten. This includes item level security permissions for the target group.



- **Preview**—preview currently applied security settings for a group. See Preview Security for more information.
- **Add/Remove Groups**—opens the Add/Remove Groups dialog on which you can search for and add or remove groups.

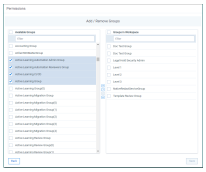
Notes:

- To add and remove groups, you must have the Edit Security permission set for the Workspace object and the Add and Delete permissions set for the Groups object (instance level security).
- Relativity displays a warning message when a System Admin attempts to edit or copy permissions for any group in a client domain. This warning makes the System Admin aware that modifying permissions may have significant consequences. For example, changing permissions may allow client domain users to modify items outside their tenancy. The System Admin can click **Manage Permissions** to proceed with the update or **Cancel** to exit the pop-up window.

35.6.1.1 Add/Remove Groups

The Add/Remove Groups window displays the following lists:

- **Available Groups**—lists available groups in your Relativity environment not yet granted access to the workspace.
- **Groups in Workspace**—lists groups granted access to the workspace.



Adding groups to a workspace

To add one or more groups to a workspace, follow these steps:

Note: If you are in a Workspace admin group, you must have the instance-level **Edit** permission to the **Group** object to add a group to a workspace.

1. Click the **Administration** tab followed by **Workspace Details**.
2. Click **Manage Workspace Permissions**.
3. Click **Add/Remove Groups** on the Group Management tab.
4. Select one or more groups from the **Available Groups** list in any order. Scroll the list or search for a specific group using the search bar.
5. Click **Add**.
6. Click **Save**.

Removing groups from a workspace

To remove one or more groups from a workspace, follow these steps:

1. Click the **Administration** tab followed by **Workspace Details**.
2. Click **Manage Workspace Permissions**.
3. Click **Add/Remove Groups** on the Group Management tab.
4. Select one or more groups from the **Groups in Workspace** list in any order. Scroll the list or search for a specific group using the search bar.
5. Click **Remove**.
6. Click **Save**.

35.6.2 Features tab

The Feature tab simplifies permission setup by reducing the number of steps needed. Instead of navigating through Object, Tab Visibility, or Admin tabs, you can enable a feature with a single action.

Each feature includes specific actions, which represent individual tasks users can perform within that feature. Granting access to actions lets you control permissions more precisely, allowing a group to perform certain tasks without providing full access to the entire feature.

A feature or action combines the required permissions drawn from the other three tabs. When you enable a feature, all associated permissions activate automatically. For an overview of features and actions, see Feature permissions, Feature actions.

35.6.2.1 Considerations

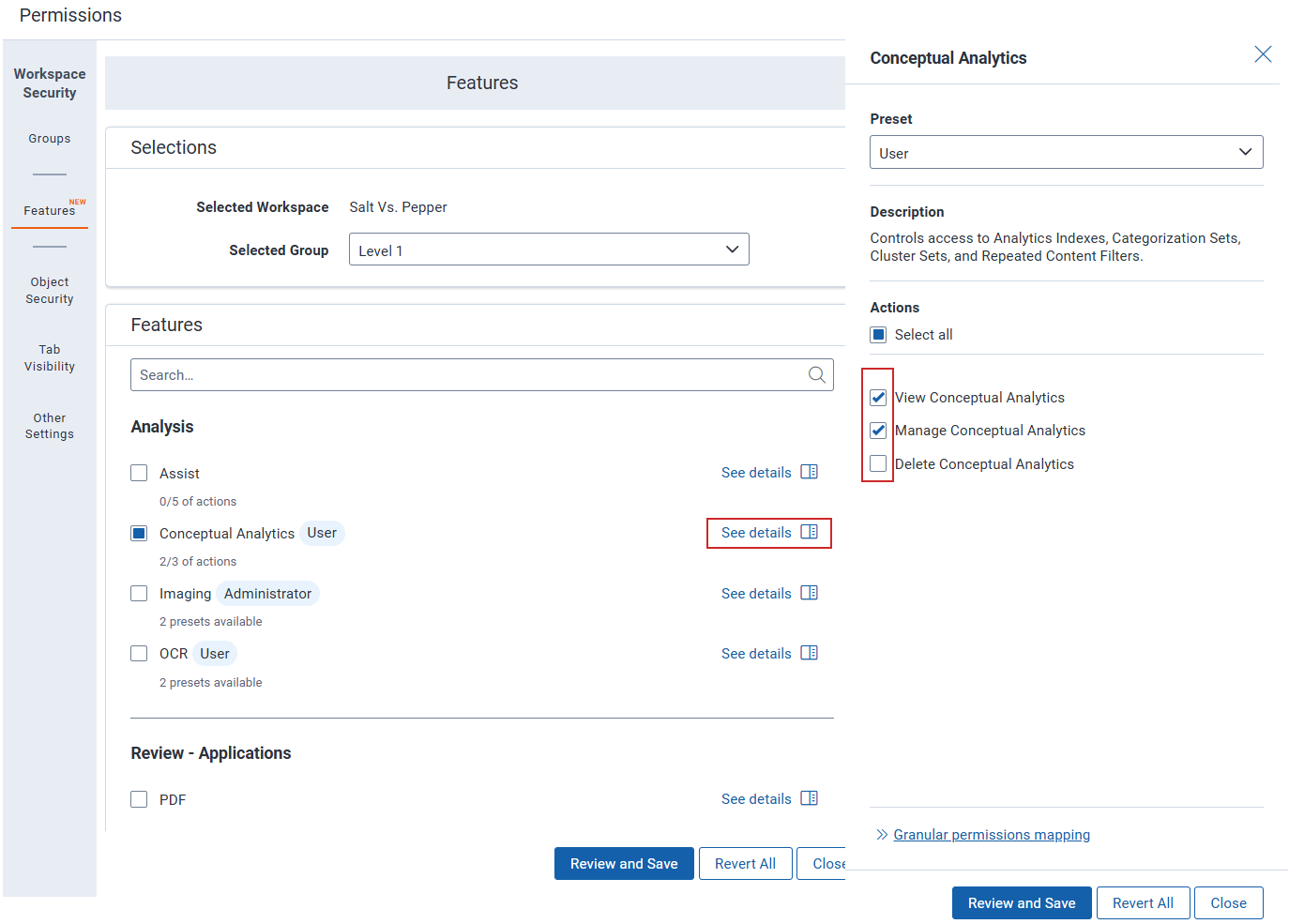
Feature and granular permission settings affect each other. The effect depends on whether the feature is modernized. For the rules and examples, see Feature permissions.

35.6.2.2 Using the Features tab

The Features tab lists the features available for the selected group. You can do the following from this tab:

- Use the **Search bar** to find a feature in the list.
- Select the checkbox next to a feature to grant access to it.
- Click **See details** to open a panel for the feature. From the panel you can select a preset, select individual actions, and open the granular permissions mapping.

For an explanation of features, actions, presets, and feature states, see Feature permissions .



35.6.2.3 Frequently asked questions

Can I still use granular permissions?
It depends on whether the feature is modernized. For a modernized feature, you manage permissions only through the Features tab, and the granular permissions are locked. For a feature that is not modernized, you can still edit granular permissions on the Object Security, Tab Visibility, and Other Settings tabs. See Feature permissions for the list of modernized features.

Why is the user not seeing a tab that should be available as part of the enabled feature?
First, ensure the user has Tab Visibility by looking for a blue check mark next to the tab name in the See Details pane of the feature. If confirmed and still not visible:

1. Check item-level Security: if the tab is secured against the selected group, it will not be available in the application.
2. Check the tab configuration: if the tab's parent is not visible, it will not appear in the side panel or hamburger menu, but it will still be accessible via Quick Nav.

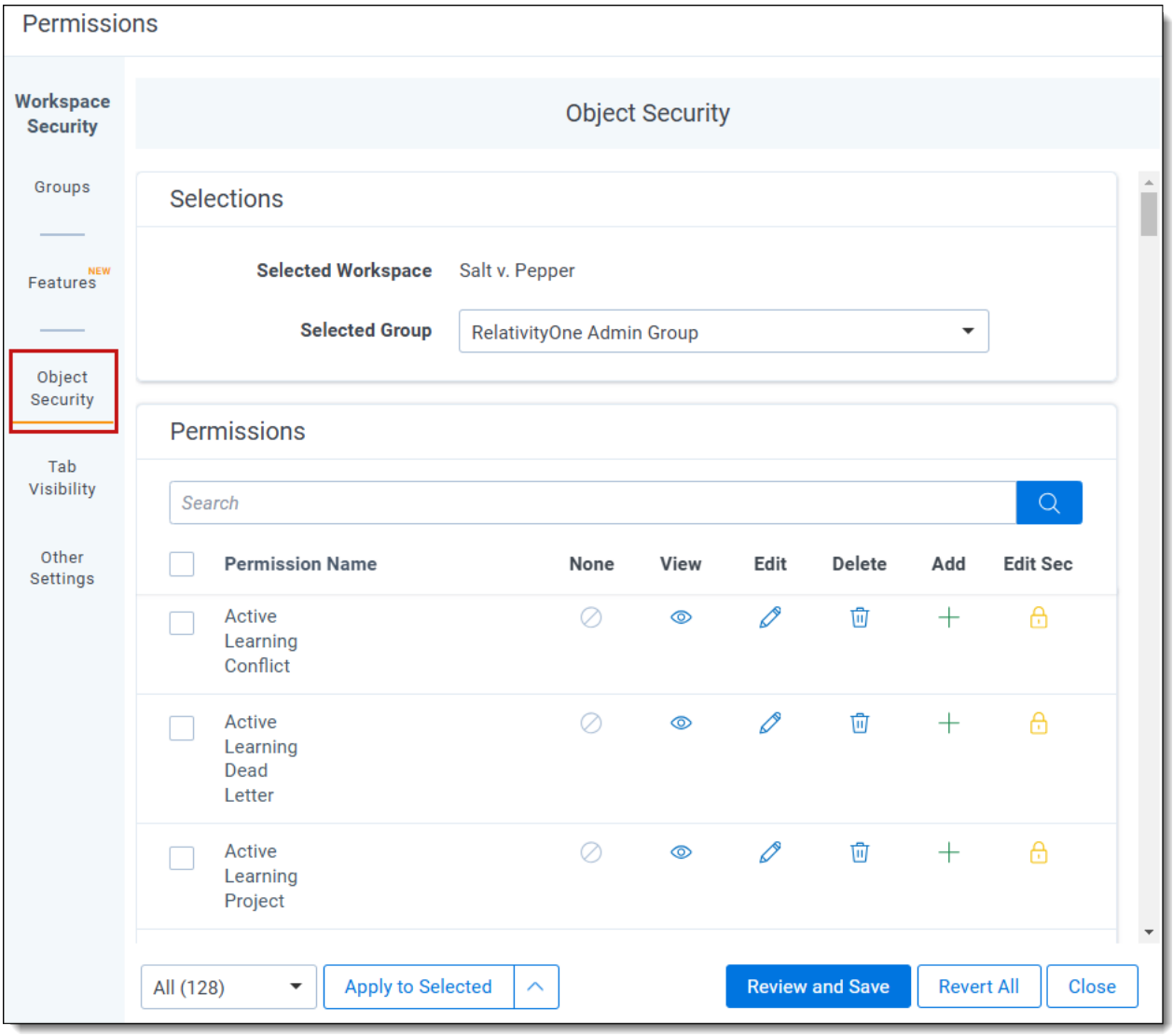
Why are certain features not available in my workspace?
Feature availability is determined by your workspace configuration. Features will only show when the relevant applications are installed in the workspace. If any necessary components are missing, the feature will not be available.

I had enabled a Feature for a specific group earlier, but now it appears as disabled for that same group. What could have caused this?
Although this situation should be rare, it can occasionally arise. This typically occurs when the feature definition is changed to include a permission that the group does not have, often because a new permission has been introduced to the system. To resolve this issue, re-enable the feature for the affected group.

35.6.3 Granular permissions

Granular permissions
Object Security tab

Use the Object Security tab to manage the following object-level permissions for a selected group:



- **None**  —denies users access to the object.
- **View**  —view the object. This is the lowest level object permission.
- **Edit**  —edit and view the object.
- **Delete**  —delete, edit, and view the object.

- **Add**  —add new objects. This icon turns blue when the setting is unsaved; once you click Save, the blue icon becomes grey. This icon turns green when you give users this permission both when the setting is unsaved and saved.
- **Edit Security**  —grants users the ability to edit the security of objects. This icon turns blue if you click twice indicating a not applicable status.

See Object list for a list of securable objects.

35.6.3.1 Assigning object-level permissions

To assign object-level security permissions to a group:

1. Click the **Administration** tab followed by **Workspace Details**.
2. Click **Manage Workspace Permissions** in the Relativity Utilities console.
3. Click **Edit Permissions** for a group on the Group Management tab. Or, click **Object Security** and select a group from the **Current Group** drop-down menu.
4. Click the applicable object security permission(s) you want to apply to the selected group. Icons for selected security permissions appear in color, and names of objects for which you changed security permissions appear in italic typeface until you save the modified permissions.
5. Click **Save**.

Assigning mass permissions to a single group

To update multiple permissions to a single group:

1. Click the applicable object security permissions
2. Click the down arrow on the menu below.
3. Select the appropriate permission type.
4. Click **Apply**.

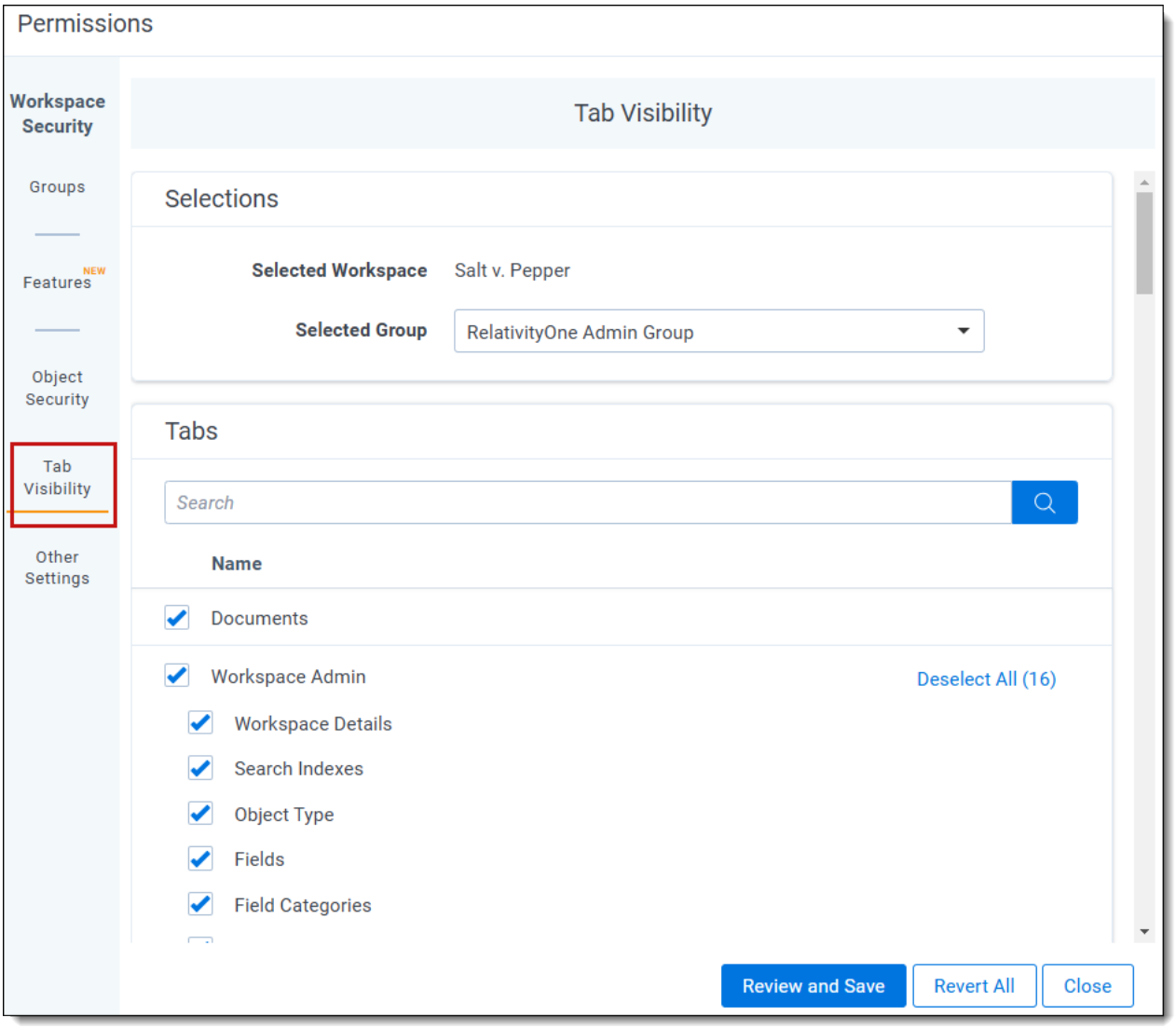
Denying object access

To deny a group any access to an object, click the icon. After setting a group's permission level to None, the icon appears in color  .

35.6.4 Tab Visibility tab

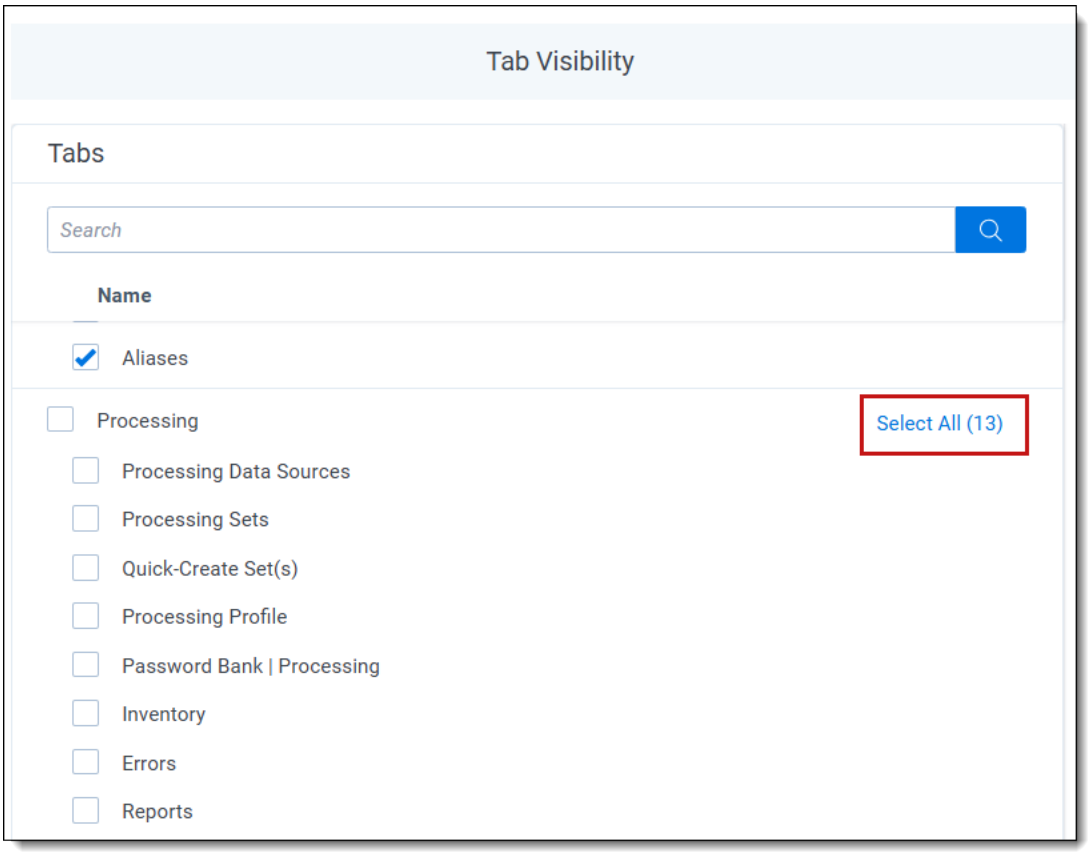
The Tab Visibility tab lists all parent and child tabs in a workspace. Combine object-level permissions and tab visibility to give users the tools they need to complete their tasks.

To grant access to workspace tabs, select all tabs you want visible for a selected group. For a complete list of tabs, see Tab Visibility.



35.6.4.1 Selecting parent and child tabs

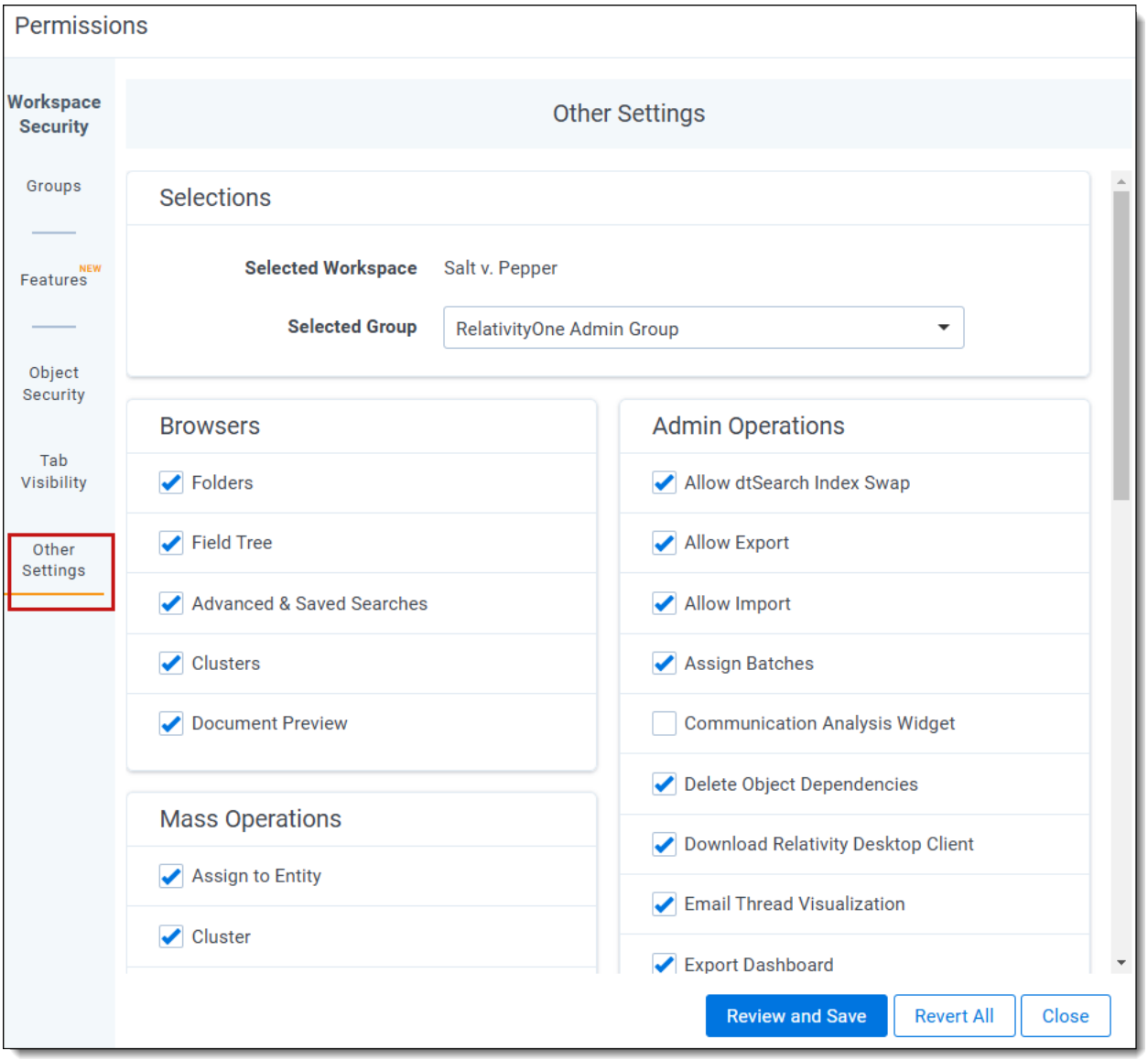
Indented tab names are child tabs of a parent tab. The following example shows the parent tab of Processing and its child tabs. To select a parent tab and all child tabs, click **Select All (#)** for the parent tab. The link changes to "Deselect all (#)", which clears all check marks.



When you select at least one child tab, the related parent tab is automatically selected. If you only want the child tab selected, click the parent tab to clear its selection.

35.6.5 Other Settings tab

The Other Settings tab lets you control browser visibility and access to mass operations and admin operations for a group in a workspace. For a complete list of admin operations, see Workspace security in the admin guide. To enable these settings for a group, select the desired options.



35.6.6 Saving permissions for a group

In the Workspace Security dialog you can switch between the Object Security, Tab Visibility, and Other Settings tabs before saving modified security permissions for a selected group. If you modify security settings on any of these three tabs, and try to close the dialog or click the Group Management tab, Relativity prompts you with the following options:

- **Save**—saves all permissions changes and applies them to the selected group.
- **Revert**—discards all unsaved permissions changes and reverts to the group's last saved permissions.
- **Cancel**—cancels the attempted dialog close or tab change action.

After making security changes on the Object Security, Tab Visibility, and Other Settings tabs, click **Save** at any time to apply the selected permissions settings.

35.7 Relativity object security

Individual items inherit their objects' rights. For example, a group's rights to an individual field are determined by the field's rights across the workspace. In some cases, you may want to change the security for certain items.

Say you have a group doing contract review, and you want the group to be able to see the custodian field, but not be able to edit it. You can customize object permissions to ensure users have view rights, and not edit rights to the custodian field object.

To change the security on individual items:

1. Navigate to the item's details page, and then click **Edit Permissions**. For example, to open the details page for a particular view in a workspace, click the **Administration** tab followed by the **Views** tab, and then click the name of a view in the list. Or, click the  icon for an object in a item list view with the Security field added.
2. Click the **Override Inherited Security** toggle on the **Group Management** tab to set one of the following options:
    - **OFF** - object inherits security settings from its parent object (i.e., case workspace).
    - **ON** - the item uses its own security settings instead of the workspace-level settings. The item starts with the same permissions as the workspace, and you can change which groups can access it and what each group can do.

    Note: Altering security permissions from override inherited security to inherit security and vice versa may involve a wait time for 50,000 records or more. If this occurs, a notification appears to inform you of the impact of the change.
3. If you set **Override Inherited Security** to **ON** to modify an object's security, click **Add/Remove Groups** to add or remove groups for which you want to set explicit object permissions.

    Note: To remove a group's access to an item completely, remove the group from the item. You can't set a group's access to **None** on an item. If a group is added to an item, the lowest level of access it can have is **View**.
4. Click **Edit Permissions** for a group to modify the group's object security rights.
5. Select any of the following object permissions to assign to the group:
    - **None**  —denies users access to the object.
    - **View**  —view the object. This is the lowest level object permission.
    - **Edit**  —edit and view the object.
    - **Delete**  —delete, edit, and view the object.
    - **Add**  —add new objects. This icon turns blue when the setting is unsaved; once you click Save, the blue icon becomes grey. This icon turns green when you give users this permission both when the setting is unsaved and saved.

- **Edit Security**  —grants users the ability to edit the security of objects. This icon turns blue if you click twice indicating a not applicable status.

Note: Not all permissions listed above apply to all objects. The Object Security tab doesn't display the icon for a permission that doesn't apply.

6. Click **Save**.

35.7.1 Securing a folder for selected groups

Folders can also be managed so that only selected groups can access a folder's contents.

To change which groups can access a folder:

1. Navigate to the Documents tab.
2. Right-click on the folder you wish to control a group's access to, and then select **Secure**.

Note: Parent-level folders cannot be secured.

3. Click **Override Inherited Security** to toggle it **ON**.
4. Click **Add/Remove Groups**.
5. Select the group or groups that you wish to add or remove, and then click the **Add** or **Remove** button.
6. Once you've added or removed all of the desired groups, click **Save**.
7. Optionally, click **Edit Permissions** next the desired group to modify that group's folder security rights.
8. Select any of the following folder permissions to assign to the group:
   - **View**  - view the folders. This is the lowest level folder permission.
   - **Edit**  - edit and view the folders.
   - **Delete**  - delete, edit, and view the folders.
   - **Add**  - add new folders. This icon turns blue when the setting is unsaved; once you click Save, the blue icon becomes grey. This icon turns green when you give users this permission both when the setting is unsaved and saved.
   - **Edit Security**  - grants users the ability to edit the security of folders. This icon turns blue if you click twice indicating a not applicable status.
9. Click **Save**.

   The folder will display a padlock icon  to show that **Override Inherited Security** has been toggled **On** for that folder.

35.7.1.1 Folder security inheritance

If a user drags a folder with item-level security into another folder, the new child folder inherits the parent folder's security.

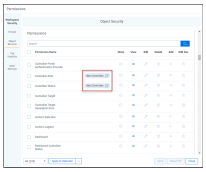
Note: For more scenario examples, see Permissions scenarios

35.7.1.2 Identify and edit item-level security

System Administrators can quickly identify why certain users can't access specific objects when item-level security permissions are set on them.

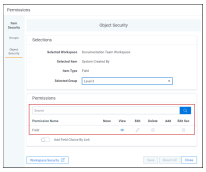
To identify and change item-level permissions that are overridden, follow these steps:

1. Navigate to the workspace Details tab and click on the Manage Workspace Permissions link.
2. On the Object Security tab, you will find a list of objects (documents, items, or other artifacts) within the workspace. If item-level security is applied to an object, it will be marked with an 'Item Overrides' link.



3. Click on the 'Item Overrides' link to open a new window. From here, the system will redirect you to the item security page to customize permissions for the chosen item.





35.8 Preview security

The preview security feature lets system admins interact with Relativity as if they are logged in as a specific user or a member of a specific group. A system admin can then easily verify that the correct permissions are applied without logging in to Relativity under a different account.

For example, say you secured a layout from a user and you want to verify that person no longer has access to the layout. With the preview security feature, you can select the user and view Relativity as that person right from your system admin account.

Be aware that if you perform a job while previewing a user's security settings, the audited action is credited to your username and not to the user whose security you were previewing when you started the job.

Notes:

- The preview security feature does not allow the system admin to monitor the actions of a user in real time. It only simulates what the user would see.
- The following features do not work with preview security:
  - Testing Review Center access
  - Testing PI Detect permissions
  - Checking out batches
  - Viewing a previewed user's Assist conversations. The preview shows the conversations of the logged-in system admin, not the previewed user's conversations.
- See Permissions scenarios for more information about how permissions work.

35.8.1 Previewing security from the Workspace Details tab

Additional permission requirements are needed for **Workspace Administrators** previewing security from the Workspace Details tab. This does **not** apply to System Administrators. To initiate a preview, at least one of the following conditions must be met:

- The group being previewed must belong to only **one** workspace and have no instance-level permissions.
- The user initiating the preview must be a member of the group they are attempting to preview.
- The user initiating the preview must have the **edit permission** on the group they are attempting to preview.

Once one of these conditions are met, a workspace administrator must follow these steps to preview the security of a user at the workspace-level, but only from the workspace details page:

1. Click the **Administration** tab, and then click **Workspace Details**.
2. Click **Manage Workspace Permissions**.
3. Click **Preview** for a group on the **Group Management** tab.
   A preview window opens and shows the workspace as it looks for any user in the group. A bar labeled **You are previewing as a member of the <group name> group** appears at the top of the window indicating that this instance of the workspace is not the system admin's view, but rather a preview of the group's view according to the assigned permissions.
4. Click **Exit Preview** in the preview bar to close the preview security session and return to workspace details.

35.8.2 Previewing security from the Groups tab

To preview security from the **Groups** tab, follow these steps as a system admin:

1. Navigate to the **Groups** tab.
2. Click the group name of the group whose permissions you want to preview.
3. Click **Preview Security.**A preview window opens and shows what members of the group see upon logging in to Relativity. A bar labeled **You are previewing as a member of the <group name> group.** appears at the top of the window indicating this instance of the workspace is not the system admin's view, but rather a preview of the group's view according to the assigned permissions.
4. Click **Exit Preview** on the preview bar to close the preview security session and return to the group details.

35.8.3 Previewing security from the Users tab

To preview security from the **Users** tab, follow these steps as a system admin:

1. Navigate to the **Users** tab.
2. Click the full name of the user whose permissions you want to preview.
3. Click **Preview Security**.A preview window opens and shows what the user sees upon logging in to Relativity. A bar labeled **You are previewing as <username>.** appears at the top of the window indicating that this instance of the workspace is not the system admin's view, but rather a preview of the user's view according to the assigned permissions.

   Note: If the user is a member of the System Administrators group, the preview security button is unavailable. The favorites menu and some options in the user menu are disabled during preview security sessions.

4. Click **Exit Preview** on the preview bar to close the preview security session and return to the user details.

35.8.4 Preview security audit

Actions made during preview security sessions are audited as actions of the system admin performing the preview session, not the user being impersonated. Any action performed by a system admin are audited. Additionally, the start and end of a security preview session are audited:

- **View Audit from User Details:** The audit lists the **User Name**, **Action**, and **Timestamp** of any preview security session. The audit reports the username of the system admin performing the preview security session and Timestamps for **Security Preview Started** and **Security Preview Ended**.
- **View Audit from Group Details:** The audit lists the **User Name**, **Action**, and **Timestamp** of any preview security session. The audit reports the username of the system admin performing the preview security session and Timestamps for **Security Preview Started** and **Security Preview Ended**.

35.9 Permissions scenarios

In this topic, you can explore various scenarios that involve managing permissions.

See the following related pages:

35.9.1 Hierarchical structure

System administrators have the highest level of managerial rights followed by workspace administrators. Standard users have limited administrative capabilities and primarily operate within the permissions assigned to them.

- **System administrators**—have the highest level of administrative rights with broad access to system settings, configuration, and management functions. Their permissions and rights supersede those of other user roles. They can control the overall system behavior, user management, security settings, and other administrative tasks.
- **Workspace administrators**—have administrative control over specific workspaces. They can manage settings, configurations, and security within their assigned workspaces. Additionally, they can modify object permissions, manage users and groups, configure layouts, and perform other workspace-specific administrative tasks.
- **Standard users**—do not have administrative privileges and cannot modify system or workspace settings. They are only allowed to access and interact with objects based on the permissions assigned to their user accounts or the groups they belong to.

35.9.2 Client domains

In the hierarchical structure of permissions, client domain permissions are positioned below system administrators but above workspace administrators and standard users. This arrangement facilitates the delegation of administrative tasks to a specific user group known as *client domain admins*. Unlike the System Administrator group, client domain admins have limited visibility and control confined to their designated client domain. This isolation feature ensures more precise administrative control over a defined segment of the environment, preventing unauthorized access or changes to the overarching Relativity aiR instance.

Client domain admins possess the flexibility to adjust permission settings for various objects within their domain, customizing them to align with their specific preferences. However, these permissions are restricted solely to their allocated domain and do not extend beyond it. This protective measure guarantees that they cannot access or modify permissions beyond their designated client domain. By implementing client domain permissions, system administrators can proficiently oversee their domain while upholding the integrity and security of the broader Relativity environment.

Note: Violating the boundary of client domains in a system like Relativity can lead to significant risks and consequences, affecting data security, compliance, and overall system integrity. Client domains serve as isolated environments within the system, providing each client with a segregated space to manage their own data and operations independently.

35.9.3 User groups

User groups serve as a means to organize and manage users who share similar roles or permissions. You can assign user groups at either the workspace level or the system level, based on the intended extent of access and management. When assigned at the workspace level, user groups pertain to a particular workspace, governing the permissions and access rights within that workspace. On the other hand, at the system level, user groups have wider-ranging implications and can influence permissions and access across multiple workspaces within the Relativity environment.

35.9.4 Template groups

Template groups can play a crucial role in efficiently copying over permissions. Template groups allow you to define and configure sets of permissions that can be applied to multiple workspaces or objects. You can create template groups to encompass specific permission settings. These can include object-level and item-level security, document-level security, and field-level security.

These templates provide predefined sets of permissions that can be applied to new workspaces. User groups can be added or removed from specific security workspace templates, allowing for granular control over access and permissions based on the needs of each template. This enables administrators to tailor the security settings for different types of workspaces. This guarantees users are assigned to appropriate groups with the necessary permissions for their roles.

35.9.4.1 Review templates

Use Review templates for the review phase of a legal case or investigation. They provide tools and features for document review, coding, tagging, and production.

There are four main customizable Review Template groups:

1. **Level 1 Reviewer:**
    - Allowed to view and apply tags to documents.
    - Mark documents as ‘responsive’ or ‘privileged’ for case relevance to help categorize and classify.
2. **Level 2 Reviewer**
    - All permissions of a Level 1 Reviewer.
    - Add and edit tags.

- Able to redact sensitive and confidential information.
- Apply highlighting to sections of a document.
- Ability to add annotations or comments in a document.

3. **Attorney Reviewer**
    - All permissions of a Level 2 Reviewer.
    - Create and modify saved searches.
    - Mass operations capabilities.
    - Create and manage redactions and annotations.
    - Access reporting features for analysis and Import/Export documents.
4. **Administrator Reviewer**
    - All permissions of an Attorney Reviewer.
    - Manage review workspace settings like creating user accounts and groups.
    - Configure fields.
    - Setting up searches and saved searches.
    - Configure security settings.
    - Manage review batches and workflow assignments.
    - Customize layouts.

35.9.4.2 Investigation templates

Investigation templates are designed for conducting investigations and offer functionality for evidence management, interview coordination, case progress tracking, and report generation. Unlike Review templates that primarily concentrate on document review and tagging, Investigation templates prioritize broader facets of the investigative process and include several key functionality:

1. **Case Management**—investigation templates offer tools to track and manage case-related information, including key dates, participants, and case notes.
2. **Evidence Tracking**—these templates track and help organize evidence which allows investigators to associate documents, interviews, and other artifacts with specific cases or subjects.
3. **Interview Management**—investigation templates may include features to manage document interviews conducted during the investigation, which can involve capturing interview transcripts, tagging key information, and linking them to the relevant case or subject.
4. **Data Analysis**—graphs can provide data analysis and visualization which allows investigators to identify patterns, connections, and trends within the collected data.
5. **Report Generation**—there are reporting capabilities in Investigation templates which allow comprehensive summaries of the investigation's findings, supporting documentation and relevant insights.

35.9.4.3 Early case assessment (ECA) templates

ECA templates focus on the initial assessment of a case or investigation. They provide tools for data ingestion, indexing, searching, and analysis to quickly identify key information used to make informed decisions. Here are some ways ECA templates differ from others:

1. **Purpose**—they are specifically designed to evaluate large volumes of data or information at the early stages of an investigation and quickly identify and rank relevant information, assess the merits of a case, and make

informed decisions regarding further actions.

2. **Data Volume and Complexity**—ECA templates can handle large and complex datasets commonly found in cases. They offer mechanisms for efficient data ingestion, indexing, and searching across various sources, such as emails, documents, and electronic records. In contrast, review templates and investigation templates may not necessarily deal with such extensive data volumes and may have different mechanisms for data organization and analysis.
3. **Time Sensitivity**—ECA templates aim to expedite the initial assessment of a case or investigation, taking into account time constraints and the necessity for rapid decision-making. They strive to pinpoint critical information, potential risks, and key players early in the process to steer subsequent actions. While review templates and investigation templates might involve longer timeframes and more intricate procedures to facilitate comprehensive analysis and evaluation.
4. **Early Case Strategy**—ECA templates often incorporate features that allow legal teams to develop an early case strategy based on the initial assessment. This includes identifying key issues, potential legal theories, and relevant documents or evidence that may impact the case.
5. **Legal Compliance and Privilege Considerations**—ECA templates need to address legal compliance requirements and considerations for maintaining attorney-client privilege and work product protections. They may provide features to flag privileged information, conduct privilege review, or track legal holds on relevant documents. Review templates and investigation templates may have different compliance requirements depending on the nature of the review or investigation.

35.9.4.4 Security workspace templates

With Security workspace templates, you can establish a secure environment within Relativity. Using these templates, you can define access controls, manage user permissions, and ensure data security within the workspace.

35.9.5 Object-level permissions

You can employ object-level security to restrict entry to specific documents or items within the workspace. These objects encompass various components such as workspaces, documents, fields, and other elements within the system.

Tailoring access to these objects can be done on an individual user or group basis. User access determines the extent of permissions and actions a specific user can perform. Group access simplifies the management of permissions for a set of users in the same category. By managing user or group access, you can determine who is authorized to view, edit, or carry out specific actions on the objects within the system.

Furthermore, objects can have document-level or field-level permission configurations. Document-level permissions allow you to control access to individual documents based on user roles or specific criteria. Similarly, field-level permissions offer the ability to regulate access to particular fields within a document. You can set restrictions on who is permitted to view or modify specific fields based on user or group permissions.

Note:
The **Manage Object Types** permission grants group members the ability to:

- Create a new tab for a new object type when adding the new object type.
- Automatically gain view, add, edit, delete, and secure permissions for all newly created object types.
- Automatically gain tab visibility for newly created tabs.

35.9.6 Item-level permissions

Item-level permissions control access to a single item in a workspace, such as one document, view, or OCR set, instead of relying on the permissions set for its object type across the workspace. With item-level permissions, you can:

- restrict an item to specific groups. When you turn on **Override Inherited Security** for an item, only the groups on that item's security list can access it.
- define what each of those groups can do with the item, such as view, edit, delete, or edit its security. Item-level permissions are most often used to give a group less access to an item than it has across the workspace, but you can also give a group more access.

When you turn on **Override Inherited Security** for an item, the item starts with the same permissions as the workspace-level settings for its object type. You can then change the permissions for that item. From then on, the system uses the item-level permissions for that item and ignores the workspace-level settings. For example, if a group has **None** for the OCR Set object at the workspace level, but you add that group to the item-level security of a specific OCR set, users in that group can view that OCR set.

Note: To remove a group's access to an item completely, remove the group from the item using the **Add/Remove Groups** button. You can't set a group's access to **None** on an item. If a group is added to an item, the lowest level of access it can have is **View**.

To change item-level permission settings, you must navigate to the specific document or object and make changes individually.

35.9.7 Document unitization

The Document unitization solution allows users to split imaged documents into many child documents. This solution consists of several components, including the Relativity application, dynamic objects with associated object rules, event handlers, manager and worker agents, and views and layouts on the Document object.

To use the Document unitization solution, users must have the following permissions:

Object Security:

- Document—View, Edit, Add
- Add Image
- Unitization Job—View

Layout Permissions:

- **View** and **Edit** permissions on the Document Unitization layout

Note: Users who need to monitor the status of unitization jobs or requests must have **View** permissions on the Unitization Job object. The solution does not function when document item-level security is enabled. To ensure compatibility, configure folder-level security instead and grant the appropriate groups **Add Document** and **Add Images** permissions per folder.

35.9.7.1 Important considerations

Take the following into consideration when using document unitization solution:

- Unitization only works on imaged documents, not native documents.
- During unitization:
  - Relativity tags the parent document as a parent and each child document as a child.
  - redactions from the parent document are not carried over to the child documents.
  - child documents do not receive any propagated metadata.
- You can unitize any document that has images.
- You can create multiple instances of manager and worker agents to distribute the workload.

- You cannot:
    - unitize child documents further.
    - perform document unitization on a parent document currently undergoing unitization. You can verify the successful creation of all child documents by checking the Related Items pane before initiating a new unitization request.
- You can access the Document Unitization layout in the mass edit drop-down menu. It's important not to use it for splitting documents since the event handler framework does not execute from the mass operation framework.
- You need to install the Document Unitization solution in at least one non-administrative workspace to confirm the agents remain active in the environment.
- Document Utilities is a Relativity application that contains two solutions: Move to Folder (a mass operation) and Document unitization. Installing the Document Utilities application automatically installs the Move to Folder mass operation.

35.9.7.2 Deployment and configuration

Note: The solution does not process any data in a workspace if the associated resource pool does not have its own manager and worker agents. In such cases, document unitization jobs will remain inactive in the queue.

Do the following to deploy and configure document unitization:

1. Add the Document Utilities application to the Application Library as a Relativity application.
2. Install and configure the Document unitization solution in the desired workspace.
3. Create at least one manager agent and one worker agent. You can generate multiple instances of these agents to distribute the workload.
4. Create the manager and worker agents on each instance of the agent server associated with the resource pools used in workspaces where the Document unitization solution will be used.

    Note: Document Unitization processes approximately 500 jobs per hour.

35.9.8 Scenarios

35.9.8.1 Additive permissions and Staging Explorer across workspaces

Setup:

You have two groups, **Group A** and **Group B**, and two workspaces, **Workspace 1** and **Workspace 2**.

Group A has permission to use **Staging Explorer**, and permission to access **Workspace 1**. This is your typical Client Domain Admin group.

Group B has permission to access **Workspace 2**. This is a typical Review group.

If a user is in both **Group A** and **Group B**, they have three permissions:

- **Permission to use Staging Explorer, which is an instance-wide permission.**
- **Permission to access Workspace 1.**
- **Permission to access Workspace 2.**

User Groups	Permissions	Access to Workspaces
Group A (Client Domain Admin)	Use Staging Explorer (instance-wide permission)	Workspace 1
Group B (Review)	Access to Workspace 2	Workspace 2
User in both Group A & B	Use Staging Explorer (instance-wide permission) Access Workspace 1 & 2	Workspace 1 & 2

Note: In this case, because permissions are additive, a user in both groups can use Staging Explorer to access the files on file shares for both Workspaces 1 and 2, even though neither group explicitly gives permissions to use Staging Explorer on the Workspace 2 file share. For more information regarding this, see the Permissions section of the Staging Explorer

35.9.9 Frequently asked questions

How can I set up an admin group so they can view Relativity Email Threads and Relativity Near Duplicates plus related fields in a workspace? Additionally, the group should be able to see the relational options in saved searches and in the relational views drop-down menu?

Action	Object Security Permission	Item Security	Tab	Admin Operation
View Relativity Email Threads	• View, Edit, Create, Delete, or Administer for Color Map • View, Edit, Create, Delete or Administer for Structured Analytics Set • View, Edit, Create, Delete, or Administer for Structured Analytics Results • Create, Read, Update, and Delete permissions on Email Thread, Document, and Saved Search objects.	Gives the group members the rights to select and re-assign an alias to a different entity when using name normalization in Analytics.	Email Threading	Email Thread Visualization

This tool is available for all email threading jobs that run as full builds. After the job finishes, you can view the visualization by opening any document in the document viewer.

To access and use the email thread visualization feature, it is essential to have certain security permissions in place.

Additionally, View security permissions are necessary for the following email fields:

- **Email Action**
- **Email Thread Group**
- **Email Author Date ID**
- **Inclusive Email**
- **Email Thread Hash**
- **Email Duplicate Spare**
- **Email Threading Display**

If any of these security permissions are not in place, you will not be able to use the email thread visualization tool.

Why can't I add permissions to a group to create fields?
To create fields, the Relativity Application view permission must be set to **View.**

Action	Object Security Permission	Item Security	Tab	Admin Operation
Create Fields	• Field - View, Edit, Delete, Add • Relativity Application - View	N/A	Workspace - Admin Fields	N/A

Why does an error message appear when users attempt to add a layout, even after I created and gave the new group the ability to add and modify layouts?
To create fields, the Relativity Application view permission must be set to **View.**

Action	Object Security Permission	Item Security	Tab	Admin Operation
Add or Modify Layouts	View, Edit, Create	View, Edit	Workspace Details, Layouts, Layout Sets, Layout Templates, Dynamic Objects	N/A

Why am I unable to access the Lockbox feature?
Check if the user has the Lockbox Manager security privilege assigned. If not, add the privilege to their security profile. Additionally, confirm the user has the Read permission for the relevant Lockbox folders.

Action	Object Security Permission	Item Security	Tab	Admin Operation
Lockbox feature access	View on the workspace object which allows you to access the workspace where the lockbox feature is configured.	View permission on the Lockbox object enables you to view and interact with the lockbox items within the workspace.	Custom tab	Requires initial configuration and setup, including defining the lockbox object, customizing tabs, and configuring security settings.

Why am I unable to view or modify documents in a Lockbox folder?
Check if the user has the necessary permissions to view or modify documents in the Lockbox folder. If not, assign the appropriate permissions to the user's security profile. Additionally, ensure that the Lockbox folder is not restricted to a specific group or user, and that the user has access to that group or user if necessary.

Action	Object Security Permission	Item Security	Tab	Admin Operation
Lockbox feature access	• View on the workspace object which allows you to access the workspace where the lockbox feature is located. • View permission on the folder object enables you to view the lockbox folder and its contents.	• View permission on the document object enables you to view the documents in the lockbox folder. • Edit permission on the document object enables you to modify the documents within the lockbox folder, including editing their content.	Custom tab	• Requires initial configuration and setup of the lockbox feature such as defining lockbox folders, assigning security settings, and customizing tabs or layouts. • Manage folder structure within the lockbox for organization.

Why am I unable to log in and get an error message indicating the default tab could not be determined?
If your instance setting **EnableCustomerLockBox** is set to true, it disallows System admin accounts from accessing workspaces. Another system admin must add the user to the group with access to the desired workspace. Additionally, it may be related to your object and item security permissions.

Action	Object Security Permission	Item Security	Tab	Admin Operation
Unable to log-in. Receiving	• View on the workspace	• View per-	The default tab error typically refers to the initial tab that is	• Requires initial

Action	Object Security Permission	Item Security	Tab	Admin Operation
an error message indicating the default tab could not be determined.	object which allows you to access the workspace where you are attempting to log-in. • View permission on the user object enables you to view user-related information, including your own user profile.	mission on the user item allows you to view and access your own user profile and associated settings. • Edit permission on the document object enables you to modify the documents within the lockbox folder, including editing their content.	displayed when you log-in. The exact name and content of this tab may vary depending on your organization's configuration and customization.	configuration and setup of the lockbox feature such as defining lockbox folders, assigning security settings, and customizing tabs or layouts. • Manage folder structure within the lockbox for organization.

Why am I not seeing the option to create an automated workflow in my workspace?
To confirm you possess the appropriate permissions, consult your workspace administrator. For a user to execute automated workflows, they must be affiliated with a group designated as a Workspace Admin or be part of the System Administrators group. Without authorization from an admin user, a non-administrator user cannot perform actions like viewing, editing, deleting, or adding automated workflows. Moreover, if a non-administrator user lacks the necessary permissions for those objects, they cannot edit or add dtSearch or search term reports actions.

Note: If a user receives the view automated workflows permissions, they can execute actions like Run Imaging Set, even if they lack Imaging Set permissions. Automated workflows necessitate a distinct group and user within your workspace for proper functioning. Upon application installation from the Application Library, the group and user will be automatically added to the workspace. You do not need to make any modifications, creations, or deletions to this user and group for your users to access automated workflows. This user and group are purposefully generated to facilitate the functionality of automated workflows applications.

Action	Object Security Permission	Item Security	Tab	Admin Operation
Create an Automated Workflow	The Create permission for the "Automated Workflow" item type.	The Create permission for "Automated Workflow" item type.	• Automation • Object Security	N/A

Why are other users in my workspace unable to see or use an automated workflow that I created?
The user who created the automated workflow needs to confirm they have shared it with the appropriate group or individuals in their workspace. They can do this by going to the automated workflow's settings and selecting the Share option.

Note: Create a view with the Security field enabled to allow the selected group or user to access the Automated Workflow.

Action	Object Security Permission	Item Security	Tab	Admin Operation
Share an Automated Workflow	Confirm users who need access have at minimum the View permission on the object associated with the workflow.	Review item-level permission settings to confirm the affected users or groups have the necessary permissions to access and work with the automated workflow.	• Automated Workflows List View • Security field enabled	N/A

How can I to restrict access to a particular automated workflow so only certain users or groups can use it?
You can set permissions on the automated workflow to control who has access to it. This can be done by going to the automated workflow's settings and selecting the Permissions option where you can specify which users or groups can access the automated workflow.

Action	Object Security Permission	Item Security	Tab	Admin Operation
Restrict access to an automated workflow	Restrict access to the Automated Workflow object.	Create permission for Automated Workflow item type.	• Security • Item Security	N/A

Why am I unable to modify an existing automated workflow?
You may not have the necessary permissions to modify automated workflows. Check with your workspace administrator to confirm you have the appropriate permissions.

Action	Object Security Permission	Item Security	Tab	Admin Operation
Modify an Automated Workflow	Allow the view and edit permissions for the Automated workflow object.	Edit for the Automated workflow.	• Automated workflow • Permissions	N/A

Why am I unable to use an automated workflow that requires access to certain fields?
The user who originally created the automated workflow may need to modify it to use fields that are accessible to all users who need to use it. It's also necessary to check with your workspace administrator to confirm you have the appropriate permissions.

Action	Object Security Permission	Item Security	Tab	Admin Operation
Use an Automated Workflow with access to certain fields.	View, Edit, Create, and Delete on documents or custom objects the automated workflow interacts with.	Confirm you have the appropriate item security permissions to access the items relevant to the automated workflow. If the automated workflow requires modifying or updating specific fields for items, you should have the necessary item security permissions to perform those actions.	Security	To configure object and item security permissions, you need the necessary administrative roles or permissions to modify security settings.

Note: Depending on the specific actions performed by the automated workflow, additional permissions may be required. If the workflow modifies or updates certain fields, you will at least need the Edit permission on those objects.

How can I confirm multiple users who need to collaborate on a workspace, only have access to the documents and data that are relevant to their work?
Set up workspace permissions that restrict access to specific documents, folders, or other items within the workspace. You can also assign different roles to different users, such as reviewer, editor, or admin, depending on their level of access and responsibility.

Action	Object Security Permission	Item Security	Tab	Admin Operation
Limit multiple users' access to documents and data relevant to their work	• Create a security group and associate it with the workspace. • Assign appropriate permissions to objects like documents and fields.	• Use the document-level security to restrict access to specific documents. • Create a document-level security profile to define which users or groups have access to a document based on criteria.	Workspace Security Console, Object Permissions tab, document security tab	N/A

How do I give a third-party vendor access to a workspace and prevent them from viewing or modifying any confidential or privileged information?
Create a new group or user role specifically for the vendor and set up workspace permissions that limit their access to only the documents and data that are relevant to their work. You can also use redaction or other security features to protect confidential information from unauthorized access.

Action	Object Security Permission	Item Security	Tab	Admin Operation
Limit third-party vendor workspace access to documents and data relevant to their work	View document, field, layout, and saved search.	Configure the security group's item security permissions to restrict access to confidential or privileged data.	• Security tab • Workspace tab Item tab	N/A

What permissions do I need to grant access to a workspace to a new team member?
Use the built-in security features of Relativity's workspace permissions to assign roles and permissions based on the user's job responsibilities and level of access. Custom roles can also be established for groups with specific projects or workflows, guaranteeing that each user has access only to the necessary data.

Action	Object Security Permission	Item Security	Tab	Admin Operation
Grant a new team member access to a workspace with the appropriate permissions.	• View permissions on the workspace object allows the team member to view and access the workspace.	View permissions on the user item allows the team member to view and access their own user profile and associated set-	• Documents tab • Search tab • Analytics • Admin or Con-	• User Provisioning will be needed to create a new user account, setting up login credentials, and assigning a user profile, also ensuring

Action	Object Security Permission	Item Security	Tab	Admin Operation
	• Create permission on the workspace object is optional if the team member needs to create new items or perform certain actions within the workspace.	tings.	figuration (depending on the user's role)	their user item is associated with the appropriate workspace. • Permission management • Workspace configuration

How can I streamline the process of assigning and managing permissions for a large team of users working on a complex project?
Use Relativity's advanced permissions management tools, such as mass operations and custom permissions templates, to simplify the process of setting up and managing workspace permissions. You can also use reporting and auditing tools to track user activity and guarantee compliance with your organization's data security policies.

36 Tabs

A workspace contains tabs that provide you with easy access to different Relativity features, including documents, search terms reports, views, and other default functionality. Relativity is a highly customizable platform. Commonly used tabs can be added to the Sidebar so that they can conveniently be accessed at any time.

Note: Relativity aiR includes a tool that allows you to choose a workspace to use as a source template for tab structure and then lets you apply that template across multiple workspaces in your instance.

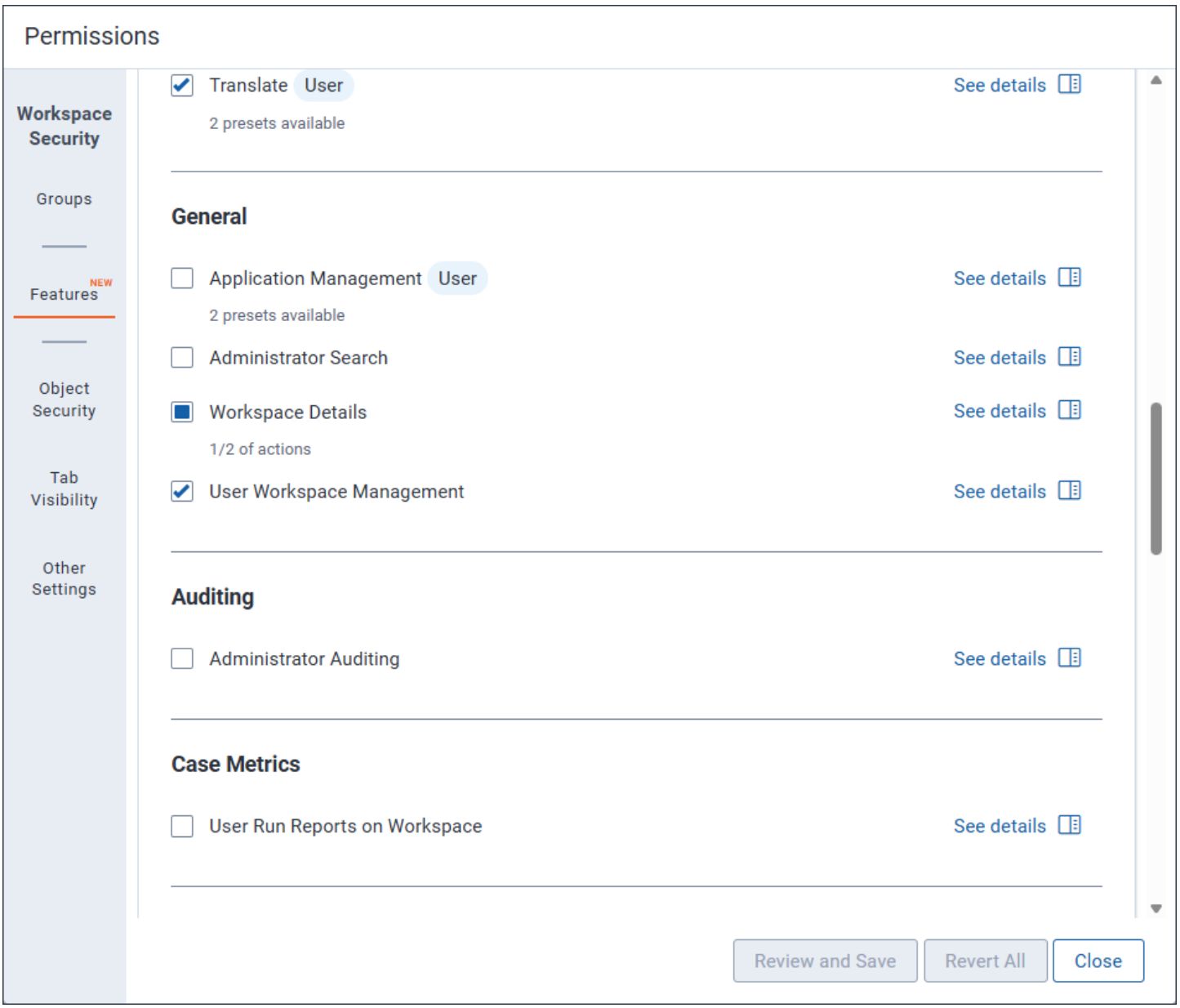
You can also apply any workspace template with a tabs arrangement that best serves your review needs. Some workspace templates also include custom tabs for specialized functionality.

You can add custom tabs in workspaces or at Home. Users with admin rights also have access to a Tabs tab from Home. The functionality of this Tabs tab is the same as the Tabs tab in a workspace.

In addition, Relativity automatically creates a tab when you add a new object type. For information about obtaining GUIDs, see Basic concepts for the application framework on the Relativity aiR Developers site. For information about obtaining GUIDs, see Basic concepts for the application framework on the Relativity RelativityaiR Developers site.

36.1 Permissions

Manage permissions for this feature on the Features tab. Grant the full feature for a group, or customize access with individual actions. For an overview of features and actions, see Feature permissions.



36.2 Creating and editing tabs

Note: We recommend avoiding sensitive data in tab names. You can secure new tabs by overriding inherited security settings and applying .item-level security.

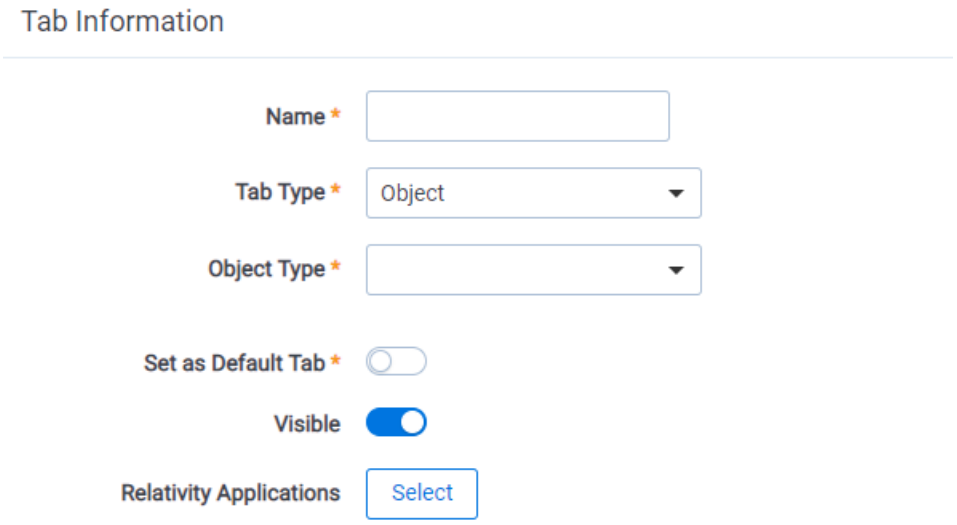
To create or edit a tab, follow these steps:

1. Click the **Tabs** tab.
2. Click **New Tab**. If you're editing an existing tab, click the **Edit** icon in the row of the tab you would like to edit.
3. Complete the fields on the form. See Fields on the next page.
4. Click **Save**.

36.3 Fields

Information on the fields in the Tab Information and Tab location are described below.

36.3.1 Tab Information



- **Name** - the tab's name. This field must be between 1 and 50 characters. Be as concise as possible when naming tabs.
- **Tab Type** - determines the type of tab you want to create:
  - **Object** - creates a tab for a non-document object in your workspace.
  - **Parent** - establishes the tab as a parent tab. Existing tabs can then be set as children of the parent tab, which causes them to display in the Sidebar's fly-out menu or in the Tab strip when the parent tab is currently selected. Selecting this option changes the layout by hiding the Object Type and Set as Default fields.
  - **External** - link to any URL or object type in Relativity.

    Note: Selecting **External** from the **Link Type** menu causes the **Link** field to appear below the **Parent** field. In the **Link** field, you can enter a web address to link to a URL. You can whitelist external domains using the **DomainNameWhiteListUrls** instance setting.

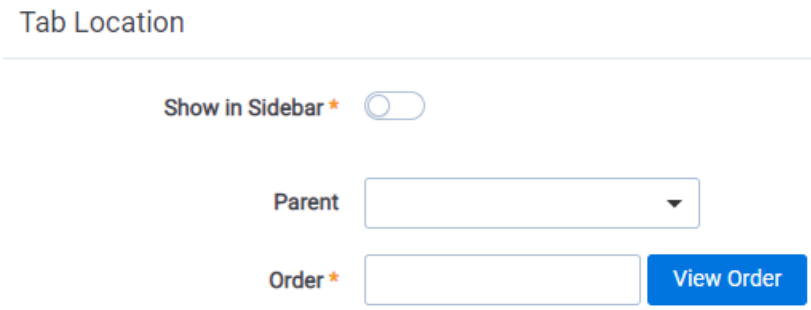
    You can create a link from a tab to an Relativity Dynamic Object (RDO) or a script, using either an Artifact ID or GUID. To create links to other objects, you must use their GUIDs. For information about working with objects that don't have GUIDs, see Tabs on page 688.
    Use the following token to link to an object: **ObjectArtifactIdentifier=[identifier]**, where [identifier] is the GUID of the object, or in the case of RDOs and scripts, the GUID or Artifact ID. For example, you would use the format **ObjectArtifactIdentifier=736b1c1f-d22f-43cf-9094-cc8acf94c60** to create a link from a tab to the object with this GUID.

Use the following case insensitive text replacement options to customize the URL, allowing you to display current details about your workspace:

Text Replacement Option	Replacement Text
%AppID%	AppID=<Current Workspace ID>
%ApplicationPath%	The actual application path
%ArtifactTypeID%	ArtifactTypeID=<Current ArtifactTypeID>
%AssociatedArtifactID%	AssociatedArtifactID=<Current Instance Artifact ID>
%AuthenticationToken%	AuthenticationToken=<New Authentication Token>
%ConnectorfieldArtifactID%	ConnectorFieldArtifactID=<Current Connector Field Artifact ID>
%ParentArtifactID%	ParentArtifactID=<Current Parent ArtifactID>
%SystemID%	SystemID=<Current System ID>
%SelectedSearchArtifactID%	SelectedSearchArtifactID =<Current Search Artifact ID>

- **Object Type** - determines which object's information is displayed in the tab for those specified as **Link Type = Object.**
- **Set as Default Tab** - toggle on to make this tab serve as the workspace's default tab. Reviewers logging in to the workspace are taken to the default tab. If a reviewer does not have access to the default tab, he or she is directed to the Documents tab instead.
- **Visible** - toggle on to display this tab from the Sidebar, Tab strip, and/or Quick nav.
- **Relativity Applications** - add this tab to a Relativity application. Clicking the **Select** button brings up a list of available applications.

36.3.2 Tab Location



- **Show in Sidebar** - select this option to add this tab to the Sidebar. Depending on the number of tabs that have already been added to the Sidebar, the Order value assigned to this tab, and your browser's resolution, the tab may be displayed in the More menu if it does not fit into the current Sidebar. Enabling this option causes the Icon option to display and also disables the Parent option described below.
- **Icon** - This option displays if Show in Sidebar is enabled. Select an icon from the drop-down menu to determine which icon is used for this tab in the Sidebar.
- **Parent** - select a parent tab to assign the current tab as a child tab. The current tab will display in the fly-out menu for the parent tab. This option is only available if Show in Sidebar is disabled.
- **Order** - represents the position of the tab by a numerical value. It can be any positive or negative integer. You cannot use decimals in this field. The lowest-numbered tab displays at the top of the Sidebar. The highest-numbered tab displays at the bottom of the Sidebar or in the More menu. Items that share the same value are

sorted in alphanumeric order.

Note: It's always a good idea to set tab order by 10's, starting with 10, then 20, then 30, etc. By numbering in groups of 10 you can insert an item into any position later in the workspace, without the need to reorder (for example, you can use 10, 20, 25, 30, 40 to insert a new tab between 20 and 30).

- **View Order** - displays a list of active tabs and their current order when you click the View Order button.

36.4 Nesting children tabs

You may prefer to nest several tabs within a parent to reduce clutter in your Relativity interface and make tabs easier to locate. You must first specify a tab as a parent (step 1) and then specify children tabs (steps 2-4).

1. Create a new tab with a **Tab Type** of **Parent** or edit an existing tab.
2. Click the **Edit** icon next to the tab you want to nest.
3. Choose the parent tab name under the **Parent** drop-down menu.
4. Click **Save**.

Repeat for each child tab you wish to nest. Hover your cursor over the parent tab to display the nested child tabs in a fly-out menu.

37 Users

Users are individuals who have access to the Relativity environment. You create users and add them to groups, which are then associated with workspaces. Users are also directly associated to clients. This diagram illustrates how clients, groups, and workspaces relate to users.

Visit Relativity Learning to explore additional learning opportunities for this topic.

37.1 User status

You can view information about users currently logged in to Relativity from the User Status tab, which is available from within any workspace or from Home. Whether or not you're in a workspace determines the functionality and information available on the User Status tab as follows:

- **Home** - the tab lists users currently logged in to Relativity. You can send web page messages and email messages to users listed on the tab. You can also force the log out of these users from the system.
- **Within a workspace** - the tab lists the subset of users accessing the current workspace. You can send web page messages and email messages to users listed on the tab.

37.2 Creating and editing a user

To create a new user, follow this procedure:

1. Navigate to the **Users** tab.
2. Click the **New User** button in the upper-left. To edit an existing user, click the  icon next to their name.
3. Complete the fields on the form. See Fields on the next page.
4. Click **Save**.

Note: Once you have created users, you can assign them to groups. When you add or remove users from a group, Relativity will execute a job and send you an email notification once it's completed. In case of an error, the email will contain a link that you can use to retry the job. Please note that to use the retry link, you need to be logged into Relativity. Additionally, you can find the retry link in the Errors tab.

Note: The (Admin) Errors tab has been permanently removed from Relativity aiR, and the ability to read errors through the API has been disabled. Job-specific errors are now addressable directly within your workspaces. For more information, see Errors tab deprecation.

Note: You can preview the security settings of any workspace available for a user by clicking Preview Security.

37.3 Adding a user log-in type

Relativity supports several authentication and log-in methods. You must assign the user at least one of these types in order for them to log-in.

See the following pages:

- **Managing users authentication methods** - for procedures to add individual authentication methods to a users.
- **Authentication** - for a general overview of the authentication system.

37.4 Fields

The User Information section fields are:

- **First Name** - the user's first name. This field must be between 1 and 50 characters.
- **Last Name** - the user's last name. This field must be between 1 and 50 characters. The system displays a user as <last name>, <first name>.
- **Email** - the user's email address. While the system won't validate this information, you must enter it in the following format: name@domain.extension.

  Note: Relativity users can have the same first and last name, but the email address must be unique.

- **Organization Type** - specifies the type of organization the user belongs to. Assign the organization type that best describes the user's organization, such as corporation, law firm, or government.
- **Title** - the user's title. You may assign a title that accurately reflects the user's role within their organization. Doing so provides clarity on the types of users engaged in your projects and supports the customization of educational materials and training programs. If Organization Type is selected, you must select a choice for Title.
  Pre-defined values for User Title:

  Note: Assigning a title is for informational purposes only. It **does not** affect user permissions, security settings, or any other authorization within Relativity.

  Organization Type - Corporate

Title
• Contract Lawyer • General Counsel • IT/Security • Legal Counsel/AGC/In-House Counsel (eDiscovery) • Legal Counsel/AGC/In-House Counsel (Employment) • Legal Counsel/AGC/In-House Counsel (Litigation) • Legal Counsel/AGC/In-House Counsel (Regulatory) • Legal Counsel/AGC/In-House Counsel (Trans-actional/Corporate/Commercial) • Legal Operations • Lit Support/eDiscovery Director • Paralegal/Legal Assistant

Organization Type - Law Firm

Title
• Barrister • eDiscovery Lawyer • IT/Security • Lit Support/eDiscovery Director • Litigator-Associate • Litigator-Counsel • Litigator-Partner/Practice Partner • Litigator-Solicitor • Paralegal/Legal Assistant • Project Manager • Reviewer/Contract Attorney/Contract Lawyer • Transactional/Corporate Lawyer

Organization Type - Other

Title
• Academic Pro-fessor • Consultant/Expert • Cyber secur-ity/Forensics

Title
• Other • Student

Organization Type - Public Sector

Title
• Attorney/Staff Attorney/Lawyer • Director • IT/Security • Lit Support/eDiscovery Director • Paralegal/Legal Assistant • Project Manager • Reviewer/Contract Lawyer/Contract Attorney • Special Litigation Counsel

Organization Type - Service Provider

Title
• Administrator • Cyber Security/Forensics • IT/Security • Project Manager • Reviewer/Contract Lawyer/Contract Attorney

- **Type** - the user type. The default values are internal or external, but you can add any type value. Type is for reference purposes only and has no impact on access or billing.
- **Client** - the client associated with the user. Click **Select** to choose from available clients.

Note: Items on the selected client list are set by a system view. It's possible you'll see only a sub-set of items.

The Other User Details section fields are:

- **Keywords** - an optional field where extra user information may be recorded.
- **Notes** - an optional field where extra user information may be recorded.

The Access section fields are:

- **Relativity aiR Access** - a toggle where you can control the user's access to Relativity.
  - **Enabled** - the default value. Enabled users can log in to Relativity aiR and, if applicable may be considered for billing under your Relativity license.
  - **Disabled** - users cannot access Relativity aiR and would not be counted or billed as named users on your Relativity license, if applicable.
  - When Relativity is first deployed, the system sets the Relativity Access field for existing users using the following criteria. A system admin can change a user's access at any time.
    - If a user is in a group with rights to a workspace, their Relativity Access is set to Enabled.
    - If a user is not in a group with rights to a workspace, their Relativity Access is set to Disabled.
- **Disable on Date (UTC)** - the date when the user's Relativity access is disabled. Use the field to auto-disable users on a specific date in the future, for example, when managing contact reviewers. When you specify the date, it can't be in the past. For more information, see Auto-disable users on page 701

  Note: The Disable on Date value is in UTC and does not represent local time.

- **Trusted IPs** - specifies a list of trusted IP addresses for a user. Authentication fails if a user attempts to log in to Relativity from an unauthorized IP address.

  Note: Relativity only supports the IPV4 format for Trusted IP addresses. It doesn't support the IPV6 format.

The Permissions sections fields are:

- **Change Settings** - users without admin rights can change their settings depending on whether the toggle is enabled or disabled.
  - First name
  - Last name
  - Email address
  - Item list page length
  - Default selected file type
  - Advanced search default
  - Enable or disable Native Viewer Cache Ahead

  Note: While "My Settings" appears grayed out in the user preview, users will still be able to access and change their own settings based on their assigned permissions.

  Feature Permissions provide an alternative to Relativity's security management by shifting the focus from Object Types and Tab Visibility to feature-based permissions. This method is an alternative option. Any feature-specific permissions information already in this and other topics is still applicable. The Feature Permissions interface enables administrators to manage permissions at the feature level, offering a more intuitive experience. By viewing granular permissions associated with each feature, administrators can ensure comprehensive control, ultimately reducing complexity and minimizing errors. For details see Instance-level permissions and Workspace-level permissions.
- **Change Document Viewer** - users can change document viewers depending on whether the toggle is enabled or disabled.
  - **Enabled** - users can select which viewer they want to use. You can still set a default viewer in the Document Viewer field, but users can switch between viewers.

    - **Disabled** - users can't select which viewer they want to use. Whatever viewer appears in the Document Viewer field in User Settings is the only viewer the user has access to.
- **Document Skip** - This feature is not currently compatible with Relativity aiR and as a result, this option does not impact a user's ability to access this feature.
- **Keyboard Shortcuts** - Choose a default setting for the keyboard shortcuts icon in the Review Interface. This property is set to Enabled by default.

The Defaults section fields are:

- **Item List Page Length** - a numeric field indicating the default list length for all views in Relativity except for views that are embedded into layouts as an Associative Object List. You can set it from 1 to 200.

  Note: Associative object lists in a layout do not inherit this value (the default number of items per page for these lists is 10 and cannot be customized).

- **Document Viewer** - Displays the Viewer used to review documents. This field is non-editable.
- **Document Viewer Preference** - determines the default viewer:
    - Viewer
    - Image
    - Long Text
    - Production
- **Show Filters** - determines whether or not filters on all columns are visible by default for that user. By default, this is set to Visible, but you can modify it as necessary. This version sets the Default Filter Visibility field to Visible for existing users whose filters are hidden.
    - **Enabled** - shows filters by default.
    - **Disabled** - hides filters by default.

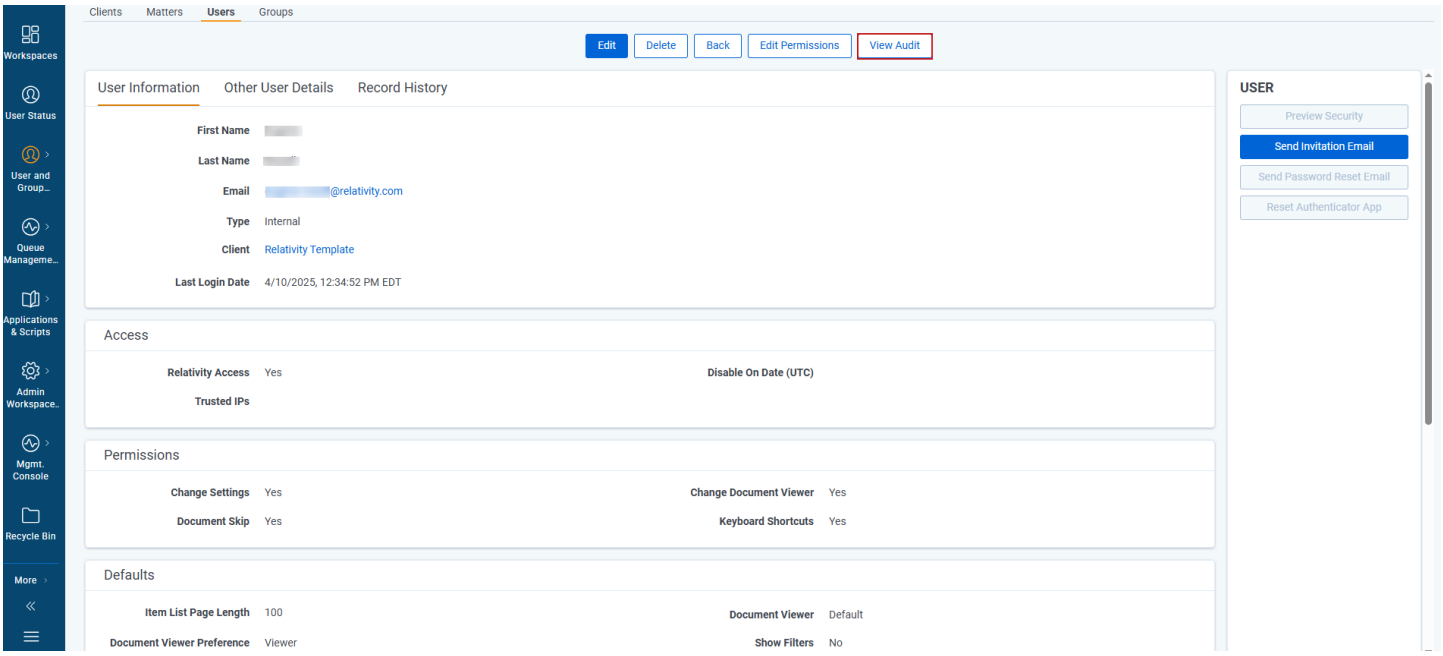
  Note: If a user is currently logged in to Relativity when a system admin modifies a setting, the user must log out and log back in for the changes to take effect. This also applies to the system admin if they are altering the setting on their own account.

- **Saved Search Owner** - determines whether saved searches are public or private by default. If Public is selected, the search is public and all users with rights to it can see it. If User is selected, the search is private and only the logged in user is able to see it. The property's default value is configurable on a system level.
- **Document Skip Preference** - controls whether or not the user has the ability to skip documents during review that no longer meet the original conditions of a view due to propagation. This field is non-editable and set by default to be disabled.
- **User-Group Email Notifications (if applicable)** - controls the type of email notifications Relativity will send to an admin that is adding or deleting users or groups. The available options are:
    - **Receive All**- receive all email notifications regarding the addition or removal of a user or group.
    - **Receive Errors Only** - receive email notifications on failed operations only regarding the addition or removal of a user or group.
    - **Do Not Receive** - receive no email notifications regarding the addition or removal of a user or group.

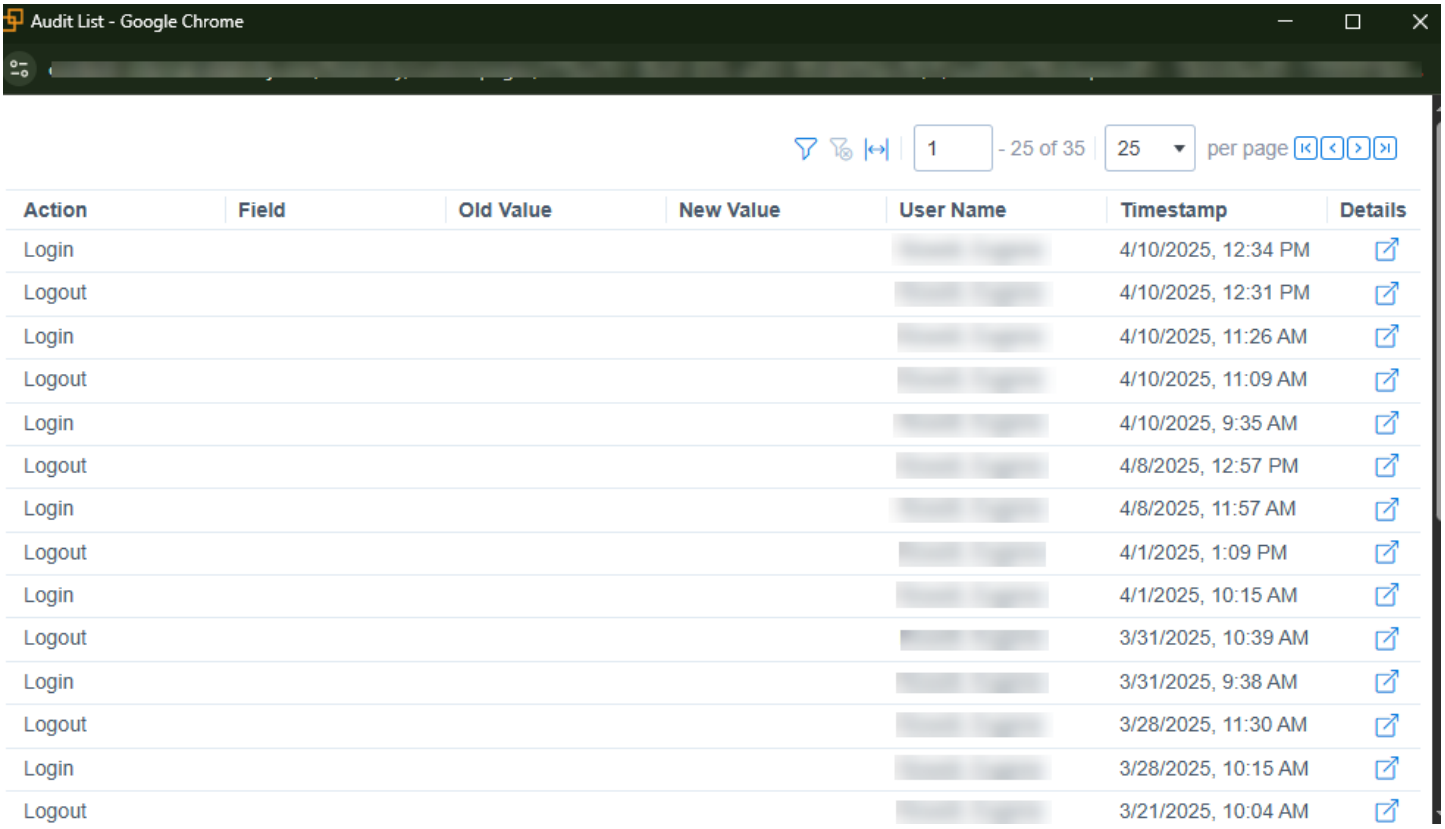
37.5 Viewing user audit records

Use the View Audit function to view a user's audited actions. To access the audit records, select the **Users** tab and click the name of a user. Then click **View Audit**.

Note: Audit records are not modified when a user is deleted or disabled. You will still be able to search for a user's audits based on their user name.



The user's history displays in a new window.



The following columns display:

- **User Name** - The name of the Relativity user who performed the action.
- **Action** - The action that was performed.
- **Timestamp** - The date and time that the action was performed.

37.6 Sending messages to users

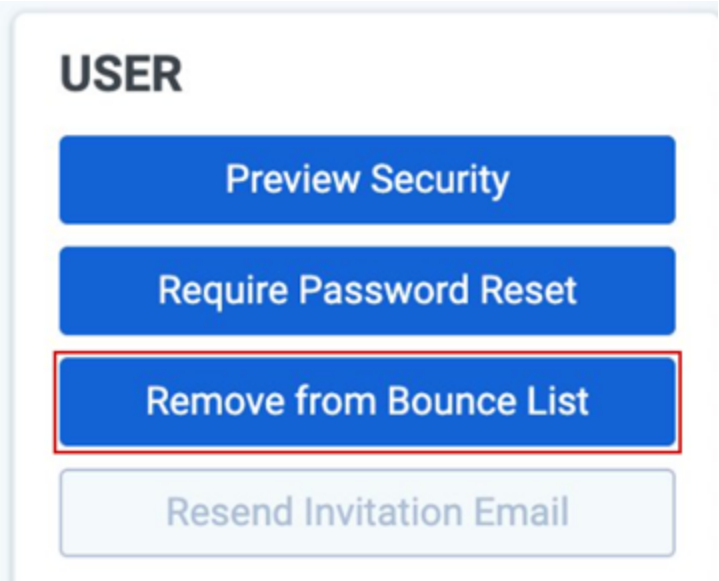
From Home or within a workspace, you can send web page messages to one or more users with the mass send message feature. Use the following steps to send a message:

1. Open the **User Status** tab in from within a workspace or from Home.
2. Select the checkbox next to the names of the users you want to send a message to.
3. Select **Send Message** from the drop-down menu at the bottom of the page.
4. Click **Go**. The Webpage Dialog appears.
5. Enter your message in the **Message** field, and then click **OK**. The selected users receive a web page message immediately.

To send an email message to an individual recipient, you can click on their email address link. This will launch your native email application, allowing you to compose the message. Your login information will identify you as the sender of the email message.

37.7 Bounce list removal

If a user reports not receiving their invitation or 2FA challenge email, the system administrator should check the User page to see if the **"Remove from Bounce List"** button is enabled.



If the button is enabled, click it to remove the user's email from the bounce list, then resend the invitation or ask the user to log in again to generate the 2FA challenge email. Follow this process to troubleshoot situations where users do not receive Relativity-sent emails. This applies to all workflows, not just user authentication.

Note: If the button is not enabled, the user is not on the bounce list, and there may be another issue with the user's email address or server. The user should check their junk email and spam folders, and may need to consult with internal IT. For more information on user invitations, see Centralized Authentication.

37.8 Forcing users to log out

From Home, you can force users to log out of Relativity from the User Status tab.

Note: When you use the Force Log Out option to terminate a user's session, any changes the user made and did not save will be lost.

Use the following steps to log users out:

1. Click your name in the upper right corner of Relativity, and click **Home**.
2. Open the **User Status** tab.
3. Select the checkbox next to the names of users you want to log out.
4. Select **Force Log Out** from the drop-down menu at the bottom of the page, and then click **Go**.
5. Click **OK** on the confirmation message. Relativity immediately logs out the users you selected.

37.9 Adding or removing users from a client domain

You can add or remove objects from client domains if you have the client domains feature activated.

Note: Client domain admins cannot add themselves to any group (even groups tied to their own client domain). Only a System Administrator can change a user's group memberships.

Use the following steps to add a user to a client domain:

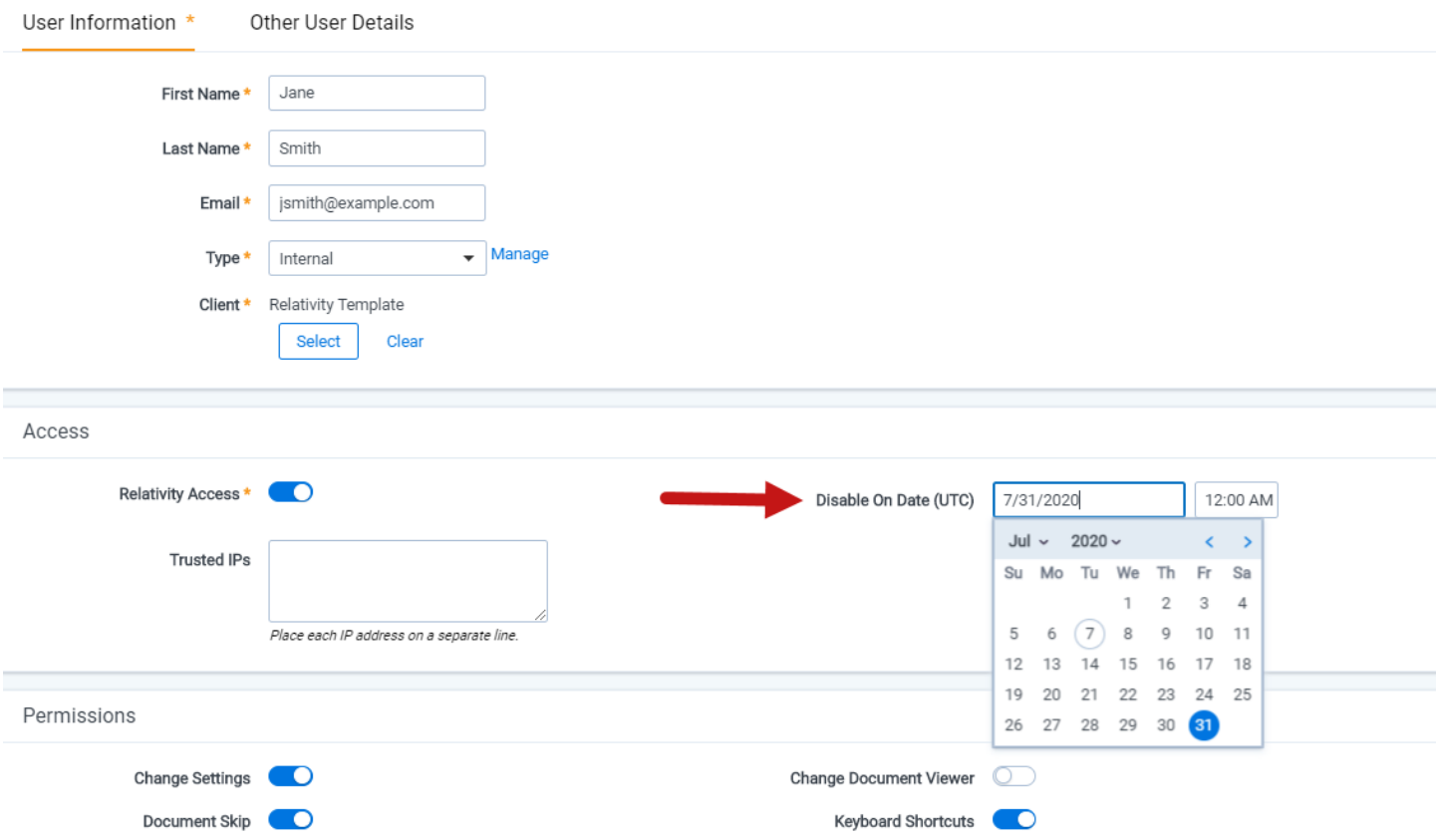
1. Navigate to the **Users** tab.
2. Click the icon to edit the user.
3. Click **Select** next to the **Client** field in **User Information** section of the **Users** tab.
4. Select the client with client domains enabled from the list.
5. Click **Save**.

Use the following steps to remove a user from a client domain:

1. Navigate to the **Users** tab.
2. Click the icon to edit the user.
3. Click **Select** next to the **Client** field in **User Information** section.
4. Select a client not associated with a client domain from the list.
5. Click **Save**.

37.10 Auto-disable users

You can auto-disable users on a specific date in the future. You can set the Disable On Date (UTC) field when creating or editing an individual user:



You can also use a mass-operation to set the Disable On Date (UTC) field for multiple users:

1. Navigate to the **Users** tab.
2. Select the checkbox next to the names of users.
3. Select **Enable** from the mass operations drop-down menu at the bottom of the page and the Enable Users dialog will open.
4. Select the checkbox next to the Disable On Date (UTC) field.
5. Enter or select the value for the Disable On Date (UTC) field. The date-time value must be in the future.

   Note: If you select the checkbox and leave the date value blank, will clear the Disable On Date (UTC) for the users.

6. Click **Ok**. The Disable On Date (UTC) field is set for the selected users, and they will be automatically logged out on the specified date and time.

38 Views

Views are customizable lists of items in Relativity. The diagram below illustrates the relationship between views and other Relativity objects.

Views are effectively special saved queries that control three things:

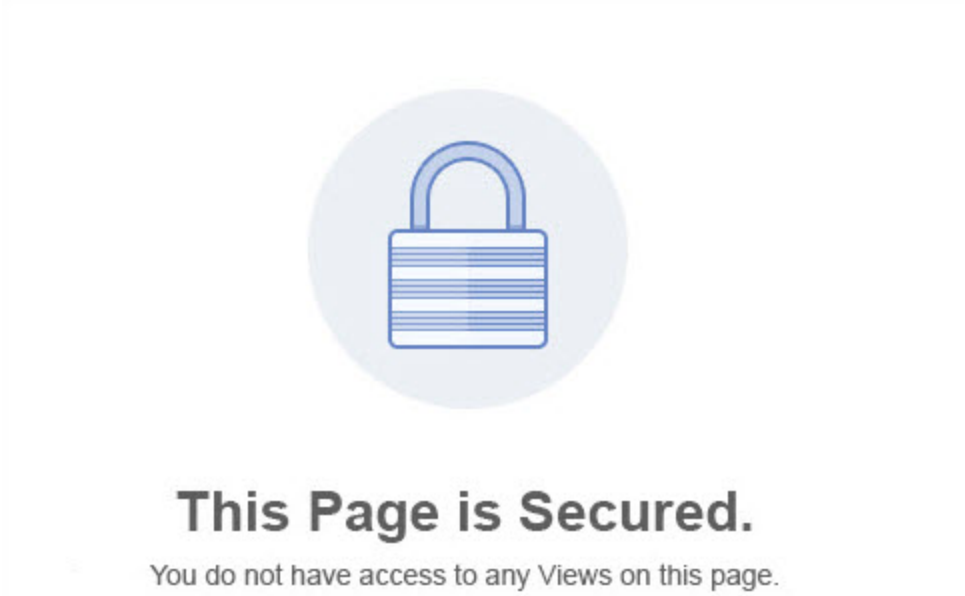
- The items displayed on the list, based on a set of criteria.
- The fields of information displayed for the returned items.
- The sort order of the returned items.

Each view corresponds to a Relativity object. For instance, to create a custom list of documents to display in the Documents tab, you must create a document view.

Note: If an Object Type List page does not have a view, it does not load and an error message appears that states no views have been created.

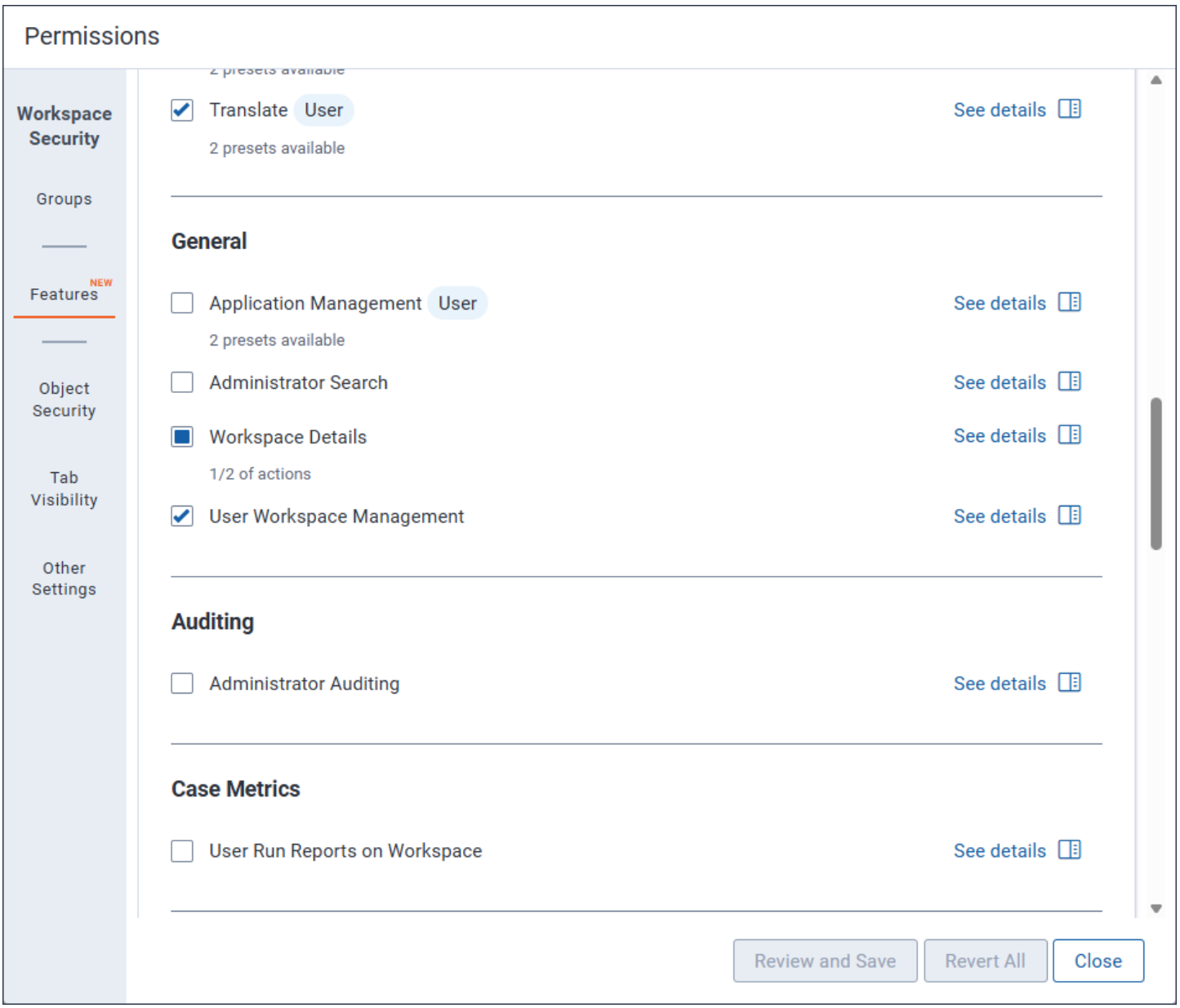
When you create a view, you can set conditions so that only objects that meet certain criteria appear in the view. However, you shouldn't rely on views to control security. If you need to prevent users from viewing an item, you must set the appropriate security permissions for that item.

If a user does not have access to any of the available views, an error message appears that states the page is secured.



38.1 Permissions

Manage permissions for this feature on the Features tab. Grant the full feature for a group, or customize access with individual actions. For an overview of features and actions, see Feature permissions.



38.2 Workspace system views

There are several workspace system views. These views display lists of items in special locations throughout the workspace. They include:

- **<Relational Field Friendly Name>** - controls which fields appear in the related items pane for relational field groups. Common examples include:
  - Family documents - controls which fields appear in the related items pane when viewing family groups.
  - Duplicate documents - controls which fields appear in the related items pane when viewing duplicate groups.

  Note: These relational views are automatically generated when you make a relational field. By default, they are not included on the Documents tab and are only used to determine the fields that appear in the related items pane for that relational group.

- **Search Results Pane view** - controls which fields are visible in the related items pane when you right-click in the viewer to run an Analytics search for similar documents.
- **History Pop up** - controls which fields appear when clicking details from the related items pane document history.
- **Production Documents** - controls which fields display for documents included on a production details page. Include the fields you use to qualify a document for production in the production documents view. You can then filter the list for disqualifying field values, providing a final QC step in the production process.
- **Markup History Details** - controls which fields appear when you launch a document's history details from the related items pane.
- **Default Search view** - controls which fields are returned, by default, on an advanced or saved search. You can always include additional fields from the advanced or saved search field selector. This view also controls the sort order of these fields as well. See Creating a saved search in the Searching guide.
- **Linked** - controls which fields are shown in the pop-up. You can then link to a document in the viewer.
- **Link Pane view** - controls which fields are shown in the related items pane showing the linked documents.
- **Batch Set Batches** - controls which fields are shown for the list of batches displayed at the bottom of the Batch Sets tab.
- **Document Batches (Default)** - controls the pop-up for searching batches on a view or an advanced or saved search.

  Note: For more information on searching with Batch fields as search conditions, see Batch field as search conditions in the Searching guide.

- **Advanced Search Browser view** - controls the fields displayed in the Advanced Search Browser.

  Note: This workspace system view is not editable in Relativity.

- **Event Handlers on Object Type** - controls the fields displayed in the pop-up for event handlers attached to an application.

  Note: This workspace system view is not editable in Relativity.

38.3 System views from Home

Any time you see a list of items in Relativity, it's a view. There are a number of system views available from Home, including page detail views and pickers.

- Page detail views:
  - **MattersOnClientPage** - controls which linked matters' fields appear on the client details page.
  - **UsersOnClientPage** - controls which linked users' fields appear on the client details page.
  - **UserViewRenderer** - controls which users fields appear on the group details page.
  - **GroupViewRenderer** - controls which group fields appear on the user details page.
- Pickers:
  - **ClientsOnPicker** - controls which client fields appear when selecting a client on the picker. The client picker is available from the new matter or new user form.

- **UsersOnPicker** - controls which user fields appear when adding a user to a group. The user picker is available from the group details page.
- **GroupsOnPicker** - controls which group fields appear when adding groups for a user. The group picker is available from the user details page.
- **WorkspacesOnPicker** - controls which workspace fields appear when selecting a template workspace on the new workspace form.
- **MattersOnPicker** - controls which matter fields appear when selecting a matter on the new workspace form.

Pickers have special restricting functionality within Relativity. You can use picker views criteria to control which items are available on the picker. For example, you can set up Relativity so that only clients with an active status are available for linking to users and matters. To accomplish this, edit the criteria for the "ClientsOnPicker" view to include status = active.

38.4 Creating a view

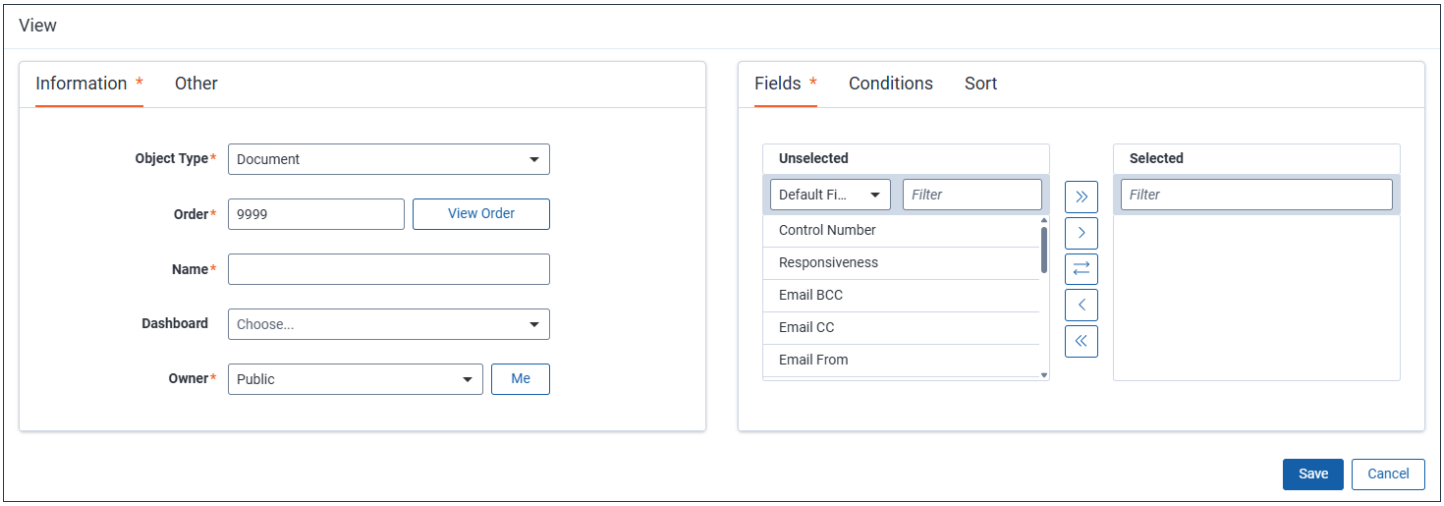
A view can be created utilizing field categories or without them depending on where you create the view. Field categories allow you to quickly and accurately apply field conditions to the document list.

Note: We recommend avoiding sensitive data in tab names. You can secure new tabs by overriding inherited security settings and applying .item-level security.

38.4.1 Creating a view with field categories

To create a view that can utilize field categories, do the following:

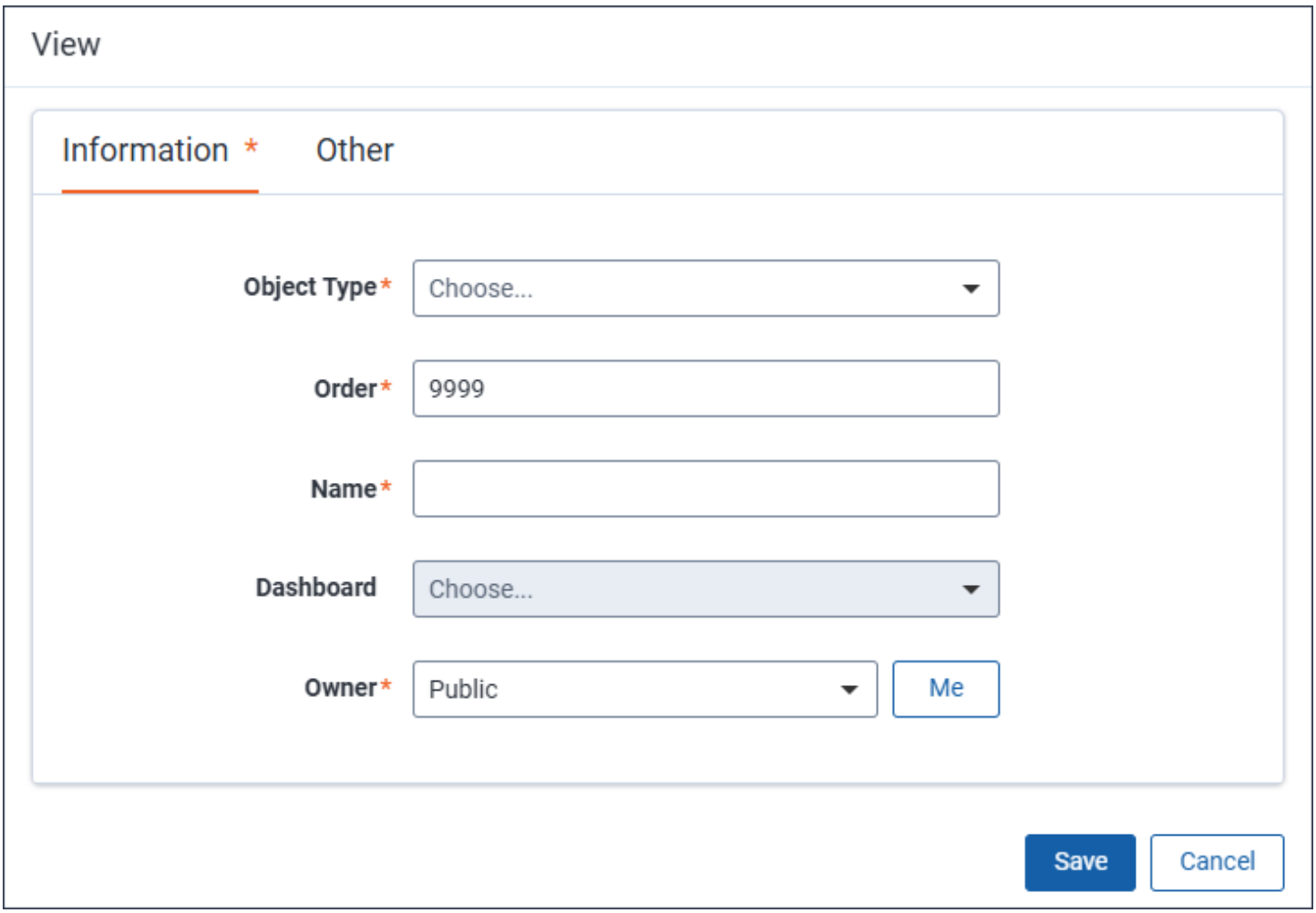
1. Navigate to the **Documents** tab.
2. Click on the View drop-down to expand the menu.
3. Click **New View**.
4. The View pop-up displays. Complete the fields on the pop-up. The fields for creating a new view are separated into five tabs.
    - Information tab on page 708
    - Other tab on page 709
    - Fields tab on page 709
    - Conditions tab on page 710
    - Sort tab on page 712



38.4.2 Creating a view without field categories

To create a view without utilizing field categories, do the following:

1. Navigate to the **Views** tab.
2. Click **New View**.
3. The View pop-up displays. Complete the fields on the pop-up. The fields for creating a new view are separated into five tabs. See the following sections to learn about each tab's fields.
    - Information tab on the next page
    - Other tab on page 709
    - Fields tab on page 709
    - Conditions tab on page 710
    - Sort tab on page 712



4. Click **Save**.

38.5 Information tab

The Information tab fields are:

- **Object Type** - is the type of view you're creating.
  When choosing an Object Type, ask yourself "What do I want to make a list of?" The answer is your object type. A common example of a type of view is the document view, which can be used when creating a view with a criterion that only shows documents that have not yet been coded. Another example is a batch view, which can be used to display only batches assigned to a specific user.
- **Order**- sets where the view appears within the view drop-down list. Items that share the same value are sorted in alphanumeric order.
  - Order can be any integer (positive or negative). No decimals are allowed.
  - The default order is 9999.

  Note: It's always a good idea to order by 10's, starting with 10, then 20, then 30, etc. By numbering in groups of 10 you can insert an item into any position later in the workspace, without the need to reorder all items.
- **Name** - the title of the view.

- **Owner**- sets the user(s) who can see the view. If the owner is set to Public, all users with rights to the view are able to see it. If the owner is set to a specific reviewer, the view is visible to only that reviewer. Clicking **Me** assigns the view to the logged in user.

38.6 Other tab

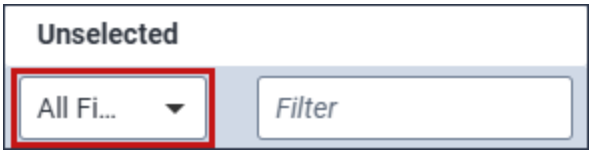
The Other tab fields are:

- **Group Definition** - includes propagated documents in the view and groups those documents together between blue lines within the document list.
- **Query Hint** - used to optimize views. Only use the query hint if instructed by the Relativity Customer Support team. Currently, you can use Hashjoin: (true/false) or Maxdop: (x) to populate the field.
- **Relativity Applications**- associate this view with an application created in the Applications tab. Click **Add** to select an existing application. This is only available for those who have the Manage Relativity Applications permission under Admin Operations.
- **Visible in Dropdown**- makes the view available in the selected object type's tab.
- **Inline Editing Enabled**- If enabled, this view allows users to edit fields using inline editing. If disabled, users cannot edit fields using inline editing while in this view.

38.7 Fields tab

In the Fields tab you select the fields that appear on your view.

All potentially available fields appear in the left box, Unselected items. If you created a view that utilizes field categories, you can select a field category from the drop-list above the Unselected items box to filter the list. This can make it easier to locate the desired fields.

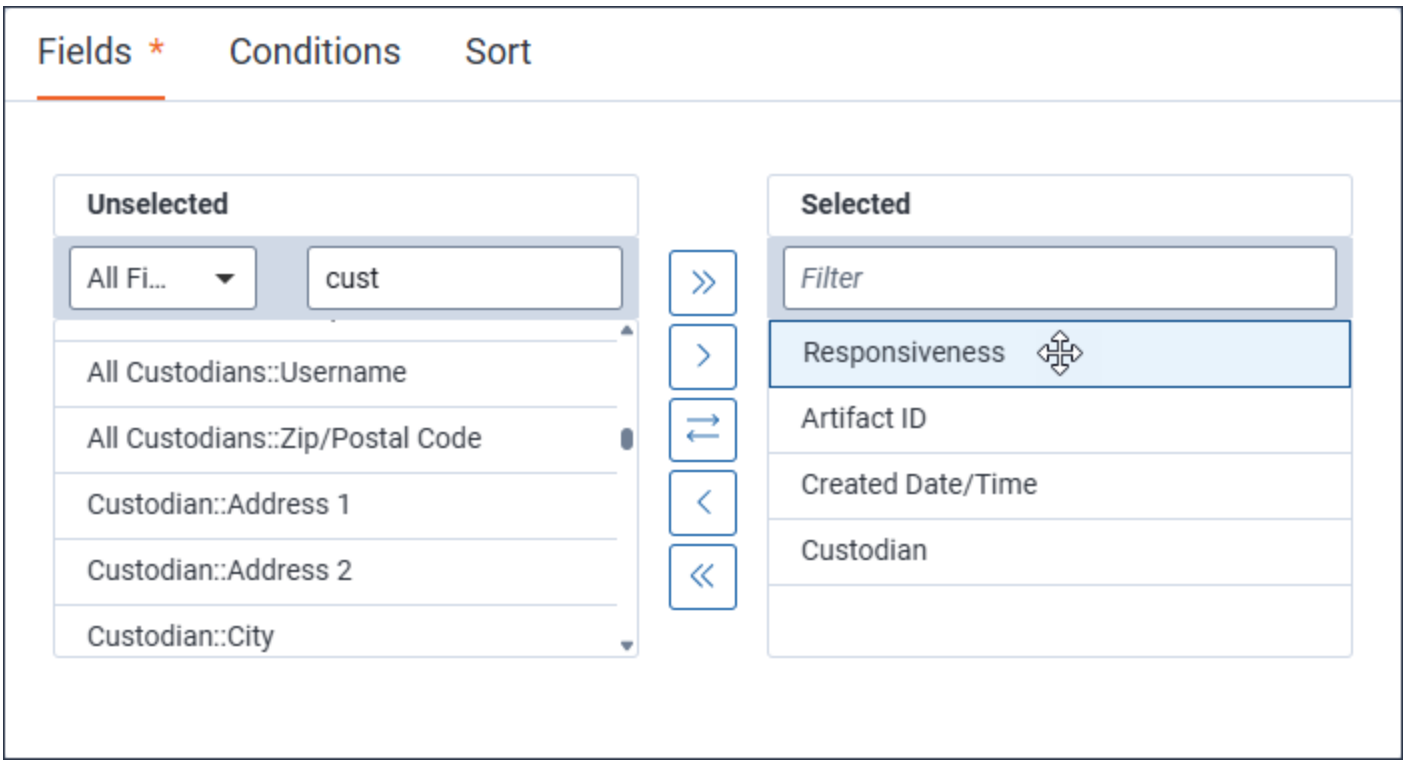


Move any fields you want in your view to the right box, Selected items. You can move fields between boxes by:

- Double-clicking the field name.
- Using the arrows between the boxes.
- Holding Shift and click or drag to select a range of items, which you can then move using the arrows.

In the Unselected items box, fields appear in alphanumeric order. Choose the fields for your view carefully, and avoid adding long text fields. Depending on the field type, you're able to get only a few fields visible on the screen. Select only those fields a user needs to see, filter on, or sort by.

In the Selected items box, fields are ordered according to their position. The topmost fields in the Selected items box are the leftmost fields on the view. The bottommost fields in the Selected items box are the rightmost fields on the view. Place your cursor in the Selected items box to order the fields using drag and drop.



There are several special system fields unique to views that you can add to a view:

- **Edit** - a hyperlinked field that opens the item in edit format.
- **Security** - a hyperlinked field that opens the item's security console.

There are filtering capabilities that you can use to help you locate fields. You can use the filter above each box to search for fields found in the corresponding box.

Note: The number of fields, or columns, you select can impact page load performance.

38.8 Conditions tab

In the Conditions tab you determine which items you want your view to return. A field condition can contain up to 4,000 characters.

When the item list for the view loads slowly due to a long running query, a message box displays with a **Cancel Request** link. This link is available when you perform other actions on item lists containing documents or Dynamic Objects that initiate a query in the background, as well as when you perform searches, filter, or sort on these objects.

Note: The Set Conditions section is similar to the Conditions section in saved searches. For more information on the available options, see Saved search in the Searching guide.



To define the criterion for your view, you can choose to add conditions, logic groups, or both.

To set a condition, complete the following steps:

1. Click the **+ Condition** button.
2. Select the field you want to apply a condition to by entering the name of the field or selecting the field from the drop-down list. The types of fields present differ based on the type of view you are creating.

   Note: If you are setting a condition on a view that can utilize field categories, you can conveniently filter the list of available fields by selecting a field category from the drop-down menu above the fields list.
3. A pop-up appears to select your search operator and enter the value to be searched. Available operators differ depending on the type of field being searched.
   With date-based fields, you can enter dates with the MM/DD/YYYY format or use the date range filter.
   Depending on the field type and operator, you can choose the value(s) from a popup picker. A popup picker is available for selecting choices and objects that provide the following operators:
   - **Any of these**
   - **None of these**
   - **All of these** (only for multi-object fields)
   - **Not all of these** (only for multi-object fields)
4. (Optional) Connect each criterion with an "AND" or "OR" operator.
5. (Optional) You can click **Clear All Conditions** to start over. Or, you can click the **Remove** icon to remove a single condition.
6. Click **Save**.

To set a Logic Group, complete the following steps:

1. Click the down arrow to the right of the **+ Condition** button and select **Logic Group**.
2. Select the conditions you would like to group together and drag and drop them into the logic group frames. Move your cursor to the left side of the condition to enable drag and drop.
3. Use the AND or OR operator to join logic groups.
4. Click **Save**.

38.9 Sort tab

In the Sort tab you define the default sort order of the view. If you don't select a sort criterion, the view sorts by artifact ID. Users are able to temporarily sort the view by any field that has Allow Sort/Tally enabled on the view.

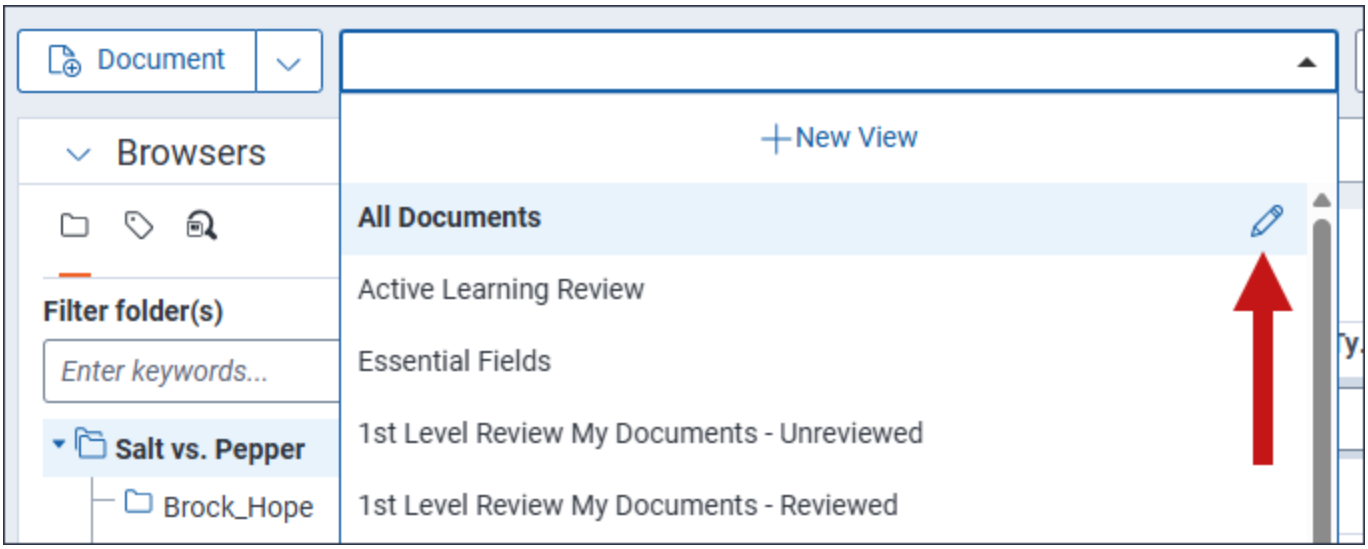


Each row represents a sort criterion. Select the desired sort field in the first column. The second column sets whether the sort should run ascending or descending. The sorts are applied in nested order.

38.10 Editing view information

You can edit views in three ways:

- In the Views tab in a workspace, click the **Edit** icon next to the desired view in the item list and move through the steps for creating a view.
- For all Relativity Dynamic Objects (RDO), and most system objects, you can click on the view drop-down to display the list of views. Next, click **Edit** icon next to the view you wish to edit, and then move through the steps for creating a view.

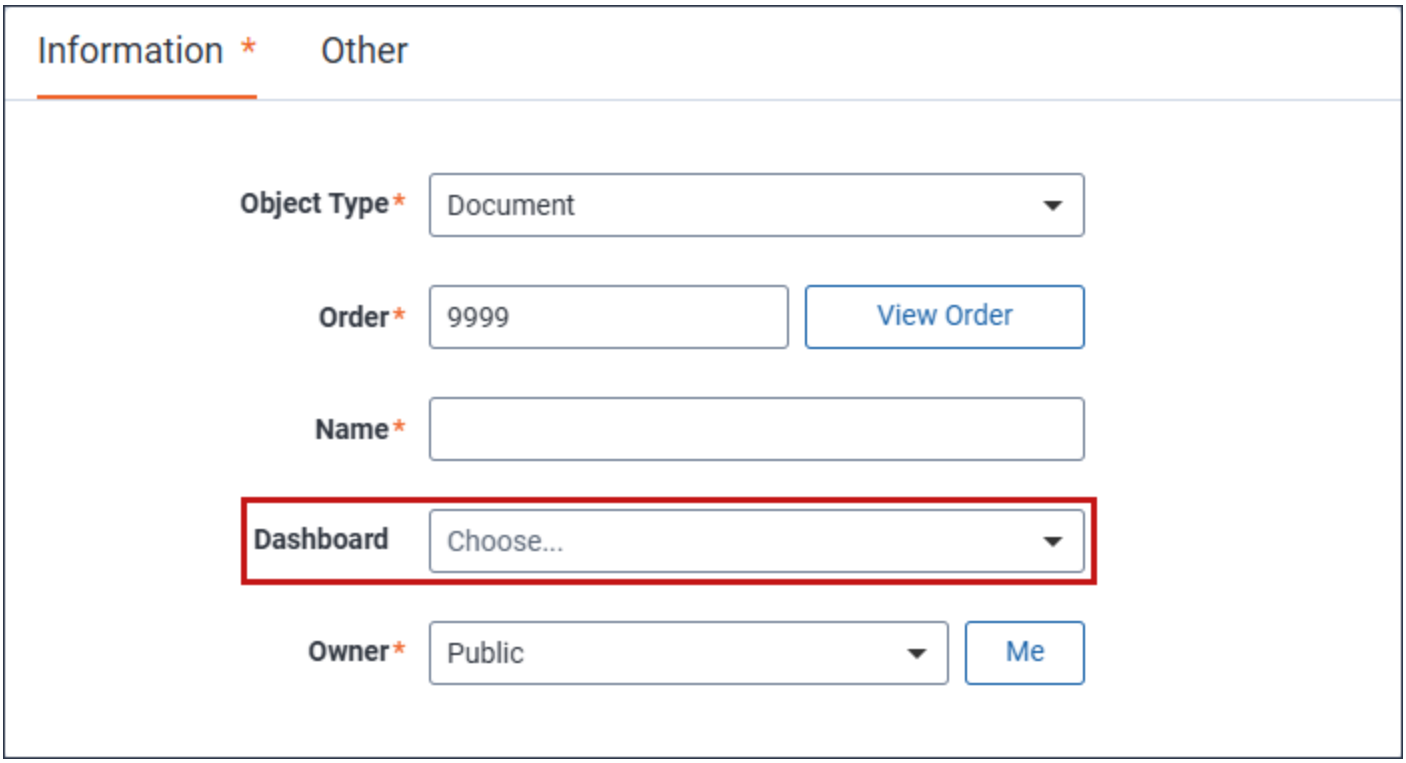


- Open the view that you want to change, click **Edit** in the view bar.

38.11 Linking a dashboard to a view

To link a dashboard to a view:

1. Create or edit a view.
2. Choose an **Object Type** from the drop-down menu that is compatible with dashboards.
3. Select the desired dashboard from the **Dashboard** drop-down menu.



4. Click **Save**.

If you switch to a different dashboard while in the view, the link breaks. There are two ways to restore this link:

- Log out of your environment, then log back in.
- Edit the view and hit **Save** again.

If you delete a dashboard, Relativity removes the link in the view.

If you delete a dashboard with dependencies, a pop-up appears with a list of dependencies.

Dashboards are available for dynamic object type views. They are also supported by the following static objects:

- Document
- Install Event Handler
- Mass Operation
- Markup Set
- Production

38.12 Displaying family groups in a view

During review, you can see how documents exist in family groups, also known as relational fields, by creating a view tailored to this goal. The family groups of documents are separated by bolded, blue lines in the documents list to help you visually identify them.

38.12.1 Creating the family group view

1. Navigate to the **Documents** tab.
2. Click on the View drop-down to expand the menu.
3. Click **New View**.
4. Enter the following in the Information section:
    - Object Type—**Document**
    - Order—**10**
    - Name—**Family Group**
    - Owner—**Public**
5. Enter the following in the Other section:
    - Group Definition—Choose a relational field from the list.
    - Visible in Dropdown—**Enabled**
6. In the Fields section, select each option below and click on the **Move selected** icon to move the field below to the Selected section:
    - Edit
    - File Icon
    - Control Number
    - Group Identifier
    - File Name, Name, or Unified Title
    - Record Type
    - Any additional fields you wish to see in the Family Group view.
7. Click on the **Sort** section and select the relational field you chose for the Group Definition field or another relational field.
8. Click **Save**.

104651	REL0000000010.0001_00018		Fam-1
104652	REL0000000010.0001_00019		Fam-1
104653	REL0000000010.0001_00020		Fam-1
104654	REL0000000010.0001_00021		Fam-1
104655	REL0000000010.0001_00022		Fam-1
104656	REL0000001728		Adams-1248
104657	REL0000001729		Adams-1248
104658	REL0000001730		Adams-1248
104659	REL0000001731		Adams-1248
104660	REL0000000001--7777		45
104661	REL0000000002.0001		45
104662	10-attachments_slice009	11/09/2018, 09:56	10-attachments_slice009
104663	10-attachments_slice009_001		10-attachments_slice009
104664	10-attachments_slice008	11/09/2018, 09:56	10-attachments_slice008
104665	10-attachments_slice008_001		10-attachments_slice008

39 Viewer

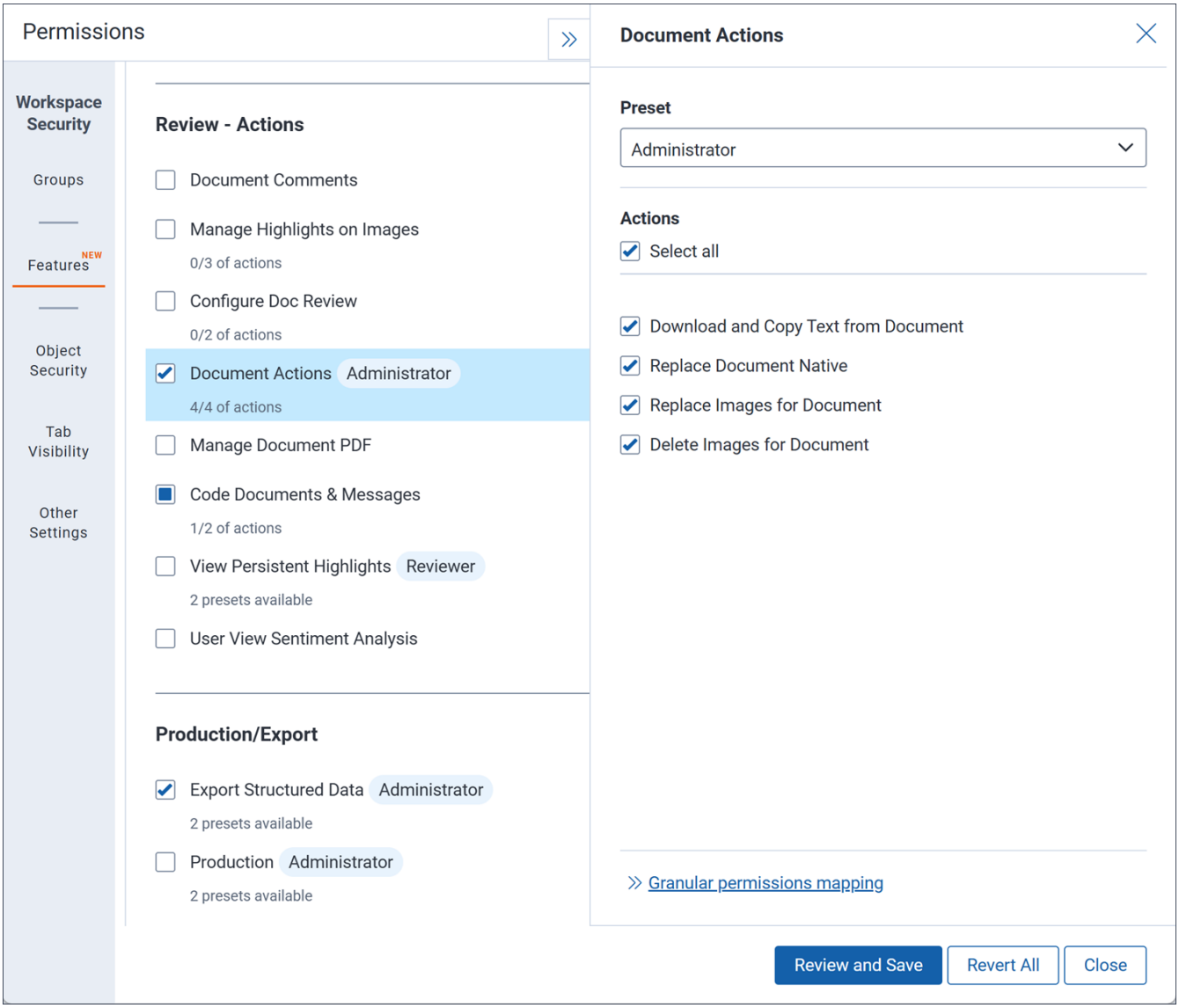
The Review Interface displays workspace documents. You can use the Viewer type tabs to toggle the loaded formats of documents, such as Native Viewer, Image Viewer, Extracted Text Viewer, or Productions Viewer. Using the Viewer, you can control the form of document that displays in the interface. If a document has not been imaged, you can image documents on-the-fly in the Viewer.

Note: Using your internet browser to zoom to any size other than 100% while using the Viewer is not supported and can cause unexpected behavior.

If you do not see the document in the Viewer, it either has not been loaded to the workspace, its conversion failed, or you do not have permission to see it.

39.1 Permissions

Note: This feature supports feature permission actions. Each action grants access to a specific task within the feature. You can grant groups access to individual actions, allowing them to perform only the tasks they need. To grant access to the entire feature, select all of its actions. Manage feature actions on the Features tab in a group's workspace permissions. For instructions, see Setting workspace permissions. For more information about feature permissions, see Feature permissions.

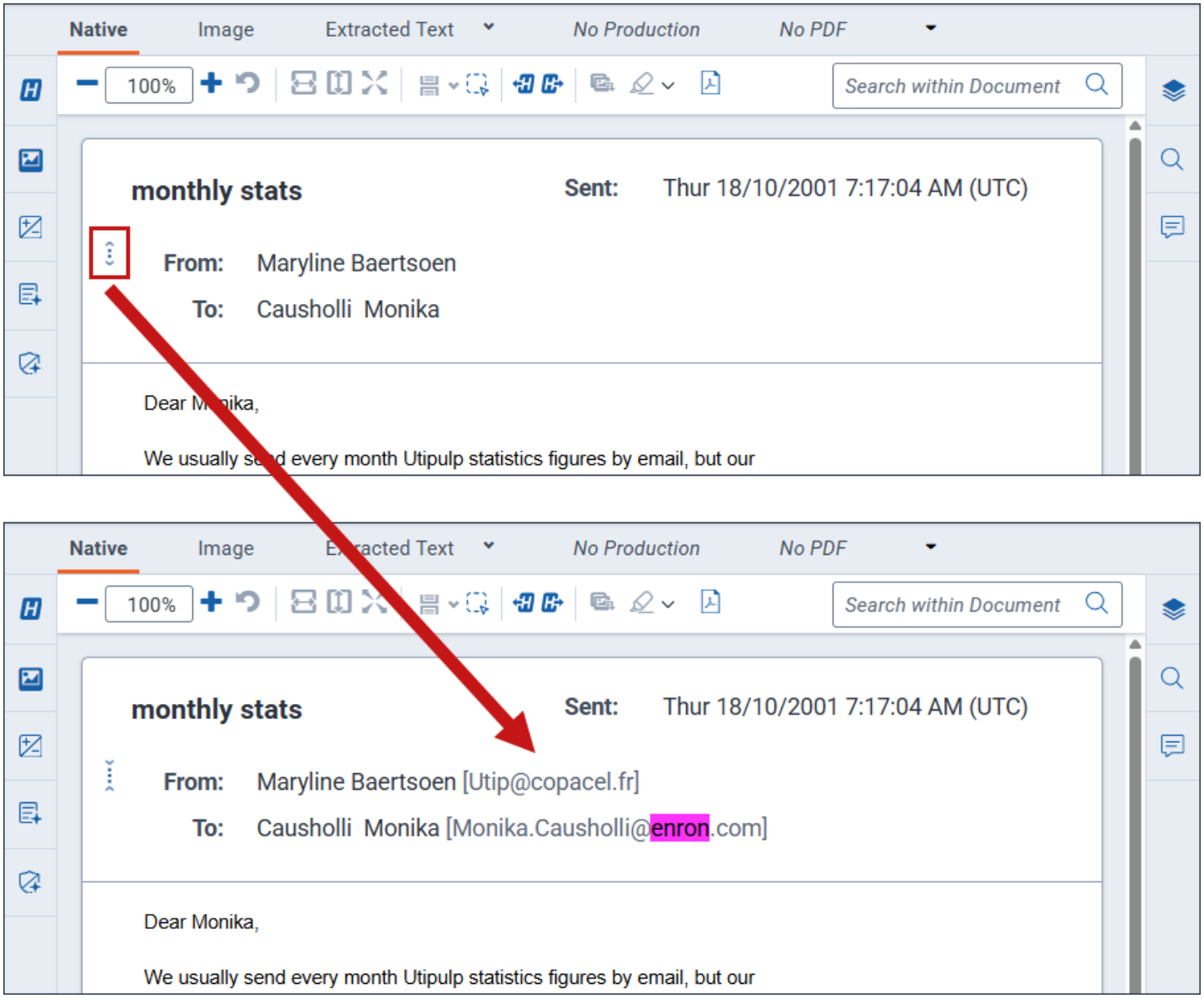


The following action must be granted to users to access all of the Viewer's features:

- **Document Actions**—Select to allow users in a group to select the options in the Document Actions menu.

39.2 Native Viewer

Note: In the Native Viewer, you can expand the email header to display full email addresses. If you collapse or expand an email header, the Viewer maintains the expanded or collapsed state as you navigate through documents in the set.



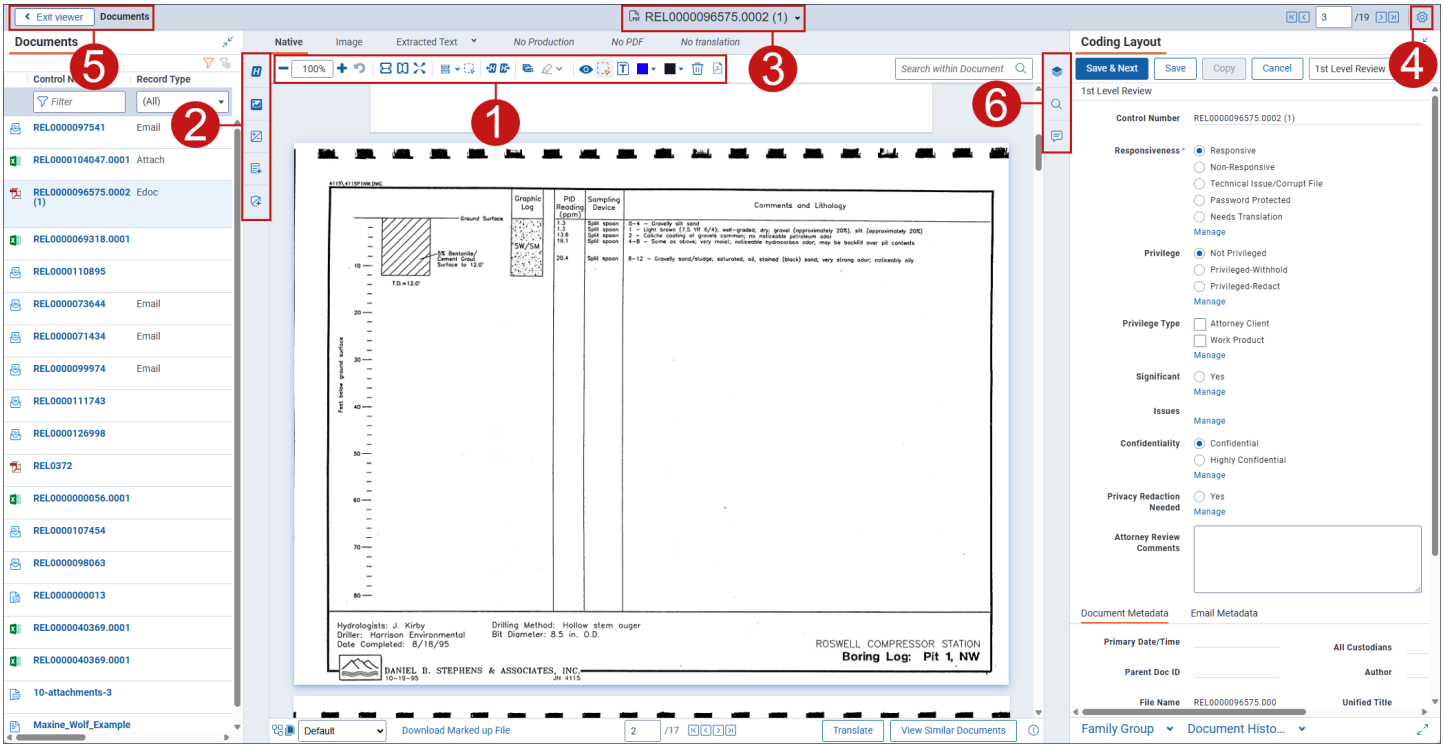
The Native Viewer displays an HTML rendering of the document that is as close to the original version of the document as possible. With the Native Viewer, you can:

- Navigate through a single document and between documents in a document set.
- Conduct text searching.
- Highlight text to copy and paste.
- Zoom, arrange, and save pages that you review in the Native Viewer.
- Print single documents by saving the document as a PDF. To learn more, see Create PDF.

Note: The Viewer displays PDF text by mapping the character codes to Unicode in most cases. To check whether PDF text has been properly encoded and will display correctly in the Viewer, copy the text in the original PDF file and paste it into another application like Microsoft Word or Notepad. If the pasted text does not display correctly, the PDF is not properly encoded. If the pasted text displays correctly in another application but not in the Viewer, contact Support for assistance.

39.2.1 Navigating the Native Viewer

The Native Viewer offers several ways of viewing and working with documents. There are options available in the following sections of the Viewer:



1. Native Viewer toolbar options
2. Left drawer Viewer options
3. Document actions menu
4. Viewer settings menu
5. Viewer breadcrumbs
6. Right drawer Viewer options

Each of these options and menus is described in more detail in the sections below.

39.2.1.1 Native Viewer toolbar options

The following toolbar options are available in the Native Viewer:



- **Zoom Out/In**—zooms out and in on the current document in increments of 10% within a range of 10% to 4,000%. If you attempt to zoom out to a percentage lower than 10%, the Viewer automatically sets the display to

10%. If you attempt to zoom in to a percentage higher than 4,000%, the Viewer automatically sets the display to 4,000%. Your zoom setting persists as you navigate through a document set. This means that if you have set one document to 150% and you go to the next document, the next document defaults to 150% zoom.
To specify a zoom percentage without using the zoom out/in toolbar buttons, type the number in the percentage field and press the **Enter** key.

- **Reset Zoom**—resets the zoom to 100%.
- **Fit Width**—increases the size of the document to fit the maximum width of the Viewer. This setting persists when you re-size the window.
- **Fit Page**—fits the entire document into the total size of the page. Clicking this zooms out the document and reduces the font size.
- **Fit Actual**—fits the document display to the actual size it was in its native application. By default, this resets the zoom percentage to 100%.
- **Layout Mode**—select one of the following options to determine how documents that are more than one page long display in the Viewer.
    - **Single**—one page of a document will display at a time. Use the page navigation options at the bottom of the Viewer to adjust which page you view.
    - **Single Continuous**—displays the pages in the document stacked vertically so you can scroll up and down to view them.
    - **Facing Continuous**—displays the pages in the document in a row horizontally so you can scroll left and right to view them.
- **Draft Mode**—click to begin Draft Mode which automatically contrasts text from the background, help you identify poorly drawn redactions, and identify corrupt OCR text. This option is only available on the Native Viewer and PDF Viewer with rendered documents.
- **Go To Next/Previous Highlight**—moves through previous and next highlighted terms in the document.
- **Rotate All Pages**—rotates all pages in a document clockwise 90 degrees. This option is only available for documents that have been paginated.
- **Designation Display**—this option determines how designations are displayed in the Viewer. This option is only available if you have the Relativity.Transcripts application installed and you are viewing an MDB file in the Native Viewer. Click on this icon and select one of the following options from the drop-down menu:
    - **Color Bars**—each designation displays as colored bars to the left of the text in the Transcribed Text panel.
    - **Highlights**—each designation displays as highlights over the text in the Transcribed Text panel.
- **Redact Markup Visibility**—this option determines how markups display in the Viewer.
It only displays if you have the Redact application installed and open a PDF or spreadsheet document in the Native Viewer.
Click the Redact Markup Visibility icon to toggle between the following modes:
    - **Solid**—Markups in the document are fully visible and cover text underneath.
    - **Transparent**—Markups in the document are partially visible so that you can still see the text underneath.
    - **Hidden**—Markups in the document are not visible.
- **Selector**—this option only displays if you open a PDF document in the Native Viewer. Click to enable the selection of markups in the Viewer using left or right click on your mouse.

- **Text Selection Mode**—this option only displays if you open a PDF document in the Native Viewer. Click to enable text highlight by clicking and dragging your cursor across it. You can then right-click on the highlighted text and copy it.
- **Clear Markups**—click to remove all markups from the currently selected markup set for this document. This icon only displays in PDF and Excel documents that have been prepared for Redact.
- **Create PDF**—click to save the current native document as a PDF file. When you click this option, the Create PDF pop-up displays. The document then opens in a new window in your browser as a PDF where you can then choose to save or print the document image.
- **Transcript Text**—This option only displays if you have an AV document open in the Native Viewer. Click to expand the card and view the transcribed text for an AV document.

39.2.1.2 Searchable PDF Improvements per Configuration

When you Create PDF from the Native Viewer or using the Mass PDF Operations bar, most types of searchable PDFs will now have significantly smaller file sizes. More specifically, images without highlights, but configured to be searchable and stamped, will benefit from the most dramatic decrease in file size. But overall, the Create PDF feature now generates reduced file saves for a wide range of configurations when creating searchable PDFs. In order to accomplish this for previously unknown file-types and mixed TIFF and JPEG Create PDF jobs, Relativity now treats each page individually, instead of treating the entire document as a whole, allowing for the best file-size-reduction technique possible for each page.

Image Format	Redactions	Highlights	File Size Reduction
TIFF	Yes	No	Up to 76%
TIFF	Yes	Yes	Up to 43%
JPEG	Yes	No	Up to 43%
JPEG	Yes	Yes	Up to 43%

After you click **Create PDF**, a copy of the document converts to a PDF file you can save from your web browser downloads. Relativity assigns a GUID for Create PDF file names.

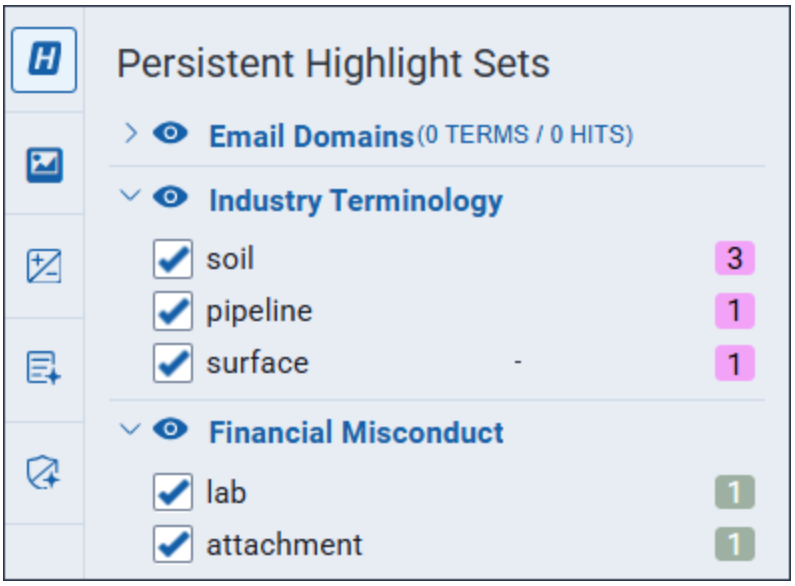
- **Search Bar** —searches for terms in the current document and navigates through the hits.
  - Entering a term and either clicking the left or right arrow button or pressing **Enter** in this text box scrolls to and highlights the text of the next instance of the term, from the placement of the cursor.
  - Searching in this text box is not case sensitive.
  - Searching supports dtSearch and so proximity, fuzziness, and stemming can be used. Unlike dtSearch, the Viewer doesn't have an alphabet file or run on an index. So, while characters like - act as word breaks for searching, they do not for proximity.
  - You can remove a term you previously searched for or all of the terms you have recently searched for from the Persistent Highlight Pane. Removing a term or terms will also remove any highlights they generated in the document. To remove a term or terms, hover your cursor over the row of the term or recent searches you wish to remove and then click on the **clear term 'x'** icon in the right side of the row.
- **Show/Hide Hidden Cells**—displays or hides all hidden cells in a Microsoft Excel spreadsheet. This functionality is only available for Excel files and does not work on imaged documents because Relativity only images unhidden cells.

39.2.1.3 Left drawer Viewer options

The following options are available in the left drawer of the review interface:



- **Persistent Highlighting**—displays or hides a card containing all recent searches from the criteria entered in the search bar and any persistent highlight sets in the workspace. You can also create a dtSearch or keyword search in the Your recent searches section. Only terms in the sets and recent searches that are in the current document will display in the pane.
  Additionally, you can control which highlights display in the current document by clicking on either the persistent set to only display highlights from that set or you can click on a specific term to only see that term highlighted in the document. You can also navigate to and from highlights using this pane.



- **Thumbnail**—click to expand the left drawer and display the Thumbnail Viewer. Each page of the document you are reviewing has its own numbered thumbnail in the Thumbnail Viewer.
- **Sentiment**—click to expand or collapse the left drawer and display sentiment analysis highlights in the Viewer.
- **aiR Review Analysis**—click to expand or collapse the left drawer and display aiR Review results. You can also enable or disable aiR Review highlights.
- **Privilege Analysis**—click to expand or collapse the left drawer and display Privilege results.

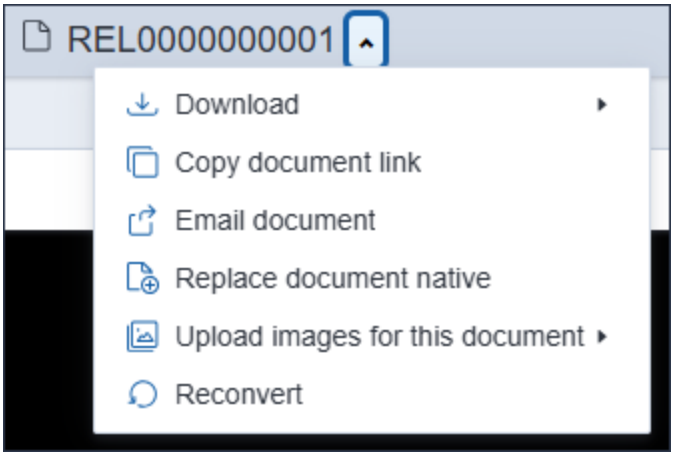
39.2.1.4 Right drawer Viewer options

The following options are available in the right drawer:



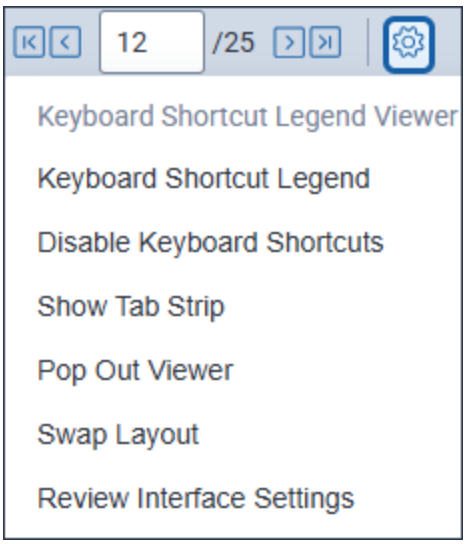
- **Hidden Content**—displays or hides information about hidden content. Hidden content can appear in Excel, Word, PDF, or Powerpoint documents. This functionality does not work on imaged documents because Relativity only images unhidden cells.
- **Contextual Search**—click to expand the right drawer and display the Contextual Search card. This feature allows you to quickly navigate to matching search terms in a document which is useful in longer documents or ones that have many matching search terms. The Contextual Search card has the same functionality as the Search Bar. To learn more about the Search Bar's functionality, see Search Bar. Additionally, each search term match is displayed in a box that includes both words before and after the search term match to make it easy for you to view the context of each one.
  Enter a term or terms in the search box and press **Enter** on your keyboard to highlight in yellow any matches in the current document. You can click on a desired search term box in the pane to jump to that place in the document. The active search term box will display with a blue border and the matching search term in the document will be highlighted in blue to make it easy to find.
- **Comments**—click to expand the right drawer and display the Comments card. From this card, reviewers can add, edit, or delete comments on any text-based or AV documents in the Native Viewer.

39.2.1.5 Document actions menu



To learn more about these options, see Document actions menu.

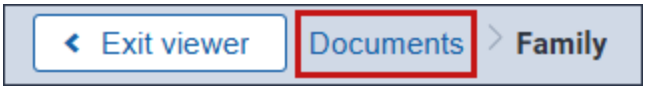
39.2.1.6 Viewer settings menu



To learn more about these options, see Viewer settings menu.

39.2.1.7 Viewer breadcrumbs

The Viewer breadcrumbs help you track your current location while browsing documents in the Related items card. The information on your current location updates as you navigate. If Documents is an active link, you can click it to return to the document you were viewing before browsing documents in the Related items card.



Additionally, to exit the Viewer and return to the page you were previously on, you can click the **Exit viewer** button at any time.

39.2.2 Copying text in the Viewer

While viewing a document in the Native Viewer, you have several right-click options, including the **Copy** option. Use this option to copy text from the document you are currently viewing and then paste it into another application.

To do this:

1. Highlight the text you want copied.
2. Right-click, and then select **Copy** from the menu.

You cannot copy text if you:

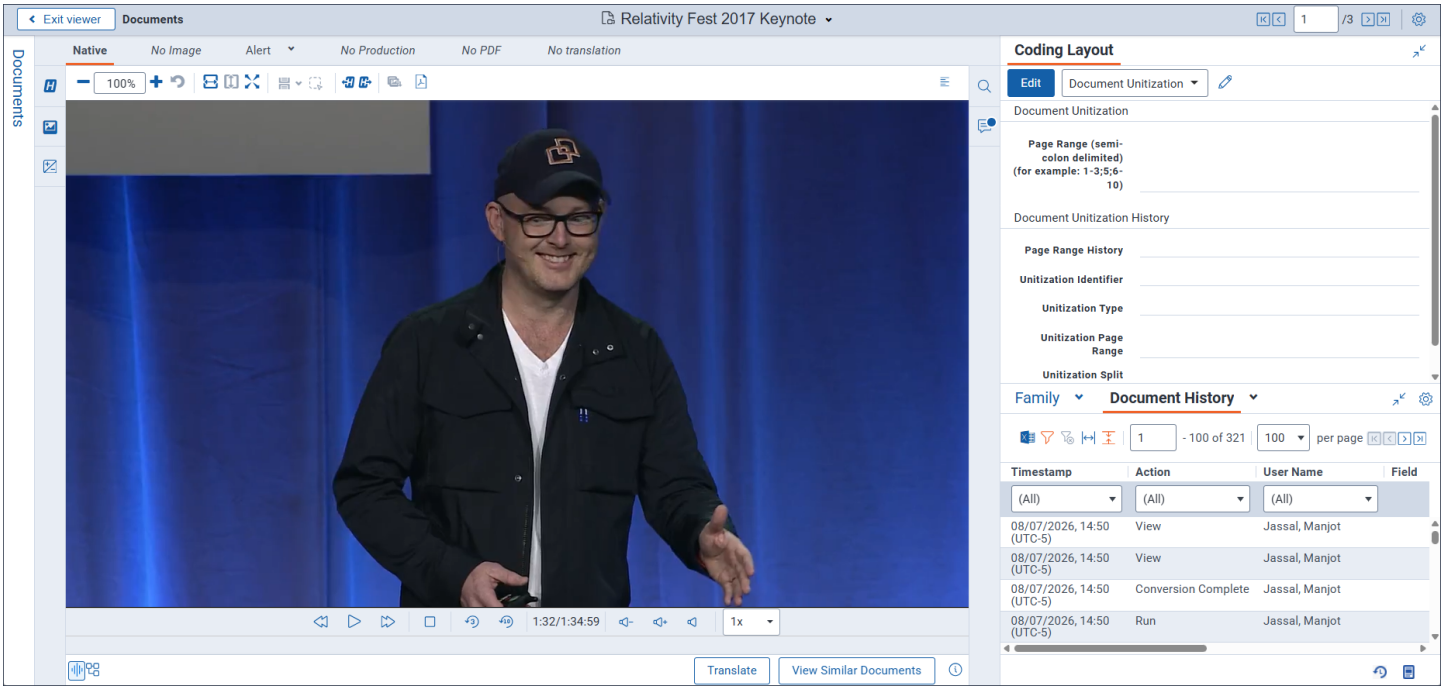
- Have not highlighted any text.
- Do not have permission to the Local Access option on the Document object. This is the same permission that permits you to open the file in its native application. For more information, see Object list in Relativity Admin guide.

Note: If you don't have permission to the Local Access option on the Document object, you can't use the Ctrl+C or Ctrl+Ins options in either the Native Viewer or the Extracted Text Viewer.

39.2.3 Streaming audio and video files

Audio and video files can be streamed in the Native Viewer. Audio and video file type compatibility varies depending on your internet browser.

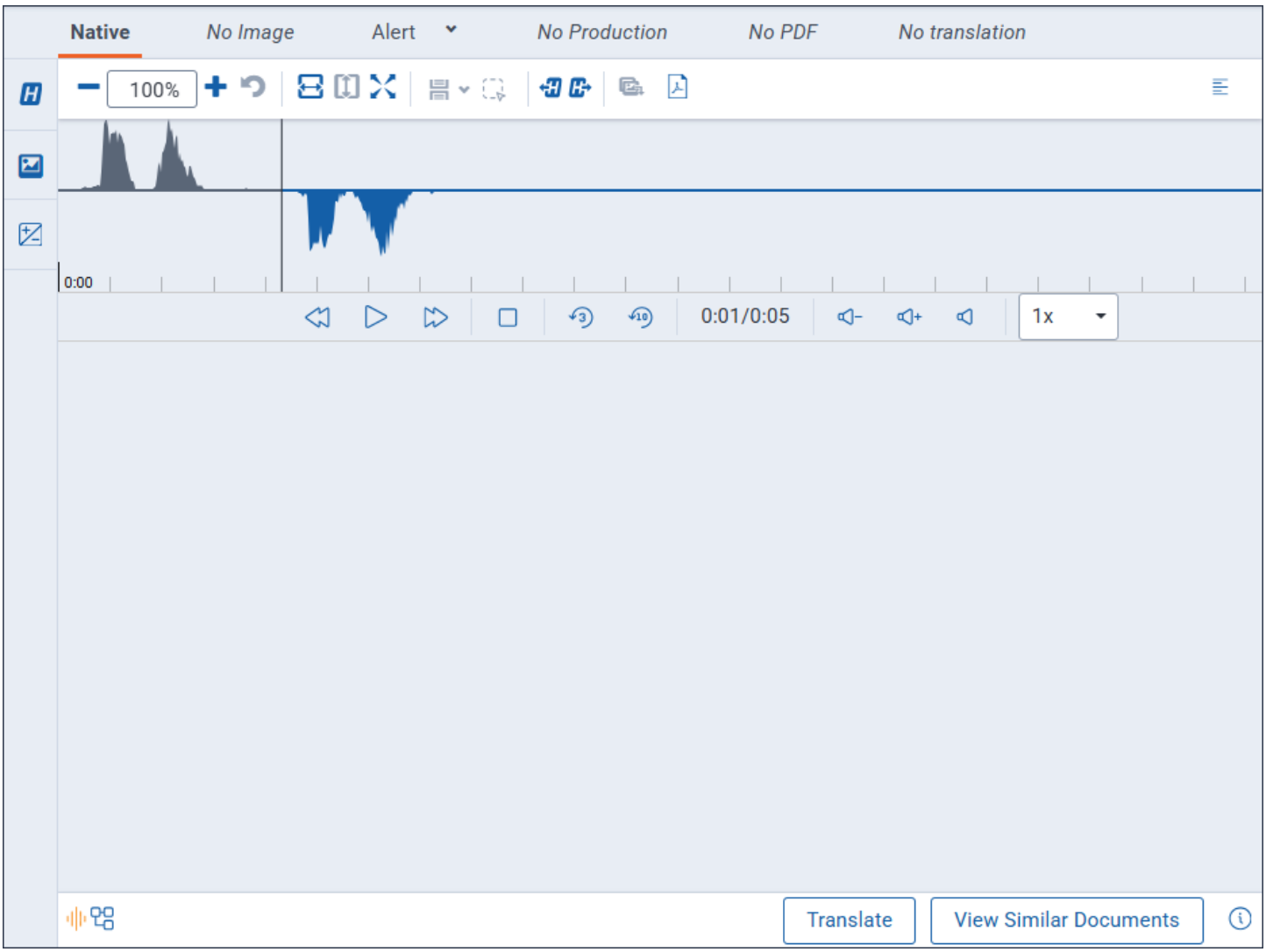
Note: If an audio or video file has not been opened in the Native Viewer, it may display with a value of **No** for the Supported by Viewer field. Once a file has been successfully opened by the Viewer, the Supported By Viewer field displays **Yes**.



39.2.3.1 Waveform audio

Note: Media files that are longer than 30 minutes do not display Waveform but can still be played in the Native Viewer. Transcribed text, which is part of AV transcription, is also not affected by this limitation.

Waveform is a visualization of sound that you can view while listening to an audio file in the Native Viewer. Click the **Show/Hide Waveform** icon to display the Waveform visualization. The visualization tracks the volume and intensity of sound to help you avoid audio inactivity. You can use the audio controls to skip these sections. The visualization also scrolls with a time scale along the bottom to help you identify when a particular audio event occurs.



39.2.4 Document Intelligence

Document Intelligence notifies you that there is hidden or annotated content, including a pivot table or a filtered pivot table, present in the current document in the Native Viewer. This hidden content are the annotations and modifications tracked in certain document formats. For more information on the file types, see Tracking annotations. When hidden content is found in a document, a pop-up modal appears in the lower-right corner. Highlighting and bordering is also visible in the Viewer where the changes were made and a annotation bar is available to sort and view each annotation. Once the notifications appear, you can then choose whether or not to view tracked changes, hidden text and comments in the Viewer.

To view highlights associated with hidden content, such as comments or annotations listed below, the corresponding content must be visible in the Viewer. This is because hidden content is embedded directly within the document and is not stored as metadata or extracted text.

39.2.4.1 Tracking annotations

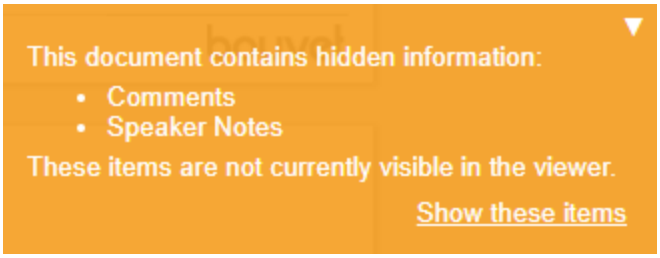
The various file types each have distinct annotations that are tracked. Below is each file type that is supported and the related tracked changes:

File type	File extensions	Annotation type	Tracked changes
Excel	.xls, .xlsx,	Tracked Changes, formulas, hidden pages/-	Inserted cell, moved cell, modified cell, cleared cell

File type	File extensions	Annotation type	Tracked changes
	.xlsb	columns/rows, Comments, concealed cell contents	Inserted column, deleted column Inserted row, deleted row Inserted sheet, renamed sheet
Word	.doc, .docx	Tracked Changes, comments, hidden text **Note:** Text within Tracked Changes cannot be searched or highlighted in the Viewer.	Insertions, deletions, moves
PowerPoint	.ppt, .pptx	Speaker notes, comments, hidden slides	
PDF	.pdf	Comments, text content outside the printable page	

39.2.4.2 Using notifications and the annotation bar

When using Document Intelligence, an orange pop-up modal appears in the bottom right corner of the Viewer when hidden content exists. Click on the pop-up modal to see the hidden content on that document. If there is no hidden content found, the modal will say so. If there is hidden content found, it lists each piece of content. Click **Show these items** to open the annotation bar.



A hidden content icon is available when a supported file type is in the Native Viewer. Click the **Hidden Content** icon to open or close the annotations bar. If you are viewing an unsupported file type, the icon is not available. For supported file types, see the Tracking annotations.

Annotation bar

The annotation bar is for sorting and viewing the hidden content found with Document Intelligence. Each annotation has a card that lists the tracked change, a description of the change, time and date, and author of the change.

If there are multiple annotation cards in the annotation bar, then you can sort them in multiple ways. Click the **Sort By** drop down menu for these options:

- Location
- Author A-Z
- Author Z-A
- Oldest first
- Newest first
- Annotation type

Annotation types and highlights

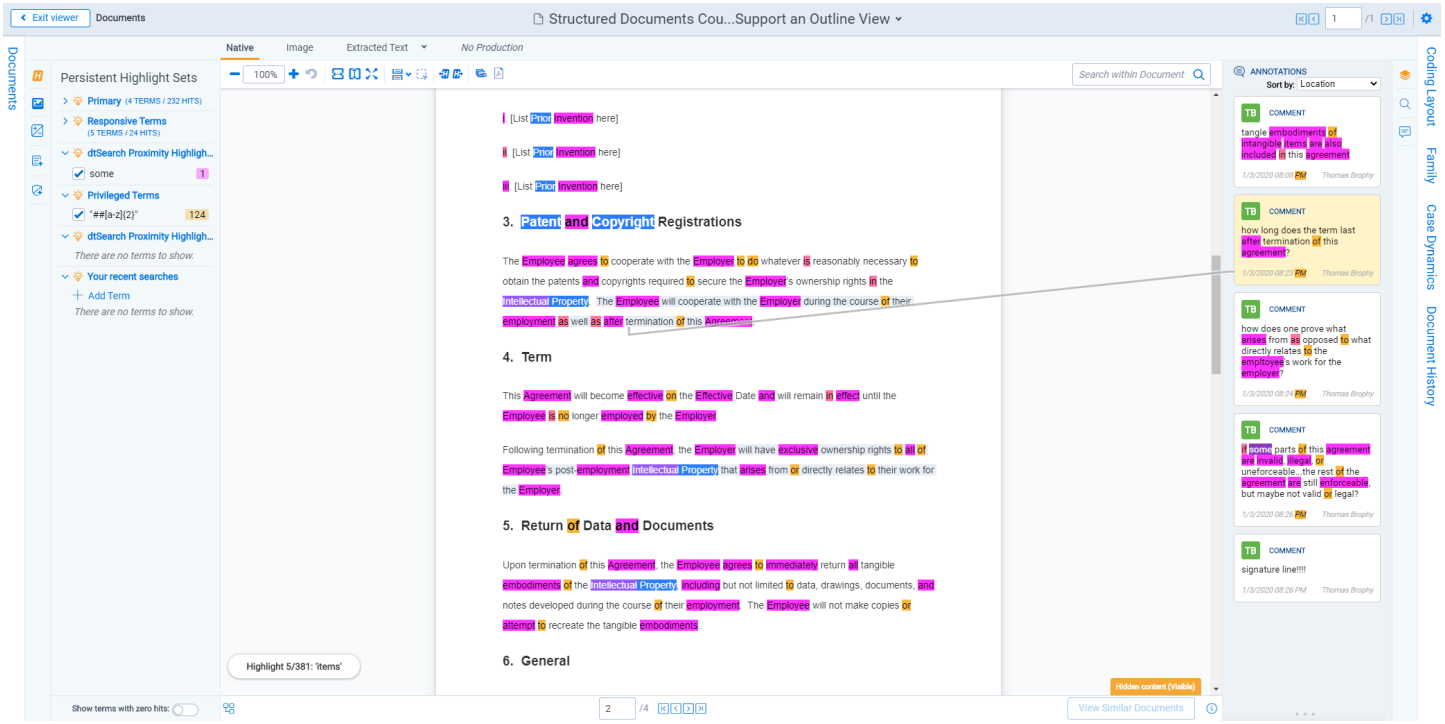
Each type of annotation comes with its distinct highlight in the Native Viewer. Below is a table that lists each annotation type with its highlight in the Viewer:

File type	Modification	Annotation
Excel	Inserted cell	Green dotted border around cell.
Excel	Deleted cell	Red dotted border around cell.
Excel	Concealed cell text	If a cell contains enough text that the column needs to be re-sized to display it all and that cell is next to another cell with text, the full text of the cell does not display. Click **Hidden Content** to display the cell's full text.
Excel	Modified cell	Purple dotted border around cell.
Excel	Moved cell	Red dotted border around original location; green dotted border around new location.
Excel	Inserted row	Green shading in the row header.
Excel	Deleted row	Red shading with "DEL" in the row header. If the row is added then deleted, the shading is purple.
Excel	Inserted column	Green shading in column header.
Excel	Deleted column	Red shading with "DEL" in the column header. If the row is added then deleted, the shading is purple.
Excel	Inserted sheet	Green shading in the sheet tab.
Excel	Hidden sheet	Grey text in the sheet tab.
Excel	Modified sheet	Purple shading on the sheet tab.
Word	Comments	Blue background on text and note bubble in document.
Word	Insertions	Green shading behind text.
Word	Deletions	Red shading behind text.
Word	Moves	Purple shading behind text.
Word	Hidden text	Red shading behind text.
PowerPoint	Speaker notes	Page under sheet. Each of these pages count toward the document's total number of pages. If you try to navigate to a speaker note, the Viewer will take you to the page above the speaker note, so you can see what the note applies to.
PowerPoint	Comments	Note bubble in presentation.
PowerPoint	Hidden slide	Hidden icon in bottom left corner of slide.
PDF	Comments	Note bubble in document.

Leader lines

Clicking on an annotation or a comment in the Viewer connects it with the related annotation or comment in the Hidden Content or Document Comments pane. If you click on another annotation or comment, the leader line updates to the most recent annotation or comment you have selected.

One connector line is available at a time, unless you moved a cell. In this case, there is a leader line where the cell was originally located and a leader line in the cell's new location. Click the same annotation to remove the leader line.



Note: The Has Hidden Data field is populated during Processing. The hidden content that the Viewer finds may not be perfectly in-sync with the hidden data that the Processing engine finds.

39.3 Image Viewer

When you switch to the Image Viewer, a .tiff or .jpeg version of the document displays. You can highlight and redact images in this mode. The Image Viewer is only available if you have loaded an imaged version of the document in the Viewer or if you have manually imaged the file using the Image on the fly option in the Document actions menu. For more information, see Imaging on the fly.

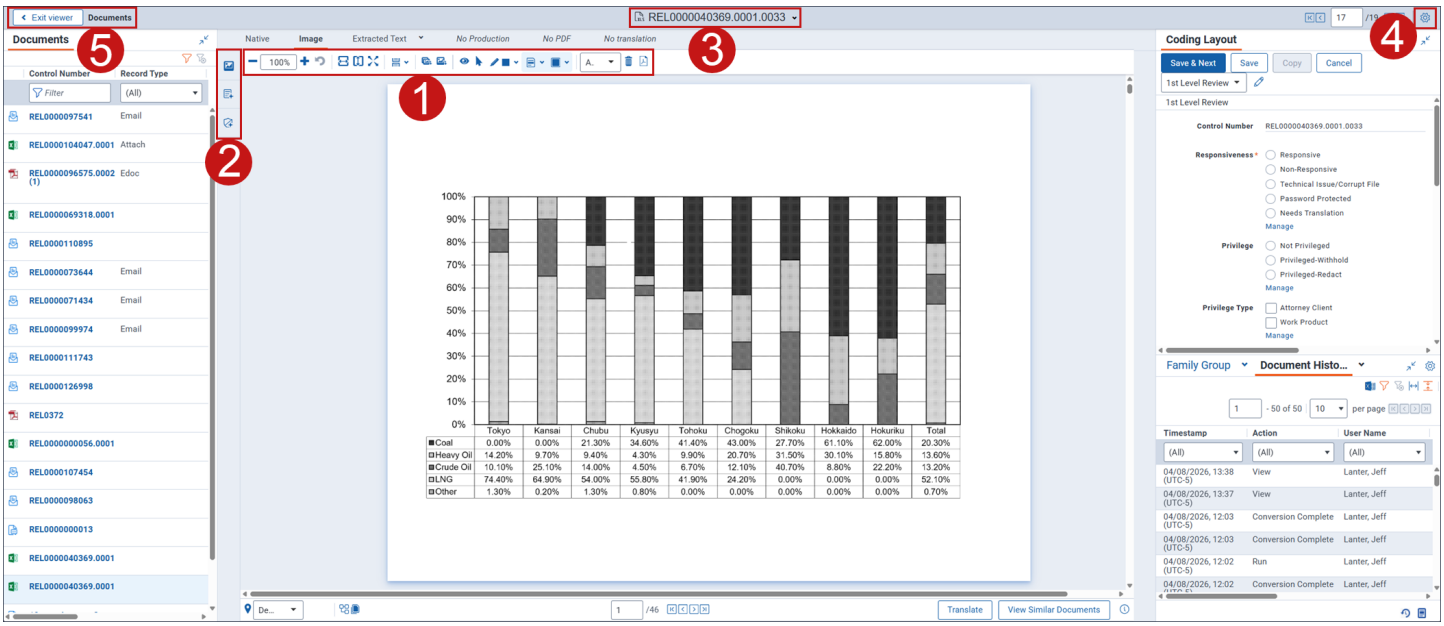
The redactions that are burned into a produced image are the redactions that were on the image at the time that you produced it. If you add or remove redactions from an image after you have produced it, then the image and the produced version of that image will be out of sync.

39.3.1 Navigating the Image Viewer

The Image Viewer offers several ways of viewing and working with documents.

Note: If you used the Basic Imaging profile to produce images of a PDF file, please note that the Viewer displays PDF text by mapping the character codes to Unicode in most cases. To check whether PDF text has been properly encoded and will display correctly in the Viewer, copy the text in the original PDF file and paste it into another application like Microsoft Word or Notepad. If the pasted text does not display correctly, the PDF is not properly encoded. If the pasted text displays correctly in another application but not in the Viewer, contact Support for assistance.

There are options available in the following sections of the Viewer:



1. Image Viewer toolbar options
2. Left drawer Viewer options
3. Document actions menu
4. Viewer settings menu
5. Viewer breadcrumbs

Each of these options and menus is described in more detail in the sections below.

39.3.1.1 Image Viewer toolbar options

The Image Viewer displays the following icons in the toolbar:



- **Zoom Out/In** —zooms out and in on the current document in increments of 10% within a range of 10% to 4,000%. If you attempt to zoom out to a percentage lower than 10%, the Viewer automatically sets the display to 10%. If you attempt to zoom in to a percentage higher than 4,000%, the Viewer automatically sets the display to 4,000%. Your zoom setting persists as you navigate through a document set. This means that if you have set one document to 150% and you go to the next document, the next document defaults to 150% zoom.
  To specify a zoom percentage without using the zoom out/in toolbar buttons, type the number in the percentage field and press the **Enter** key.
- **Reset Zoom** —resets the zoom to 100%.
- **Fit Width** —increases the size of the document to fit the maximum width of the Viewer. This setting persists when you re-size the window.
- **Fit Page** —fits the entire document into the total size of the page. Clicking this zooms out the document and reduces the font size.
- **Fit Actual** —fits the document display to the actual size it was in its native application. By default, this resets the zoom percentage to 100%.

- **Layout Mode** —select one of the following options to determine how documents that are more than one page long display in the Viewer.
  - **Single** —one page of a document will display at a time. Use the page navigation options at the bottom of the Viewer to adjust which page you view.
  - **Single Continuous** —displays the pages in the document stacked vertically so you can scroll up and down to view them.
  - **Facing Continuous** —displays the pages in the document in a row horizontally so you can scroll left and right to view them.
- **Rotate all pages** —rotates all pages in a document clockwise 90 degrees.
- **Rotate current page** —rotates only the current page clockwise 90 degrees.

Note: Image rotation is persistent. Any pages that you rotate will be rotated the next time you return to them in the Viewer and for other users who view them after you rotate them. Rotation is also applied when you run the production containing the images.

- **Selector** —select within a document.
- **Markup Visibility** —changes the visibility mode of the markups between full visibility, transparent and hidden. By default, this is set to Solid, which means all highlights and redactions appear as solid as you applied them.
- **Highlight - <Color>** —highlights the selected text with the color you specify from the drop-down menu. The default color is blue. Select from the following:
  - Blue
  - Green
  - Orange
  - Pink
  - Purple
  - Yellow
- **Redaction Mode - Basic Redact** —enables the basic redaction tool. For more information, see Creating inverse redactions on page 344.
- **Redaction Mode - Full page** —enables the full-page redaction tool. The drop-down menu for this redaction type offers the same options as the basic Redact icon, except that the redaction you choose is applied to the entire page. For example, if you select White, the entire page becomes white. For more information, see Creating full-page redactions on page 344.
- **Redaction Mode - Inverse** —enables the inverse redaction tool. For more information, see Creating inverse redactions on page 344.
- **Redaction Mode - Mass Redact** —apply a full-page redaction across all images or a range of images in the document. For more information, see Creating mass redactions on page 345.
- **Redaction Type - <Style>** —enables single redaction tool. For more information on redacting, see Creating basic redactions on page 343. Select from the following types of redactions:
  - **Black** —applies a solid black box to the selected text.
  - **Cross** —applies a white box with an X in the middle of it over the selected text.

- **Text** —applies a box over the selected text, in which you can add text such as "Privileged" or "Redacted."
- **White** —applies a solid white box over the selected text.

- **Font Size** —change the font size of the text within a text box redaction.
- **Delete Highlights** —mass delete markups from any or all images in the document. For more information, see Mass deleting markups on page 349.
- **Create PDF** —gives you the option of saving the image as a PDF. For more information, see Saving an image as a PDF.

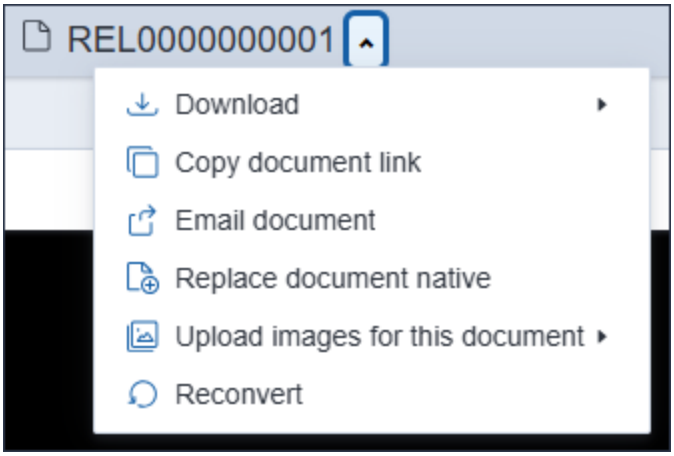
39.3.1.2 Left drawer Image Viewer options

The following options are available in the left drawer:



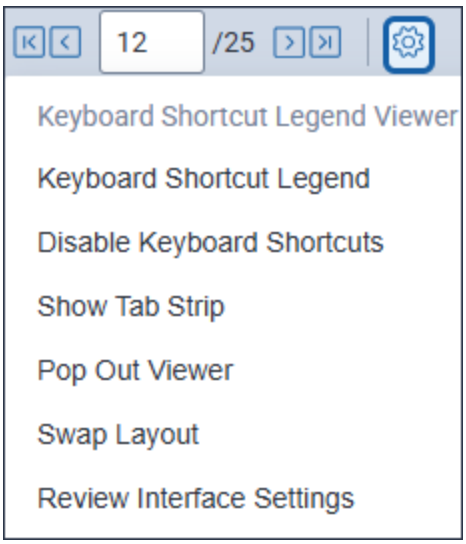
- **Thumbnail**—click to expand the left drawer and display the Thumbnail Viewer. Each page of the document you are reviewing has its own numbered thumbnail in the Thumbnail Viewer. To learn more, visit Thumbnail Viewer.
- **aiR Review Analysis**—click to expand or collapse the left drawer and display aiR Review results. You can also enable or disable aiR Review highlights.
- **Privilege Analysis**—click to expand or collapse the left drawer and display Privilege results.

39.3.1.3 Document actions menu



To learn more about these options, see Document actions menu.

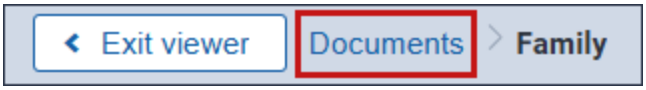
39.3.1.4 Viewer settings menu



To learn more about these options, see Viewer settings menu.

39.3.1.5 Viewer breadcrumbs

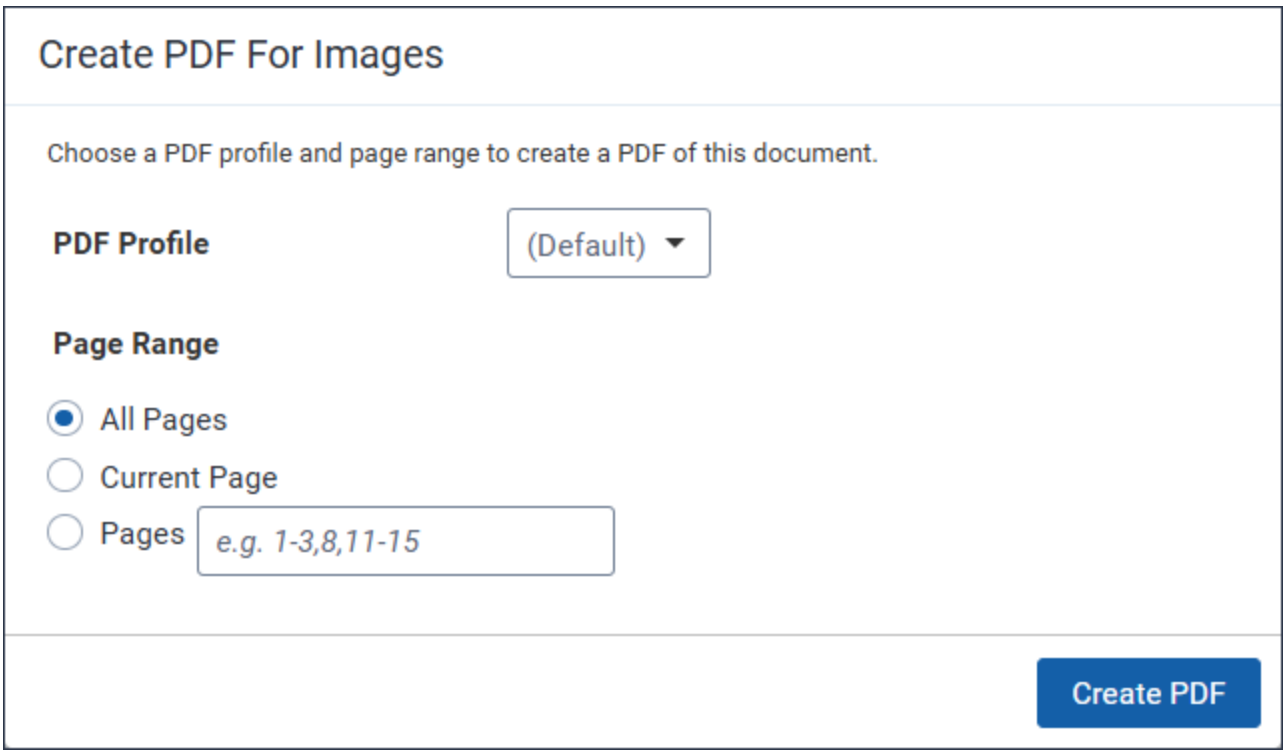
The Viewer breadcrumbs help you track your current location while browsing documents in the Related items card. The information on your current location updates as you navigate. If Documents is an active link, you can click it to return to the document you were viewing before browsing documents in the Related items card.



Additionally, to exit the Viewer and return to the page you were previously on, you can click the **Exit viewer** button at any time.

39.3.2 Saving an image as a PDF

Clicking the **Create PDF** icon brings up the following window, in which you can specify your PDF settings:



- **PDF Profile**—select the desired PDF profile to determine how the PDF will be customized.
- **Page Range**—select from the following standard print range options:
  - **All pages**—saves all pages in the document.
  - **Current Page**—saves only the page you are currently on.
  - **Pages**—saves a range of pages that you specify in the text box to the right.

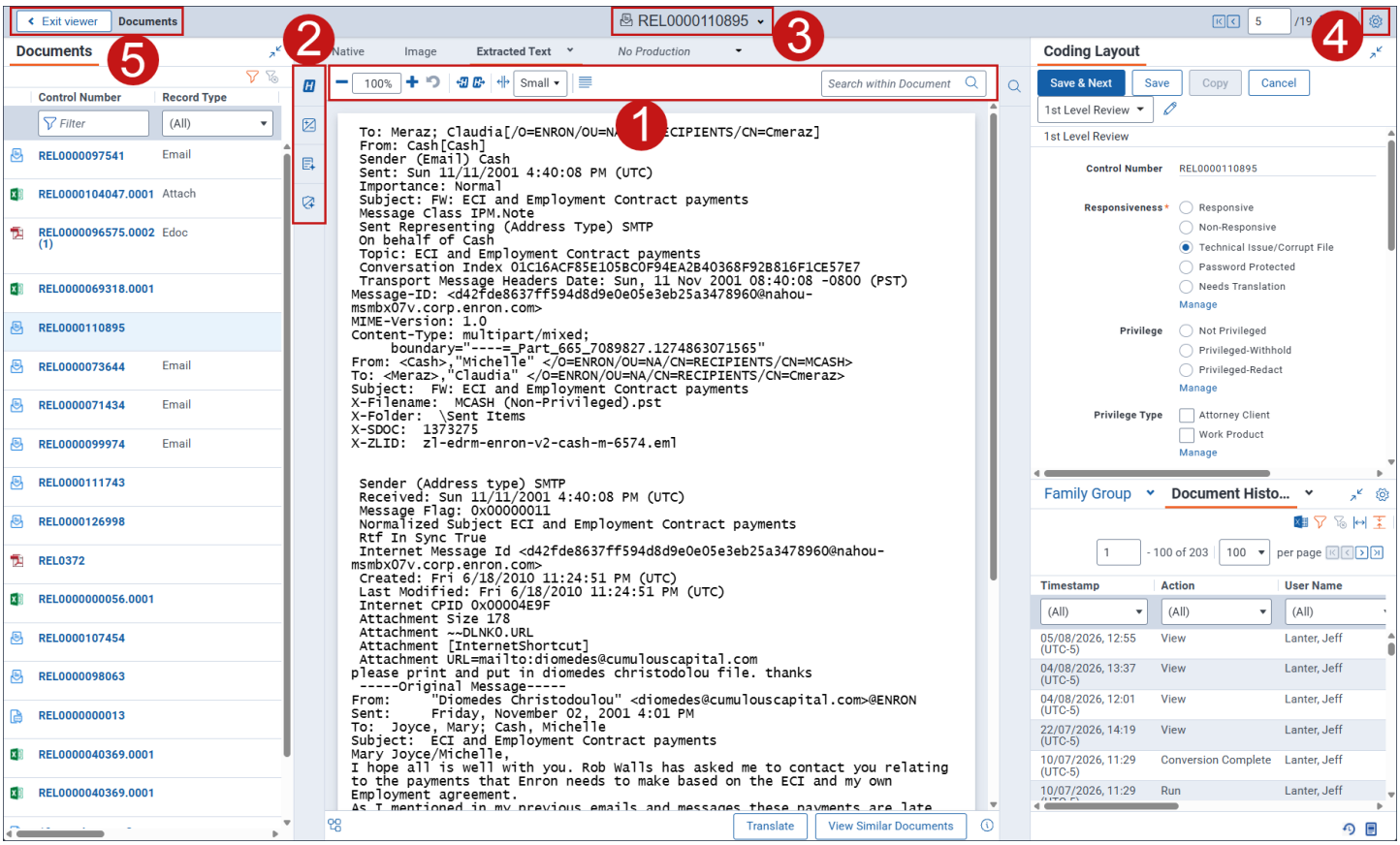
39.4 Extracted Text Viewer

When you switch to Extracted Text Viewer in the Viewer type tabs, you can access a drop-down menu on the right side of the Extracted Text tab where all extracted text and all long text fields on the field edit/creation page are available. See Creating and editing fields. The drop-down menu lists long-text fields that contain text for the current document open in the Viewer and those you have permissions to.

Notes: Relativity displays all long text fields made available in the Viewer in the drop-down menu, regardless of whether that field contains text for the current document. If you select a long text field from the drop-down list, and the current document does not have text for that field, the Viewer displays a message stating, "This page is empty". The Viewer displays PDF text by mapping the character codes to Unicode in most cases. To check whether PDF text has been properly encoded and will display correctly in the Viewer, copy the text in the original PDF file and paste it into another application like Microsoft Word or Notepad. If the pasted text does not display correctly, the PDF is not properly encoded. If the pasted text displays correctly in another application but not in the Viewer, contact Support for assistance.

39.4.1 Navigating the Extracted Text Viewer

The Extracted Viewer offers several ways of viewing and working with documents. There are options available in the following sections of the Viewer:



1. Extracted Text Viewer toolbar options
2. Left drawer Viewer options
3. Document actions menu
4. Viewer settings menu
5. Viewer breadcrumbs

Each of these options and menus is described in more detail in the sections below.

39.4.2 Extracted Text Viewer toolbar options

The Extracted Text Viewer provides the following options:



- **Zoom Out/In** —zooms out and in on the current document in increments of 10% within a range of 10% to 4,000%. If you attempt to zoom out to a percentage lower than 10%, the Viewer automatically sets the display to 10%. If you attempt to zoom in to a percentage higher than 4,000%, the Viewer automatically sets the display to 4,000%. Your zoom setting persists as you navigate through a document set. This means that if you have set one document to 150% and you go to the next document, the next document defaults to 150% zoom.
  To specify a zoom percentage without using the zoom out/in toolbar buttons, type the number in the percentage field and press the **Enter** key.
- **Reset Zoom** —resets the zoom to 100%.
- **Go To Next/Previous Highlight** —moves through previous and next highlighted terms in the document.

- **Tab character size** —select an option from the drop-down menu to determine the amount of space that is taken when the Tab key was used in the current document. This option can help you ensure that the spacing in a spreadsheet document is aligned and works best when the Tab key is used after each column in the spreadsheet.
- **Toggle WordWrap** —determines whether the text in the current document will wrap so that it fits on the current page or not.
  - **Enabled** —text in the current document will be forced onto the next line if it cannot display in the current window size. You cannot scroll horizontally with Toggle WordWrap enabled.
  - **Disabled**—text in the current document will not be forced onto the next line will display in more horizontal fashion. You can scroll horizontally to control to view the desired text
- **Search Bar**—searches for terms in the current document and navigates through the hits.
  - Entering a term and either clicking the left or right arrow button or pressing **Enter** in this text box scrolls to and highlights the text of the next instance of the term, from the placement of the cursor.
  - Searching in this text box is not case sensitive.
  - Searching supports dtSearch and so proximity, fuzziness, and stemming can be used. Unlike dtSearch, the Viewer doesn't have an alphabet file or run on an index. So, while characters like - act as word breaks for searching, they do not for proximity.

Note: If you don't have permission to the Local Access option on the Document object, you can't use the Ctrl+C or Ctrl+Ins options in either the Native Viewer or the Extracted Text Viewer.

39.4.3 Left drawer Viewer options

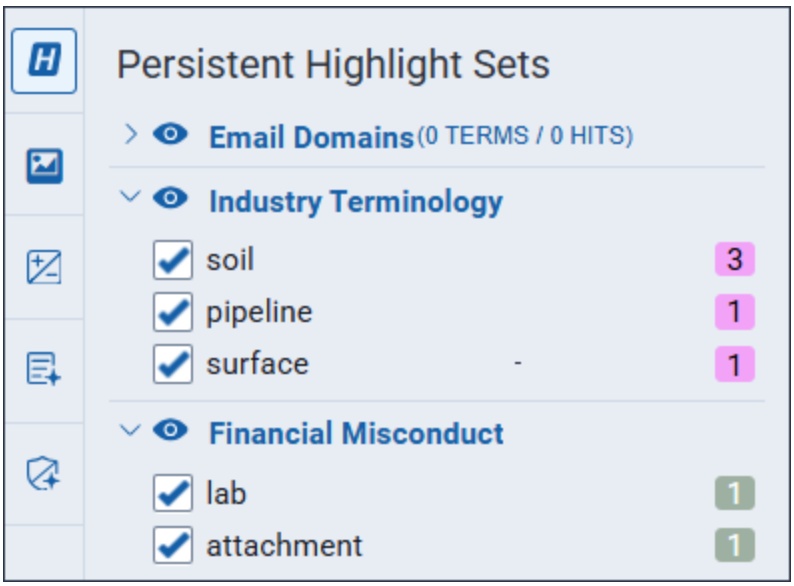
The following options are available in the left drawer:



- **Persistent Highlighting**—displays or hides a card containing all recent searches from the criteria entered in the search bar and any persistent highlight sets in the workspace. You can also create a dtSearch or keyword search in the Your recent searches section. Only terms in the sets and recent searches that are in the current document will display in the pane.

  Note: Because the extracted text varies from the text in the Native Viewer, persistent highlight functionality may differ and some terms might be highlighted in one Viewer and not the other.

  Additionally, you can control which highlights display in the current document by clicking on either the persistent set to only display highlights from that set or you can click on a specific term to only see that term highlighted in the document. You can also navigate to and from highlights using this pane.



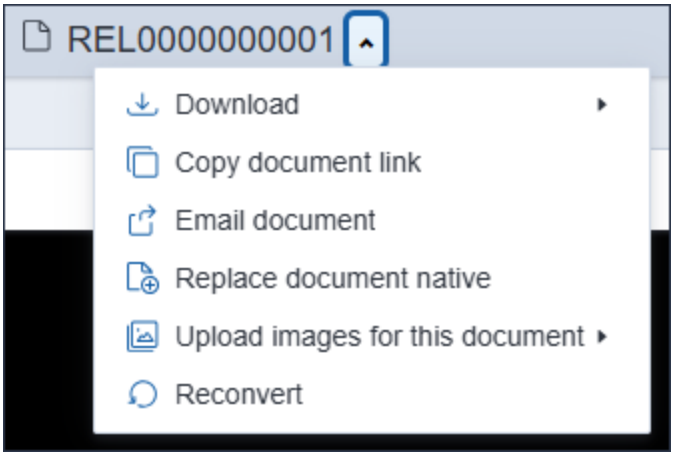
- **Sentiment**—click to expand or collapse the left drawer and display sentiment analysis highlights in the Viewer.
- **aiR Review Analysis**—click to expand or collapse the left drawer and display aiR Review results. You can also enable or disable aiR Review highlights.
- **Privilege Analysis**—click to expand or collapse the left drawer and display Privilege results.

39.4.4 Right drawer Viewer options

The following option is available in the right drawer:

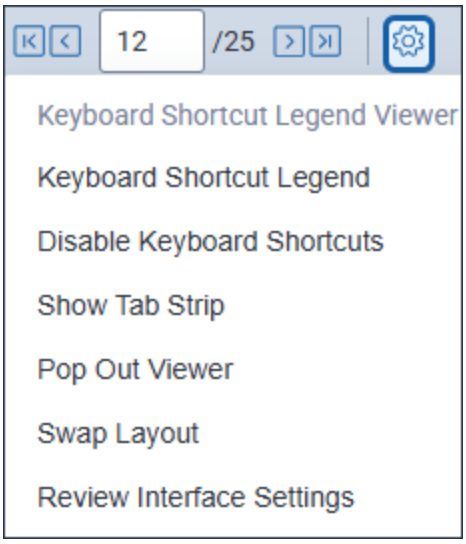
- **Contextual Search**—click to expand the right drawer and display the Contextual Search card. This feature allows you to quickly navigate to matching search terms in a document which is useful in longer documents or ones that have many matching search terms. The Contextual Search card has the same functionality as the Search Bar. To learn more about the Search Bar's functionality, see Search Bar. Additionally, each search term match is displayed in a box that includes both words before and after the search term match to make it easy for you to view the context of each one.
  Enter a term or terms in the search box and press **Enter** on your keyboard to highlight in yellow any matches in the current document. You can click on a desired search term box in the pane to jump to that place in the document. The active search term box will display with a blue border and the matching search term in the document will be highlighted in blue to make it easy to find.

39.4.5 Document actions menu



To learn more about these options, see Document actions menu.

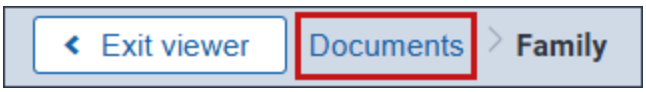
39.4.6 Viewer settings menu



To learn more about these options, see Viewer settings menu.

39.4.7 Viewer breadcrumbs

The Viewer breadcrumbs help you track your current location while browsing documents in the Related items card. The information on your current location updates as you navigate. If Documents is an active link, you can click it to return to the document you were viewing before browsing documents in the Related items card.



Additionally, to exit the Viewer and return to the page you were previously on, you can click the **Exit viewer** button at any time.

39.5 Productions Viewer

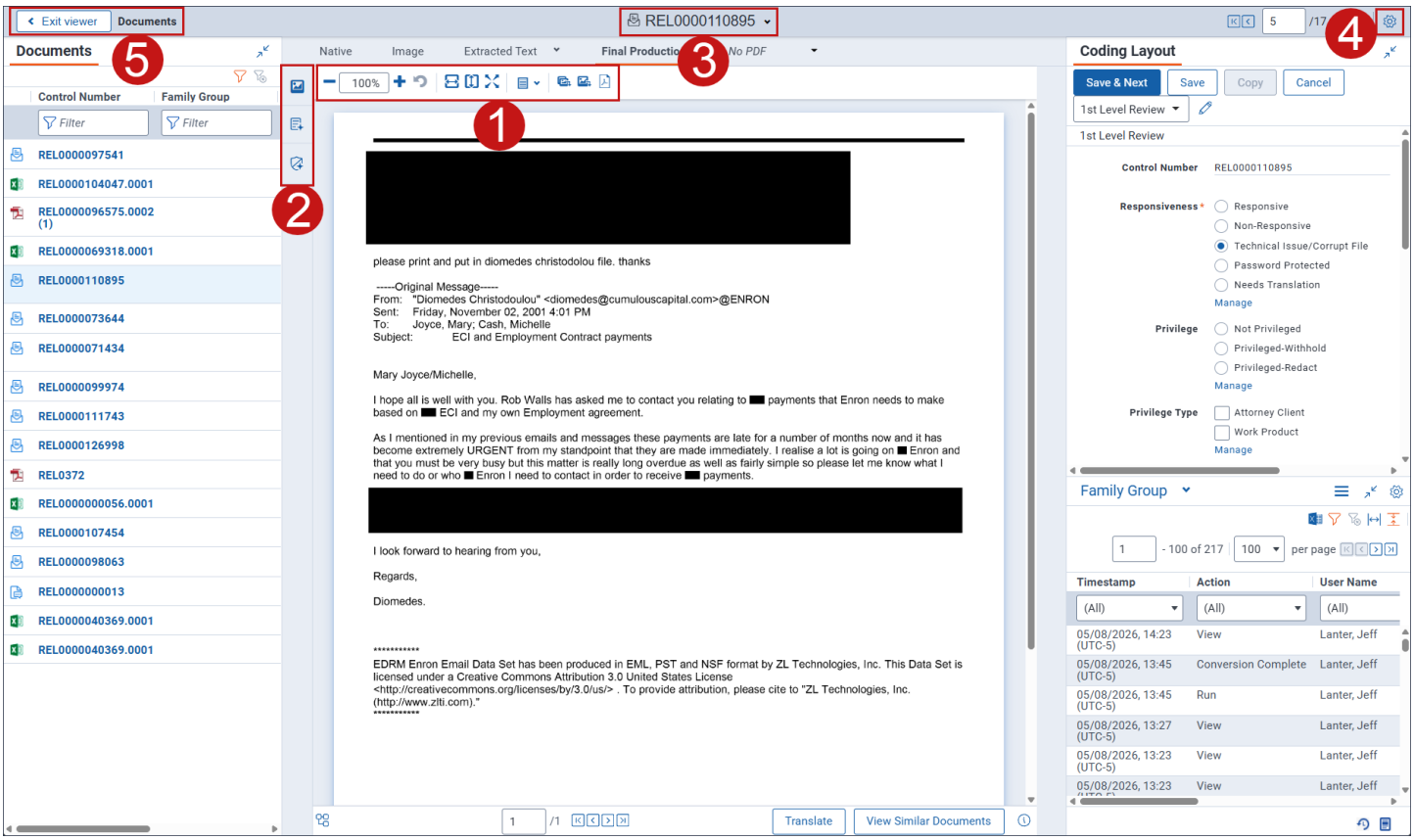
When you switch to the Productions Viewer in the Viewer type tabs, you can access a drop-down menu on the right side of the Productions Viewer tab that displays available production sets that contain the current document. For information about creating production sets, see Production sets in the Admin guide.

Note: The redactions that are burned into a produced image are the redactions that were on the image at the time that you produced it. If you add or remove redactions from an image after you have produced it, then the image and the produced version of that image will be out of sync.

Select a production set from the drop-down menu to see how a document was produced in the selected production. If a document is not included in a production, the productions mode option is unavailable.

39.5.1 Navigating the Productions Viewer

The Productions Viewer offers several ways of viewing and working with documents. There are options available in the following sections of the Viewer:



1. Productions Viewer toolbar options
2. Left drawer Viewer options
3. Document actions menu
4. Viewer settings menu
5. Viewer breadcrumbs

Each of these options and menus is described in more detail in the sections below.

39.5.1.1 Productions Viewer toolbar options

Productions Viewer provides the following options:



- **Create PDF** —gives you the option of saving the image as a PDF. For more information, see Saving an image as a PDF.
- **Zoom Out/In** —zooms out and in on the current document in increments of 10% within a range of 10% to 4,000%. If you attempt to zoom out to a percentage lower than 10%, the Viewer automatically sets the display to 10%. If you attempt to zoom in to a percentage higher than 4,000%, the Viewer automatically sets the display to 4,000%. Your zoom setting persists as you navigate through a document set. This means that if you have set one document to 150% and you go to the next document, the next document defaults to 150% zoom.
  To specify a zoom percentage without using the zoom out/in toolbar buttons, type the number in the percentage field and press the **Enter** key.
- **Reset Zoom** —resets the zoom to 100%.

- **Fit Width** —increases the size of the document to fit the maximum width of the Viewer. This setting persists when you re-size the window.
- **Fit Page** —fits the entire document into the total size of the page. Clicking this zooms out the document and reduces the font size.
- **Fit Actual** —fits the document display to the actual size it was in its native application. By default, this resets the zoom percentage to 100%.
- **Layout Mode** —select one of the following options to determine how documents that are more than one page long display in the Viewer.
    - **Single** —one page of a document will display at a time. Use the page navigation options at the bottom of the Viewer to adjust which page you view.
    - **Single Continuous** —displays the pages in the document stacked vertically so you can scroll up and down to view them.
    - **Facing Continuous** —displays the pages in the document in a row horizontally so you can scroll left and right to view them.
- **Rotate all pages** —rotates all pages in a document clockwise 90 degrees.
- **Rotate current page** —rotates only the current page clockwise 90 degrees.

Note: Image rotation is persistent. Any pages that you rotate will be rotated the next time you return to them in the Viewer and for other users who view them after you rotate them. Rotation is also applied when you run the production containing the images.

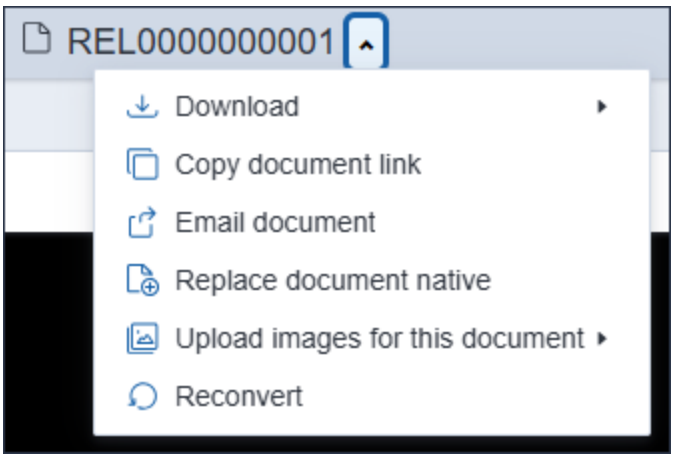
39.5.1.2 Left drawer Productions Viewer options

The following options are available in the left drawer:



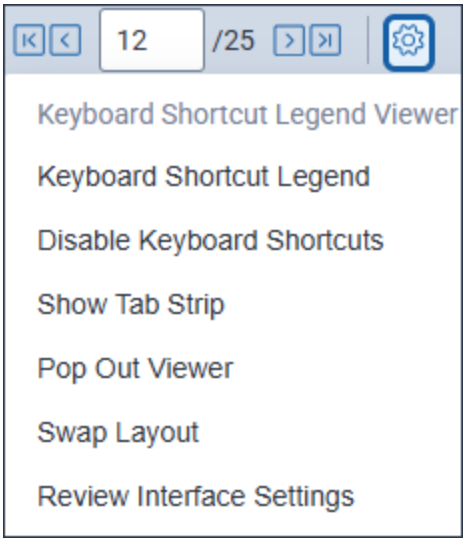
- **Thumbnail**—click to expand the left drawer and display the Thumbnail Viewer. Each page of the document you are reviewing has its own numbered thumbnail in the Thumbnail Viewer. To learn more, visit Thumbnail Viewer.
- **aiR Review Analysis**—click to expand or collapse the left drawer and display aiR Review results. You can also enable or disable aiR Review highlights.
- **Privilege Analysis**—click to expand or collapse the left drawer and display Privilege results.

39.5.1.3 Document actions menu



To learn more about these options, see Document actions menu.

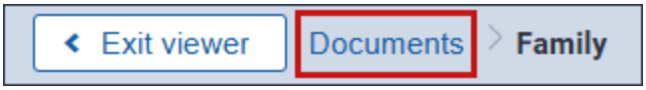
39.5.1.4 Viewer settings menu



To learn more about these options, see Viewer settings menu.

39.5.1.5 Viewer breadcrumbs

The Viewer breadcrumbs help you track your current location while browsing documents in the Related items card. The information on your current location updates as you navigate. If Documents is an active link, you can click it to return to the document you were viewing before browsing documents in the Related items card.



Additionally, to exit the Viewer and return to the page you were previously on, you can click the **Exit viewer** button at any time.

39.5.2 Imaging on the fly

You can image a single document in the Viewer by selecting the Image on the fly option from the Document actions menu at the top-center of the page.

Using this feature, you can select any imaging profile you have permissions to view and use it to image the document.

Note: If the source file of the document you are imaging is changed during the conversion process, for example through overlay, that document becomes undeliverable and you receive an error. To resolve this error, refresh the page or re-image the document.

After imaging a document on the fly, you can access thumbnail renderings of the imaged pages of the document.

Imaging some file formats can cause problems. Consider the following:

- Many PDFs render and image very well. However, you may have problems rendering and imaging some PDFs due to the variety of their content.
- While most Microsoft Office documents render and image well, you may experience issues when imaging documents with embedded files.
- You may have problems rendering and imaging vector-based documents like Visio and CAD.

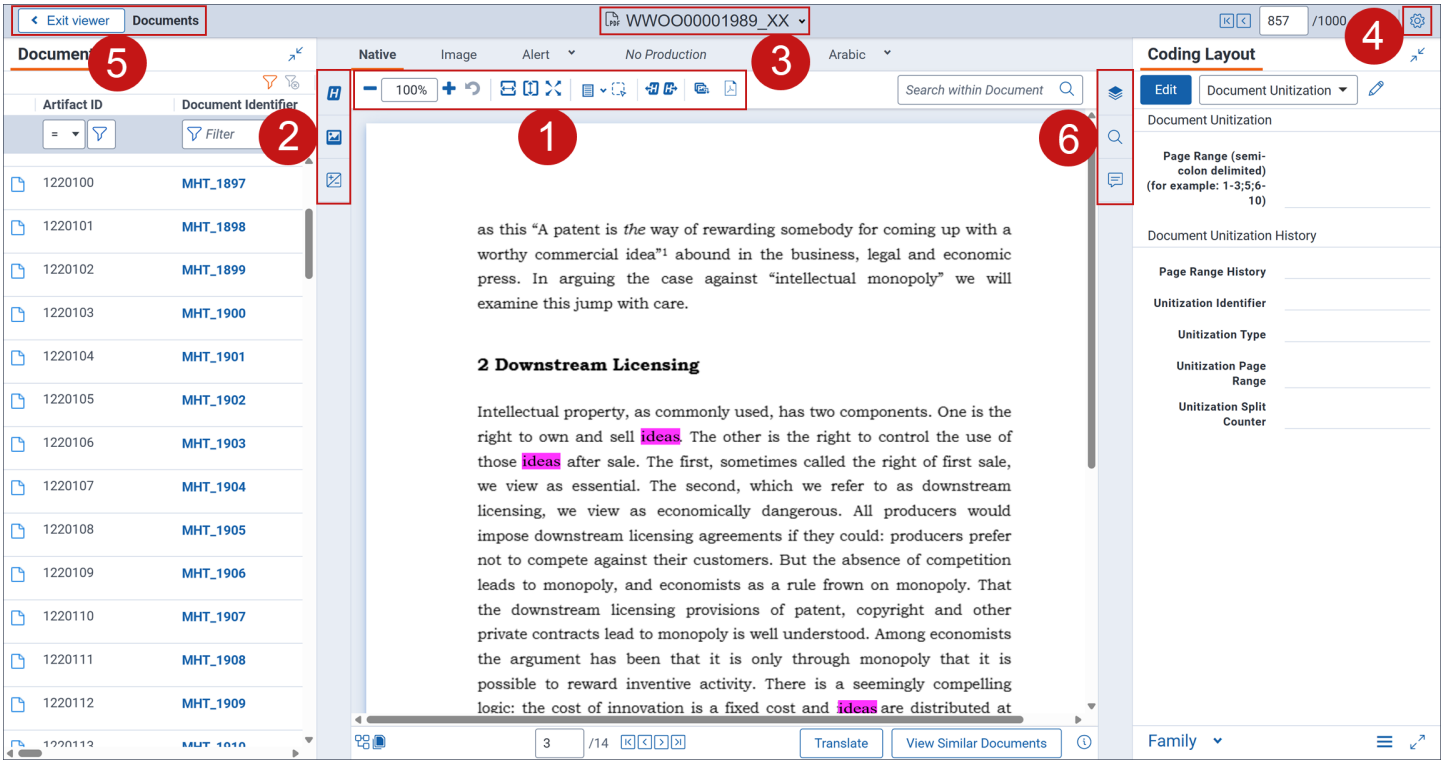
39.6 PDF Viewer

Note: To ensure maximum PDF Viewer performance, we recommend using Google Chrome version 126 or above.

The PDF Viewer allows you to view PDF files in the Review Interface.

Note: You may experience slowness if you try to open PDF documents that are larger than 300 megabytes. The Viewer displays PDF text by mapping the character codes to Unicode in most cases. To check whether PDF text has been properly encoded and will display correctly in the Viewer, copy the text in the original PDF file and paste it into another application like Microsoft Word or Notepad. If the pasted text does not display correctly, the PDF is not properly encoded. If the pasted text displays correctly in another application but not in the Viewer, contact Support for assistance.

There are options available in the following sections of the Viewer:



1. PDF Viewer toolbar options
2. Left drawer Viewer options
3. Document actions menu
4. Viewer settings menu
5. Viewer breadcrumbs
6. Right drawer Viewer options

Each of these options and menus is described in more detail in the sections below.

39.6.1 PDF Viewer toolbar options

The PDF Viewer provides the following options:



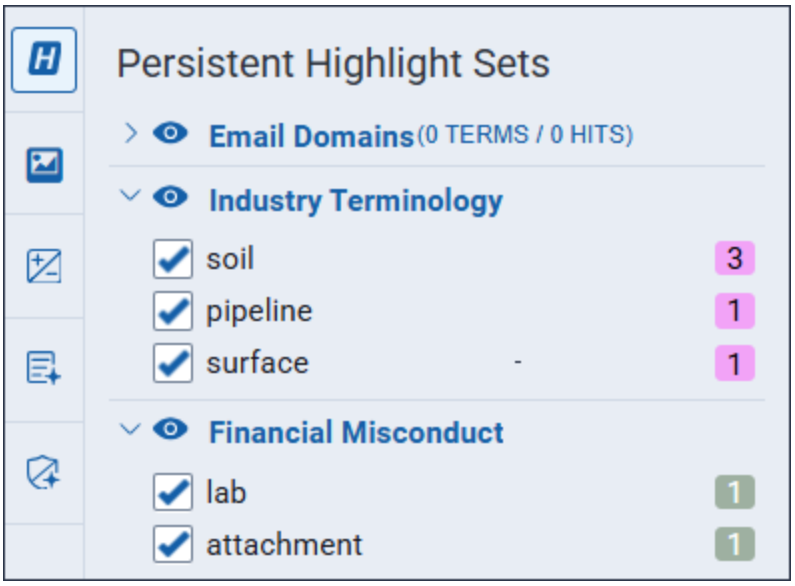
- **Zoom Out/In** —zooms out and in on the current document in increments of 10% within a range of 10% to 4,000%. If you attempt to zoom out to a percentage lower than 10%, the Viewer automatically sets the display to 10%. If you attempt to zoom in to a percentage higher than 4,000%, the Viewer automatically sets the display to 4,000%. Your zoom setting persists as you navigate through a document set. This means that if you have set one document to 150% and you go to the next document, the next document defaults to 150% zoom.
  To specify a zoom percentage without using the zoom out/in toolbar buttons, type the number in the percentage field and press the **Enter** key.
- **Reset Zoom** —resets the zoom to 100%.
- **Fit Width** —increases the size of the document to fit the maximum width of the Viewer. This setting persists when you re-size the window.
- **Fit Page** —fits the entire document into the total size of the page. Clicking this zooms out the document and reduces the font size.
- **Fit Actual** —fits the document display to the actual size it was in its native application. By default, this resets the zoom percentage to 100%.
- **Layout Mode** —select one of the following options to determine how documents that are more than one page long display in the Viewer.
  - **Single** —one page of a document will display at a time. Use the page navigation options at the bottom of the Viewer to adjust which page you view.
  - **Single Continuous** —displays the pages in the document stacked vertically so you can scroll up and down to view them.
  - **Facing Continuous** —displays the pages in the document in a row horizontally so you can scroll left and right to view them.
- **Draft Mode** —click to begin Draft Mode which automatically contrasts text from the background, help you identify poorly drawn redactions, and identify corrupt OCR text. This option is only available on the Native Viewer and PDF Viewer with rendered documents.
- **Go To Next/Previous Highlight** —moves through previous and next highlighted terms in the document.

39.6.2 Left drawer Viewer options

The following options are available in the left drawer:



- **Persistent Highlighting**—displays or hides a card containing all recent searches from the criteria entered in the search bar and any persistent highlight sets in the workspace. You can also create a dtSearch or keyword search in the Your recent searches section. Only terms in the sets and recent searches that are in the current document will display in the pane.
  Additionally, you can control which highlights display in the current document by clicking on either the persistent set to only display highlights from that set or you can click on a specific term to only see that term highlighted in the document. You can also navigate to and from highlights using this pane.



- **Thumbnail**—click to expand the left drawer and display the Thumbnail Viewer. Each page of the document you are reviewing has its own numbered thumbnail in the Thumbnail Viewer.
- **Sentiment**—click to expand or collapse the left drawer and display Sentiment Analysis Highlights in the Viewer.
- **aiR Review Analysis**—click to expand or collapse the left drawer and display aiR Review results. You can also enable or disable aiR Review highlights.
- **Privilege Analysis**—click to expand or collapse the left drawer and display Privilege results.

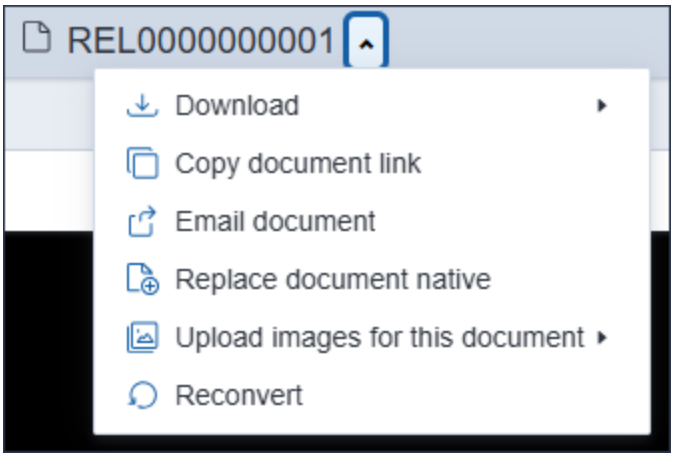
39.6.3 Right drawer Viewer options

The following options are available in the right drawer:



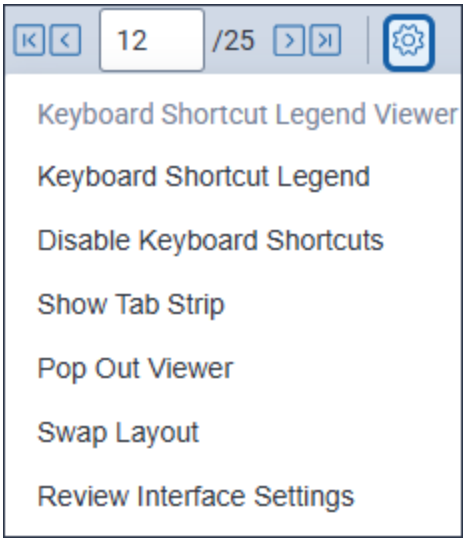
- **Hidden Content**—displays or hides information about hidden content. Hidden content can appear in Excel, Word, PDF, or Powerpoint documents. This functionality does not work on imaged documents because Relativity only images unhidden cells.
- **Contextual Search**—click to expand the right drawer and display the Contextual Search card. This feature allows you to quickly navigate to matching search terms in a document which is useful in longer documents or ones that have many matching search terms. The Contextual Search card has the same functionality as the Search Bar. To learn more about the Search Bar's functionality, see Search Bar. Additionally, each search term match is displayed in a box that includes both words before and after the search term match to make it easy for you to view the context of each one.
  Enter a term or terms in the search box and press **Enter** on your keyboard to highlight in yellow any matches in the current document. You can click on a desired search term box in the pane to jump to that place in the document. The active search term box will display with a blue border and the matching search term in the document will be highlighted in blue to make it easy to find.

39.6.4 Document actions menu



To learn more about these options, see Document actions menu.

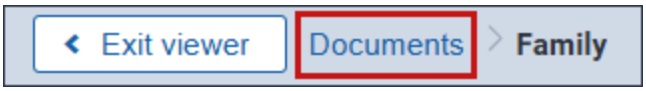
39.6.5 Viewer settings menu



To learn more about these options, see Viewer settings menu.

39.6.6 Viewer Breadcrumbs

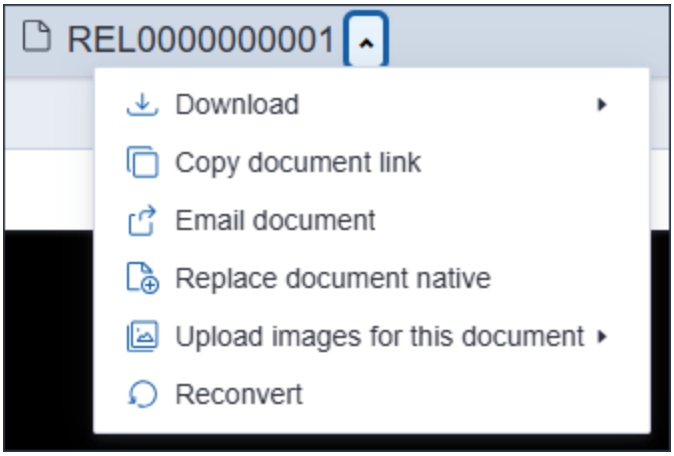
The Viewer Breadcrumbs help you track your current location while browsing documents in the Related items card. The information on your current location updates as you navigate. If Documents is an active link, you can click it to return to the document you were viewing before browsing documents in the Related items card.



Additionally, to exit the Viewer and return to the page you were previously on, you can click the **Exit viewer** button at any time.

39.7 Document actions menu

The following options are available in the Document actions menu:



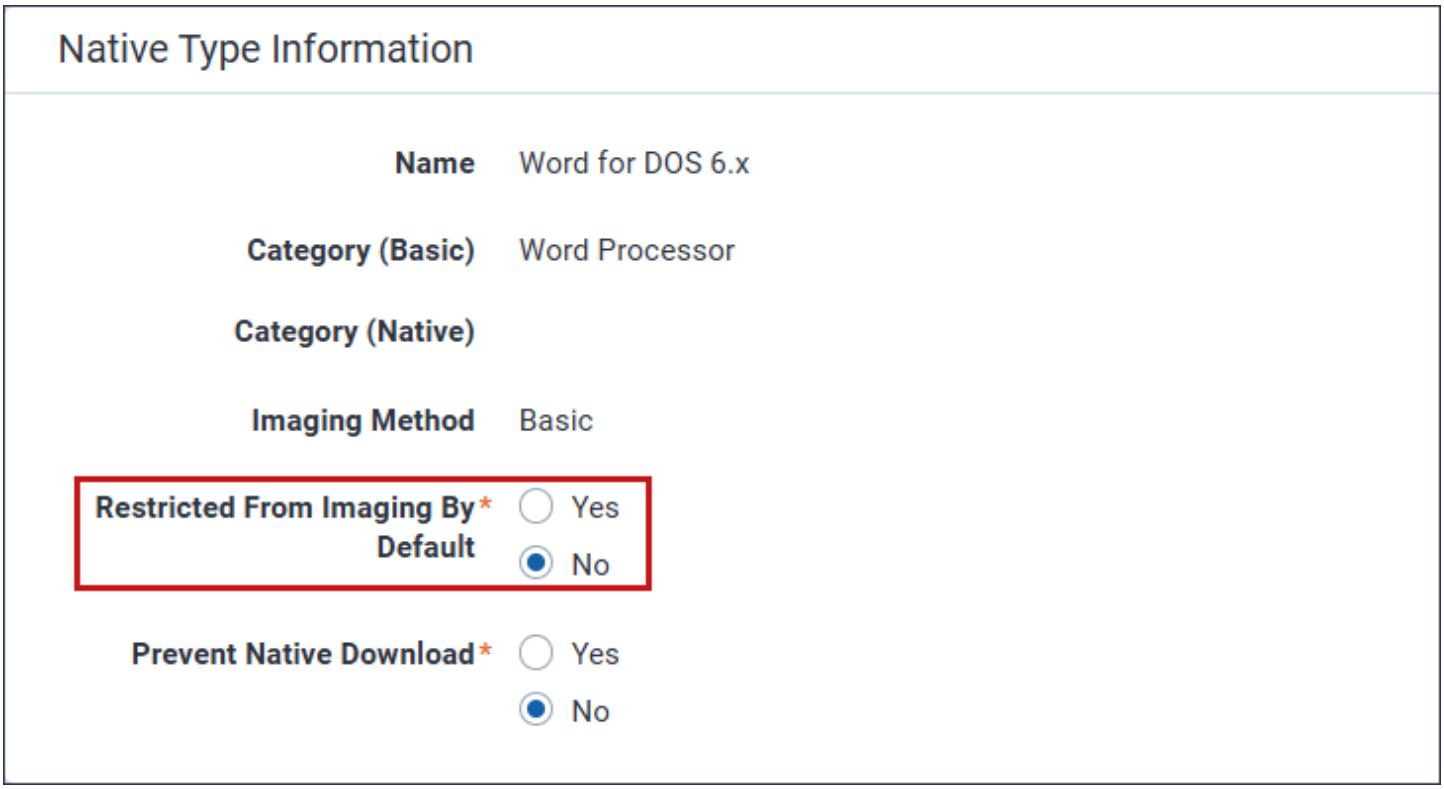
- **Download**—hover your cursor over this option and select one of the following:

  Note: Files over 2 GB cannot be downloaded using this option. If you have a document that is over 2 GB, you can create a saved search that includes any documents you wish to export and then export them using Import/Export.

  - **Active Production**—select to download a copy of the produced document. A user must be granted the Documents - Local Access (Download, Copy Text) permission to use this option.
  - **Document native**—select to download a copy of the current document. A user must be granted the Documents - Local Access (Download, Copy Text) permission to use this option. The Documents - Local Access (Download, Copy Text) permission does not prevent users from being able to download native file on an RDO.
    If you cannot download a copy of the document, this option is grayed out. Hover your cursor over this option to view a tooltip that contains an explanation why this option is disabled.
    A system or case administrator can determine which native file types users can and cannot download by doing the following:
    1. Navigate to the **Native Types** tab.
    2. Click the **Edit** icon in the row of the desired file type.
    3. On the **Prevent Native Download** field, select **Yes** to prevent users from downloading it or **No** to allow users to download it.
  - **PDF**—select to download a copy of the stored PDF of the current document. To create a stored PDF, use Mass PDF. A user must be granted the Documents - Local Access (Download, Copy Text) permission to use this option.
    If you cannot download a copy of the document, this option is grayed out. Hover your cursor over this option to view a tooltip that contains an explanation why this option is disabled.
- **Copy document link**—select to copy the URL to the current document to your clipboard.
- **Email document**—select to open an email in your default email application with the URL to the current document included in the body of the email. The subject of the email will include the name of the workspace and the current document.
- **Replace document native**—select to replace the native file of the current document with a new file.
- **Image on the fly/Delete all images for this document**—Image on the fly will display if the current document has not been imaged. If the current document has been imaged, delete all images for this document will display instead.
  - **Delete all images for this document**—select to delete all original images associated with the current document.

    Note: If the document has produced images, these are not affected by this option. To remove the produced images from a document, delete the production set instead.
  - **Image on the fly**—to image the current document from the Viewer, hover your cursor over this option and the Image Profile options will display. Select the desired profile option to begin the imaging process.
    A system or case administrator can determine which native file types can or cannot be imaged using Image on the fly by doing the following:
    1. Navigate to the **Native Types** tab.
    2. Click the **Edit** icon in the row of the desired file type.

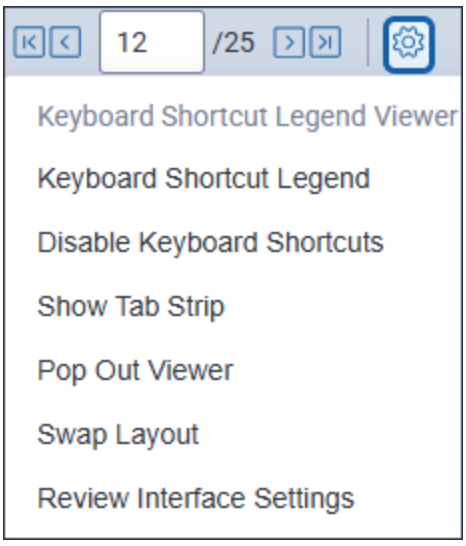
3. On the **Restricted From Imaging By Default** field, select **Yes** to prevent users from using this option to image the native type or **No** to allow users to image the native file type.



- **Replace images for this document**—to replace the images for the current document using an imaging profile, hover your cursor over this option and select the desired Imaging Profile option to begin the imaging process.
- **Reconvert**—select to clear your internet browser's cache and reload the current document for review.
- **Download translated document**—hover your cursor over this option and select the desired language to download a copy of the document in the selected language. This option only displays if a document has been translated.

39.8 Viewer settings menu

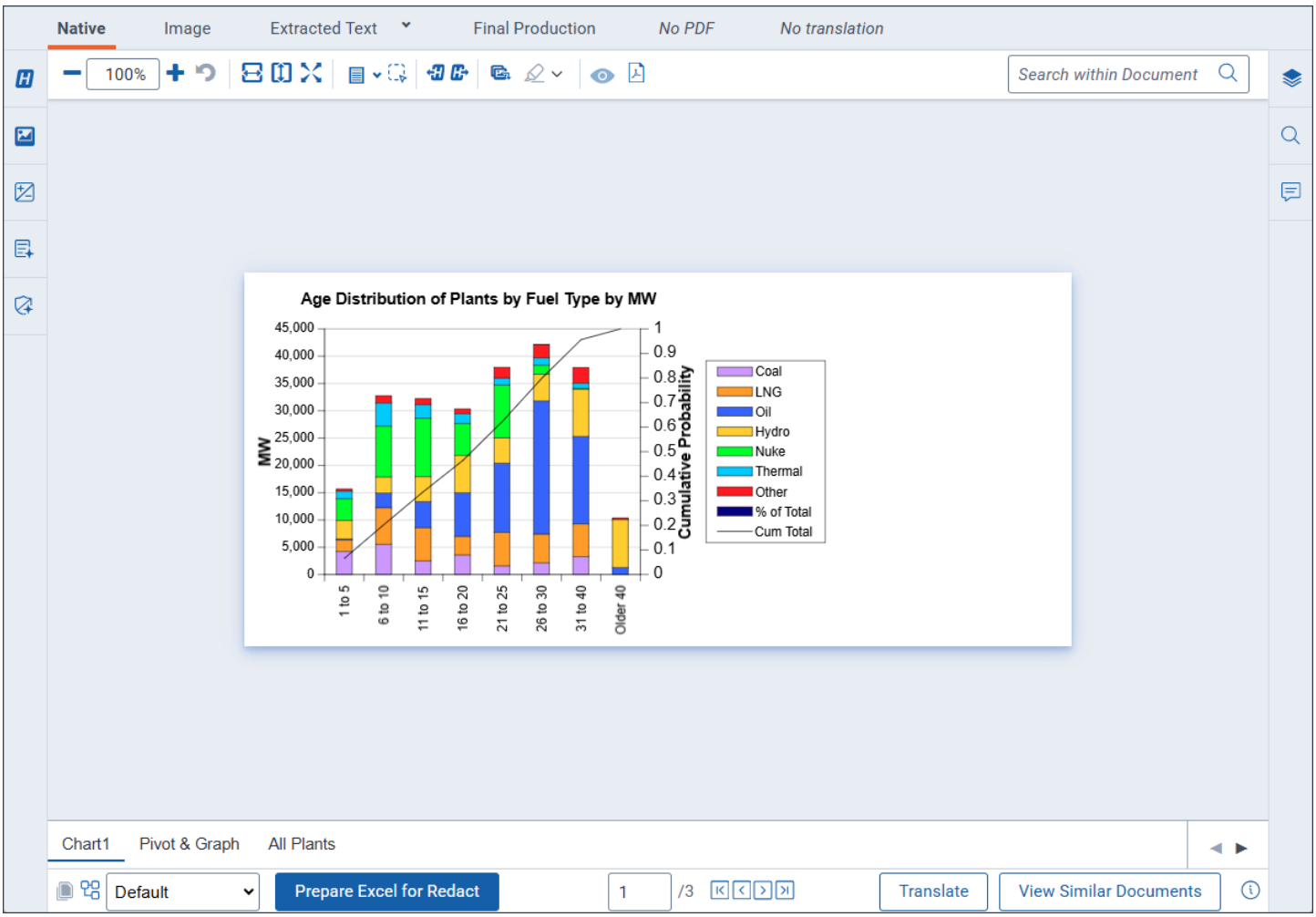
The following options are available in the Viewer settings menu:



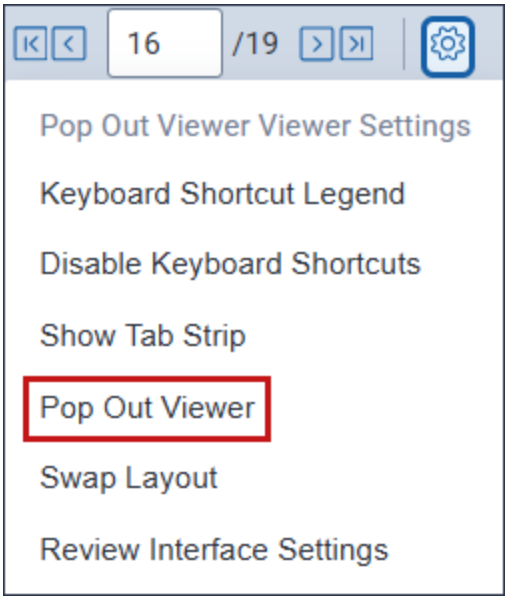
- **Keyboard Shortcut Legend**—select to open the Keyboard Shortcut Legend pop-up modal to view the current keyboard shortcuts available in the Viewer.
- **Enable/Disable Keyboard Shortcuts**—select to enable or disable the keyboard shortcuts feature while in the Viewer.
- **Show/Hide Tab Strip**—select to show or hide the sidebar and tab strip in the Native Viewer.
- **Pop Out Viewer**—select to open the Viewer in a new window in your browser. To learn more, visit Pop Out Viewer.
- **Swap Layout**—select to move the coding layout and the document card to the opposite side of the Viewer from where they are currently located.
- **Review Interface Settings**—Allows a third-party developer to temporarily enable or disable other extensions and settings in the Review Interface while they are developing their extension. This option only displays in the Viewer Settings menu if a user has the Document - Review Interface Settings permission. This permission is disabled by default for all users other than System Administrators.
  You can toggle instance settings, persistent highlighting, and extensions on or off for the current user to help troubleshoot problems. Settings that are edited only apply to the current user and do not impact settings across the instance. If you edit any of the options on this page, a message displays at the top of the Viewer indicating that the settings have been changed. You may need to refresh your browser for the changes to be reflected in the Viewer. Any changes made do not persist across user sessions and once you log out, the Viewer will return to the state prior to editing the Review Interface Settings.
  If you would like to return to the prior Viewer state, click **Reset Default Settings** at the bottom of the page to restore the settings back to their original values.

39.9 Pop Out Viewer

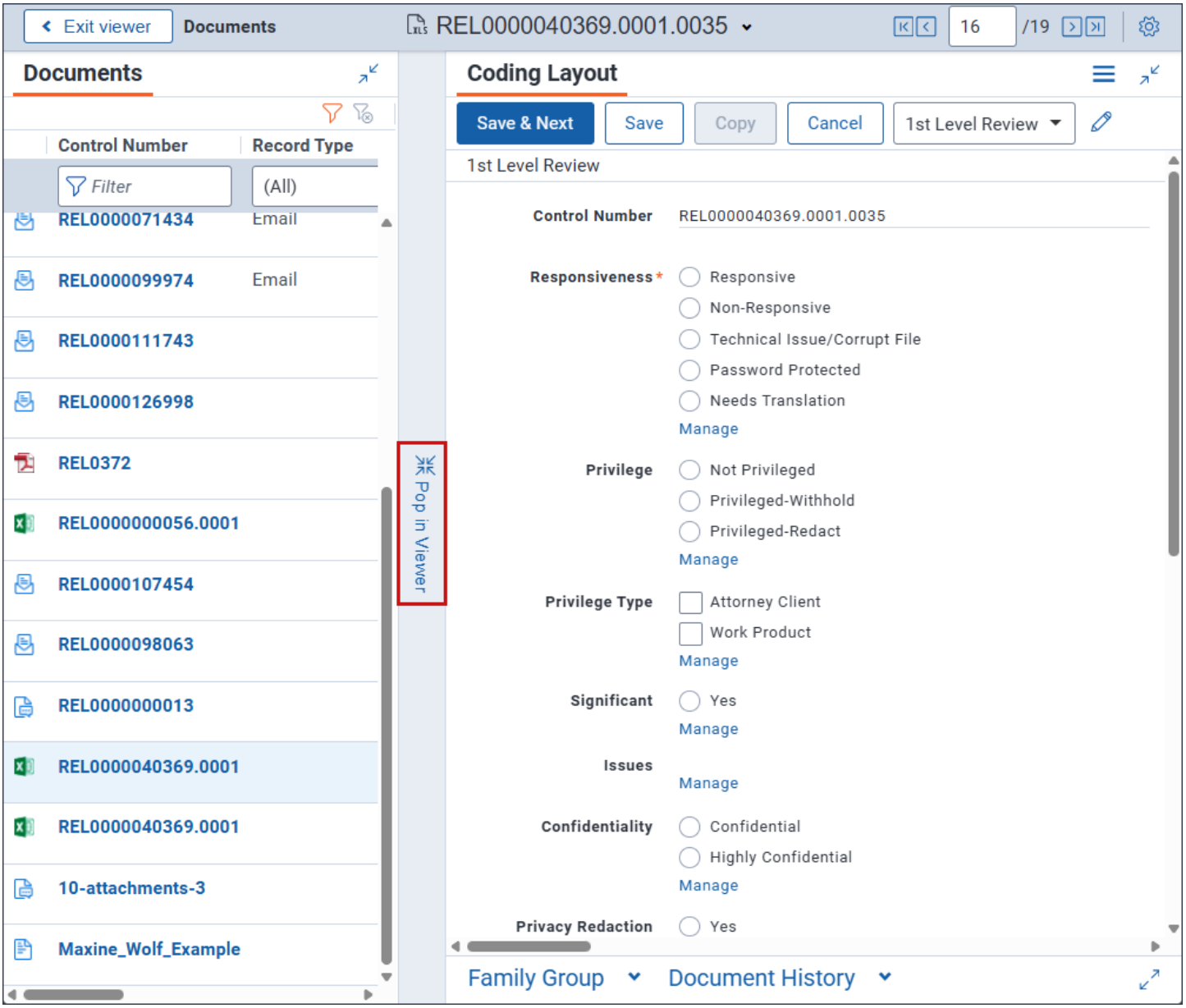
You can open the Viewer in a new window in your browser using the Pop Out Viewer. The Document card and the Coding card remain in the previously opened browser window. They can be expanded to a greater width to take advantage of the space freed up by the Pop Out Viewer. The Pop Out Viewer retains the same functionality as the Viewer. For example, you can switch Viewer types and view highlights or the Thumbnail Viewer as desired.



To open the Pop-Out Viewer in a new browser window, select the **Pop Out Viewer** option from the Viewer settings menu in the upper-right corner.



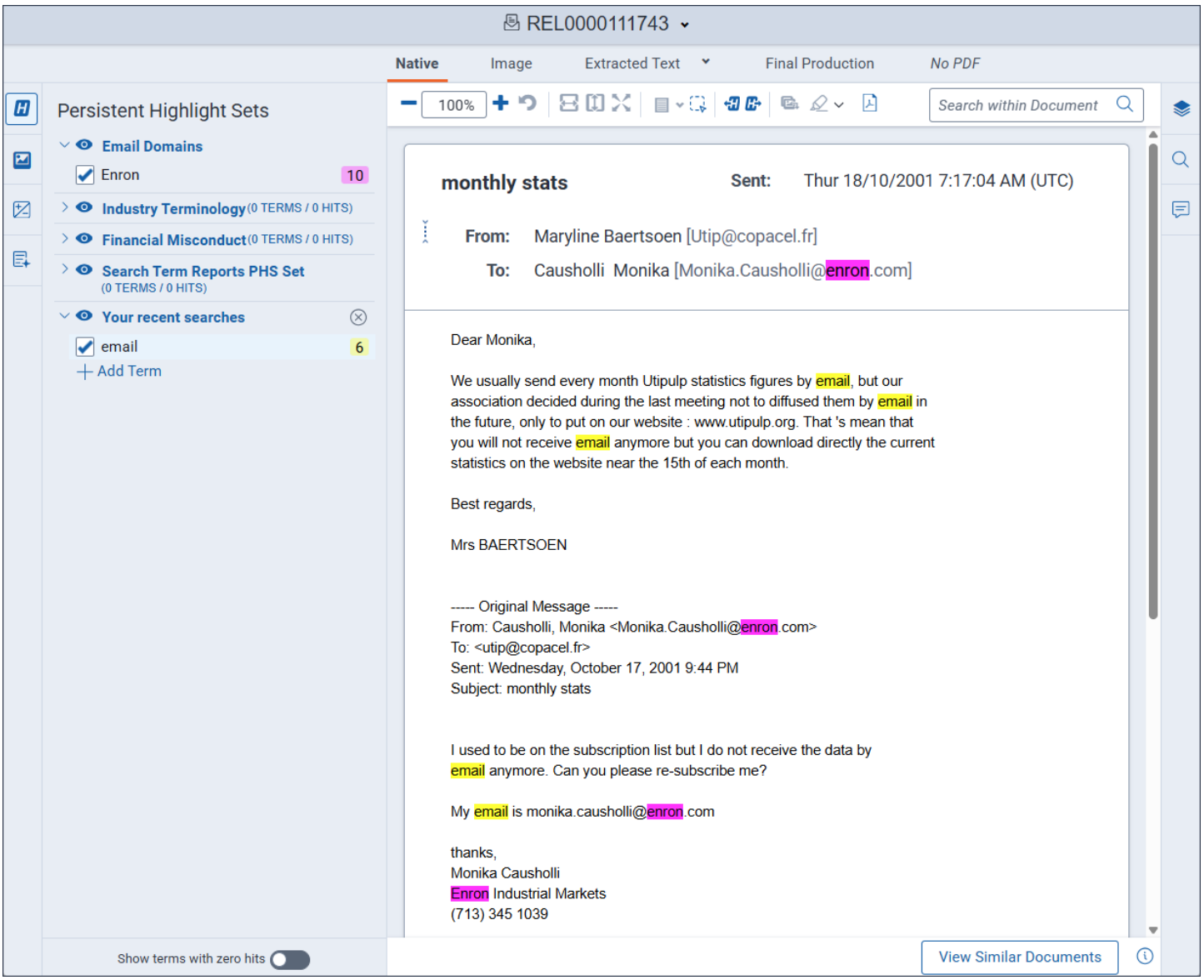
To return the Viewer to the previous browser window where the Document card and Coding card are located, you can click either the **Pop In Viewer** button on the previous browser window or you can select the **Pop In Viewer** option from the Viewer settings menu in the upper-right.



Alternatively, if you close the browser window that the popped out Viewer is in, the Viewer pops in to the Review Interface or in other words, returns to the original browser window.

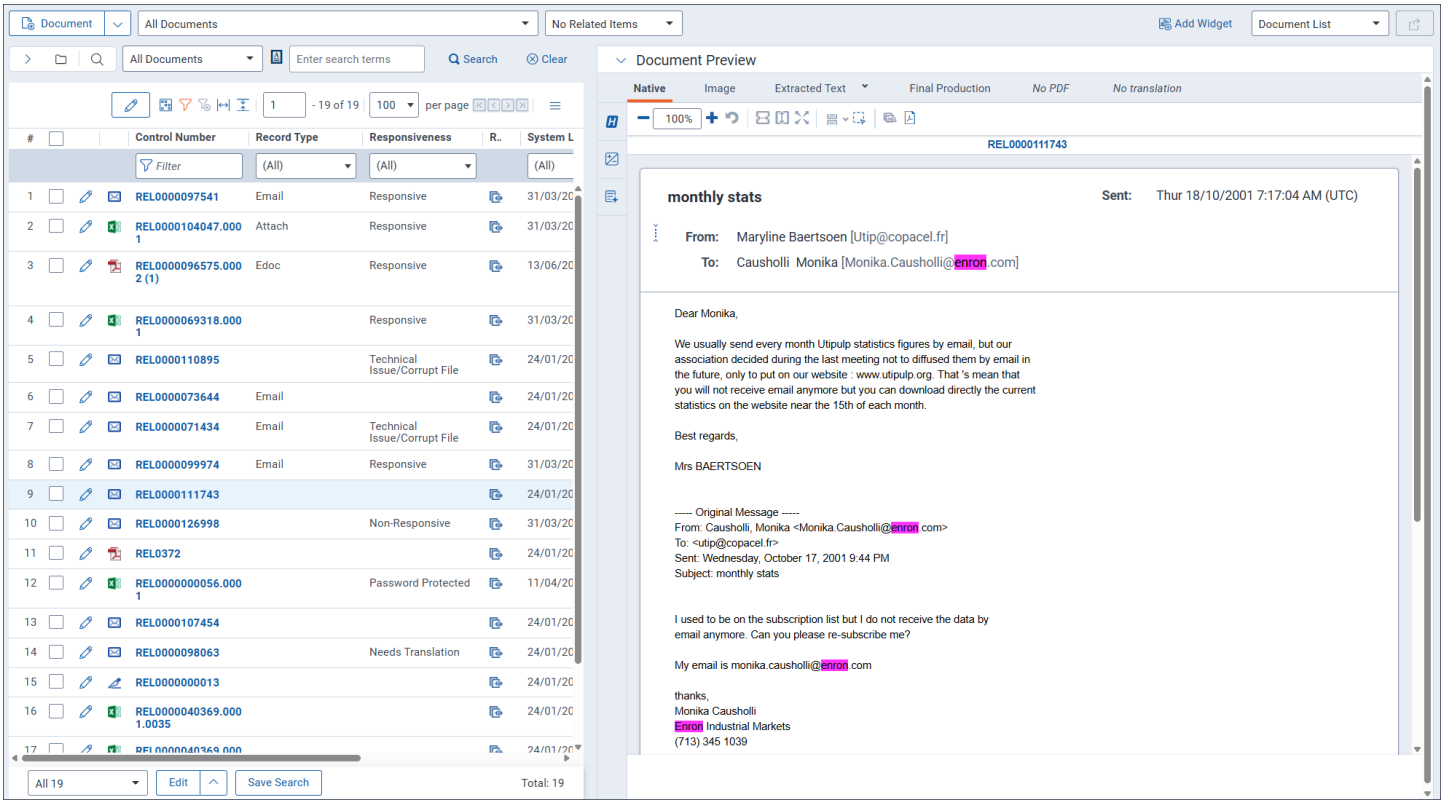
39.9.1 Standalone Viewer

To view a document in a separate browser window, click the file icon in the Document list or in the Viewer on the Documents card or Family card. Launching the Standalone Viewer from either the Documents and Family card launch the Review interface.



39.9.2 Document preview panel

The Document preview panel allows you to view documents in the document list before launching the Viewer. It also allows you to filter the list and quickly view documents in the results which makes the process of finding documents more efficient. To learn more, visit



39.10 Related items card

The related items card is located at the bottom-right corner of the Viewer. Related items are customizable groups of documents within a workspace. Common examples are family groups, duplicates, or similar documents.

The Edit field will be available in the Related items card if you add it to the Relational card view.

The related items toolbar includes the following:



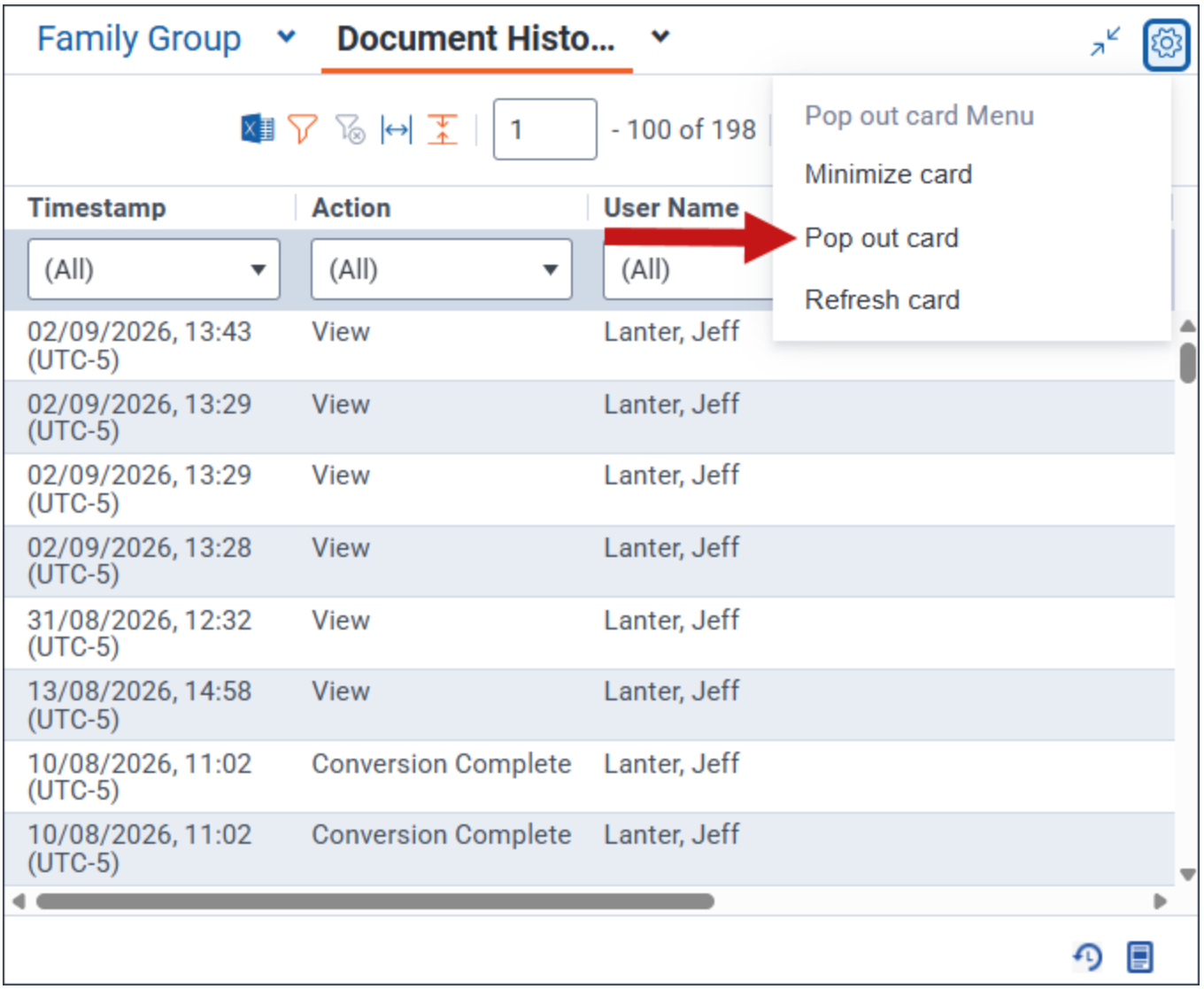
- **Related items** —displays a group of documents related to the active document. Options vary within the workspace. Hover over each icon to display the name of the item. Examples include: family group, duplicates, and thread group.
- **Document history** —displays a history of actions taken on the current document. You may not have access to document history. If you store your audits in Data Grid, this displays the field name, old value, and new value.

  Note: In the Document History card, you can click the **Details** link to display a pop-up with the audit history for the document. Click **Run Details** to display information about document imaging jobs, including the name of the imaging profile and the formatting options used during mass imaging or imaging on the fly.

- **Production** —displays all productions in which the document was included. You may not have permissions to view production information.
- **Linked** —displays all linked records on the active document.
- **Search results**—displays the results of an Analytics search.
- **Batch sets**—shows all the batch sets for the active record. See Batches on page 156. Batches in the Admin manual. You may not have permissions to view this section.

When a coding decision is made, the information in the Related Items card automatically refreshes. If there are two or more reviewers on the same document, a user can refresh this card by clicking on the Menu icon and selecting **Refresh card**.

The Related items card can be opened in a separate browser window. Click the Menu icon and select **Pop out card** to open the card in its own window. Click the Menu icon and select **Pop in card** to close the browser window and return the card to the Viewer.

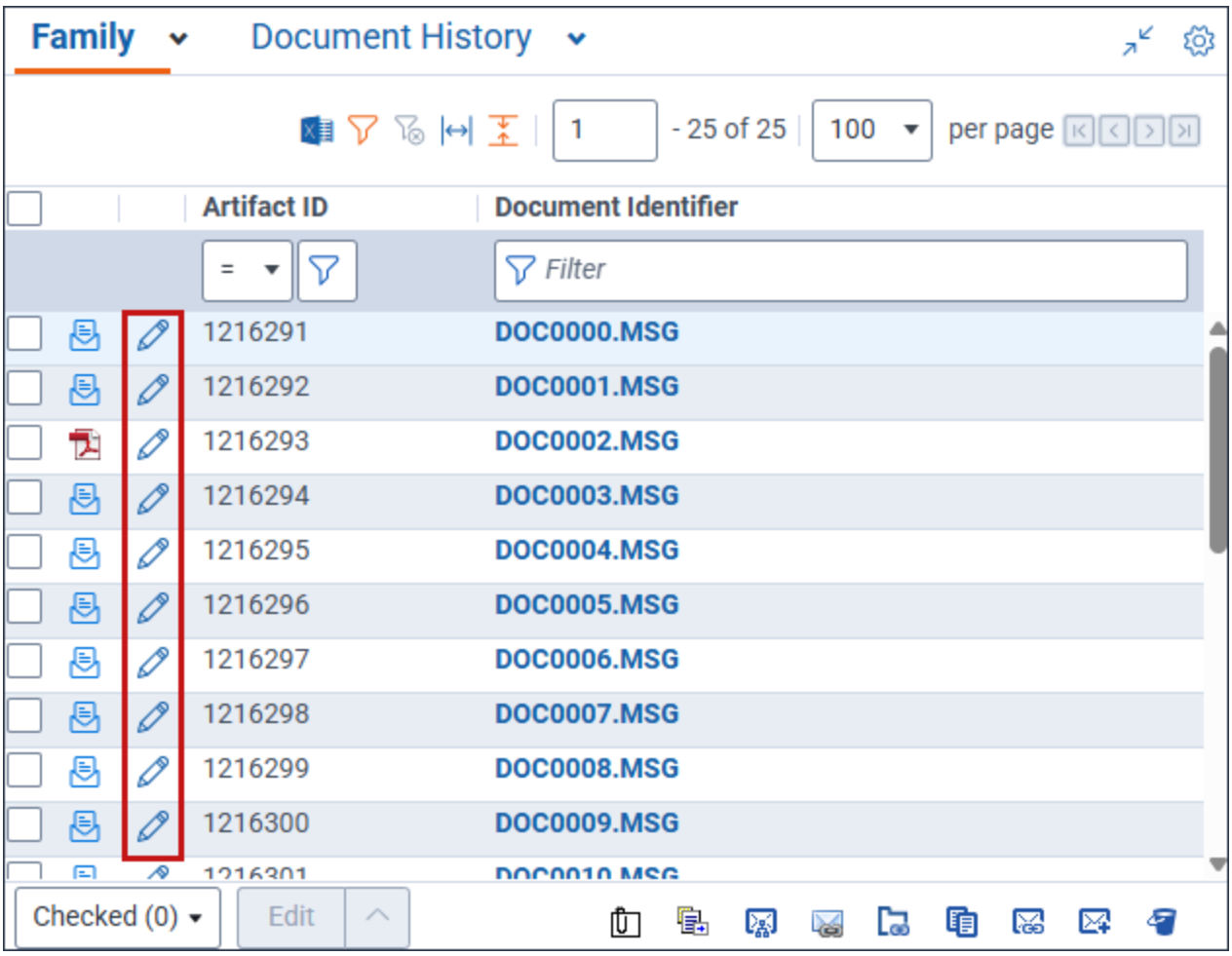


39.10.1 Document actions in the related items card

You can use the related items card to quickly identify documents related to the active document. You can also use this card to act on those groups of related items.

For instance, in the example of the Related items card below, you can select some or all of the documents in the Related items card and click **Edit**. This opens a window for you to access all of your active layouts – the same layouts available in the layouts pane. Using these layouts, you can make coding decisions and apply them to the selected documents using mass editing. Alternatively, you can mass PDF, Save as List, Image, or Tally/Sum/Average. To learn more, see Mass operations in the Admin guide.

If you add the Edit field to your relational card view, you can click the Edit icon in the row of a document and immediately open that document in the Viewer with the layout ready to be edited.



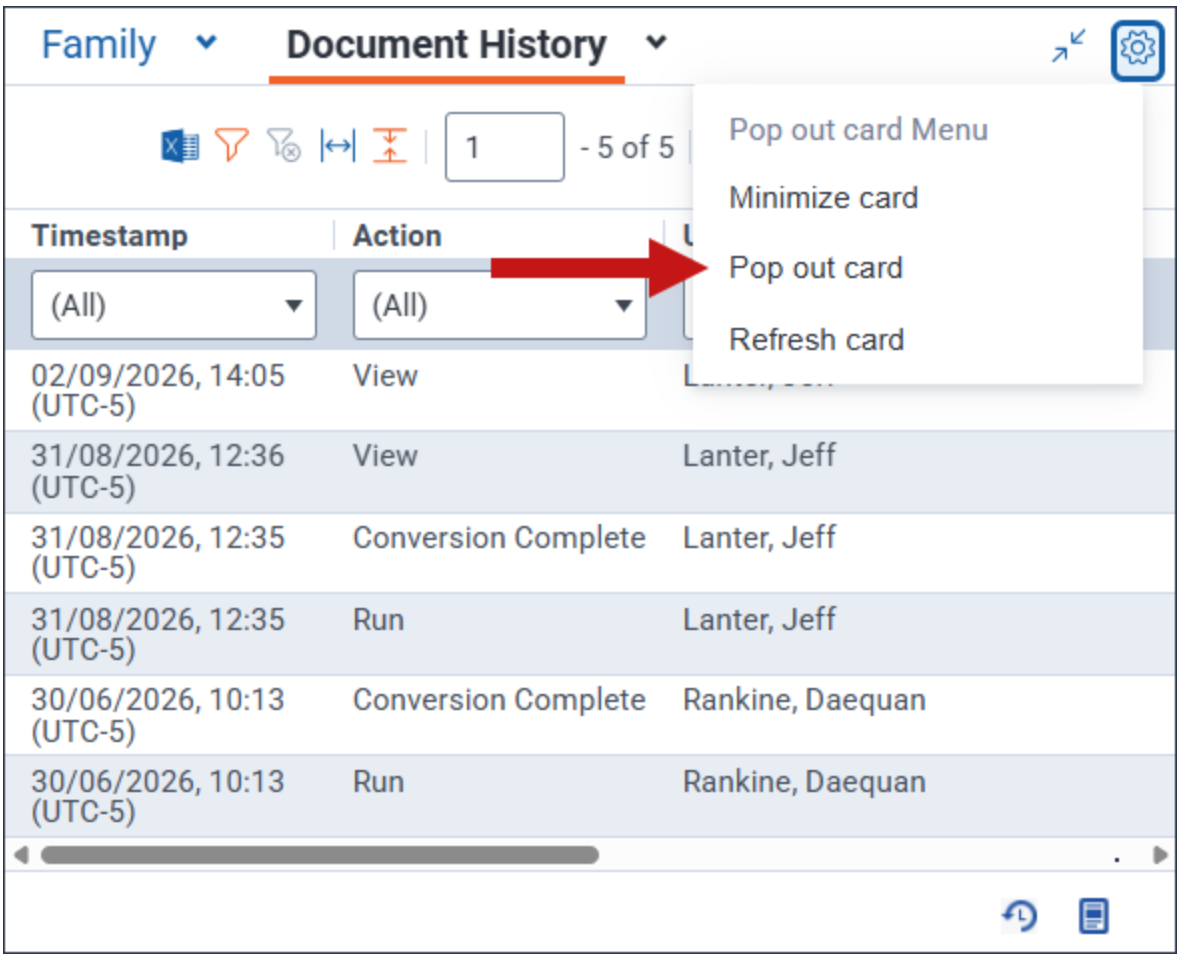
39.11 Document and Production History card

The Document History and Production History card is located in the bottom-right of the Viewer. This card displays either the document history or the production history, depending on which you have selected. The Document History card displays information about the most recent actions taken by users with the current document. The Production History card displays information on any productions that the current document was included in.

You can filter the columns to help find information or export the information in the Document History card to a .csv file.

You can refresh this card by clicking on the Menu icon and selecting **Refresh card**.

The Document History card can be opened in a separate browser window. Click the Menu icon and select **Pop out card** to open the card in its own window. Click the Menu icon and select **Pop in card** to close the browser window and return the card to the Viewer.



39.11.1 Document and Production History card permissions

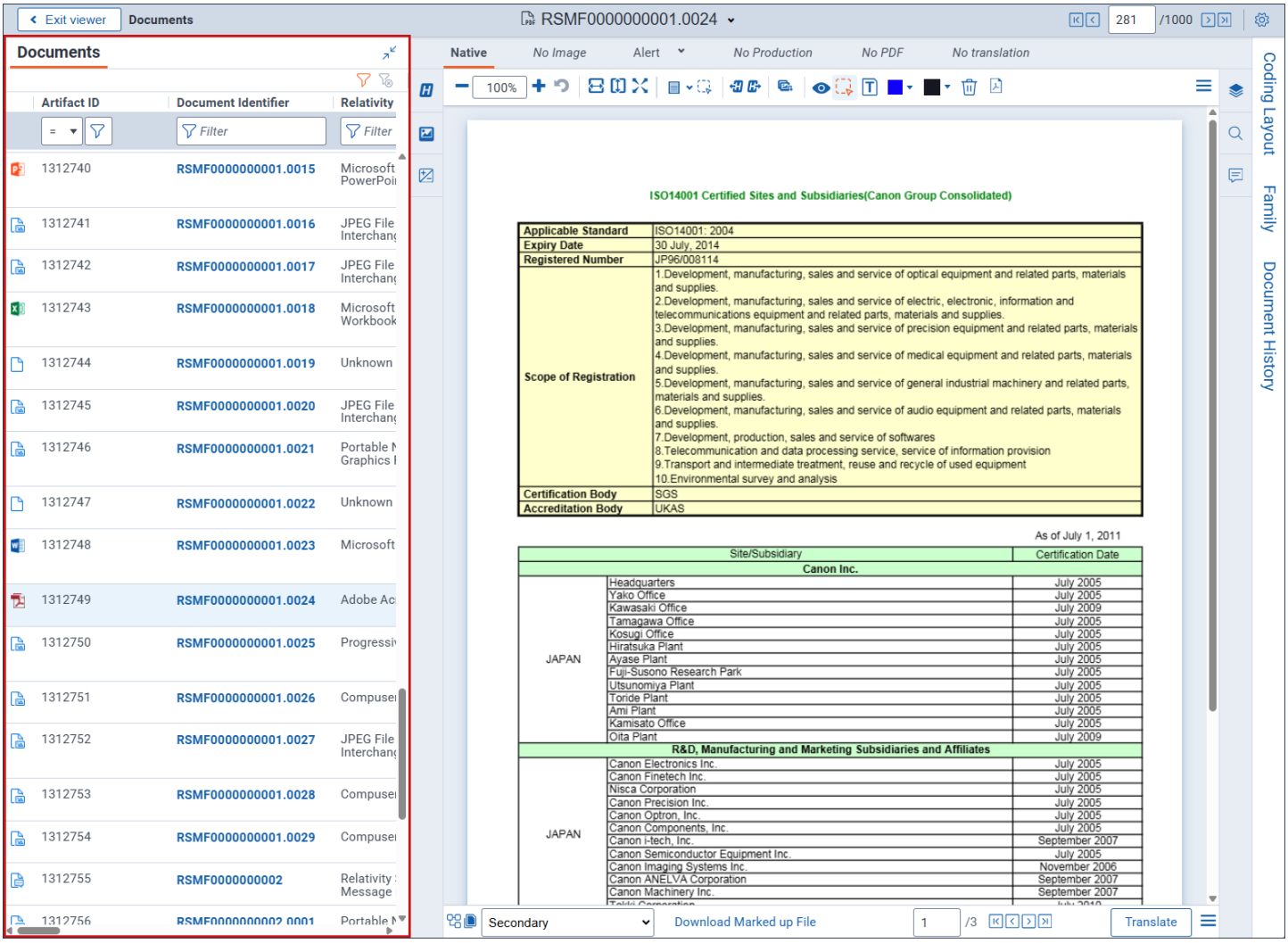
The following permissions are required to access Document and Production History:

Object Security	Tab Visibility	Admin Operations
• **Document** - View • **Production** - View		• View All Audits

39.12 Documents card

The Documents card contains the document list so you can conveniently navigate from document-to-document without having to leave the Viewer. The fields that display in the card are based on which view is selected in the document list. Each time that you save a coding decision in the Viewer, the Documents card refreshes to show the latest results. The highlighted document in the document list now updates when you navigate from document-to-document to make tracking even easier.

If you're using Review Center, the Documents card shows the documents in your current queue. For more information, see Reviewing documents using Review Center in the Review Center guide.



39.12.1 Email thread visualization tool

When you have installed and run an email threading structured analytics set for documents, you can use the email thread visualization tool. Launch the Email Thread Visualization pane, click the **email thread visualization** icon in the lower right corner of the displayed document in the Viewer. The email thread visualization pane expands and shows the thread group for the selected email in the Viewer.

Using this tool, you can visually examine email threads and how they are coded. You can also easily perform mass editing from this tool. See Email thread visualization in the Analytics guide for more information.

39.13 .eml and .msg header dates and times in the Viewer

.eml, .msg and RSMF documents have header dates and times in Coordinated Universal Time (UTC) format. The Relativity Native Time Zone Offset field determines how these date/time values are displayed in the Native Viewer, based on the desired time zone and its offset from UTC.

Note: Relativity does not automatically account for Daylight Savings Time. For documents processed in Relativity, DST rules are automatically taken into account when calculating the Relativity Native Time Zone Offset value. For all other documents, if you need the Viewer to account for Daylight Savings Time, deploy the Set Native Timezone Offset With DST script. You must be a Relativity admin to deploy this script.

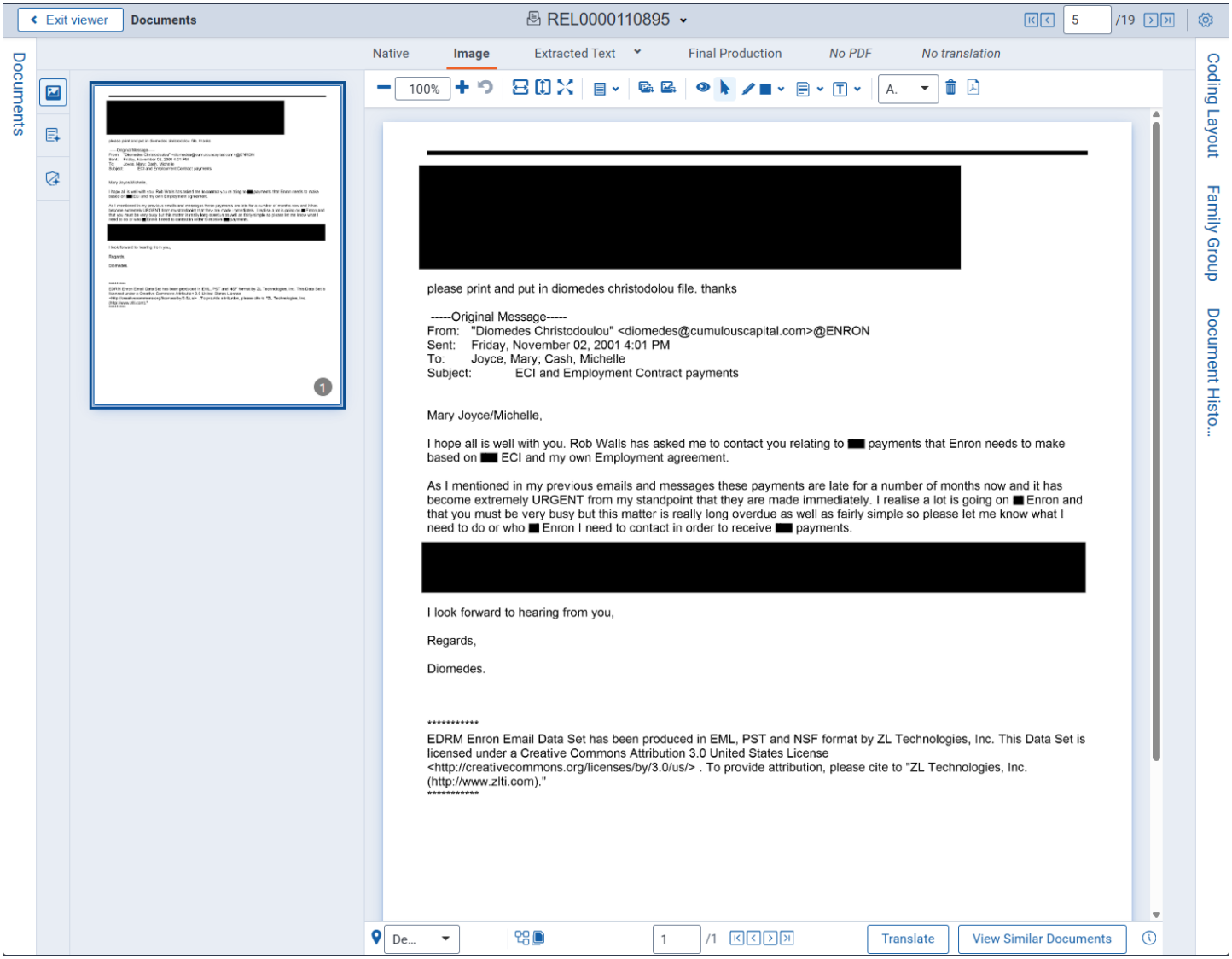
39.14 Thumbnail Viewer

When in the Native Viewer, Image Viewer, or Productions Viewer, you can access and browse thumbnail renderings of a document's pages. Quickly scan, locate, and navigate to pages in an open document.

To open the Thumbnail Viewer, click **Thumbnail** icon in the left drawer. The left drawer expands and displays the Thumbnail Viewer. Scroll up and down to navigate all pages in the open document and click a page to view it. As you scroll through the document, the thumbnail viewer scrolls simultaneously to keep the viewed pages in focus.

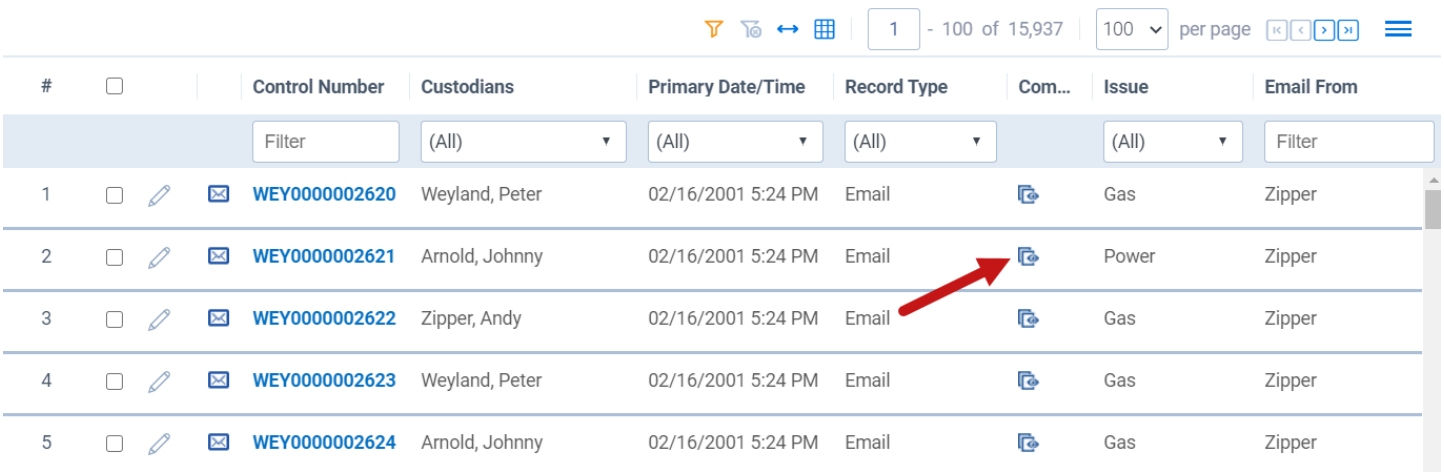
The Thumbnail Viewer is compatible with word processor, presentation, vector image, and raster image file types.

Note: The Thumbnail Viewer may not be available in the Native Viewer for document types that do not paginate such as spreadsheets or plain text.



39.15 Document Compare

You can use Document Compare to view the key differences between the extracted text of two documents. Unlike most fields, the Relativity Compare field is not visible on the Fields tab. To access Document Compare, you must first add the Relativity Compare system field to a view. See Views on page 702 Views in the Admin guide.

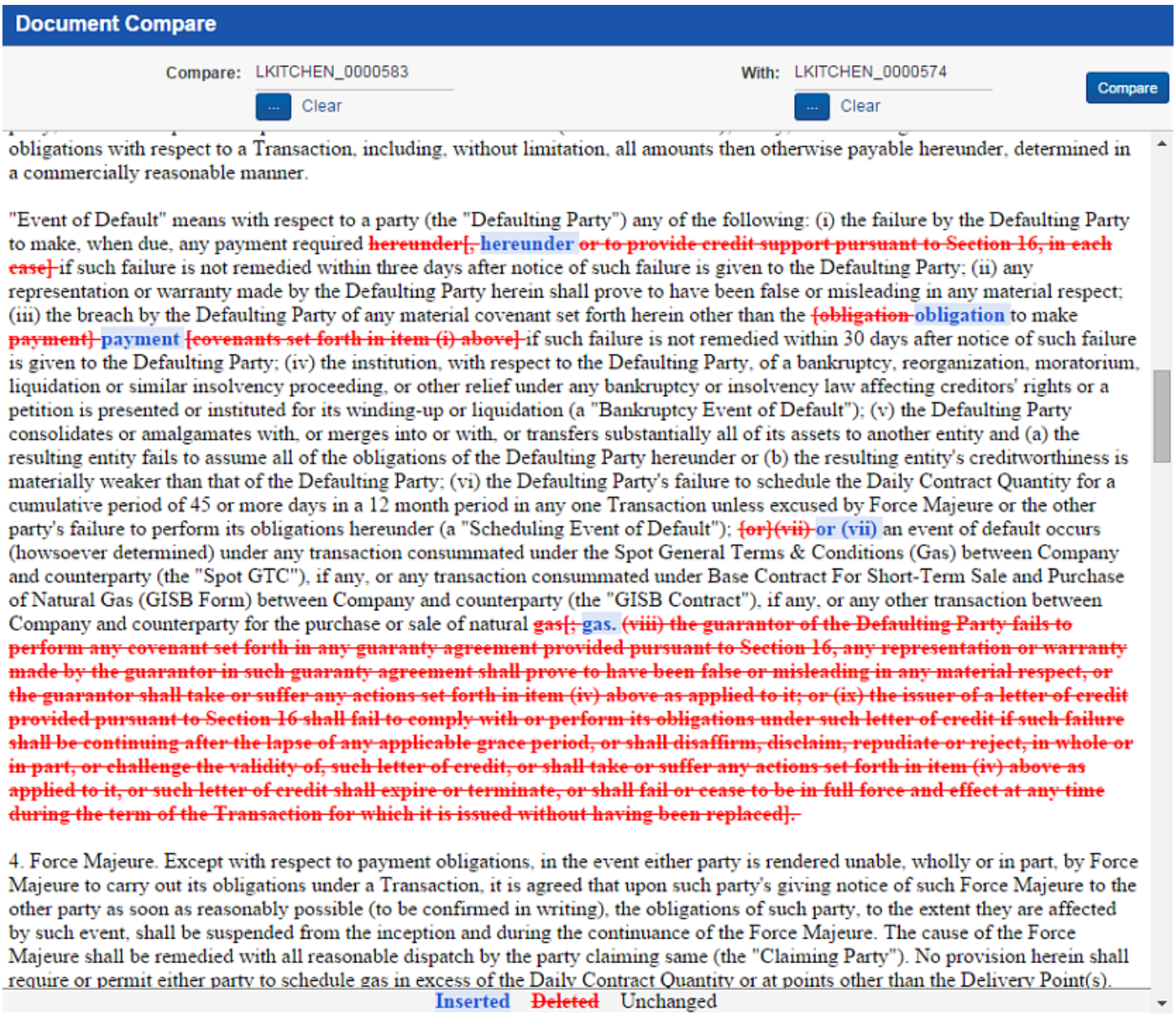


To compare two documents in Relativity from the document list:

1. Click on the **Compare** icon to open the Document Compare selection window. By default the document identifier of the selected document populates the Document Compare window.
2. Click on the **Select** button next to the With field to select a document with which to compare it. A Select Item pop-up window displays.

   Note: You can change the value of either of the fields at any time while in the Document Compare window.

3. Select the desired document from the list and click **Set**. The Document Compare window displays the selected document in the With field.
4. Click on **Compare**. The window displays the similarities and differences between the documents.
5. The similarities and differences between the documents are reflected in the legend at the bottom of the window:
   - **Inserted** - text appears in the "With" document but doesn't appear in the "Compare" document.
   - **Deleted** - text appears in the "Compare" document but doesn't appear in the "With" document.
   - **Unchanged** -text appears in both documents.



You can also compare related documents from within the Viewer. To compare related documents in the Viewer, open the Related Items pane and click on the **Compare** icon next to the document you want to compare. The Document Compare selection window opens. The document you select from the Related Items pane automatically populates in the With field, while the document open in the Viewer automatically populates the Compare field.

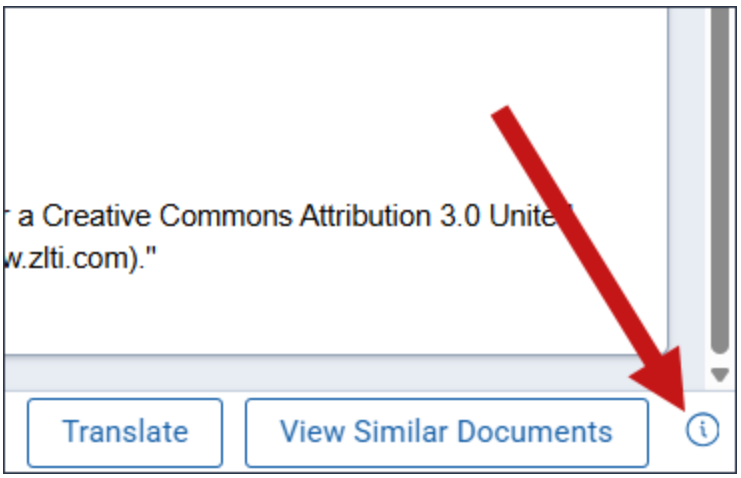
39.16 Viewer-supported file types

Relativity uses the Viewer to display rendered versions of native files. Reviewers can see how the file looked in its native application without opening the file in that native application.

When converting email file types such as EML, the Viewer will not download images from the internet. Any linked images will display as a gray box in the Viewer.

This document provides a comprehensive list of files types supported by the Viewer. Find out which Viewer version you have by navigating to your Viewer and clicking the **About Viewer** icon.

See the Admin guide for more information on the Viewer.



Note: Relativity does not support any third-party applications after the user downloads a file. This includes specific browser and media-player combinations, such as Internet Explorer and Windows Media Player.

Supported file types differ slightly in processing, imaging, and the viewer. See *Supported file types for imaging* and *Supported file types for processing* for details specific to those features.

39.16.1 Categories

Archive | Database, spreadsheets | Document, text, word processors | Email, messaging, chat | Graphics, images | Other

File type	File extension	File Type/Version and Notes
Archive	.7z	**Note:** BZIP2 and split archives are not supported.
7z Self Extracting exe	.exe	**Note:** BZIP2 and split archives are not supported.
LiveNote Evidence File	.lef	
LZA Self Extracting Compress	.lza	
LZH Compress	.lzh	
Microsoft Cabinet (CAB)	.cab	
Microsoft Office Binder	.obd	95, 97
PKZip	.zip	
RAR	.rar	1.5, 2.0, 2.9
TextMap Evidence File	.xmef	
UNIX Compress	.z	
UNIX GZip	.gz	
UNIX tar	.tar	
Uuencode	.uue	
Zip	.zip	PKZip, WinZip

File type	File extension	File Type/Version and Notes
File type	**File extension**	**Notes**
Database, spreadsheets		
Apache Office Calc (ODF 1.2)		3.x, 4.x
Apple iWork Numbers (MacOS, text, and PDF preview)	.numbers	09
Cellebrite Encrypted Excel Report File	.xlsx	
Cellebrite Excel Report File	.xlsx	
DataEase	.dba	4.x
DBase	.dbf	III, IV, V
Enable Spreadsheet		3.0 - 4.5
First Choice DB	.fol	Through 3.0
First Choice SS		Through 3.0
Framework DB		3.0
Framework SS		3.0
IBM Lotus Symphony Spreadsheets		1.x
Kingsoft WPS Spreadsheets		2010
Libre Office Calc (ODF 1.2)		3.x, 4.x
Lotus 1-2-3	.wk1, .wk3, .wk4, .wks	Through Millennium 9.8
Lotus 1-2-3 Charts (DOS and Windows)	.wk1, .wk3, .wk4, .wks	Through 5.0
Lotus 1-2-3 for OS/2		2.0
Microsoft Access	.accdb	2007/2010
Microsoft Excel Charts	.xlsx, .xls	2.x - 2007
Microsoft Excel for Macintosh	.xlsx, .xls	98 – 2011
Microsoft Excel for Windows	.xlsx, .xls	3.0 - 2016 **Note:** Excel files with slicers will convert and display normally in the Viewer, but slicer elements in those files will not display.
Microsoft Excel for Windows (.xlsb)	.xlsb	2007-2013 (Binary)
Microsoft Works DB for DOS	.wdb	2.0

File type	File extension	File Type/Version and Notes
Microsoft Works DB for DOS	.wdb	1.0
Microsoft Works DB for Macintosh	.wdb	2.0
Microsoft Works DB for Windows	.wdb	3.0, 4.0
Microsoft Works SS for DOS	.wks	2.0
Microsoft Works SS for Macintosh	.wks	2.0
Microsoft Works SS for Windows	.wks	3.0, 4.0
Multiplan	.sylk	4.0
Novell PerfectWorks Spreadsheet	.wpw	2.0
Office Calc (ODF 1.2)		4.x
OpenOffice Calc	.sdc	1.1-3.0
Oracle Open Office Calc	.sdc	3.x
Paradox for DOS	.db	2.0 - 4.0
Paradox for Windows	.db	1.0
PFS: Plan		1.0
Q&A Database	.db	Through 2.0
Quattro Pro Win	.qpw	X7
QuattroPro for DOS	.wb1	Through 5.0
QuattroPro for Windows	.qpw, .wb3, .wb2, .wb1	Through X5
R:Base	.rb1, .rb2, .rb3	R:Base 5000, R:Base System V
Reflex	.rdx	2
SmartWare II DB	.db	1.02
SmartWare II SS	.def	1.02
SmartWare Spreadsheet	.def	
StarOffice Calc	.sdc	5.2 – 9.0
SuperCalc	.cal	5.0
Symphony	.wrk	Through 2.0
VP-Planner		1.0

File type	File extension	Notes
Adobe FrameMaker (MIF	.mif	3.0 - 6.0

Document, text, word processors

File type	File extension	File Type/Version and Notes
only)		
Adobe Illustrator Postscript	.eps	Level 2
Ami		
Ami Pro for OS2	.sam	
Ami Pro for Windows	.sam	2.0, 3.0
Apache Office Writer (ODF 1.2)		3.x, 4.x
Apple iWork Pages (MacOS, text and PDF pre-view)	.pages	09
ANSI Text	.ans	7 & 8 bit
ASCII Text	.asc	7 & 8 bit
DEC DX	.dx	Through 4.0
DEC DX Plus	.dx, .wpl	4.0, 4.1
DOS character set		
EBCDIC		
Enable Word Processor		3.0 - 4.5
First Choice WP	.pfx	1.0, 3.0
Framework WP		3.0
Hangul	.hwp	97 - 2010
HTML (CSS rendering not supported)	.html	1.0 – 4.0
IBM DCA/RFT		
IBM DCA/FFT	.dca, .fft	
IBM DisplayWrite	.rft, .dca	2.0-5.0
IBM Writing Assistant	.iwa	1.01
Ichitaro	.jtd	5.0, 6.0, 8.0 - 13.x, 2004 - 2014
JustWrite	.jw	Through 3.0
Kingsoft WPS Writer	.wps	2010
Legacy	.leg	1.1
Libre Office Writer (ODF 1.2)		3.x, 4.x
Lotus Manuscript	.manu	Through 2.0
Macintosh character set		
MacWrite II	.mcw	1.1

File type	File extension	File Type/Version and Notes
Mail Rule DXL		
Mass 11	.m11	Through 8.0
Microsoft Word for DOS	.doc	4.0 – 6.0
Microsoft Word for Macintosh	.doc	4.0-6.0, 98 - 2016
Microsoft Word for Windows	.doc, .docx	1.0 – 2016
Microsoft WordPad	.rtf	
Microsoft Works WP for DOS	.wps	2.0
Microsoft Works WP for Macintosh	.wps	2.0
Microsoft Works WP for Windows	.wps	3.0, 4.0
Microsoft Write for Windows	.wri	1.0 – 3.0
MultiMate	.dox	Through 4.0
MultiMate Advantage	.dox	2
Navy DIF	.dif	
Nota Bene	.nb	3.0
Novell PerfectWorks Word Processor	.wpw	2.0
OfficeWriter		4.0-6.0
OpenOffice Writer	.sdw	1.1 - 3.0
Oracle Open Office Writer	.sdw	3.x
PC File Doc		5.0
PFS: Write	.pfs	A, B
Professional Write for DOS		1.0, 2.0
Professional Write Plus for Windows		1.0
Q&A Write	.jw	2.0, 3.0
Rich Text Format (RTF)	.rtf	
Samna Word IV	.sam	1.0 – 3.0
Samna Word IV+	.sam	
Signature		1.0
SmartWare II WP	.def	1.02

File type	File extension	File Type/Version and Notes
Sprint	.spr	1.0
StarOffice Writer	.sdw	5.2 – 9.0
Total Word		1.2
UTF-8		
Unicode Text	.txt	3.0, 4.0
Wang IWP	.iwp	Through 2.6
Wireless Markup Language	.wml	
WordMarc Composer		
WordMarc Composer+		
WordMarc Word Processor		
WordPerfect for DOS	.wpd	4.2
WordPerfect for Macintosh	.wpd	1.02 - 3.1
WordPerfect for Windows	.wpd	5.1 – X5
Wordstar 2000 for DOS	.wsd	1.0 - 3.0
Wordstar for DOS	(none defined)	3.0 - 7.0
Wordstar for Windows	.ws1	1.0
XyWrite	.xy	Through III+

File type	File extension	Notes
Apple Mail Message (EMLX)	.emlx	2
EML with Digital Signature	.eml	SMIME **Note:** EML files that have a password or are encrypted are not supported in the Viewer. These documents will display the attachment but the body will appear blank.
Encoded mail messages		MHT Multi Part Alternative Multi Part Digest Multi Part Mixed Multi Part News Group Multi Part Signed TNEF
IBM Lotus Notes Domino XML Language DXL	.xml	8.5
IBM Lotus Notes NSF (Win32, Win64, Linux x86-32 and Oracle Solaris 32-bit only with Notes Client or	.nsf. .ntf	8.x

Email, messaging, chat

File type	File extension	File Type/Version and Notes
Domino Server)		
MBOXMailbox	.mbox	RFC 822 **Note:** An MBOX file is characterized as a text file with the string "From<space>email address<space>date string". When a file of this nature is viewed in Relativity, it may appear to only show summaries of messages. Essentially, if that "from" line is at the top of the document, Relativity treats it as MBOX and displays it as an archive.
Microsoft Outlook (MSG)	.msg	97 - 2013
Microsoft Outlook (OST)	.ost	97 - 2010, 2013
Microsoft Outlook (PST)	.pst	97 - 2013
Microsoft Outlook Express (EML)	.eml	
Microsoft Outlook Forms Template (OFT)	.oft	97 - 2013
Microsoft Outlook OLM for Mac		2011
Microsoft Outlook PST (Mac)	.pst	2001
MSG with Digital Signature	.msg	SMIME **Note:** MSG files that have a password or are encrypted are not supported in the Viewer. If you open an .MSG file that is encrypted in the Viewer, the body of the document will be blank and the contents of the encrypted data is placed into a single attachment with a .p7m file extension.

File type	File extension	Notes
Graphics, images		
Adobe Illustrator XMP		11 – 13 (CS 1 - 5)
Adobe InDesign Interchange XMP only		
Adobe InDesign XMP		3.0 – 5.0 (CS 1 - 5)
Adobe PDF	.pdf	1.0 – 1.7 (Acrobat 1 - 10)
Adobe PDF Package	.pdf	1.7 (Acrobat 8 - 10)
Adobe PDF Portfolio	.pdf	1.7 (Acrobat 8 - 10)

File type	File extension	File Type/Version and Notes
Adobe Photoshop	.psd	4
Adobe Photoshop XMPonly		8.0 - 10.0 (CS 1-5)
Ami Draw	.sdw	SDW
Apple iWork Keynote File Preview	.key, .keynote	09
Apple iWork Keynote Numbers File Preview	.numbers	09
Apple iWork Pages File Preview	.pages	09
AutoCAD Drawing	.dwg	2013
AutoCAD Drawing	.dwg	2.5, 2.6, 9.0-14.0, 2000i -2012
AutoShade Rendering	.rnd	2
CALS Raster (GP4)	.cg4, .cal	Type I-II
Computer Graphics Metafile	.cgm	ANSI, CALS, NIST
Corel Draw	.cdr	X4 - X7
Corel Draw Clipart	.cmx	5.0, 7.0
Encapsulated PostScript (EPS)	.eps	TIFF Header only
Enhanced Metafile (EMF)	.emf	
Escher Graphics	.egr	
FrameMaker Graphics (FMV)	.fmv	3.0 – 5.0
Gem File (Vector)	.img	
GEM Image (Bitmap)	.bmp	
Graphics Interchange Format (GIF) **Note:** Relativity fully supports .gif files and you can now view a .gif's entire sequence in the Viewer.	.gif	
Harvard Graphics	.cht	98
Harvard Graphics Chart DOS	.ch3	2.0 – 3.0
Harvard Graphics for Windows	.prs	
HEIC Image file	.heic	

File type	File extension	File Type/Version and Notes
Note: HEIC rendering is not currently supported in the Viewer, as HEIC files are natively supported only in Safari and not in Chrome, Firefox, or Edge.		
HP Graphics Language	.hp, .hpg	2.0
IBM Graphics Data Format (GDF)	.gdf	1.0
IBM Picture Interchange Format	.pif	1.0
IGES Drawing	.iges	5.1 – 5.3
JBIG2		Graphic Embeddings in PDF
JFIF (JPEG not in TIFF format)	.jfif	
JPEG	.jpg	
JPEG 2000		JP2
Kodak Flash Pix	.fpx	
Kodak Photo CD	.pcd	1.0
Lotus PIC	.pic	
Lotus Snapshot		
Macintosh PICT	.bmp	BMP only
Macintosh PICT2	.bmp	BMP only
MacPaint	.pntg	
Micrografx Designer	.dsf	Version 6
Micrografx Designer	.drw	Through 3.1
Micrografx Draw	.drw	Through 4.0
Microsoft Visio: Stencil Template Macro Enabled Drawing Macro Enabled Stencil Macro Enabled Template	.vsd	5.0 – 2007, 2013
Microsoft Windows Bitmap	.bmp	
Microsoft Windows Cursor		
Microsoft Windows Icon	.ico	
Novell PerfectWorks Draw		2.0

File type	File extension	File Type/Version and Notes
OpenOffice Draw	.sda	1.1 – 3.0
Oracle Open Office Draw	.sda	3.x
OS/2 Bitmap		
OS/2 Warp Bitmap		
Paint Shop Pro (Win32 only)	.psp	5.0, 6.0
PC Paintbrush (PCX)	.pcx	
PC Paintbrush DCX (multi-page PCX)	.dcx	
Portable Bitmap (PBM)	.pbm	
Portable Graymap PGM	.pgm	
Portable Network Graphics (PNG)	.png	
Portable Pixmap (PPM)	.ppm	
Progressive JPEG	.jpg, .jpeg, .jpe	
StarOffice Draw		6.x - 9.0
Sun Raster	.srs	
SVG (processed as XML, not rendered)	.xml	
TIFF	.tif, .tiff	Group 5 & 6
TIFF CCITT		Group 3 & 4
TruVision TGA (Targa)	.tga	2.0
Visio (Page Preview mode WMF/EMF)	.wmf, .emf	4.0
WBMP wireless graphics format		
WebP		**Note:** WebP files are only available in the Native Viewer.
Windows Metafile	.vmf	
Word Perfect Graphics	.wpg	1.0
WordPerfect Graphics	.wpg, .wpg2	2.0 – 10.0
X-Windows Bitmap	.xbm	x10 compatible
X-Windows Dump	.xdm	x10 compatible
X-Windows Pixmap	.xpm	x10 compatible
File type	**File extension**	**Notes**

File type	File extension	File Type/Version and Notes
Apache Office Draw (ODF 1.2)		3.x, 4.x
Apache Office Impress (ODF 1.2)		3.x, 4.x
Apple iWork Keynote (MacOS, text and PDF-preview)	.key, .keynote	09
Harvard Graphics Presentation DOS	.prs	03
IBM Lotus Symphony Presentations		1.x
Kingsoft WPS Presentation		2010
Libre Office Draw (ODF 1.2)		3.x, 4.x
Libre Office Impress (ODF 1.2)		3.x, 4.x
Lotus Freelance	.prz	1.0 - Millennium 9.8
Lotus Freelance for OS/3		2
Lotus Freelance for Windows		95, 97, SmartSuite 9.8
Microsoft Live Messenger (via XMLfilter)		10.0
Microsoft OneNote	.one	2007, 2010, 2013
Microsoft Outlook, Google Calendar, and Apple Calendar	.ics	
Microsoft PowerPoint 2016	.pptx	2016 **Note:** PPTX files that have Ink drawings are supported in the Native and Image Viewer.
Microsoft PowerPoint for Macintosh	.ppt	4.0 - 2011
Microsoft PowerPoint for Windows	.ppt	3.0 – 2013
Microsoft PowerPoint for Windows Slideshow	.ppt	2007-2013
Microsoft PowerPoint for Windows Template	.pot	2007-2013
Microsoft Project (sheet view only, Gantt Chart, Net-	.mpp	98-2013

File type	File extension	File Type/Version and Notes
work Diagram, and graph not supported)		
Microsoft Project (sheet view only, Gantt Chart, Network Diagram, and graph not supported)	.mpp	2007, 2010, 2013
Microsoft Windows DLL	.dll	
Microsoft Windows Executable	.dll	
Novell Presentations	.shw	3.0, 7.0
OpenOffice Impress	.sdd	1.1, 3.0
Oracle Open Office Impress	.odp	3.x
StarOffice Impress	.sda, .sdd	5.2 - 9.0
Trillian Text Log File (via text filter)	.txt	4.2
vCalendar	.vcs	2.1
vCard	.vcf	2.1
WordPerfect Presentations		5.1 - X5
Yahoo! Messenger	.yps	6.x – 8

Note: Program/file types listed with text only or PDF preview only can be reviewed in the Viewer as listed. If PDF preview only, a PDF file saved as part of the native will be viewed. Text only will just display the text without any formatting.

39.16.2 Viewer audio and video-supported file types

Relativity can stream audio and video files within the Viewer.

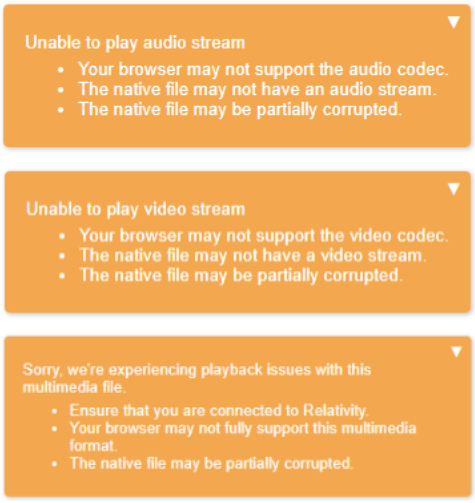
This document provides a comprehensive list of files types supported by the Viewer. Certain file types may not be compatible with your internet browser, refer to the sections below to learn more about browser compatibility. Find out which Viewer version you have, by navigating to your Viewer and clicking .

See the Admin guide for more information on the Viewer.

Note: Relativity does not support any third-party applications after the user downloads a file. This includes specific browser and media-player combinations, such as Internet Explorer and Windows Media Player.

39.16.3 Troubleshooting errors

If an audio or video file cannot be streamed in the Viewer, one of the following messages will display:



To resolve the error, ensure that your internet browser can play the selected file type. If that does not resolve the error, check the **MaximumNativeSizeForViewerForMediaFilesinMegaBytes** instance setting to ensure that the file type is not too big for the Viewer to stream.

39.16.4 Supported audio file types

Note: Safari works with Mac OSX only.

File Format	Container - Audio Codec	Chrome	Edge	Firefox	Safari
FI_RIFFWAVE	wave - pcm	✓	✓	✓	
Quicktime Movie	mov - aac	✓	✓	✓	✓
Quicktime Movie	mov - vorbis	✓	✓		
MPEG Layer3 ID3 Ver 1.x	mp3 - mp3	✓	✓	✓	
MPEG Layer3 ID3 Ver 2.x	mp3 - mp3	✓	✓	✓	✓
FI_MPGAV2L3	mp3 - mp3	✓	✓	✓	
MPEG-4 file	mp4 - aac	✓	✓	✓	✓
MPEG-4 file	mp4 - opus	✓	✓		
MPEG-4 file	mp4 - vorbis	✓	✓		
MPEG-1 audio - Layer 3	mov - mp3	✓	✓	✓	✓
MPEG-1 audio - Layer 2	mp4 - mp2	✓	✓	✓	
MPEG-1 audio - Layer 3	mp4 - mp3	✓	✓	✓	
Ogg Opus	ogg - opus	✓	✓	✓	
Ogg Vorbis	ogg - vorbis	✓	✓	✓	

39.16.5 Supported video file types

Note: Safari works with Mac OSX only.

File Format	Container - Video Codec - Audio Codec	Chrome	Edge	Firefox	Safari
Quicktime Movie	mov - h264 - aac	✓	✓	✓	
Quicktime Movie	mov - h264 - dolby_digital	✓	✓	✓	
Quicktime Movie	mov - h264 - mp2	✓	✓	Video-only	
Quicktime Movie	mov - h264 - mp3	✓	✓	✓	✓
Quicktime Movie	mov - h264 - vorbis	✓	✓	✓	
Quicktime Movie	mov - h264 - wma1	✓	✓	✓	
Quicktime Movie	mov - h264 - wma2	✓	✓	✓	
Quicktime Movie	mov - mpeg4 - aac	Audio-only	Audio-only	Audio-only	✓
Quicktime Movie	mov - mpeg4 - mp3	Audio-only	Audio-only	Audio-only	
Quicktime Movie	mov - mpeg4 - vorbis	Audio-only	Audio-only		✓
Quicktime Movie	mov - theora - aac	✓	✓	Audio-only	
Quicktime Movie	mov - theora - dolby_digital	✓	✓		
Quicktime Movie	mov - theora - mp2	✓	✓		
Quicktime Movie	mov - theora - mp3	✓	✓	Audio-only	
Quicktime Movie	mov - theora - vorbis	✓	✓		
Quicktime Movie	mov - theora - wma1	✓	✓		
Quicktime Movie	mov - theora - wma2	✓	✓		
MPEG-4 file	mp4 - h264 - aac	✓	✓	✓	
MPEG-4 file	mp4 - h264 - dolby_digital	✓	✓	✓	✓
MPEG-4 file	mp4 - h264 - mp2	✓	✓	✓	✓
MPEG-4 file	mp4 - h264 - mp3	✓	✓	✓	✓
MPEG-4 file	mp4 - h264 - opus	✓	✓		✓
MPEG-4 file	mp4 - h264 - vorbis	✓	✓	✓	✓
MPEG-4 file	mp4 - mpeg4 - aac	Audio-only	Audio-only		✓
MPEG-4 file	mp4 - mpeg4 - mp2	Audio-only	Audio-only	Audio-only	✓
MPEG-4 file	mp4 - mpeg4 - mp3	Audio-only	Audio-	Audio-	✓

File Format	Container - Video Codec - Audio Codec	Chrome	Edge	Firefox	Safari
			only	only	
MPEG-4 file	mp4 - mpeg4 - opus	Audio-only	Audio-only		✓
MPEG-4 file	mp4 - mpeg4 - vorbis	Audio-only	Audio-only		✓
MPEG-4 file	mp4 - vp9 - aac	✓	✓	✓	
MPEG-4 file	mp4 - vp9 - dolby_digital	Audio-only	Audio-only	Audio-only	
MPEG-4 file	mp4 - vp9 - mp2	✓	✓	✓	
MPEG-4 file	mp4 - vp9 - mp3	✓	✓	✓	
MPEG-4 file	mp4 - vp9 - opus	✓	✓		
MPEG-4 file	mp4 - vp9 - vorbis	✓	✓	✓	
Ogg Theora Opus	ogg – theora - opus	✓	✓	✓	
Ogg Theora Vorbis	ogg – theora - vorbis	✓	✓	✓	
Ogg VP8 Opus	ogg – vp8- opus	✓	✓	Audio-only	
Ogg VP8 Vorbis	ogg – vp8 - vorbis	✓	✓	Audio-only	

39.16.6 Text-only designation

Some file types have a "text only" designation. When viewing these files in the Native Viewer, the document's text is the only data that renders. For Microsoft Project files and XML files, the view doesn't display items such as Gantt charts, icons, or other graphics. There is typically no formatting (bold, italics, fonts, etc.) of the text.

File Type	File extension	Notes
Database and spreadsheet		
Microsoft Access	.accdb, .mdb	1.0, 2.0, 95 - 2010
Microsoft Excel for Windows	.xml	2003 XML
Document and text		
XML	.xml	
Graphics, images, and computer-aided design		
Microsoft XPS		
Visio		2013
Multimedia		
Flash	.swf	6.x, 7.x, Lite
Word processors		

File Type	File extension	Notes
Lotus WordPro	.lwp, .mwp	9.7, 96 - Millennium 9.8
Microsoft Word for Windows		2003 XML

39.16.7 File ID only designation

Some file types have a "file ID only" designation. The Viewer is able to identify the file ID correctly, but it returns an error message indicating that the file format is not supported. Despite returning an error message, the Viewer identifies the file so that you can easily locate it and open it in an alternate application.

File type	File extension	Notes
Database and spreadsheet		
Microsoft Access Report Snap-shot		2000-2003
Strict Open XML - Spreadsheet		2013, 2016
Document and text		
XHTML		1.0
Email, messaging, chat		
IBM Lotus Notes NSF		7.x, 8.x
Graphics, images, and computer-aided design		
Adobe Photoshop PSD		
Visio XML VSX		2007
WebP		
Multimedia		
DICOM		
Flash		9, 10
Real Media		
MPEG-1 Video V 2	.mpg	
MPEG-1 Video V 3	.mpg	
MPEG-2 Audio	.mpg	
Windows Media Playlist		
Other		
AOL Messenger		
Microsoft InfoPath		2007
Microsoft Office Theme files		2007-2013
Microsoft Windows Compiled Help	.chm	
Microsoft Windows Explorer	.scf	

File type	File extension	Notes
Command		
Microsoft Windows Help	.hlp	
Microsoft Windows Shortcut	.ink	
Strict Open XML - Presentation **Note:** Relativity does not support the password protected version for these three Strict Open XML file formats.		2013, 2016
Trillian XML Log File		4.2
TrueType Font	.ttf, .ttc	
Word processors		
Microsoft Publisher		2003-2007
Samsung JungUm Global		
Strict Open XML - Document		2013, 2016

40 Workspaces

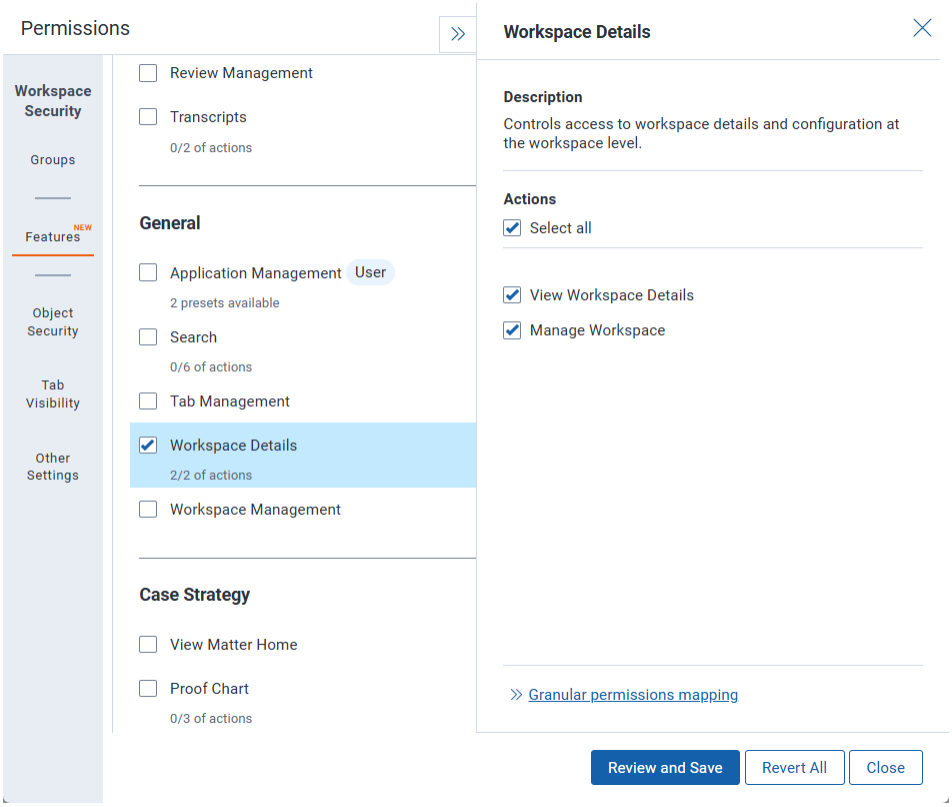
In Relativity, a workspace provides a secure data repository for documents used in cases or for applications developed with dynamic objects. You can store all types of documents, such as productions, witness testimony, and so on, in a workspace to facilitate searching, organizing, and categorizing content. In addition, you can use granular security settings to grant or deny permissions to specific content stored in the workspace.

At the workspace level, you can also define views, layouts, fields, and choices. These features streamline workflows, as well as simplify the processes for organizing and categorizing content. Views support filtering on item lists, while layouts, fields, and choices are used for categorizing documents.

40.1 Permissions

Access to the Workspace Details tab comes from the **Workspace Details** feature. Access to the workspace itself comes from instance-level permissions.

Note: This feature supports feature permission actions. Each action grants access to a specific task within the feature. You can grant groups access to individual actions, allowing them to perform only the tasks they need. To grant access to the entire feature, select all of its actions. Manage feature actions on the Features tab in a group's workspace permissions. For instructions, see Setting workspace permissions. For more information about feature permissions, see Feature permissions.



The Workspace Details feature includes the following actions:

- **View Workspace Details**—grants read-only access to the Workspace Details tab.
- **Manage Workspace**—grants edit, delete, and secure access to the workspace, in addition to viewing it.

The Workspace Details feature grants access within a workspace. To reach a workspace, a group also needs instance-level permissions for the **Workspace** object and the **Workspaces** tab. The instance-level **Workspace Management** feature grants those. Granting instance-level permissions does not grant the Workspace Details tab. Grant both levels.

Note: A group with this action can delete the workspace.

40.2 Creating and editing a workspace

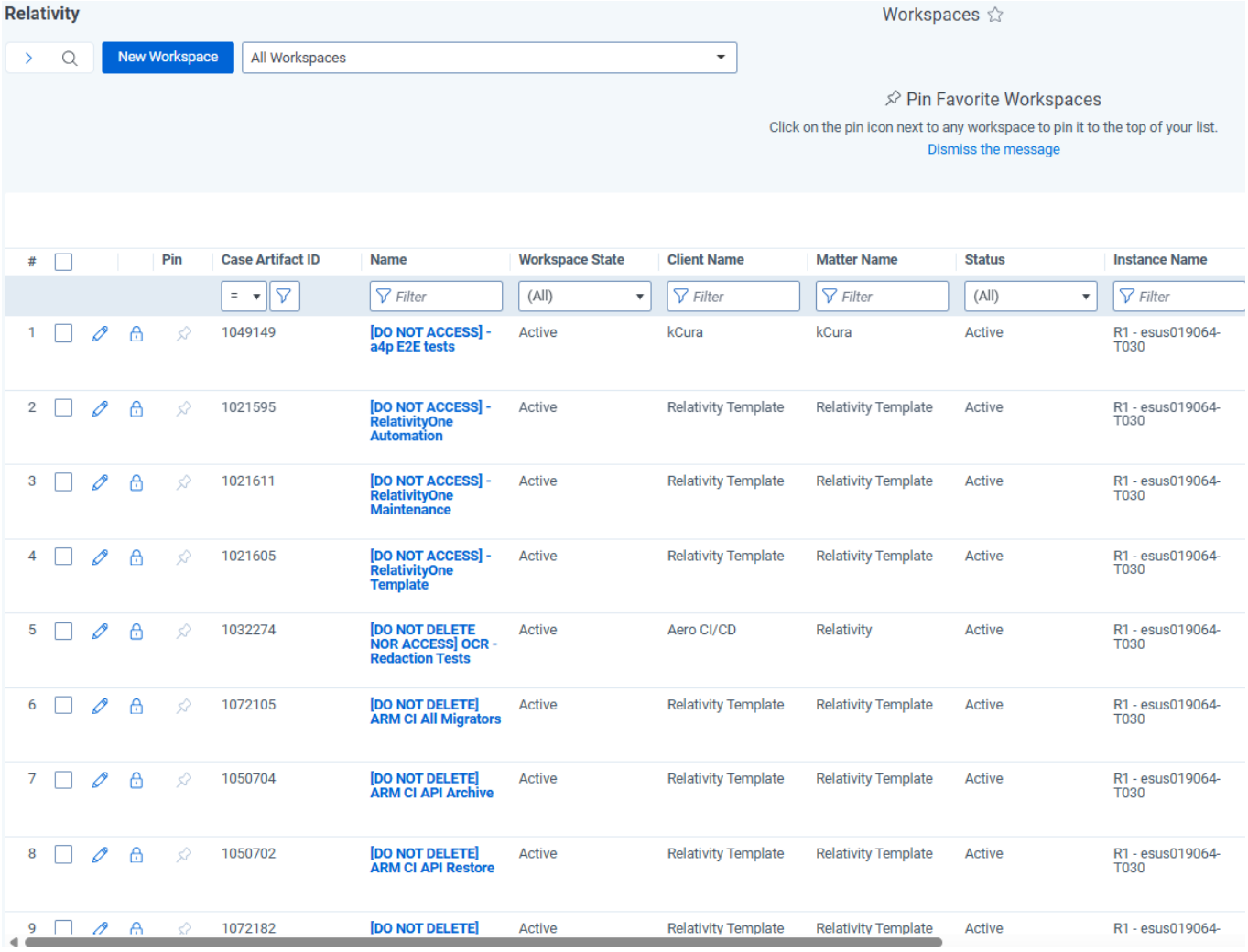
To create or edit a workspace:

1. Navigate to the **Workspaces** tab.
2. Click **New Workspace** to create a new workspace. If you want to edit an existing workspace, click the pencil icon next to the workspace name.
3. Complete the fields in the form. See Fields on the next page.
4. Click **Save**. A window displays the progress of the workspace creation process. You cannot access the workspace until it is created and its status is Active. If needed, close the progress window to continue working in Relativity aiR. This will not interfere with the creation process.

   Note: The workspace creation process cannot be canceled once it begins.

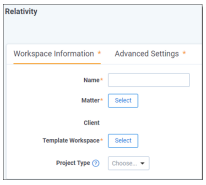
   To find out the status of the workspace, review the Workspace State column in the Workspaces list:

- **Active**—the workspace is available for use.
- **Creating**—the workspace is in the process of being created.
- **Cold storage**—the workspace has been migrated to Cold Storage. This is reflected in the system defined Workspace State field. See Cold storage management on page 785.



40.3 Fields

The Workspace Information section fields are:



- **Name**—the name used to identify the workspace. This must not exceed 50 characters and cannot contain any of the following characters:
  / \ : ? < > " | *

Note: You can edit a workspace name at any time without affecting any data. The root folder name for the workspace updates along with the workspace name.

- **Matter**—the case or legal action associated with the workspace. Click **Select** to choose a matter. The Select Item - Matter modal displays a list of matters based on the conditions set in the MattersOnPicker view.
- **Template Workspace**—use an existing workspace structure used to create the new workspace. Click **Select** to select a template. The Select Item - Template Workspace modal lists templates based on the conditions in the **WorkspacesOnPicker** view.For more information, see the Admin Guide.

Notes:

- Any groups that are part of a template workspace will also be a part of the client domain workspace. We recommend removing these non-client domain groups to prevent the client domain admin from seeing information on non-client domain users and groups.
- We recommend selecting an empty workspace without any documents as a template to prevent potential errors when trying to clean up all the references.
- Workspace Admin and Client Domain Admin permissions are not copied from the workspace template when a new workspace is created. They are taken from the Sys Admin permissions.

- All of the following non-document objects in the template copy to the new workspace:
  - aiR suite (aiR Review, Privilege, Case Strategy)
  - Analytics indexes
  - Analytics profiles
  - Automated workflows
  - Choices
  - Conditional Coding Rules
    - Conditional Coding Rules configured in the template workspace transfer to the new workspace and function as intended.
  - Custom tabs
  - Fields
  - Filters for Repeated Content and Regular Expressions
  - Groups, and permissions
  - Imaging profiles
  - Imaging sets

    Note: To enable an automatic carryover of Imaging Sets to newly created workspaces, confirm the **Copy Instances on Workspace Creation** setting within the corresponding Object Type template workspace (Imaging Set) is set to **Yes**.
  - Integration Point profiles

    Note: Only export type Integration Point profiles with a source and destination of Relativity are copied.

- Layouts
- Markup sets
- Native types
- OCR profiles
- OCR sets

  Note: To enable an automatic carryover of OCR sets to newly created workspaces, confirm the **Copy Instances on Workspace Creation** setting within the corresponding Object Type template workspace (OCR Set) is set to **Yes**.

- Persistent highlight sets
- Pivot profiles
- Placeholders
- Saved searches using Keyword, dtSearch, or Analytics indexes
- Scripts
- Search term reports
- Structured analytics sets
- Summary reports
- User objects
- Views

  Note: Folders are not copied from the workspace template. Because folders are not copied, saved searches that reference specific folders may not return expected results in the new workspace.

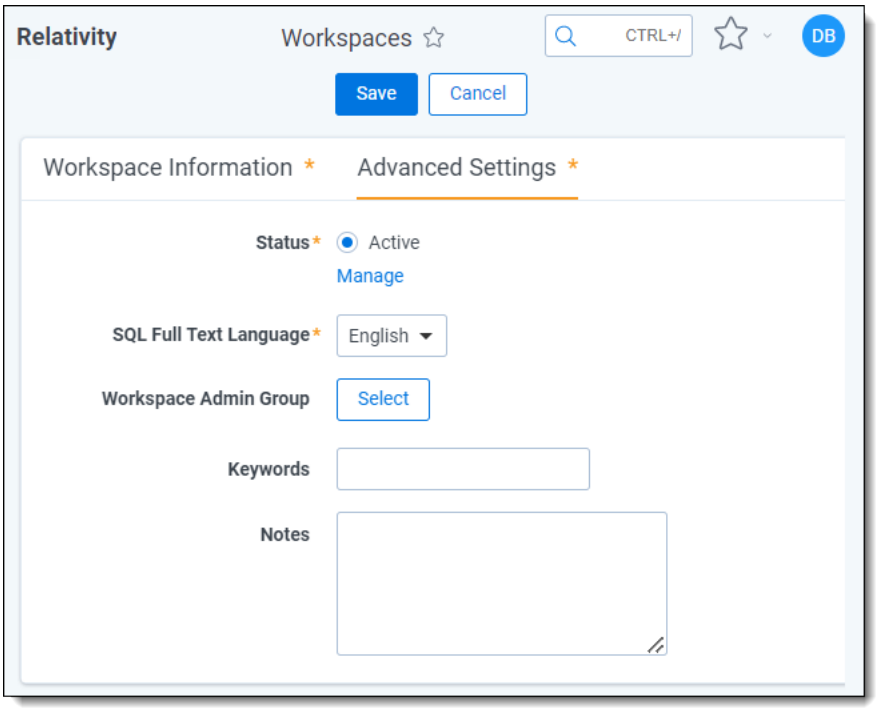
- **Project Type**—A categorization for workspaces. If desired, assign a project type to simplify monitoring, management, and exploration of your projects in Cost Explorer. **This field is required.**

  Note: Do not enter confidential customer or personal information.

  - Pre-defined values for your project type are listed below:
    - Contract Reviews
    - Data Breach Response
    - Data Subject Access Requests (DSARs)
    - Freedom of Information Act (FOIA) Requests
    - Internal Investigations
    - Litigation - Antitrust and Competition
    - Litigation - Class Actions and Mass Torts
    - Litigation - Commercial and Financial
    - Litigation - Criminal

- Litigation - Data Protection, Privacy, and Security
- Litigation - Intellectual Property
- Litigation - Labor, Employment, and Civil Rights
- Litigation - Other Civil
- Litigation - Regulatory and Environment
- M&A Clearance, 2nd Requests, Phase II Inquiries
- Merger & Acquisition (M&A) Due Diligence
- Operational Efficiency
- Personal Data Identification and Anonymization
- Public Records / Transparency
- Regulatory Requests
- Third-Party Subpoenas
- Other

- The Advanced Settings section fields are:



  - **Status**—this field has no impact on workspace functionality or billing. It is used only for filtering and reporting purposes. Default values are active and inactive, but users can add custom values to this field.
  - **SQL Full Text Language**—determines the correct word-break characters used in the full text index. Select the primary language for documents added to the workspace. The default setting is English. Note that for multiple language workspaces, Microsoft recommends setting the most complex prevalent language as the SQL Full Text language.

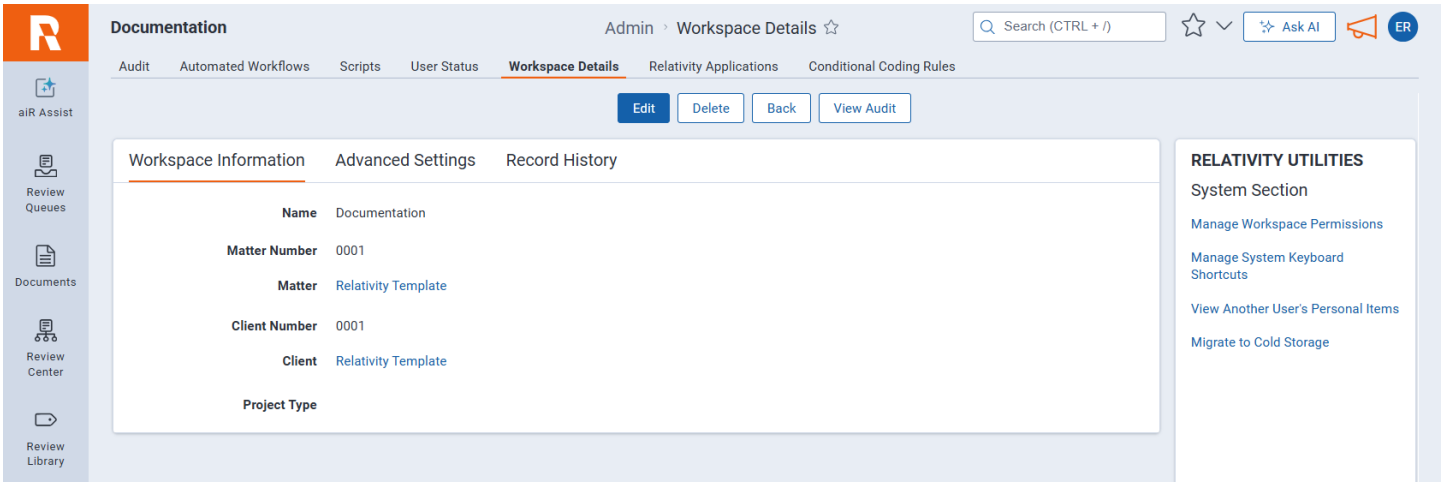
Note: The SQL Server settings determine the languages available in this list. Contact your system admin if you require additional languages. For information on configuring and managing word breakers, go to Microsoft's guidance on Configuring & managing word breakers & stemmers for search (SQL server).

- **Workspace Admin Group**—determines the group that has workspace admin permissions over this workspace. Click **Select** to choose a workspace admin group. See Workspace admin group on page 786 for more information.
- **Keywords**—any keywords you want to associate with the workspace.
- **Notes**—any notes you want to add to describe the purpose of the workspace.

Note: Changing the matter and/or client associated with a workspace has no impact on the groups and permissions within the workspace; if a matter is changed after a user was assigned to a group within a workspace, the user will still belong to that group and will still have the same access as before.

40.4 Viewing workspace details

On the Workspace Details tab, Relativity displays read-only workspace fields, history information, Relativity Utilities console, Production Restrictions, and the Workspace Admin Group field. You can update the Production Restrictions field when you edit a workspace. See Adding and editing production restrictions on page 785.



Note: Once a workspace is created, only System Administrators and Client Domain Administrators can make updates to the Matter object. Even users with full permissions for Matters and Clients will not have the ability to modify this object unless they are System Administrators or Client Domain Administrators.

40.4.1 Deleting a workspace

From the Workspace Details tab, you can delete the current workspace. Clicking **Delete** moves the workspace to the Recycle Bin. After you click **Delete**, a confirmation message appears with the Dependencies button. See the Relativity Documentation Site.

Note: You must have Delete permissions for the workspace object in order to delete a workspace.

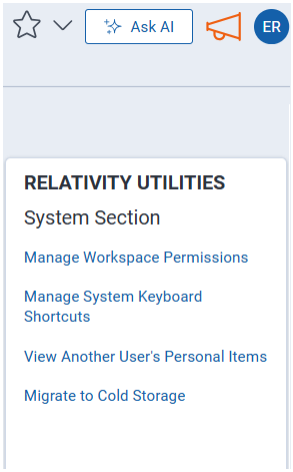
When you delete a workspace in Relativity, it automatically moves to the Recycle Bin, providing a safety net for deleted workspaces. You can manually choose to permanently delete the workspace from the system or restore it within the **seven-day period** in the Recycle Bin.

During off-hours, the Case Manager agent deletes the following:

- Any documents in the Relativity file repository, except those loaded with pointers.
- dtSearch indexes.
- Analytics indexes and staging areas.
- The SQL database (Relativity does not delete database logs and backups).

40.5 Using the utilities console

Additional administrative features are available through the **Relativity Utilities** console on the Workspace Details tab.



40.5.1 System Settings

The console includes the following in the System Section:

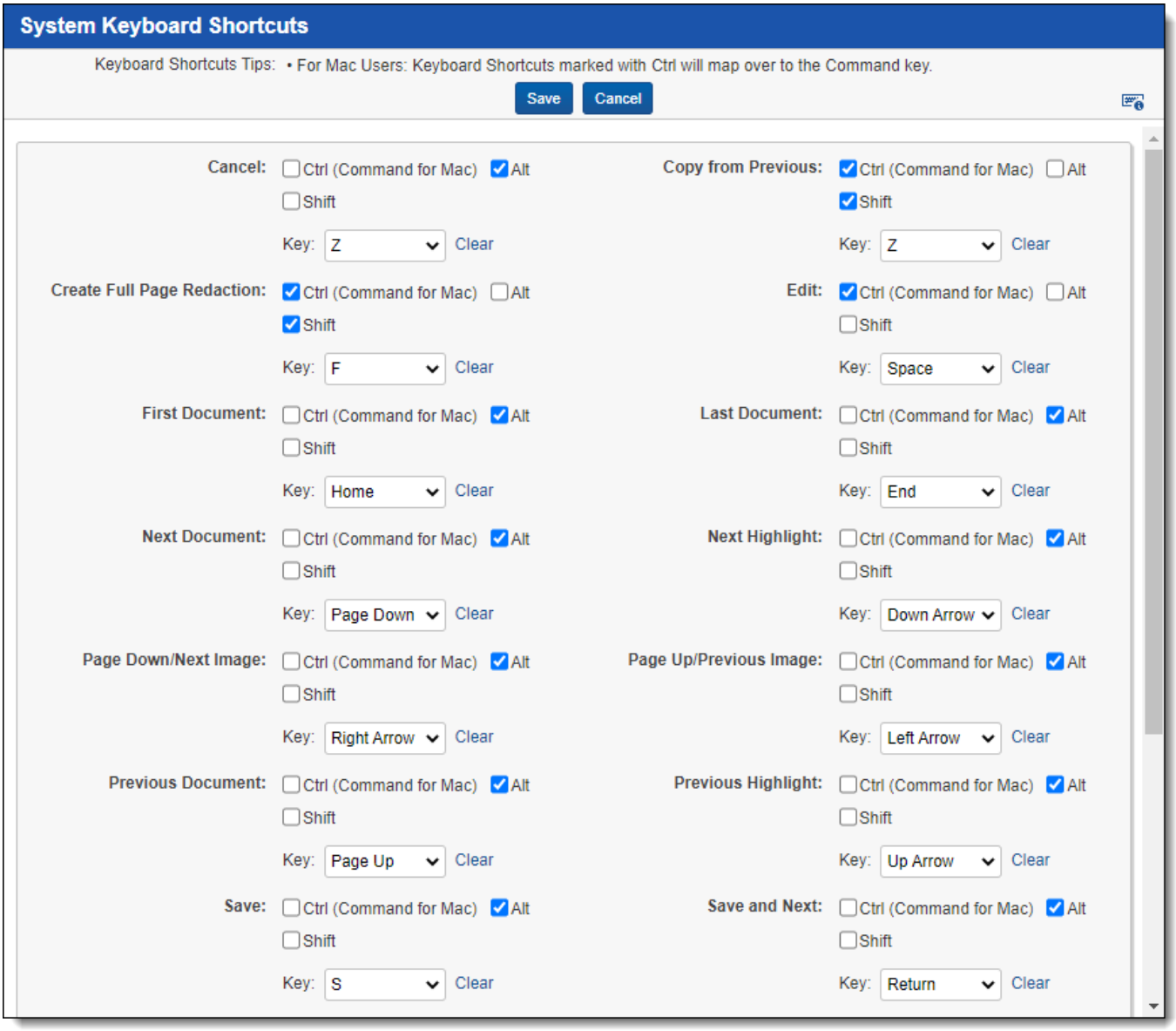
- **Manage Workspace Permissions**—set permissions for the workspace.
- **Manage System Keyboard Shortcuts**—displays a pop-up for modifying the key combination used by system shortcuts. To use this, you must have security permission for the Admin Operation called *Modify System Keyboard Shortcuts*. See Managing system keyboard shortcuts below.
- **View Another User's Personal Items**—displays a pop-up for selecting workspace users where you can view a user's personal items. This button is only available to system admins. See Viewing the personal items of workspace users on page 785.
- **Migrate to Cold Storage**—displays a pop-up for migrating workspaces to Cold Storage. To use this, you must be a system admin and have the security permission for the Admin Operation called *Manage Cold Storage*. See Migrating and retrieving workspaces to and from Cold Storage.

40.6 Managing system keyboard shortcuts

You can modify the system keyboard shortcuts for a workspace. These keyboard shortcuts are defined in Relativity for use in the review interface. You must have security permissions for the Admin Operation called *Modify System Keyboard Shortcuts*.

To manage system keyboard shortcuts, follow these steps:

1. Navigate to the **Workspace Details** tab.
2. Click **Manage System Keyboard Shortcuts** in the Relativity Utilities console.



Use the following instructions to modify a system keyboard shortcut key:

- Select or deselect one or more of the following check boxes: **Ctrl**, **Alt**, or **Shift** for the Control, Alt, and Shift keys, respectively.

  Note: You must select either or both the **Ctrl** and **Alt** checkboxes. Relativity displays the error message <Invalid Keyboard Shortcut> when these checkboxes are not selected.

- In the **Key** drop-down menu, select a letter, number, or navigation key. The navigation keys include End, Home, Space, Return, Down Arrow, Up Arrow, Left Arrow, Right Arrow, Page Down, and Page Up.
- Click the **Keyboard Legend** icon to display a list of keyboard shortcuts currently in use by the System and browsers. See Keyboard shortcuts legend.
- Click **Clear** to reset the options for keyboard shortcuts.

After you have completed your updates, click **Save** to display the Workspace Details page.

Note: You can create user-defined shortcuts when you add a new field to Relativity. See Creating and editing fields, and Creating keyboard shortcuts.

40.7 Viewing the personal items of workspace users

Access to View User's Personal Items is granted to System Administrators by default. All other groups must have the proper permissions. To view personal items, follow these steps:

1. Navigate to the **Workspace Details** tab.
2. Click **View Another User's Personal Items** in the Relativity Utilities console.
3. Select one or more users whose personal items you want to view, and move them to the right box using the arrows.

   Note: To move multiple users between boxes, click the double arrows. You can also select and double-click on user names to move the between boxes.
4. Click **Save**.

40.8 Cold storage management

Cold storage stores data for retention when it's not accessed regularly. To use this feature, you need specific permissions and processes to migrate, retrieve, and delete workspaces. For more information, see Cold Storage.

40.9 Adding and editing production restrictions

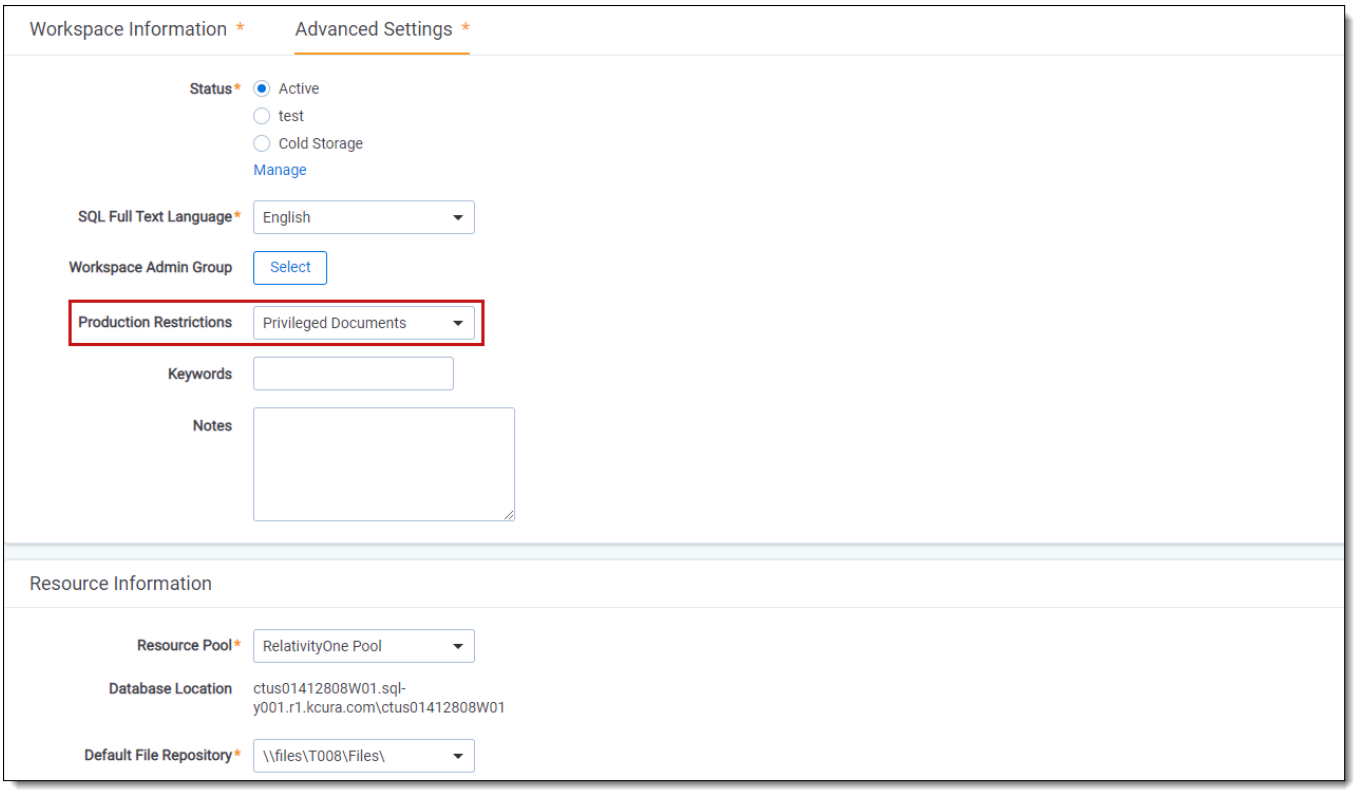
Using the Production Restrictions option, you can ensure that your production set does not include privileged or other confidential documents. You can select a saved search that returns documents that you want excluded from the production set. When you run a production, Relativity compares these documents against those in the production and alerts you to any conflicts.

Note: You need permissions to the documents in a production to resolve production-restriction conflicts. See Check for production conflicts.

To add a production restriction:

1. Create a saved search with criteria that returns documents that you want excluded from the production set. Include family groups in your saved search so that all of the family items are kept together and can be removed if necessary.
2. Click to edit the workspace details page. You can only update the **Production Restrictions** option when editing a workspace. See Creating and editing a workspace on page 777.

3. Select your saved search in the **Production Restrictions** option. The default value is <no restriction>.



4. Run your production set. If a conflict occurs, you can override the production restriction if you're a system admin with the Override Production Restrictions permission. See Workspace security.

40.9.1 Managing production restrictions in templates

If you use a workspace with production restrictions as a template, you'll see a warning message that requires you to select one of the following options:

- Select a New Production Restriction
- Continue With No Production Restriction

You cannot delete the saved search that the Production Restriction option uses. You must first edit the Production Restriction option so that it no longer references the search.

40.10 Workspace admin group

A system admin can assign any group in Relativity to have full admin rights over a particular workspace. A workspace admin has near-complete control over all objects within the workspace, but members of the group do not have the script permissions available only to system admins.

Note: While Workspace Administrators have extensive control over their respective workspaces, they do not automatically inherit the full range of system administrator privileges. Non-standard permissions like "**New Document**" must be added. Additionally, the "**Workspace**" permission is initially set only to "**View**" status.

Use the following steps to set a designate a workspace admin group:

1. Click **Edit** on the **Workspace Details** tab.
2. Click **Select** in the **Workspace Admin Group** field.

3. Select the group you want to set as the workspace admin group.
4. Click **Ok**.

Note: You can only designate one group per workspace as a workspace admin group.

40.11 Repository workspaces in Relativity aiR

When setting up a workspace for documents, it is useful to understand that Relativity aiR provides administrators the flexibility to setup a workspace either as a regular workspace or as a repository workspace.

This topic highlights some of the items that admins need to be aware of as they create the repository workspace in Relativity aiR. It also covers how to prepare and handle the flow of data between the review and the repository workspaces.

40.11.1 Setting up a repository workspace

All organizations start with a template that is shipped with Relativity aiR or a template that is customized for your instance that meets your workflow requirements. The workflows described here will apply towards all such template workspaces in your Relativity aiR environment.

Here are some advantages of executing these workflows in the below scenarios to designating repository / review workspaces:

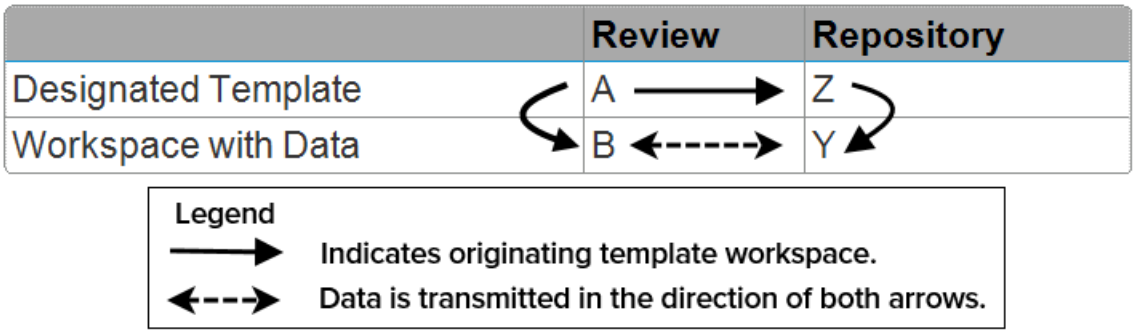
- You have the same fields / layouts / views available in both workspaces (repository and review) so the learning curve for the teams administering the case is minimal.
- When you promote data between repository and review workspace (using Integration Points) you can use the same field names and types to push data between them, reducing the opportunity for errors since both workspaces are born out of Template Review Workspace (Workspace –A) originally.

Below, we'll describe two scenarios for creating a Repository Workspace, followed by a few quick workflows that will come in handy as you use those workspaces.

40.11.2 Example 1

You currently have a Review Template (Workspace-A). You can create a new workspace (Workspace-Z) from Workspace-A, add the Repository application to Workspace-Z and designate it as a Repository Template.

1. In Repository Template Workspace-Z remember to setup the appropriate security groups that limit access to case admins and disable access to the reviewer groups.
2. You have two designated workspace templates – one for review (Workspace–A) and one for repository (Workspace-Z).
3. You can create Review Workspace-B and Repository Workspace-Y from these templates.

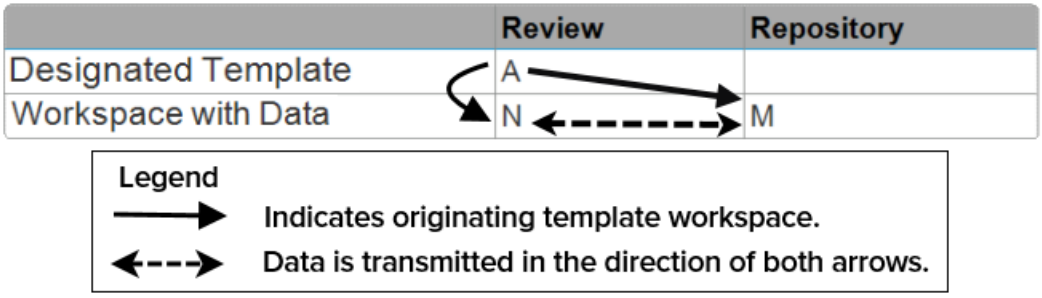


40.11.3 Example 2

You currently only have a Review Template Workspace-A. You have created a new Review Workspace-M and loaded data into it and are well into review. With time you receive more data and the size of the workspace is expected to increase dramatically.

At this point, you can still take advantage of the Repository feature and here is how:

1. Create a new review workspace called Workspace-N (from Template Workspace-A).
2. Now, add the Repository application to the original Review Workspace-M and from this point on it becomes your repository workspace.
3. Turn off Review access to Workspace-M.
4. Promote the reviewed data from Workspace-M to your new Review Workspace-N.
5. Proceed with review in Workspace-N.



40.11.4 Special considerations

- Administrators can load data in using Import/Export.
- Repurpose some of the suggested Data Load / Analytics / Searching Dashboards to facilitate analysis and culling your data sets for promotion.
- When promoting subsets of data:
  - Promotion workflow is not limited to just repository to review (ex: documents and metadata), it will also work between review and repository (ex: overlay Priv Coding designations).
  - It is recommended to tag documents that were promoted on an admin field in the repository workspace to facilitate easy QC.
  - Following promotion of, inclusive & non-duplicate emails or some documents from certain clusters, trying to rerun the email threading or clustering (in these examples) in the review workspace, will result in different results, by design.
  - To avoid being billed for the same data in two workspaces, we strongly recommend promoting sets of documents via links only, rather than copying files, to standard review workspaces. When you promote via links, the documents are billed at the review workspace rate only, and you are not charged separately for those documents in the repository workspace.
  - If you choose to promote actual files (copies) to your review workspace, your calculated data usage will include both the original files in the repository workspace, billed at the reduced repository rate, and the duplicated files in the standard review workspace, billed at the standard review rate. Refer to your contract for specific details on how this is calculated.

- If you promote documents via links from repository to review workspace – keep in mind that if you did delete the documents in the repository workspace or delete the repository workspace itself, the links to the promoted documents in the review workspace will be broken.

- When using Relativity Processing:
  a. Administrators can load data in using Import/Export and processed data via Relativity Processing in the repository.
  b. If you are loading data via Import/Export:
     i. Watch out for deduplication challenges across the mixed data.
     ii. To avoid errors on retry (of processing errors), use unique control numbers that will not conflict with the Relativity Processing Numbering scheme (Ex: HardCopy-xxxxx or LoadFile-xxxxx).
  c. Process data with deduplication turned off on the processing profile and use theProcessing Duplication Workflow to cull your data. It provides better flexibility in case of changes in dedupe order / type.

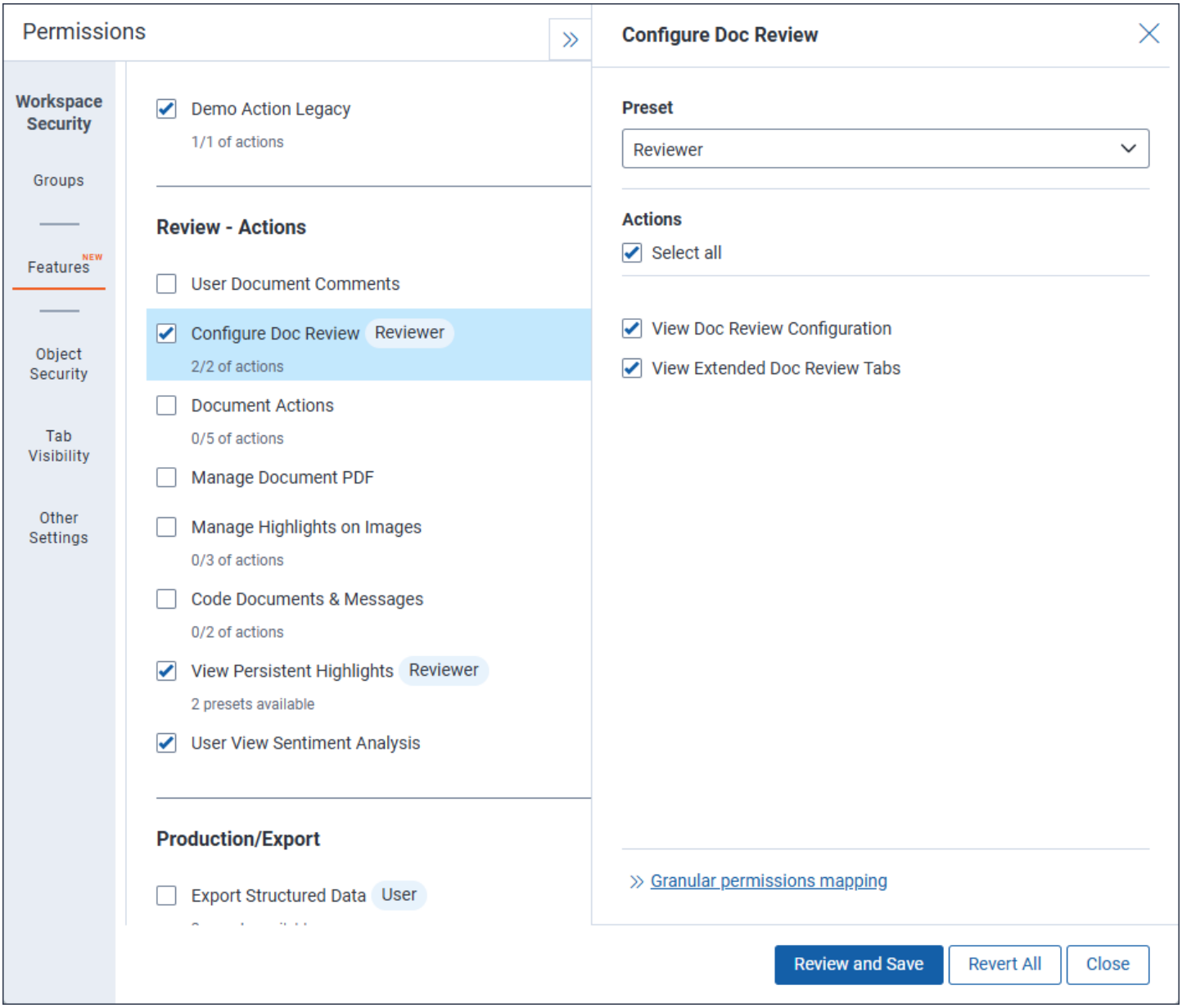
- When using Analytics:
  a. For structured analytics sets - Evaluate if you need to repopulate text or update only new documents. For more information, see Running structured analytics in the Analytics guide.
  b. For conceptual indexes – Evaluate if you need to do a full index update or an incremental one. For more information, see Best practices for updating a conceptual index in the Analytics guide.
  c. When clustering documents, evaluate if you would like to cluster the entire universe or just a subset of documents based on your needs.

40.12 Document and item list navigation

The workspace offers several ways to view documents and items. Using the Browsers panel, you can navigate from folder to folder to see the documents contained within each. The Document Preview panel allows you to view specific documents from the document list. Additionally, you can also sort and filter the document or item list based on any fields in the current view or using the search panel.

40.12.1 Permissions

Note: This feature supports feature permission actions. Each action grants access to a specific task within the feature. You can grant groups access to individual actions, allowing them to perform only the tasks they need. To grant access to the entire feature, select all of its actions. Manage feature actions on the Features tab in a group's workspace permissions. For instructions, see Setting workspace permissions. For more information about feature permissions, see Feature permissions.



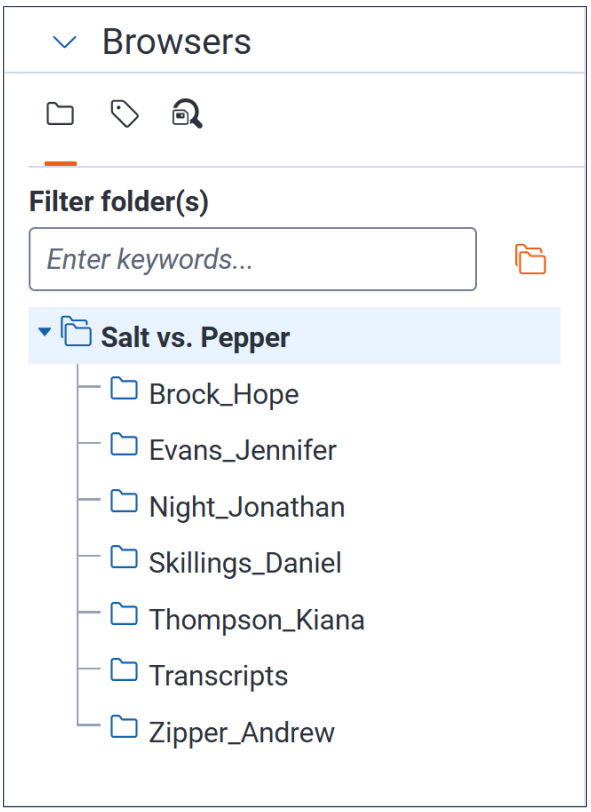
40.12.2 Browsers panel

The Browsers panel is located on the left side of the workspace. Depending on your permissions, you may not see the Browsers panel.

The Browsers panel may contain the following options for browsing through your documents:

- Folders
- Field Tree
- Saved Searches

No matter which of these options you use, there are several display options you can use to customize your workspace.



The Browsers panel opens by default. Hide or expand the Browsers panel by clicking the carrot to the left of Browsers. If both the Browsers and Search Conditions panels are hidden, click on the **Expand Browsers Panel** icon to display it. You can also re-size the Browsers panel by hovering over the line separating the panel from the other panel or document list until the line is highlighted. You may then click-and-drag the line to the desired dimensions.

40.12.2.1 Document browser menu

The Document browser menu is located directly below the Browsers panel. Click on one of the menu's options to display that mode of the browser:

Icon	Name	Description
	Folders	Navigate the folder hierarchy for your workspace.
	Field Tree	Browse your documents according to how they were coded or grouped.
	Saved Searches	Create a new search, or browse previously saved searches.See Saved Search in the Searching Guide.

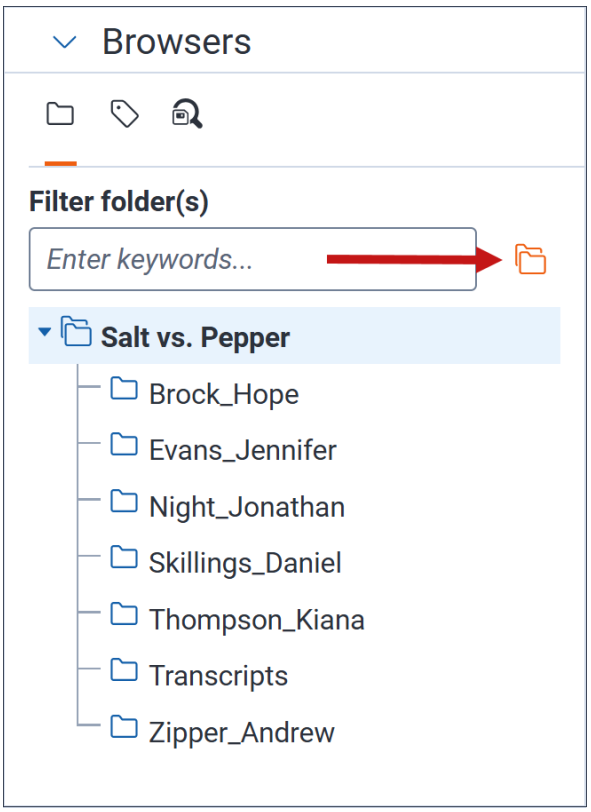
Folders

Click on the **Folders** icon to navigate the folder hierarchy for your workspace. The folder structure is set when documents are imported. It can be based on the document's source, or according to a folder structure set by your Relativity administrator. Clicking on a folder displays that folder's documents in the document list.

Note: To ensure stable performance, we recommend creating no more than 250,000 folders in a workspace and having 15 sub-folders or less within each folder.

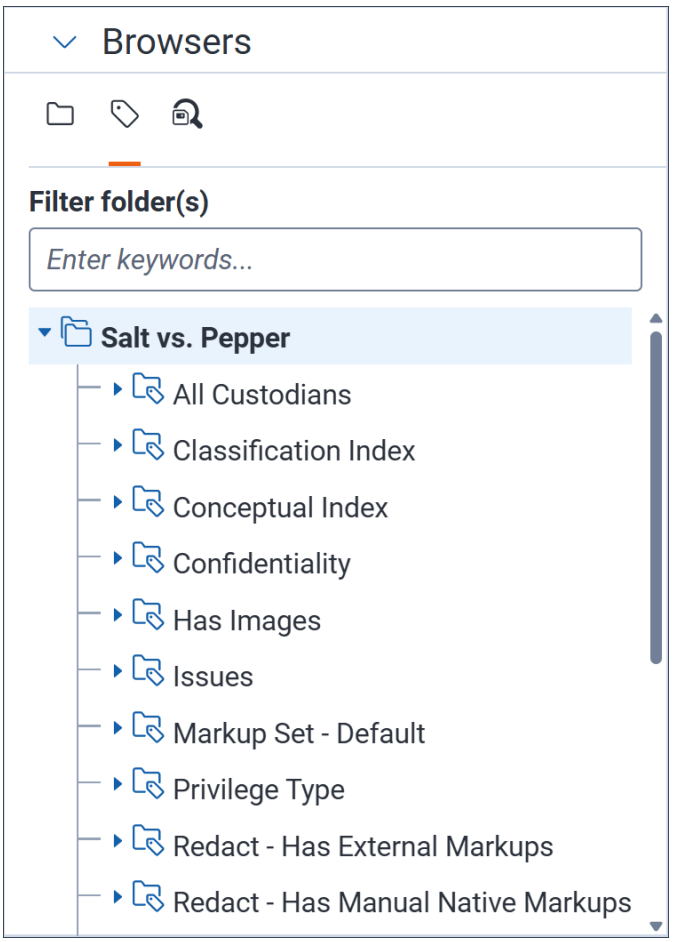
A folder often has multiple sub-folders. Click on the folder to view the sub-folders. Click on the arrow next to the folder to hide the sub-folders.

To change the folder scope, click on the **This folder and subfolders** or **Only this folder** icon.



Field tree

Click on the **Field Tree** icon to display the field tree in the browser. Selected single and multiple-choice list fields and their choices appear in a tree structure.

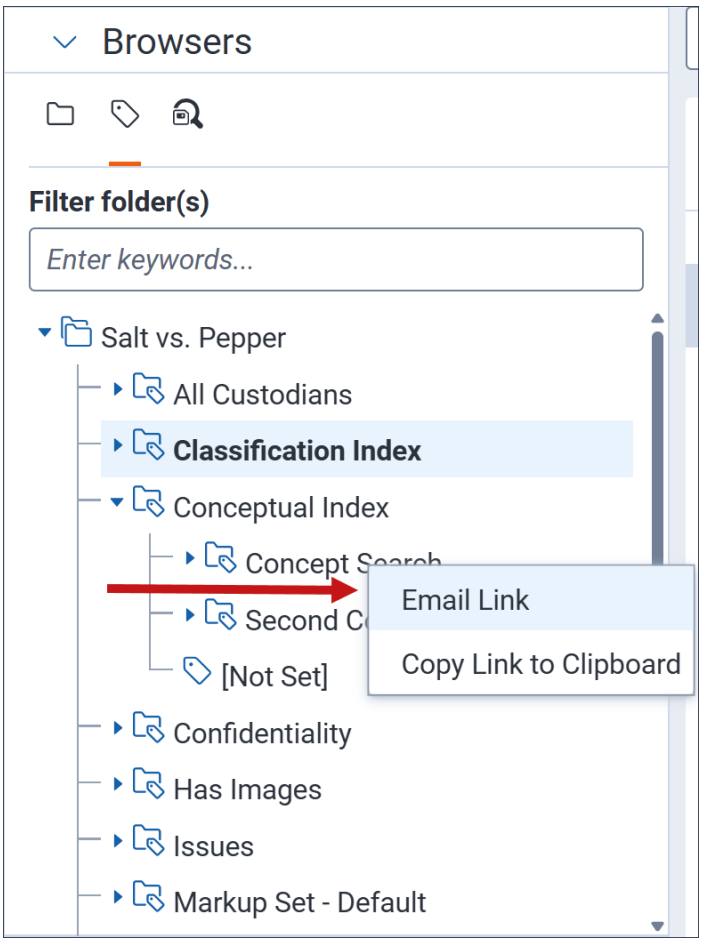


Each single and multiple-choice field has its own choice folder in the field tree. The field's choices appear as sub-folders. Each field also has a [Not Set] choice, which displays null values for the field.

You can click on a choice in the field tree to display all the documents in the document list that have the selected choice value and meet the criteria of the active view.

Sending email links to choices

You can send an email with a link to a view that contains the choice, a choice folder, or the document list that appears when the field tree is open. In the field tree, right-click on a choice or a choice folder and select the **Email Link** option.



The subject line of the email pre-populates with the following text: Relativity Review - <Workspace Name> - <Choice Name: Value>. If you send an email link to a choice folder, the subject line displays the folder name instead of choice name and value.

When the recipient clicks on the link, the documents associated with the choice or folder appear in the document list. If the recipient does not have required permissions for the choice folder or field associated with the choice, a permissions denied message displays instead.

Alternatively, you can select **Copy Link to Clipboard** to copy a link to a view that contains the choice, a choice folder, or the document list that appears when the field tree is open.

40.12.3 View bar

The View bar consists of the following elements:



- **New documents**—click to upload new documents using Simple File Upload. If the Transcripts application is installed in this workspace, this icon is replaced with a drop-down menu that allows you to choose between uploading a new document or a new transcript.
- **Views drop-down menu**—click to select a view.
  - **New view**—click to create a new view from within the view drop-down menu. This icon only displays if you have permission to add a new view. If the icon is not present, contact your Relativity administrator to add a view.

    - **Edit view icon**—click to edit a view that displays within the view drop-down menu. This icon only displays if you have permission to edit the view. If the icon is not present, contact your Relativity administrator to edit the current view.
- **Include Related Items drop-down menu**—returns documents related to the documents currently in the view. The options vary by workspace, but may include email family groups, duplicates, or similar documents.
- **Add Widget**—click to add a custom widget to your document list dashboard.
- **Dashboard drop-down menu**—select a custom dashboard to view in the document list. See Dashboards in the Navigation section of the Admin Guide for more information.
    - **New view**—click to create a new dashboard from within the dashboard drop-down menu. This icon only displays if you have permission to add a new dashboard. If the icon is not present, contact your Relativity administrator to add a dashboard.
    - **Edit dashboard icon**—click to edit a dashboard that displays within the dashboards drop-down menu. This icon only displays if you have permission to edit the dashboard. If the icon is not present, contact your Relativity administrator to edit the current dashboard.
- **Export Dashboard**—click and select a dashboard widget to download to your workstation as an editable Excel file. See Dashboards in the Admin Guide for more information.

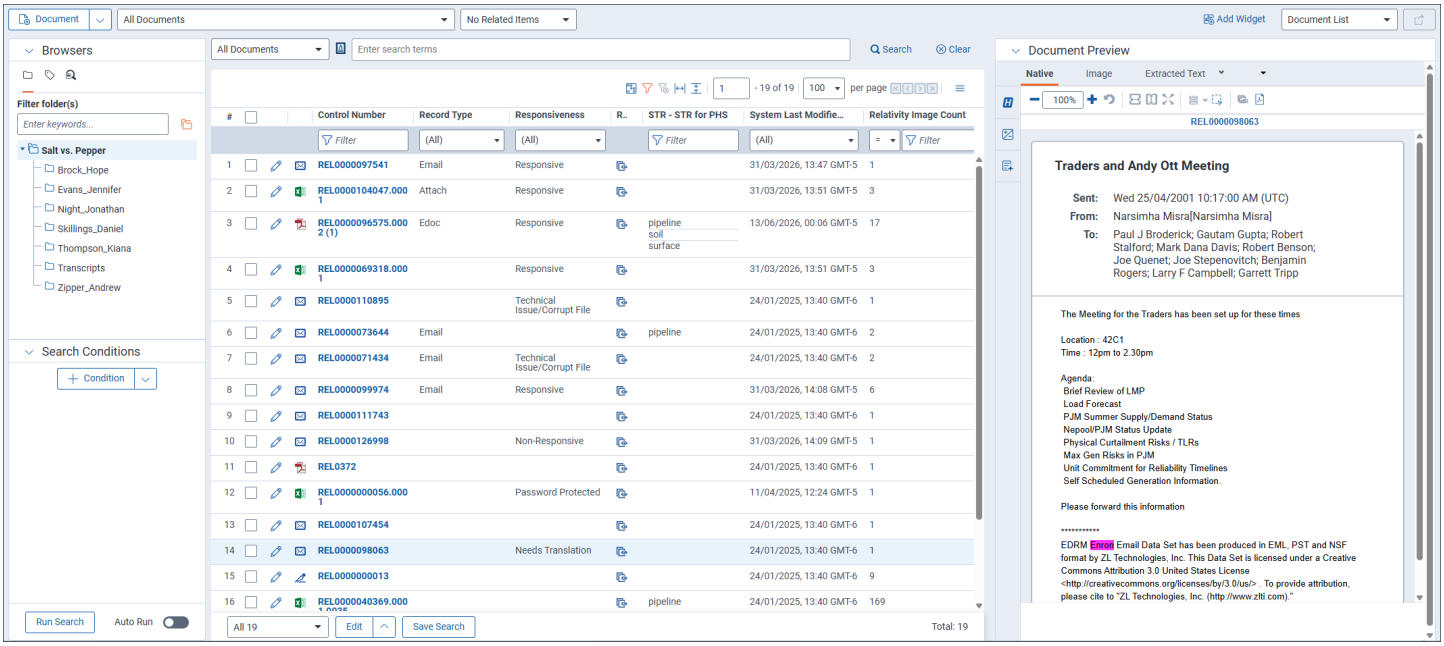
For more information, see the Views chapter of the Admin guide.

40.12.4 Document Preview panel

The Document Preview panel allows you to view documents similarly to the Viewer, while remaining on the document list. This allows you to filter the document list as desired and view the results without leaving the Documents tab. You can view and navigate through highlight hits for any previously created persistent highlight sets as well. However, you cannot search or create search terms in the Document Preview panel. Additionally, searching for terms in the document list will not create highlights in a document you are viewing in the Document Preview panel.

To access the Document Preview panel, the **EnableDocumentPreview** instance setting should be set to True. The Show Document Preview Panel icon will then display in the upper-right. Additionally, users must have the **Document Preview** permission in Other Settings assigned to use this feature.

Note: The Document Preview panel does not support viewing hidden content, creating or modifying markups, or editing coding decisions. Open the document in the Viewer instead to perform these tasks.



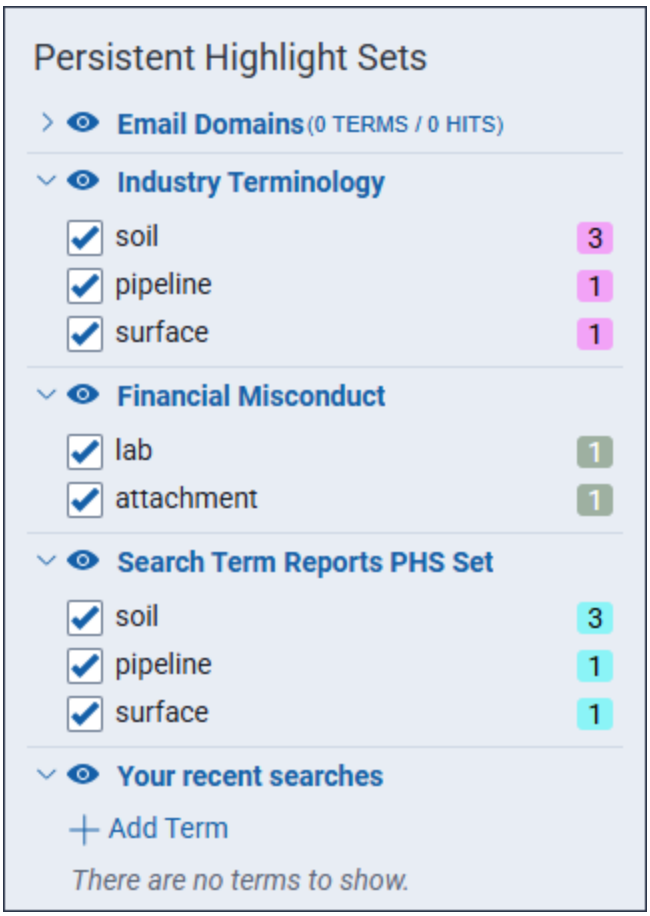
40.12.4.1 Navigating the Document Preview panel

The Document Preview panel can be re-sized at any time by clicking on the edge of the panel and dragging your cursor to the desired size.

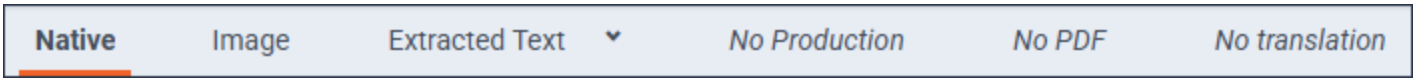
The Document Preview panel can be moved from the right or left side of the document list to the other side as well. To move the preview panel, click in the upper-left corner and drag the window to the blue strip on the other side of the screen.

The following options are available in the Document Preview panel:

- **Persistent Highlighting**—displays or hides a panel containing any persistent highlight sets in the workspace. Only terms that are in the current document will display in the pane. Additionally, you can control which highlights display in the current document by clicking on either the persistent set to only display highlights from that set or you can click on a specific term to only see that term highlighted in the document.



- **Document preview panel Viewers**—click on the name of the Viewer in which you would like to view the document. Viewer names that are displayed in black indicate that the document is available for viewing. The Viewer that is currently open is bold with an orange underline underneath the name. If a name appears in italics, that Viewer is not available for the current document.



- **Markup set**—displays the active markup set in a drop-down menu. Choose a markup set from the drop-down menu to make a different set active. This menu only appears when viewing a document in the Image Viewer of the Document Preview panel.
- **Page navigator**—use any of the following options to help you navigate the pages in the document you are previewing:

Option	Description
	Click to move to the first page in the document.
	Click to move to the previous page in the document.
	Click to move to the next page in the document.
	Click to move the last page in the document.

40.12.5 Item list

The item list contains items as well as navigational and other controls for working with the list.

Icon	Description
 Inline Editing	Click to enable edit mode where a user can edit eligible fields from the document list. **Note:** User access to Inline Editing is determined by permissions as well as on the view by a system administrator. As a result, some users may not see this icon, depending on which view they are using.
 Freeze/Unfreeze columns	Click the blue snowflake icon to refreeze columns that were most recently frozen. If the icon is orange, click it to unfreeze the columns. This option only displays if you have already frozen a column this session.
 Sampling	If you have proper permissions, clicking the Sampling icon lets you create random sample sets from the item list using

Icon	Description
	three different methodologies from the pop-up menu that appears.
 Show/Hide filters	Click the blue filter icon to show filters for columns in the item list. Click the orange icon to hide them.
 Clear filters	Click the blue clear filter icon to clear any filters applied to the item list.
 Reset column sizes	Click the blue Reset column sizes icon to return to the original settings for the columns.
 Turn Grid style on/off	Click the blue grid icon to turn grid style on. This shrinks the row padding and alternates row shading to make your data more compact and easier to read. Click the orange icon to turn grid style off.
	Use these navigational controls to navigate the pages in the document list.

The fields that appear in the item list are based on the selected view, which you can edit. You can also edit a view to rearrange the order that the columns display. Contact your Relativity administrator to change the fields in your view.

To change a column's size, hover over the white line at the edge of the column header. A double arrow appears, indicating that you can resize the column. Drag it in either direction to adjust the column width. The other columns on

the page automatically adjust to fill the rest of the window. Column data can be cut off. If you wish to return to the original settings click the **Reset Column Sizes** icon.

40.12.5.1 Freeze and unfreeze columns in a list

When viewing and interacting with items in a list, you can freeze one or more columns so that they are locked in place which allows you to scroll to the right and view any columns in the list side-by-side with the frozen columns.

To freeze a column or columns, do the following:

1. In the right-most column that you wish to freeze, hover your cursor over the column's title and click on the ellipses.
2. Select **Freeze Columns**.
   The column, or columns, to the left of the one you selected are frozen and will remain static as you scroll to the right and left in the list.

   Note: Once you have frozen a column or columns, you can freeze additional columns to the right of the frozen columns by repeating steps 1-2.

To unfreeze a column or columns, do either of the following:

- Hover your cursor over the right-most frozen column, click on the ellipses, and select **Unfreeze Columns**.
- Click the **Unfreeze Column** icon in the upper-right section of the list.

40.12.5.2 Copy column values

You can copy up to 10,000 values in a single column to clipboard. If you would like to copy more than 10,000 columns, we recommend using Mass export to file.

Note: You can determine if a user has access to this feature by enabling or disabling the Copy Mass Operations permission.

To copy column values:

1. In the column that you wish to copy, hover your cursor over the column's title and click on the ellipses.
2. Select **Copy column values**.
   A modal displays the total number of column values that were successfully copied to clipboard.

40.12.5.3 Saving a search from the Documents tab

You can save the conditions you have currently set up for the item list as a new search using the Save Search button located next to the mass operations bar at the bottom of the item list.

40.12.5.4 Previewing a document

If you hover your mouse pointer over a record's file icon, you can click to open a pop-up viewer showing the record.

Note: If your item list does not contain the file icon, contact your Relativity administrator to add it.

40.12.5.5 Sorting

You can use any field in the view to sort all of the results in an item list.

Click any field heading once to sort the items in that field in ascending order, alphabetically. A down arrow appears next to the heading name, as in the Responsive field below. Click a second time to sort the items in descending order, alphabetically. An up arrow appears. Clicking the field name a third time clears the sort and returns the field to its original order.

If you are not able to sort a particular field, contact your administrator to make sure the field has the Sort option set to Yes.

40.13 Cold Storage

Cold Storage is a feature that allows you to archive inactive workspaces for long-term retention when they are not regularly accessed. By moving a workspace to Cold Storage, you can reduce storage costs for dormant cases while preserving the data. When the workspace becomes needed again, you can retrieve it from Cold Storage to return it to an active state for use. Cold Storage is ideal for cases on hold or near completion. It provides a lower-cost storage tier for inactive data, with the trade-off of limited accessibility until retrieval. You migrate workspaces to Cold Storage to archive them, retrieve workspaces to bring them back for use, and can delete workspaces after a minimum retention period in Cold Storage.

40.13.1 Permissions

Certain security permissions are required to migrate or retrieve workspaces to/from Cold Storage. These permissions involve both instance-level and workspace-level settings:

Instance-level permissions:

Object Security	Tab Visibility	Other Settings: Admin Operations
Workspace: View, Edit, and Delete		Manage Cold Storage

Workspace-level permissions:

Object Security	Tab Visibility	Other Settings: Admin Operations
Workspace: View, Edit	Workspace Details	View Workspace Details

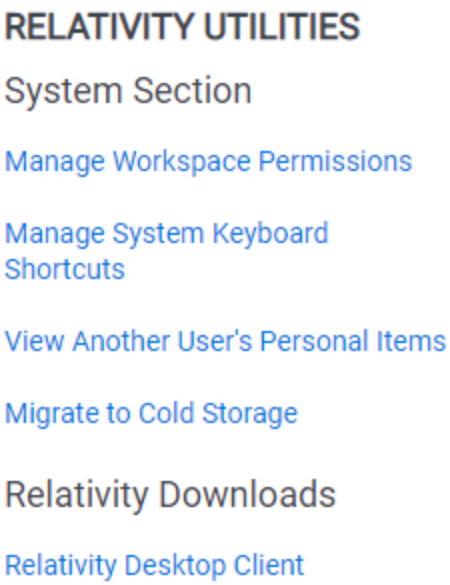
40.13.2 Migrating a Workspace to Cold Storage

Before migrating a workspace to Cold Storage, ensure you have the necessary security permissions. In general, you must be a system admin with the Manage Cold Storage admin operation permission, and have appropriate rights to the workspace. If your workspace was recently migrated from Relativity Server to Relativity aiR, you should also run any pending Text Migration jobs (for Data Grid) on the workspace before Cold Storage migration.

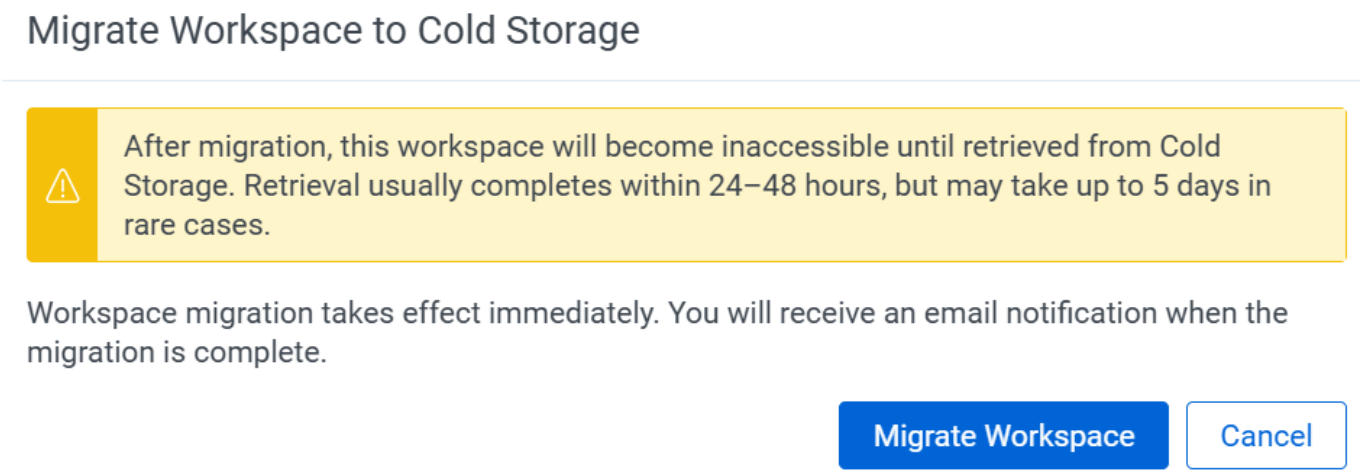
To migrate a workspace to Cold Storage:

1. **Navigate to the Workspace** – Go to the Workspace Details tab in Relativity aiR. You must have the correct permissions to see the Workspace Details tab.

2. **Initiate Cold Storage Migration** – In the Relativity Utilities console on the Workspace Details tab, click Migrate to Cold Storage. A Cold Storage confirmation dialog appears.



3. **Confirm the Migration** – In the confirmation dialog, click Migrate Workspace to proceed. The workspace will immediately move to Cold Storage.



Note: Once you confirm, the migration takes effect immediately. The workspace's **Workspace State** field will update to "Cold Storage," indicating the workspace is now archived. (The workspace Status field is not linked to Cold Storage state and changing it to "Cold Storage" manually will not affect the actual state or billing.)



Workspace is in Cold Storage

This workspace is currently archived. You can delete this workspace after it has been in Cold Storage for at least 30 days.
Deletion available on: **5.03.2026**.

Need this workspace back?
Retrieve it to restore full access. Retrieval usually takes **24–48 hours** (up to 5 days).

Retrieve Workspace

Return to Workspaces

After migration:

- **Inaccessible Data** – The workspace and its documents become read-only and inaccessible to users until retrieved. You cannot enter or work in a Cold Storage workspace .
- **Workspace Restrictions** – A workspace in Cold Storage cannot be used as a template for new workspaces. It also cannot be used for data imports/exports or by Integration Points jobs. Essentially, no modifications or data transfers can occur until the workspace is restored to active status.
- **Billing Implications** – For more information on billing implications, click the Community link: Understanding and Measuring Cost in Relativity aiR.
- **Retention Requirement for Deletion** – Once in Cold Storage, a workspace must remain in Cold Storage for at least 30 days before it can be deleted. After 30 days, the option to delete becomes available. See the Deleting from Cold Storage section below for details.

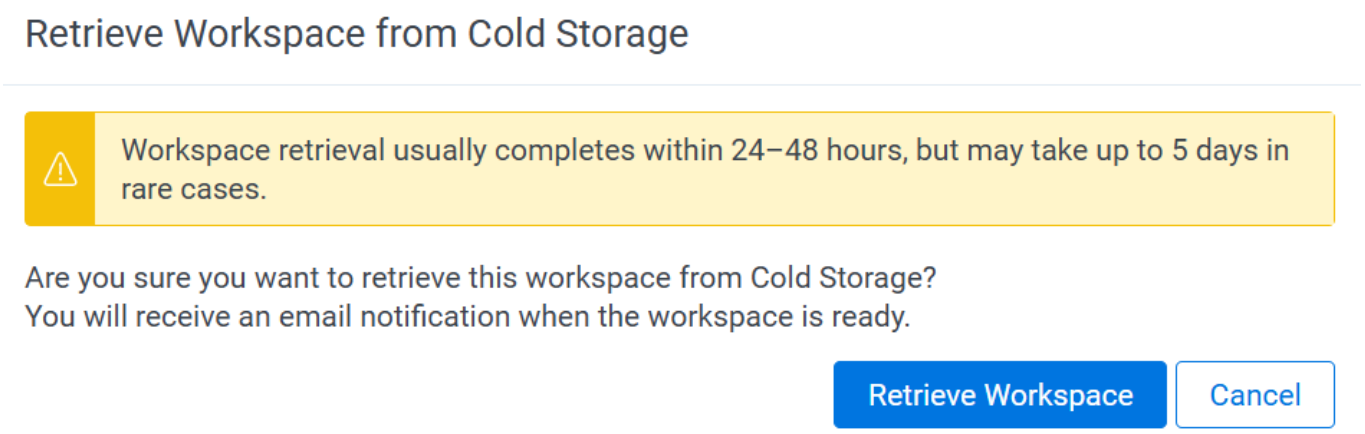
Note: Migrating a workspace to Cold Storage does not impact any active billing period or due date charges for that month. If needed, you can also archive Cold Storage workspaces using ARM without retrieving them first (see Creating and running an Archive Jobsee for more information).

40.13.3 Retrieving a Workspace from Cold Storage

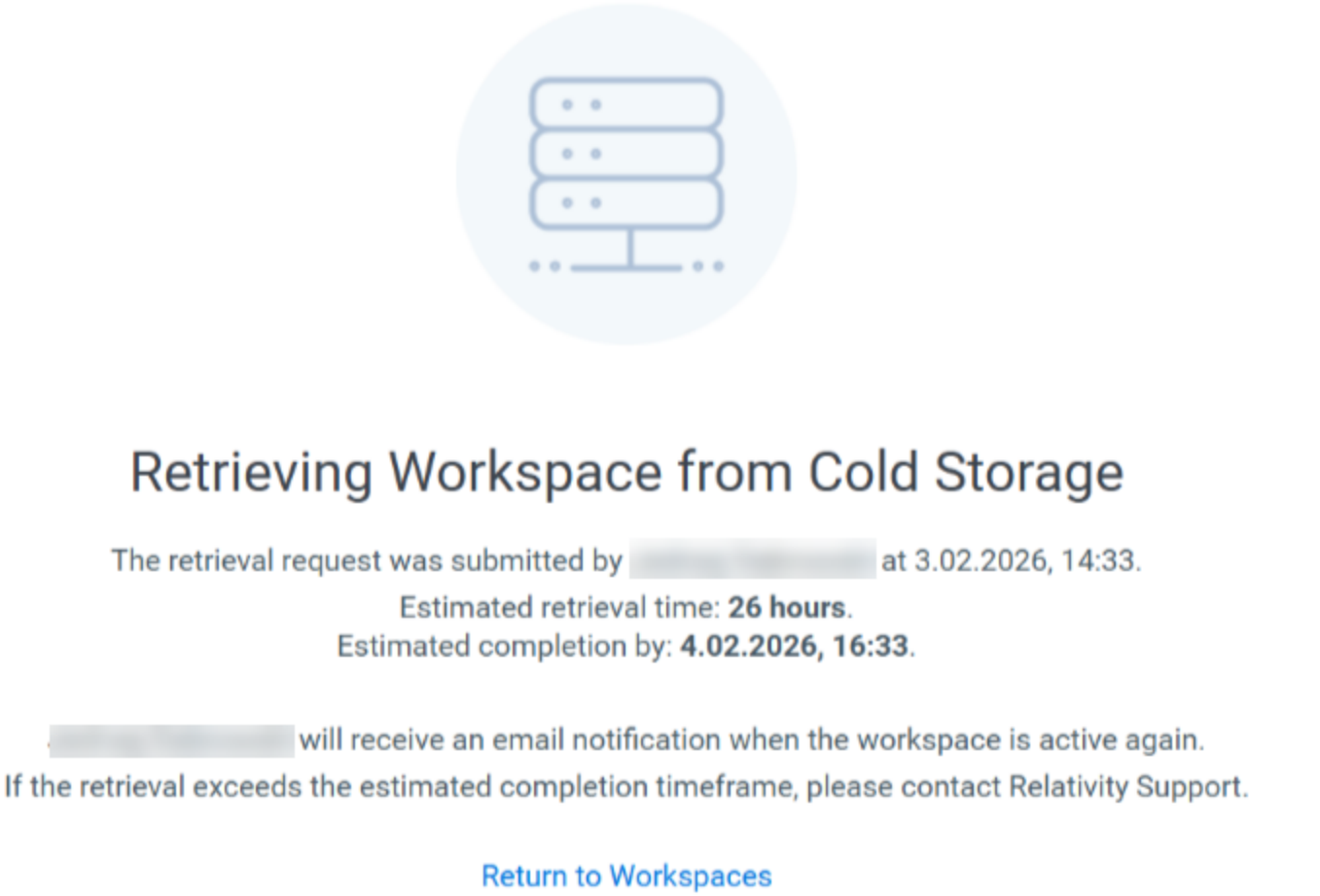
Retrieving a workspace brings it out of Cold Storage back into an active state so users can access it again. You will need the same level of permissions to retrieve a workspace as for migrating one (workspace edit rights and the Manage Cold Storage admin permission). Keep in mind that retrieval is not instantaneous and is a queued operation that requires some time to complete.

To retrieve workspaces from cold storage, follow these steps:

1. Navigate to the **Workspaces** tab.
2. Click the workspace name of the workspace you want to retrieve from cold storage. The Cold Storage Retrieval page displays.
3. Click **Retrieve Workspace** to retrieve the workspace from cold storage. The Cold Storage Retrieval Confirmation pop-up displays.



4. Click **Retrieve Workspace** to retrieve the workspace from cold storage. The Cold Storage Retrieval confirmation page displays. After you submit a retrieval request, the workspace undergoes a restoration process to become active again. **Retrieval occurs asynchronously.** Your request is placed into a queue and handled by back-end Cold Storage services and agents. It will take some time for the workspace to be available.



40.13.3.1 Key points about Cold Storage retrieval:

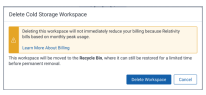
- **Timeline** - *Most* workspace retrievals complete within 24 to 48 hours. However, larger or numerous concurrent retrievals may take longer. 5 days is the maximum time you should expect in normal circumstances. Every retrieval, even for a very small workspace, follows this same timeline and queue process. None are instantaneous.
    - This is an automated process that cannot be sped up or bypassed by support; there is no “expedite” option for Cold Storage retrievals. Once a workspace is in Cold Storage, you must wait for the system to restore it.
- **Plan Ahead** - If you know you will need to use a Cold Storage workspace by a certain date or deadline, initiate the retrieval well in advance of that date. Do not wait until the last minute. It’s recommended to start retrieval at least one full day (24 hours) before you need the workspace active, or even earlier for safety. You should wait for the completion email (see below) before assuming the workspace is available.
- **Progress During Retrieval** - The workspace's Workspace State stays on *ColdStorage* until the restore completes, then changes to Active. To check progress in the meantime, open the workspace from the Workspaces list. The Cold Storage Retrieval page shows the estimated retrieval time and the estimated completion timestamp. Developers can also check retrieval progress programmatically through the Cold Storage Manager REST API's endpoint.
- **Completion Notification** - The user who initiated the retrieval will receive an email notification when the workspace has finished restoring and is active again. Additionally, once complete, the workspace's state will revert to Active in the Workspaces list, and it can be used like any other active workspace.
- **Limitations during Retrieval** - After a retrieval is started, you cannot cancel it mid-process. You also cannot prioritize one workspace's retrieval over another; all requested restores share the same pool of system resources in the queue.

Note: A back-end agent called the **Cold Storage Case Retrieval Agent** must be present and running in your Relativity aiR environment for workspaces to be retrieved from Cold Storage. If a workspace is not coming out of Cold Storage as expected, verify that this agent is enabled. All Cold Storage migration and retrieval actions are logged in the audit history for traceability.

40.13.4 Deleting a workspace from Cold Storage

If you decide a workspace is no longer needed at all, you can delete it after it has been in Cold Storage for at least **30 days**. Relativity aiR enforces this 30-day retention period to prevent accidental or premature deletion of recently archived workspaces.

To delete a workspace that is in Cold Storage, navigate to that workspace’s Cold Storage page (by clicking the workspace name from the Workspaces list). The page will display **a countdown of how many days remain** until deletion is allowed. Once the workspace has been in Cold Storage for the full 30 days, a **Delete Workspace** option becomes available. Clicking **Delete Workspace** will prompt for confirmation, and then move the workspace to the Recycle Bin.



40.13.4.1 Key points about Cold Storage deletion:

- You cannot delete a Cold Storage workspace until the 30-day period has elapsed. The system will not allow it, and the UI will not present a delete option.

- After 30 days in Cold Storage, you may delete the workspace. This will follow the standard deletion safeguards (Recycle Bin retention) that apply to any workspace deletion.
- If you need to free up space or no longer require a workspace's data, but 30 days have not yet passed, you must wait out the period. Planning your Cold Storage usage is important if deletion is a goal.

40.13.5 Frequently Asked Questions (FAQ)

How long does a retrieval take if the workspace is very small?
Even very small workspaces follow the same Cold Storage retrieval process and queue. You should still expect the standard window of about 24–48 hours, up to a maximum of 5 days. Smaller workspaces may end up on the lower end of that timeframe, but none are restored immediately upon request.

Can I retrieve multiple workspaces at the same time?
Yes. You can initiate retrieval for multiple workspaces. Each request is queued independently, but behind the scenes they share the same resources for restoration.

Why can't I track the progress of a Cold Storage restore?
Cold Storage retrieval runs on back-end infrastructure without a user-facing progress bar or status updates API. In the interface, the workspace will simply show Retrieving status until it's done. You will get an email when the process is complete. Relativity aiR currently doesn't offer real-time tracking for this operation.

What should I do if a retrieval is still not complete after 5 days?
It is uncommon for a restore to exceed 5 days. If it does, you should contact Relativity Support for assistance. Provide them with the workspace details (Workspace ID, the date/time you initiated the retrieval, and any relevant screenshots showing the status) so they can investigate the delay.

Can I delete a workspace while it is in Cold Storage?
Not immediately. You can delete a Cold Storage workspace only after 30 days have passed since it was migrated to Cold Storage. Before 30 days, the deletion option is not available. After 30 days, you may delete it (which moves it to Recycle Bin for final disposition). If you need to remove the workspace completely, plan to leave it in Cold Storage for at least 30 days first.

I clicked "Retrieve Workspace" by accident. Can I cancel the retrieval?
No. Once a retrieval is initiated and confirmed, it cannot be canceled mid-process. Even though an accidental click is unlikely due to the confirmation prompt, if you started a retrieval in error, the workspace will still be restored. There is no way to stop it. You'll have to wait for the restore to finish, and then you could potentially migrate the workspace back to Cold Storage again if it's not needed, or simply leave it active.

40.13.6 Troubleshooting Cold Storage Operations

Retrieval exceeds 5 days: If a workspace has not returned to Active status within five days of clicking Retrieve Workspace, gather the relevant details and contact Relativity Support. Provide the Workspace ID, the date and time you initiated the retrieval, and a screenshot of the workspace's status (if available) showing it stuck in "Retrieving." Support can assist in determining if an issue occurred in the restore queue.

Accidental or unnecessary retrievals: As noted, you cannot cancel a retrieval once it's in progress. Always double-check that you truly need to restore a workspace before clicking Retrieve Workspace. (A confirmation dialog is in place to help prevent mistakes.) If you initiate a retrieval in error, you will have to wait until it completes. To avoid this, use Cold Storage planning and communication – for example, clearly label Cold Storage workspaces and ensure team members know not to retrieve them unless necessary.

"Manage Cold Storage" option not visible: If you do not see the Migrate to Cold Storage or Retrieve Workspace options where expected, you likely do not have the required permissions. Confirm that your account or group has the

Manage Cold Storage admin operation and the necessary workspace rights, or have a system admin perform the action (see the Required Permissions section above).

40.13.6.1 Additional Considerations

Use Cold Storage for true long-term inactive workspaces: If a workspace might need to be accessed frequently or on short notice, consider whether Cold Storage is the right choice. Cold Storage is best for workspaces you do not anticipate needing for a while (weeks or months). For short-term holds or pauses, leaving the workspace active (or using a Repository workspace) might be more convenient despite cost. Use Cold Storage primarily to reduce costs for dormant data where some lead time for restoration is acceptable.

Security and auditing: All Cold Storage actions require admin permissions and are tracked. Make sure only authorized personnel manage Cold Storage to prevent unwanted migrations or deletions. Review the audit logs if there's any question about who migrated or retrieved a workspace.

40.14 Recycle Bin

With the Recycle Bin feature, you can recover deleted workspaces within a specified time-frame at no additional cost. It also provides a self-service option for restoring workspaces that have been accidentally deleted, which can minimize downtime and data loss.

40.14.1 Billing and permissions

Workspaces stored in the Recycle Bin do not contribute to monthly billing calculations, ensuring accurate cost considerations.

The Recycle Bin feature is only accessible at the System Administrator level.

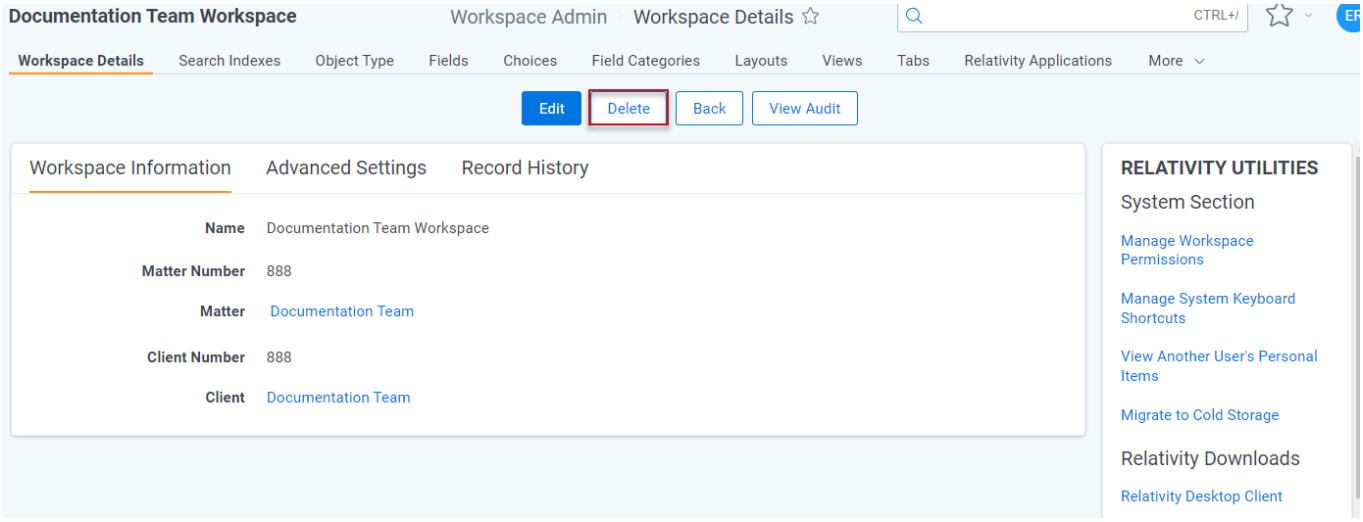
40.14.2 Moving to the Recycle Bin

When you delete a workspace, it is automatically moved to the Recycle Bin, which provides a safety net for deleted workspaces.

You can choose to permanently delete the workspace from the system manually or restore it at any time before the expiration of the seven-day period in the Recycle Bin.

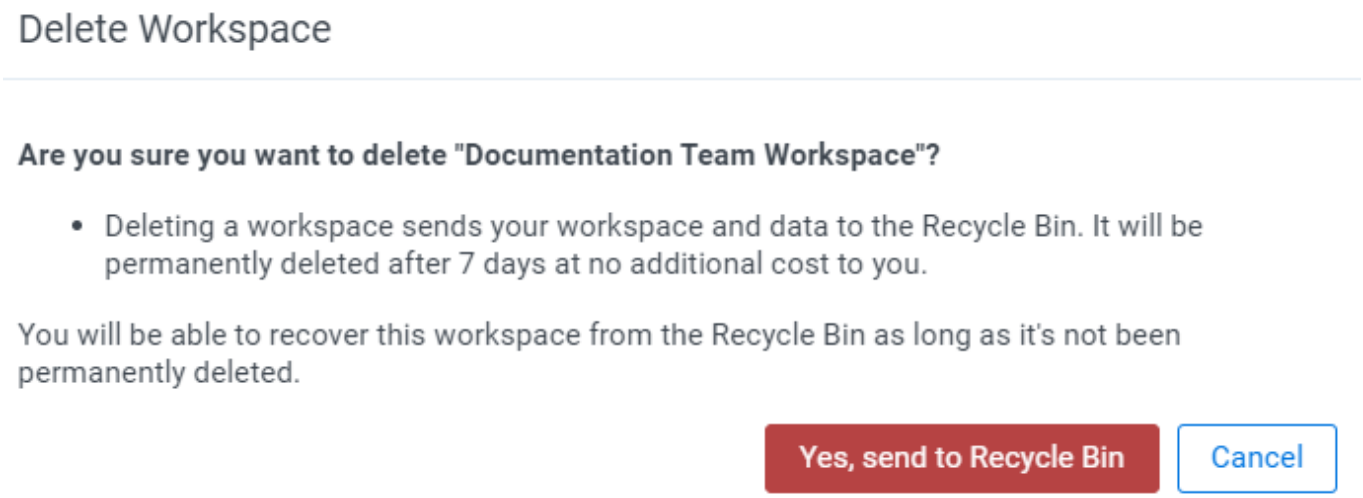
To move a workspace to the Recycle bin, follow these steps:

1. Load the workspace you want to delete.
2. Navigate to the workspace details tab.
3. Click the **Delete** button.



A pop-up window will appear to confirm to moving the workspace to the Recycle bin.

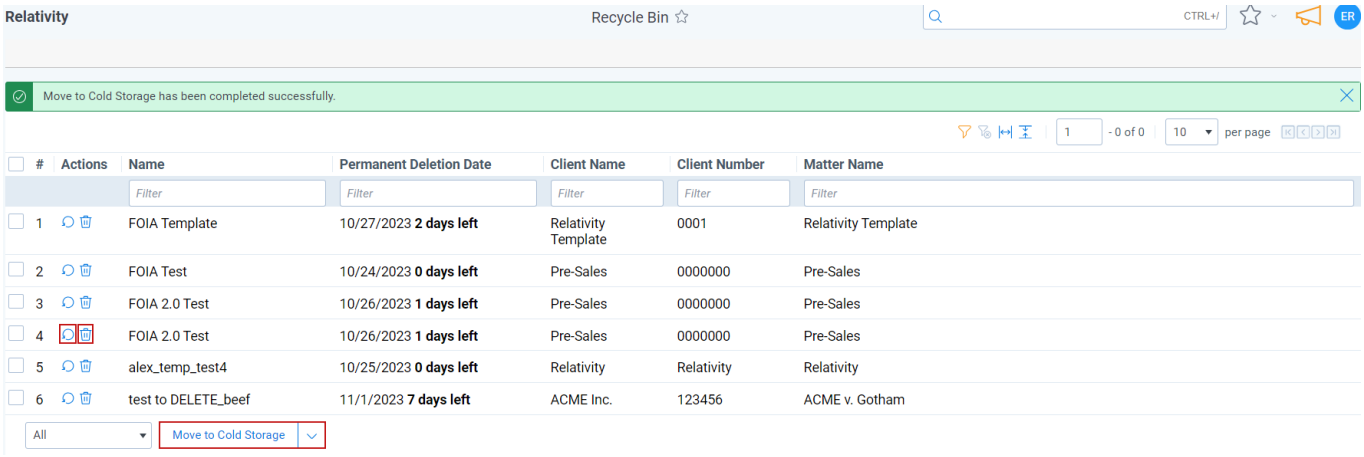
4. Click **Yes, send to Recycle Bin**.



40.14.3 Managing workspaces in the recycle bin

There are three options for workspaces in the Recycle Bin. They can be retrieved, permanently deleted, or moved to Cold Storage.

- To recover a workspace, click the  restore icon.
- To permanently delete a workspace, click the  trash can icon.
- To move one or more workspaces to Cold Storage, click the button below the table.



41 Resources

In addition to this guide, we provide a host of resources to help you use Relativity and its applications.

41.1 Tutorials

Relativity provides video tutorials to teach you the basics of Relativity and its features. You can find the tutorials at https://help.relativity.com/topic.html?t=H6HK2.

41.2 Relativity Community

The Relativity Community is a collection of ideas, discussions, documentation, reports, articles and support tickets that Relativity clients can use to improve their knowledge of the application. Log in to the Relativity Community to search through the numerous resources available to you. Access the Relativity Community at http://rcp.relativity.com/home/home.jsp.

41.3 Relativity Support team

If you need technical assistance or help troubleshooting an issue you are having, please contact our Support team through our Support page.

Note: All customer data is treated as sensitive and confidential. Relativity Support will not accept any customer data from clients for use in Relativity software troubleshooting or software development without explicit permissions from the client. In the rare case where customer data is necessary to troubleshoot the issue, the document troubleshooting will be contained in the Relativity aiR environment on secure region-specific Relativity aiR Jumpboxes.

Proprietary Rights

This documentation ("**Documentation**") and the software to which it relates ("**Software**") belongs to Relativity ODA LLC and/or Relativity's third party software vendors. Relativity grants written license agreements which contain restrictions. All parties accessing the Documentation or Software must: respect proprietary rights of Relativity and third parties; comply with your organization's license agreement, including but not limited to license restrictions on use, copying, modifications, reverse engineering, and derivative products; and refrain from any misuse or misappropriation of this Documentation or Software in whole or in part. The Software and Documentation is protected by the **Copyright Act of 1976**, as amended, and the Software code is protected by the **Illinois Trade Secrets Act**. Violations can involve substantial civil liabilities, exemplary damages, and criminal penalties, including fines and possible imprisonment.

©2026. Relativity ODA LLC. All rights reserved. Relativity® is a registered trademark of Relativity ODA LLC.