

---

## Configure Endpoint Information Profiles

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

Enterprise users can connect to the enterprise's networks and resources from a variety of locations and using a variety of endpoints, or remote computing devices, including smartphones, laptops, desktops, tablets, and internet-of things (IoT) devices. Endpoint devices represent vulnerable points of entry, places where attackers can attempt to infiltrate the enterprise network or exploit vulnerabilities.

To protect the enterprise network and resources, you can create endpoint information profiles (EIPs), which ensure that the endpoint devices that access the enterprise network maintain and adhere to enterprise security standards before they access enterprise network resources. With EIPs, you collect information about the security status of the endpoint devices connecting to your networks, such as whether they have the latest security patches and antivirus definitions installed. You then classify endpoints based on multiple types endpoint posture information, defining rules that allow the VOS SASE software to extract information from endpoint devices and then match the information to enforce security policy. You can configure notifications that alert users about the reason for access denial and that allow users to access the installation program for missing encryption software.

Concerto EIP allows you to classify EIP information into the following security-related categories:

- Antimalware
- Antiphishing
- Browser
- Cloud storage
- Custom
- Data loss prevention
- Disk backup
- Disk encryption
- Firewall
- General
- Health agent
- Management status
- Messenger
- Patch management
- Public file sharing

- Remote control
- Virtual machine

To configure EIP, you create three building blocks for each tenant:

- EIP profiles—Collect the EIP objects, which are the match criteria, into a profile that is evaluated together for monitoring and for enforcing security policy for SASE portals and gateways.
- EIP agent profile—Define the conditions that the SASE client uses to filter information from endpoint devices. When you configure a SASE portal policy, you associate the agent profile with the enforcement action in the policy.
- EIP objects—Define the match criteria to use in an EIP profile. The match criteria filter the raw data reported by endpoint devices.

After registration of endpoint devices, the SASE client collects device information based on the EIP agent profile associated with the SASE portal policy and reports this information to the SASE gateway. The gateway evaluates the information and enforces the associated security policy. For example, you can create an EIP agent profile to verify if endpoint devices have installed the mandatory antivirus software. If the SASE client finds a device that has not installed the mandatory software, it does not allow the user to connect to the enterprise network and displays a message to install the software.

The frequency of how often the client collects and reports data depends on the posture check interval configured in the secure access profile.

This article describes how to:

- View predefined EIP objects and to configure custom EIP objects.
- View predefined EIP profiles, to configure custom EIP profiles, and to use EIP objects to configure EIP profile rules.
- View predefined EIP agents and to configure custom EIP objects.
- Associate an EIP profile with secure service edge rules.
- Associate an EIP agent profile with an SCA rule.

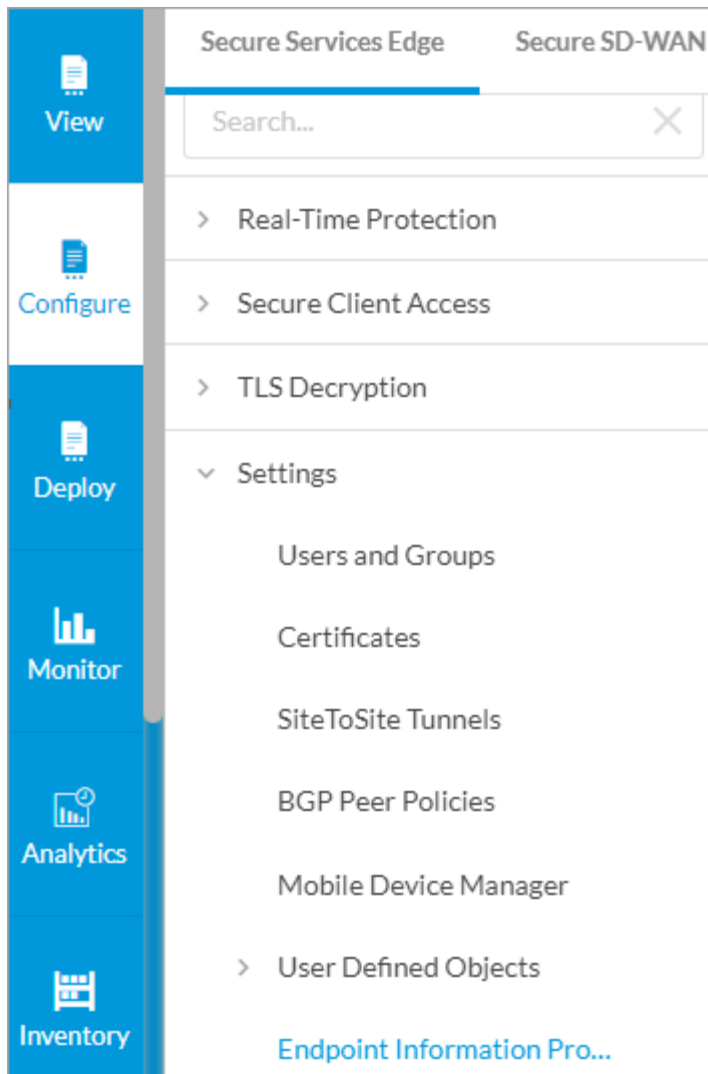
---

## View Predefined EIP Objects

Concerto supports predefined EIP objects that you can use to define rules associated with EIP profiles.

To view predefined EIP objects:

1. Go to Configure > Settings > End Information Profile.



2. Select the EIP Objects tab and then select the Predefined tab to view the predefined EIP objects that Concerto supports. The table displays the name, description, category, and details of the object.

Configure > SASE > Settings > Endpoint Information Profile (EIP) > Predefined EIP Objects

**Publish**

EIP Profiles **EIP Objects** EIP Agents

User Defined **Predefined**

Search by keyword or name | Filter Refresh Select Columns

OBJECT NAME	DESCRIPTION	CATEGORY	OBJECT DETAILS
elip-object-antimalware-any-installed	Any antimalware software installed	AntiMalware	Installed: True
elip-object-antimalware-any-running	Any antimalware software installed and running	AntiMalware	Installed: True Running: True
elip-object-antimalware-vendor-avast	EIP object associated with Avast antimalware software	AntiMalware	Vendor: AVAST Software a.s. Product: Avast Premium Security
elip-object-antimalware-vendor-bitdefender	EIP object associated with Bitdefender antimalware software	AntiMalware	Vendor: Bitdefender
elip-object-antimalware-vendor-eset	EIP object associated with ESET antimalware software	AntiMalware	Vendor: ESET

- To customize which columns display, click Select Columns down arrow and then click the columns to select or deselect the ones you want to display. Click Reset to return to the default column display settings.

## Configure a Custom EIP Object

You can use EIP objects to define rules associated with EIP profiles.

To configure a custom EIP object:

- Go to Configure > Settings > End Information Profile.
- Select the EIP Objects tab and then select the User Defined tab.

EIP Profiles **EIP Objects** EIP Agents

**User Defined** Predefined

Search by keyword or name | Filter + Add Clone Delete Refresh Select Columns

OBJECT NAME	DESCRIPTION	CATEGORY	OBJECT DETAILS
<input type="checkbox"/> AntiMalware-Object		AntiMalware	Installed: Disabled Configured: True Running: True Realtime: disabled
<input type="checkbox"/> AntiPhishing		Antiphishing	Category: Antiphishing Installed: True Configured: True Running: Disabled

- To customize which columns display, click Select Columns down arrow, and then click the columns to select or deselect the ones you want to display. Click Reset to return to the default column display settings.

Select Columns

☒
Description

☒
Category

☒
Object Details

Reset

4. Click + Add to add a new EPS object. The Add EIP Object screen displays. Enter information for the following fields.

Add EIP Object

Name\*

Description

Category

-- Select --

Cancel

Add

Field	Description
Name	Enter a name for the EIP object.
Description	Enter a text description for the EIP object.
Category	Select the EIP category. There are 17 categories, and each EIP object belongs to only one category. The name of the field changes depending on the value you select in the category field.

5. For each EIP object, enter information in the following fields to configure when the SASE client should filter the object.

Field	Description
Antimalware	<p>Configure when the SASE client should validate information related to antimalware security. By default, all information extraction is disabled.</p> <div> <div>Add EIP Object</div> <div> <div>Name*</div> <div></div> </div> <div> <div>Description</div> <div></div> </div> <div> <div>Category</div> <div>AntiMalware ▾</div> </div> <div> <div> <div>Installed</div> <div><input type="checkbox"/> No</div> </div> <div> <div>Configured</div> <div><input type="checkbox"/> No</div> </div> <div> <div>Running</div> <div><input type="checkbox"/> No</div> </div> <div> <div>Realtime</div> <div><input type="checkbox"/> No</div> </div> </div> <div> <div>Last Definition Update Time(in hours)</div> <div></div> </div> <div> <div>Last Engine Update Time(in hours)</div> <div></div> </div> <div> <div>Last Scan Time(in hours)</div> <div></div> </div> <div> <div>Vendor</div> <div>Search for Vendor</div> </div> <div> <div>Product</div> <div>Search for Product</div> </div> <div> <div>Major</div> <div> <input checked="" type="radio"/> Disabled <input type="radio"/> Value <input type="radio"/> Range </div> </div> <div> <div>Minor</div> <div> <input checked="" type="radio"/> Disabled <input type="radio"/> Value <input type="radio"/> Range </div> </div> <div> <div>Service</div> <div> <input checked="" type="radio"/> Disabled <input type="radio"/> Value <input type="radio"/> Range </div> </div> <div> <div>Patch</div> <div> <input checked="" type="radio"/> Disabled <input type="radio"/> Value <input type="radio"/> Range </div> </div> <div> <div>Cancel</div> <div>Add</div> </div> </div>
<ul style="list-style-type: none"> <li>◦ Configured</li> <li>◦ Installed</li> <li>◦ Running</li> <li>◦ Real Time</li> </ul>	<p>Whether to match the antimalware software configuration, installation, or running status, or real-time information:</p> <ul style="list-style-type: none"> <li>◦ Disabled—Perform no validation. This is the default.</li> <li>◦ False—Perform validation, and if the endpoint</li> </ul>



	<p>reports the status as False, the match is successful.</p> <ul style="list-style-type: none"> <li>◦ True—Perform validation, and if the endpoint reports the status as True, the match is successful.</li> </ul>
◦ Last Definition Update Time	<p>Enter how often to validate the last definition update time of the antimalware software, in hours.</p> <ul style="list-style-type: none"> <li>◦ <i>Range:</i> 1 through 65535 hours</li> <li>◦ <i>Default:</i> 0</li> </ul>
◦ Last Engine Update Time	<p>Enter how often to validate the last engine update time of the antimalware software, in hours.</p> <ul style="list-style-type: none"> <li>◦ <i>Range:</i> 1 through 65535 hours</li> <li>◦ <i>Default:</i> 0</li> </ul>
◦ Last Scan Time	<p>Enter how often to validate the last scan time of the antimalware software, in minutes.</p> <ul style="list-style-type: none"> <li>◦ <i>Range:</i> 1 through 65535 minutes</li> <li>◦ <i>Default:</i> 0</li> </ul>
◦ Vendor	Select the antimalware software vendor name.
◦ Product	Select the antimalware software product name. When you select the product name, the Major field is enabled.
◦ Major	<p>Whether to validate</p> <ul style="list-style-type: none"> <li>◦ Disabled—Click to not validate the major software version. This is the default.</li> <li>◦ Range—Click and then select a range for the major software version.</li> <li>◦ Value—Click and then select a value for the major software version.</li> </ul>
◦ Minor	<p>Whether to validate the minor version of the antimalware software installed on the SASE client. When you select the minor version, the Service field is enabled.</p> <ul style="list-style-type: none"> <li>◦ Disabled—Click to not validate the minor software version. This is the default.</li> </ul>

	<ul style="list-style-type: none"> <li>◦ Range—Click and then select a range for the minor software version.</li> <li>◦ Value—Click and then select a value for the minor software version.</li> </ul>
<ul style="list-style-type: none"> <li>◦ Service</li> </ul>	<p>Whether to validate the antimalware software service number on the SASE client. After you select the service, the Patch field is enabled.</p> <ul style="list-style-type: none"> <li>◦ Disabled—Click to not validate the software service number. This is the default.</li> <li>◦ Range—Click and then select a range for the service software number.</li> <li>◦ Value—Click and then select a value for the service software number.</li> </ul>
<ul style="list-style-type: none"> <li>◦ Patch</li> </ul>	<p>Whether to validate the latest patch number available for the antimalware software package.</p> <ul style="list-style-type: none"> <li>◦ Disabled—Click to not validate the latest patch number. This is the default.</li> <li>◦ Range—Click and then select a range for the latest patch number.</li> <li>◦ Value—Click and then select a value for the latest patch number.</li> </ul>
Antiphishing Browser Cloud storage Data loss prevention Disk backup Disk encryption Firewall Health agent Messenger	<p>Configure when the SASE client should filter information related to EIP security. By default, all information extraction is disabled.</p>



<p>Patch management</p> <p>Public file sharing</p> <p>Remote control</p> <p>Virtual machine</p>	<div data-bbox="857 210 1624 1047"> <h3>Add EIP Object</h3> <p>Name*</p> <input type="text"/> <p>Description</p> <input type="text"/> <p>Category</p> <div>Antiphishing</div> <div> <div> <div>Installed</div> <div><input type="radio"/> No</div> </div> <div> <div>Configured</div> <div><input type="radio"/> No</div> </div> <div> <div>Running</div> <div><input type="radio"/> No</div> </div> </div> <div> <div>Vendor</div> <div>Search for Vendor</div> </div> <div> <div>Product</div> <div>Search for Product</div> </div> <div> <div>Major</div> <div> <input checked="" type="radio"/> Disabled <input type="radio"/> Value <input type="radio"/> Range </div> </div> <div> <div>Minor</div> <div> <input checked="" type="radio"/> Disabled <input type="radio"/> Value <input type="radio"/> Range </div> </div> <div> <div>Service</div> <div> <input checked="" type="radio"/> Disabled <input type="radio"/> Value <input type="radio"/> Range </div> </div> <div> <div>Patch</div> <div> <input checked="" type="radio"/> Disabled <input type="radio"/> Value <input type="radio"/> Range </div> </div> <div> <div>Cancel</div> <div>Add</div> </div> </div>
<ul style="list-style-type: none"> <li>Configured</li> <li>Installed</li> <li>Running</li> </ul>	<p>Whether to match the configuration, installation, or running status of the selected security software:</p> <ul style="list-style-type: none"> <li>Disabled—Perform no validation. This is the default.</li> <li>False—Perform validation, and if the endpoint reports the status as False, the match is successful.</li> <li>True—Perform validation, and if the endpoint reports the status as True, the match is successful.</li> </ul>
<ul style="list-style-type: none"> <li>Vendor</li> </ul>	<p>Select the security software vendor name.</p>
<ul style="list-style-type: none"> <li>Product</li> </ul>	<p>Select the security software product name of the software. When you select the product name, the Major field is enabled.</p>
<ul style="list-style-type: none"> <li>Major</li> </ul>	<p>Whether to validate the major version of the security</p>

	<p>software installed on the SASE client. When you select the major version, the Minor field is enabled.</p> <ul style="list-style-type: none"> <li>◦ Disabled—Click to not validate the major software version. This is the default.</li> <li>◦ Range—Click and then select a range for the major software version.</li> <li>◦ Value—Click and then select a value for the major software version.</li> </ul>
◦ Minor	<p>Whether to validate the minor version of the security software installed on the SASE client. When you select the minor version, the Service field is enabled.</p> <ul style="list-style-type: none"> <li>◦ Disabled—Click to not validate the minor software version. This is the default.</li> <li>◦ Range—Click and then select a range for the minor software version.</li> <li>◦ Value—Click and then select a value for the minor software version.</li> </ul>
◦ Service	<p>Whether to validate the security software service number on the SASE client. When you select the service, the Patch field is enabled.</p> <ul style="list-style-type: none"> <li>◦ Disabled—Click to not validate the software service number. This is the default.</li> <li>◦ Range—Click and then select a range for the service software number.</li> <li>◦ Value—Click and then select a value for the service software number.</li> </ul>
◦ Patch	<p>Whether to validate the latest patch number available for the security software package.</p> <ul style="list-style-type: none"> <li>◦ Disabled—Click to not validate the latest patch number. This is the default.</li> <li>◦ Range—Click and then select a range for the latest patch number.</li> <li>◦ Value—Click and then select a value for the latest patch number.</li> </ul>

Custom	<p>Configure when the SASE client should filter information related to custom security. By default, all information extraction is disabled.</p> <div data-bbox="860 399 1518 1165"> <p><b>Add EIP Object</b></p> <p>Name*</p> <input type="text"/> <p>Description</p> <input type="text"/> <p>Category</p> <div>Custom ▾</div> <p>Windows Files</p> <p>Absolute Path Of The File</p> <div> <input type="text"/> <span>−</span> <span>+</span> </div> <p>Windows Registry</p> <div> <p>Registry Path (Including Key)</p> <input type="text"/> <p>Value</p> <input type="text"/> </div> <div> <span>Cancel</span> <span>Add</span> </div> </div>
<ul style="list-style-type: none"> <li>Windows Files</li> </ul>	<p>Enter the absolute path of a Windows file to determine whether the file is present on the end device, for example, C:\Windows\System32\drivers\fileinfo.sys.</p> <p>Click the  Add icon to add another row.</p>
<ul style="list-style-type: none"> <li>Windows Registry</li> </ul>	<p>Enter the absolute path of a registry to determine the value of the registry on the end device, for example, HKEY_LOCAL_MACHINE\SYSTEM\State\DateTime\</p> <p>NTP Enabled. Click the  Add icon to add another row.</p>
General	<p>Configure when the SASE client should filter information related to general security. By default, all</p>

	<div>information extraction is disabled.</div> <div><div>Add EIP Object</div><div><div>Name*</div><div></div></div><div><div>Description</div><div></div></div><div><div>Category</div><div>General</div></div><div><div>hostname</div><div></div><div>hostID</div><div></div></div><div><div>Windows Domain</div><div></div><div>Username</div><div></div></div><div><div>OS Vendor</div><div></div><div>OS Product</div><div></div></div><div><div>OS Major</div><div><div><input checked="" type="radio"/> Disabled</div><div><input type="radio"/> Value</div><div><input type="radio"/> Range</div></div><div>OS Minor</div><div><div><input checked="" type="radio"/> Disabled</div><div><input type="radio"/> Value</div><div><input type="radio"/> Range</div></div></div><div><div>OS Service</div><div><div><input checked="" type="radio"/> Disabled</div><div><input type="radio"/> Value</div><div><input type="radio"/> Range</div></div><div>OS Patch</div><div><div><input checked="" type="radio"/> Disabled</div><div><input type="radio"/> Value</div><div><input type="radio"/> Range</div></div></div><div><div>Cancel</div><div>Add</div></div></div>
--	---

<ul style="list-style-type: none"> <li>◦ OS Major</li> </ul>	<p>Whether to validate the major version of the OS software installed on the SASE client. When you select an OS major software version, the Minor field is enabled.</p> <ul style="list-style-type: none"> <li>◦ Disabled—Click to not validate the OS major software version. This is the default.</li> <li>◦ Range—Click and then select a range for the OS major software version.</li> <li>◦ Value—Click and then select a value for the OS major software version.</li> </ul>
<ul style="list-style-type: none"> <li>◦ OS Minor</li> </ul>	<p>Whether to validate the minor version of the OS software installed on the SASE client. When you select an OS minor software version, the OS Service field is enabled.</p> <ul style="list-style-type: none"> <li>◦ Disabled—Click to not validate the OS major software version. This is the default.</li> <li>◦ Range—Click and then select a range for the OS minor software version.</li> <li>◦ Value—Click and then select a value for the OS minor software version.</li> </ul>
<ul style="list-style-type: none"> <li>◦ OS Service</li> </ul>	<p>Whether to validate the service version of the OS software installed on the SASE client. When you select an OS service software version, the OS Patch field is enabled.</p> <ul style="list-style-type: none"> <li>◦ Disabled—Click to not validate the OS service software version. This is the default.</li> <li>◦ Range—Click and then select a range for the OS service software version.</li> <li>◦ Value—Click and then select a value for the OS service software version.</li> </ul>
<ul style="list-style-type: none"> <li>◦ OS Patch</li> </ul>	<p>Whether to validate the latest OS patch number of the OS software installed on the SASE client:</p> <ul style="list-style-type: none"> <li>◦ Disabled—Click to not validate the OS patch range. This is the default.</li> <li>◦ Range—Click and then select a range for the OS patch range.</li> <li>◦ Value—Click and then select a value for the OS patch range.</li> </ul>

<p>Management status</p>	<p>Configure when the SASE client should filter information related to management status security. By default, all information extraction is disabled.</p> <div data-bbox="857 399 1520 932"> <p><b>Add EIP Object</b></p> <p>Name*</p> <input type="text"/> <p>Description</p> <input type="text"/> <p>Category</p> <div> Management Status </div> <p>Managed</p> <p> <input type="radio"/> Disabled <input type="radio"/> True <input type="radio"/> False </p> <p> <input type="button" value="Cancel"/> <input type="button" value="Add"/> </p> </div>
<ul style="list-style-type: none"> <li>Managed</li> </ul>	<p>Whether to validate if the endpoint device is managed by the organization:</p> <ul style="list-style-type: none"> <li>Disabled—Click to neither validate nor not validate. This is the default.</li> <li>False—Click to not validate.</li> <li>True—Click to validate.</li> </ul>

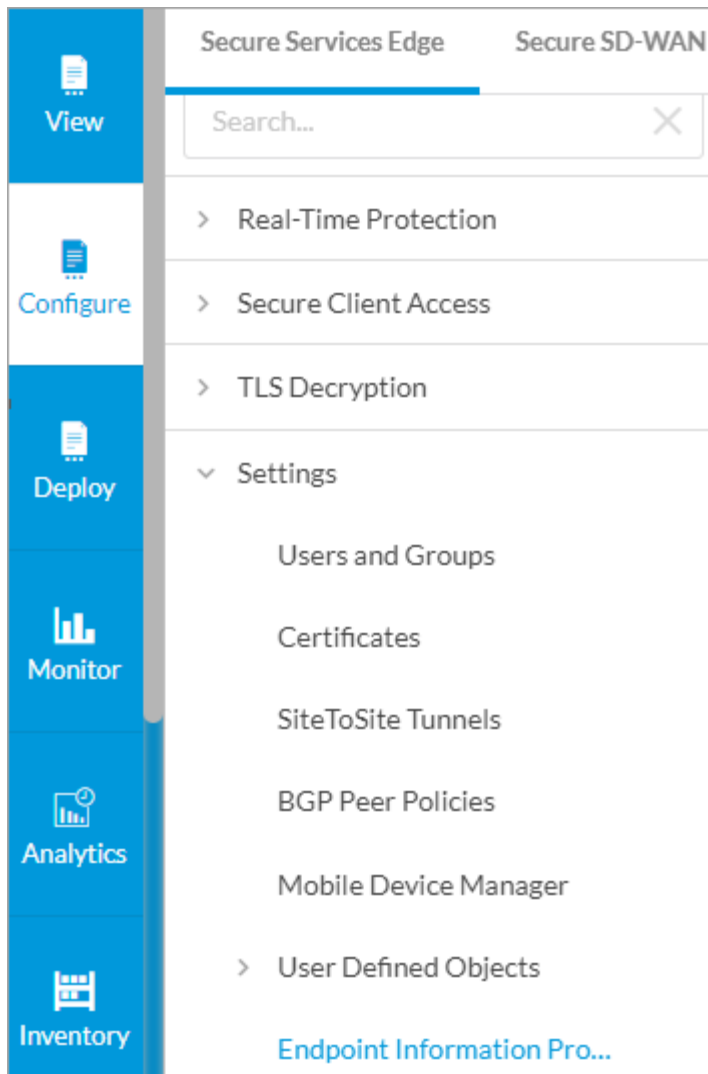
6. Click Add.

## View Predefined EIP Profiles

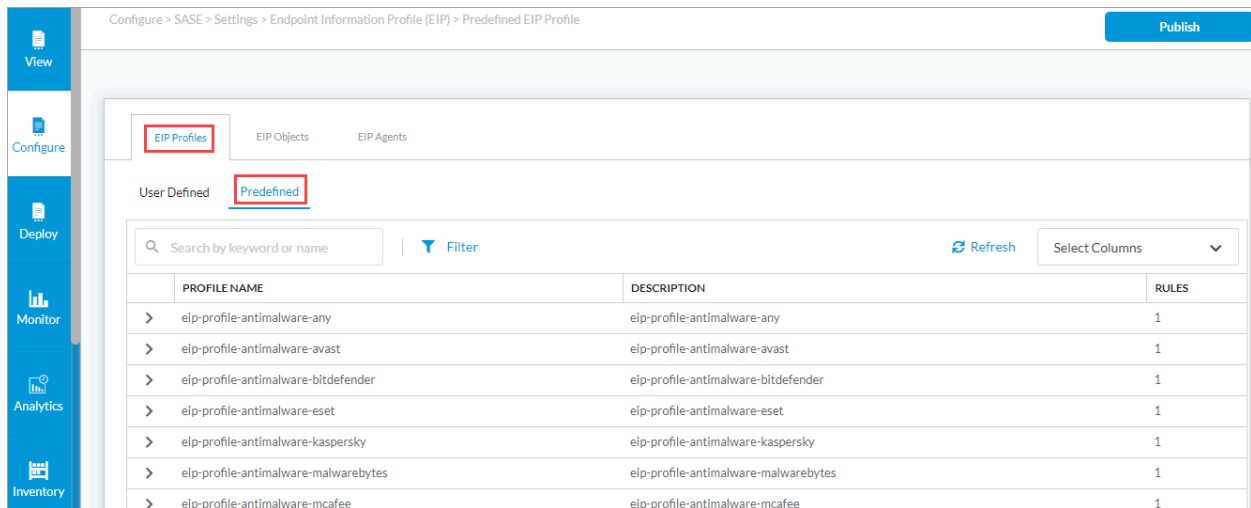
Concerto supports predefined EIP profiles that you can use to create security rules.

To view predefined EIP profiles:

- Go to Configure > Settings > End Information Profile.



The following screen displays:



[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_Endpoint\\_Informati...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Endpoint_Informati...)

Updated: Wed, 23 Oct 2024 08:39:28 GMT

Copyright © 2024, Versa Networks, Inc.

- 2. Select the EIP Profile tab and then select the Predefined tab to view the predefined endpoint information profiles that Concerto supports. The table displays the name of the profile, a description for the profiles, and the number of rules that the profile supports.
- 3. To customize which columns display, click Select Columns down arrow and then click the columns to select or deselect the ones you want to display. Click Reset to return to the default column display settings.
- 4. Click the down arrow next to a predefined profile to view the rules that are part of the EIP profile.

PROFILE NAME		DESCRIPTION		RULES
eip-profile-antimalware-any		eip-profile-antimalware-any		1
NAME	CATEGORY	OBJECTS	USER DEFINED OBJECTS	PREDEFINED OBJECTS
r1		2		<div>&gt; eip-object-antimalware-any-installed</div> <div>&gt; eip-object-antimalware-any-running</div>

Field	Description
Name	Displays the name of the EIP rule.
Category	Displays the category of the rule.
Objects	Displays the number of EIP objects associated with the rule.
User-Defined Objects	Displays the number of custom EIP objects associated with the rule.
Predefined Objects	Displays the number of predefined EIP objects associated with the rule.

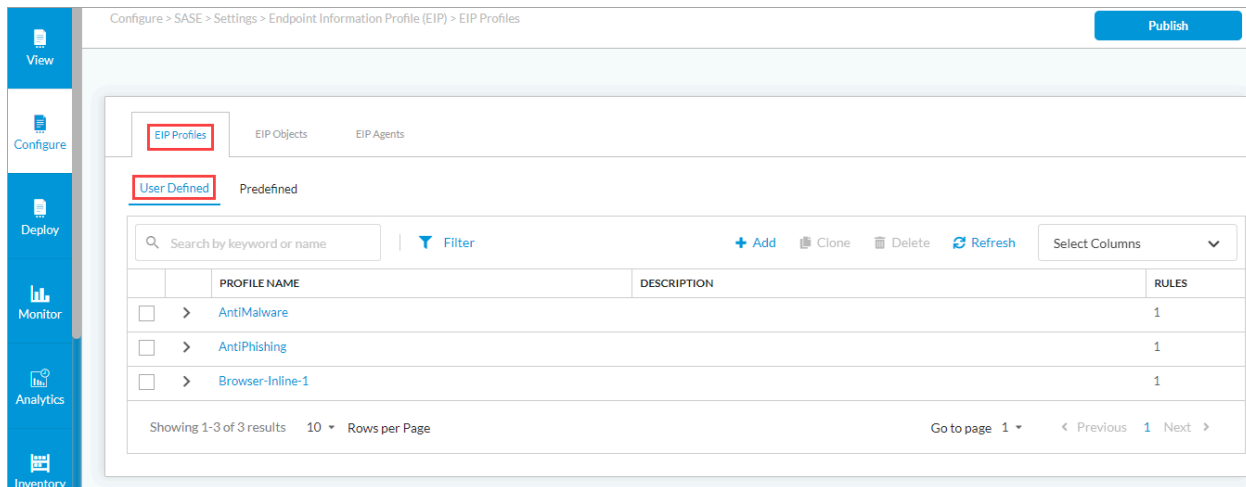
## Configure a Custom EIP Profile

In addition to using predefined EIP profiles, you can create custom EIP profiles to suit your endpoint security policy.

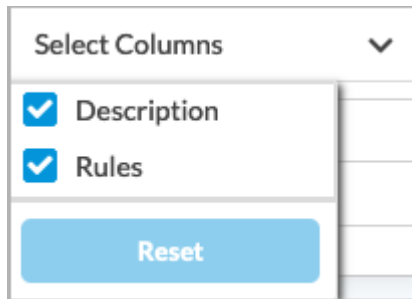
To configure a custom EIP profile:

- 1. Go to Configure > Settings > End Information Profile. The following screen displays.

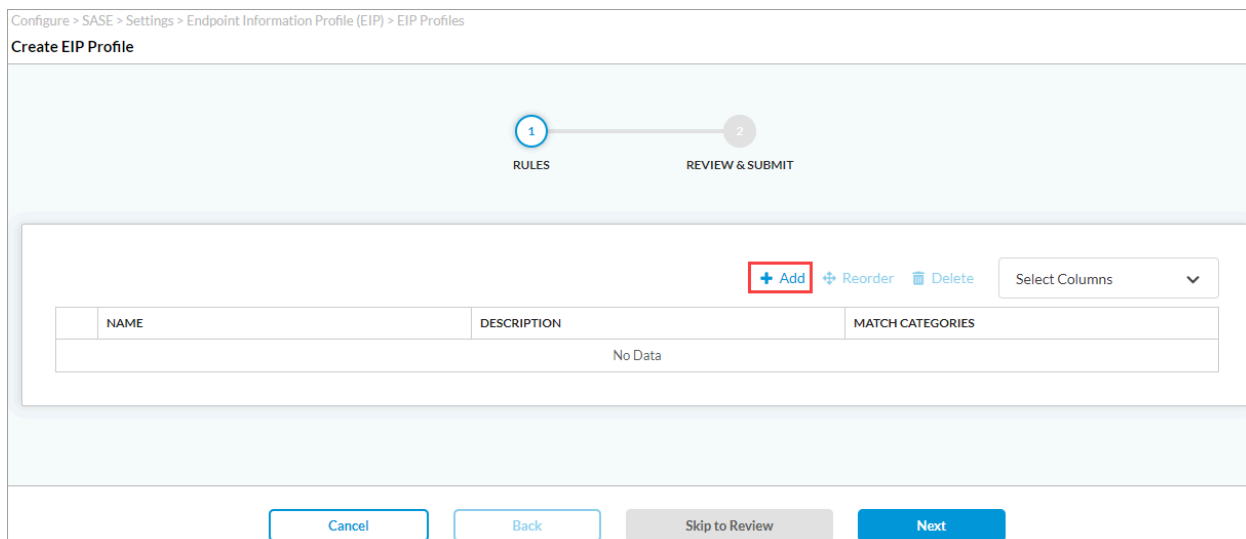




2. Select the EIP Profile tab, and then select the User Defined tab.
3. To customize which columns display, click Select Columns down arrow and then click the columns to select or deselect the ones you want to display. Click Reset to return to the default column display settings.



4. Click + Add to add an EIP profile. The Create EIP Profile screen displays.



5. Under Rules, click + Add to add an EIP rule.

Add Rules

Name\*

Description

+ Add

Delete

Select Columns

CATEGORY	OBJECTS	USER DEFINED OBJECTS	PREDEFINED OBJECTS
No Data			

Cancel

Add

- Click + Add to add a predefined or custom EIP object to the rule. In the Add EIP Object popup window, enter information for the following fields. You must add at least one EIP object to the rule. An EIP object identifies particular information about the software such as management status, AD domain, and unique host ID of an endpoint. For more information, see [Configure a Custom EIP Object](#), above.

Add EIP Object

Category

-- Select --

User Defined EIP Objects

Predefined EIPObjects

Cancel

Add

Field	Description
Category	<p>Click the down arrow, and then select an EIP object category in the drop-down list. Versa EIP supports the following classification categories on Linux, Mac, and Windows devices:</p> <ul style="list-style-type: none"> <li>◦ Antimalware</li> <li>◦ Antiphishing</li> <li>◦ Browser</li> <li>◦ Cloud storage</li> <li>◦ Custom</li> <li>◦ Data loss prevention</li> <li>◦ Disk backup</li> <li>◦ Disk encryption</li> <li>◦ Firewall</li> <li>◦ General</li> <li>◦ Health agent</li> <li>◦ Management status</li> <li>◦ Messenger</li> <li>◦ Patch management</li> <li>◦ Public file sharing</li> <li>◦ Remote control</li> <li>◦ Virtual machine</li> </ul>
User-Defined EIP Objects	Click the down arrow, and then select one or more user-defined EIP object categories in the drop-down list. For more information, see <a href="#">Configure a Custom EIP Object</a> .
Predefined EIP Objects	Click the down arrow, and select one or more predefined EIP object categories in the drop-down list.

- Click Add to add the EIP objects to the EIP rule.
- Click Next.
- In the Review and Submit screen, in the General section, enter a name for the EIP rule. Optionally, you can add a description and one or more tags. A tag is an alphanumeric descriptor, with no white spaces or special characters, that you can use to search the objects.

Configure > SASE > Settings > Endpoint Information Profile (EIP) > EIP Profiles

### Create EIP Profile

RULES

REVIEW & SUBMIT

Review your EIP Profiles configuration below

#### General

Name\* ⓘ
  
Profile Name

Description
  
Enter description name

Tags
  
Press Enter to add

#### Rules

NAME	CATEGORY	OBJECTS	USER DEFINED OBJECTS	PREDEFINED OBJECTS
Rule-1	AntiMalware	1		> elp-object-antimalware-any-running

Cancel Back Save

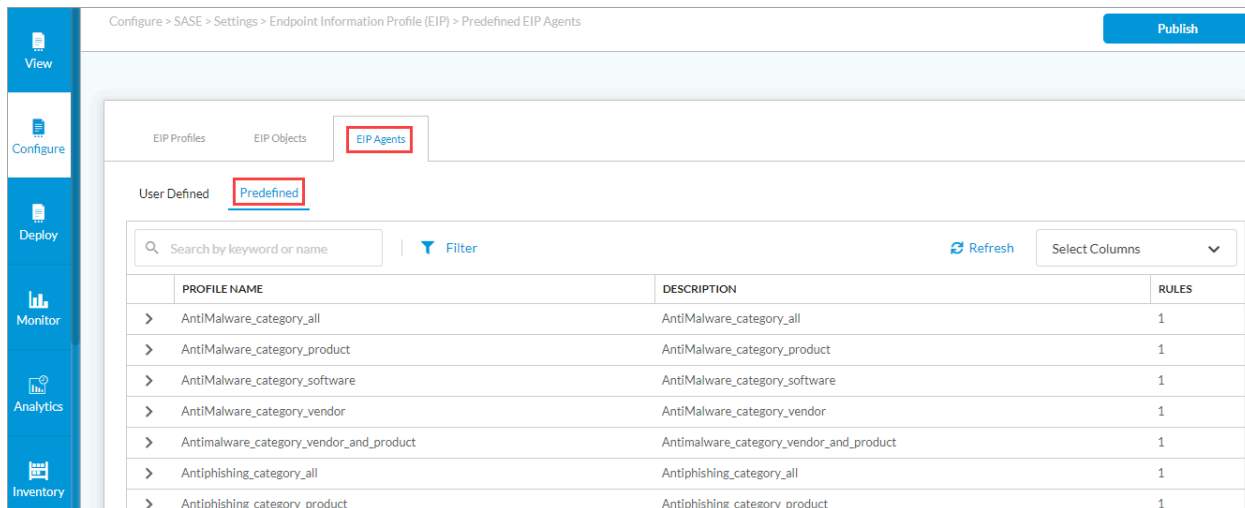
- Review the configuration entries, and click the Edit icon to make any needed changes.
- Click Save to create the new EIP rule.

## View Predefined EIP Agent Profiles

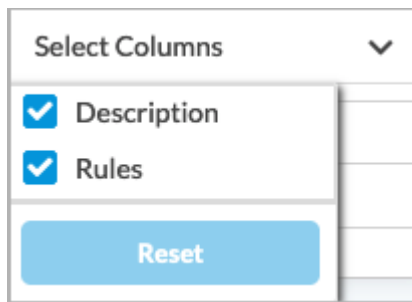
Concerto supports predefined EIP agent profiles that you can use to create rules.

To view predefined EIP agent profiles:

- Go to Configure > Settings > End Information Profile.
- Select the EIP Agents tab and then select the Predefined tab to view the predefined EIP agent profiles that Concerto supports. The table displays the profile name, description, and the number of rules associated with the profile.



- To customize which columns display, click Select Columns down arrow and then click the columns to select or deselect the ones you want to display. Click Reset to return to the default column display settings.

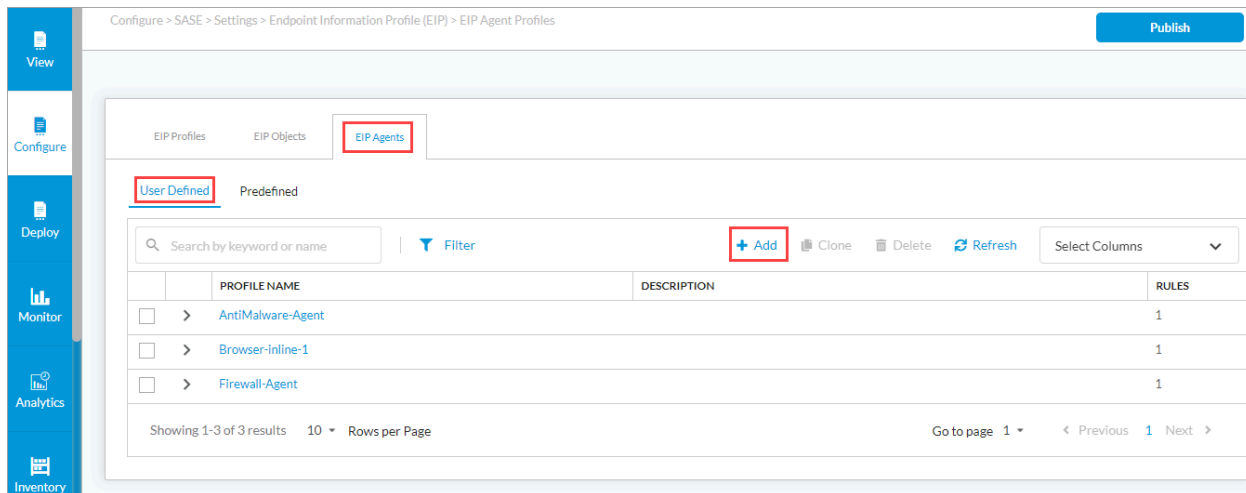


## Configure a Custom EIP Agent Profile

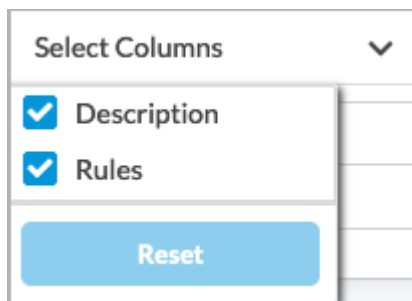
You configure an EIP agent profile to define when the SASE client must extract information from endpoint devices. You associate predefined or custom EIP agents with secure client access rules to enforce EIP security.

To configure a custom EIP object:

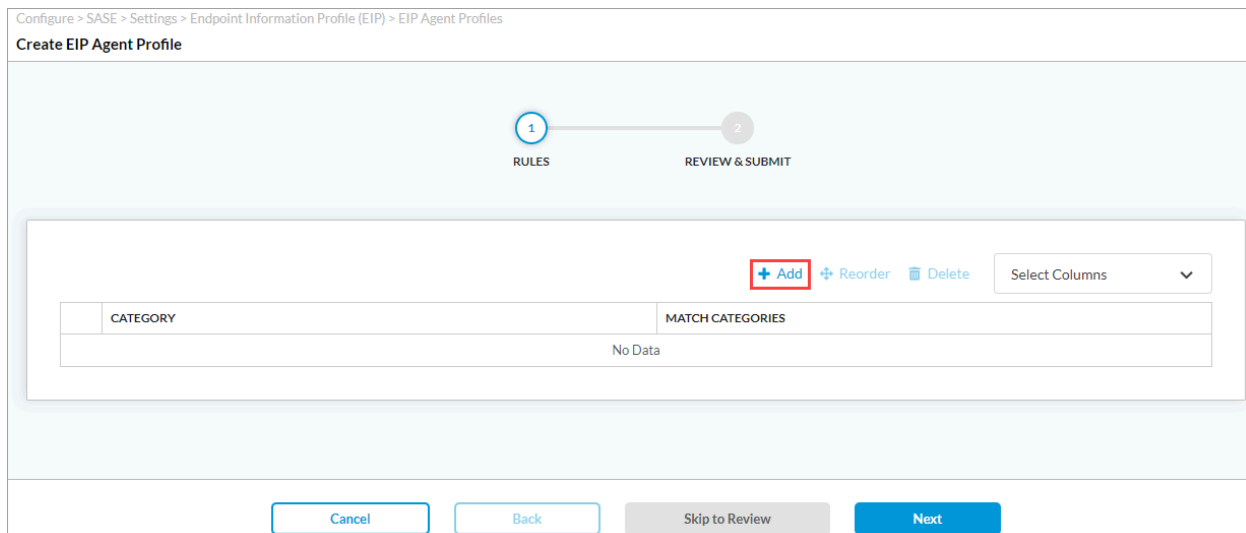
- Go to Configure > Settings > End Information Profile.
- Select the EIP Agents tab and then select the User Defined tab. The following screen displays.



- To customize which columns display, click Select Columns down arrow, and then click the columns to select or deselect the ones you want to display. Click Reset to return to the default column display settings.



- Click + Add to add an EPS agent profile. The Create EIP Agent Profile screen displays.



- Under Rules, click + Add to add a rule to the EIP agent profile. In the Add Rules popup window, enter information for the following fields.

Add Rules

Category

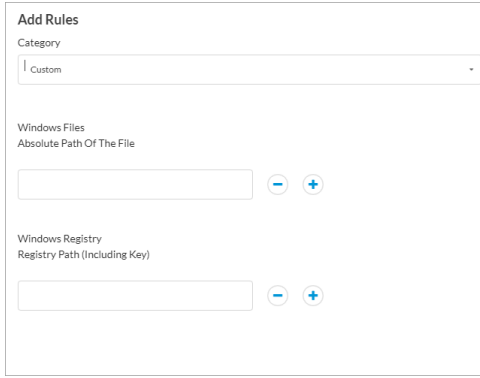

-- Select --


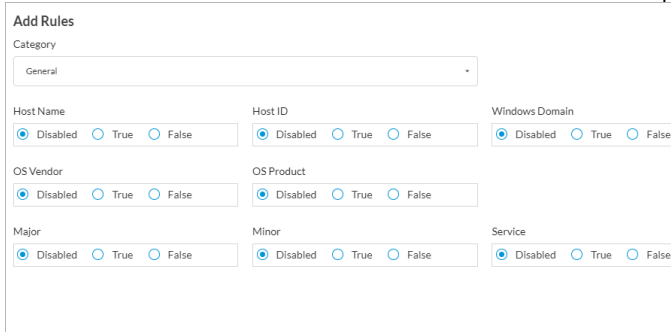
Cancel

Add

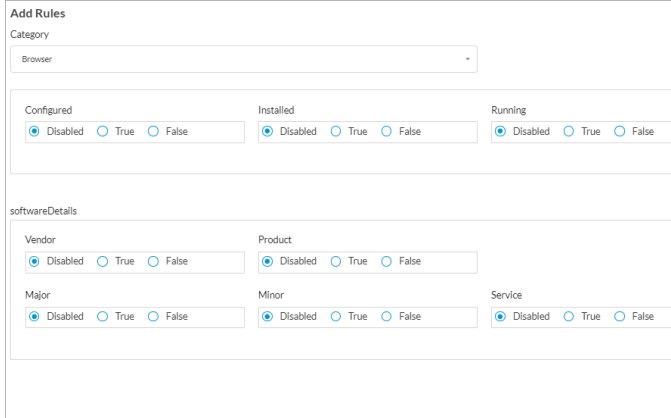
EIP Category and Field	Description
Antimalware	<p>Configure when the SASE client should extract information related to antimalware security type from the endpoint device traffic. For each item, select one of the following options:</p> <ul style="list-style-type: none"> <li>◦ False—Click to not extract the information.</li> <li>◦ True—Click to extract the information.</li> </ul>
<ul style="list-style-type: none"> <li>◦ Configured</li> <li>◦ Installed</li> <li>◦ Running</li> <li>◦ Realtime</li> </ul>	Whether to extract the antimalware software configuration, installation, or running status, or real-time information.
<ul style="list-style-type: none"> <li>◦ Last Definition Update Time (in hours)</li> </ul>	Whether to extract information about the last definition update time of the antimalware software, in hours.
<ul style="list-style-type: none"> <li>◦ Last Engine Update Time (in hours)</li> </ul>	Whether to extract the last engine update time of the antimalware software, in hours.
<ul style="list-style-type: none"> <li>◦ Last Scan Time (in minutes)</li> </ul>	Whether to extract the last scan time of the antimalware software, in minutes.
<ul style="list-style-type: none"> <li>◦ Software Details (Group of Fields)</li> </ul>	
<ul style="list-style-type: none"> <li>◦ Vendor</li> </ul>	Whether to extract the antimalware software vendor name on the SASE client.
<ul style="list-style-type: none"> <li>◦ Product</li> </ul>	Whether to extract the antimalware software product name on the SASE client.
<ul style="list-style-type: none"> <li>◦ Major</li> </ul>	Whether to extract the major version of the



	antimalware software installed on the SASE client.
◦ Minor	Whether to extract the minor version of the antimalware software installed on the SASE client.
◦ Service	Whether to extract the antimalware software service number on the SASE client.
◦ Patch	Whether to extract the latest patch number available for the antimalware software package
Custom	<p>Configure when the SASE client should extract information for the custom security type from the endpoint device traffic.</p> 
◦ Windows Files	<p>Enter the absolute path of a Windows file to determine whether the file is present on the end device, for example, C:\Windows\System32\drivers\fileinfo.sys.</p> <p>Click the  Add icon to add another row.</p>
◦ Windows Registry	<p>Enter the absolute path of a registry to determine the value of the registry on the end device, for example, HKEY_LOCAL_MACHINE\SYSTEM\State\DateTime\NTP Enabled.</p>

	<p>Click the  Add icon to add another row.</p>
General	<p>Configure when the SASE client should extract information related to general security from the endpoint device traffic. For each item, select one of the following options:</p> <ul style="list-style-type: none"> <li>◦ False—Click to not extract the information.</li> <li>◦ True—Click to extract the information.</li> </ul> 
◦ Hostname	Whether to extract the name of the Windows host.
◦ Host ID	Whether to extract the unique identification number of the host.
◦ Windows Domain	Whether to extract the Windows domain information of the end device.
◦ Username	Whether to extract the username to log in to the system.
◦ OS Vendor	Whether to extract the vendor name of the installed endpoint operating system installed.
◦ OS Product	Whether to extract the product name of the installed endpoint operating system.

<ul style="list-style-type: none"> <li>◦ OS Major</li> </ul>	Whether to extract the installed OS major software version.
<ul style="list-style-type: none"> <li>◦ OS Minor</li> </ul>	Whether to extract the installed OS minor software version.
<ul style="list-style-type: none"> <li>◦ OS Service</li> </ul>	Whether to extract the OS software service number.
<ul style="list-style-type: none"> <li>◦ OS Patch</li> </ul>	Whether to extract the latest patch number and OS versions available for each software package.
Management Status	<p>Configure when the SASE client should extract information related to management status security.</p> <p>For each item, select one of the following options:</p> <ul style="list-style-type: none"> <li>◦ False—Click to not extract the information.</li> <li>◦ True—Click to extract the information.</li> </ul> <div> <div> Add Rules Category Management Status Managed <input checked="" type="radio"/> Disabled <input type="radio"/> True <input type="radio"/> False </div> <div>Cancel</div> </div>
Antiphishing Browser Cloud Storage Data Loss Prevention Disk Backup Disk Encryption Firewall	<p>Configure when the SASE client should extract information for the EIP security type from the endpoint device traffic .For each item, select one of the following options:</p> <ul style="list-style-type: none"> <li>◦ False—Click to not extract the information.</li> <li>◦ True—Click to extract the information.</li> </ul>

Health Agent Messenger Patch Management Public File Sharing Remote Control Virtual Machine	
◦ Configured	Whether to extract information about the configuration status of the software.
◦ Installed	Whether to extract information about the installation status of the software.
◦ Running	Whether to extract information about the running status of the software.
◦ Software Details (Group of Fields)	
◦ Vendor	Whether to extract the vendor software.
◦ Product	Whether to extract the software product name.
◦ Major	Whether to extract the major software version of the installed software.
◦ Minor	Whether to extract the minor software versions of the installed software.
◦ Service	Whether to extract the software service number.

◦ Patch	Whether to extract the latest software package patch number.
---------	--

- Click Add to add the EIP rule to the EIP agent profile.
- Click Next.
- In the Review and Submit screen, in the General section, enter a name for the EIP agent profile. Optionally, you can add a description and one or more tags. A tag is an alphanumeric descriptor, with no white spaces or special characters, that you can use to search the objects.

Configure > SASE > Settings > Endpoint Information Profile (EIP) > EIP Agent Profiles

### Create EIP Agent Profile

✓

2

RULES

REVIEW & SUBMIT

Review your EIP Agents configuration below

#### General

Name \*

Description

Profile Name

Enter description name

#### Rules [Edit](#)

CATEGORY	MATCH CATEGORIES
AntiMalware	Installed: Disabled Configured: Disabled Running: Disabled Last Definition Update Time(in hours): Disabled Last Engine Update Time(in hours): Disabled <a href="#">Show More</a>

Cancel

Back

Save

- Review the configuration entries, and click the [Edit](#) icon to make any needed changes.
- Click Save.

## Associate an EIP Profile with Secure Service Edge Rules

To enforce EIP profile rules, you associate predefined or custom EIP profiles with internet protection (IP) rules, secure client access (SCA) rules, and TLS decryption rules.

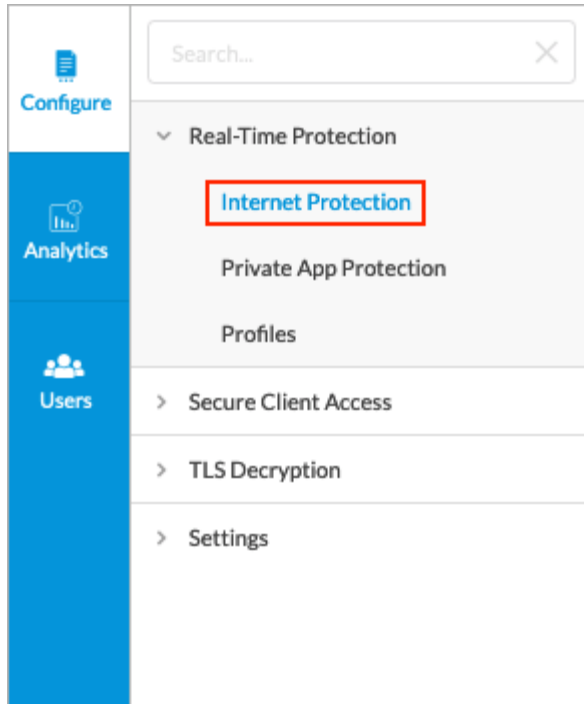
### Associate an EIP Profile with an IP Rule

- Go to Configure > Secure Services Edge > Real-Time Protection > Internet Protection.

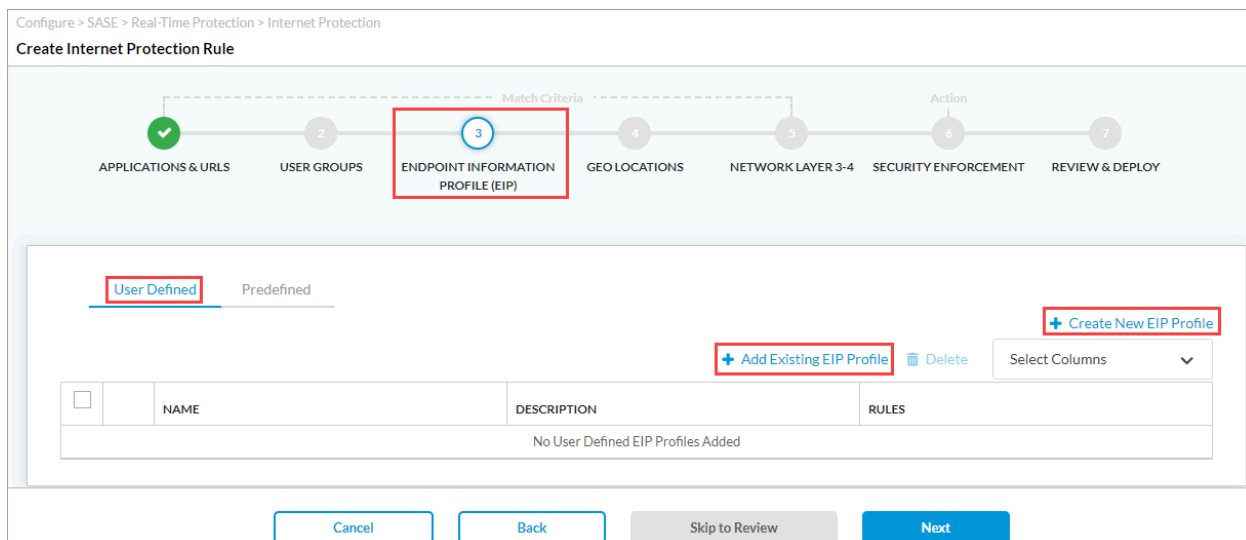
[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_Endpoint\\_Informati...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Endpoint_Informati...)

Updated: Wed, 23 Oct 2024 08:39:28 GMT

Copyright © 2024, Versa Networks, Inc.



2. In the Internet Protection Rules List screen, click + Add to create a rule or select an existing rule. The Create/Edit Internet Protection Rule screen displays. For more information, see [Configure SASE Internet Protection Rules](#).



3. Select the Endpoint Information Profile (EIP) tab.
4. To associate an existing custom EIP profile with the IP rule, select the User Defined tab, and then click + Add Existing EIP Profile. The Add User Defined EIP Profile popup screen displays.

Add User Defined EIP Profile

Cancel
Add

5. Select a custom EIP profile in the drop-down list, and then click Add.
6. To add a new EIP profile, click Create New EIP Profile. The Create EIP Profile screen displays. For more information, see [Configure a Custom EIP Profile](#), above.
7. To associate a predefined EIP profile with the IP rule, select the Predefined tab in the Endpoint Information Profile (EIP) tab.

Configure > SASE > Real-Time Protection > Internet Protection

Create Internet Protection Rule

1

2

3

4

5

6

7

APPLICATIONS & URLS

USER GROUPS

ENDPOINT INFORMATION PROFILE (EIP)

GEO LOCATIONS

NETWORK LAYER 3-4

SECURITY ENFORCEMENT

REVIEW & DEPLOY

User Defined

Predefined

+ Add Existing EIP Profile

Delete

Select Columns

	NAME	DESCRIPTION	RULES
No Predefined EIP Profiles Added			

Cancel
Back
Skip to Review
Next

8. Click + Add Existing EIP Profile. The Add Predefined EIP Profile popup screen displays.

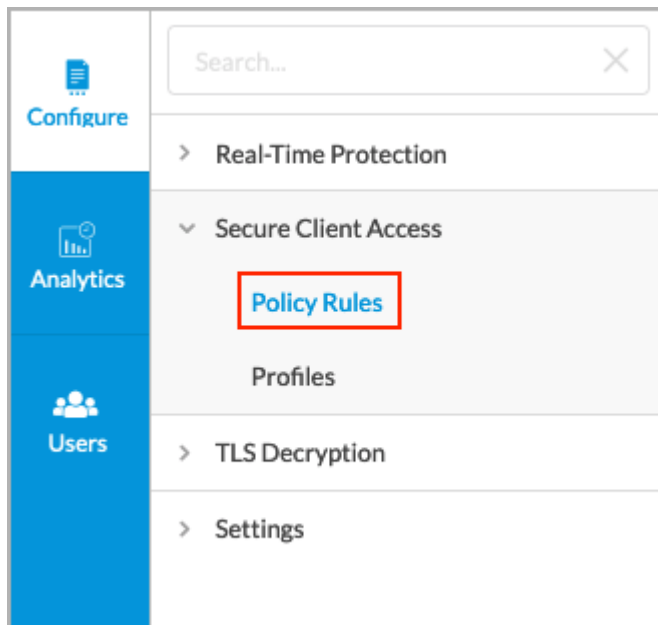
Add Predefined EIP Profile

Cancel
Add

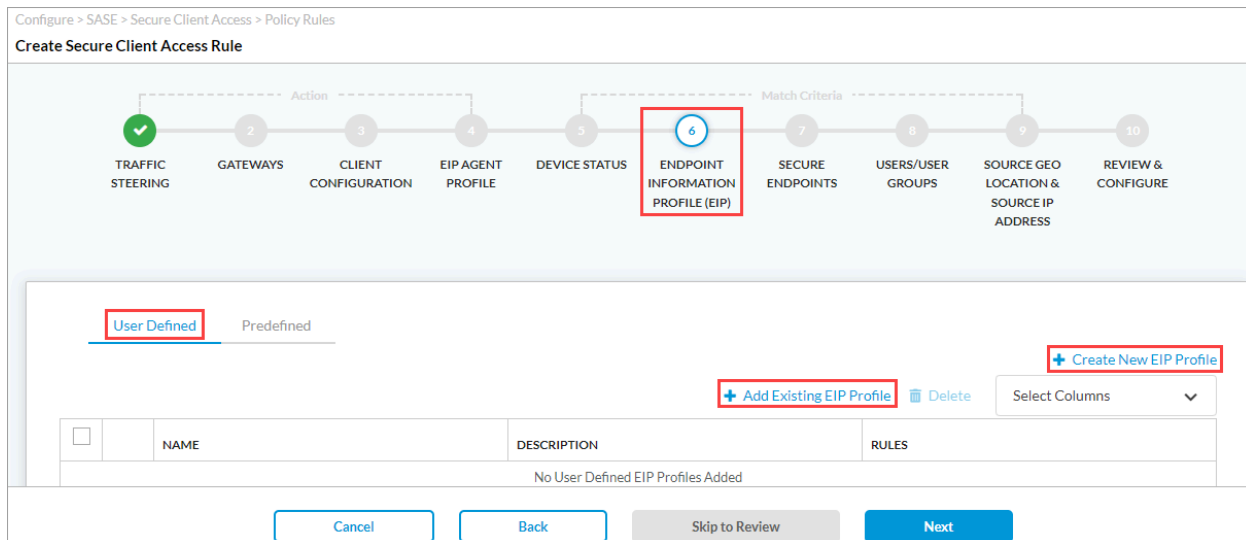
9. Select a predefined EIP profile in the drop-down list, and then click Add.
10. Save the IP rule.

## Associate an EIP Profile with an SCA Rule

1. Go to Configure > Secure Services Edge > Secure Client Access > Policy Rules.



2. In the Secure Client Access Rule List screen, click + Add to create a rule or select an existing rule. The Create/Edit Secure Client Access Rule screen displays. For more information, see [Configure SASE Secure Client Access Rules](#).



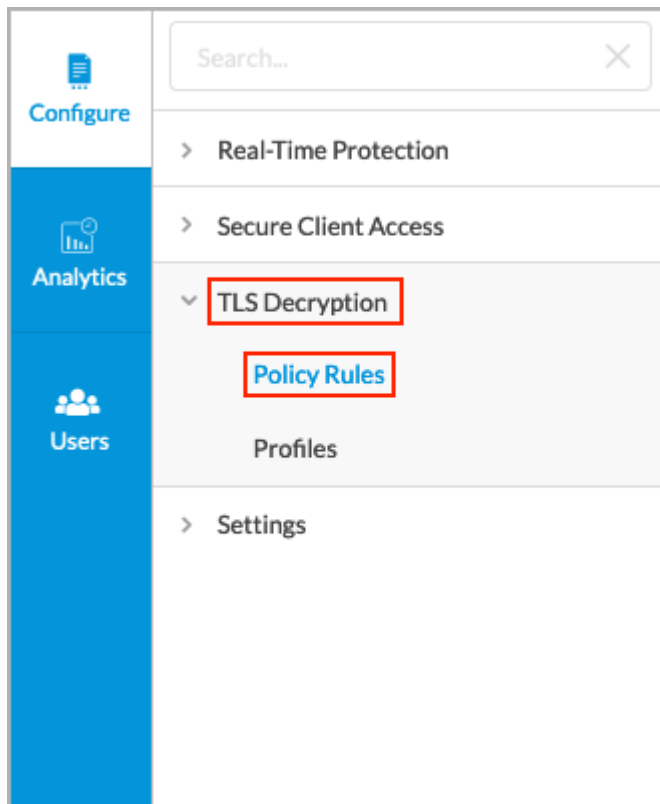
3. Select the Endpoint Information Profile (EIP) tab.
4. To associate an existing custom EIP profile with the SCA rule, select the User Defined tab, and then click + Add Existing EIP Profile. The Add User Defined EIP Profile popup screen displays.



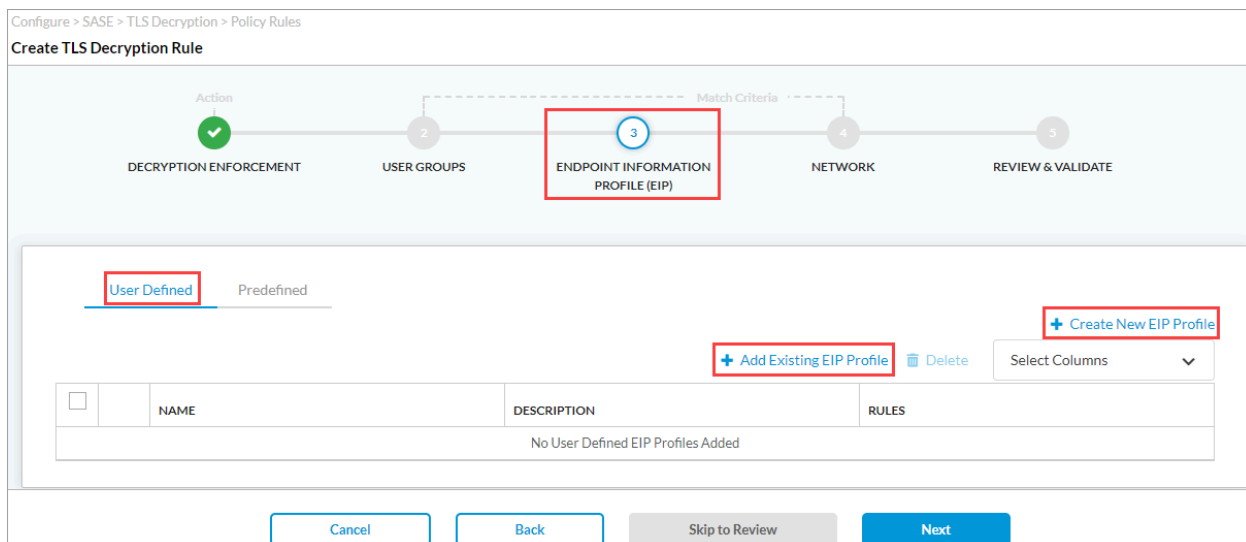


## Associate an EIP Profile with a TLS Decryption Rule

1. Go to Configure > Secure Services Edge > TLS Decryption > Policy Rules.



2. In the TLS Decryption Rules List screen, click + Add to create a rule or select an existing rule. The Create/Edit TLS Decryption Rule screen displays. For more information, see [Configure TLS Decryption Rules](#).



3. Select the Endpoint Information Profile (EIP) tab.

- To associate an existing custom EIP profile with the TLS decryption rule, select the User Defined tab, and then click + Add Existing EIP Profile. The Add User Defined EIP Profile popup screen displays.

The screenshot shows a modal window titled "Add User Defined EIP Profile" with a close button (X) in the top right corner. Below the title is a large empty text input field. At the bottom right, there are two buttons: "Cancel" and "Add".

- Select a custom EIP profile in the drop-down list and click Add.
- To add a new EIP profile, click Create New EIP Profile. The Create EIP Profile screen displays. For more information, see [Configure a Custom EIP Profile](#), above.
- To associate a predefined EIP profile with the TLS decryption rule, select the Predefined tab in the Endpoint Information Profile (EIP) tab.

The screenshot shows the "Create TLS Decryption Rule" screen. At the top, there is a breadcrumb trail: "Configure > SASE > TLS Decryption > Policy Rules". Below it, the title "Create TLS Decryption Rule" is displayed. A progress bar with five steps is shown: 1. Action (checked), 2. USER GROUPS, 3. ENDPOINT INFORMATION PROFILE (EIP) (highlighted with a red box), 4. NETWORK, and 5. REVIEW & VALIDATE. Below the progress bar, there are two tabs: "User Defined" and "Predefined" (highlighted with a red box). To the right of the tabs is a button "+ Add Existing EIP Profile" (highlighted with a red box) and a "Delete" button. Below the tabs is a table with columns: NAME, DESCRIPTION, and RULES. The table is empty, and a message "No Predefined EIP Profiles Added" is displayed. At the bottom, there are four buttons: "Cancel", "Back", "Skip to Review", and "Next".

- Click + Add Existing EIP Profile. The Add Predefined EIP Profile popup screen displays.

The screenshot shows a modal window titled "Add Predefined EIP Profile" with a close button (X) in the top right corner. Below the title is a large empty text input field. At the bottom right, there are two buttons: "Cancel" and "Add".

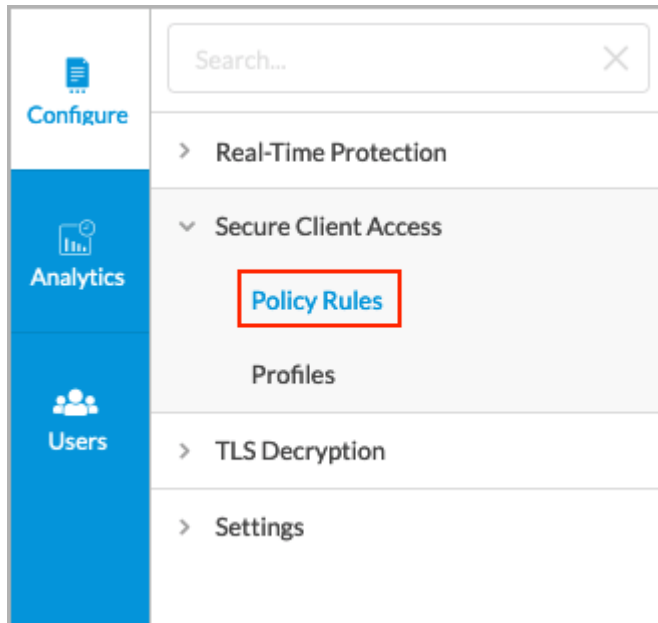
- Select a predefined EIP profile in the drop-down list, and then click Add.
- Save the TLS decryption rule.

## Associate an EIP Agent Profile with an SCA Rule

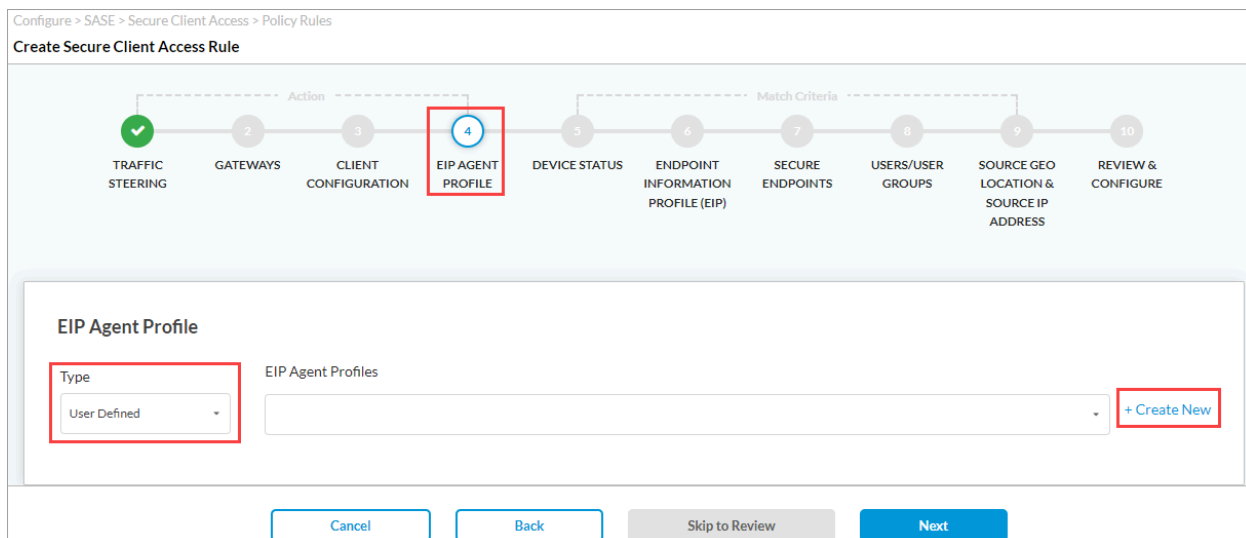
To enforce EIP agent profile rule, you associate predefined or custom EIP agent profiles with SCA rules.

To associate an EIP agent profile with an SCA rule:

1. Go to Configure > Secure Services Edge > Secure Client Access > Policy Rules.



2. In the Secure Client Access Rule List screen, click + Add to create a rule or select an existing rule. The Create/Edit Secure Client Access Rule screen displays. For more information, see [Configure SASE Secure Client Access Rules](#).



3. Select the EIP Agent Profile tab.

- To associate an existing custom EIP agent profile with the SCA rule, select User Defined in the Type drop-down list.
- Select a custom profile in the EIP Agent Profiles drop-down list. To add a new EIP Agent Profile, click + Create New. The Create EIP Agent Profile screen displays. For more information, see [Configure a Custom EIP Agent Profile](#), above.
- To associate a predefined EIP agent profile with the SCA rule, select Predefined in the Type field, and then select a profile in the EIP Agent Profiles drop-down list.

Configure > SASE > Secure Client Access > Policy Rules

### Create Secure Client Access Rule

1

TRAFFIC STEERING

2

GATEWAYS

3

CLIENT CONFIGURATION

4

EIP AGENT PROFILE

5

DEVICE STATUS

6

ENDPOINT INFORMATION PROFILE (EIP)

7

SECURE ENDPOINTS

8

USERS/USER GROUPS

9

SOURCE GEO LOCATION & SOURCE IP ADDRESS

10

REVIEW & CONFIGURE

Type

Predefined

EIP Agent Profiles

AntiMalware\_category\_software

CATEGORY	MATCH CATEGORIES
AntiMalware	Installed : Disabled Configured : Disabled Running : Disabled Realtime : True Last Definition Update Time(in hours) : True <a href="#">Show More</a>

Cancel

Back

Skip to Review

Next

- Save the SCA rule.

## Supported Software Information

Releases 11.3.1 and later support all content described in this article.

## Additional Information

[Configure SASE Internet Protection Rules](#)

[Configure SASE Secure Client Access Rules](#)

[Configure TLS Decryption Rules](#)