



Authentication Guide

May 10, 2024 | Version 12.3.805.2

For the most recent version of this document, visit our [documentation website](#).

Table of Contents

1 Authentication	4
1.1 Authentication overview	4
1.1.1 Authentication methods	4
1.1.2 Authentication object model	5
1.1.3 Authentication object permissions	6
1.2 Configuring Relativity authentication	6
1.2.1 Enabling authentication provider types	6
1.2.2 Creating authentication providers	6
1.2.3 Assigning a login method to individual users	7
1.3 Authentication provider settings	7
1.4 OpenID Connect with Microsoft Azure AD	9
1.4.1 Configuring your external identity provider	9
1.4.2 Configuring this method in Relativity	14
1.4.3 Completing your external identity provider set up	15
1.4.4 Adding users to the application in Azure	19
1.5 Using Relativity as an OpenID Connect Provider	20
1.6 SAML 2.0 provider	22
1.6.1 Configuring Okta as a SAML 2.0 identity provider	23
1.6.2 Configuring ADFS as a SAML 2.0 identity provider	28
2 Authentication procedures	30
2.1 Setting IP address range	30
2.2 Configuring integrated authentication	31
2.3 Sending Email	31
2.4 RSA configuration	32
3 Logging into Relativity	34
3.1 Logging in to Relativity with a password	34
3.2 Password	34
3.3 Two-factor authentication	34
3.4 Active Directory	36
3.5 Integrated Authentication	37

3.6 RSA	37
3.7 OpenID Connect	37
3.8 SAML 2.0	38
3.9 Creating or resetting a password	38
4 Managing user authentication methods	41
4.1 Invitation workflow	41
4.1.1 Password	41
4.1.2 Two-factor authentication	42
4.1.3 Password Outside Trusted IP	43
4.1.4 Password reset	44
4.2 Manually setting passwords	44
4.3 Active Directory	45
4.4 Integrated Authentication	45
4.5 OpenID Connect	46
4.6 SAML 2.0	46
4.7 RSA	47
5 OAuth2 clients	48
5.1 Creating or editing an OAuth2 client	48
5.2 Resetting a client secret	50
5.3 Deleting an OAuth2 client	50
Viewing an OAuth2 client audit history	51
6 Federated instances	52
6.1 Creating or editing a federated instance	52
6.2 Deleting a federated instance	53
Viewing a federated instance audit history	53

1 Authentication

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

If you are upgrading from a prior version of Relativity, there are some important differences to be aware of. See the following page:

- [Upgrade considerations for Relativity - Authentication](#)

1.1 Authentication overview

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

1.1.1 Authentication methods

Relativity supports the following authentication mechanisms.

- **Password**—a method that includes a username, the user's email address, and a password.
- **RSA**—a method using an RSA SecurID token, a third party security solution, and validates credentials from an RSA server.
- **Active Directory**—a method using an email address and user's Active Directory password.
- **Integrated Authentication**—previously called Windows authentication. A method using a directory service, such as Kerberos or NTLM (NT LAN Manager). The authentication attempt is automatically initiated if the user logs in from a specific IP address range.
- **OpenID Connect**—a protocol for an external identity provider, authenticating against an external identity provider using the OpenID Connect protocol. OpenID Connect is a modern authentication protocol can be used to connect to providers such as Azure Active Directory. See [OpenID Connect](#) for more information.
- **SAML 2.0**—a method that authenticates against an external identity provider using the SAML 2.0 protocol. SAML 2.0 is an older authentication protocol that is still in widespread use. See [SAML 2.0](#) for more information.

Notes:

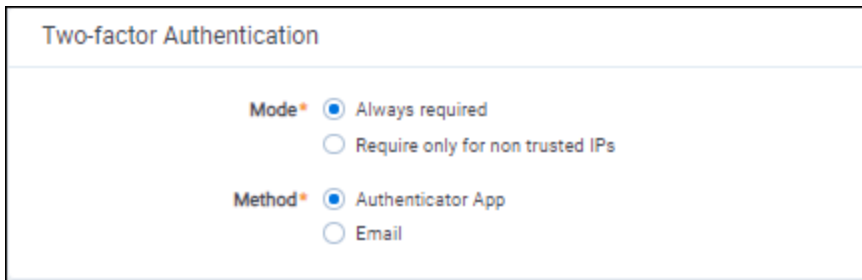
- When implementing single sign-on (SSO) across Relativity instances, the following scenarios are supported:
 - Identity Provider-initiated SSO using SAML 2.0
 - ID provider and service provider-initiated SSO with OpenID Connect

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

- **Two-factor Authentication**—when logging in with the Password method, you can require the user to pass an additional two-factor check based on an email or message sent to the user's phone

through a mobile email gateway.

- **Mode**—always required or require only for non-trusted IPs
- **Method**—authenticator app or email. For more information, see the authenticator app's documentation.



The screenshot shows a configuration window titled "Two-factor Authentication". It contains two sections: "Mode" and "Method". Under "Mode", there are two radio buttons: "Always required" (which is selected) and "Require only for non trusted IPs". Under "Method", there are two radio buttons: "Authenticator App" (which is selected) and "Email".

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

1.1.2 Authentication object model

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

Authentication Provider Type. Each authentication protocol is represented by an Authentication Provider Type object. You can navigate to the **Authentication Provider Type** tab in Home mode to see all of the environment's protocols and whether they are enabled or not. In Relativity you can disable specific Provider Types that you do not intend to use in your environment. As a best practice you should disable any Provider Types that will not be used.

Note: Users log in to the Relativity Desktop Client (RDC) with the same provider method as they have with Relativity. The RDC supports most Relativity authentication providers, such as password, Integrated Authentication, and OpenID Connect, by displaying the Relativity login page within the RDC as a dialog window. The only provider that does not work with the RDC is SAML because the Relativity's IdP-initiated SAML does not display the Relativity login page directly.

Authentication Provider. Authentication Providers allow you to configure the specific settings for a login protocol. For example, you can add the Password Provider to your environment to set minimum and maximum password length, password history settings, and more. Some protocols have multiple configuration options, while others have very few. Every instance of Relativity has Default Password, Default Integrated Authentication, Default Active Directory, Default RSA, and Default Smart Card providers. You cannot have additional, non-default, providers of those types.

You can add OpenID Connect and SAML 2.0 external identity providers. Unlike the previous five protocols, you can have as many of these Providers as you wish in an environment.

Login Method. The **AuthenticationData** field on the User page has been replaced with the Login Method associated list. Users can have one or more Login method objects that binds that user to a particular Authentication Provider. For example, if you have a Password Authentication Provider in the environment, the Password Login Method contains the specific password for a given user. If you have Azure Active Directory configured as a Provider, each user's AAD subject identifier would be stored in an associated Login method.

User. The User object still holds the TrustedIPs setting. By setting a TrustedIP for a user, that user will only be able to authenticate with Relativity from that IP range. All other authentication-related fields have been moved from the User object to the Provider and Method objects.

1.1.3 Authentication object permissions

These default object permissions are recommended for managing user authentication:

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

1.2 Configuring Relativity authentication

System admins must assign users at least one authentication method in order for users to log in. To create and to assign methods, follow these steps.

1.2.1 Enabling authentication provider types

Authentication Provider Types are Relativity dynamic object (RDOs) types that permit authentication methods for users to log in with. You cannot add or delete provider types, only enable or disable them. By default, provider types are enabled. You enable methods in two places: the authentication provider type tab and the authentication providers tab. To be enabled, the method has to be enabled in both places.

To enable or disable an authentication provider type:

1. Select **Authentication Provider Type** tab.
2. Click on a provider type name. The Authentication Provider Information section appears.
3. Click **Edit**.
4. Select Enabled status **Yes** or **No**. **Yes** enables those methods, and **No** disables them throughout the Relativity instance.
5. Click **Save**.

1.2.2 Creating authentication providers

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

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

You may only have one instance of each provider type. The exceptions are for OpenID Provider and SAML 2.0 provided types. You can have multiple instances of those if they have different names.

To create an Authentication Provider:

1. Select the **Authentication Provider** tab.
2. Click the **New Authentication Provider** button.
3. Enter a **Name**. This is the friendly name of the provider instance.
4. Optionally select the **Enabled** status. By default, each authentication provider is enabled. If not enabled, then users cannot log in with that method.
5. Select a **Provider Type** from among the authentication provider types. You can select OpenID Connect or SAML2.
The **Authentication Provider Settings** section appears.
6. Set the Authentication Provider Settings, if any. See [Authentication provider settings below](#) for the specific method.
7. Click **Save**.

1.2.3 Assigning a login method to individual users

You assign an authentication method to each user for them to log in with. Each user must have at least one authentication method in order for them to log in but you may assign multiple methods. See [Managing user authentication methods on page 41](#).

1.3 Authentication provider settings

Authentication providers may have associated settings that you can configure and applies to all instances of that authentication provider.

Each provider instance has at least one setting: Enabled. If set to **Yes**, this authentication provider is available. If **No**, you cannot use this method to log in with. To enable an instance both this setting and the Enabled for the Authentication Provider must be set to **Yes**. If either one is set to **No**, that method is not available for the user.

Authentication providers that do not require additional settings:

- **Default Integrated Authentication provider**
- **Default Active Directory provider**
- **Default RSA provider**
You may need to set RSA configuration files to the web server prior to users logging in with this method. See [RSA configuration on page 32](#) for additional details.

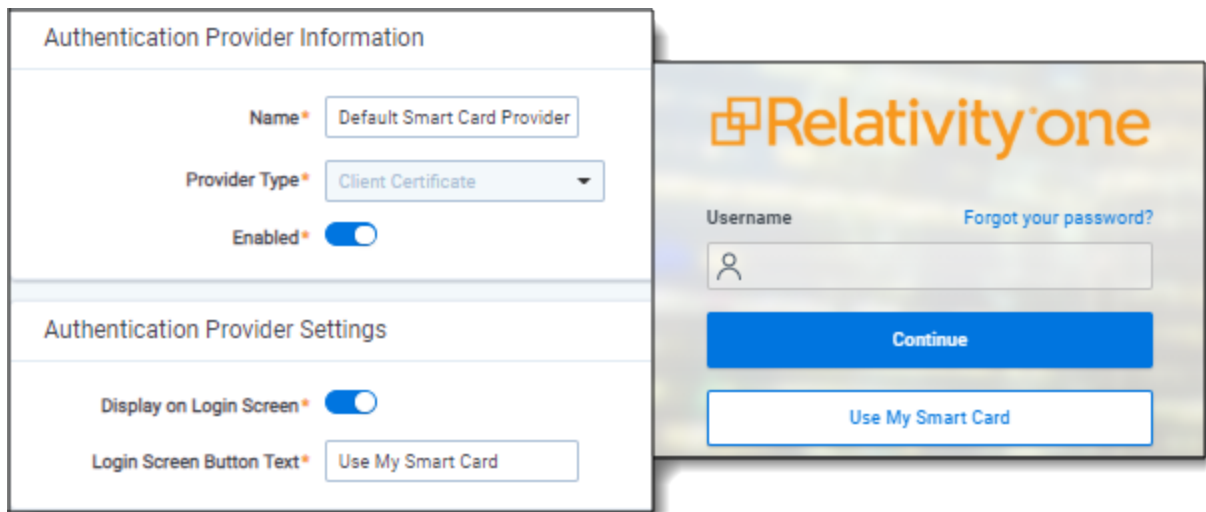
Authentication providers that require additional settings:

- **Default Password provider**—additional settings for the Default Password provider include:
 - **Minimum Password Length**—sets the minimum number of characters for a password.
 - **Maximum Password Length**—sets the maximum number of characters for a password.
 - **Maximum Password Attempts Before Reset Required**—sets the maximum number of consecutive unsuccessful login attempts before being locked out. You must send the user a password reset request before they can attempt to log in again.
 - **Maximum Password Age (in days)**—sets the maximum number of days a password remains valid. The user will be prompted for a new password on a log on at the expiration date. If set to zero, the password does not expire.
 - **Users Can Change Password Default**—enables the user to change their password.
 - **Allow Password Recovery via Email**—enables the user to use email to recover a forgotten password. **Yes** displays the Forgot Password link on the user's login screen.
 - **Password Recovery Request Limit**—sets the maximum number of password resets before Relativity locks out the user. You must send the user a password reset request before they can attempt to log in again. This value resets to zero on each successful log in.
 - **Maximum Password History**—sets the maximum number of previous passwords that users cannot use for a new password. The default value of zero enables any previous password.
 - **Additional Work Factor**—increases the number of encryption hashes. Relativity already provides several built in hash levels represented by the default zero value. Changing this value to 1, 2, or 3 adds additional encryption protection but may significantly increase login time.

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

- **Default smart card provider** - additional settings for the Default smart card provider include:
 - **Display on Login Page**—determines if the client certificate button displays in the login screen.
 - **Login Screen Button Text**—sets the client certificate button text.

The example below illustrates the relationship between the two settings and the login screen.



- **OpenID Connect with Microsoft Azure AD**—see [OpenID Connect with Microsoft Azure AD below](#).
- **SAML 2.0 provider**—see [SAML 2.0 provider on page 22](#).

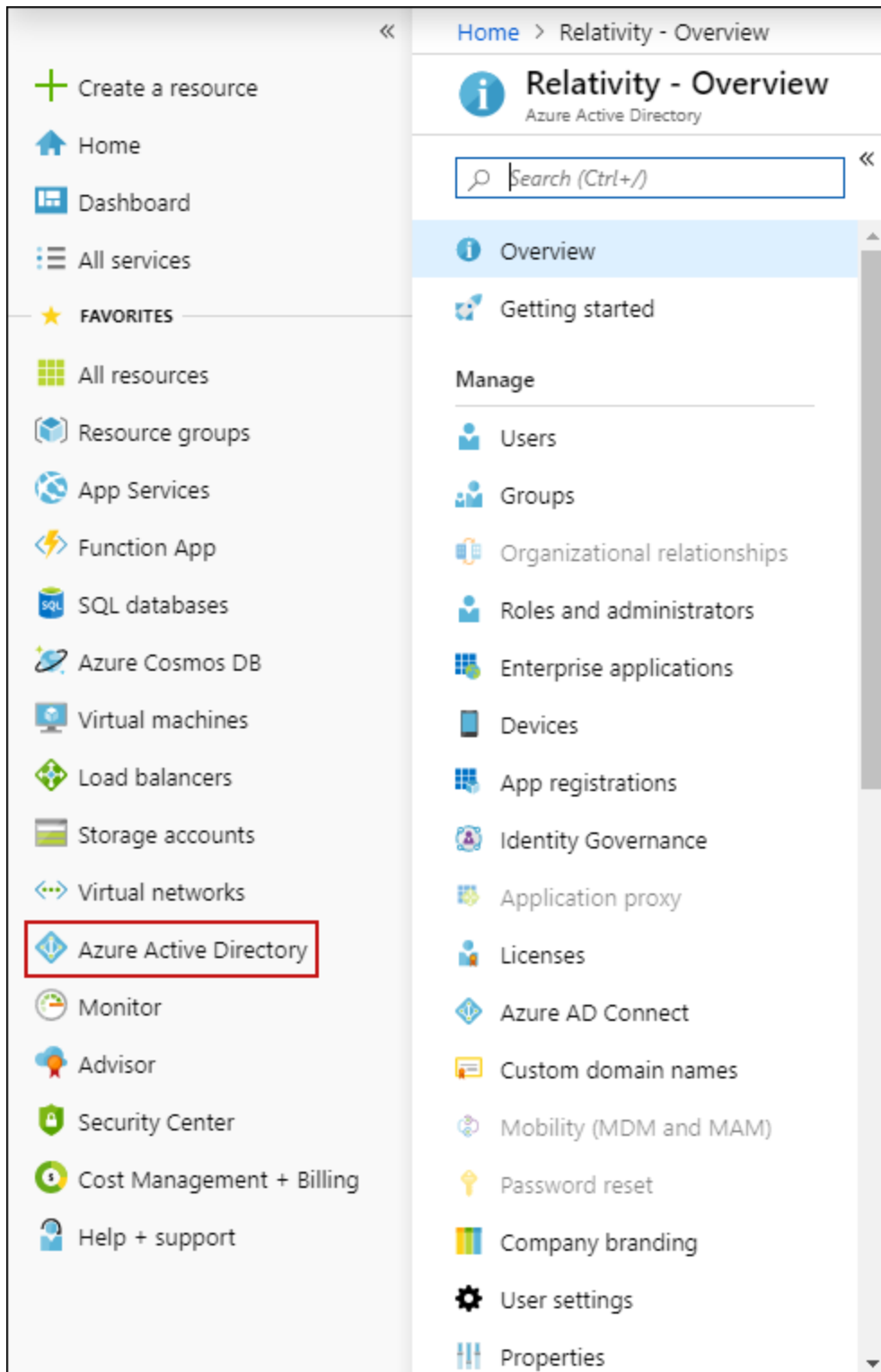
1.4 OpenID Connect with Microsoft Azure AD

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. Clients can verify the identity of the end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user. You can use any provider that supports the OpenID Connect protocol. The examples here use Microsoft Azure AD.

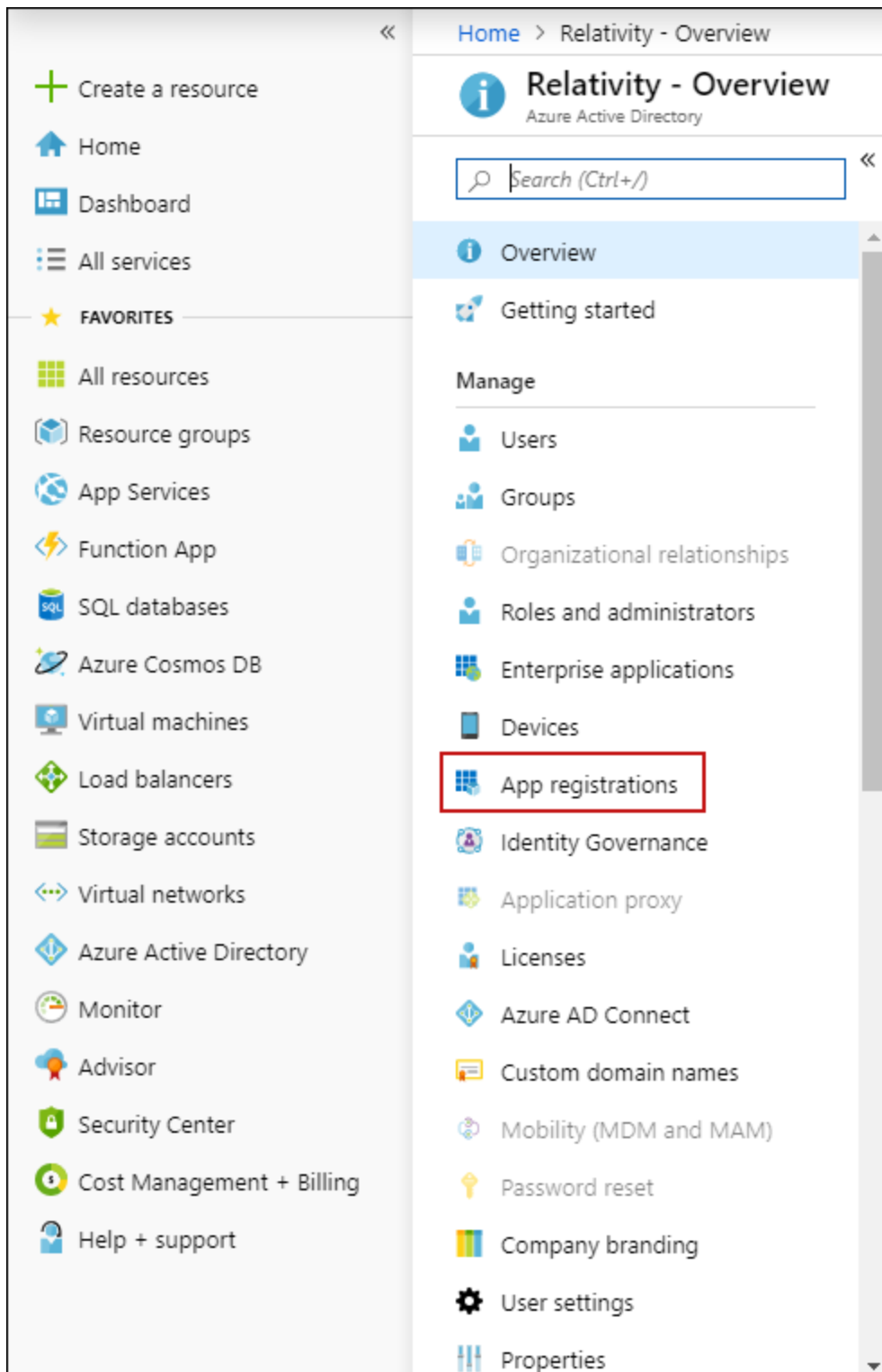
Note: OpenID Connect 1.0 authentication providers are not compatible with Relativity User Load Balancing (RULB).

1.4.1 Configuring your external identity provider

1. Log in to Azure Portal.
2. Click **Azure Active Directory**.



3. Click **App registrations**.



4. Click **New registration**.

5. Give the application a name.

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

 ✓

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Relativity only - Single tenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

[By proceeding, you agree to the Microsoft Platform Policies](#)

Register

6. Click **Register**.
7. Copy the Application (client) ID.

Relativity SSO

Search (Ctrl+*/*)

- Overview
- Quickstart
- Manage
 - Branding
 - Authentication
 - Certificates & secrets
 - API permissions
 - Expose an API
 - Owners
 - Roles and administrators (Previ...
 - Manifest
- Support + Troubleshooting
 - Troubleshooting
 - New support request

Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn


Display name : Relativity SSO

Application (client) ID : [REDACTED]

Directory (tenant) ID : [REDACTED]

Object ID : [REDACTED]

Call APIs

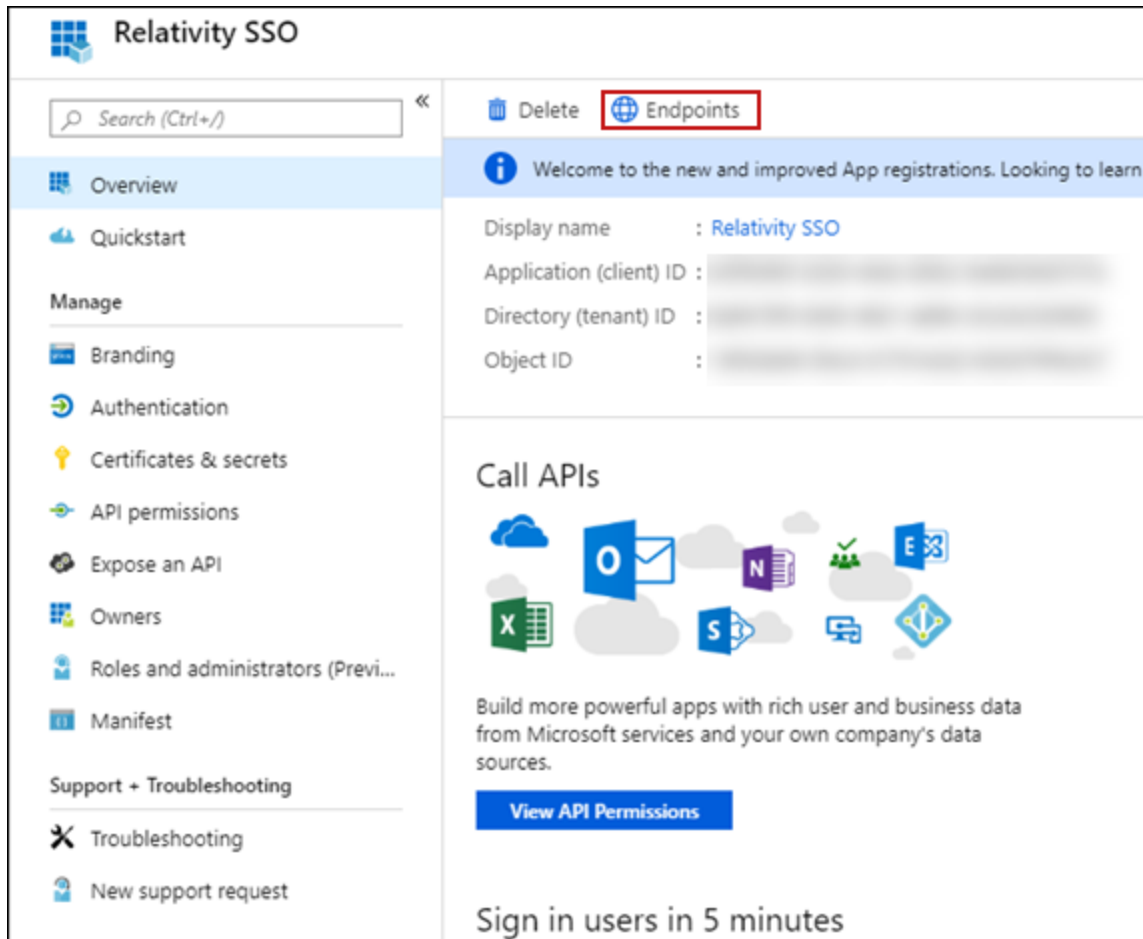


Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

[View API Permissions](#)

Sign in users in 5 minutes

8. Click the **Endpoints** button.



9. Copy the OAuth 2.0 authorization endpoint (v2) URL.
10. Trim the `oauth2/v2.0/authorize` from the URL. For example:

```
https://login.microsoftonline.com/8a3fa923-3223-4978-9d4d-fa012e19898b/oauth2/authorize  
https://login.microsoftonline.com/8a3fa923-3223-4978-9d4d-fa012e19898b/
```

1.4.2 Configuring this method in Relativity

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

1.4.2.1 Authentication Provider Information

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

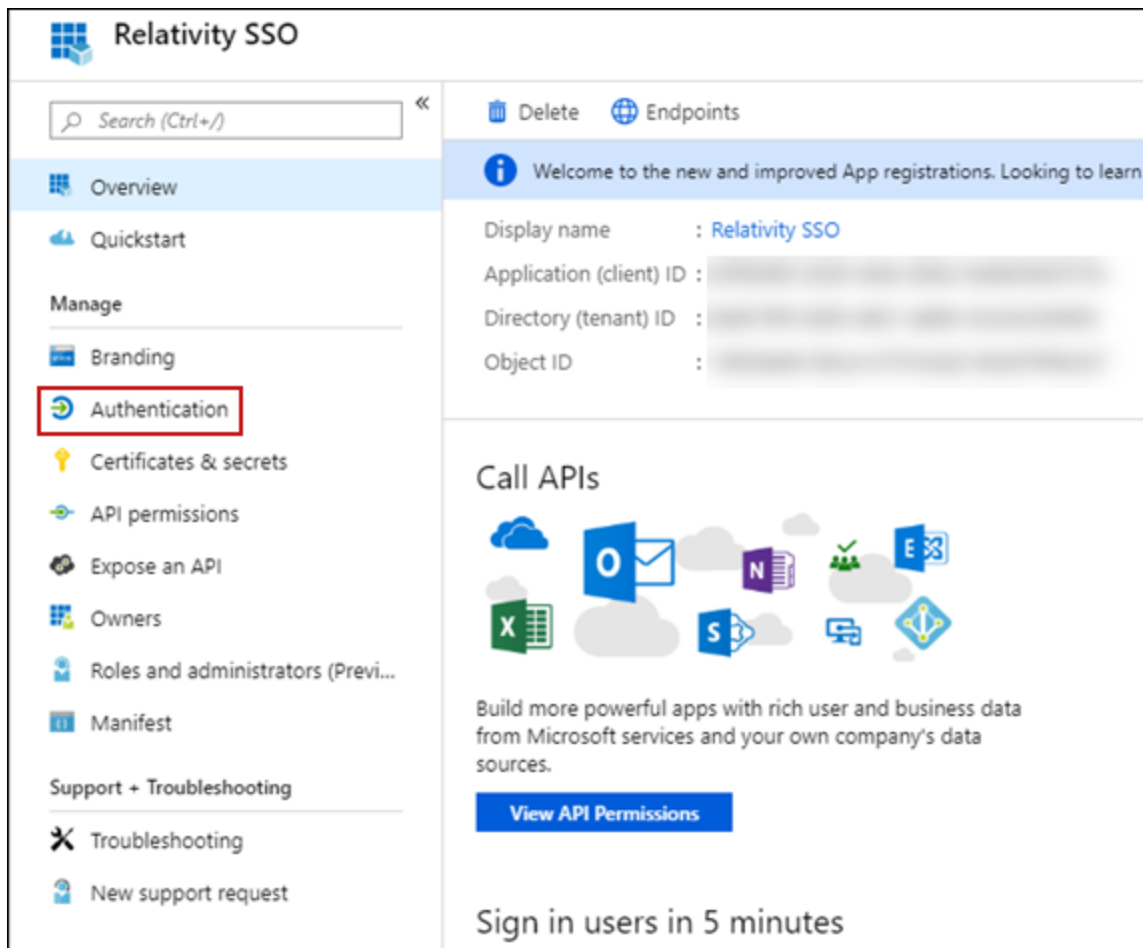
1.4.2.2 Authentication Provider Settings

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

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

1.4.3 Completing your external identity provider set up

1. Log in to Azure AD and navigate to the application you created earlier, if you have closed the window.
2. Click **Authentication**.

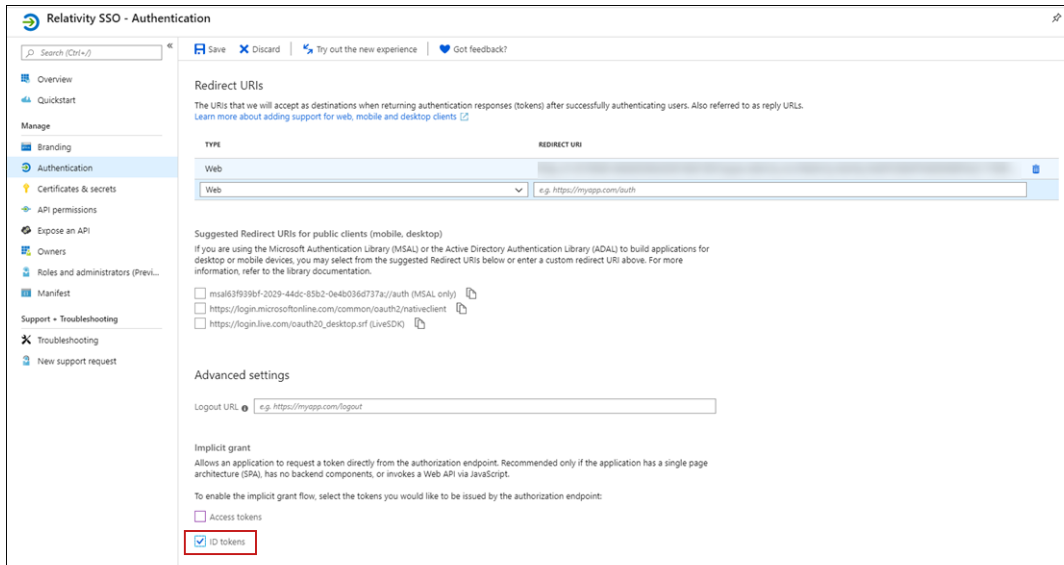


3. Add your Redirect URL from the Relativity Authentication Provider.

Note: Leave the Type as Web.

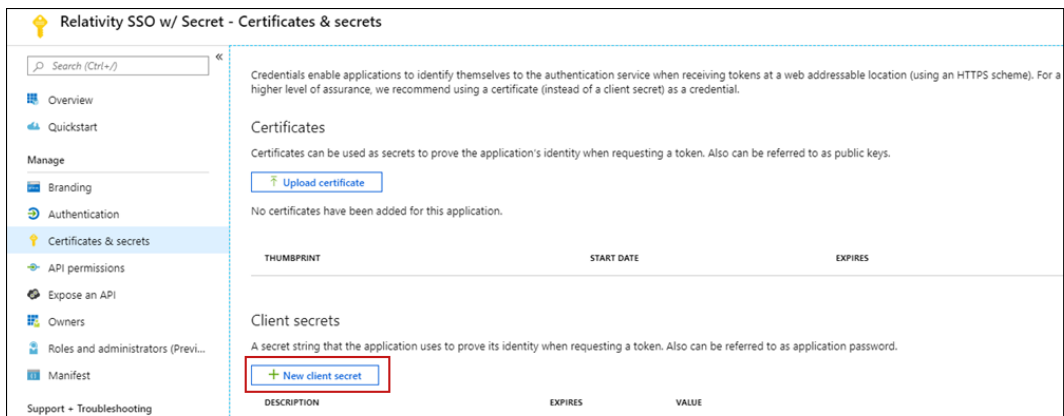
4. Complete the scenario that matches the value you selected for OAuth2 Flow.

- Scenario: you selected **Implicit** for OAuth2 Flow.
 - Check the **ID Tokens** box.



- Click **Save**.

- Scenario: you selected **Code** for OAuth2 Flow.
 - Click **Certificates & Secrets**.
 - Click **New client secret**.



- Click **Add**.

Add a client secret

Description

Expires

In 1 year

In 2 years

Never

Add Cancel

- Copy the client secret value.
- Navigate back to the Authentication Provider in Relativity.
- Click **Edit**.
- Paste the value for Client Secret with the value from step 4.

The image shows a configuration interface for an authentication provider, divided into two sections: 'Authentication Provider Information' and 'Authentication Provider Settings'.

Authentication Provider Information:

- Name*: AzureADProvider
- Provider Type*: OpenID Connect
- Enabled*:
- Site URL*: https://documentation-a.r1.1

Authentication Provider Settings:

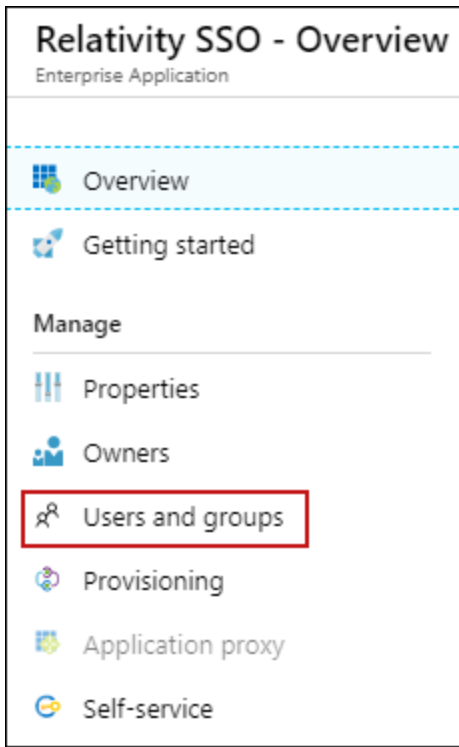
- OAuth2 Flow*: Code
- Client ID*: 1a2b345c-d67e-8901-2345-f
- Client Secret*: DocumentationExample (highlighted with a red arrow)
- Display on Login Screen*:
- Login Screen Button Text*: Team Azure Test
- Authority URL*: https://login.microsoftonline
- Scopes*: openid, email, profile
- Subject Claim Type*: sub
- Alternative Issuer(s):

- Click **Save**.

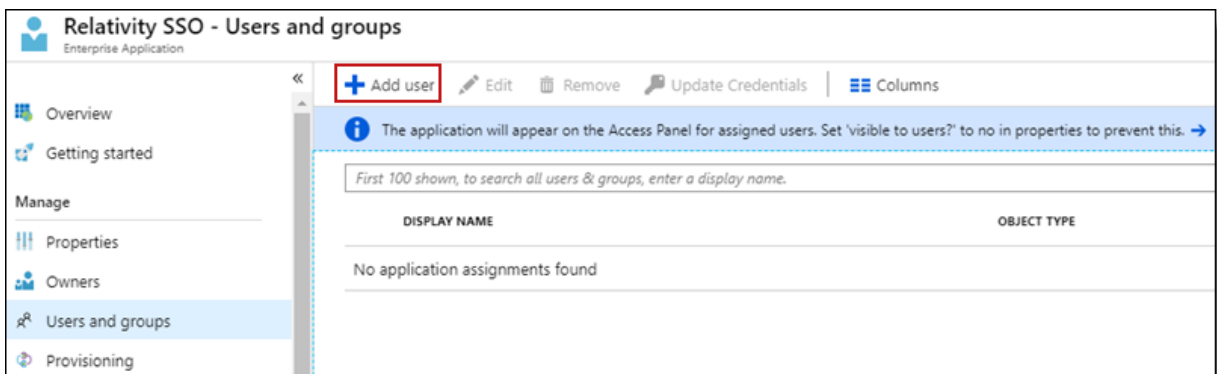
1.4.4 Adding users to the application in Azure

1. Click **Azure Active Directory**.
2. Click **Enterprise Applications**.
3. Click into the application that you have created for Relativity authentication.

4. Click **Users and groups**.



5. Click **Add user**.



6. Select your users.
7. Click **Assign**.

1.5 Using Relativity as an OpenID Connect Provider

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

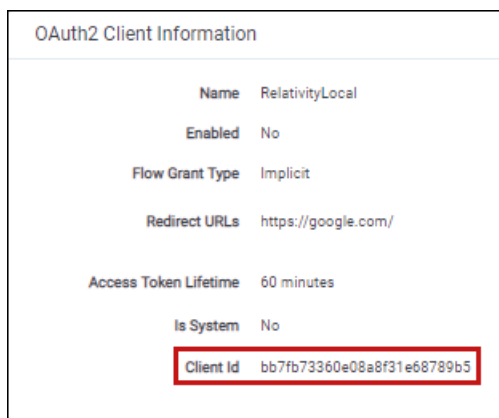
Before you begin:

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

Configuring an OpenID Connect provider for Relativity

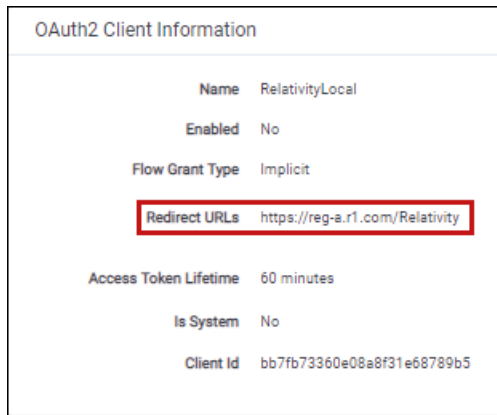
To configure an OpenID Connect provider for Relativity:

1. Navigate to the primary instance and set up an OAuth2 client. You must specify Implicit as the OAuth2 Flow.
Initially, you do not have the redirect URL value. You get it when you set up the Authentication Provider on the secondary instance. Specify any placeholder URL instead. For more information, see [OAuth2 clients on page 48](#).
2. After you save the OAuth2 client, note the generated value of the Client Id. This is required to set up the authentication provider in the secondary instance.

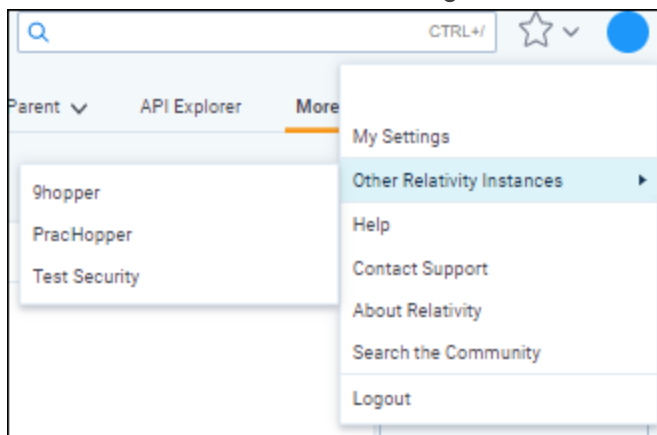


3. Navigate to the secondary instance and configure a new OpenID Connect authentication provider using the Client Id value from the previous step.
The OAuth2 Flow values must also be Implicit, and the Authority URL must point to the Relativity Identity service of the primary instance. An example of a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

6. Navigate back to the primary instance and update the OAuth2 provider with the Redirect URL.



7. In the primary instance, set up a federated instance pointing to the secondary Relativity instance. Note the use of the Home Realm Discovery (HRD) URL parameter to provide a single sign-on experience. The Home Realm discovery URL is generated when the Authentication Provider is created and can be found in the Authentication Provider Information section of the Authentication Provider page. For more information, see [Federated instances on page 52](#).
8. Navigate back to the secondary instance and set up a federated instance pointing to the primary Relativity instance. Do not set up the HRD redirect for that federated instance.
9. Log out of the secondary instance.
10. Use the federated instance link to log in to the secondary instance from the primary instance.



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

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

1.6 SAML 2.0 provider

SAML is an open-standard format for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP). As a service provider, Relativity supports SAML IdP-initiated single sign-on (SSO). SP-initiated SSO is not supported. Relativity uses SAML assertions (tokens) to verify

the users mapped to the identity provider.

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

Note: SAML assertions must be cryptographically signed for Relativity to verify their authenticity. Make sure your SAML IdP is configured accordingly.

You can use Relativity with any SAML 2.0-compliant IdP, such as Centrify, Okta, Microsoft Active Directory Federation Service (ADFS), or OneLogin.

Note: SAML 2.0 authentication providers are not compatible with Relativity User Load Balancing (RULB).

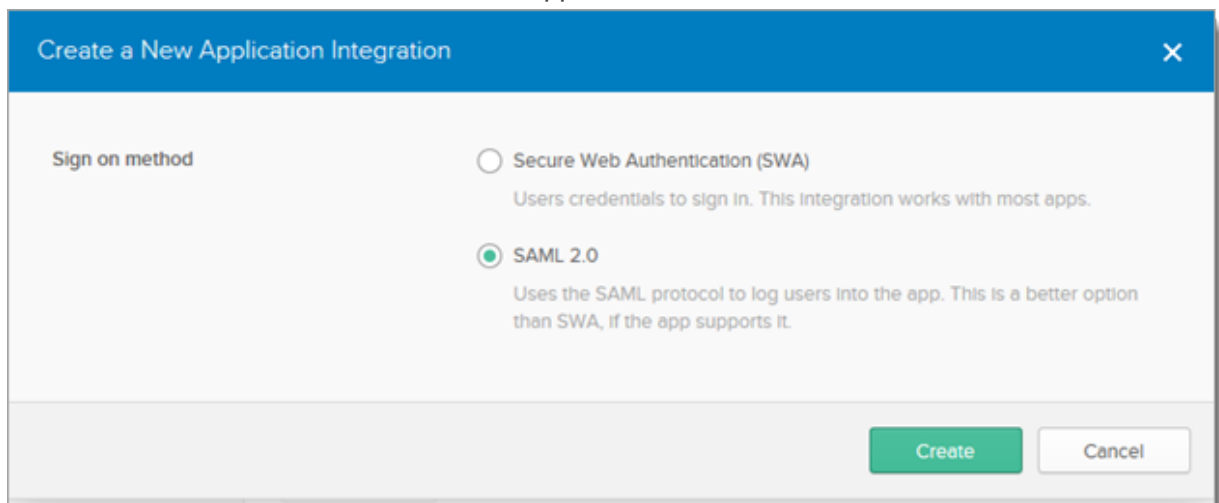
The following sections provides the guidelines for integrating Relativity with Okta and [ADFS](#).

1.6.1 Configuring Okta as a SAML 2.0 identity provider

This is an example of configuring Okta.

Initial configuration:

1. In Okta admin console, create a SAML 2.0 application:



2. Specify these SAML settings:

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

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

- Application user name you would like to use for logging in. In this use case, select **Email**.
- For Assertion Signature, select Signed.

A SAML Settings

GENERAL

Single sign on URL ? Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

[Hide Advanced Settings](#)

Response ?

Assertion Signature ?

Signature Algorithm ?

Digest Algorithm ?

Assertion Encryption ?

Enable Single Logout ? Allow application to Initiate Single Logout

Authentication context class ?

Honor Force Authentication ?

SAML Issuer ID ?

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text"/>

- You have now partially configured you application in Okta to set up logging in to Relativity. You must now configure the SAML provider in Relativity. You need these Okta values:

- The Audience URI. SP Entity ID, from the previous step.
- The Identity Provider Issuer. In Okta, click **View Setup Instructions** on the Sign On tab.
- The X.509 Certificate. Also in Setup instructions.

2 Identity Provider Issuer:

http://www.okta.com/exk6jszbyx1cCJMB0h7

3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDmJCCAoKgAwIBAgIGAUsUVd/yMA0GCSqGSIb3DQEBBQUAMIGNMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNU2FueIEZyYW5jaXNjbzENMAAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdm1kZXIxDjAMBgNVBAMMBWtjdXJhMRwwGgYJKoZIhvcNAQkBFg1pbmZv
QG9rdGEuY29tMB4XDTE1MDEyMzAxMDgwN1oXDTE1MDEyMzAxMDkwN1owGy0xCzAJBgNVBAYTA1VT
MRMwEQYDVQQIDApDYWxpZm9ybmlhMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQ0wCwYDVQQKDARP
a3RhMRQwEgYDVQQQLDAtTU09Qcm92aWR1c2EOMAwGA1UEAwwFa2N1cmExHDAaBgkqhkiG9w0BCQEW
DW1uZm9Ab2t0YS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQNfXqI5by9TIUL
mt9cEaLomn1DjgqbgOf1gzT7yz9koJEtEb67n+5h4ZeFocghHcX1chGRAPSDeqHV4aAiR/7kX0E
G5hac4a1BWGAmF4gwz79bzATssCEaTSMyaa2JvRRSW1tuGFDv9r5Hzn2wb6IGwG0xK7SWCGn8WY2
iMpneQJbbJVgk53yuHj05kfAwVM2cMiY3seib112A6xYbWzoan2726Lefcs53EvnG0qnB11xGvkx
Ho/GSYBG7eDpgUBhssy+nB8/v5qQnb2hc3yV+X8o6fVcaykHnmuywXt/j6J1Y10/YBThjhV/jDw+
LRbgwVYbrhrF4AHMeF9HB/9AgMBAEEwDQYJKoZIhvcNAQEFBQADggEBAF1xHSmkNWT1WQpx8zJe
myWzBJX12XBSa86ZoSCUu61PVfF13yg6dg1mW3EY7WrOkDggi2bujqFZKGA5vvL1QNkyGhr+2PQ9
BykYFduSZWUHV+v4oxNVzdHs+/h06PURK+hwtssQyv0N1c3Qr79eHHp11ZMcV5Z1jMFDJQQ9q4
rqc6F8mULUrFf83pJ/286XcMC+jaAkkxdhIeR0Isia+zgUgc4kHiH+NIMND29sp4Id0FKu7bteH5
NiWfD+PAG1RX3pJvHRXUZiUHuIZHQ1dy3HY01kA2vYz6+6u/+UZWLsol01JeomS+LVQ/mcK9mnT
/H8zmJmJz+mkcFsyu6k=
-----END CERTIFICATE-----
```

Download certificate

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

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

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

The screenshot shows a configuration page for an authentication provider. It is divided into two main sections: "Authentication Provider Information" and "Authentication Provider Settings".

Authentication Provider Information:

- Name:** OktaProvider
- Provider Type:** SAML2 (selected in a dropdown menu)
- Enabled:** A toggle switch is turned on.
- Site URL:** https://mycompany.com/Re

Authentication Provider Settings:

- Audience:** https://mycompany.com/Re
- Issuer URL:** https://www.okta.com/exk6
- Certificate:** A text area containing a base64-encoded X.509 certificate. The text starts with "-----BEGIN CERTIFICATE-----" and ends with "-----".
- Subject Claim Type:** An empty text input field.

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

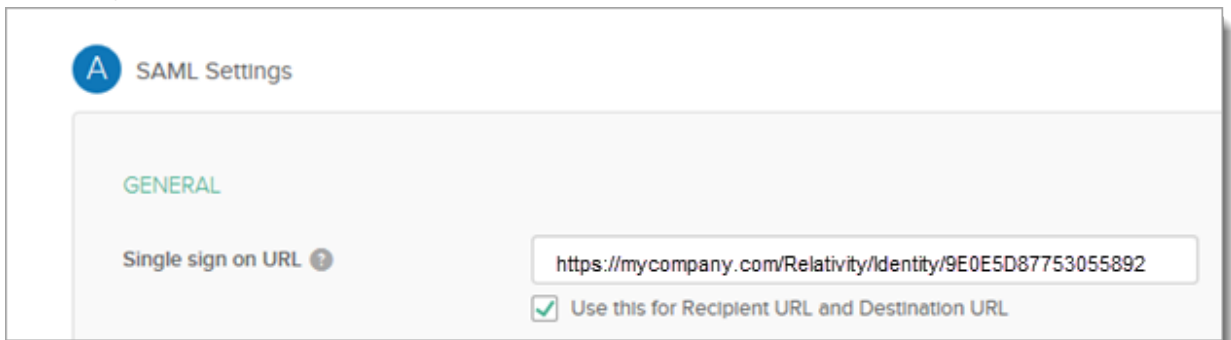
11. Click **Save**.
12. Note the Redirect URL on your new authentication provider.



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

Next, finish setting up the SAML IdP in Okta:

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



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

Note: You must also assign Okta users to the SAML application, and then map the users to SAML login method in Relativity. When configuring the login method, you must specify the user's email in the SAML2 Subject field, if you select Email as the application user name in Okta. For more information, see [Managing user authentication methods on page 41](#).

1.6.2 Configuring ADFS as a SAML 2.0 identity provider

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

Note these terminology difference between Relativity and ADFS:

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

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

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

2 Authentication procedures

- [Sending Email on the next page](#)

2.1 Setting IP address range

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

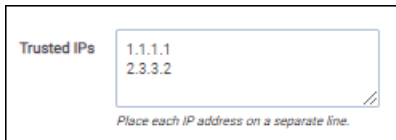
The first uses the instance setting `Relativity.Authentication.WindowsAuthIpRange` to define the valid range for the Relativity instance. The default defines all IP addresses as valid.

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

Note: The settings (`WindowsAuthIpRange` and Trusted IP range) cannot be used to prevent users from logging in if they access Relativity from the same server where it is installed. To secure Relativity login from the server where it is installed, you must disable non-admin user remote access to the server.

To set the user Trusted IP range:

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



5. Click **Save**.

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

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

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

	Description	Example
Asterisk (*) (Asterisk wildcard)	Matches zero or more characters.	192.168.31.*. You can't use this notation with the match range of digits wildcard.
Hash (#) (Hash wildcard)	Matches any single digit 0-9.	192.168.31.##. You can't use this notation with the match range of digits wildcard.

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

2.2 Configuring integrated authentication

Enabling a server to accept integrated authentication log ins must be configured explicitly. You use the **UseWindowsAuthentication** and **WindowsAuthIpRange** instance settings to define integrated authentication behavior. Integrated authentication follow these guidelines.

- If **UseWindowsAuthentication** is **False**, then integrated authentication can't be used. In this case, Relativity ignores the **WindowsAuthIpRange** value.
- If **UseWindowsAuthentication** is **True** and **WindowsAuthIpRange** isn't set, then integrated authentication will always be used regardless of IP address.
- If **UseWindowsAuthentication** is **True** and **WindowsAuthIpRange** is an IP address or address range, then Integrated Authentication is used when the computer's IP address falls within the **WindowsAuthIpRange** value. If the IP address falls outside the **WindowsAuthIpRange**, the log in screen displays other assigned log in methods.

You can configure your environment so that some Web servers use Integrated Authentication, while others don't use it. To specify a server to use integrated authentication , create a new instance setting of **UseWindowsAuthentication**with the following values:

- Set **MachineName** to the web server name
- Set **Value** to **True**.

You must create a new **UseWindowsAuthentication** instance setting for each server

2.3 Sending Email

Several authentication providers may send email, such as part of a two factor password authentication or a password reset. You will need an SMTP server. Contact your IT system admin for additional details. Use the following instance settings to define the emails addresses and body text. For more information, see the Instance setting guide.

- **AuthenticationEmailFrom** - sets the email address that appears in the From field of email messages that contain authentication information for users.
- **EmailFrom** - sets the email address populated in the "From" field when sending email notifications.
- **ForgotPasswordRequestEmailFrom** - sets the value in the From field for the forgotten password request email message.

2.4 RSA configuration

Before you integrate RSA SecurID with Relativity, you must complete the following tasks:

- Make sure that your web server has a 64-bit version of the Windows operating system.
- Install Relativity, and verify that it is working properly.
- Set up the RSA Authentication Manager server. Relativity 2023 supports RSA Authentication Manager 8.1.

Note: Relativity isn't certified to work with any version of *RSA Authentication Agent for Web for Internet Information Services*.

- Set up the Authentication agent on the RSA Authentication Manager server. You can add this agent through the RSA Security Console, where you must set the **Agent Type** field to **Standard Agent**. The RSA Authentication Manager server uses this setting to communicate with Relativity. For more information, see the documentation provided for your RSA Authentication Manager server.

Note: You must add one agent for each web server in your Relativity environment. For example, if there are two web servers, set up two Authentication agents on the RSA Authentication Manager server.

You must copy the RSA configuration files to your Relativity web server before you configure RSA authentication in Relativity.

Use the following procedure to copy the required RSA configuration files:

1. Open the **RSA Security Console**.
2. Locate the **sdconf.rec** and **sdopts.rec** configuration files in the console.
3. Download the **sdconf.rec** and **sdopts.rec** files to your machine.
4. Log in to the Relativity web server.
5. Copy these files to the `RSAConfigFilePath` directory. The following is the default path:

```
%SYSTEMDRIVE%\Program Files\kCura Corporation\Relativity\EDDS\RSA
```

Note: You can use a different location for your **RSAConfigFilePath** directory.

6. Update the value of the `RSAConfigFilePath` instance setting in the EDDS database with the location where you copied the files in step 5. See Instance setting table in the Relativity 2023 Documentation site.

Note: The RSAConfigFilePath value must include the drive letter. For example,

```
C:\Program Files\kCura Corporation\Relativity\EDDS\RSA
```

You cannot use the %SYSTEMDRIVE% environment variable.

7. Verify that the **DOMAIN\EDDSServiceAccount** has **Write** permissions to the RSAConfigFilePath directory. The Relativity application pool runs under the DOMAIN\EDDSServiceAccount account.

3 Logging into Relativity

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

3.1 Logging in to Relativity with a password

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

Note: The **Forgot your password?** link only displays if the admin enables Allow Password Recovery via Email setting, for more information see the Authentication Guide.

3.2 Password

This method uses only a user name and a password. Your system admin provides you with the following:

- Login email address.
- Password request email.

Prior to logging in, if you have not already, create your password. See [Creating or resetting a password on page 38](#).

To log in:

1. Navigate to the Relativity site.
2. Log in with your password. See [Logging in to Relativity with a password above](#)

3.3 Two-factor authentication

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

- Login email address.
- Password request email.

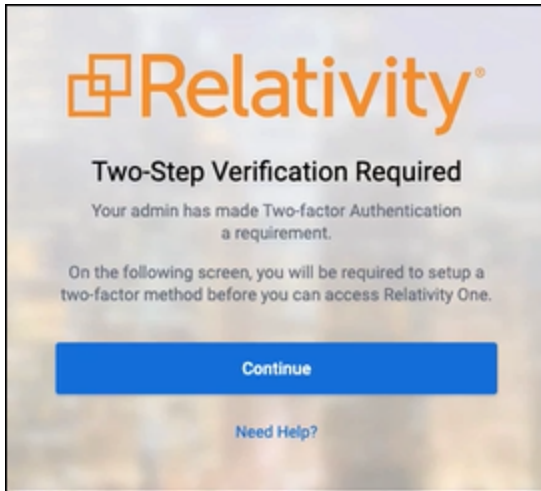
Prior to logging in, if you have not already, create your password. See [Creating or resetting a password on page 38](#).

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

Note: When using email for two-factor authentication, your web servers must have access to the SMTP server so it can distribute emails and passwords to authenticate.

To connect your authentication app,

1. Enter your user name.
2. Enter your password.
3. On the Two-Step Verification Required step, click **Continue**.



4. Open your authenticator app on your device.
5. In your app, tap the button to add a new account.
6. Hold phone up and scan the QR code provided by Relativity.



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

7. Click **Next**.

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

To log in with an authenticator app method:

1. Navigate to the Relativity site.
2. Log in with your password.
3. Follow the instructions on the app or enter the authentication code from the authentication app.
4. Click **Next**.

To log in with the Relativity email method:

1. Navigate to the Relativity site.
2. Log in with your password. An **Authenticate Login** dialog appears. The system immediately emails you a passcode, and the passcode will be different each time.
3. Enter that value in **Passcode**.



4. Click **Login**.

3.4 Active Directory

This method uses Microsoft Active Directory Domain Services to log in. You must log in from a computer within a valid domain. Your system admin provides you with the following:

- Login email address.
- An account on a Windows domain.
- Windows network password.

To log in:

1. Navigate to the Relativity site.
2. Enter your Relativity email address in **Username**.
3. Click **Continue**.
4. Enter your Windows network password in **Password**.
Contact your system admin or IT department for password requirements.
5. Click **Login**.

3.5 Integrated Authentication

This method uses Integrated Windows Authentication to log in. There are no additional requirements to log in other than having a Windows domain account.

To log in, navigate to the Relativity site. The system automatically logs you in to Relativity. If you are not connected or if the [Relativity logon dialog](#) appears, contact your system admin.

3.6 RSA

This method requires an RSA SecurID token along with a username and passcode. Your system admin provides you with the following:

- Username
- RSA SecurID token
- (Optional) PIN

To log in:

1. Navigate to the Relativity site.
2. Enter your username in **Username**.
3. Click **Continue**.
4. Enter your RSA password in **Password** in the format set by your system administrator. This password is either:
 - The RSA tokencode, the eight-digit number from the RSA SecurID token hardware, if you have not been assigned or created a PIN
 - Your combined PIN and RSA tokencode without a space between them
5. Click **Login**.

You may also be asked to create or to reset your PIN. Follow the instructions on those screens.

3.7 OpenID Connect

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

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

To log in:

1. Navigate to the Relativity site.
2. Click the Relativity OpenID Connect button name.
3. Enter your user name.
4. Click **Logon**.
5. Authenticate with your OpenID provider.

3.8 SAML 2.0

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

To log in:

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

3.9 Creating or resetting a password

Use this procedure if you are logging in to Relativity for the first time or if you are resetting your password. Your system admin must send you a password reset email. If you forget your password, you can click the **Forgot your password** link on the login screen if it is available, or contact your system admin. In either case, the system sends you a new password email.

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

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

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

[Reset Password](#)

We recommend opening this link in Internet Explorer.

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

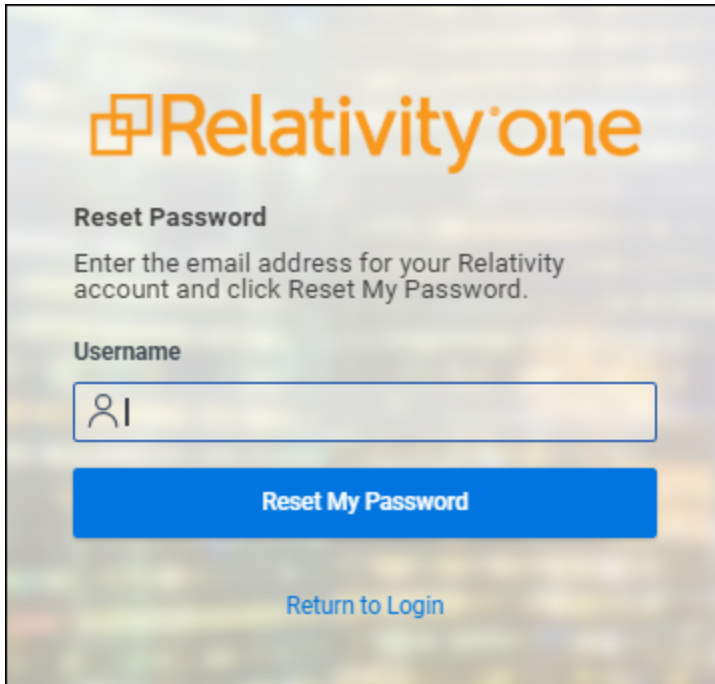
<https://ml14.testing.corp/Relativity/Identity/ResetPassword?token=74a572da-60e1-4058-2ffe-20b36965c0f9>

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

Please do not reply to this email.

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

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



Relativity one

Reset Password

Enter the email address for your Relativity account and click Reset My Password.

Username

Reset My Password

[Return to Login](#)

3. Click **Submit**.

4. Click **Return to Relativity**.

4 Managing user authentication methods

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

4.1 Invitation workflow

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

Note: For Relativity 9.4.378.21 and above, you must set the RelativityInstanceURLInstance setting if you want to use this feature and don't have OpenID Connect or SAML providers configured in your environment. Ensure that the value for this setting is the URL for your Relativity instance. For example, the URL would have the format: *https://example.relativity.com/Relativity*. The user receiving the invitation email must have access to this URL. For more information, see the Instance Settings Guide.

The invitation workflow applies to the following methods:

- [Password below](#)
- [Two-factor authentication on the next page](#)
- [Password Outside Trusted IP on page 43](#)

4.1.1 Password

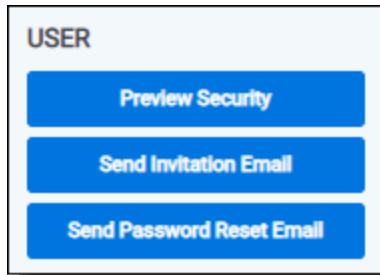
The password option requires the user to enter only a password for authentication. It does not require an additional check or two-factor criterion.

To assign and to configure this option for a user:

1. After creating a new user, edit their profile (**Users** tab, and click their full name).
2. In the **Login Method (User)** section, click **New**.
3. In the **Login Method Information** pop-up window, select the password provider method from the Provider drop-down list. The password provider name may vary for each Relativity instance. See [Authentication on page 4](#) for creating and naming a password method instance. The **Default Password Settings** section appears.
4. Disable the **Enable Two-factor Authentication** toggle. For more information, see [Two-factor authentication on the next page](#).
5. Set the **Default Password Settings**.
 - **Can Change Password** - enable to let user change the password at any point.
 - **Require Change Password on Next Login** - enable to have user change given password.
 - **Maximum Password Age** - enable to set number of days a password can work. Set the num-

ber of days in the text box.

- **Set Password for User** - enable to create a password for the user.
6. Click **Save**.
 7. Click **Send Invitation Email**.



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

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

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

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

To customize the invitation email, use the following instance settings:

- **InvitationEmailRequestBody (Relativity.Authentication section)** - the invitation email message text. The email text must be formatted as HTML.
- **InvitationEmailRequestFrom (Relativity.Authentication section)** – the invitation email message sender's email address.
- **InvitationEmailRequestSubject (Relativity.Authentication section)** – the invitation email message subject.
- **InvitationLinkLifetimeInMin (Relativity.Authentication section)** – the number of minutes the link sent in the invitation email remains valid.

4.1.2 Two-factor authentication

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

To assign and configure this option for a user,

1. Edit their profile (**Users** tab, and click their full name).
2. In the **Login Method (User)** section, click **New**.
3. In the **Login Method Information** pop-up window, select the password provider method from the Provider drop-down list. The password provider name may vary for each Relativity instance. See

[Authentication on page 4](#) for creating and naming a password method instance. The **Default Password Settings** section appears.

4. Enable the **Enable Two-factor Authentication** toggle.
5. Select the **Mode**, "always provide passcode" or "ignore passcode for Trusted IPs."
6. Select the **Method**, use an "authenticator app" or "email" address.
7. Set the preferred **Default Password Settings**.
8. Click **Save**.

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

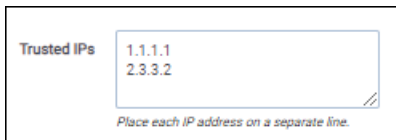
Note: The link in the email is valid for 5 minutes, and only the most recently-sent email can be used. The link expiration time is not configurable.

4.1.3 Password Outside Trusted IP

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

To define a Trusted IP range:

1. After creating a new user, edit their profile (**Users** tab, and click their full name).
2. In the **User Information** section enter the IP range in the **Trusted IPs** field.
You can specify an individual address, a range of IP addresses, or multiple addresses. Each address must be on a separate line, and you can use wildcards. For more information on setting trusted IP addresses, see [Setting IP address range on page 30](#). The default value of empty defines all IP addresses as untrusted. You can enter *.*.* to trust any IP address.



Note: Relativity only supports the IPV4 format for Trusted IP addresses. It doesn't support the IPV6 format.

3. Click **Save**.

To assign and to configure this option for a user:

1. After creating a new user, edit their profile (**Users** tab, and click their full name).
2. In the **Login Method (User)** section, click **New**.
3. In the **Login Method Information** section, select the password provider method from the Provider drop-down list. The password provider name may vary for each Relativity instance. See [Authentication on page 4](#) for creating and naming a password method instance. The **Login Method Settings**

section appears. You can assign only one instance from among Password, RSA, and Active Directory methods.

4. Select **Require only for non Trusted IPs** in the **Two-factor Authentication** section.
5. Enter the user's email address you want to send the password to in the Email Address field. This address can be different from the email in the user's profile.
6. Click **Save** and then **Back**.
7. Click **Send User Invitation Email**.

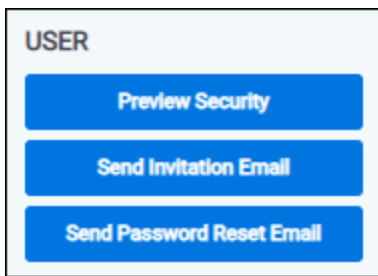
4.1.4 Password reset

Sometimes it may be necessary to reset a user's password. In Relativity, passwords are reset by sending the user an email with a reset link.

Note: If using a Relativity version earlier than 9.4.378.21, the **Send Password Reset Email** is also used to send out invitations for new users.

To reset a user's password:

- Click **Send Password Reset Email**.



The link within the email is valid for 15 minutes, and only the most recently sent email can be used.

Note: You can use the PasswordResetEmailExpirationInMinutes instance setting to increase the default reset link expiration period.

4.2 Manually setting passwords

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

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

To set a password, use the following procedure.

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

3. In the **Login Method Information** section, select the password provider method from the **Provider** drop-down list.
The password provider name may vary for each Relativity instance. See [Authentication on page 4](#) for creating and naming a password method instance. The **Login Method Settings** section appears. You can assign only one instance from among Password, RSA, and Active Directory methods.
4. Select **Set Password to True**.
The password requirements appear.
5. Enter the password in the **Password** field.
6. Re-enter the password in the **Retype Password** field.
7. Click **Save** and then **Back**.

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

4.3 Active Directory

The Active Directory method uses Windows Active Directory to authenticate the user.

To assign and to configure this option for a user.

1. After creating a new user, edit their profile (**Users** tab, and click their full name).
2. In the **Login Method (User)** section, click **New**.
3. In the **Login Method Information** section, select the active directory provider method from the **Provider** drop-down list. The provider name may vary for each Relativity instance. See [Authentication on page 4](#) for creating and naming a password method instance. The **Login Method Settings** section appears. You may have only one instance from among Password, Active Directory, or RSA methods.
4. Enter the user's Windows domain and username in **Active Directory Account**.
An example of the *domain\username* format is if the user's email address is *jsmith@example.com*, you'd enter *example\jsmith*. Alternatively, you can use the user's email address without the domain ending, such as *jsmith@example*. If an LDAP server is installed, you can use the full email address, such as *jsmith@example.com*.
5. Click **Save** and then **Back**.

4.4 Integrated Authentication

Integrated Authentication (previously called Windows Authentication or Integrated Windows Authentication) uses Windows supported authentication protocols, such as Kerberos, to automatically log in users. Make sure the following instance settings are configured correctly.

- **UseWindowsAuthentication** - must be set to **True** to use Integrated Authentication. If False, Integrated Authentication isn't active.
- **WindowsAuthIpRange** - set this to the IP address or addresses for a trusted range of computers. If a user logs in within the trusted IP range, they will automatically be logged in with their integrated

authentication credentials. If a user logs in outside of the trusted IP range, the user will be prompted with the login page. If the user has another assigned authentication method, they can use that to complete their login. The IP address can use wildcards.

To assign and to configure this option for a user:

1. After creating a new user, edit their profile (**Users** tab, and click their full name).
2. In the **Login Method (User)** section, click **New**.
3. In the **Login Method Information** section, select the integrated authentication provider method from the **Provider** drop-down list.
The provider name may vary for each Relativity instance. See [Authentication on page 4](#) for creating and naming a password method instance. The **Login Method Settings** section appears.
4. Enter the user's Windows domain and username in **Windows Account**.
An example of the *domain\username* format is if someone's email address is *jsmith@example.com*, you'd enter *example\jsmith*.
5. Click **Save** and then **Back**.

4.5 OpenID Connect

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

4.6 SAML 2.0

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

4.7 RSA

This method requires a user to have an RSA SecurID token that is registered with your RSA Authentication provider.

1. If you need to configure RSA files for the web server, see the [RSA configuration on page 32](#)
2. After creating a new user, edit their profile (**Users** tab, and click their full name).
3. In the **Login Method (User)** section, click **New**.
4. In the **Login Method Information** section, select the RSA provider method from the **Provider** drop-down list.
The provider name may vary for each Relativity instance. See [Authentication on page 4](#) for creating and naming a password method instance. The **Login Method Settings** section appears.
5. Enter the subject identifier for the authentication provider as the **RSA Subject**.
6. Click **Save** and then **Back**.

5 OAuth2 clients

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

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

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

To set up an OAuth2 client in Relativity, you must correctly determine the grant type required for your application. The OAuth2 client setup information also includes a client ID, a redirect URI, and a client secret key. These details will be used to validate your application and authorize the API calls. Occasionally it may be necessary to reset the client secret for security purposes.

5.1 Creating or editing an OAuth2 client

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

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

Note: You can't change the flow value when editing an OAuth2 client.

- **Implicit**—for lightweight browser-based or mobile applications typically implemented using a scripting language such as JavaScript. The implicit grant type is used to obtain access tokens (it does not support the issuance of refresh tokens) and is optimized for public clients known to operate a particular redirection URI. The client receives the access token as the result of the authorization request. This grant type does not require a client secret.
 - **Resource Owner**—suitable in cases where the resource owner has a trust relationship with the client, such as the device operating system or a highly privileged application. The authorization server should take special care when enabling this grant type and only allow it when other flows are not viable. This grant type can be used for clients capable of obtaining the resource owner's credentials (username and password, typically using a command line prompt). It is also used to migrate existing clients using direct authentication schemes such as HTTP Basic or Digest authentication to OAuth by converting the stored credentials to an access token. This grant type requires a client secret.
 - **Redirect URLs**—the URLs that the user can be redirected back to after the request is authorized. Specify values only if Implicit or Code are selected in the Flow field. The URLs must include the *http* or *https* protocol prefix.
 - **Context User**—Relativity user context for OAuth2 client authorization. This enables an administrator to restrict the access privileges on an OAuth2 client based on the user's permissions as well as audit. Context User is required if Client Credentials is selected as the OAuth2 flow, and can't be specified for other flows.
 - **Access Token Lifetime**—the duration (in minutes) for which access tokens issued to the clients are valid. The recommended value varies depending on the specified OAuth2 flow:
 - Client Credentials and Code Flow must have a short lifetime. It is recommended that the value match the Identity Server default of 1 hour (60). For more information, see [Identity Server documentation \(https://identityserver.github.io/Documentation/docsv2/configuration/clients.html\)](https://identityserver.github.io/Documentation/docsv2/configuration/clients.html).
 - Resource Owner access token must also have a lifetime of 1 hour because a client secret and a refresh token are available.
 - Implicit flow tokens must match Relativity's token lifetime of 10 hours (600), after which the user must log in again.
4. Click **Save**. The form displays the new OAuth2 client with these generated field values:
- **Enabled** – yes/no value indicating whether the client will be given access to Relativity.
 - **Flow Grant Type** - the mechanism for acquiring an authentication token also known as OAuth2 grant type.
 - **Redirect URLs** - the URLs that the user can be redirected back to after the request is authorized.

- **Access Token Lifetime** - the duration (in minutes) for which access tokens issued to the clients are valid.
- **IsSystem** – specifies whether the OAuth2 client is part of an internal Relativity application.

OAuth2 Client Information

Name *

Enabled

Flow Grant Type *

Access Token Lifetime *
Enter value in minutes

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

You have set up Relativity for access by an OAuth2 client application.

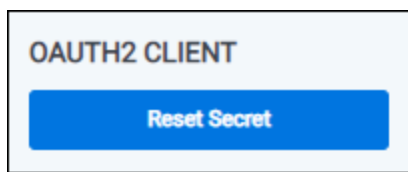
5.2 Resetting a client secret

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

- Client Credential
- Resource Owner
- Code

To reset an OAuth2 client secret:

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



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

5.3 Deleting an OAuth2 client

To delete an OAuth2 client:

1. From the **OAuth2 client** tab, locate and open the OAuth2 client you wish to delete.
2. Click **Delete**.

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

Note: System clients can't be deleted.

Viewing an OAuth2 client audit history

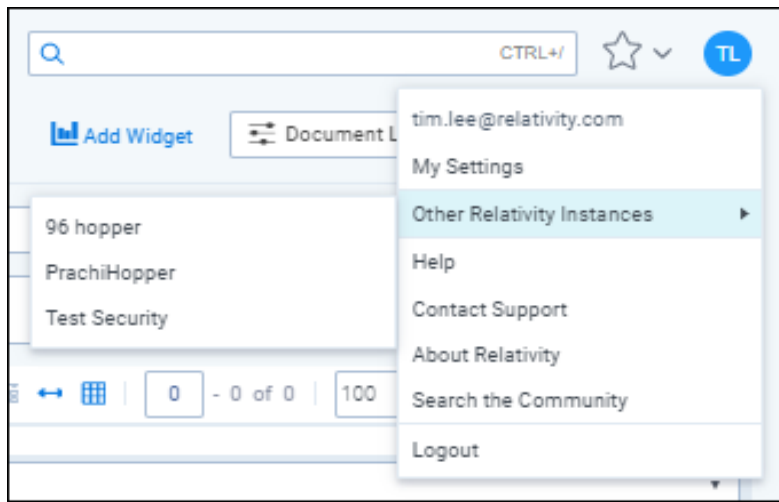
Use the OAuth2 client audit history to view all actions taken on a record. Use this information to view what the values were prior to a change.

To view an OAuth2 client's audit history:

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

6 Federated instances

Federated instances provide a way for reviewers to easily switch to other Relativity environments. In Relativity, links to federated instances appear in the User drop-down.



You can use federated instances in combination with OAuth2 clients and authentication providers to enable single sign-on for multiple environments in your Relativity ecosystem.

6.1 Creating or editing a federated instance

To create a federated instance or edit information for an existing federated instance:

1. Open the **Federated Instances** tab.
2. Click **New Federated Instance** to create a new federated instance, or click **Edit** next to the federated instance you want to edit. The Federated Instance Information form appears.
3. Complete the following fields:
 - **Name** – the name of the federated instance. Enter a name that makes the instance easy for users to recognize, like RelativityOne Reviewer.

Note: You can't change the name of an existing federated instance.

- **Instance URL** – the URL address of the instance you want to create a link to. To obtain this URL, navigate to the Relativity instance you want to appear in the dropdown. Copy and paste the URL from that instance into this field.
You can also choose to add the Home Realm Discovery (HRD) parameter to mimic single sign-on experience inside your Relativity cluster. HRD is a redirect URL to a configured authentication provider for the federated instance. It is supported for OpenId Connect, Integrated Authentication, and Client Certificate providers.

The HRD parameter value can be found in the individual provider details on the Authentication Provider tab. Generally, it is as follows:

- **OpenId Connect** – the name of the authentication provider:

```
https://mycompany.com/Relativity?HRD=<Provider Name>
```

- **Winauth** – *integrated*:

```
https://mycompany.com/Relativity?HRD=integrated
```

- **Client Certificate** – *smartcard*:

```
https://mycompany.com/Relativity?HRD=smartcard
```

By setting the HRD Hint, you enable the users to automatically sign into another instance by clicking the federated instance link from the user dropdown. Note that the authentication provider must be set up correctly for single sign-on to work. If the authentication by the provider fails, the user will be presented with the login screen of the Federated Instance.



The screenshot shows a dialog box titled "Federated Instance Information". It contains two fields: "Name" with the value "RelOne" and "Instance URL" with the value "https://secondary.mycompany.com/Relativity?HRD=Relativity+On+Prem2". The Instance URL field is highlighted with a red rectangular box.

4. Click **Save**.

The federated instance appears in the User dropdown.

You can restrict access to the federated instances you create using the padlock icon and assigning the appropriate groups access to the instance. If you restrict access to a federated instance, it doesn't appear in the User dropdown.

6.2 Deleting a federated instance

To delete a federated instance:

1. Navigate to the **Federated Instance** tab.
2. Locate and open the federated instance you wish to delete.
3. Click **Delete**.
4. From the confirmation dialog, click **Ok**.

The federated instance is removed.

Viewing a federated instance audit history

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

To view a federated instance's audit history:

1. Navigate to the Federated Instance tab.
2. Locate and click the federated instance for which you wish to view its history.

3. Click **View Audit**. A dialog appears, listing all actions taken on that federated instance.
4. (Optional) Using the **Export to File** drop-down list at the bottom of the dialog, click **Go** to export the following audit history details in a .CSV file:
 - User Name
 - Action
 - Timestamp
5. Close the dialog when finished viewing the audit.

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.

©2024. Relativity ODA LLC. All rights reserved. Relativity® is a registered trademark of Relativity ODA LLC.