
Configure Versa Secure Access Objects

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

In secure access gateway or portal policy rules, you can use predefined or custom operating system (OS) or endpoint objects to secure end user connections.

Configure OS Objects

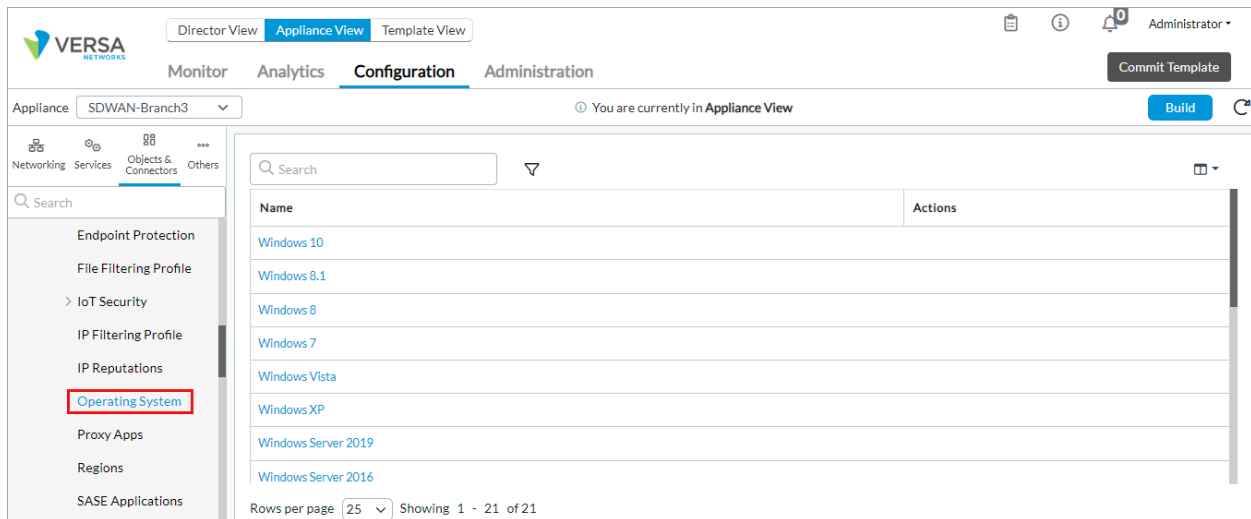
You can use predefined operating system (OS) objects or create custom OS objects and associate these objects with secure access gateway or portal policy rules. For more information, see [Add a Secure Access Gateway Policy Rule](#) and [Add a Secure Access Portal Policy Rule](#).

View Predefined OS Objects

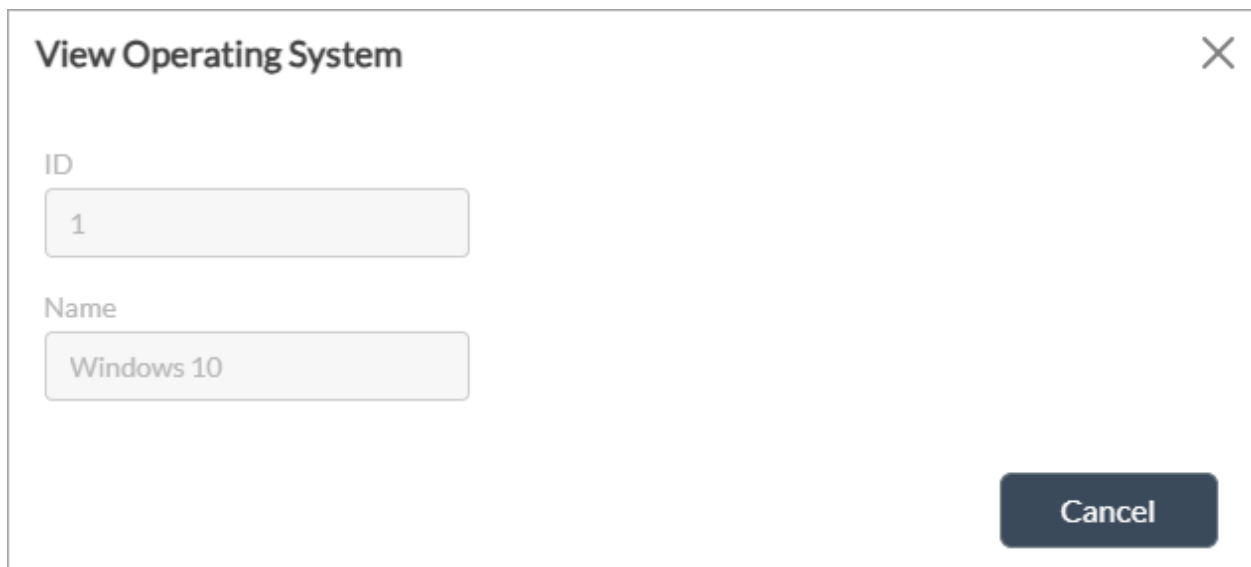
Versa Director provides predefined OS objects, including multiple versions of Android, MacOS, and Windows, that you can use as matches in secure access policy rules.

To view the predefined OS objects:

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 pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Predefined > Operating System in the left menu bar. The main pane displays the predefined OS objects.



4. Click an OS object to view its name and identifier.



Add Custom OS Objects

You can create custom OS objects to use in secure access policy rules. You may want to do this when the OS running on an end-user device is not included in the predefined OS objects.

You can create OS objects as one of the following:

- Predefined OS object and OS version number
- Pattern entered as a regular expression (regex)

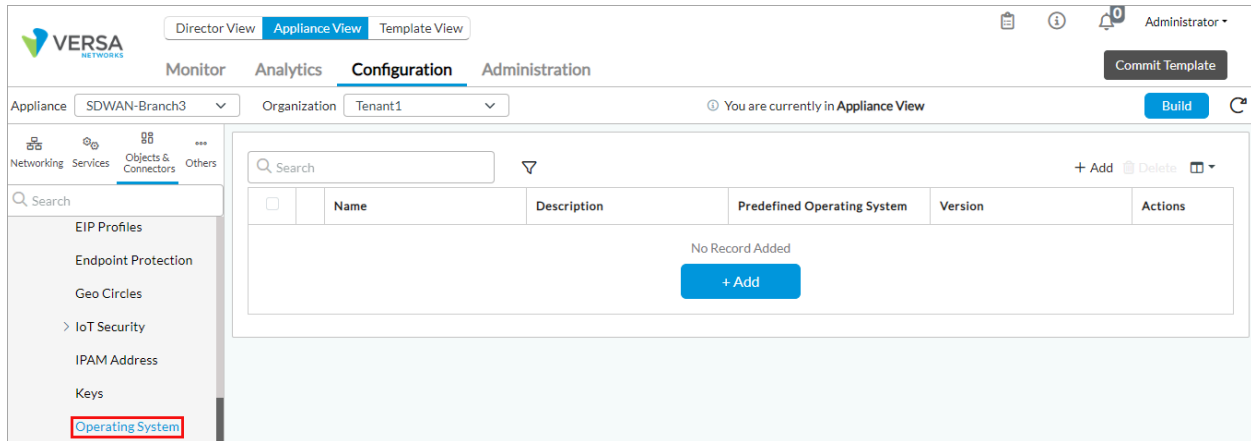
To add a custom OS object:


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

Updated: Wed, 23 Oct 2024 08:43:34 GMT

Copyright © 2024, Versa Networks, Inc.

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 pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > Operating System in the left menu bar.




4. Click the  Add icon to add a custom OS object. In the Add Operating System popup window, enter information for the following fields.

The 'Add Operating System' popup window contains the following fields:

- Name ***: A text input field.
- Description**: A text input field.
- Pattern**: A text input field with a dropdown arrow and a '+ Add' button.
- Predefined Operating Systems**: A dropdown menu with the option '---Please Select---'.
- Build Versions**: A text input field.
- Security Package Versions**: A text input field.
- Versions**: A text input field.

At the bottom of the window, there are 'OK' and 'Cancel' buttons.

Field	Description
Name (Required)	Enter a name for the OS object.
Description	Enter a text description for the OS object.
Pattern	<p>Click to enter a pattern to match the OS object, and then click the  Add icon to enter the pattern. Enter the pattern using the syntax <i>/regex/regex-options</i>. In this field, you can use the standard Perl-compatible regular expression (PCRE) pattern <i>i</i>, to indicate a case-insensitive match). You cannot use other PCRE patterns.</p> <p>For example, to match any Windows version, enter the pattern <i>/windows/i</i>, where <i>i</i> ignores the case. This pattern matches a query for Windows regardless of the case, matching, for example, windows, Windows, and WINDOWS.</p> <p>If you enter a pattern, you cannot also select a value in the Predefined Operating Systems field.</p>
Predefined Operating Systems	<p>Select a predefined OS object to match:</p> <ul style="list-style-type: none"> ◦ Android ◦ Fedora ◦ MacOS ◦ MacOS X ◦ MacOS X Server ◦ RedHat Enterprise Linux ◦ Ubuntu ◦ Windows 7 ◦ Windows 8 ◦ Windows 8.1 ◦ Windows 10 ◦ Windows 10 Mobile ◦ Windows Server 2012 ◦ Windows Server 2012 R2

	<ul style="list-style-type: none"> ◦ Windows Server 2016 ◦ Windows Server 2019 ◦ Windows Vista ◦ Windows XP <p>If you select a value in the Predefined Operating Systems field, you cannot also enter a pattern in the Pattern field.</p>
Build Versions	Enter a build version for the OS object. The version can be a single version, a range of versions, or a comma-separated list of versions. For syntax examples, see the description of the Versions field, below.
Security Package Versions	Enter the security package version of the OS object. The version can be a single version, a range of versions, or a comma-separated list of versions. For syntax examples, see the description of the Versions field, below.
Versions	<p>Enter the version of the OS object that you selected in the Security Package Versions field. The version can be a single version, a range of versions, or a comma-separated list of versions, using the syntax in the following examples:</p> <ul style="list-style-type: none"> ◦ Example of a single-version <ul style="list-style-type: none"> ▪ 10.0 ◦ Examples of ranges <ul style="list-style-type: none"> ▪ 10-15 (version 10 through 15) ▪ 10.2-15 (version 10.2 through 15) ▪ 10.2.2-15 (version 10.2.2 through 15) ▪ 10.2-15.2 (version 10.2 through 15.2) ▪ 10.2.2- (versions 10.2.2 and later) ▪ 10.2- (versions 10.2 and later) ▪ -10.2 (versions prior to 10.2) ▪ -10 (versions prior to 10) ◦ Examples of comma-separated lists <ul style="list-style-type: none"> ▪ 10, 11, 12, 13, 16 ▪ 10.2, 10.3, 10.6 ▪ 10.2, 10.3.5, 12.2-18, 20- (10.2,10.3.5, 12.2 through 18, and 20 and later)

5. Click OK.

Configure Endpoint-Protection Objects

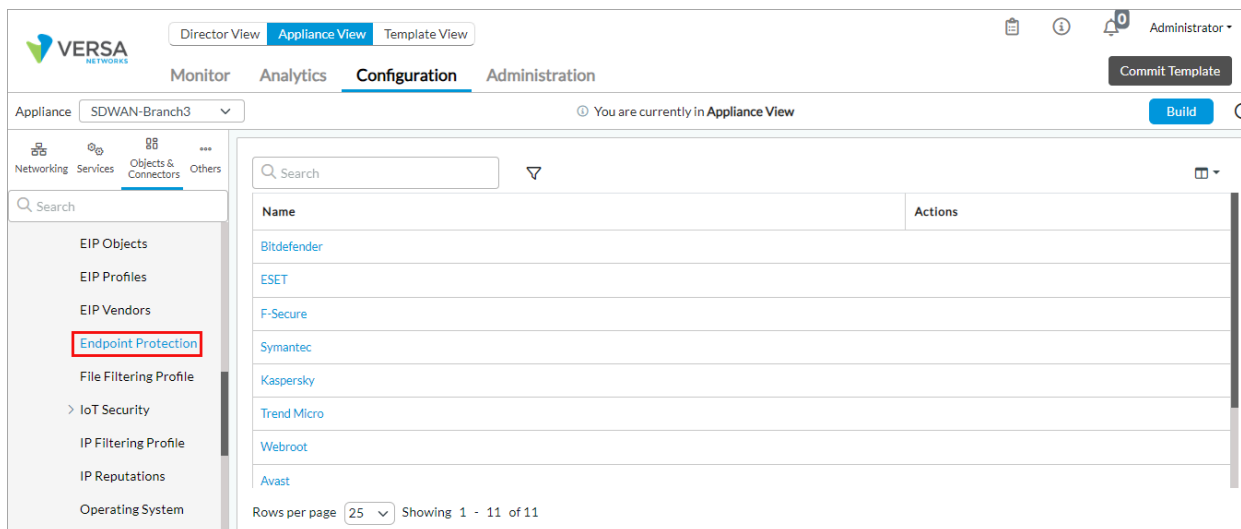
Endpoint protection ensures that the connection of endpoint devices such as laptops, tablets, mobile phones, internet-of-things (IoT) devices, and other wireless devices to an enterprise network is secure. In secure access gateway or portal policy rules, you can use predefined endpoint-protection objects or you can create custom endpoint-protection objects. An endpoint-protection object is the name of an endpoint protection provider, such as Avast, Kaspersky, and McAfee. For more information, see [Add a Secure Access Gateway Policy Rule](#) and [Add a Secure Access Portal Policy Rule](#) in [Configure the Versa Secure Access Service](#).

View Predefined Endpoint-Protection Objects

Versa Director provides predefined endpoint-protection objects, such as Avast, Kaspersky, and McAfee, that you can use to match in secure access policy rules.

To view predefined endpoint-protection objects:

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 > Objects > Predefined > Endpoint Protection in the left menu bar to view the list of predefined endpoint-protection objects.



4. Click an endpoint-protection object to view its name and identifier.

View Endpoint Protection

ID

4

Name

Symantec

Cancel

Add Custom Endpoint-Protection Objects

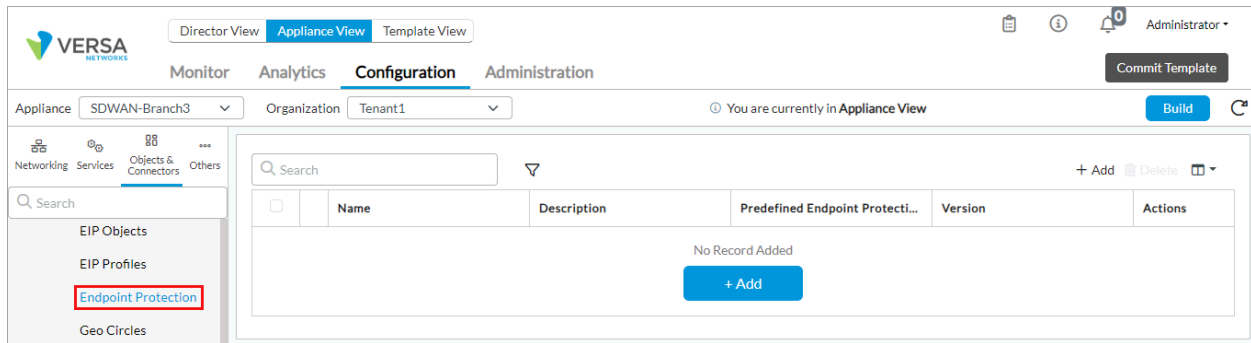
You can create custom endpoint-protection objects to use in secure access policy rules. You may want to do this when the endpoints or entry points of end-user devices you are using are not included in the list of predefined endpoint-protection objects.

You can create endpoint-protection objects as one of the following:

- Predefined endpoint-protection object and endpoint object version number
- Pattern entered as regular expression (regex)
- Predefined endpoint protection with software version number and virus definition number; for example, McAfee software version 8.0.0 and virus definition 4558.

To add a custom endpoint-protection object:

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 > Objects > Custom Objects > Endpoint Protection in the left menu bar.



- Click the + Add icon to add a custom endpoint-protection object. In the Add Endpoint Protection window, enter information for the following fields.

Add Endpoint Protection

Name *

Description

Predefined Endpoint Protection

---Please Select---

Update Versions

Versions

Pattern


+

No Records to Display

OK

Cancel

Field	Description
Name (Required)	Enter a name for the endpoint-protection object.
Description	Enter a text description for the endpoint-protection object.
Predefined Endpoint Protection	<p>Select a predefined endpoint-protection object:</p> <ul style="list-style-type: none"> ◦ Avast ◦ Bitdefender ◦ ESET ◦ F-secure ◦ Kaspersky ◦ McAfee ◦ Panda ◦ Symantec ◦ Trend Micro ◦ Webroot ◦ Windows Defender <p>If you select a value in the Predefined Endpoint Protection field, you cannot also enter a pattern in the Pattern field.</p>
Update Versions	Enter the virus update version of the endpoint-protection object. For example, if you selected McAfee, the update version can be 4558. The version can be a single version, a range of versions, or a comma-separated list of versions. For syntax examples, see the description of the Versions field, below.
Versions	<p>Enter the version of the endpoint-protection object that you selected in the Update Versions field. The version can be a single value, a range of values, or a comma-separated list of values, using the syntax in the following examples:</p> <ul style="list-style-type: none"> ◦ Example of a single version <ul style="list-style-type: none"> ▪ 10.0 ◦ Examples of ranges

	<ul style="list-style-type: none"> ▪ 10-15 (version 10 through 15) ▪ 10.2-15 (version 10.2 through 15) ▪ 10.2.2-15 (version 10.2.2 through 15) ▪ 10.2-15.2 (version 10.2 through 15.2) ▪ 10.2.2- (versions 10.2.2 and later) ▪ 10.2- (versions 10.2 and later) ▪ -10.2 (versions prior to 10.2) ▪ -10 (versions prior to 10) ◦ Examples of comma-separated lists <ul style="list-style-type: none"> ▪ 0, 11, 12, 13, 16 ▪ 10.2, 10.3, 10.6 ▪ 10.2, 10.3.5, 12.2-18, 20- (10.2,10.3.5, 12.2 through 18, and 20 and later)
Pattern	<p>Click to enter a pattern to match the endpoint-protection object, and then click the  Add icon to enter the pattern. Enter the pattern using the syntax <i>/regex/regex-options</i>. In this field, you can use the standard PCRE pattern <i>i</i>, to indicate a case-insensitive match). You cannot use other PCRE patterns.</p> <p>For example, to match any webroot version, enter the pattern <i>/webroot/i</i>, where <i>i</i> ignores the case. This pattern matches a query for webroot regardless of the case, matching, for example, webroot, Webroot, and WEBROOT.</p> <p>If you enter a pattern, you cannot also select a value in the Predefined Endpoint Protection field.</p>

5. Click OK.

Supported Software Information

Releases 21.2.1 and later support all content described in this article.

Additional Information

[Configure the Versa Secure Access Service](#)

[Configure Versa SASE Clients](#)