

Vertiv™ Avocent® MP1000 Management Platform and Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance

Mapping Local User Groups to External Authentication Provider User Groups Technical Note

FEBRUARY 2025

Technical Note Section Outline

1. Overview
2. Process Diagram
3. Sequence of Operations
4. (Prerequisite) Setting Up an External Authentication Provider
5. Creating a Local User Group
6. Assigning a System Role to the Local User Group
7. Creating a Resource Group
8. Assigning a Resource Group to a Local User Group
9. Creating a Target Role
10. Assigning a Target Role to the Resource Group Assigned to a Local User Group
11. Mapping a Local User Group to an External Authentication Provider User Group
12. Generating a Certificate Signing Request (CSR)
13. Updating Web UI Certificate with CA Signed Certificate
14. Importing a CA Signed Certificate to a Client Machine Trust Store

1. Overview

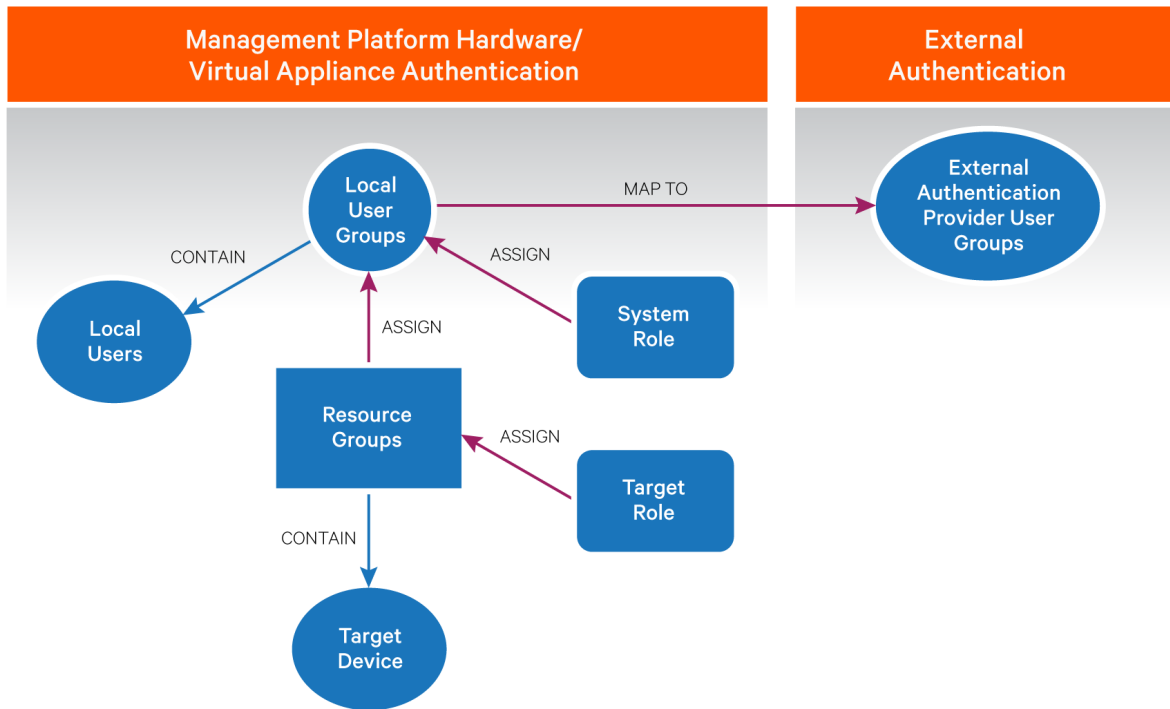
This technical note provides step-by-step instructions to map local user groups to user groups from an external authentication provider such as Active Directory (AD) or LDAP. Given the complexity of the mapping process, refer to the [Process Diagram](#) and [Sequence of Operations](#) sections for a summary of the operations that must be completed to successfully map local user groups. In order to map local user groups to external authentication provider user groups, you must follow the outlined procedures for configuring the local user group, resource group, and target role. Role permissions must be assigned to target devices in the resource group associated with the local user group. After the mapping is completed, members of the external authentication provider user groups will have the same target role permissions as the users from the local user groups.

This technical note applies to the following Vertiv™ Avocent® DSView™ Solution products:

- Vertiv™ Avocent® MP1000 Management Platform
- Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance

2. Process Diagram

The following diagram describes the components in the Vertiv™ Avocent® MP1000 Management Platform and Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance that must be configured to allow mapping of a local user group to an external authentication provider user group. The purple arrows indicate the configuration processes that are described in this technical note.



3. Sequence of Operations

This section describes the sequence of operations for mapping a local user group to a user group from an external authentication provider.

1. Ensure an external authentication provider has already been added, enabled, and tested on the management platform appliance. If the provider has not been set up, refer to [\(Prerequisite\) Setting Up an External Authentication Provider](#). If the provider has already been set up, continue to the next operation.
2. Create a local user group with one or more users or use an existing group. To create a new local user group, refer to the [Creating a Local User Group](#) section.
3. Assign a system role to the local user group. Refer to the [Assigning a System Role to the Local User Group](#) section.
4. Create a new resource group that contains one or more target devices or use an existing group. To create a new resource group, refer to the [Creating a Resource Group](#) section.
5. Assign the resource group to the local user group. Refer to the [Assigning a Resource Group to a Local User Group](#) section.
6. Create a target role that allows users from a local user group to perform specific target device operations based on the permissions assigned to the target role. Refer to the [Creating a Target Role](#) section.
7. Assign the target role to the resource group. Refer to the [Assigning a Target Role to the Resource Group Assigned to a Local User Group](#) section.
8. Map the local user group to a user group from the previously configured external authentication provider. Refer to the [Mapping a Local User Group to An External Authentication Provider User Group](#) section. When a user from the external authentication provider group logs into the management platform appliance, they will have the same role permissions that are assigned to the local user group.
9. Perform a test to connect to the external authentication provider with a user from an external authentication provider user group that has been previously mapped to a local user group. Refer to the [Testing Access to an External Authentication Provider](#) section.

4. (Prerequisite) Setting Up an External Authentication Provider

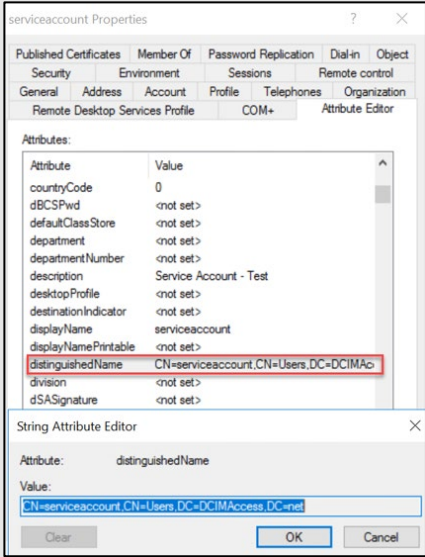
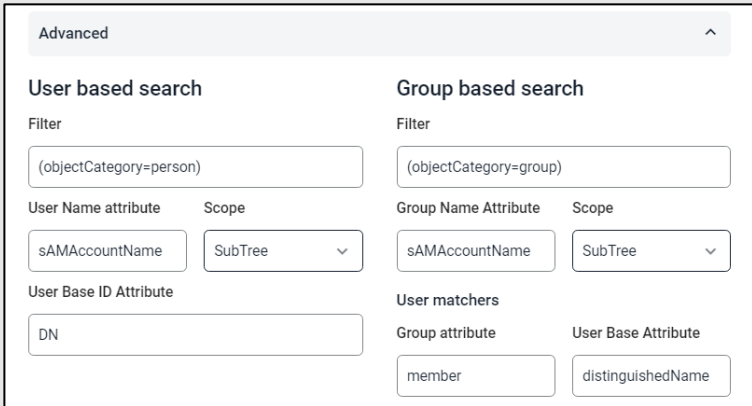
Before mapping a local user group to an external authentication provider user group, an external authentication provider (AD or LDAP) must be added to either the Vertiv™ Avocent® MP1000 Management Platform or Vertiv™ Avocent® MP1000VA Management Platform Virtual Appliance. Once added, the provider must be enabled, and you should test the connection to the provider to ensure it is successful.

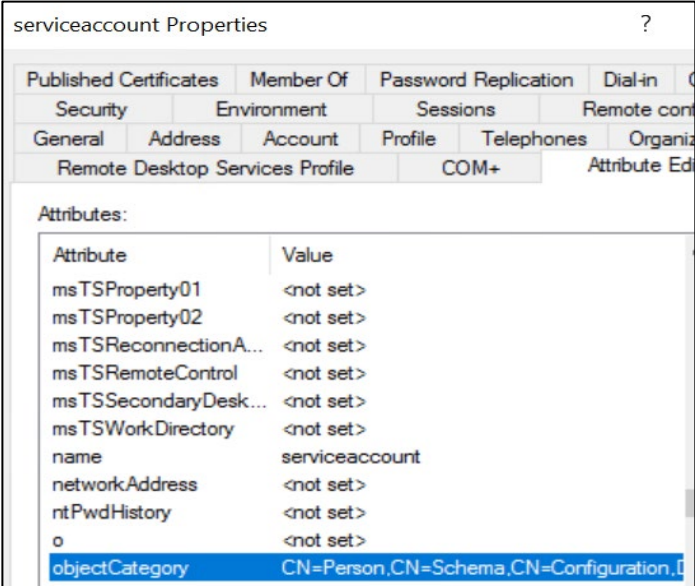
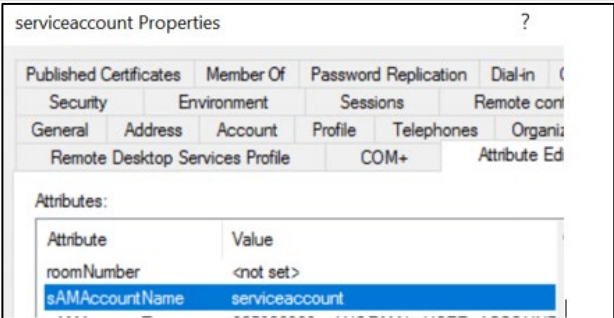
Adding an external authentication provider

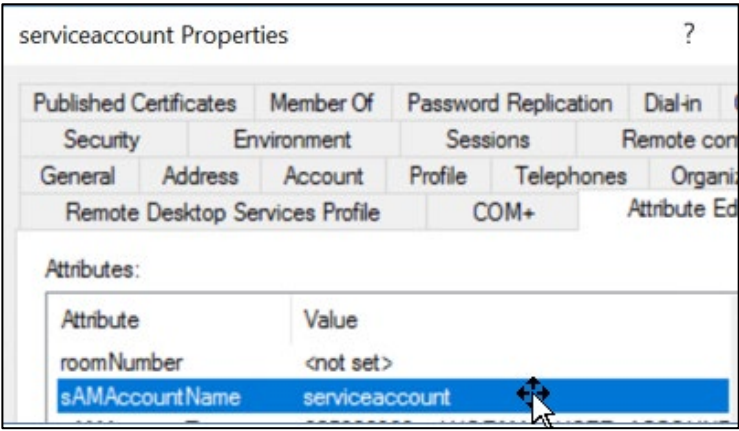
NOTE: If the management platform is part of a High Availability (HA) cluster, the external authentication provider should be added to the Primary node in the cluster.

1. From the left-hand sidebar, click *Administration - Authentication Providers* screen.
2. Click the Add icon (+) at the top right corner.
3. Select the *AD/LDAP* authentication provider option. A dialogue box appears for the chosen authentication provider.
4. Enter the required configuration information for the authentication provider, according to the table below.

PARAMETER	INSTRUCTION
Template Type	Choose the template to use for each authentication type: <i>AD Secure</i> , <i>AD Insecure</i> , <i>LDAP Secure</i> or <i>LDAP Insecure</i> .
Name	Enter the name of the server for the selected authentication type.
Port	Enter the port to use for the selected authentication type. The default port for AD Secure and LDAP Secure connections is 636. The default port for AD Insecure and LDAP Insecure connections is 389. NOTE: If you selected the AD Secure or LDAP Secure template type, ensure that access to the management platform web UI does not generate any certificate errors on the browser. If a certificate error occurs, refer to the Generating a Certificate Signing Request (CSR), Updating Web UI Certificate with CA Signed Certificate and Importing a CA Signed Certificate to a Client Machine Trust Store sections in this document.
Host	Enter the hostname or IP address for the authentication server. It is recommended to enter the hostname for the external authentication provider. NOTE: If you selected the AD Secure or LDAP Secure template type, ensure that you specify the fully qualified domain name (FQDN) of the domain controller for the External Authentication Provider in the Host field. If you select the AD Insecure or LDAP Insecure template type, you may specify the IP address of the domain controller for the External Authentication Provider in the Host field.
User Base DN	Enter a User Base DN on the authentication server. For example, if the server is DCIMAccess.net, then the User Base DN is DC=DCIMAccess,DC=net.
Group Base DN	Enter a Group Base DN on the authentication server. For example, if the server is DCIMAccess.net, then the Group Base DN is DC=DCIMAccess,DC=net. Make sure that the Group Base DN value does not contain the CN property.

PARAMETER	INSTRUCTION
Username	<p>Enter the distinguished name attribute for the user associated with the authentication server. In the example below, the AD or LDAP user account, which will be linked to the management platform, is a service account. To access the Properties panel for the service account, select the COM+ tab and copy and paste the value from the distinguishedName property.</p> 
Password	Enter the password for the service account in the authentication server.
Group Mapping Mode	<p>Select the appropriate group mapping mode:</p> <ul style="list-style-type: none"> • <i>Map or match groups by name</i> • <i>Map external groups</i> • <i>Match external groups by name</i> (recommended for large external groups)
SSL Mode	Enable/disable secure SSL connections for AD Insecure or LDAP Insecure authentication types.
Advanced (Optional)	<p>Select the Advanced drop-down list to display a list of options to search based on users or groups on the AD or LDAP authentication server.</p> 

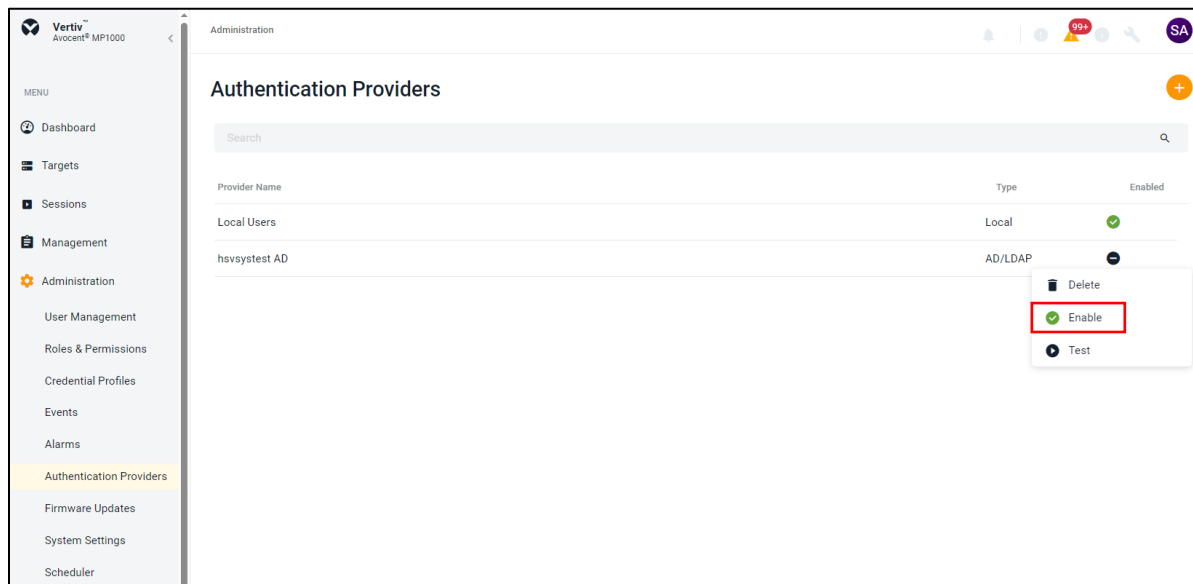
PARAMETER	INSTRUCTION
<p>User Based Search (Optional)</p>	<ul style="list-style-type: none"> Filter - Enter the object category “(objectCategory=person)” filter. See the example below for the service account user. 
<p>User Based Search (continued)</p>	<ul style="list-style-type: none"> User Name attribute - Enter the “sAMAccountName” attribute for the authentication server. See the example below for the service account user.  <ul style="list-style-type: none"> Scope - Leave as default: <i>SubTree</i> User Base ID Attribute - Enter DN as the attribute.

PARAMETER	INSTRUCTION
Group Based Search (Optional)	<ul style="list-style-type: none"> Filter - Enter the object category “(objectCategory=group)” filter. Group Name attribute - Enter the “sAMAccountName” attribute for the authentication server.  <ul style="list-style-type: none"> Scope - Leave as default: <i>SubTree</i> User Matchers <ul style="list-style-type: none"> Group attribute – Enter member as the attribute. User Base Attribute – Enter distinguishedName as the attribute.

- After entering the configuration information, click the *Add Provider* button. The new authentication provider will be displayed on the Authentication Providers screen.
- Next, enable the external authentication provider. Refer to the [Enabling the External Authentication Provider](#) section.
- After the provider has been enabled, perform a test to connect to the provider with any user, such as a service account, from an external authentication provider user group. Refer to the [Testing Access to an External Authentication Provider](#) section.

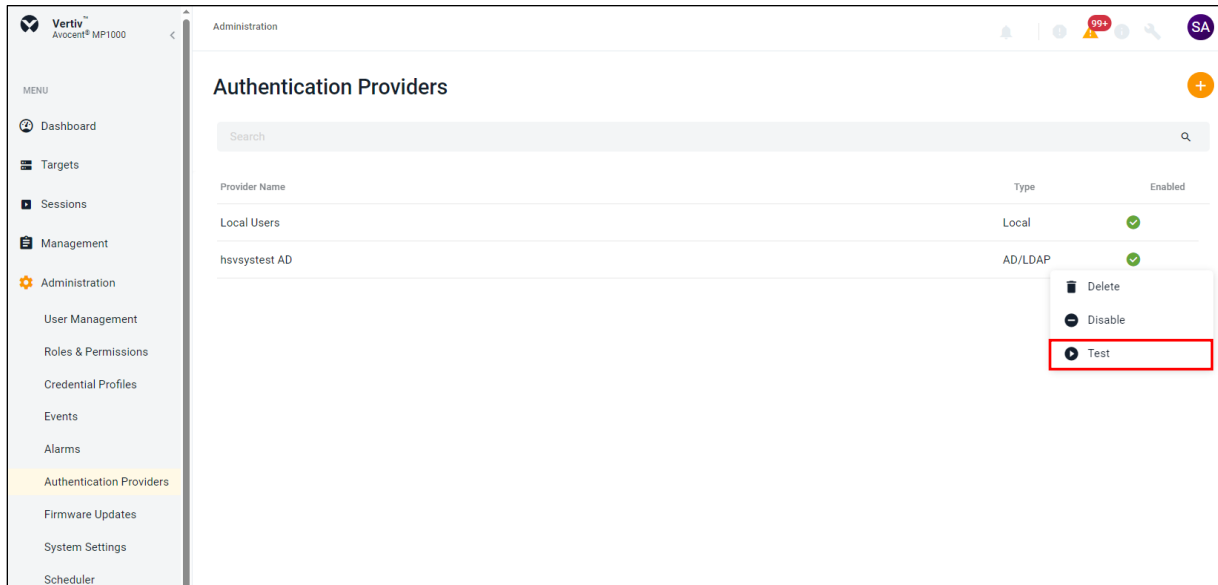
Enabling an External Authentication Provider

- From the *Administration – Authentication Providers* screen, select the external authentication provider to enable.
- Hover your mouse over the row of the provider, click on the vertical ellipsis on the right side of the row and then click *Enable*.

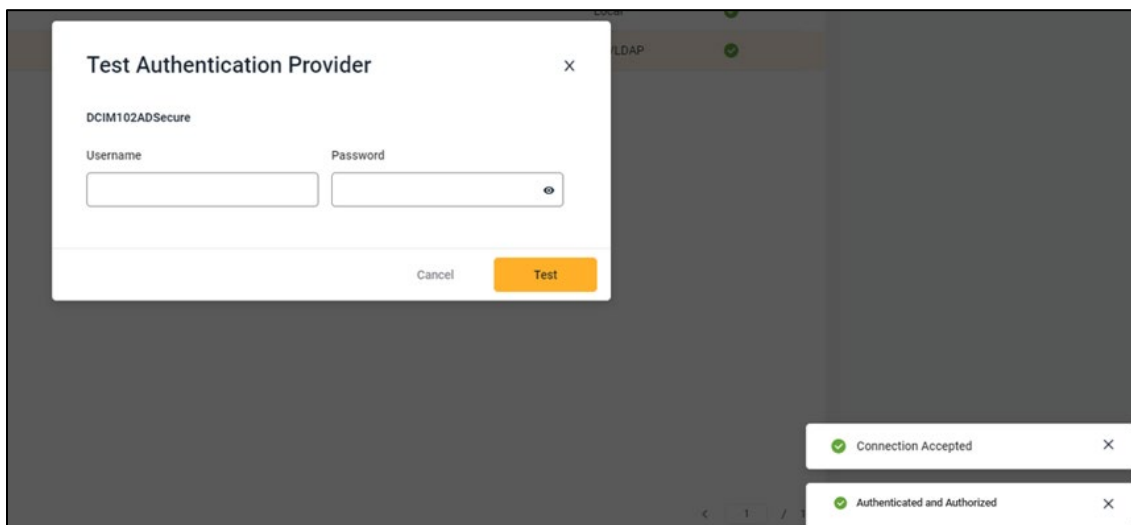


Testing Access to an External Authentication Provider

1. From the *Administration – Authentication Providers* screen, select the external authentication provider to test.
2. Click on the vertical ellipsis on the right side of the row and click *Test*.



3. The Test Authentication Provider dialogue box appears. Enter a valid username and password for a user that belongs to a group in the external authentication provide and click the *Test* button.
4. Verify that a confirmation message appears, indicating that a connection to the external authentication provider has been accepted and the user has been authenticated and authorized. If the connection is not authorized, refer to [Sequence of Operations](#).



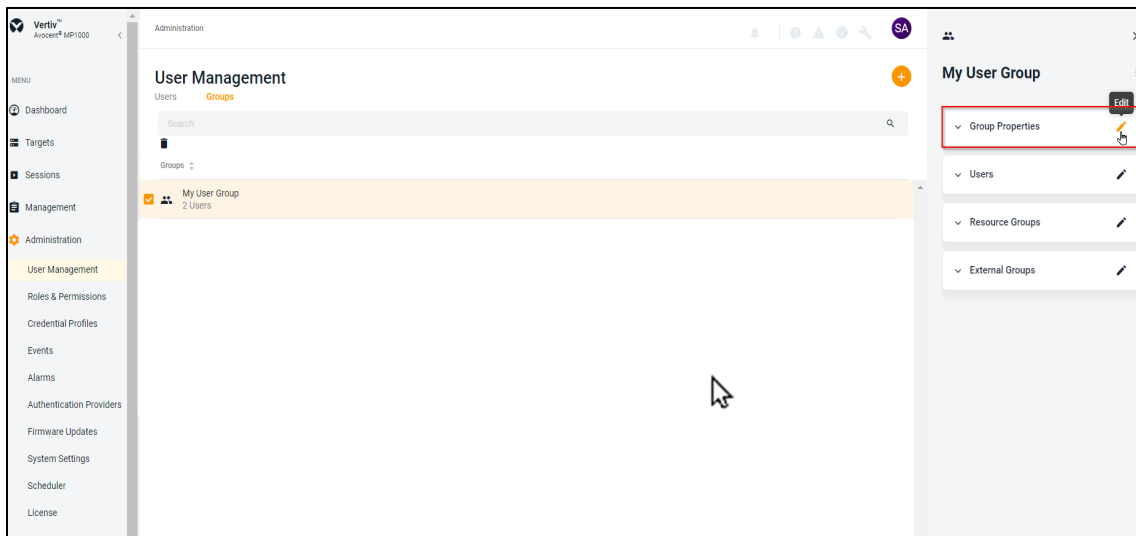
5. If the connection has been accepted and authenticated but not authorized, proceed to the next step in the [Sequence of Operations](#) section to map a local user group with external authentication provider user groups and to authorize the connection to the provider.

5. Creating a Local User Group

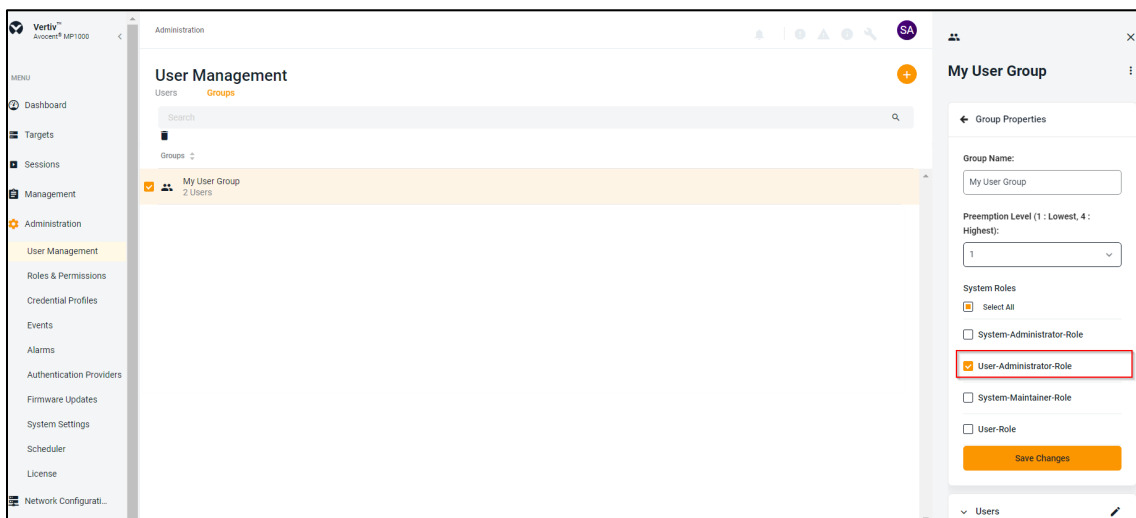
1. From the *Administration - User Management* screen, select the *Groups* tab and click the plus icon (+) in the top right corner to add a local user group.
2. An Add New Group dialogue box appears. In the Group Name field, enter the name for the local user group.
3. Check the boxes for each user you want to add to the local user group. The local user group must contain at least one user.
4. Click the *Add Group* button.

6. Assigning a System Role to the Local User Group

1. From the *Administration - User Management* screen, select the *Groups* tab.
2. Click on the local user group to which you are assigning a system role. The Properties side panel opens.
3. Click the Edit icon (pencil) for the Group Properties section.



4. Check the box of a system role to assign to the local user group. In the example below, the *User-Administrator-Role* has been assigned to the local user group *My User Group*.



5. Click the *Save Changes* button.

7. Creating a Resource Group

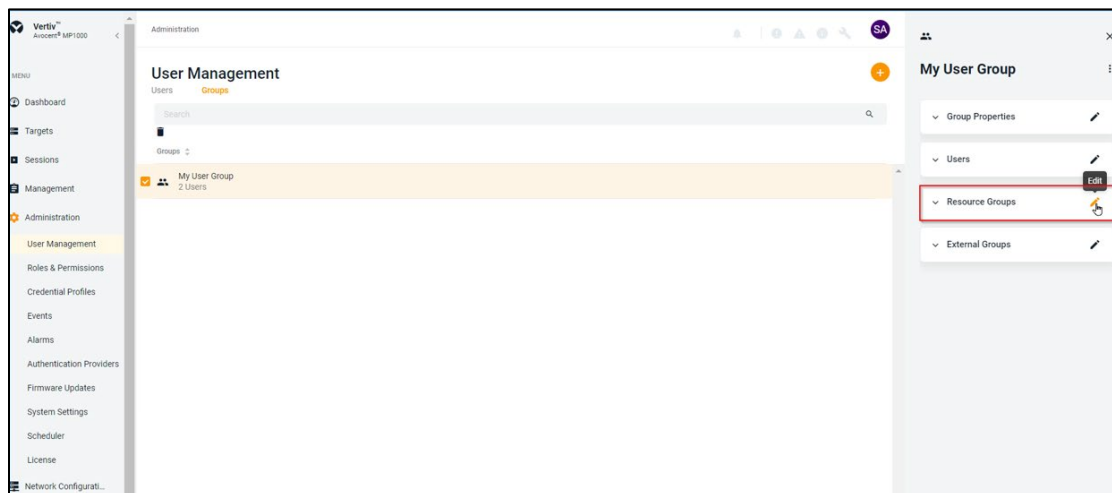
You can create a resource group to manage one or more target devices as a group.

1. From the *Targets – Resource Groups* screen, click the plus icon (+) in the top right corner.
2. An Add Resource Group dialogue box appears. In the Group Name field, enter the name of the resource group.
3. Check the boxes for each target you want to add to the resource group or check the Select All box to add all targets to the resource group.
4. Click the *Add Resource Group* button. The new resource group and its associated targets are now displayed on the Resource Groups screen.

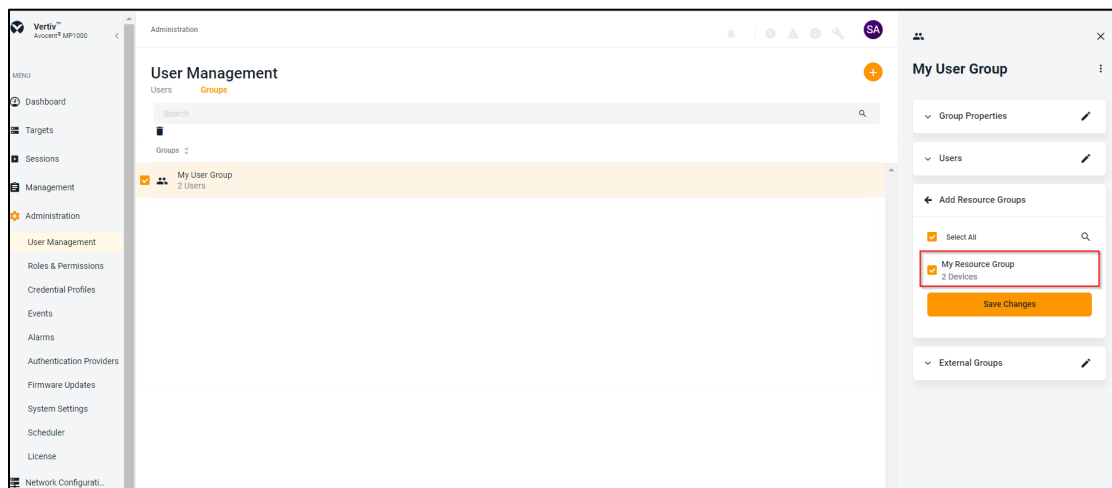
8. Assigning a Resource Group to a Local User Group

You can assign the resource group to the local user group. This allows users of the local user group to access the target devices in the resource group and perform specific operations on the target devices based on the target role that is associated with the resource group.

1. From the *Administration - User Management* screen, select the *Groups* tab.
2. Select the local user group to which you are assigning a resource group. The Properties side panel opens.
3. Click the Edit icon (pencil) for the Resource Groups section.



4. Select a resource group to assign to the local user group. In the example below, the resource group *My Resource Group* has been assigned to the local user group *My User Group*.

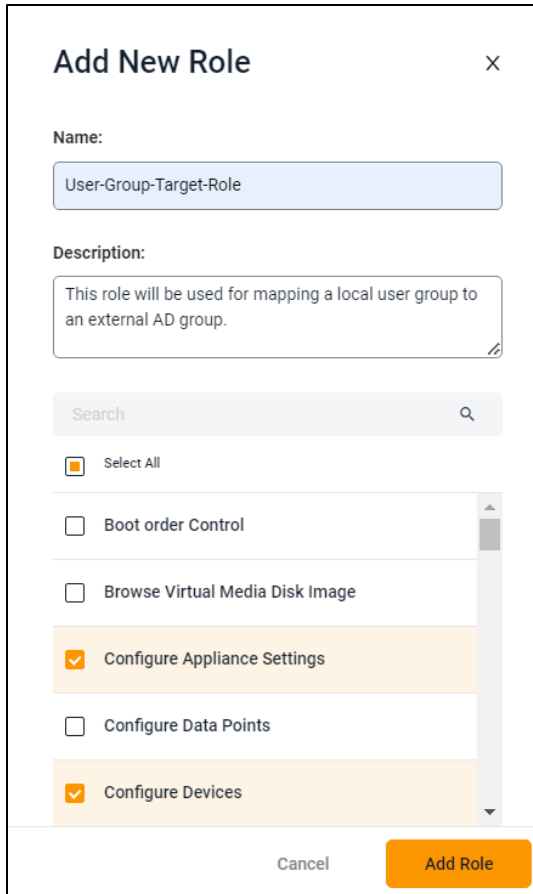


5. Click the *Save Changes* button.

9. Creating a Target Role

You can create a target role which will have permissions to perform specific operations on target devices.

1. From the *Administration – Roles & Permissions* screen, click the plus icon (+) in the top right corner to add a target role.
2. An Add New Role dialogue box appears. Enter the name of the target role and provide a description for the target role.
3. Select the permission(s) to be assigned to the target role. In the example below, the name of the target role is User-Group-Target-Role and both the Configure Appliance Settings and Configure Devices permissions have been assigned to the target role.



Add New Role ×

Name:
User-Group-Target-Role

Description:
This role will be used for mapping a local user group to an external AD group.

Search

Select All

- Boot order Control
- Browse Virtual Media Disk Image
- Configure Appliance Settings
- Configure Data Points
- Configure Devices

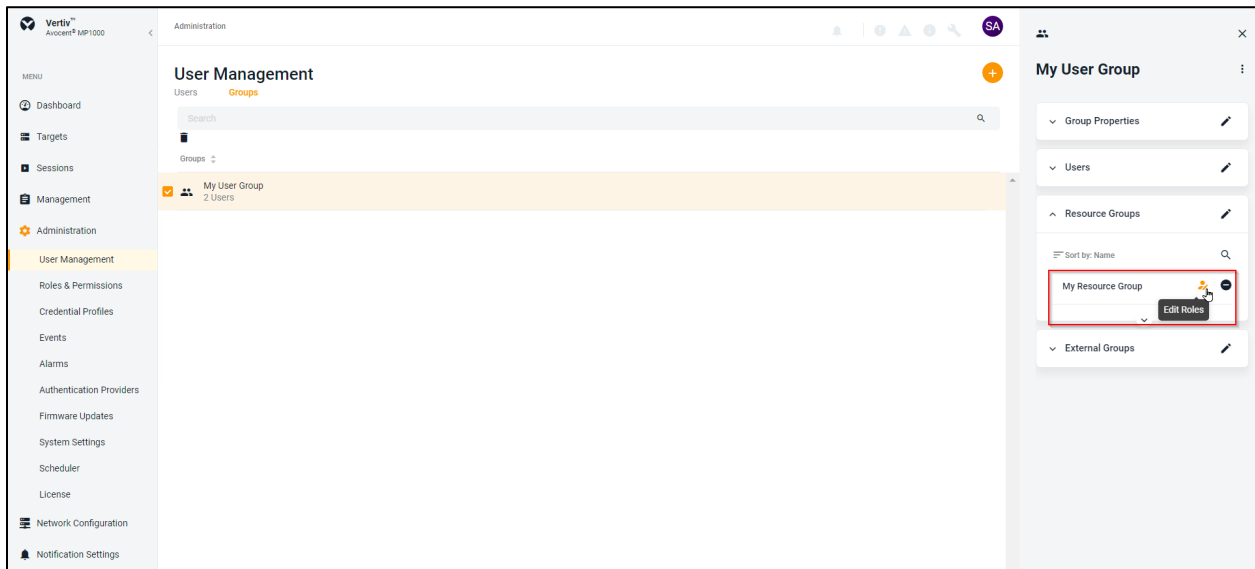
Cancel Add Role

4. Click the *Add Role* button. The new target role is now added to the Roles & Permissions screen.

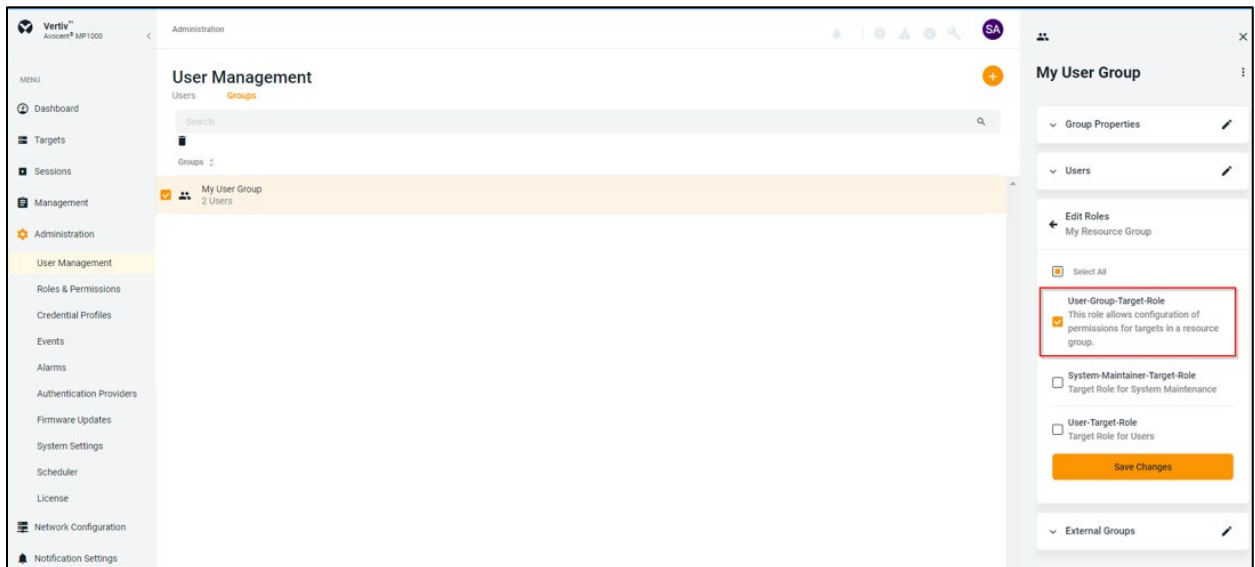
10. Assigning a Target Role to the Resource Group Assigned to a Local User Group

You can assign a target role which will have permissions to perform specific operations on target devices to a local resource group.

1. From the *Administration - User Management* screen, select the *Groups* tab.
2. Click on the local user group to which you are assigning a target role to the resource group associated with the local user group. The Properties side panel opens.
3. Click the Edit icon (pencil) for the Resource Groups section.
4. Click the Edit Roles icon next to the name of the resource group.



5. Select the target role associated with the local user group.

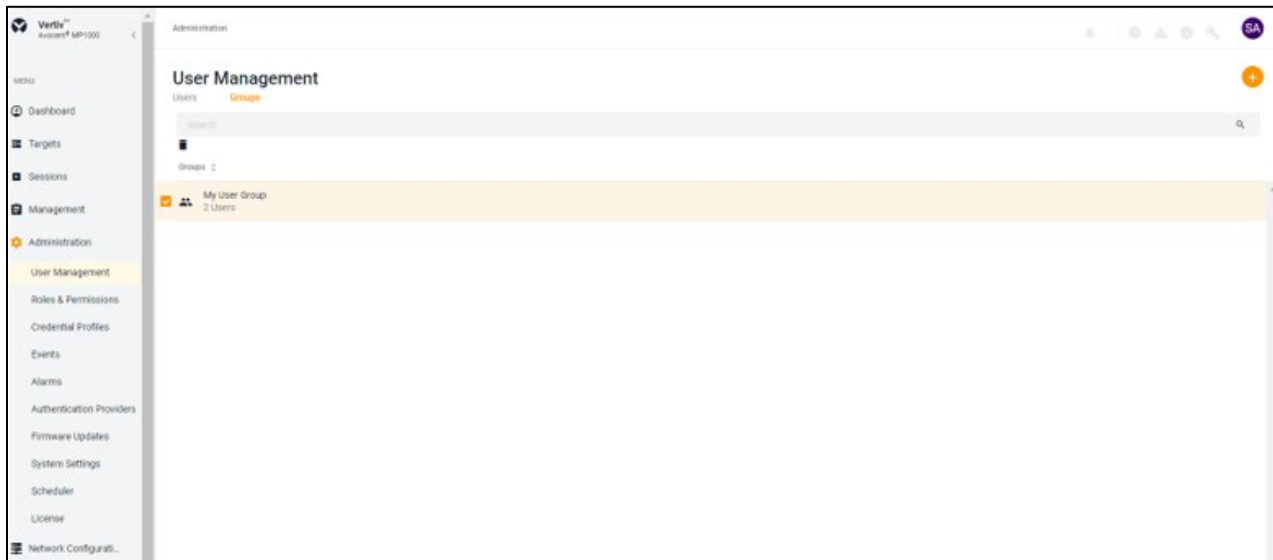


6. Click the *Save Changes* button.

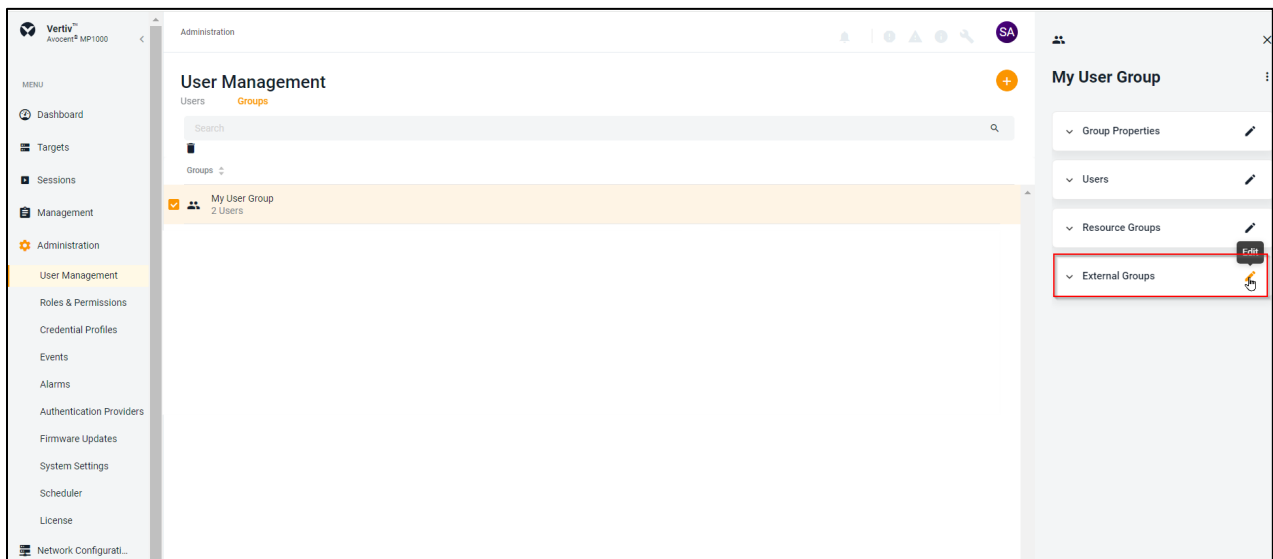
11. Mapping a Local User Group to an External Authentication Provider User Group

After adding, enabling, and testing the external authentication provider on the management platform appliance and completing all other configuration procedures described in this document, you can now map a local user group to an external authentication provider user group.

1. From the *Administration - User Management* screen, select the *Groups* tab.
2. Click on the local user group that you are mapping to a user group from an external authentication provider.

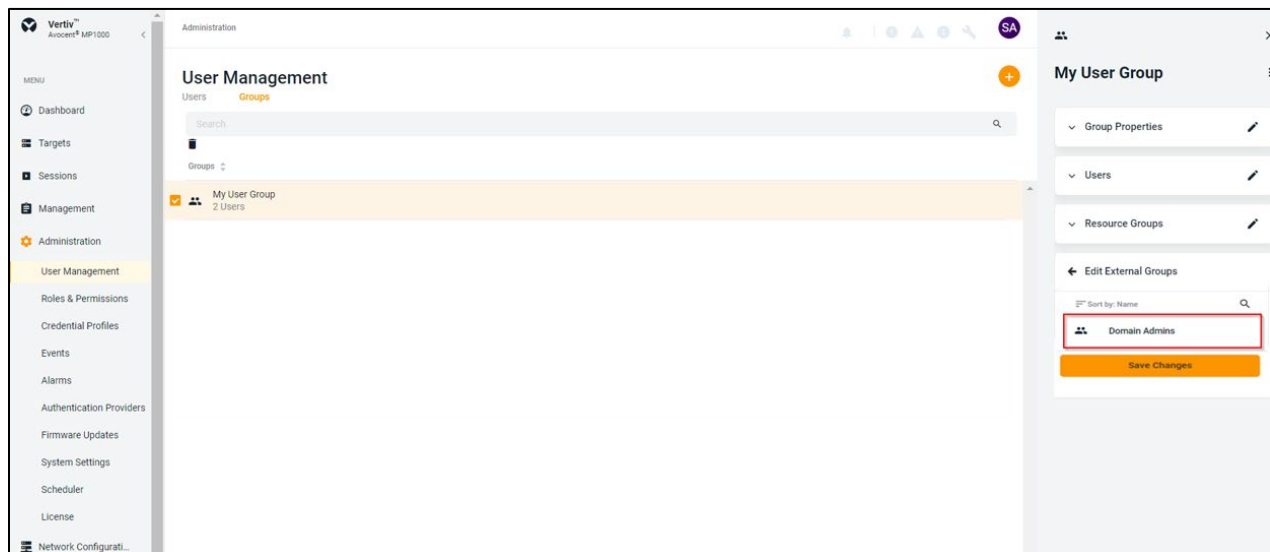


3. Click the Edit icon (pencil) associated with the External Groups section.



- Select the group or groups from the external authentication provider to be mapped to the local user group. In the example below, the external authentication provider group Domain Admins will be mapped to the local user group My User Group.

NOTE: If the list of external authentication provider user groups is long, you may edit the properties on the external authentication provider and configure both the User Base DN and Group Base DN to narrow the search for user groups before mapping the external authentication provider user group to the local user group. After the mapping is completed, you can remove the configuration for User Base DN and Group Base DN as needed.



- Click the *Save Changes* button.

12. Generating a Certificate Signing Request (CSR)

If you need to request a signed certificate from a certificate authority (CA), you can generate a CSR.

- From the *Administration – System Settings – Certificate* screen, click the Generate signing request icon in the top right corner. The Generate Certificate Signing Request dialog box appears.
- Fill out the information and click the *Generate* button. The CSR generates and downloads to your local system as a PEM file called *certificate.pem*.

NOTE: To establish a secure connection with the web UI, you must include the FQDN (Fully Qualified Domain Name) in the SAN (Subject Alternative Name) field of the CSR request.

- Submit the generated CSR file to a CA to get a signed certificate in PEM format.

NOTE: The signed certificate must be in PEM format. If you receive the signed certificate from CA in a different format such as pb7 or p12, then you must convert the signed certificate to PEM format before replacing the self-signed certificate with the CA signed certificate.

13. Updating Web UI Certificate with CA Signed Certificate

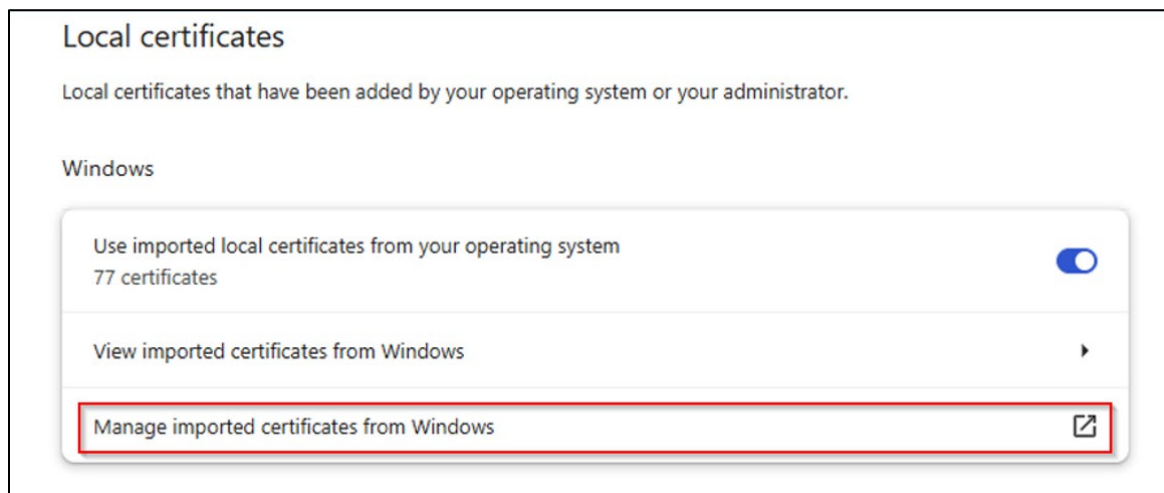
After obtaining the signed certificate from a CA in PEM format, you can update the default management platform web UI certificate.

- From the *Administration – System Settings – Certificate* screen, click the Update certificate icon in the top right corner.
- Using the File Explorer Window pop-up, select the signed certificate file that was obtained from the CA and click the *Open* button to update the existing web UI certificate.
- The Certificate screen refreshes and displays the updated certificate information.

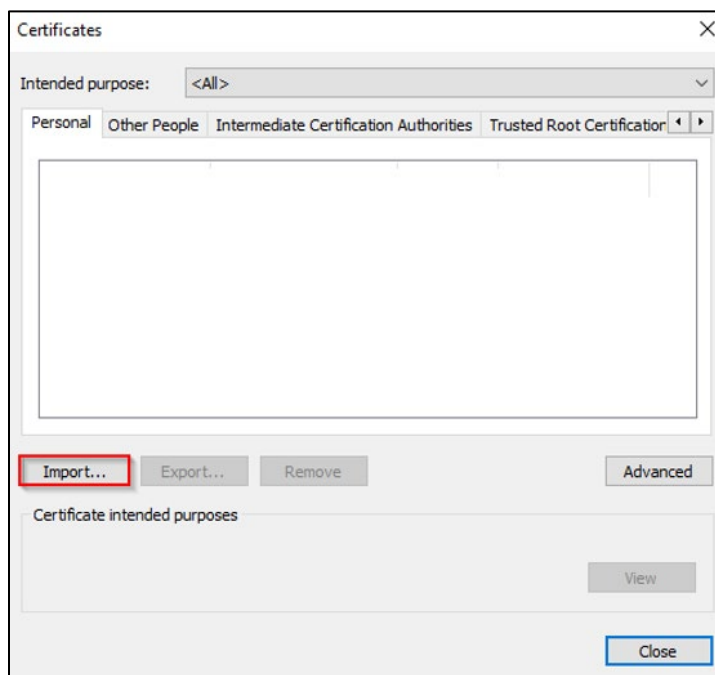
14. Importing a CA Signed Certificate to a Client Machine Trust Store

After receiving a signed certificate from a certificate authority (such as Verisign), you must add the signed certificate to the Windows trust store on the client machine. If the signed certificate is not in PEM format (P7b, P12), you will need to convert the signed certificate to a certificate with PEM file extension before importing it to the client machine trust store.

1. Open the Google Chrome browser.
2. From the top right corner of the browser, click the main menu, and then click *Settings – Privacy and Security – Security – Manage Certificates*.
3. From the Certificate Manager screen, click the *Manage imported certificates from Windows* option to display the Certificates dialog box.



4. From the dialogue box, click the *Import...* button.



5. The Certificate Import Wizard appears. Click the *Next* button.
6. From the File to Import screen, click the *Browse...* button, locate the signed certificate on the local machine, and click the *Next* button.
7. Click the radio button for the Place all certificates in the following store option and click the *Browse...* button.

8. Click on the *Trusted Root Certificate Authorities* trust store and click *OK*.
9. Click the *Next* button.
10. The *Completing the Certificate Import Wizard* screen appears. Click the *Finish* button.
11. Click *Yes* to accept the security warning.
12. A message displays, indicating that the *Import Certificate* operation was successful. The signed certificate has been added to the *Trusted Root Certification Authorities* trust store. Click the *OK* button and then close the *Certificates* dialogue box.