
Enable SAML Authentication



For supported software information, click [here](#).

Security Assertion Markup Language (SAML) is a common standard for authenticating users so that they can access multiple services and applications. SAML is a common standard for exchanging authentication between parties, and it is most commonly used for web browser-based single sign-on (SSO). SSO authenticates a user once and then communicates that authentication to multiple applications. Using SAML-based SSO in Versa secure access improves the user experience, because users do not have to enter user credentials frequently.

To enable SAML authentication, you do the following:





1. Configure the SSO URL in the SAML application.
2. Configure a SAML profile.
3. Associate the SAML profile with an authentication profile.
4. Associate the SAML authentication profile with a Versa secure access portal.
5. Associate the SAML authentication profile with a Versa secure access gateway.

Configure the SSO URL in the SAML Application

To enable SAML authentication, configure the SSO URL in the SAML application in the following format. This is the URL to which the Versa secure access client sends the SAML response.

`https://domain-name/secure-access/services/saml/login-consumer`

Configure a SAML Profile

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Object and Connectors  > Connectors  > Users/Groups  > SAML Profile  in the left menu bar to

configure SAML profile.






4. Click the  Add icon. The Add SAML Profile popup window displays.



The image shows a 'Add SAML Profile' popup window with a light blue header and a dark blue body. The form contains the following fields: 'Name' (with a red asterisk) containing 'SAML VSA'; 'Description' (empty); 'Host' and 'Prefix ID' (empty); 'Single Sign-on URL' (empty); 'Single Sign-out URL' (empty); 'SP Entity ID' and 'IDP Entity ID' (empty); 'SP Certificate' and 'IDP Certificate' (both set to '--Select--' with dropdown arrows). At the bottom right are 'OK' and 'Cancel' buttons.

5. In the Name field, enter a name for the SAML profile (here, SAML VSA).
6. For information about configuring the other fields, see [Configure SAML Profiles](#).
7. Click OK.

Associate the SAML Profile with an Authentication Profile

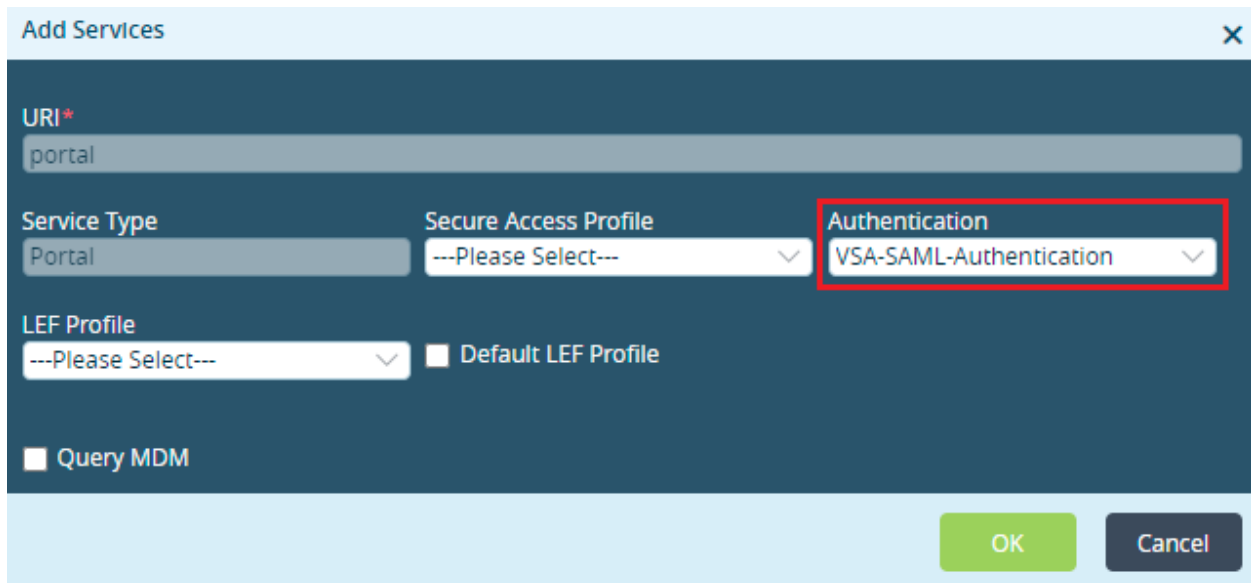
1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors  > Connectors  > Users/Groups  > Authenticator Profiles  in the left menu bar.
4. Click the  Add icon. The Add Authentication Profiles popup window displays.

5. In the Name field, enter a name for the authentication profile (here, VSA-SAML-Authetication).
6. In the SAML Profile field, select the SAML profile you configured in [Configure a SAML Profile](#) above. To add an SAML Profile, click + Create SAML Profile.
7. Click OK.

Associate the SAML Authentication Profile with a Versa Secure Access Portal

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.






3. Select Services  > Secure Access  > Portal  > Servers  in the left menu bar.
4. Click the  Edit icon. The Add Services popup window displays.

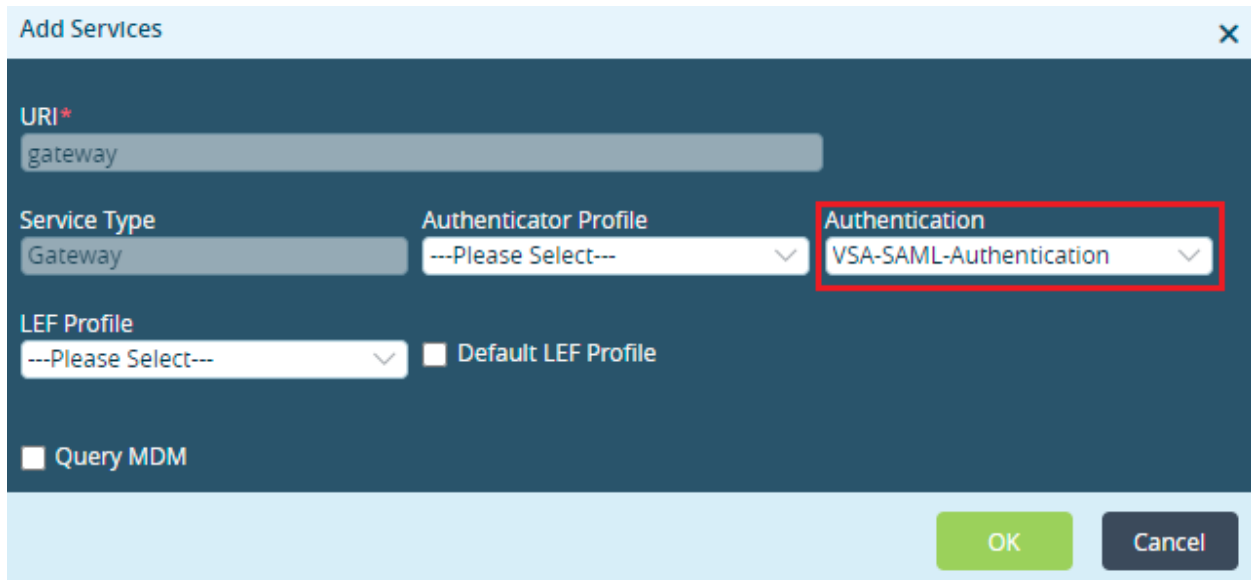


The 'Add Services' popup window is shown with a dark blue background. It contains the following fields: 'URI*' with the value 'portal'; 'Service Type' with a dropdown menu showing 'Portal'; 'Secure Access Profile' with a dropdown menu showing '---Please Select---'; 'Authentication' with a dropdown menu showing 'VSA-SAML-Authentication' (this field is highlighted with a red rectangle); 'LEF Profile' with a dropdown menu showing '---Please Select---' and a checkbox for 'Default LEF Profile'; and a checkbox for 'Query MDM'. At the bottom right, there are 'OK' and 'Cancel' buttons.

5. In the Authentication field, select the authentication profile you configured in [Associate the SAML Profile with an Authentication Profile](#), above (here, VSA-SAML-Authentication).
6. For information about configuring the other fields, see [Add a Secure Access Portal](#).
7. Click OK.

Associate the SAML Authentication Profile with a Versa Secure Access Gateway

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services  > Secure Access  > Gateway  > General  in the left menu bar.
4. Click the  Edit icon. The Add Services popup window displays.



Add Services

URI*
gateway

Service Type: Gateway

Authenticator Profile: ---Please Select---

Authentication: VSA-SAML-Authentication

LEF Profile: ---Please Select---

☐ Default LEF Profile

☐ Query MDM

OK Cancel

5. In the Authentication field, select the authentication profile you configured in [Associate the SAML Profile with an Authentication Profile](#), above (here, VSA-SAML-Authentication).
6. For information about configuring the other fields, see [Configure a Secure Access Gateway](#).
7. Click OK.

Supported Software Information

Releases 20.2.2 and later support all content described in this article.

Additional Information

[Configure User and Group Policy](#)

[Configure the Versa Secure Access Service](#)