10 Logging in to Relativity with client certificate authentication
1 Authentication

Relativity uses several industry-standard technologies, enabling versatile authentication options. It supports local (such as password related) or external (such as smart cards, or 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 pages for a list of those points.

- Authentication changes from previous versions
- Upgrade considerations for Relativity 9.5 - Authentication

1.1 Authentication mechanisms

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.
- **Client Certificate** – an external method requiring a smart card and PIN. This method validates from an IIS server. It may also be referred to as smart card authentication.
- **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 that 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.

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).
- **Trusted IP Range** – limit access to the Relativity application based on the user’s source IP address.
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. Relativity allows you to 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 doesn't work with the RDC is SAML because the Relativity's IdP-initiated SAML doesn't 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 which allows you 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 can't 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.

1.2.1 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
1.3 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. **Enable authentication provider types.** Authentication Provider Types are Relativity dynamic object (RDOs) types that permit authentication processes. You can only enable or disable each provider type. See [Enable authentication provider types below](#). By default, each authentication provider type is enabled.

2. **Create authentication providers.** Authentication Providers are instances of an authentication provider type. Each provider type that you plan to use requires creating an instance of that type. See [Creating authentication providers on the next page](#).

3. **Assign 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 47](#).

1.4 Enable authentication provider types

Authentication Provider Types are Relativity dynamic object (RDOs) types that permit authentication methods for users to log in with. You can't 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**.
1.5 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 can't 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.

1.5.1 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 can't 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 isn't available for the user.

Not all authentication providers have additional settings.

Select your authentication method:

- Default Integrated Authentication provider on the next page
- Default Active Directory provider on the next page
- Default RSA provider on the next page
- Default Password provider on the next page
- Default smart card provider on the next page
- OpenID Connect provider on page 10
- SAML 2.0 provider on page 22
1.5.2 Default Integrated Authentication provider
No authentication provider settings.

1.5.3 Default Active Directory provider
No authentication provider settings.

1.5.4 Default RSA provider
No authentication provider settings.
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 35 for additional details.

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

1.5.6 Default smart card provider
- **Display on Login Page** – determines if the client certificate button displays in the logon screen.
- **Login Screen Button Text** – sets the client certificate button text.
The example below illustrates the relationship between the two settings and the logon screen.
1.5.7 OpenID Connect provider

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to 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).
1.5.7.1 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).
   Relativity SSO

   **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
   e.g. https://myapp.com/auth

   By proceeding, you agree to the Microsoft Platform Policies

   Register

6. Click **Register**.

7. Copy the Application (client) ID.
Welcome to the new and improved App registrations. Looking to learn more about Relativity SSO?

**Display name:** Relativity SSO

**Application (client) ID:** 

**Directory (tenant) ID:** 

**Object ID:** 

**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/`

### 1.5.7.2 Configuring this method in Relativity

Enter these settings:

- **Site URL** (in the Authentication Provider Information section) - sets the URL users enter into the browser to access this instances of Relativity.

- **OAuth2 Flow** – set to either Implicit or Code.

- **Client Secret** – enter a dummy value. If you selected Code for OAuth2 Flow, you will populate this with the correct value later.

- **Client ID** – enter the Azure AD’s Application ID.

- **Authority URL** – enter the Authority from the trimmed OAUTH 2.0 AUTHORIZATIONENDPOINT from step 9 in Configuring your external identity provider.
- **Subject Claim Type** - The ID token from the Azure AD application that will be sent to Relativity. See [Microsoft identity platform ID tokens](#) for a full list of token identifiers.

  **Note**: If you are using an email address as the token, enter *upn* for the Subject Claim Type. *upn* must be lowercase.

- **Redirect URL** – sets the URL to the Relativity entry point. This value is read only and is generated by Relativity.

- **Display on Login Screen** – determines if the OpenID Connect button displays the on the logon screen.

- **Login Screen Button Text** – determines the text that appears on the button on the login page.

### 1.5.7.3 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.
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**.
1. Copy the client secret value.

2. Navigate back to the Authentication Provider in Relativity.

3. Click **Edit**.

4. Paste the value for Client Secret with the value from step 4.

5. Click **Save**.

6. Reset the IIS on all web servers.

**1.5.7.4 Adding users to the application in Azure**

1. Click **Azure Active Directory**.

2. Click **Enterprise Applications**.

3. Click into the application that you’ve created for Relativity authentication.
4. Click **Users and groups**.

5. Click **Add user**.

6. Select your users.

7. Click **Assign**.

1.5.7.5 Example: Setting up Relativity as an OpenID Connect authentication 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 an on-premises 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.

Complete these steps:

1. Navigate to the primary instance and set up an OAuth2 client. You must specify Code as the OAuth2 Flow.
   Note that initially you don’t have the redirect URL value (you get it when you set up the Authentication Provider on the secondary instance), so specify any placeholder URL instead. For more information, see OAuth2 clients on page 55.

   ![OAuth2 Client Information](image)

2. After you save the OAuth2 client, note the generated values of the Client Id and Client Secret. They are 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 and Client Secret values from the previous step. Note that the OAuth2 Flow values must also be Code, and the Authority URL must point to the Relativity Identity service of the primary instance.

   ![Authentication Provider Information](image)

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 user(s) to use the Authentication Provider as the Login Method, specifying the user’s email (Relativity user ID) as the OpenID Connect Subject field value. For more information, see Managing user authentication methods.

6. Reset the IIS server for the secondary instance.
7. Navigate back to the primary instance and update the OAuth2 provider with the Redirect URL.

8. 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 59.

9. Navigate back to the secondary instance and set up a federated instance pointing to the primary Relativity instance. Don’t set up the HRD redirect for that federated instance.

10. Log out of the secondary instance.
11. Use the federated instance link to log in to the secondary instance from the primary instance.

![Federated instance link](image)

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

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

### 1.5.8 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. Assertions protect this information by cryptography signing it. An Assertion is only valid if it is from a known Issuer URL to the expected Audience and correctly signed.

**Note:** 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.

1.5.8.1 Example: 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 username you would like to use for logging in. In this use case, select Email.
   - For Assertion Signature, select Signed.
3. You have now partially configured your application in Okta to set up logging in to Relativity. You must now configure the SAML provider in Relativity. You need these Okta values:
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 dropdown.

<table>
<thead>
<tr>
<th>Authentication Provider Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: OktaProvider</td>
</tr>
<tr>
<td>Provider Type: SAML2</td>
</tr>
<tr>
<td>Site URL: <a href="https://mycompany.com/Relativity">https://mycompany.com/Relativity</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authentication Provider Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audience:</td>
</tr>
<tr>
<td>Issuer URL:</td>
</tr>
<tr>
<td>Certificate: BEGIN CERTIFICATE--</td>
</tr>
</tbody>
</table>

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.

![Redirect URL](https://mycompany.com/Relativity)

**Redirect URL:** https://mycompany.com/Relativity/9E020C975390589207F8B00F46198EB

13. Perform an IIS reset on all web servers, so that the configuration setting changes provider take effect.

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

**Note:** You must also assign Okta users to the SAML application, and then map the users to SAML login method in Relativity. When configuring the login method, you must specify the user’s email in the SAML2 Subject field (if you select Email as the application username in Okta). For more information, see [Managing user authentication methods on page 47](#).

### 1.5.8.2 Example: Configuring ADFS as a SAML 2.0 identity provider

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

Note these terminology difference between Relativity and ADFS:

| ADFS |  
| Audience | Relying Party Identifier (s) | https://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 page 31
- Enabling Integrated Authentication on page 31

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.

![Trusted IPs](image)

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:
<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asterisk (*) (Asterisk wildcard)</td>
<td>Matches zero or more characters. 192.168.31.*. You can't use this notation with the match range of digits wildcard.</td>
</tr>
<tr>
<td>Hash (#) (Hash wildcard)</td>
<td>Matches any single digit 0-9. 192.168.31.##. You can't use this notation with the match range of digits wildcard.</td>
</tr>
<tr>
<td>[start-end] (Match range of digits wildcard)</td>
<td>Matches a range of digits. 192.168.31. [0-255]. You can't use this notation with the asterisk and/or hash wildcards.</td>
</tr>
<tr>
<td>16-bit mask</td>
<td>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.</td>
</tr>
<tr>
<td>24-bit mask</td>
<td>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.</td>
</tr>
<tr>
<td>25-bit mask</td>
<td>A 25-bit number that masks an IP address. 2.168.31.0/25 is the same as 2.168.31.0/255.255.255.128. Network address range is 2.168.31.0 - 192.168.31.127.</td>
</tr>
</tbody>
</table>

### 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 Enabling Integrated Authentication

**Note:** You need to complete the following steps if you have installed Relativity 9.5.253.62 or below, and want to use Active Directory (AD) for Integrated Authentication.

If you aren’t currently using this authentication type for your Relativity installation, you can set up an application that uses Active Directory (AD) for Integrated Authentication.

**Note:** Update your IIS settings by changing the WebAPI to Anonymous Authentication rather than Windows Authentication. You must update this setting to Anonymous Authentication to publish documents to a workspace or process data to Data Grid.

### 2.4.1 Setting up an application with Integrated Authentication

Use these steps to set up an application with Integrated Authentication.

**Note:** To identify the application set up for Integrated Authentication, the following steps use **WindowsAuthWebAPI** as the naming convention for the application, application pool, and folder created for this purpose.

1. On your web server, stop the IIS.
2. To create a folder for the application’s physical path, complete the following steps:
   a. In the Windows Explorer, navigate to your Relativity installation folder. When you install Relativity, the default file path is `C:\Program Files\kCura Corporation`.  
b. Locate the **RelativityWebAPI** folder in the installation directory.

c. Copy this folder and rename it to **WindowsAuthWebAPI**.

3. To add an application pool, complete the following steps:
   a. Open the **IIS Manager** on your web server.
   b. Right-click on **Application Pools** and select **Add Application Pool**.
   c. In the Add Application Pool dialog, enter **WindowsAuthWebAPI** in the **Name** box.
   d. Select **.NET Framework v 4.0** in the **.NET Framework version** drop-down box.
   e. Verify that the **Manager pipeline mode** is set to **Integrated**. Click **OK**.

   ![Add Application Pool dialog](image)

   f. Confirm that user running the application pool is the Relativity service account:
      i. Click on **Application Pools** to display a list of them.
      ii. Locate your application pool in the list.
      iii. Right-click on your application pool and click **Advanced Settings**.
      iv. Confirm that the **Identity** field is set to the name of your Relativity service account.
         (Click to expand)
v. Click OK.

4. To add an application, complete the following steps:
   a. In the Connections pane, right-click on the website hosting Relativity, and click Add Application.
   b. On the Add Application dialog, enter WindowsAuthWebAPI in the Alias box.
   c. Click Select for the application pool to choose WindowsAuthWebAPI.
   d. In the Physical path box, click ... to browse for the WindowsAuthWebAPI folder. Click
5. To disable anonymous authentication, complete the following steps:
   a. Click on the **WindowsAuthWebAPI** site.
   b. In the Features view, click **Authentication**.
   c. In the Authentication view, right-click on **Anonymous Authentication** and click **Disable**.
   d. Right-click on **Windows Authentication** and click **Enable**.
   e. To update the web.config file, locate it in the following folder:
      C:\Program Files\kCura Corporation\Relativity\WindowsAuthWebAPI
   f. Open the file in an editor. Update the authentication mode and authorization sections as follows:
      ```xml
      <system.web>
      <authentication mode="Windows" />
      ```
2.5 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 9.5 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 9.5 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 Authentication changes from previous versions

The authentication system in this version represents a significant change from previous versions. The new authentication system is more flexible and more secure but some workflows have changed as well as the Relativity API in order to support the new workflows. If you are upgrading from a prior version of Relativity, there are some important differences to be aware of.

3.1 Changes from previous versions

The following are some of the more significant changes to the authentication system.

- **The AuthenticationData Field Deprecation.** Authentication options used to be configured for each user through the AuthenticationData field by a single string value with slashes and colons. We replaced this error-prone system with a rich object model that provides improved safety and flexibility when configuring authentication.

- **Individual Provider Types Can be Enabled / Disabled.** You can selectively turn off authentication protocols that you never intend to use. This improves security and prevents another system admin from trying to configure an authentication method that should not be used. This includes the Password Provider Type. In previous versions of Relativity all user passwords were stored in the database. Now, you can completely remove Password authentication from your instance and exclusively use another login approach such as OpenID Connect or RSA.

- **Built-in Support for SAML and OpenID Connect.** Relativity now has built-in support for the OpenID and SAML protocols, which allows you to connect your instance to an external identity provider. If your environment has a custom solution for external authentication, you are strongly encouraged to use the built-in functionality instead.

- **The Password Workflow has Changed.** Password handling has changed significantly. This change improves the security of a Relativity instance. See the Password workflow changes below for more details.

- **Schema / API Changes.** Due to the significant changes to authentication, both the User table and the User API in RSAPI / REST has changed. You must update any custom solutions that directly query the User database table. The RSAPI and REST APIs have the same fields on the User object, but the behavior for some of those fields has changed. You can find out more information about the schema updates from Database schema updates for Relativity.

3.2 Password workflow changes

Passwords are handled differently than prior versions of Relativity. Although this introduces some necessary changes to how Relativity users are managed in an environment, the goal is to improve the overall security of the Relativity instance by following industry best practices.

There are two major changes to the Password workflow:

- **Passwords can no longer be sent through email to users or administrators.** Email is an inherently insecure method for sharing passwords. Many email systems use unencrypted communication, and there are security implications with storing a password unencrypted in an email system. Because of the security limitations of using email, Relativity no longer supports sending the
user's password through email.

- **Administrators are no longer allowed to set passwords for users.** In order to protect a user’s account, only that user should know their password. By default Relativity no longer allows administrators to set passwords when creating the user. Instead, Relativity expects the end user to manage their own password (according to the complexity rules defined by the system admin). Of course, users still need a secure way to set their password and log in to Relativity for the first time. There is a new feature called the *Invitation Workflow* that can be used to send users a link through email to set up their password for the first time. See [Invitation workflow on page 47](#) for more information.

You may have a developer or test environment that is not connected up to an SMTP server. For these non-production environments there is an instance setting that you can use to restore the ability to set passwords for individual users. See [Manually setting passwords](#) for more information.
4 Logging in to Relativity

Relativity offers several ways to log in and it's 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.

4.1 Password only

This method uses only a username and a password. Your system admin provides you with:

- your log in email address
- a password request email

Prior to logging in, if you've not already, create your password. See Creating or resetting a password on page 42.

To log in:

1. Navigate to the Relativity site.
2. Log in with your password. See Logging in to Relativity with a password on page 45.

4.2 Password: two factor

The two factor password method requires a passcode in addition to the username and password. The systems emails you the passcode during log in and is different each time. Your system admin provides you with:

- your login email address
- a password request email

Prior to logging in, if you've not already, create your password. See Creating or resetting a password on page 42.

To log in:

1. Navigate to the Relativity site.
2. Log in with your password. An Authenticate Login dialog appears. The system immediately emails you a passcode.
3. Enter that value in Passcode.
4. Click **Login**.

### 4.3 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:

- your login email address
- an account on a Windows domain
- a 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**.
4.4 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.

4.5 Client Certificate

To use this method, you must have a configured smart card and a computer with a smart card reader. Your system admin provides you with:

- a personalized smart card
- a PIN
- a smart card reader
- the client certificate name
- the client certificate button name

To log in:

1. Insert the smart card into the card reader.
2. Navigate to the Relativity site.
3. Enter your username in Username.
4. Click the client certificate button name that your system admin indicated.
5. Select the certificate name that your system admin indicated.
6. Click OK.
7. Enter your PIN associated with your card.
8. Click OK.

4.6 RSA

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

- your username
- an RSA SecurID token
- optionally a 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.

### 4.7 OpenID Connect

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

- an OpenID Connect account
- the Relativity OpenID Connect button name

To log in:

1. Navigate to the Relativity site.
2. Click the Relativity OpenID Connect button name.
3. Enter your username.
4. Click **Logon**.

### 4.8 SAML 2.0

This method requires you to have an account with SAML 2.0 authentication provider, for example, Okta, set up by your system admin.

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.

### 4.9 Creating or resetting a password

Use this procedure if you're logging in to Relativity for the first time or if you're 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 logon screen if it is available, or contact your system admin. In either case, the system sends you a new password email.
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 don't have to log in immediately.

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

6. Click **Return to Relativity**.
4.10 Logging in to Relativity with a password

1. Enter your **Username**.

![Username input field]

2. Click **Continue**.

3. Enter your password.

![Password input field]

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 Authentication.
5 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.

5.1 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, you must set the RelativityInstanceURL instance 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 Only below
- Password Two-Factor on the next page
- Password Outside Trusted IP on page 49

5.1.1 Password Only

The password only 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 section, select the password provider method from the Provider drop-down list. The password provider name may vary for each Relativity instance. See Creating authentication providers on page 8 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 None from the Two Factor Mode drop-down list.
5. Click Save and then Back.
6. Click Send User 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.

### 5.1.2 Password Two-Factor

The two-factor password is a variation of the Password method that requires a passcode in addition to a password. The system emails a passcode to the user during logon, and it’s different each time.

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 [Creating authentication providers on page 8](#) for creating 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 Always from the Two Factor Mode drop-down list.
5. Enter the user’s email address that the password is emailed to in **Two Factor Info**. 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**.

**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.

---

### 5.1.3 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. The default value of empty defines all IP addresses as untrusted. You can enter `.*.*.*` to trust any IP address.
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 Creating authentication providers on page 8 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 **Outside Trusted IPs** from the **Two Factor Mode** drop-down list.
5. Enter the user’s email address that the password is emailed to in **Two Factor Info**. 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**.

---

### 5.1.4 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 lower 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.

### 5.2 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 [Creating authentication providers on page 8](#) 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.
5.3 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 Creating authentication providers on page 8 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.

5.4 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 on outside this range, the log on will be successful and Relativity displays the password dialog. 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 Creating authentication providers on page 8 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.
5.5 Client Certificate

This client certificate authentication uses a smart card assigned to a user. Contact your smart card provider for card details.

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 client certificate provider method from the Provider drop-down list.
   The provider name may vary for each Relativity instance. See Creating authentication providers on page 8 for creating and naming a password method instance. The Login Method Settings section appears.
4. Enter the subject alternate name in Certificate Subject in Certificate Subject. The subject alternate name is the value from the certificate's Subject Alternate Name. In the following example, use jsmith@example.com. However, your smart card vendor may provide a different specification and you should use that instead.

   ![Certificate dialog box showing the certificate details](image)

   - Field: Subject Constraints
     - Value: Subject Type=End Entity, Pat...
   - Field: Key Usage
     - Value: Digital Signature, Non-Repudiation...
   - Field: Subject Alternative Name
     - Value: DNS Name = jmsith@example.com

5. Click Save and then Back.
5.6 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 35.
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 Creating authentication providers on page 8 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.

5.7 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 Creating authentication providers on page 8 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.

5.8 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 Creating authentication providers on page 8 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.
We're providing the OAuth2 client functionality as a preview release so that you can evaluate it and provide us with feedback. The preview release offers a functional feature which will continue to undergo minor changes and further enhancements. Feedback >>
6 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.

6.1 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.
   - **Flow** – the mechanism for acquiring an authentication token also known as OAuth2 grant type. Relativity supports the following grant types:
     - **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.
     - **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.
- **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.

- **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.

- **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).
  - 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:

- **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.

- **Enabled** – yes/no value indicating whether the client will be given access to Relativity.
■ **IsSystem** – specifies whether the OAuth2 client is part of an internal Relativity application.

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

### 6.2 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.

### 6.3 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 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.
7 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 dropdown.

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.

7.1 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:
  ```plaintext
  https://mycompany.com/Relativity?HRD=<Provider Name>
  ```

- **Winauth – integrated:**
  ```plaintext
  https://mycompany.com/Relativity?HRD=integrated
  ```

- **Client Certificate – smartcard:**
  ```plaintext
  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.

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.

### 7.2 Deleting a federated instance

To delete a federated instance:

1. From the **Federated Instance** tab, locate and open the federated instance you wish to delete.
2. Click **Delete**.
3. 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. From the Federated Instance tab, locate and click the federated instance for which you wish to view its history.
2. Click **View Audit**. A dialog appears, listing all actions taken on that federated instance.
3. (Optional) Using the **Export to File** drop-down 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.
8 Client certificate authentication

Relativity supports client certificate authentication, which may also be referred to as smart card authentication. This two factor authentication method uses a PIN and a client certificate stored on a personal identity verification (PIV) card. When logging in to Relativity, the user inserts a PIV card into the card reader, and clicks a PIV login button. Next, the user selects the appropriate certificate on the PIV card, and then enters a PIN.
9 Configuring a user for client certificate authentication

In Relativity, you configure client certificate authentication at the user level.

Before you begin, obtain the value in the **Subject Alternative Name** field of the certificate generated for a user. Contact your system or other administrator responsible for generating these certificates in your organization for this information.

Use the following steps to configure a user for client certificate authentication:

1. Log in to Relativity with system admin credentials.
2. Select **Home** from the user drop-down menu.
3. Click the **Users** tab.
4. Click the **Edit** link next to an existing username, or create a new user. See Users on the Relativity 9.5 Documentation site.
5. In the Login Method section, click **New** to open the Login Method Information form.
6. Select a **Smart Card Provider**.
7. In the Certificate Subject field, enter `<Subject Alternative Name>`. The Subject Alternative Name is associated with the certificate on the smart card used to log in to Relativity.

For example, if the Subject Alternative Name is jsmith@example, then you would enter jsmith@example in the Certificate Subject field.

8. Click **Save**. The user can now use client certificate authentication to log in to Relativity.
10 Logging in to Relativity with client certificate authentication

You can log in to Relativity by inserting your PIV card into your smart card reader, selecting a certificate, and entering your PIN.

Use the following steps to log in to Relativity:

1. Insert your PIV card into the smart card reader for your computer.
2. Browse to your Relativity website with the URL provided by your system admin.
3. Enter your email address in the Username box.
4. Click the button under the External Login heading. Your system admin may customize the label on the button for your Relativity application.
5. On the Select a certificate dialog, highlight the certificate used for logging in to Relativity.
6. Click **OK**.

7. Enter your **PIN** for your smart card, and click **OK**.
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® is a registered trademark of Relativity ODA LLC.