

Identity Provider Configuration for Endpoint

Friday, October 11, 2019

Contents

Tenant Administrator	3
Install software and authenticate users.....	3
Adding an Active Directory Domain Controller	4
Domain Controller Settings for Active Directory	5
Adding Identity Servers.....	5
Sample SAML IdP Metadata XML.....	6
Sample SAML SP Metadata XML.....	7
Creating Certificates for SAML Integration.....	7
Automatically Creating Users from a SAML Response.....	10
Mapping SAML Attributes	12
Identity Provider Use Cases.....	14
Creating and Inviting Local Users	23
Index.....	25

Tenant Administrator

The tenant administrator is a person within your company who can view backup and recovery jobs, events, alerts, reports, and resources for the endpoint devices associated with your company. The tenant administrator is responsible for the following operations:

- Adding company endpoint users to the data protection solution
- Managing existing endpoint users
- Adding and managing endpoint devices
- Monitoring the status of daily backup operations
- Conducting on-demand restores

Install software and authenticate users

To backup and monitor endpoint data, the Endpoint package must be installed on your users' laptops and desktops. You can ask your users to download and to install the laptop package, or you can perform a silent installation of the laptop package. To decide which method to use in your environment, review the details of each method.

Interactive installations

User authentication	Tenant administrator action	User action
Active Directory	<ul style="list-style-type: none"> • Configure an Active Directory identity server. • Distribute the link for the laptop package and the auth code to users. Users can also use their email addresses to register their laptops. 	Download and install the laptop package, and then register the laptop or desktop with the auth code provided by the tenant administrator or your email address.
SAML	<ul style="list-style-type: none"> • Configure an identity provider that supports SAML. • Distribute the link for the laptop package and the auth code to users. 	Download and install the laptop package, and then register the laptop or desktop with the auth code provided by the tenant administrator.
Local	Create users and automatically send the users email invitations. The email invitation contains a link for the laptop package and user credentials.	Download and install the laptop package, and then register the laptop or desktop with the credentials in the invitation email.

Silent installations

User authentication	Tenant administrator action	User action
Active Directory	<ul style="list-style-type: none"> • Configure an Active Directory identity server. • Install the laptop package by using a third-party tool and the auth code. 	None
SAML	<ul style="list-style-type: none"> • Configure an identity provider that supports SAML. • Install the laptop package by using a third-party tool and the auth code. 	None

Adding an Active Directory Domain Controller

You can add (register) a domain controller (also referred to as name server or identity server) so that users who are members of the domain can log on with their domain credentials.

Before You Begin

If you want to use Active Directory single sign-on, configure LDAP on the Active Directory Server.

Procedure

1. From the navigation pane, go to **Security > Identity server**.
The **Identity servers** page appears.
2. In the upper-right corner of the page, click **Add**.
The **Add domain** dialog box appears.
3. On the **AD** tab, click the **Directory type** list and choose a domain controller type.
4. Enter the information according to the type of domain controller you want to add:
 - Active Directory (on page 5)
5. To associate the domain controller with a company, from the **Create for company** list, select the company.
6. Click **Save**.

Domain Controller Settings for Active Directory

When adding or editing an Active Directory domain controller, you must enter the following information:

- **NETBIOS name:** The fully qualified domain name that you use to identify this network resource, for example, my.domain.example.com.
- **Domain name:** The fully qualified domain name, for example, my.domain.example.com.
- **Username, Password:** The domain credentials (domain\username) for a user who has at least read permission for the domain.
- **Create for Company:** (Optional) The company to associate the domain controller with in the CommCell environment.

Adding Identity Servers

You can add third-party identity providers (IdP), such as Okta, OneLogin, and ADFS, so that users can be authenticated. SAML metadata is used to share configuration information between the Identity Provider (IdP) and the Service Provider (SP). Metadata for the IdP and the SP is defined in XML files:

- The IdP metadata XML file contains the IdP certificate, the entity ID, the redirect URL, and the logout URL. For an example, see [Sample SAML IdP Metadata XML](#) (on page 6).
- The SP metadata XML file contains the SP certificate, the entity ID, the Assertion Consumer Service URL (ACS URL), and a log out URL (SingleLogoutService). For an example, see [Sample SAML SP Metadata XML](#) (on page 7).

Before using SAML to log on to the Web Console or Command Center, metadata from the IdP must be uploaded and metadata from the SP must be generated. After the SP metadata is generated, it must be securely shared with the IdP. Contact the IdP for instructions on sharing the SP metadata.

Before You Begin

1. Create or get an Identity Provider (IdP) metadata XML file using the SAML protocol. For SAML metadata specifications, go to the Oasis (<https://www.oasis-open.org/>) website, *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*.

For an example, see [Sample SAML IdP Metadata XML](#) (on page 6).

2. Create a keystore file. For information on keystore files, see [Creating Certificates for SAML Integration](#) (on page 7).

Procedure

1. From the navigation pane, go to **Security > Identity servers**.

The **Identity servers** page appears.

2. To create an identity server, click **Add**.

The **Add SAML App** dialog box appears.

3. In the **Application Name** box, enter an application name.
4. If you are an MSP administrator creating the SAML app for a company, in the **Created for company** box, select the company.

If you are creating the SAML app for the entire CommCell environment or if you are a tenant administrator, a company is not needed.

5. Upload the IdP metadata:
 - a. Next to the **Upload IDP metadata** box, click **Browse**.
 - b. Browse to the location of the XML file that contains the IdP metadata, select the file, and click **Open**.
6. Generate the SP metadata:
 - a. Under **Generate new SP metadata**, next to the **Upload key store file** box, click **Browse**.
 - b. Browse to the location of the keystore file, for example, C:\security\mykeystore.jks, select the file, and click **Open**.
7. Enter the keystore file values for **Alias name**, **Key Store Password**, and **Key Password**.
8. To generate the SP metadata and to save the IdP metadata, click **Save**.

After the SP metadata is generated, it must be securely shared with the IdP. Contact the IdP for instructions on sharing the SP metadata.

What to Do Next

After you add the Identity server, create redirect rules to automatically add users from the SAML response to a specific domain. For more information, see [Automatically Creating Users from a SAML Response](#) (on page 10).

Sample SAML IdP Metadata XML

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor validUntil="2024-08-13T07:37:40.675Z"
entityID="https://test.my.company.com"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:IDPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
WantAuthnRequestsSigned="false">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>encoded_certificate</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

```

    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified</md:NameIDFormat>
    <md:SingleLogoutService
Location="https://test.my.company.com/adfs/ls/IDPLogout"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
    <md:SingleSignOnService
Location="https://test.my.company.com/idp/endpoint/HttpRedirect"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
    </md:IDPSSODescriptor>
</md:EntityDescriptor>

```

Sample SAML SP Metadata XML

```

<?xml version="1.0" encoding="UTF-8"?>
<EntityDescriptor entityID="https://client.mydomain.com:443/webconsole"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
WantAssertionsSigned="true">
    <AssertionConsumerService isDefault="true" index="0"
Location="https://client.mydomain.com:443/webconsole/samlAcsIdpInitCallback.do?s
amlAppKey=NjZEOUQ1RDRCQjE1NEI0"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="
https://client.mydomain.com:443/webconsole/server/SAMLSingleLogout?samlAppKey=Mz
U2MkNDQTFBQzZczNEZG"
ResponseLocation="https://client.mydomain.com:443/webconsole/server/SAMLSingleLo
gout"/>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Location=" https://client.mydomain.com:443/webconsole/server/SAMLSingleLog
out?samlAppKey=MzU2MkNDQTFBQzZczNEZG"ResponseLocation="https://client.mydomain.co
m:443/webconsole/server/SAMLSingleLogout"/>
    <KeyDescriptor>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>encoded_certificate</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:entity</NameIDFormat>
  </SPSSODescriptor>
</EntityDescriptor>

```

Creating Certificates for SAML Integration

In Service Provider (SP) initiated SAML, a SAML request is prepared by the SP. The SP digitally signs the request using a private key. When the request is received by the Identity Provider (IdP), the digital signature is verified using the public key sent by the SP in a certificate. Certificates are self-signed or signed by a certification authority (CA).

A Java keystore file stores the certificate and the private key. To create the Java keystore file, use the keytool utility, the Java key and certificate management tool. For more information on the keytool utility, go to the Oracle Documentation (<http://www.oracle.com/technetwork/documentation/index.html>) website, *keytool - Key and Certificate Management Tool*.

Procedure

Creating a Self-Signed Certificate and a Private Key

Use the keytool utility to create a keystore file that contains a private key and a self-signed certificate that holds a public key.

1. Run the following command from the C:\Program Files\Java\java_version\bin folder after substituting the parameter values.
2. The command can be run from %JAVA_HOME%\bin if the %JAVA_HOME% environment variable is set.

```
keytool -genkey -keyalg RSA -alias <aliasName> -keystore
<file_path\keystoreFilename.jks> -validity <daysValid> -keysize 2048
```

3. The following table displays the parameters for the keytool command:

Parameter	Description of Parameter Values
alias	The alias name for the certificate.
keystore	The file path and file name for the .jks file created by the keytool.
validity	The number of days the keystore file is valid starting from the day the keystore file is created.

Example

```
keytool -genkey -keyalg RSA -alias selfsigned -keystore "C:\mykeystore.jks" -
validity 365 -keysize 2048
```

4. When prompted, enter the information requested by the keytool command.
5. Make note of the following values:
 - name and location of the keystore file
 - alias name
 - keystore password
 - key password

Use these values to create the SP metadata XML file. For information, see *Adding Identity Servers* (on page 5).

Creating a CA-signed Certificate and a Private Key

Use the keytool utility to create a keystore file that contains a private key and a CA-signed certificate that holds a public key.

1. Create a keystore file containing a local certificate:

- a. Run the following command from the C:\Program Files\Java\java_version\bin folder after substituting the parameter values.

The command can be run from %JAVA_HOME%\bin if the %JAVA_HOME% environment variable is set.

```
keytool -genkey -keyalg RSA -alias <aliasName> -keystore <file_path\keystoreFilename.jks>
```

The following table displays the parameters for the keytool command:

Parameter	Description of Parameter Values
alias	The alias name for the certificate. The alias name is used to import the CA-signed certificate.
keystore	The file path and file name for the .jks file created by the keytool.

Example

```
keytool -genkey -keyalg RSA -alias casigned -keystore "C:\mykeystore.jks"
```

- b. When prompted, enter the information requested by the keytool command.

For CA-signed certificates, the company and location information must be accurate, for example, when prompted for the **Organization Name**, enter the full legal name of your organization.

- c. Make note of the following values:

- name and location of the keystore file
- alias name
- the keystore password
- the key password

After the CA-signed certificate is imported into the keystore file, use these values to create the SP metadata XML file. For information, see [Adding Identity Servers](#) (on page 5).

2. Generate a Certificate Signing Request (CSR) and submit it to the CA.

- a. Run the following command from the C:\Program Files\Java\java_version\bin folder after substituting the parameter values.

The command can be run from %JAVA_HOME%\bin if the %JAVA_HOME% environment variable is set.

```
keytool -certreq -keyalg RSA -alias <aliasName> -file <request_file_name.csr> -keystore <file_path\keystoreFilename.jks>
```

The following table displays the parameters for the keytool command:

Parameter	Description of Parameter Values
alias	The alias name for the certificate. The alias name is used to import the CA-signed certificate.
file	The file name of the .csr file.
keystore	The file path and file name for the .jks file created by the keytool.

Example

```
keytool -certreq -keyalg RSA -alias casigned -file certreq.csr -keystore "C:\mykeystore.jks"
```

- b. Submit the .csr file to your CA according to their procedure.
3. Import the CA-signed certificate into the keystore file according to the procedure provided by the CA.

Run the following command from the C:\Program Files\Java\java_version\bin folder after substituting the parameter values.

The command can be run from %JAVA_HOME%\bin if the %JAVA_HOME% environment variable is set.

```
keytool -importcert -file <CertificateFileName> -keystore <keystoreFileName> -alias <AliasName>
```

The following table displays the parameters for the keytool command:

Parameter	Description of Parameter Values
file	The file name of the .csr file.
keystore	The file path and file name for the .jks file created by the keytool.
alias	The alias name for the certificate.

Example

```
keytool -importcert -file certificate.cer -keystore "C:\mykeystore.jks" -alias casigned
```

Automatically Creating Users from a SAML Response

Metallic users can be automatically created from SAML identity provider (IdP) responses that contain a user email address. The users are identified by their SMTP address. After a user is automatically created, that user can be automatically added to a user group.

Procedure

1. From the navigation pane, go to **Security > Identity servers**.

The **Identity servers** page appears.

2. In the **Application name** column, click the application name.

The application details page appears.

3. Under **General**, click the **Auto create user** toggle key.

4. To automatically add users to a user group, choose the user group:

- a. To the right of **User group**, click **Edit**.

The **Edit default user group** dialog box appears.

- b. In the **User group** list, click the user group to associate with the users who are automatically created.

- c. Click **Save**.

5. Under **Identity redirect rule**, click **Add identity redirect rule**.

The **Add identity redirect rule** page appears.

6. Optional: In the **Domain name** box, select an existing domain, or type a new domain name. The users that are automatically created are added to the selected domain.

7. In the **Associated SMTP** box, enter an SMTP address, and then click **Add**.

The SMTP address identifies the users who need to be automatically created.

8. Click **Save**.

Related Topics

Mapping SAML Attributes (on page 12)

Mapping SAML Attributes

You can map attributes in the identity provider (IdP) response to user attributes used in the Metallic software. For example, by default, a user email address is expected in the **NameID** element in the IdP response. If your IdP sends the user email address in an attribute instead of in the **NameID** element, you can map that attribute so that the value of the attribute is used for the user email address.

Available Attributes

You can map IdP response attributes to the user attributes in the following table. Your mappings take precedence over default sources.

User Attribute	Details
user name	<p>The mapping for the user name attribute is used to validate the user when they log on. The default source for the user name attribute is the NameID element.</p> <pre><Subject> <NameID>jknight</NameID> ... </Subject></pre>
user groups	<p>Applies to: AD FS and Okta identity providers</p> <p>The mapping for the user groups attribute is used to associate or disassociate the user with domain groups (external groups) that were added to the CommCell environment.</p>
email	<p>The mapping for the email attribute is used to validate the user when they log on. The default source for the email attribute is the NameID element.</p> <pre><Subject> <NameID>jknight@mycompany.com</NameID> ... </Subject></pre>
user GUID	<p>If the Auto create user option is selected, the mapping for the user GUID attribute is used as the user GUID. If the Auto create user option is selected and a mapping is not provided, the user GUID is a system-generated value.</p>
SID	<p>Applies to: Active Directory identity providers</p>
Group SID	<p>The mappings for the SID attribute and the group SID attribute are used to facilitate the ACL (Access Control List) browse for agents such as the Windows File System Agent and the SharePoint Server Agent.</p>

Procedure

1. From the navigation pane, go to **Security > Identity servers**.

The **Identity servers** page appears.

2. In the **Application name** column, click the application name.

The application details page appears.

3. Under **Attribute mappings**, click **Edit**.

The **Edit attributes** dialog box appears.

4. Click **Add mappings**.

5. In the **SAML attributes** box, enter the attribute from the IdP response.

For example, enter **<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>**.

6. In the **User attributes** list, click the user attribute that the IdP response attribute maps to.

For example, if the IdP response attribute is <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>, click **Email**.

7. To add additional mappings, click **Add mappings**.

8. Click **Save**.

Examples

The following samples are mappings and the results of the mappings:

SAML Attribute	User Attribute	Attribute statement	Result
http://schemas.microsoft.com/2012/12/certificatecontext/field/subject	email	<pre><AttributeStatement> <Attribute Name="http://schemas.microsoft.com/2012/12/certificatecontext/field/subject"> <AttributeValue>jknight@mycompany.com</AttributeValue> </Attribute> </AttributeStatement></pre>	The value jknight is used to validate the user.

http://schemas.xmlsoap.org/claims/Group	user groups	<pre><Attribute Name="http://schemas.xmlsoap.org/claims/Group"> <AttributeValue>Domain Users</AttributeValue> </Attribute></pre>	The user is associated with the Domain Users group.
---	-------------	--	--

Identity Provider Use Cases

In the Command Center, the procedure for setting up a SAML app for an identity provider (IdP) is the same, but each IdP has their own procedure. The Active Directory Federation Services (AD FS) use case, the Azure Active Directory use case, and the Okta use case demonstrate different methods for setting up an IdP.

AD FS

AD FS (Active Directory Federation Services) is a service that allows federation partners to share identities. To integrate with AD FS, do the following:

- In AD FS, retrieve IdP (identity provider) metadata
- In the Command Center, add a SAML application
- In AD FS, create a relying party trust

Before You Begin

- Use the Microsoft Server Manager to install the AD FS role service. For instructions, go to the Microsoft (<https://docs.microsoft.com>) website, *Install the AD FS Role Service*.
- **Important:** Because AD FS only accepts a relying party trust that has an HTTPS URL in the metadata, your Web Console must use HTTPS.

Procedure

Retrieving the IdP Metadata

1. To open the AD FS Management console, from the Microsoft Server Manager, in the upper right, expand **Tools**, and then click **AD FS Management**.
2. In the left navigation pane, expand **AD FS > Service**, and then click **Endpoints**.
3. In the right pane, under **Endpoints > Metadata**, in the **Federation Metadata** row, copy the URL path.

For example, copy **FederationMetadata/2007-06/FederationMetadata.xml**

4. Add the host name of the AD FS computer to the URL path you copied as follows:
`https://hostname/FederationMetadata/2007-06/FederationMetadata.xml`
5. To retrieve the IdP (identity provider) metadata, in a browser, paste the complete URL.
6. Save the IdP metadata as an XML file.
7. Leave the AD FS Management console open.

Creating a SAML app in the Command Center

1. Open the Command Center.
2. From the navigation pane, go to **Security > Identity servers**, and then create the SAML app using the IdP metadata file that you saved.

For information about adding a SAML application in the Command Center, see [Adding a SAML Application](#) (on page 5).

3. After the SP (service provider) metadata is generated, place the SP metadata on the AD FS machine.

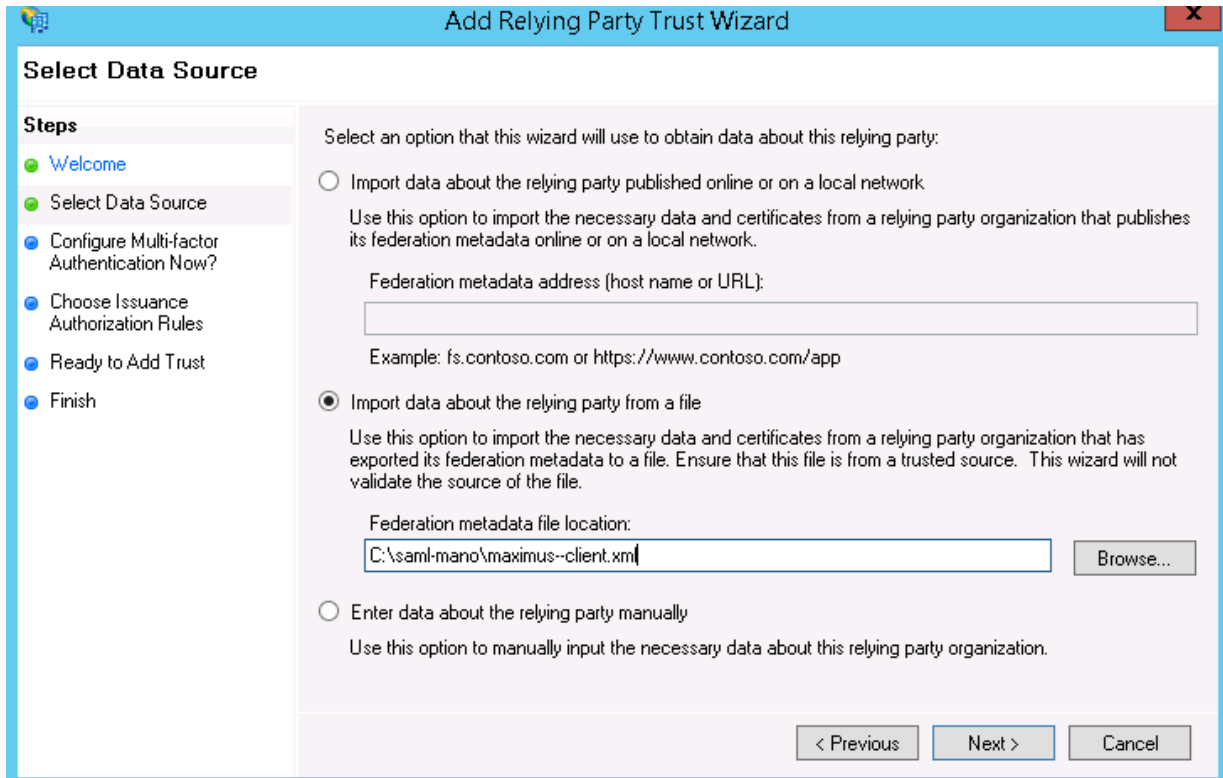
Creating a Relying Party Trust

1. From the AD FS Management console, in the left navigation pane, expand **AD FS > Trust Relationships**.
2. Right-click **Relying Party Trusts**, and then click **Add Relying Party Trust**.

The **Welcome** page of the **Add Relying Party Trust Wizard** window appears.

3. Click **Start**.
4. On the **Select Data Source** page, click **Import data about the relying party from a file**.

- In the **Federation metadata file location** box, browse to the location of the SP metadata that you placed on the AD FS machine.



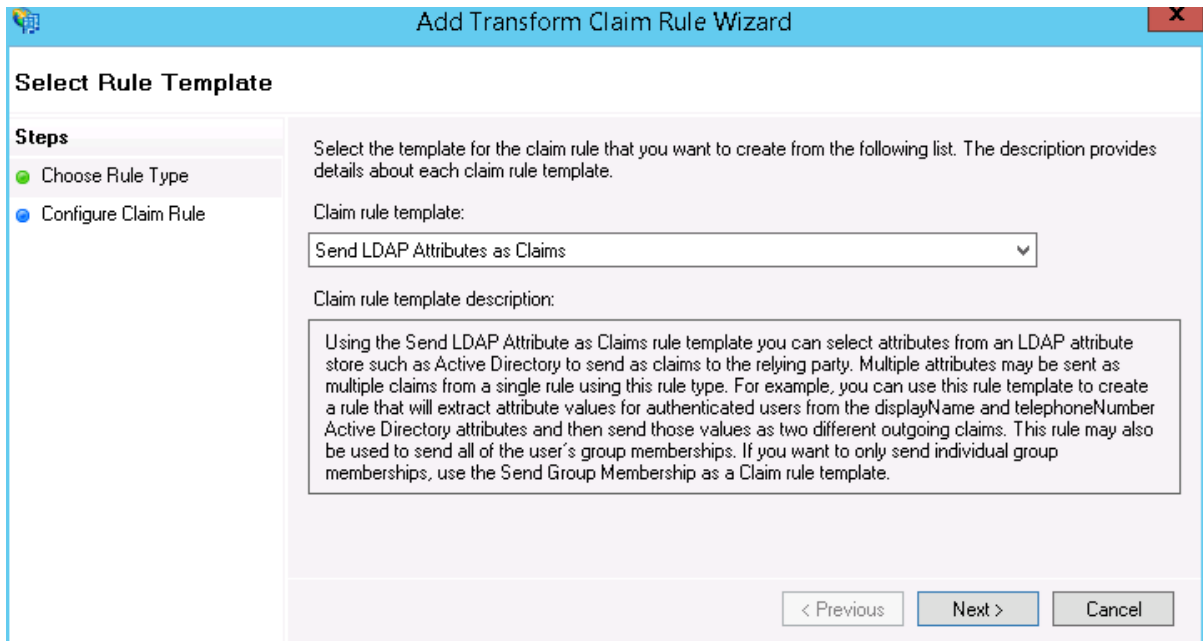
- Click **Next**.
- Continue to go through the wizard, referring to Microsoft documentation to configure additional features such as multi-factor authentication and issuance authorization rules.
- After you complete the wizard, click **Close**.

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

- On the **Issuance Transform Rules** tab, click **Add Rule**.

The **Select Rule Template** page of the **Add Transform Claim Rule Wizard** window appears.

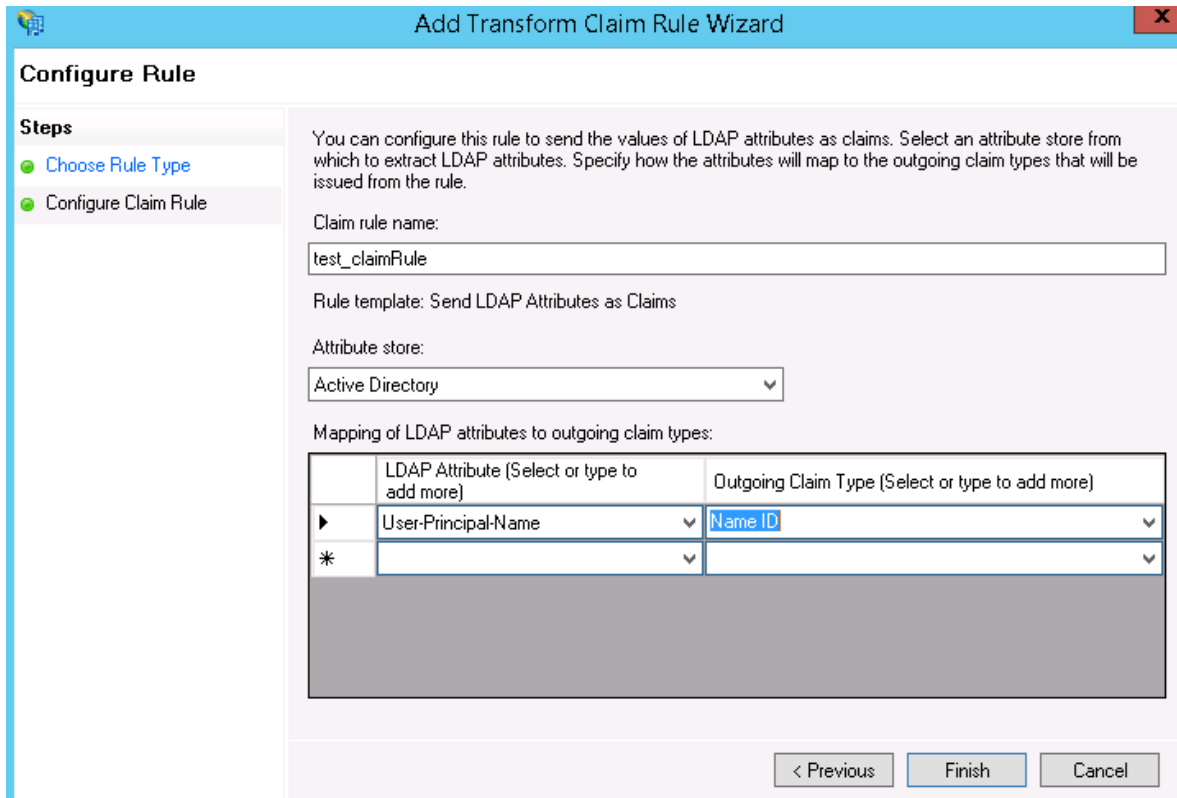
- From the **Claim rule template** list, click **Send LDAP Attributes as Claims**.



- Click **Next**.

The **Configure Rule** page appears.

- In the **Claim rule name** box, enter a name for the rule.
- From the **Attribute store** list, click **Active Directory**.
- In the **Mapping of LDAP attributes to outgoing claim types** table, add the LDAP attribute and the outgoing claim type:
 - From the **LDAP Attribute** list, select either **Email Addresses** or **User-Principal-Name**.
 - From the **Outgoing Claim Type** list, select **Name ID**.



15. Click **Finish**, and then click **OK**.

Azure

Azure Active Directory (Azure AD) is a third-party identity provider that can act as the IdP when your users log on to the Web Console or the Command Center.

To integrate with Azure AD, add a SAML application in the Command Center and in your Azure AD account.

Before You Begin

You must have the Azure Active Directory Premium P1 or Premium P2 edition. For information, go to the Microsoft Azure Active Directory documentation <https://docs.microsoft.com/en-us/azure/active-directory/>.

Procedure

1. In the Command Center, begin to configure the SAML application:
 - a. Open the **Add SAML App** dialog box, and in the **Webconsole url** box, copy the URL.

For example, `https://mycompany:443/webconsole`

For information about adding a SAML application in the Command Center, see [Adding Identity Servers](#) (on page 5).

- b. Keep the **Add SAML App** dialog box open.
2. From the Microsoft Azure portal <https://portal.azure.com>, create a new application using SAML as the sign on method:
 - a. From the navigation pane, go to **Azure Active Directory > Enterprise applications**, and then click **New application** (**+ New application**).
 - b. Under **Add an application**, click the **Non-gallery application** tile.
 - c. Enter a name for the application, and then click **Add**.
 - d. Review the overview, and complete the following steps required by Microsoft: **Assign a user for testing** and **Create your test user in test**.
 - e. Click **Configure single sign-on**.
 - f. Under **Single sign-on**, in the **Single Sign-on Mode** list, click **SAML-based Sign-on**.


The SAML single sign-on options appear.


- g. Under **Domain and URLs**, in the **Identifier** box, paste the entity ID that you copied from the SAML app in the Command Center.

Similarly, in the **Reply URL** box, paste the single sign-on URL that you copied from the Command Center.

Domain and URLs

Values for the fields below are provided by test. You may enter or [upload a metadata file](#) if test provide one.

* Identifier 
Pattern: <http://adapplicationregistry.onmicrosoft.com/customappsso/primary>

* Reply URL 
Pattern: <https://127.0.0.1:444/applications/default.aspx>

- h. Under **User Attributes**, in the **User Identifier** box, enter **user.userprincipalname**.

User Attributes [Learn more](#)


Edit the user information sent in the SAML token when user sign in to test.

User Identifier  

- i. To download the IdP metadata file, under **SAML Signing Certificate**, in the **DOWNLOAD** column, click **Metadata XML**.

SAML Signing Certificate [Learn more](#)

Manage the certificate used by Azure AD to sign SAML tokens issued to test.

App Federation Metadata Url 

STATUS	EXPIRATION	THUMBPRINT	DOWNLOAD
Active	4/12/2021	28A542B3314229B13EA75D54427FB14330461D...	Certificate (Base64) Certificate (Raw) Metadata XML

3. In the Command Center, complete the SAML application:
 - a. To upload the IdP metadata XML file, in the open **Add SAML App** dialog box, next to **Upload IDP metadata**, click **Browse**.
 - b. Select the IdP metadata XML file that you downloaded from the Microsoft Azure portal.
 - c. Complete the application and click **Save**.

For information about adding a SAML application in the Command Center, see [Adding Identity Servers](#) (on page 5).

Okta

Okta is a third-party identity provider that can act as the IdP when your users log on to the Web Console or the Command Center.

To integrate with Okta, add a SAML application in the Command Center and in your Okta account.

Procedure

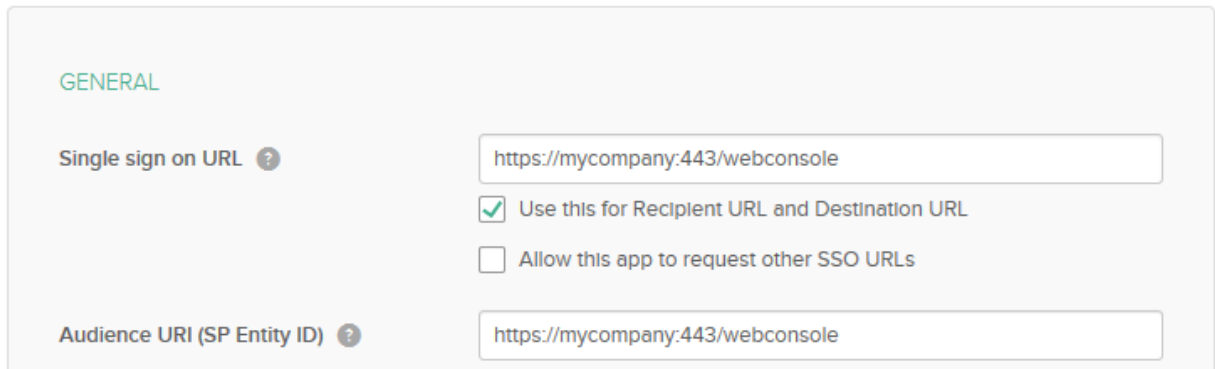
1. In the Command Center, begin to configure the SAML application:
 - a. Open the **Add SAML App** dialog box, and in the **Webconsole url** box, copy the URL.

For example, `https://mycompany:443/webconsole`

For information about adding a SAML application in the Command Center, see [Adding Identity Servers](#) (on page 5).
 - b. Keep the **Add SAML App** dialog box open.
2. In your Okta account, create a new application using SAML 2.0 as the sign on method:
 - a. Follow the wizard for the general settings.

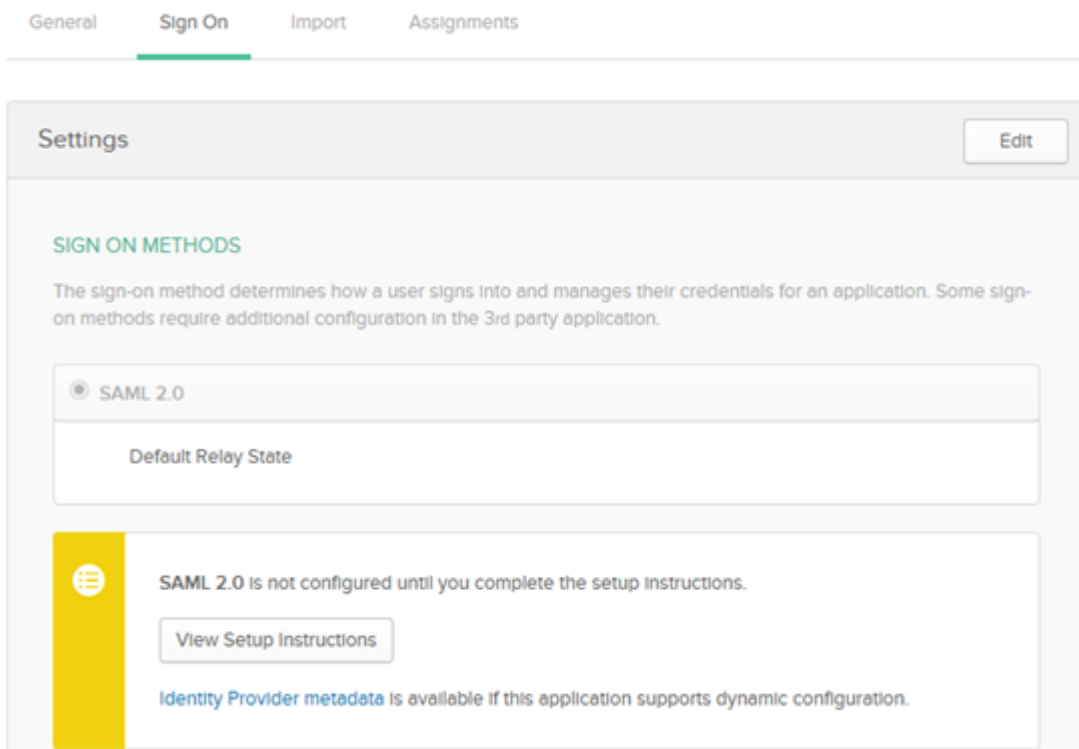
- b. Under **Configure SAML > SAML Settings**, in the **Single sign on URL** box and the **Audience URI (SP Entity ID)** box, paste the URL that you copied from the Command Center.

A SAML Settings



The screenshot shows the 'GENERAL' tab of the SAML Settings configuration page. It contains two text input fields, both containing the URL 'https://mycompany:443/webconsole'. The first field is labeled 'Single sign on URL' and has a help icon. Below it is a checked checkbox labeled 'Use this for Recipient URL and Destination URL' and an unchecked checkbox labeled 'Allow this app to request other SSO URLs'. The second field is labeled 'Audience URI (SP Entity ID)' and also has a help icon.

- c. From the **Name ID format** list, select **Email Address**.
- d. Continue to follow the wizard and accept the default values.
- e. Click **Finish**.
- f. Open the application, and then click **Sign On**.



The screenshot shows the 'Sign On' tab of the SAML Settings configuration page. At the top, there are navigation tabs: 'General', 'Sign On' (which is active), 'Import', and 'Assignments'. Below the tabs is a 'Settings' section with an 'Edit' button. Underneath is the 'SIGN ON METHODS' section, which includes a description: 'The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.' There is a radio button selected for 'SAML 2.0'. Below this is a 'Default Relay State' field. A yellow banner with a globe icon contains the message: 'SAML 2.0 is not configured until you complete the setup instructions.' with a 'View Setup Instructions' button. At the bottom, it says 'Identity Provider metadata is available if this application supports dynamic configuration.'

- g. To download the IdP metadata file, under the **View Setup Instructions** button, click **Identity Provider metadata**.
 - h. Save the IdP metadata file as an XML file.
 3. In the Command Center, complete the SAML application:
 - a. To upload the IdP metadata XML file, in the open **Add SAML App** dialog box, beside **Upload IDP metadata**, click **Browse**.
 - b. Select the IdP metadata XML file that you downloaded from Okta.
 - c. Complete the application, and then click **Save**.

For information about adding a SAML application in the Command Center, see *Adding Identity Servers* (on page 5).

4. Open the **Identity Servers** page in the Command Center, and copy the **Single sign-on url**.
5. In your Okta account, under **Configure SAML > SAML Settings**, in the **Single sign on URL** box, paste the URL that you copied from the Command Center.
6. **Optional:** To configure single logout in Okta, complete the following steps:
 - a. From the generated SP metadata XML, copy the following information:
 - SP EntityId
 - SingleLogoutService location with POST binding
 - b. To download the signature certificate, log on to the Command Center, and then in your web browser, type the SAML App URL in the following format, and then press **Enter**.

https://webconsole_hostname/adminconsole/downloadSPCertificate.do?appName=URL encoded SAML app name

Example: `https://company.com/adminconsole/downloadSPCertificate.do?appName=app%20Name`

- c. In your Okta account, under **General > Advanced Settings**, select the **Enable Single Logout** box.
 - d. In the **Single Logout URL** box, type the SingleLogoutService location that you copied from the SP metadata file.
 - e. In the **SP Issuer** box, type the entityID that you copied from the SP metadata file.
 - f. In the **Signature Certificate** box, upload the certificate that you downloaded from the SAML app URL.
 7. To assign other Okta users access to your Okta account, complete the following steps:
 - a. In your Okta account, under **Assignments**, click **Assign**, and then select one of the following options:
 - To assign individual Okta users, click **Assign to People**.

- To assign a user group, click **Assign to Groups**.
 - b. Select the user or group that you want to assign, and then click **Add**.
8. Optional: To assign domain users based on Okta's user groups SAML attribute, complete the following steps:
- a. In your Okta account, under **Group Attribute Statements**, click **Add**.
 - b. In the **Name** box, type **user_groups**.
 - c. In the **Filter** box, assign filters as required. For example, to assign users from a user group name that starts with "domain users", select **Starts With**, and then type **domain users**.
 - d. Preview the SAML assertion and verify that your Idp response XML includes the user group attribute. For example:

```
<saml2:Attribute Name="user_groups"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml2:AttributeValue
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="xs:string">GroupName Match Starts with "domain users" (ignores
case)
  </saml2:AttributeValue>
</saml2:Attribute>
```
 - e. In the Command Center, map Okta's **user_group** SAML attribute with the **user group** user attribute. For more information on mapping attributes, see Mapping SAML Attributes (on page 12).

Creating and Inviting Local Users

Create local users and automatically send the users email invitations. The email invitation contains a link for to the Endpoint package and user credentials.

Note: If you set up Active Directory authentication or SAML authentication, you do not need to create local users.

Procedure

1. From the navigation pane, go to **Security > Users**.
2. The **Users** page appears.
3. In the upper right of the page, click **Add user**.
4. In the **Add user** dialog box, provide the user information.
5. To assign this user to a user group, from the **User group** list, select the user group.

6. Decide how to create the password for the user:
 - To auto-generate a password for local users, select the **Use system generated password** check box.
 - To manually set a password for the user, in the **Password** box, type a password.
7. To send an email invitation to the user to install the Endpoint package, select the **Invite User** check box.

The **Invite User** option applies if this user's laptop or desktop must be backed up by the Laptop solution, and you want the user to interactively install the Endpoint package. If an administrator will install the Endpoint package, do not select the **Invite User** option.

8. Click **Save**.

Index

A

AD FS • 14

Adding an Active Directory Domain Controller • 4

Adding Identity Servers • 5, 8, 9, 15, 19, 20, 22

Automatically Creating Users from a SAML Response •
6, 10

Available Attributes • 12

Azure • 18

C

Creating and Inviting Local Users • 23

Creating Certificates for SAML Integration • 5, 7

D

Domain Controller Settings for Active Directory • 4, 5

E

Examples • 13

I

Identity Provider Use Cases • 14

Install software and authenticate users • 3

M

Mapping SAML Attributes • 11, 12, 23

O

Okta • 20

P

Procedure • 13

S

Sample SAML IdP Metadata XML • 5, 6

Sample SAML SP Metadata XML • 5, 7

T

Tenant Administrator • 3

©1999-2019 Metallic, Inc. All rights reserved.



Metallic | metallic.io | 888.555.5555

©2019 Metallic, Inc.