How-To Library

Informatica

# Enabling SAML Authentication with Azure Active Directory 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 10.5 domain using Security Assertion Markup Language (SAML) v2.0 and the Azure Active Directory identity provider.

# Supported Versions

- Informatica Data Engineering Integration 10.5
- Informatica Enterprise Data Catalog 10.5
- Informatica Enterprise Data Preparation 10.5
- Informatica Metadata Manager 10.5

# Table of Contents



# Overview

You can configure Security Assertion Markup Language (SAML) authentication in an Informatica 10.5 domain using the Azure Active Directory 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 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

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

# Before you begin

Before you begin to configure Azure Active Directory identity provider and Informatica, complete the tasks in this section.

## *Prerequisites*

Perform the following prerequisite tasks:

- Verify that you have deployed and configured Informatica version 10.5 in the same network domain as the Azure Active Directory implementation.
- Verify that the Azure subscription is a premium subscription including Azure Active Directory SAML SSO.
- Ask your IT administrator to assign IP addresses in the same network domain for the LDAP server.

## *Verify the Informatica deployment on Azure*

Before you configure Azure Active Directory as the identity provider for Informatica, verify the Informatica deployment.

Verify the following requirements:

- Informatica is deployed on a virtual machine in the Azure environment.
- Verify that Informatica is deployed in the same virtual network (VN) as the Azure Active Directory identity provider.

# Configure Azure Active Directory identity provider

Perform the steps in this section to configure Azure Active Directory for integration with Informatica.

## *Create an application*

Create an application that provides authentication for Informatica from the Azure Active Directory identity provider.

1. Log in to the Azure portal at the following URL: `https://portal.azure.com/`.
2. Search for Azure Active Directory.
3. Browse to **Enterprise applications** > **New application**.
4. Select **Non-gallery applications**.
5. Enter the application name and click **Apply**.
6. In the created application, select **Single Sign-on**.

7. In the **Basic SAML Configuration** section, supply values for the following properties:

| Property | Value |
|---|---|
| Identifier | Name of the service provider connection. Enter the Identifier (Entity ID). |
| Reply URL | URL of the service provider web app. Enter the URL of the Informatica Administrator console. |

8. The Service provider user attribute allows the administrator to map message attributes that are included in an incoming or outgoing message with Active Directory SAML SSO session attributes.
In the **User Attributes and Claims** section, configure the following attribute elements:

| Element | Description |
|---|---|
| Name | Identifies the attribute as a holder of the principal user name. |
| Value | Value of the *user* attribute element. Enter the following string:<br>`user.userprincipalname` |

9. Click **Save**.

## *Enable Azure Active Directory Domain Services*

Perform the steps in this section to enable Azure Active Directory Domain Services.

### Prerequisites

Verify the following prerequisites:

- You have an active Azure premium subscription.
- You have an Azure Active Directory tenant associated with your subscription, either synchronized with an on-premises directory or a cloud-only directory.
- You have global administrator privileges in your Azure Active Directory (AD) tenant to enable Azure AD Domain Services (DS).
- You have the following privileges:
  - Global administrator privileges in your Azure AD tenant to enable Azure AD DS.
  - Contributor privileges in your Azure subscription to create the required Azure AD DS resources.

### Create and configure an Azure Active Directory Domain Services managed domain

Use the Azure portal to create and configure the managed domain on Azure Active Directory Domain Services.

1. Create a managed domain. See Create a managed domain in Azure documentation.
2. Deploy the managed domain. See Deploy the managed domain in Azure documentation.
3. Update DNS settings for the Azure virtual network. See Update DNS settings for the Azure virtual network in Azure documentation.
4. Enable user accounts. See Enable user accounts for Azure AD DS in Azure documentation.

## Create a certificate

Create a digital certificate to secure authentication.

See the Azure documentation.

**Note:** Use the powershell command described in the Azure documentation. Azure Secure LDAP requires the certificate to have extended key usage. Other tools such as OpenSSL cannot create a compatible certificate.

## Export the Certificate

Export the certificate as a .PFX certificate file.

The .PFX certificate file includes the private key that the domain needs to communicate with the AAD managed domain.

Perform the steps under the heading "Export a certificate for Azure AD DS" in the Azure documentation.

## Export the SAML signing certificate

Signed assertion of SAML requests requires a SAML signing certificate on the domain. Download this file from the application that you created.

In the application that you created, browse to the SAML Signing Certificate section. Download the certificate to your computer.

## Enable Secure LDAP

Enable secure LDAP on the managed domain.

See the Azure documentation.

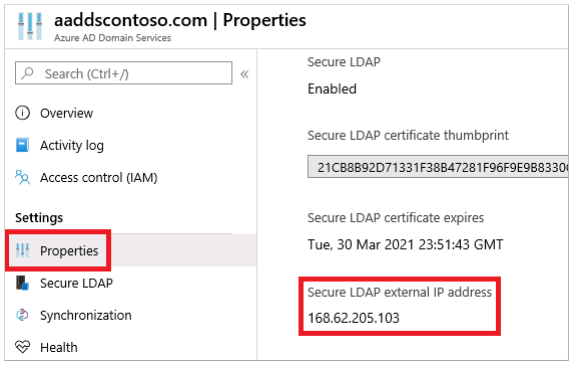
## Get the External LDAP IP Address

Get the external LDAP IP address from the Azure AD managed domain.

Get the IP address so that you can input it in the Informatica domain and client etc/hosts file:

1. Browse to the **Properties** tab for the Azure AD managed domain.
2. Locate and copy the Secure LDAP External IP address.

The following image shows how the managed domain control panel displays the IP address:



See the Azure documentation.

# Enable the Domain for Azure Active Directory

Configure elements on the domain to enable integration with Azure Active Directory as the identity provider.

## *Edit the hosts/etc file on domain and client machines*

Add the hostname and IP address of the Azure Active Directory LDAP managed domain host to the `etc/hosts` file on domain hosts and on client machines.

Use the following syntax in the hosts file:

```
<public ip address> ldaps.<Azure AD domain services name>
```

Verify that the host information is added to every machine that runs a Developer tool that communicates with the Azure Active Directory LDAP managed domain.

## *Import the truststore certificate*

Integration with Azure Active Directory requires two certificates that you import to the domain:

- The certificate that you created and exported in the steps "Create a certificate " on page 5 and "Export the Certificate" on page 5.
- The certificate to enable signed assertion that you downloaded in "Export the SAML signing certificate" on page 5.

1. Use the keytool utility to import the certificate file to the following location on the domain: `<Informatica home directory>\java\jre\lib\security\cacerts`.
2. Locate the certificate to enable signed assertion that you downloaded in "Export the SAML signing certificate" on page 5.
3. Use the keytool utility to import the certificate file to the domain and rename it. For example,

   ```
   keytool -import -alias SAML -file "<file path>/Informatica.cer" -keystore /<Informatica home directory>/source/services/shared/security/infa_truststore.jks -storepass <password>
   ```
4. Restart the domain.

For more information about using keytool to import the truststore certificate, see the *Informatica Security Guide*.

## *Update domain SAML configuration*

Use the infasetup updateDomainSAMLConfig command to enable SAML authentication on the domain and specify the identity provider URL.

For example: `./infasetup.sh updateDomainSAMLConfig -saml true -iu http://<Identity provider host>:<port>/<directory path>/samlv20`

**Note:** The example does not contain all required options. See the information about infasetup updateDomainSAMLConfig in the *Informatica Command Reference*.

The -spid option is required for Informatica releases 10.2.2 and higher. The option specifies the relying party trust name. Use the value that you provided for the Identifier property in Step 7 of "Create an application " on page 3.

## *Optional: Configure the certificate alias on gateway nodes*

If you use the assertion signing feature, update gateway nodes with the Azure Active Directory truststore certificate alias.

The certificate alias refers to the truststore certificate that enables signed assertion.

1. Run the following command to configure the certificate alias:
   `./infasetup.sh updateGatewayNode -saml true -asca <alias>`
2. After the command runs, recycle the Informatica domain.

## *Synchonize Azure Active Directory LDAP users*

Synchronize users from the LDAP directory that resides on the Oracle Access Manager with the domain.

### Add LDAP server connection properties

Run the addLDAPConnectivity command to add the connection information for an LDAP server. The LDAP server connection enables the Service Manager sets up the connection to an LDAP server and imports the user accounts of the LDAP security domains which are configured to this LDAP server.

Syntax: `infacmd.sh addLDAPConnectivity -dn <domain name> -un <domain user name> -pd <domain user password> -la <LDAP Server Address> -lt <LDAP types> -lp <LDAP principal> -lc <LDAP credential> -lcn <LDAP host configuration name>`

### Add the identity provider namespace

Run the addNamespace command to add the identity provider user namespace to the domain. The command can filter the namespace by user name and group names.

Syntax: `infacmd.sh addNamespace -dn <domain name> -un <user name> -pd <password> -ns <namespace> -usb <usersearchbase> -uf <userfilter> -gsb <groupsearchbase> -gf <groupfilter> -lcn <LDAP host configuration name>`

### Synchronize users

Run the SyncSecurityDomains command to synchronize security domain users and groups with LDAP users and groups.

Syntax: `infacmd.sh SyncSecurityDomains -dn <domain name> -un <user name> -pd <password> -sdn <security domain name> -sn <namespace to sync>`

See the *Informatica Command Reference* for more information about each command.

## *Grant privileges to the SAML namespace user*

Grant administrator permissions to the domain to the identity provider SAML user:

1. In the Administrator tool, click the Security tab.
2. Search for the identity provider SAML user.
3. Assign Administrator permissions to the user.

# Author

**Mark Pritchard**