Integrate Versa Director with Azure SSO

For supported software information, click here.

When a network administrator accesses Versa Director, they can be authenticated using a number of different authentication techniques. This article discusses how to integrate a Versa Director that uses SAML authentication with Azure SSO.

This article discusses the two use cases that are supported for integrating Versa Director with SAML authentication:

- The provider or the provider and all the provider's tenant organizations are authenticated using a single identity provider (IdP). The IdP is typically the provider's IdP, and all network administrators regardless of the organization to which they belong are authenticated using the provider's IdP.
- SAML authentication is associated with the provider's organization or with any of the tenant's organizations. Here, authentication methods are applied on a per-organization basis. This means, for example, that network administrators of Tenant A may be authenticated using the tenant's IdP, and the provider or other tenant organization may use some other method or other IdP for authentication.

For the discussion in this article, the IdP is Azure. However, other IdPs exist, such as Okta).

This article discusses to service provider (SP)–initiated SSO. It does not discuss IdP-initiated SSO.

One advantage of using a centrally hosted authentication platform, such as SAML, is that the customer or organization can manage user access to systems and platforms from a single pane of glass, that is, the Azure portal. Such a management scheme avoids having to manually add or delete user accounts on the customer's or organization's third-party systems and platforms as part of the regular user lifecycle management process.

Network Administrator's Perspective of Accessing Versa Director

When a network administrator opens their web browser and accesses Versa Director, the following sequence of events occurs to validate the network administrator:

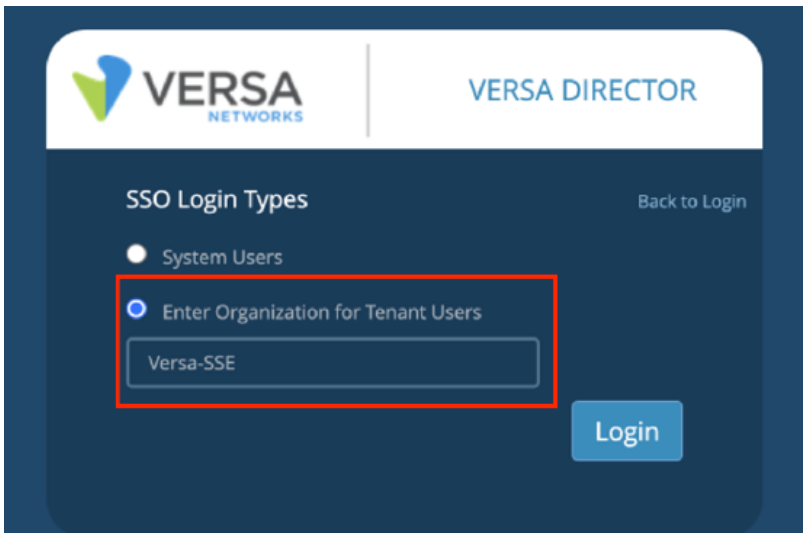
1. The Versa Director, acting as a service provider, creates an authentication request and automatically redirects the network administrator to the IdP.
2. The IdP requests the network administrator's credentials.
3. The IdP validates the credentials.
4. The IdP redirects the network administrator to Versa Director with the login response.
5. The Versa Director validates the login response.

6. If the validation successful, the network administrator is allowed to log in to the Versa Director.

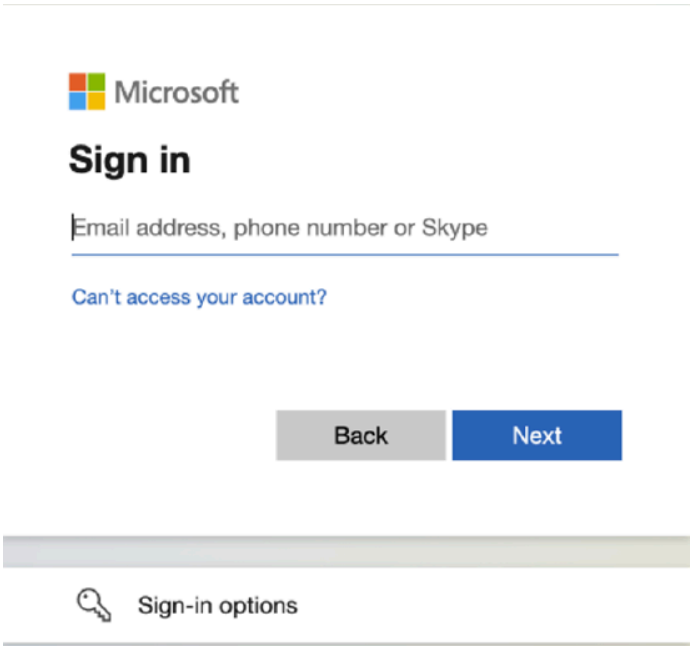
The following steps detail what the network administrator experiences:

1. The network administrator opens a browser on their PC and attempts to access their Versa Director instance.
2. The network administrator selects the Login with Single Sign-On hyperlink:

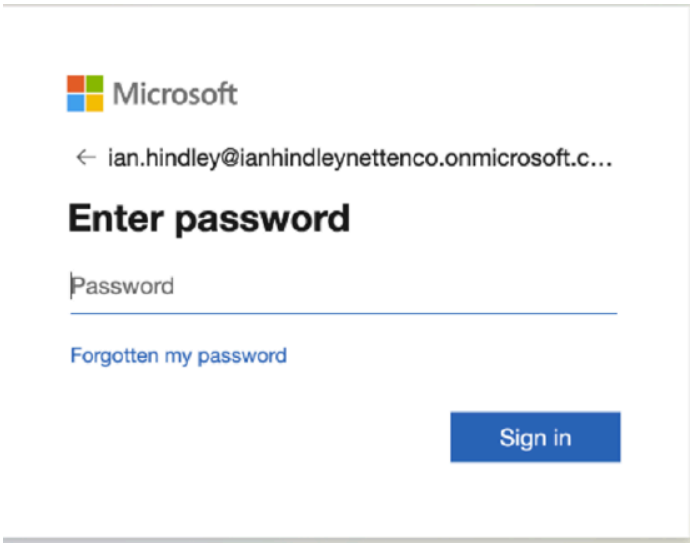
3. The network administrator selects the SSO login type. For provider-level access, they select System Users. For tenant-level access, as shown in the following screenshot, they select Enter Organization for Tenant Users and then enter the tenant organization name. Note that the tenant organization name is case-sensitive, and it must match the name configured on the Director node.



4. The Director node then redirect the network administrator to the IdP, which, here, is Azure. The network administrator then enters their username.

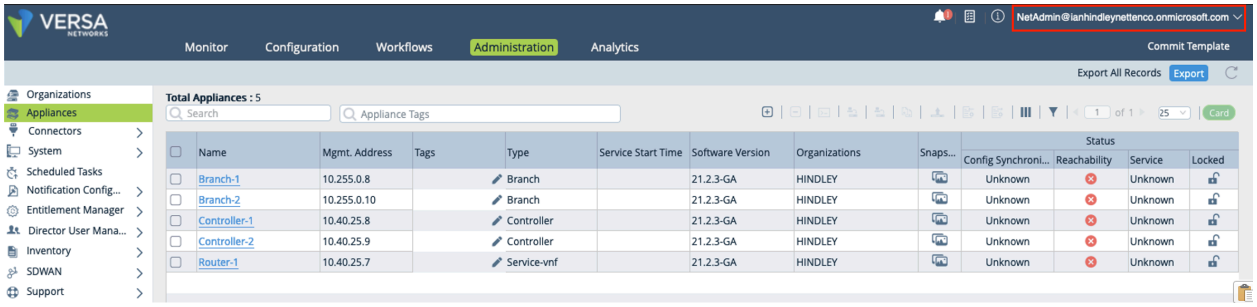


5. The network administrator is prompted to enter their password.

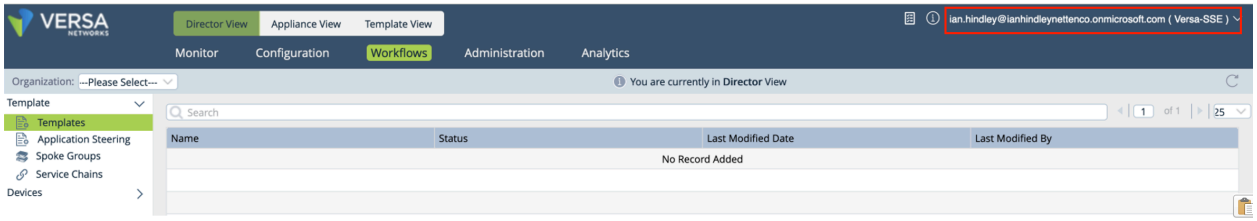


6. After the network administrator enters the correct credentials, they are automatically logged in to the Director node.

   The following screenshot shows that the user is a provider user, because they selected the System Users option in Step 3. Note the username in the top right does not have an organization name in parenthesis, because it is a provider user.



The following screenshot shows that the user is a tenant user. Note the username in the top right has the tenant organization name in parenthesis, which, here, is Versa-SSE.



In both cases, the username is hosted and authenticated by Azure. Usernames are not stored and not configured on the Director node.

SAML Design Use Cases

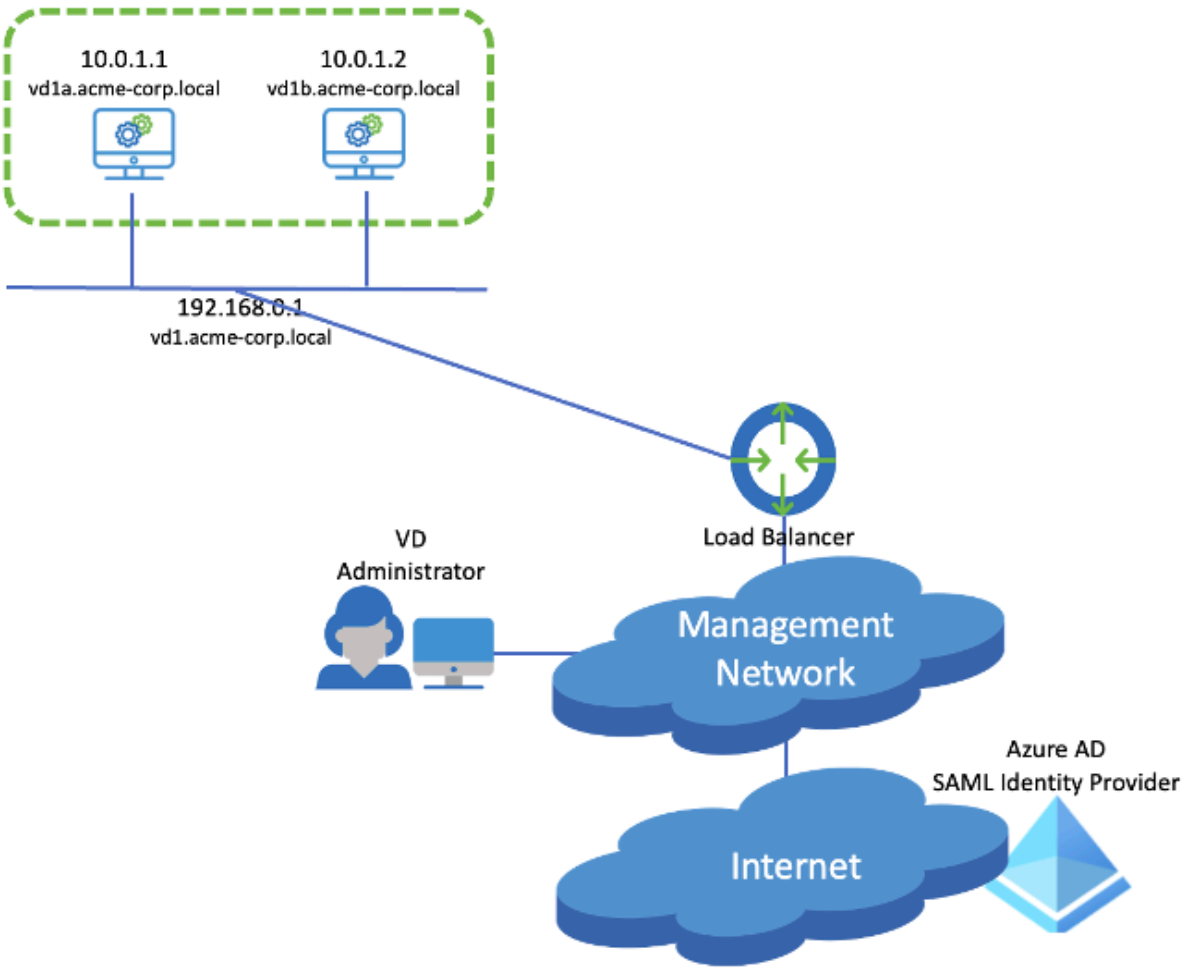
This section describes two typical uses cases that demonstrate how to integrate Versa Director with Azure SSO:

- Integrate Azure SSO with a high availability (HA) pair of Director nodes.
- Integrate Azure SSO with multiple HA pairs of Director nodes.

This section provides high-level configuration guidelines only. The detailed configuration steps are described later in this article.

Integrate Azure SSO with One HA Pair of Director Nodes

We illustrate the use case in which you integrate Azure SSO with a single HA pair of Director nodes with the HA pair of Director nodes named vd1a.acme-corp.local and vd1b.acme-corp.local, as shown in the following figure. Director administrators access the active Director node by connecting to a virtual IP address (vd1.acme-corp.local) that is hosted on a load balancer. The load balancer polls the Director servers to determine which one is the active node and which is the backup. To access the Director nodes, the administrators are authenticated through SAML using Azure Active Directory (AD).

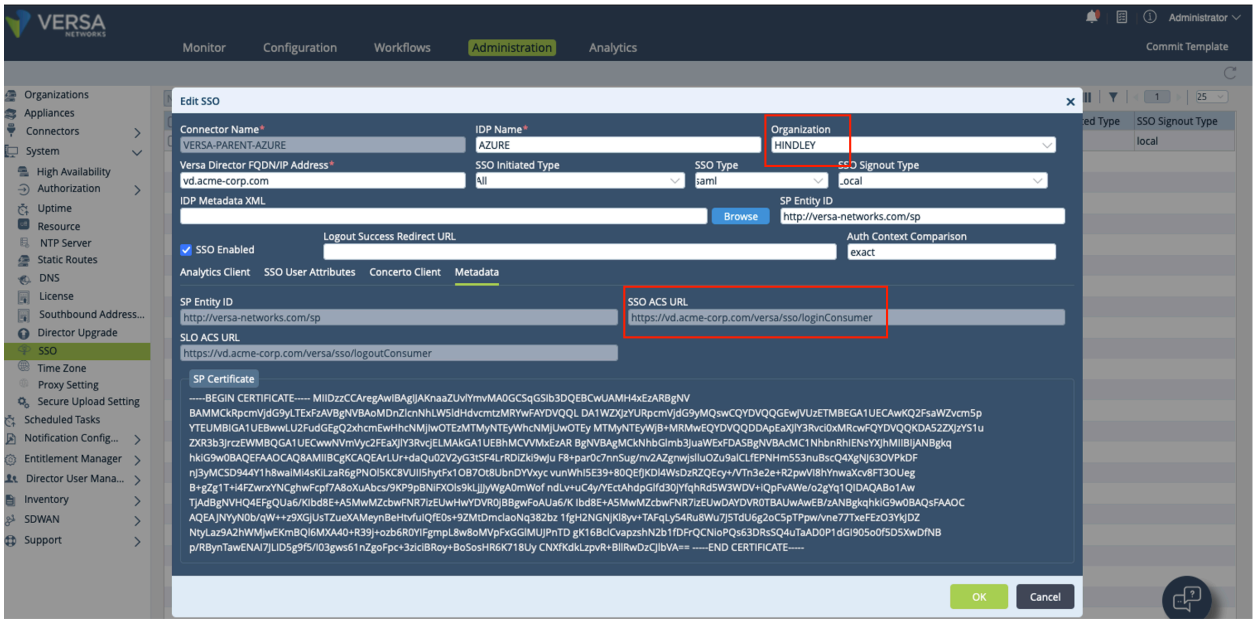


For this use case, we make the following assumptions:

- A load balancer is used in front of the Director servers, and the load balancer has the virtual IP address of the Director node.
- All Director administrators connect to the primary Director node using the virtual IP address hosted on the load balancer.
- The load balancer is monitoring the health of the Director node. If the primary Director node fails, the load balancer forwards new sessions to the backup Director node.

For the configuration to integrate Azure SSO with a single HA pair of Director nodes, at a high level, you configure a connector on the Director node. The detailed steps are described later in this article.

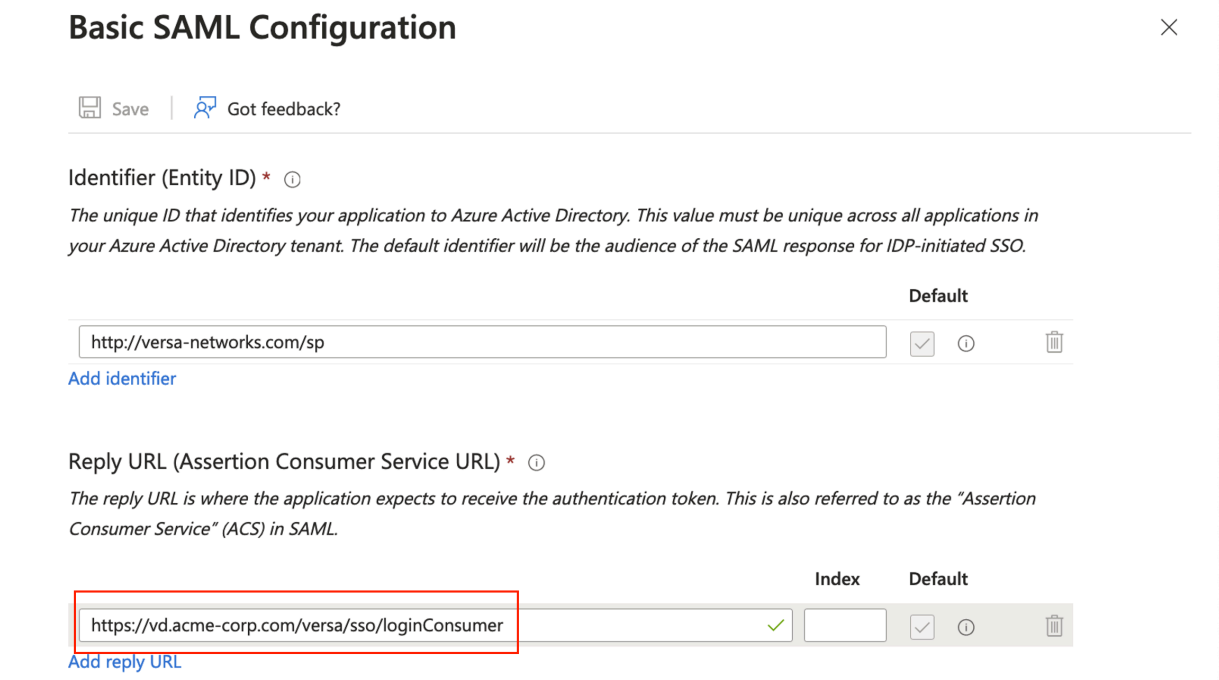
The following screenshot shows how to configure the connector on the Director node.



The FQDN or IP address of the Director node relates to the virtual address hosted on the load balancer. In this example, the FQDN is vd.acme-corp.com, which resolves to the IP address 192.168.0.1 that is hosted on the load balancer.

You enter the name of the organization that you want to send to SAML for authentication. In this example, the provider organization is HINDLEY.

The following screenshot shows the corresponding configuration on Azure.



Note that the value in the SSO ACS URL field on the Director node and value in the Reply URL field on Azure match. The SSO ACS URL is automatically generated from a concatenation of the Director FQDN or IP address with /versa/sso/loginConsumer, and it is the URL that is passed to the client after it is successfully authenticated by Azure.

Although not highlighted in the screenshots, note the value in the SP Entity ID field on the Director node and the value in the Identifier (Entity ID) field on Azure match. These values must match so that Azure can associate the SP request from the Director node with the correct application hosted in Azure.

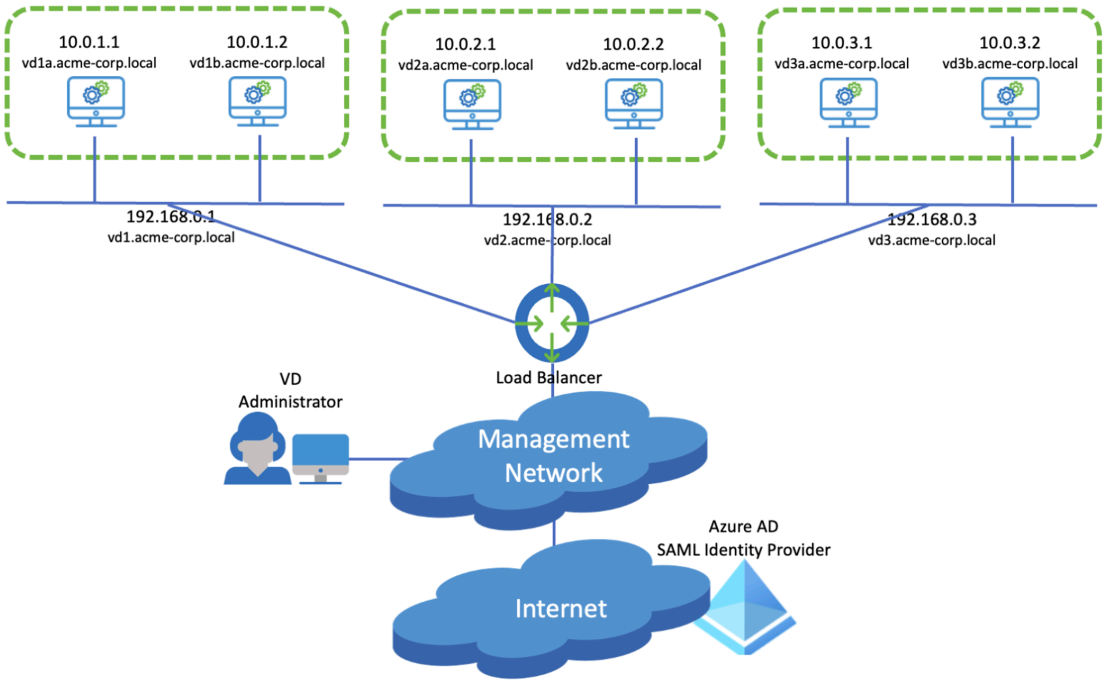
By design, the Sign on URL, Relay State, and Logout URL fields on the Director node are left blank. (For brevity, these fields are not shown in the screenshot.)

On the Director node, you can globally configure only a single default IdP connector or a single IdP connector. Therefore, although you could create two connectors, one for each Director instance in the HA pair, you can associate only one of them with the Default or Single field. Although this may work for a while, if the primary Director node fails, SAML users are then unable to connect to the Director node. More specifically, authentication would succeed, but the SSO ACS URL response from Azure would redirect the user to the default or single Director IP address. Because this would be the Director node that has failed, users would never be presented with the Director node hosted on the backup server. This scenario is also the reason to use a load balancer in front of Director node. The Reply URL should be the FQDN or IP address of the virtual IP address of the load balancer.

Integrate Azure SSO with Multiple HA Pairs of Director Nodes

The second use case is to integrate Azure SSO with multiple HA pairs of Versa Directors. To support SAML authentication using Azure for multiple HA pairs of Director node, the Azure administrator can either create an application for each Director HA pair or they can create a single application for all the Director HA pairs.

We illustrate this type of integration using three HA pairs of Director nodes, as shown in the following figure. Director administrators connect to the active Director node by connecting to a virtual IP address (vd1.acme-corp.local, vd2.acme-corp.local, or vd3.acme-corp.local) that is hosted on the load balancer. The load balancer polls the Director servers to determine which is active for each HA pair. When accessing the Director node for each HA pair, Director administrators are authenticated through SAML using Azure AD.



For this use case, we make the following assumptions:

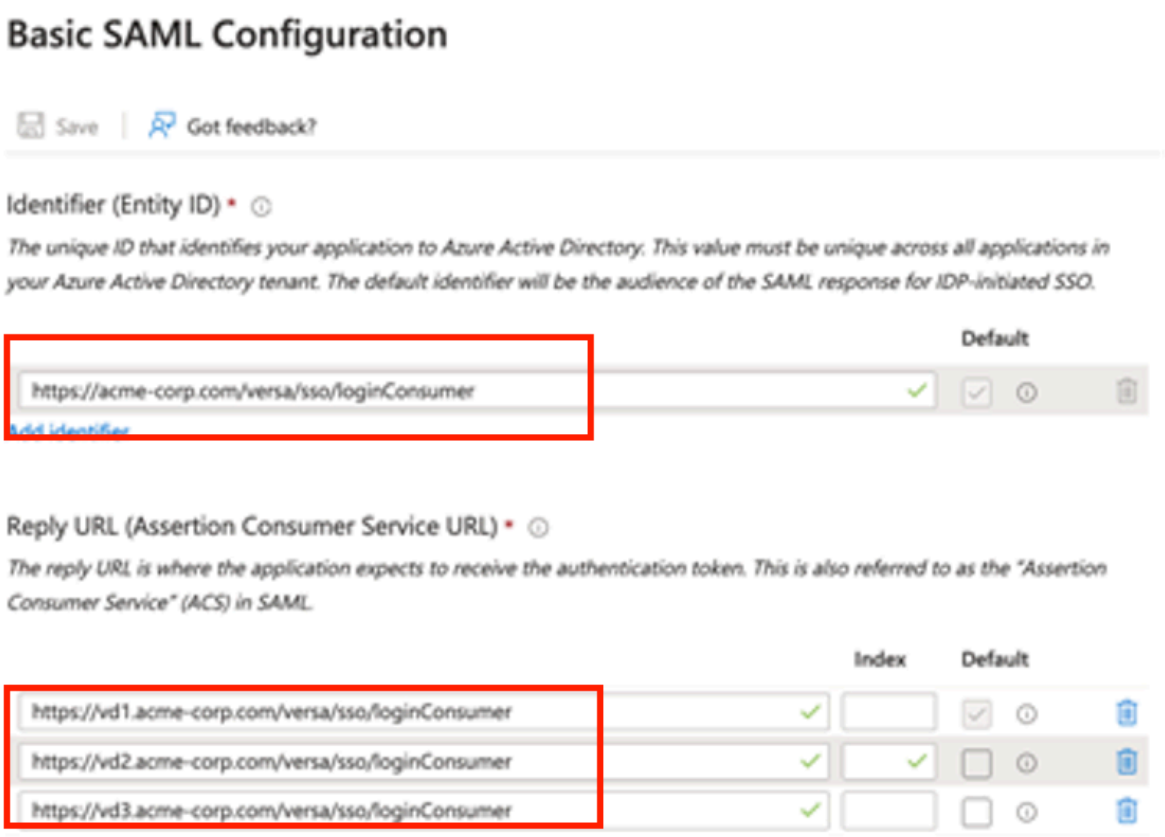
- A load balancer is used in front of each HA pair of Director servers, and the load balancer has the virtual IP address of the Director node.
- All users connect to the corresponding primary Director node using the virtual IP address hosted on the load balancer.
- The load balancer is monitoring the health of each Director node. If the primary Director node fails, the load balancer forwards new sessions to the backup Director node for that HA pair.

For the configuration to integrate Azure SSO with multiple HA pairs of Director nodes, at a high level, you can configure one application for each Director HA pair or you can configure a single application for all pairs. The detailed steps are described later in this article.

To configure an application for each Director HA pair, you create connectors, as described for integrating a single HA pairs, above, creating a connector for each HA pair. For each connector, an Azure application is created for each HA pair of Director nodes. In this example, there are three HA pairs so there are three Azure applications.

If you configure a single application for all the Director HA pairs, a single application in Azure is created. All the Director instances use the same Entity ID, as shown in the following screenshot. The screenshot below also shows the three Director HA pairs the organization acme-corp.com. The three HA pairs share a single application on Azure. The Director FQDNs are vd1.acme-corp.com, vd2.acme-corp.com, and vd3.acme-corp.com. (Note that you can use the load balancer virtual IP address for each Director HA pair instead of using the FQDNs if you prefer). For the entity ID, you can use any URL that is unique to that Azure instance. The screenshot below uses https://acme-corp.com/versa/sso/loginConsumer. Unlike the Identifier (Entity ID), the Reply URL (ACS URL) must be unique for each Director HA pair of VD. The Sign on URL, Relay State, and Logout URL fields are left blank. (For brevity, these fields are not shown in the

screenshot.)



General Configuration Notes

The remaining sections in this article describe how to configure, verify, and troubleshoot SP-initiated SSO. They do not describe the configuration for IdP-initiated SSO. The screenshots shown are for VOS Release 21.3.

The following are general notes that apply to the configuration process itself and to the specific example in this article:

- When Director nodes have multiple interfaces, SAML authentication requests are forwarded over the interface with the most preferred route to the IdP provider. In most cases, this is the default route over the Director northbound interface.
- Network Time Protocol (NTP) must be running on the Director nodes, and the Director node time must be synchronized using NTP. Using NTP ensures that both the Director nodes and the IdP (that is, Azure) are synchronized to within a few milliseconds of Coordinated Universal Time (UTC). If the clocks differ between the two platforms, authentication fails. For more information, see Troubleshoot Versa Director, below.
- At the time of writing, a Director node accepts only email ID format-based responses from the IdP. This means that if the response is in a user principal name (UPN) format (for example, 12345@test) instead of an email format (for example, 12345@test.com), authentication fails. For more information, see Troubleshoot Versa Director, below.
- To avoid any doubt, SAML-hosted network administrator usernames are not configured on the Director nodes. All usernames are stored in Azure.

- The Azure administrator for the provider or tenant is responsible for ensuring that the correct user role is associated with each network administrator. You configure the roles in Azure under the user profile attribute called user.jobtitle.
- If the Azure administrator is already populating the user.jobtitle attribute with data that does not align with the user roles on the Director node, you can configure SSO role mappings on the Director node. These role mappings take the value configured as the user's job title in Azure and map it to a user role on the Director node. For more information, see Create SSO Role Mappings, below.
- There are no equivalent mappings for the Azure user.department attribute and the Director node organization or provider. Therefore, in the user profile hosted on Azure, you must append the user.department to the organization name on the Director node or, for provider-level access, to the provider name.
- The process of integrating a Director node with Azure SSO described in this article also allows a network administrator to access Versa Analytics through the Director node with no additional configuration. However, if customers require that network administrators be authenticated through Azure SSO when accessing Versa Analytics directly from the network administrator's browser, additional steps are required. For more information, see Integrate Versa Analytics with Azure SSO, below.
- According to webpage https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/tutorial-manage-certificates-for-federated-single-sign-on, when you add a new application and configure a SAML-based sign-on, Azure AD generates a self-signed certificate for the application that is valid for three years. According to the same webpage, the Azure administrator can customize the validity period, for example, to extend or shorten the default time period. Note that Azure AD sends email notifications 60, 30, and 7 days before a SAML certificate expires. If a new certificate is required, the Azure administrator must create and download it from the Azure portal. Then, the network administrator uploads the certificate to the Director node for the organization. You upload the certificate to the IdP Metadata XML section, as described in the configuration steps below.
- Director nodes have two configurable user types: provider and tenant. The provider user is the parent organization, and the tenant user is a child organization with a parent organization. For each user type of user, you can associate a role with the user, which determines the access level for individual users. By combining the user type and the role, you can associate the following preconfigured profiles with users:
  - Provider users
    - ProviderDataCenterAdmin—Super-admin role with no access to the certain system-level resources.
    - ProviderDataCenterOperator—Read-only access to all resources.
    - ProviderDataCenterSystemAdmin—Super-admin role with access to the entire Director system for all tenants.
  - Tenant users
    - TenantDashboardOperator—Read-only access to resources.
    - TenantOperator—Read-only access for the tenant to which the user belongs.
    - TenantSecurityAdmin—Can perform all security operations for the tenant to which the user belongs and can perform operations for features such as firewall, zones, and ZTP.
    - TenantSuperAdmin—Super-admin role that can perform all operations for the tenant.

  For more information, including the resources that are accessible for each preconfigured role, see Configure AAA.

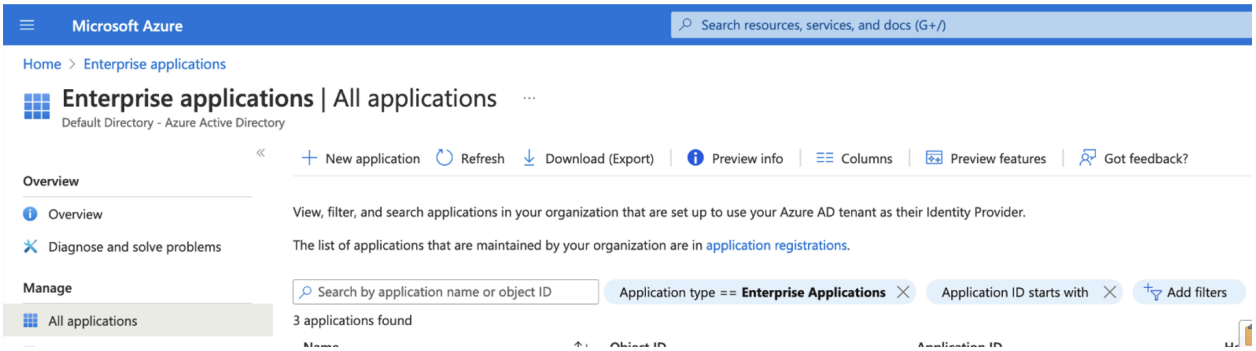
Configure an Azure SAML IdP

To configure an Azure SAML IdP, you create a new application, and then you associate users with the application.

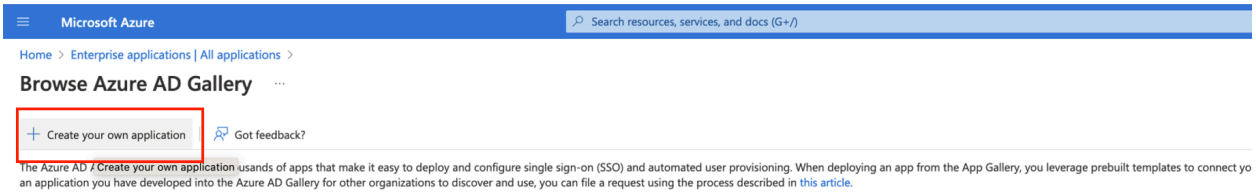
Create a New Application

To configure SAML authentication, you configure a new application on Azure:

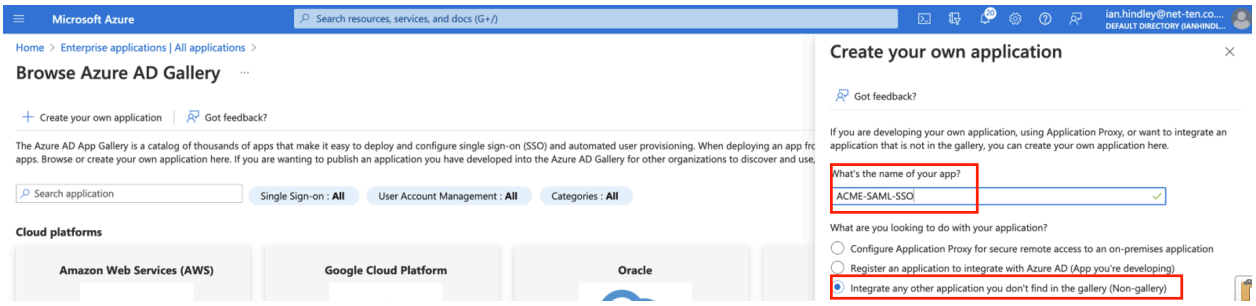
1. Log in to the Azure portal.
2. Select Enterprise Applications.
3. Select + New Application.



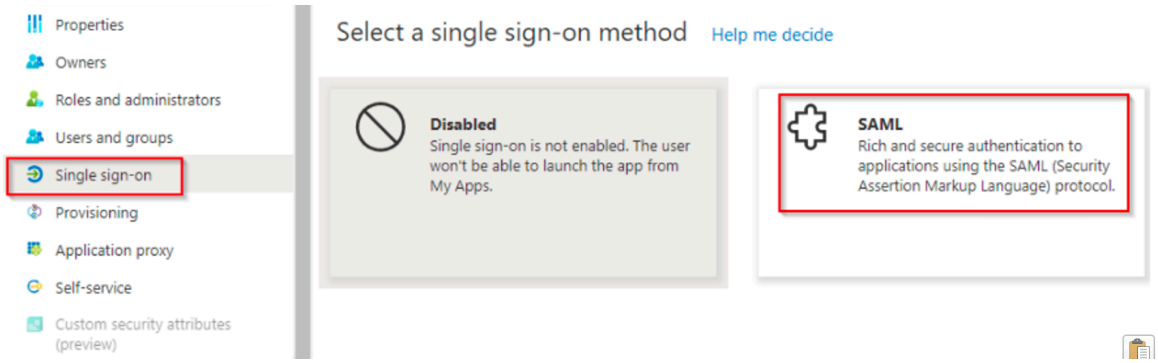
4. Select Create Your Own Application.



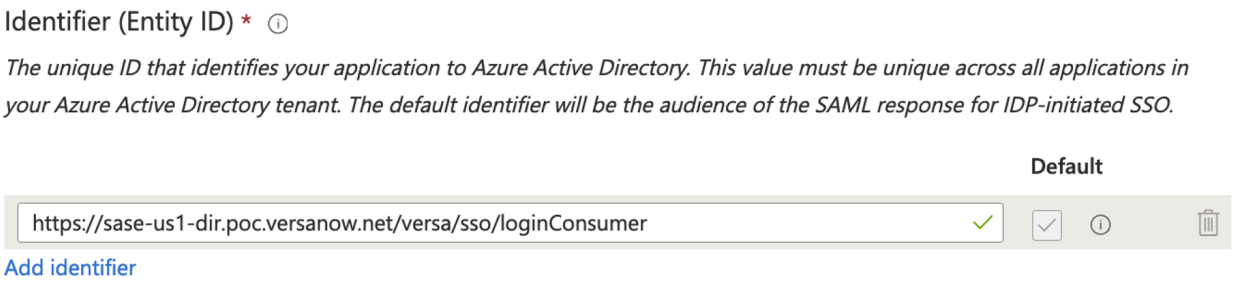
5. Create a name, and then select Integrate Any Other.



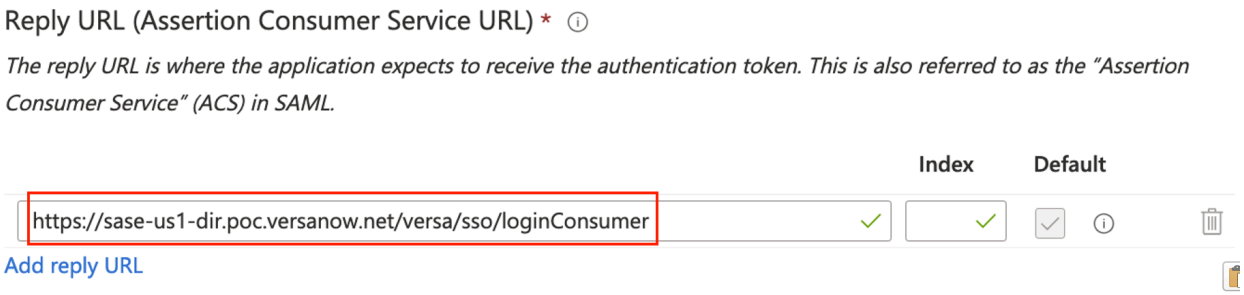
6. Select Single Sign-On, and then select SAML.



7. Enter the identifier, or entity ID. In this example, we use the URL of the Director instance concatenated with the string /versa/sso/loginConsumer, so the identifier is https://sase-us1-dir.poc.versanow.net/versa/sso/loginConsumer. This combination creates a unique identifier and therefore a unique Azure application for each Director HA pair instance. (Although not shown below, another option is to create a single entity ID that all Director HA pair instances share. In this case, you create a single Azure application.)

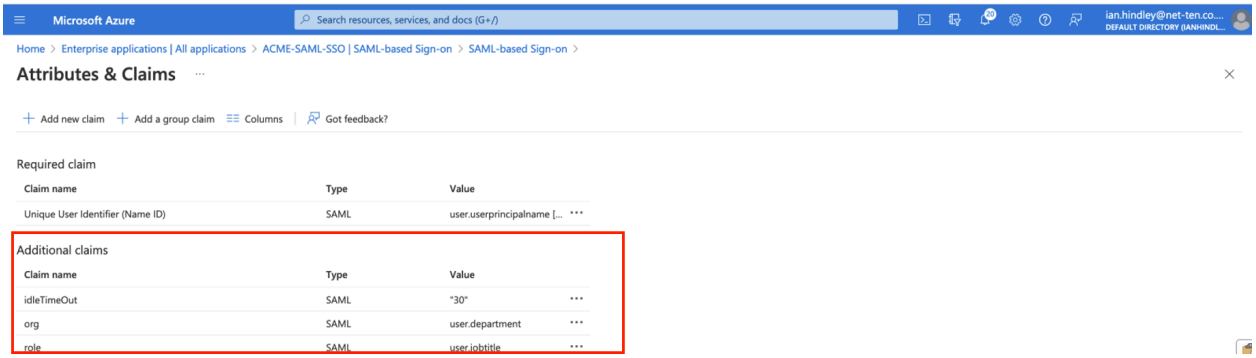


8. Enter the Reply URL (Assertion Consumer Service URL).In this example, we use the same URL as the entity ID used above, https://sase-us1-dir.poc.versanow.net/versa/sso/loginConsumer. Also, in this example, we use the FQDN of the HA pair. Alternately, you can ue the virtual IP address of the Director HA pair. (Although not shown in the screenshot below, if multiple Director HA pair instances share the same Azure application, one Reply URL row for each VD HA pair is created.)

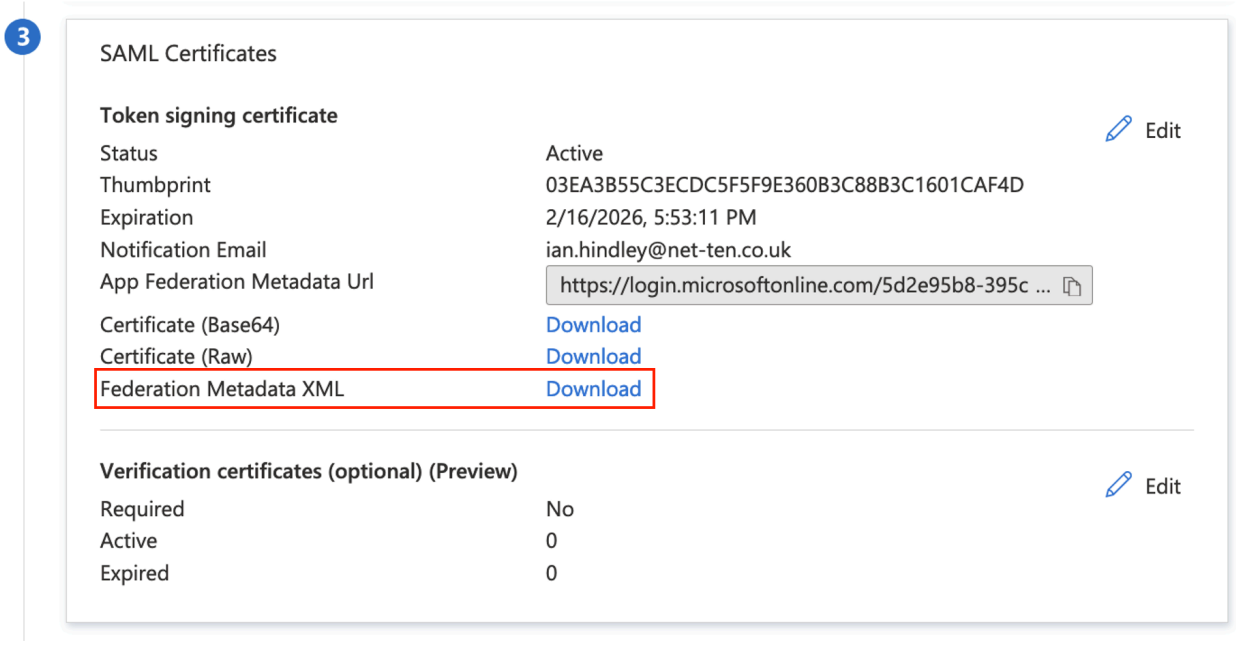


9. Click to edit the Attributes and Claims. You must configure three attributes, which are passed to the Director nodes:
   • idleTimeOut—Time, in minutes, after which the user is automatically timed out of the Director node following a period of idleness. In this example, we set the time to 30 minutes.
   • org—Value of the Azure predefined user.department attribute.
   • role—Value of the Azure predefined user.jobtitle attribute.
   In this example, the Unique User Identifiers value is already mandated by Azure in the application. Therefore, we do not need to manually configure it. In this example, the unique user identifier is also the email address of the

user, and the network administrator uses it as the login name. If this claim is missing from your Azure instance, add it (or use the user email address if that is what you are using). If you are using the user principal name, ensure that it is in an email format.
Configure claims as shown in the screenshot below, and then click Add New Claim.



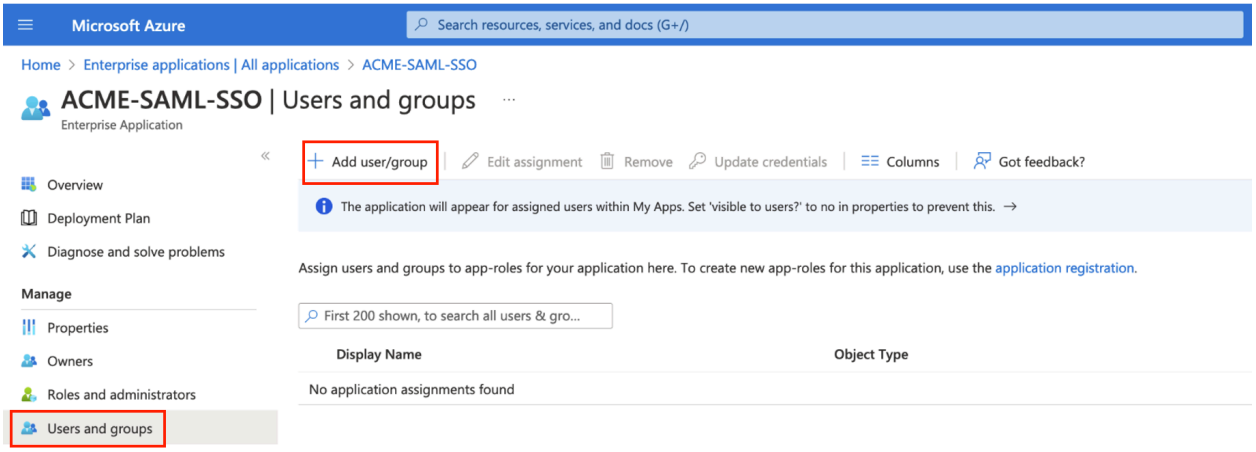
10. Download the federation metadata XML. You upload this XML to the Director node later in the process.



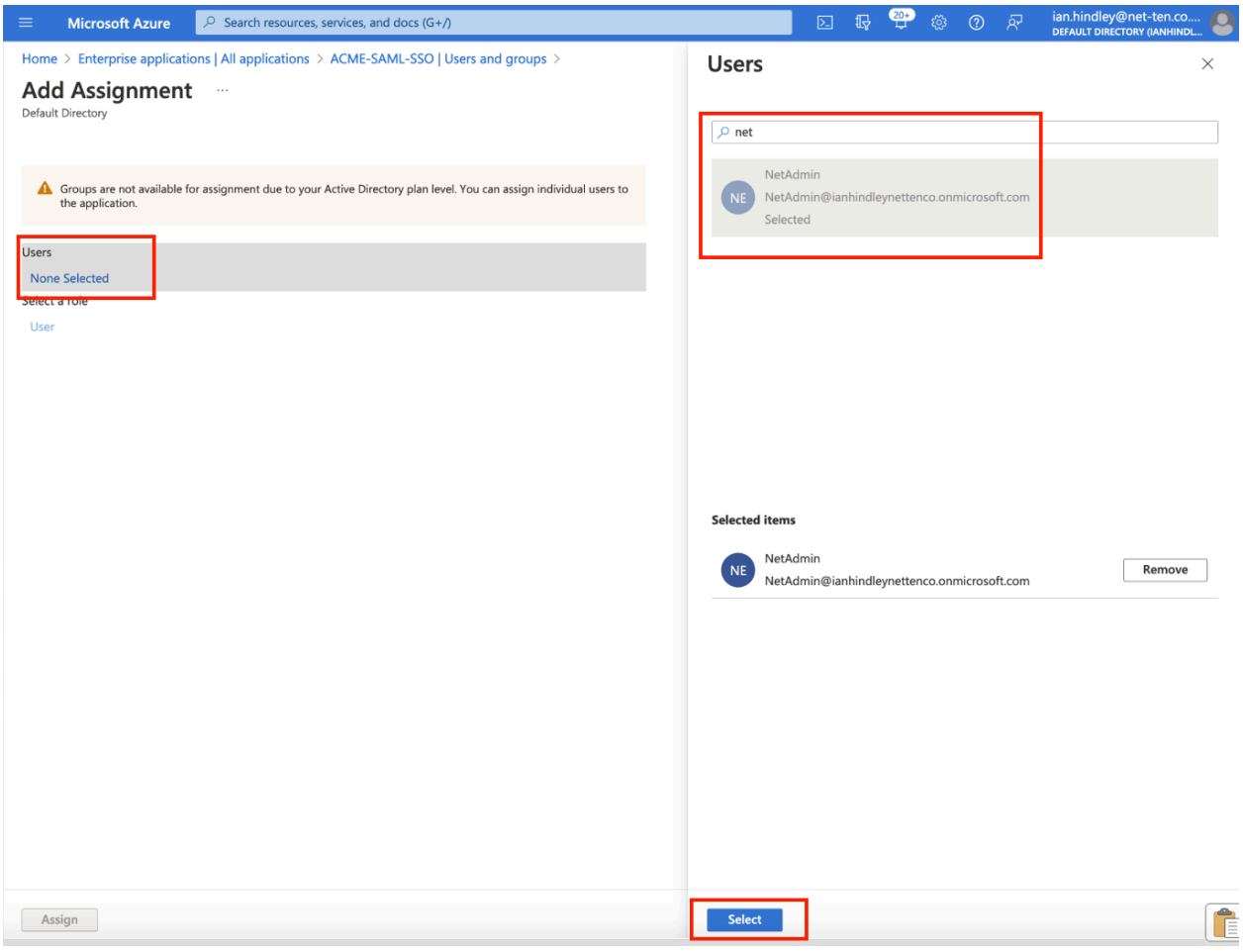
Associate Users with the New Application

After you create a new application, associate users with the application:

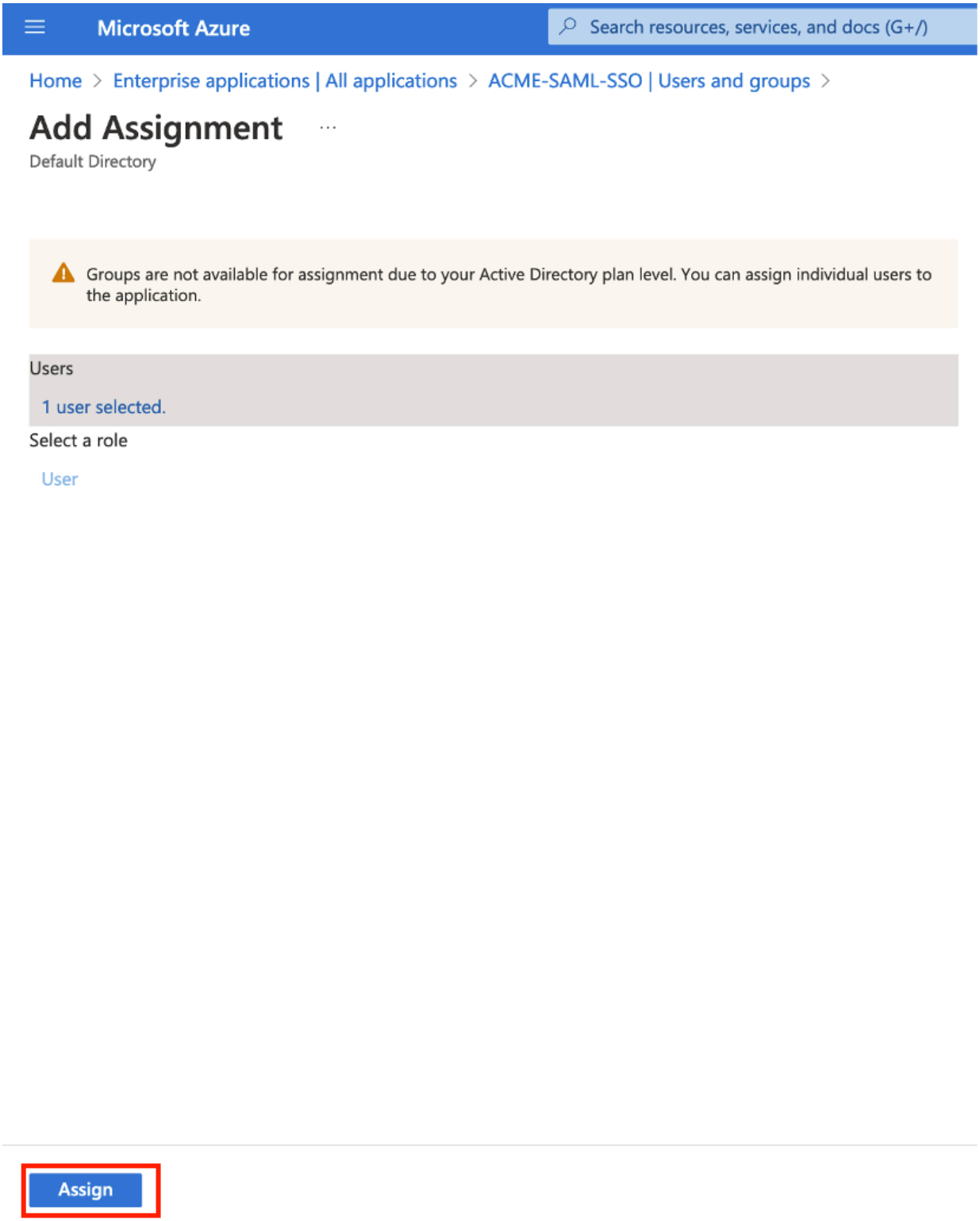
1. Select User and Groups, and then click +Add User/Group.



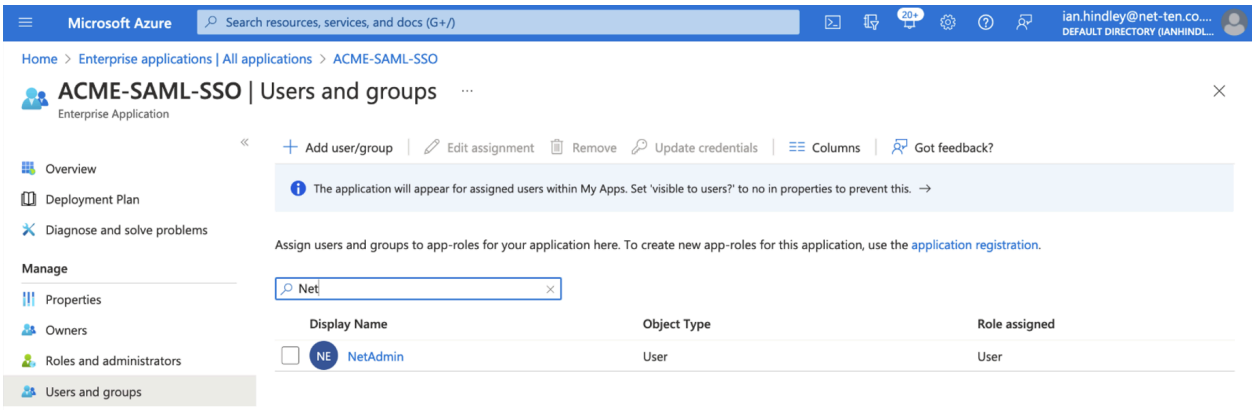
2. Select the users.



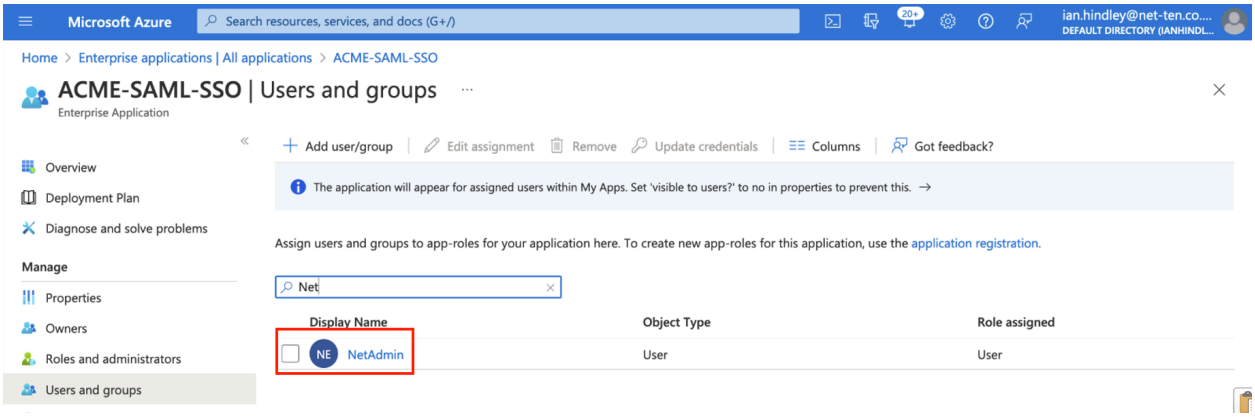
3. Select Assign.



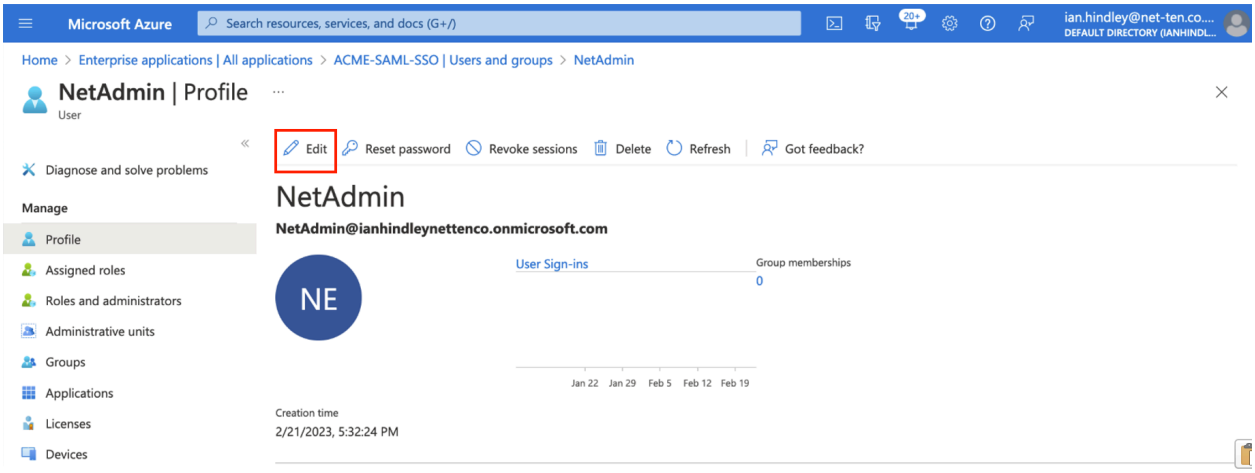
4. The user is then added to the application, allowing them to log in to the Director node through the application.



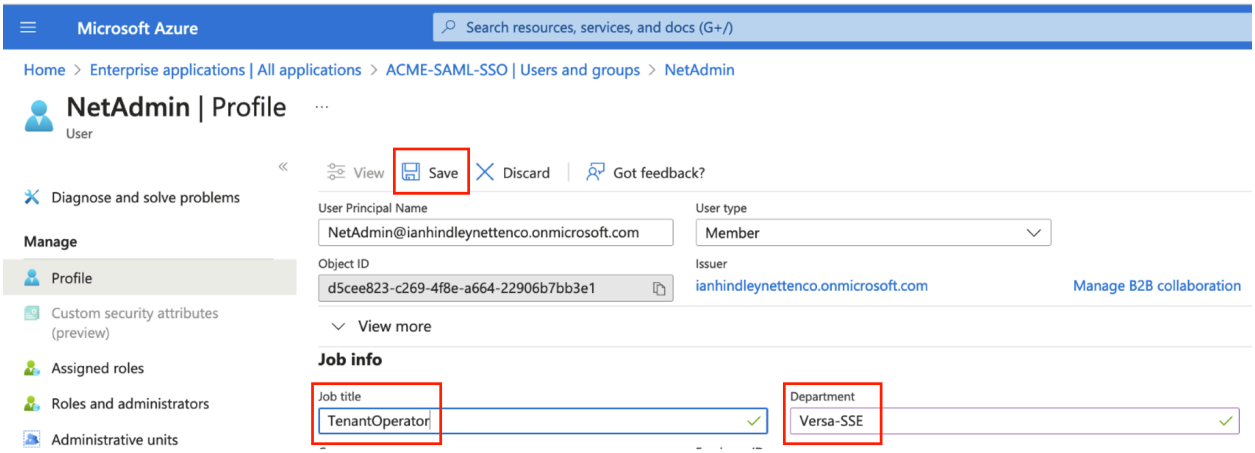
5. Repeat Steps 2 through 4 to add other network administrators to the application.
6. Populate the claims associated with the application. These are the claims you configured when creating the application. In the example here, we created two claims, user.jobtitle and user.department, and this data needs to be populated in Azure so that Azure can inform the Director node which organization to associate the user with and which permissions to provide to the user.
   a. Click the user that you assigned to the application.



   b. Click Edit.



c. Enter information for job title and department.



- Set the job title—This is equivalent to a role on the Director node. In the screenshot, we use the predefined Director group called TenantOperator, which is a read-only account. For a list of preconfigured roles, see General Configuration Notes, above. Note that if a job title already exists and cannot be modified, see Create SSO Role Mappings, below, which explains how to create a mapping on the Director node that you can use to map the Azure job title to a Director role.
- Set the department—This is equivalent to the name of the organization on the Director node that the user wants to log in to. In the screenshot, we use the tenant organization called Versa-SSE. Note that this field is case sensitive.

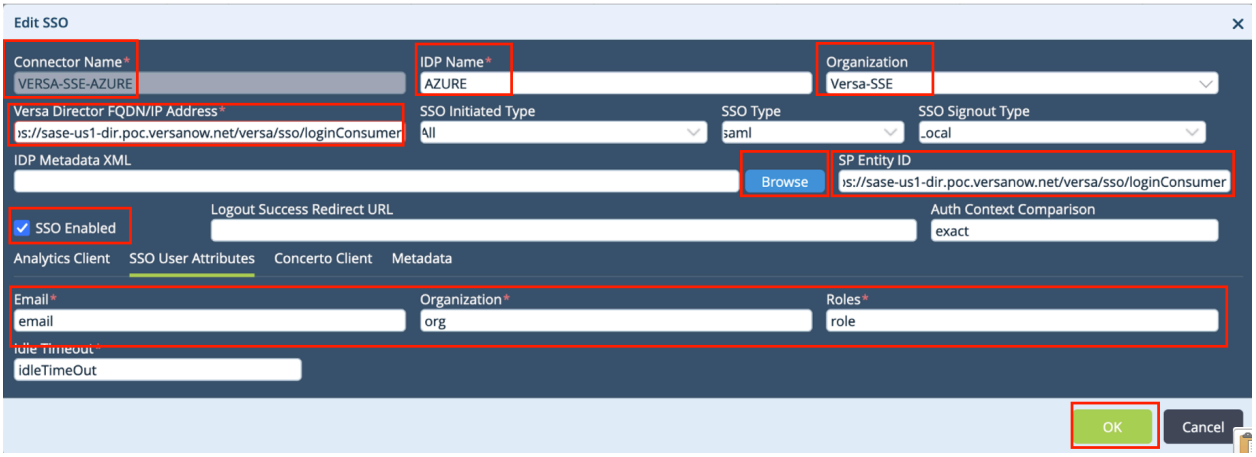
d. Click Save.

Configure Versa Director

On the Director node, you configure a Connector to use for SSO. If necessary, you also create SSO role mappings.

Create the SSO Connector

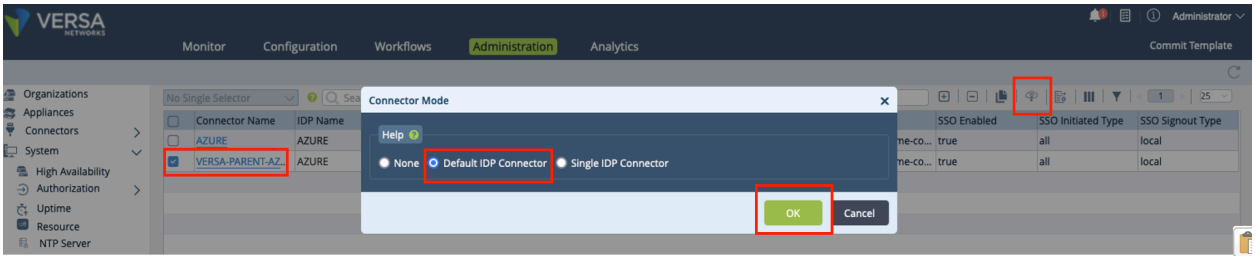
1. Select Administration > System > SSO, and then click the + Add icon.
2. In the Edit SSO popup window, enter information for the following fields.



Field	Description
Connector Name	Enter a name for the SSO connector. In this example, we use VERSA-SSE-AZURE. This name is derived using the following naming scheme: *organization-name*-AZURE. This is one example of a naming scheme.
IdP Name	Enter the name of the IdP. Here, the name is AZURE.
Organization	Select the name of the organization.
SSO Enabled	Click to enable SSO for the organization.
Versa Director FQDN/IP Address	In this example, we use the FQDN of the Director HA pair. You can also use the virtual IP address VIP of the Director HA pair instead.
IdP Metadata XML	Click Browse, and then navigate to the federation metadata XML that you downloaded earlier from Azure. Then click Open.
SP Entity ID	Enter the URL that identifies the authentication request to Azure, which is the same value as the entity ID configured on the Azure portal. In this example, the URL is https://sase-us1-dir.poc.versanow.net/versa/sso/loginConsumer.
SSO User Attributes (Tab)	Select the SSO User Attributes tab, and ensure that the values shown in the screenshot are displayed. These values are automatically populated by the Director node, so you should not need to enter or modify them. These values match the claim values on the Azure portal. Note these values are case sensitive.

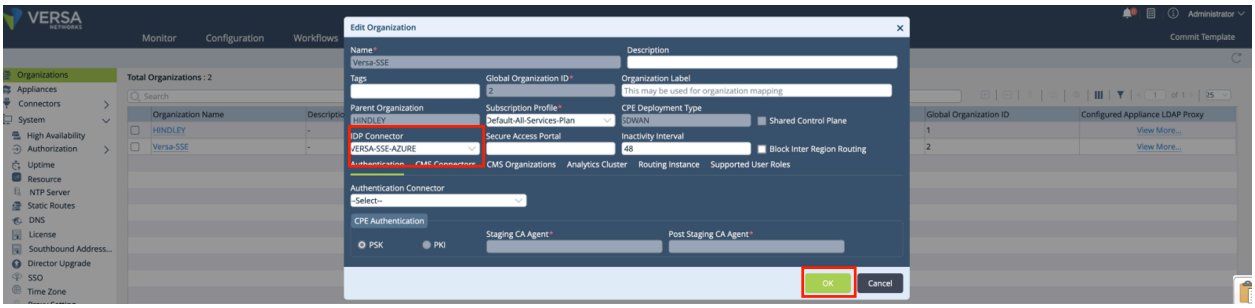
3. If you are using the connector to authenticate all network administrators regardless of whether they are provider or tenant users, perform this step. This step relates to the first use case described in SAML Design Use Cases, above, in which the provider and tenant organizations are authenticated using a single IdP. This IdP is typically the provider's IdP, and all network administrators regardless of the organization to which they belong to are authenticated using the provider's IdP. Otherwise, continue to Step 4.
    a. In the main pane, click to select the provider's connector.
    b. Select the Connector Mode icon in the horizontal menu bar.
    c. In the Connector Mode popup window, click Single IdP Connector. Note that globally, you can associate only one connector with the Single IdP Connector option. If you configure another connector with this option, any other connector that was previously configured with this option reverts to the connector mode None.
    d. Click OK.

4. If you are using the connector to authenticate provider users, perform this step. This step relates to the second case described in SAML Design Use Cases, above, in which you associate SAML authentication with the provider organization or any of the tenant organizations. That is, authentication methods are applied on a per-organization basis. So, for example, network administrators of Tenant A may be authenticated using the tenant's IdP, while the provider or other tenant organizations may use some other method (or IdP) for authentication. Otherwise, continue to Step 5.
    a. In the main pane, click to select the provider's connector.
    b. Select the Connector Mode icon in the horizontal menu bar.
    c. In the Connector Mode popup window, click Default IdP Connector.
    d. Click OK.



5. If you are using the connector to authenticate tenant users, perform this step. This step also relates to the second case described in SAML Design Use Cases, above, in which you associate SAML authentication with the provider organization or any of the tenant organizations. That is, authentication methods are applied on a per-organization basis. So, for example, network administrators of Tenant A may be authenticated using the tenant's IdP, while the provider or other tenant organizations may use some other method (or IdP) for authentication.
    a. In the main pane, click to select the provider's connector.
    b. Select the Connector Mode icon in the horizontal menu bar.
    c. In the Connector Mode popup window, click None.
    d. Click OK.

6. Select Administration > Organizations, and then select the organization to enable for SSO.
    a. In the IdP Connector field, enter the name of the connector that you created above. Here, we use VERSA-SSE-AZURE.
    b. Click OK.

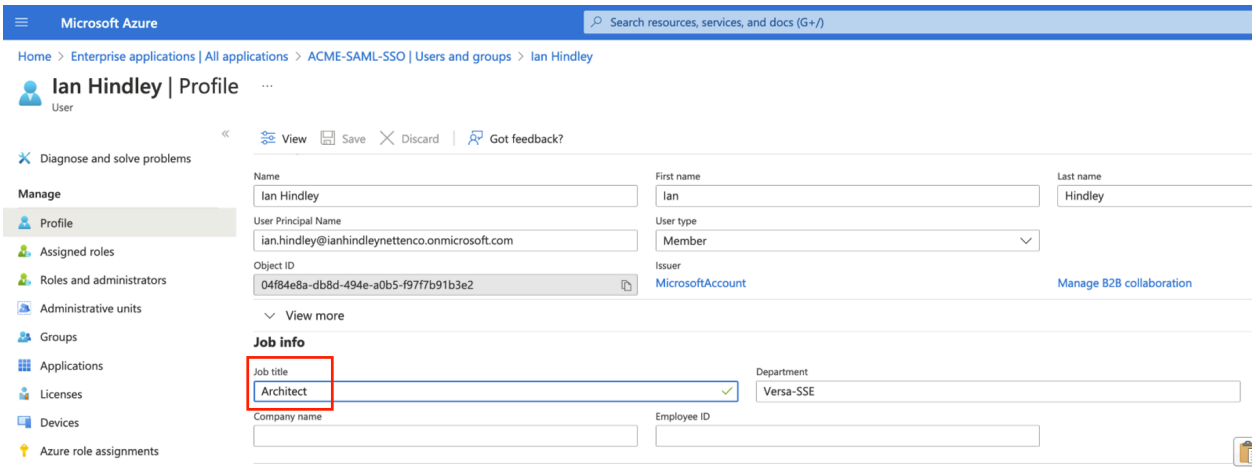


Create SSO Role Mappings

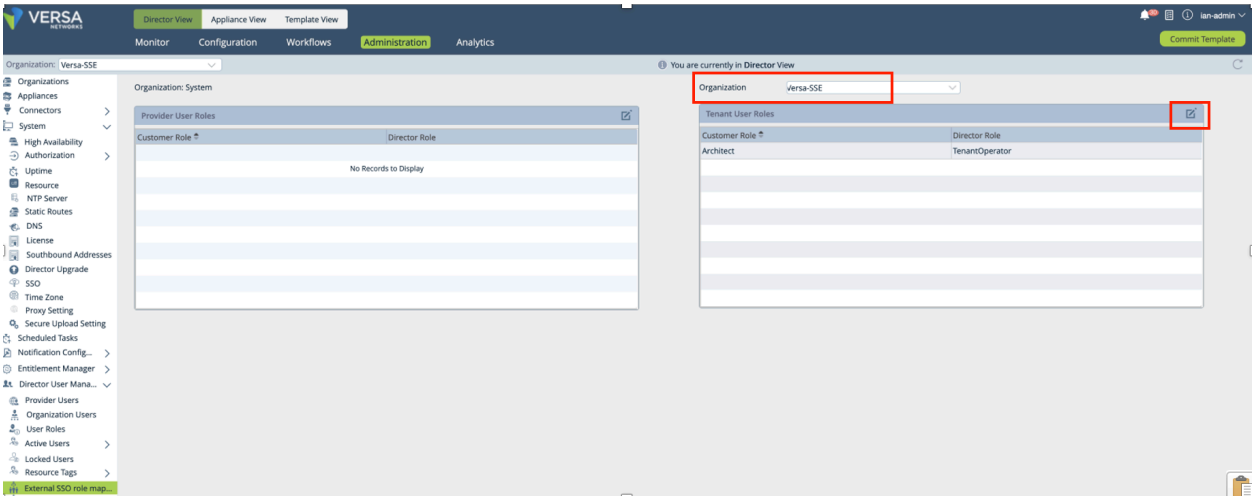
As described in Associate Users with the New Application, above, on the Azure portal, the user's department and job title are used to inform the Director node about the user's permissions and the organization with which the SSO network administrator is associated. For the job title, the customer may not want this information to be amended to a VOS-defined value, such as TenantOperator. To resolve this, you can create an SSO role mapping on the Director node so that the Director node can map the value returned by Azure to a different value. For example, if the user's job title is Architect, this is not a predefined user group on the Director node, so it must be translated to the actual user group configured on the Director node, which is TenantOperator.

To create role mappings:

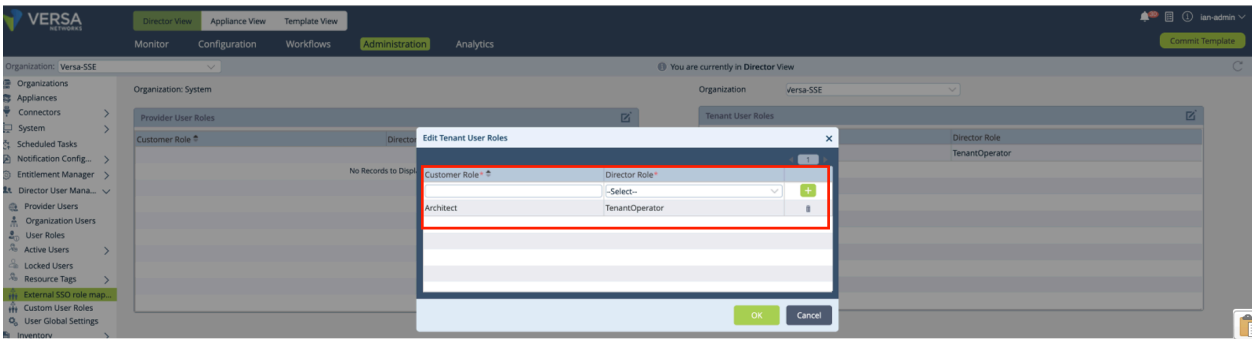
1. In Azure, check the job title of the user. In the example here, it is Architect.



2. On the Director node, create an SSO role that maps the job title Architect to the user group TenantOperator. Navigate to Administration > System > Director User Management > External SSO Role Mapping. Then select the organization and click the Edit icon.



3. In the Edit Tenant User Roles popup window, in the Customer Role field, add the job title as it is defined on the Azure portal. In this example, the job title is Architect. Select the appropriate Director role for the customer role. In this example, the customer role is the user group TenantOperator. Then click the + Add icon.

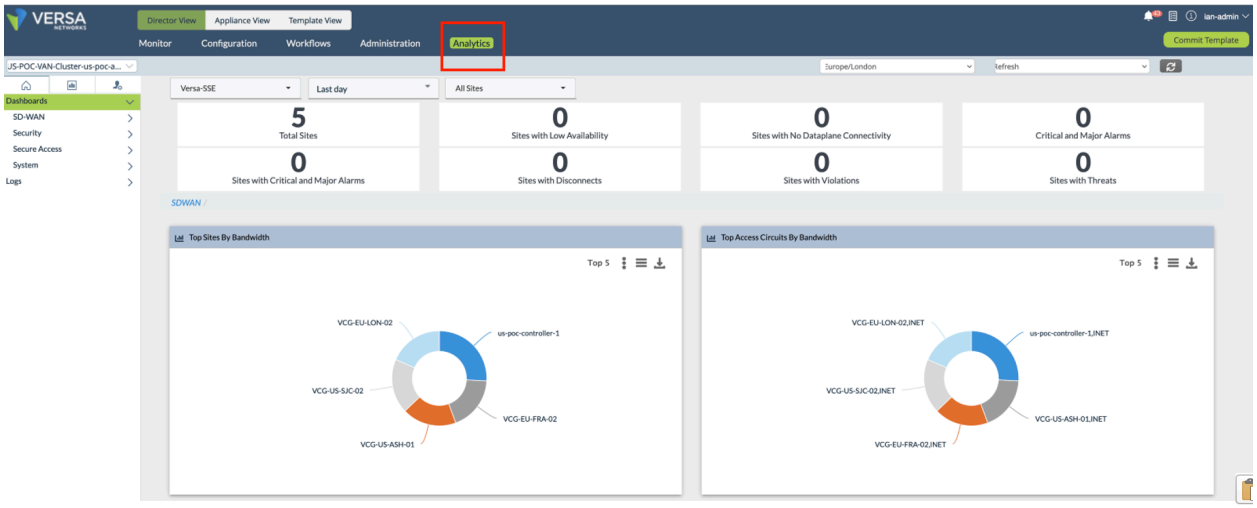


4. Click OK.

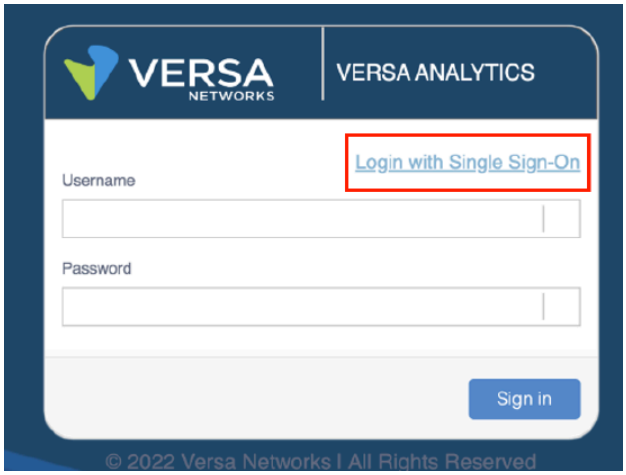
With this configuration, when a network administrator with the job title Architect logs in to a Director node, the Director node maps the job title Architect to the role TenantOperator. This role is a known role that provides read-only access to the platform

Integrate Versa Analytics with Azure SSO

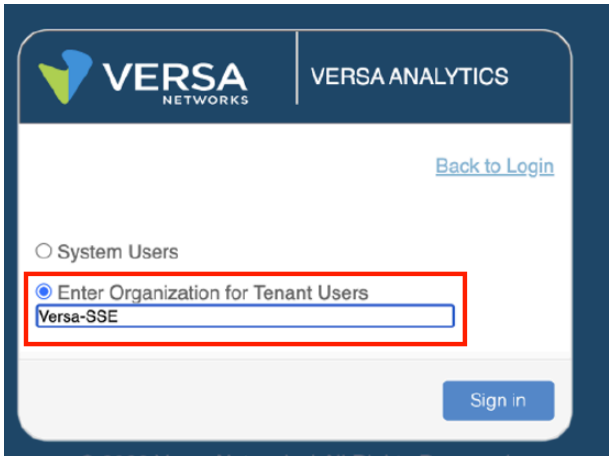
This procedures described in this article that integrate Versa Director with Azure SSO also allow the network administrator to access Versa Analytics through the Director node, as shown in the following screenshot.



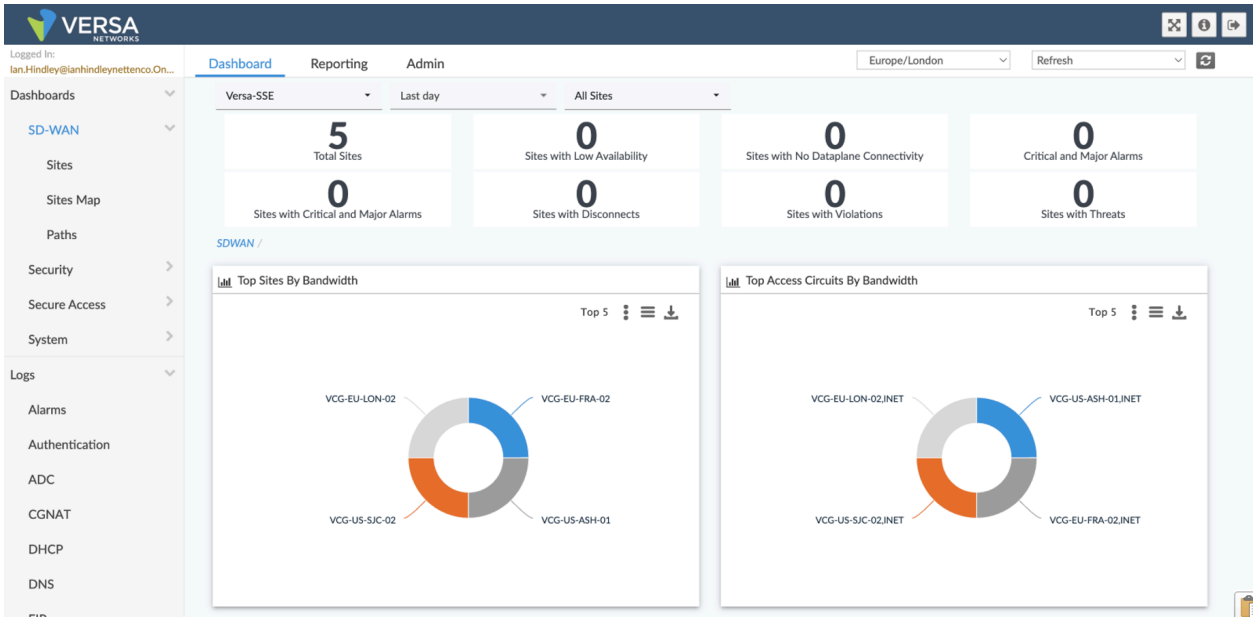
However, if you want to authenticate network administrators using Azure SSO when they access Versa Analytics directly from their browser, you must do some additional configuration. With this configuration, the user can access Versa Analytics directly through their browser, as shown in the following screenshot.



When the user clicks Login with Single Sign-On, they are presented with the screen shown in the following screenshot. On this screen, network administrators for the parent organization click System Users, and network administrators for a tenant organization click Enter Organization for Tenant Users and then enter the organization, as shown in the screenshot. Note that the organization name is case sensitive.

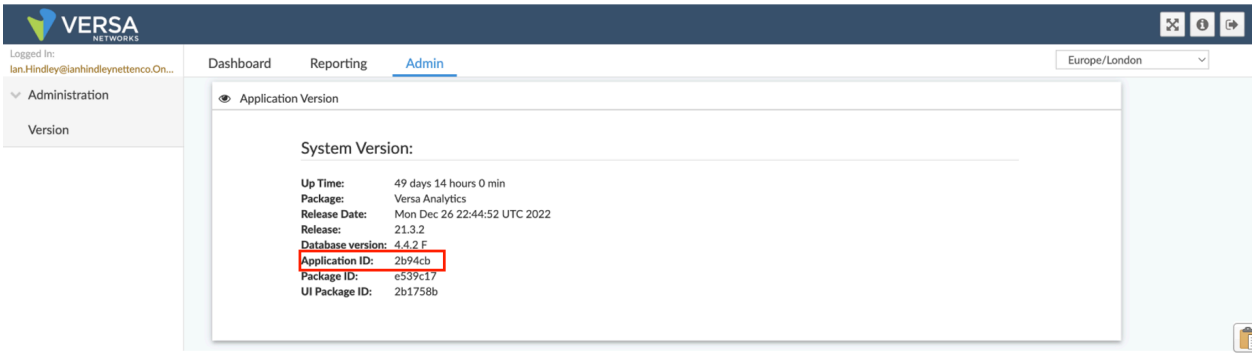


After the user clicks Sign In, the same IdP screenshots shown earlier in this article are presented to them. After the user has entered their username and password and the authentication is successful, the user is then logged in to the Analytics node, as shown in the following screenshot.

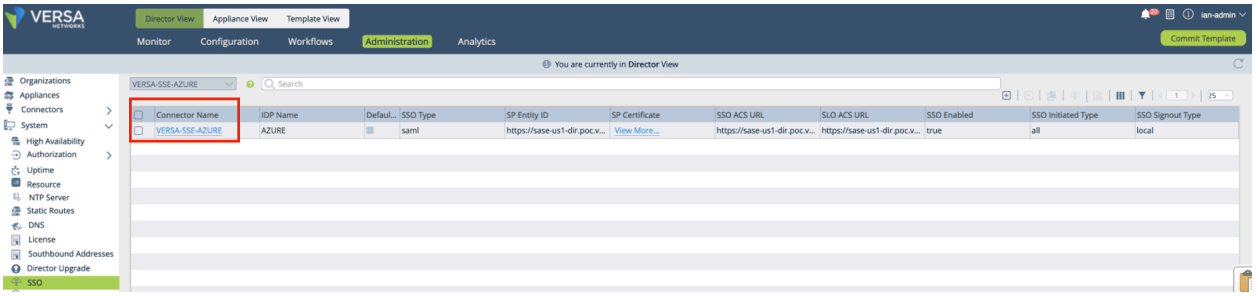


To integrate Versa Analytics with Azure SSO:

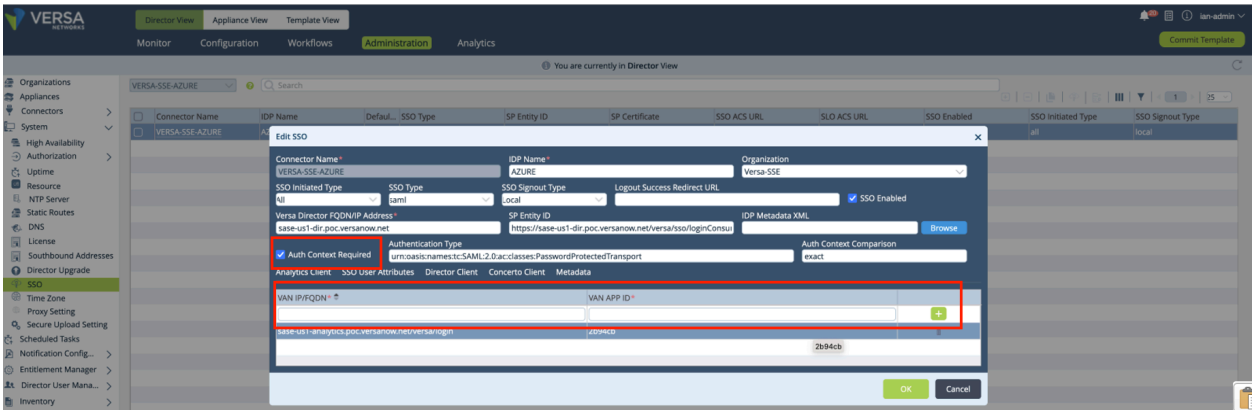
1. On the Analytics node, make a note of the Versa Analytics application ID. This is required to configure the SSO connector on the Director node.



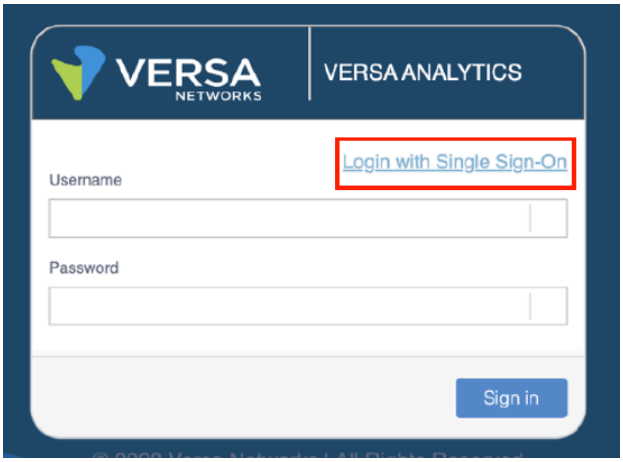
2. Log in to the Director node, and then select Administration > System > SSO. Click the connector name you created earlier. In this example, the name is VERSA-SSE-AZURE.



3. In the Edit SSO popup window, select the Analytics Client tab. Enter the FQDN or IP address of the Analytics node, enter the Analytics application ID, click the + Add icon, and then click OK.



4. To log in to the Analytics node directly, click Login with Single Sign-On.



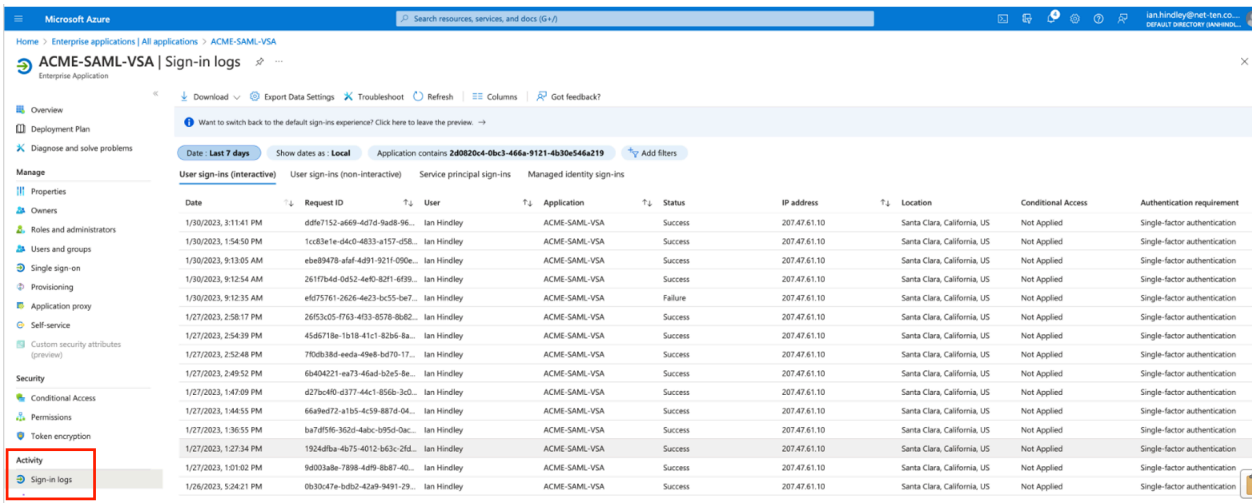
Verify the Configuration

To check the configuration works as expected when logging in to the Director node, follow the steps in Network Administrator's Perspective of Accessing Versa Director, above, which show how to log in to the Director node using single sign-on.

To check that the configuration works as expected when logging in directly to Versa Analytics, follow the steps in Integrate Versa Analytics with Azure SSO, above.

Troubleshoot Azure

You can monitor SSO events, including success and failure attempts by the end user, from the sign-in logs, as shown in the following screenshot.



Troubleshoot Versa Director

As described in General Configuration Notes, above, the Director node must be synchronized with NTP to ensure that both the Director node and the IdP (that is, Azure) are synchronized to within a few milliseconds of UTC. If the clocks differ between the two platforms, authentication fails. To check that the time is synchronized, from the CLI on the Director node, tail the following logs:

```
# cd /var/log/vnms/spring-boot
# tail -f vnms-spring-boot.log vnms-spring-rest.log
```

If the clocks are not synchronized, the logs show an event similar to the following:

```
tail -f vnms-spring-boot.log vnms-spring-rest.log

[22-Jun-2020 08:10:14.114] [ERROR][tomcat-exec-7] [com.versa.vnms.core.sso.saml.SAMLLoginResponseParser] Exception while validating response

java.lang.Exception: Timing issues. Possible reasons include: SAML expired, service's clock setting is not UTC.
```

For general troubleshooting, if SSO using SAML fails, check that the the username is in an email format. Then, on the Director node, tail the following logs, which show the dialog between the Director node and Azure. The messages include the response from Azure and the attributes user.jobtitle and user.department.

```
# cd /var/log/vnms/spring-boot
# tail -f vnms-spring-boot.log vnms-spring-rest.log
```

The following shows an example of a successful login. Note the role uses a predefined role on the Director node, here, TenantSuperAdmin. The organization name is correct (including capitalization) as defined on the Director node, here, Versa-SSE.

```
==> vnms-spring-rest.log <==
[28-Feb-2023 09:47:09.017][,,][INFO][https-jsse-nio-9183-exec-76][com.versa.rest.controller.sso.saml.SSOServiceController] Mapped role... roleName=TenantSuperAdmin type=TENANT privileges=null
[28-Feb-2023 09:47:09.017][,,][INFO][https-jsse-nio-9183-exec-76][com.versa.rest.controller.sso.saml.SSOServiceController] orginal role... TenantSuperAdmin

==> vnms-spring-boot.log <==
[28-Feb-2023 09:47:09.021][,,][INFO][https-jsse-nio-9183-exec-76][com.versa.vnms.cdbadaptor.cdbdao.TrackRBACRulesDAO] SupportedOrgRoles for org Versa-SSE
[28-Feb-2023 09:47:09.023][,,][INFO][https-jsse-nio-9183-exec-76][com.versa.vnms.cdbadaptor.cdbdao.TrackRBACRulesDAO] Completed SupportedOrgRoles for org Versa-SSE

==> vnms-spring-rest.log <==
[28-Feb-2023 09:47:09.023][,,][INFO][https-jsse-nio-9183-exec-76][com.versa.rest.controller.sso.saml.SSOServiceController] Valid user name ian.hindley@ianhindleynettenco.onmicrosoft.com
[28-Feb-2023 09:47:09.024][,,][INFO][https-jsse-nio-9183-exec-76][com.versa.rest.controller.sso.saml.SSOServiceController] CustomRole... TenantSuperAdmin
```

```
==> vnms-spring-rest.log <==
[28-Feb-2023 09:47:39.992][,,][INFO][https-jsse-nio-9183-exec-96][com.versa.rest.controller.UserTrackingController] < findOne ian.hindley@ianhindleynettenco.onmicrosoft.com result
UserTracking{userName='ian.hindley@ianhindleynettenco.onmicrosoft.com'orgName='Versa-SSE', accountStatus=ACTIVE, loginFailCount=0, creationDate=2023-02-28 09:24:20.167, lastSuccessfulLogin=2023-02-28 09:38:32.642, successfulLogin=2023-02
09:47:09.869, lockedTime=null, currentlyLogged=true, resetPassword=true, lastResetPasswordChangedDate=null, remoteAddress='null', lastResetPasswordRequest='null'}
```

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

Configure AAA