Enabling SAML Authentication in an Informatica 10.2.x Domain
Abstract

You can enable users to log into Informatica web applications using single sign-on. This article explains how to configure single sign-on in an Informatica 10.2.x domain using Security Assertion Markup Language (SAML) and Microsoft Active Directory Federation Services (AD FS).

Supported Versions

- Informatica Big Data Management™ 10.2 x
- Informatica Data Quality 10.2 x
- Informatica Data Services 10.2 x
- Informatica Data Transformation 10.2 x
- Informatica PowerCenter® 10.2 x

Table of Contents

SAML Authentication Overview .......................................................... 2
SAML Authentication Process ........................................................... 3
Web Application User Experience ....................................................... 3
SAML Authentication Setup ............................................................... 3
  Before You Enable SAML Authentication ........................................ 4
  Step 1. Create a Security Domain for Web Application User Accounts .................. 4
  Step 2. Export the Certificate from AD FS ........................................ 8
  Step 3. Import the Certificate into the Truststore Used for SAML Authentication ............ 11
  Step 4. Configure Active Directory Federation Services ............................. 12
  Step 5. Add Informatica Web Application URLs to AD FS .......................... 19
  Step 6. Enable SAML Authentication in the Domain ................................ 21
  Step 7: Enable SAML Authentication on the Gateway Nodes ....................... 24

SAML Authentication Overview

You can configure Security Assertion Markup Language (SAML) authentication for Informatica web applications.

Security Assertion Markup Language is an XML-based data format for exchanging authentication and authorization information between a service provider and an identity provider. In an Informatica domain, the Informatica web application is the service provider. Microsoft Active Directory Federation Services (AD FS) 2.0 is the identity provider, which authenticates web application users with your organization's LDAP or Active Directory identity store.

Note: SAML authentication cannot be used in an Informatica domain configured to use Kerberos authentication.
SAML Authentication Process

Informatica web applications and Active Directory Federation Services exchange authentication and authorization information to enable SAML authentication in an Informatica domain.

The following steps describe the basic SAML authentication flow:

1. A user logs into an Informatica web application.
2. The application sends a SAML authentication request to AD FS.
3. AD FS authenticates the user’s credentials against the user account information in the LDAP or Active Directory identity store.
4. AD FS creates a session for the user and sends a SAML assertion token containing security-related information about the user to the web application.
5. The application validates the assertion.

Web Application User Experience

Use SAML authentication to provide single sign-on capabilities to users of supported Informatica web applications.

A user logs in to an Informatica web application enabled to use SAML authentication through an LDAP security domain containing Informatica web application user accounts. The user’s credentials are sent in a SAML authentication request to AD FS, which authenticates the user.

Subsequent authentication is managed through session cookies set in the web browser during the initial authentication. The authenticated user can access another Informatica web application configured to use SAML authentication in the same browser session by selecting the LDAP security domain on the application login page. The user does not need to supply a user name or password.

When authentication is complete, the user remains logged in to all Informatica web applications that are running in the same browser session. If AD FS is configured to issue persistent cookies, the user remains logged in after closing and restarting the browser.

However, if the user logs out of an Informatica web application, the user is also logged out of other Informatica web applications running in the same browser session.

Users not enabled to use SAML authentication select the native security domain on the web application login page, and then provide the user name and password for the native account.

SAML Authentication Setup

Configure Active Directory Federation Services (AD FS), the Informatica domain, and the gateway nodes within the domain to use SAML authentication.

To configure SAML authentication for supported Informatica web applications, perform the following tasks:

1. Create an LDAP security domain for Informatica web application user accounts, and then import the users into the domain from Active Directory.
2. Export the Identity Provider Assertion Signing Certificate from AD FS.
3. Import the Identity Provider Assertion Signing certificate into a truststore file on each gateway node in the domain. You can import the certificate into the Informatica default truststore file, or into a custom truststore file.
4. Add Informatica as a relying party trust in AD FS and map LDAP attributes to the corresponding types used in security tokens issued by AD FS.
5. Add the URL for each Informatica web application to AD FS.
7. Enable SAML authentication on every gateway node in the domain.

**Before You Enable SAML Authentication**

Ensure the Windows network and Informatica domain gateway nodes are configured to use SAML authentication.

To ensure that the Informatica domain can use SAML authentication, validate the following requirements:

**Verify that the required services are deployed and configured on the Windows network.**

SAML authentication requires the following services:

- Microsoft Active Directory
- Microsoft Active Directory Federation Services 2.0

**Ensure the Informatica web application services use secure HTTPS connections.**

By default, AD FS requires that web application URLs use the HTTPS protocol.

**Ensure that the system clocks on the AD FS host and all gateway nodes in the domain are synchronized.**

The lifetime of SAML tokens issued by AD FS is set according to the AD FS host system clock. Ensure that the system clocks on the AD FS host and all gateway nodes in the domain are synchronized.

To avoid authentication issues, the lifetime of a SAML token issued by AD FS is valid if the start time or end time set in the token is within 120 seconds of a gateway node’s system time by default.

**Step 1. Create a Security Domain for Web Application User Accounts**

Create a security domain for web application user accounts that will use SAML authentication, and then import each user's LDAP account from Active Directory into the domain.

You must import the LDAP accounts for all users that use SAML authentication into the security domain. After importing the accounts into the domain, assign the appropriate Informatica domain roles, privileges and permissions to the accounts within the LDAP security domain.

1. In the Administrator tool, click the **Users** tab, and then select the **Security** view.
2. Click the **Actions** menu and select **LDAP Configuration**.
   
   The **LDAP Configuration** dialog box opens.
3. Click the **LDAP Connectivity** tab.
4. Configure the connection properties for the Active Directory server.

   The following table describes the server connection properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Host name or IP address of the Active Directory server.</td>
</tr>
<tr>
<td>Port</td>
<td>Listening port for the Active Directory server. The default value is 389.</td>
</tr>
<tr>
<td>LDAP Directory Service</td>
<td>Select Microsoft Active Directory.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name</td>
<td>Distinguished name (DN) for the principal LDAP user. The user name often consists of a common name (CN), an organization (O), and a country (C). The principal user name is an administrative user with access to the directory. Specify a user that has permission to read other user entries in the directory service.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the principal LDAP user.</td>
</tr>
<tr>
<td>Use SSL Certificate</td>
<td>Indicates that the LDAP server uses the Secure Socket Layer (SSL) protocol. If the LDAP server uses SSL, you must import the certificate into a truststore file on every gateway node within the Informatica domain. You must also set the INFA_TRUSTSTORE and INFA_TRUSTSTORE_PASSWORD environment variables if you do not import the certificate into the default Informatica truststore.</td>
</tr>
<tr>
<td>Trust LDAP Certificate</td>
<td>Determines whether the Service Manager can trust the SSL certificate of the LDAP server. If selected, the Service Manager connects to the LDAP server without verifying the SSL certificate. If not selected, the Service Manager verifies that the SSL certificate is signed by a certificate authority before connecting to the LDAP server.</td>
</tr>
<tr>
<td>Not Case Sensitive</td>
<td>Indicates that the Service Manager must ignore case sensitivity for distinguished name attributes when assigning users to groups. Enable this option.</td>
</tr>
<tr>
<td>Group Membership Attribute</td>
<td>Name of the attribute that contains group membership information for a user. This is the attribute in the LDAP group object that contains the distinguished names (DNs) of the users or groups who are members of a group. For example, member or memberof.</td>
</tr>
<tr>
<td>Maximum size</td>
<td>Maximum number of user accounts to import into a security domain. If the number of user to be imported exceeds the value for this property, the Service Manager generates an error message and does not import any user. Set this property to a higher value if you have many users to import. The default value is 1000.</td>
</tr>
</tbody>
</table>
The following image shows the connection details for an LDAP server set in the LDAP Connectivity panel of the LDAP Configuration dialog box.

5. Click **Test Connection** to verify that the connection to the Active Directory server is valid.
6. Click the **Security Domains** tab.
7. Click **Add** to create a security domain.
8. Enter the security domain properties.
The following table describes the security domain properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Domain</td>
<td>Name of the LDAP security domain. The name is not case sensitive and must be unique within the domain. The name cannot exceed 128 characters or contain the following special characters: , , + / &lt; &gt; @ ; \ % ? The name can contain an ASCII space character except for the first and last character. All other space characters are not allowed.</td>
</tr>
<tr>
<td>User search base</td>
<td>Distinguished name (DN) of the entry that serves as the starting point to search for user names in the LDAP directory service. The search finds an object in the directory according to the path in the distinguished name of the object. In Active Directory, the distinguished name of a user object might be <code>cn=UserName,ou=OrganizationalUnit,dc=DomainName</code>, where the series of relative distinguished names denoted by <code>dc=DomainName</code> identifies the DNS domain of the object. For example, to search the Users container that contains user accounts in the example.com Windows domain, specify <code>CN=USERS,DC=EXAMPLE,DC=COM</code>.</td>
</tr>
<tr>
<td>User filter</td>
<td>An LDAP query string that specifies the criteria for searching for users in Active Directory. The filter can specify attribute types, assertion values, and matching criteria. For Active Directory, format the query string as: <code>sAMAccountName=&lt;account&gt;</code></td>
</tr>
<tr>
<td>Group search base</td>
<td>Distinguished name (DN) of the entry that serves as the starting point to search for group names in Active Directory.</td>
</tr>
<tr>
<td>Group filter</td>
<td>An LDAP query string that specifies the criteria for searching for groups in the directory service.</td>
</tr>
</tbody>
</table>
The following image shows the properties for an LDAP security domain named SAML_USERS set in the Security Domains panel of the LDAP Configuration dialog box. The user filter is set to import all users beginning with the letter "s".

9. Click Synchronize Now.
   The security domain appears in the Users view.

10. Expand the domain in the Navigator to view the imported user accounts.

11. Set the appropriate roles, privileges, and permissions on the user accounts that will access each web application.

**Step 2. Export the Certificate from AD FS**

Export the Assertion Signing certificate from AD FS.

The certificate is a standard X.509 certificate used to sign the assertions within the SAML tokens that AD FS issues to Informatica web applications. You can generate a self-signed Secure Sockets Layer (SSL) certificate for AD FS, or you can get a certificate from a certificate authority and import it into AD FS.

1. Log in to the AD FS Management Console.

2. Expand the Service > Certificates folder.
3. Right-click the certificate under Token-signing in the Certificates pane, and then select View Certificate, as shown in the following image:

The Certificate dialog appears.
4. Click the **Details** tab, and then click **Copy to File**, as shown in the following image:

The **Certificate Export Wizard** appears.
5. Select **DER encoded binary X.509 (.CER)** as the format, as shown in the following image:

![Certificate Export Wizard](image)

6. Click **Next**.

7. Enter the certificate file name and the location to export it to, and click **Next**.

8. Click **OK**, and then click **Finish** to complete the export.

**Step 3. Import the Certificate into the Truststore Used for SAML Authentication**

Import the assertion signing certificate into the truststore file used for SAML authentication on every gateway node within the Informatica domain.

You can import the certificate into the default Informatica truststore file, or into a custom truststore file.

The file name of the default Informatica truststore file is `infa_truststore.jks`. The file is installed in the following location on each node:

`<Informatica installation directory>\services\shared\security\infa_truststore.jks`

**Note:** Do not replace the default `infa_truststore.jks` file with a custom truststore file.

If you import the certificate into a custom truststore file, you must save the truststore file in a different directory than the directory containing the default Informatica truststore file. The truststore file name must be `infa_truststore.jks`. 
Use the Java keytool key and certificate management utility to import the certificate into the truststore file on each gateway node.

1. Copy the certificate files to a local folder on a gateway node within the Informatica domain.
2. From the command line, go to the location of the keytool utility on the node:
   `<Informatica installation directory>\java\jre\bin`
3. From the command line, run the following command:
   ```
   keytool -importcert -alias <certificate alias name> -file <certificate path>\<certificate filename> -keystore <path to infa_truststore.jks> -storepass <keystore password>
   ```
   Include the password for the truststore file.
4. Restart the node.

**Step 4. Configure Active Directory Federation Services**

Configure AD FS to issue SAML tokens to Informatica web applications.

Use the AD FS Management Console to perform the following tasks:

- Add Informatica as a relying party trust in AD FS. The relying party trust definition enables AD FS to accept authentication requests from Informatica web applications.
- Edit the Send LDAP Attributes as Claims rule to map LDAP attributes in your identity store to the corresponding types used in SAML tokens issued by AD FS.

**Note:** All strings are case sensitive in AD FS, including URLs.

1. Log in to the AD FS Management Console.
2. Expand the **Trust Relationships > Relying Party Trusts** folder.
3. Right-click the **Relying Party Trusts** folder, and then select **Add Relying Party Trust** as shown in the following image:

   ![Add Relying Party Trust Wizard](image)

   The **Add Relying Party Trust Wizard** appears.
4. Click **Start**.
   The **Select Data Source** panel appears.

5. Click **Enter data about the relying party manually** as shown in the following image:

6. Click **Next**

7. Enter “Informatica” as the display name, and then click **Next**.
8. Click **AD FS 2.0 profile** as shown in the following image:

![AD FS 2.0 profile](image)

9. Click **Next**.

   Skip the certificate configuration panel in the wizard.
10. Check **Enable support for the SAML WebSSO protocol**, and then enter the complete URL for the Administrator tool, as shown in the following image:

![Add Relying Party Trust Wizard](image)

11. **Click Next.**

12. Enter “Informatica” in the Relying party trust identifier field. **Click Add**, and then click **Next.**
13. Select **Permit all users to access the relying party** as shown in the following image:

![Add Relying Party Trust Wizard](image)

**Choose Issuance Authorization Rules**

- **Permit all users to access this relying party**
  - The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

14. Click **Next**.
15. Check **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** as shown in the following image:

![Add Relying Party Trust Wizard](image)

- **Finish**
  - Finish

16. Click **Close**.

The **Edit Claim Rules for Informatica** dialog box appears.

17. Click **Add Rule**.

The **Add Transform Claim Rule Wizard** opens.

18. Select **Send LDAP Attributes as Claims** from the menu, as shown in the following image:
Select Rule Template

<table>
<thead>
<tr>
<th>Steps</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Choose Rule Type</td>
<td>Configure Claim Rule</td>
</tr>
</tbody>
</table>

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule templates:

- **Send LDAP Attributes as Claims**

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the display name and telephone number Active Directory attributes and then send those values as two separate outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

Tell me more about this rule template...

![Select Rule Template](image.png)

19. Click **Next**.
20. Enter any string as the claim rule name, as shown in the following image:

21. Select Active Directory from the Attribute store menu.
22. Select SAM-Account-Name from the LDAP Mapping menu.
23. Enter "username" in the Outgoing Claim Type field.
24. Click Finish, then click OK to close the wizard.

**Step 5. Add Informatica Web Application URLs to AD FS**

Add the URL for each Informatica web application using SAML authentication to AD FS.

You provide the URL for an Informatica web application to enable AD FS to accept authentication requests sent by the application. Providing the URL also enables AD FS to send the SAML token to the application after authenticating the user.

You do not need to add the URL for the Administrator tool, because you already entered it as part of configuring AD FS.

1. Log in to the AD FS Management Console.
2. Expand the Trust Relationships > Relying Party Trusts folder.
3. Right-click the Informatica entry and select Properties, as shown in the following image:

![Informatica Properties dialog box]

4. Click the Endpoints tab.

The Add an Endpoint dialog box appears.
5. Select **SAML Assertion Consumer** from the **Endpoint** type menu, and then select **POST** from the **Binding** menu, as shown in the following image:

![Informatica Properties](image)

6. Enter the complete URL for a supported Informatica web application, and then click **OK**. Repeat this procedure for each web application.

**Step 6. Enable SAML Authentication in the Domain**

You can enable SAML authentication in an existing Informatica domain, or you can enable it when you install or create a domain.

Select one of the following options:

**Enable SAML authentication when you install the Informatica services.**

You can enable SAML authentication and specify the identity provider URL when you configure the domain as part of the installation process.

**Enable SAML authentication in an existing domain.**

Use the `infasetup updateDomainSamlConfig` command to enable SAML authentication in an existing Informatica domain. You can run the command on any gateway node within the domain.

**Enable SAML authentication when you create a domain.**

Use the `infasetup defineDomain` command to enable SAML authentication when you create a domain.
infasetup updateDomainSamlConfig Command Options

Set the SAML options in the infasetup updateDomainSamlConfig command to enable SAML authentication in a domain. Shut down the domain before you run the command.

Specify the identity provider URL as the value for the `-iu` option. The following example shows the command usage:

```
```

The following table describes the options and arguments:

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-EnableSaml</code></td>
<td><code>-saml</code></td>
<td>true</td>
</tr>
<tr>
<td><code>-idpUrl</code></td>
<td><code>-iu</code></td>
<td>identity_provider_url Required if the <code>-saml</code> option is true. Specify the identity provider URL for the domain. You must specify the complete URL string.</td>
</tr>
<tr>
<td><code>-ClockSkewTolerance</code></td>
<td><code>-cst</code></td>
<td>clock_skew_tolerance_in_seconds Optional. The allowed time difference between the Active Directory Federation Services (AD FS) host system clock and the master gateway node's system clock. The lifetime of SAML tokens issued by AD FS by is set according to the AD FS host system clock. The lifetime of a SAML token issued by AD FS is valid if the start time or end time set in the token is within the specified number seconds of the master gateway node’s system clock. Values must be from 0 to 600 seconds. Default is 120 seconds.</td>
</tr>
</tbody>
</table>

See the Informatica Command Reference for instructions on using the infasetup updateDomainSamlConfig command.

infasetup DefineDomain Command Options

Use the infasetup defineDomain command to enable SAML authentication when you create a domain.

The following example shows the SAML options as the final six options at the command prompt:

```
```

The following table describes the SAML options and arguments:

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-EnableSaml</code></td>
<td><code>-saml</code></td>
<td>true</td>
</tr>
<tr>
<td><code>-idpUrl</code></td>
<td><code>-iu</code></td>
<td>identity_provider_url Required if the <code>-saml</code> option is true. Specify the identity provider URL for the domain. You must specify the complete URL string.</td>
</tr>
</tbody>
</table>
Option Argument Description

- ClockSkewTolerance -cst
  clock_skew_toleranc_in_seconds Optional. The allowed time difference between the Active Directory Federation Services (AD FS) host system clock and the master gateway node’s system clock.
  The lifetime of SAML tokens issued by AD FS by is set according to the AD FS host system clock. The lifetime of a SAML token issued by AD FS is valid if the start time or end time set in the token is within the specified number seconds of the master gateway node’s system clock.
  Values must be from 0 to 600 seconds. Default is 120 seconds.

- AssertionSigningCertificateAlias -asca
  idp_assertion_signing_certificate_alias Required if the -saml option is true. The alias name specified when importing the identity provider assertion signing certificate into the truststore file used for SAML authentication.

-SamlTrustStoreDirectory -std
  saml_truststore_directory Optional. The directory containing the custom truststore file required to use SAML authentication on gateway nodes within the domain. Specify the directory only, not the full path to the file.
  SAML authentication uses the default Informatica truststore if no truststore is specified.

-SamlTrustStorePassword -stp
  saml_truststore_password Required if you use a custom truststore. The password for the custom truststore file.

See the Informatica Command Reference for instructions on using the infasetup defineDomain command.

Getting the Identity Provider URL

You must provide the SAML 2.0/WS-Federation URL for the AD FS server to enable SAML authentication.

You set this URL as the value for the -iu option when you run the infasetup updateDomainSamlConfig command or the infasetup defineDomain command. Use Windows PowerShell on the AD FS server to get the URL.

1. Open the Windows PowerShell command prompt window on the AD FS server. Select the Run as administrator option when you open the command prompt.
2. Type the following command at the Windows PowerShell command prompt:
   Get-ADFSFeature
3. Find the FullUrl value returned for the SAML 2.0/WS-Federation protocol, as shown in the following image:

ClientCredentialType : Anonymous
Enabled : True
FullUrl : https://adfs.company.com/adfs/ls/
Proxy : False
Protocol : SAML 2.0/WS-Federation
SecurityMode : Transport
AddressPath : /adfs/ls/
Version : default
Step 7: Enable SAML Authentication on the Gateway Nodes

You must configure SAML authentication on every gateway node in the Informatica domain. Configure every gateway node in the domain to use SAML to ensure the SAML configuration on each node matches the domain level SAML configuration.

Select one of the following options to configure SAML authentication on a gateway node:

**Enable SAML authentication when you define a gateway node on a machine.**

Use the infasetup DefineGatewayNode command to enable SAML authentication on the gateway node.

**Enable SAML authentication when you configure a gateway node to join a domain that uses SAML authentication.**

Use the infasetup UpdateGatewayNode command to enable SAML authentication on the gateway node.

**Enable SAML authentication when you convert a worker node to a gateway node.**

Use the isp SwitchToGatewayNode command to enable SAML authentication on the node.

**Gateway Node Command Options**

Use the infasetup DefineGatewayNode command to enable SAML authentication when you create a gateway node. Use infasetup UpdateGatewayNode or infacmd isp SwitchToGatewayNode to enable SAML authentication on an existing node.

The SAML options are identical for all of these commands. The following example shows the SAML options as the final four options on the infasetup DefineGatewayNode command line:

```
```

The following table describes the options and arguments:

<table>
<thead>
<tr>
<th>Option</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-EnableSaml</td>
<td>saml</td>
<td>Required. Enables SAML authentication in the Informatica domain. Set this value to true to enable SAML authentication in the domain. Set this value to false to disable SAML authentication in the domain.</td>
</tr>
<tr>
<td>-AssertionSigningCertificateAlias</td>
<td>idp_assertion_signing_certificate_alias</td>
<td>Required if SAML authentication is enabled for the domain. The alias name specified when importing the identity provider assertion signing certificate into the truststore file used for SAML authentication.</td>
</tr>
<tr>
<td>-SamlTrustStoreDir</td>
<td>std</td>
<td>Optional. The directory containing the custom truststore file required to use SAML authentication on gateway nodes within the domain. Specify the directory only, not the full path to the file. The default Informatica truststore is used if no truststore is specified.</td>
</tr>
<tr>
<td>-SamlTrustStorePassword</td>
<td>stp</td>
<td>Required if you use a custom truststore. The password for the custom truststore file.</td>
</tr>
</tbody>
</table>

See the Informatica Command Reference for instructions on using the infasetup DefineGatewayNode, the infasetup UpdateGatewayNode, and the infacmd isp SwitchToGatewayNode commands.