# Table of Contents

1 Relativity upgrade overview ............................................................................................................. 7
  1.1 Addressing custom solutions pre-upgrade .................................................................................. 7
  1.2 Addressing custom scripts that trigger imaging jobs ................................................................. 7
  1.3 Required pre-upgrade steps for all Relativity versions ............................................................... 8
    1.3.1 Obtain credentials for service and database accounts ....................................................... 8
    1.3.2 Review system and other requirements ............................................................................. 8
    1.3.3 Apply a trusted certificate for the Analytics server .......................................................... 9
    1.3.4 Back up your Relativity environment ............................................................................... 9
    1.3.5 Reboot machines with Windows updates ......................................................................... 9
    1.3.6 Download the Relativity installer ...................................................................................... 9
  1.4 8.1, 8.2, or 9.x to 9.3 upgrade workflow ..................................................................................... 9
  1.5 8.0 to 9.3 upgrade workflow ..................................................................................................... 10
  1.6 7.x to 9.3 upgrade workflow ..................................................................................................... 10
  1.7 6.x to 9.3 upgrade workflow ..................................................................................................... 10

2 Upgrade considerations for Relativity 9.3 ...................................................................................... 11
  2.1 9.x to 9.3 Relativity updates ...................................................................................................... 11
    Analytics ......................................................................................................................................... 11
    2.1.1 Authentication ............................................................................................................... 12
    Data Grid ..................................................................................................................................... 13
    Fields ........................................................................................................................................... 15
    Imaging profiles ....................................................................................................................... 15
    2.1.2 Installation of a certificate on the database server ............................................................ 16
    2.1.3 Instance settings ............................................................................................................. 16
    2.1.4 New UI framework ........................................................................................................ 16
    2.1.5 Processing ..................................................................................................................... 17
    Production .............................................................................................................................. 19
    2.1.6 Required certificates for Relativity ................................................................................ 21
    2.1.7 Service Host Manager HTTPS configuration ................................................................. 21
    2.1.8 System requirements ................................................................................................... 21
Imaging profiles .................................................................................................................. 35
2.3.2 Installation of a certificate on the database server .................................................. 36
License Relativity and Processing ..................................................................................... 36
2.3.3 New UI framework .................................................................................................. 37
Processing upgrade notes ................................................................................................. 37
Production .......................................................................................................................... 38
RAR upgrade notes ............................................................................................................ 39
2.3.4 Required certificates for Relativity .......................................................................... 39
Viewer ............................................................................................................................... 39
2.3.5 Viewer (ActiveX) ...................................................................................................... 39
2.3.6 Configure the viewer drawing delay ........................................................................ 39
Upgrade custom applications or code .............................................................................. 40
2.3.7 System requirements ............................................................................................... 40
2.3.8 Windows or Integrated Windows authentication .................................................... 40
2.4 6.x to 9.3 Relativity updates ......................................................................................... 41
2.4.1 Analytics .................................................................................................................. 41
2.4.2 Authentication .......................................................................................................... 42
dtSearch index considerations .......................................................................................... 42
Document Table Trigger removal considerations .......................................................... 43
Imaging profiles ................................................................................................................ 43
2.4.3 Installation of a certificate on the database server .................................................. 43
2.4.4 License Relativity ................................................................................................... 44
2.4.5 New UI framework ................................................................................................. 44
Pre-installation steps for web servers ................................................................................ 44
Production .......................................................................................................................... 45
2.4.6 Required certificates for Relativity .......................................................................... 45
2.4.7 System requirements ............................................................................................... 46
Viewer ............................................................................................................................... 46
2.4.8 Viewer (ActiveX) ...................................................................................................... 46
Upgrade agents and other components ........................................................................... 46
2.4.9 Windows or Integrated Windows authentication .................................................... 46
3 Upgrading your primary SQL Server ................................................................. 47
  3.1 Primary SQL Server upgrade ......................................................................... 47
  3.2 Distributed SQL Server upgrade .................................................................. 50
4 Upgrading your agent server .............................................................................. 53
  4.1 Agent server upgrade ................................................................................... 53
  4.2 Service Host Manager HTTPS configuration ............................................... 55
5 Upgrading your web server .................................................................................. 56
  5.1 Web server upgrade ....................................................................................... 56
  5.2 Verifying the machine key settings on the IIS .............................................. 58
  5.3 Upgrading a web server configured for mixed authentication with AD .......... 60
  5.4 Service Host Manager HTTPS configuration .............................................. 61
6 Upgrading a worker manager server installation ............................................... 62
  6.1 Upgrade exceptions ...................................................................................... 62
  6.2 Installing Microsoft Visual C++ Redistributable Packages ......................... 63
  6.3 Upgrading the Invariant Database and Queue Manager ............................... 63
  6.4 Automatically upgrading the worker ............................................................ 63
7 Upgrading workspaces ......................................................................................... 64
  7.1 Monitoring upgrades with the Workspace Upgrade queue ......................... 64
    7.1.1 Populating the Workspace Upgrade queue ........................................... 64
    7.1.2 Workspace Upgrade queue columns .................................................... 65
    7.1.3 Upgrade statuses descriptions .............................................................. 66
  7.2 Editing upgrade priority and order for a workspace ..................................... 66
  7.3 Troubleshooting upgrades ............................................................................ 68
    7.3.1 Viewing upgrade errors ......................................................................... 68
    7.3.2 Canceling or retrying workspace upgrades ........................................... 70
8 Upgrading or installing your Analytics server ....................................................... 71
  8.1 Upgrading your Analytics server .................................................................. 71
  8.2 Running the Analytics installer ...................................................................... 72
  8.3 Upgrading clusters for CAAT 3.17.2 and higher from Relativity 9.1 and below 77
  8.4 Addressing "Could not configure security" installer warning ....................... 80
  8.5 Post-upgrade: Updating the default SSL/TLS certificate for CAAT® ............. 80
1 Relativity upgrade overview

Use the following workflows to upgrade your current Relativity installation to Relativity 9.3. To begin your upgrade process, address custom solutions and scripts before downloading the Relativity installer. Once you complete the workflow specific to your upgrade path, we recommend completing the post-installation verification tests post-upgrade to confirm that your environment has been upgraded properly.

As a best practice, we recommend preparing for your upgrade process by using the Pre-Upgrade Checklist. You can use this document to discuss an upgrade strategy for your current installation of Relativity with the Client Services team (support@relativity.com).

If you are installing Relativity for the first time, contact the Client Services team (support@relativity.com) for additional information. You may also want to review the information on the Relativity installation page on the Relativity 9.3 Documentation site.

1.1 Addressing custom solutions pre-upgrade

Before upgrading, consider that your environment may contain custom components that are not compatible with your new version of Relativity.

Custom components may include scripts, event handlers, agents, applications, or in-house developed code that is not part of a standard Relativity deployment.

To help you address potential compatibility issues, you can run a script prior to upgrade that identifies the custom components developed by kCura Custom Development.

There are currently three versions of this script available in the Relativity Community:

- Relativity - KCD Solution Snapshot - 8.0 - 9.3
  
  **Note:** This version is also compatible with Relativity 9.4.

- Relativity - KCD Solution Snapshot - 7.5
- Relativity - KCD Solution Snapshot - 7.0-7.4

  **Note:** For the 7.0-7.4 and 7.5 versions of the KCD Solution Snapshot, contact Client Services at support@relativity.com.

To access these scripts, log in to the Relativity Community and search for "KCD Solution Snapshot.” Make sure to run the script and send the results to support@relativity.com for analysis several weeks before your planned upgrade.

1.2 Addressing custom scripts that trigger imaging jobs

If you plan on upgrading to Relativity and you use custom scripts that programmatically trigger imaging jobs in your current Relativity environment, those scripts will no longer work after you upgrade.

This is because the components that those custom scripts rely upon no longer exist due to the changes made to the imaging framework, which are listed below. The imaging operations performed by these custom scripts aren’t accounted for in the KCD Snapshot Solution script.
The Imaging Set Manager and Worker agents have been deprecated.
The Imaging Set Queue table has been deprecated.
The Imaging API now submits an imaging job directly to Invariant (worker manager server).

Before you upgrade to Relativity 9.3, contact Client Services at support@relativity.com for instructions on how to adjust your custom scripts.

1.3 Required pre-upgrade steps for all Relativity versions

Before you begin your upgrade, you must complete the following pre-upgrade steps.

Required pre-upgrade steps for all Relativity versions
Complete the following steps and verify you have the necessary information required for all upgrades of Relativity. Depending on your upgrade path, you may have additional configuration or other tasks to perform specific to the version of Relativity you're installing.

Make sure you have the appropriate System Admin permissions in Relativity before beginning the upgrade. For more information, see Managing security on the Relativity 9 Documentation site.

Confirm that jobs aren't running in any of the queues. If the agents are running, they may attempt to run a job against a database that doesn't have an upgraded schema and cause serious errors in your Relativity environment.

1.3.1 Obtain credentials for service and database accounts

To upgrade Relativity, you need credentials for the following accounts:

- **Relativity Service account** (Windows Workgroup/Domain account) - Run the Relativity upgrade logged in as the Relativity Service account. This account must have local Administrator permissions on the target server, and SQL sysadmin role privileges on the SQL Server.
- **EDDSDBO account** (SQL account)

**Note:** Do not begin the upgrade process until you obtain the credentials for these accounts. They are required when you run the installer.

1.3.2 Review system and other requirements

Confirm that your environment is configured with the prerequisites before you begin upgrading Relativity. See the following documents for more information:

- Relativity System Requirements - Includes software and hardware requirements for servers, databases, and other components of a Relativity installation.
- Relativity Workstation Configuration guide - Includes information about setting up workstations for users and viewer installation instructions.
- Relativity Environment optimization guide - Includes best practices for maintaining and optimizing a Relativity environment.
- Upgrade path instructions - Contain detailed information about requirements for your specific upgrade path.
1.3.3 Apply a trusted certificate for the Analytics server

As of Relativity 9.3, a trusted certificate is required for all HTTPS traffic, including the internal traffic for the Analytics server. We recommend placing the certificate and testing it after the upgrade to Relativity 9.3. See [Post-upgrade: Update the default SSL/TLS certificate for CAAT®](https://www.relativity.com/support/post-upgrade-update-the-default-ssl-tls-certificate-for-caat) for more information.

1.3.4 Back up your Relativity environment

Back up your SQL databases and your Relativity IIS websites before you begin the upgrade process. You should also back up both the structured analytics sets and analytics indexes before your upgrade to ensure that there is no data loss. This may take a while so it's recommended to run analytics backups either during the week of or the week prior to your upgrade. Usually this data does not change daily, so this helps to mitigate any data loss.

1.3.5 Reboot machines with Windows updates

After installing Windows updates, reboot your machines before attempting to install Relativity. Complete this step to ensure that all Relativity components are properly installed. Incomplete Windows updates lock system files, which may cause silent failures and prevent the proper installation of Relativity components.

1.3.6 Download the Relativity installer

To receive the correct Relativity installer package for your upgrade workflow contact the Client Services team (support@relativity.com).

1.4 8.1, 8.2, or 9.x to 9.3 upgrade workflow

Use the following workflow when upgrading from Relativity 8.1 or 8.2 to Relativity 9.3.

**Note:** Never upgrade your Relativity version while there are jobs of any type currently in progress in your environment. Doing this leads to inaccurate results when you attempt to finish those jobs after your upgrade is complete. This is especially important for imaging and processing jobs.

8.x & 9.x to 9.3 upgrade workflow

1. Stop all agent services.
2. Stop the IIS.
3. Run the Relativity installer on your [Upgrading your primary SQL Server on page 47](https://www.relativity.com/support/upgrading-your-primary-sql-server) on the Primary SQL Server to upgrade the EDDS database and install the required library applications. You can’t access your Relativity environment until you complete this step. Depending on what version you’re upgrading from, this process may start automatically after the installer is finished running..
4. Run the Relativity installer on the Agent server. See [Upgrading your agent server on page 53](https://www.relativity.com/support/upgrading-your-agent-server).
5. Run the Relativity installer on the Web server. See [Upgrading your web server on page 56](https://www.relativity.com/support/upgrading-your-web-server).
6. Restart the IIS.
7. (Optional) Log in to Relativity and click the **Workspace Upgrade queue**. Set the priority or order on the workspaces as necessary. For more information, see Upgrading workspaces on the on the
Relativity 9.3 Documentation site. You can monitor your workspaces in the Monitoring upgrades with the Workspace Upgrade queue on page 64.

Note: After you run the installer on at least one agent server, the system begins upgrading individual workspaces. You can now log in to Relativity to monitor workspace upgrades via the Workspace Upgrade queue.

8. Upgrade your worker manager server. See worker manager server Installation guide.

9. Upgrade Relativity Analytics. See Upgrading or installing your Analytics server on page 71.

1.5 8.0 to 9.3 upgrade workflow

Please contact the Client Services team (support@relativity.com) for more information on upgrading your 8.0 Relativity environment to Relativity 9.

1.6 7.x to 9.3 upgrade workflow

Please contact the Client Services team (support@relativity.com) for more information on upgrading your 7.x Relativity environment to Relativity 9.

1.7 6.x to 9.3 upgrade workflow

Please contact the Client Services team (support@relativity.com) for more information on upgrading your 6.x Relativity environment to Relativity 9.
2 Upgrade considerations for Relativity 9.3

This page explains some of the key changes in Relativity 9.3 that you should be aware of before upgrading.

Refer to this page to learn more about changes in your environment from a previous version of Relativity to Relativity 9.3.

2.1 9.x to 9.3 Relativity updates

Learn more about the changes that occur to your Relativity 9.x environment after you upgrade to Relativity 9.3.

9.x to 9.3 Relativity updates

- Analytics below
- Authentication on the next page
- Data Grid on page 13
- Fields on page 15
- Imaging profiles on page 15
- Installation of a certificate on the database server on page 16
- Instance settings on page 16
- New UI framework on page 16
- Processing on page 17
- Production on page 19
- Required certificates for Relativity on page 21
- Service Host Manager HTTPS configuration
- System requirements on page 21
- Viewer (ActiveX) on page 22
- Viewer (ActiveX and HTML) on page 22
- Windows or Integrated Windows authentication on page 23
- Worker manager queue on page 23
- Telemetry

Analytics

Upon upgrade to Relativity 9.2 and above, the Textual Near Duplicate Identification algorithm is in place with the following benefits:
The new algorithm greatly improved performance for both large and complex data sets.

With the new algorithm you can scale your Analytics server by adding CPU cores and RAM in order to achieve faster performance.

Prior to Relativity 9.2, scaling environments did not impact performance. Without scaling past eight cores, you should experience performance comparable to pre-Relativity 9.2 on most data sets. The Textual Near Duplicate Identification algorithm in Relativity 9.2 uses different, more efficient methods to obtain similar results. However, results may differ slightly from pre-Relativity 9.2 results if a Full Analysis is run against a preexisting structured analytics set. If you need preexisting results use an Incremental Analysis instead. The incremental analysis keeps the pre-Relativity 9.2 results for all preexisting documents, but the newly added documents use the new algorithm to match with existing groups.

**Updating the default SSL/TLS certificate for Content Analyst**

You must update the default SSL/TLS certificate on your Analytics server because Relativity requires a certificate signed by a trusted certificate authority (CA). By default, the CAAT service runs over an untrusted SSL/TLS certificate. For more information, see Post-upgrade: Updating the default SSL/TLS certificate for CAAT® on page 80.

### 2.1.1 Authentication

Relativity 9.3.452.1 introduces significant user authentication changes. Consider the following for upgrading:

- You no longer see the AuthenticationData field in the Users User Information section. You now enter the information you previously entered here in the individual authentication methods. This permits more versatile and detailed method implementations.

- Note that when you upgrade, Relativity creates a copy of the eddsdbo.User table before making any modifications. The table is for reference only, and the copy is named based on the Relativity version being upgraded from, such as 9_2_AuthenticationUserTableBackupRecord. If after upgrading and making sure all users converted successfully, you may delete the copy table.

- Use the Authentication Profile system to enable only the protocols you need in an environment. In some cases the upgrade process may enable more protocols than you want. This is due to the parsing rules for the AuthenticationData column. Specifically, if you are using Active Directory or Client Certificate authentications in your environment, the upgrade process may also enable Integrated Authentication. If you don't want the Integrated Authentication, you can remove that provider from the Authentication Profile after upgrade.

#### 2.1.1.1 User and authentication object permissions

With authentication enhancement in Relativity 9.4, a number of new objects have been introduced, such as Authentication Provider Type, Authentication Provider, and Login Method. Upon upgrading to Relativity 9.4, permissions are as follows:

- A user, who has the permissions to view the user objects before an upgrade, post upgrade can view users, authentication provider types, authentication providers, and login methods.

- A user, who has the permissions to edit (or delete, a higher level of permission than edit) the user objects before an upgrade, post upgrade can edit users and login methods. They can also view authentication provider types, and authentication providers.
After upgrade only users in the System Administrators group will have access to view and edit OAuth2Client objects.

Data Grid
The following items are new to Data Grid beginning in Relativity 9.3.376.35:

- Beginning in Relativity 9.3.376.35, Shield is supported for Relativity Data Grid. For more information, see Configuring Shield authentication.
- The new audit template available in Relativity 4.3.361.5 provides a way to prevent mapping errors during audit migration. If you are upgrading to Relativity 9.3.376.35 from a version before Relativity 9.3.332.21, you need to follow alternate steps to update your audit template. For more information, see Updating the Audit template.

Beginning in Relativity 9.3.297.13, Elasticsearch 2.1.2 is supported for Relativity Data Grid. This means that you have the option of installing Elasticsearch 2.1.2 or upgrading from 1.7.x to 2.1.2 beginning in Relativity 9.3.297.13. For more information, see Upgrading from Data Grid 1.7.x to 2.1.2.

The following infrastructure items are new to Data Grid™ beginning in Relativity 9.3:

- The new Data Grid Kepler Host agent is responsible for running the Data Grid Kepler Server. This agent is part of the Data Grid Core application and as such is automatically installed when one upgrades to or installs Relativity 9.3. This agent is configured to be limited to only one agent per server.
For more information, see the Relativity Data Grid guide.

- The Instance Settings table and corresponding Relativity tab now include the ServiceHTTPEndPoint and ServiceHTTPEndPointPort settings to accommodate the connection between the Kepler service and Data Grid services.
For more information, see the Relativity Data Grid guide

**Fields**

2.1.1.2 Allow HTML fields

Starting in Relativity 9.3, for any existing fields with the Allow HTML value set to Yes, you must set the new instance setting SanitizeHTMLOutput to False in order to add HTML alerts and links when a user opens a document for review.

**Imaging profiles**

Existing imaging profiles receive the following updates based on their imaging method when upgrading to Relativity 9.3.

If your environment is set up for native imaging, the following changes occur upon upgrade:

- Relativity renames the default imaging profile to Native Default.
- The imaging method is set to Native for all current imaging profiles including Native Default.
- Relativity creates a new basic default imaging profile with the following settings:
  - Imaging Method: Basic
  - Basic Image Output Quality (DPI): 300
  - Basic Image Format: TIFF
  - Basic Image Height: Original Setting

- For any imaging set with an imaging method set to basic, the following changes occur:
  - The imaging profile previously linked to the imaging set is copied.
  - Relativity sets the imaging method for the copied profile to basic.
  - The copied basic imaging profile is linked to the imaging set and is appended with Basic to the front of the name.

If your environment is not set up for native imaging, the following changes occur upon upgrade:

---

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Value</th>
<th>Description</th>
<th>Section</th>
<th>Machine Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Edit</td>
<td>ServiceHttpEndpoint</td>
<td>HTTP EndPoint For Access Data Grid Services</td>
<td>Relativity/DataGrid</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Edit</td>
<td>ServiceHttpEndPointPort</td>
<td>Port which will be used by Data Grid Kepler Service Default Port 6005</td>
<td>Relativity/DataGrid</td>
<td></td>
</tr>
</tbody>
</table>

Viewing the First 2 of 2 items in sets of 25 per page
Relativity renames the default imaging profile to Basic Default.

- The imaging method is set to basic for all current imaging profiles including Basic Default.

### 2.1.2 Installation of a certificate on the database server

The Relativity 9.3 installer adds a certificate called RelativityIdentityCertificate to the EDDS database on your primary database during a first time installation or an upgrade. The authentication framework uses the thumbprint of the certificate to sign identity tokens, which are JSON web tokens (JWTs). The IdentityCertificateThumbprint instance setting stores the thumbprint associated with your certificate. For more information, see Instance setting values on the Relativity 9.3 Documentation site.

You also have the option to use your own authentication token-signing certificate. For more information, see Optionally configure an authentication token-signing certificate on the Pre-installation page in the Relativity 9.3 Documentation site.

For a clustered environment, you need to export a copy of your RelativityIdentityCertificate from the primary database server, and install the certificate to each database server hosting the EDDS. See the following instructions for more information:

- Optionally configure an authentication token-signing certificate on the Pre-installation page in the Relativity 9.3 Documentation site - These instructions describe the process for configuring your own custom token-signing certificate, but you can follow these basic steps to install RelativityIdentityCertificate to each database server in a distributed environment.

### 2.1.3 Instance settings

Beginning in Relativity 9.3, configuration table values are now referred to as instance settings. Upon upgrade to 9.3, configuration table values convert to instance settings. Likewise, the eddsdbo.Configuration table becomes the eddsdbo.InstanceSetting table in SQL Server.

**Note:** If a new 9.3 install or upgrade fails, a back up table, edds.Configuration_backup, exists as a record of all the instance settings in SQL. Do not use this table for any purpose other than a record in the event of an install/upgrade failure.

### 2.1.3.1 Backwards compatibility

For any existing applications that reference the pre-9.3 EDDS.Configuration table, a SQL view, Configuration, exists to act as a layer on top of the Instance Setting table.

This view contains the same columns as the old Configuration table and you can use it to examine the information as it was pre-Relativity 9.3.

### 2.1.4 New UI framework

Relativity 9.3 introduces a new UI framework, which is turned off by default. If you want to enable the new UI framework for the Document list, click **Switch to New UI** from the user drop-down within a workspace. For more information, see Navigation in the Admin guide. When you enable the new UI framework, the following Relativity features update with the new framework:
Cluster visualization
Dashboards
Document list and tabs throughout Relativity
Pivot
Sampling
Search panel and search browser

2.1.5 Processing
The following infrastructure items are new to processing in Relativity 9.3:

- Beginning in Relativity 9.3, you must enable token authentication on your web server for certain Relativity features, such as the worker manager server, which requires this authentication type for processing.

  If you're upgrading to Relativity 9.3 from 9.2 or lower, you must edit the ProcessingWebAPIPath Instance Setting. This setting identifies the URL that directs to the Relativity token-authenticated endpoints that Invariant uses to process files. Processing requires this URL and a Relativity admin must enter it.

  To do this, perform the following steps to comply with this change:

  - While in Home mode, navigate to the Instance Settings tab.
  - In the default All Instance Settings view, enable filters and enter ProcessingWebAPIPath in the Name field.
  - Click the ProcessingWebAPIPath name and click Edit in the instance setting layout.
In the **Value** field change the existing ProcessingWebAPI URL to the RelativityWebAPI URL.

Click **Save**.

If you're installing Relativity 9.3 for the first time as a fresh installation and not an upgrade, you need to enable the RelativityWebAPI setting in IIS for Anonymous authentication in order to publish documents to a workspace.

To do this, perform the following steps:

- Open IIS.
- To enable anonymous authentication, complete the following steps:
  - Click on the **RelativityWebAPI** site.
  - In the Features view, click **Authentication**.
  - In the Authentication view, right-click on **Anonymous Authentication** and click
To update the web.config file, locate it in the following folder: C:\Program Files\kCura Corporation\Relativity\WebAPI
Open the file in an editor. Update the authentication mode and authorization sections as follows:

```xml
<system.web>
  <authentication mode="None" />
  <authorization><allow users="*" /></authorization>
</system.web>
```

- Restart the IIS.

The CompressMetadata flag, which is an Invariant setting that controls how metadata is saved to the database, is enabled by default starting in Relativity 9.3.332.21. Making this flag enabled provides ingestion performance improvements and reduces the size of your store databases. To assist with troubleshooting and to give you control over this setting, there is a new entry in the AppSettings table called CompressMetadata, which by default, has CompressMetadata enabled for when you create a new store either through Relativity or the RPC. To disable CompressMetadata, set this value to 0 (false/disabled).

Note that the CompressMetadata flag is also set on all of your Invariant stores when you upgrade to Relativity 9.3.332.21. If you need to disable metadata compression on any of your stores, you must manually change the value from 4 (true/enabled) to 0 (false/disabled).

Contact Support at support@relativity.com if you need assistance determining when to disable metadata compression on your stores.

**Production**

The following section discusses the changes to the Production application on upgrade from Relativity 9.x to Relativity 9.3. Certain upgrade changes only affect upgrades from Relativity 9.1 or 9.2 to Relativity 9.3, and the changes are clearly marked with the affected versions.
Beginning in Relativity 9.3.332.21 you can choose to upgrade only your Production application using a RAP file. For more information, see the Admin Guide.

**General Production upgrade considerations:**

- An upgrade can fail if the workspace you're upgrading already contains a Relativity dynamic object with the name Production Placeholder. You must rename this object.
- An upgrade from Relativity 9.1 to 9.3 can fail if the workspace you're upgrading already contains a Relativity dynamic object with the name Production Data Source.
- An upgrade from Relativity 9.2 and below to 9.3 can fail if the workspace you're upgrading already contains a Relativity dynamic object with the name Relativity Color Map. You must rename this object.
- An upgrade from Relativity 9.2 and below to 9.3 can fail if the workspace you're upgrading already contains a Relativity dynamic object with the name Field Catalog. You must rename this object.
- If you have a full-text index populating the production upgrade stops. Try upgrading again once the full-text index is finished populating.
- Relativity deduces the First Bates Value and Last Bates Value for all imported and upgraded productions.
- If you are updating your Production application to a version of Relativity 9.3 before 9.3.297.13, the upgrade can fail if you update the Binders application before it. Update the production application first or upgrade to 9.3.297.13.
- If you upgrade from Relativity 9.2 to Relativity 9.3 and you were previously using the Production Tracker application, review the Production Tracker 9.3 considerations PDF in the Relativity Community.

**Changes to agents and objects:**

- On upgrade to Relativity 9.3 the Relativity.Core agents for production and branding are upgraded to ADS Deployed agents. The Relativity.Core agents for production and branding are not available in a 9.3 environment.
- The Markup Set table is converted to the Markup Set dynamic object.
- The Production Object table is converted to the Production dynamic object.

**Changes to pre-existing Productions:**

- Any staged or errored productions in an environment are set to a status of New and you must restage the production before running.
- Productions migrated from Relativity 9.1 and 9.2 receive a legacy placeholder stating, "No Tiff Included For This Record."
- Productions migrated from Relativity 9.1 to Relativity 9.3 have a data source created containing the production documents for each produced and errored production.
- If any produced productions contain native files with their Bates numbers previously stored in the Document table, the Bates numbers for the native files are moved to the Production object, and may not reflect actual Bates values if those values were overwritten.
- The Production Error field no longer exists on the Production object.

- If you upgrade from an earlier version of Relativity 9.3 and your custom placeholders contain square brackets, you may see an error the next time you run the production or re-save the custom placeholder. To correct the error, escape the square brackets using a backslash and re-run the production.

**Changes to Production fields and views:**

- On upgrade from 9.2 to 9.3 the Produced Documents field exists in the environment, but the field is not populated.
- The production document view no longer exists.
- The multi-object field Produced Documents is replaced with the Production Information RDO when upgrading from Relativity 9.2. The field is not deleted from the workspace, but is disassociated from the production application.

- On upgrade from 9.x to 9.3 the Add Image Placeholder field changes to Use Image Placeholder. If the Add Image Placeholder field was set to no, it updates to Never Use Placeholders. If the Add Image Placeholder field was set to yes, it updates to Always Use Image Placeholders.

**Changes to Production permissions:**

- Users with full permissions to the Production object prior to upgrading to Relativity 9.3 do not automatically gain permissions to the new Production Data Source object, unless they also have the Manage Object Types permission under Admin Operations. Users need rights to the new Production Data Source object to add or edit production data sources after upgrading to Relativity 9.3.

### 2.1.6 Required certificates for Relativity

Relativity 9.3 now verifies that all HTTPS services running in your environment have a trusted certificate. You need to verify the certificates to components of your Relativity installation running HTTPS services to avoid error messages and insecure-connection icons. For more information, see Required certificates for Relativity in the Pre-installation guide.

We recommend placing the new Analytics server certificate and testing it prior to the day of the upgrade to Relativity 9.3. For more information, see Pre-upgrade: Update the default SSL/TLS certificate for CAAT® in the Upgrading or installing your Analytics server section.

### 2.1.7 Service Host Manager HTTPS configuration

Service Host Manager runs Relativity services on all web and agent servers in your environment. The services are used by applications like Production and Processing on. Starting with Relativity 9.3.362.9 (March 30, 2016 update), special setup is required for HTTPS access to web and agent servers.

For more information, see Service Host Manager on the Relativity 9.3 Documentation site.

### 2.1.8 System requirements

- Upon upgrade to Relativity 9.3, Windows Server 2008 R2 (64-bit) is no longer compatible with 9.3. Relativity 9.3 is only compatible with Windows Server 2008 R2 (64-bit) w Service Pack 1.
As of August 31, 2017, we no longer support Internet Explore (IE) 10. Please upgrade to a compatible version of IE 11.

2.1.9 Viewer (ActiveX)
To use the ActiveX viewer in Relativity 9.3 you must have Microsoft .NET 4.5.1 runtime installed on the client machine.

2.1.10 Viewer (ActiveX and HTML)
For users who haven’t upgraded their Relativity version since the general release of Relativity 9.2, note that, beginning in the Relativity 9.2.337.3 - September 30, 2015 product update, the following is applicable.

When viewing documents with an .HTM, .HTML, or .XML extension in Native mode, the viewer displays the raw file markup instead of rendering the content.

You can control this option with the TreatHtmlAndXmlAsText instance setting, which is set to True by default. When set to "True", this prevents JavaScript from executing when viewing these documents in the Native mode in the viewer. See the Instance Setting Guide to learn more about this new value.

Pre the Relativity 9.2.337.3 - September 30, 2015 product update:

As of the Relativity 9.2.337.3 - September 30, 2015 product update:
2.1.11 Windows or Integrated Windows authentication

If your Relativity installation currently uses Windows authentication or Integrated Windows authentication, you must set the UseWindowsAuthentication instance setting to True after upgrading your environment. For more information, see the Instance setting guide on the Relativity 9.3 Documentation site.

You may want to configure your environment so that some servers use Windows authentication, while others don’t use it. In this case, you need to add another row for this instance setting to the Instance setting table, update the machine name in this new row, and then set the value to True or False based on the Windows authentication requirements for the server.

In addition, you can set the WindowsAuthIpRange instance setting, which specifies a group of IP addresses that Relativity uses to validate the address of the user during login. If a request originates from an IP address added to the WindowsAuthIpRange instance setting, the server uses Windows Authentication to log the user in to Relativity. Relativity uses forms authentication to log in the user, when the IP address is outside the specified range. For more information, see Instance settings on the Relativity 9.3 Documentation site.

2.1.12 Worker manager queue

Beginning in Relativity 9.2.337.3 (released on September 30, 2015), revisions in the queue manager code have led to the following enhancements:

- A reduction in the volume of connections to the SQL server
- A reduction in lock waits and thread pool waits
- A general increase in queue parallelism
- A reduction in the number of queries per second hitting the SQL server
There is no reduction or change in actual queue functionality as a result of these changes. Likewise, the user experience with the queue manager hasn’t changed, with the exception of potential performance increases, depending on the size of your environment.

No additional server configurations, or other such action items, are required beyond upgrading to Relativity 9.2.337.3 in order to procure the improved queue manager.

2.1.13 Telemetry
After you install Relativity, complete the steps to enable telemetry in your environment. Telemetry allows you to collect metrics for performance, usage, and billing. For more information, see Telemetry on the Relativity 9.3 Documentation site.

2.2 8.x to 9.3 Relativity updates
Learn more about the changes to your Relativity 8.x environment after you upgrade to Relativity 9.3.

- Agents on the next page
- Analytics 9.3 upgrade on the next page
- Authentication on the next page
- Data Grid on page 26
- Document table trigger removal on page 28
- Imaging profiles on page 28
- Imaging sets on page 29
- Installation of a certificate on the database server on page 29
- New UI framework on page 29
- Performance baselines and recommendations on page 29
- Processing on page 30
- Production on page 30
- Required certificates for Relativity on page 31
- Servers on page 31
- Service Host Manager HTTPS configuration on page 31
- Structured Analytics on page 32
- System requirements on page 32
- Viewer on page 32
- Windows or Integrated Windows authentication on page 32
- Workspaces on page 32
Agents
With the introduction of the new viewer, the following agents have been removed in Relativity 9.3:

- Imaging set manager
- Imaging worker

The work of processing, document conversion, imaging set, image-on-the-fly, and mass imaging jobs are performed by workers, which you can add in the Servers tab. For more information, see the Servers section of the Relativity Admin Guide.

Analytics 9.3 upgrade
When you run the Relativity Analytics Server Setup wizard, the wizard automatically:

- Installs the CAAT service
- Deploys the Relativity library files
- Configures the java heap size (set by default to half of RAM)
- Allows you to set an index path on new install, thus eliminating the need to manually set the location of indexes
- Sets the CAAT Windows service to log in as the Relativity Service Account

For more information, see Upgrading or installing your Analytics server on page 71.

Updating the default SSL/TLS certificate for the Content Analyst
You must update the default SSL/TLS certificate on your Analytics server because Relativity requires a certificate signed by a trusted certificate authority (CA). By default, the CAAT service runs over an untrusted SSL/TLS certificate. For more information, see Post-upgrade: Updating the default SSL/TLS certificate for CAAT® on page 80.

2.2.1 Authentication
Relativity 9.3.452.1 introduces significant user authentication changes. Consider the following for upgrading:

- You no longer see the AuthenticationData field in the Users User Information section. You now enter the information you previously entered here in the individual authentication methods. This permits more versatile and detailed method implementations.

- Note that when you upgrade, Relativity creates a copy of the edd MDB. User table before making any modifications. The table is for reference only, and the copy is named based on the Relativity version being ungraded from, such as 9_2_AuthenticationDataBackupRecord. If after upgrading and making sure all users converted successfully, you may delete the copy table.

- Use the Authentication Profile system to enable only the protocols you need in an environment. In some cases the upgrade process may enable more protocols than you want. This is due to the parsing rules for the AuthenticationData column. Specifically, if you are using Active Directory or Client Certificate authentications in your environment, the upgrade process may also enable Integrated Authentication. If you don’t want the Integrated Authentication, you can remove that provider from the Authentication Profile after upgrade.
Data Grid

The following items are new to Data Grid beginning in Relativity 9.3.376.35:

- Beginning in Relativity 9.3.376.35, Shield is supported for Relativity Data Grid. For more information, see Configuring Shield authentication.

- The new audit template available in Relativity 4.3.361.5 provides a way to prevent mapping errors during audit migration. If you are upgrading to Relativity 9.3.376.35 from a version before Relativity 9.3.332.21, you need to follow alternate steps to update your audit template. For more information, see Updating the Audit template.

Beginning in Relativity 9.3.297.13, Elasticsearch 2.1.2 is supported for Relativity Data Grid. This means that you have the option of installing Elasticsearch 2.1.2 or upgrading from 1.7.x to 2.1.2 beginning in Relativity 9.3.297.13. For more information, see Upgrading from Data Grid 1.7.x to 2.1.2.

The following infrastructure items are new to Data Grid beginning in Relativity 9.3:

- The new Data Grid Kepler Host agent is responsible for running the Data Grid Kepler Server. This agent is part of the Data Grid Core application and as such is automatically installed when one upgrades to or installs Relativity 9.3. This agent is configured to be limited to only one agent per server.
For more information, see the Relativity Data Grid guide.

- The Instance Settings table and corresponding Relativity tab now include the ServiceHTTPEndpoint and ServiceHTTPEndpointPort settings to accommodate the connection between the Kepler service and Data Grid services.
For more information, see the Relativity Data Grid guide

**Document table trigger removal**

If you're upgrading from Relativity 8.1, note that 8.1 included enhancements that may affect certain areas of your existing environment when you upgrade. Improvements to the database schema make Relativity run faster in 9 than in previous versions. If your environment contains custom-developed functionality that involves the RelationalIndex_X tables or explicitly uses the RI_X columns in the Document tables, then you should refer to the Document table trigger removal documentation.

**Imaging profiles**

Existing imaging profiles receive updates based on their imaging method when upgrading to Relativity 9.3.

If your environment is set up for native imaging, the following changes occur upon upgrade:

- Relativity renames the default imaging profile to Native Default.
- The imaging method is set to Native for all current imaging profiles including Native Default.
- Relativity creates a new Basic Default imaging profile with the following settings:
  - Imaging Method: Basic
  - Basic Image Output Quality (DPI): 300
  - Basic Image Format: TIFF
  - Basic Image Height: Original Setting
- For any imaging set with it an imaging method set to Basic, the following changes occur:
  - The imaging profile the imaging set was linked to is copied.
  - Relativity sets the copied profile’s imaging method is set to Basic.
  - The copied profile is appended with Basic to the front of the name.

If your environment is not set up for native imaging, the following changes occur upon upgrade:

- Relativity renames the default imaging profile to Basic Default.
- The imaging method is set to Basic for all current imaging profiles including Basic Default.
2.2.2 Imaging sets

If you upgrade to Relativity 9.3 and your environment contains imaging sets with errors, the Retry errors button on the Imaging Set console is disabled, and you won’t be able to retry those errors in Relativity 9.3. You will, however, be able to re-run the imaging set that contains the errors after you upgrade to Relativity 9.3.

2.2.3 Installation of a certificate on the database server

The Relativity 9.3 installer adds a certificate called RelativityIdentityCertificate to the EDDS database on your primary database during a first time installation or an upgrade. The authentication framework uses the thumbprint of the certificate to sign identity tokens, which are JSON web tokens (JWTs). The IdentityCertificateThumbprint instance setting stores the thumbprint associated with your certificate. For more information, see Instance setting values on the Relativity 9.3 Documentation site.

You also have the option to use your own authentication token-signing certificate. For more information, see Optionally configure an authentication token-signing certificate on the Pre-installation page in the Relativity 9.3 Documentation site.

For a clustered environment, you need to export a copy of your RelativityIdentityCertificate from the primary database server, and install the certificate to each database server hosting the EDDS. See the following instructions for more information:

- Optionally configure an authentication token-signing certificate on the Pre-installation page in the Relativity 9.3 Documentation site - These instructions describe the process for configuring your own custom token-signing certificate, but you can follow these basic steps to install RelativityIdentityCertificate to each database server in a distributed environment.

For more information, see the Imaging section of the Relativity Admin Guide.

2.2.4 New UI framework

Relativity 9.3 introduces a new UI framework which is turned off by default. If you want to enable the new UI framework for the Document list, click Switch to New Ui from the user dropdown within a workspace. When you enable the new UI framework, the following Relativity features update with the new framework:

- Cluster visualization
- Dashboards
- Document list and tabs throughout Relativity
- Pivot
- Sampling
- Search panel and search browser

Performance baselines and recommendations

For Relativity 9.3 Pre-release, performance testing is not yet complete. All performance metrics will be available by full release on November 23, 2015.
2.2.5 Processing
The following infrastructure items are new to processing in Relativity 9.3:

- Processing now uses Invariant 4.3.
- The WebAPI setting in IIS is now set to Anonymous Authentication by default and is no longer set to Windows Authentication. You must keep this set to Anonymous Authentication in order to publish documents to a workspace using the worker manager server.

- For users who haven't upgraded their Relativity version since the general release of Relativity 9.2, note that, beginning in Relativity 9.2.237.3 (the product update released on 6/24/2015), Invariant servers require .NET Framework 4.5.1.
- You will now use an installation file to install the worker manager server instead of the install wizard you previously used. For more information, see the Worker Manager Server Installation Guide.

Production
The following changes occur to existing productions on upgrade:

- On upgrade to Relativity 9.3 the Relativity.Core agents for production and branding are upgraded to ADS Deployed agents. The Relativity.Core agents for production and branding are not available in a 9.3 environment.
- Any staged or errored productions in an environment are set to a status of New and you must restage the production before running.
- If any produced productions contain native files with their Bates numbers previously stored in the Document table, the Bates numbers for the native files are moved to the Production object, and may not reflect actual Bates values if those values were overwritten.
- The Production Error field no longer exists on the Production object.
- Production sets you ran before upgrading to Relativity 9.3 aren’t available to select for merging with new production sets when you select the new Existing production numbering choice. ny custom production work-arounds break upon upgrade. For more information on new productions functionality, see the Admin guide.

- Users with full permissions to the Production object prior to upgrading to Relativity 9.3 do not automatically gain permissions to the new Production Data Source object, unless they also have the Manage Object Types permission under Admin Operations. Users need rights to the new Production Data Source object to add or edit production data sources after upgrading to Relativity 9.3.

- Any preexisting production fields are converted to a production data source upon upgrade.

- If you are updating your Production application to a version of Relativity 9.3 previous to 9.3.297.13, the upgrade can fail if you update the Binders application before it. Update the production application first or upgrade to 9.3.297.13.

- If you upgrade to Relativity 9.3 and you were previously using the Production Tracker application, review the Production Tracker 9.3 considerations PDF in the Relativity Community.

2.2.6 Required certificates for Relativity

Relativity 9.3 now verifies that all HTTPS services running in your environment have a trusted certificate. You may need to install additional certificates to components of your Relativity installation running HTTPS services to avoid error messages and insecure-connection icons. For more information, see the Pre-installation Guide.

Servers

There are a number of new server types installed automatically with Relativity 9.3:

- **Worker manager server** - this uses workers to perform imaging, conversion, and all phases of processing, including inventory, discovery, and publish. This is a required component of Relativity 9.3. If you are not licensed for processing, then the worker manager server only handles document conversion and imaging. For more information, see Worker manager server installation documentation.

- **Worker** - this is the machine a worker manager server uses to complete imaging, document conversion, and processing jobs. Workers are designed to centralize and streamline some of the jobs that used to be performed exclusively by agents. When you add a worker manager server to your Relativity environment, you specify the workers that you want that worker manager server to govern. Thus, it’s impossible to add workers without adding a worker manager server. For more information, see the Servers section of the Relativity Admin Guide.

- **Cache location server** - this temporarily stores natives, images, productions, and other file types the viewer uses. Add cache location servers to the resource pools that are associated with workspaces. You must provide a valid UNC path for the location of your cache. For more information, see the Servers section of the Relativity Admin Guide.

2.2.7 Service Host Manager HTTPS configuration

Service Host Manager runs Relativity services on all web and agent servers in your environment. The services are used by applications like Production and Processing on. Starting with Relativity 9.3.362.9
(March 30, 2016 update), special setup is required for HTTPS access to web and agent servers.
For more information, see Service Host Manager on the Relativity 9.3 Documentation site.

Structured Analytics
If upgrading to Relativity 9.3 from a version prior to 8.2, Relativity automatically updates the Minimum similarity percentage value for Structured Analytics textual near duplicate identification to the new minimum value of 80 if it is currently set between 70-79. See Creating a structured analytics set in the Analytics Guide.

2.2.8 System requirements
- Upon upgrade to Relativity 9.3, Windows Server 2008 R2 (64-bit) is no longer compatible with 9.3. Relativity 9.3 is only compatible with Windows Server 2008 R2 (64-bit) w Service Pack 1.
- As of August 31, 2017, we no longer support Internet Explore (IE) 10. Please upgrade to a compatible version of IE 11.

Viewer
The document viewer has been dramatically improved and you are no longer required to download or install any browser plug-ins in order to review documents in this new viewer. In addition, there are some functionality enhancements available in the new viewer. For more information, see the Viewer section of the Relativity Admin Guide.
You can still revert back to the Active X viewer that was available in versions prior to Relativity 9.3. You can enable this either per environment or per user. To use the ActiveX viewer in Relativity 9.3 you must have Microsoft .NET 4.5.1 runtime installed on the client machine.

Workspaces
In Relativity 9.3, workspaces include a new required field called Default Cache Location. The default cache location is a UNC path to the location on your network where the natives, images, productions, and other file types used by the viewer are temporarily stored. You can select any one of the cache locations included in the resource pool chosen for the workspace. For more information, see the Workspaces section of the Relativity Admin Guide.

2.2.9 Windows or Integrated Windows authentication
If your Relativity installation currently uses Windows authentication or Integrated Windows authentication, you must set the UseWindowsAuthentication instance setting to True after upgrading your environment. For more information, see the Instance setting guide on the Relativity 9.3 Documentation site.
You may want to configure your environment so that some servers use Windows authentication, while others don't use it. In this case, you need to add another row for this instance setting to the Instance setting table, update the machine name in this new row, and then set the value to True or False based on the Windows authentication requirements for the server.
In addition, you can set the WindowsAuthIpRange instance setting, which specifies a group of IP addresses that Relativity uses to validate the address of the user during login. If a request originates from an IP address added to the WindowsAuthIpRange instance setting, the server uses Windows Authentication to log the user in to Relativity. Relativity uses forms authentication to log in the user, when
the IP address is outside the specified range. For more information, see Instance settings on the Relativity 9.3 Documentation site.

2.3 7.x to 9.3 Relativity updates

Learn more about the changes to your Relativity 7.x environment after you upgrade to Relativity 9.3. This section also includes post-upgrade processes you'll need to follow.

7.x to 9.3 Relativity updates

- Analytics below
- Authentication on the next page
- dtSearch index considerations on page 35
- Imaging profiles on page 35
- Installation of a certificate on the database server on page 36
- License Relativity and Processing on page 36
- New UI framework on page 37
- Processing upgrade notes on page 37
- Production on page 38
- RAR upgrade notes on page 39
- Required certificates for Relativity on page 39
- System requirements on page 40
- Windows or Integrated Windows authentication on page 40
- Viewer on page 39
- Viewer (ActiveX) on page 39
- Upgrade custom applications or code on page 40

Analytics

Relativity 9.3 includes a Textual Near Duplicate Identification algorithm with the following benefits:

- The new algorithm can greatly improve performance for both large and complex data sets.
- With the new algorithm you can scale your Analytics server by adding CPU cores and RAM in order to achieve faster performance.

Prior to Relativity 9.3, scaling environments did not impact performance. Without scaling past 8 cores, you should experience performance comparable to pre-9.3 on most data sets. The Textual Near Duplicate Identification algorithm in Relativity 9.3 uses different, more efficient methods to obtain similar results. However, results may differ slightly from pre-9.3 results if a Full Analysis is run against a preexisting structured analytics set. If you need preexisting results use an Incremental Analysis instead. The incremental analysis keeps the pre-9.3 results for all preexisting documents, but the newly added documents use the new algorithm to match with existing groups.

Note the following when upgrading to Relativity 9.3:
In the Relativity Applications Library, the Analytics application contains the structured data analytics functionality, and the **Analytics Core** application contains Analytics profiles, repeated content filters, and Analytics categorization sets.

**Note:** On upgrade to Relativity 9.3, you can choose whether or not to include the Analytics application (structured data analytics). The Analytics Core application deploys automatically.

Beginning in Relativity 8, Primary Language Identification (PLI) is no longer supported. As a result, you don’t have to import PLI data into Relativity or set up a search index or categorization set to use PLI anymore. Instead, you can use the language identification operation when creating a Structured Data Analytics set.

Content Analyst 3.14 is required to use Analytics in Relativity 9.3.

See the Analytics Guide for more information on Language Identification.

### 2.3.1 Authentication

Relativity 9.3.452.1 introduces significant user authentication changes. Consider the following for upgrading:

- You no longer see the AuthenticationData field in the Users User Information section. You now enter the information you previously entered here in the individual authentication methods. This permits more versatile and detailed method implementations.

- Note that when you upgrade, Relativity creates a copy of the `eddsdbo.User` table before making any modifications. The table is for reference only, and the copy is named based on the Relativity version being ungraded from, such as `9_2_AuthenticationUserTableBackupRecord`. If after upgrading and making sure all users converted successfully, you may delete the copy table.

- Use the Authentication Profile system to enable only the protocols you need in an environment. In some cases the upgrade process may enable more protocols than you want. This is due to the parsing rules for the `AuthenticationData` column. Specifically, if you are using Active Directory or Client Certificate authentications in your environment, the upgrade process may also enable Integrated Authentication. If you don’t want the Integrated Authentication, you can remove that provider from the Authentication Profile after upgrade.

### Upgrading/installing Relativity Analytics 9.3

An Analytics server install or upgrade is required for Relativity 9.3. To install Relativity Analytics 9.3, you must run the Relativity Analytics Server Setup wizard after installing or upgrading your Relativity instance. When you run the Relativity Analytics Server Setup wizard, the wizard automatically:

- Installs the CAAT service
- Deploys the Relativity library files
- Configures the java heap size (set by default to half of RAM)
- Allows you to set an index path on new install, thus eliminating the need to manually set the location of indexes
- Sets the CAAT Windows service to log in as the Relativity Service Account
**Updating the default SSL/TLS certificate for the Content Analyst**

You must update the default SSL/TLS certificate on your Analytics server because Relativity requires a certificate signed by a trusted certificate authority (CA). By default, the CAAT service runs over an untrusted SSL/TLS certificate. For more information, see Post-upgrade: Updating the default SSL/TLS certificate for CAAT® on page 80.

**dtSearch index considerations**

There is a new paradigm to configuring and building dtSearch indexes. Keep these items in mind about your indexes after you upgrade:

- For indexes built in Relativity 5.9 or below, you must perform a Full Build for them to work normally.
- Any active indexes built in Relativity 6.2 or above continue work normally.
- After upgrading, you must initially perform a full build of a dtSearch index before you are able to run incremental builds. You can then perform incremental builds, which follow the new paradigm.
- For indexes that are in progress or in an error state when you upgrade, you must perform a Full Build.
- Indexes with document level errors continue to work normally.

**Adding dtSearches as choices to resource pools**

When upgrading from Relativity 7.x, you need to create a choices with paths to your dtSearch repositories, and then add these choices to the appropriate resource pools.

Use the following procedure to add dtSearches to resource pools:

1. Log in to Relativity.
2. From Home, click the **Choices** tab.
3. Click **New Choice**.
4. In the **Field** option, select **dtSearch Index Share Location**.
5. In the **Name** option, enter the UNC path to the dtSearch repository that is shared with the Relativity Services Account. The share must give this account read and write permissions.
6. Click **Save**.
7. Click the **Resource Pools** tab.
8. Click on the name of the resource pool where you want to add the dtSearch choice.
9. On the details view, locate the **dtSearch Index Share Locations** section.
10. Click **Add** to display the Select dtSearch Index Share Locations dialog.
11. Select the checkbox for your dtSearch Index Share Location and click **OK**. The details view now displays this share location in the dtSearch Index Share Locations section.

**Imaging profiles**

Existing imaging profiles receive updates based on their imaging method when upgrading to Relativity 9.3.

If your environment is set up for native imaging, the following changes occur upon upgrade:
- Relativity renames the default imaging profile to Native Default.
- The imaging method is set to Native for all current imaging profiles including Native Default.
- Relativity creates a new Basic Default imaging profile with the following settings:
  - Imaging Method: Basic
  - Basic Image Output Quality (DPI): 300
  - Basic Image Format: TIFF
  - Basic Image Height: Original Setting
- For any imaging set with it an imaging method set to Basic, the following changes occur:
  - The imaging profile the imaging set was linked to is copied.
  - Relativity sets the copied profile’s imaging method is set to Basic.
  - The copied profile is appended with Basic to the front of the name.

If your environment is not set up for native imaging, the following changes occur upon upgrade:

- Relativity renames the default imaging profile to Basic Default.
- The imaging method is set to Basic for all current imaging profiles including Basic Default.

2.3.2 Installation of a certificate on the database server

The Relativity 9.3 installer adds a certificate called RelativityIdentityCertificate to the EDDS database on your primary database during a first time installation or an upgrade. The authentication framework uses the thumbprint of the certificate to sign identity tokens, which are JSON web tokens (JWTs). The IdentityCertificateThumbprint instance setting stores the thumbprint associated with your certificate. For more information, see Instance setting values on the Relativity 9.3 Documentation site.

You also have the option to use your own authentication token-signing certificate. For more information, see Optionally configure an authentication token-signing certificate on the Pre-installation page in the Relativity 9.3 Documentation site.

For a clustered environment, you need to export a copy of your RelativityIdentityCertificate from the primary database server, and install the certificate to each database server hosting the EDDS. See the following instructions for more information:

- Optionally configure an authentication token-signing certificate on the Pre-installation page in the Relativity 9.3 Documentation site - These instructions describe the process for configuring your own custom token-signing certificate, but you can follow these basic steps to install RelativityIdentityCertificate to each database server in a distributed environment.

License Relativity and Processing

As part of the upgrade to Relativity 9.3, you need to apply a new Relativity and optional Processing license to your installation.
Relativity installations only
If you aren't using Processing in your Relativity installation, run the Relativity Database Upgrader on all databases, then request a new Relativity license key from Relativity Client Services, and apply the activation key. For more information, see the Relativity Licensing guide.

Relativity installations with Processing
If you are running Processing as part of your Relativity installation, complete the following steps to upgrade your licenses:

1. Run the Relativity installer on the Primary SQL Server as described in Upgrading your primary SQL Server on page 47.
2. Run the Relativity Database Upgrader only on the master (EDDS) database. See .
3. Request a new Relativity license key from Relativity Client Services, and apply the activation key. For more information, see the Relativity Licensing guide.
4. Request a new Processing license key from Relativity Client Services, and apply the activation key.

Note: You must apply the new Processing license before running the Relativity Database Upgrader. If you don't complete this step, the Relativity Database Upgrader can't upgrade your Processing application.

5. Run the Relativity Database Upgrader on your workspace databases.

2.3.3 New UI framework
Relativity 9.3 introduces a new UI framework which is turned off by default. If you want to enable the new UI framework for the Document list, click Switch to New UI from the user dropdown within a workspace. When you enable the new UI framework, the following Relativity features update with the new framework:

- Cluster visualization
- Dashboards
- Document list and tabs throughout Relativity
- Pivot
- Sampling
- Search panel and search browser

Processing upgrade notes
When upgrading the Processing application from 7.5 to Relativity 9.3, we strongly recommend that you first complete any outstanding processing sets in 7.5 before upgrading. However, note the following if you perform an upgrade and outstanding processing sets exist in 7.5:

- All documents published in 7.5 will retain the 7.5 document numbering format of nine digits.
- All documents published or republished in Relativity 9.3 will have the new 10 digit document numbering format. This new format extends to the Attachment Document ID, Parent Document ID, and Group ID fields.
Documents republished in Relativity 9.3 could potentially be duplicated with the new document numbering format.

Reference fields such as the Attachment Document ID, Parent Document ID, and Group ID on documents republished in Relativity 8 may not accurately reference the correct documents. Specific versions of Invariant are exclusively compatible with specific versions of Relativity. For this reason, don't attempt to upgrade Invariant independent of Relativity, as doing so will result in significant issues. For example, don't upgrade from Invariant 3.3, which is supported by Relativity 8.2, to Invariant 4.0 without also upgrading to Relativity 9.0. The following table breaks down which versions of Invariant are supported by which versions of Relativity:

<table>
<thead>
<tr>
<th>Invariant version</th>
<th>Relativity version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invariant 3.0</td>
<td>Relativity 7.5</td>
</tr>
<tr>
<td>Invariant 3.1</td>
<td>Relativity 8.0</td>
</tr>
<tr>
<td>Invariant 3.2</td>
<td>Relativity 8.1</td>
</tr>
<tr>
<td>Invariant 3.3</td>
<td>Relativity 8.2</td>
</tr>
<tr>
<td>Invariant 4.0</td>
<td>Relativity 9.0/9.1</td>
</tr>
<tr>
<td>Invariant 4.2</td>
<td>Relativity 9.2</td>
</tr>
<tr>
<td>Invariant 4.3</td>
<td>Relativity 9.3</td>
</tr>
</tbody>
</table>

**Production**

The following changes occur to existing productions on upgrade:

- On upgrade to Relativity 9.3 the Relativity.Core agents for production and branding are upgraded to ADS Deployed agents. The Relativity.Core agents for production and branding are not available in a 9.3 environment.

- Any staged or errored productions in an environment are set to a status of New and you must restage the production before running.

- If any produced productions contain native files with their Bates numbers previously stored in the Document table, the Bates numbers for the native files are moved to the Production object, and may not reflect actual Bates values if those values were overwritten.

- The Production Error field no longer exists on the Production object.

- Production sets you ran before upgrading to Relativity 9.3 aren't available to select for merging with new production sets when you select the new Existing production numbering choice. Any custom production work-arounds break upon upgrade. For more information on new productions functionality, see the Admin guide.

- Users with full permissions to the Production object prior to upgrading to Relativity 9.3 do not automatically gain permissions to the new Production Data Source object, unless they also have the Manage Object Types permission under Admin Operations. Users need rights to the new Production Data Source object to add or edit production data sources after upgrading to Relativity 9.3.

- Any preexisting production fields are converted to a production data source upon upgrade.

- If you upgrade to Relativity 9.3 and you were previously using the Production Tracker application, review the Production Tracker 9.3 considerations PDF in the Relativity Community.
RAR upgrade notes
You can upgrade an Assisted Review project while review is in progress for a round or between rounds. No work is required to ensure that Assisted Review operates properly in Relativity 9.3 before or after you upgrade Assisted Review from Relativity 7.5; however, it may be helpful to note the following tasks that Relativity automatically completes when you upgrade Assisted Review. Relativity:

- Gives old rounds a round type value of 7.5.
- Creates an Assisted Review saved searches folder if it didn't already exist.
- Creates a project-specific saved searches folder.
- Copies the project saved search to the new folder and creates four saved searches if categorization has already occurred.
- Sets all issues to a Medium Importance level.
- Replaces the Net Change graph in the Round Summary with Volatility. Note that it will take several rounds to generate volatility information; for example, if you upgrade prior to starting the fourth round, volatility displays in the report after you finish the fifth round.

**Note:** When upgrading from version 7.5 to 9, every project that is currently active (in the middle of a round) will receive an error until you set the positive choice for designation.

**2.3.4 Required certificates for Relativity**
Relativity 9.3 now verifies that all HTTPS services running in your environment have a trusted certificate. You may need to install additional certificates to components of your Relativity installation running HTTPS services to avoid error messages and insecure-connection icons. For more information, see the Pre-installation Guide.

**Viewer**
Relativity 9.3 uses Oracle Outside In version 8.4.0. When you upgrade to Relativity 9.3, you can install the new version of the viewer using the steps described in the Workspace Configuration guide. Previous versions of the viewer aren't upgraded, but you can run two versions of the viewer concurrently, so there's no need to uninstall previous versions.

**2.3.5 Viewer (ActiveX)**
To use the ActiveX viewer in Relativity 9.3 you must have Microsoft .NET 4.5.1 runtime installed on the client machine.

**2.3.6 Configure the viewer drawing delay**
If you anticipate multiple users using the same machine at the same time to perform a review, you can use a registry value to establish a drawing delay in the image viewer. This is only recommended when the standard refresh rate causes CPU utilization issues, which should only occur in a Citrix environment.

This value represents the number of milliseconds between calls to redraw the screen. In previous versions of Relativity, the image viewer behaved as though this value were set to 250. Increasing this value will reduce CPU usage when creating and/or modifying redactions and highlights, but it will also result in a choppier experience.
Changes to this value are not reflected in real-time, so you'll have to reload the image viewer for changes to take effect.

To configure the drawing delay, perform the following steps:

1. Click the **Start** button and type `regedit` in the search box, then click **Enter**.
2. Navigate to the appropriate location:
   - If you're using a 64-bit OS, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\kCura\ImageViewer`
   - If you're using a 32-bit OS, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\kCura\ImageViewer`

   **Note:** If this is your first time using this feature, the ImageViewer registry key won't exist and you'll have to create it. To create this new key, right-click the `kCura` folder and hover over **New**, then click **Key**.

3. Right-click the **ImageViewer** folder and hover over **New**, then click **DWORD (32-bit) Value**.
4. Double-click the new value to open the Edit DWORD (32-bit) Value popup.
5. In the **Value name** field, enter **DrawingDelay**.
6. In the **Value data** field, enter the appropriate value for your environment.

**Upgrade custom applications or code**

If your environment uses custom applications or code, you may also need to upgrade event handlers, and other components. For additional upgrade information, see the Relativity Developers site.

**2.3.7 System requirements**

- Upon upgrade to Relativity 9.3, Windows Server 2008 R2 (64-bit) is no longer compatible with 9.3. Relativity 9.3 is only compatible with Windows Server 2008 R2 (64-bit) w Service Pack 1.
- As of August 31, 2017, we no longer support Internet Explorer (IE) 10. Please upgrade to a compatible version of IE 11.

**2.3.8 Windows or Integrated Windows authentication**

If your Relativity installation currently uses Windows authentication or Integrated Windows authentication, you must set the `UseWindowsAuthentication` instance setting to **True** after upgrading your environment. For more information, see the Instance setting guide on the Relativity 9.3 Documentation site.

You may want to configure your environment so that some servers use Windows authentication, while others don't use it. In this case, you need to add another row for this instance setting to the Instance setting table, update the machine name in this new row, and then set the value to **True** or **False** based on the Windows authentication requirements for the server.

In addition, you can set the `WindowsAuthIpRange` instance setting, which specifies a group of IP addresses that Relativity uses to validate the address of the user during login. If a request originates from an IP address added to the WindowsAuthIpRange instance setting, the server uses Windows Authentication to log the user in to Relativity. Relativity uses forms authentication to log in the user, when
the IP address is outside the specified range. For more information, see Instance settings on the Relativity 9.3 Documentation site.

2.4 6.x to 9.3 Relativity updates

Learn more about the changes to your Relativity 6.x environment after you upgrade to Relativity 9.3. This section also includes post-upgrade processes you'll need to follow.

6.x to 9.3 Relativity updates

- Analytics below
- Authentication on the next page
- dtSearch index considerations on the next page
- Document Table Trigger removal considerations on page 43
- Imaging profiles on page 43
- Installation of a certificate on the database server on page 43
- License Relativity on page 44
- New UI framework on page 44
- Pre-installation steps for web servers on page 44
- Production on page 45
- Required certificates for Relativity on page 45
- System requirements on page 46
- Windows or Integrated Windows authentication on page 46
- Viewer on page 46
- Viewer (ActiveX) on page 46
- Upgrade agents and other components on page 46

2.4.1 Analytics

Relativity 9.3 introduces a new Textual Near Duplicate Identification algorithm with the following benefits:

- The new algorithm can greatly improve performance for both large and complex data sets.
- With the new algorithm you can scale your Analytics server by adding CPU cores and RAM in order to achieve faster performance.

Prior to Relativity 9.3, scaling environments did not impact performance. Without scaling past 8 cores, you should experience performance comparable to pre-9.3 on most data sets. The Textual Near Duplicate Identification algorithm in Relativity 9.3 uses different, more efficient methods to obtain similar results. However, results may differ slightly from pre-9.3 results if a Full Analysis is run against a preexisting structured analytics set. If you need preexisting results use an Incremental Analysis instead. The incremental analysis keeps the pre-9.3 results for all preexisting documents, but the newly added documents use the new algorithm to match with existing groups.
Updating the default SSL/TLS certificate for the Content Analyst

You must update the default SSL/TLS certificate on your Analytics server because Relativity requires a certificate signed by a trusted certificate authority (CA). By default, the CAAT service runs over an untrusted SSL/TLS certificate. For more information, see Post-upgrade: Updating the default SSL/TLS certificate for CAAT® on page 80.

2.4.1.1 Upgrading/installing Relativity Analytics 9.3

An install or upgrade of Relativity Analytics 9.3 is required for Relativity 9.3. To install Relativity Analytics 9.3, you must run the Relativity Analytics Server Setup wizard after installing or upgrading your Relativity instance.

When you run the Relativity Analytics Server Setup wizard, the wizard automatically:

- Installs the CAAT service
- Deploys the Relativity library files
- Configures the java heap size (set by default to half of RAM)
- Allows you to set an index path on new install, thus eliminating the need to manually set the location of indexes
- Sets the CAAT Windows service to log in as the Relativity Service Account

2.4.2 Authentication

Relativity 9.3.452.1 introduces significant user authentication changes. Consider the following for upgrading:

- You no longer see the AuthenticationData field in the Users User Information section. You now enter the information you previously entered here in the individual authentication methods. This permits more versatile and detailed method implementations.

- Note that when you upgrade, Relativity creates a copy of the eddsdbo.User table before making any modifications. The table is for reference only, and the copy is named based on the Relativity version being ungraded from, such as 9_2_AuthenticationUserTableBackupRecord. If after upgrading and making sure all users converted successfully, you may delete the copy table.

- Use the Authentication Profile system to enable only the protocols you need in an environment. In some cases the upgrade process may enable more protocols than you want. This is due to the parsing rules for the AuthenticationData column. Specifically, if you are using Active Directory or Client Certificate authentications in your environment, the upgrade process may also enable Integrated Authentication. If you don’t want the Integrated Authentication, you can remove that provider from the Authentication Profile after upgrade.

dtSearch index considerations

There is a new paradigm to configuring and building dtSearch indexes. Keep these items in mind about your indexes after you upgrade:

- For indexes built in Relativity 5.9 or below, you must perform a Full Build for them to work normally.
- Any active indexes built in Relativity 6.2 or above continue work normally.
- After upgrading, you must initially perform a full build of a dtSearch index before you are able to run incremental builds. You can then perform incremental builds, which follow the new paradigm.

- For indexes that are in progress or in an error state when you upgrade, you must perform a Full Build.

- Indexes with document level errors continue to work normally.

**Document Table Trigger removal considerations**

Relativity 9.0 includes enhancements that may affect certain areas of your existing environment when you upgrade. Improvements to the database schema make Relativity run faster in 8.1 than in previous versions. If your environment contains custom-developed functionality that involves the RelationalIndex_X tables or explicitly uses the RI_X columns in the Document tables, then you should refer to the Document table trigger removal documentation.

**Imaging profiles**

Existing imaging profiles receive updates based on their imaging method when upgrading to Relativity 9.3. If your environment is set up for native imaging, the following changes occur upon upgrade:

- Relativity renames the default imaging profile to Native Default.

- The imaging method is set to Native for all current imaging profiles including Native Default.

- Relativity creates a new Basic Default imaging profile with the following settings:
  - **Imaging Method**: Basic
  - **Basic Image Output Quality (DPI)**: 300
  - **Basic Image Format**: TIFF
  - **Basic Image Height**: Original Setting

- For any imaging set with it an imaging method set to Basic, the following changes occur:
  - The imaging profile the imaging set was linked to is copied.
  - Relativity sets the copied profile’s imaging method is set to Basic.
  - The copied profile is appended with Basic to the front of the name.

If your environment is not set up for native imaging, the following changes occur upon upgrade:

- Relativity renames the default imaging profile to Basic Default.

- The imaging method is set to Basic for all current imaging profiles including Basic Default.

**2.4.3 Installation of a certificate on the database server**

The Relativity 9.3 installer adds a certificate called RelativityIdentityCertificate to the EDDS database on your primary database during a first time installation or an upgrade. The authentication framework uses the thumbprint of the certificate to sign identity tokens, which are JSON web tokens (JWTs). The IdentityCertificateThumbprint instance setting stores the thumbprint associated with your certificate. For more information, see Instance setting values on the Relativity 9.3 Documentation site.
You also have the option to use your own authentication token-signing certificate. For more information, see Optionally configure an authentication token-signing certificate on the Pre-installation page in the Relativity 9.3 Documentation site.

For a clustered environment, you need to export a copy of your RelativityIdentityCertificate from the primary database server, and install the certificate to each database server hosting the EDDS. See the following instructions for more information:

- Optionally configure an authentication token-signing certificate on the Pre-installation page in the Relativity 9.3 Documentation site - These instructions describe the process for configuring your own custom token-signing certificate, but you can follow these basic steps to install RelativityIdentityCertificate to each database server in a distributed environment.

### 2.4.4 License Relativity

As part of the upgrade to Relativity 9.3, you need to apply a new Relativity license to your installation. Run Procuro on all databases, and then request a new Relativity license key from Relativity Client Services, and apply the activation key. For more information, see the Relativity Licensing guide.

### 2.4.5 New UI framework

Relativity 9.3 introduces a new UI framework which is turned off by default. If you want to enable the new UI framework for the Document list, click Switch to New UI from the user dropdown within a workspace. When you enable the new UI framework, the following Relativity features update with the new framework:

- Cluster visualization
- Dashboards
- Document list and tabs throughout Relativity
- Pivot
- Sampling
- Search panel and search browser

### Pre-installation steps for web servers

This section describes pre-installation steps that are required for upgrading Relativity 6.x installations. They must be completed on all web servers before installing Relativity 9.3.

### Setting IIS options

Use these instructions to update IIS settings and other configuration options for environments running Windows Server 2008 or higher with IIS 7.5. These updates must be made on all web servers in your Relativity installation.
1. Install .NET Framework 4.0 on all web servers.

2. Configure the Legacy Unhandled Exception Policy on all web servers.
   a. Browse to the following directory on your web server: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\n   b. Open the Aspnet.config file in a text editor.
   c. Locate the tag <legacyUnhandledExceptionPolicy>. Set the enabled attribute to true.
   d. Save the changes to the file.

Production

The following changes occur to existing productions on upgrade:

- On upgrade to Relativity 9.3 the Relativity.Core agents for production and branding are upgraded to ADS Deployed agents. The Relativity.Core agents for production and branding are not available in a 9.3 environment.
- Any staged or errored productions in an environment are set to a status of New and you must restage the production before running.
- If any produced productions contain native files with their Bates numbers previously stored in the Document table, the Bates numbers for the native files are moved to the Production object, and may not reflect actual Bates values if those values were overwritten.
- The Production Error field no longer exists on the Production object.
- Production sets you ran before upgrading to Relativity 9.3 aren’t available to select for merging with new production sets when you select the new Existing production numbering choice. Any custom production work-arounds break upon upgrade. For more information on new productions functionality, see the Admin guide.
- Users with full permissions to the Production object prior to upgrading to Relativity 9.3 do not automatically gain permissions to the new Production Data Source object, unless they also have the Manage Object Types permission under Admin Operations. Users need rights to the new Production Data Source object to add or edit production data sources after upgrading to Relativity 9.3.
- Any preexisting production fields are converted to a production data source upon upgrade.
- If you upgrade from Relativity 9.2 to Relativity 9.3 and you were previously using the Production Tracker application, review the Production Tracker 9.3 considerations PDF in the Relativity Community.

2.4.6 Required certificates for Relativity

Relativity 9.3 now verifies that all HTTPS services running in your environment have a trusted certificate. You may need to install additional certificates to components of your Relativity installation running HTTPS services to avoid error messages and insecure-connection icons. For more information, see the Pre-installation Guide.
2.4.7 System requirements

- Upon upgrade to Relativity 9.3, Windows Server 2008 R2 (64-bit) is no longer compatible with 9.3. Relativity 9.3 is only compatible with Windows Server 2008 R2 (64-bit) w Service Pack 1.
- As of August 31, 2017, we no longer support Internet Explore (IE) 10. Please upgrade to a compatible version of IE 11.

Viewer
Relativity 9.3 uses Oracle Outside In version 8.4.0. When you upgrade to Relativity 9.3, you can install the new version of the viewer using the steps described in the Workspace Configuration guide. Any previous versions of the viewer aren't upgraded, but you can run two versions of the viewer concurrently, so there's no need to uninstall previous versions.

2.4.8 Viewer (ActiveX)
To use the ActiveX viewer in Relativity 9.3 you must have Microsoft .NET 4.5.1 runtime installed on the client machine.

Upgrade agents and other components
Confirm that your environment has all the required agents and other software components added in prior versions. For more information, see the Relativity Upgrade Guide v6.10 in the Relativity Community.

If your environment uses custom applications, you may also need to upgrade event handlers, and other components. For more upgrade information, see the Relativity 9.3 Developers site.

Note: For information about recompiling syncs, contact the Client Services team (support@relativity.com).

2.4.9 Windows or Integrated Windows authentication
If your Relativity installation currently uses Windows authentication or Integrated Windows authentication, you must set the UseWindowsAuthentication instance setting to True after upgrading your environment. For more information, see the Instance setting guide on the Relativity 9.3 Documentation site.

You may want to configure your environment so that some servers use Windows authentication, while others don't use it. In this case, you need to add another row for this instance setting to the Instance setting table, update the machine name in this new row, and then set the value to True or False based on the Windows authentication requirements for the server.

In addition, you can set the WindowsAuthIpRange instance setting, which specifies a group of IP addresses that Relativity uses to validate the address of the user during login. If a request originates from an IP address added to the WindowsAuthIpRange instance setting, the server uses Windows Authentication to log the user in to Relativity. Relativity uses forms authentication to log in the user, when the IP address is outside the specified range. For more information, see Instance settings on the Relativity 9.3 Documentation site.
3 Upgrading your primary SQL Server

Follow these steps to upgrade your primary SQL server. Before you follow the steps below, you must have completed the required pre-upgrade steps for all Relativity versions.

Note: This page also contains steps for upgrading a distributed SQL Server. You must upgrade your primary SQL server before proceeding with these upgrades.

3.1 Primary SQL Server upgrade

The master database called the EDDS resides on the primary SQL Server. You must update the primary database before upgrading any other feature. After upgrade the primary SQL Server, you can upgrade the web and agent features in parallel.

Save the following files to the root directory of any server contributing to the Relativity environment:

- **Relativity.exe** - The executable file that installs Relativity components determined by the values entered in the RelativityResponse.txt file.
  
  Note: You must save Relativity.exe on a drive local to the server. Running Relativity.exe from a shared location results in upgrade or installation failure.

  Note: The Relativity.exe file does not open a user interface. Use Install.bat to proceed with installation.

- **Install.bat** - The code that prompts Relativity.exe to proceed with the installation process. You must edit line 11 of the Install.bat file with the exact name of the Relativity installation file.

  ```
  start /wait "" "INSERT EXACT NAME OF RELATIVITY INSTALLATION FILE" /log InstallLog.txt /responsefilepath=RelativityResponse.txt
  ```

  Note: You may need to run this file from an elevated command line prompt to avoid permission issues.

  Note: You must surround the name of the Relativity installation file with quotation marks.

- **RelativityResponse.txt** - The text file that determines which components Relativity.exe installs, uninstalls, or upgrades on the server.

  Note: Every line in the RelativityResponse.txt file that starts with ### is a comment and meant to provide instruction.

Open the RelativityResponse.txt file in a text editor and edit the parameters as follows to upgrade Relativity on the machine that serves the role of the primary SQL Server:
3.1.0.1 Common properties

- **INSTALLPRIMARYDATABASE** - Set this value to one.
  
  ```
  INSTALLPRIMARYDATABASE=1
  ```

- **INSTALLDISTRIBUTEDDATABASE** - Verify that this value is set to zero. You can't store the distributed database on the same machine as the primary database.
  
  ```
  INSTALLDISTRIBUTEDDATABASE=0
  ```

- **INSTALLDIR** - Enter the installation directory. This is the target directory for all files related to the local installation. This path must be local to the machine and accessible by the server. You must use ASCII characters for this path.
  
  ```
  INSTALLDIR=C:\Program Files\kCura Corporation\Relativity
  ```

- **PRIMARYSQLINSTANCE** - Enter the primary SQL instance. If you are installing to a cluster, specify the cluster and instance name. If you are installing to a named instance, specify the server and instance name. All features require this input.
  
  ```
  PRIMARYSQLINSTANCE=ML12
  ```

- **EDDSDBOPASSWORD** - Enter the EDDSDBO password.
  
  ```
  EDDSDBOPASSWORD=MySecretPassword
  ```

- **SERVICEUSERNAME** - Enter the service username. The Windows login must already exist.
  
  ```
  SERVICEUSERNAME=example\exampleusername
  ```

- **SERVICEPASSWORD** - Enter the Service password.
  
  ```
  SERVICEPASSWORD=MySecretPassword
  ```

- **USEWINAUTH** - Set the value to one to use Windows authentication for the SQL server.
  
  ```
  USEWINAUTH=1
  ```

  **Note:** If the **USEWINAUTH** value is set to one, then the user running the installer must be a SQL sysadmin, and any values entered for **SQLUSERNAME** and **SQLPASSWORD** are ignored.

- **SQLUSERNAME** - Enter the SQL username if you want to use SQL Server login authentication.
  
  ```
  SQLUSERNAME=mySqlUserName
  ```

  **Note:** This value is ignored if **USEWINAUTH** is set to one.

- **SQLPASSWORD** - Enter the SQL password if you want to use SQL Server login authentication.
  
  ```
  SQLPASSWORD=myPassword
  ```
Note: This value is ignored if USEWINAUTH is set to one.

3.1.0.2 Primary database properties

- **DEFAULTFILEREPORATORY** - Enter the default file repository. This path must be a shared folder to which both the user running the installer and the Relativity Service Account have read and write permissions.
  
  ```
  DEFAULTFILEREPORATORY=\yourmachine\FileShare
  ```

- **DTSEARCHINDEXPATH** - Enter the dtSearch index. This path must be a shared folder to which both the user running the installer and the Relativity Service Account have read and write permissions.
  
  ```
  DTSEARCHINDEXPATH=\yourmachine\dtSearch
  ```

- **RELATIVITYINSTANCENAME** - Enter the Relativity instance name. Only set this value during a first-time installation. The installer ignores this value on upgrade.
  
  ```
  RELATIVITYINSTANCENAME=My Relativity Instance
  ```

- **EDDSFILESHARE** - Enter the EDDS fileshare path. This path must be a shared folder to which both the user running the installer and the Relativity Service Account have read and write permissions.
  
  ```
  EDDSHARE=\yourmachine\Fileshare
  ```

3.1.0.3 Common database properties

We recommend that the following database paths are local to the SQL Server and accessible. However, we also support UNC paths on SQL Server 2012 and above.

- **DATABASEBACKUPDIR** - Enter the database backup directory.
  
  ```
  DATABASEBACKUPDIR=C:\Backup
  ```

- **LDFDIR** - Enter the LDF directory.
  
  ```
  LDFDIR=C:\Logs
  ```

- **MDFDIR** - Enter the MDF directory.
  
  ```
  MDFDIR=C:\Data
  ```

- **FULLTEXTDIR** - Enter the full text directory.
  
  ```
  FULLTEXTDIR=C:\FullText
  ```

Save your edits to the *RelativityResponse.txt* file, and launch the *Install.bat* file to proceed with the upgrade.

A sample RelativityResponse.txt file for a primary SQL database upgrade using Windows authentication looks like this:
3.2 Distributed SQL Server upgrade

If your Relativity environment uses a distributed SQL server, then you need to run the installer on a machine other than the one that hosts the primary SQL database. After you have upgraded the primary SQL server, you can upgrade the distributed database server and the web and agent server upgrades in parallel. Make sure that you review the steps for the database server setup in the Pre-installation Guide, including those in the Optionally configure an authentication token-signing certificate section.

Open the `RelativityResponse.txt` file in a text editor and edit the parameters as follows to upgrade Relativity on the machine that serves the role of the distributed SQL server:

### 3.2.0.1 Common properties

- **INSTALLPRIMARYDATABASE** - Set this value to zero. You can't store the distributed database on the same machine as the primary database.

  ```
  INSTALLPRIMARYDATABASE=0
  ```

- **INSTALLDISTRIBUTEDDATABASE** - Set this value to one.

  ```
  INSTALLDISTRIBUTEDDATABASE=1
  ```

- **INSTALLDIR** - Enter the installation directory. This is the target directory for all files related to the local installation. This path must be local to the machine and accessible by the server. You must use ASCII characters for this path.

  ```
  INSTALLDIR=C:\Program Files\kCura Corporation\Relativity
  ```

- **PRIMARYSQLINSTANCE** - Enter the primary SQL instance. If you are installing to a cluster, specify the cluster and instance name. If you are installing to a named instance, specify the server and instance name. All features require this input.

  ```
  PRIMARYSQLINSTANCE=ML12
  ```

**Note:** Every line in the `RelativityResponse.txt` file that starts with `###` is a comment and meant to provide instruction.
**EDDSDBOPASSWORD** - Enter the EDDSDBO password.

```
EDDSDBOPASSWORD=MySecretPassword
```

**SERVICEUSERNAME** - Enter the service username. The Windows login must already exist.

```
SERVICEUSERNAME=example\exampleusername
```

**SERVICEPASSWORD** - Enter the Service password.

```
SERVICEPASSWORD=MySecretPassword
```

**USEWINAUTH** - Set this to one to use Windows authentication for the SQL server.

```
USEWINAUTH=1
```

**SQLUSERNAME** - Enter the SQL username to use SQL Server login authentication.

```
SQLUSERNAME=mySqlUserName
```

**SQLPASSWORD** - Enter the SQL password to use SQL Server login authentication.

```
SQLPASSWORD=myPassword
```

**DATABASEBACKUPDIR** - Enter the database backup directory. This path must be local to the SQL Server and accessible.

```
DATABASEBACKUPDIR=C:\Backup
```

**LDFDIR** - Enter the LDF directory. This path must be local to the SQL Server and accessible.

```
LDFDIR=C:\Logs
```

---

**Note:** If the **USEWINAUTH** value is set to one, then the user running the installer must be a SQL sysadmin, and any values entered for **SQLUSERNAME** and **SQLPASSWORD** are ignored.

---

**DISTRIBUTEDSQLINSTANCE** - Enter the Distributed SQL instance. You can’t store the distributed database on the same machine as the primary SQL Server.

```
DISTRIBUTEDSQLINSTANCE=ML14
```

---

**3.2.0.3 Common database properties**

**DATABASEBACKUPDIR** - Enter the database backup directory. This path must be local to the SQL Server and accessible.

```
DATABASEBACKUPDIR=C:\Backup
```

**LDFDIR** - Enter the LDF directory. This path must be local to the SQL Server and accessible.

```
LDFDIR=C:\Logs
```
**MDFDIR** - Enter the MDF directory.

```
MDFDIR=C:\Data
```

**FULLTEXTDIR** - Enter the full text directory.

```
FULLTEXTDIR=C:\FullText
```

Save your edits to the `RelativityResponse.txt` file, and launch the `Install.bat` file to proceed with the upgrade.

A sample response file for a distributed SQL database upgrade using Windows authentication looks like this:

```
INSTALLDISTRIBUTEDDATABASE=1
INSTALLDIR=C:\Program Files\kCura Corporation\Relativity
PRIMARYSQLINSTANCE=ML12
EDDSDBOPASSWORD=MySecretPassword
SERVICEUSERNAME=example\exampleusername
SERVICEPASSWORD=MySecretPassword
DISTRIBUTEDSQLINSTANCE=ML14
DATABASEBACKUPDIR=C:\Backup
LDFDIR=C:\Logs
MDFDIR=C:\Data
FULLTEXTDIR=C:\FullText
USEWINAUTH=1
```

**Note:** Every line in the `RelativityResponse.txt` file that starts with `###` is a comment and meant to provide instruction.
4 Upgrading your agent server

This section provides the prerequisites and the steps required to upgrade your agent server to a new version of Relativity.

Before you begin upgrading your agent server, confirm that you have upgraded the SQL Server and have started the SQL service.

4.1 Agent server upgrade

Contact Relativity Client Services to get a copy of the Relativity installer.

Save the following files to the root directory of any server contributing to the Relativity environment:

- **Relativity.exe** - The executable file that installs Relativity components determined by the values entered in the RelativityResponse.txt file.

  **Note:** You must save Relativity.exe on a drive local to the server. Running Relativity.exe from a shared location results in upgrade or installation failure.

  **Note:** The Relativity.exe file does not open a user interface. Use Install.bat to proceed with installation.

- **Install.bat** - The code that prompts Relativity.exe to proceed with the installation process. You must edit line 11 of the Install.bat file with the exact name of the Relativity installation file.

  ```
  start /wait "" "INSERT EXACT NAME OF RELATIVITY INSTALLATION FILE" /log InstallLog.txt /responsefilepath=RelativityResponse.txt
  ```

  **Note:** You may need to run this file from an elevated command line prompt to avoid permission issues.

  **Note:** You must surround the name of the Relativity installation file with quotation marks.

- **RelativityResponse.txt** - The text file that determines which components Relativity.exe installs, uninstalls, or upgrades on the server.

  **Note:** Every line in the RelativityResponse.txt file that starts with #### is a comment and meant to provide instruction.

To upgrade the agent server:

Open the RelativityResponse.txt file in a text editor and edit the parameters as follows to upgrade Relativity on the machine that serves the role of the agent server:

**Note:** The following settings assume that the same machine does not host the agent server that hosts the primary or distributed SQL database servers.
4.1.0.1 Common properties

- **INSTALLDIR** - Enter the installation directory. This is the target directory for all files related to the local installation. This path must be local to the machine and accessible by the server. You can't use unicode special characters for this path.

  \[\text{INSTALLDIR=C:\Program Files\kCura Corporation\Relativity}\]

- **PRIMARYSQLINSTANCE** - Enter the primary SQL instance. If you are installing to a cluster, specify the cluster and instance name. If you are installing to a named instance, specify the server and instance name. All features require this input.

  \[\text{PRIMARYSQLINSTANCE=ML12}\]

- **EDDSDBOPASSWORD** - Enter the EDDS database object password.

  \[\text{EDDSDBOPASSWORD=MySecretPassword}\]

- **SERVICEUSERNAME** - Enter the service username. The Windows login must already exist.

  \[\text{SERVICEUSERNAME=example\exampleusername}\]

- **SERVICEPASSWORD** - Enter the service password.

  \[\text{SERVICEPASSWORD=MySecretPassword}\]

- **USEWINAUTH** - Set this to one to use Windows authentication for the SQL server.

  \[\text{USEWINAUTH=1}\]

  **Note:** If the **USEWINAUTH** value is set to one, then the user running the installer must be a SQL sysadmin, and any values entered for **SQLUSERNAME** and **SQLPASSWORD** are ignored.

- **SQLUSERNAME** - Enter the SQL username to use SQL Server login authentication.

  \[\text{SQLUSERNAME=mySqlUserName}\]

  **Note:** This value is ignored if **USEWINAUTH** is set to one.

- **SQLPASSWORD** - Enter the SQL password to use SQL Server login authentication.

  \[\text{SQLPASSWORD=myPassword}\]

  **Note:** This value is ignored if **USEWINAUTH** is set to one.

Save your edits to the **RelativityResponse.txt** file, and launch the **Install.bat** file to proceed with the upgrade.

A sample RelativityResponse.txt file for a agents only upgrade looks like this:

\begin{verbatim}
INSTALLAGENTS=1
INSTALLDIR=C:\Program Files\kCura Corporation\Relativity
\end{verbatim}
4.2 Service Host Manager HTTPS configuration

Service Host Manager runs Relativity services on all web and agent servers in your environment. The services are used by applications like Production and Processing on. Starting with Relativity 9.3.362.9 (March 30, 2016 update), special setup is required for HTTPS access to web and agent servers.

For more information, see Service Host Manager on the Relativity 9.3 Documentation site.
5 Upgrading your web server

This section provides the prerequisites and the steps required to upgrade your agent server to a new version of Relativity.

Before you begin upgrading your web server, confirm that you have upgraded the SQL Server, started the SQL service, and that IIS is stopped.

**Note:** When you install Relativity, it is configured to use HTTPS by default. If you decided not to use HTTPS in your environment, you must set the CookieSecure instance setting to **False** before logging in to Relativity, or you receive an error message. For more information, see Instance setting on the Relativity 9.3 Documentation site. If you later decide to use HTTPS in your environment, you can find information about how to set up this functionality in the section called *Configuring SSL on a web server* on the Pre-installation page.

5.1 Web server upgrade

The web server hosts Relativity and its services, such as the Services and Web APIs. After you have installed the primary SQL server, you can run the web and agent server, as well as the distributed database server installations in parallel.

Contact Relativity Client Services to get a copy of the Relativity installer.

Save the following files to the root directory of any server contributing to the Relativity environment:

- **Relativity.exe** - The executable file that installs Relativity components determined by the values entered in the RelativityResponse.txt file.

  **Note:** You must save Relativity.exe on a drive local to the server. Running Relativity.exe from a shared location results in upgrade or installation failure.

  **Note:** The Relativity.exe file does not open a user interface. Use Install.bat to proceed with installation.

- **Install.bat** - The code that prompts Relativity.exe to proceed with the installation process. You must edit line 11 of the Install.bat file with the exact name of the Relativity installation file.

  ```
  start /wait "" "INSERT EXACT NAME OF RELATIVITY INSTALLATION FILE" /log InstallLog.txt /responsefilepath=RelativityResponse.txt
  ```

  **Note:** You may need to run this file from an elevated command line prompt to avoid permission issues.

  **Note:** You must surround the name of the Relativity installation file with quotation marks.

- **RelativityResponse.txt** - The text file that determines which components Relativity.exe installs, uninstalls, or upgrades on the server.
The following settings assume that the same machine does not host the web server that hosts the primary or distributed SQL database servers.

Open the RelativityResponse.txt file in a text editor and edit the parameters as follows to install Relativity on the machine that serves the role of the web server:

### 5.1.0.1 Common properties

- **INSTALLWEB** - Set this value to one.
  
  INSTALLWEB=1

  **Note:** If the web server is already installed on this machine and the above value is set to zero, the installer removes the previously existing web server.

- **INSTALLDIR** - Enter the installation directory. This is the target directory for all files related to the local installation. This path must be local to the machine and accessible by the server. You can't use unicode special characters for this path.
  
  INSTALLDIR=C:\Program Files\kCura Corporation\Relativity

- **PRIMARYSQLINSTANCE** - Enter the primary SQL instance. If you are installing to a cluster, specify the cluster and instance name. If you are installing to a named instance, specify the server and instance name. All features require this input.
  
  PRIMARYSQLINSTANCE=ML12

- **EDDSDBOPASSWORD** - Enter the EDDS database object password.
  
  EDDSDBPASSWORD=MySecretPassword

- **SERVICEUSERNAME** - Enter the service username. The Windows login must already exist.
  
  SERVICEUSERNAME=example\exampleusername

- **SERVICEPASSWORD** - Enter the service password.
  
  SERVICEPASSWORD=MySecretPassword

- **USEWINAUTH** - Set this to one to use Windows authentication for the SQL server.
  
  USEWINAUTH=1

  **Note:** If the USEWINAUTH value is set to one, then the user running the installer must be a SQL sysadmin, and any values entered for SQLUSERNAME and SQLPASSWORD are ignored.

- **SQLUSERNAME** - Enter the SQL username to use SQL Server login authentication.
  
  SQLUSERNAME=mySqlUserName
**Note:** This value is ignored if `USEWINAUTH` is set to one.

- **SQLPASSWORD** - Enter the SQL password to use SQL Server login authentication.
  
  ```
  SQLPASSWORD=myPassword
  ```

  **Note:** This value is ignored if `USEWINAUTH` is set to one.

Save your edits to the `RelativityResponse.txt` file, and launch the `Install.bat` file to proceed with the upgrade.

A sample `RelativityResponse.txt` file for a web only upgrade looks like this:

```
INSTALLWEB=1
INSTALLDIR=C:\Program Files\kCura Corporation\Relativity
PRIMARYSQLINSTANCE=ML12
EDDSDBOPASSWORD=MySecretPassword
SERVICEUSERNAME=example\exampleusername
SERVICEPASSWORD=MySecretPassword
```

**Note:** Every line in the `RelativityResponse.txt` file that starts with `###` is a comment and meant to provide instruction.

### 5.2 Verifying the machine key settings on the IIS

When setting up the IIS for a Relativity installation, you need to verify that the machine keys are configured to use the appropriate methods for the encryption and decryption of forms authentication data.

Use these steps to set the machine key for the IIS:

1. Open the IIS Manager.
2. On the IIS dashboard, highlight your Relativity website to display configuration options in the Feature View.
3. Double-click the **Machine Key** icon.
4. Update the following fields for your version of Windows server:
   - **Windows Server 2008 R2** - Select **SHA1** for the **Encryption method** and **AES** for the **Decryption method**.

   **Note:** You could also select Auto for the Decryption method, but we recommend setting it to AES.
Windows Server 2012 R2 - Select SHA1 for the Validation method and AES for the Encryption method.
5. Save your changes.

5.3 Upgrading a web server configured for mixed authentication with AD

Use the following steps to upgrade a web server configured for mixed mode authentication with Active Directory (AD). For information about setting up a web server configured for mixed authentication with AD, see Authentication on the Relativity 9.3 Documentation site.

1. To update the UseWindowsAuthentication instance setting, open SQL Server Management Studio on your Relativity database server.
2. Connect to the EDDS database.
3. Execute one of the following SQL statement to set the WindowsAuthentication instance setting to True:
   - Update all servers to use Windows Authentication.
- Update a specific server to use Windows Authentication. Replace `YourServerName` in the WHERE clause to the name of your machine, which you want to configure for Windows Authentication. You only need the machine name if you want to set this setting per server.

```
UPDATE EDDS.eddsdbo.InstanceSetting SET
  value = 'True'
WHERE
  Name = 'UseWindowsAuthentication'
```

- Add a new row to the instance setting table for each additional machine that you need to enable AD authentication. Use this option when you want AD enabled on multiple web servers in your Relativity environment, but not on all of them. You need to execute the following SQL statement with the name of the additional machine, which you want to configure for Windows Authentication. Replace `YourSecondServerName` with the name of that machine.

```
INSERT INTO EDDS.eddsdbo.InstanceSetting
VALUES ('Relativity.Authentication','UseWindowsAuthentication','True', 'YourSecondServerName','Determines whether Relativity uses Windows Authentication. Set this value False if you want to disable WinAuth. Set it to True if you want to enable WinAuth and require the user to log in to Relativity from the current machine.' )
```

### 5.4 Service Host Manager HTTPS configuration

Service Host Manager runs Relativity services on all web and agent servers in your environment. The services are used by applications like Production and Processing on. Starting with Relativity 9.3.362.9 (March 30, 2016 update), special setup is required for HTTPS access to web and agent servers.

For more information, see Service Host Manager on the Relativity 9.3 Documentation site.
6 Upgrading a worker manager server installation

You can use these instructions for upgrading the Invariant Database, Queue Manager, and Worker. When you upgrade to a new version of Invariant, the installer removes any components from the previous version installed on the local machine before it replaces them with the upgraded version. You must be logged in as the Relativity Service Account to perform the upgrade.

Specific versions of Invariant are exclusively compatible with specific versions of Relativity. For this reason, don't attempt to upgrade Invariant independent of Relativity, as doing so will result in significant issues. For example, don't upgrade from Invariant 3.3, which is supported by Relativity 8.2, to Invariant 4.0 without also upgrading to Relativity 9.0. The following table breaks down which versions of Invariant are supported by which versions of Relativity:

<table>
<thead>
<tr>
<th>Invariant version</th>
<th>Relativity version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invariant 3.0</td>
<td>Relativity 7.5</td>
</tr>
<tr>
<td>Invariant 3.1</td>
<td>Relativity 8.0</td>
</tr>
<tr>
<td>Invariant 3.2</td>
<td>Relativity 8.1</td>
</tr>
<tr>
<td>Invariant 3.3</td>
<td>Relativity 8.2</td>
</tr>
<tr>
<td>Invariant 4.0</td>
<td>Relativity 9.0/9.1</td>
</tr>
<tr>
<td>Invariant 4.2</td>
<td>Relativity 9.2</td>
</tr>
<tr>
<td>Invariant 4.3</td>
<td>Relativity 9.3</td>
</tr>
</tbody>
</table>

If you’re performing separate upgrades for the Invariant components, you must upgrade the Invariant database first, and then the Queue Manager. Invariant workers automatically upgrade when the database is upgraded.

If the Invariant Worker Network File Path you specified during installation is not stored on the same SQL server as the Invariant database, instead of upgrading, you should uninstall Invariant and perform a fresh installation of Invariant. When you install the new version, be sure to select a folder that's stored on the same SQL server as the Invariant database. If this folder is not stored on the same server, you could lose all your data and be unable to uninstall or upgrade.

**Note:** When you apply a new processing license in your Relativity environment, all jobs in the processing queue must complete before Relativity identifies any additional worker manager servers that you may have purchased as licensed.

6.1 Upgrade exceptions

**For upgrades from Relativity 8.0/Invariant 3.1 or lower,** you must first manually install the required .NET 4.5 on all of your pre-existing Invariant Database, Queue Manager, and Worker machines before running the installer. Similarly, you must install the required Microsoft Visual C++ Redistributable on all of your pre-existing Worker machines before running the installer.

The 3.2 and above installers only validate whether .NET 4.5 is installed; they don't install the software. For brand new Worker installations, the installer verifies that .NET 4.5 is installed. Installing a new Worker will automatically install MS Visual C++ 2012 for you.

**For upgrades from Relativity 7.3/Invariant 2.0,** you must first upgrade to a later Invariant version (2.1, 3.0, 3.1, 3.2, or 3.3) before you upgrade to Invariant 4.0.
6.2 Installing Microsoft Visual C++ Redistributable Packages

When upgrading to Relativity 9.3/Invariant 4.3, you need to manually install the following versions of C++ on all of your worker servers prior to running the Invariant installation files for your upgrade:

- Microsoft Visual C++ 2010 x86 Redistributable x86 or x64
- Microsoft Visual C++ 2012 Redistributable x86 or x64

Note: This is not required for initial installations of Relativity 9.3/Invariant 4.3, as the installer will automatically install these C++ components.

6.3 Upgrading the Invariant Database and Queue Manager

You'll use the same installation files you used to install the Invariant Database and Queue Manager to upgrade them. To access the steps for performing an upgrade, see the Worker Manager Installation guide. These installation files upgrade both the Invariant and Relativity Imaging databases. During an upgrade, you can't modify the SQL Instance name, the Queue Manager Service Username, or the installation location of the Queue Manager. If you need to change any of these settings, you need to uninstall and reinstall the Invariant Database or Queue Manager.

Note: If you have an alternative configuration where the Invariant Database and the Queue Manager are on separate servers, you must upgrade the database first. However, this type of configuration is not recommended.

6.4 Automatically upgrading the worker

When you upgrade the Invariant Database, all Worker machines are also automatically upgraded. The Invariant Installer does not allow manual upgrades to a Worker machine. If you attempt a manual upgrade, an error message displays.

Note: By default, when you install Relativity, each worker in your environment is designated to do all available work (conversion, processing, and imaging). It's recommended that you change this designation so that, for every one hundred simultaneous users in your environment, you have one worker dedicated to conversion only and another worker dedicated to processing and/or imaging (but not conversion).
7 Upgrading workspaces

You can use the Workspace Upgrade queue to monitor the progress of scripts as they update workspace database schemas. In addition, you can also monitor upgrades to applications currently installed in workspaces. It also provides you with the ability to view detailed error messages when a script or application upgrade fails. You can use the advanced mass operations on the queue to edit the priority and order of workspace upgrades, as well as retry failed upgrades, and cancel upgrades.

7.1 Monitoring upgrades with the Workspace Upgrade queue

You can view the Workspace Upgrade queue from Home. Select the Queue Management tab, and click Workspace Upgrade Queue. The Workspace Upgrade queue displays the current status and the progress of the upgrade for each workspaces as shown in the following screen shot. For descriptions of the columns, see Workspace Upgrade queue columns on the next page.

As part of the database upgrade process, the Procuro utility automatically runs on your database server. Procuro automatically sets the Upgrade Status of the workspaces to Pending in the Workspace Upgrade queue. This status indicates to the upgrade agents running in your environment that they can begin upgrading the workspaces immediately. You can use the advanced mass operation options to change the upgrade priority and order of workspaces or to prevent workspaces from upgrading. For more information, see Editing upgrade priority and order for a workspace on page 66.

The workspace upgrader uses agents that run jobs for upgrading the workspace database schemas and installing applications. You must configure these agents through the Agents tab in Relativity. See Populating the Workspace Upgrade queue below.

If you don't see any activity in the Workspace Upgrade queue, these agents haven't been configured. An alert message lists the agents that you need to configure.

For configuration information, see Running the Relativity installer and Agents on the Relativity 9.3 Documentation site.

7.1.1 Populating the Workspace Upgrade queue

The Workspace Upgrade queue is continually populated with status information by the upgrade agents as they run scripts to update workspace databases and installed applications. The following agents run the scripts and the application upgrades:
- **Workspace Upgrade Worker** - picks up pending jobs in the queue for script updates.

**Note:** On an SQL server profile, you can edit the **Workspace Upgrade Limit** field, which controls the number of agents accessing the server during an upgrade. The setting entered in this field can’t exceed the setting in the **GlobalWorkspaceUpgradeLimit** instance setting value. If you enter a number that exceeds this instance setting value, an error occurs that cancels your update. For more information, see Instance setting values and Upgrading workspaces.

- **Workspace Upgrade Manager** - queues applications required for installation in workspaces.
- **Application Installation Manager** - installs required applications to workspaces.

For more information about agents, see Agents on the Relativity9.3 Documentation site.

During a Relativity upgrade, the agents complete the following tasks and then update the statuses displayed on the Workspace Upgrade queue:

- **Step 1 - Set upgrade status to Pending.** Procuro runs and sets the status on workspaces in the Workspace Upgrade queue to Pending.
- **Step 2 - Pick up pending jobs.** The Workspace Upgrade Worker sees a pending job in the queue, picks it up, and begins upgrading the workspace.
- **Step 3 - Run upgrade scripts.** The Workspace Upgrade Worker sets the status of the workspace to Upgrading scripts and runs the SQL scripts to update the workspace database schema. When the scripts complete, the upgrade status on the workspace is set to Pending Application Upgrade.
- **Step 4 - Set upgrade status to Upgrading Applications.** The Workspace Upgrade Manager queues applications required for installation in workspaces in the Application Install table, and it sets the upgrade status to Upgrading Applications.
- **Step 5 - Install applications.** The Application Installation Manager installs the required applications.
- **Step 6 - Complete installation.** When the application upgrades have installed successfully, the Workspace Upgrade Manager checks the application status, and then sets the status of the workspace to Completed.

### 7.1.2 Workspace Upgrade queue columns

The Workspace Upgrade queue displays the following columns:

- **Artifact ID** - the Artifact ID of a workspace undergoing an upgrade.
- **Workspace Name** - the name of a workspace undergoing an upgrade. Click on the name to display the document list in the workspace.
- **Upgrade Status** - the status of the workspace upgrade as determined by the current Procuro stage. See Upgrade statuses descriptions on the next page.
- **Priority** - the upgrade order assigned to the workspace. Priorities include Low, Medium, and High. See Editing upgrade priority and order for a workspace on the next page.
- **Workspace Status** - the value assigned to the Status field on the workspace details page. See Upgrade statuses descriptions on the next page.
- **Current Relativity Version** - the workspace is currently updated to this version of Relativity.
- **Upgrade Progress** - the percentage of the upgrade process that has completed. It uses the following colors to indicate the upgrade status:
  - **Blue** - indicates the upgrade is in progress.
  - **Green** - indicates a completed upgrade.
  - **Red** - indicates an error or failure occurred.

### 7.1.3 Upgrade statuses descriptions

The following table contains descriptions for the statuses displayed in the Upgrade Status column on the Workspace Upgrade queue:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canceled</td>
<td>The user canceled the upgrade when it had the status of Pending, Pending Application Upgrade, Upgrading Scripts, or Upgrading Applications. See <a href="#">Canceling or retrying workspace upgrades on page 70</a>.</td>
</tr>
<tr>
<td>Completed</td>
<td>The upgrade of the workspace completed successfully.</td>
</tr>
<tr>
<td>Failed Application Upgrade</td>
<td>An error occurred while upgrading applications in the workspace. See <a href="#">Troubleshooting upgrades on page 68</a>.</td>
</tr>
<tr>
<td>Failed Script Upgrade</td>
<td>An error occurred while upgrading SQL scripts for the workspace. See <a href="#">Troubleshooting upgrades on page 68</a>.</td>
</tr>
<tr>
<td>Pending</td>
<td>The workspace has been added to the Workspace Upgrade queue, but the Workspace Upgrade Worker hasn’t picked it up yet.</td>
</tr>
<tr>
<td>Pending Application Upgrade</td>
<td>The Workspace Upgrade Manager populates the application installation queue with any required applications.</td>
</tr>
<tr>
<td>Upgrading Applications</td>
<td>The Application Installation Manager upgrades the applications in the workspace.</td>
</tr>
<tr>
<td>Upgrading Scripts</td>
<td>The Workspace Upgrade Worker runs Procuro scripts against the workspace database.</td>
</tr>
</tbody>
</table>

### 7.2 Editing upgrade priority and order for a workspace

You can set order and priority on workspaces for upgrades. Relativity always upgrades ordered workspaces before unordered workspaces regardless of their priority. Relativity uses priority to determine which of the workspaces to upgrade first when you don’t assign an order.

In addition, if you assign the same order to a group of workspaces, Relativity uses their Artifact ID to determine the upgrade order. It follows a similar process if you assign the same priority to a group of workspaces.

The priority and order options provide you with the flexibility needed to control the workspaces that Relativity upgrades first and those that are upgraded later. For example, you might upgrade workspaces in high demand, so that they are available to users sooner than those less frequently accessed workspaces. The default priority for workspaces is Medium and the default order is blank.
**Note:** Your users may notice decreased Relativity performance if they are using a workspace on the same SQL Server where you are upgrading other workspaces. However, if you are upgrading workspaces on another server in a distributed environment, users shouldn’t notice any change in performance.

Use this procedure to change the priority and order:

1. Perform one of these tasks to select the workspaces:
   - To set the priority for only a specific group of workspaces, select their checkboxes. In the mass operations bar, choose **Checked**.
   - To set the priority for all workspaces, choose **All Items** in the mass operations bar.

2. Select **Edit Priority** in the mass operations bar.

3. Click **Go** to display the Edit Upgrade Priority dialog.

4. Perform one or both of the following tasks:
   - Select the **Priority** checkbox. Choose **Low**, **Medium**, or **High** from the drop-down menu. This value determines the upgrade sequence from among workspaces with the same Order, including those with blank values, with High Priority upgrading before Medium and finally Low. When both the Order and Priority values are each the same, workspaces upgrade in ascending ArtifactID order.
   - Select the **Order** checkbox. Enter a value in the text box. You use this value to specify the order that you want used for workspace upgrades. Relativity upgrades workspaces with a smaller Order values before those with a larger values. The default value for Order is blank. Workspaces with an explicitly specified Order value, regardless of its value, upgrade before an Order value of blank.

5. Click **Ok** to save your changes.
7.3 Troubleshooting upgrades

From the Workspace Upgrade queue, you can view script and application errors, which may have occurred during an upgrade. You can also use the mass operations for retrying a workspace upgrade from the queue or canceling an upgrade. For more information, see the following sections:

- View upgrade errors
- Canceling or retrying workspace upgrades

7.3.1 Viewing upgrade errors

When an application or script fails to upgrade properly, the Upgrade Status column displays a link that you can use to view additional information about the error that occurred.

**Note:** You can also view errors, upgrade status, script details, and other information on the History of Workspace dialog. To display this information, click the Workspace Details tab, and then click the View Audit button.

7.3.1.1 Script or other non-application upgrade fails

When a script upgrade fails, click the Failed Script Upgrade link to display the Error Information dialog, which includes a detailed error message, server, source, and other information.
You can’t access a workspace when a script or other upgrade non-application error occurs. If you attempt to open a workspace with these upgrade errors, you receive a message indicating that the workspace is inaccessible. Click the Return to Home link to display the default Home tab.

**Note:** If you only want to display workspaces that are fully upgraded and accessible, add a condition on the workspace view where the Workspace Accessibility field is set to Enabled. This setting filters only upgrade accessible workspaces, and hides any workspaces that users can't interact with.

When a script error occurs during an upgrade, review the details of the failure in the error message available from the Failed Script Upgrade link. You may also want to rerun the upgrade using the Retry Upgrade option. See [Canceling or retrying workspace upgrades on the next page](#).

### 7.3.1.2 Application upgrade fails in a workspace

When an application upgrade fails, click the Failed Application Upgrade link to display the Application Errors dialog. If multiple applications failed to upgrade, click this link to display a pop-up with links to the error pages for these applications.

When an application error occurs, review the details of the failure in the error message available from the Failed Application Upgrade link. You can resolve locking conflicts that occur when a locked application prevents an upgrade, and naming conflicts that occur when an object type in an application shares the same name as another object type in the workspace. To resolve these errors, perform one of the following tasks:
- **Locking conflicts** - Click the Failed Application Upgrade link to display the detailed error message. Select the Unlock <Application Name> checkbox, and click Retry Import on the error message.

- **Naming conflicts** - Click the Failed Application Upgrade link to display the detailed error message. Select Rename from the drop-down box, enter a new name for the object in the text box, and click Retry Import on the error message.

In addition, you can perform these tasks for resolving locking and naming conflicts through the Application Library tab.

You can continue accessing a workspace when an application that it contains fails to upgrade successfully for additional troubleshooting. From the Relativity Applications tab, you can view the application details to resolve application errors. When a workspace contains an application in this failed upgrade state, Relativity displays an orange message bar across most of its pages, which contains with a warning indicating that workspace upgrade isn't complete.

For more information, see Troubleshooting application errors in the Relativity 9.3 Developers site.

### 7.3.2 Canceling or retrying workspace upgrades

You can cancel an upgrade job on a workspace or retry an upgrade job as necessary. After you cancel a job, the workspace remains in a partially upgraded state so it is no longer accessible. You must attempt to complete a successful upgrade in order to access the workspace.

Use this procedure to cancel or retry an upgrade job:

1. Perform one of these tasks to select the workspaces:
   - To retry or cancel the upgrade jobs for only a specific group of workspaces, select their checkboxes. In the mass operations bar, choose Checked.
   - To retry or cancel the upgrade jobs for all workspaces, choose All Items in the mass operations bar.

2. Select Retry Upgrade or Cancel Upgrade in the mass operations bar.

3. Click Go to display a confirmation dialog.

4. Click OK if you want to continue with your selected action.
8 Upgrading or installing your Analytics server

An upgrade of your Analytics server is required for Relativity 9.3. To upgrade to Relativity Analytics 9.3, you must first:

1. Install or upgrade your Relativity instance. Install or upgrade your Relativity instance.
2. Run the Relativity Analytics Server Setup wizard.

When you run the Relativity Analytics Server Setup wizard, the wizard automatically:

- Installs the CAAT service
- Deploys the Relativity library files
- Configures the java heap size (set by default to half of RAM)
  - If you re-install the Analytics server after already adjusting the java heap size settings, the new installation will overwrite the java heap adjustments you made.
- Allows you to set an index path on new install, thus eliminating the need to manually set the location of indexes
- Sets the CAAT Windows service to log in as the Relativity Service Account

This topic contains the following sections:

- Upgrading your Analytics server below
- Running the Analytics installer on the next page
- Upgrading clusters for CAAT 3.17.2 and higher from Relativity 9.1 and below on page 77
- Addressing "Could not configure security" installer warning on page 80
- Post-upgrade: Updating the default SSL/TLS certificate for CAAT® on page 80
- Disabling TLS 1.0 and 1.1 (optional) on page 84
- Installing Analytics server when SQL Server uses SSL encryption on page 85
- Changing the REST password on page 86
- Uninstalling the Relativity Analytics server on page 86

8.1 Upgrading your Analytics server

Follow these steps to upgrade your analytics server(s). Before upgrading the Analytics server(s), make sure you’ve completed the steps contained in the following sections:

1. Required upgrade steps for all Relativity versions.
2. Install or upgrade the primary SQL server in your Relativity instance.
3. See Analytics server setup in the Pre-Installation Guide.

Note: Before attempting an upgrade, stop all CAAT processes (i.e., ensure that all Java and Postgres processes are stopped), and then back up the CAAT install directory and the CAAT data directory. If something goes wrong with the upgrade, this will greatly reduce any downtime spent to fix the problem.
You need the following items in order to successfully run the Relativity Analytics Server Setup wizard:

- The primary database server instance name and corresponding EDDSDBO password. If your SQL Server uses SSL encryption, see Installing Analytics server when SQL Server uses SSL encryption on page 85 before beginning the Analytics server installation.
- The Relativity Service Account username and password.
- All SQL servers must be active and accessible at the time of the installation.

8.2 Running the Analytics installer

The following steps may be necessary when installing Analytics:

Running Relativity Analytics server setup
Note the following before running the Relativity Analytics Server Setup:

- Run the server setup as the Relativity Service Account.
- You must have admin rights to both the Analytics server and the index share path in order to run the installer without interruption. If you don't, the installer informs you that the directories can't be configured and that you must check to make sure that your permissions are correct.

**Note:** If a "Could not configure security for the following directories" warning occurs during your Analytics installation or upgrade, see Addressing "Could not configure security" installer warning on page 80.

Follow these steps to run the Relativity Analytics Server Setup:

2. Click Next on the Relativity Analytics Server Setup welcome dialog.
3. Enter values for the following **Primary Database Server Configuration** fields and click **Next**:

- **Primary Database Server Instance** - the primary database server to which you want to install the Content Analyst service. The value you enter must match the **Name** value recorded on the **Servers** tab in Relativity.

- **EDDSDBO Password** - the password to the EDDSDBO account of the primary database. If you change the password to your primary database server instance, you must re-run the Relativity Analytics Server Setup wizard.

- **Relativity Service Account** - the service account of the Relativity instance that is using this installation of Content Analyst. You must use the following format for the service account name: `<domain>\<user>`. 

- **Relativity Service Account Password** - the password for the Relativity instance.

4. Enter values for the following REST API configuration fields and click **Next**. These values must match those of the corresponding fields on the Analytics server object in Relativity. For more information, see Servers in the Admin Guide.
5. Check, edit, or enter the values for the following **Relativity Analytics Server Installation** fields and click **Install**. These are automatically populated and are editable only if there is no existing installation of Content Analyst. If there is an existing installation of Content Analyst that has a non-default service name, Relativity isn't able to detect that installation. Thus, you must enter the correct values for these fields to successfully upgrade your installation of CAAT:
- **Analytics Server folder** - the path to the folder containing the Analytics installation files.
  - We recommend using the default folder of C:\CAAT (or C:\ContentAnalyst for a legacy installation).
  - This path must be absolute, and it can't contain spaces or invalid characters.
  - If the installer can't find or access the location you specify, it installs the application to the default C:\CAAT folder.

- **Analytics Server Service Name** - the Windows service name of the Analytics instance. We recommend leaving this as the default value. This can't contain any invalid characters and it can't exceed 80 characters.

- **Analytics Server Port Number** - the port number of the Analytics server. The default port is 8080, but you can configure a different port number.

- **Analytics Index Directory** - the directory where indexes and structured analytics sets are stored on disk.
  - We recommend that you not keep the index directory on the C: drive due to the size requirements.
  - We recommend you use locally-attached storage referenced by a drive letter, i.e. E:\CAATIndexes, rather than a UNC path. For more information, see Index directory requirements.
Do not create a local drive map to a UNC. For example, do not open \server-name\CAAT1 and map it to drive Z:. This is because drive mappings are specific to each Windows user and may not be available to the Relativity Service Account.

This path must be absolute, and it can’t contain spaces, invalid characters, or any Unicode.

Always use the installer to make changes to your Analytics configuration, including the index directory. If you need to specify a new folder path, see Moving Analytics indexes and structured analytics sets in the Admin Guide.

**Note:** If using a UNC path for the Analytics Server Folder and (Optional) Analytics Index Share Folder fields, the path must point to a Windows server directory.

When you first click Install, Relativity unzips the Analytics installer. This can take several minutes to complete.

6. (Optional) Monitor the status of the installation. You don’t have to click next once this process is complete.

7. (Optional) Note the installation specifications in the command line window. Don’t close this during installation. It closes automatically when installation is complete and the final step of the wizard appears.

```
1. Installation directory: C:\CAAT
You have selected the following:
1. Java jre1.7.0_17 to be installed
2. Directory: C:\CAAT \WEB-INSTALL
3. HTTP Port: 8888
4. License Key File: C:\CAAT\webapps\nexus\WEB-INF\lib\caat-3.14.0\kCura-2016.jar
5. Windows Service: yes
   Service name: Content Analyst CAAT
Installing Java to: C:\CAAT\jre1.7.0_17
This may take a while. Please wait...

Java successfully installed.
Installing to: C:\CAAT

Unpackaged application files.
Created the start/stop scripts.
Deleting obsolete or unwanted files.
Registering Windows Service: Content Analyst CAAT ... successful
Installing the CAAT license key from C:\CAAT\webapps\nexus\WEB-INF\lib\caat-3.14.0\kCura-2016.jar...
Testing installed binaries...
Testing binary: C:\CAAT\webapps\nexus\WEB-INF\lib\WindowsAMD64\kCura.exe ... successful
Testing binary: C:\CAAT\webapps\nexus\WEB-INF\lib\WindowsAMD64\booleng.exe
```

8. Click **Finish** to complete the installation.
9. Relativity 9.3 requires a certificate signed by a trusted certificate authority (CA). By default, the CAAT service runs over an untrusted SSL/TLS certificate. For steps to modify, see Post-upgrade: Updating the default SSL/TLS certificate for CAAT® on page 80.

10. (Optional) Confirm that all components of the Analytics service are running by visiting http://<Analytics Server Hostname>:<CA Port>/nexus/services and checking the Available Services list. Make sure to specify your Analytics server host name and CA port in the URL.

11. If this is a new Analytics server, add it to the Servers list. For these steps, see Adding an Analytics or worker manager server on the Documentation site. If the server has already been added, navigate to the Servers tab and activate it. Make sure to enter the information on the server layout the same as you did in the Analytics installer.

   - If you enter the information correctly, you can successfully save the server.
   - If you receive a not found error on the server, make sure the Analytics service is running and that you used the correct port.
   - If you get an unauthorized error, make sure that you entered the credentials correctly.

Content Analyst is now installed in your environment.

8.3 Upgrading clusters for CAAT 3.17.2 and higher from Relativity 9.1 and below

Upgrading clusters for CAAT 3.17.2 and higher from Relativity 9.1 or lower

Note: The instructions in this section are only necessary when upgrading to Relativity from Relativity 9.1 or below.
Relativity 9.2.271.9 installs CAAT 3.17.2 which includes clustering performance improvements. You must upgrade your existing clusters if they were created using a version of CAAT previous to 3.17.2.

To upgrade your clusters, use one of the following upgrade methods:

- Run Create Cluster Upgrade Jobs script below
- Upgrade clusters on the fly on the next page

8.3.0.1 Run Create Cluster Upgrade Jobs script

Complete the following steps to automate the cluster set upgrade process by creating upgrade jobs for one workspace or all workspaces using the Create Cluster Upgrade Jobs script:

1. Navigate to Home.
2. Click the Relativity Script Library tab.
3. Locate and click the Create Cluster Upgrade Jobs script.
4. Click Run Script.
5. Select the workspace that contains the clusters you want to upgrade from the Workspace Name drop-down menu or select <All Workspaces> to upgrade all clusters in all of your workspaces.

6. Click Run followed by OK.
7. Close the Create Cluster Upgrade Jobs script dialog.

Cluster upgrade jobs added by the Create Cluster Upgrade Jobs script are managed by the Cluster Upgrade Worker agent. See the Agents guide for more information regarding the Cluster Upgrade Worker
agent. See the Admin Guide for additional details regarding the Create Cluster Upgrade Jobs script and script results.

8.3.0.2 Monitor cluster upgrade jobs
The Monitor Cluster Upgrade Jobs script checks and reports the status of all Analytics cluster upgrade jobs added using the Create Cluster Upgrade Jobs script.

Complete the following steps to view a count of clusters that are upgraded and not upgraded by workspace:

1. Navigate to Home.
2. Click the Relativity Script Library tab.
3. Locate and click the Monitor Cluster Upgrade Jobs script.
4. Click Run Script.
5. Click Run. With the Monitor Cluster Upgrade Jobs dialog still open, click Run again to refresh the list.


See the Admin Guide for additional details regarding the Monitor Cluster Upgrade Jobs script and script results as well as steps to identify failed cluster upgrades.

8.3.0.3 Upgrade clusters on the fly
If you have any clusters created using versions of Content Analyst previous to CAAT 3.17.2 that weren’t upgraded using the Create Cluster Upgrade Jobs script, the system automatically calculates and stores the cluster distance data on the fly when a user first clicks to view a cluster's nearby cluster visualization.

The on the fly upgrade and calculation require anywhere from a few seconds to a number of minutes depending on the size and complexity of the data. While the system upgrades a cluster and calculates the distance data, the cluster can’t be accessed using cluster visualization, and a notification message informs the user the cluster data is being updated.
When the upgrade and calculation processes complete for a cluster, users can access the cluster using cluster visualization with the performance improvements in effect.

### 8.4 Addressing "Could not configure security" installer warning

Addressing "Could not configure security" installer warning

The following warning message may occur when upgrading or installing Relativity Analytics:

*Could not configure security for the following directories:*

*Please confirm that the Relativity Service account has full control on them.*

This warning indicates that the user account running the installer failed to update the permissions on the listed directories for the Relativity Service account. After you acknowledge the warning, continue and complete the installation or upgrade of Analytics. The installation is still valid.

After finishing the Analytics installation or upgrade, complete the following steps to ensure the Relativity Service account has appropriate access to the directories listed in the warning message:

1. Stop the Content Analyst CAAT Windows service if it's running.
2. Add the Relativity Service Account user to the Administrators and Users groups.
3. Grant the Relativity Service Account Full Control permissions on C:\CAAT (the installation directory).
4. Grant the Users group Full Control permissions on C:\CAAT\pgsql\data.
5. If the installation contains a C:\CAAT\data-default folder, grant the Users group Full Control permissions on this folder.
6. If the index directory is different from the default (i.e. on another drive or share), ensure the Relativity Service Account has Full Control permissions on the index directory.
7. Restart the Analytics server after updating the user and group permissions.
8. Verify the Relativity Service Account is running the CAAT Content Analyst Windows Service.

### 8.5 Post-upgrade: Updating the default SSL/TLS certificate for CAAT®

As of Relativity 9.3, Relativity requires a trusted certificate for all HTTPS traffic, including the internal traffic for the Analytics server. We recommend placing the certificate and testing it prior to the day of the upgrade.
to Relativity 9.3. By default, the Content Analyst (CAAT®) service runs over an untrusted SSL/TLS certificate. There are several options for getting a trusted certificate in place. You most likely already have a certificate for your externally facing web servers. However, it’s likely that the domain name for that certificate doesn’t match the internal fully qualified domain name (FQDN) of the Analytics server(s). If it DOES match, you may use the same certificate currently on your web server. For example, if the external certificate is *company.com but your domain is *.company.corp, then this does not match and cannot be used. If it does not, we strongly recommend purchasing one from a trusted certificate authority and placing it on the Analytics server before the upgrade. If you choose not to purchase a certificate, it is possible to use a self-signed certificate as a temporary measure. Should you choose to do this, we recommend using the fully qualified domain name when creating the self-signed certificate so that it can be swapped for a real certificate from a trusted authority later on.

To check the fully qualified domain name (FQDN) of the Analytics server:

1. Open the Control Panel.
2. Navigate to **Control Panel\System** and **Security\System**.
3. Under the Computer name section, find the entry for **Full Computer Name**.
4. If you have an existing certificate, verify that it matches the FQDN of the Analytics server.
   - If it does not, you must either purchase a new certificate or generate a self-signed certificate.

Perform the following steps to use a trusted certificate:

1. **Delete** the default, unsigned certificate.
2. Either **import a trusted certificate** (that uses the FQDN) or **generate a self-signed certificate**.

   **Note:** It is recommended that you use a certificate from a trusted authority (if possible). For workgroup environments, a self-signed certificate is necessary.

3. **Verify the Analytics server** in Relativity.
   1. Deleting the default, unsigned certificate:
      Complete the following steps to delete the default, unsigned certificate:

      1. Log in to the analytics server as the Relativity Service Account.
      2. Open a command prompt window.
      3. View a list of all certificates in the keystore by running the following command:

      ```
      C:\CAAT\jdk1.8.0_25\bin\keytool.exe -list -keystore C:\CAAT\etc\ssl\server.keystore -v
      ```

      **Note:** These commands assume that the CAAT installation directory is C:\CAAT. They may need to be modified to account for differing installation drive letters or installation folder names.

      4. You will be prompted to enter a keystore password. The default password is **caat4me**. Type this into the command prompt and then hit **Enter**.

      **Note:** The password will not appear on the screen while typing.

      5. Take note of the certificate(s) listed in the keystore. The alias name for the default CAAT® certificate to be deleted is **contentanalyst**.
6. To delete the default CAAT certificate, run the following command:

```
C:\CAAT\jdk1.8.0_25\bin\keytool.exe -delete -keystore C:\CAAT\etc\ssl\server.keystore -alias contentanalyst
```

2A. Importing a trusted certificate:

Complete the following steps to import a trusted certificate:

1. If you have a valid certificate matching the FQDN of the analytics server, import it to the keystore. You will be prompted again for the keystore password. If the certificate is a PKCS12 certificate, run the following command, replacing `<Certificate>` with the file path, name, and extension of the certificate (i.e., C:\folder\RelativityCert.pfx) and replace `<CertPassword>` and `<DestinationPassword>` with the relevant passwords:

```
C:\CAAT\jdk1.8.0_25\bin\keytool.exe -importkeystore -srckeystore <Certificate> -srcstorepass <CertPassword> -srcstoretype pkcs12 -destkeystore C:\CAAT\etc\ssl\server.keystore -destkeypass <DestinationPassword> -deststoretype JKS
```

**Note:** The default password for the keystore is `caat4me`. The password for the certificate must match the password for the keystore. The password will not appear on the screen while typing.

2. Verify that the certificate is in the keystore by running the following command to list the certificates:

```
C:\CAAT\jdk1.8.0_25\bin\keytool.exe -list -keystore C:\CAAT\etc\ssl\server.keystore -v
```

3. Restart the Content Analyst CAAT windows service.

**Note:** The endpoint for the CAAT certificate is `https://<servername.FQDN>:8443/nexus/r1/`.

4. Test the certificate by opening a browser from the Analytics server and at least one other server and navigating to the endpoint above. You should not get a certificate error when navigating to the URL.

5. Proceed to to [Verifying the Analytics server in Relativity](#).

6. Import the certificate to the Trusted Root of the following servers:
   - Analytics servers
   - Agent servers
   - Primary and distributed SQL servers
   - Web servers

To do so, follow these instructions:


b. A warning will appear indicating there is a problem with the website’s security certificate. Click "continue to this website (not recommended)".

   Upon clicking continue, you will be prompted to enter your REST account credentials.

c. Click on the certificate error in the address bar.

d. Click [View Certificates](#).
e. Click Install Certificate....

f. Import the certificate to either the **Current User** or **Local Machine** store location.

g. Select "Place all certificates in the following store" and browse for "Trusted Root Certification Authorities".

h. Click Finish.

i. Test that the import was successful by navigating to the REST site again.

j. Repeat this process for each server listed above.

2B. Creating a self-signed certificate:
Complete the following steps to create a self-signed certificate:

1. If you would like to create a self-signed certificate, run this command from the Analytics server:

   ```
   C:\CAAT\jdk1.8.0_25\bin\keytool.exe -genkey -keyalg RSA -alias selfsigned -keystore C:\CAAT\etc\ssl\server.keystore -storepass caat4me -validity 360 -keysize 2048
   ```

2. You will be prompted several times. Enter the FQDN of the Analytics server for all prompts except the last, which is just the country abbreviation.

3. Use the same keypass as the keystore when prompted. You can either hit return or type in `caat4me`.

4. Export the certificate using the following command:

   ```
   C:\CAAT\jdk1.8.0_25\bin\keytool.exe -export -alias selfsigned -file C:\selfsigned.crt -keystore C:\CAAT\etc\ssl\server.keystore
   ```

5. Restart the Content Analyst CAAT windows service.

6. Import the certificate to the Trusted Root of the following servers:
   - Analytics servers
   - Agent servers
   - Primary and distributed SQL servers
   - Web servers

To do so, follow these instructions:


b. A warning will appear indicating there is a problem with the website’s security certificate. Click "continue to this website (not recommended)".

   Upon clicking continue, you will be prompted to enter your REST account credentials.

c. Click on the certificate error in the address bar.

d. Click **View Certificates**.

e. Click Install Certificate....

f. Import the certificate to either the **Current User** or **Local Machine** store location.
g. Select "Place all certificates in the following store" and browse for "Trusted Root Certification Authorities".

h. Click Finish.

i. Test that the import was successful by navigating to the REST site again.

j. Repeat this process for each server listed above.

7. Proceed to Verifying the Analytics server in Relativity.

3. Verifying the Analytics server in Relativity
Verify in Relativity that the Analytics server URL uses the FQDN and not the server name or IP address. Navigate to the Servers tab, and check the URL of the Analytics server. If it does not contain the FQDN, then follow these steps:

1. Add a new Analytics server from the Servers tab in Relativity. See Adding an Analytics server in the Admin Guide for more information. When entering the URL:
   a. Use this format: http://<servername.FQDN>:8080/nexus/services/
   b. Duplicate all other settings from the original Analytics server.

2. Add the new Analytics server to all of the same Resource Pools as the original server.

3. Place the Analytics Move script into the Relativity Script Library.

4. Test functionality by creating a small structured analytics set or index.

5. Run the Analytics Move script to swap all references from the original server to the new server just created.

6. Delete the old Analytics server from the Servers tab in Relativity.

7. Optional: For instructions on how to change and obfuscate the default Jetty passwords, reach out to Support at support@relativity.com.

8.6 Disabling TLS 1.0 and 1.1 (optional)

Note: The following instructions apply to versions of Relativity using CAAT versions 3.19 and above. Earlier versions of CAAT do not support disabling TLS 1.0 -- all versions of CAAT support communication over TLS 1.2.

1. Open C:\CAAT\jetty\etc\jetty-ssl.xml.

2. Insert <Set name="ExcludeProtocols"> in the configuration file as shown below at the end of Configure a TLS (SSL) Context Factory.

```xml
<Item>SSL_RSA_EXPORT_WITH_DES40_CBC_SHA</Item>
<Item>SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA</Item>
<Item>SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA</Item>
</Array>
</Set>
```
3. Restart the Content Analyst (CAAT) Windows service.

4. Update the registry key on all web and agent servers:
   a. Create or update the following registry keys on each server as shown below. You should be able to create a *.reg file out of the snippet below.

   ```plaintext
   Windows Registry Editor Version 5.00
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
   "SchUseStrongCrypto"=dword:00000001
   [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319]
   "SchUseStrongCrypto"=dword:00000001
   ``

   b. Restart IIS or the agent service on each applicable server.

5. Verify that the connection works by clicking Save in the Analytics Server layout.

### 8.7 Installing Analytics server when SQL Server uses SSL encryption

When your primary SQL Server uses SSL encryption, you must satisfy the following additional environment requirements in order for the Analytics server to communicate with SQL Server:

- The SQL Server's certificate is installed in the Analytics server KeyStore. See Install a SQL Server certificate in the Analytics server KeyStore below
- The Common Name (CN) property of the SQL Server's certificate matches the server name value recorded for the SQL Server in Relativity. See Use the CN property of a SQL Server certificate in Relativity on the next page.

#### 8.7.1 Install a SQL Server certificate in the Analytics server KeyStore

Complete the following steps to install a SQL Server's certificate in your Analytics server KeyStore:

1. Export the SQL Server's certificate in X.509 DER format and place a copy of the certificate on the Analytics server.
2. Note the CN property value recorded in the certificate.
3. Open the following directory in a command prompt on your Analytics server:

   `<CAAT install drive>\jdk1.x\jre\lib\security`
The <CAAT install drive> reference represents the Analytics server installation folder, and x represents the version of the JDK installed on your Analytics server. Browse to the security directory using Windows Explorer first to ensure you use the correct Analytics server installation path.

4. Run the following command from the command prompt:
   
   `..\bin\keytool.exe -import -alias <CN> -keystore cacerts -file <path to cert file from Step 1>`
   
   Replace <CN> with the CN property recorded in the SQL Server's certificate and replace <path to cert file from Step 1> with the path location of the certificate file you copied to the Analytics server.

5. Enter your Java KeyStore password followed by yes when prompted to install the certificate.

   **Note:** This step is only required if your Java KeyStore is password protected. Please refer to Oracle for default Java password information.

### 8.7.2 Use the CN property of a SQL Server certificate in Relativity

When running an Analytics server with a SQL Server that uses SSL encryption, the name of the SQL Server recorded on the **Servers** tab in Relativity and the name entered during Analytics server installation must match the **CN** value recorded in the SQL Server's security certificate. When running the Relativity Analytics Server installation, enter the **CN** property value from your SQL Server's certificate in the **Primary Database Server Instance** field on the Primary Database Server Configuration dialog.

   **Note:** If your SQL Server's **Name** value recorded on the **Servers** tab in Relativity doesn't match the **CN** property in the SQL Server's security certificate, contact [support@relativity.com](mailto:support@relativity.com) for assistance with updating the SQL Server name in Relativity. Change the SQL Server's **Name** value in Relativity after you complete the Analytics installation.

### 8.8 Changing the REST password

If you need to change the REST password, perform the following steps:

1. Rerun the Analytics installer and enter the new password in the **REST Password** field.
2. Go to the **Servers** tab in Relativity select the Analytics server.
3. Enter the new password in the now-optional **REST API password** field and click **Save**.

### 8.9 Uninstalling the Relativity Analytics server

We don’t recommend uninstalling the Relativity Analytics Server application for any reason as it causes data loss. If you uninstall the Relativity Analytics Server application from the analytics server, all structured analytics sets created in Relativity 8.2 and higher can't be used with another installation. There is no way to merge a previous Relativity Analytics Server installation with a new installation. As a result, structured analytics sets created in Relativity 8.2 and higher become unusable.

You shouldn't uninstall the application from the server unless you're certain you won't use the server for Analytics functionality in the future, and you understand that uninstalling Relativity Analytics renders structured analytics sets created in Relativity 8.2 and higher unusable.
If you still need to uninstall the Relativity Analytics components from the server, complete the following steps:

1. Click your **Start** menu.
2. Select **Add or remove programs**.
3. Right-click on **Relativity Analytics Server** and select **Uninstall**.

Uninstalling the Relativity Analytics server automatically:

- Removes the version key from the registry
- Unregisters the Windows Service

**Note:** When you uninstall Relativity Analytics server, the indexes aren't deleted. However, any structured analytics sets created in Relativity 8.2 and higher are no longer usable.
9 Upgrading Data Grid

There are two strategies for upgrading your Data Grid instance:

- Shut down the entire cluster (all nodes), upgrade, and then restart your nodes. Shut down the master node first to ensure Relativity doesn’t send reads or writes to the cluster, then shut down the client node, then the data nodes. When you bring the nodes back up, start with the data nodes, then the client node, then the master node.

- Take one node down, upgrade it, restart it, and then repeat those steps for each node. Upgrade the data nodes first, then upgrade the client node, then upgrade the master node.

Before upgrading Data Grid, perform the following:

- Verify that no reads or writes to Data Grid occur during the upgrade process.
- Disable all migration agents.
- Verify that all imports or publishing from processing have stopped.
- Save a backup of one set of your old lib and bin folders to mitigate the possibility of restoration. Don’t save the backup files to the installer folder.

Note that you must turn off recovery mode on the cluster to avoid automatic re-balancing of shards during cluster maintenance. The re-balancing process can be resource intensive. Since you’re upgrading with your cluster in a controlled state (maintenance), you can turn off re-balancing. See Restarting nodes and clusters on page 100 for instructions.

The Data Grid service requires access to SQL Server, and specifically needs to have read, write, and bulk permissions for all workspace databases.

9.1 Upgrading a node

Use the following steps to upgrade a node from an old version of Data Grid to the latest version:

1. Prepare your cluster for node restart before uninstalling the kService. See Preparing the cluster for node restart on page 100 for more information.

2. Extract the Elasticsearch upgrade folder to the desktop of each machine on the cluster.

3. Open the elasticsearch-main folder that contains the previous version of Data Grid.

4. Uninstall the previous version of the kService by opening a command prompt to the following path:

   C:\RelativityDataGrid\elasticsearch-main

5. Enter the following command:

   bin\kservice.bat stop

6. Press Enter.

7. Enter the following command:

   bin\kservice.bat remove
8. Press **Enter**.
9. Delete the old lib and bin folders from `C:\RelativityDataGrid\elasticsearch-main`.
10. Copy the lib and bin folders from the new version of Data Grid copied onto your desktop in step one, and paste them into `C:\RelativityDataGrid\elasticsearch-main`.
11. If you are also upgrading Java versions, open the command prompt and run the following command:

```bash
SETX /M KCURA_JAVA_HOME "C:\Program Files\java\jdk1.8.0_45"
```

**Note:** The previous example assumes you are upgrading to Java 8 Update 45 (64-bit). Edit the version number appropriately.

12. Press **Enter**.
13. Close and reopen the command prompt, and navigate to the following path:

```
C:\RelativityDataGrid\elasticsearch-main
```
14. Enter the following command:

```
bin\kservice.bat install
```
15. Press **Enter**.
16. Run the GUI manager to reset the Java and Log On values, which were reset when you uninstalled. To do this, perform the following steps:
   a. Enter `\kservice.bat manager` and press **Enter**.
   b. Click the Java tab and configure the **Maximum memory pool** to be **30 GB** or half of the total RAM available (whichever is less). You can enter identical values for the **Initial memory pool** and **Maximum memory pool** settings. It's recommended that you keep the **Thread stacks size** value at its default of **256**.
Elasticsearch (elasticsearch-service-x64) Properties

General  Log On  Logging  Java  Startup  Shutdown

- Use default
- Java Virtual Machine:
  c:\program files\java\jre\bin\server\vm.dll

- Java Classpath:
  ;C:\RelativityDataGrid\lib\elasticsearch-###.jar;C:\RelativityDataGrid\lib

- Java Options:
  -XX:+UseParNewGC
  -Xms256m
  -Xmx1g
  -Djava.awt.headless=true

- Initial memory pool: 4096 MB
- Maximum memory pool: 4096 MB
- Thread stack size: 256 KB

OK  Cancel  Apply
c. Select the **Log On** tab. In the **Log on as** setting, select **This account**. Enter a valid Relativity service account domain name and password and confirm the password.

![Elasticsearch Properties](image)

<table>
<thead>
<tr>
<th>Log on as:</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Local System account</td>
<td>[ ] Allow service to interact with desktop</td>
<td>[ ] This account:</td>
<td>domain\relativity.service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Browse...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Password:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Confirm Password:</td>
</tr>
</tbody>
</table>

**Click OK.**

e. Return to the command prompt.

17. **Enter the following command:**

```
bin\kservice.bat start
```

18. **Press Enter.**

19. **Navigate to the endpoint (localhost:9200) and verify the version number field matches the latest version.** It should look similar to the following image:
20. Once all nodes are upgraded, turn recovery mode back on in the cluster. See Restarting nodes and clusters on page 100 for instructions.
10 Configuring Shield authentication

Shield allows you to easily protect your data from unintentional modification or unauthorized access while simplifying your architecture. Without Shield, anyone who knows the correct endpoint or URL can query, update, or delete all data in Data Grid. With default Shield installation, only Relativity can access Data Grid data, and all traffic between servers is encrypted. In addition, system admins can specify custom authentication realms so that targeted users can interact with Data Grid data outside of Relativity (via plugins and endpoints).

When you install Data Grid 2.1.2, Shield is enabled by default; however, you still need to configure Shield's authentication on every node.

The basic procedure for configuring Shield authentication is the following:

1. Install the authenticate Shield plugin on every node. See Installing the Shield plugins.
2. Configure custom authentication. See Configuring custom authentication.
4. Enable SSL in the node configuration. See Enabling SSL in the node configuration.
5. Restart Data Grid.

Note: With Shield on by default, other plugins like Marvel or Head aren’t operational until you configure Kibana to use your other plugins. For information on configuring Kibana, see Configuring Kibana to work with Shield.

10.1 Installing the Shield plugins

To install the authenticate and Shield plugins, perform the following steps on every node:

1. Copy the authenticate and Shield plugins from the elasticsearch-main\plugins folder in the zip file to the plugins folder.
2. Restart Data Grid.

Note: Relativity 9.3.389.9 includes a change to the Shield plugin. Data Grid no longer needs to send credentials back to Relativity for verification, which enhances security between Data Grid and Relativity. If you adopted Shield before Relativity 9.3.389.9, we recommend you update your elasticsearch.yml file with the new Shield configuration on every node to get the benefits of this change to Data Grid authentication. For more information, see Installing Data Grid 2.1.2.

10.2 Configuring custom authentication

With Shield authentication, you can also specify custom authentication that allows targeted users to interact with Data Grid data outside of Relativity. To specify custom authentication, you must first define roles in the roles.yml file, located in <installDirectory>\plugins\shield\config\roles.yml, and assign users to roles using your preferred authentication realm.
10.2.1 Defining roles

The roles.yml file contains a default role called admin, which Relativity uses to access the data stored in Relativity. The admin role has complete system admin rights to all data stored in Data Grid.

**Note:** The node manages the roles.yml file locally; the cluster doesn't manage the yml file globally. This means that with a typical multi-node cluster, you need to apply the exact same changes on each and every node in the cluster. A safer approach would be to apply the change on one of the nodes and have the roles.yml distributed/copied to all other nodes in the cluster (either manually or using a configuration management system such as Puppet or Chef).

If you want to create a new role with a different permission set, you must configure the roles.yml file to specify the unique role name(s) and the cluster and indices permissions associated with it. For example:

```
# All cluster rights
# All operations on all indices
admin:
  cluster: all
  indices:
    '*':
      privileges: all

# Monitoring cluster privileges
# All operations on all indices
power_user:
  cluster: monitor
  indices:
    '*':
      privileges: all

# Only read operations on indices
user:
  indices:
    '*':
      privileges: read

# Only read operations on indices named events_*
events_user:
  indices:
    'events_*':
      privileges: read
```

See the complete list of cluster and indices privileges [here](#).

Once you create your roles, you can create users using any of the following authentication realms and associate them to a role to determine the level of permissions they have to access data stored in Data Grid.

10.2.2 Elastic Shield realm

Using the Elastic Shield realm allows you to add a user to your cluster and specify a password. This realm is not recommended because it potentially undermines Shield authentication.

To configure the Elastic Shield realm:
1. Open the command prompt and navigate to `elasticsearch/bin/shield`.
2. Enter the following command to add a new user to your cluster and specify a password for that user:
   ```
   esusers useradd <username> -p <secret>
   ```
3. To add users to roles, enter the following command.
   ```
   esusers roles <username> -a <comma-separated list of roles> -r <comma-separated list of roles>
   ```
   The `-a` option adds a comma-separated list of roles to a user. The `-r` option removes a comma-separated list of roles from a user.

### 10.2.3 LDAP realm

To integrate with LDAP you must configure an LDAP realm and assign LDAP groups to Shield roles in the role mapping file.

To configure the LDAP realm with User search, add the following settings to the `elasticsearch.yml` file in a text editor:

```yaml
shield.authc.realms:
  ldap1:
    type: ldap
    order: 1
    url: "LDAP://Test-DC01.testing.corp:389"
    bind_dn: "CN=Administrator,CN=Users,DC=testing,DC=corp"
    bind_password: P@ssw0rd@1
    user_search:
      base_dn: "DC=testing,DC=corp"
      attribute: sAMAccountName
    group_search:
      base_dn: "DC=testing,DC=corp"
```

**Settings with User template**

To configure the LDAP realm with User templates, add the following settings to the `elasticsearch.yml` file in a text editor:

```yaml
ldap2:
  type: ldap
  order: 2
  url: "LDAP://Test-DC01.testing.corp:389"
  user_dn_templates:
    - "cn={0},OU=Testing - Users,DC=testing,DC=corp"
  group_search:
    base_dn: "DC=testing,DC=corp"
```

To assign LDAP groups to Shield roles, add the following settings for your user to the `role_mapping.yml` file in a text editor:

```yaml
admin:
  - "OU=Testing - Admins,DC=testing,DC=corp"
  - "OU=Testing - Users,DC=testing,DC=corp"
  - "CN=Jane Smith,OU=Testing - Users,DC=testing,DC=corp"
```
10.2.4 Active Directory (AD) realm
To configure the Active Directory realm, add the following settings to the elasticsearch.yml file in a text editor:

```
active_directory:
  type: active_directory
  order: 2
  domain_name: testing.corp
  url: ldap://testing.corp:636
  user_dn_templates:
    - "CN=Administrator,OU=Testing - Users,DC=testing,DC=corp"
  group_search:
    base_dn: "DC=testing,DC=corp"
```

10.3 Installing an X.509 certificate
Installing an X.509 certificate consists of the following tasks:

1. Create a keystore and generate a node certificate.
2. Create a certificate signing request (CSR).
3. Send the certificate to your certificate authority (CA) for signing OR set up your certificate authority to sign the certificate.
4. Add the signed certificate to the node's keystore.

10.3.1 Create a keystore and generate a keypair
1. Create a keystore and import your certificate authority's (CA) certificate or a trusted certificate using Java Keytool. This process configures the node to trust certificates signed by the CA. For example, the following command creates a keystore for node01 and imports the CA certificate cacert.pem. Local self-signed certificates are not recommended. The keytool can be found in the following:

   ```
   cd \Program Files\Java\jdk1.8.*\bin keytool -importcert -keystore node01.jks -file cacert.pem -alias my_ca
   ```

   The Java keystore file (.jks) securely stores certificates for the node. The CA cert must be a PEM encoded certificate. If you need to convert your certificate to PEM file, you can use a tool such as OpenSSL to convert a certificate.

   When you create a keystore, you are prompted to set a password. This password protects the integrity of the keystore. You need to provide it whenever you interact with the keystore.

   **Note:** When the CA certificate expires, you must update the node’s keystore with the new CA certificate.

   You can also store the CA certificate in a separate truststore. For more information, see Configuring a truststore.

   2. Generate a private key and certificate for the node with Java Keytool. For example, the following command creates a key and certificate for node01:
This command creates an RSA private key with a key size of 2048 bits and a public certificate that is valid for 712 days. The key and certificate are stored in the node01.jks keystore.

The `san` value specifies all alternative names for the node. The generated certificate is valid for the DNS names and IP addresses specified as alternative names. You can specify multiple DNS or IP address entries as a comma-separated list.

When you run `keytool -genkey`, Keytool prompts you for the information needed to populate the node’s distinguished name that’s stored the certificate. Use a trusted domain wildcard certificate that can be trusted among many nodes. For example:

```
What is your first and last name?
[Unknown]: *.domain.corp

What is the name of your organizational unit?
[Unknown]: test

What is the name of your organization?
[Unknown]: Relativity

What is the name of your City or Locality?
[Unknown]: Chicago

What is the name of your State or Province?
[Unknown]: Illinois

What is the two-letter country code for this unit?
[Unknown]: US

Is CN=*.domain.corp, OU=test, O=Relativity, L=Chicago, ST=Illinois, C=US correct?
[no]: yes

Enter key password for <node01>
(RETURN if same as keystore password):
```

10.3.2 Create a certificate signing request (CSR)

A node’s certificate needs to be signed by a trusted CA for the certificate to be trusted. To get a certificate signed, you need to create a certificate signing request (CSR) and send it to your CA.

To create a CSR with Java Keytool, use the `keytool -certreq` command. You specify the same alias, keystore, key algorithm, and DNS names and IP addresses that you used when you created the node certificate. Specify where you want to store the CSR with the `-file` option.

```
keytool -certreq -alias node01 -keystore node01.jks -file node01.csr -keyalg rsa -ext
san=dns:*domain.corp,ip:192.168.1.1
```

10.3.3 Send the certificate to your certificate authority (CA) for signing

To get a signed certificate, send the generated CSR file to your CA. The CA will sign it and send you the signed version of the certificate.
10.3.4 Install the signed certificate
To install the signed certificate, use `keytool -importcert` to add it to the node’s keystore. You specify the same alias and keystore that you used when you created the node certificate.

```
cd CONFIG_DIR/shield
keytool -importcert -keystore node01.jks -file node01-signed.crt -alias node01
```

10.4 Enabling SSL in the node configuration
Once you’ve added the signed certificate to the node’s keystore, you need to modify the node configuration to enable SSL then restart Data Grid.

To enable SSL, make the following changes in `elasticsearch.yml`:

1. Specify the location of the node’s keystore and the password(s) needed to access the node’s certificate. For example:

   ```
system
   shield.ssl.keystore.path: /home/es/config/shield/node01.jks
   shield.ssl.keystore.password: myPass
   shield.ssl.keystore.key_password: myKeyPass
   shield.ssl.hostname_verification: false
   
   The first line indicates the full path to the node keystore file. This must be a location within the Data Grid configuration directory.
   2. Enable SSL on the transport networking layer to ensure that communication between nodes is encrypted:

      ```
system
      shield.transport.ssl: true
      
      3. Enable SSL on the HTTP layer to ensure that communication between HTTP clients and the cluster is encrypted:

         ```
system
         trueshield.http.ssl: true
         
         4. Restart Data Grid so these configuration changes take effect.

10.5 Configuring Kibana to work with Shield
When you install or update to Relativity 9.3, Shield is enabled by default. With Shield on by default, other plugins like Marvel or Head are not supported. In order to use your other plugins, you need to provide the Kibana server with credentials so it can access the .kibana index and monitor the cluster.

To configure credentials for the Kibana server:

1. Assign the `kibana4_server` role to a user in Shield. For more information, see Configuring a Role for the Kibana 4 Server in the Shield documentation.

2. Set the `kibana_elasticsearch_username` and `kibana_elasticsearch_password` properties in `kibana.yml` to specify the credentials of the user you assigned to the `kibana4_server` role:

   ```
   kibana_elasticsearch_username: kibana4-user
   kibana_elasticsearch_password: kibana4-password
   ```
3. Update the following setting in kibana.yml to false:

```
elasticsearch.ssl.verify: false
```

Kibana 4 users also need access to the .kibana index so they can save and load searches, visualizations, and dashboards. For more information, see Configuring Roles for Kibana 4 Users in the Shield documentation.
11 Restarting nodes and clusters

Because of the way that Data Grid rebalances data as nodes enter and exit the cluster, you must be careful when bringing down clusters or nodes for maintenance. This page explains how to restart nodes and clusters.

11.1 Preparing the cluster for node restart

Data Grid automatically detects when a data node leaves the cluster and immediately rebalances data across the cluster while accounting for the node's absence. Each time the cluster re-balances, there is a cost to your server resources. If you have a window of maintenance time, you can turn off automatic recovery re-balancing by setting the node to persistent and the cluster.routing.allocation.enable configuration value to "none."

**Note:** Run any of the Sense queries below on a client node except when executing a shutdown. Run shutdown queries on a master node unless you only want to shut down a specific node locally. Run shutdown queries for the entire cluster on the master node so that all nodes shut down before the master node. If you want to run a shutdown locally, you can run it on that specific node instead of the master.

Before restarting a node, disable your Data Grid Audit Migrator agents and stop all indexing and importing in all Data Grid-enabled workspaces for five minutes. This will allow the sync process to complete before you begin the node restart process.

Run the following command to turn off re-balancing and set the cluster to persistent. The synced flush ensures that all shards have been synced after five minutes. The persistent state ensures that re-balancing stays off when the cluster restarts.

```
GET _cluster/settings
POST /_all/_flush/synced
PUT _cluster/settings
{
  "persistent":{"cluster.routing.allocation.enable": "none"}
}
```

11.2 Shutting down a node

Use the following steps to shut down a node:

1. Run the Windows command prompt as an administrator.
2. Navigate to the bin directory in the RelativityDataGrid folder.
   
   ```
   C:\RelativityDataGrid\elasticsearch-main\bin
   ```
3. Stop the Data Grid service by running the following command:
   
   ```
   .\kservice.bat stop
   ```
11.3 Restarting a node

Before restarting the node, apply the following cluster setting:

```json
PUT /_cluster/settings
{
  "persistent" : {"cluster.routing.allocation.balance.threshold" : "100.0f"
}
}
```

You must restart the Data Grid service on each node individually to bring the cluster back up online. Use the following steps to restart a node:

1. Run the Windows command prompt as an administrator.
2. Navigate to the bin directory in the RelativityDataGrid folder.

   ```sh
   C:\RelativityDataGrid\elasticsearch-main\bin
   ```
3. Start the Data Grid service by running the following command and wait for the cluster to go from red to yellow:

   ```sh
   .\kservice.bat start
   ```
4. Use the following command to re-enable re-balancing of shards:

   ```json
   PUT _cluster/settings
   { 
     "persistent":{"cluster.routingallocation.enable": "all"}
   }
   ```

Once the node restarts and displays a green status, re-apply the following default setting:

```json
PUT /_cluster/settings
{ 
  "persistent" : {"cluster.routing.allocation.balance.threshold" : "1.0f"
}
}
```

11.4 Restarting a cluster

Use the following command before restarting a cluster:

```sh
GET _cluster/settings
PUT _cluster/settings
{ 
  "persistent":{"cluster.routingallocation.enable": "none"}
}
```

Once all nodes come back green, use the following command to re-enable allocation:

```json
PUT _cluster/settings
{ 
  "persistent":{"cluster.routing.allocation.enable": "all"}
}
```
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.

©2019. Relativity ODA LLC. All rights reserved. Relativity® are registered trademarks of Relativity ODA LLC.