
Configure Application Reverse Proxy

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

Application reverse proxy protects software as a service (SaaS) applications from direct access from unmanaged devices that do not have Versa client installed to connect to the Versa Cloud Gateways.

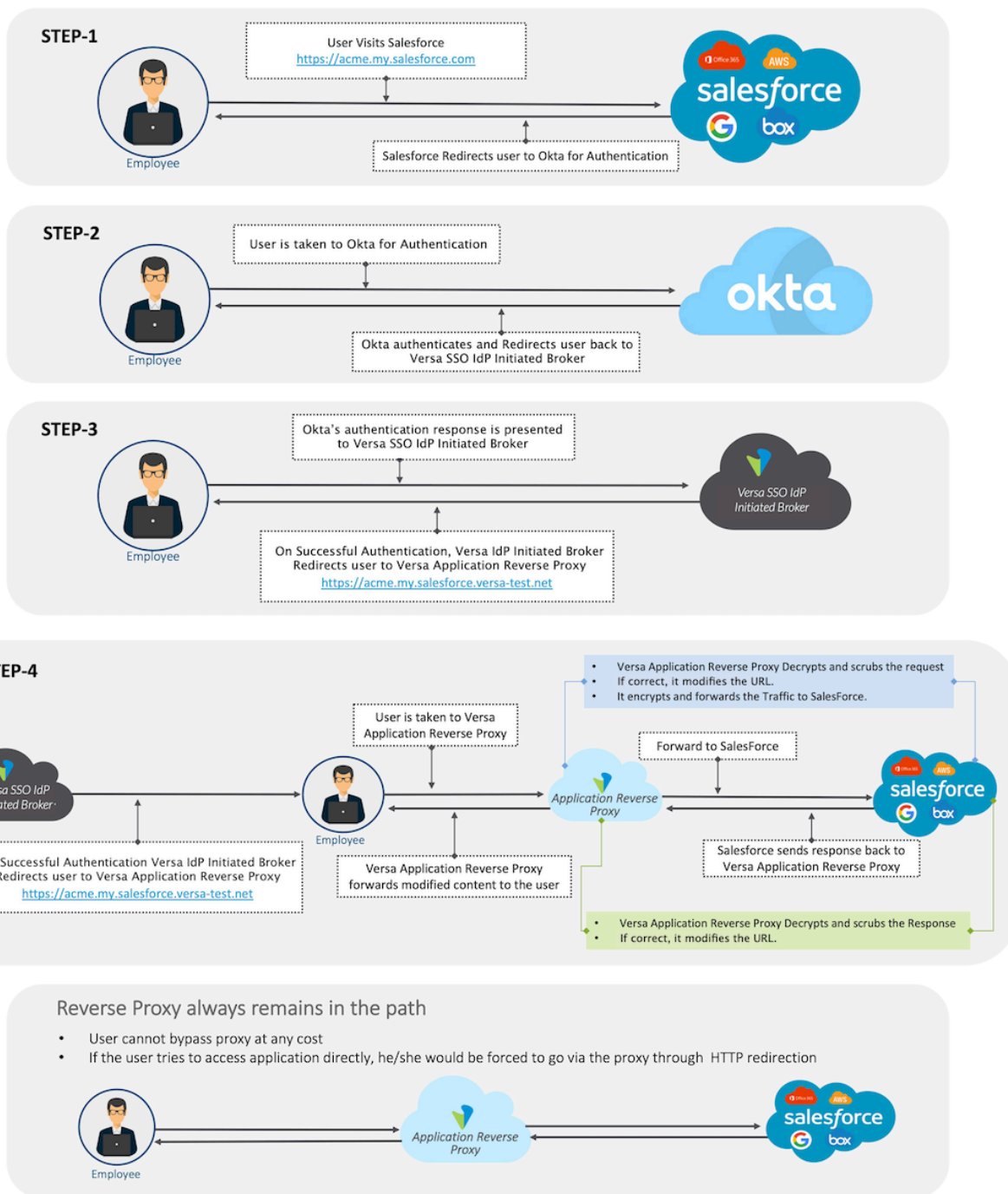
When you configure a SaaS application with single sign-on (SSO) through a third-party identity provider such as Azure AD, OneLogin, Okta, or PingIdentity, the Security Assertion Markup Language (SAML) directs the user to an identity provider (IdP) for user authentication. After the IdP authenticates the user, the IdP directs the traffic to application reverse proxy so that the proxy can enforce real-time protection policies applicable for that application for the user.

Versa supports both IdP-initiated and SaaS application-initiated reverse proxy flows.

IdP-initiated Flow

You configure the SaaS application to authenticate the user directly with the third-party IdP. When an endpoint accesses a SaaS application (such as `acme.box.com`), the SaaS provider (for example, `box.com`) redirects the endpoint to the IdP for SSO. After successful authentication, the IdP presents the SAML assertion to the Versa IdP broker (that is, the ACS URL points to Versa IdP broker). The result is that the Versa reverse proxy comes in the path to the SaaS application and enforces zero-trust network access (ZTNA), secure web gateway (SWG), cloud access security broker (CASB), data loss prevention (DLP), and other security features.

IdP Initiated Flow



SaaS Application-initiated Flow

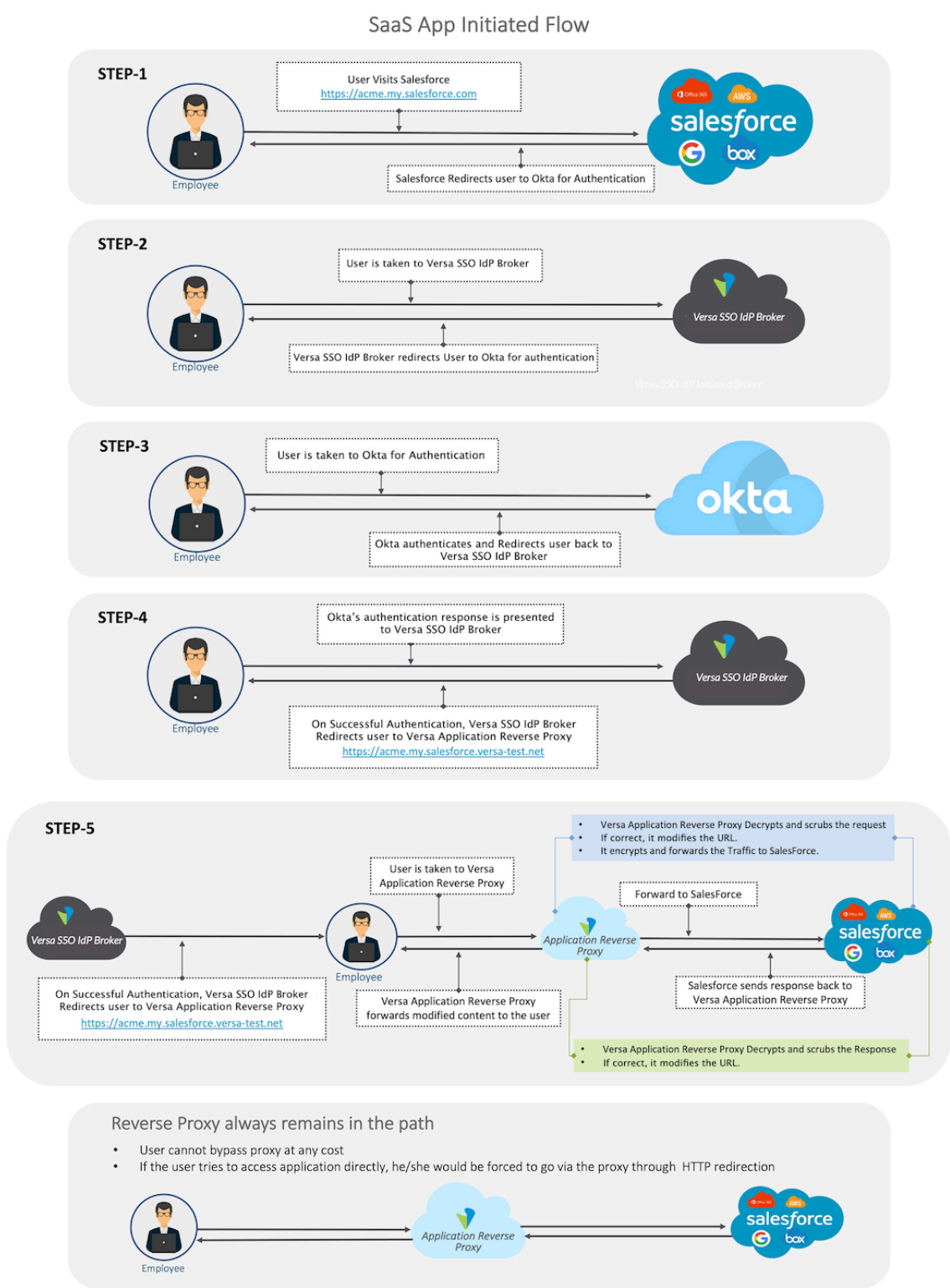
You configure SaaS application with Versa Cloud Gateway as the IdP. When an endpoint accesses a SaaS application (such as acme.box.com), the SaaS provider (for example, box.com) redirects the endpoint to Versa IdP broker, which, after applying policies, redirects the endpoint to endpoint's real IdP (such as Azure AD or Okta). After successful

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Director/Application_Reverse_Proxy/Co...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Director/Application_Reverse_Proxy/Co...)

Updated: Wed, 23 Oct 2024 08:44:22 GMT

Copyright © 2024, Versa Networks, Inc.




authentication by the endpoint's real IdP, the IdP presents an assertion to the Versa IdP broker, which ensures that the Versa reverse proxy remains in the path to SaaS application and enforces ZTNA, SWG, CASB, DLP and other security features.

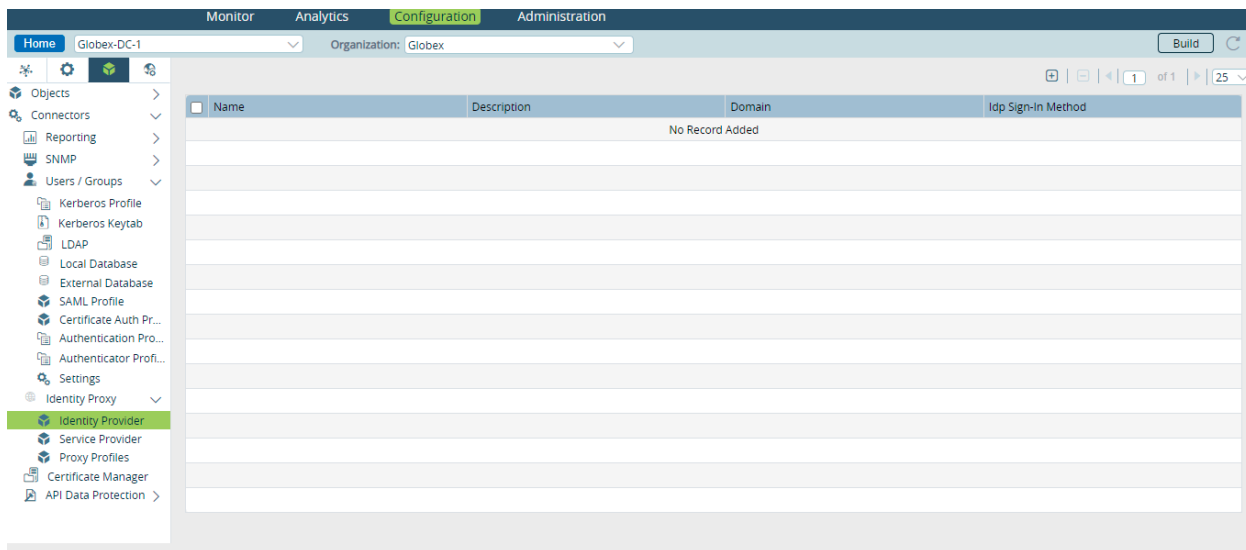



Configure Application Reverse Proxy

This section describes how to set up application reverse proxy to integrate with an IdP and a sanctioned SaaS application provider.

Configure Identity Provider

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 and Connectors  > Connectors  > Identity Proxy  > Identity Provider in the left menu bar.



4. Click the  Add icon to add identity provider details. In the Add Identity Provider popup window, enter information for the following fields.

Add Identity Provider

Name*

Description

Domain

Idp Sign-In Method

SAML

SAML Config

Login Url

Logout Url

Error Url

Forgot Password Url

Acs Url

Prefix

SAML Version

SAML 2.0

Saml Request Binding

HTTP-REDIRECT

Saml Response Binding

HTTP-POST

Entity Id

Certificate

Ca chain

Relay State

☐ Signed Request

☐ Signed Response

OK




Cancel

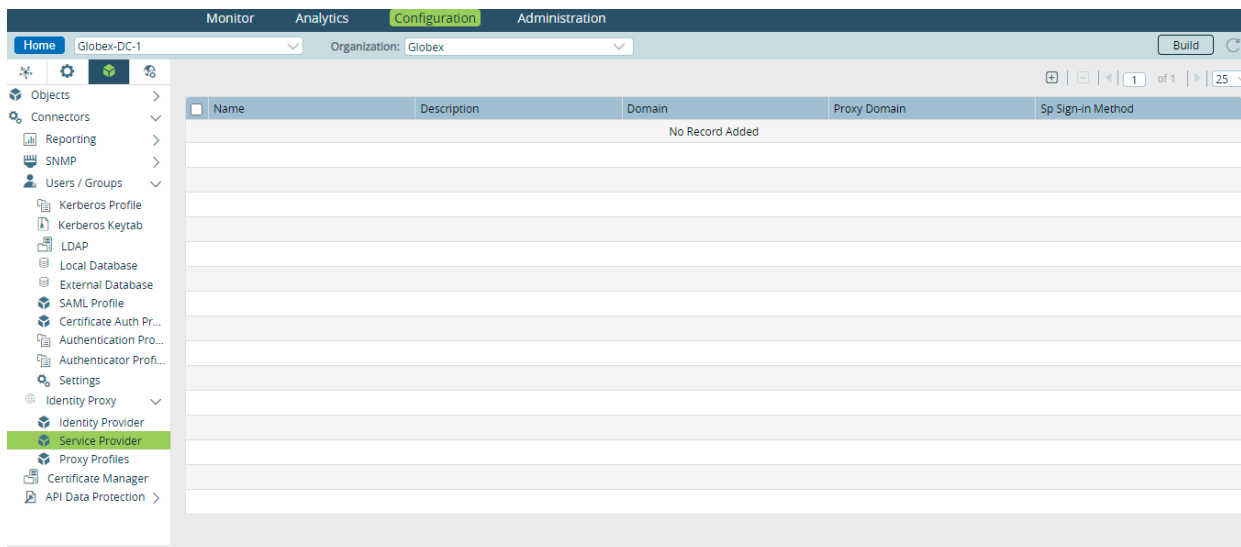
Field	Description
Name	Enter a name for the identity provider.
Description	Enter a text description for the identity provider.
Domain	Enter the domain name.
IdP Sign-In Method	Select the IdP sign in method.
SAML Config (Group of Fields)	
◦ Login URL	Enter the location to which to submit the SAML authentication request.
◦ Logout URL	Enter the location to which to send the log out response.
◦ Error URL	Enter the location to which to send the error response.
◦ Forgot Password URL	Enter the location to which to send the forgot password response.
◦ ACS URL	Enter the location to which to submit SAML assertion.
◦ Prefix	Enter the prefix to use in the request identifier.
◦ SAML Version	Select the SAML version.
◦ SAML Request Binding	Select the SAML request binding: <ul style="list-style-type: none"> ◦ HTTP Post ◦ HTTP Redirect
◦ SAML Respond Binding	Select the SAML response binding: <ul style="list-style-type: none"> ◦ HTTP Post ◦ HTTP Redirect
◦ Entity ID	Enter the entity ID.
◦ Certificate	Enter the certificate name for authentication.


◦ CA Chain	Enter the certificate authority (CA) chain for the server certificate.
◦ Relay State	Enter the default relay state value for IdP-initiated flow.
◦ Signed Request	Select if it is necessary to sign SAML authentication request.
◦ Signed Response	Select if it is necessary to sign SAML authentication response.

5. Click OK

Configure Service Provider

- In Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.
 - Select a device name in the main panel. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Objects and Connectors  > Connectors  > Identity Proxy  > Service Provider in the left menu bar.



- Click the  Add icon to add service provider details. In the Add Service Provider popup window, enter information for the following fields.

Add Service Provider

Name*

Description

Domain

Proxy Domain

Sp Sign-in Method

SAML

SAML Config

Login Url

Logout Url

Error Url

Forgot Password Url

Acs Url

Prefix

SAML Version

SAML 2.0

Saml Request Binding

HTTP-REDIRECT

Saml Response Binding

HTTP-POST

Entity Id

Certificate

Ca chain

Relay State

☐ Signed Request

☐ Signed Response

OK




Cancel

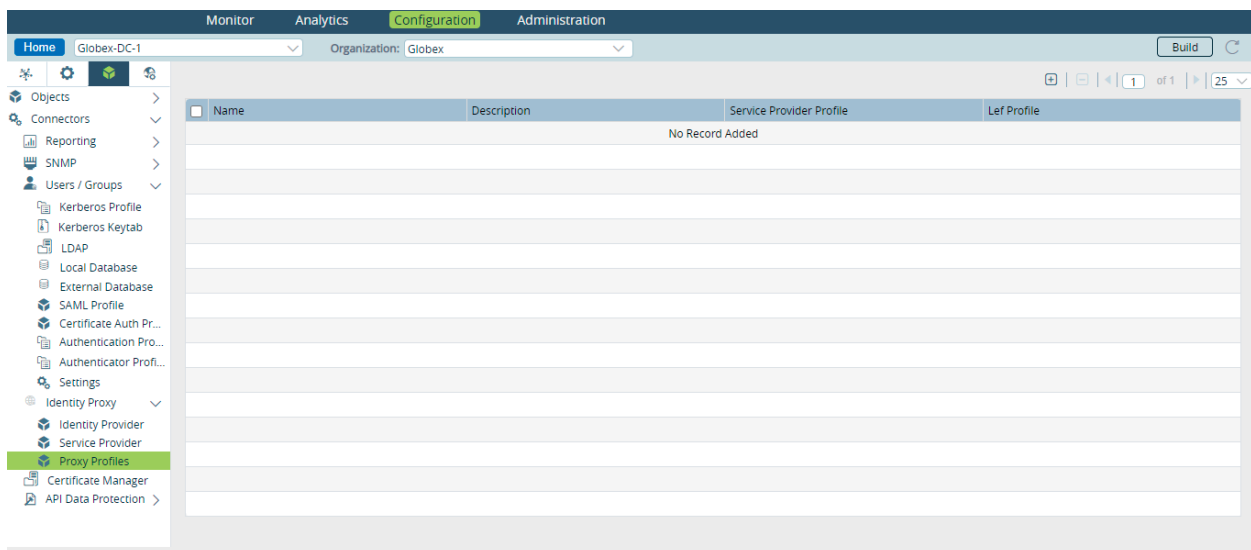
Field	Description
Name	Enter a name for the identity provider.
Description	Enter a text description for the identity provider.
Domain	Enter the domain name.
Proxy Domain	Enter a proxy domain name.
SP Sign In Method	Select the service provider sign in method.
SAML Config (Group of Fields)	
◦ Login URL	Enter the location to which to submit the SAML authentication request.
◦ Logout URL	Enter the location to which to send the log out response.
◦ Error URL	Enter the location to which to send the error response.
◦ Forgot Password URL	Enter the location to which to send the forgot password response.
◦ ACS URL	Enter the location to which to submit SAML assertion.
◦ Prefix	Enter the prefix to use in the request identifier.
◦ SAML Version	Select the SAML version.
◦ SAML Request Binding	Select the SAML request binding: <ul style="list-style-type: none"> ◦ HTTP Post ◦ HTTP Redirect
◦ SAML Respond Binding	Select the SAML response binding: <ul style="list-style-type: none"> ◦ HTTP Post ◦ HTTP Redirect
◦ Entity ID	Enter the entity ID.


◦ Certificate	Enter the certificate name for authentication.
◦ CA Chain	Enter the certificate authority (CA) chain for the server certificate.
◦ Relay State	Enter the default relay state value for IdP-initiated flow.
◦ Signed Request	Select if it is necessary to sign SAML authentication request.
◦ Signed Response	Select if it is necessary to sign SAML authentication response.

5. Click OK

Configure Proxy Profiles

- In Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.
 - Select a device name in the main panel. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Objects and Connectors  > Connectors  > Identity Proxy  > Proxy Profiles in the left menu bar.



- Click the  Add icon to add proxy profiles details. Select the General tab, and then enter information for the following fields.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Director/Application_Reverse_Proxy/Co...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Director/Application_Reverse_Proxy/Co...)

Updated: Wed, 23 Oct 2024 08:44:22 GMT

Copyright © 2024, Versa Networks, Inc.

Add Proxy Profiles

General Rules

Name *

Description

Service Provider Profile ---Please Select---

Lef Profile ---Please Select---

Default Action

Mode ---Please Select---

Authentication Profile ---Please Select---

Identity Provider Profile ---Please Select---

OK Cancel

Field	Description
Name	Enter a name for the proxy profile.
Description	Enter a text description for the proxy profile.
Service Provider Profile	Select a service provider profile
LEF Profile	Select a log export functionality (LEF) profile to use to capture logs for the proxy profile.
Default Action (Group of Fields)	
<ul style="list-style-type: none"> Mode 	Select a mode: <ul style="list-style-type: none"> Proxy Service
<ul style="list-style-type: none"> Authentication Profile 	If you select service, select an authentication profile.
<ul style="list-style-type: none"> Identity Provider Profile 	If you select proxy mode, select an identity provider profile.

5. Select the Rules tab, and then click the Add icon to add a proxy profile rule.

6. In the Add Rule popup window, enter information for the following fields.

Field	Description
Name	Enter a name for the rules profile.
Description	Enter a description for the rules profile.
Type	Select the rule type: <ul style="list-style-type: none"> ◦ Request ◦ Response

7. For the Request rule type, select the Match tab, and then enter information for the following fields.

Add Rule

Name *

Description

Type

Request

Match

Set

Geo Location

---Please Select---

+

No Records to Display

Devices

+

No Records to Display

Users

+

No Records to Display

Groups



+

No Records to Display

OK

Cancel

Field	Description
Geolocation	Select the geographic location, and then click the <div>+</div> Add icon.
Devices	Enter the device name, and then click the <div>+</div> Add icon.

Field	Description
Users	Enter the username, and then click the  Add icon.
Groups	Enter the group name, and then click the  Add icon.

8. Select the Set tab, and then enter information for the following fields.

Add Rule
×

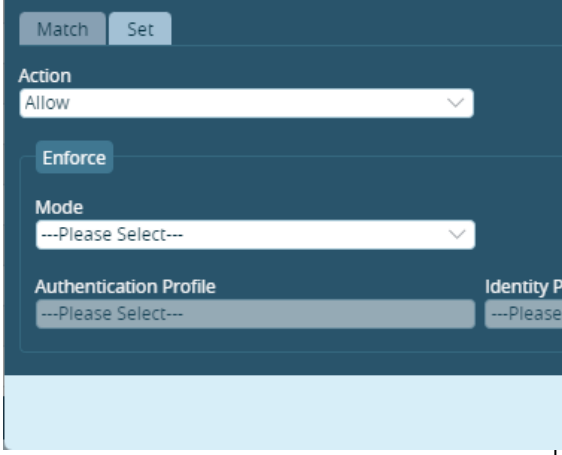
Name*

Description
Type
Request

Match
Set

Action
---Please Select---

OK
Cancel

Field	Description
Action	<p>Select an action:</p> <ul style="list-style-type: none"> ◦ Allow—select the mode: <ul style="list-style-type: none"> ▪ Proxy—Select proxy mode and then select an identity provider profile. ▪ Service—Select service mode and then select an authentication profile.  <ul style="list-style-type: none"> ◦ Deny

9. Click OK.

10. For a Response rule type, select the Match tab, and then enter information for the following fields.

Add Rule

Name*

Description

Type

Response

Match

Set

Geo Location

---Please Select---

+

No Records to Display

Devices

+

No Records to Display

Users

+

No Records to Display





Groups

+

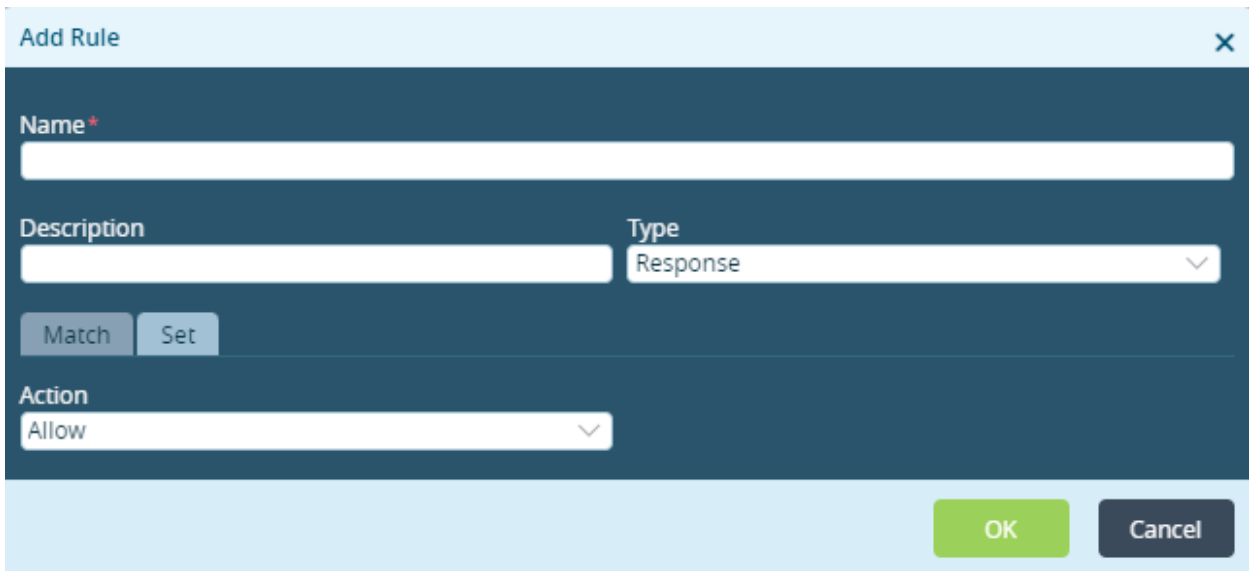
No Records to Display

OK

Cancel

Field	Description
Geolocation	Select the geographic location, and then click the  Add icon.
Devices	Enter the device name, and then click the  Add icon.
Users	Enter the username, and then click the  Add icon.
Groups	Enter the group name, and then click the  Add icon.

11. Select the Set tab, and then select an action.



12. Click OK.

Supported Software Information

Releases 21.2.3 and later support all content described in this article.

Additional Information

[Configure Single Sign-On Using Director](#)

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Director/Application_Reverse_Proxy/Co...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Director/Application_Reverse_Proxy/Co...)

Updated: Wed, 23 Oct 2024 08:44:22 GMT

Copyright © 2024, Versa Networks, Inc.