How-To Library

Informatica

Enabling SAML Authentication with NetScaler for Web Applications

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 domain using Security Assertion Markup Language (SAML) v2.0 and the Citrix NetScaler 13.0 identity provider.

Supported Versions

- Informatica Data Engineering Integration 10.4.1
- Informatica Enterprise Data Catalog 10.4.1
- Informatica Enterprise Data Preparation 10.4.1
- Informatica Metadata Manager 10.4.1

Table of Contents

Overview

You can configure Security Assertion Markup Language (SAML) authentication in an Informatica version 10.4.1 domain using the NetScaler identity provider.

An identity provider is an entity that provides authentication as a consumable service by applications. Platforms like Amazon Web Services (AWS) and Microsoft Azure support various third-party identity providers to authenticate requests by applications on their platforms.

SAML is an XML-based data format for exchanging authentication information between a service provider and an identity provider. In an Informatica domain, an Informatica web application is the service provider.

You can configure the following Informatica web applications to use SAML authentication:

- Informatica Administrator
- Informatica Analyst
- Metadata Manager
- Enterprise Data Catalog
- Enterprise Data Preparation

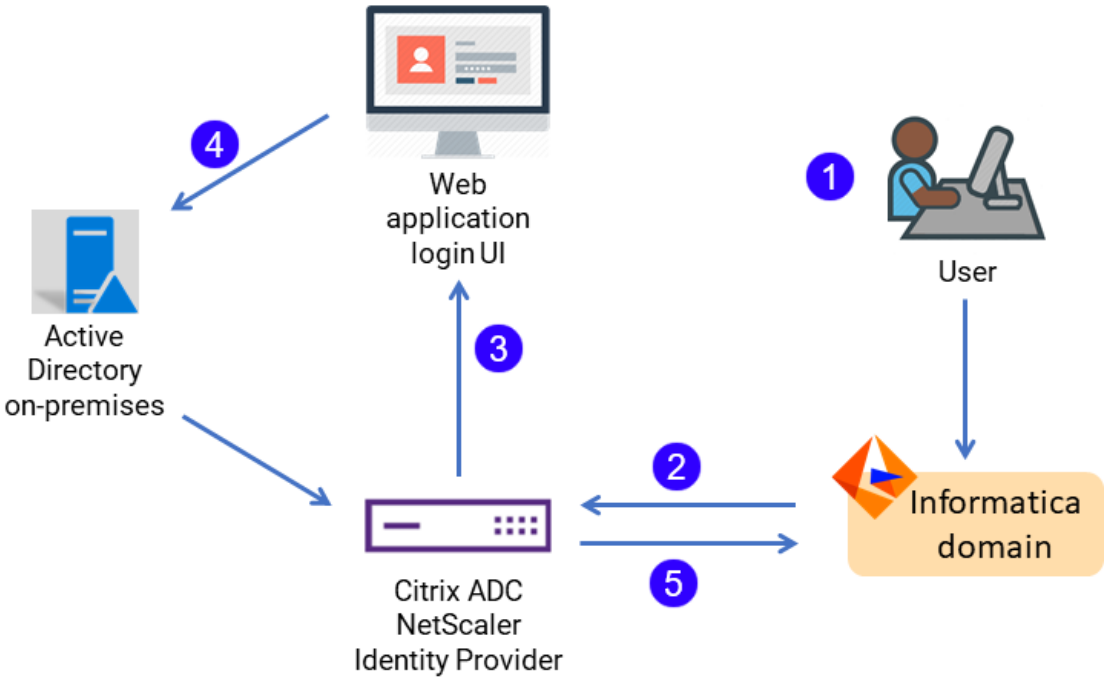
Informatica 10.4.1 supports NetScaler version 13.0.

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

SAML Authentication Process for Identity Providers

Informatica web applications and the NetScaler identity provider exchange authentication information to enable SAML authentication in an Informatica domain.

The following image illustrates the process flow for SAML authentication for Informatica users:



The following steps correspond to the numbered elements in the illustration:

1. The user uses a URL to access a resource of a service provider. In Informatica, the service provider is the domain, and the resource is a web application that the domain serves. For example, the Administrator tool web UI.
2. The service provider forwards the unauthenticated user to the identity provider (idP) via saml:authnRequest.
3. The identity provider points to its SingleSignOnService URL, so the user must sign in.
4. The IdP checks the entered credentials against a user database such as Active Directory and forms a saml:response about the status of the verification request.
5. The IdP sends the saml:response in the form of an XHTML form back to the service provider. This XHTML form contains, among other things, the AssertionConsumerService URL, which is automatically opened for the user.

The existing user session in the browser is used for subsequent authentication. To access another Informatica web application configured to use SAML authentication, the user selects the LDAP security domain on the application log in page. It is not necessary for the user to supply a user name or password.

The user remains logged in to all Informatica web applications that are running in the same browser session. However, if the user logs out of a web application, the user is also logged out of other Informatica web applications running in the same browser session.

Before You Begin

Before you begin to configure NetScaler and Informatica, complete the tasks in this section.

Download NetScaler

Download and deploy the NetScaler identify provider.

Download and deploy Citrix NetScaler 13.0 in your network domain. Verify that the VM where you deploy NetScaler meets the following requirements:

- 2 CPUs
- At least 2 GB RAM
- At least 20 GB storage

Prerequisites

Perform these prerequisite tasks:

Verify that you have a valid Enterprise or Platinum NetScaler license, and complete basic configuration of NetScaler.

Verify that the NetScaler server, the Active Directory server, and the Informatica deployment reside in the same network domain.

Ask your IT administrator to assign IP addresses in the same network domain for the following system nodes:

- LDAP server
- Authentication, authorization and auditing (AAA) server

Certificates

NetScaler requires an identity provider certificate, a server certificate, and a service provider certificate. Each of these certificates is used to certify the element whose profile it represents.

Create each of these certificates:

Service provider (SP) certificate

The service provider signing certificate uses a private key that resides on the service provider, while NetScaler holds the public key.

In this case, Informatica is the service provider.

Identify provider (IDP) certificate

The identity provider certificate is used to sign the assertions within the SAML tokens that NetScaler issues to Informatica web applications.

Server certificate

The server certificate is bound to the authentication, authorization and auditing (AAA) server.

The same certificate file can serve as both the identity provider certificate and the server certificate. This certificate should be a "wildcard" certificate that permits access to the entire domain where NetScaler, the AAA server, and the LDAP server are installed.

Choose how to create this certificate:

- In NetScaler, create a self-signed certificate.
- Separately create a certificate signed by a public or private certificate authority.

Import the Service Provider Certificate

Import the service provider certificate from the domain to NetScaler.

When you configure an LDAP domain on the Informatica domain, you generate a SAML certificate. For NetScaler, this is known as the service provider certificate. IIt contains authentication authority for the Informatica domain.

Import this certificate file to NetScaler.

Install the Server Certificate

Create and install the server certificate in the NetScaler server.

1. In the NetScaler web interface, click **Traffic Management** > **SSL** > **Certificates** > **Server Certificates**.
2. Click **Install**.
3. Provide a name for the certificate - key pair.
4. In the Certificate File Name field, add the wildcard certificate file name.
5. In the Key File Name field, type the name of the key file.
6. Click **Install**.

Configure the NetScaler Server

Integrating Informatica Data Engineering with NetScaler requires you to configure NetScaler before you configure the Informatica domain to work with it.

This section provides an overview of the steps to create, configure or verify the NetScaler elements that are required for integration with Informatica. Consult the NetScaler 13.0 documentation for assistance with these steps.

Configure Authentication LDAP Server

Configure an LDAP server in NetScaler to provide authentication for web applications.

1. In the NetScaler web interface, click **Policies** > **Authentication** > **LDAP** > **Server**.
2. Click **Add** to add an authentication server.
3. Enter values for the following properties:

Property	Value
Name	Enter a descriptive name for the LDAP server.
Server IP	Enter the IP address of the LDAP server
Security type	Plaintext
Port	Port number of the LDAP server
Server Type	Select AD
Authentication	Select the **Authentication** check box.

It is not necessary to change or provide values for any of the other settings in this area.

4. Enter values for the Connection Settings:

Property	Value

Base DN (location of users)	Users base domain name. Enter the following string:
	`cn=users.dc=<domain>.dc=com`
	where <domain> is the domain where NetScaler and the Informatica domain are installed. For example:
	`cn=users.dc=platformkrb.dc=com`

Administrator Bind DN	Email address of the LDAP server administrator
Administrator Password	Password for the administrator

It is not necessary to change or provide values for any of the other settings in this area.

5. In the Other Settings area, enter the following values:

Property	Value
Server Logon Name Attribute	Select New and type the following value: `samAccountName`
Search Filter	Enter the same string as you entered for the Base DN property in the previous step.
Sub Attribute Name	Type `cn`. The string `cn` stands for common name.

It is not necessary to change or provide values for any of the other settings in this area.

Note: Each of the fields in the Other Settings area is an LDAP attribute. Each one of these attributes contains metadata about the LDAP user who logs on to the Informatica web application using NetScaler SAML authentication. For example, user attributes include the name, the group which the user is a member of, the user's email address, and so on.

Each of these attributes is numbered in order, so that the Server Logon Name Attribute is known as Attribute 1. You use this when you configure the SAML IdP profile.

6. In the Nested Group Extraction area, it is not necessary to change any of the default values.
7. In the Attribute Fields area, enter the following value:

Property	Value
Attribute 1	Enter the same value that you entered for Server Logon Name Attribute: `samAccountName`

It is not necessary to change or provide values for any of the other settings in this area.

8. Click **OK**.

Enable the Authentication, Authorization and Auditing Server

The authentication, authorization, and auditing (AAA) server supports authentication, authorization, and auditing for all application traffic. Enable the AAA server to handle authentication requests.

1. In the NetScaler web interface, click **System** > **Settings** > **Modes and Features** > **Configure Basic Features**.
2. Verify that the following items in the list of features are selected:
   - SSL Offloading
   - Load Balancing
   - Citrix Gateway and Authentication
   - Authorization and Auditing
3. Click **OK**.

Configure the NTP Server Setting

Ensure that the service provider and NetScaler are in the same time zone.

1. In the NetScaler web interface, click the **Configuration** tab.
2. Click **Host Name** > **DNS IP Adddress** > **Time Zone** > **NTP Server**.
3. Select the time zone where the Informatica domain is deployed.
4. Click **OK**.

Create SAML IdP Profile

Create a SAML profile that points to the service provider and the service provider certificate.

1. In the NetScaler web interface, click **Policies** > **Authentication** > **SAML IdP**.
2. Select the Profiles tab, click **Add**, and enter values for the following properties:

Property	Description
Name	Name of the profile to create
Assertion Consumer Service URL	URL of the Informatica web application.
SAML Binding	Binding method. Select POST.
SP Certificate Name	Service provider certificate file name. The service provider is Informatica. This certificate is created on the Informatica domain when you create an LDAP configuration.
IDP Certificate Name	Identity provider certificate file name
Service Provider ID	Enter the service provider ID or spid. This is the same as the name of the profile to create.

3. Click **More**, and enter values for the following properties:

Property	Description
Audience	Enter the spid name. This is the same as the name of the SAML IdP Profile in the previous step.
Name ID Format	Select Unspecified
Name ID Expression	Enter `HTTP.REQ.USER.ATTRIBUTE(1)`
Sign Assertion	Select Assertion.
Signature Algorithm	Select RSA-SHA256.
Digest Algorithm	Select SHA256.

Property	Description
Attribute1	Enter the username of the LDAP user to authenticate.
Attribute 1 Expression	Enter the following value: `HTTP.REQ.USER.ATTRIBUTE(1)`

Note: LDAP "attributes" correspond to metadata about LDAP users.

4. Click **Save**.

Create and Configure SAML IdP Policy

Create a SAML policy that uses the SAML profile that you created.

1. In the NetScaler web interface, click **Policies** > **Authentication** > **SAML IdP**.
2. Select the Policies tab and click **Add**.
3. Enter values for the following settings:

Property	Value
Name	Enter a name for the policy.
Action	Select the name of the SAML IdP profile that you created in the previous step.
Expression	Enter the following string: `http.req.url.contains("saml")` Include all punctuation.

4. Click **OK**.

Configure Authentication LDAP Policy

Create an LDAP policy to use the Active Directory server for authentication.

1. In the NetScaler web interface, click **Policies** > **Authentication** > **LDAP** > **Policies**.
2. Click **Add** to add an authentication policy.
3. Enter values for the following properties:

Property	Value
Name	Enter a descriptive name for the LDAP policy.
Server	Choose **AD** to select the Active Directory server.
Expression	Enter the following string: `ns_true`

Configure AAA Virtual Server

Configure a virtual server for authentication, authorization and auditing (AAA).

1. In the NetScaler web interface, click **Security** > **AAA-Application Traffic** > **Virtual Servers**.
2. Click **Add** to add a virtual server.
3. Enter values for the following properties:

Property	Value
Name	Enter a descriptive name for the AAA server.
IP Address Type	Enter "IP address".
IP Address	Enter the IPv4 address of the virtual AAA server.
Port	Port number of the virtual server
Authentication	Select the Authentication check box.
State	Select the State check box.

4. Click **Continue**.
5. Select **No server Certificate** and attach the server certificate file.
6. Click **Continue**.
7. Select **No SAML IDP Policy** and attach the SAML IdP policy you created in "Configure SAML IdP Policy."
8. Click **Continue**.
9. Under Basic Authentication Policies, select **No LDAP Policy** and attach the LDAP policy you created in "Configure Authentication LDAP Policy.".
10. Click **Done**.

Enable NetScaler SAML Authentication in the Domain

Follow the steps in this section to configure Informatica domain settings to interact with the NetScaler identity provider.

Before you begin, you must have performed all the steps in preceding sections to download, deploy, and configure NetScaler in your network.

Note: If you enabled SAML authentication when you created the domain, it is not necessary to perform the steps to update the SAML configuration or update the gateway nodes.

Configure Hosts Files

Add host names and IP addresses to the `etc/hosts` files on the machines that host the NetScaler server, and the machines that host the domain.

1. Edit the `etc/hosts` file on the NetScaler server VM to add the host name and IP address of the machine that hosts the Informatica domain.

2. Edit the `etc/hosts` file on the machine that hosts the domain. Perform this step on all domain nodes. Add host name sand IP addresses for the following VMs:
   - NetScaler server
   - AAA server
   - Active Directory server
3. Repeat Step 2 on each machine from which a user accesses the web application.

Create or Verify the Security Domain

When you configure an Informatica domain to use NetScaler, you use Microsoft Active Directory as the identity store. The security domain imports Active Directory accounts to make them available for SAML authentication.

SAML authentication requires an LDAP configuration and a security domain for web application user accounts stored in Active Directory.

Each account in Active Directory must be imported into the security 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.

You can use an existing security domain. To create a security domain, perform these steps.

1. In the Administrator tool, click the **Users** tab, and then select the **Security** view.
2. Click the **Actions** menu and select **LDAP Configuration**.

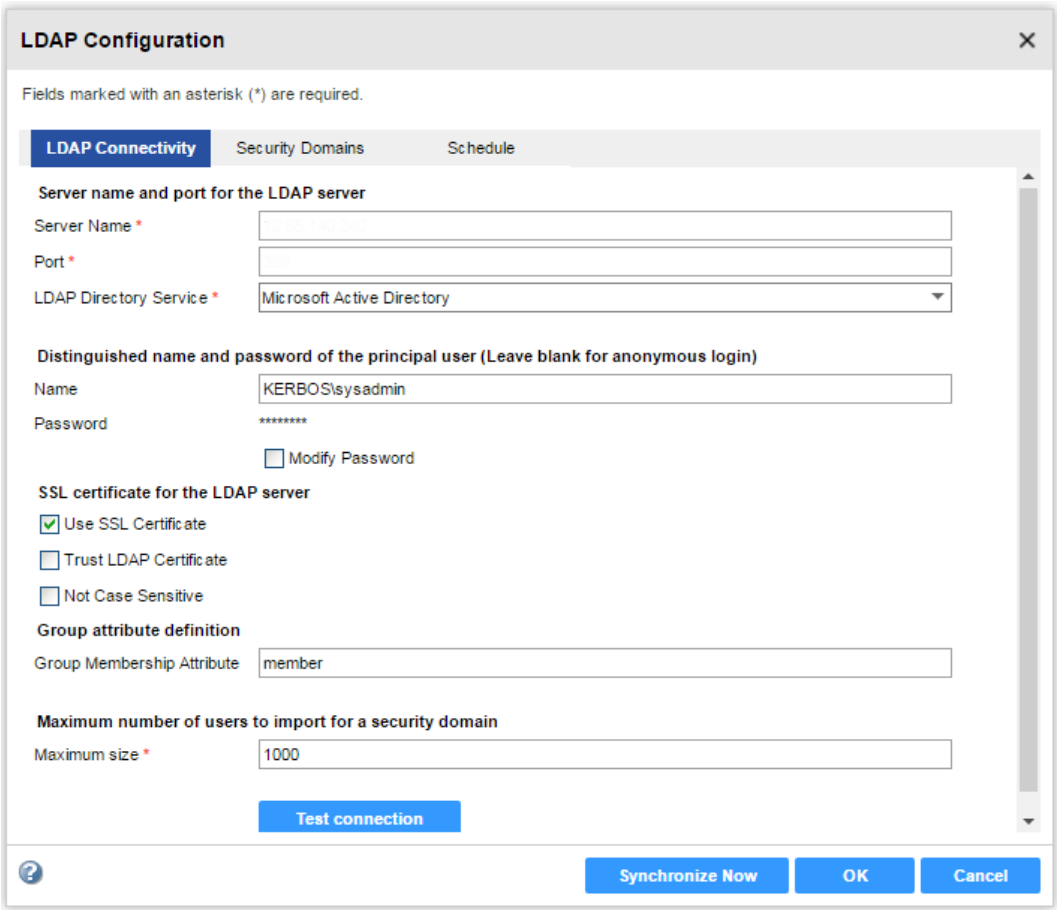
   The **LDAP Configuration** dialog box opens.
3. Click the **LDAP Connectivity** tab.
4. Configure the connection properties for the Active Directory server.

   The following table describes the server connection properties:

Property	Description
Server Name	Host name or IP address of the Active Directory server.
Port	Listening port for the Active Directory server. Default is 389.
LDAP Directory Service	Select **Microsoft Active Directory**.
Name	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.
Password	Password for the principal LDAP user.
Use SSL Certificate	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.

Property	Description
Trust LDAP Certificate	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.
Not Case Sensitive	Indicates that the Service Manager must ignore case sensitivity for distinguished name attributes when assigning users to groups. Enable this option.
Group Membership Attribute	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*.
Maximum size	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. Default is 1000.

The following image shows the connection details for an LDAP server set in the LDAP Connectivity panel of the **LDAP Configuration** dialog box.



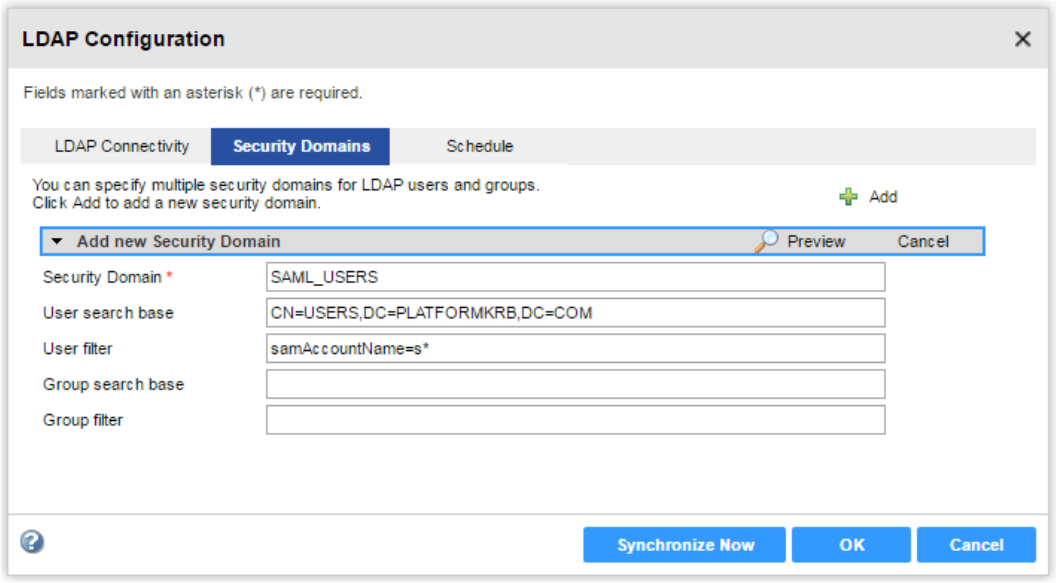
5. Click **Test Connection** to verify that the connection to the Active Directory server is valid.
6. Click the **Security Domains** tab.

7. Click **Add** to create a security domain.
8. Enter the security domain properties.

   The following table describes the security domain properties:

Property	Description
Security Domain	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: , + / < > @ ; \ % ? The name can contain an ASCII space character except for the first and last character. All other space characters are not allowed.
User search base	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: `cn=UserName,ou=OrganizationalUnit,dc=DomainName` where the series of relative names denoted by `dc=DomainName` identifies the DNS domain of the object. Use commas to separate name elements. For example, to search the Users container that contains user accounts in the example.com Windows domain, specify `CN=USERS,DC=EXAMPLE,DC=COM`.
User filter	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, the syntax to format the query string: `sAMAccountName=<account>`
Group search base	Distinguished name (DN) of the entry that serves as the starting point to search for group names in Active Directory.
Group filter	An LDAP query string that specifies the criteria for searching for groups in the directory service.

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 **Synchonize 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.

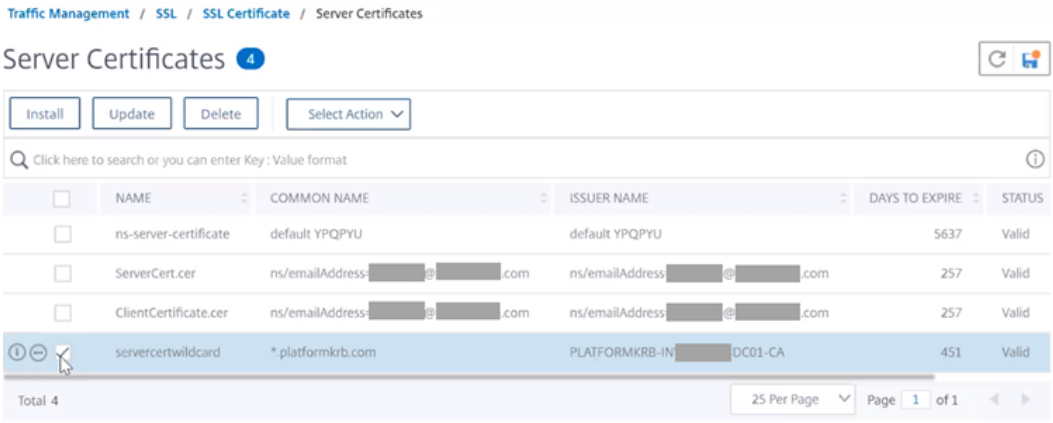
Export the Assertion Signing Certificate from NetScaler

Use the NetScaler interface to export the identity provider assertion signing certificate.

The exported certificate takes the form of a file. It should be a wildcard file that contains signing certification for an entire domain.

Use the NetScaler interface to access the certificate file.

1. Click the Configuration tab.
2. Browse to **Traffic Management** > **SSL** > **SSL Certificate** > **Server Certificates**.
3. Select the certificate to export.
   The redacted image below shows one of the certificates selected:



4. From the **Select Action** control, select **Download**.
5. Save the file in a location of your choice on the machine that hosts the Informatica domain.

Import the Certificate into the Truststore Used for SAML Authentication

Import the assertion signing certificate used by the identity provider 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`.

You can use the Java keytool key and certificate management utility to create an SSL certificate or a certificate signing request (CSR) as well as keystores and truststores in JKS format. The keytool is available in the following directory on domain nodes:

```
<Informatica installation directory>\java\bin
```

If the domain nodes run on AIX, you can use the keytool provided with the IBM JDK to create an SSL certificate or a Certificate Signing Request (CSR) as well as keystores and truststores.

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.
3. Run the keytool utility to import the certificate.
4. Restart the node.

Enable SAML Authentication in the Domain

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

When you enable a domain to use SAML authentication, all web applications that run in the domain use the default identity provider you specify when you enable SAML authentication in the domain. For example, if you configure AD FS as the identity provider, all web applications use AD FS as the identity provider, unless you configure a web application to use a different identity provider.

Select one of the following options:

Enable SAML authentication when you run Informatica installer.

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.

See the *Informatica Command Reference* for instructions on using the commands.

infasetup DefineDomain Command Options

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

The following example shows the options to configure a domain to use an identity provider:

```
infasetup defineDomain -cs "jdbc:informatica:oracle://host:1521;sid=DB2" -dt oracle -dn TestDomain -
ad test_admin -pd test_admin -ld $HOME/ISP/1011/source/logs -nn TestNode1 -na host1.company.com -
saml true -iu <identity provider URL> -spid Prod_Domain -cst 240 -asca adfscert -std \custom
\security\ -stp password -mi 10000 -ma 10200 -rf $HOME/ISP/BIN/nodeoptions.xml
```

The following table describes the SAML options and arguments:

Option	Description
-EnableSaml -saml	Required. Set this value to true to enable SAML authentication for supported Informatica web applications within the Informatica domain. Set this value to false to disable SAML authentication for supported Informatica web applications within the Informatica domain.
-idpUrl -iu	Required if the -saml option is true. Specify the identity provider URL for the domain. You must specify the complete URL string.
-ServiceProviderId -spid	Optional. The relying party trust name or the service provider identifier for the domain as defined in the identity provider. If you specified "Informatica" as the relying party trust name in the identity provider, you do not need to specify a value.
-ClockSkewTolerance -cst	Optional. The allowed time difference between the identity provider host system clock and the master gateway node's system clock. The lifetime of SAML tokens issued by the identity provider by is set according to the the identity provider host system clock. The lifetime of a SAML token issued by the identity provider 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	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.

Option	Description
-SamlTrustStoreDir -std	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	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.

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 to configure a domain to use <identity provider> as the identity provider:

```
infasetup updateDomainSamlConfig -saml true -iu https://01.00.000.00:9031/idp/SSO.saml2 -spid
<identity provider>_ProdDomain -cst 240
```

The following table describes the options and arguments:

Option	Description
-EnableSaml -saml	Required. Set this value to true to enable SAML authentication for supported Informatica web applications within the Informatica domain. Set this value to false to disable SAML authentication for supported Informatica web applications within the Informatica domain.
-idpUrl -iu	Required. Specify the <identity provider> URL for the domain. You must specify the complete URL string.
-ServiceProviderId -spid	Optional. The relying service provider identifier for the domain as defined in the <identity provider>. If you specified "Informatica" as the service provider name, you do not need to specify a value.
-ClockSkewTolerance -cst	Optional. The allowed time difference between the <identity provider> host system clock and the master gateway node's system clock. The lifetime of SAML tokens issued by the identity provider by is set according to the host system clock. The lifetime of a SAML token issued by the identity provider 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.

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

Enable SAML Authentication on the Gateway Nodes

You must configure SAML authentication on every gateway node in the Informatica domain.

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.

See the *Informatica Command Reference* for instructions on using the commands.

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:

```
infasetup defineGatewayNode -cs "jdbc:informatica:oracle://host:1521;sid=xxxx" -du test_user -dp
test_user -dt oracle -dn TestDomain -nn TestNode1 -na host2.company.com:1234 -ld $HOME/ISP/1011/
source/logs -rf $HOME/ISP/BIN/nodeoptions.xml -mi 10000 -ma 10200 -ad test_admin -pd test_admin -
saml true -asca pingcert -std \custom\security\ -stp password
```

The following table describes the options and arguments:

Option	Description
-EnableSaml -saml	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.
-AssertionSigningCertificateAlias -asca	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.
-SamlTrustStoreDir -std	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.
-SamlTrustStorePassword -stp	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 DefineGatewayNode, the infasetup UpdateGatewayNode, and the infacmd isp SwitchToGatewayNode commands.

Sync LDAP Users

Synchronize LDAP users with the domain.

1. Use infacmd to add LDAP connectivity to the domain. For example:

```
infacmd.sh addLDAPConnectivity -dn ISPDomain -un ispadmin -pd <password> -la
<Informatica domain IP address>:<port number> -lt "MicrosoftActiveDirectory" -lp
isplldapuser -lc "<password>" -lcn SAML_test
```

2. Use infacmd to add a namespace. For example:

```
infacmd.sh addNamespace -dn ISPDomain -un ispadmin -pd <password> -ns SAML -usb
cn=users,dc=platformkrb,dc=com -uf "(objectclass=user)" -gsb
"cn=users,dc=platformkrb,dc=com" -gf "(objectclass=group)" -lcn SAML_test
```

3. Use infacmd to sync the security domain. For example:

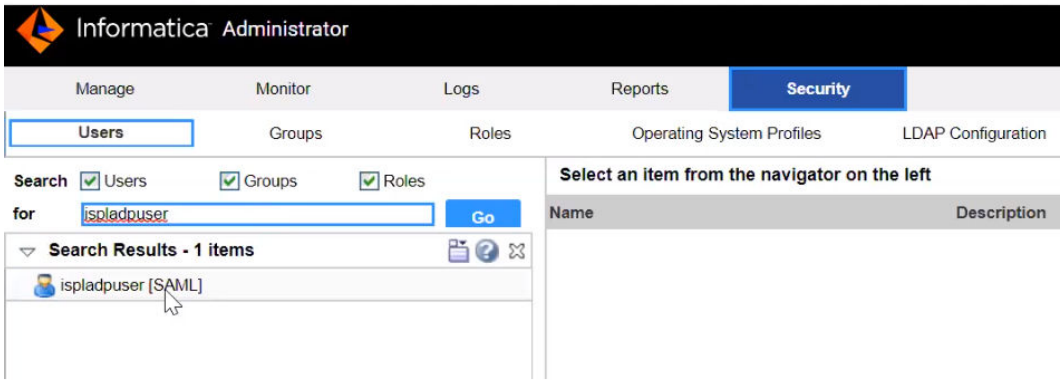
```
infacmd.sh SyncSecurityDomains -dn ISPDomain -un ispadmin -pd <password> -sdn Native -sn
SAML
```

Provide Domain Privileges to a SAML Namespace User

Use the Administrator tool to grant privileges on the domain to the SAML user.

1. Click the **Security** tab and then the **Users** tab.
2. Select the **Security Domains** tab.
3. Select the user you want to use to log into to SAMLauthentication-enabled web applications.

   You might have to use the search function to find the user. Select the user in search results. The image below shows a user in the results list:

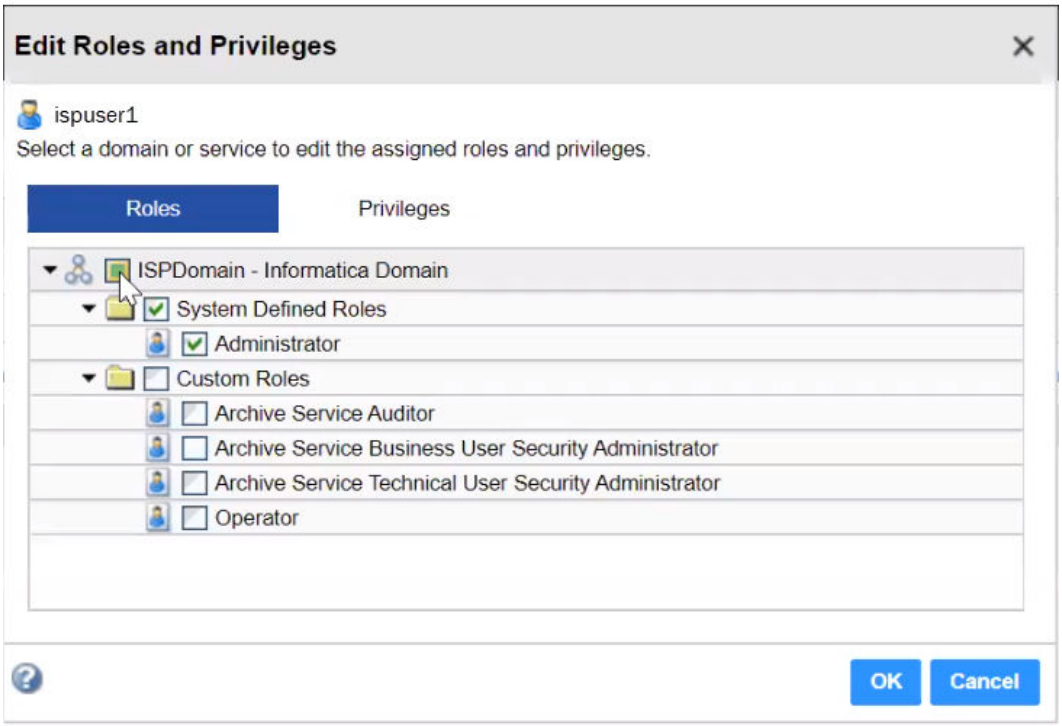


4. Click the **Privileges** tab.
5. Click the **Edit** button.

   The image below shows the location of the Edit button:

6. Use the **Edit Roles and Privileges** dialog box to grant privileges.

   The image below shows the **Edit Roles and privileges** dialog box:



7. Click **OK**.

For more information about domain privileges, see the chapter on Privileges and Roles in the *Informatica Security Guide*.

Add the Web Application URL in Assertion Consumer Service URL Endpoints

Add the URL for the Informatica web application, such as the Administrator tool, to the NetScaler IdP profile.

1. Determine the URL of the web application. For example, the URL of the Administrator tool would be like the following address:

   `https://vm.company.com:<port number>/administrator/`

2. In the NetScaler interface, browse to **Citrix Gateway** > **Policies** > **Authentication**and select **SAML IDP**.
3. Click the **Profiles** tab.

4. Select the Authentication profile that you created for Informatica and click **Edit**.
5. Paste the URL of the web application in the Assertion Consumer Service URL field.

   Note: Only one assertion consumer URL can be configured for a SAML IDP profile.
6. Click **OK**.

Author

Mark Pritchard