Step-By-Step Guide for Endpoint Identity Profile (EIP) Configuration

About This Document

This guide provides a comprehensive, use case based step-by-step configuration for setting up Versa SSE Secure Access policies and Protection Rules to use EIP for compliance and access control.

Endpoint Identity Profile (EIP) is an advanced security feature in Versa's SASE architecture that enables dynamic, context-aware access control based on the user device's posture and identity. EIP collects rich telemetry from endpoints—including device type, OS, patch level, running processes, security posture, and more—and uses this data to enforce Zero Trust policies in real time.

EIP ensures that access to sensitive applications and resources is granted only to trusted, compliant, and authenticated devices. Whether managed or unmanaged, each endpoint is evaluated against customizable policy criteria before access is allowed.

As part of the Versa Secure Access Service Edge (SASE) framework, EIP enhances identity- and posture-based access by seamlessly integrating with the Versa Secure Private Access (VSPA) solution. This empowers organizations to enforce least-privilege access, reduce their attack surface, and enable secure remote work with confidence.

EIP combines endpoint telemetry, identity management, and security intelligence to deliver continuous, adaptive access control across distributed environments, simplifying Zero Trust enforcement for enterprise users and devices.

Document Information

Title	**Step-By-Step Guide for Endpoint Identity Profile (EIP) Configuration**
Author	Versa Professional Services
Version	V 1.0

Disclaimer

Information contained in this document regarding Versa Networks (the Company) is considered proprietary.

Before you begin

Before you proceed with the steps outlined in this document, please ensure you've met the following prerequisites.

- The provider administrator must complete your tenant configuration. If you haven't received this information, please contact your Managed Service Provider or Account Manager for assistance.
- You have the Enterprise Administrator (Tenant Admin) credentials for the Versa SASE portal, also called the Concerto User Interface.
- You have administrative access to the Microsoft Azure Portal, specifically App registrations, Enterprise applications, and Intune configuration pages

Contents

Introduction

Endpoint Information Profiles (EIPs) protect the enterprise network and resources by ensuring that endpoint devices accessing the network maintain and adhere to enterprise security standards.

Versa EIP Building Blocks

EIP Objects: Define the match criteria for an EIP profile. The match criteria filter the raw data reported by endpoint devices (fetched by the SASE client and matched on SSE gateways).

EIP Profiles: Groups a collection of EIP objects as match criteria within the Secure Access Rules and Security Policy, which are evaluated when a user attempts to connect to SASE portals and gateways, or when permitting user traffic through Protection rules.

EIP Agent: Define the conditions that the SASE client uses to filter information from endpoint devices for continuous evaluation. When you configure a SASE portal policy, you associate the agent profile with an enforcement action.

General Configuration Steps for EIP

Now that we have covered the concepts of EIP Object, Profile, and Agent, let's move on to the configuration process.

Configure EIP Objects

Endpoint Information Profile (EIP) objects in Versa SASE define the criteria for evaluating endpoint device posture. These objects enable the system to collect and validate endpoint attributes such as antivirus status, firewall settings, and browser presence.

Each EIP object operates according to strict logic, meaning that all configured conditions must be met for the object to register a successful match. As referenced in the Versa documentation, "all elements in [a rule] must match for entities to be associated with the… EIP profile.

There are two types of EIP objects available:

- Predefined Objects: Delivered by Versa and ready to use on EIP Objects, there are already 156 EIP objects created under different categories.

EIP Categories – Description Table (Versa SSE)

Category	Description

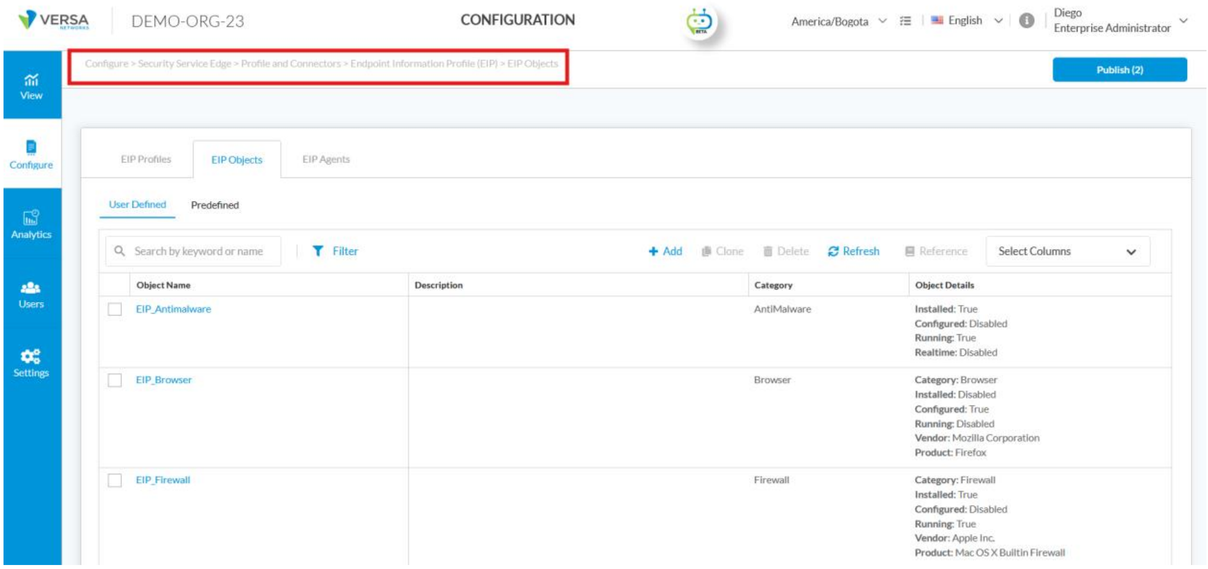
Antimalware	Identifies and categorises endpoint applications that detect, block, or remove malware such as viruses, trojans, ransomware, and similar threats.
AntiPhishing	Covers endpoint components designed to detect or prevent phishing attempts, including URL reputation checks and suspicious-link filtering.
Disk Backup	Includes backup agents and utilities responsible for local or cloud-based data backup and recovery operations on endpoints.
Browser	Classifies browser applications or browser extensions that can influence web access, security posture, or data handling.
Cloud Storage	Identifies applications used for cloud-based file synchronisation and storage (e.g., OneDrive, Dropbox, Google Drive, iCloud).
Custom	A flexible category intended for user-defined classifications that do not fall under standard EIP categories.
Data Loss Prevention (DLP)	Categorises endpoint tools that monitor, detect, or block unauthorised handling or movement of sensitive data.
Disk Encryption	Covers encryption agents that secure data at rest on endpoint storage devices (e.g., Bitdefender, Versacrypt).
Endpoint Security	Represents comprehensive endpoint security suites that include multiple protection capabilities (AV, behavioural analysis, etc.).
Firewall	Identifies local host-based firewall components that control inbound and outbound network traffic on the endpoint.
General	A broad category for benign or standard applications that do not pose significant security or data-handling implications.
Health Agent	Includes security posture, compliance, or device-health monitoring agents used for enterprise policy enforcement.
Management Status	Covers remote monitoring and management (RMM) or device-management agents that handle configuration, updates, and inventory.
Messenger	Classifies messaging and collaboration applications used for real-time chat, communication, or file exchange.
Patch Management	Identifies agents responsible for OS and application updates, vulnerability remediation, and patch deployment.
Public File Sharing	Includes applications designed to share files publicly or peer-to-peer, often requiring strict control in secure environments.
Remote Control	Covers remote desktop and remote-assistance applications that enable remote access

	to endpoint systems.
Virtual Machine	Identifies hypervisors, virtualization platforms, or VM management tools used to run isolated computing environments.

- User-Defined Objects: Customizable by administrators to fit specific endpoint requirements.

To demonstrate how to configure a user-defined EIP object, create an object that verifies whether a firewall is both installed and running on an endpoint:

Navigate to the EIP Object Configuration. Go To: Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Objects

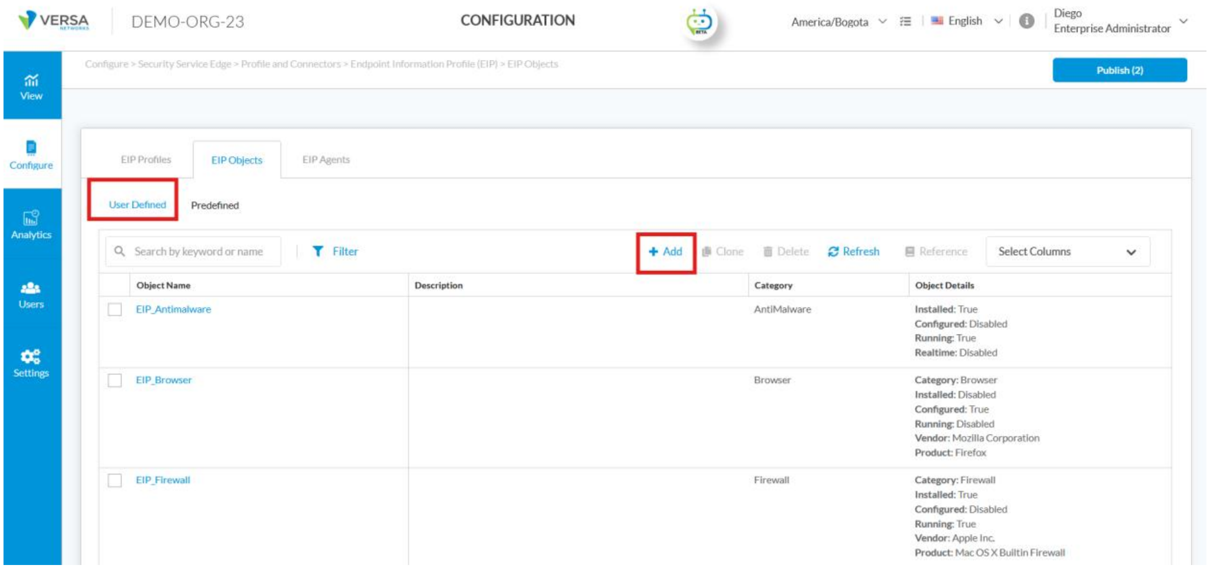


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Objects

	Object Name	Description	Category	Object Details
□	EIP_Antimalware		AntiMalware	**Installed:** True **Configured:** Disabled **Running:** True **Realtime:** Disabled
□	EIP_Browser		Browser	**Category:** Browser **Installed:** Disabled **Configured:** True **Running:** Disabled **Vendor:** Mozilla Corporation **Product:** Firefox
□	EIP_Firewall		Firewall	**Category:** Firewall **Installed:** True **Configured:** Disabled **Running:** True **Vendor:** Apple Inc. **Product:** Mac OS X Builtin Firewall

Step 1 Add EIP Object

Click on User-defined. Click the **+ Add** button to open the "Add EIP Object" window.



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Objects

	Object Name	Description	Category	Object Details
□	EIP_Antimalware		AntiMalware	**Installed:** True **Configured:** Disabled **Running:** True **Realtime:** Disabled
□	EIP_Browser		Browser	**Category:** Browser **Installed:** Disabled **Configured:** True **Running:** Disabled **Vendor:** Mozilla Corporation **Product:** Firefox
□	EIP_Firewall		Firewall	**Category:** Firewall **Installed:** True **Configured:** Disabled **Running:** True **Vendor:** Apple Inc. **Product:** Mac OS X Builtin Firewall

Step 2 Fill in the EIP Object Settings

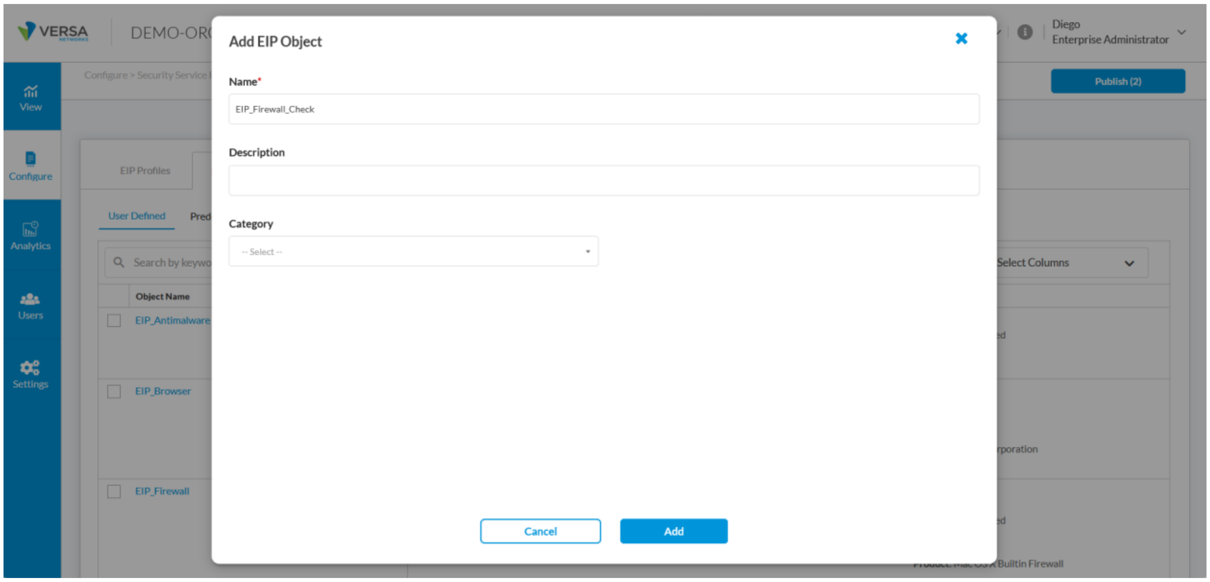
- **Name**: Enter a meaningful name (e.g., EIP_Firewall_Check).
- **Category**: Select **Firewall** from the drop-down.
- Installed: Set to True.
- **Running**: Set to **True**.
- (Optional) Add other parameters such as:
  - **Vendor** (e.g., Microsoft Corporation)
  - **Product** (e.g., *Windows Firewall*)
  - **Version fields**: Specify ranges or values for Major, Minor, Patch, or Service if needed.
  - **Realtime**, **Configured**, or **Scan Times** can also be configured based on the endpoint posture you want to evaluate.

Note:

For the **True**, **False**, and **Disabled** parameters, you can define how each posture attribute is interpreted during compliance checks:

- **True:** the condition must be met for the object to match the posture criteria.
- **False:** the condition must not be met for the object to match.
- **Disabled:** the condition is ignored and not evaluated.

These settings determine how the EIP Profile applies its match criteria when validating endpoint posture.



Add EIP Object

Name*

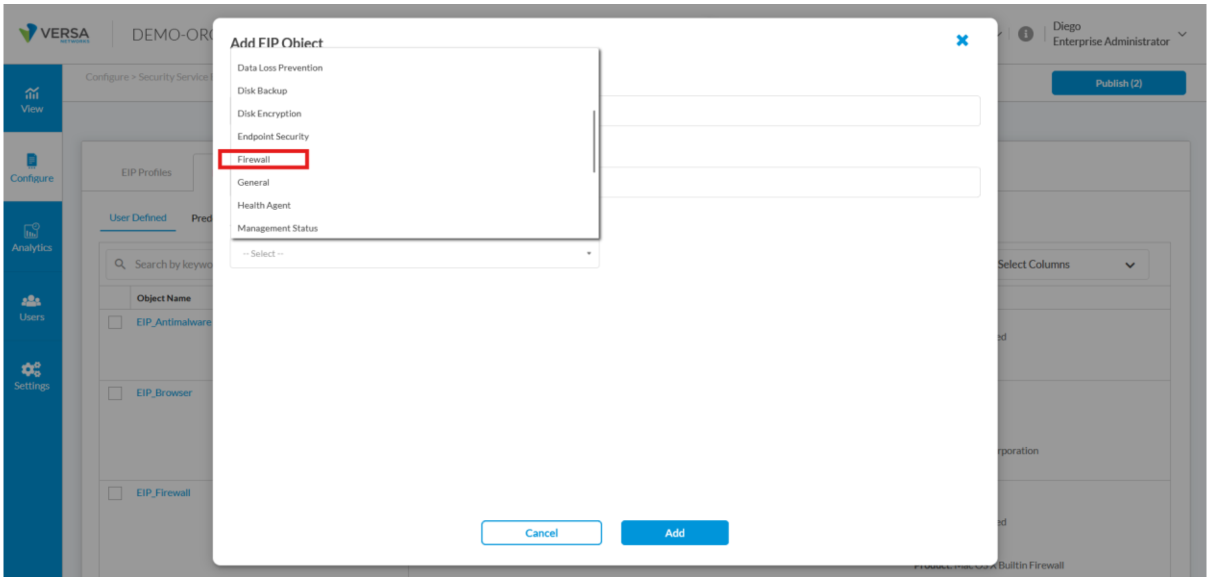
EIP_Firewall_Check

Description

Category

-- Select --

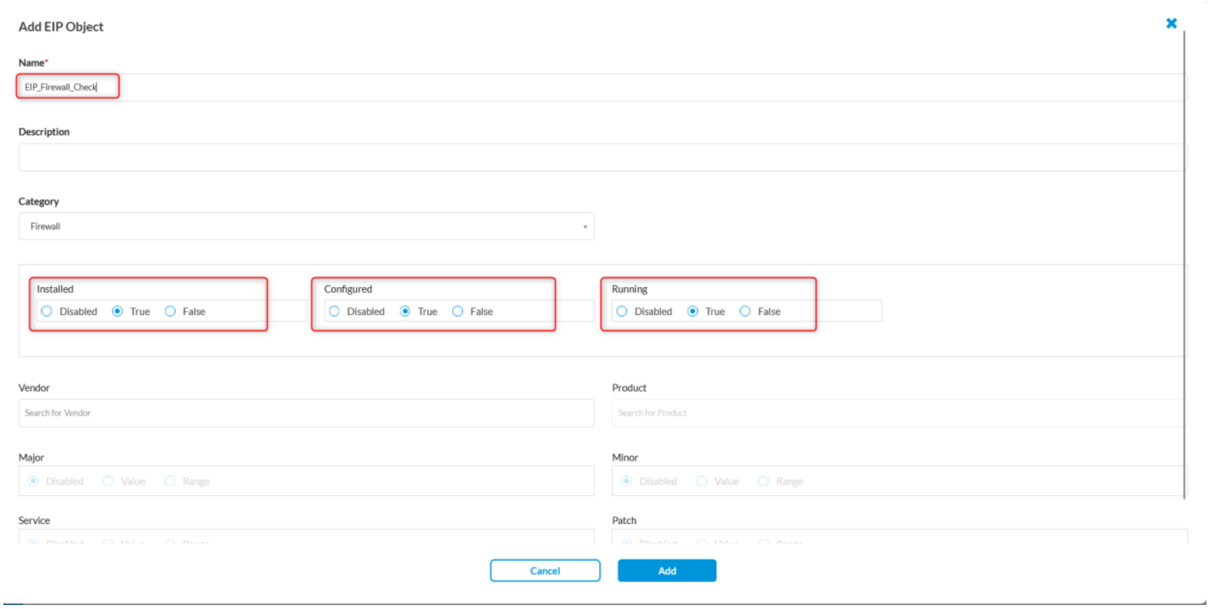
Drop-down category to firewall option



Add EIP Object

- Data Loss Prevention
- Disk Backup
- Disk Encryption
- Endpoint Security
- Firewall
- General
- Health Agent
- Management Status

-- Select --



Add EIP Object

Name*: EIP_Firewall_Check

Description:

Category: Firewall

Installed: ○ Disabled ● True ○ False

Configured: ○ Disabled ● True ○ False

Running: ○ Disabled ● True ○ False

Vendor: Search for Vendor

Product: Search for Product

Major: ● Disabled ○ Value ○ Range

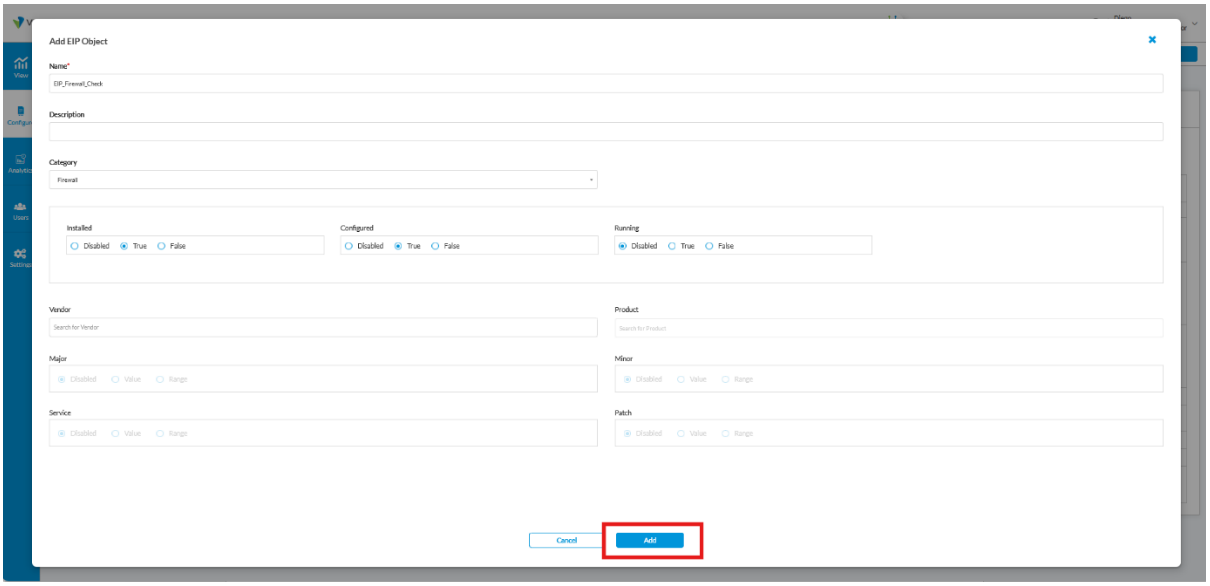
Minor: ● Disabled ○ Value ○ Range

Service

Patch

Step 3 Save EIP object

Click **Add** to create the EIP object.



Add EIP Object

Name*: EIP_Firewall_Check

Description:

Category: Firewall

Installed: ○ Disabled ● True ○ False

Configured: ○ Disabled ● True ○ False

Running: ● Disabled ○ True ○ False

Vendor: Search for Vendor

Product: Search for Product

Major: ● Disabled ○ Value ○ Range

Minor: ● Disabled ○ Value ○ Range

Service: ● Disabled ○ Value ○ Range

Patch: ● Disabled ○ Value ○ Range

EIP objects created can now be included in any EIP Profile to enforce policy based on the presence and status of endpoint firewalls. Similarly, other categories like Anti-Malware, Browser, or others can be configured using the same procedure to strengthen your Zero Trust enforcement.

Configure EIP Profiles.

An **Endpoint Information Profile (EIP)** defines the logic for evaluating endpoint posture to enforce access policies. Unlike **EIP Agent Profiles**, which specify *what data* is collected from the endpoint, an EIP Profile determines *how that data is matched* against predefined or user-defined posture objects to decide whether an endpoint is compliant.

Each EIP Profile is composed of one or more **rules**, and each rule includes:

- A **category** (e.g., Antimalware, Firewall, Browser, etc.)
- A list of **EIP Objects** (posture definitions).

- **Within each rule** (Inside same category): Matching is based on an **OR operation** — the rule is satisfied if **any one** of the selected EIP Objects matches the collected posture data.
- **Across rules in the profile** (different categories): Matching is based on an **AND operation** — the **entire EIP Profile** is considered a match **only if all rules** are satisfied.

Example:

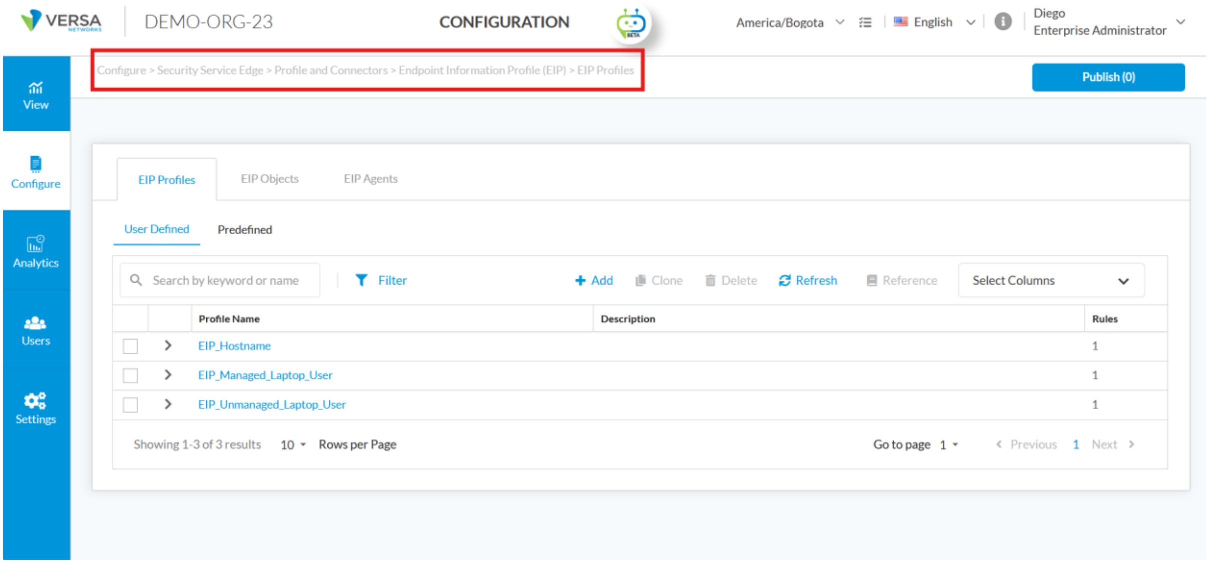
If a profile contains:

- Rule 1: AntiMalware (Bitdefender or Defender installed and running)
- Rule 2: Browser (Chrome or Firefox present)
- Rule 3: Firewall (Windows Firewall running)

Then, for the profile to match, the endpoint must satisfy **at least one object in each rule**. All three rules must match — one from each category.

To demonstrate how to review an EIP profile, the example eip-profile-antiphishing-popular is used. This profile gathers details about anti-phishing software.

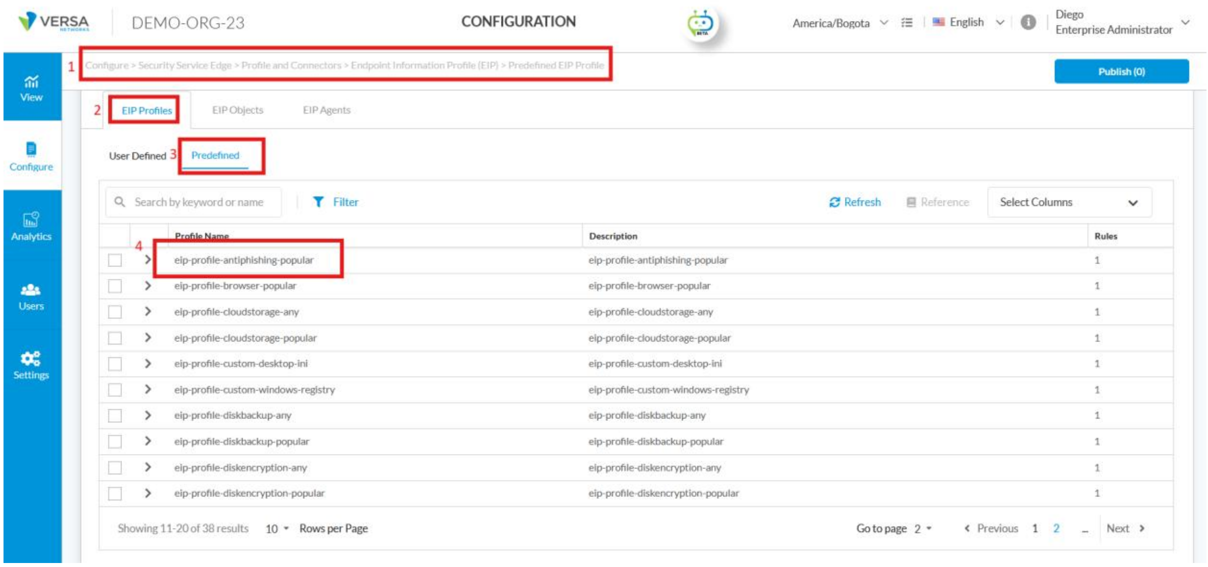
So, Navigate to Configure > SASE > Settings > Endpoint Information Profile (EIP) > EIP Profiles



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Profile Name	Description	Rules
EIP_Hostname		1
EIP_Managed_Laptop_User		1
EIP_Unmanaged_Laptop_User		1

Showing 1-3 of 3 results 10 Rows per Page Go to page 1 Previous 1 Next



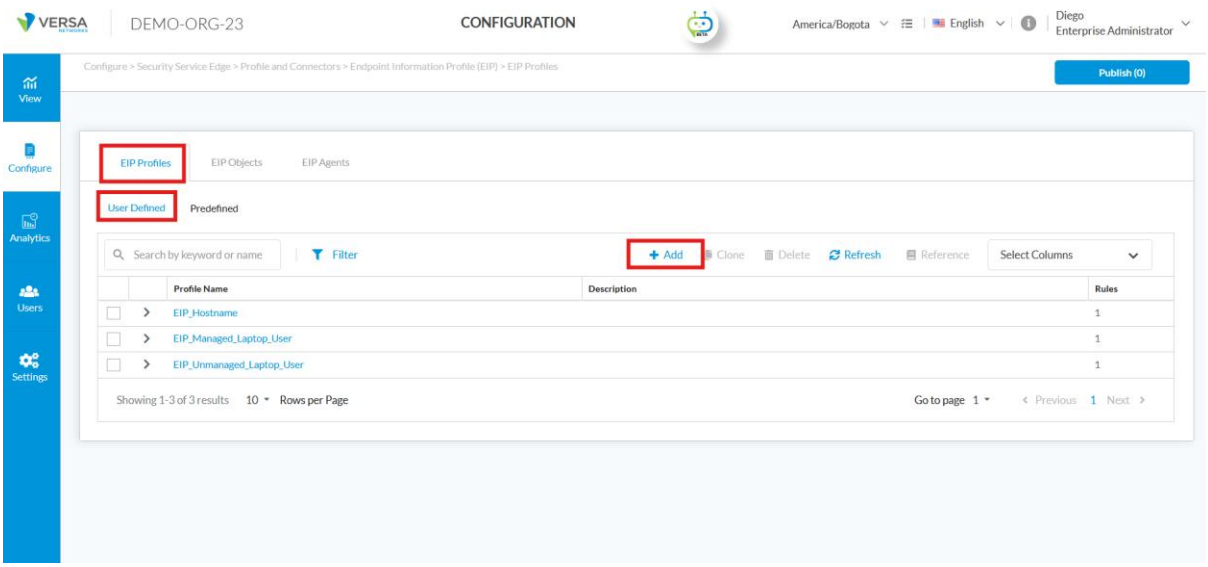
1 Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > Predefined EIP Profile

Profile Name	Description	Rules
eip-profile-antiphishing-popular	eip-profile-antiphishing-popular	1
eip-profile-browser-popular	eip-profile-browser-popular	1
eip-profile-cloudstorage-any	eip-profile-cloudstorage-any	1
eip-profile-cloudstorage-popular	eip-profile-cloudstorage-popular	1
eip-profile-custom-desktop-ini	eip-profile-custom-desktop-ini	1
eip-profile-custom-windows-registry	eip-profile-custom-windows-registry	1
eip-profile-diskbackup-any	eip-profile-diskbackup-any	1
eip-profile-diskbackup-popular	eip-profile-diskbackup-popular	1
eip-profile-diskencryption-any	eip-profile-diskencryption-any	1
eip-profile-diskencryption-popular	eip-profile-diskencryption-popular	1

Showing 11-20 of 38 results 10 Rows per Page Go to page 2 Previous 1 2 ... Next

To create a user-defined following the next steps: navigate to Configure > SASE > Settings > Endpoint Information Profile (EIP) > EIP Profiles, then User defined, and click + **Add.**

- Step 1: Navigate to EIP Profile Configuration
  - Go to: Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles
  - Click + **Add** to begin creating a new EIP profile.



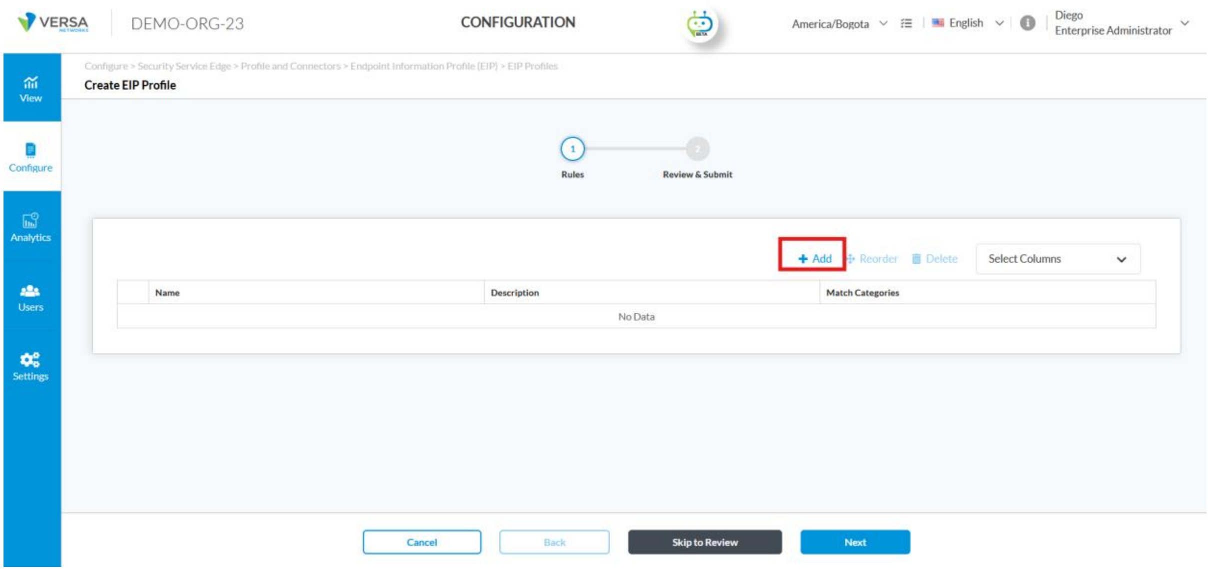
Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

		Profile Name	Description	Rules
□	>	EIP_Hostname		1
□	>	EIP_Managed_Laptop_User		1
□	>	EIP_Unmanaged_Laptop_User		1

Showing 1-3 of 3 results 10 Rows per Page Go to page 1 Previous 1 Next

- Step 2: Add Rules to the EIP Profile
  - Click + **Add** under the Rules section.
  - Enter a **Name** and **Description** for the rule (e.g., Rule1).
  - In the Category dropdown, select a posture category such as:
    - AntiMalware
    - AntiPhishing
    - Browser
    - Cloud Storage
    - Data Loss Prevention
    - ...or others available.

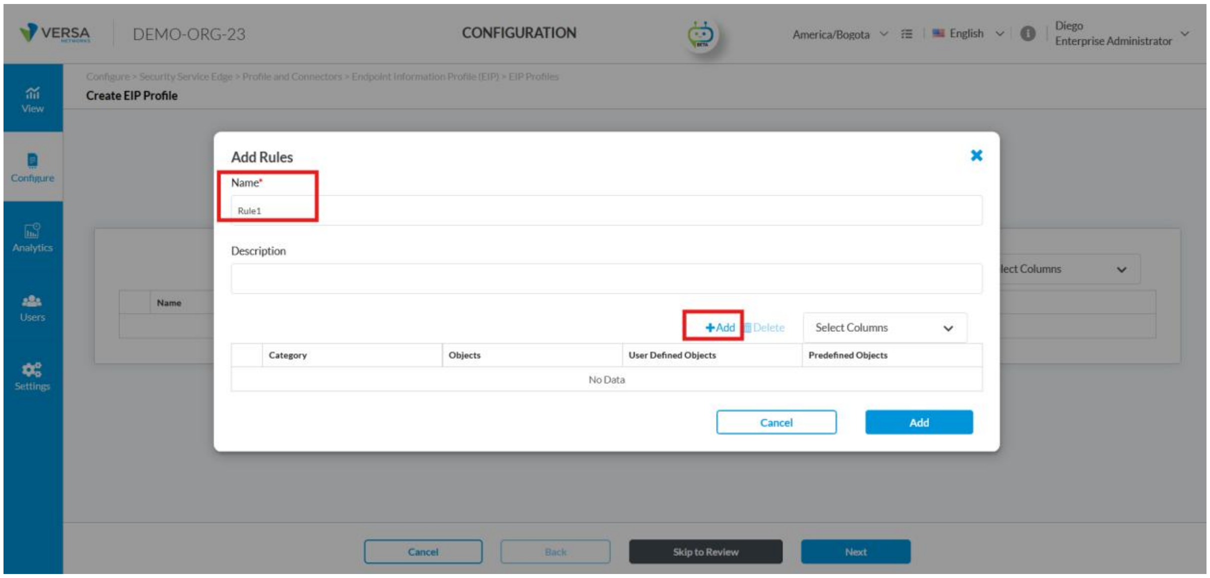
These categories determine the type of endpoint information that will be collected.



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Create EIP Profile

Name	Description	Match Categories
No Data		



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

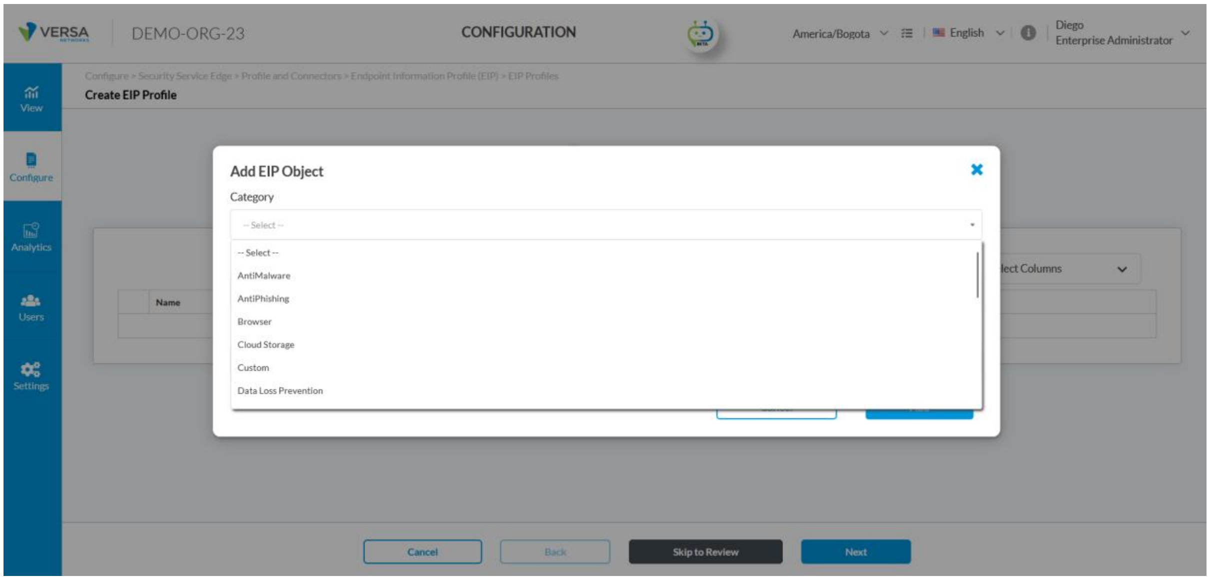
Create EIP Profile

Add Rules

Name*: Rule1

Description

Category	Objects	User Defined Objects	Predefined Objects
No Data			



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Create EIP Profile

Add EIP Object

Category

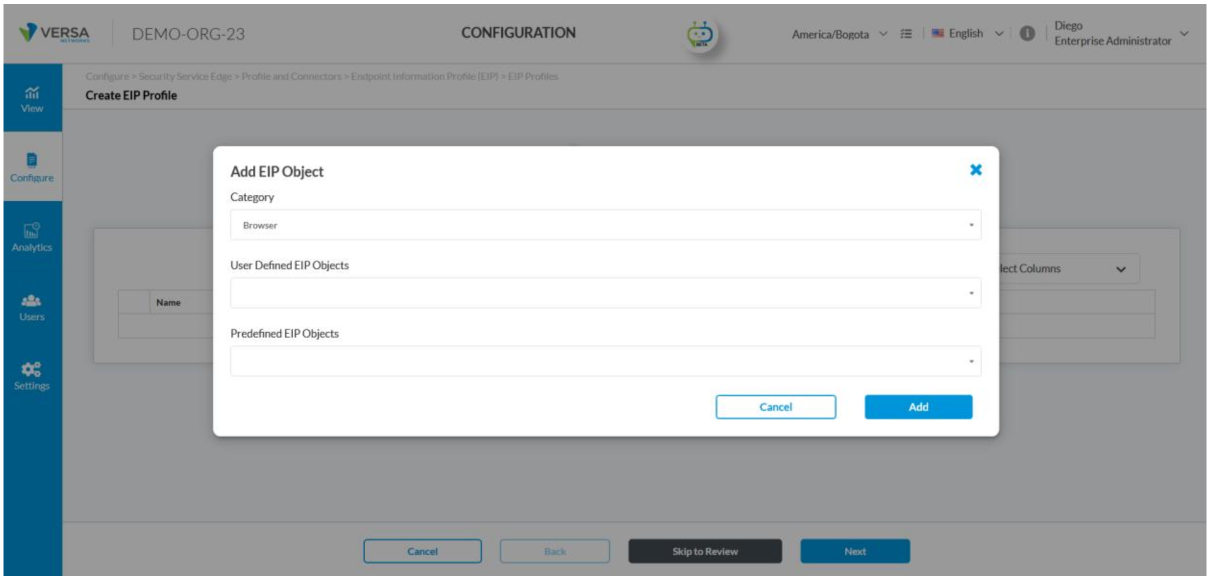
-- Select --

- -- Select --
- AntiMalware
- AntiPhishing
- Browser
- Cloud Storage
- Custom
- Data Loss Prevention

Step 3: Add User-Defined and Predefined EIP Objects

- Once a category is selected, you can choose:
  - Predefined EIP Objects: Preconfigured objects provided by Versa (e.g., eip-object-browser-chrome)
  - User Defined EIP Objects: Custom objects created by the administrator (e.g., EIP_Browser)
- Select the objects relevant to the Profile, then click Add.

Note: You can add multiple objects under the same profile by repeating this process.



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

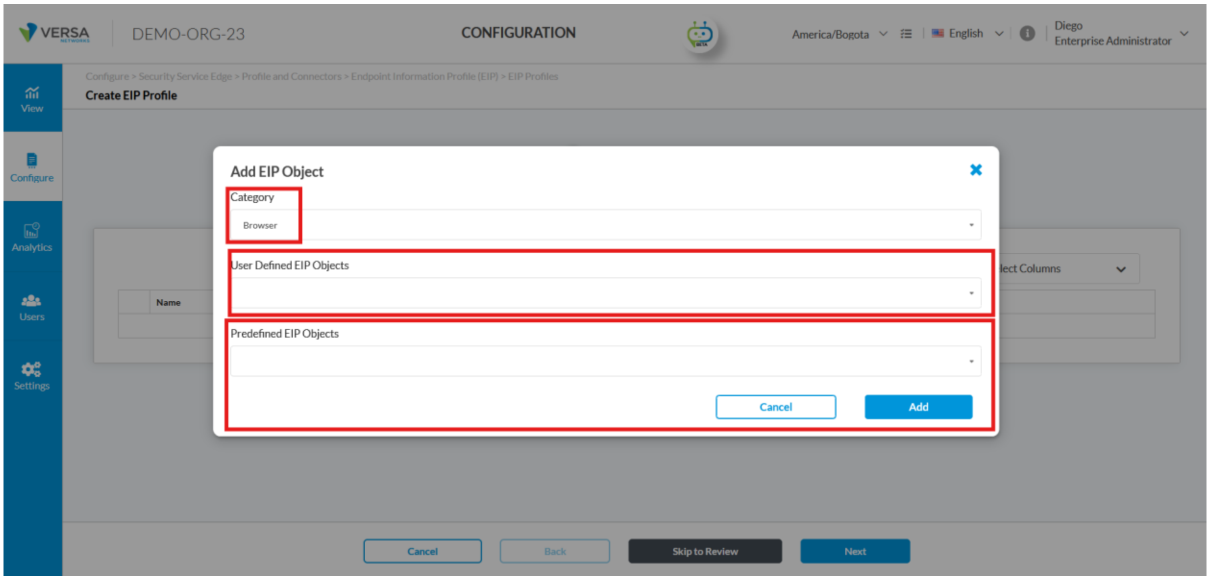
Create EIP Profile

Add EIP Object

Category: Browser

User Defined EIP Objects:

Predefined EIP Objects:



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

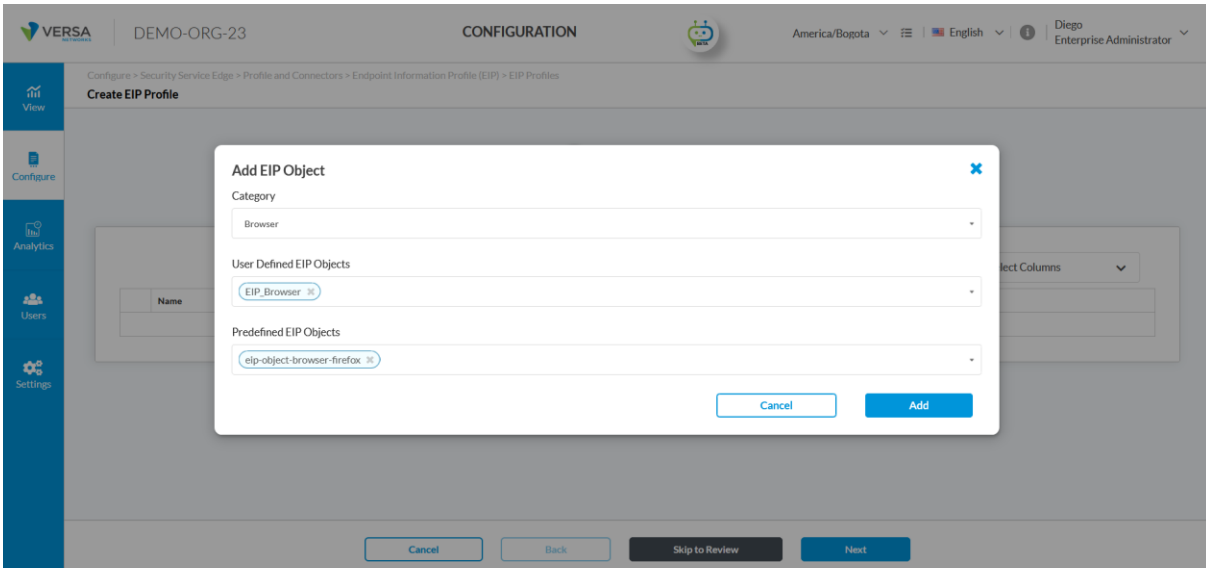
Create EIP Profile

Add EIP Object

Category: Browser

User Defined EIP Objects:

Predefined EIP Objects:



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

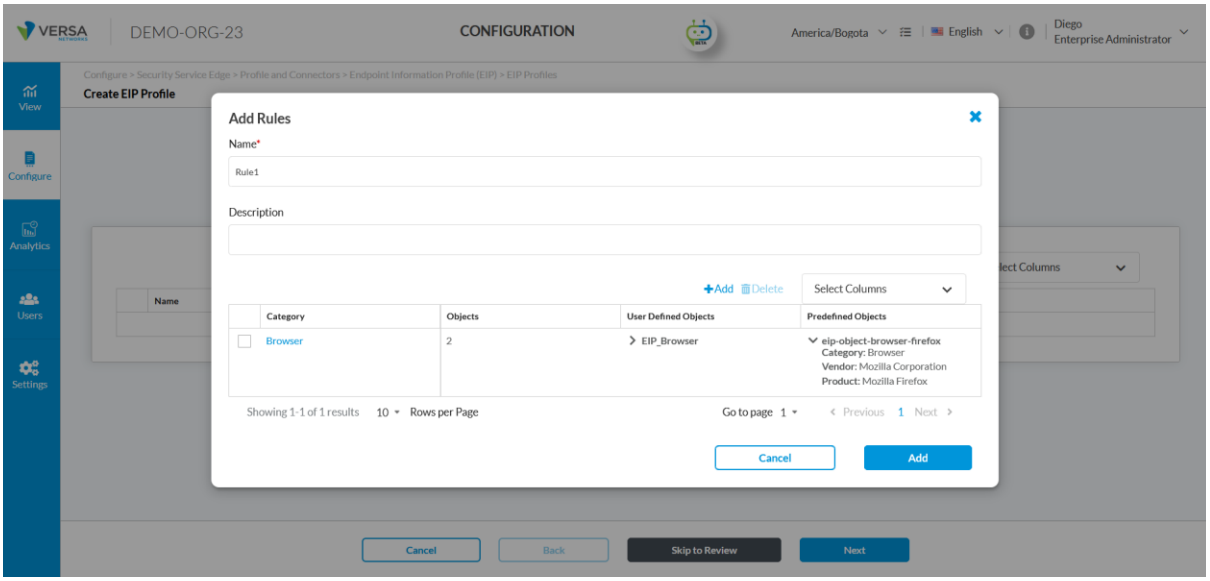
Create EIP Profile

Add EIP Object

Category: Browser

User Defined EIP Objects: EIP_Browser

Predefined EIP Objects: eip-object-browser-firefox



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Create EIP Profile

Add Rules

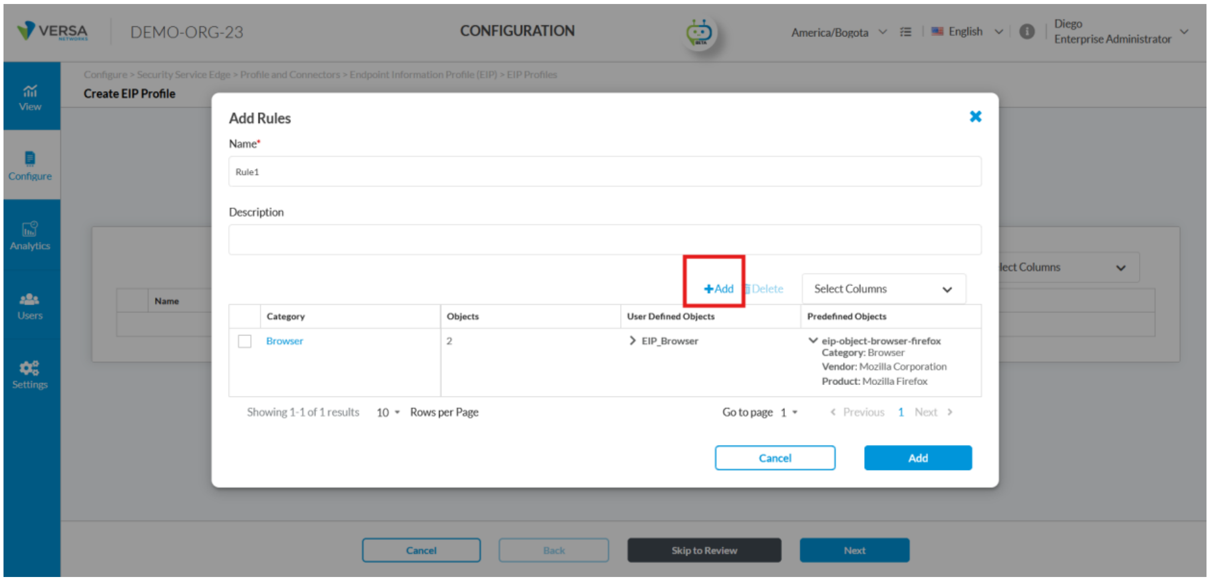
Name*: Rule1

Description:

	Category	Objects	User Defined Objects	Predefined Objects
□	Browser	2	EIP_Browser	eip-object-browser-firefox **Category:** Browser **Vendor:** Mozilla Corporation **Product:** Mozilla Firefox

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next

+ **Add** if it requires more than one.



Add Rules

Name*

Rule1

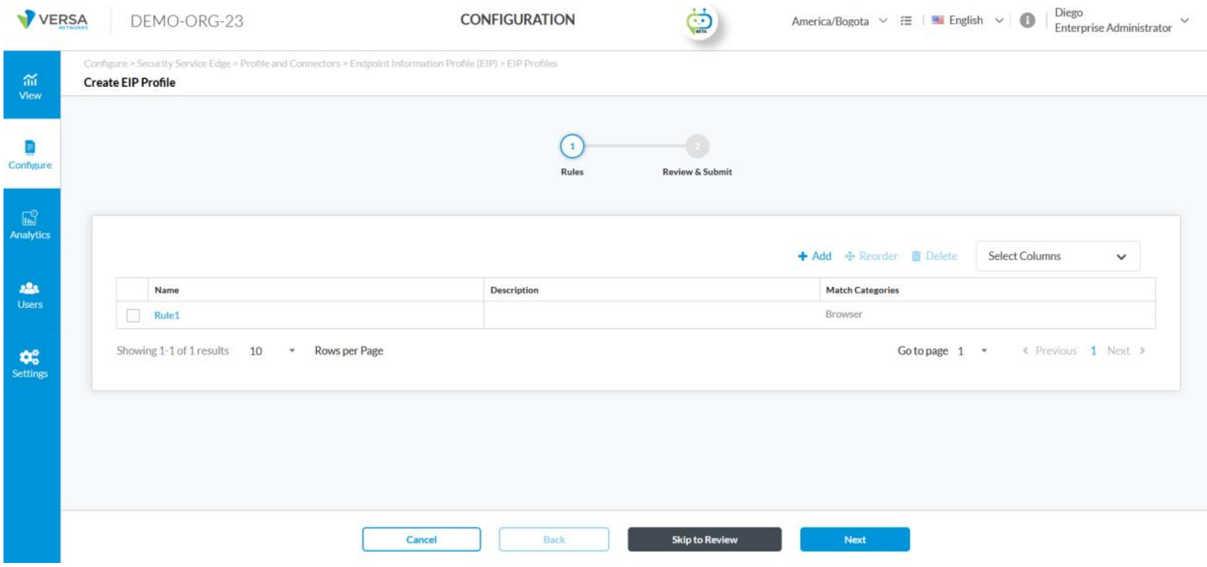
Description

	Category	Objects	User Defined Objects	Predefined Objects
□	Browser	2	> EIP_Browser	eip-object-browser-firefox **Category:** Browser **Vendor:** Mozilla Corporation **Product:** Mozilla Firefox

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next

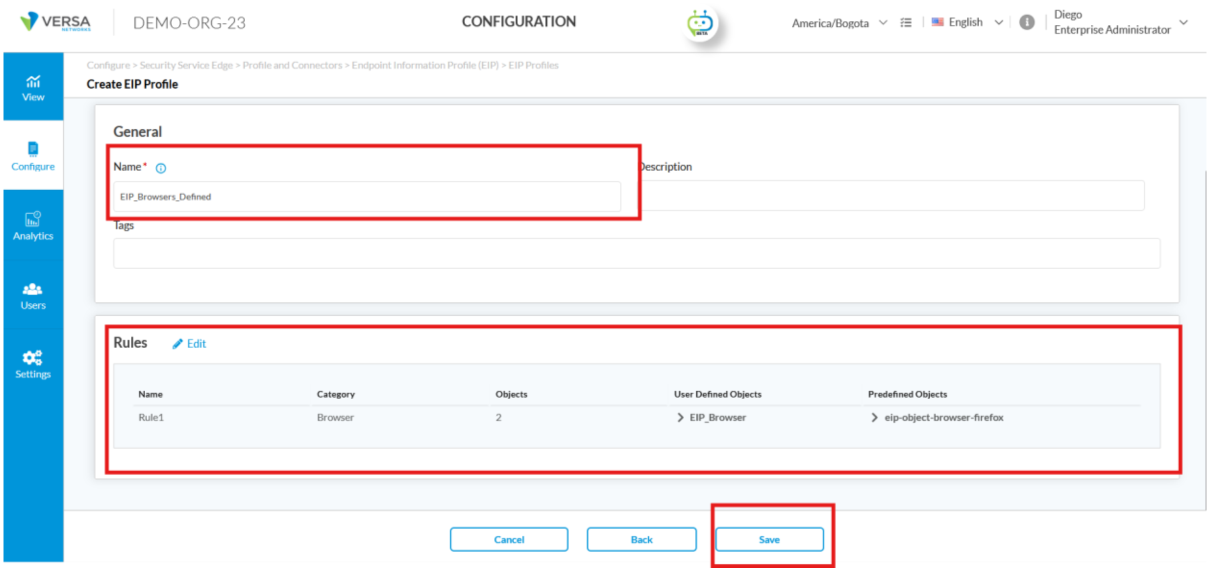
Step 4: Review and Save

- After adding all necessary rules, click **“Next”** or **“Skip to Review”**.
- On the **Review & Submit** screen, verify the name, description, and categories.
- Click **Save** to create the profile.



	Name	Description	Match Categories
□	Rule1		Browser

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Create EIP Profile

General

Name*: EIP_Browsers_Defined

Description:

Tags:

Rules

Name	Category	Objects	User Defined Objects	Predefined Objects
Rule1	Browser	2	EIP_Browser	eip-object-browser-firefox

Configure EIP Agent Profiles

An EIP Agent Profile defines the conditions and categories that the SASE client uses to extract security and posture information from an endpoint device for continuous evaluation.

To collect endpoint posture information, you must associate an **EIP Agent Profile** with a Secure Access Rule.

As a best practice, the EIP Agent Profile and the EIP profile attached to the same Secure Access Policy should be the same.

The process flows as follows:

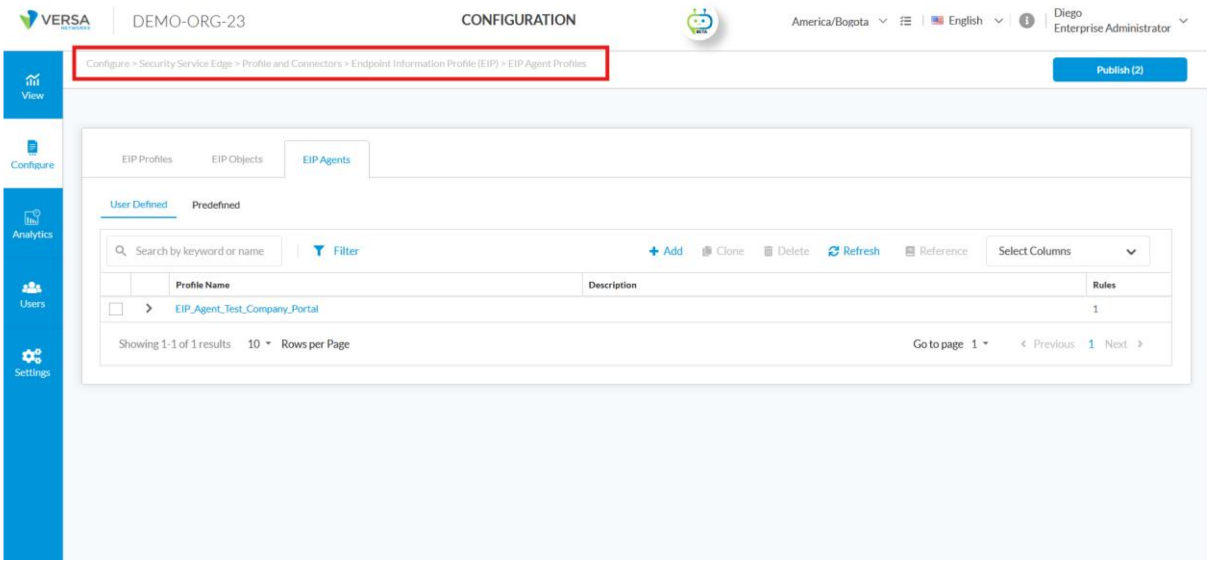
1. **An EIP Agent Profile** is associated with a policy to trigger the collection of endpoint data.
   a. For a Secure Client Access (SCA) policy, you associate the EIP Agent Profile with an SCA rule.
   b. For a SASE Portal policy, when you configure a SASE Portal policy, you associate the agent profile with the enforcement action in the policy.
   c. (Example, versa recommended) to associate with the rule.
2. Data Collection and Enforcement:
   a. After an endpoint device registers and matches a policy rule with an associated EIP Agent Profile, the Versa SASE Client receives the profile.
   b. The client then collects information according to the conditions defined in the EIP Agent Profile.

c. This information is reported on the SASE gateway.

d. The gateway evaluates the information and enforces the security policy. For example, if the profile checks for mandatory antivirus software and the client reports it is missing, the gateway can deny the connection and display a message to the user.

Note: If you make changes to an EIP Agent Profile, the Versa SASE client must be reregistered for the changes to take effect

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

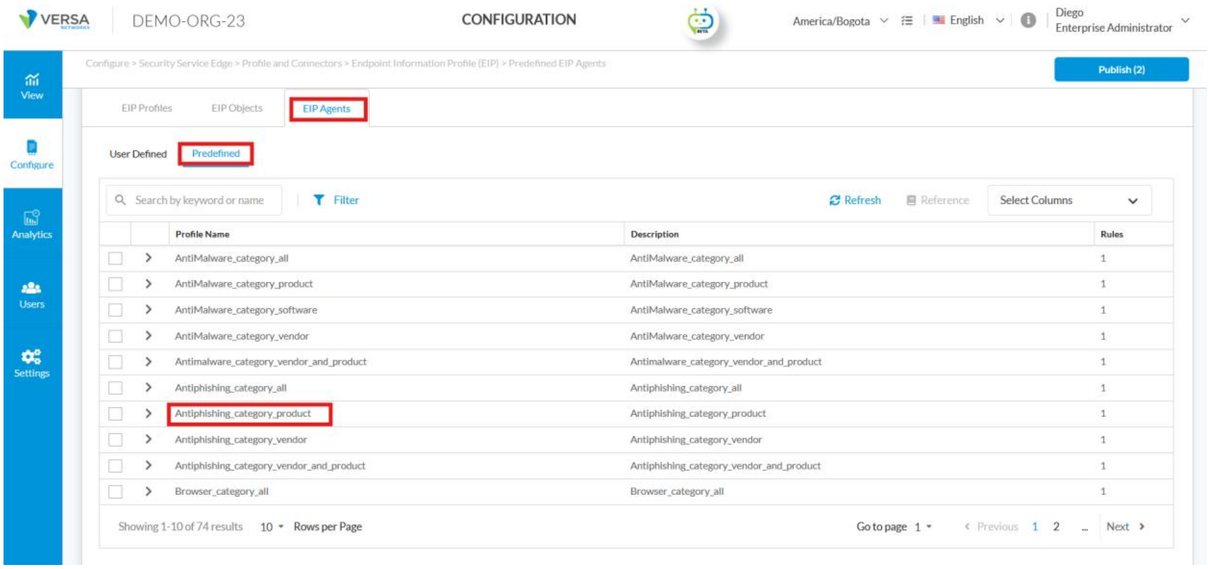


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Profile Name	Description	Rules
EIP_Agent_Test_Company_Portal		1

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next

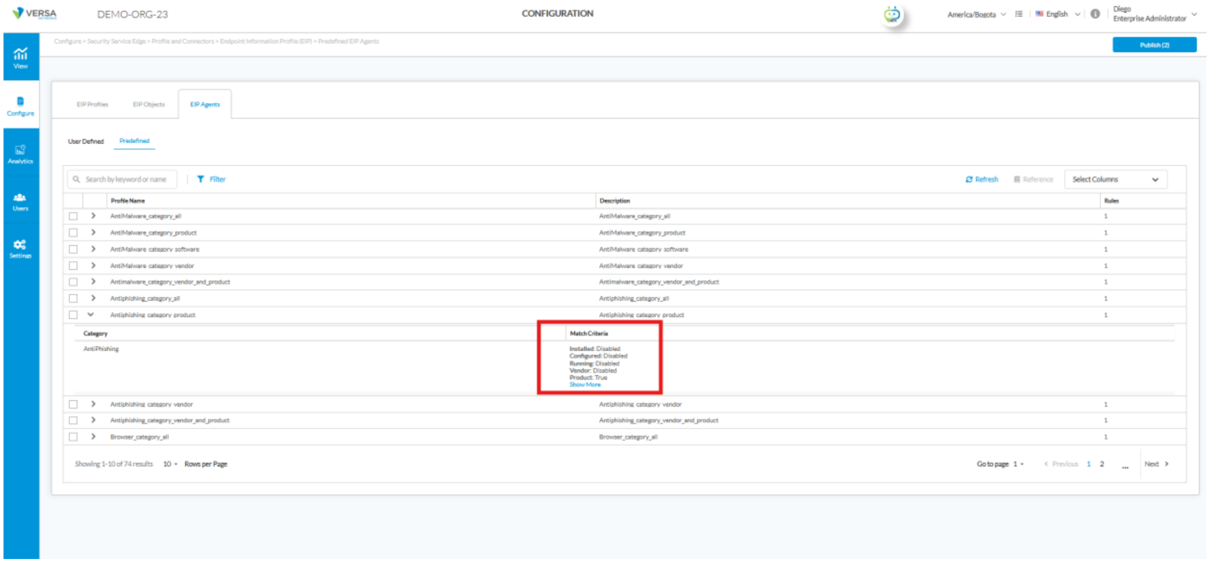
To demonstrate how to review an EIP agent profile, the example **Antiphishing_category_product** is used. This profile gathers details about anti-phishing software, including its installation status, configuration, and running state.



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > Predefined EIP Agents

Profile Name	Description	Rules
AntiMalware_category_all	AntiMalware_category_all	1
AntiMalware_category_product	AntiMalware_category_product	1
AntiMalware_category_software	AntiMalware_category_software	1
AntiMalware_category_vendor	AntiMalware_category_vendor	1
Antimalware_category_vendor_and_product	Antimalware_category_vendor_and_product	1
Antiphishing_category_all	Antiphishing_category_all	1
Antiphishing_category_product	Antiphishing_category_product	1
Antiphishing_category_vendor	Antiphishing_category_vendor	1
Antiphishing_category_vendor_and_product	Antiphishing_category_vendor_and_product	1
Browser_category_all	Browser_category_all	1

Showing 1-10 of 74 results 10 Rows per Page Go to page 1 Previous 1 2 ... Next



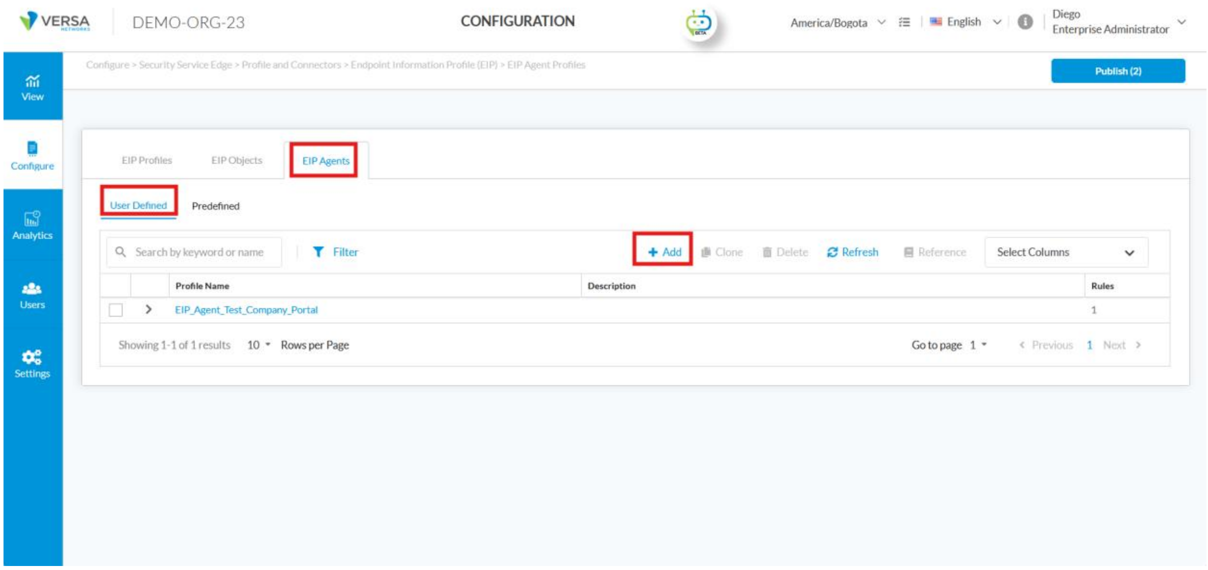
Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > Predefined EIP Agents

Profile Name	Description	Rules
AntiMalware_category_all	AntiMalware_category_all	1
AntiMalware_category_product	AntiMalware_category_product	1
AntiMalware category software	AntiMalware category software	1
AntiMalware category vendor	AntiMalware category vendor	1
Antimalware_category_vendor_and_product	Antimalware_category_vendor_and_product	1
Antiphishing_category_all	Antiphishing_category_all	1
Antiphishing category product	Antiphishing category product	1
Antiphishing category vendor	Antiphishing category vendor	1
Antiphishing_category_vendor_and_product	Antiphishing_category_vendor_and_product	1
Browser_category_all	Browser_category_all	1

Category	Match Criteria
AntiPhishing	Installed: Disabled Configured: Disabled Running: Disabled Vendor: Disabled Product: True Show More

Showing 1-10 of 74 results 10 Rows per Page Go to page 1 Previous 1 2 ... Next

To create User defined following the next steps: navigate to **Configure > SASE > Settings > Endpoint Information Profile (EIP) > EIP Agent Profiles** then User defined and click + **Add**.



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Profile Name	Description	Rules
EIP_Agent_Test_Company_Portal		1

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next

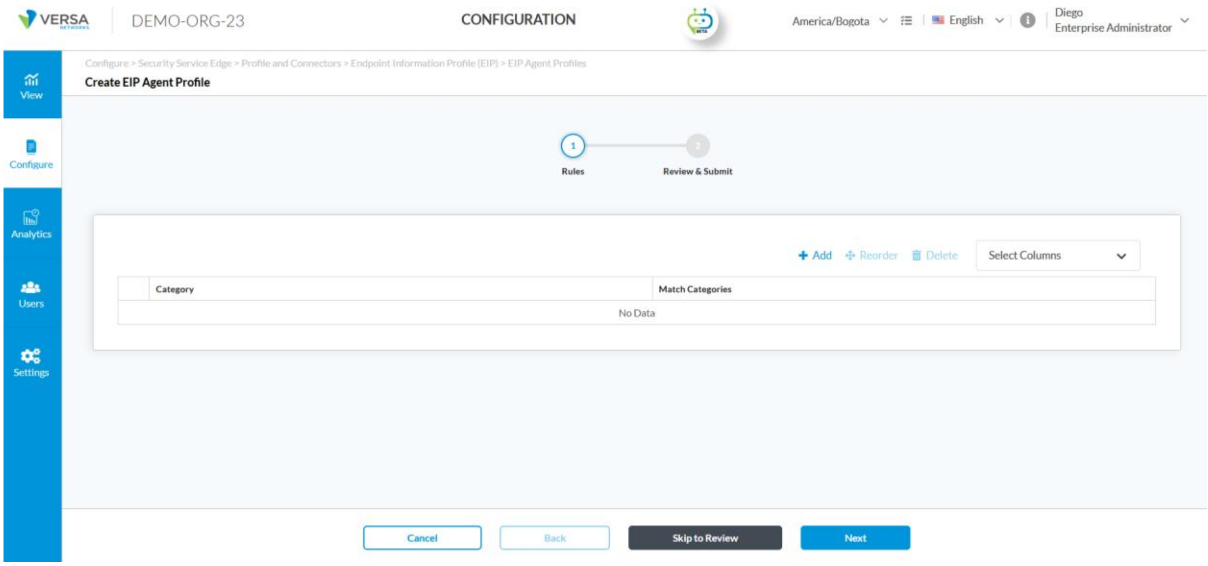
for creating a Versa EIP Agent Profile using the AntiMalware, Browser, and Firewall categories as examples.

Step 2: Add Rule — AntiMalware Category

1. In the **Rules** section, click **+ Add**.
2. From the **Category** dropdown, select **AntiMalware**.
3. Configure the following options:

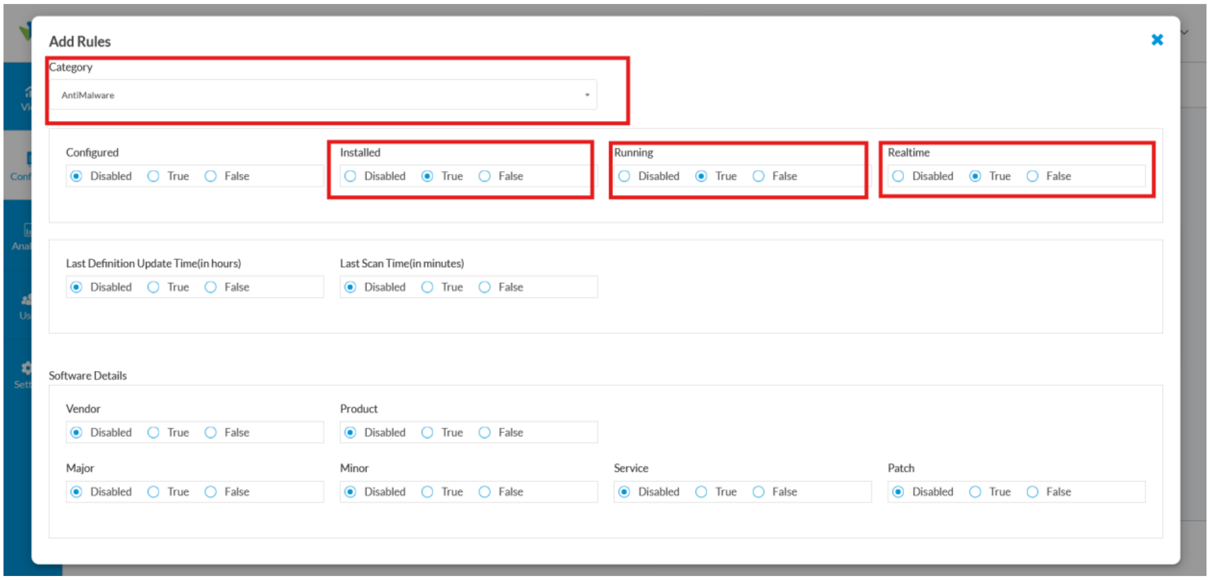
- Installed: True
- Running: True
- **Realtime:** True (optional but recommended)
- (Other fields like Vendor, Product, or version can be left as Disabled unless required)

4. Click **Add** to save the AntiMalware rule.



Create EIP Agent Profile

Category	Match Categories
No Data	



Add Rules

Category: AntiMalware

Configured: ● Disabled ○ True ○ False

Installed: ○ Disabled ● True ○ False

Running: ○ Disabled ● True ○ False

Realtime: ○ Disabled ● True ○ False

Last Definition Update Time(in hours): ● Disabled ○ True ○ False

Last Scan Time(in minutes): ● Disabled ○ True ○ False

Software Details

Vendor: ● Disabled ○ True ○ False

Product: ● Disabled ○ True ○ False

Major: ● Disabled ○ True ○ False

Minor: ● Disabled ○ True ○ False

Service: ● Disabled ○ True ○ False

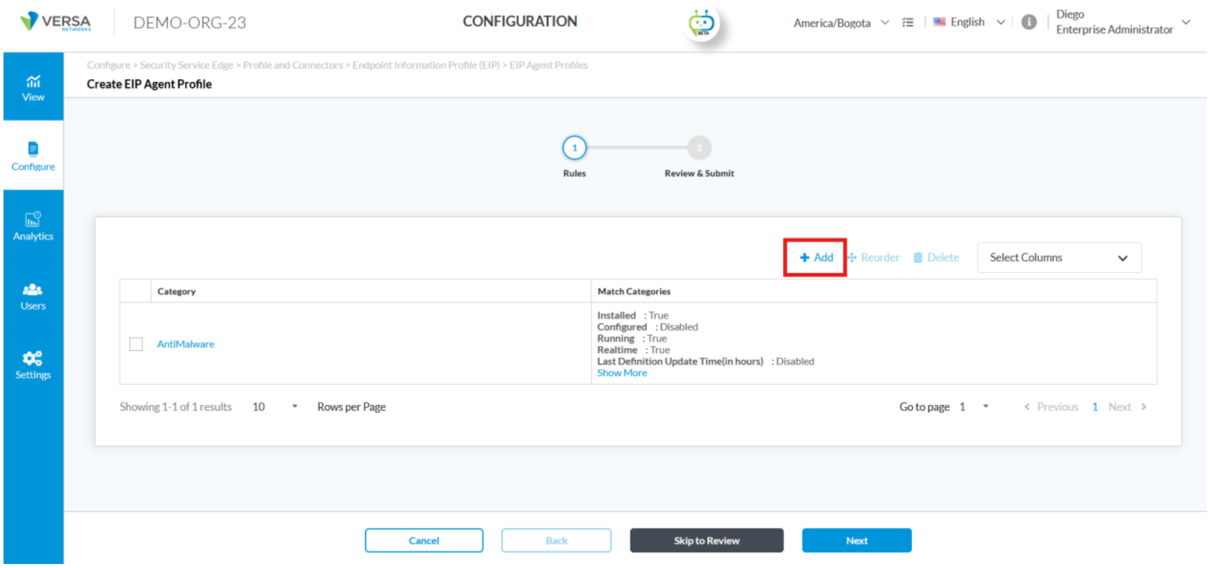
Patch: ● Disabled ○ True ○ False

Step 3: Add Rule — Browser Category

1. Again, click **+ Add** in the Rules section.
2. From the **Category** dropdown, select **Browser**.
3. Configure the following options:

- Installed: True
- **Running:** (optional, set to True if you want to detect currently running browsers)
- Leave other fields as Disabled unless you want to target a specific browser.

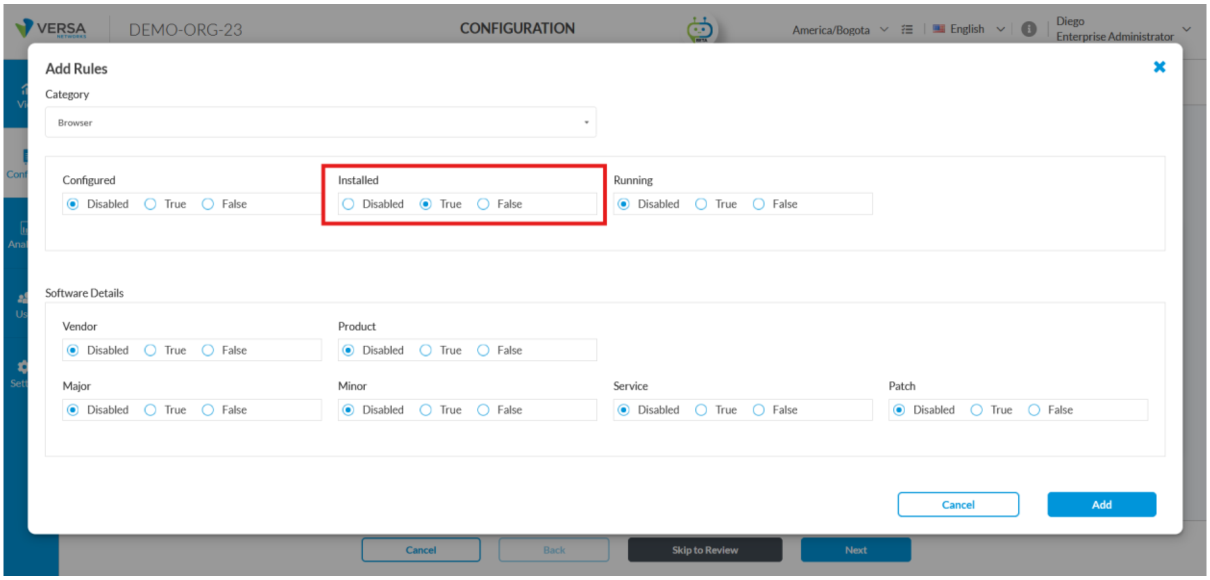
4. Click **Add** to save the Browser rule.



Create EIP Agent Profile

	Category	Match Categories
□	AntiMalware	Installed : True Configured : Disabled Running : True Realtime : True Last Definition Update Time(in hours) : Disabled Show More

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next



Add Rules

Category: Browser

Configured: ● Disabled ○ True ○ False

Installed: ○ Disabled ● True ○ False

Running: ● Disabled ○ True ○ False

Software Details

Vendor: ● Disabled ○ True ○ False

Product: ● Disabled ○ True ○ False

Major: ● Disabled ○ True ○ False

Minor: ● Disabled ○ True ○ False

Service: ● Disabled ○ True ○ False

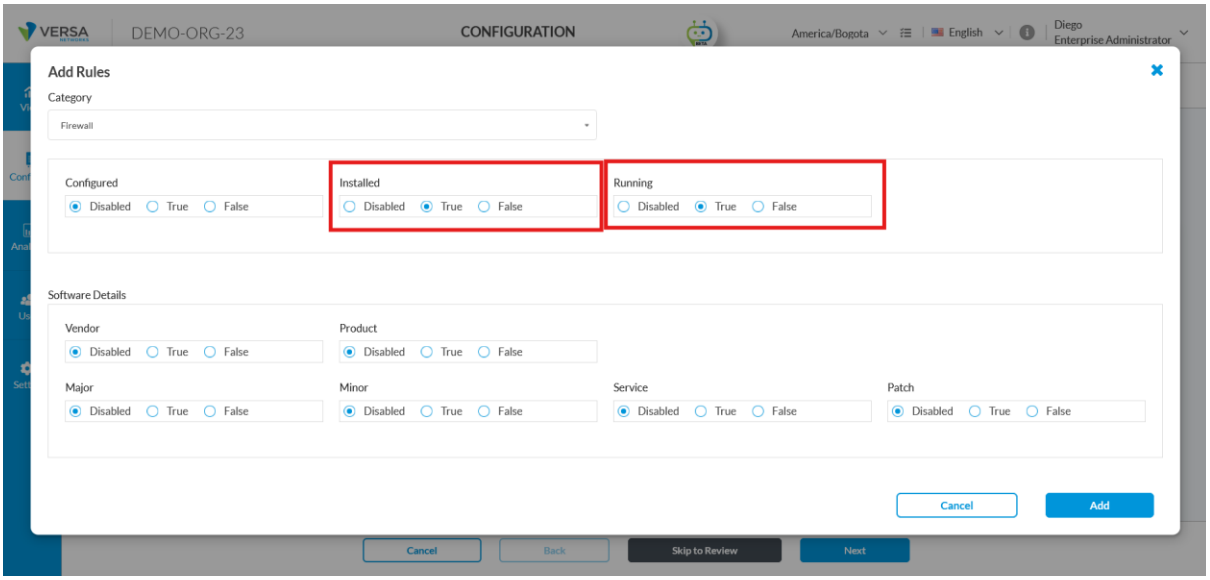
Patch: ● Disabled ○ True ○ False

Step 4: Add Rule — Firewall Category

1. Click **+ Add** again.
2. Select **Firewall** from the **Category** dropdown.
3. Configure the following:

- Installed: True
- Running: True
- Optionally, configure Vendor/Product/version fields if you want to match a specific firewall.

4. Click **Add** to save the Firewall rule.



Add Rules

Category: Firewall

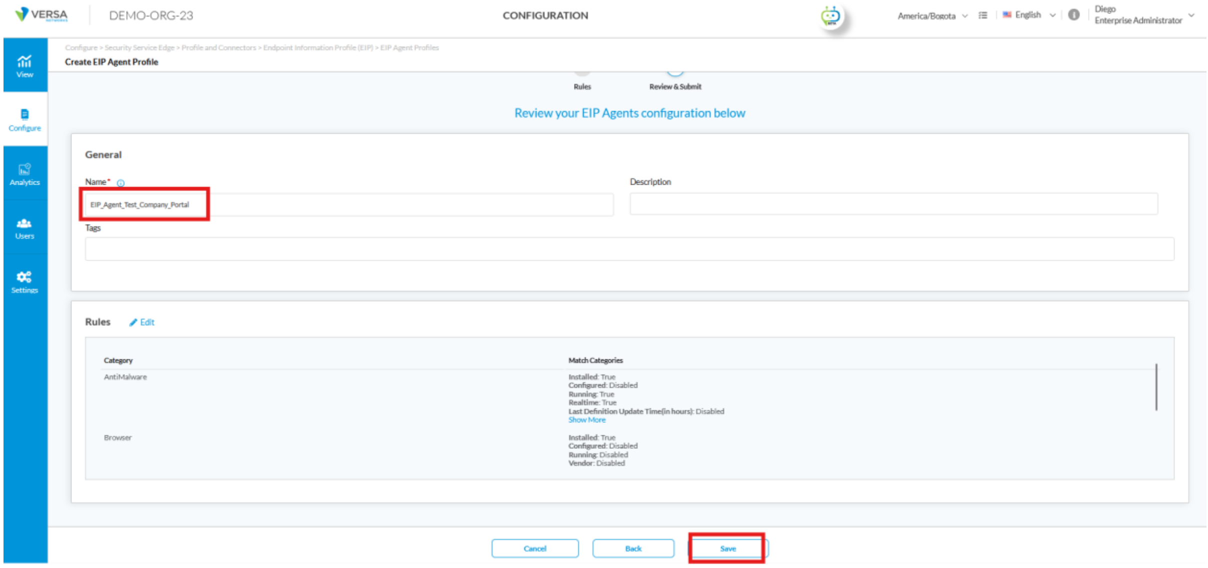
Configured ● Disabled ○ True ○ False	Installed ○ Disabled ● True ○ False	Running ○ Disabled ● True ○ False

Software Details

Vendor ● Disabled ○ True ○ False	Product ● Disabled ○ True ○ False		
Major ● Disabled ○ True ○ False	Minor ● Disabled ○ True ○ False	Service ● Disabled ○ True ○ False	Patch ● Disabled ○ True ○ False

Step 5: Review and Submit the Profile

1. After adding all three rules (AntiMalware, Browser, Firewall), click **Next** or **Skip to Review**.
2. On the Review and Submit screen:
   - Enter the **Profile Name** (e.g., EIP_Agent_Test_Company_Portal).
   - (Optional) Add a **Description** for the profile.
3. Click **Submit** to save the profile.



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Create EIP Agent Profile

Rules | Review & Submit

Review your EIP Agents configuration below

General

Name*: EIP_Agent_Test_Company_Portal

Description:

Tags:

Rules ✎ Edit

Category	Match Categories
AntiMalware	Installed: True Configured: Disabled Running: True Realtime: True Last Definition Update Time(in hours): Disabled Show More
Browser	Installed: True Configured: Disabled Running: Disabled Vendor: Disabled

Cancel | Back | Save

Configure EIP on Secure Client Access Rules

In Versa SASE, **Secure Access policy rules** enable administrators to enforce access controls based on the endpoint's security posture. This is achieved by associating two key components within the rule:

1. **EIP Profile** – A match condition defines **how the collected data** is evaluated against a set of predefined or user-defined posture conditions in the attached profiles.
2. **EIP Agent Profile** – Defines **what posture information** the SASE client should collect from the endpoint post registration (e.g., Antimalware status, Firewall state, installed browsers).

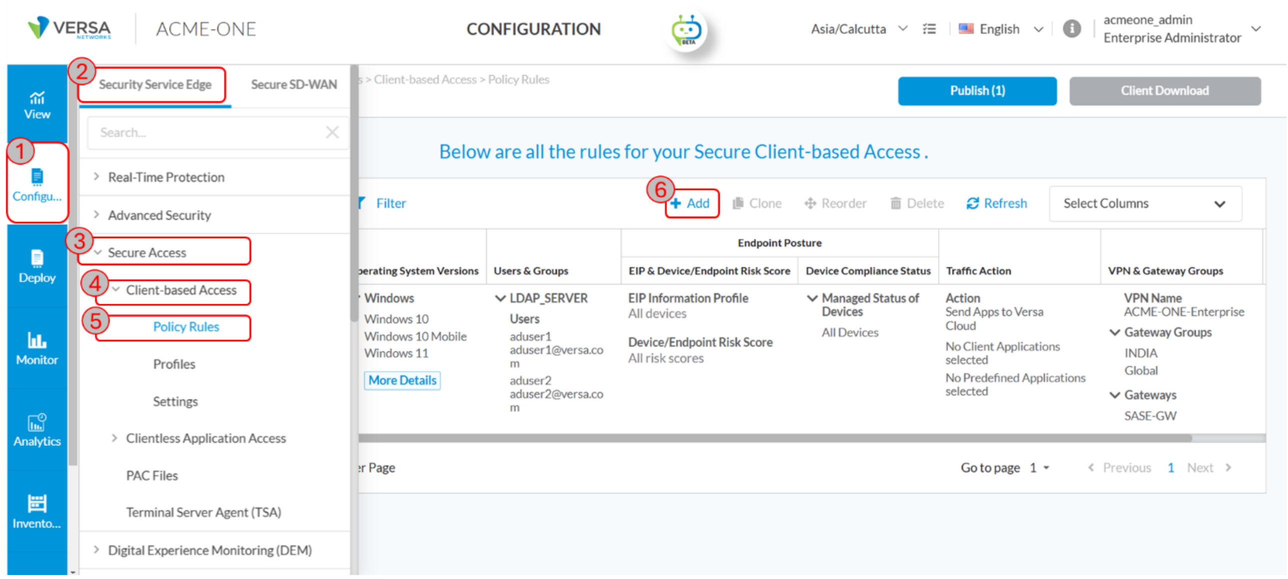
When a Secure Client-based Access rule is triggered, the following flow occurs:

- On the **first connection**, the **EIP Profile** is required to validate compliance before access is granted.
- If the **EIP Agent Profile** is configured in the Secure Access match rule, it is then pushed to the client for **continuous posture evaluation** during subsequent sessions.
- The client collects posture data based on the categories defined in the EIP Agent Profile.
- The collected data is then evaluated at the SSE Gateway using the logic defined in the associated **EIP Profile**.
- The **EIP Profile enforces compliance**: if the endpoint posture satisfies the conditions, access

is granted; if not, access is denied regardless of the rest of the rule's configuration.

This approach ensures that only endpoints with compliant posture—such as running antivirus, enabled firewall, or verified software—can connect and then access protected resources.

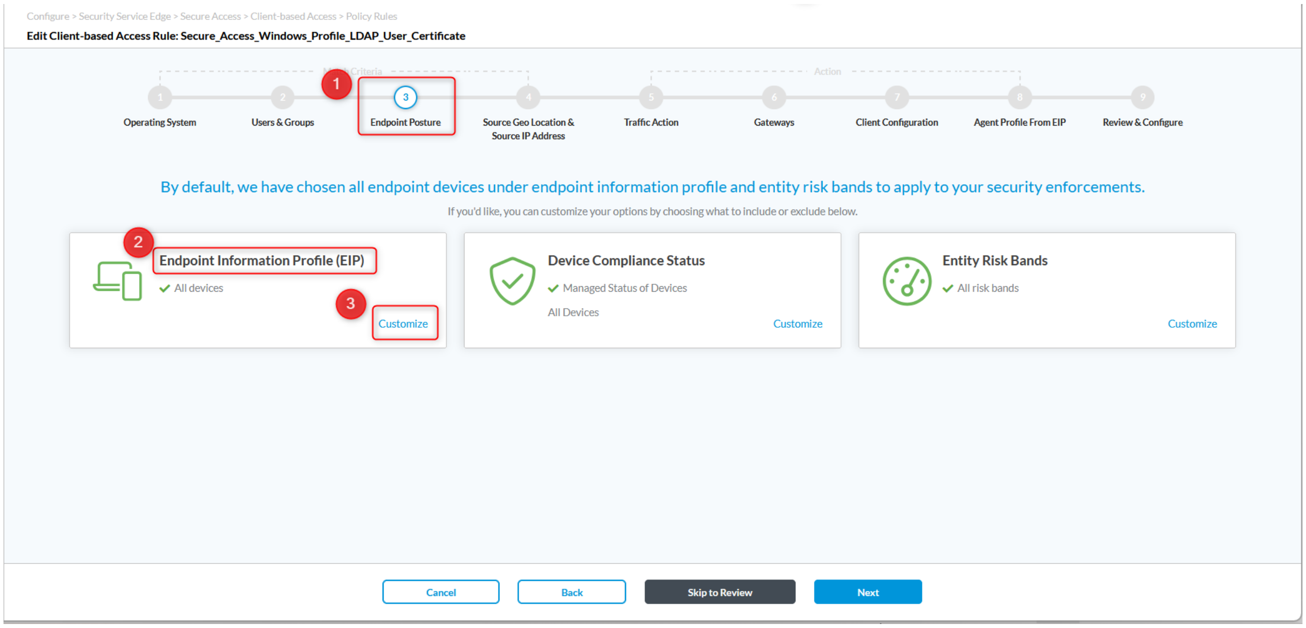
To configure a secure client access rule, navigate to Configure > Security Service Edge > Secure Access > Client-based Access > Rules and click on +Add.



Below are all the rules for your Secure Client-based Access .

erating System Versions	Users & Groups	Endpoint Posture		Traffic Action	VPN & Gateway Groups
		EIP & Device/Endpoint Risk Score	Device Compliance Status		
Windows Windows 10 Windows 10 Mobile Windows 11 More Details	LDAP_SERVER Users aduser1 aduser1@versa.com aduser2 aduser2@versa.com	EIP Information Profile All devices Device/Endpoint Risk Score All risk scores	Managed Status of Devices All Devices	Action Send Apps to Versa Cloud No Client Applications selected No Predefined Applications selected	VPN Name ACME-ONE-Enterprise Gateway Groups INDIA Global Gateways SASE-GW

In the rule editor, go to the **Endpoint Posture** step and locate the **Endpoint Information Profile (EIP)** tile. Click **Customize**.



Edit Client-based Access Rule: Secure_Access_Windows_Profile_LDAP_User_Certificate

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

Endpoint Information Profile (EIP): ✓ All devices

Device Compliance Status: ✓ Managed Status of Devices, All Devices

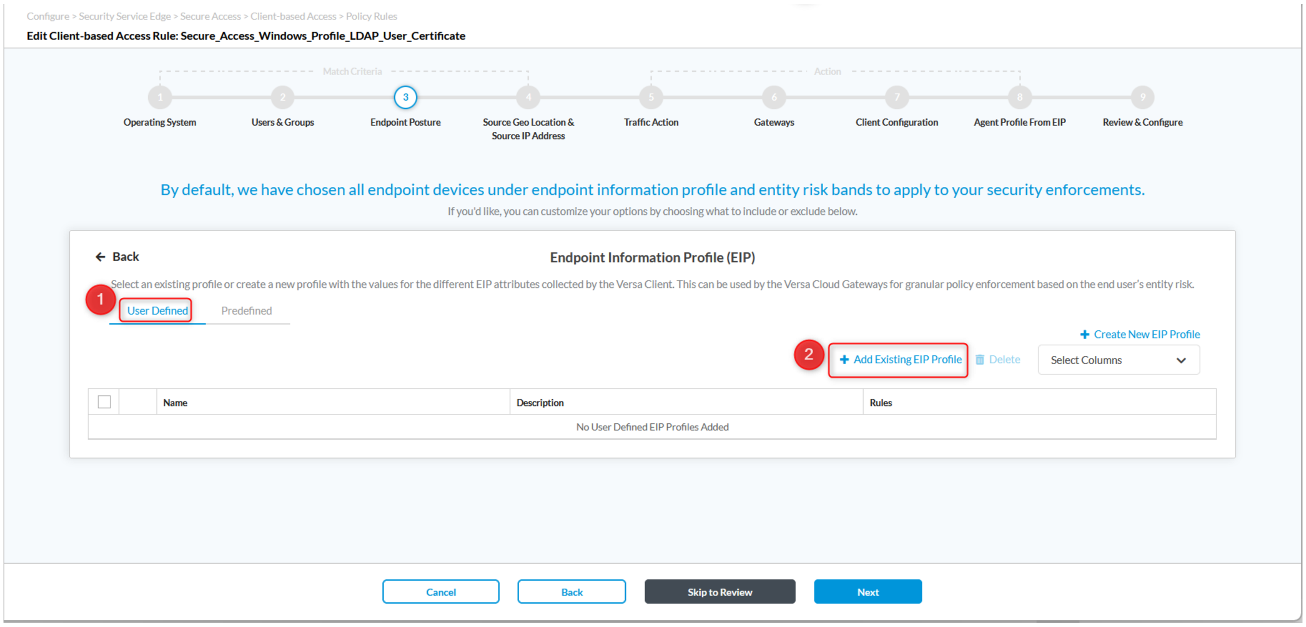
Entity Risk Bands: ✓ All risk bands

Note: In a Secure Access rule, all **Match Criteria** are evaluated using **AND** logic.

Inside the **Endpoint Posture** tab, multiple EIP Profiles follow **OR** logic — the endpoint needs to match **only one** of the selected EIP Profiles for this tab to pass.

In the Endpoint Information Profile (EIP) window:

- Select **User Defined** if you want to use one of your custom EIP profiles, or
- Select **Predefined** to use a Versa-provided profile. Then click **Add Existing EIP Profile**.



Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure_Access_Windows_Profile_LDAP_User_Certificate

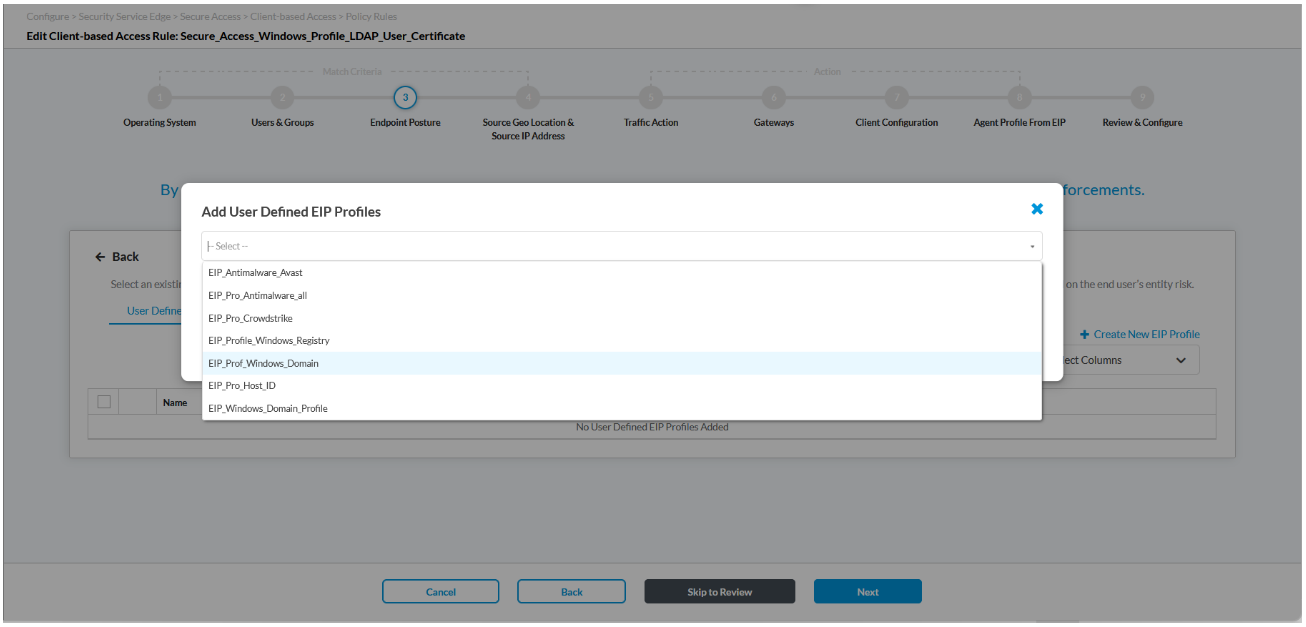
By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

Endpoint Information Profile (EIP)

Select an existing profile or create a new profile with the values for the different EIP attributes collected by the Versa Client. This can be used by the Versa Cloud Gateways for granular policy enforcement based on the end user's entity risk.

□		Name	Description	Rules
		No User Defined EIP Profiles Added		



Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure_Access_Windows_Profile_LDAP_User_Certificate

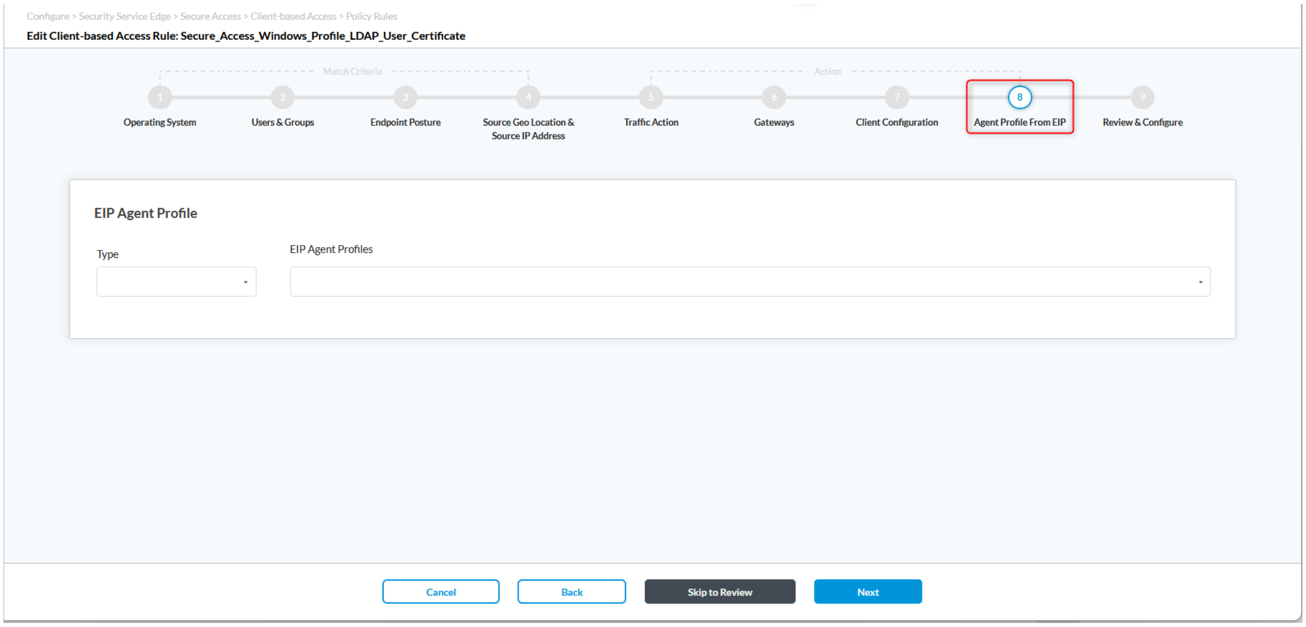
Add User Defined EIP Profiles

-- Select --

- EIP_Antimalware_Avast
- EIP_Pro_Antimalware_all
- EIP_Pro_Crowdstrike
- EIP_Profile_Windows_Registry
- EIP_Prof_Windows_Domain
- EIP_Pro_Host_ID
- EIP_Windows_Domain_Profile

After selecting the **EIP Profile**, the next step in the Secure Access rule is to optionally apply an **EIP Agent Profile**. This step is not mandatory — the EIP Agent Profile is only required if you want the SASE client to perform **continuous posture evaluation**.
When configured, the EIP Agent Profile defines which posture attributes the SASE client must collect after registration, ensuring that ongoing posture updates are sent to the gateway for evaluation.

In the rule editor, go to the **Agent Profile From EIP** section under *Action*. This is where you can optionally attach an EIP Agent Profile for continuous posture evaluation.



Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure_Access_Windows_Profile_LDAP_User_Certificate

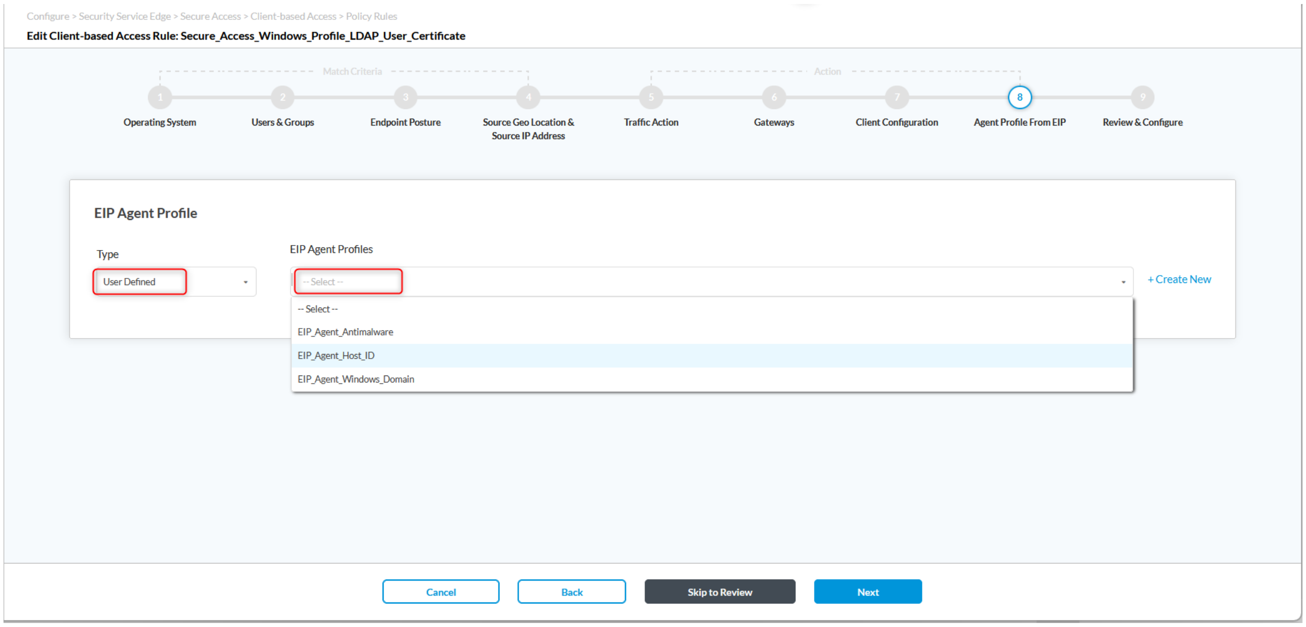
EIP Agent Profile

Type

EIP Agent Profiles

Select the profile type Open the **Type** dropdown and choose **User Defined** or **Predefined**, depending on if want to uses predefined Versa the Agent Profile or it was created.

Choose the EIP Agent Profile From the **EIP Agent Profiles** dropdown, select the profile you want to apply to this Secure Access rule.



Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure_Access_Windows_Profile_LDAP_User_Certificate

EIP Agent Profile

Type: User Defined

EIP Agent Profiles: -- Select --

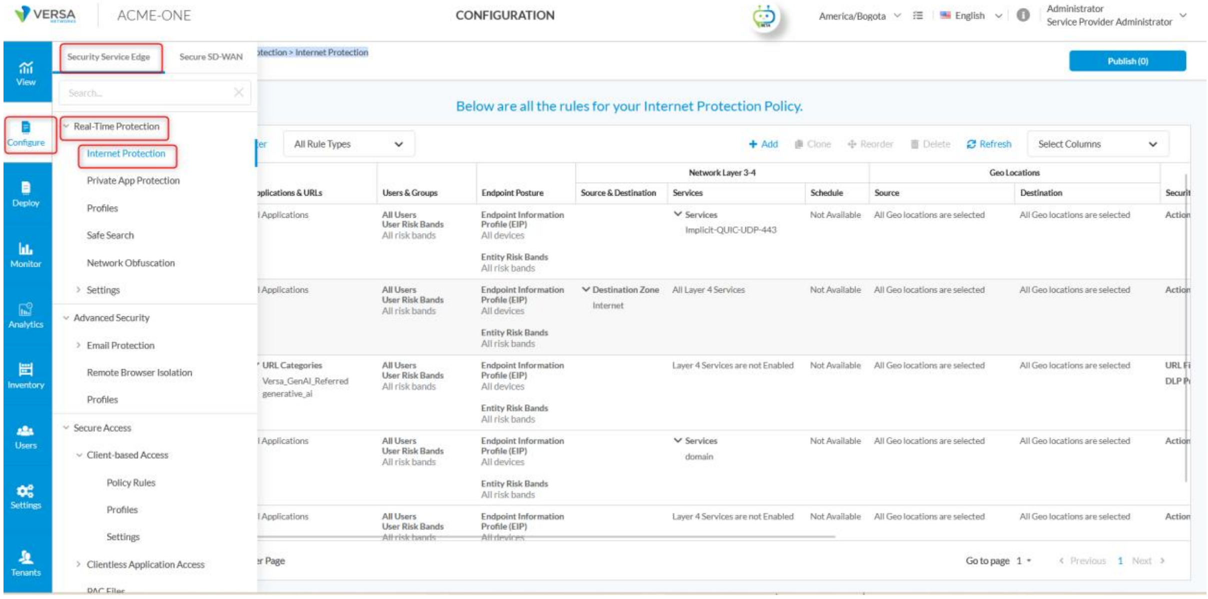
- -- Select --
- EIP_Agent_Antimalware
- EIP_Agent_Host_ID
- EIP_Agent_Windows_Domain

Continue with the rule configuration Click **Next** to move to the final review and complete the Secure Access rule.

Configure EIP on Real-Time Protection Rules

In Versa SSE, Real-Time Protection Rules use EIP Profiles as match conditions to evaluate endpoint posture attributes (AV, firewall, disk encryption, etc.) reported by the SASE client. The SSE Gateway continuously validates this telemetry against the EIP Profile associated with the Internet Protection rule. If the device falls out of compliance, the rule will allow access that does not match, triggering the blocking of all new access requests from that endpoint until posture is restored.

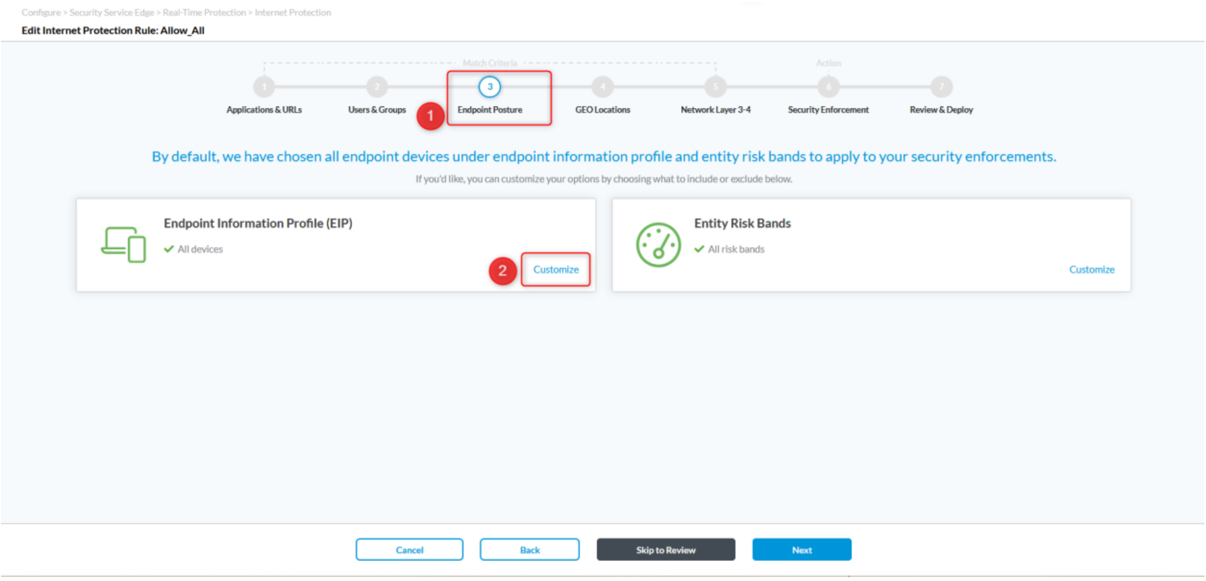
To configure a secure client access rule, navigate to **Configure > Security Service Edge > Real-Time Protection > Internet Protection and click on +Add** or from the list of Internet Protection rules, select the rule you want to edit, then **Edit**.



Below are all the rules for your Internet Protection Policy.

			Network Layer 3-4			Geo Locations		
plications & URLs	Users & Groups	Endpoint Posture	Source & Destination	Services	Schedule	Source	Destination	Securit
l Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands		Services Implicit-QUIC-UDP-443	Not Available	All Geo locations are selected	All Geo locations are selected	Action
l Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands	Destination Zone Internet	All Layer 4 Services	Not Available	All Geo locations are selected	All Geo locations are selected	Action
URL Categories Versa_GenAI_Referred generative_ai	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands		Layer 4 Services are not Enabled	Not Available	All Geo locations are selected	All Geo locations are selected	URL Fi DLP P
l Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices Entity Risk Bands All risk bands		Services domain	Not Available	All Geo locations are selected	All Geo locations are selected	Action
l Applications	All Users User Risk Bands All risk bands	Endpoint Information Profile (EIP) All devices		Layer 4 Services are not Enabled	Not Available	All Geo locations are selected	All Geo locations are selected	Action

In the Match Criteria go to Endpoint posture then click Customize on the Endpoint Information Profile (EIP).



By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

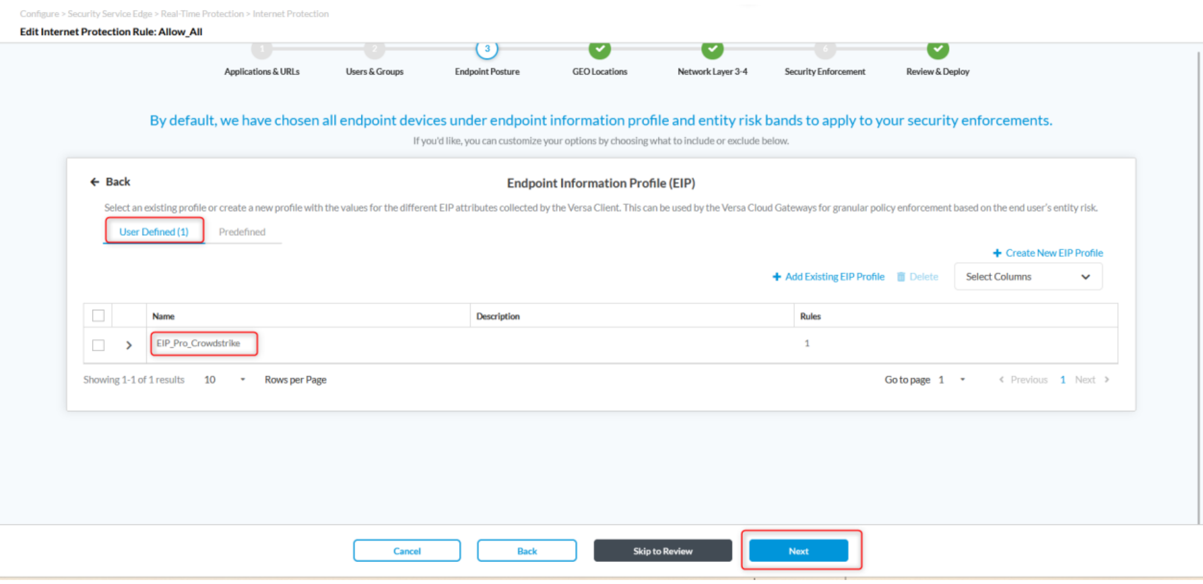
If you'd like, you can customize your options by choosing what to include or exclude below.

Endpoint Information Profile (EIP)
✓ All devices

Entity Risk Bands
✓ All risk bands

The Endpoint Information Profile (EIP) window appears.

- Choose **User Defined** to select a custom EIP profile (for example, **EIP_Pro_Crowdstrike**), or **Predefined** to use a Versa default profile.
- Select the desired profile and click **Add**.
- Click **Next**.



Configure > Security Service Edge > Real-Time Protection > Internet Protection

Edit Internet Protection Rule: Allow_All

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

← Back

Endpoint Information Profile (EIP)

Select an existing profile or create a new profile with the values for the different EIP attributes collected by the Versa Client. This can be used by the Versa Cloud Gateways for granular policy enforcement based on the end user's entity risk.

□		Name	Description	Rules
□	>	EIP_Pro_Crowdstrike		1

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next

Click **Save**, then **Publish** to apply the policy.

Key points

- EIP Posture Update Frequency:
    - By default, the SASE client sends posture data to gateways every 10 minutes.
    - The interval determines how often **EIP data is transmitted** to the gateway.
- Full Data Updates:

EIP posture updates are **always sent as complete datasets**—**not incremental**—because gateways **do not cache** previous posture information.

- Posture Change Detection:
    - If the device's posture remains unchanged, no update is sent.
    - However, the SASE client **continues collecting data** and **detecting changes** by comparing data hash values.
    - Only upon detecting a change does the client transmit a new posture update to the gateway.
- Real-Time Detection (Selective Categories):

For specific categories like **Anti-Malware**, **real-time posture monitoring** can be enabled. In this mode, the SASE client collects and sends updates to the gateway **every 10 minutes** when changes are detected.

- Pre-Registration Posture Collection:

The **"Versa Recommended" EIP agent profile** is embedded in the SASE client. It begins **collecting all specified endpoint posture information prior to portal registration**, ensuring enforcement policies are applied from the moment the client connects.

EIP Scenario-Based Use Cases for Windows

The following provides some use cases for configuring EIP validation on Windows Hosts.

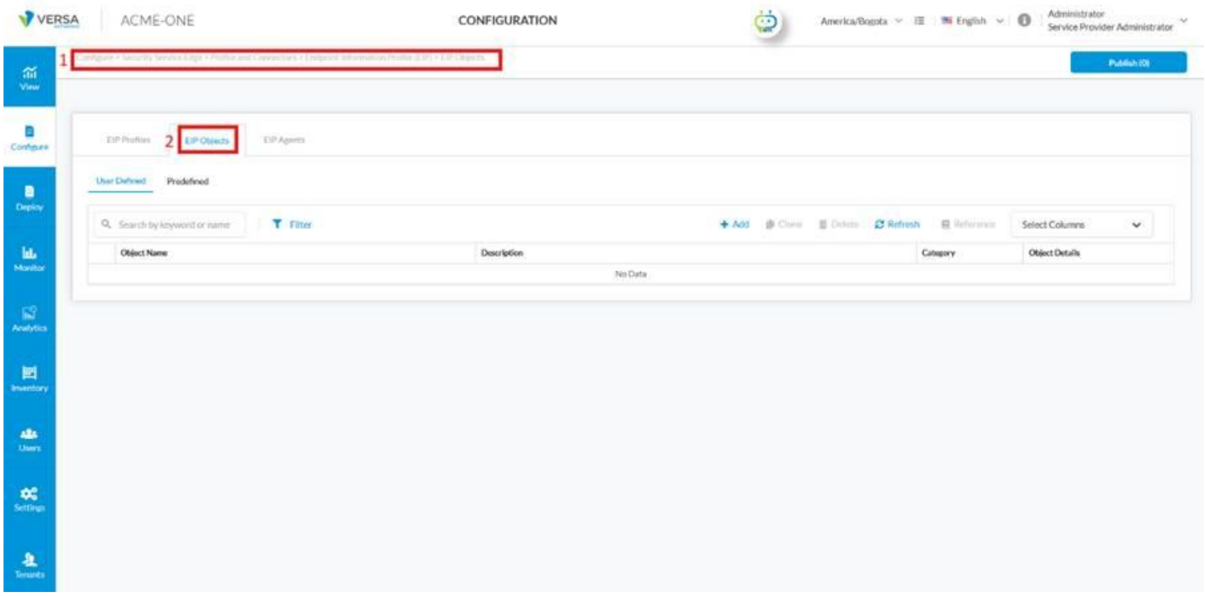
Windows Registry Path and Key

Leveraging Windows registry paths and keys within an EIP Profile allows administrators to validate the presence or configuration of specific applications on endpoints. This is useful when enforcing access policies based on critical software installations, such as VPN clients or endpoint protection tools not in the Versa EIP object list.

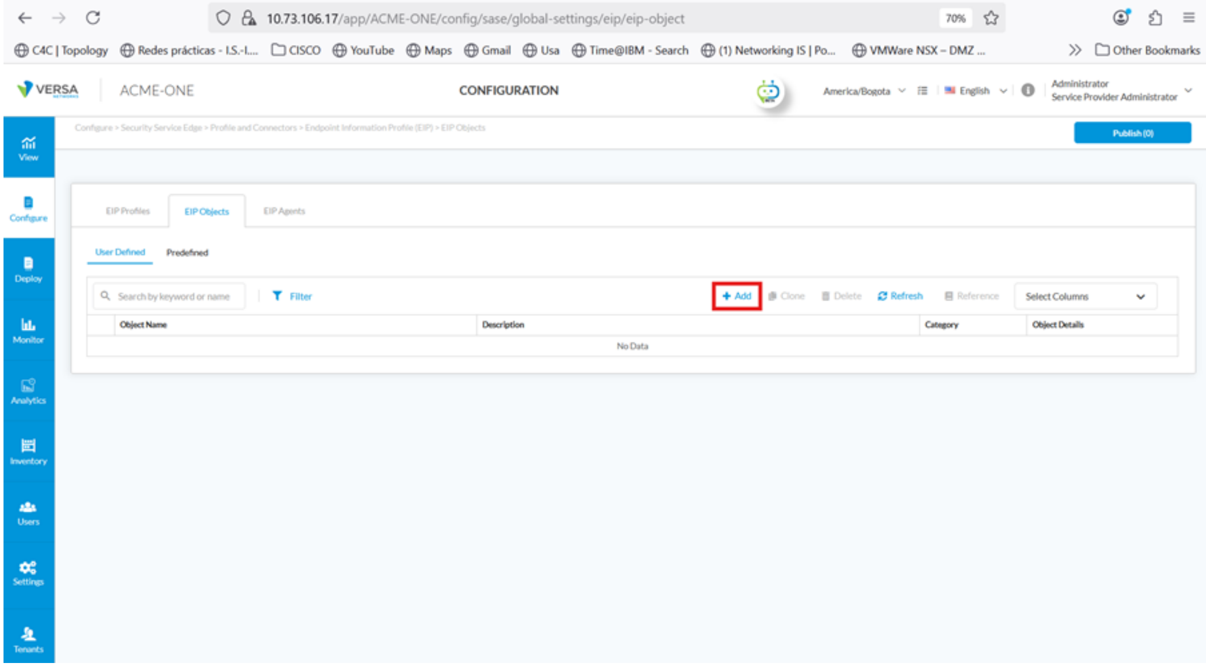
For example, Versa can check a registry path or key to confirm whether an antivirus application (E.g., Avast) is installed. If the key is missing or the value does not match the expected configuration, the endpoint is flagged as non-compliant, and access to corporate resources may be restricted.

Step 1: Create an EIP Object with Windows Registry Path

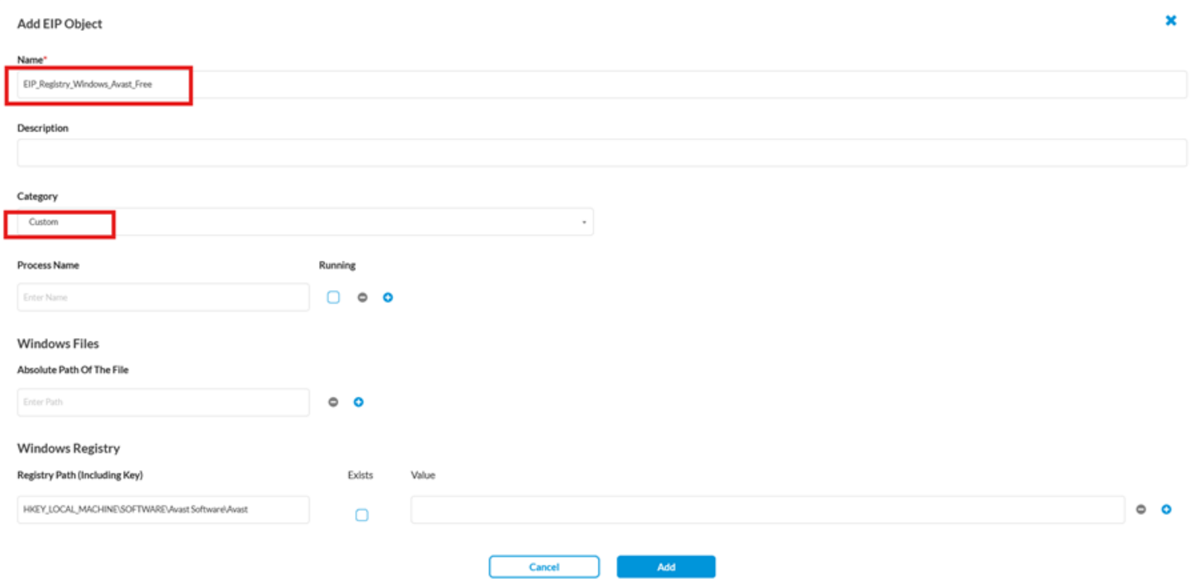
Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Objects



Click on “+ Add” to create a new EIP Object.



Enter a descriptive name for your EIP object. ***Example:*** **EIP_Registry_Windows_Avast_Free.** And Select Custom from the dropdown.



Add EIP Object

Name*: EIP_Registry_Windows_Avast_Free

Description:

Category: Custom

Process Name: Enter Name — Running □

Windows Files

Absolute Path Of The File: Enter Path

Windows Registry

Registry Path (Including Key)	Exists	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Avast Software\Avast	□	

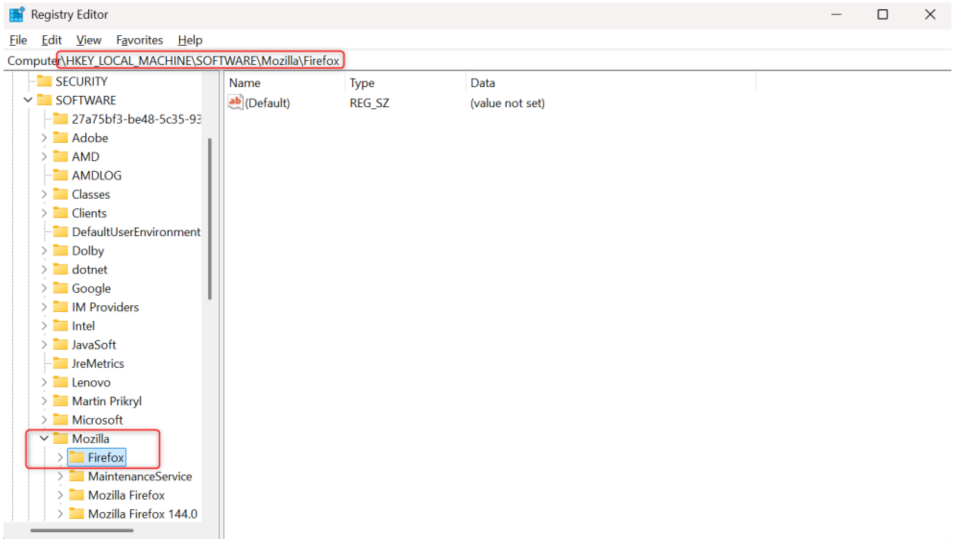
Go to Windows Registry Validation and enter the **full path** of the registry key you want to check ***Example:*** `HKEY_LOCAL_MACHINE\SOFTWARE\Avast Software\Avast`

Steps to Find Registry Path

To find the correct registry path for other applications, open the Windows Registry Editor (regedit) and navigate under one of the following common locations:

- `HKEY_LOCAL_MACHINE\SOFTWARE\[Vendor]\[Product]`
- `HKEY_CURRENT_USER\SOFTWARE\[Vendor]\[Product]`

You can also search for an application name using **Ctrl+F** in Registry Editor. As shown below, you would obtain the path for Firefox as an example. Once identified, copy the full registry path and enter it exactly in the EIP configuration field.

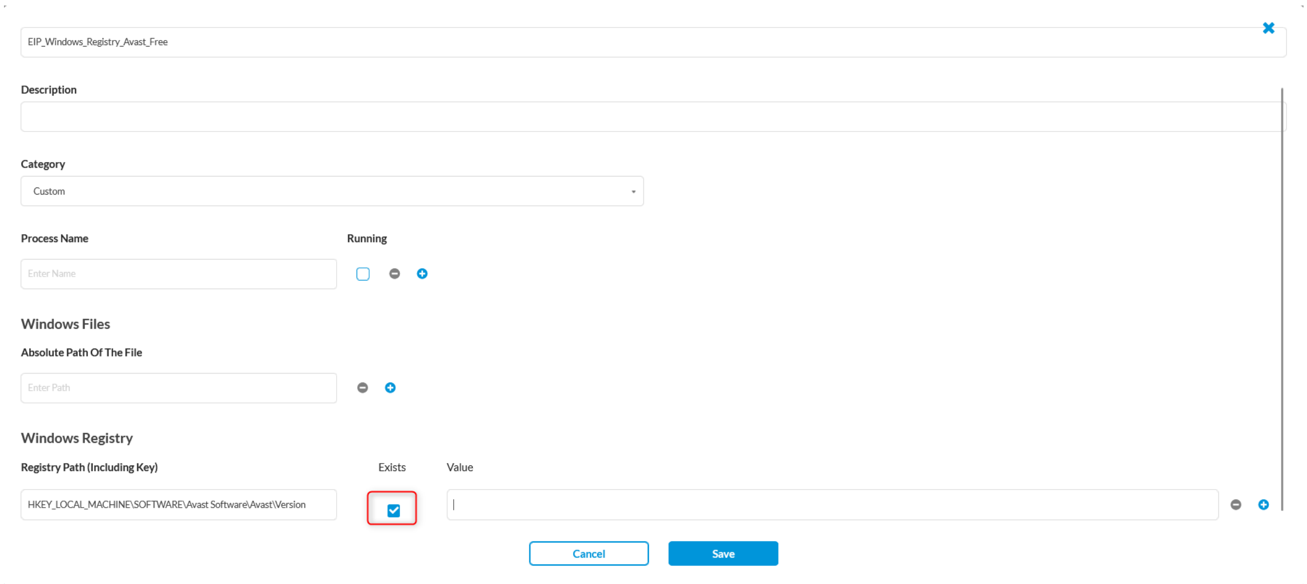


Registry Editor

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Firefox

Name	Type	Data
(Default)	REG_SZ	(value not set)

"Exists" Checkbox: If checked, it verifies that the key exists and, if you enter a value in the **Value** field, it will also validate that the registry key's data matches that specific value. If the **Value** field is left empty, the gateway will validate *only* that the registry key exists. **If "Exists" is unchecked, the registry key is not evaluated at all, and no validation is performed.**



EIP_Windows_Registry_Avast_Free

Description

Category: Custom

Process Name: Enter Name

Running: □

Windows Files

Absolute Path Of The File: Enter Path

Windows Registry

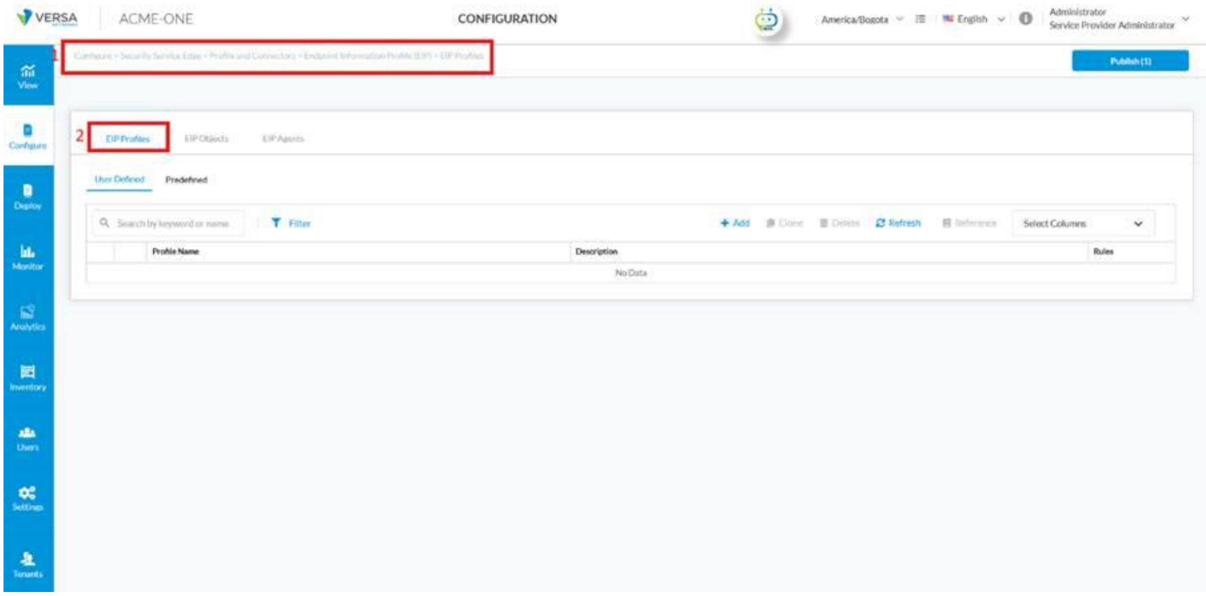
Registry Path (Including Key): HKEY_LOCAL_MACHINE\SOFTWARE\Avast Software\Avast\Version

Exists: ☑

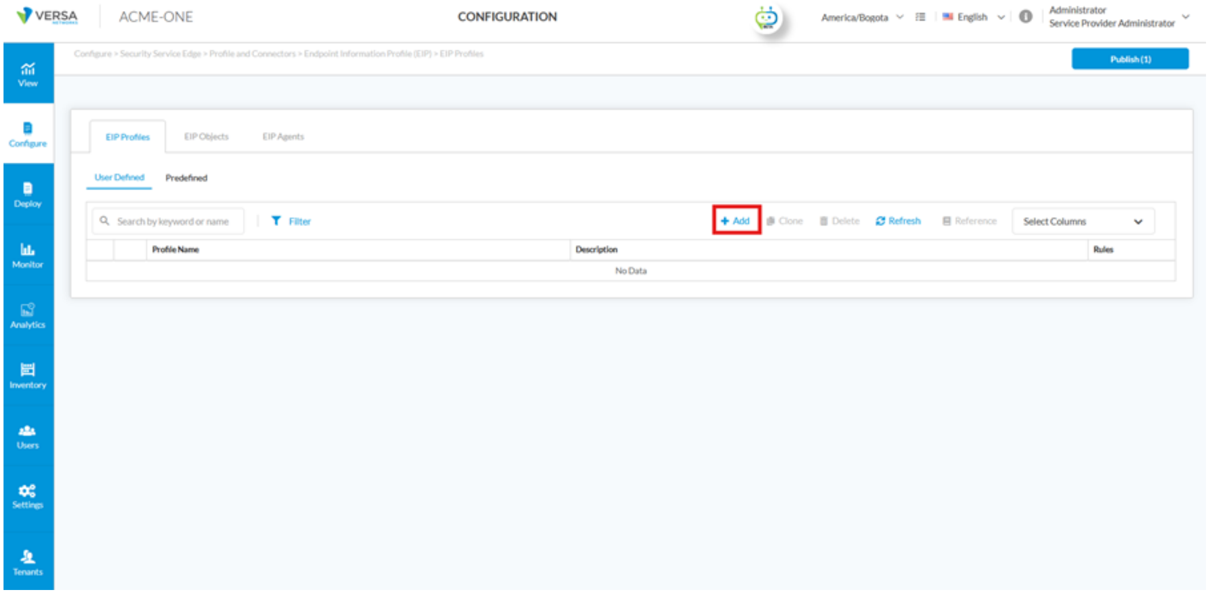
Value: |

Step 2: Create an EIP Profile Using Windows Registry Keys

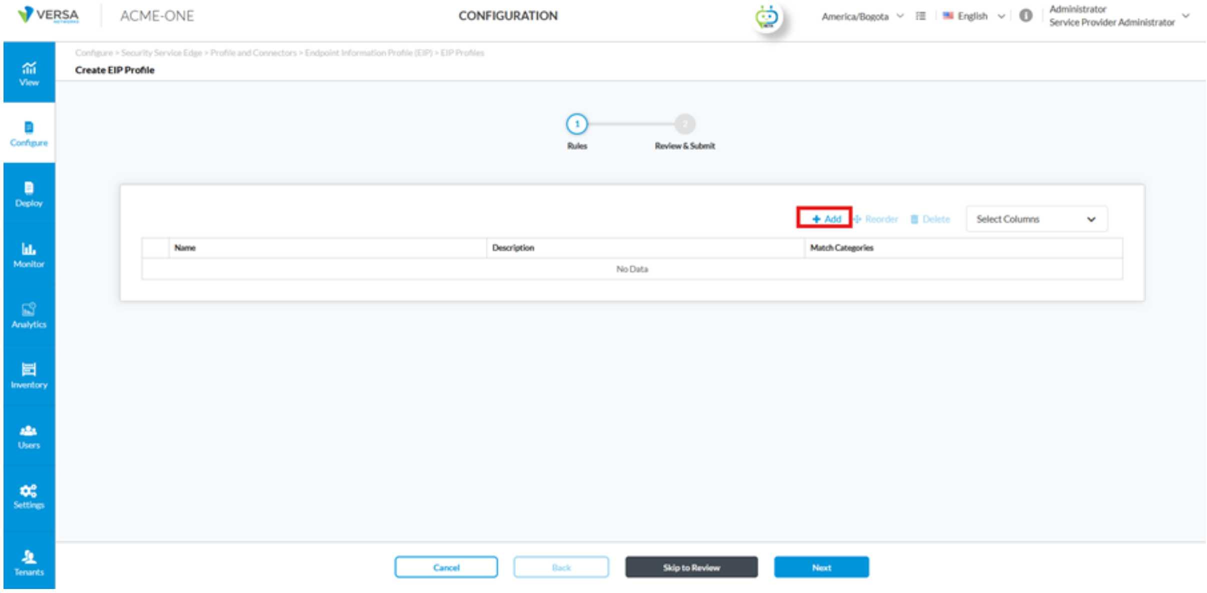
Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles, then go to EIP Profiles.



Click on "+ Add" to start creating a new profile.



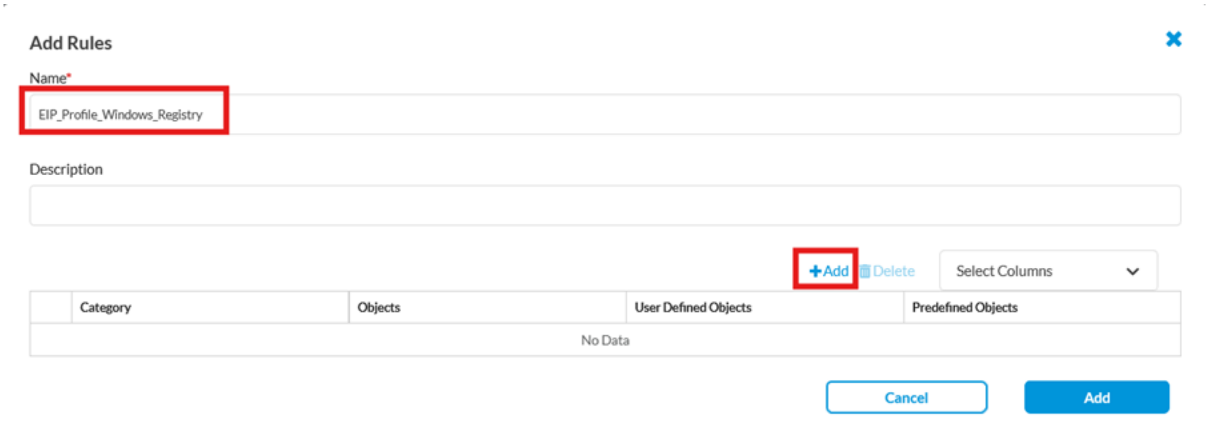
In the **Create EIP Profile** window, Click on "+ Add" to define a new rule.



Enter a Name for your rule, for Example, **EIP_Profile_Windows_Registry**.

You would (Optional) Add a description for clarity.

Click "+ Add" to attach an EIP Object.



Add Rules

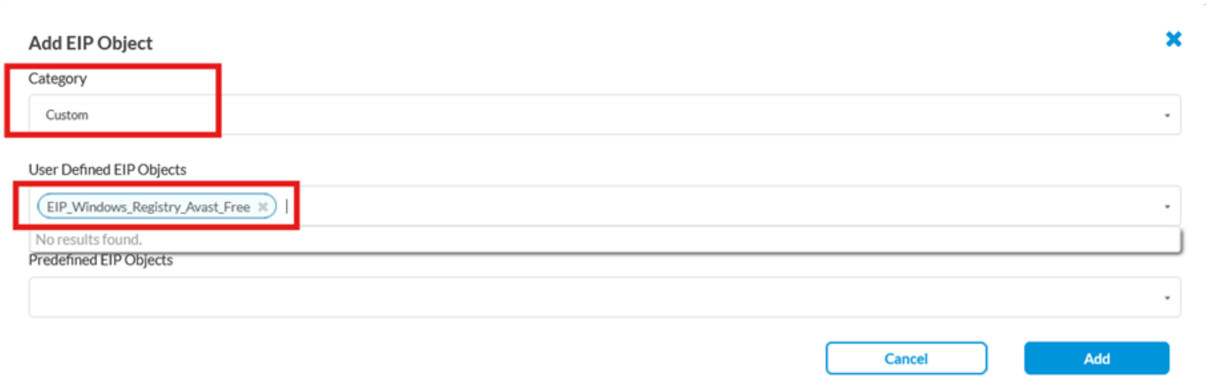
Name*: EIP_Profile_Windows_Registry

Description

	Category	Objects	User Defined Objects	Predefined Objects
	No Data			

In Add EIP Object dialog, choose the Category. Example **Custom**.

Select an existing EIP Object or create a new one. For example, an object was created to verify if Avast Free Antivirus in the previous section.



Add EIP Object

Category: Custom

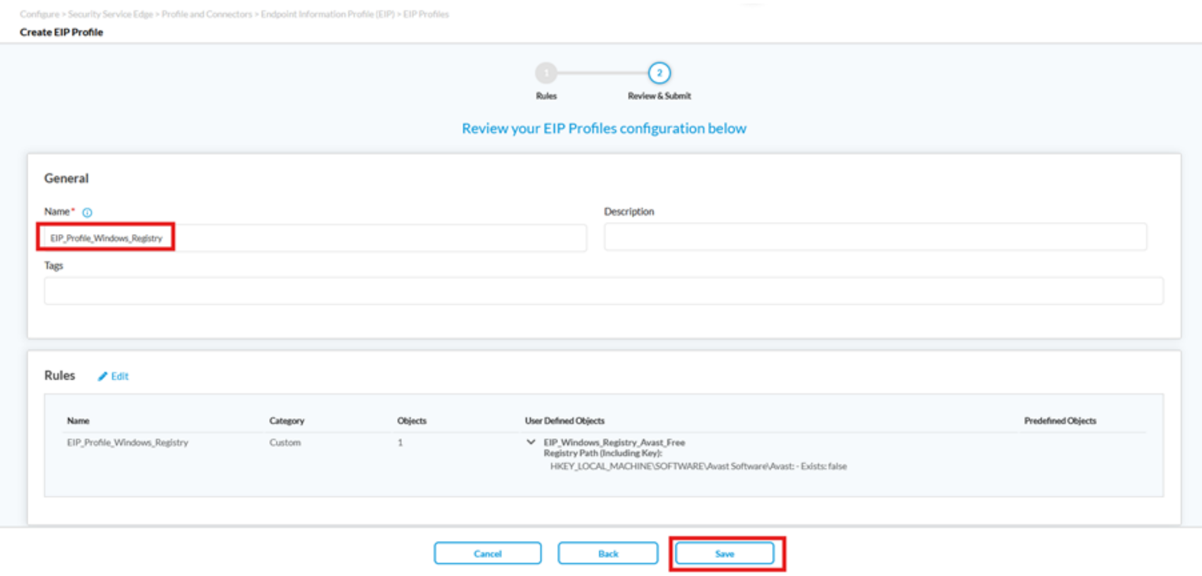
User Defined EIP Objects: EIP_Windows_Registry_Avast_Free

No results found.

Predefined EIP Objects

Click **Next** and then Enter a descriptive name for your EIP object. ***Example:*** **EIP_Profile_Windows_Registry.**

Review and **Save** the Profile creation



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Create EIP Profile

Review your EIP Profiles configuration below

General

Name*: EIP_Profile_Windows_Registry

Description:

Tags:

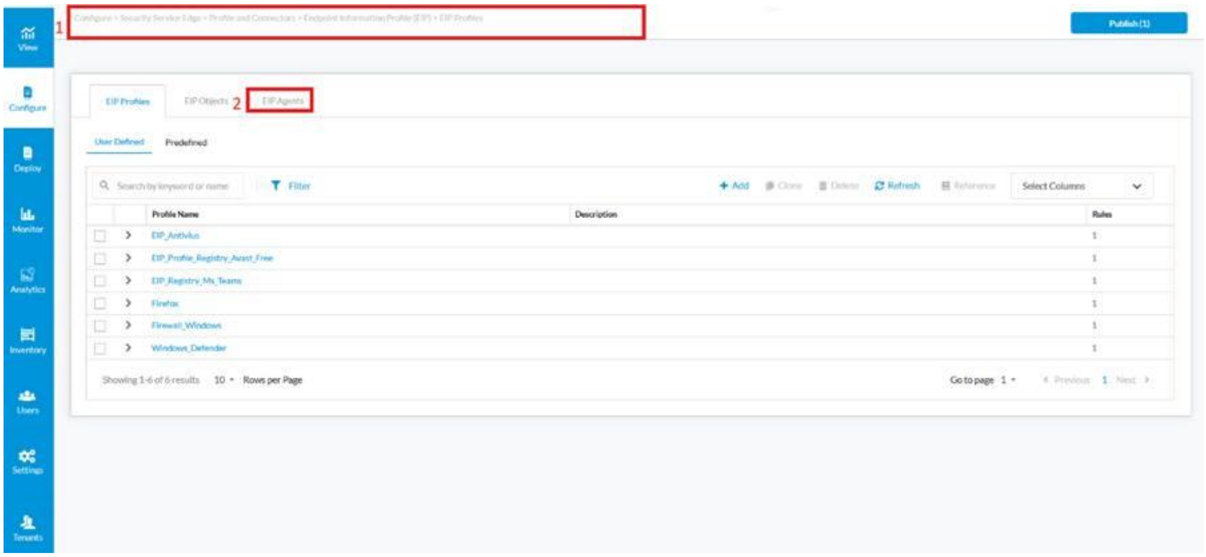
Rules ✎ Edit

Name	Category	Objects	User Defined Objects	Predefined Objects
EIP_Profile_Windows_Registry	Custom	1	EIP_Windows_Registry_Avast_Free Registry Path (Including Key): HKEY_LOCAL_MACHINE\SOFTWARE\Avast Software\Avast: - Exists: false	

Note: After creating the EIP Object and configuring the EIP Profile and Agent Profile, you must apply them to the Secure Access Client policy to enforce device posture validation and continue evaluation.

Step 3: Navigate to the EIP Agent Section

Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Agents

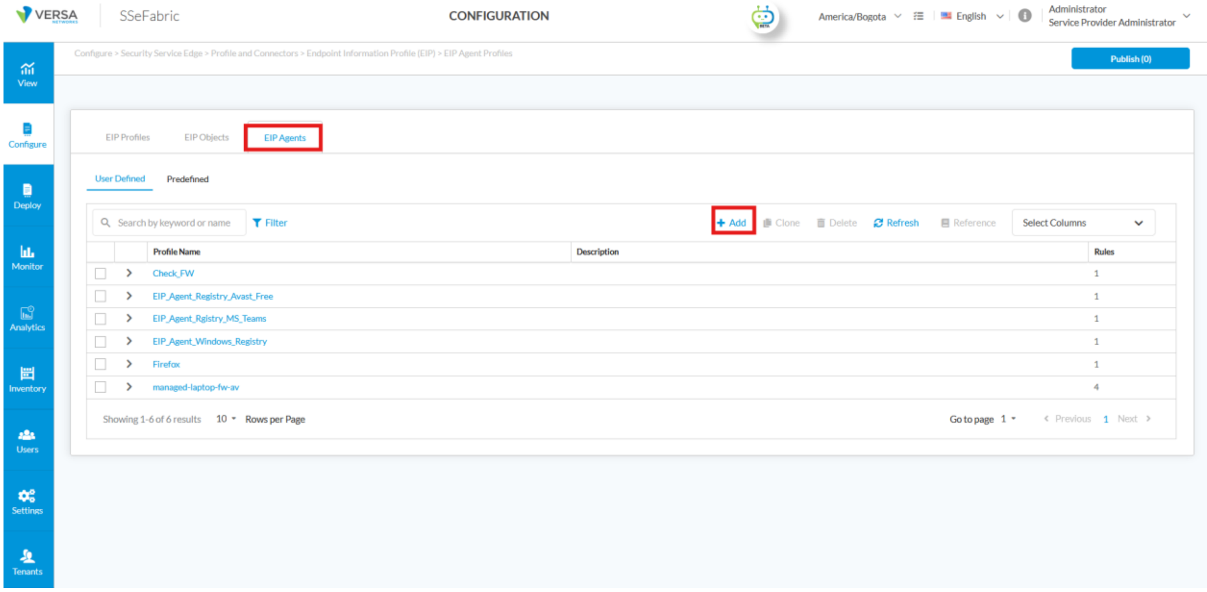


Profile Name	Description	Rules
EIP_Antivirus		1
EIP_Profile_Registry_Avast_Free		1
EIP_Registry_Ms_Teams		1
Firefox		1
Firewall_Windows		1
Windows_Defender		1

Showing 1-6 of 6 results 10 Rows per Page Go to page 1 Previous 1 Next

Step 4: Create an EIP Agent Profile

Click on Add to create a new Agent profile.

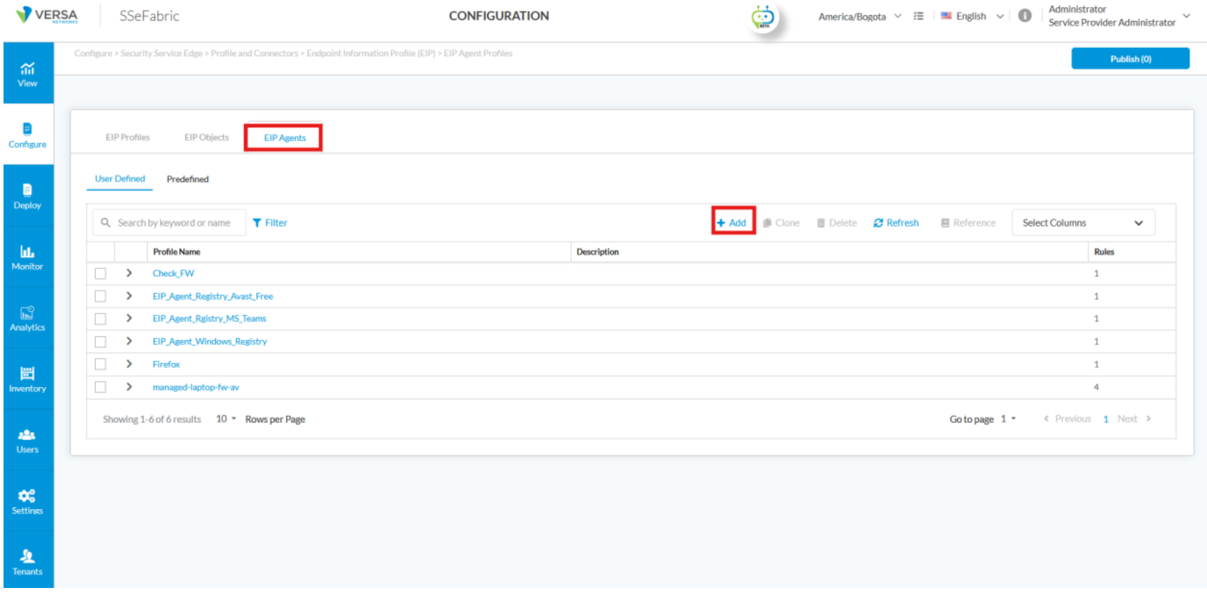


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

		Profile Name	Description	Rules
□	>	Check_FW		1
□	>	EIP_Agent_Registry_Avast_Free		1
□	>	EIP_Agent_Rgistry_MS_Teams		1
□	>	EIP_Agent_Windows_Registry		1
□	>	Firefox		1
□	>	managed-laptop-fw-av		4

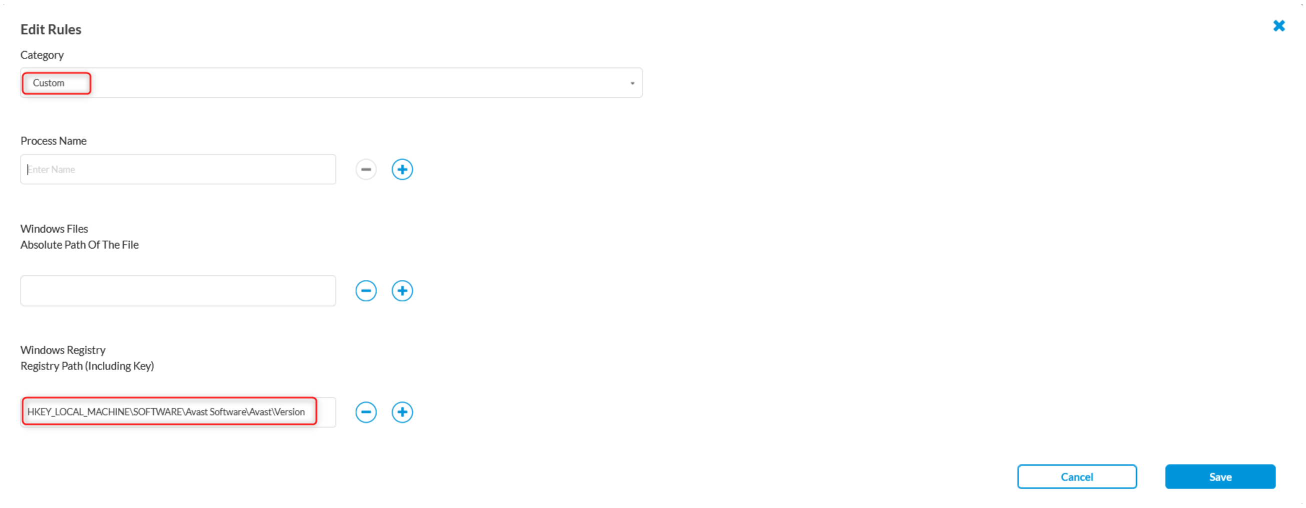
Showing 1-6 of 6 results 10 Rows per Page Go to page 1 Previous 1 Next

Click on "+Add" to create a new rule. Then choose Custom


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

		Profile Name	Description	Rules
□	>	Check_FW		1
□	>	EIP_Agent_Registry_Avast_Free		1
□	>	EIP_Agent_Rgistry_MS_Teams		1
□	>	EIP_Agent_Windows_Registry		1
□	>	Firefox		1
□	>	managed-laptop-fw-av		4

Showing 1-6 of 6 results 10 Rows per Page Go to page 1 Previous 1 Next



Edit Rules

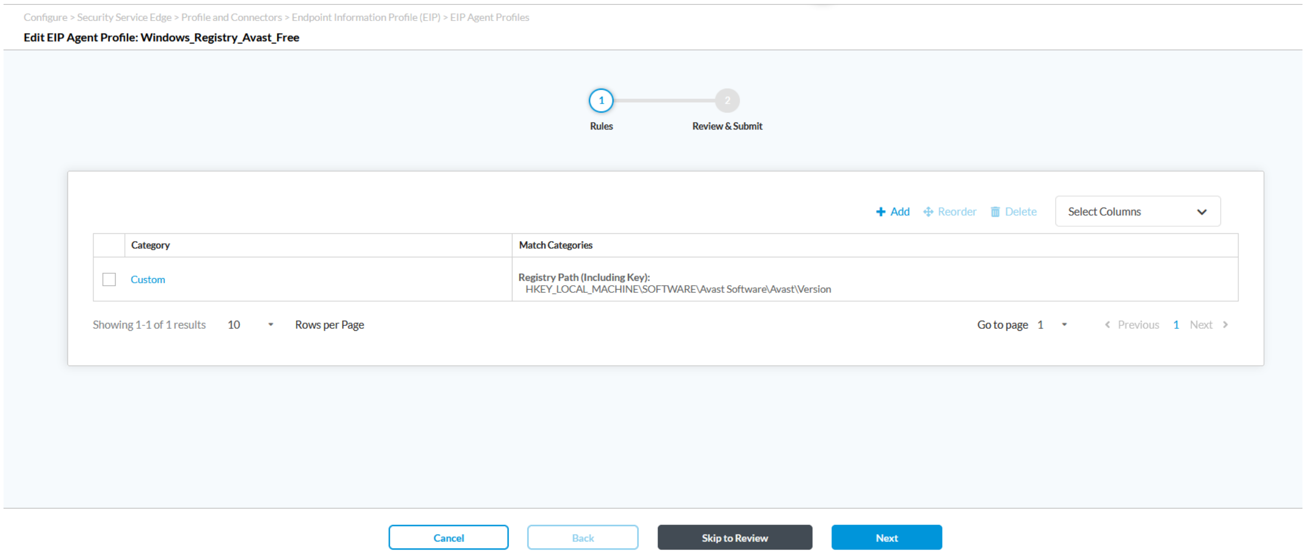
Category: Custom

Process Name: Enter Name

Windows Files
Absolute Path Of The File

Windows Registry
Registry Path (Including Key): HKEY_LOCAL_MACHINE\SOFTWARE\Avast Software\Avast\Version

Click on “next” to enter a descriptive Profile Name (e.g., **EIP_Agent_Windows_Registry**).

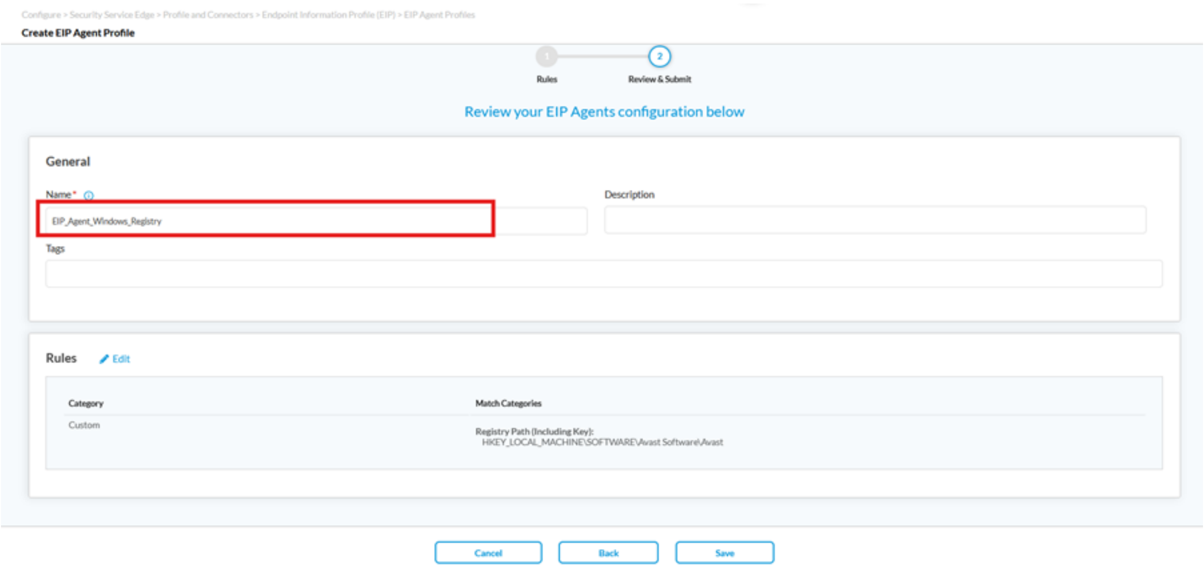


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Edit EIP Agent Profile: Windows_Registry_Avast_Free

Category	Match Categories
□ Custom	Registry Path (Including Key): HKEY_LOCAL_MACHINE\SOFTWARE\Avast Software\Avast\Version

Showing 1-1 of 1 results 10 Rows per Page



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Create EIP Agent Profile

Review your EIP Agents configuration below

General

Name* : EIP_Agent_Windows_Registry

Description

Tags

Rules Edit

Category	Match Categories
Custom	Registry Path (Including Key): HKEY_LOCAL_MACHINE\SOFTWARE\Avast Software\Avast

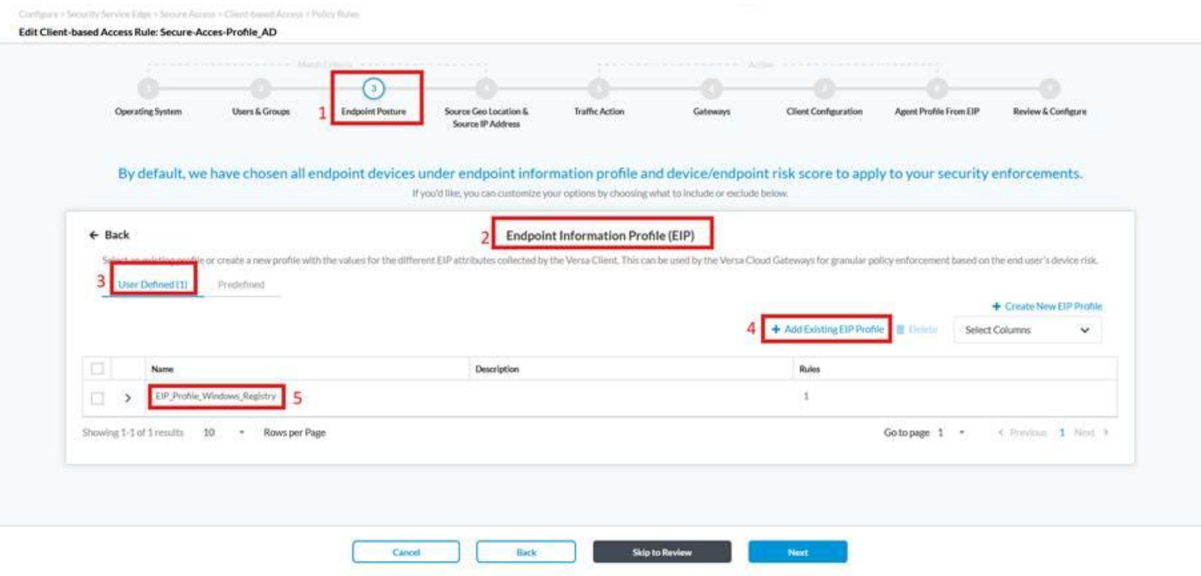
Step 5: Configure Secure Client Access Rule

Navigate to:

Configure > Security Service Edge > Secure Access > Client-based Access > Rules.

Click "**+ Add**" to create a new Secure Access Client rule or edit an existing rule.

In the Match Criteria configuration, go to the ***Endpoint Posture*** section. Under the *Endpoint Information Profile (EIP)* panel, select the desired profile by navigating to the ***User Defined*** tab and clicking on *Add Existing EIP Profile*. Then, choose the EIP profile you previously created. Example EIP_Profile_Windows_Registry).



Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure-Acces-Profile_AD

By default, we have chosen all endpoint devices under endpoint information profile and device/endpoint risk score to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

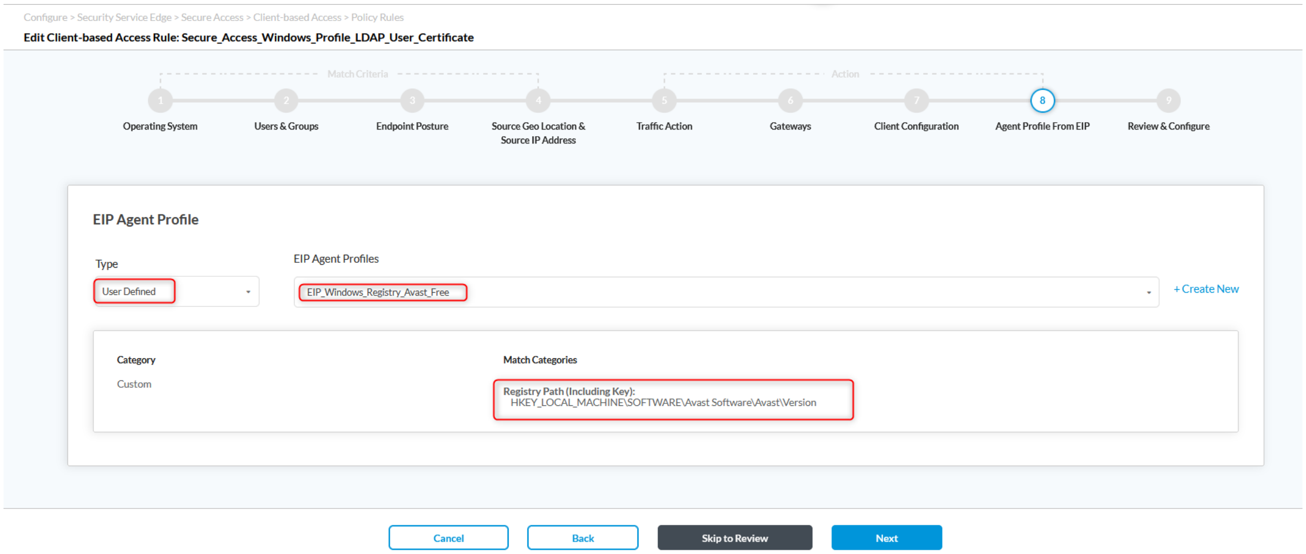
2 Endpoint Information Profile (EIP)

Select an existing profile or create a new profile with the values for the different EIP attributes collected by the Versa Client. This can be used by the Versa Cloud Gateways for granular policy enforcement based on the end user's device risk.

□		Name	Description	Rules
□	>	EIP_Profile_Windows_Registry 5		1

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 < Previous 1 Next >

In action configuration, under the **Agent Profile From EIP** section, set the Type to **User Defined** and select the **EIP Agent Profile** you previously created. Example EIP_Agent_Windows_Registry. *The Match Categories panel displays the defined validation criteria, such as registry paths or process checks, ensuring that the selected EIP Agent Profile is applied during endpoint posture verification*.



Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure_Access_Windows_Profile_LDAP_User_Certificate

EIP Agent Profile

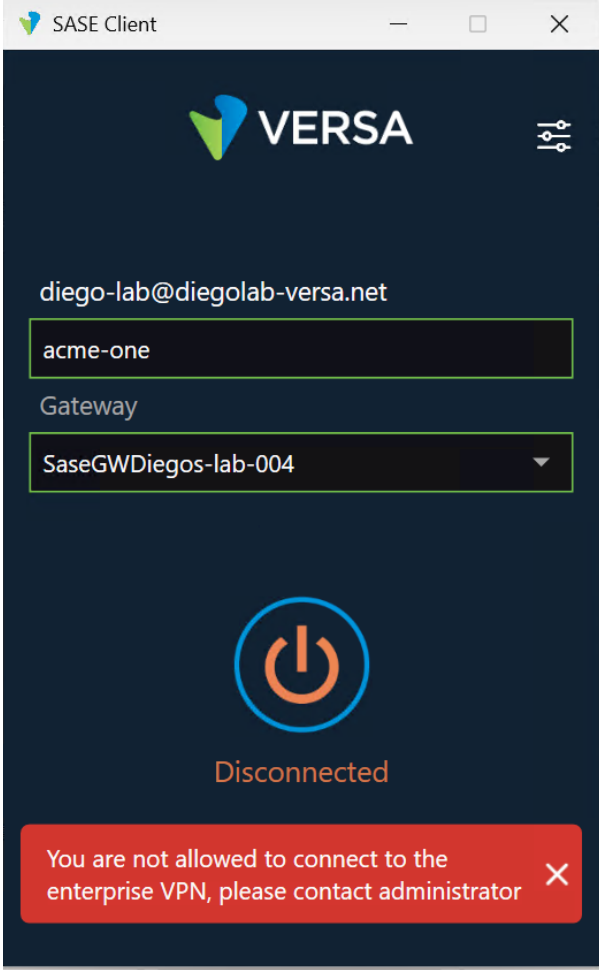
Type: User Defined

EIP Agent Profiles: EIP_Windows_Registry_Avast_Free

Category	Match Categories
Custom	Registry Path (Including Key): HKEY_LOCAL_MACHINE\SOFTWARE\Avast Software\Avast\Version

Verification

After a re-registered is not allowed to connect. This is due to the Avast Free antivirus Registry Path is not present.



diego-lab@diegolab-versa.net

acme-one

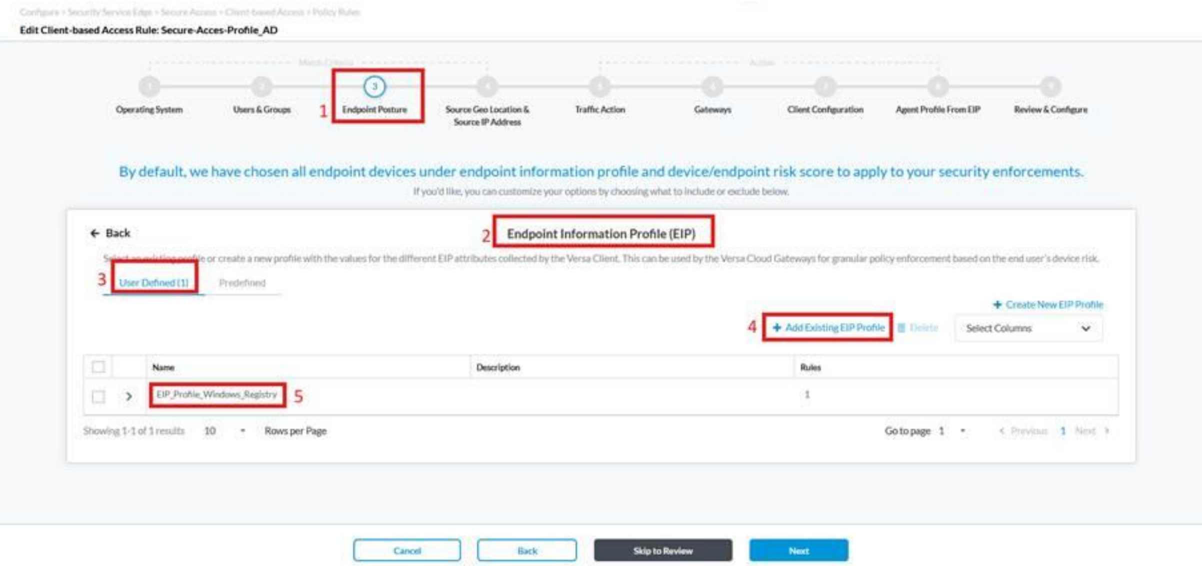
Gateway

SaseGWDiegos-lab-004

Disconnected

You are not allowed to connect to the enterprise VPN, please contact administrator

Validate EIP profile applied on Secure Client Access Rule. Navigate to ***Configure*** > ***Security Service Edge*** > ***Secure Access*** > ***Client-based Access*** > Choose appropriate Secure Access Profile click on **"Name"** go to EIP profile



By default, we have chosen all endpoint devices under endpoint information profile and device/endpoint risk score to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

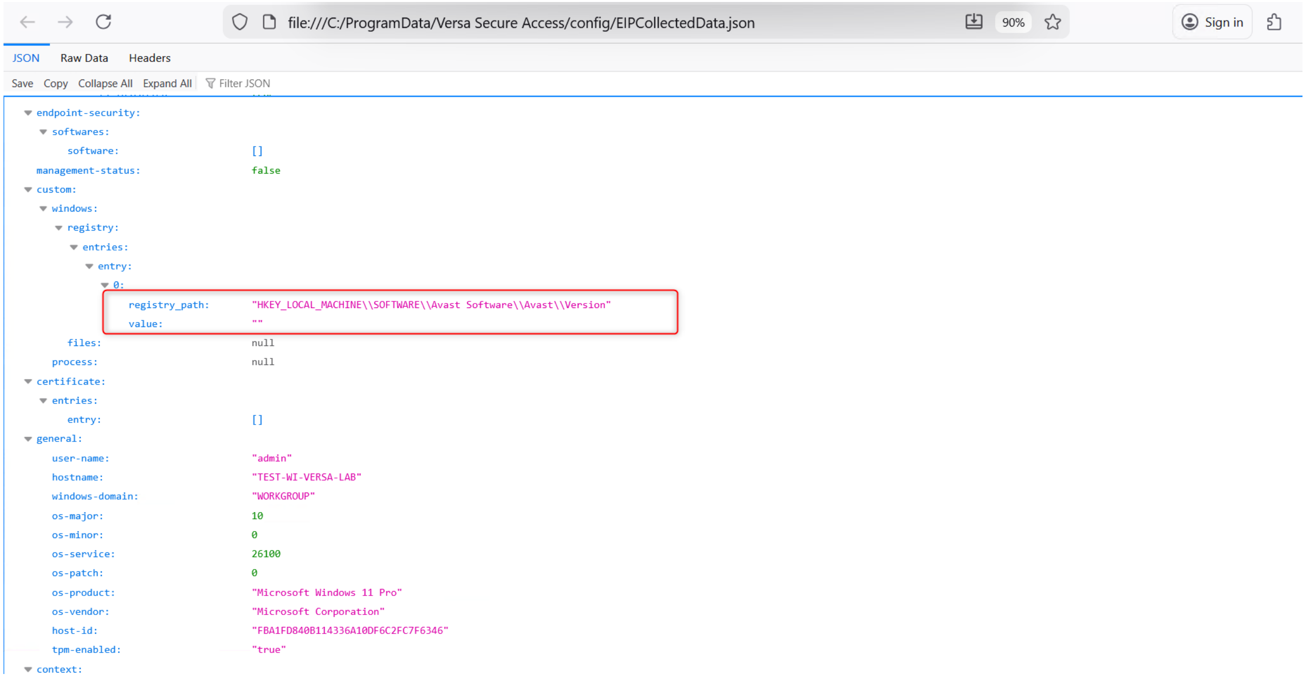
Select an existing profile or create a new profile with the values for the different EIP attributes collected by the Versa Client. This can be used by the Versa Cloud Gateways for granular policy enforcement based on the end user's device risk.

Name	Description	Rules
EIP_Profile_Windows_Registry		1

Showing 1-1 of 1 results 10 Rows per Page

Review on json file "EIPCollectedData.json" In the Path C:\ProgramData\Versa Secure Access\config

Go to custom windows registry and check entries. There is Avast free entry however value is empty.

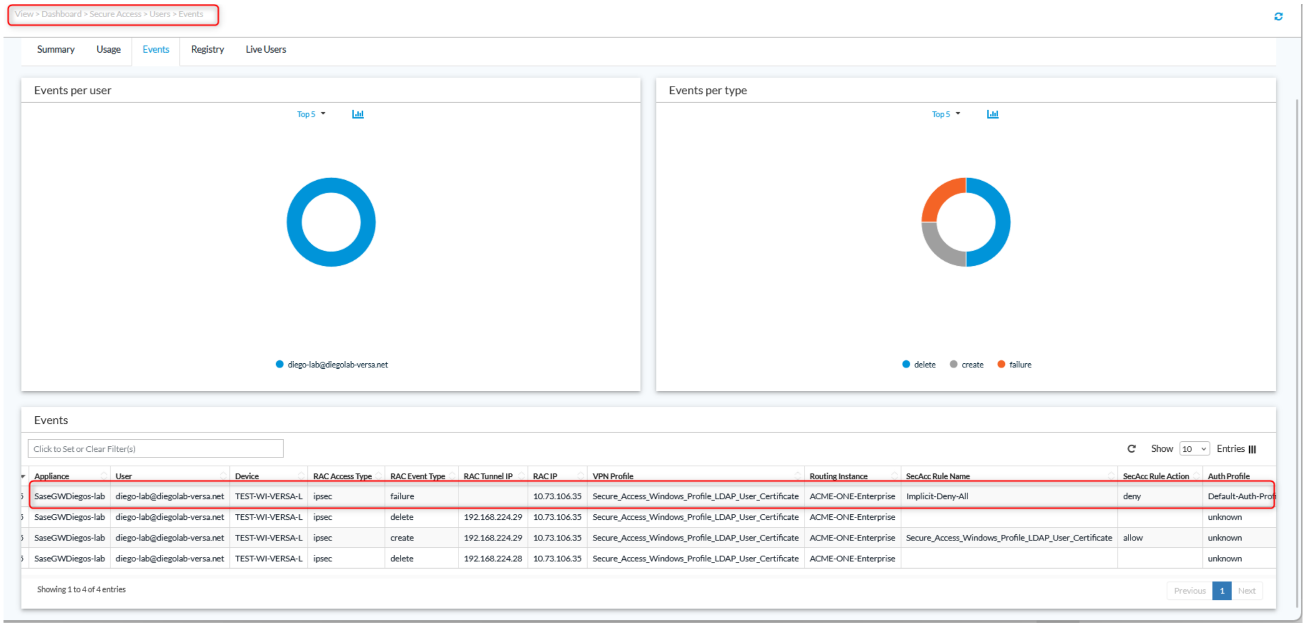


file:///C:/ProgramData/Versa Secure Access/config/EIPCollectedData.json
90%
Sign in
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON

```
endpoint-security:
  softwares:
    software:                []
  management-status:         false
custom:
  windows:
    registry:
      entries:
        entry:
          0:
            registry_path:   "HKEY_LOCAL_MACHINE\\SOFTWARE\\Avast Software\\Avast\\Version"
            value:           ""
    files:                   null
  process:                   null
certificate:
  entries:
    entry:                   []
general:
  user-name:                 "admin"
  hostname:                  "TEST-WI-VERSA-LAB"
  windows-domain:            "WORKGROUP"
  os-major:                  10
  os-minor:                  0
  os-service:                26100
  os-patch:                  0
  os-product:                "Microsoft Windows 11 Pro"
  os-vendor:                 "Microsoft Corporation"
  host-id:                   "FBA1FD840B114336A10DF6C2FC7F6346"
  tpm-enabled:               "true"
context:
```

Additionally, you can verify posture and access events directly from the SASE Portal.

Navigate to: **View > Dashboard > Secure Access > Users > Events**

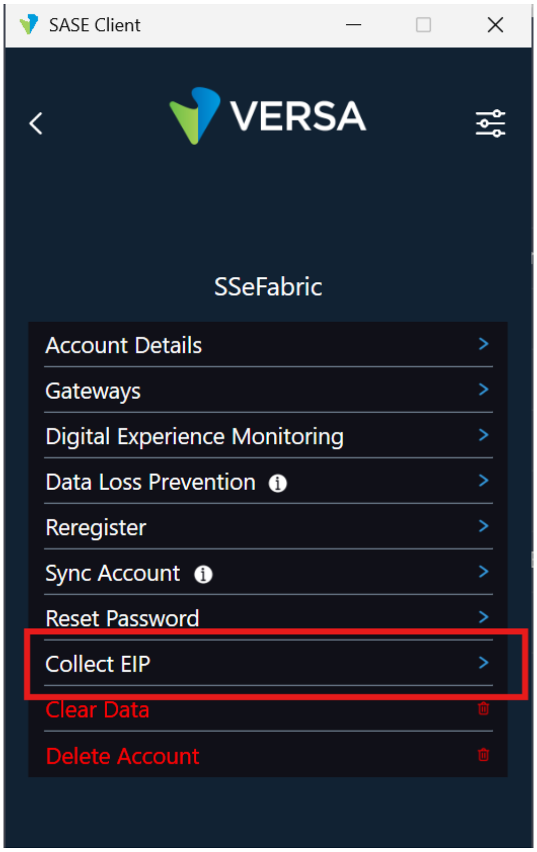


Appliance	User	Device	RAC Access Type	RAC Event Type	RAC Tunnel IP	RAC IP	VPN Profile	Routing Instance	SecAcc Rule Name	SecAcc Rule Action	Auth Profile
SaseGWDiegos-lab	diego-lab@diegolab-versa.net	TEST-WI-VERSA-L	ipsec	failure		10.73.106.35	Secure_Access_Windows_Profile_LDAP_User_Certificate	ACME-ONE-Enterprise	Implicit-Deny-All	deny	Default-Auth-Prof
SaseGWDiegos-lab	diego-lab@diegolab-versa.net	TEST-WI-VERSA-L	ipsec	delete	192.168.224.29	10.73.106.35	Secure_Access_Windows_Profile_LDAP_User_Certificate	ACME-ONE-Enterprise			unknown
SaseGWDiegos-lab	diego-lab@diegolab-versa.net	TEST-WI-VERSA-L	ipsec	create	192.168.224.29	10.73.106.35	Secure_Access_Windows_Profile_LDAP_User_Certificate	ACME-ONE-Enterprise	Secure_Access_Windows_Profile_LDAP_User_Certificate	allow	unknown
SaseGWDiegos-lab	diego-lab@diegolab-versa.net	TEST-WI-VERSA-L	ipsec	delete	192.168.224.28	10.73.106.35	Secure_Access_Windows_Profile_LDAP_User_Certificate	ACME-ONE-Enterprise			unknown

Showing 1 to 4 of 4 entries

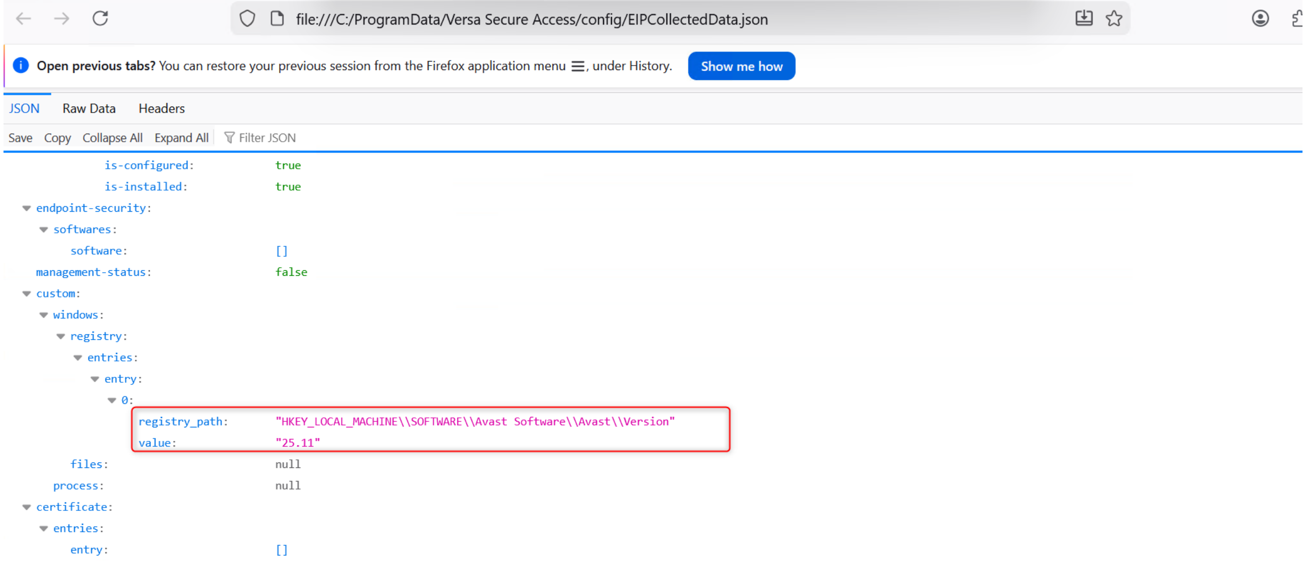
As you can see, the device is falling into the implicit Deny-All Rule

After Avast Free was installed again. In the Sase Client go to **Reregister**.



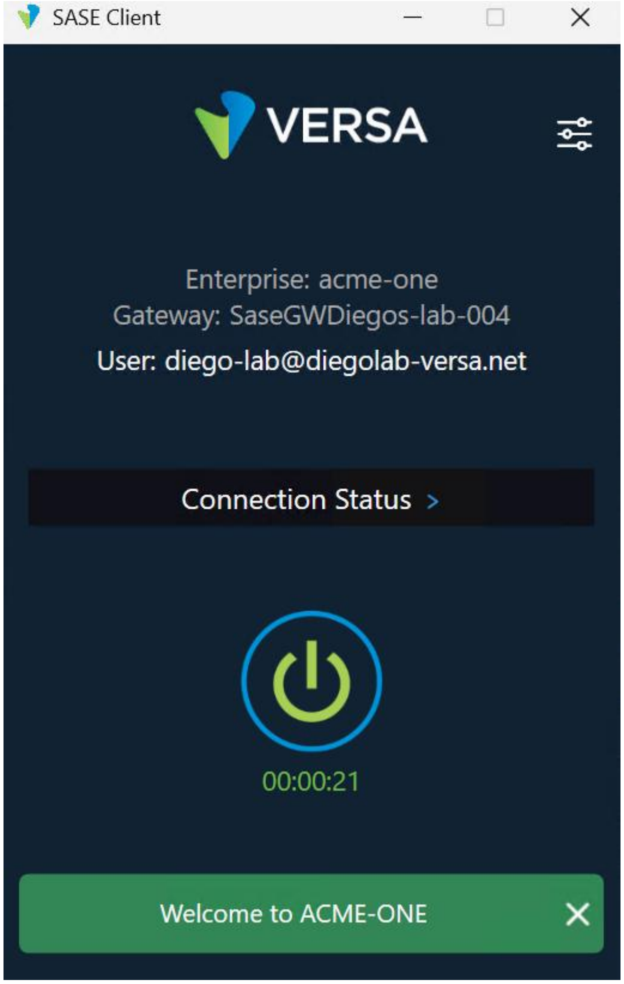
Review on json file “EIPCollectedData.json” In the Path C:\ProgramData\Versa Secure Access\config

Go to **Custom** Section. Now Avast free Registry is attached.


file:///C:/ProgramData/Versa Secure Access/config/EIPCollectedData.json
Open previous tabs? You can restore your previous session from the Firefox application menu ☰, under History.
Show me how
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON

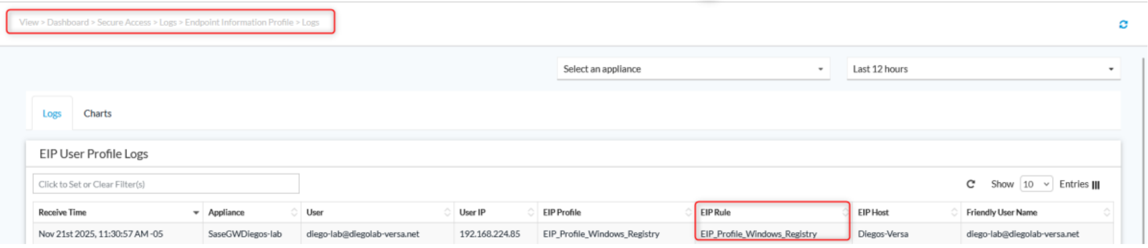
```
            is-configured:          true
            is-installed:           true
  ▼ endpoint-security:
    ▼ softwares:
        software:                   []
    management-status:              false
  ▼ custom:
    ▼ windows:
      ▼ registry:
        ▼ entries:
          ▼ entry:
            ▼ 0:
                registry_path:      "HKEY_LOCAL_MACHINE\\SOFTWARE\\Avast Software\\Avast\\Version"
                value:              "25.11"
        files:                      null
      process:                      null
  ▼ certificate:
    ▼ entries:
        entry:                      []
```

Now authentication is allowed.



Enterprise: acme-one
Gateway: SaseGWDiegos-lab-004
User: diego-lab@diegolab-versa.net

Additionally, you can check the EIP matching rule by going to View > Dashboard > Secure Access > Logs > Endpoint Information Profile > Logs and then selecting Endpoint Information Profile.


View > Dashboard > Secure Access > Logs > Endpoint Information Profile > Logs
Select an appliance
Last 12 hours
Logs
Charts

EIP User Profile Logs

Click to Set or Clear Filter(s)
Show 10 Entries

Receive Time	Appliance	User	User IP	EIP Profile	EIP Rule	EIP Host	Friendly User Name
Nov 21st 2025, 11:30:57 AM -05	SaseGWDiegos-lab	diego-lab@diegolab-versa.net	192.168.224.85	EIP_Profile_Windows_Registry	EIP_Profile_Windows_Registry	Diegos-Versa	diego-lab@diegolab-versa.net

Domain Validation

Domain validation in an Endpoint Identity Profile (EIP) verifies whether an endpoint is joined to the expected corporate Active Directory (AD) domain. This check ensures that devices are managed in accordance with enterprise policies and controls.

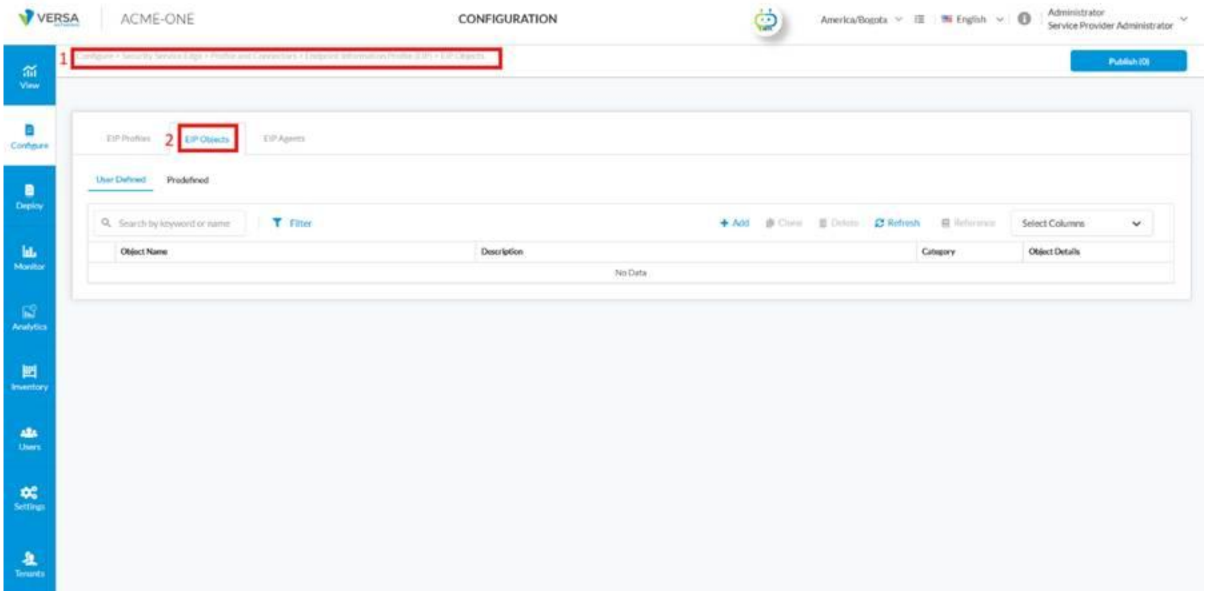
Scenario:

An organisation requires all Windows laptops accessing internal applications to be joined to acme-one.com. In the EIP Profile, the administrator configures a domain validation check for that domain. When a user connects:

- If the laptop is joined to acme-one.com, the device is compliant and access is allowed.
- If it is part of another domain or not domain-joined, the device is non-compliant and access is denied.

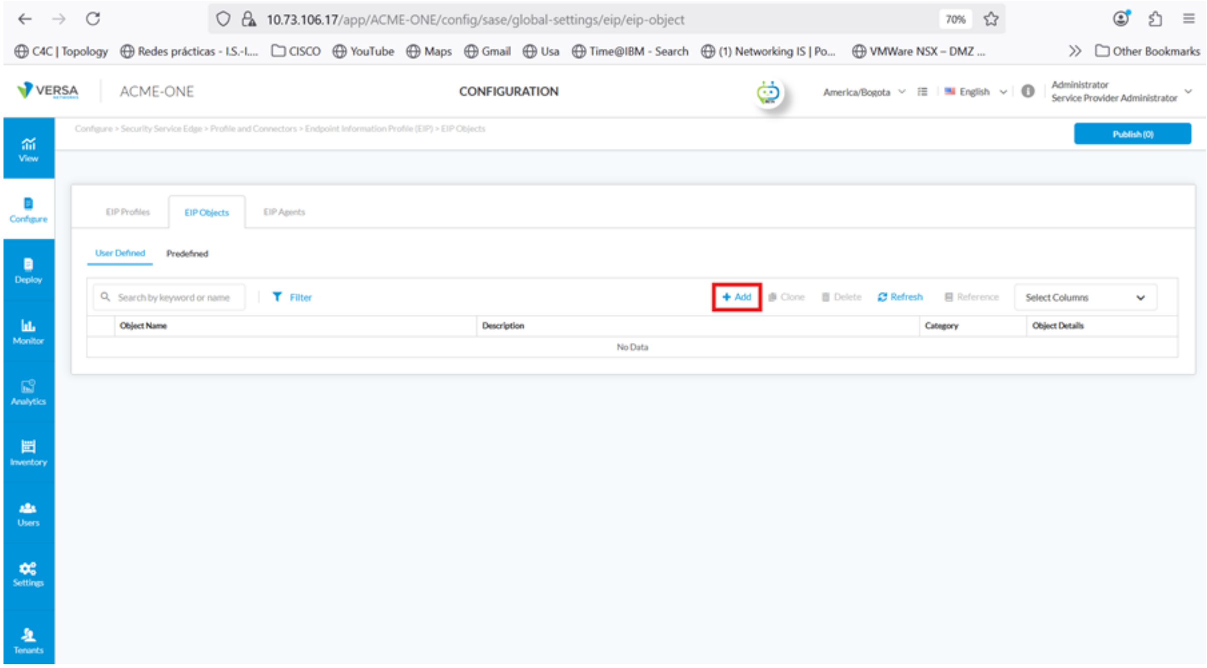
Step 1: Create an EIP Object with Windows domain

Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Objects

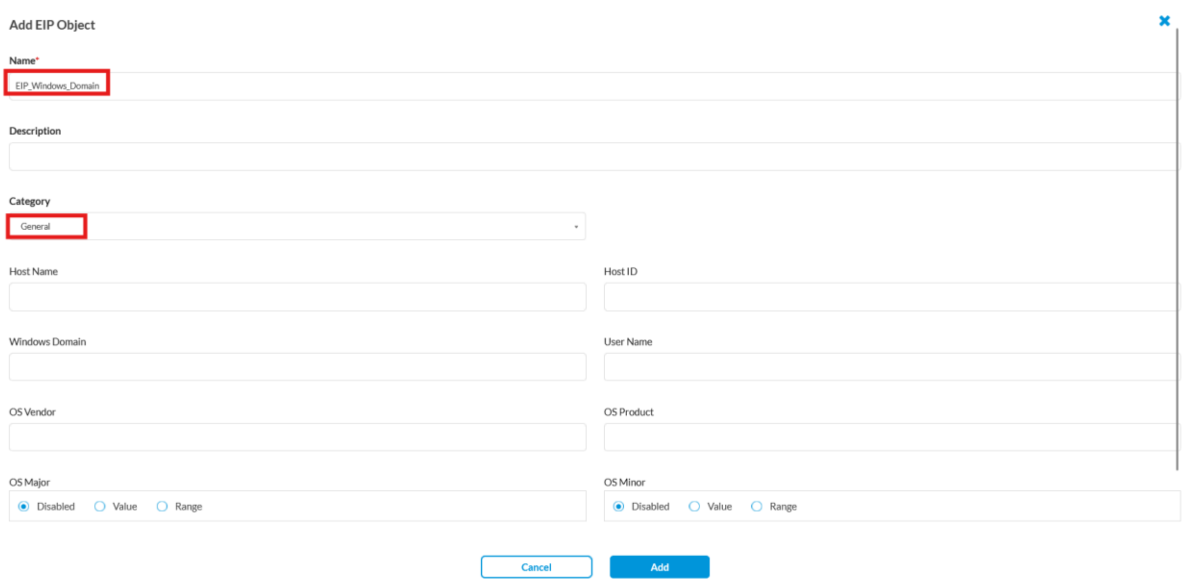


	Object Name	Description	Category	Object Details
	No Data			

Click on "+ Add" to create a new EIP Object.



Enter a descriptive name for your EIP object. ***Example:*** **EIP_Windows_Domain.** And Select general from the dropdown.


Add EIP Object

Name*: EIP_Windows_Domain

Description:

Category: General

Host Name:

Host ID:

Windows Domain:

User Name:

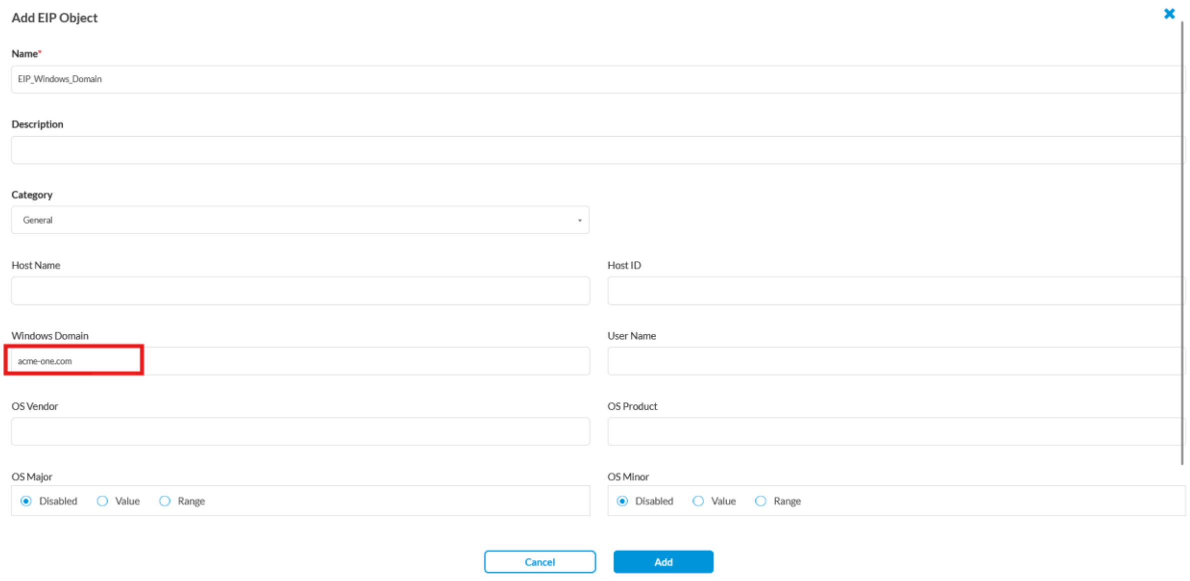
OS Vendor:

OS Product:

OS Major: ● Disabled ○ Value ○ Range

OS Minor: ● Disabled ○ Value ○ Range

Go to Windows Domain and enter the **domain name** to check ***Example:*** acme-one.com



Add EIP Object

Name*: EIP_Windows_Domain

Description:

Category: General

Host Name:

Host ID:

Windows Domain: acme-one.com

User Name:

OS Vendor:

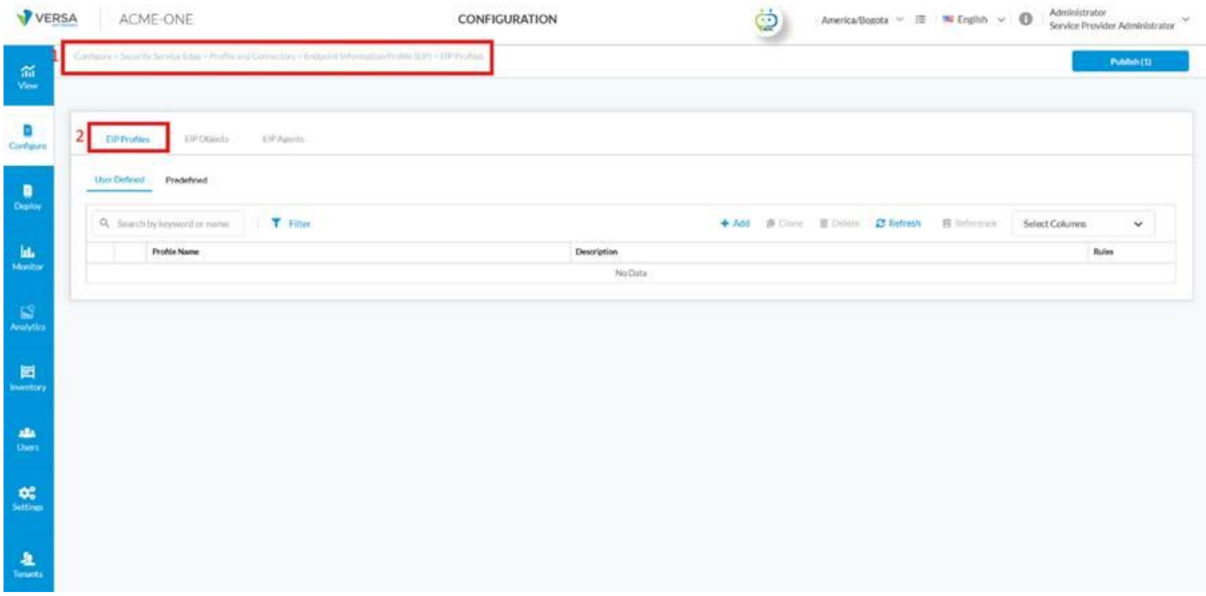
OS Product:

OS Major: ● Disabled ○ Value ○ Range

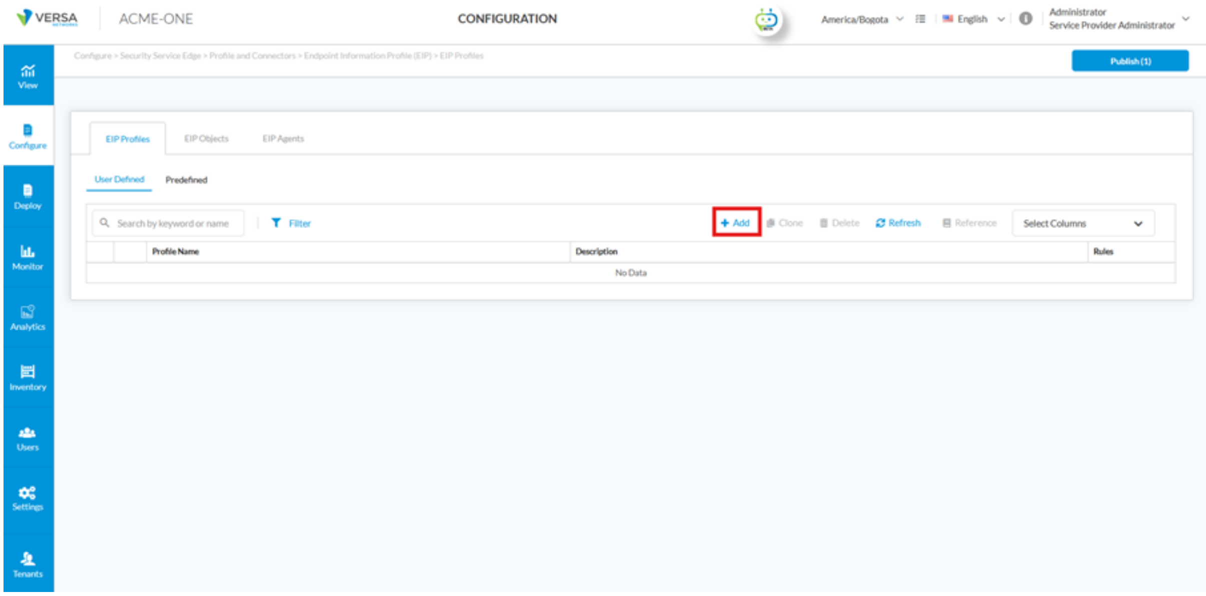
OS Minor: ● Disabled ○ Value ○ Range

Step 2: Create an EIP Profile Using Windows Domain

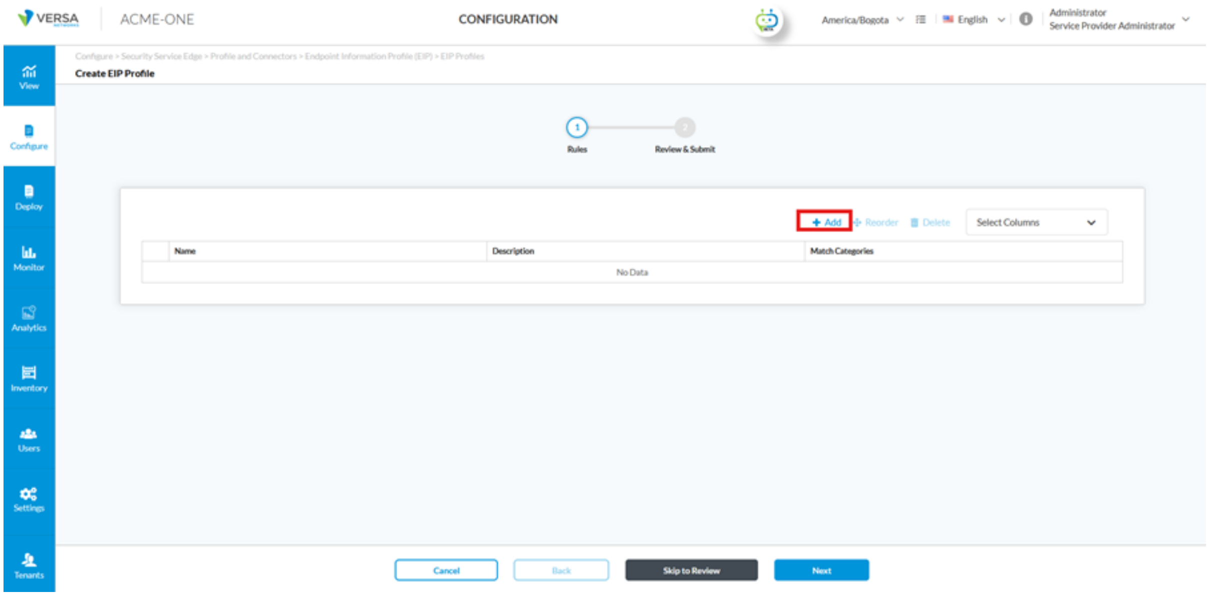
Navigate to **Configure** > **Security Service Edge** > **Profile and Connectors** > **Endpoint Information Profile (EIP)** > **EIP Profiles** then go **EIP Profiles**



Click on "+ **Add"** to start creating a new profile.



In the **Create EIP Profile** window, Click on "+ **Add**" to define a new rule.



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

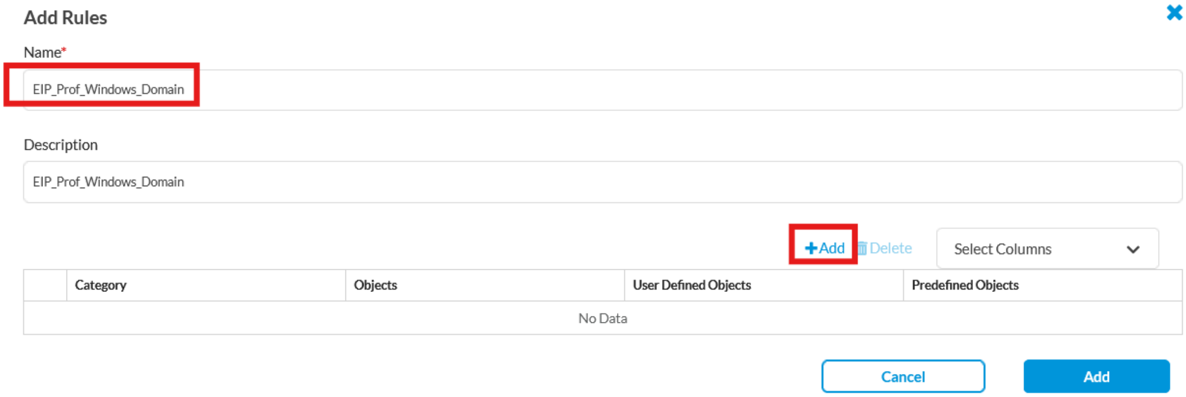
Create EIP Profile

	Name	Description	Match Categories
	No Data		

Enter a Name for this rule, Example, **EIP_Prof_Windows_Domain**.

You would (Optional) Add a description for clarity.

Click "+ Add" to attach an EIP Object.



Add Rules

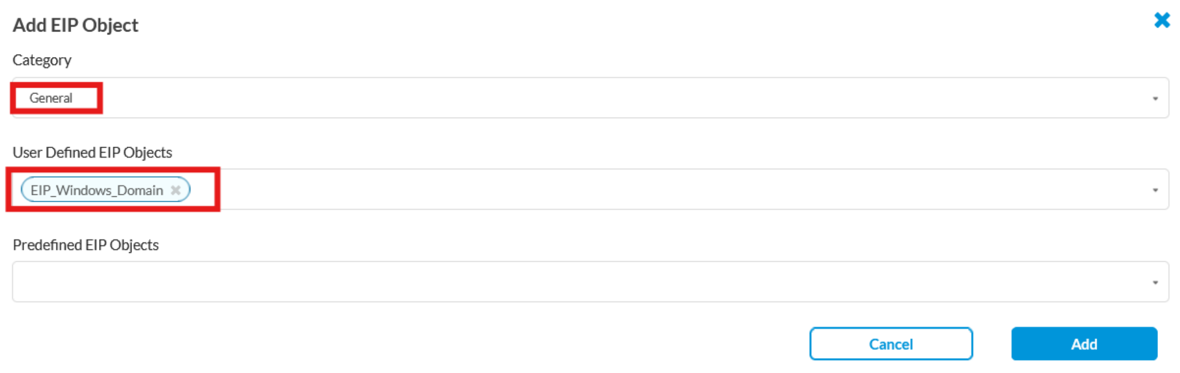
Name*: EIP_Prof_Windows_Domain

Description: EIP_Prof_Windows_Domain

	Category	Objects	User Defined Objects	Predefined Objects
	No Data			

In Add EIP Object dialog, choose the Category. Example **general**.

Select an existing EIP Object or create a new one. For example, an object was created to verify if windows domain in the previous section.



Add EIP Object

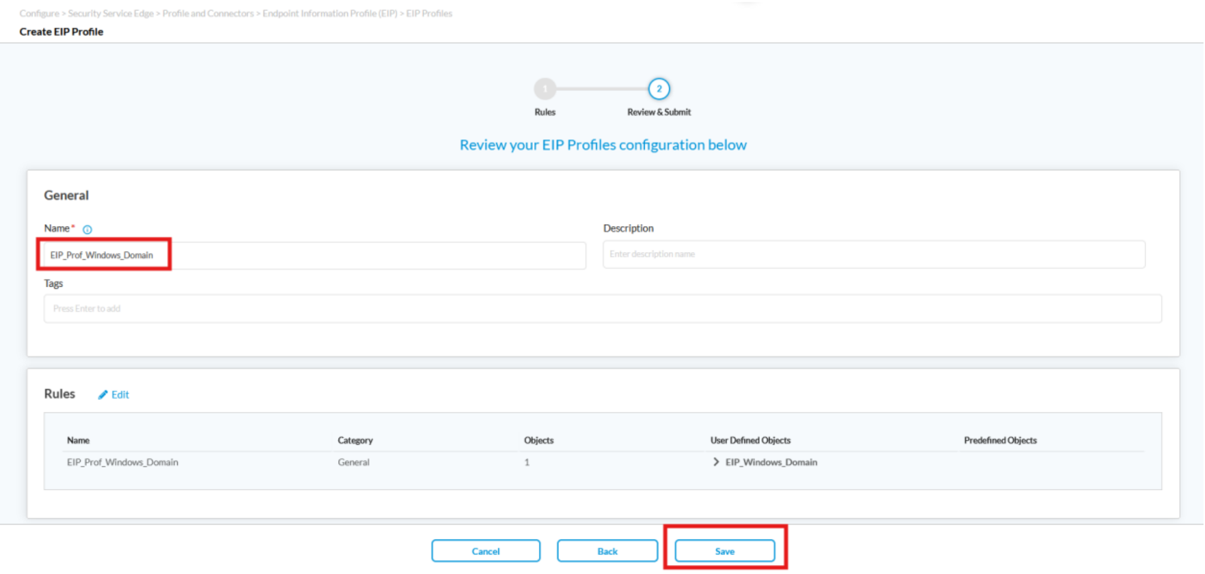
Category: General

User Defined EIP Objects: EIP_Windows_Domain

Predefined EIP Objects

Click **Next** and then Enter a descriptive name for your EIP object. ***Example:*** **EIP_Prof_Windows_Domain.**

Review and **Save** the Profile creation



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Create EIP Profile

Review your EIP Profiles configuration below

General

Name*: EIP_Prof_Windows_Domain

Description: Enter description name

Tags: Press Enter to add

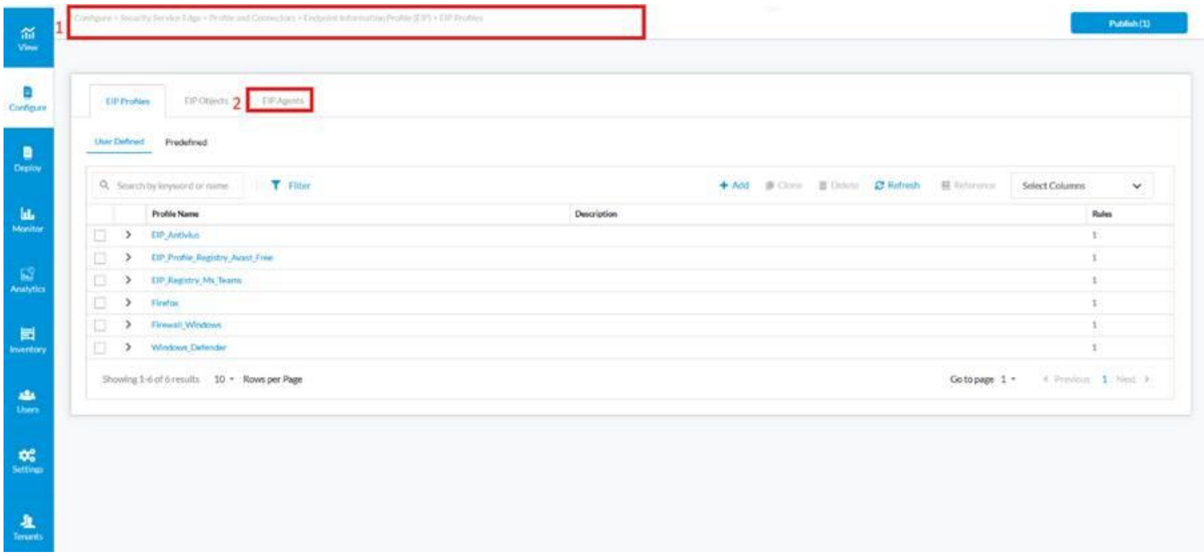
Rules

Name	Category	Objects	User Defined Objects	Predefined Objects
EIP_Prof_Windows_Domain	General	1	EIP_Windows_Domain	

Note: After creating the EIP Object and configuring the EIP Profile and Agent Profile, you must apply them to the Secure Access Client policy to enforce device posture validation and continue evaluation.

Step 3: Navigate to the EIP Agent Section

Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Agents

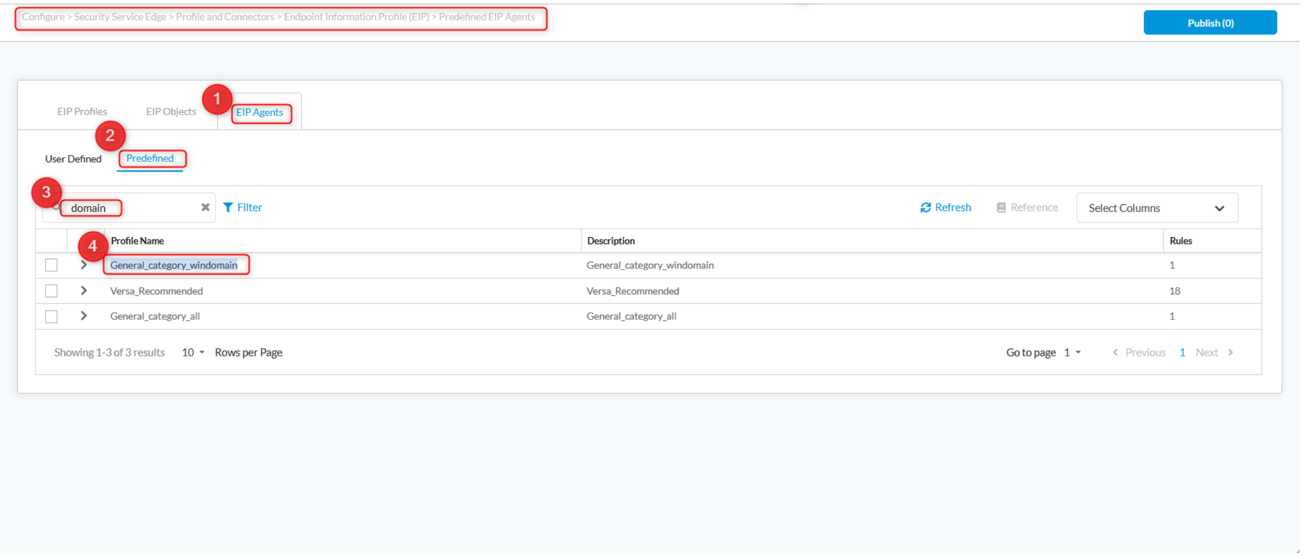


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Profile Name	Description	Rules
EIP_Antivius		1
EIP_Profile_Registry_Avast_Free		1
EIP_Registry_Ms_Teams		1
Firefox		1
Firewall_Windows		1
Windows_Defender		1

Step 4: Create an EIP Agent Profile

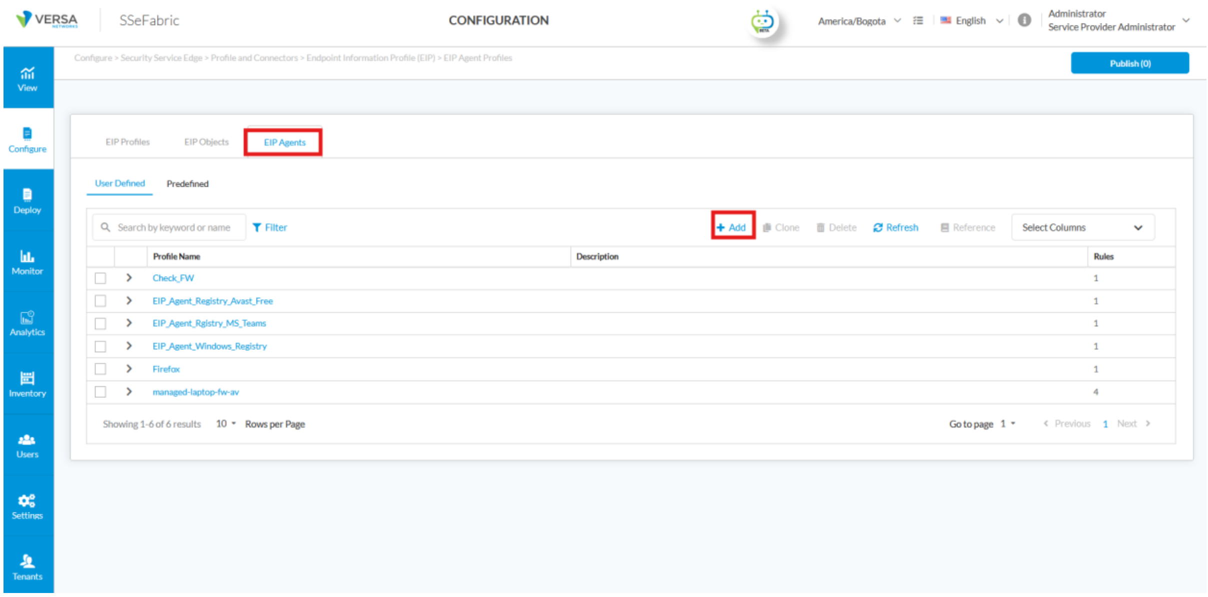
Important Note: Instead of creating a new agent manually, you can also use a predefined Versa Windows Domain agent. In the Predefined tab, search for the domain and select **General_category_windomain**, which already includes the rule Windows Domain: True.



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > Predefined EIP Agents

Profile Name	Description	Rules
General_category_windomain	General_category_windomain	1
Versa_Recommended	Versa_Recommended	18
General_category_all	General_category_all	1

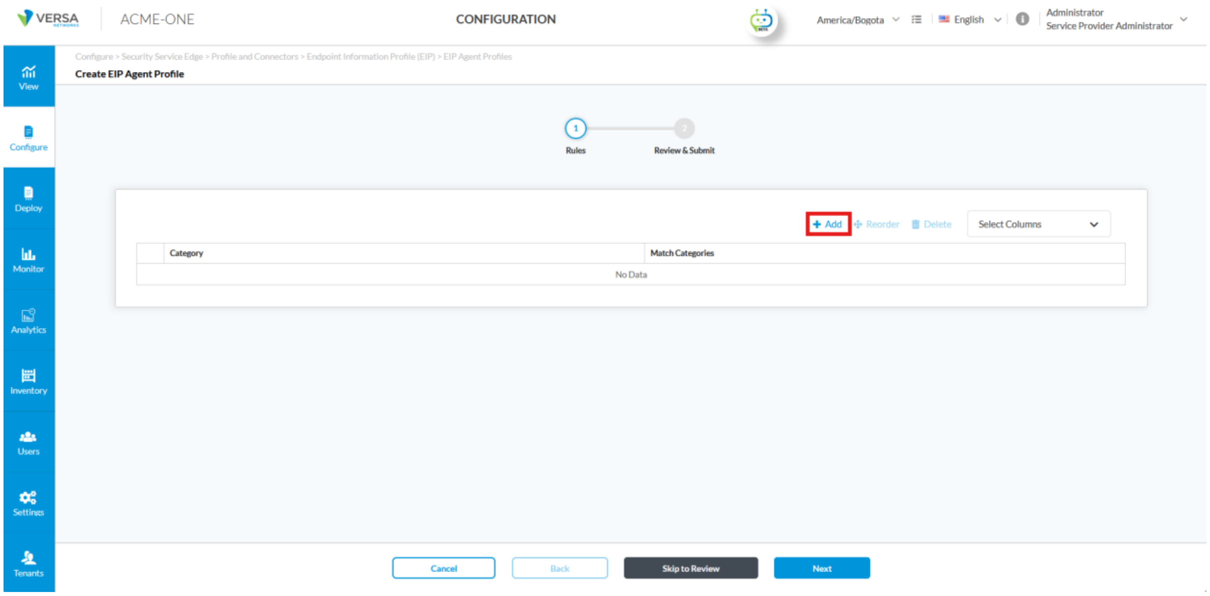
Click on **Add** to create a **new Agent profile**.



Profile Name	Description	Rules
Check_FW		1
EIP_Agent_Registry_Avast_Free		1
EIP_Agent_Rglstry_MS_Teams		1
EIP_Agent_Windows_Registry		1
Firefox		1
managed-laptop-fw-av		4

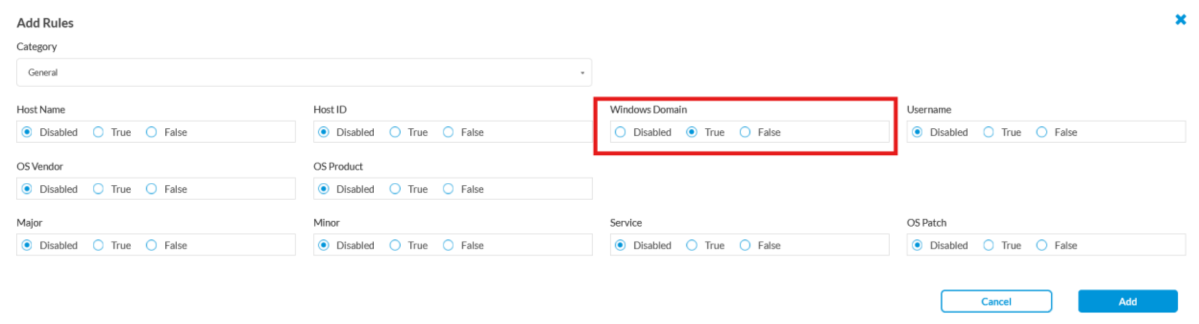
Showing 1-6 of 6 results 10 Rows per Page Go to page 1 Previous 1 Next

Click on “+Add” to create a new rule. Then choose general



Category	Match Categories
No Data	

In the **general** section, locate click Windows Domain by default is set to Disable change to true, then Click Add.



Add Rules

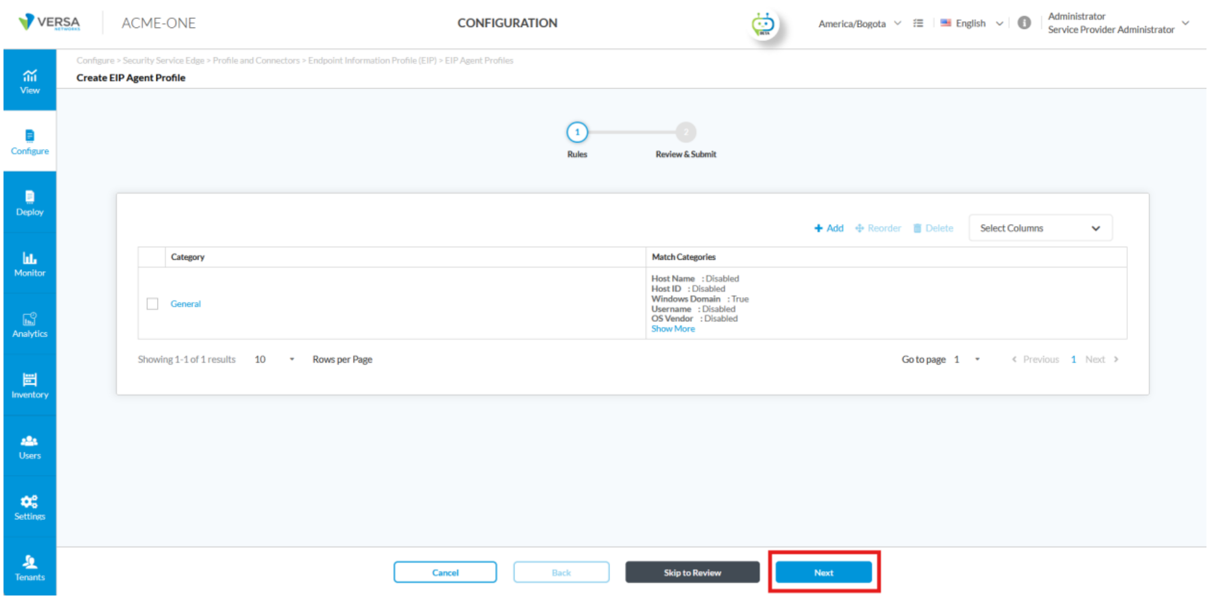
Category: General

Host Name	Host ID	Windows Domain	Username
● Disabled ○ True ○ False	● Disabled ○ True ○ False	○ Disabled ● True ○ False	● Disabled ○ True ○ False

OS Vendor	OS Product
● Disabled ○ True ○ False	● Disabled ○ True ○ False

Major	Minor	Service	OS Patch
● Disabled ○ True ○ False	● Disabled ○ True ○ False	● Disabled ○ True ○ False	● Disabled ○ True ○ False

Click on “next” to enter a descriptive Profile Name (Example., **EIP_Agent_Windows_Domain**).

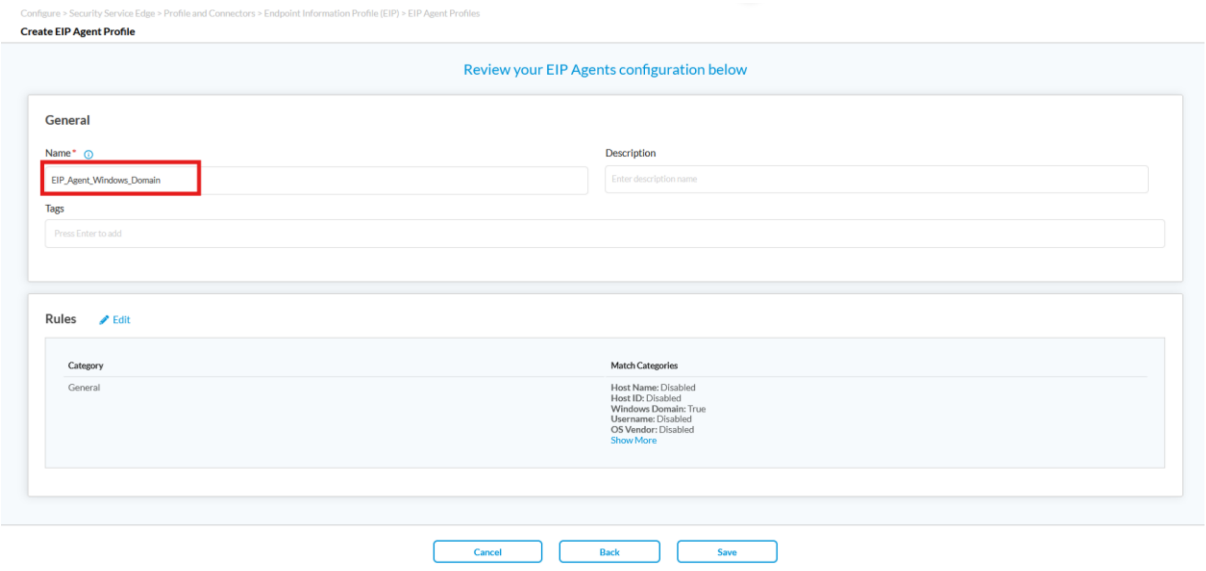


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Create EIP Agent Profile

	Category	Match Categories
□	General	Host Name : Disabled Host ID : Disabled Windows Domain : True Username : Disabled OS Vendor : Disabled Show More

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Create EIP Agent Profile

Review your EIP Agents configuration below

General

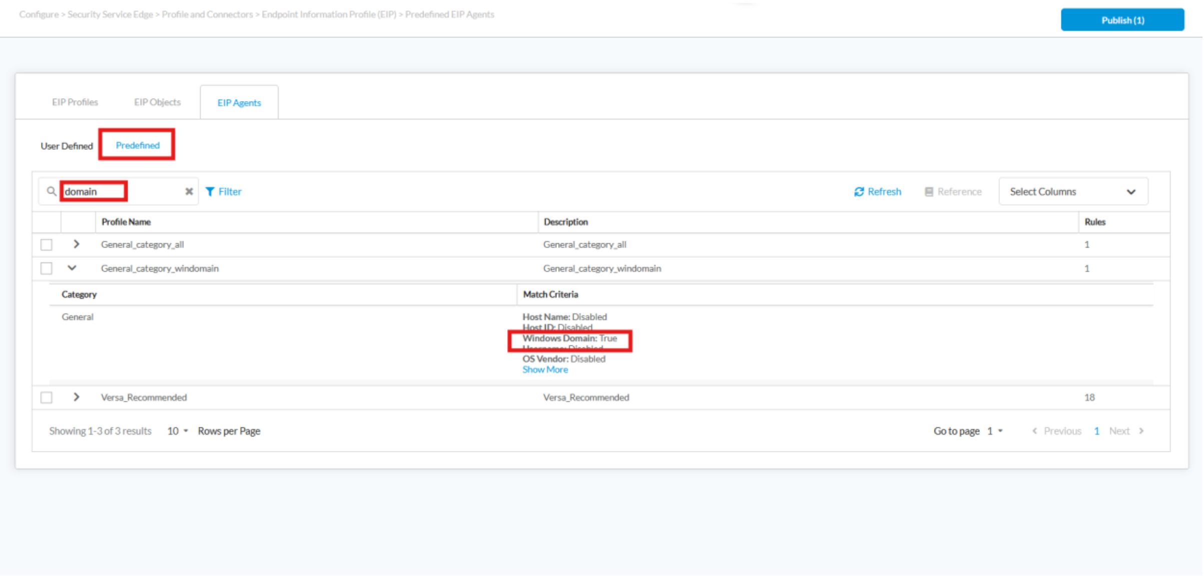
Name*: EIP_Agent_Windows_Domain

Description: Enter description name

Tags: Press Enter to add

Rules Edit

Category	Match Categories
General	Host Name: Disabled Host ID: Disabled Windows Domain: True Username: Disabled OS Vendor: Disabled Show More



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > Predefined EIP Agents

domain

Profile Name	Description	Rules
General_category_all	General_category_all	1
General_category_windomain	General_category_windomain	1
Versa_Recommended	Versa_Recommended	18

Category	Match Criteria
General	Host Name: Disabled Host ID: Disabled Windows Domain: True Username: Disabled OS Vendor: Disabled Show More

Showing 1-3 of 3 results 10 Rows per Page Go to page 1 Previous 1 Next

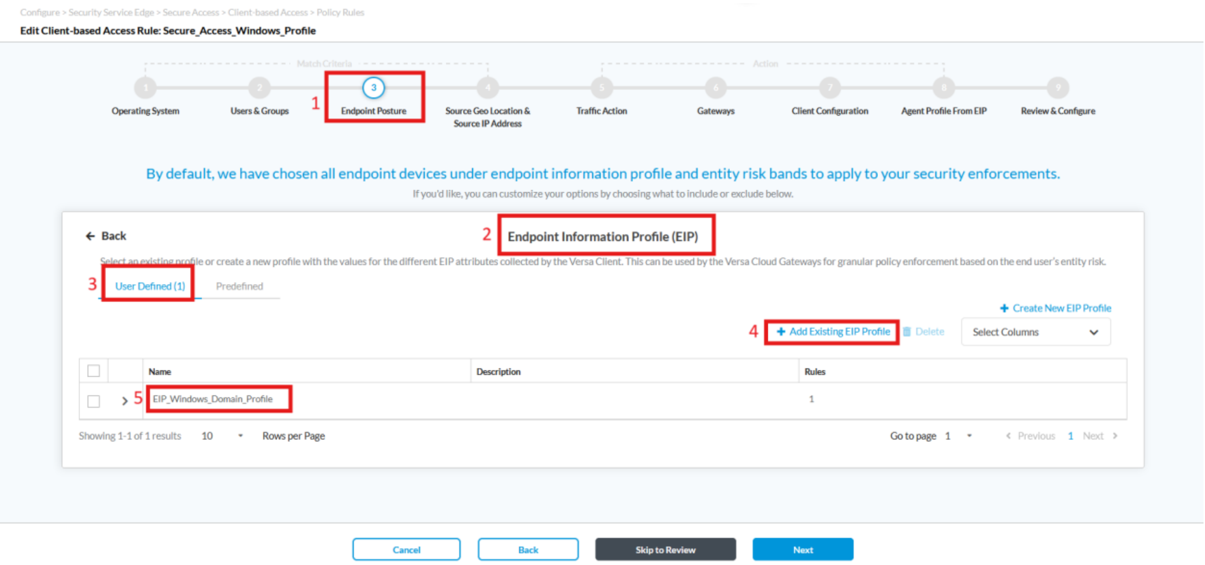
Step 5: Configure Secure Client Access Rule

Navigate to:

Configure > Security Service Edge > Secure Access > Client-based Access > Rules.

Click "**+ Add**" to create a new Secure Access Client rule or edit an existing rule.

In the Match Criteria configuration, go to the ***Endpoint Posture*** section. Under the *Endpoint Information Profile (EIP)* panel, select the desired profile by navigating to the ***User Defined*** tab and clicking on *Add Existing EIP Profile*. Then, choose the EIP profile you previously created. Example EIP_Prof_Windows_Domain).



Edit Client-based Access Rule: Secure_Access_Windows_Profile

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

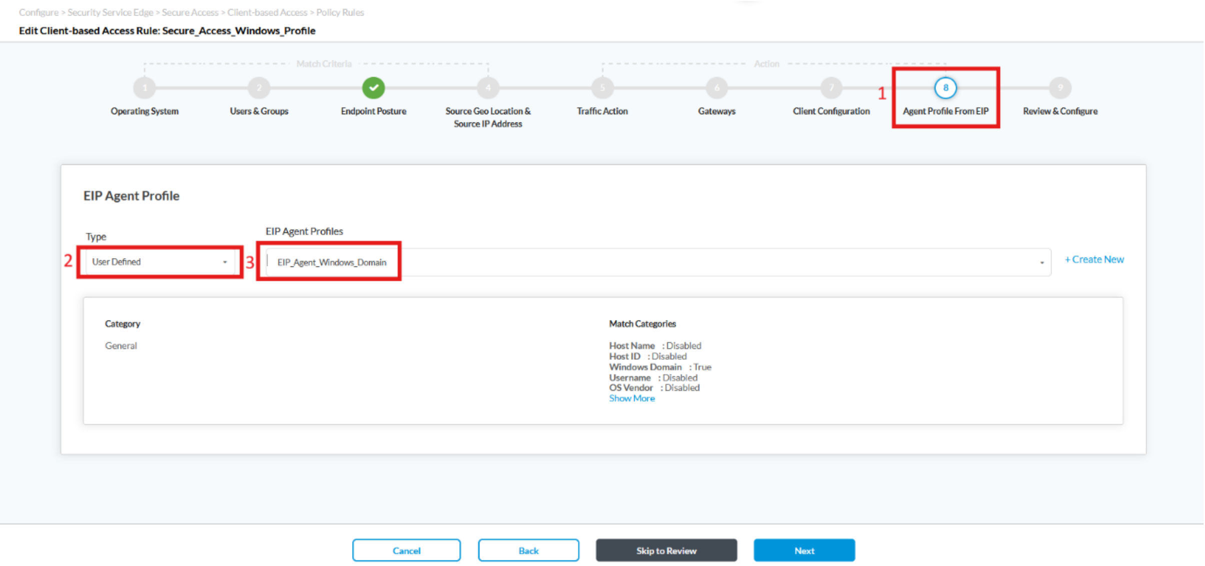
Endpoint Information Profile (EIP)

Select an existing profile or create a new profile with the values for the different EIP attributes collected by the Versa Client. This can be used by the Versa Cloud Gateways for granular policy enforcement based on the end user's entity risk.

□	Name	Description	Rules
□	EIP_Windows_Domain_Profile		1

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next

In action configuration, under the **Agent Profile From EIP** section, set the Type to **User Defined** and select the **EIP Agent Profile** you previously created. Example EIP_Agent_Windows_Domain. *The Match Categories panel will display the defined validation criteria, such as registry paths or process checks, ensuring that the selected EIP Agent Profile is applied for endpoint posture verification*.



Edit Client-based Access Rule: Secure_Access_Windows_Profile

EIP Agent Profile

Type: User Defined

EIP Agent Profiles: EIP_Agent_Windows_Domain

Category

General

Match Categories

Host Name : Disabled
Host ID : Disabled
Windows Domain : True
Username : Disabled
OS Vendor : Disabled

Host ID or System UUID

Host ID validation in an Endpoint Identity Profile (EIP) uniquely identifies endpoints using their hardware-based System UUID. Unlike MAC addresses, the UUID is tied to the motherboard and remains consistent throughout the device's lifecycle.

Scenario:

An organisation requires all corporate laptops accessing internal applications to be validated by their UUIDs. The administrator configures Host ID validation in the EIP Profile with the authorized UUID list. When a user connects:

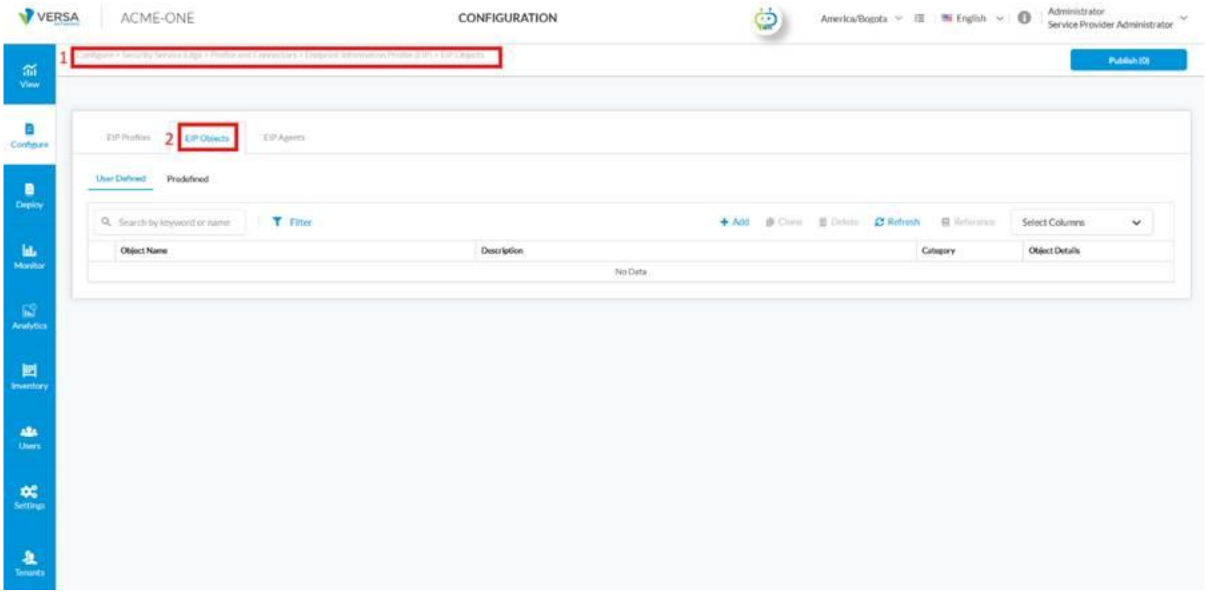
- If the UUID matches, the device is compliant and access is allowed.
- If not, the device is non-compliant and access is denied.

To retrieve the UUID in Windows PowerShell:

```
Get-CimInstance -ClassName Win32_ComputerSystemProduct | Select-Object UUID
```

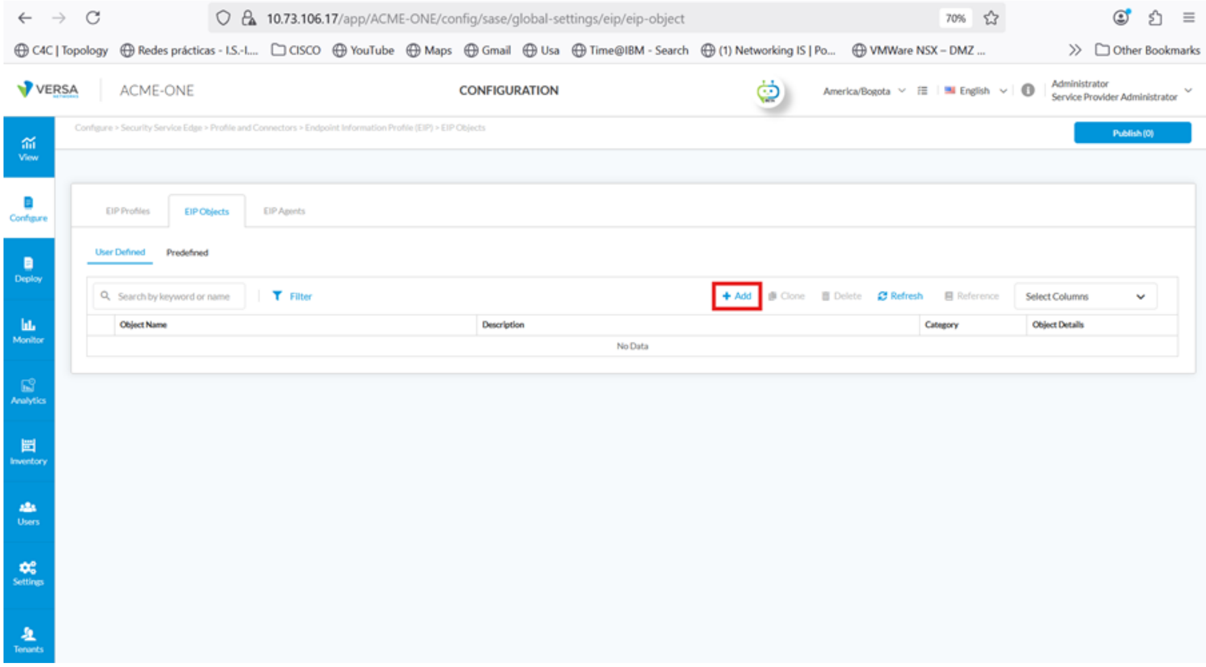
Step 1: Create an EIP Object with a Windows domain

Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Objects

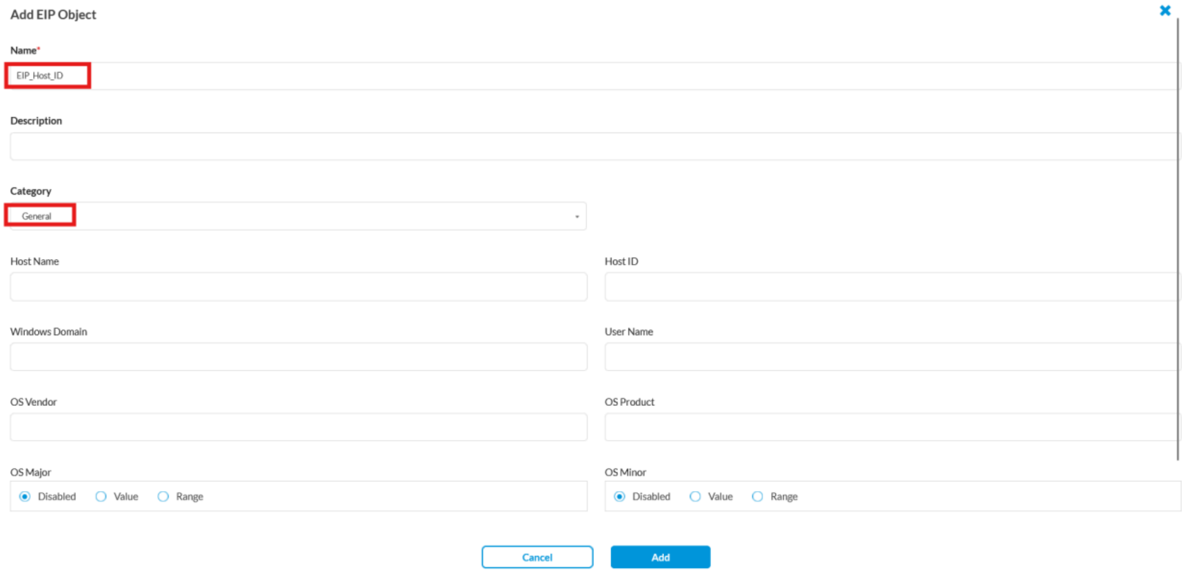


Object Name	Description	Category	Object Details
No Data			

Click on "+ Add" to create a new EIP Object.



Enter a descriptive name for your EIP object. ***Example:*** **EIP_Host_ID.** And Select general from the dropdown.


Add EIP Object

Name*: EIP_Host_ID

Description

Category: General

Host Name | Host ID

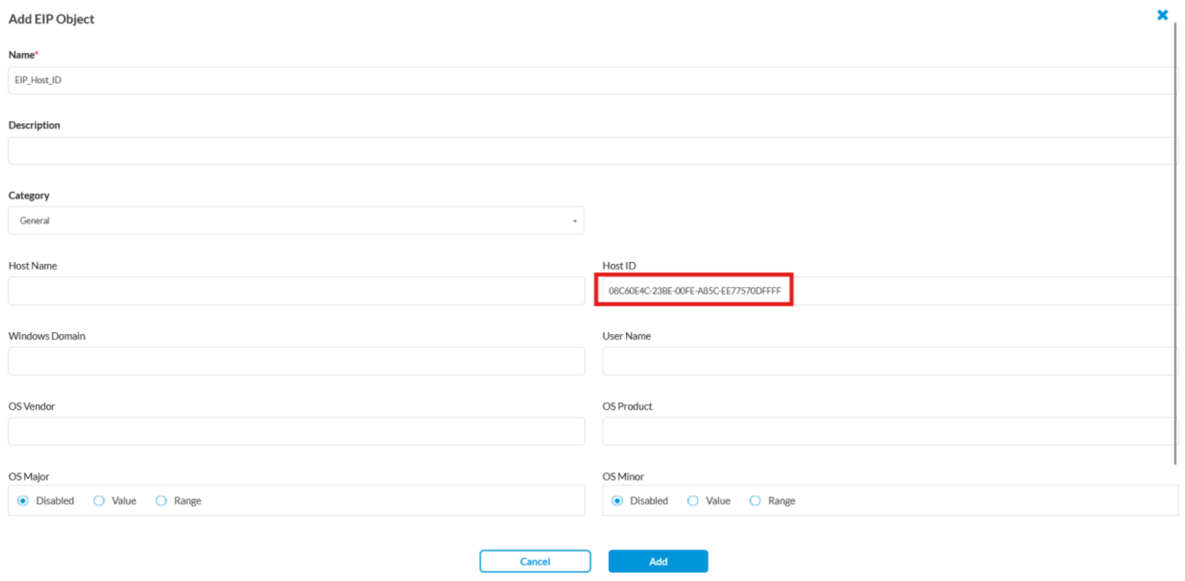
Windows Domain | User Name

OS Vendor | OS Product

OS Major: ● Disabled ○ Value ○ Range

OS Minor: ● Disabled ○ Value ○ Range

Go to Host ID and Enter the System UUDI to check *Example:* 08C60E4C-23BE-00FE-A85C-EE77570DFFFF



Add EIP Object

Name*: EIP_Host_ID

Description:

Category: General

Host Name:

Host ID: 08C60E4C-23BE-00FE-A85C-EE77570DFFFF

Windows Domain:

User Name:

OS Vendor:

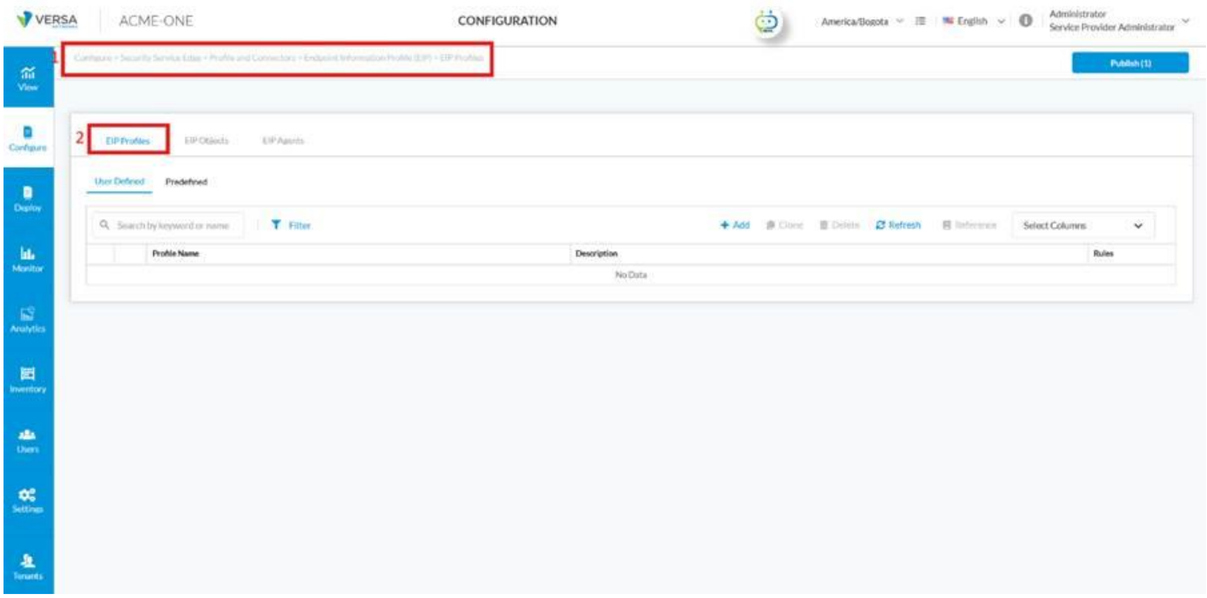
OS Product:

OS Major: ● Disabled ○ Value ○ Range

OS Minor: ● Disabled ○ Value ○ Range

Step 2: Create an EIP Profile Using Host ID

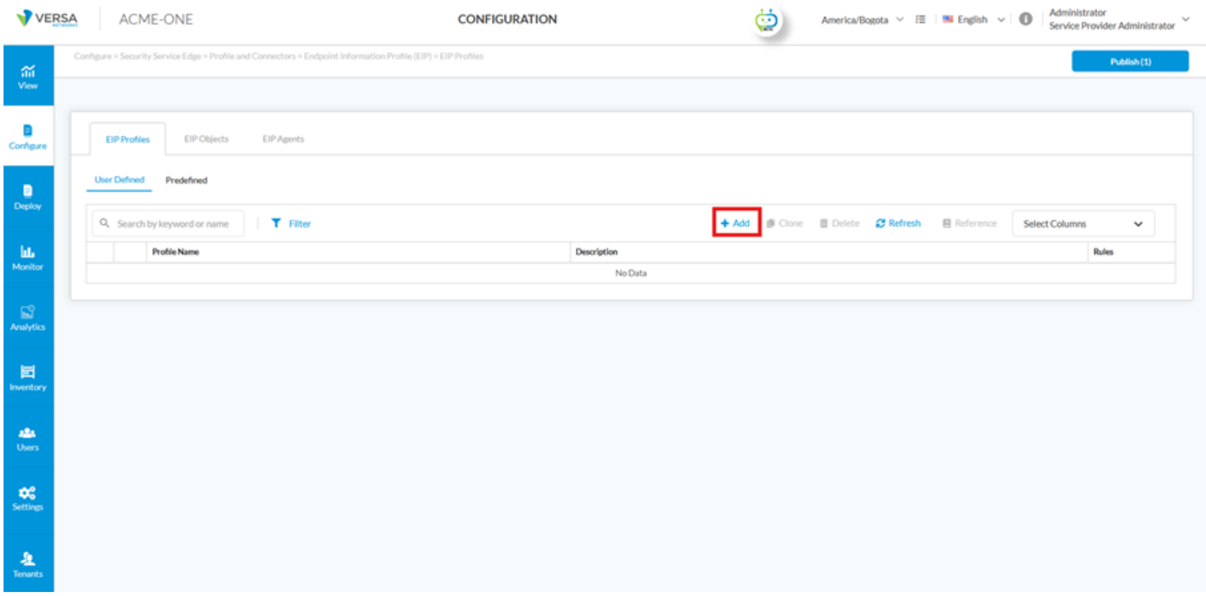
Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Profiles



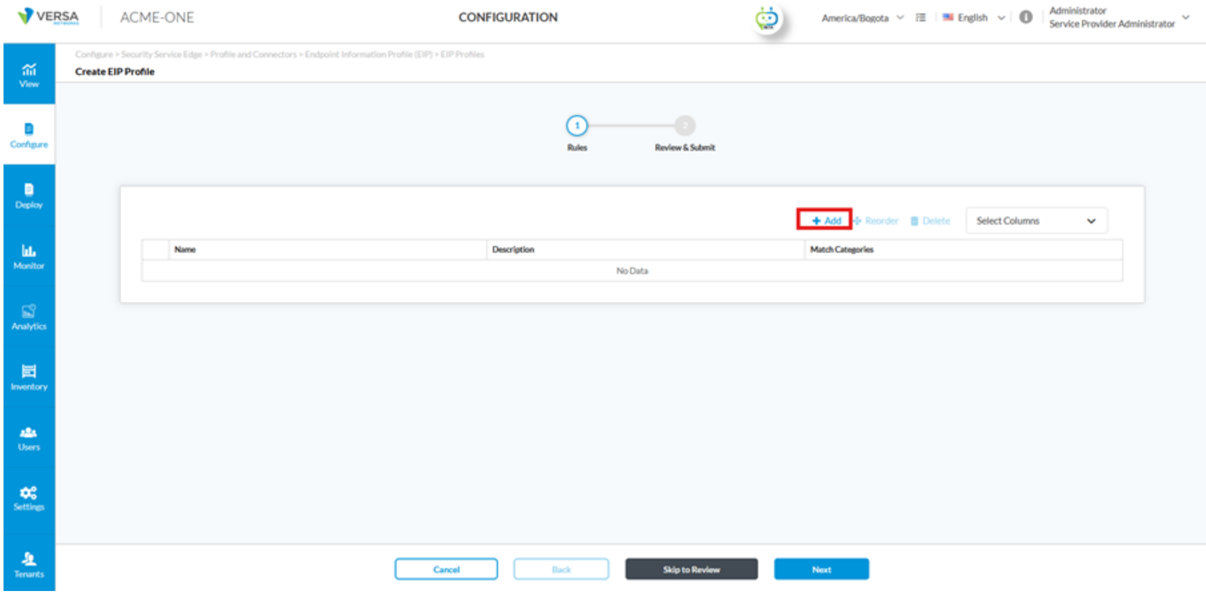
Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

		Profile Name	Description	Rules
			No Data	

Click on "+ Add" to start creating a new profile.



In the **Create EIP Profile** window, Click on "+ Add" to define a new rule.

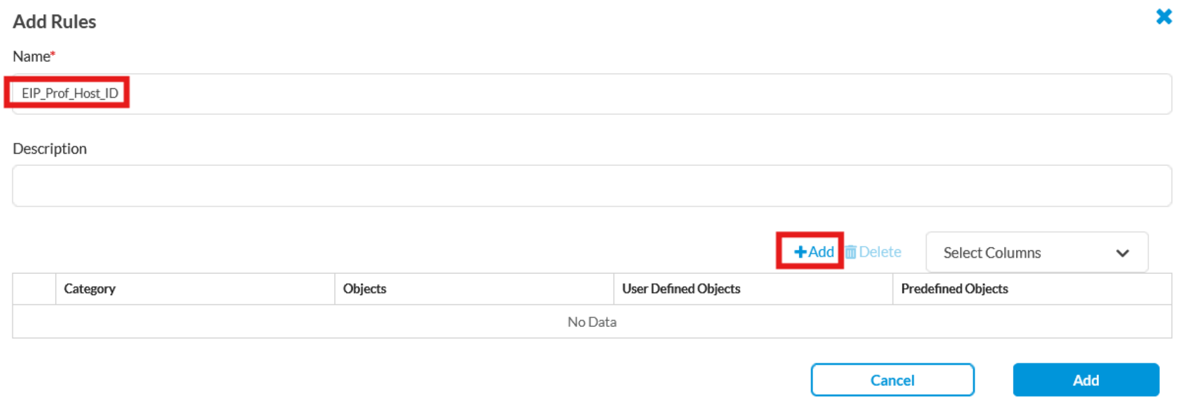


Create a General Rule for Windows Domain

Enter a Name for your rule, Example, EIP_Prof_Host_ID.

You would (Optional) Add a description for clarity.

Click "+ Add" to attach an EIP Object.



Add Rules

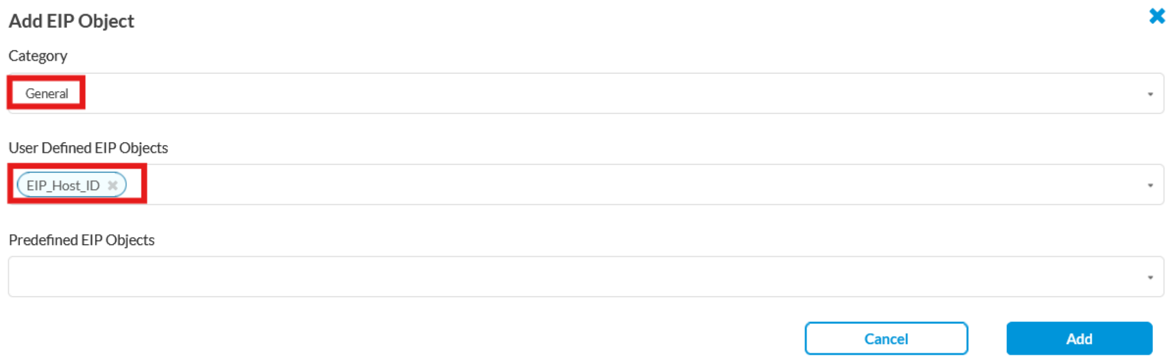
Name*: EIP_Prof_Host_ID

Description:

	Category	Objects	User Defined Objects	Predefined Objects
	No Data			

In Add EIP Object dialog, choose the Category. Example **general**.

Select an existing EIP Object or create a new one. For example, an object was created to verify if windows host ID in the previous section.



Add EIP Object

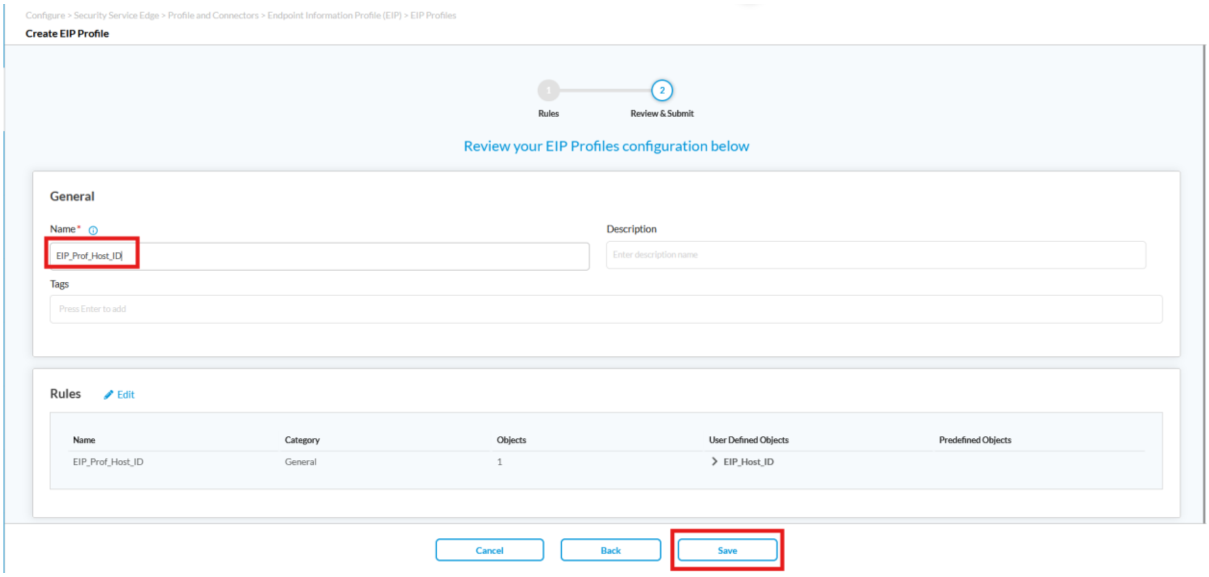
Category: General

User Defined EIP Objects: EIP_Host_ID

Predefined EIP Objects:

Click **Next** and then Enter a descriptive name for your EIP object. ***Example:*** **EIP_Prof_Host_ID.**

Review and **Save** the Profile creation



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Create EIP Profile

Review your EIP Profiles configuration below

General

Name*: EIP_Prof_Host_ID

Description: Enter description name

Tags: Press Enter to add

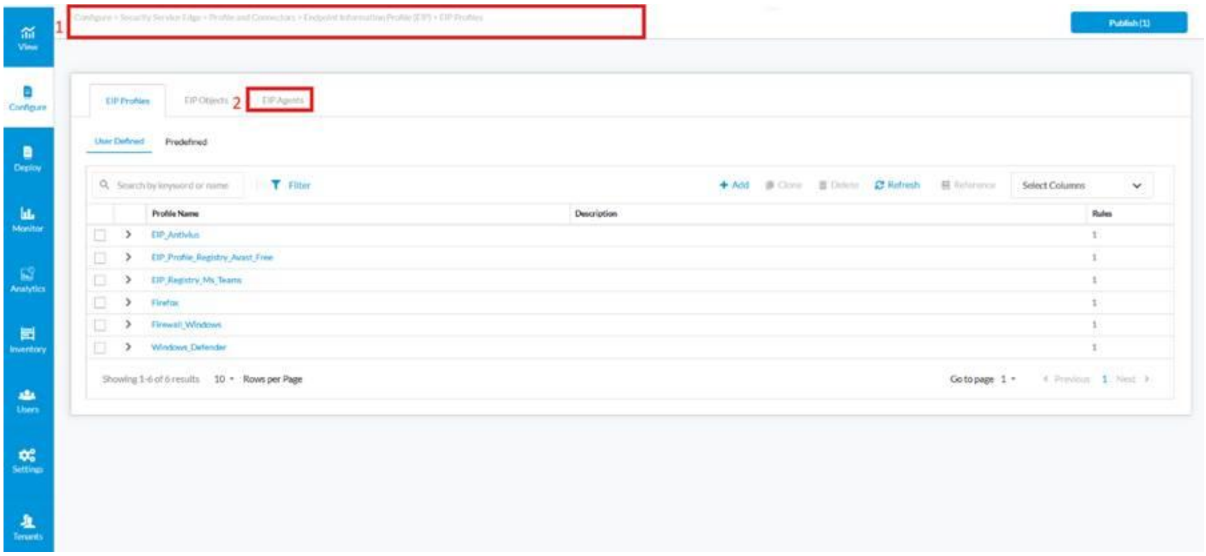
Rules ✎ Edit

Name	Category	Objects	User Defined Objects	Predefined Objects
EIP_Prof_Host_ID	General	1	› EIP_Host_ID	

Note: After creating the EIP Object and configuring the EIP Profile and Agent Profile, you must apply them to the Secure Access Client policy to enforce device posture validation and continue evaluation.

Step 3: Navigate to the EIP Agent Section

Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Agents



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

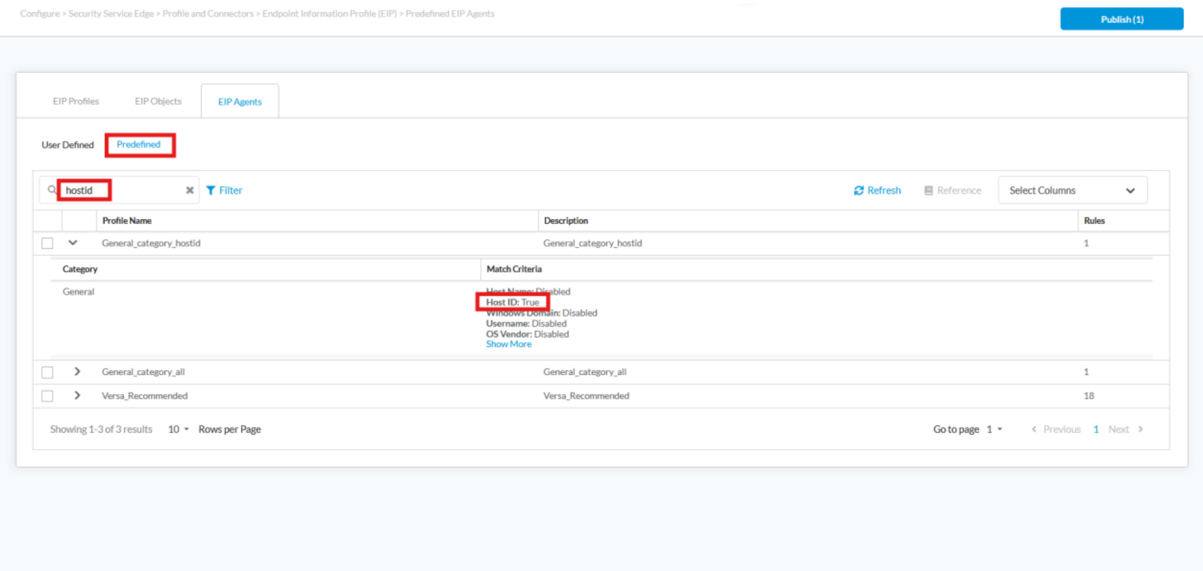
		Profile Name	Description	Rules
□	›	EIP_Antivirus		1
□	›	EIP_Profile_Registry_Avast_Free		1
□	›	EIP_Registry_Ms_Teams		1
□	›	Firefox		1
□	›	Firewall_Windows		1
□	›	Windows_Defender		1

Showing 1-6 of 6 results 10 Rows per Page Go to page 1 Previous 1 Next

Step 4: Create an EIP Agent Profile

Important Note: Instead of creating a new agent manually, you can also use a predefined Versa Host Id agent. In the

Predefined tab, search for domain and select General_category_hostid, which already includes the rule Windows Domain: True.



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > Predefined EIP Agents

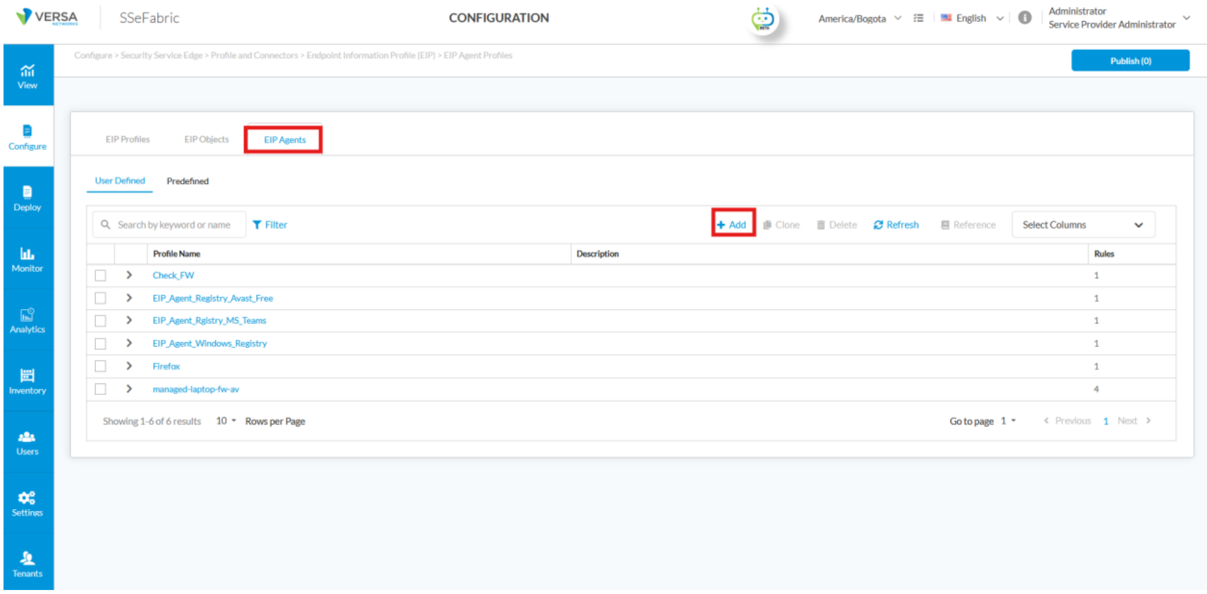
Search: hostid

Profile Name	Description	Rules
General_category_hostid	General_category_hostid	1
General_category_all	General_category_all	1
Versa_Recommended	Versa_Recommended	18

Category	Match Criteria
General	Host Name: Disabled Host ID: True Windows Domain: Disabled Username: Disabled OS Vendor: Disabled Show More

Showing 1-3 of 3 results 10 Rows per Page Go to page 1 Previous 1 Next

Click on **Add** to create a **new Agent profile**.

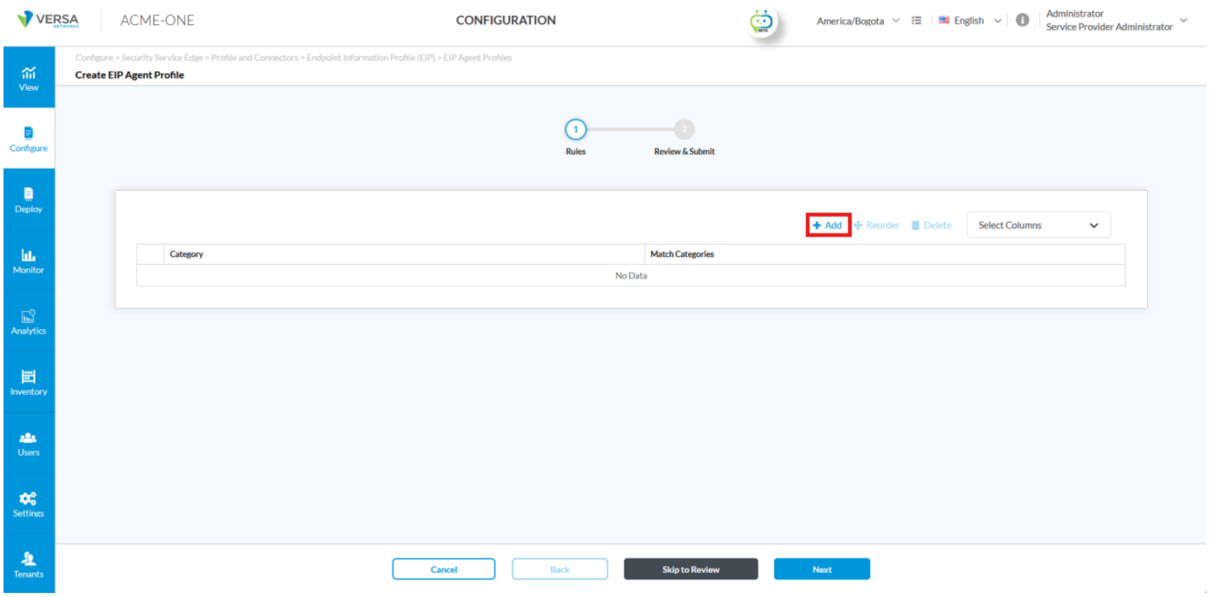


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

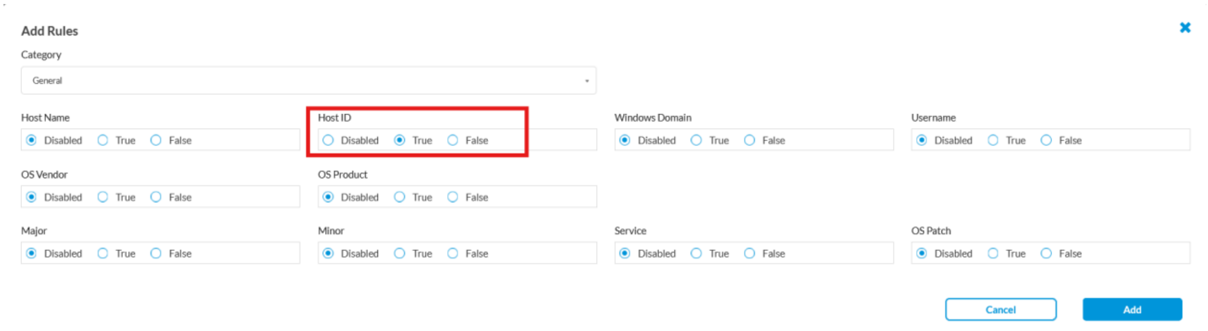
Profile Name	Description	Rules
Check_FW		1
EIP_Agent_Registry_Avast_Free		1
EIP_Agent_Rgistry_MS_Teams		1
EIP_Agent_Windows_Registry		1
Firefox		1
managed-laptop-fw-av		4

Showing 1-6 of 6 results 10 Rows per Page Go to page 1 Previous 1 Next

Click on "+Add" to create a new rule. Then choose general



In the **general** section, locate click Host ID by default is set to Disable change to true, then Click Add.


Add Rules

Category: General

Host Name: ● Disabled ○ True ○ False

Host ID: ○ Disabled ● True ○ False

Windows Domain: ● Disabled ○ True ○ False

Username: ● Disabled ○ True ○ False

OS Vendor: ● Disabled ○ True ○ False

OS Product: ● Disabled ○ True ○ False

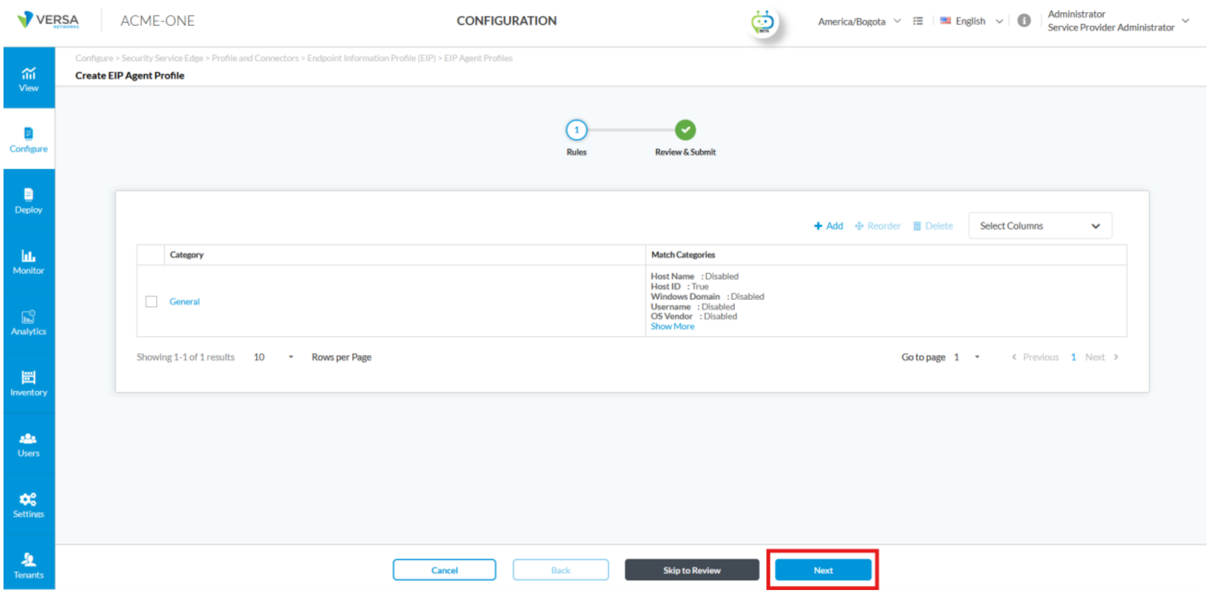
Major: ● Disabled ○ True ○ False

Minor: ● Disabled ○ True ○ False

Service: ● Disabled ○ True ○ False

OS Patch: ● Disabled ○ True ○ False

Click on “next” to enter a descriptive Profile Name (Example., **EIP_Agent_Host_ID**).

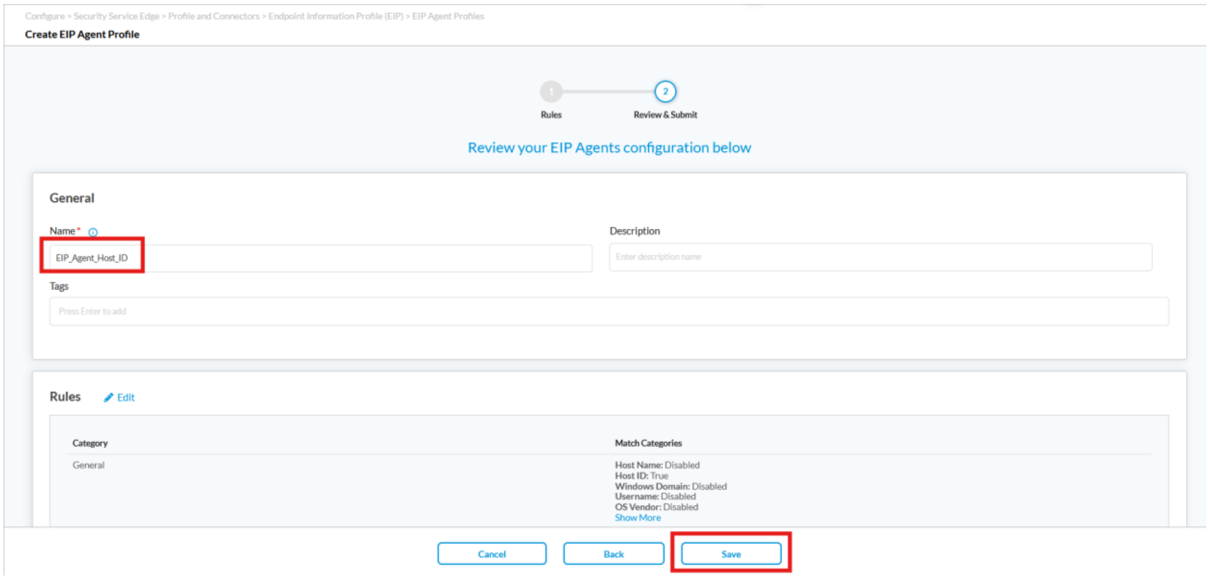


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Create EIP Agent Profile

	Category	Match Categories
□	General	Host Name : Disabled Host ID : True Windows Domain : Disabled Username : Disabled OS Vendor : Disabled Show More

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 ‹ Previous 1 Next ›



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Create EIP Agent Profile

Review your EIP Agents configuration below

General

Name* : EIP_Agent_Host_ID

Description : Enter description name

Tags : Press Enter to add

Rules

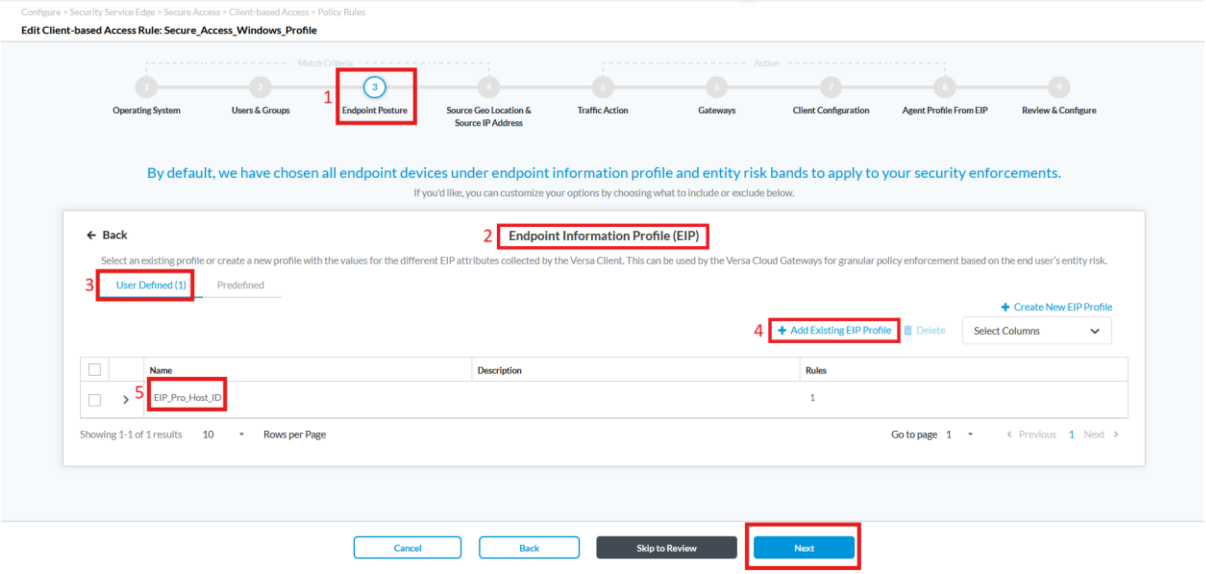
Category	Match Categories
General	Host Name: Disabled Host ID: True Windows Domain: Disabled Username: Disabled OS Vendor: Disabled Show More

Step 5: Configure Secure Client Access Rule

Navigate to: Configure > Security Service Edge > Secure Access > Client-based Access > Rules.

Click "**+ Add**" to create a new Secure Access Client rule or edit an existing rule.

In the Match Criteria configuration, go to the ***Endpoint Posture*** section. Under the *Endpoint Information Profile (EIP)* panel, select the desired profile by navigating to the ***User Defined*** tab and clicking on *Add Existing EIP Profile*. Then, choose the EIP profile you previously created. Example EIP_Prof_Host_ID).



Edit Client-based Access Rule: Secure_Access_Windows_Profile

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

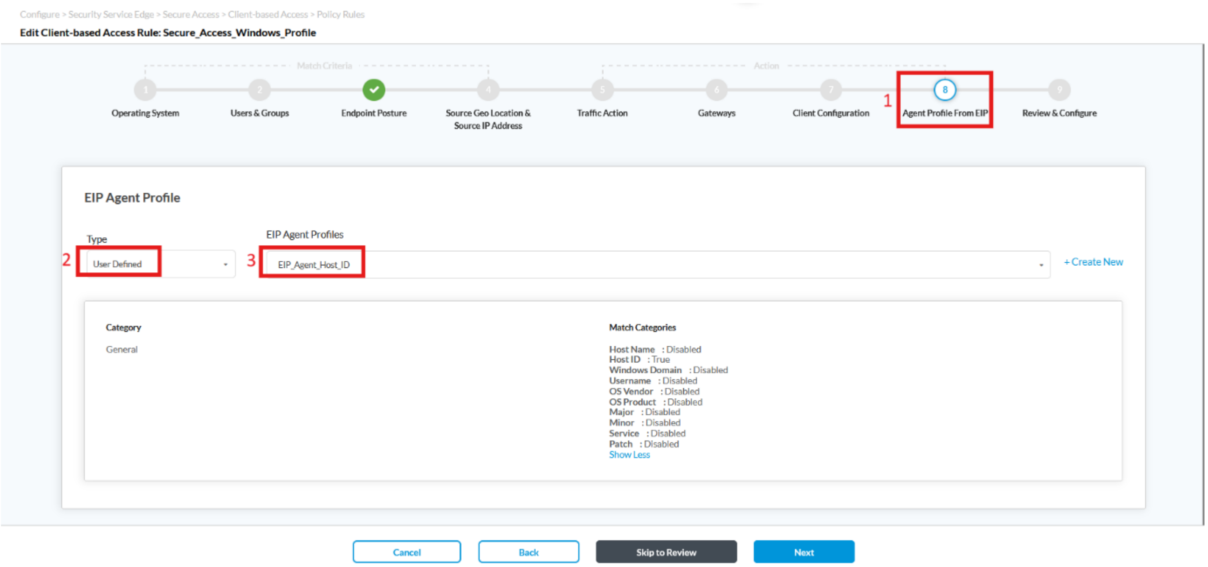
Endpoint Information Profile (EIP)

Select an existing profile or create a new profile with the values for the different EIP attributes collected by the Versa Client. This can be used by the Versa Cloud Gateways for granular policy enforcement based on the end user's entity risk.

□		Name	Description	Rules
□	›	EIP_Pro_Host_ID		1

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 ‹ Previous 1 Next ›

In action configuration, under the **Agent Profile From EIP** section, set the Type to **User Defined** and select the **EIP Agent Profile** you previously created. Example EIP_Agent_Host_ID. *The Match Categories panel will display the defined validation criteria, such as registry paths or process checks, ensuring that the selected EIP Agent Profile is applied for endpoint posture verification*.



Edit Client-based Access Rule: Secure_Access_Windows_Profile

EIP Agent Profile

Type: User Defined

EIP Agent Profiles: EIP_Agent_Host_ID

Category: General

Match Categories
Host Name : Disabled
Host ID : True
Windows Domain : Disabled
Username : Disabled
OS Vendor : Disabled
OS Product : Disabled
Major : Disabled
Minor : Disabled
Service : Disabled
Patch : Disabled

Use Cases for MacOS

Endpoint Information Profiles (EIP) classify endpoints based on their posture information, enabling organizations to enforce security policies that ensure devices adhere to enterprise standards before accessing network resources. This is a core capability within a Zero Trust framework, which eliminates implicit trust for users or devices.

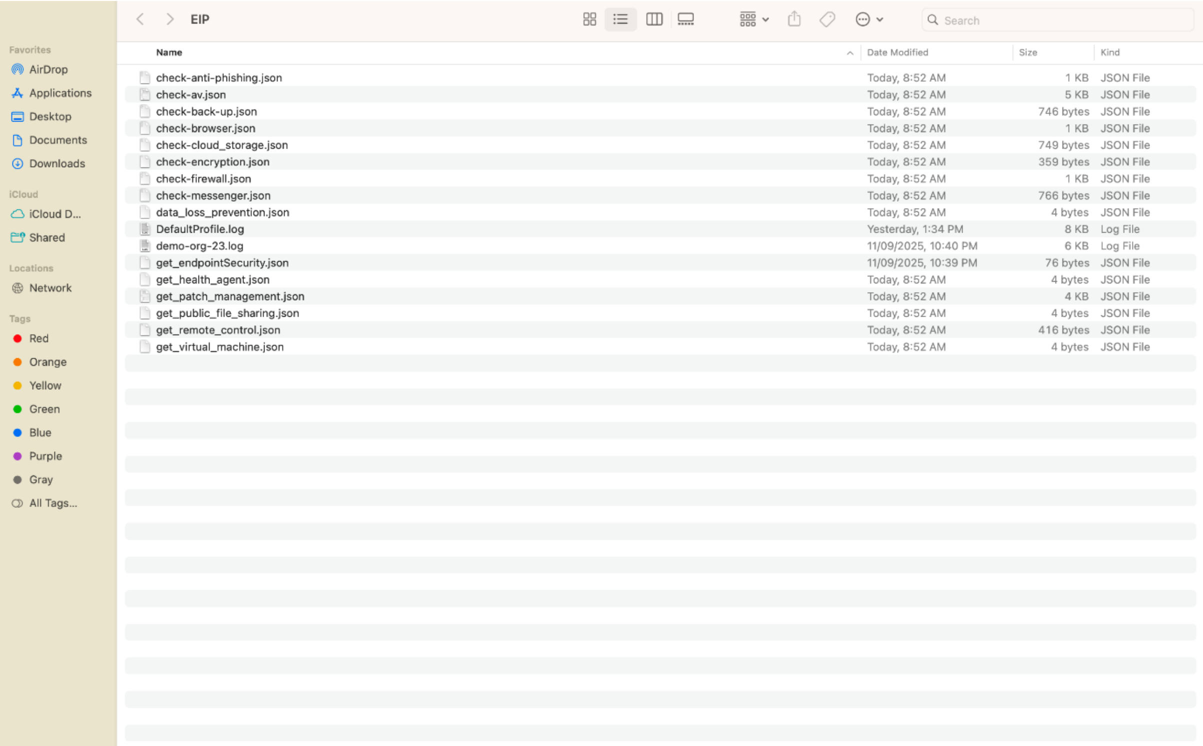
For macOS devices, EIP can be leveraged to validate multiple attributes and determine compliance before granting access. Common criteria for EIP selection include:

- **Operating System:** macOS major/minor version and the presence of required security updates (patch level).
- **Antivirus / Endpoint Protection:** Status and version of the installed macOS endpoint security agent — for example, CrowdStrike Falcon, SentinelOne, Jamf Protect, Malwarebytes, or Microsoft Defender for Endpoint (the latter is available but less commonly used on macOS).
- **Disk Encryption:** FileVault status (enabled/disabled) and encryption compliance for the system drive.
- **Firewall & Network Controls:** Built-in macOS firewall state and whether any corporate network filtering or DNS proxy agents are present and running.
- **Software Installation:** Whether required corporate applications or security tools are installed and active.

By leveraging these checks, administrators can enforce granular access policies. For example, a policy can be configured to allow access to critical SaaS applications only if the macOS device is encrypted with FileVault, has an approved endpoint security solution installed, and runs a supported OS version. This ensures that only compliant macOS endpoints connect to sensitive enterprise resources, strengthening security and posture validation.

On macOS posture attributes can be verified locally by reviewing the EIP output files generated on the device, located under:

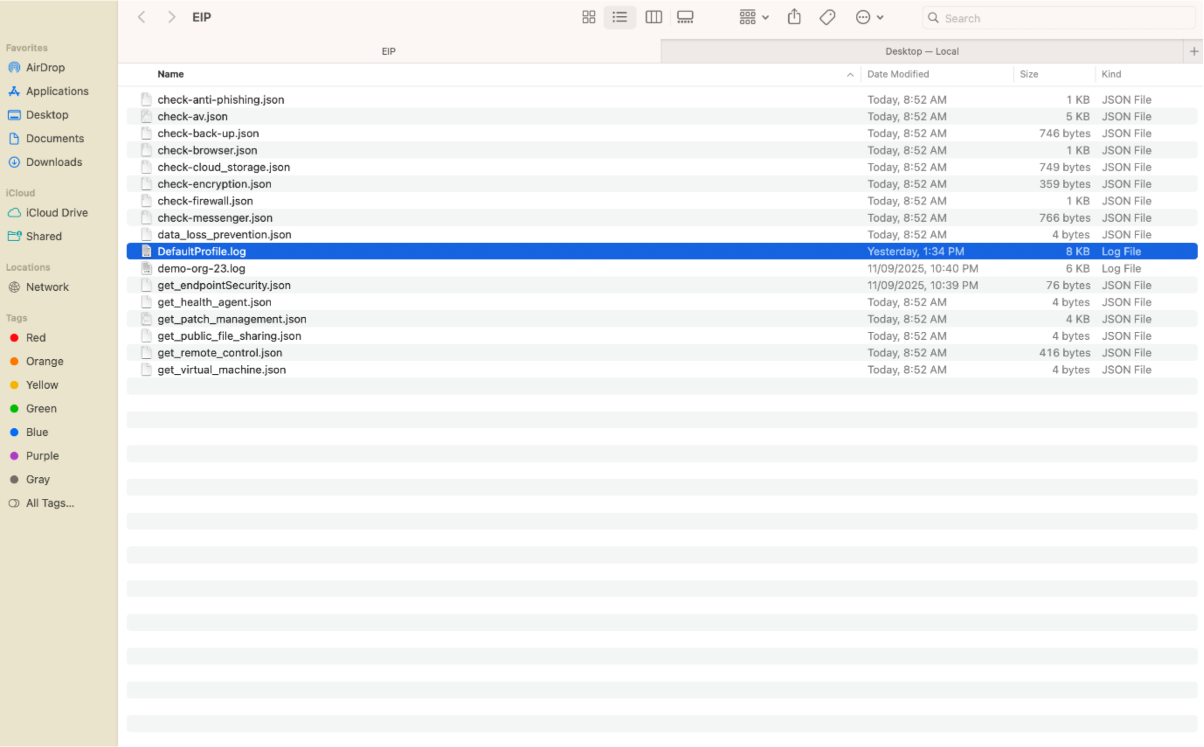
/private/var/log/versa/EIP/



Name	Date Modified	Size	Kind
check-anti-phishing.json	Today, 8:52 AM	1 KB	JSON File
check-av.json	Today, 8:52 AM	5 KB	JSON File
check-back-up.json	Today, 8:52 AM	746 bytes	JSON File
check-browser.json	Today, 8:52 AM	1 KB	JSON File
check-cloud_storage.json	Today, 8:52 AM	749 bytes	JSON File
check-encryption.json	Today, 8:52 AM	359 bytes	JSON File
check-firewall.json	Today, 8:52 AM	1 KB	JSON File
check-messenger.json	Today, 8:52 AM	766 bytes	JSON File
data_loss_prevention.json	Today, 8:52 AM	4 bytes	JSON File
DefaultProfile.log	Yesterday, 1:34 PM	8 KB	Log File
demo-org-23.log	11/09/2025, 10:40 PM	6 KB	Log File
get_endpointSecurity.json	11/09/2025, 10:39 PM	76 bytes	JSON File
get_health_agent.json	Today, 8:52 AM	4 bytes	JSON File
get_patch_management.json	Today, 8:52 AM	4 KB	JSON File
get_public_file_sharing.json	Today, 8:52 AM	4 bytes	JSON File
get_remote_control.json	Today, 8:52 AM	416 bytes	JSON File
get_virtual_machine.json	Today, 8:52 AM	4 bytes	JSON File

There are two ways to check the posture information:

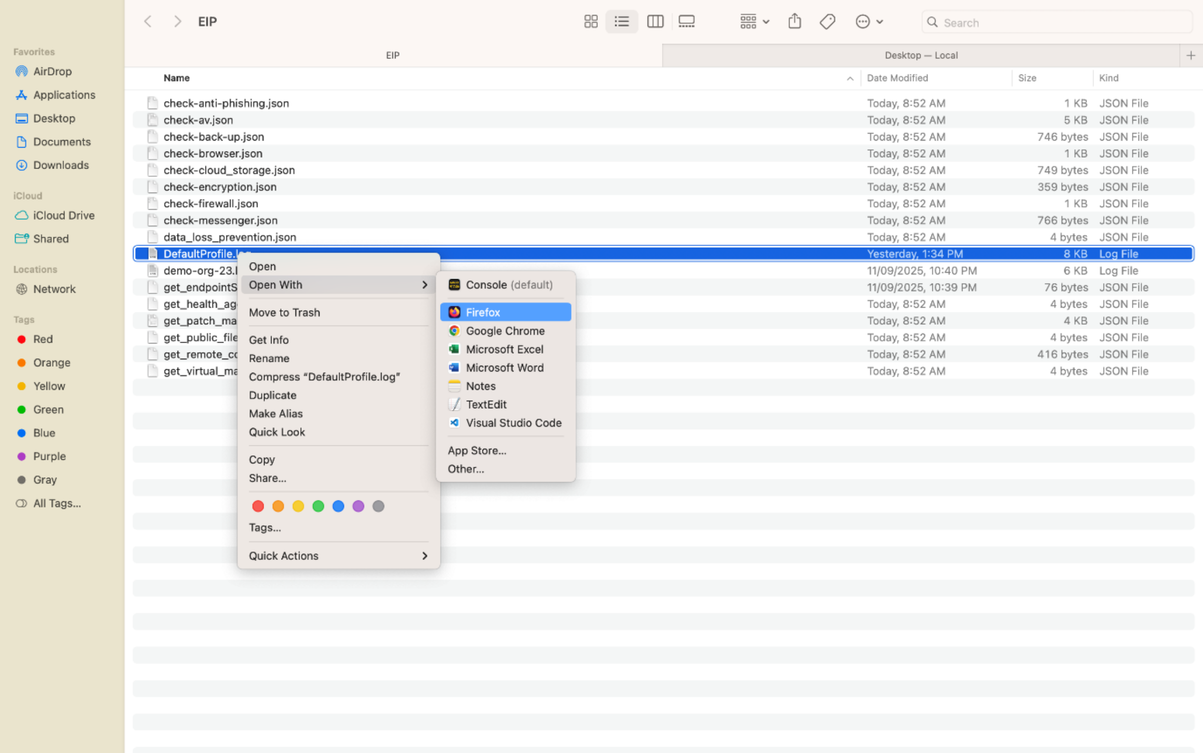
- To validate a specific control such as antivirus, anti-phishing, firewall, or encryption, open the corresponding JSON file (e.g., **check-av.json, check-anti-phishing.json, check-firewall.json, check-encryption.jso**n). Each JSON file contains detailed results for that module.
- To view all posture checks together, review **DefaultProfile.log** or **Tenant-name.log** in this case **demo-org-23.log**, which aggregates the results from every module.



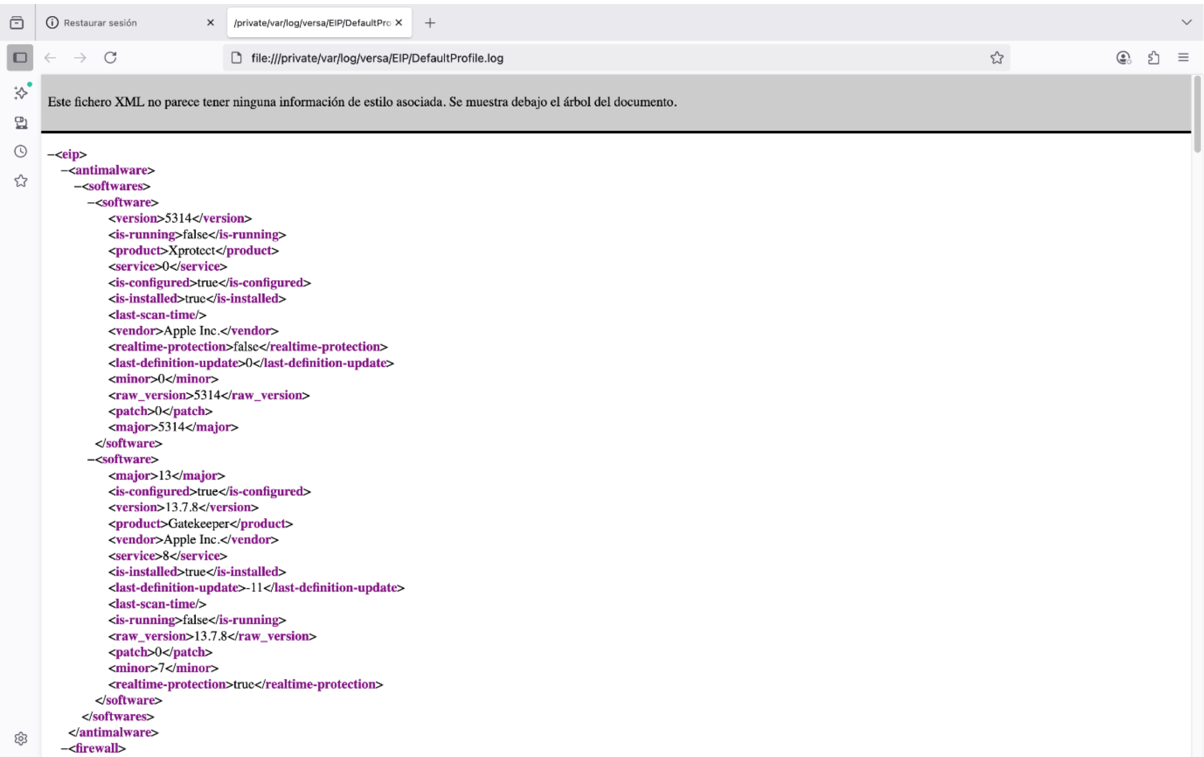
Name	Date Modified	Size	Kind
check-anti-phishing.json	Today, 8:52 AM	1 KB	JSON File
check-av.json	Today, 8:52 AM	5 KB	JSON File
check-back-up.json	Today, 8:52 AM	746 bytes	JSON File
check-browser.json	Today, 8:52 AM	1 KB	JSON File
check-cloud_storage.json	Today, 8:52 AM	749 bytes	JSON File
check-encryption.json	Today, 8:52 AM	359 bytes	JSON File
check-firewall.json	Today, 8:52 AM	1 KB	JSON File
check-messenger.json	Today, 8:52 AM	766 bytes	JSON File
data_loss_prevention.json	Today, 8:52 AM	4 bytes	JSON File
DefaultProfile.log	Yesterday, 1:34 PM	8 KB	Log File
demo-org-23.log	11/09/2025, 10:40 PM	6 KB	Log File
get_endpointSecurity.json	11/09/2025, 10:39 PM	76 bytes	JSON File
get_health_agent.json	Today, 8:52 AM	4 bytes	JSON File
get_patch_management.json	Today, 8:52 AM	4 KB	JSON File
get_public_file_sharing.json	Today, 8:52 AM	4 bytes	JSON File
get_remote_control.json	Today, 8:52 AM	416 bytes	JSON File
get_virtual_machine.json	Today, 8:52 AM	4 bytes	JSON File

Graphical (macOS):

1. Right-click a JSON or log file.
2. Choose Open With > Firefox (for better readability of JSON) or Open With > TextEdit.
3. Review the posture results directly in the viewer.



Name	Date Modified	Size	Kind
check-anti-phishing.json	Today, 8:52 AM	1 KB	JSON File
check-av.json	Today, 8:52 AM	5 KB	JSON File
check-back-up.json	Today, 8:52 AM	746 bytes	JSON File
check-browser.json	Today, 8:52 AM	1 KB	JSON File
check-cloud_storage.json	Today, 8:52 AM	749 bytes	JSON File
check-encryption.json	Today, 8:52 AM	359 bytes	JSON File
check-firewall.json	Today, 8:52 AM	1 KB	JSON File
check-messenger.json	Today, 8:52 AM	766 bytes	JSON File
data_loss_prevention.json	Today, 8:52 AM	4 bytes	JSON File
DefaultProfile.l	Yesterday, 1:34 PM	8 KB	Log File
demo-org-23.l	11/09/2025, 10:40 PM	6 KB	Log File
get_endpointS	11/09/2025, 10:39 PM	76 bytes	JSON File
get_health_ag	Today, 8:52 AM	4 bytes	JSON File
get_patch_ma	Today, 8:52 AM	4 KB	JSON File
get_public_file	Today, 8:52 AM	4 bytes	JSON File
get_remote_cc	Today, 8:52 AM	416 bytes	JSON File
get_virtual_ma	Today, 8:52 AM	4 bytes	JSON File



Restaurar sesión
/private/var/log/versa/EIP/DefaultPro
file:///private/var/log/versa/EIP/DefaultProfile.log

Este fichero XML no parece tener ninguna información de estilo asociada. Se muestra debajo el árbol del documento.

```
–<eip>
  –<antimalware>
    –<softwares>
      –<software>
          <version>5314</version>
          <is-running>false</is-running>
          <product>Xprotect</product>
          <service>0</service>
          <is-configured>true</is-configured>
          <is-installed>true</is-installed>
          <last-scan-time/>
          <vendor>Apple Inc.</vendor>
          <realtime-protection>false</realtime-protection>
          <last-definition-update>0</last-definition-update>
          <minor>0</minor>
          <raw_version>5314</raw_version>
          <patch>0</patch>
          <major>5314</major>
        </software>
      –<software>
          <major>13</major>
          <is-configured>true</is-configured>
          <version>13.7.8</version>
          <product>Gatekeeper</product>
          <vendor>Apple Inc.</vendor>
          <service>8</service>
          <is-installed>true</is-installed>
          <last-definition-update>-11</last-definition-update>
          <last-scan-time/>
          <is-running>false</is-running>
          <raw_version>13.7.8</raw_version>
          <patch>0</patch>
          <minor>7</minor>
          <realtime-protection>true</realtime-protection>
        </software>
      </softwares>
    </antimalware>
  –<firewall>
```

Terminal (macOS):

- view AV check (raw)

```
cat /private/var/log/versa/EIP/check-av.json
```

- view formatted JSON (if python is available)

```
python3 -m json.tool /private/var/log/versa/EIP/check-av.json | less
```

Anti-malware

Anti-malware validation within an Endpoint Identity Profile (EIP) provides a way to confirm that endpoints are running an approved security agent and that the protection status is healthy. This method helps ensure devices are protected against malicious software before being granted access to enterprise resources.

For macOS devices, administrators can check the installed and running anti-malware software either through the EIP posture logs **(/private/var/log/versa/EIP/check-av.json**) or directly from the system:

- To verify if a specific process (e.g., CrowdStrike, Jamf Protect, Malwarebytes) is running:

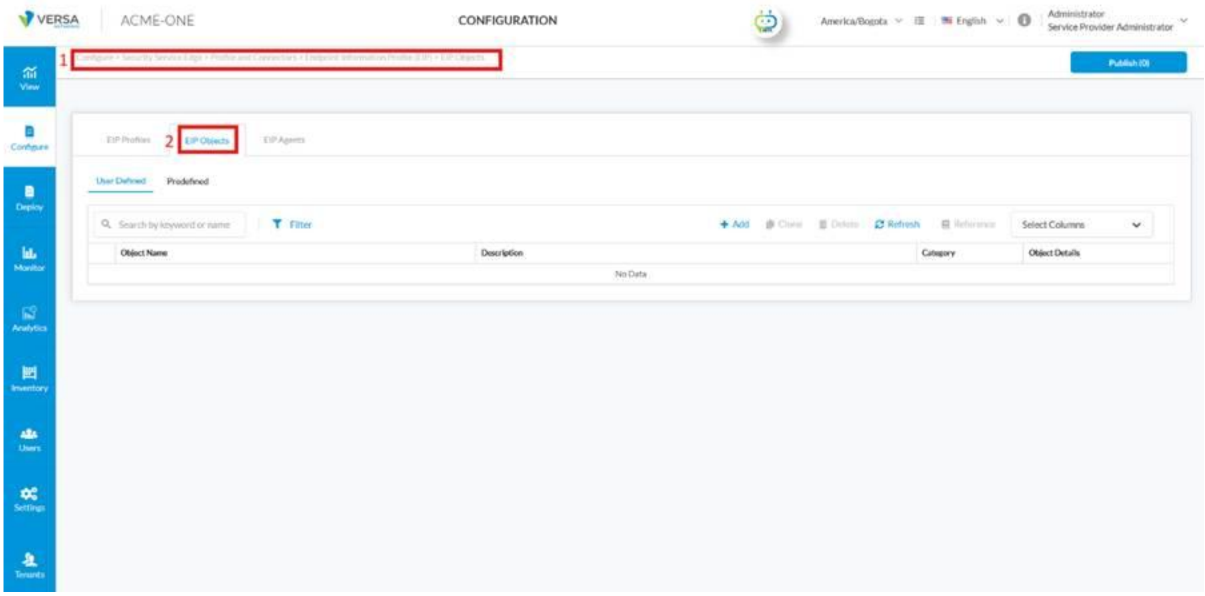
```
ps aux | grep -i crowdstrike
```

Scenario: An organization requires that all corporate laptops have an approved anti-malware agent installed and active (for example, CrowdStrike Falcon, Malwarebytes or Jamf Protect). In the EIP Profile, the administrator defines compliance rules for anti-malware. When a device connects:

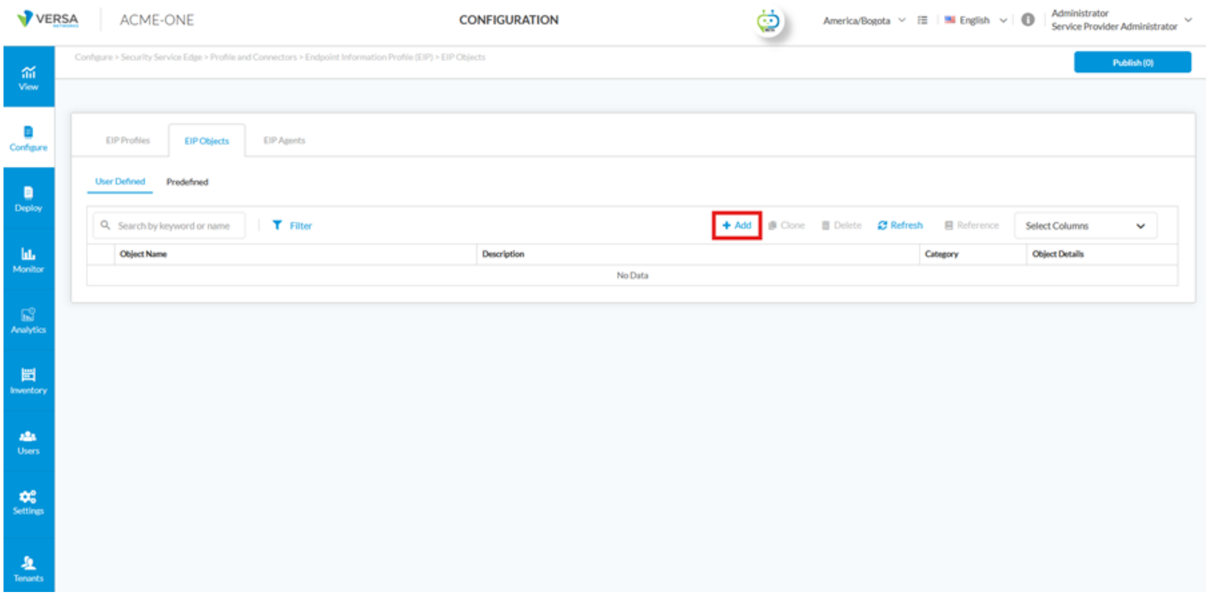
- If the anti-malware software is installed and running, the device is considered compliant.
- If the software is missing or inactive, the device is flagged as non-compliant and access may be restricted.
- This ensures that only endpoints with active anti-malware protection can access sensitive corporate applications, reinforcing Zero Trust posture validation.

Step 1: Create an EIP Object with AntiMalware

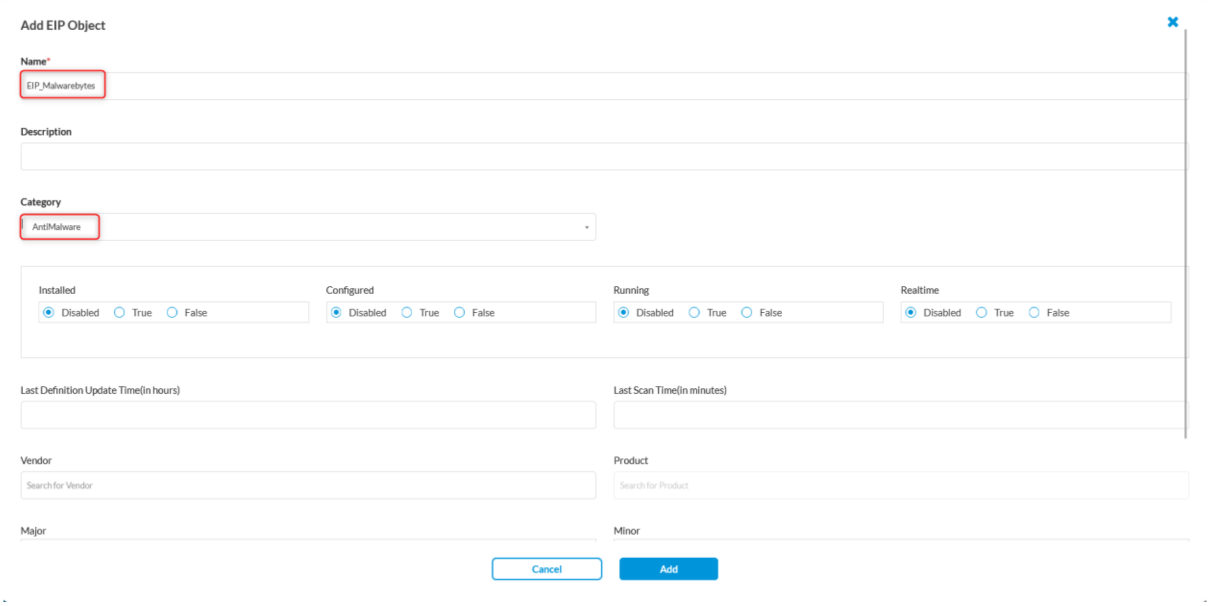
Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Objects



Click on "+ Add" to create a new EIP Object.



Enter a descriptive name for your EIP object. ***Example:*** **EIP_AntiMalware_Malwarebytes.** And Select **AntiMalware** from the dropdown.



Add EIP Object

Name*
EIP_Malwarebytes

Description

Category
AntiMalware

Installed
● Disabled ○ True ○ False

Configured
● Disabled ○ True ○ False

Running
● Disabled ○ True ○ False

Realtime
● Disabled ○ True ○ False

Last Definition Update Time(in hours)

Last Scan Time(in minutes)

Vendor
Search for Vendor

Product
Search for Product

Major

Minor

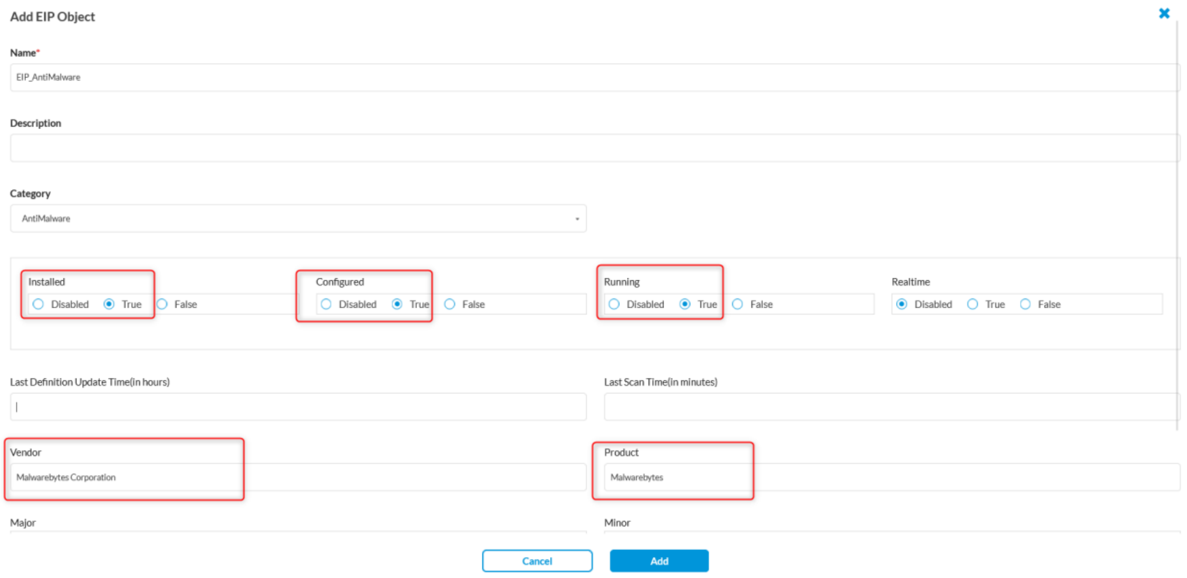
In the **Anti-Malware** section of the EIP object, configure the following options to validate that the endpoint is protected:

- Installed: True
- Configured: True
- Running: True
- **Realtime**: True (optional but recommended)
- **Vendor / Product**: Specify the approved anti-malware solution.

As an example, the screenshot below shows Malwarebytes configured with the values:

  - **Vendor**: Malwarebytes Corporation
  - **Product**: Malwarebytes

This configuration ensures that endpoints are only considered compliant if Malwarebytes is both installed and actively running. If the product is missing or inactive, the device will be flagged as non-compliant and may be denied access to corporate resources.


Add EIP Object

Name*: EIP_AntiMalware

Description:

Category: AntiMalware

Installed: ○ Disabled ● True ○ False

Configured: ○ Disabled ● True ○ False

Running: ○ Disabled ● True ○ False

Realtime: ● Disabled ○ True ○ False

Last Definition Update Time(in hours):

Last Scan Time(in minutes):

Vendor: Malwarebytes Corporation

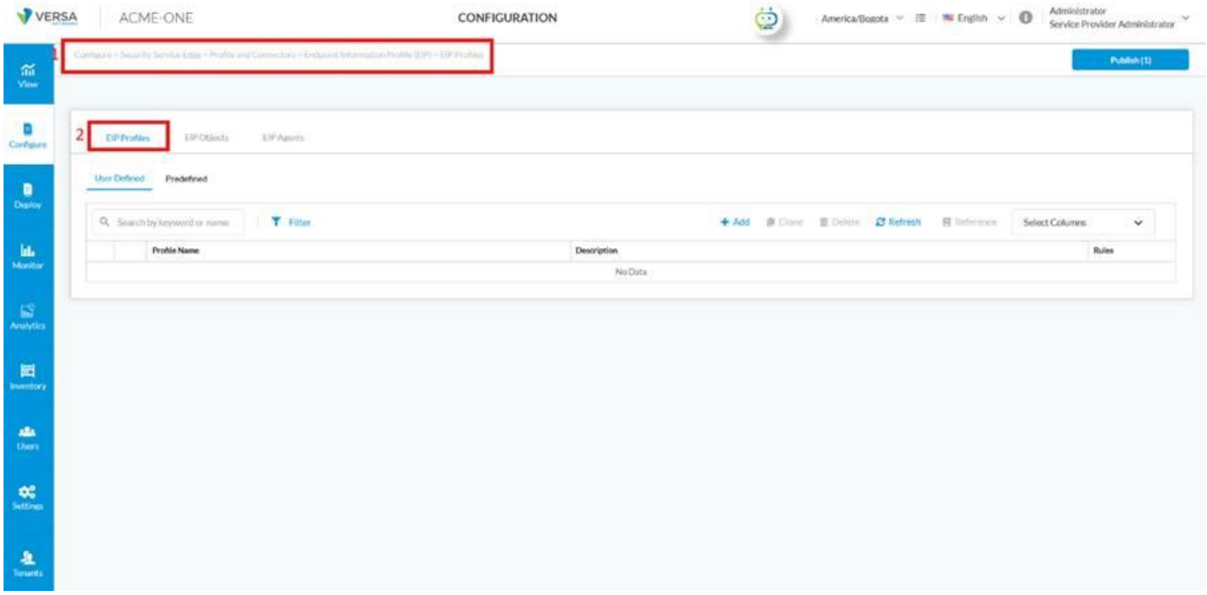
Product: Malwarebytes

Major

Minor

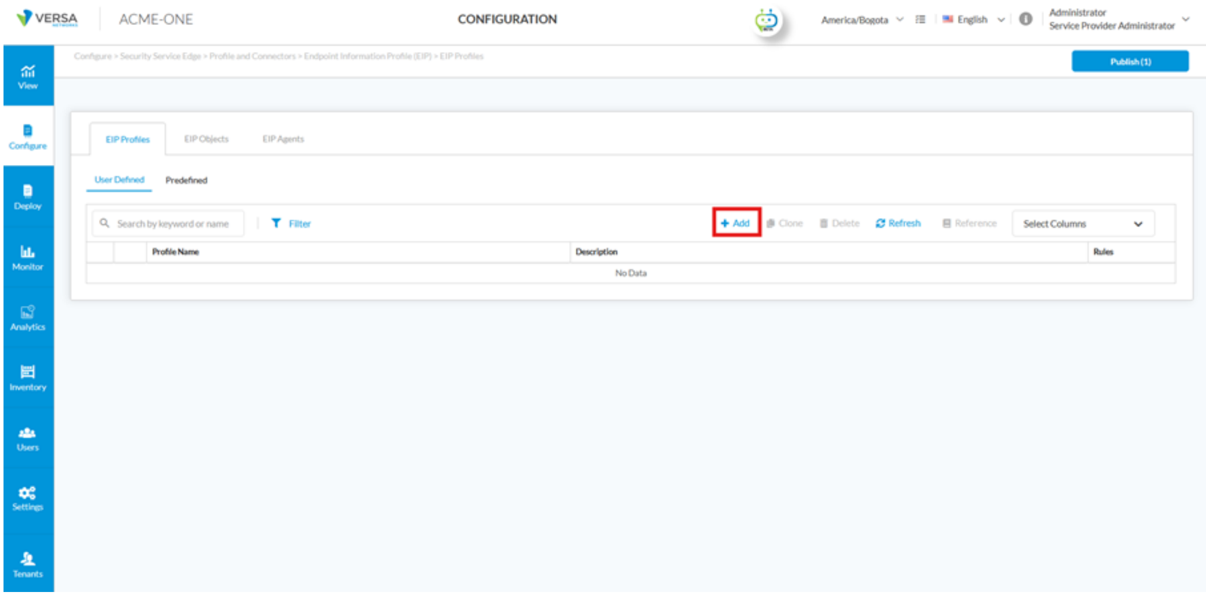
Step 2: Create an EIP Profile Using AntiMalware

Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Profiles

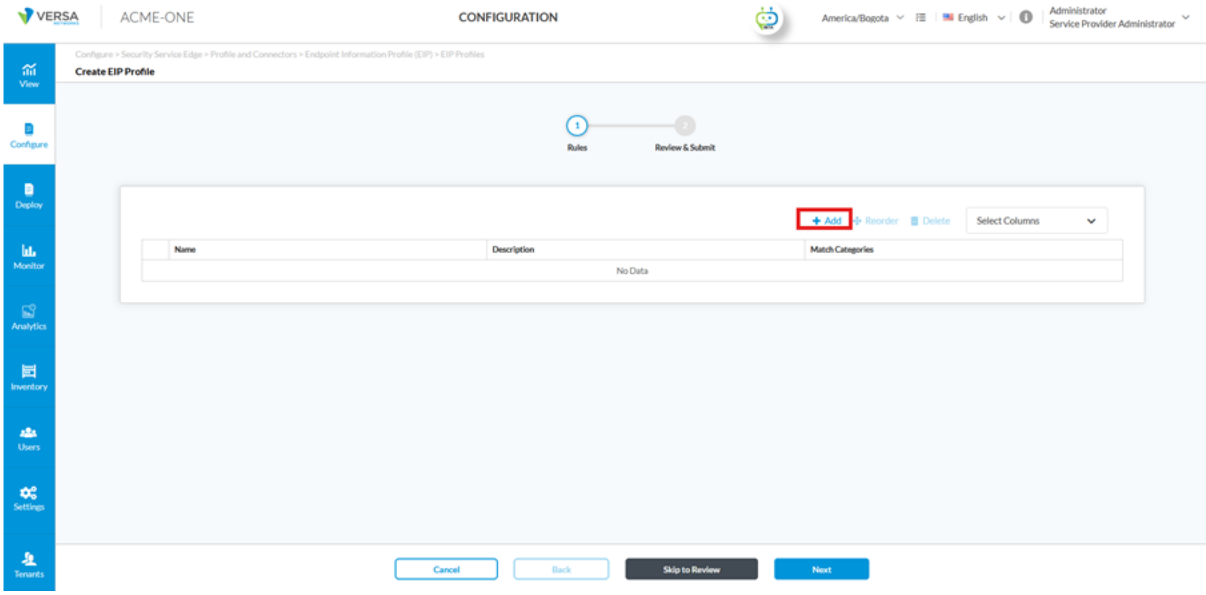


	Profile Name	Description	Rules
		No Data	

Click on “+ Add” to start creating a new profile.



In the **Create EIP Profile** window, Click on "+ Add" to define a new rule.

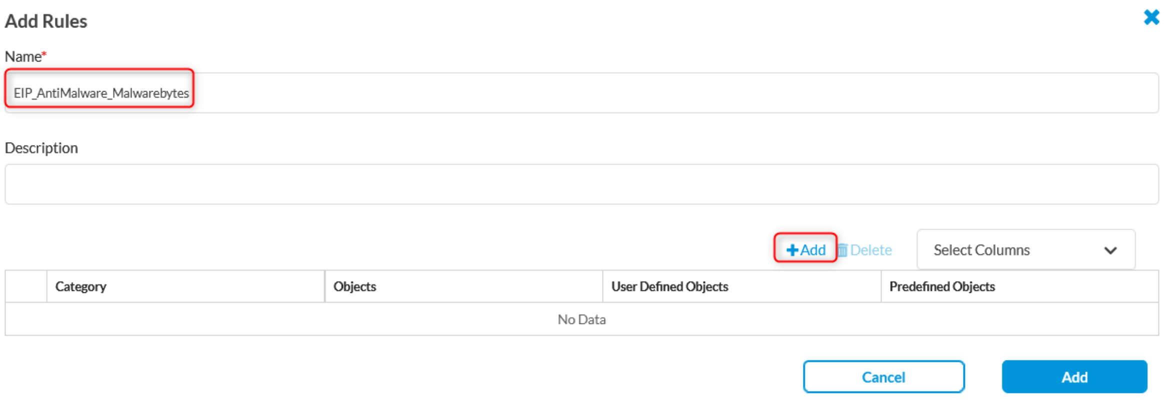


Create a Rule for AntiMalware

Enter a Name for your rule, Example, EIP_AntiMalware_Malwarebytes.

You would (Optional) Add a description for clarity.

Click "+ Add" to attach an EIP Object.



Add Rules

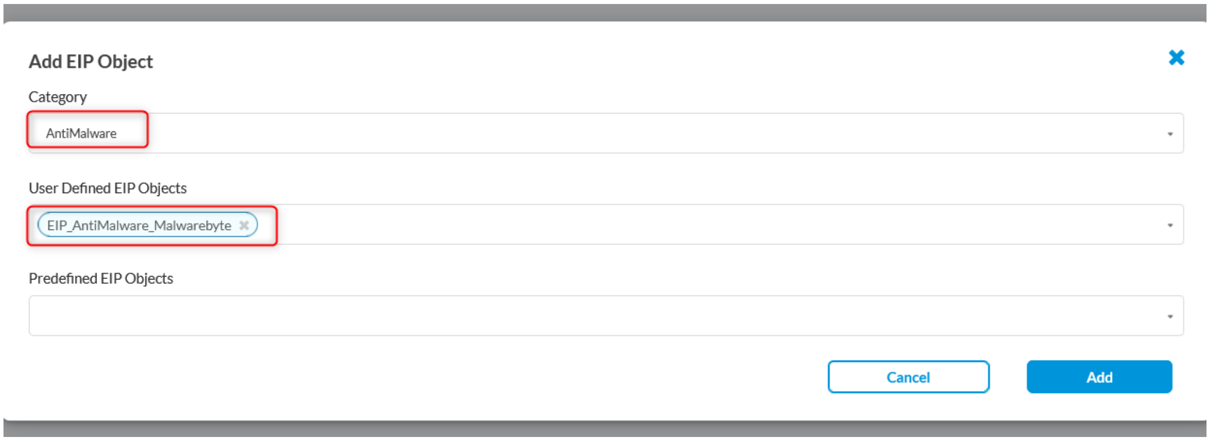
Name*: EIP_AntiMalware_Malwarebytes

Description:

	Category	Objects	User Defined Objects	Predefined Objects
No Data				

In Add EIP Object dialog, choose the Category. Example **AntiMalware**.

Select an existing EIP Object or create a new one. For example, an object was created to verify if MacOs AntiMalware Malwarebytes is installed, running and configured in the previous section.



Add EIP Object

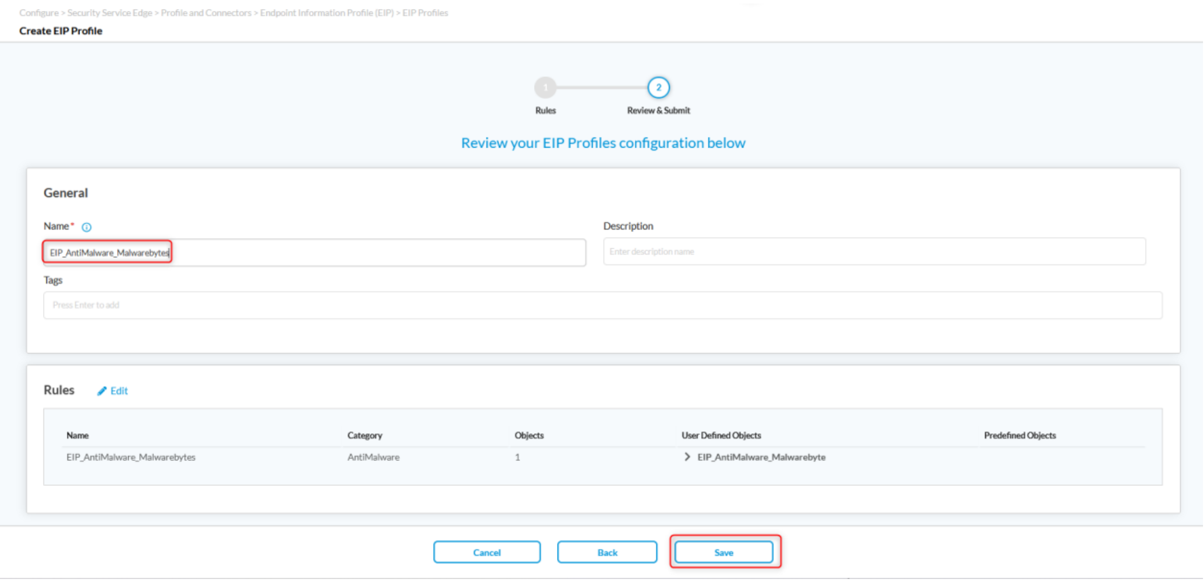
Category: AntiMalware

User Defined EIP Objects: EIP_AntiMalware_Malwarebyte

Predefined EIP Objects:

Click **Next** and then Enter a descriptive name for your EIP object. ***Example:*** EIP_AntiMalware_Malwarebytes**.**

Review and **Save** the Profile creation



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Create EIP Profile

Review your EIP Profiles configuration below

General

Name*: EIP_AntiMalware_Malwarebytes

Description: Enter description name

Tags: Press Enter to add

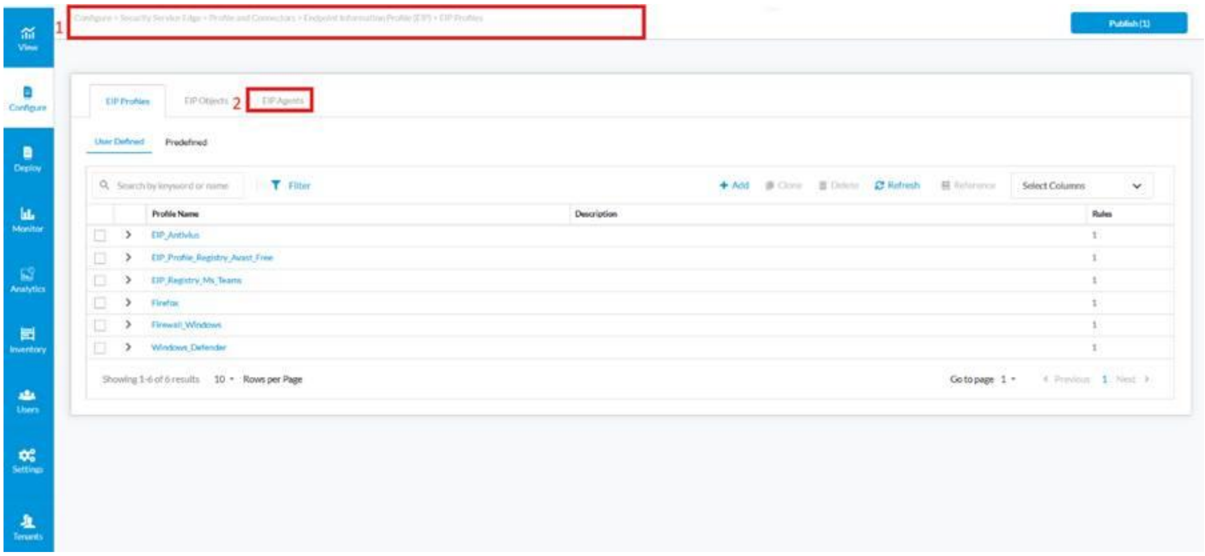
Rules

Name	Category	Objects	User Defined Objects	Predefined Objects
EIP_AntiMalware_Malwarebytes	AntiMalware	1	> EIP_AntiMalware_Malwarebyte	

Note: After creating the EIP Object and configuring the EIP Profile and Agent Profile, you must apply them to the Secure Access Client policy to enforce device posture validation and continue evaluation.

Step 3: Navigate to the EIP Agent Section

Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Agents



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

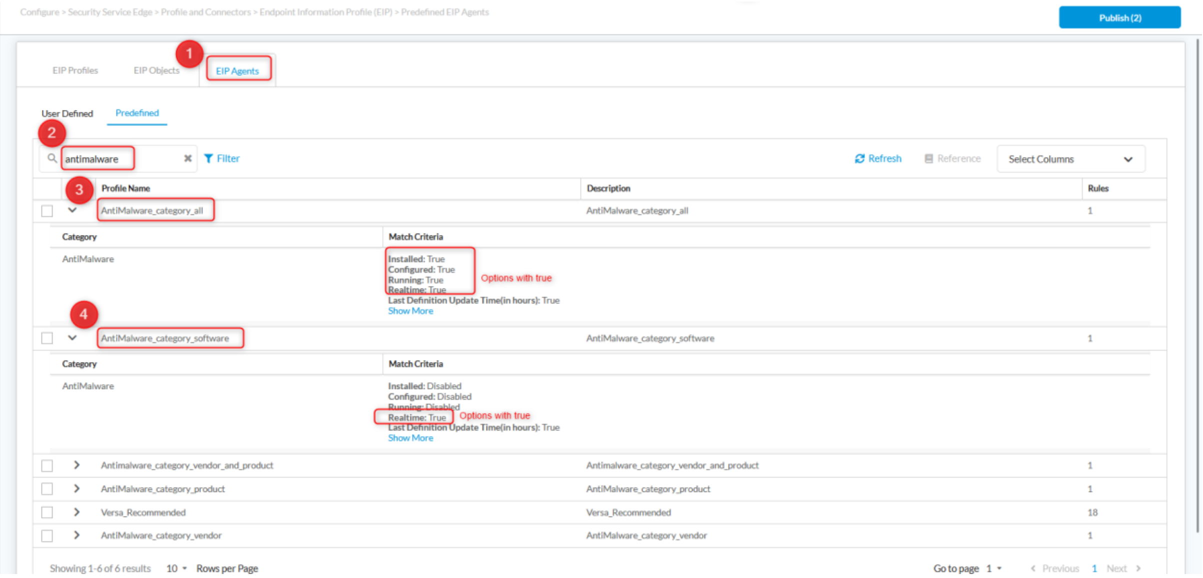
		Profile Name	Description	Rules
□	>	EIP_Antivius		1
□	>	EIP_Profile_Registry_Avast_Free		1
□	>	EIP_Registry_Ms_Teams		1
□	>	Firefox		1
□	>	Firewall_Windows		1
□	>	Windows_Defender		1

Showing 1-6 of 6 results 10 Rows per Page Go to page 1 Previous 1 Next

Step 4: Create an EIP Agent Profile

Important Note: Instead of creating a new agent manually, you can also use a predefined Versa Anti-Malware agent.

In the *Predefined* tab, search for **antimalware** and select the predefined category that matches your requirements. This option already includes baseline rules such as **Installed: True**, **Configured: True**, and others.



	Profile Name	Description	Rules
□	AntiMalware_category_all	AntiMalware_category_all	1
□	AntiMalware_category_software	AntiMalware_category_software	1
□	Antimalware_category_vendor_and_product	Antimalware_category_vendor_and_product	1
□	AntiMalware_category_product	AntiMalware_category_product	1
□	Versa_Recommended	Versa_Recommended	18
□	AntiMalware_category_vendor	AntiMalware_category_vendor	1

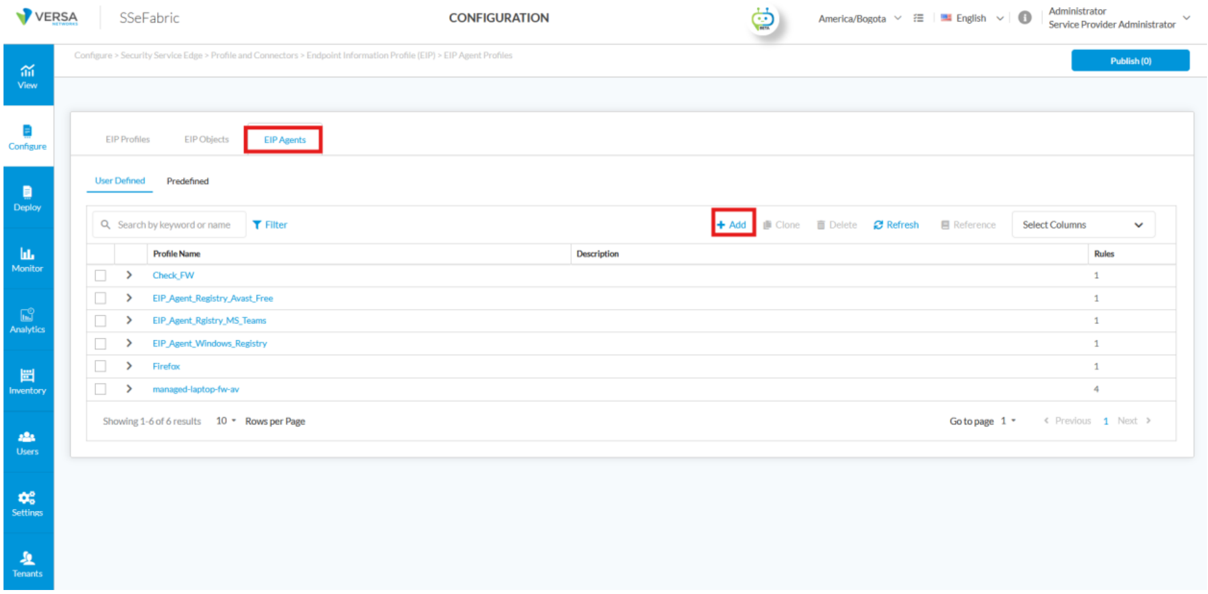
AntiMalware_category_all:

Category	Match Criteria
AntiMalware	**Installed:** True **Configured:** True **Running:** True **Realtime:** True **Last Definition Update Time(in hours):** True

AntiMalware_category_software:

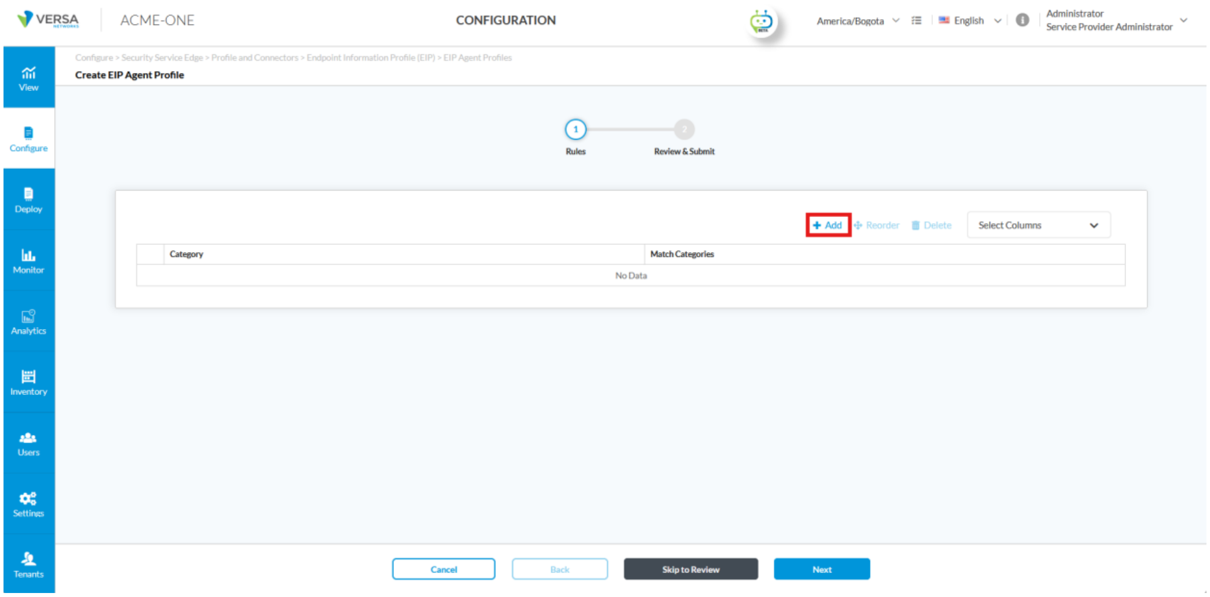
Category	Match Criteria
AntiMalware	**Installed:** Disabled **Configured:** Disabled **Running:** Disabled **Realtime:** True **Last Definition Update Time(in hours):** True

Click on **Add** to create a **new Agent profile**.



	Profile Name	Description	Rules
□	Check_FW		1
□	EIP_Agent_Registry_Avast_Free		1
□	EIP_Agent_Rgistry_MS_Teams		1
□	EIP_Agent_Windows_Registry		1
□	Firefox		1
□	managed-laptop-fw-av		4

Click on “+Add” to create a new rule. Then choose general



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

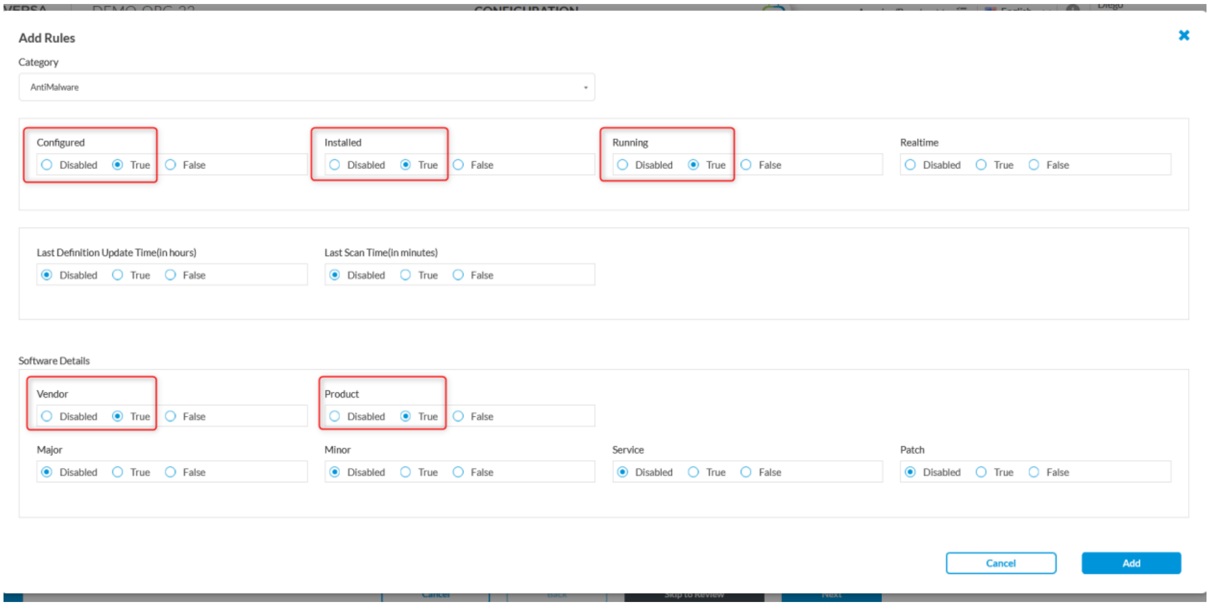
Create EIP Agent Profile

	Category	Match Categories
	No Data	

In the *Anti-Malware* category of the Agent Profile, configure the following options:

- Installed: True
- Configured: True
- Running: True
- **Realtime**: True (optional but recommended)
- **Vendor**: True
- Product: True

This configuration ensures that endpoints are validated for the presence and activity of anti-malware protection. Devices that fail any of these checks will be flagged as non-compliant and may be restricted from accessing corporate resources.



Add Rules

Category: AntiMalware

Configured: ○ Disabled ● True ○ False

Installed: ○ Disabled ● True ○ False

Running: ○ Disabled ● True ○ False

Realtime: ○ Disabled ○ True ○ False

Last Definition Update Time(in hours): ● Disabled ○ True ○ False

Last Scan Time(in minutes): ● Disabled ○ True ○ False

Software Details

Vendor: ○ Disabled ● True ○ False

Product: ○ Disabled ● True ○ False

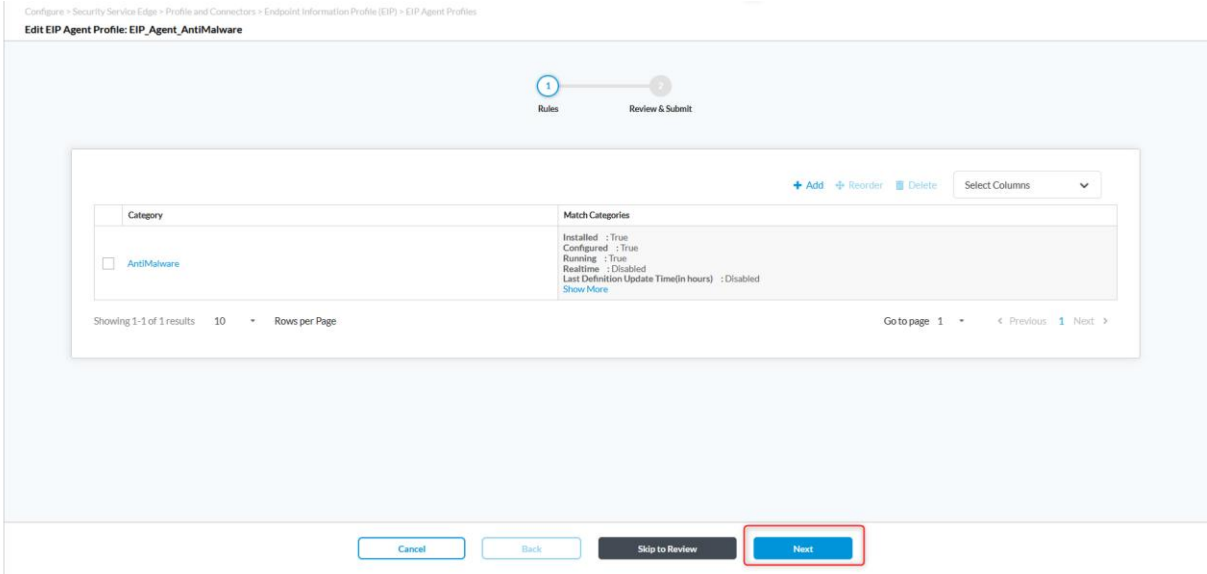
Major: ● Disabled ○ True ○ False

Minor: ● Disabled ○ True ○ False

Service: ● Disabled ○ True ○ False

Patch: ● Disabled ○ True ○ False

Click on “next” to enter a descriptive Profile Name (Example., **EIP_Agent_AntiMalware**).

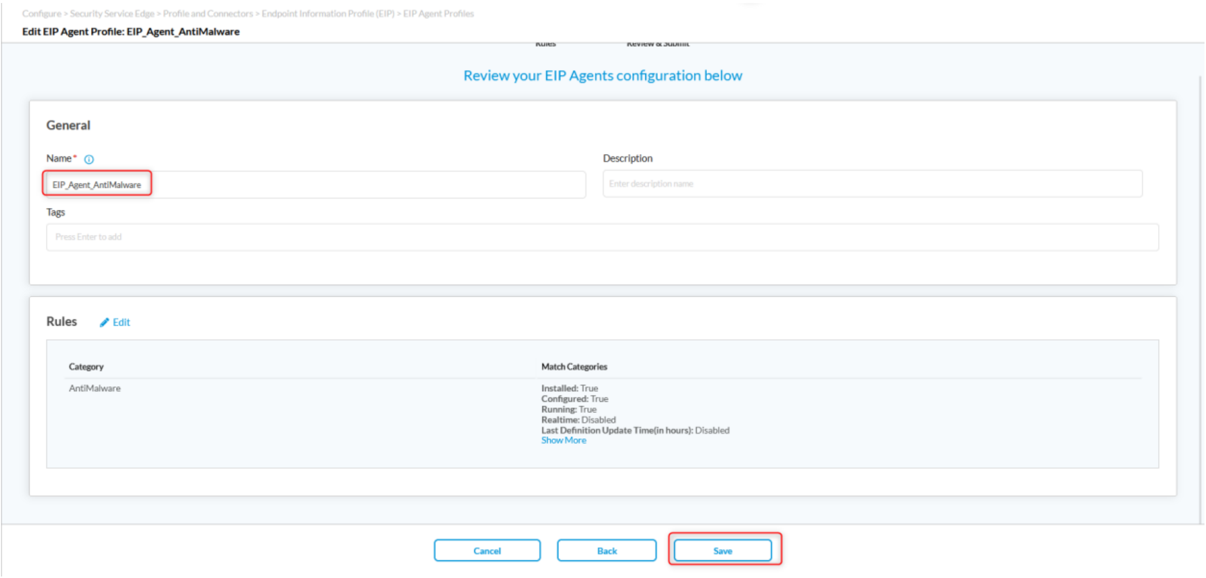


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Edit EIP Agent Profile: EIP_Agent_AntiMalware

	Category	Match Categories
□	AntiMalware	Installed : True Configured : True Running : True Realtime : Disabled Last Definition Update Time(in hours) : Disabled Show More

Showing 1-1 of 1 results 10 Rows per Page



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Edit EIP Agent Profile: EIP_Agent_AntiMalware

Review your EIP Agents configuration below

General

Name*: EIP_Agent_AntiMalware

Description: Enter description name

Tags: Press Enter to add

Rules

Category	Match Categories
AntiMalware	**Installed:** True **Configured:** True **Running:** True **Realtime:** Disabled **Last Definition Update Time(in hours):** Disabled Show More

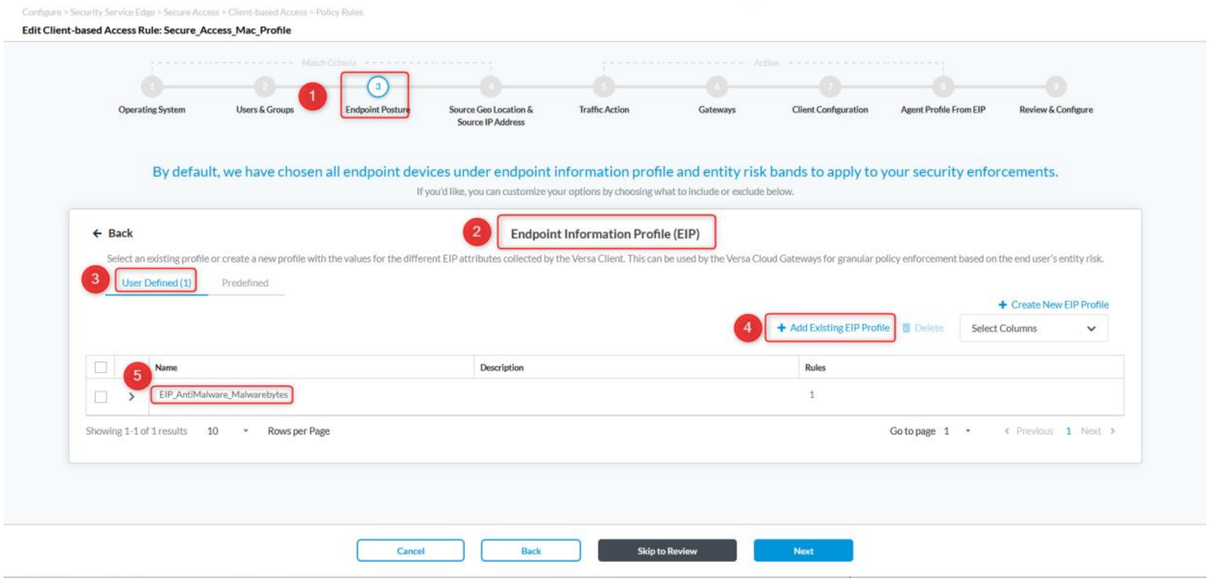
Step 5: Configure Secure Client Access Rule

Navigate to:

Configure > Security Service Edge > Secure Access > Client-based Access > Rules.

Click “**+ Add**” to create a new Secure Access Client rule or edit an existing rule.

In the Match Criteria configuration, go to the ***Endpoint Posture*** section. Under the *Endpoint Information Profile (EIP)* panel, select the desired profile by navigating to the ***User Defined*** tab and clicking on *Add Existing EIP Profile*. Then, choose the EIP profile you previously created. Example EIP_AntiMalware_Malwarebytes).



Edit Client-based Access Rule: Secure_Access_Mac_Profile

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

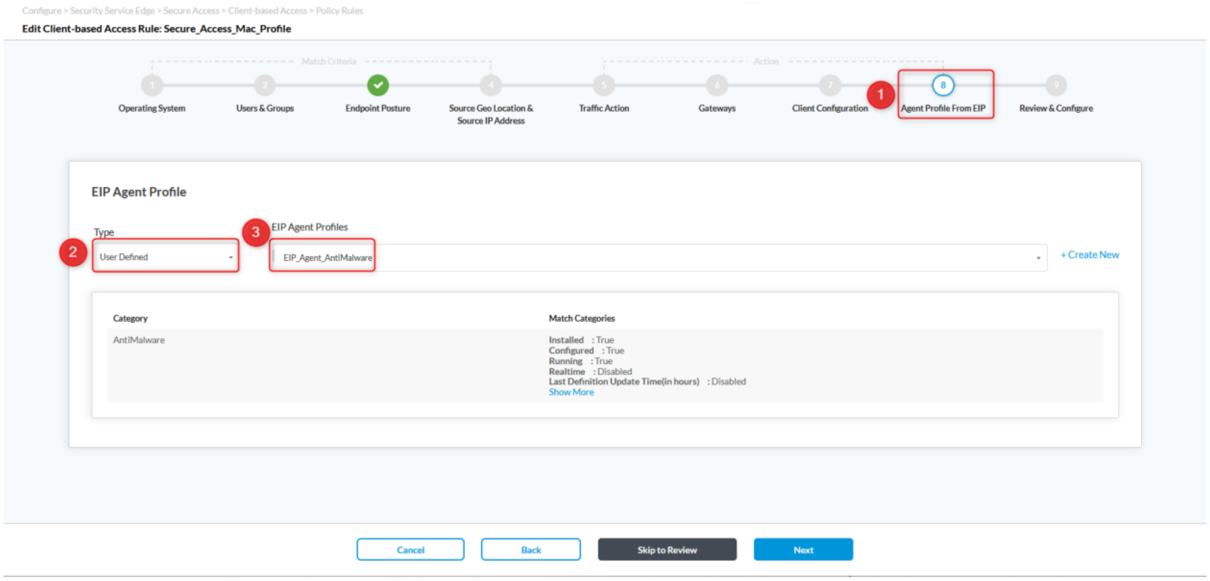
If you'd like, you can customize your options by choosing what to include or exclude below.

Endpoint Information Profile (EIP)

Select an existing profile or create a new profile with the values for the different EIP attributes collected by the Versa Client. This can be used by the Versa Cloud Gateways for granular policy enforcement based on the end user's entity risk.

Name	Description	Rules
EIP_AntiMalware_Malwarebytes		1

In action configuration, under the **Agent Profile From EIP** section, set the Type to **User Defined** and select the **EIP Agent Profile** you previously created. Example EIP_AntiMalware. *The Match Categories panel will display the defined validation criteria, such as registry paths or process checks, ensuring that the selected EIP Agent Profile is applied for endpoint posture verification*.



Edit Client-based Access Rule: Secure_Access_Mac_Profile

EIP Agent Profile

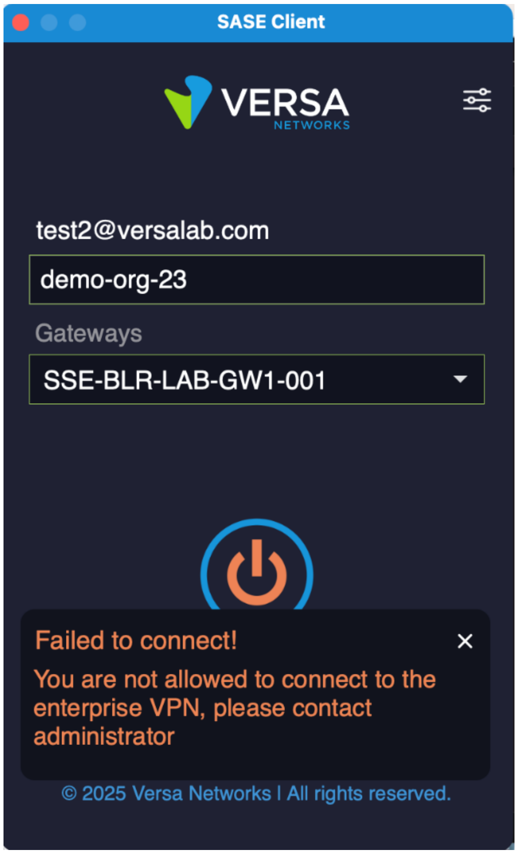
Type: User Defined

EIP Agent Profiles: EIP_Agent_AntiMalware

Category	Match Categories
AntiMalware	Installed : True Configured : True Running : True Realtime : Disabled Last Definition Update Time(in hours) : Disabled

Verification

At this time, the macOS device does not have **Malwarebytes** installed. When the Versa SASE Client attempts to connect, the authentication fails due to the EIP policy that requires an approved antimalware product.



SASE Client

test2@versalab.com

demo-org-23

Gateways

SSE-BLR-LAB-GW1-001

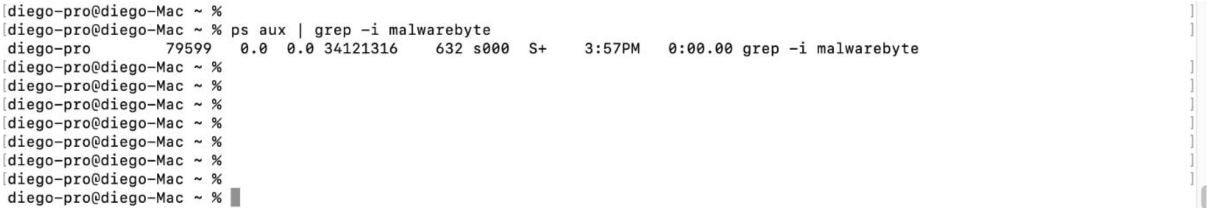
Failed to connect!

You are not allowed to connect to the enterprise VPN, please contact administrator

© 2025 Versa Networks | All rights reserved.

To confirm the posture on the endpoint, you would check whether Malwarebytes is installed or running by executing the following command in Terminal:

ps aux | grep -i Malwarebytes



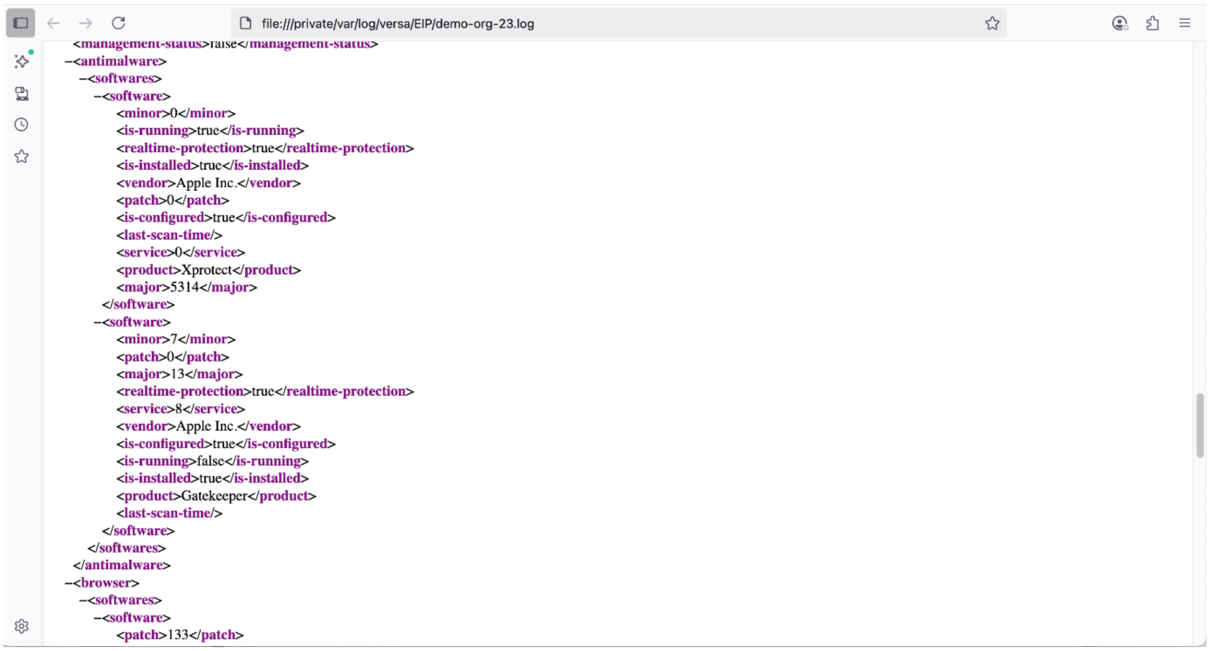
```
[diego-pro@diego-Mac ~ %
[diego-pro@diego-Mac ~ % ps aux | grep -i malwarebyte
 diego-pro        79599   0.0  0.0 34121316    632 s000  S+    3:57PM   0:00.00 grep -i malwarebyte
[diego-pro@diego-Mac ~ %
[diego-pro@diego-Mac ~ %
[diego-pro@diego-Mac ~ %
[diego-pro@diego-Mac ~ %
[diego-pro@diego-Mac ~ %
[diego-pro@diego-Mac ~ %
[diego-pro@diego-Mac ~ %
 diego-pro@diego-Mac ~ %
```

The command output shows no active Malwarebytes process, which validates that the software is not present before installation.

In addition, reviewing the EIP posture log collected from the device confirms that only the native Apple security components are detected:

- **Vendor:** Apple Inc.
- **Product:** XProtect – version 5314
- **Product:** Gatekeeper – version 13.7.8

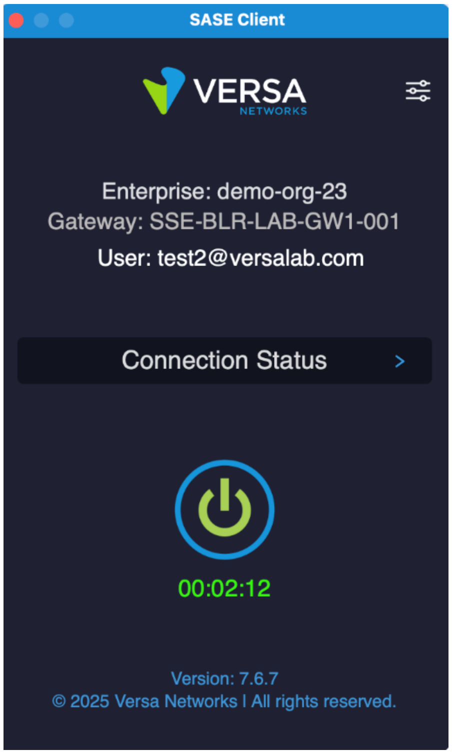
This baseline confirms that the macOS endpoint currently relies only on built-in protections (XProtect and Gatekeeper) and does not yet meet the policy requirement for Malwarebytes



file:///private/var/log/versa/EIP/demo-org-23.log

```
    <management-status>false</management-status>
  –<antimalware>
    –<softwares>
      –<software>
          <minor>0</minor>
          <is-running>true</is-running>
          <realtime-protection>true</realtime-protection>
          <is-installed>true</is-installed>
          <vendor>Apple Inc.</vendor>
          <patch>0</patch>
          <is-configured>true</is-configured>
          <last-scan-time/>
          <service>0</service>
          <product>Xprotect</product>
          <major>5314</major>
        </software>
      –<software>
          <minor>7</minor>
          <patch>0</patch>
          <major>13</major>
          <realtime-protection>true</realtime-protection>
          <service>8</service>
          <vendor>Apple Inc.</vendor>
          <is-configured>true</is-configured>
          <is-running>false</is-running>
          <is-installed>true</is-installed>
          <product>Gatekeeper</product>
          <last-scan-time/>
        </software>
      </softwares>
    </antimalware>
  –<browser>
    –<softwares>
      –<software>
          <patch>133</patch>
```

After installing **Malwarebytes**, the Versa SASE Client is now able to authenticate successfully and establish a secure connection to the enterprise VPN.



SASE Client

Enterprise: demo-org-23
Gateway: SSE-BLR-LAB-GW1-001
User: test2@versalab.com

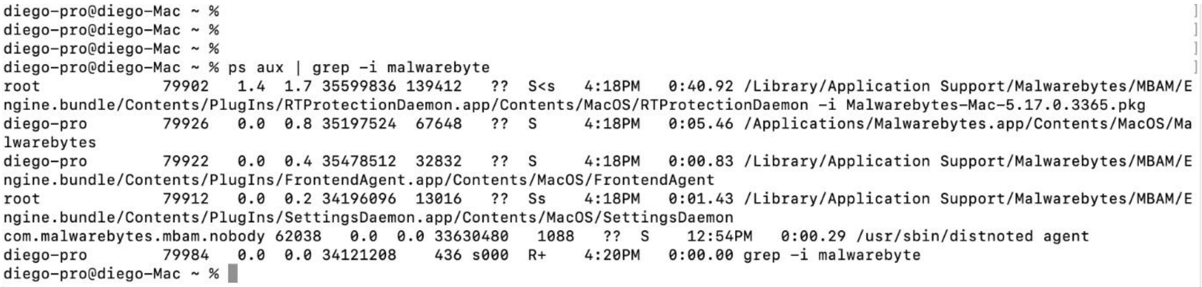
Connection Status >

00:02:12

Version: 7.6.7
© 2025 Versa Networks I All rights reserved.

To confirm the posture on the endpoint, you would check again whether Malwarebytes is installed and running by executing the following command in Terminal:

ps aux | grep -i Malwarebytes

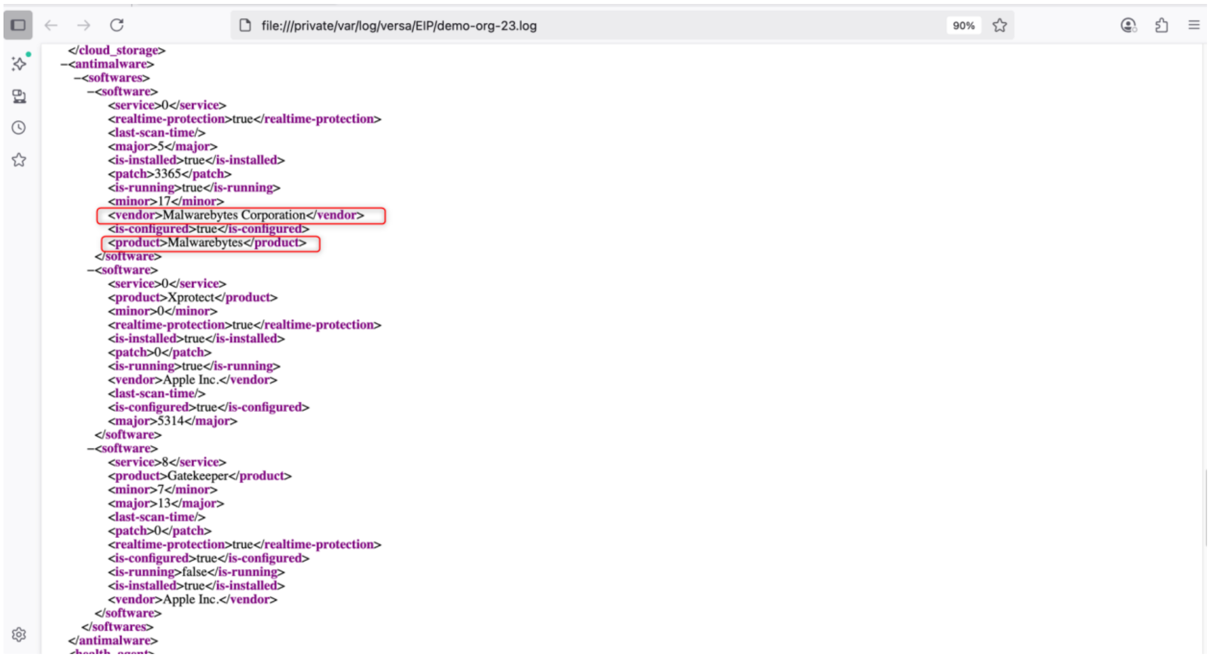


```
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ % ps aux | grep -i malwarebyte
root             79902   1.4  1.7 35599836 139412   ??  S<s   4:18PM   0:40.92 /Library/Application Support/Malwarebytes/MBAM/E
ngine.bundle/Contents/PlugIns/RTProtectionDaemon.app/Contents/MacOS/RTProtectionDaemon -i Malwarebytes-Mac-5.17.0.3365.pkg
diego-pro        79926   0.0  0.8 35197524  67648   ??  S     4:18PM   0:05.46 /Applications/Malwarebytes.app/Contents/MacOS/Ma
lwarebytes
diego-pro        79922   0.0  0.4 35478512  32832   ??  S     4:18PM   0:00.83 /Library/Application Support/Malwarebytes/MBAM/E
ngine.bundle/Contents/PlugIns/FrontendAgent.app/Contents/MacOS/FrontendAgent
root             79912   0.0  0.2 34196096  13016   ??  Ss    4:18PM   0:01.43 /Library/Application Support/Malwarebytes/MBAM/E
ngine.bundle/Contents/PlugIns/SettingsDaemon.app/Contents/MacOS/SettingsDaemon
com.malwarebytes.mbam.nobody 62038   0.0  0.0 33630480   1088   ??  S    12:54PM   0:00.29 /usr/sbin/distnoted agent
diego-pro        79984   0.0  0.0 34121208    436 s000  R+    4:20PM   0:00.00 grep -i malwarebyte
diego-pro@diego-Mac ~ %
```

the command output shows multiple active processes related to Malwarebytes, including the **RTProtectionDaemon**, **FrontendAgent**, and **SettingsDaemon**, which indicates that the antimalware agent is installed and running properly.

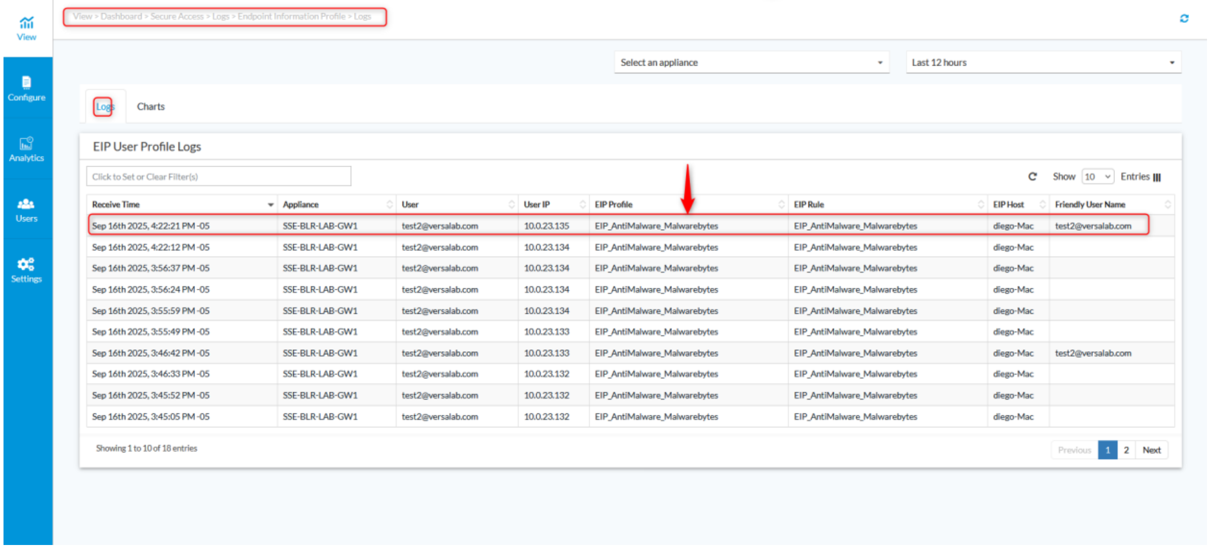
Reviewing the updated EIP posture log confirms detection of Malwarebytes alongside the native Apple protections:

- **Vendor:** Malwarebytes Corporation
- **Product:** Malwarebytes – version 5.17.0.3365
- **Vendor:** Apple Inc.
- **Product:** XProtect – version 5314
- **Product:** Gatekeeper – version 13.7.8



```
  </cloud_storage>
 −<antimalware>
   −<softwares>
     −<software>
        <service>0</service>
        <realtime-protection>true</realtime-protection>
        <last-scan-time/>
        <major>5</major>
        <is-installed>true</is-installed>
        <patch>3365</patch>
        <is-running>true</is-running>
        <minor>17</minor>
        <vendor>Malwarebytes Corporation</vendor>
        <is-configured>true</is-configured>
        <product>Malwarebytes</product>
      </software>
     −<software>
        <service>0</service>
        <product>Xprotect</product>
        <minor>0</minor>
        <realtime-protection>true</realtime-protection>
        <is-installed>true</is-installed>
        <patch>0</patch>
        <is-running>true</is-running>
        <vendor>Apple Inc.</vendor>
        <last-scan-time/>
        <is-configured>true</is-configured>
        <major>5314</major>
      </software>
     −<software>
        <service>8</service>
        <product>Gatekeeper</product>
        <minor>7</minor>
        <major>13</major>
        <last-scan-time/>
        <patch>0</patch>
        <realtime-protection>true</realtime-protection>
        <is-configured>true</is-configured>
        <is-running>false</is-running>
        <is-installed>true</is-installed>
        <vendor>Apple Inc.</vendor>
      </software>
    </softwares>
  </antimalware>
  <health_agent>
```

You check the Concerto logs to validate that the EIP authentication profile matches the expected profile. In Concerto From the log view (**View > Dashboard > Secure Access > Logs > Endpoint Information Profile > Logs**).



View > Dashboard > Secure Access > Logs > Endpoint Information Profile > Logs
View
Configure
Analytics
Users
Settings
Select an appliance
Last 12 hours
Logs
Charts
Click to Set or Clear Filter(s)
Show 10 Entries
Previous
1
2
Next

EIP User Profile Logs

Receive Time	Appliance	User	User IP	EIP Profile	EIP Rule	EIP Host	Friendly User Name
Sep 16th 2025, 4:22:21 PM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.135	EIP_AntiMalware_Malwarebytes	EIP_AntiMalware_Malwarebytes	diego-Mac	test2@versalab.com
Sep 16th 2025, 4:22:12 PM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.134	EIP_AntiMalware_Malwarebytes	EIP_AntiMalware_Malwarebytes	diego-Mac	
Sep 16th 2025, 3:56:37 PM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.134	EIP_AntiMalware_Malwarebytes	EIP_AntiMalware_Malwarebytes	diego-Mac	
Sep 16th 2025, 3:56:24 PM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.134	EIP_AntiMalware_Malwarebytes	EIP_AntiMalware_Malwarebytes	diego-Mac	
Sep 16th 2025, 3:55:59 PM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.134	EIP_AntiMalware_Malwarebytes	EIP_AntiMalware_Malwarebytes	diego-Mac	
Sep 16th 2025, 3:55:49 PM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.133	EIP_AntiMalware_Malwarebytes	EIP_AntiMalware_Malwarebytes	diego-Mac	
Sep 16th 2025, 3:46:42 PM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.133	EIP_AntiMalware_Malwarebytes	EIP_AntiMalware_Malwarebytes	diego-Mac	test2@versalab.com
Sep 16th 2025, 3:46:33 PM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.132	EIP_AntiMalware_Malwarebytes	EIP_AntiMalware_Malwarebytes	diego-Mac	
Sep 16th 2025, 3:45:52 PM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.132	EIP_AntiMalware_Malwarebytes	EIP_AntiMalware_Malwarebytes	diego-Mac	
Sep 16th 2025, 3:45:05 PM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.132	EIP_AntiMalware_Malwarebytes	EIP_AntiMalware_Malwarebytes	diego-Mac	

Showing 1 to 10 of 18 entries

Entry show that the endpoint matches the **EIP_AntiMalware_Malwarebytes** profile and rule after Malwarebytes is installed. The appliance, user, and host details confirm that the macOS device, associated with user, is evaluated against the correct profile. This confirms that the endpoint is recognized as compliant, the EIP profile and rule are enforced, and secure access is granted according to the posture policy.

Hostname

Hostname validation within an Endpoint Identity Profile (EIP) provides a way to identify endpoints based on their configured system name. This method can help enforce organizational naming standards and provide an additional layer of compliance control.

For macOS devices, administrators can configure or verify hostnames directly from the terminal:

- To set the hostname:

```
sudo scutil --set HostName "your-new-name.domain.com"
```

- To check the hostname:

```
scutil --get HostName
```

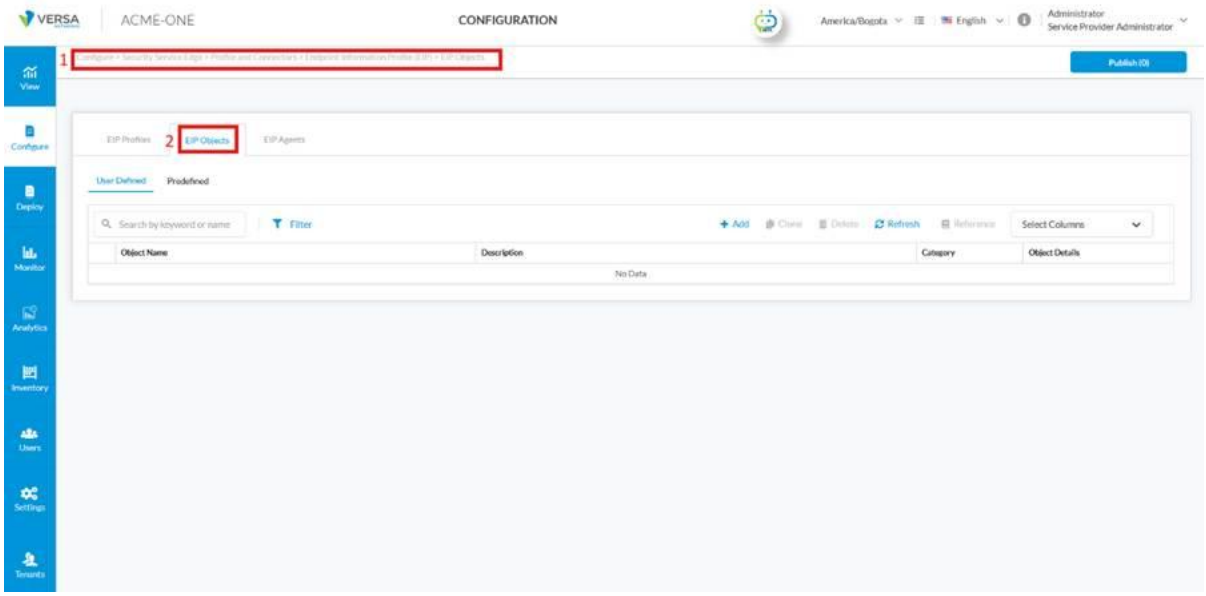
Scenario: An organization requires all corporate laptops to follow a naming convention, such as hostname.department.corp.local. In the EIP Profile, the administrator defines an allowed list of hostnames. When a device connects:

- If the hostname matches an entry in the allowed list, the device is considered compliant.
- If the hostname does not match, the device is flagged as non-compliant and may be restricted from accessing corporate resources.

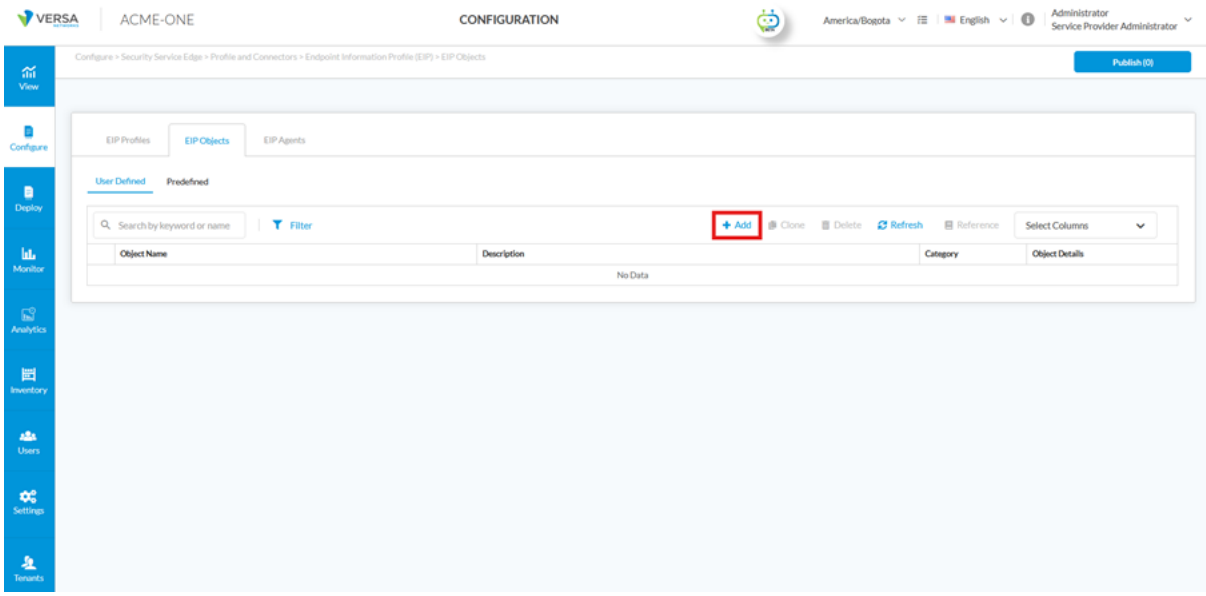
This ensures that only systems configured with the approved naming scheme can access protected applications.

Step 1: Create an EIP Object with hostname

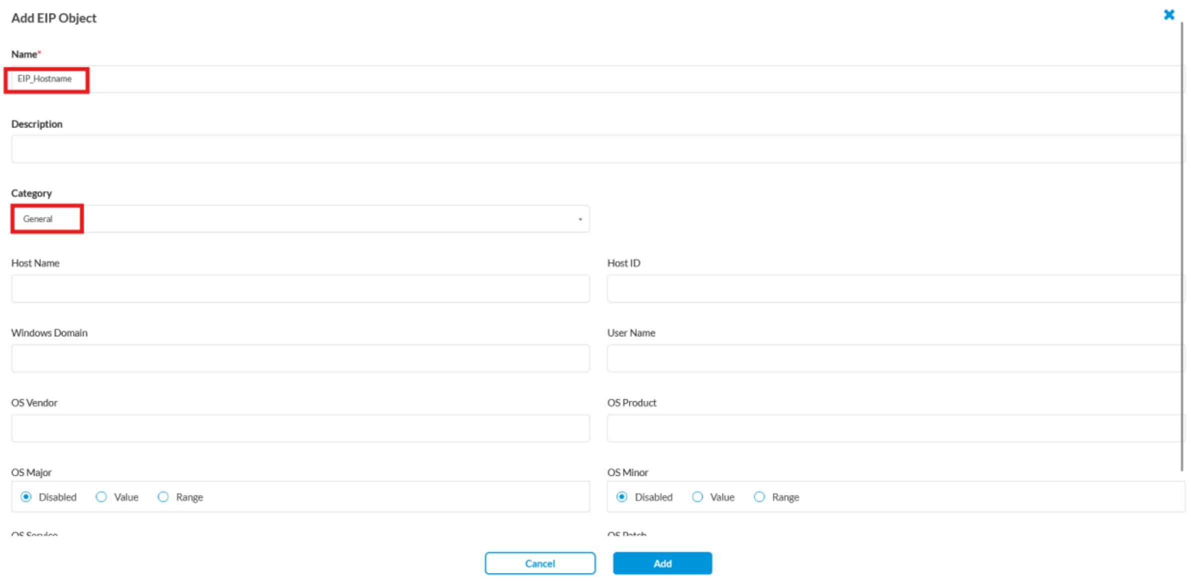
Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Objects



Click on “+ Add” to create a new EIP Object.



Enter a descriptive name for your EIP object. ***Example:*** **EIP_Hostname.** And Select general from the dropdown.



Add EIP Object

Name*
EIP_Hostname

Description

Category
General

Host Name

Host ID

Windows Domain

User Name

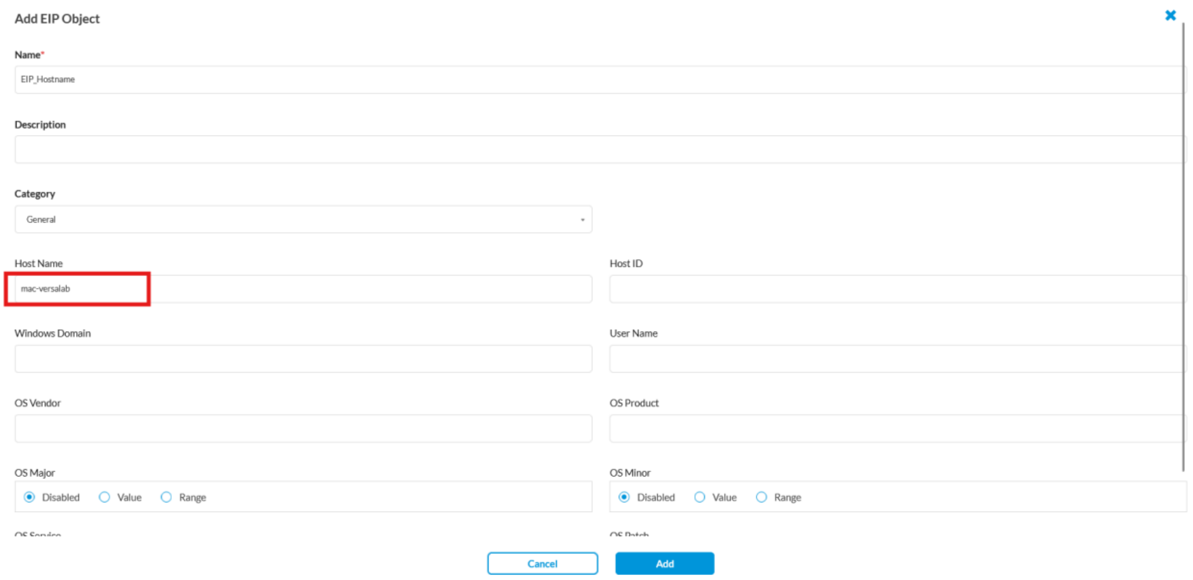
OS Vendor

OS Product

OS Major
● Disabled ○ Value ○ Range

OS Minor
● Disabled ○ Value ○ Range

Go to Hostname and Enter the **hostname** to check ***Example:*** mac-versalab



Add EIP Object

Name*
EIP_Hostname

Description

Category
General

Host Name
mac-versalab

Host ID

Windows Domain

User Name

OS Vendor

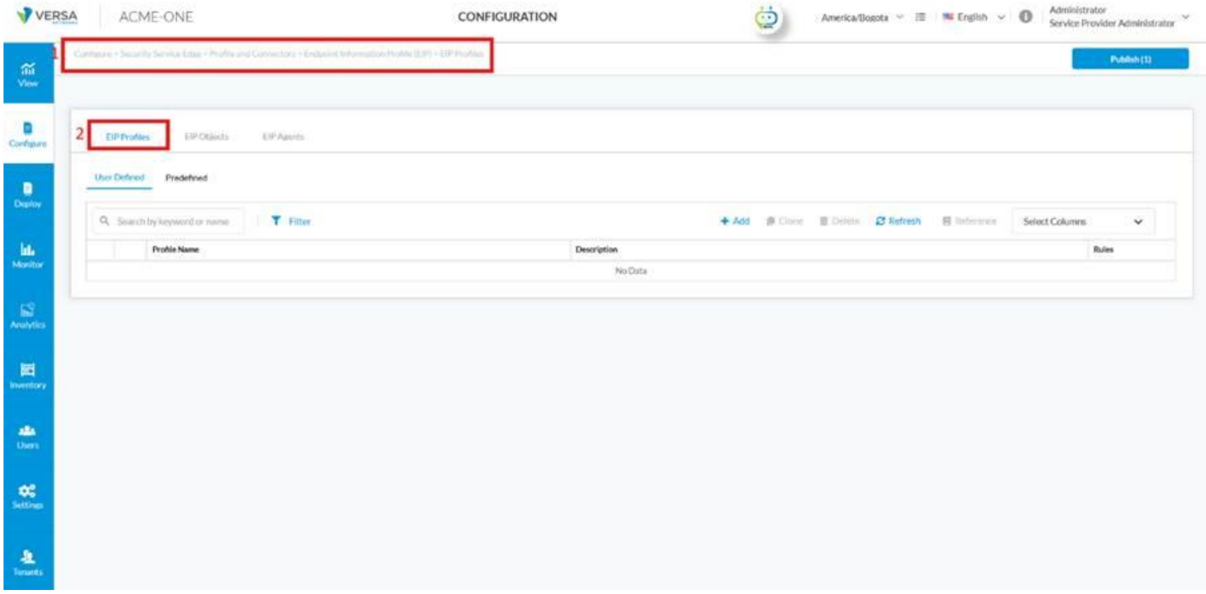
OS Product

OS Major
● Disabled ○ Value ○ Range

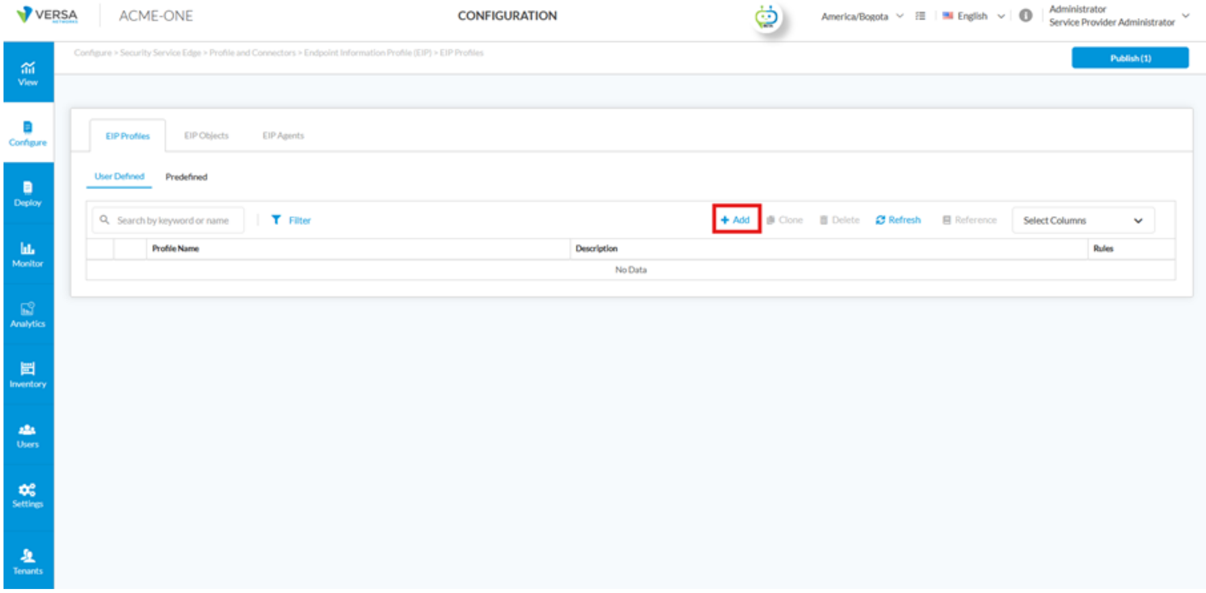
OS Minor
● Disabled ○ Value ○ Range

Step 2: Create an EIP Profile Using Host ID

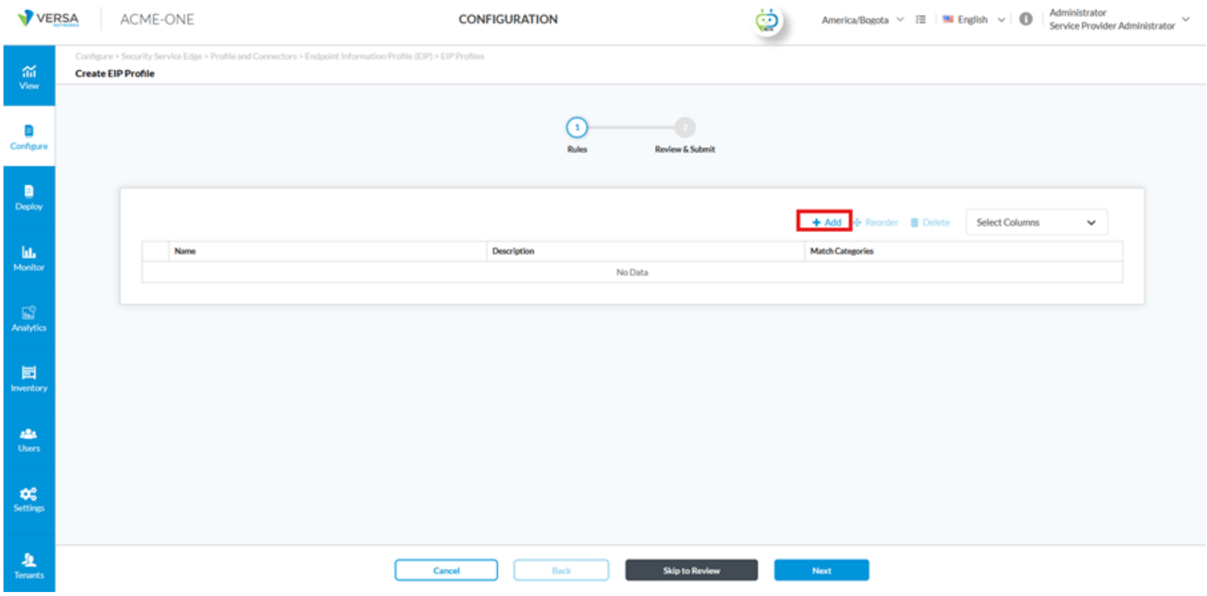
Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Profiles



Click on “+ Add” to start creating a new profile.



In the **Create EIP Profile** window, Click on “+ Add” to define a new rule.



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Create EIP Profile

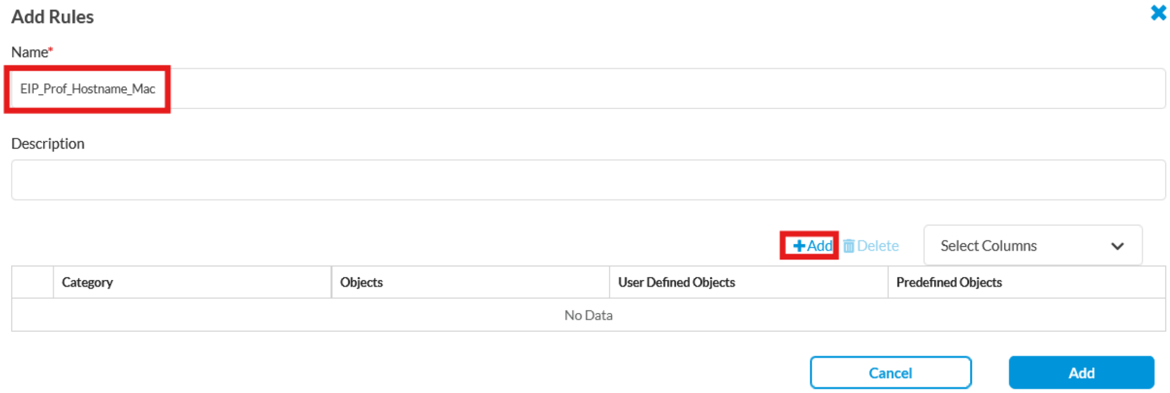
	Name	Description	Match Categories
No Data			

Create a General Rule for hostname

Enter a Name for your rule, Example, EIP_Prof_Hostname_Mac.

You would (Optional) Add a description for clarity.

Click "+ Add" to attach an EIP Object.



Name*

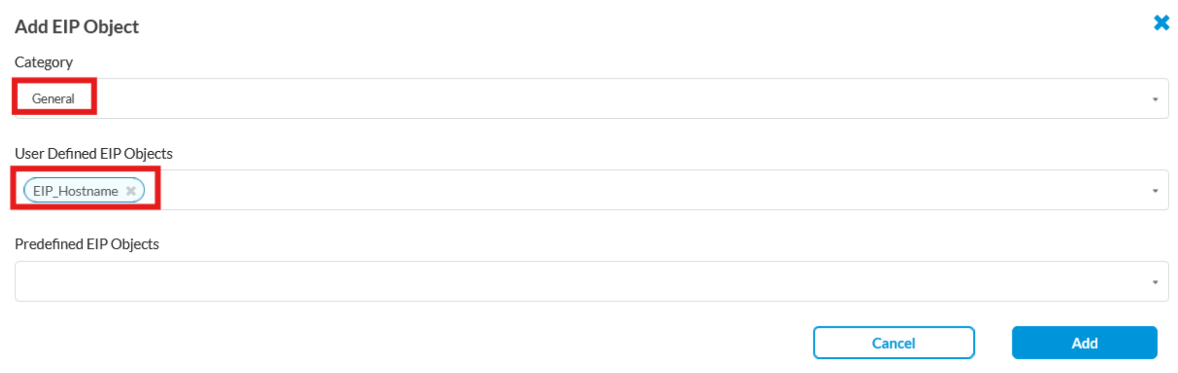
EIP_Prof_Hostname_Mac

Description

	Category	Objects	User Defined Objects	Predefined Objects
No Data				

In Add EIP Object dialog, choose the Category. Example **general**.

Select an existing EIP Object or create a new one. For example, an object was created to verify if MacOs Hostname in the previous section.



Add EIP Object

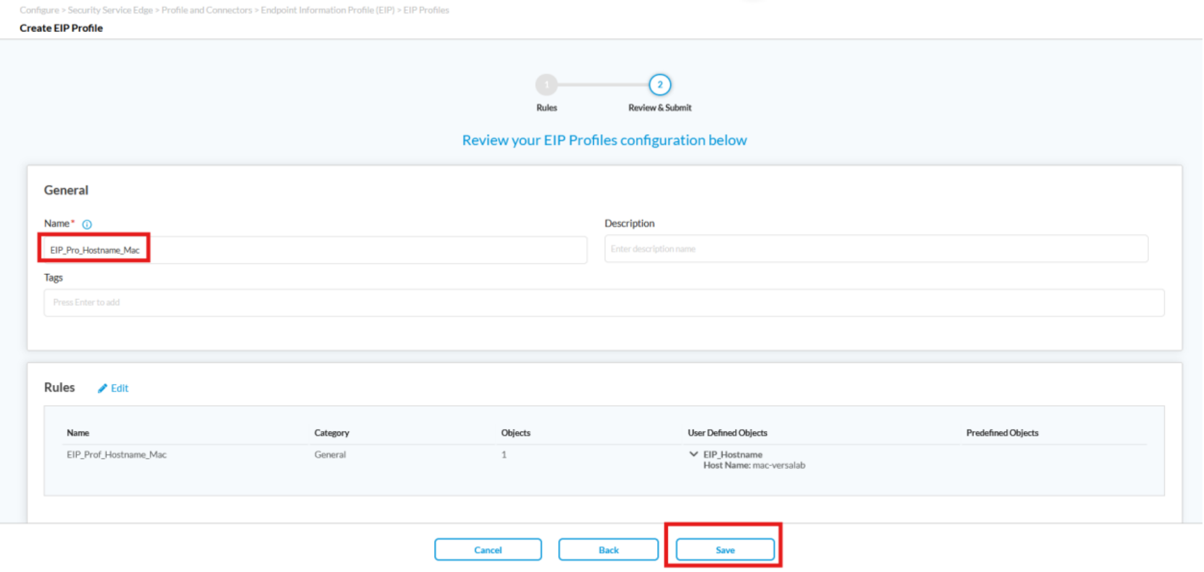
Category: General

User Defined EIP Objects: EIP_Hostname

Predefined EIP Objects

Click **Next** and then Enter a descriptive name for your EIP object. ***Example:*** EIP_Hostname**.**

Review and **Save** the Profile creation



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Create EIP Profile

Review your EIP Profiles configuration below

General

Name*: EIP_Pro_Hostname_Mac

Description: Enter description name

Tags: Press Enter to add

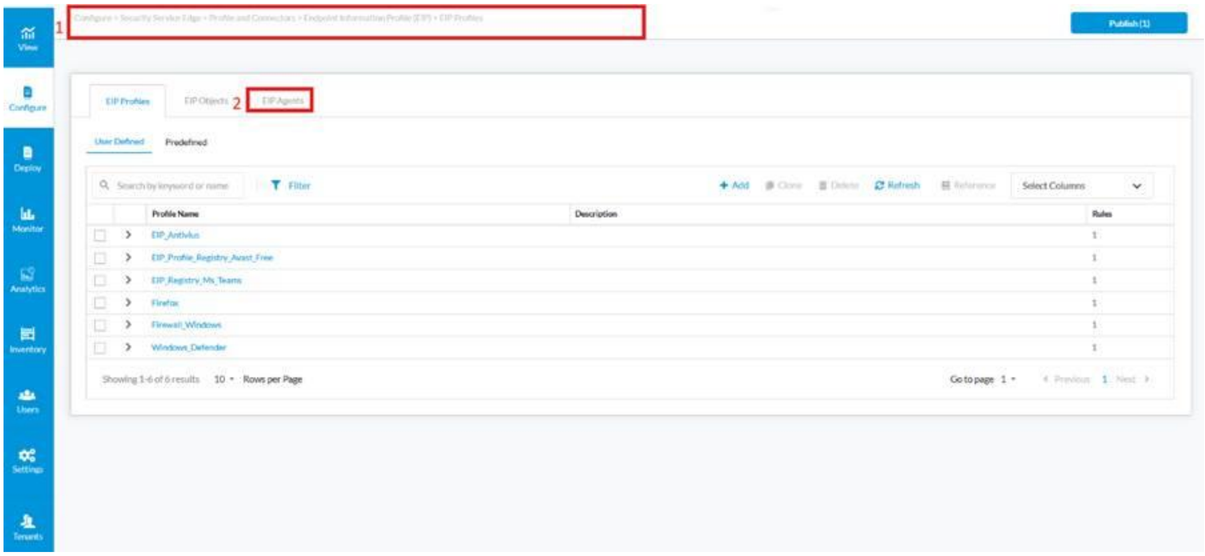
Rules

Name	Category	Objects	User Defined Objects	Predefined Objects
EIP_Prof_Hostname_Mac	General	1	EIP_Hostname Host Name: mac-versalab	

Note: After creating the EIP Object and configuring the EIP Profile and Agent Profile, you must apply them to the Secure Access Client policy to enforce device posture validation and continue evaluation.

Step 3: Navigate to the EIP Agent Section

Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Agents



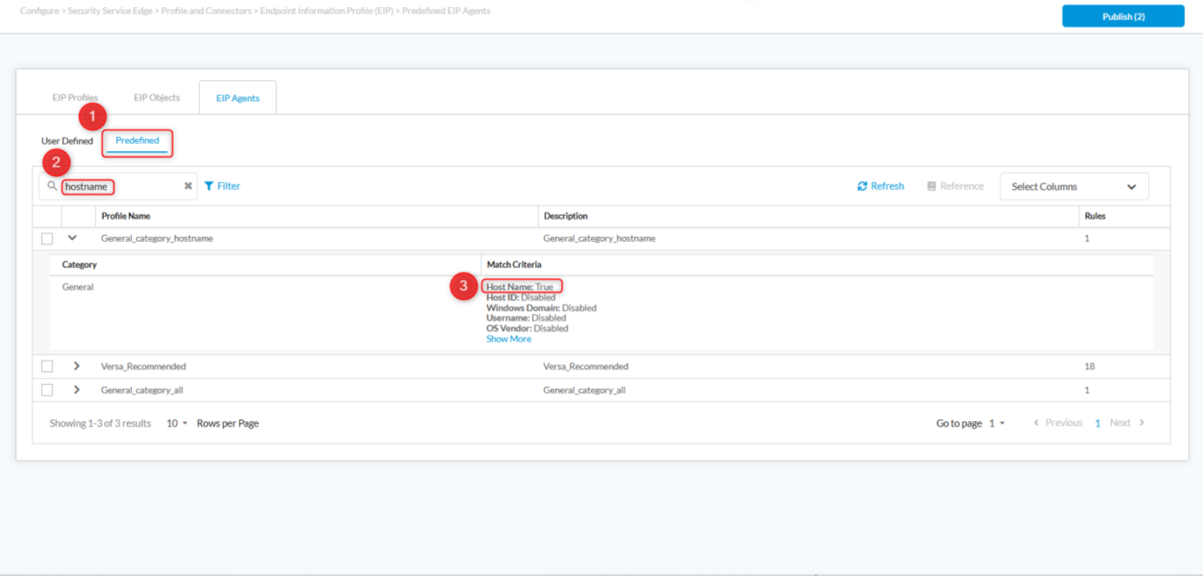
1 Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Profile Name	Description	Rules
EIP_Antivius		1
EIP_Profile_Registry_Avast_Free		1
EIP_Registry_Ms_Teams		1
Firefox		1
Firewall_Windows		1
Windows_Defender		1

Showing 1-6 of 6 results 10 Rows per Page Go to page 1 Previous 1 Next

Step 4: Create an EIP Agent Profile

Important Note: Instead of creating a new agent manually, you can also use a predefined Versa Hostname agent. In the Predefined tab, search for domain and select General_category_hostname, which already includes the rule hostname: True.



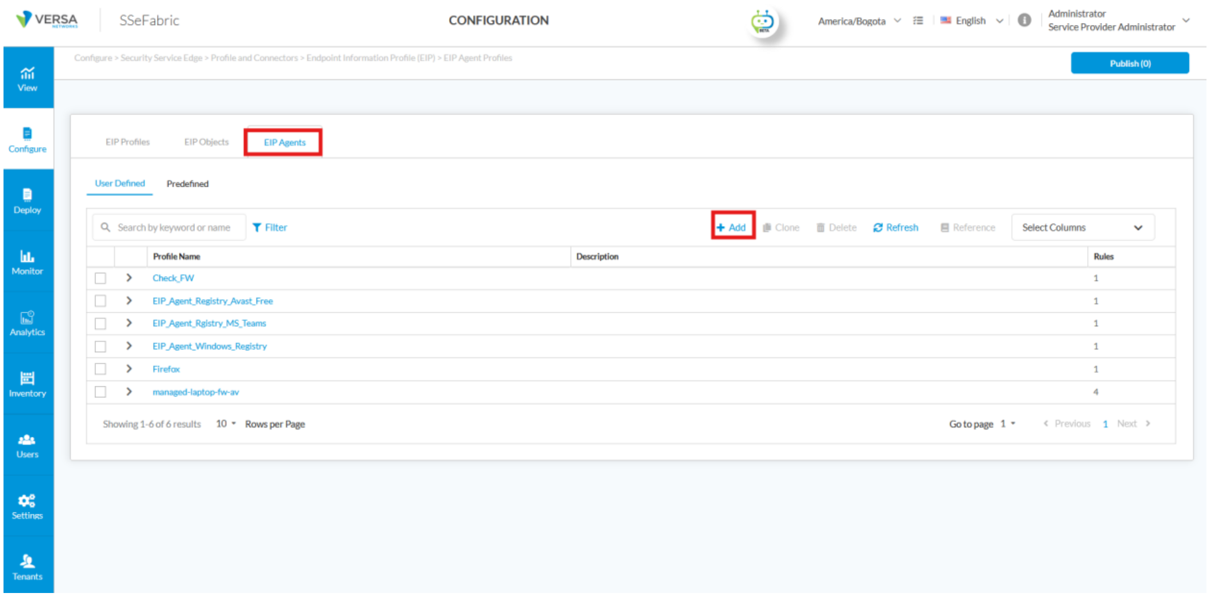
Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > Predefined EIP Agents

Profile Name	Description	Rules
General_category_hostname	General_category_hostname	1
Versa_Recommended	Versa_Recommended	18
General_category_all	General_category_all	1

Category	Match Criteria
General	**Host Name:** True **Host ID:** Disabled **Windows Domain:** Disabled **Username:** Disabled **OS Vendor:** Disabled Show More

Showing 1-3 of 3 results 10 Rows per Page Go to page 1 Previous 1 Next

Click on **Add** to create a **new Agent profile**.

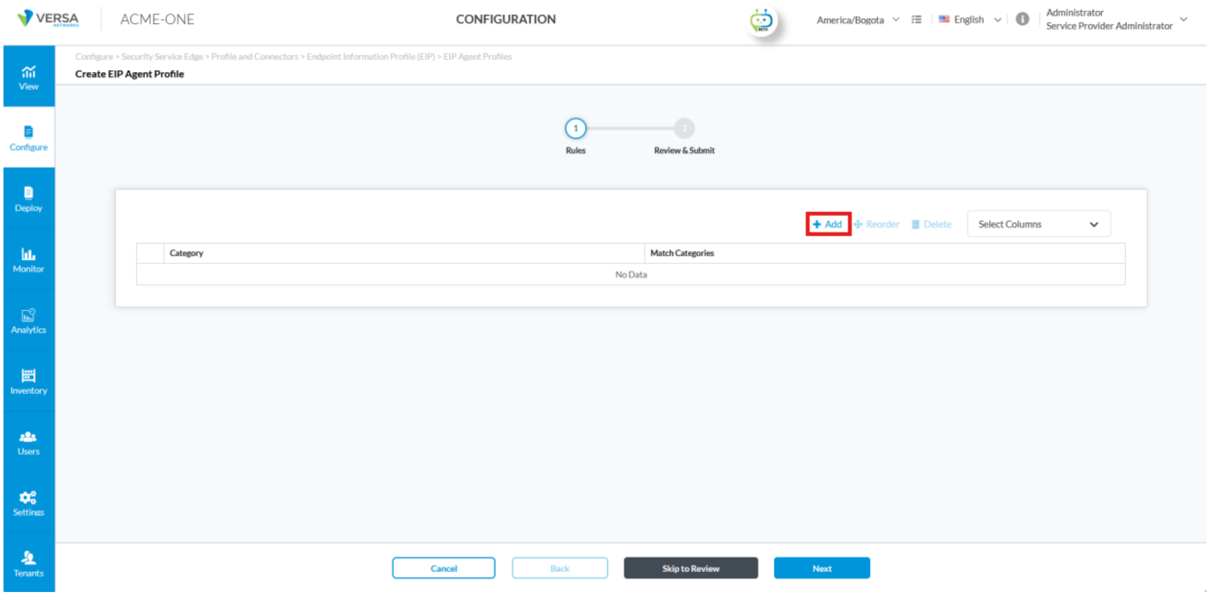


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Profile Name	Description	Rules
Check_FW		1
EIP_Agent_Registry_Avast_Free		1
EIP_Agent_Rglstry_MS_Teams		1
EIP_Agent_Windows_Registry		1
Firefox		1
managed-laptop-fw-av		4

Showing 1-6 of 6 results 10 Rows per Page Go to page 1 Previous 1 Next

Click on "+Add" to create a new rule. Then choose general

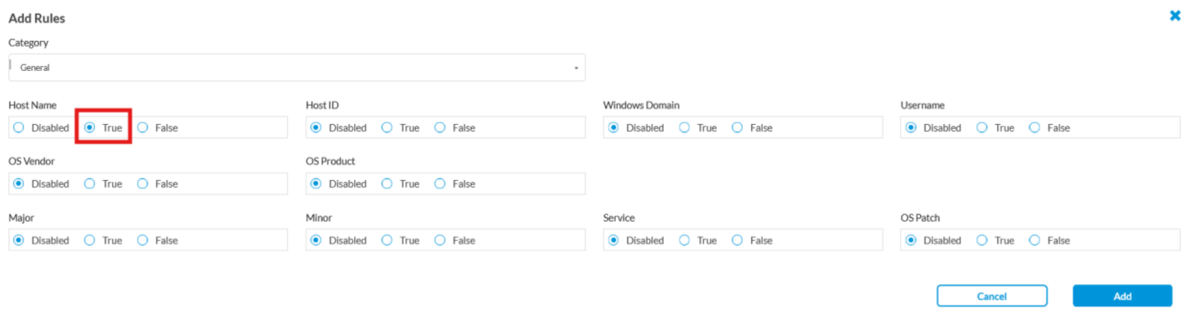


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Create EIP Agent Profile

Category	Match Categories
No Data	

In the **general** section, locate click hostname by default is set to Disable change to true, then Click Add.



Add Rules

Category: General

Host Name: ○ Disabled ● True ○ False

Host ID: ● Disabled ○ True ○ False

Windows Domain: ● Disabled ○ True ○ False

Username: ● Disabled ○ True ○ False

OS Vendor: ● Disabled ○ True ○ False

OS Product: ● Disabled ○ True ○ False

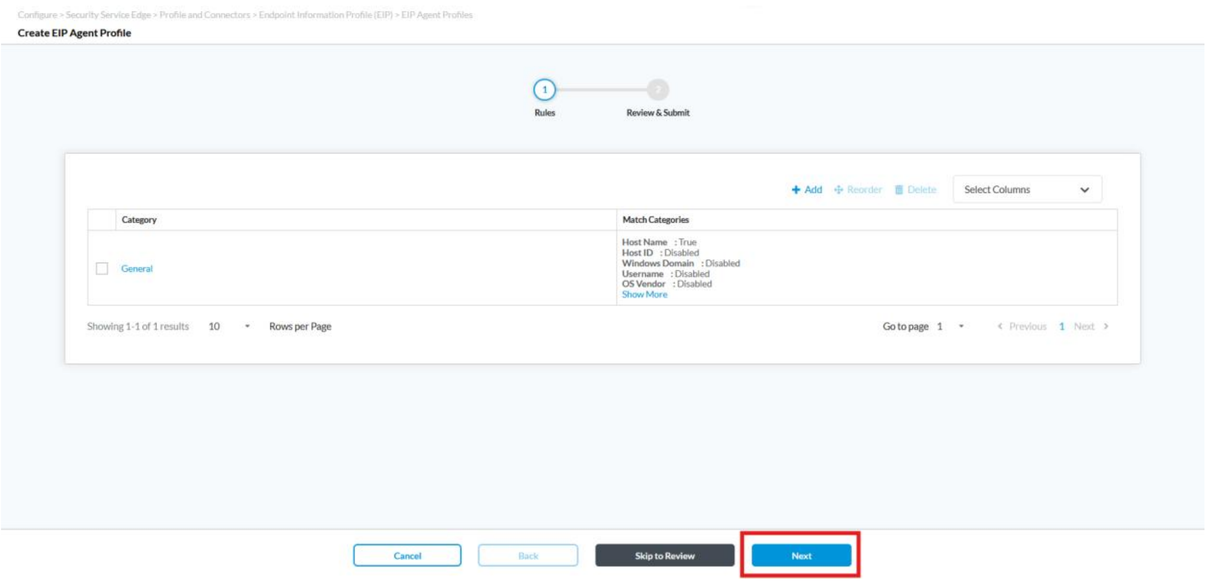
Major: ● Disabled ○ True ○ False

Minor: ● Disabled ○ True ○ False

Service: ● Disabled ○ True ○ False

OS Patch: ● Disabled ○ True ○ False

Click on “next” to enter a descriptive Profile Name (Example., **EIP_Agent_Hostname**).

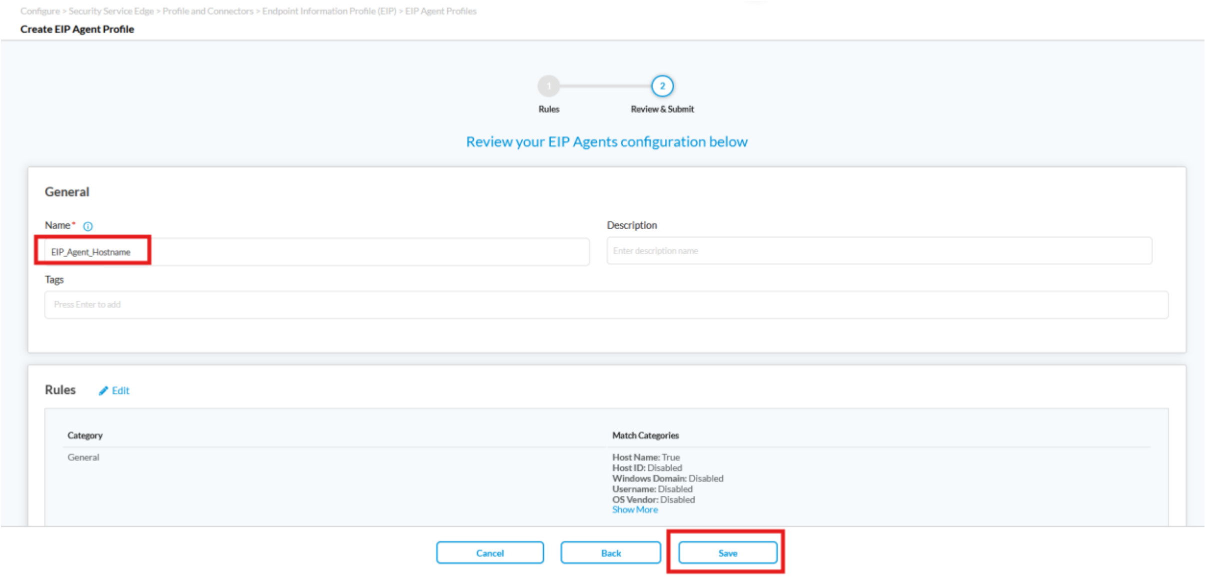


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Create EIP Agent Profile

	Category	Match Categories
□	General	Host Name : True Host ID : Disabled Windows Domain : Disabled Username : Disabled OS Vendor : Disabled Show More

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Create EIP Agent Profile

Review your EIP Agents configuration below

General

Name*: EIP_Agent_Hostname

Description: Enter description name

Tags: Press Enter to add

Rules Edit

Category	Match Categories
General	Host Name: True Host ID: Disabled Windows Domain: Disabled Username: Disabled OS Vendor: Disabled Show More

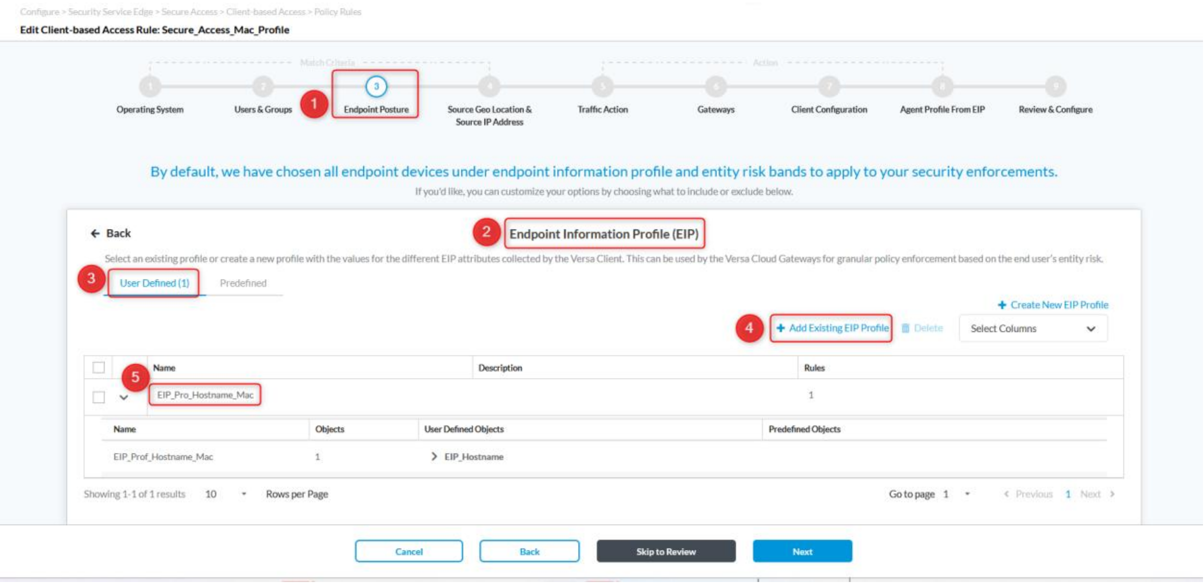
Step 5: Configure Secure Client Access Rule

Navigate to:

Configure > Security Service Edge > Secure Access > Client-based Access > Rules.

Click “**+ Add**” to create a new Secure Access Client rule or edit an existing rule.

In the Match Criteria configuration, go to the ***Endpoint Posture*** section. Under the *Endpoint Information Profile (EIP)* panel, select the desired profile by navigating to the ***User Defined*** tab and clicking on *Add Existing EIP Profile*. Then, choose the EIP profile you previously created. Example EIP_Prof_Hostname_Mac).


Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure_Access_Mac_Profile

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

Endpoint Information Profile (EIP)

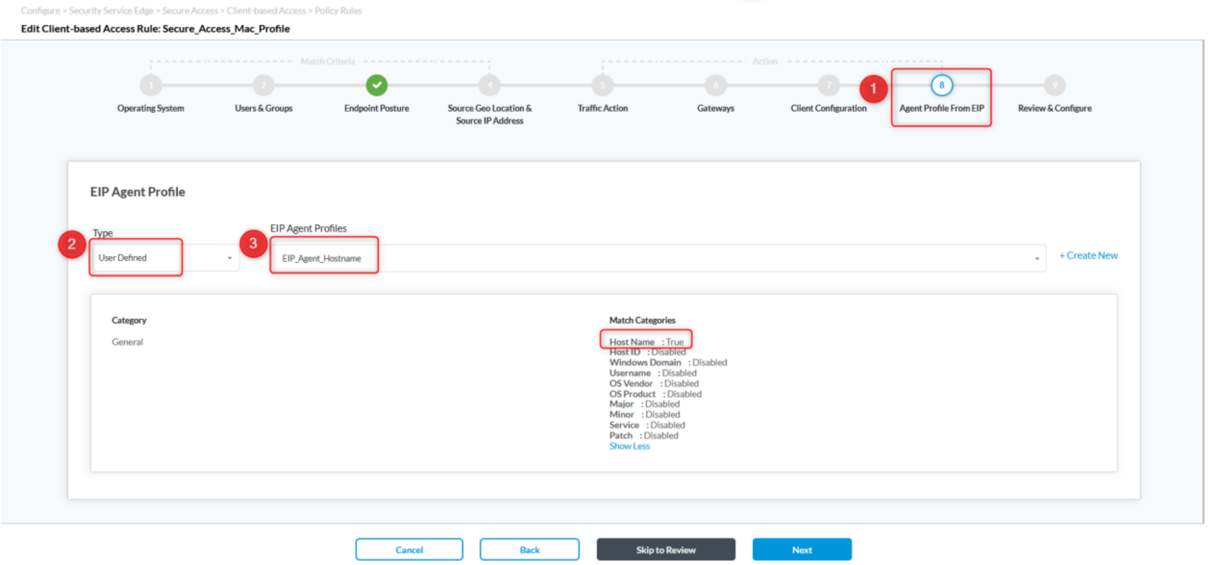
Select an existing profile or create a new profile with the values for the different EIP attributes collected by the Versa Client. This can be used by the Versa Cloud Gateways for granular policy enforcement based on the end user's entity risk.

□	Name	Description	Rules
□	EIP_Pro_Hostname_Mac		1

Name	Objects	User Defined Objects	Predefined Objects
EIP_Prof_Hostname_Mac	1	> EIP_Hostname	

Showing 1-1 of 1 results 10 Rows per Page

In action configuration, under the **Agent Profile From EIP** section, set the Type to **User Defined** and select the **EIP Agent Profile** you previously created. Example EIP_Agent_Host_ID. *The Match Categories panel will display the defined validation criteria, such as registry paths or process checks, ensuring that the selected EIP Agent Profile is applied for endpoint posture verification*.



Edit Client-based Access Rule: Secure_Access_Mac_Profile

EIP Agent Profile

Type: User Defined

EIP Agent Profiles: EIP_Agent_Hostname

Category: General

Match Categories
Host Name : True
Host ID : Disabled
Windows Domain : Disabled
Username : Disabled
OS Vendor : Disabled
OS Product : Disabled
Major : Disabled
Minor : Disabled
Service : Disabled
Patch : Disabled

Disk- Encryption

Disk encryption validation within an EIP verifies that endpoints use full-disk encryption before access is granted, helping protect data at rest on lost or stolen devices.

For macOS devices, administrators can check encryption status either through the EIP posture logs (/private/var/log/versa/EIP/check-encryption.json) or directly from the system:

- To verify FileVault status from the command line:

fdesetup status

- **FileVault is On** > the system drive is encrypted.
- **FileVault is Off** > the system drive is not encrypted.
- **Encryption in progress** > the drive is currently encrypting.
-

Note (macOS): Disk encryption is available natively via **FileVault** (built in by default). You can enable it in **System Settings → Privacy & Security → FileVault** or via CLI (sudo fdesetup enable). If your organization uses a third-party disk-encryption tool, confirm that the EIP posture checks recognize that solution before enforcing compliance.

Scenario: An organization requires all corporate Macs to have disk encryption enabled (As an Example FileVault). In the EIP Profile, the administrator defines compliance rules for disk encryption. When a device connects:

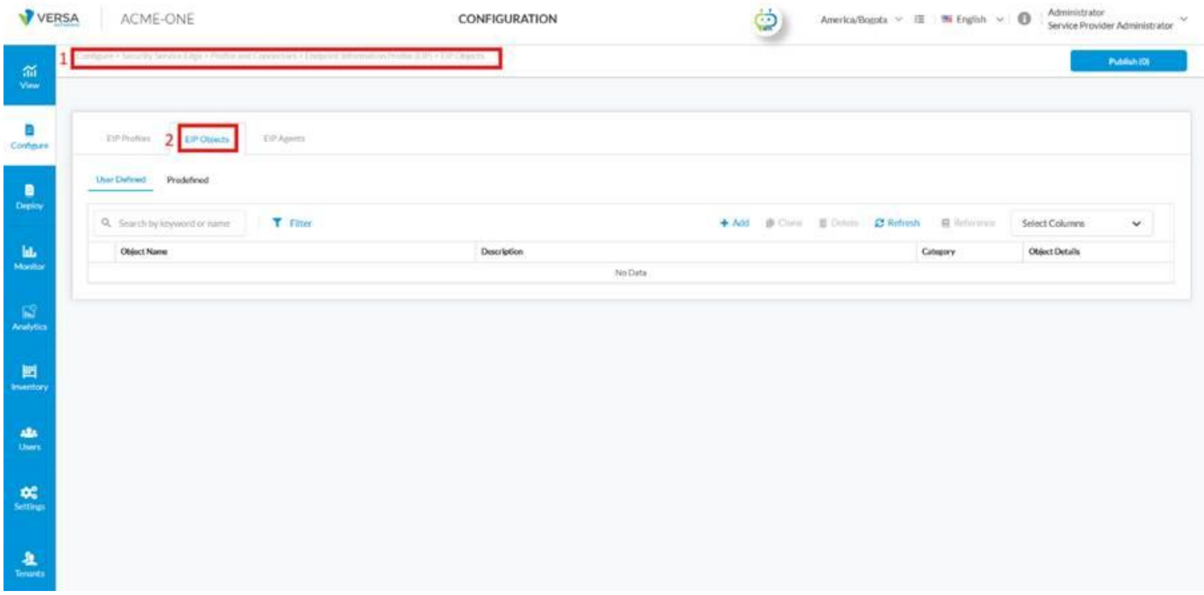
- If disk encryption is **enabled and running**, the device is considered **compliant**.
- If disk encryption is **disabled, enabled but is not detected**, the device is **non-compliant** and

access may be restricted.

- This ensures only endpoints with full-disk encryption can access sensitive corporate applications, reinforcing Zero Trust posture validation.

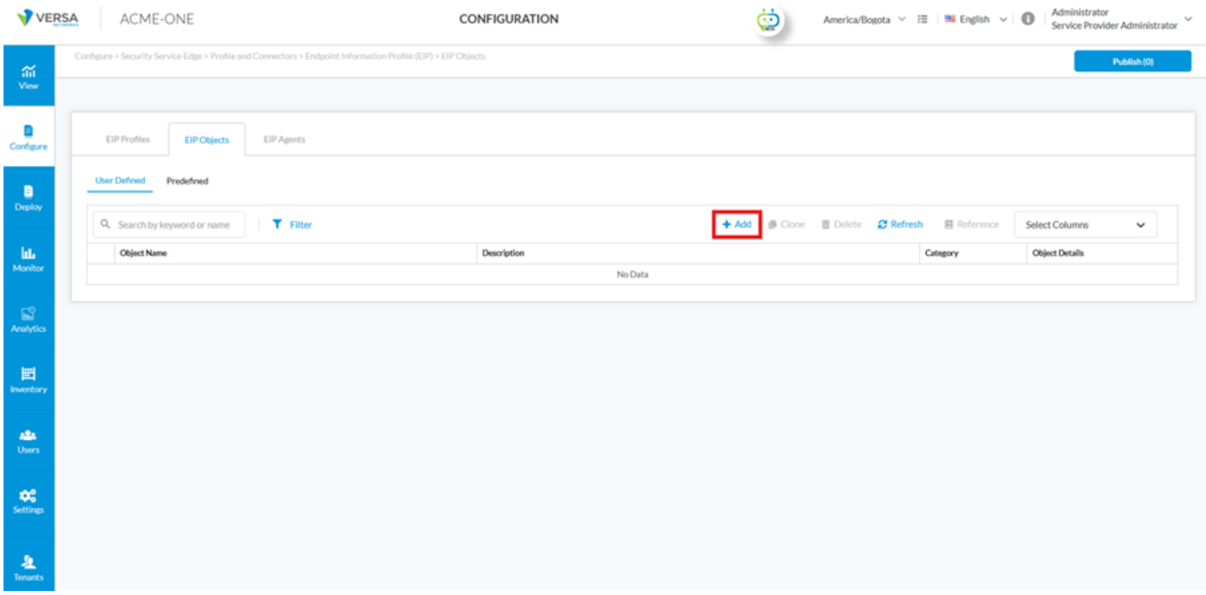
Step 1: Create an EIP Object with Disk Encryption

Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Objects

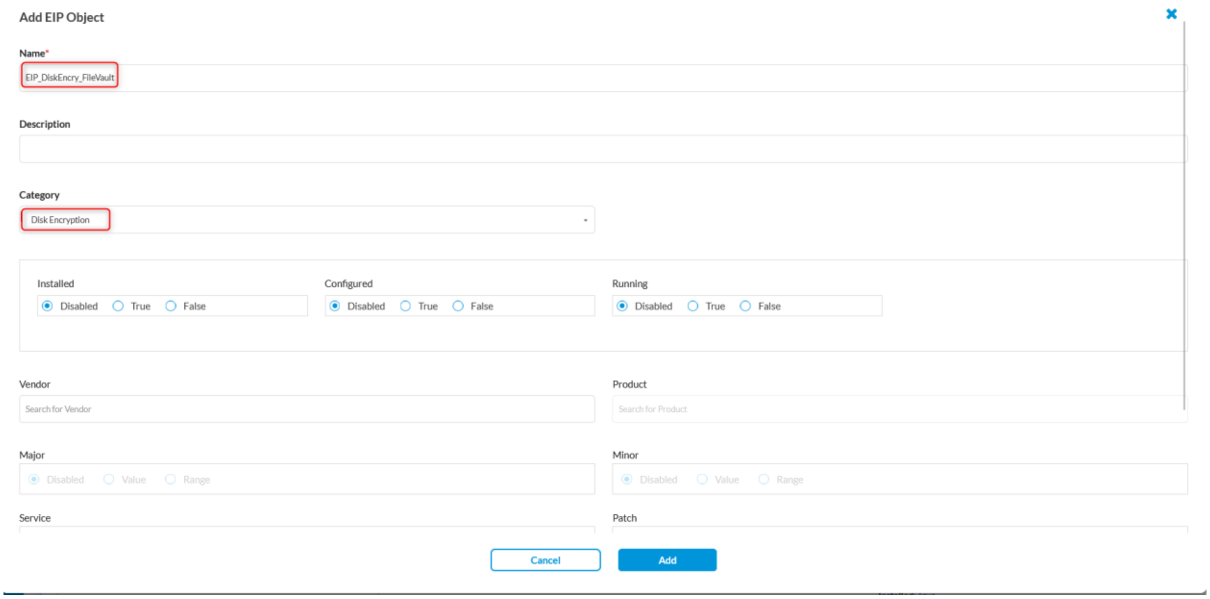


Object Name	Description	Category	Object Details
No Data			

Click on "+ Add" to create a new EIP Object.



Enter a descriptive name for your EIP object. ***Example:* EIP_DiskEncryption.** And Select **DiskEncryption** from the dropdown.



Add EIP Object

Name*: EIP_DiskEncry_FileVault

Description:

Category: Disk Encryption

Installed: ● Disabled ○ True ○ False

Configured: ● Disabled ○ True ○ False

Running: ● Disabled ○ True ○ False

Vendor: Search for Vendor

Product: Search for Product

Major: ● Disabled ○ Value ○ Range

Minor: ● Disabled ○ Value ○ Range

Service

Patch

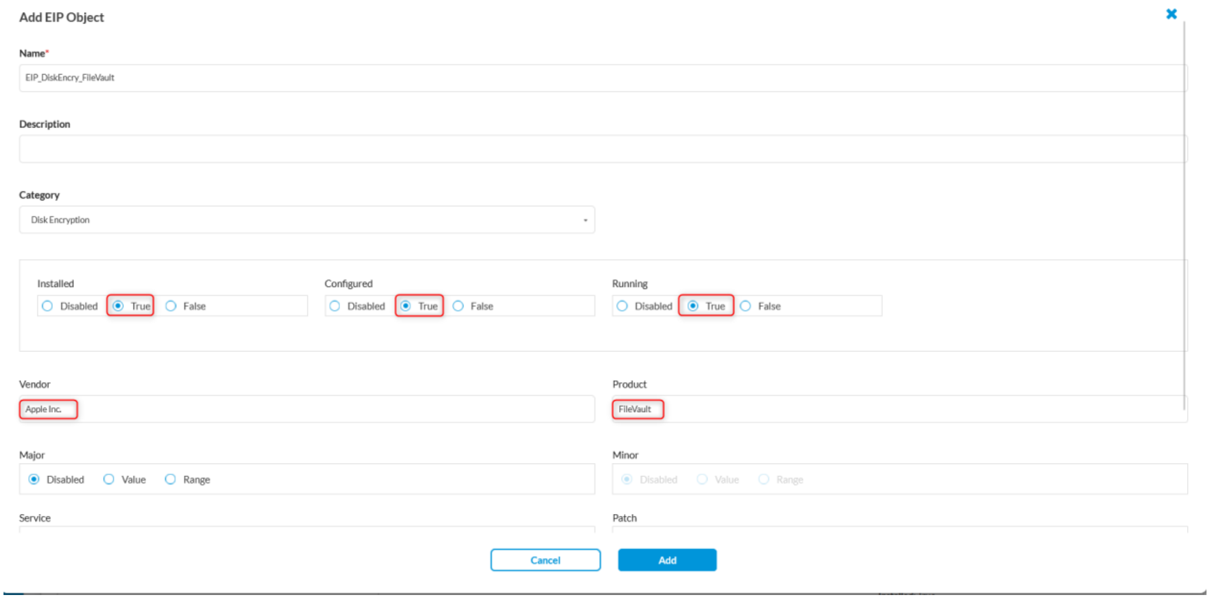
In the **Disk-Encryption** section of the EIP object, configure the following options to validate that the endpoint is protected:

- Installed: True
- Configured: True
- Running: True
- **Vendor / Product**: Specify the approved Disk Encryption solution.

As an example, the screenshot below shows FileVault by Apple configured with the values:

- **Vendor**: Apple
- **Product**: FileVault

This configuration ensures that endpoints are only considered compliant if **FileVault disk encryption is installed, configured, and actively running**. If FileVault is disabled or not active, the device is flagged as non-compliant and may be denied access to corporate resources.



Add EIP Object

Name*: EIP_DiskEncry_FileVault

Description:

Category: Disk Encryption

Installed: ○ Disabled ● True ○ False

Configured: ○ Disabled ● True ○ False

Running: ○ Disabled ● True ○ False

Vendor: Apple Inc.

Product: FileVault

Major: ● Disabled ○ Value ○ Range

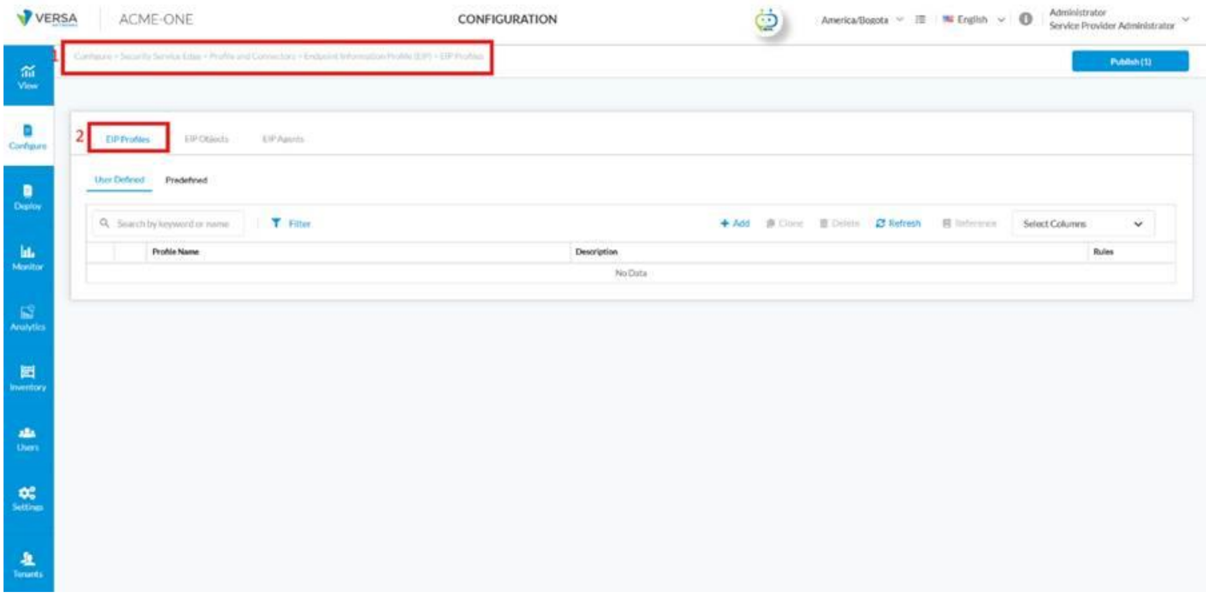
Minor: ● Disabled ○ Value ○ Range

Service

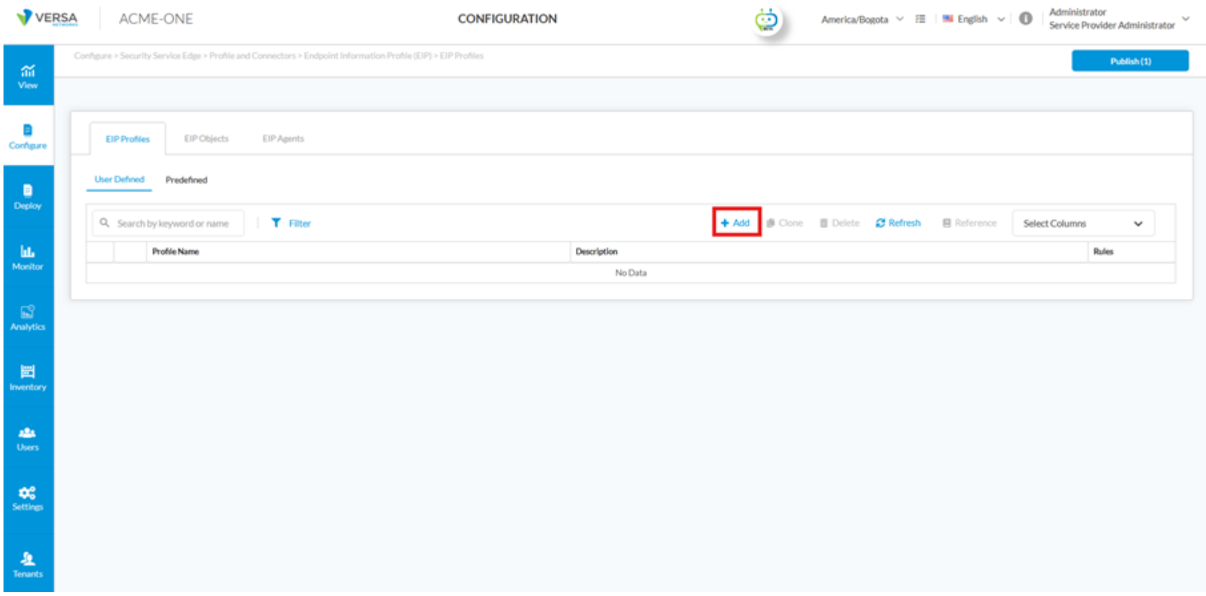
Patch

Step 2: Create an EIP Profile Using Disk Encryption

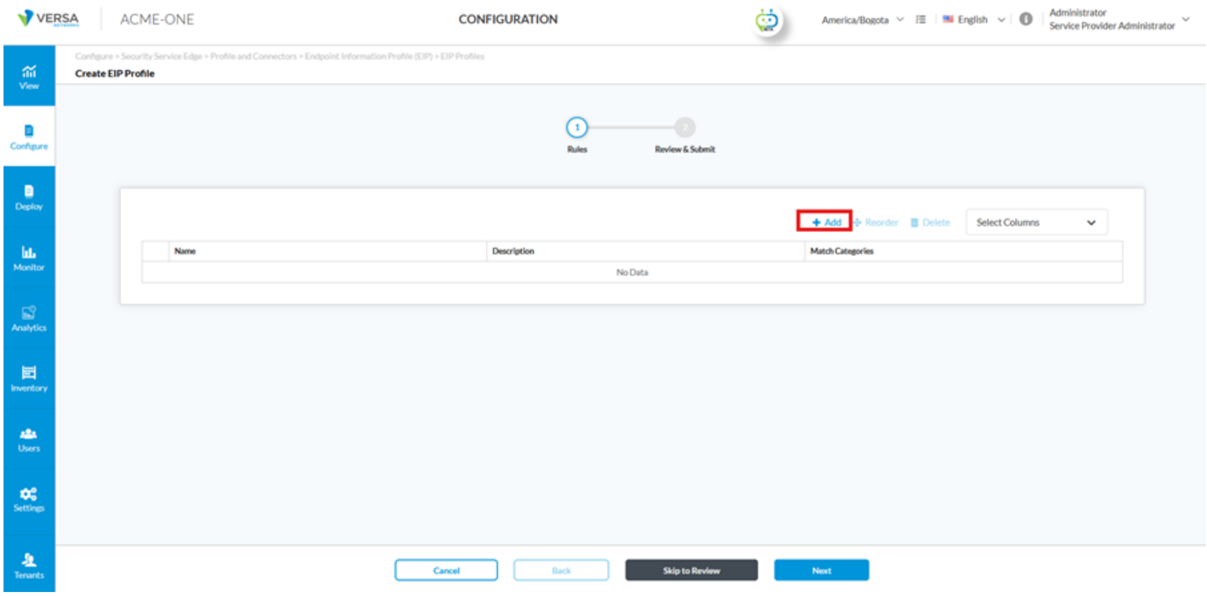
Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Profiles



Click on “+ Add” to start creating a new profile.



In the **Create EIP Profile** window, Click on “+ Add” to define a new rule.



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Create EIP Profile

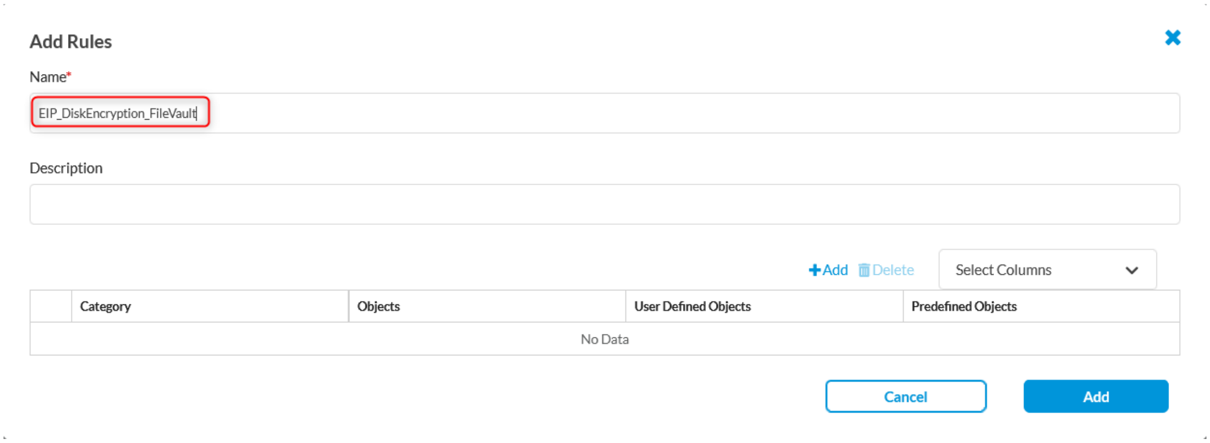
	Name	Description	Match Categories
No Data			

Create a Rule for Disk Encryption

Enter a Name for your rule, Example, EIP_DiskEncryption_FileVault.

 You would (Optional) Add a description for clarity.

Click “+ Add” to attach an EIP Object.



Add Rules

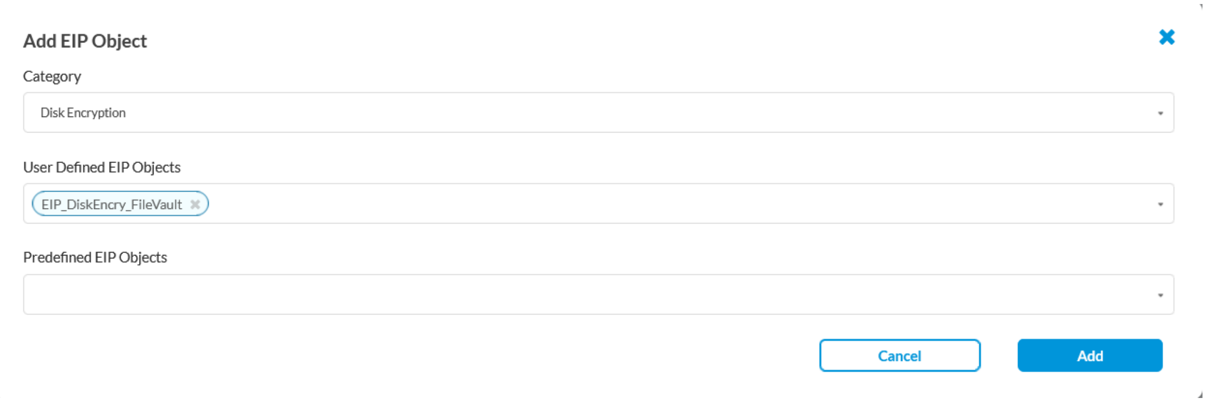
Name*: EIP_DiskEncryption_FileVault

Description:

	Category	Objects	User Defined Objects	Predefined Objects
No Data				

In Add EIP Object dialog, choose the Category. Example **DiskEncryption**.

Select an existing EIP Object or create a new one. For example, an object was created to verify if MacOs DiskEncryption is installed, running and configured in the previous section.



Add EIP Object

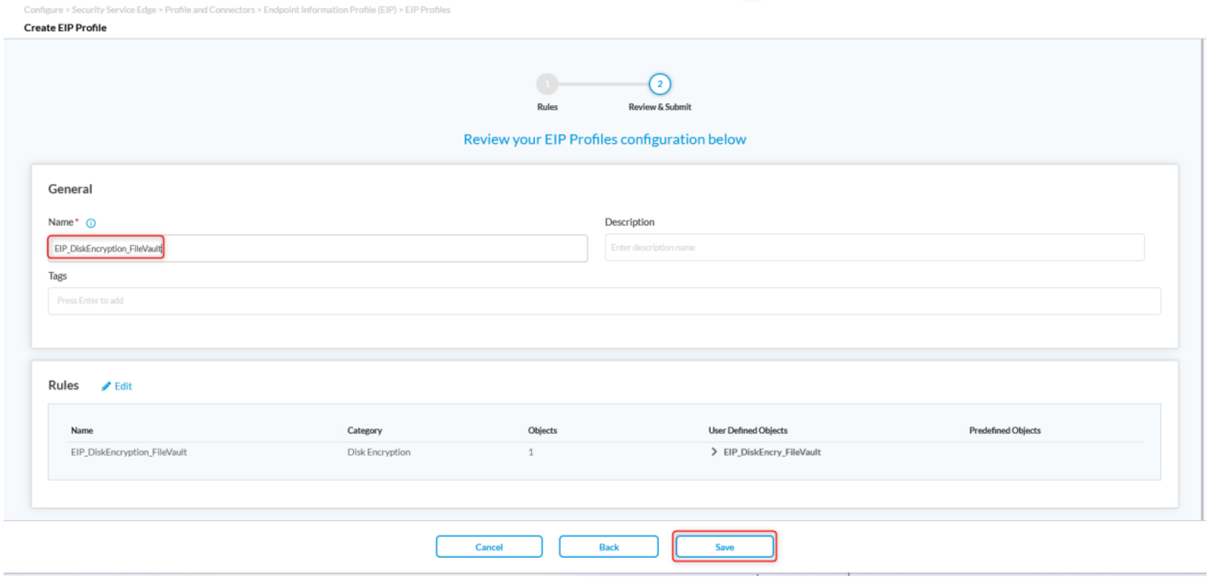
Category: Disk Encryption

User Defined EIP Objects: EIP_DiskEncry_FileVault

Predefined EIP Objects:

Click **Next** and then Enter a descriptive name for your EIP object. ***Example:*** EIP_DiskEncry_FileVault**.**

Review and **Save** the Profile creation



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Create EIP Profile

Review your EIP Profiles configuration below

General

Name*: EIP_DiskEncryption_FileVault

Description: Enter description name

Tags: Press Enter to add

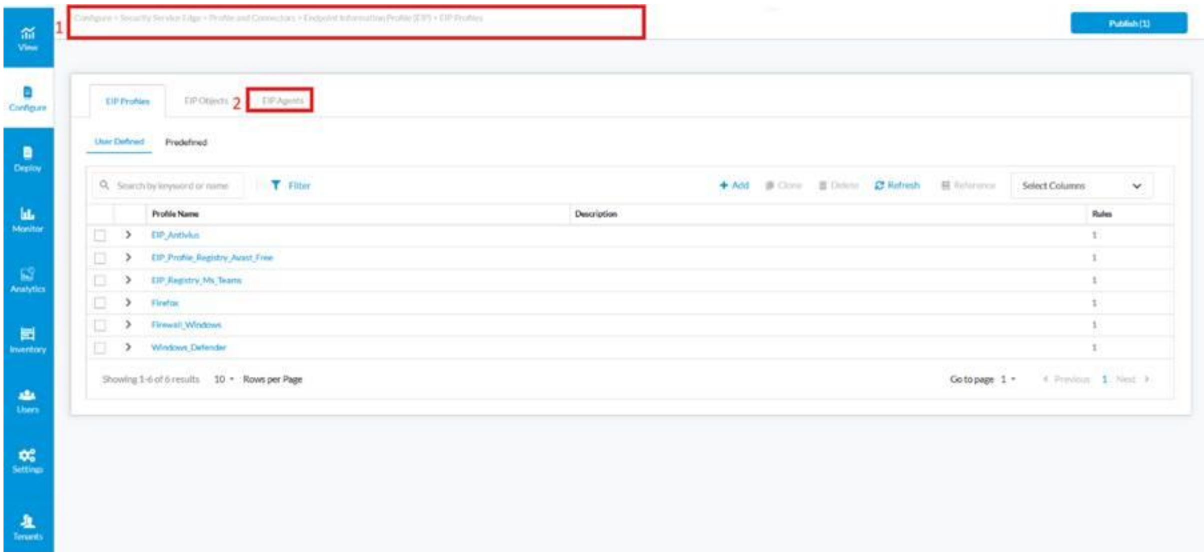
Rules

Name	Category	Objects	User Defined Objects	Predefined Objects
EIP_DiskEncryption_FileVault	Disk Encryption	1	> EIP_DiskEncry_FileVault	

Note: After creating the EIP Object and configuring the EIP Profile and Agent Profile, you must apply them to the Secure Access Client policy to enforce device posture validation and continue evaluation.

Step 3: Navigate to the EIP Agent Section

Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Agents



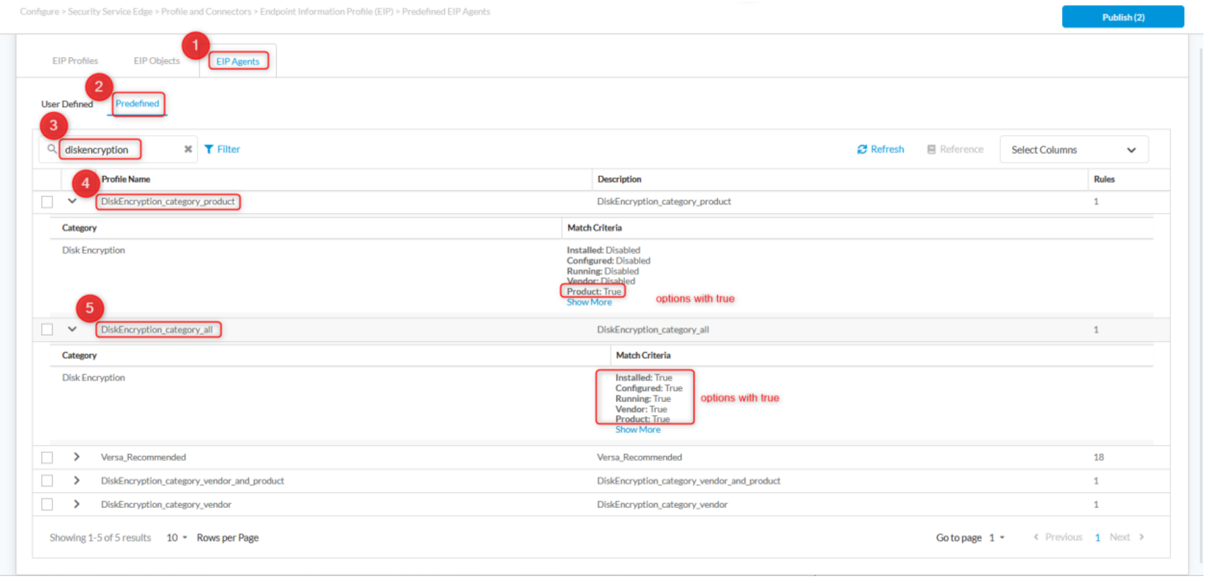
Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Profile Name	Description	Rules
EIP_Antivius		1
EIP_Profile_Registry_Avast_Free		1
EIP_Registry_Ms_Teams		1
Firefox		1
Firewall_Windows		1
Windows_Defender		1

Showing 1-6 of 6 results 10 ▾ Rows per Page Go to page 1 ▾ ‹ Previous 1 Next ›

Step 4: Create an EIP Agent Profile

Important Note: Instead of creating a new agent manually, you can also use a predefined Versa Disk-Encryption agent. In the *Predefined* tab, search for **diskencryption** and select the predefined category that matches your requirements. This option already includes baseline rules such as **Installed: True**, **Configured: True**, and others.



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > Predefined EIP Agents

diskencryption

Profile Name	Description	Rules
DiskEncryption_category_product	DiskEncryption_category_product	1
DiskEncryption_category_all	DiskEncryption_category_all	1
Versa_Recommended	Versa_Recommended	18
DiskEncryption_category_vendor_and_product	DiskEncryption_category_vendor_and_product	1
DiskEncryption_category_vendor	DiskEncryption_category_vendor	1

DiskEncryption_category_product:

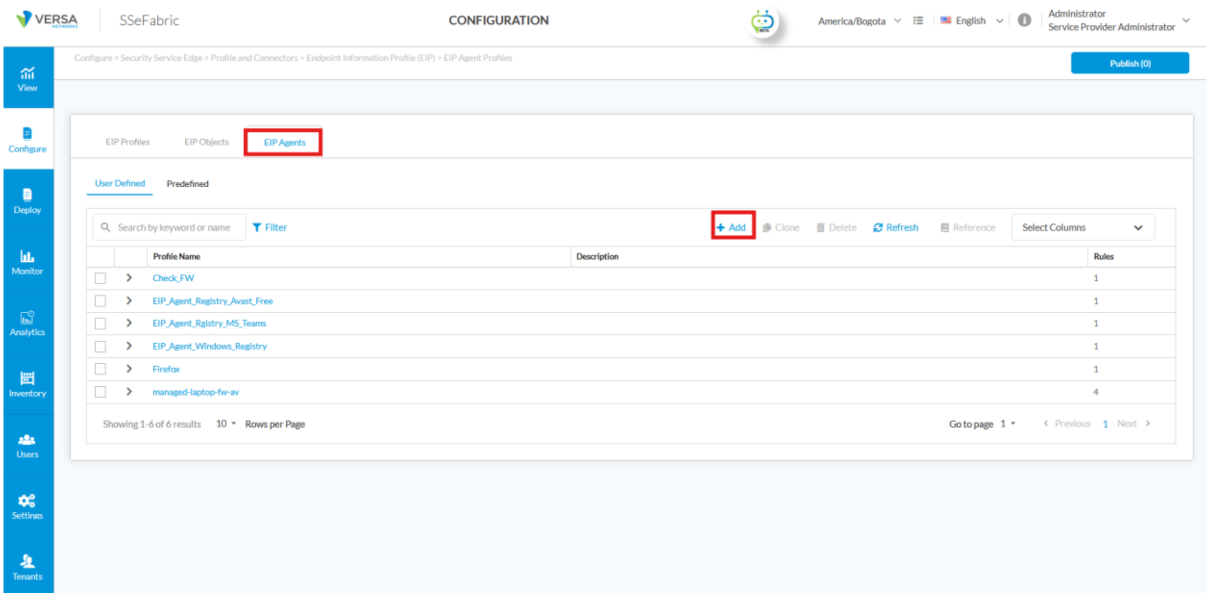
Category	Match Criteria
Disk Encryption	**Installed:** Disabled **Configured:** Disabled **Running:** Disabled **Vendor:** Disabled **Product:** True Show More

DiskEncryption_category_all:

Category	Match Criteria
Disk Encryption	**Installed:** True **Configured:** True **Running:** True **Vendor:** True **Product:** True Show More

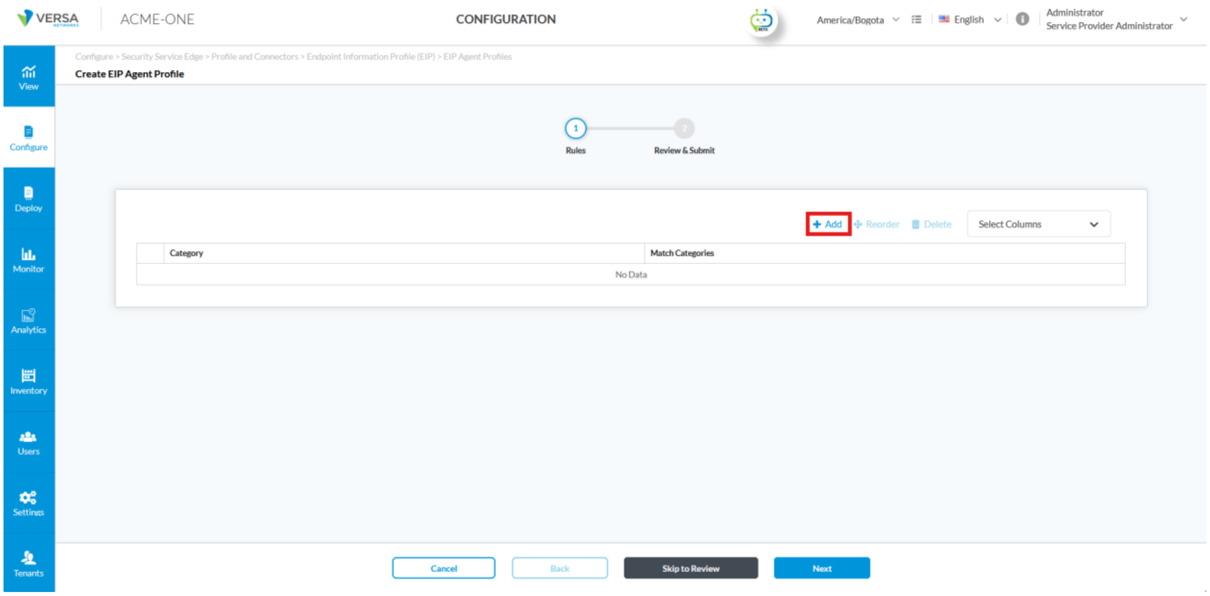
Showing 1-5 of 5 results 10 ▾ Rows per Page Go to page 1 ▾ ‹ Previous 1 Next ›

Click on **Add** to create a **new Agent profile**.



Profile Name	Description	Rules
Check_FW		1
EIP_Agent_Registry_Avast_Free		1
EIP_Agent_Rgistry_MS_Teams		1
EIP_Agent_Windows_Registry		1
Firefox		1
managed-laptop-fw-av		4

Click on "+Add" to create a new rule. Then choose general

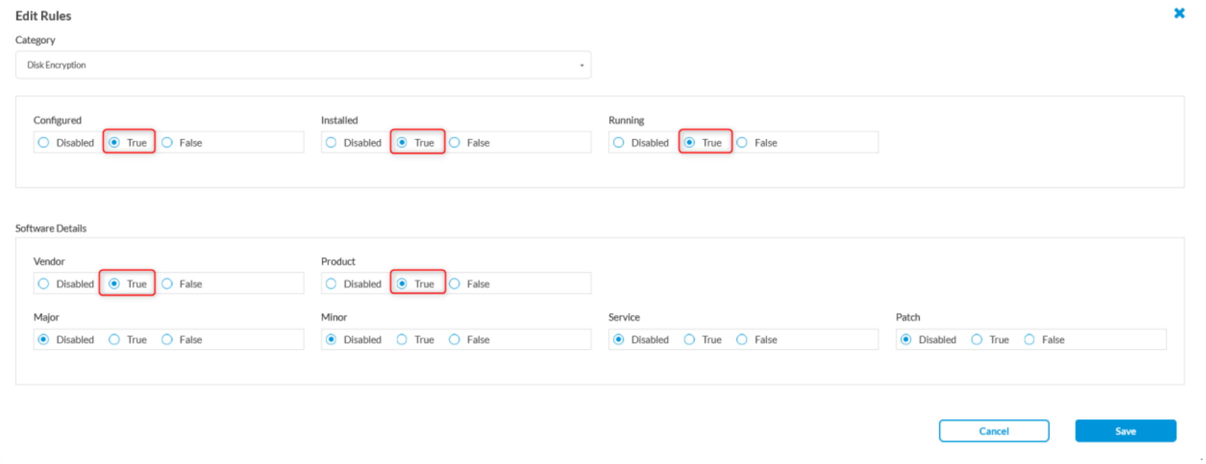


Category	Match Categories
No Data	

In the *Disk Encryption* category of the Agent Profile, configure the following options:

- Installed: True
- Configured: True
- Running: True
- Vendor True
- Product True

This configuration ensures that endpoints are validated for the presence and activity of disk encryption. Devices that fail any of these checks are flagged as non-compliant and may be restricted from accessing corporate resources.



Edit Rules

Category: Disk Encryption

Configured: ○ Disabled ● True ○ False

Installed: ○ Disabled ● True ○ False

Running: ○ Disabled ● True ○ False

Software Details

Vendor: ○ Disabled ● True ○ False

Product: ○ Disabled ● True ○ False

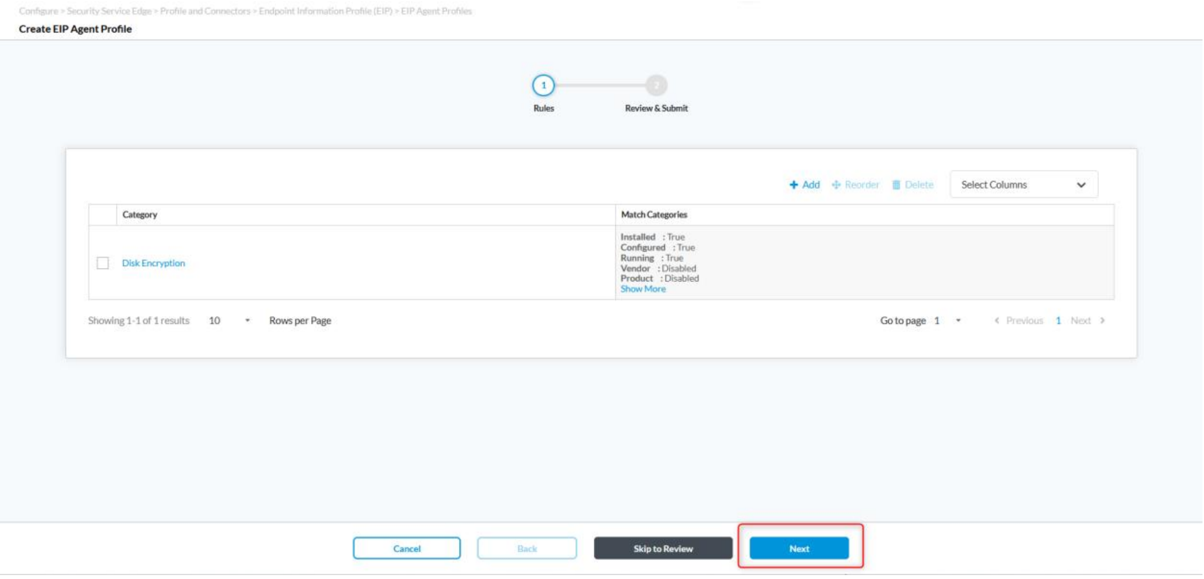
Major: ● Disabled ○ True ○ False

Minor: ● Disabled ○ True ○ False

Service: ● Disabled ○ True ○ False

Patch: ● Disabled ○ True ○ False

Click on “next” to enter a descriptive Profile Name (Example., **EIP_Agent_DiskEncryp_FileVault**).

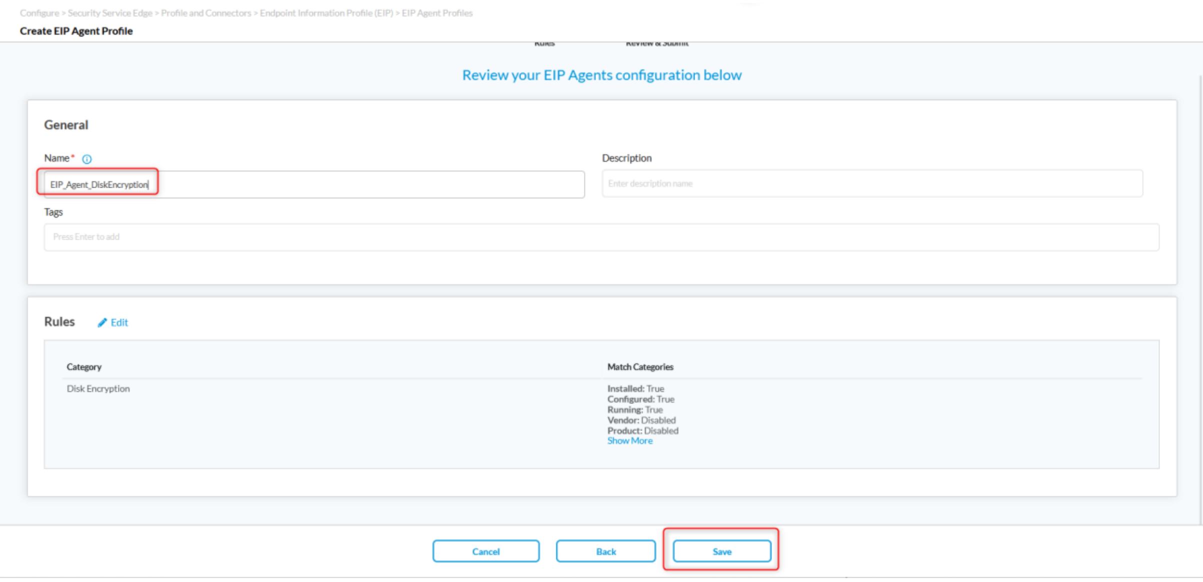


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Create EIP Agent Profile

	Category	Match Categories
□	Disk Encryption	Installed : True Configured : True Running : True Vendor : Disabled Product : Disabled Show More

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Create EIP Agent Profile

Review your EIP Agents configuration below

General

Name*: EIP_Agent_DiskEncryption

Description: Enter description name

Tags: Press Enter to add

Rules

Category	Match Categories
Disk Encryption	**Installed:** True **Configured:** True **Running:** True **Vendor:** Disabled **Product:** Disabled Show More

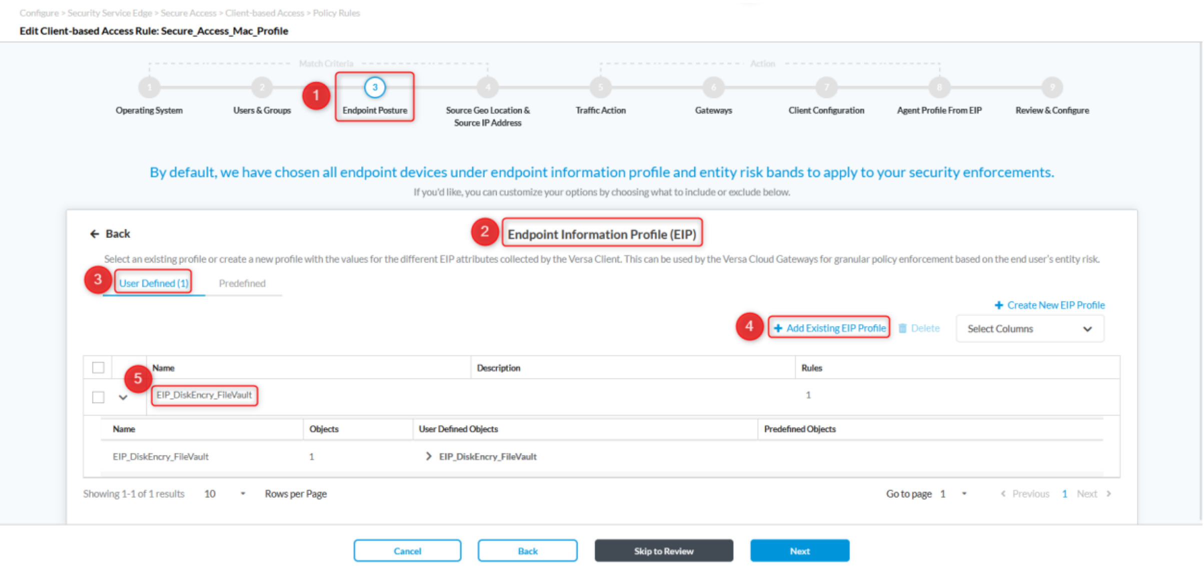
Step 5: Configure Secure Client Access Rule

Navigate to:

Configure > Security Service Edge > Secure Access > Client-based Access > Rules.

Click "**+ Add**" to create a new Secure Access Client rule or edit an existing rule.

In the Match Criteria configuration, go to the ***Endpoint Posture*** section. Under the *Endpoint Information Profile (EIP)* panel, select the desired profile by navigating to the ***User Defined*** tab and clicking on *Add Existing EIP Profile*. Then, choose the EIP profile you previously created. Example EIP_DiskEncry_FileVault).



Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure_Access_Mac_Profile

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

Endpoint Information Profile (EIP)

Select an existing profile or create a new profile with the values for the different EIP attributes collected by the Versa Client. This can be used by the Versa Cloud Gateways for granular policy enforcement based on the end user's entity risk.

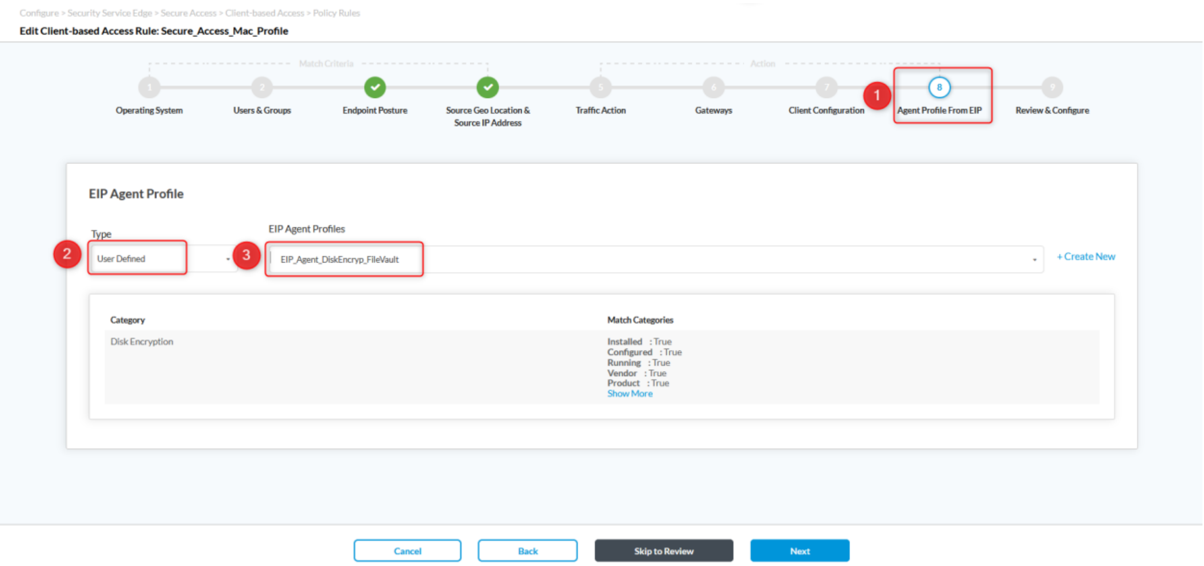
Name	Description	Rules
EIP_DiskEncry_FileVault		1

Name	Objects	User Defined Objects	Predefined Objects
EIP_DiskEncry_FileVault	1	EIP_DiskEncry_FileVault	

Showing 1-1 of 1 results 10 Rows per Page

Go to page 1 Previous 1 Next

In action configuration, under the **Agent Profile From EIP** section, set the Type to **User Defined** and select the **EIP Agent Profile** you previously created. Example EIP_Agent_DiskEncryp_FileVault. *The Match Categories panel will display the defined validation criteria, such as registry paths or process checks, ensuring that the selected EIP Agent Profile is applied for endpoint posture verification*.



Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure_Access_Mac_Profile

EIP Agent Profile

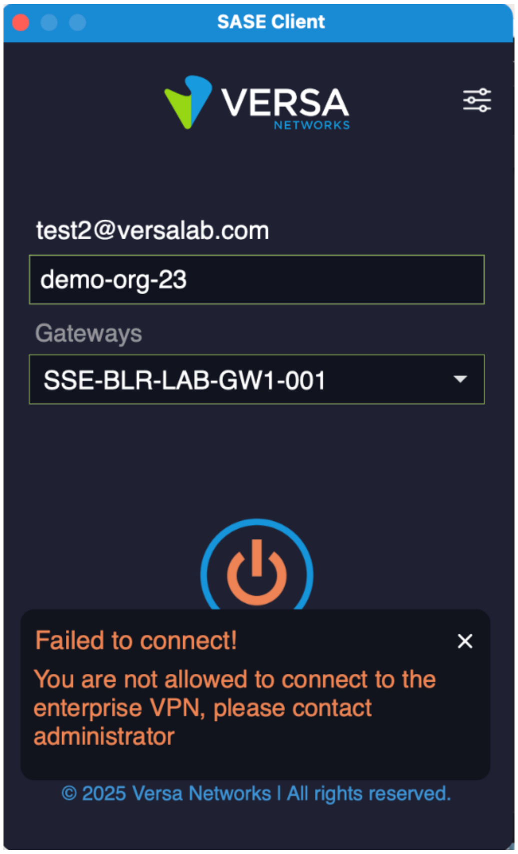
Type: User Defined

EIP Agent Profiles: EIP_Agent_DiskEncryp_FileVault

Category	Match Categories
Disk Encryption	Installed : True Configured : True Running : True Vendor : True Product : True

Verification

At this time, the macOS device has FileVault disk encryption installed and configured; however, it is not running. When the Versa SASE Client attempts to connect, the authentication fails due to the EIP policy that requires active disk encryption.



SASE Client

test2@versalab.com

demo-org-23

Gateways

SSE-BLR-LAB-GW1-001

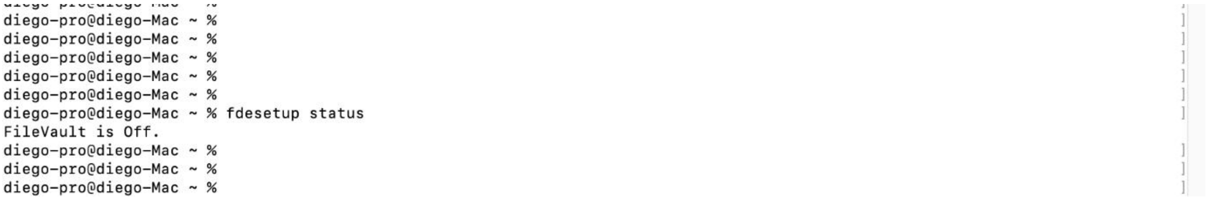
Failed to connect!

You are not allowed to connect to the enterprise VPN, please contact administrator

© 2025 Versa Networks | All rights reserved.

To confirm the posture on the endpoint, you would check whether FileVault is enabled and running by executing the following command in Terminal:

```
fdesetup status
```



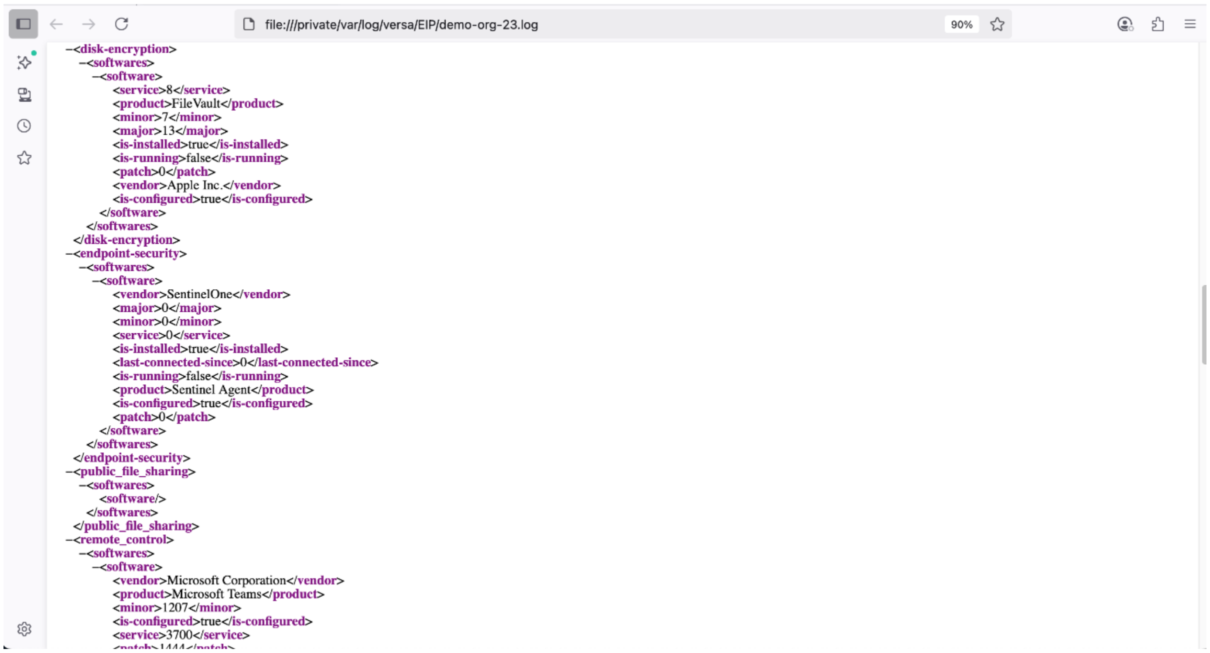
```
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ % fdesetup status
FileVault is Off.
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
```

The command output shows that FileVault is not active, which validates that disk encryption is not running on the device.

In addition, reviewing the EIP posture log collected from the device confirms that **FileVault disk encryption** is detected:

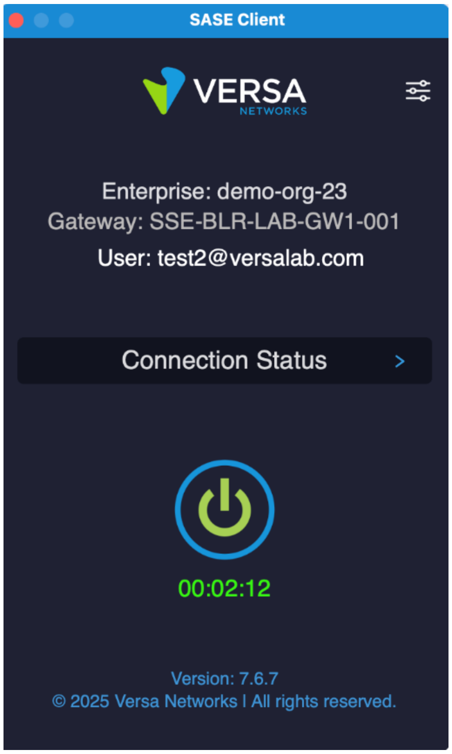
- **Vendor:** Apple Inc.
- **Product:** FileVault – version 13.7
- Installed: True
- Configured: True
- Running: False

This indicates that FileVault is present on the macOS endpoint but not actively running, meaning the device does not yet meet the EIP policy requirement for disk encryption.



```
–<disk-encryption>
  –<softwares>
    –<software>
       <service>8</service>
       <product>FileVault</product>
       <minor>7</minor>
       <major>13</major>
       <is-installed>true</is-installed>
       <is-running>false</is-running>
       <patch>0</patch>
       <vendor>Apple Inc.</vendor>
       <is-configured>true</is-configured>
     </software>
   </softwares>
 </disk-encryption>
–<endpoint-security>
  –<softwares>
    –<software>
       <vendor>SentinelOne</vendor>
       <major>0</major>
       <minor>0</minor>
       <service>0</service>
       <is-installed>true</is-installed>
       <last-connected-since>0</last-connected-since>
       <is-running>false</is-running>
       <product>Sentinel Agent</product>
       <is-configured>true</is-configured>
       <patch>0</patch>
     </software>
   </softwares>
 </endpoint-security>
–<public_file_sharing>
  –<softwares>
     <software/>
   </softwares>
 </public_file_sharing>
–<remote_control>
  –<softwares>
    –<software>
       <vendor>Microsoft Corporation</vendor>
       <product>Microsoft Teams</product>
       <minor>1207</minor>
       <is-configured>true</is-configured>
       <service>3700</service>
       <patch>1444</patch>
```

After enabling **FileVault** and disk encryption is running, the Versa SASE Client is able to authenticate successfully and establish a secure connection to the enterprise VPN.



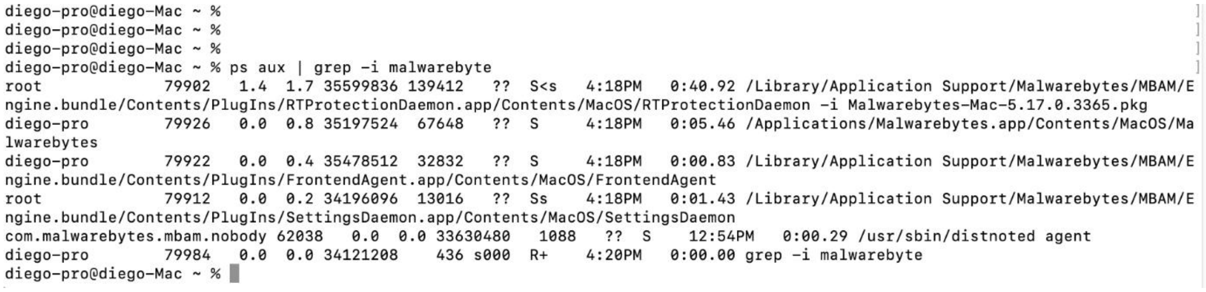
Enterprise: demo-org-23
Gateway: SSE-BLR-LAB-GW1-001
User: test2@versalab.com

00:02:12

Version: 7.6.7
© 2025 Versa Networks I All rights reserved.

To confirm the posture on the endpoint, you would check again whether **FileVault** disk encryption is enabled and running by executing the following command in Terminal:

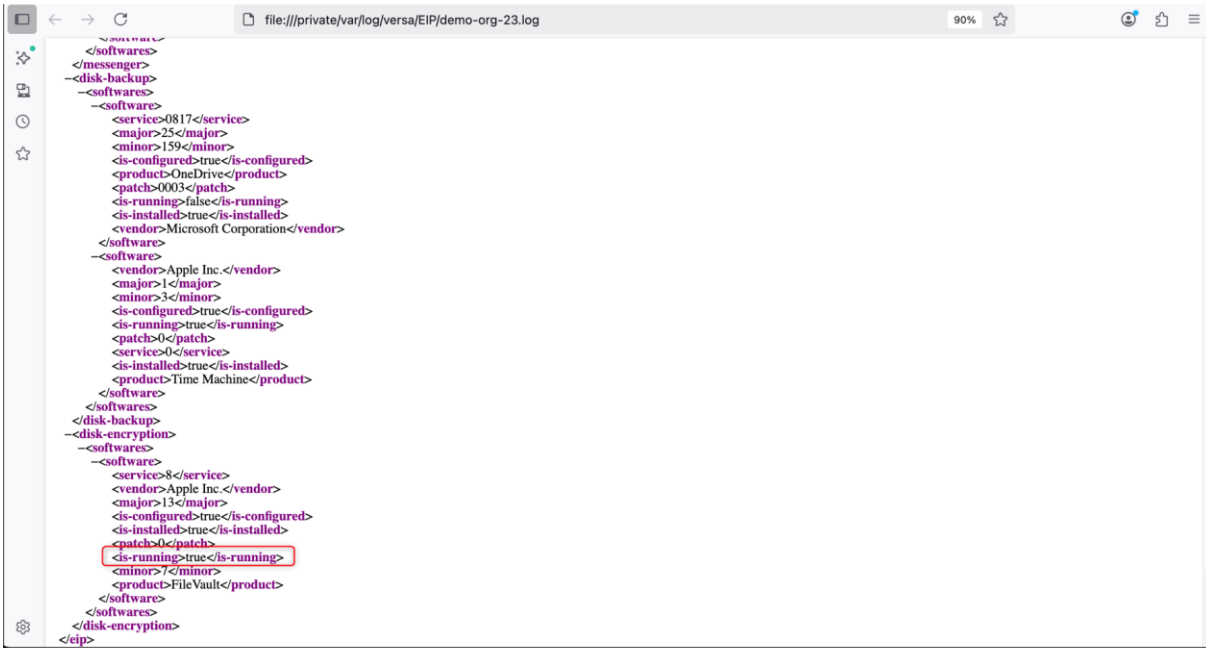
fdesetup status



```
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ % ps aux | grep -i malwarebyte
root             79902   1.4  1.7 35599836 139412   ??  S<s   4:18PM   0:40.92 /Library/Application Support/Malwarebytes/MBAM/E
ngine.bundle/Contents/PlugIns/RTProtectionDaemon.app/Contents/MacOS/RTProtectionDaemon -i Malwarebytes-Mac-5.17.0.3365.pkg
diego-pro        79926   0.0  0.8 35197524  67648   ??  S     4:18PM   0:05.46 /Applications/Malwarebytes.app/Contents/MacOS/Ma
lwarebytes
diego-pro        79922   0.0  0.4 35478512  32832   ??  S     4:18PM   0:00.83 /Library/Application Support/Malwarebytes/MBAM/E
ngine.bundle/Contents/PlugIns/FrontendAgent.app/Contents/MacOS/FrontendAgent
root             79912   0.0  0.2 34196096  13016   ??  Ss    4:18PM   0:01.43 /Library/Application Support/Malwarebytes/MBAM/E
ngine.bundle/Contents/PlugIns/SettingsDaemon.app/Contents/MacOS/SettingsDaemon
com.malwarebytes.mbam.nobody 62038   0.0  0.0 33630480   1088   ??  S    12:54PM   0:00.29 /usr/sbin/distnoted agent
diego-pro        79984   0.0  0.0 34121208    436 s000  R+    4:20PM   0:00.00 grep -i malwarebyte
diego-pro@diego-Mac ~ %
```

The command output shows **"FileVault is On"**, which validates that disk encryption is enabled and actively protecting the macOS device.

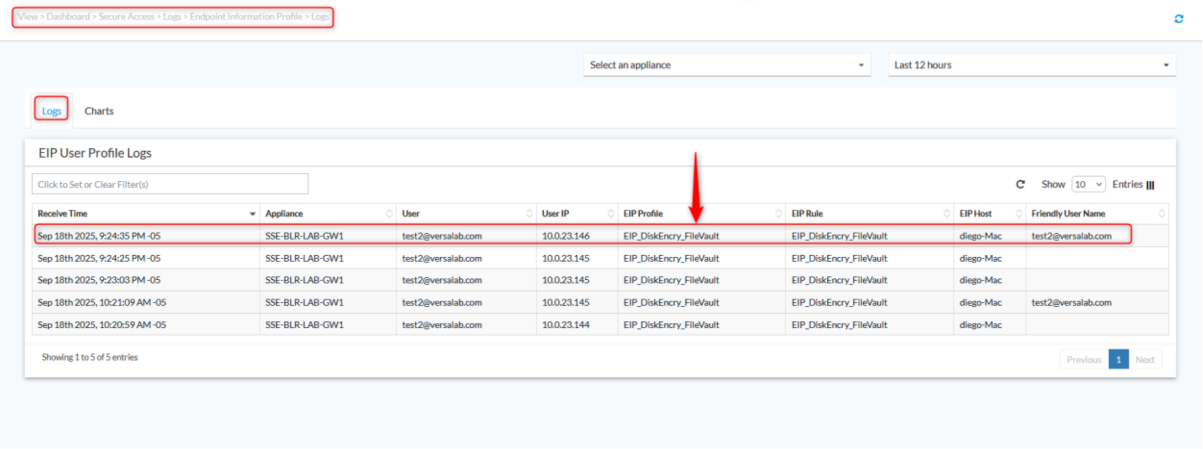
You are able to check the disk encryption status directly in the EIP posture logs located under /private/var/log/versa/EIP/demo-org-23.log. In the log, the **Disk Encryption** section lists **FileVault** with the attributes is-installed: true, is-configured: true, and is-running: true. This confirms that FileVault disk encryption is enabled and actively protecting the macOS device, allowing the endpoint to meet the EIP policy requirement for disk encryption compliance.



file:///private/var/log/versa/EIP/demo-org-23.log

```
      </software>
    </softwares>
  </messenger>
 −<disk-backup>
   −<softwares>
     −<software>
        <service>0817</service>
        <major>25</major>
        <minor>159</minor>
        <is-configured>true</is-configured>
        <product>OneDrive</product>
        <patch>0003</patch>
        <is-running>false</is-running>
        <is-installed>true</is-installed>
        <vendor>Microsoft Corporation</vendor>
      </software>
     −<software>
        <vendor>Apple Inc.</vendor>
        <major>1</major>
        <minor>3</minor>
        <is-configured>true</is-configured>
        <is-running>true</is-running>
        <patch>0</patch>
        <service>0</service>
        <is-installed>true</is-installed>
        <product>Time Machine</product>
      </software>
    </softwares>
  </disk-backup>
 −<disk-encryption>
   −<softwares>
     −<software>
        <service>8</service>
        <vendor>Apple Inc.</vendor>
        <major>13</major>
        <is-configured>true</is-configured>
        <is-installed>true</is-installed>
        <patch>0</patch>
        <is-running>true</is-running>
        <minor>7</minor>
        <product>FileVault</product>
      </software>
    </softwares>
  </disk-encryption>
</eip>
```

You check the Concerto logs to validate that the EIP authentication profile matches the expected profile. In Concerto From the log view (**View > Dashboard > Secure Access > Logs > Endpoint Information Profile > Logs**).


View > Dashboard > Secure Access > Logs > Endpoint Information Profile > Logs
Select an appliance
Last 12 hours
Logs
Charts
EIP User Profile Logs
Click to Set or Clear Filter(s)
Show 10 Entries

Receive Time	Appliance	User	User IP	EIP Profile	EIP Rule	EIP Host	Friendly User Name
Sep 18th 2025, 9:24:35 PM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.146	EIP_DiskEncry_FileVault	EIP_DiskEncry_FileVault	diego-Mac	test2@versalab.com
Sep 18th 2025, 9:24:25 PM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.145	EIP_DiskEncry_FileVault	EIP_DiskEncry_FileVault	diego-Mac	
Sep 18th 2025, 9:23:03 PM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.145	EIP_DiskEncry_FileVault	EIP_DiskEncry_FileVault	diego-Mac	
Sep 18th 2025, 10:21:09 AM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.145	EIP_DiskEncry_FileVault	EIP_DiskEncry_FileVault	diego-Mac	test2@versalab.com
Sep 18th 2025, 10:20:59 AM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.144	EIP_DiskEncry_FileVault	EIP_DiskEncry_FileVault	diego-Mac	

Showing 1 to 5 of 5 entries

Entry show that the endpoint matches the **EIP_DiskEncry_FileVault** profile and rule after DiskEncryption is running. The appliance, user, and host details confirm that the macOS device, associated with user, is evaluated against the correct profile. This confirms that the endpoint is recognized as compliant, the EIP profile and rule are enforced, and secure access is granted according to the posture policy.

Combined Posture Validation: Disk Encryption + Firewall (CrowdStrike)

This case validates that macOS endpoints not only have full-disk encryption enabled but also run an approved firewall solution. By combining these checks, organizations can enforce stronger posture requirements that protect both **data at rest** and **network-level security** before granting access to enterprise resources.

For macOS devices, administrators can verify both controls using the EIP posture logs (/private/var/log/versa/EIP/demo-org-23.log) or directly from the system:

- To verify disk encryption status (FileVault):
  - fdesetup status
    - *FileVault is On* → the system drive is encrypted.
    - *FileVault is Off* → the system drive is not encrypted.
    - *Encryption in progress* → the drive is currently encrypting.
- To verify the firewall (CrowdStrike Falcon):
  - ps aux | grep -i crowdstrike

This confirms if the CrowdStrike Falcon agent, which provides firewall and network protection on macOS, is installed and actively running.

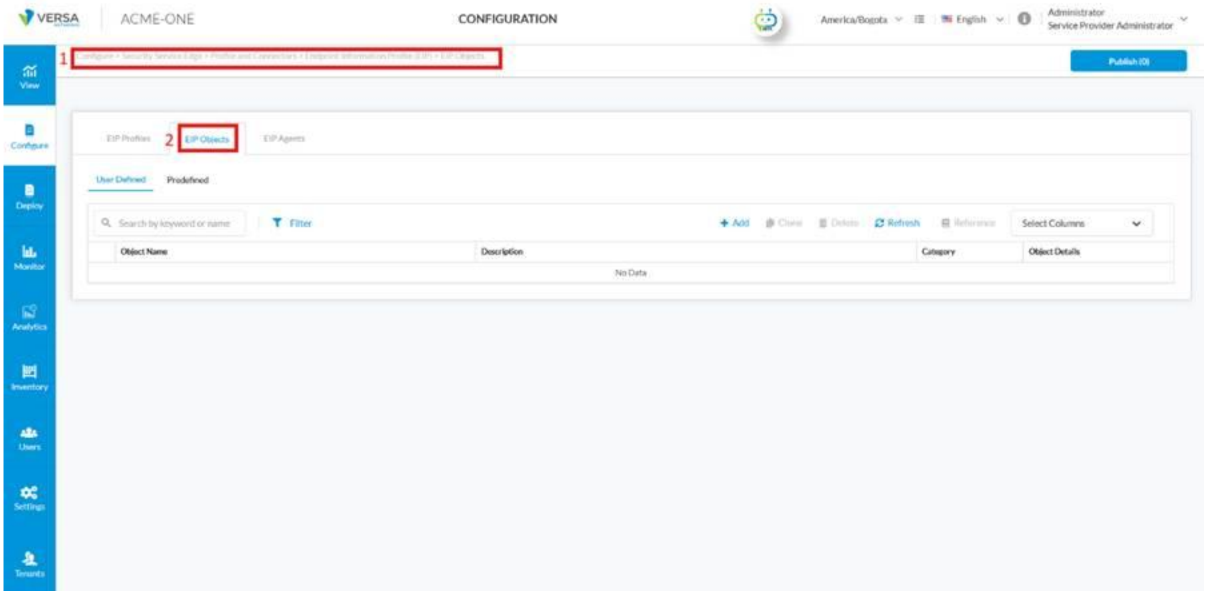
Scenario: An organization requires all corporate Macs to have **FileVault enabled** and the **CrowdStrike Falcon firewall service active**. In the EIP Profile, the administrator defines compliance rules for both **Disk**

Encryption and **Firewall** categories. When a device connects:

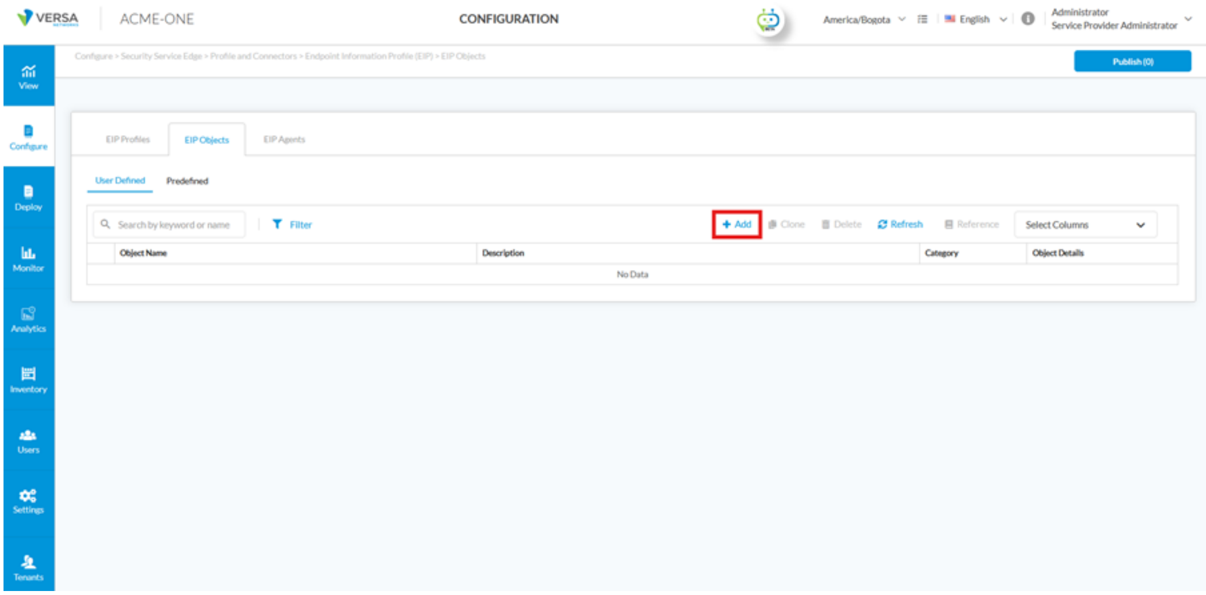
- If FileVault is enabled and running **and** the CrowdStrike Falcon firewall is installed and active, the device is considered **compliant**.
- If either control is missing, disabled, or not detected, the device is **non-compliant** and access may be restricted.
- This ensures that only endpoints providing both strong encryption and active network protection can access sensitive corporate applications, reinforcing Zero Trust posture validation.

Step 1: Create an EIP Object Disk Encryption

Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Objects



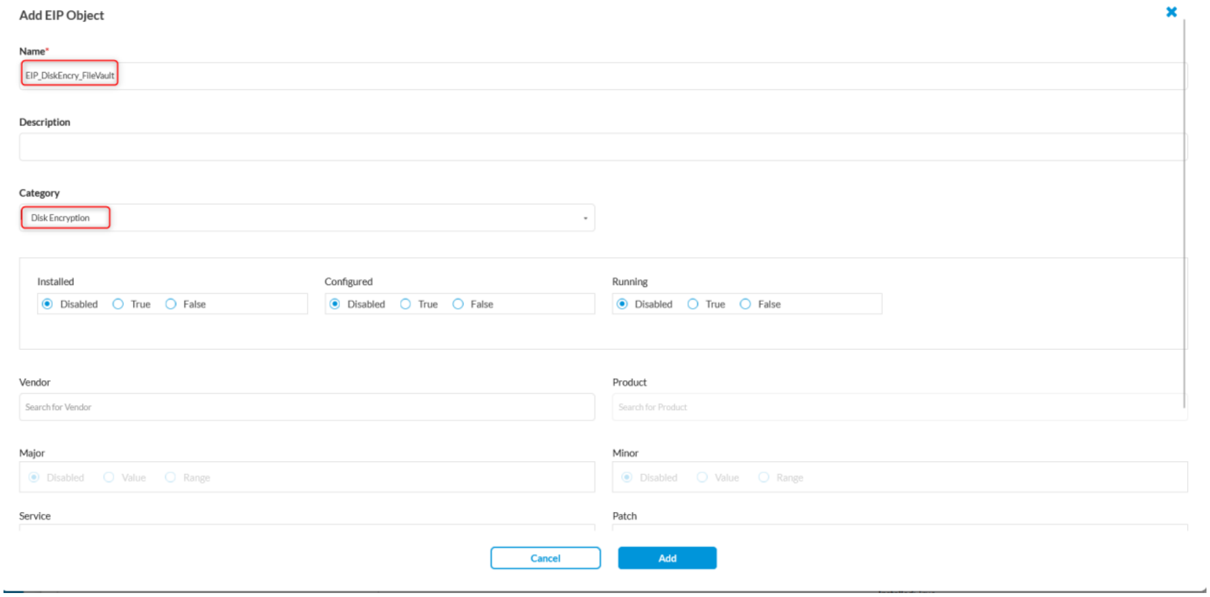
Click on "+ Add" to create a new EIP Object.



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Objects

Object Name	Description	Category	Object Details
No Data			

Enter a descriptive name for your EIP object. ***Example:*** **EIP_DiskEncryption.** And Select **DiskEncryption** from the dropdown.



Add EIP Object

Name*: EIP_DiskEncry_FileVault

Description:

Category: Disk Encryption

Installed: ● Disabled ○ True ○ False

Configured: ● Disabled ○ True ○ False

Running: ● Disabled ○ True ○ False

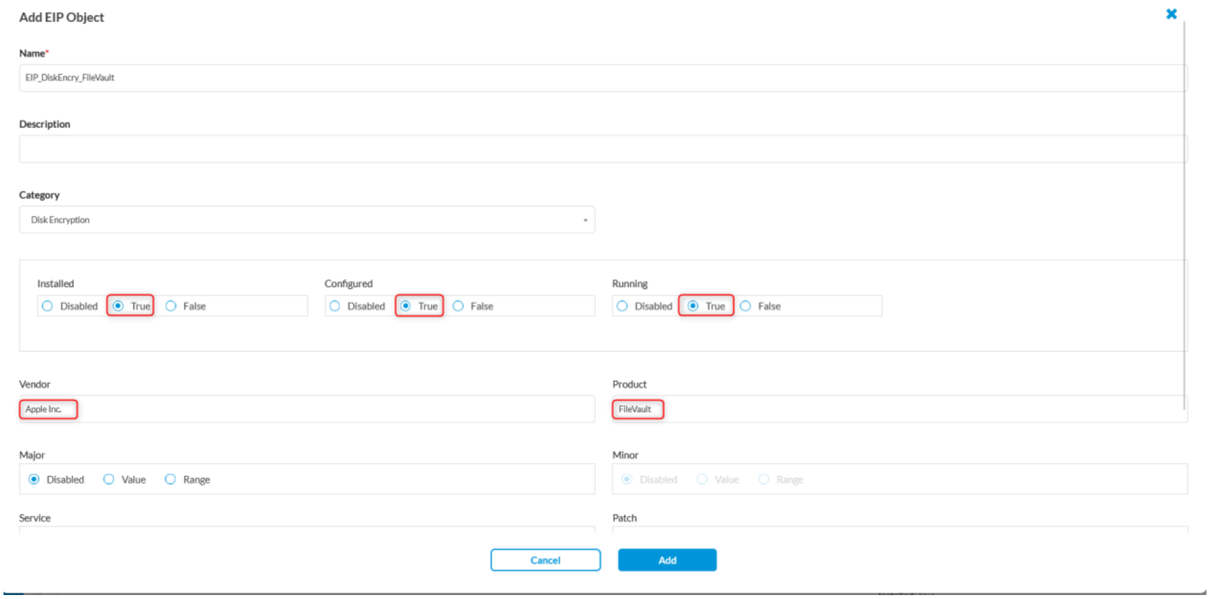
In the **Disk-Encryption** section of the EIP object, configure the following options to validate that the endpoint is protected:

- Installed: True
- Configured: True
- Running: True
- **Vendor / Product**: Specify the approved Disk Encryption solution.

As an example, the screenshot below shows FileVault by Apple configured with the values:

- **Vendor**: Apple
- **Product**: FileVault

This configuration ensures that endpoints are only considered compliant if **FileVault disk encryption is installed, configured, and actively running**. If FileVault is disabled or not active, the device is flagged as non-compliant and may be denied access to corporate resources.



Add EIP Object

Name*: EIP_DiskEncry_FileVault

Description:

Category: Disk Encryption

Installed: ○ Disabled ● True ○ False

Configured: ○ Disabled ● True ○ False

Running: ○ Disabled ● True ○ False

Vendor: Apple Inc.

Product: FileVault

Major: ● Disabled ○ Value ○ Range

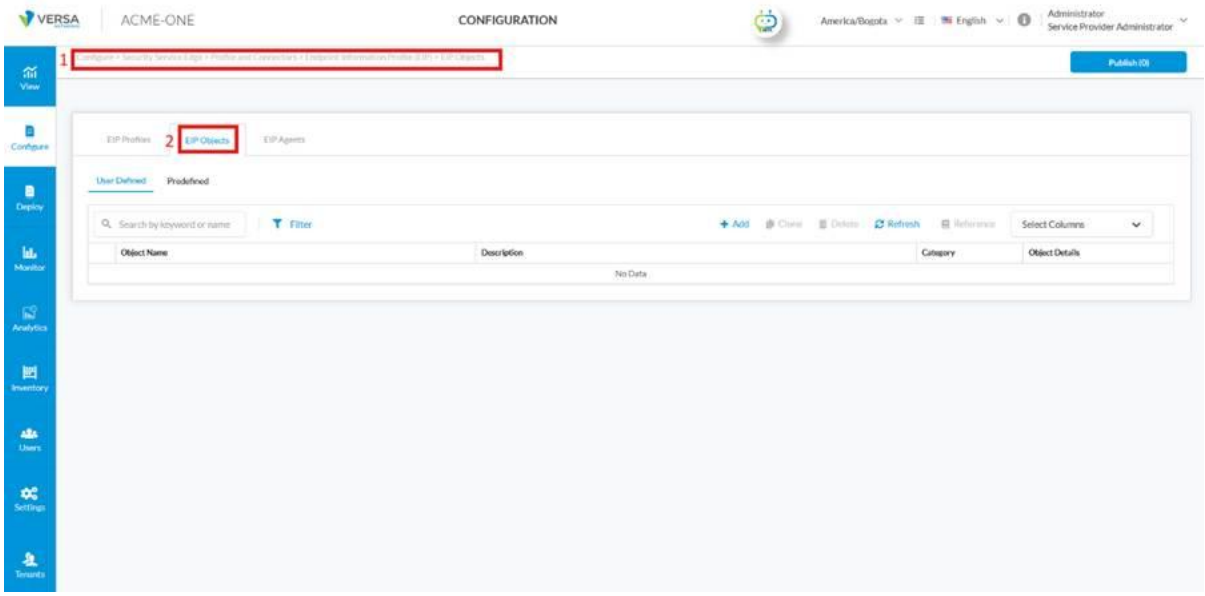
Minor: ● Disabled ○ Value ○ Range

Service

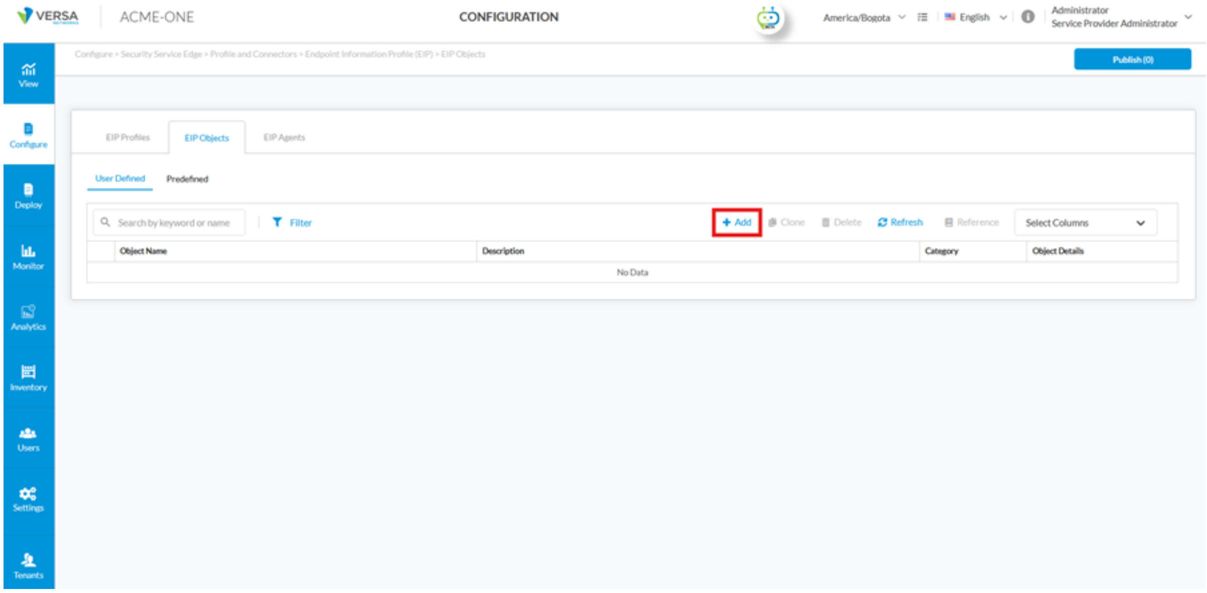
Patch

Step 2: Validate an EIP Object for Firewall (CrowdStrike)

Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Objects



Click on "+ Add" to create a new EIP Object.



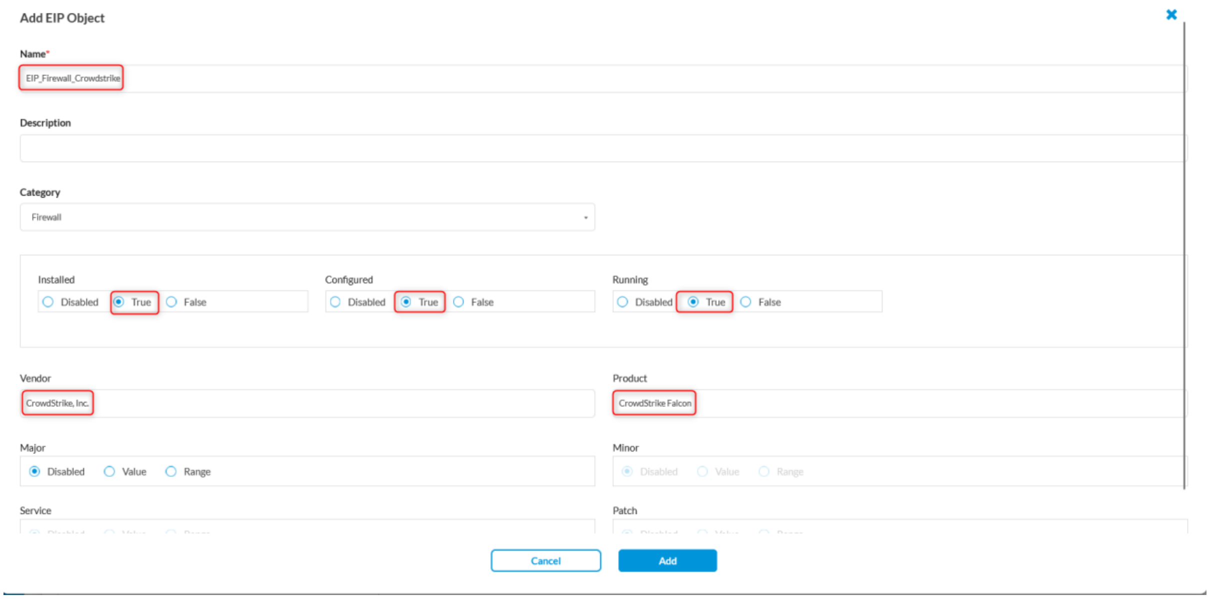
In the **Firewall** section of the EIP object, configure the following options to validate that the endpoint is protected:

- Installed: True
- Configured: True
- Running: True
- **Vendor / Product**: Specify the approved Crowdstrike solution.

As an example, the screenshot below shows Falcon Crowdstrike by CrowdStrike Falcon configured with the values:

  - **Vendor**: Crowdstrike
  - **Product**: crowdstrike

This configuration ensures that endpoints are only considered compliant if **CrowdStrike Falcon is installed, configured, and actively running**. If Crowdstrike is disabled or not active, the device is flagged as non-compliant and may be denied access to corporate resources.



Add EIP Object

Name*: EIP_Firewall_Crowdstrike

Description:

Category: Firewall

Installed: ○ Disabled ● True ○ False

Configured: ○ Disabled ● True ○ False

Running: ○ Disabled ● True ○ False

Vendor: CrowdStrike, Inc.

Product: CrowdStrike Falcon

Major: ● Disabled ○ Value ○ Range

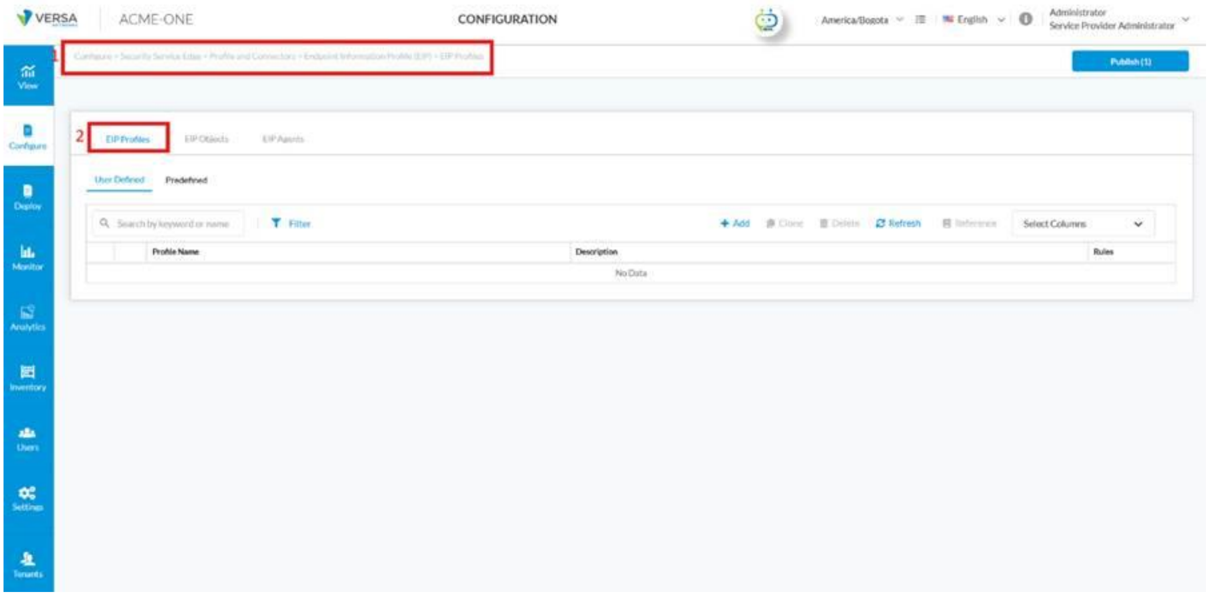
Minor: ● Disabled ○ Value ○ Range

Service

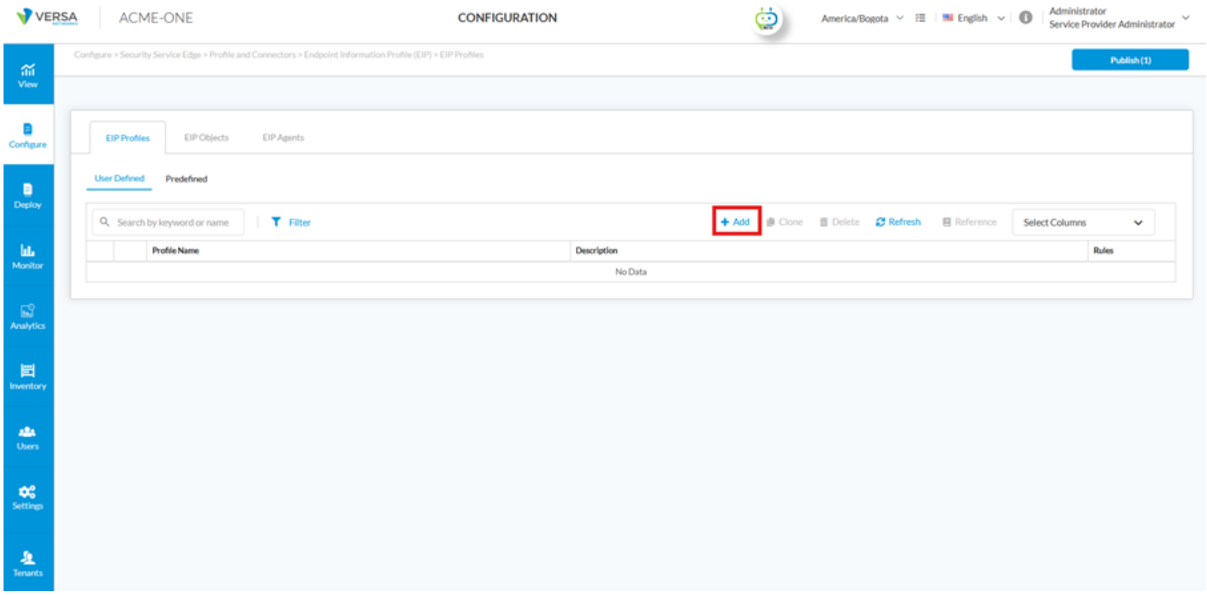
Patch

Step 3: Create an EIP Profile with Combined Posture Validation (Disk Encryption + Endpoint Security)

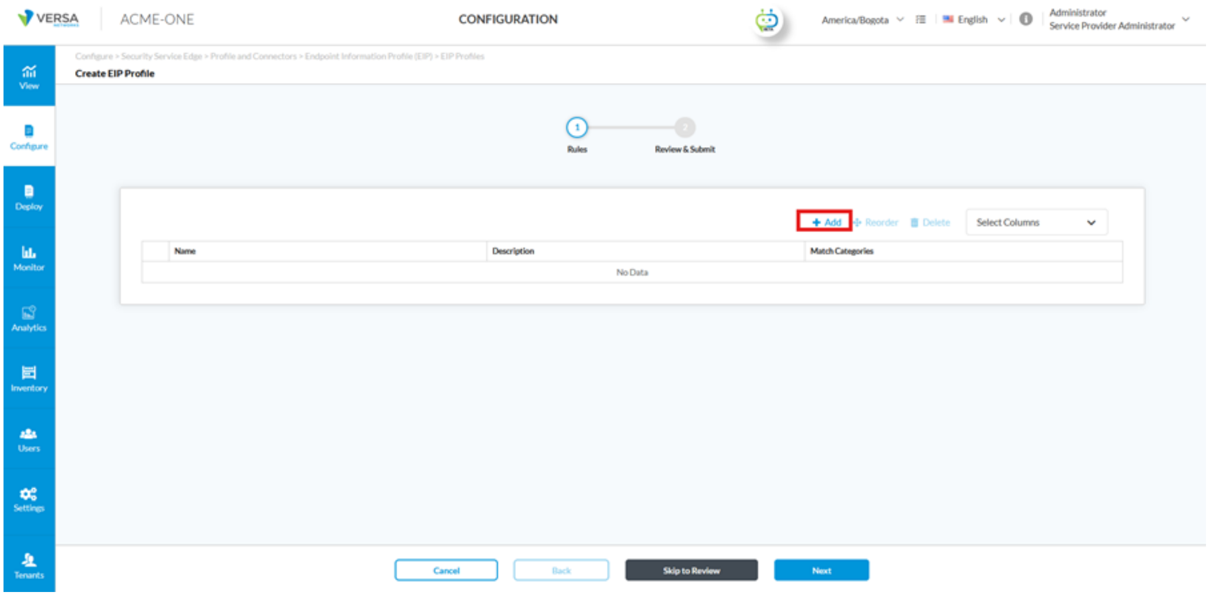
Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Profiles



Click on "+ Add" to start creating a new profile.



In the **Create EIP Profile** window, Click on "+ Add" to define a new rule.



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Create EIP Profile

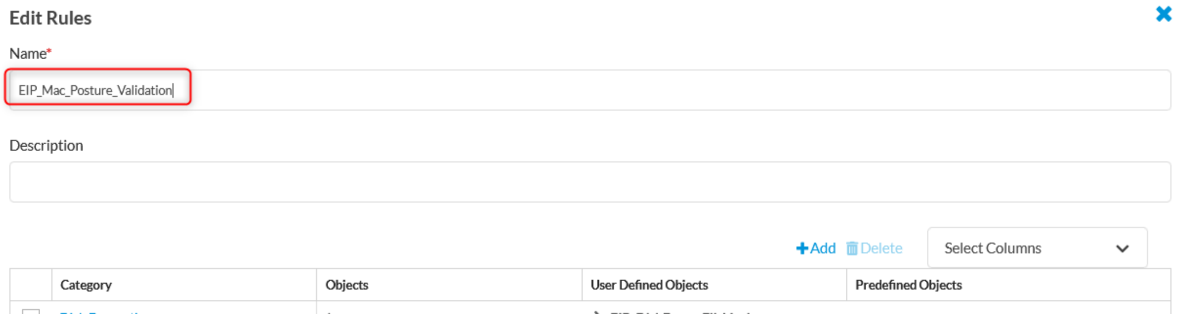
	Name	Description	Match Categories
		No Data	

Create a Rule for Disk Encryption

Enter a Name for your rule, Example, EIP_DiskEncryption_FileVault.

 You would (Optional) Add a description for clarity.

Click “+ Add” to attach an EIP Object.



Edit Rules

Name*

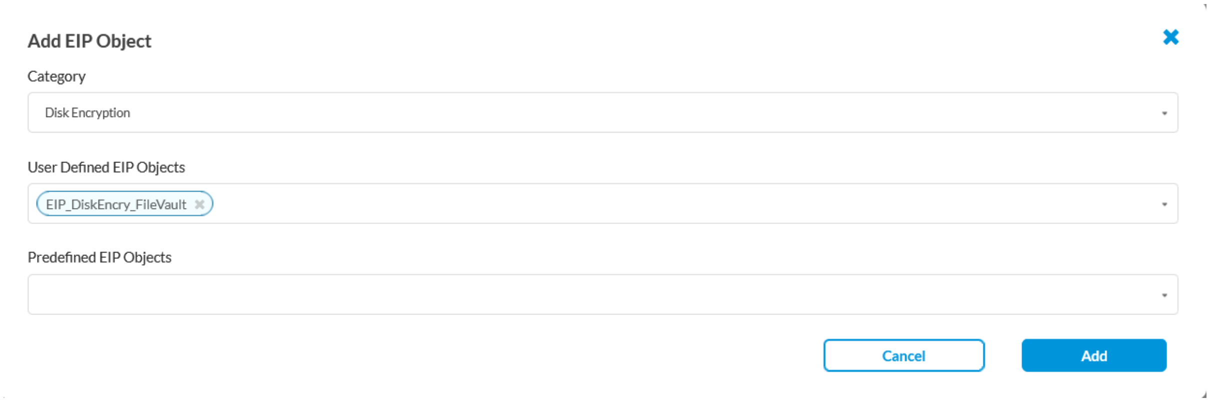
EIP_Mac_Posture_Validation

Description

	Category	Objects	User Defined Objects	Predefined Objects

In Add EIP Object dialog, choose the Category. Example **DiskEncryption**.

Select an existing EIP Object or create a new one. For example, an object was created to verify if MacOs DiskEncryption is installed, running and configured in the previous section.



Add EIP Object

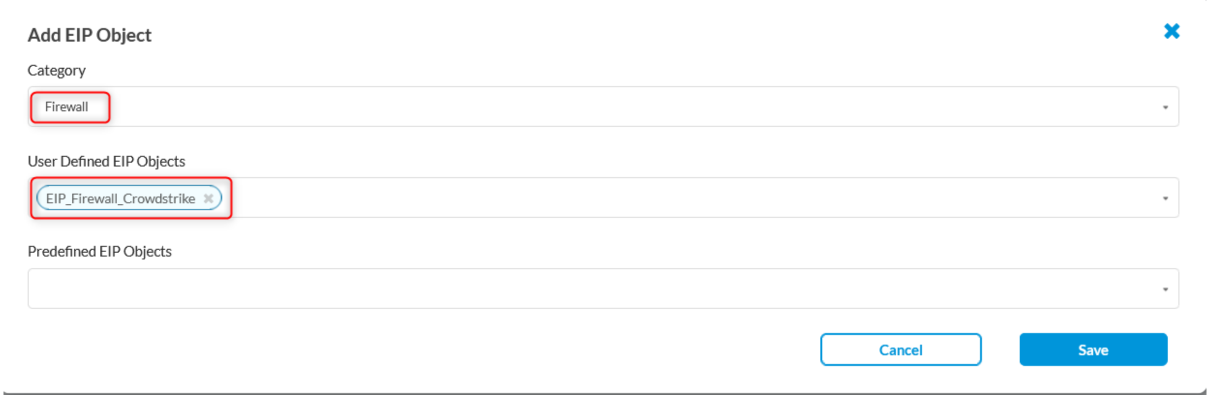
Category: Disk Encryption

User Defined EIP Objects: EIP_DiskEncry_FileVault

Predefined EIP Objects:

Now add other object **In Add EIP Object** dialog, choose the Category. Example **Firewall**.

Select a EIP Object for crowdstrike (“EIP_Firewall_Crowdstrike”). For example, this object verifies if Crowdstrike Falcon is installed, running, etc. Those steps explained in the previous section.



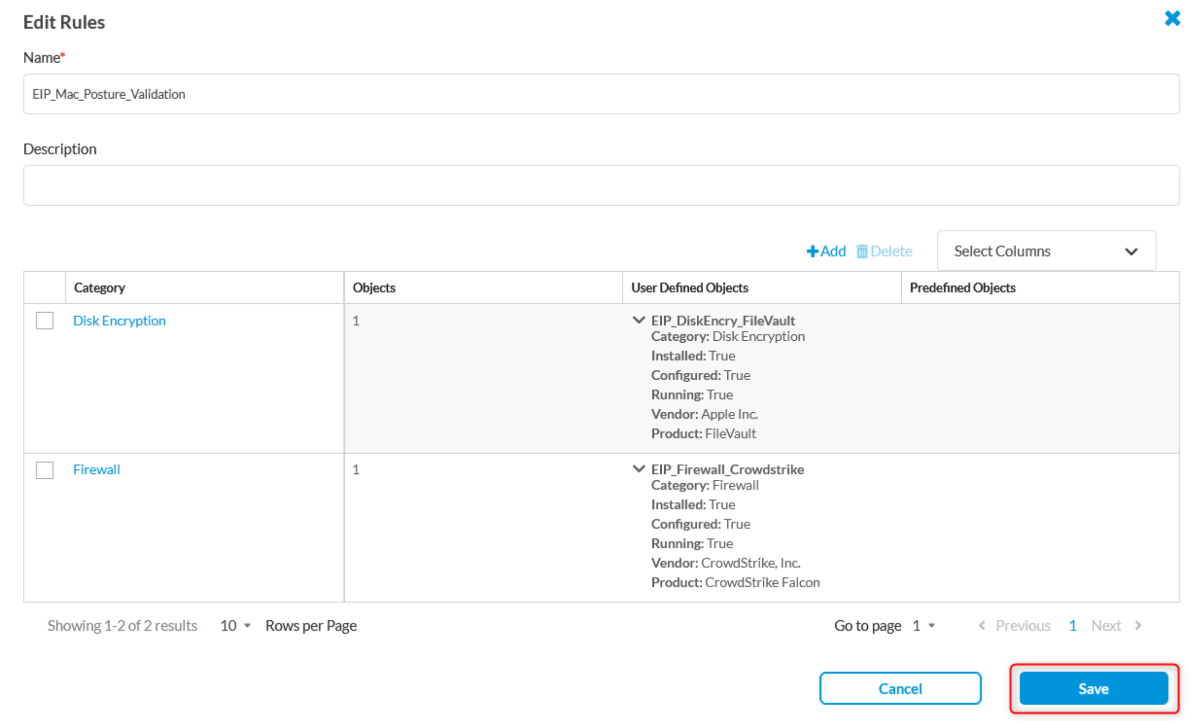
Add EIP Object

Category: Firewall

User Defined EIP Objects: EIP_Firewall_Crowdstrike

Predefined EIP Objects:

Now **Save** Rule



Edit Rules

Name*

EIP_Mac_Posture_Validation

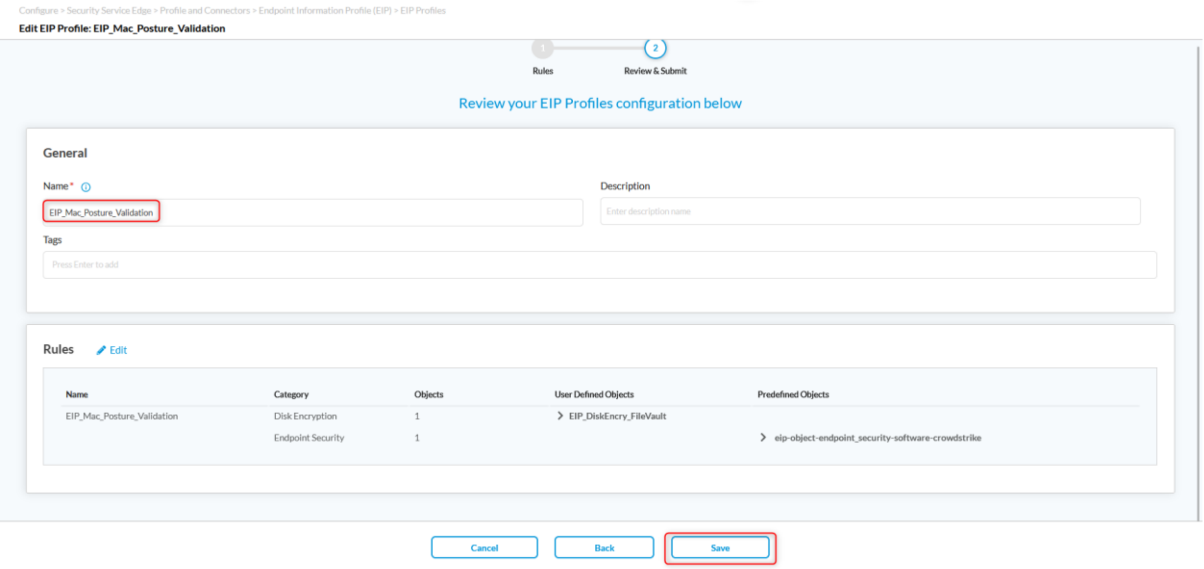
Description

	Category	Objects	User Defined Objects	Predefined Objects
□	Disk Encryption	1	EIP_DiskEncry_FileVault **Category:** Disk Encryption **Installed:** True **Configured:** True **Running:** True **Vendor:** Apple Inc. **Product:** FileVault	
□	Firewall	1	EIP_Firewall_Crowdstrike **Category:** Firewall **Installed:** True **Configured:** True **Running:** True **Vendor:** CrowdStrike, Inc. **Product:** CrowdStrike Falcon	

Showing 1-2 of 2 results 10 Rows per Page

Click **Next** and then Enter a descriptive name for your EIP object. ***Example:*** EIP_Mac_Posture_Validation**.**

Review and **Save** the Profile creation



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

Edit EIP Profile: EIP_Mac_Posture_Validation

Review your EIP Profiles configuration below

General

Name*: EIP_Mac_Posture_Validation

Description: Enter description name

Tags: Press Enter to add

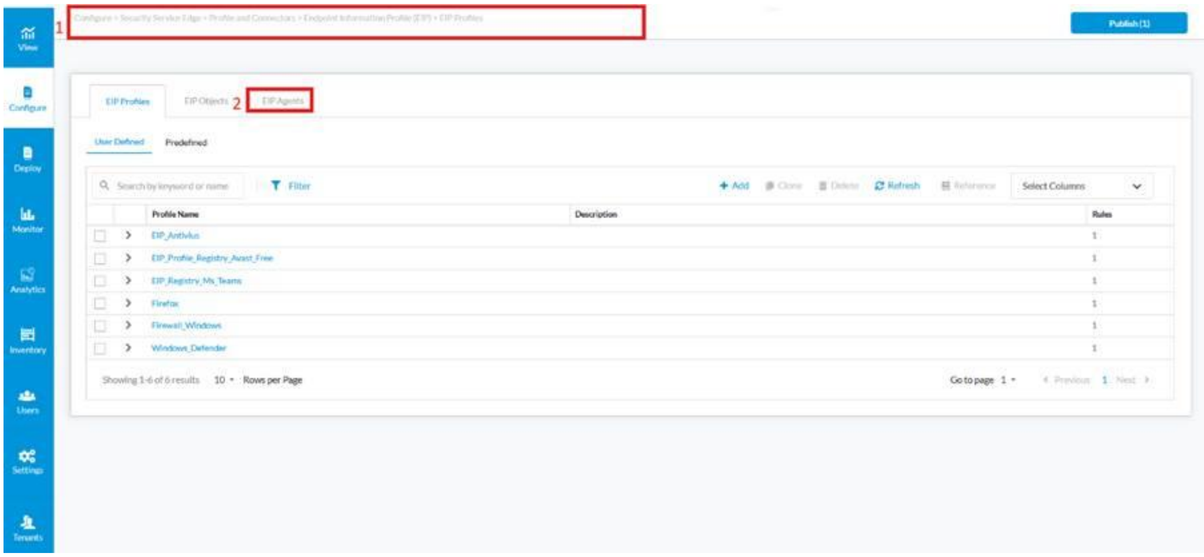
Rules

Name	Category	Objects	User Defined Objects	Predefined Objects
EIP_Mac_Posture_Validation	Disk Encryption	1	EIP_DiskEncry_FileVault	
	Endpoint Security	1		eip-object-endpoint_security-software-crowdstrike

Note: After creating the EIP Object and configuring the EIP Profile and Agent Profile, you must apply them to the Secure Access Client policy to enforce device posture validation and continue evaluation.

Step 4: Navigate to the EIP Agent Section

Navigate to Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles then go EIP Agents



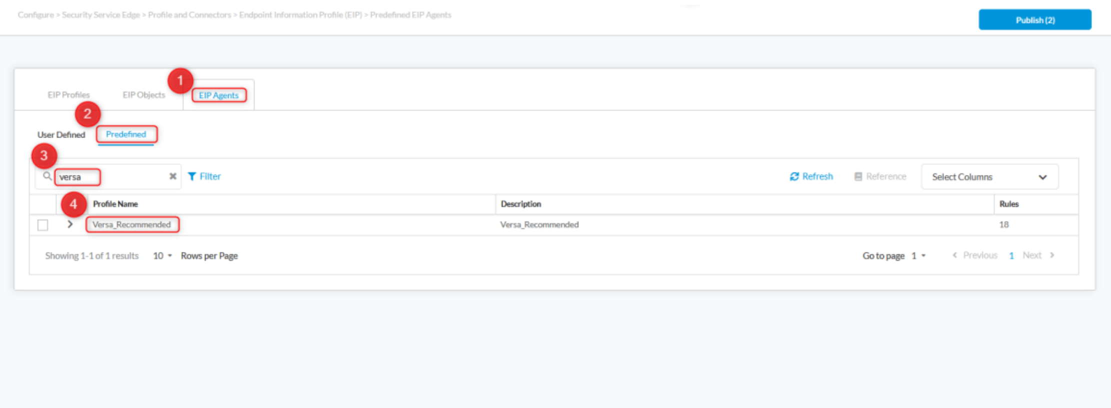
Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Profiles

		Profile Name	Description	Rules
□	›	EIP_Antivirus		1
□	›	EIP_Profile_Registry_Avast_Free		1
□	›	EIP_Registry_Ms_Teams		1
□	›	Firefox		1
□	›	Firewall_Windows		1
□	›	Windows_Defender		1

Showing 1-6 of 6 results 10 Rows per Page

Step 5: Create an EIP Agent Profile

Important Note: Instead of creating a new agent manually, you can also use a predefined Versa ***Versa_Recommend*** agent. In the *Predefined* tab, search for **Versa**. This option already includes baseline rules such as **Installed: True**, **Configured: True**, **etc**. for multiple categories and others.



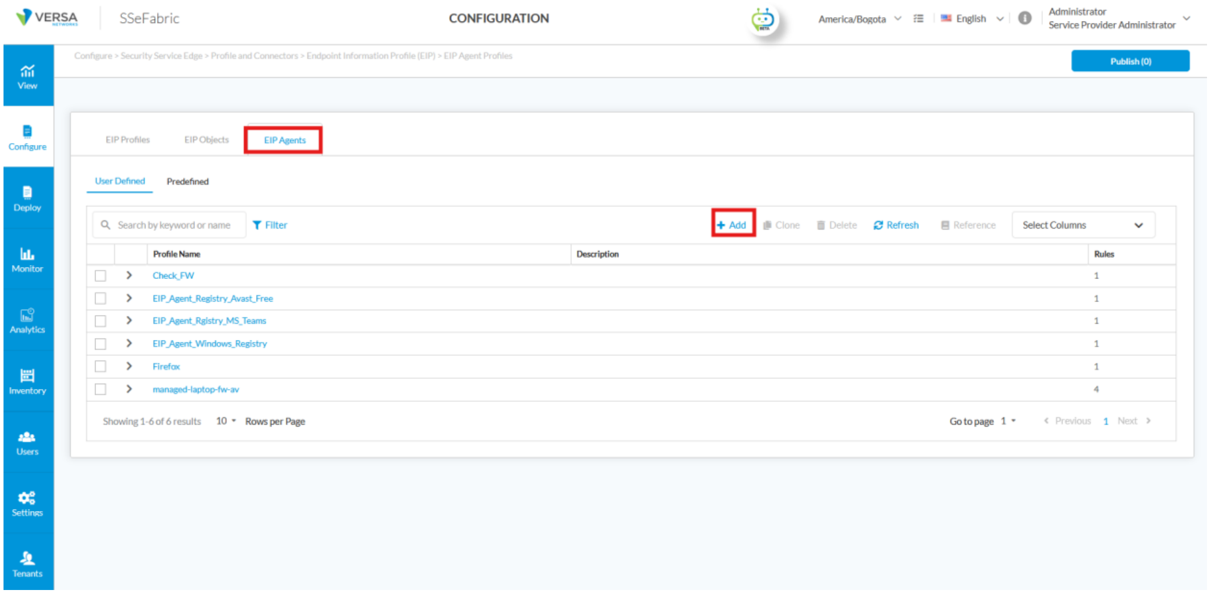
Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > Predefined EIP Agents

versa

		Profile Name	Description	Rules
□	›	Versa_Recommended	Versa_Recommended	18

Showing 1-1 of 1 results 10 Rows per Page

Click on **Add** to create a **new Agent profile**.

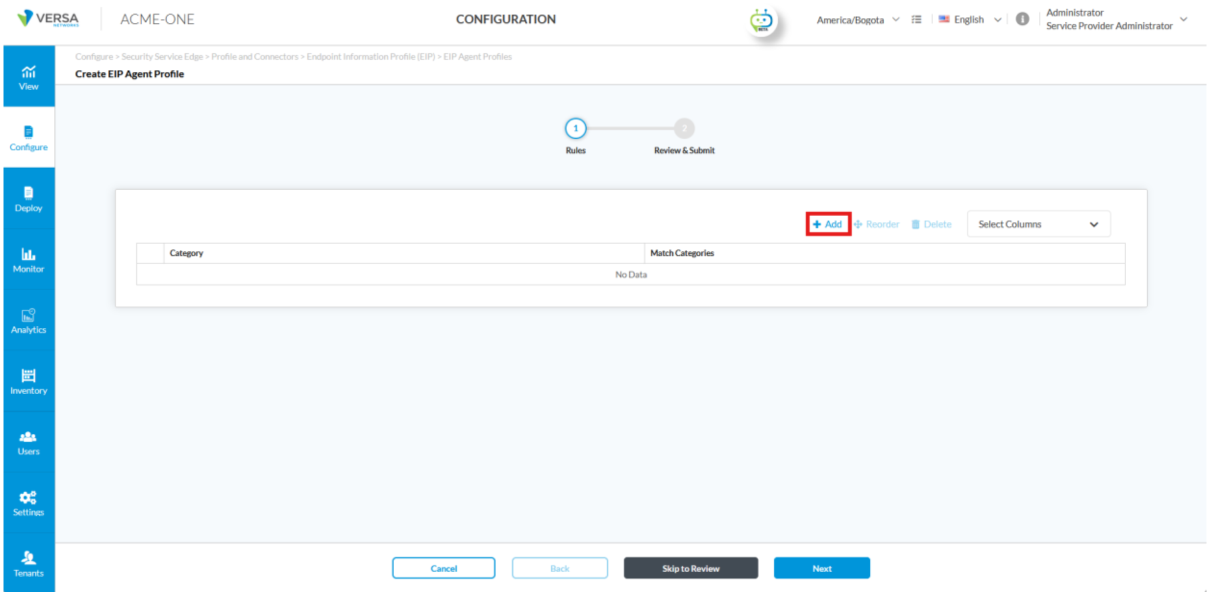


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Profile Name	Description	Rules
Check_FW		1
EIP_Agent_Registry_Avast_Free		1
EIP_Agent_Rgistry_MS_Teams		1
EIP_Agent_Windows_Registry		1
Firefox		1
managed-laptop-fw-av		4

Showing 1-6 of 6 results 10 Rows per Page Go to page 1 Previous 1 Next

Click on "+Add" to create a new rule. Then choose general



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

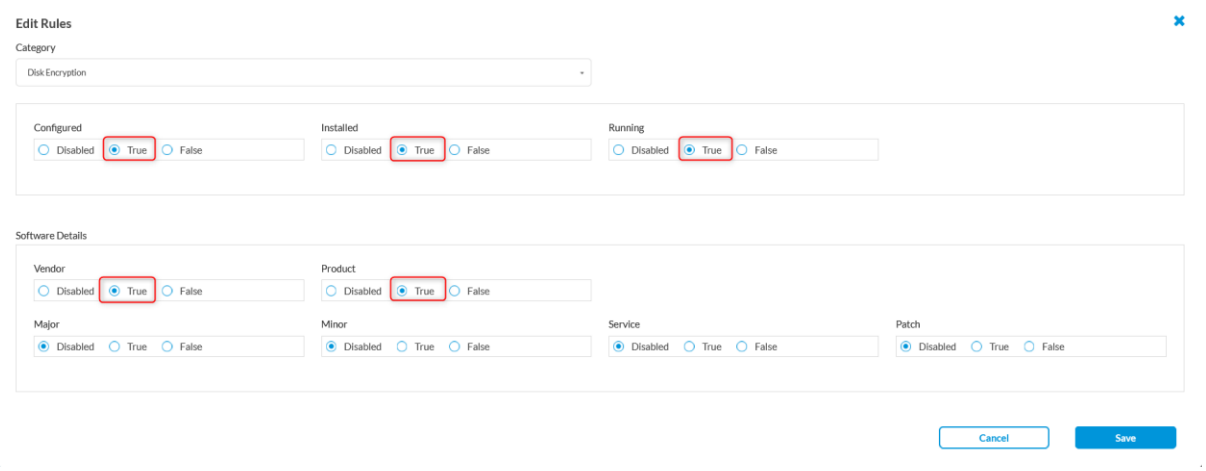
Create EIP Agent Profile

Category	Match Categories
No Data	

In the *Disk Encryption* category of the Agent Profile, configure the following options:

- Installed: True
- Configured: True
- Running: True
- Vendor True
- Product True

This configuration ensures that endpoints are validated for the presence and activity of disk encryption. Devices that fail any of these checks are flagged as non-compliant and may be restricted from accessing corporate resources.



Edit Rules

Category: Disk Encryption

Configured: ○ Disabled ● True ○ False

Installed: ○ Disabled ● True ○ False

Running: ○ Disabled ● True ○ False

Software Details

Vendor: ○ Disabled ● True ○ False

Product: ○ Disabled ● True ○ False

Major: ● Disabled ○ True ○ False

Minor: ● Disabled ○ True ○ False

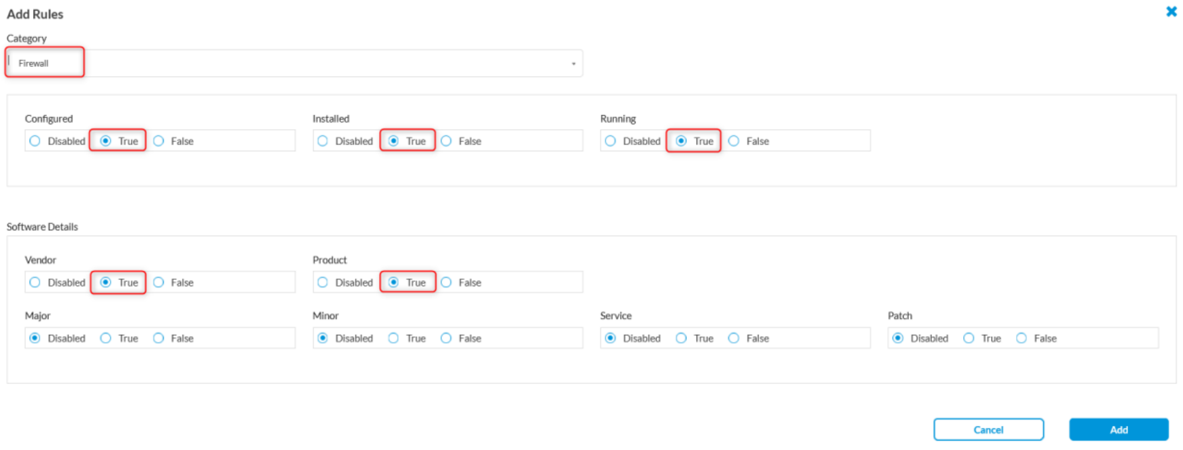
Service: ● Disabled ○ True ○ False

Patch: ● Disabled ○ True ○ False

Add another category, **Firewall** in the Agent Profile and configure the following options:

- Installed: True
- Configured: True
- Running: True
- Vendor: True
- Product: True

This configuration ensures that endpoints are validated for the presence and activity of the endpoint security agent. When combined with the **Disk Encryption** category, the EIP posture validation enforces that both FileVault disk encryption and the firewall solution (CrowdStrike Falcon) are active.



Add Rules

Category: Firewall

Configured: ○ Disabled ● True ○ False

Installed: ○ Disabled ● True ○ False

Running: ○ Disabled ● True ○ False

Software Details

Vendor: ○ Disabled ● True ○ False

Product: ○ Disabled ● True ○ False

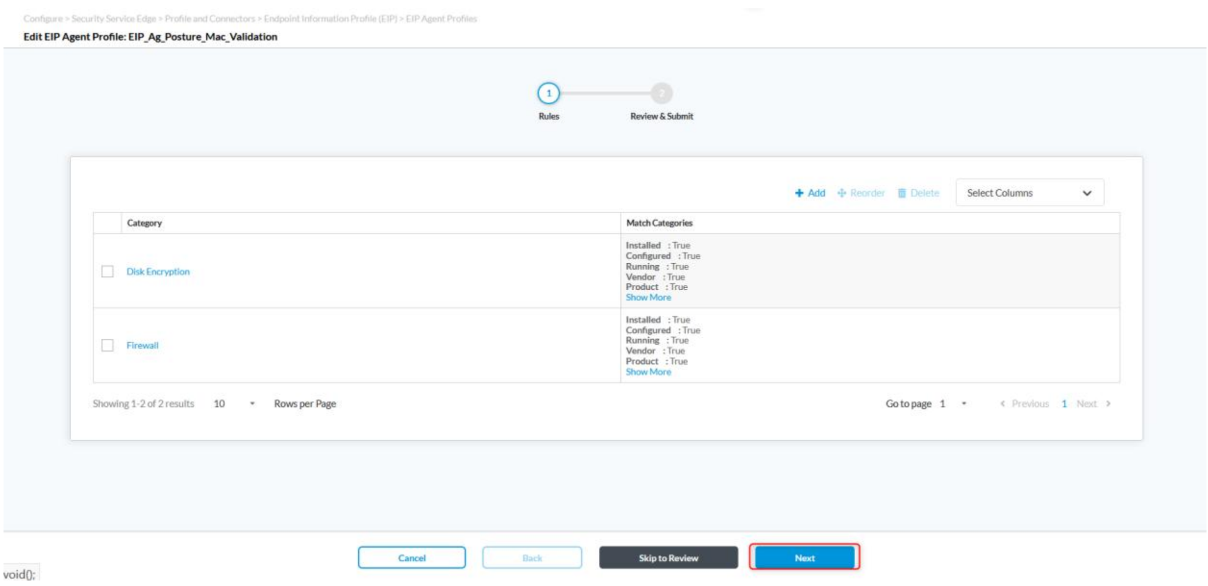
Major: ● Disabled ○ True ○ False

Minor: ● Disabled ○ True ○ False

Service: ● Disabled ○ True ○ False

Patch: ● Disabled ○ True ○ False

Click on “next” to enter a descriptive Profile Name (Example., **EIP_Ag_Posture_Mac_Validation**).

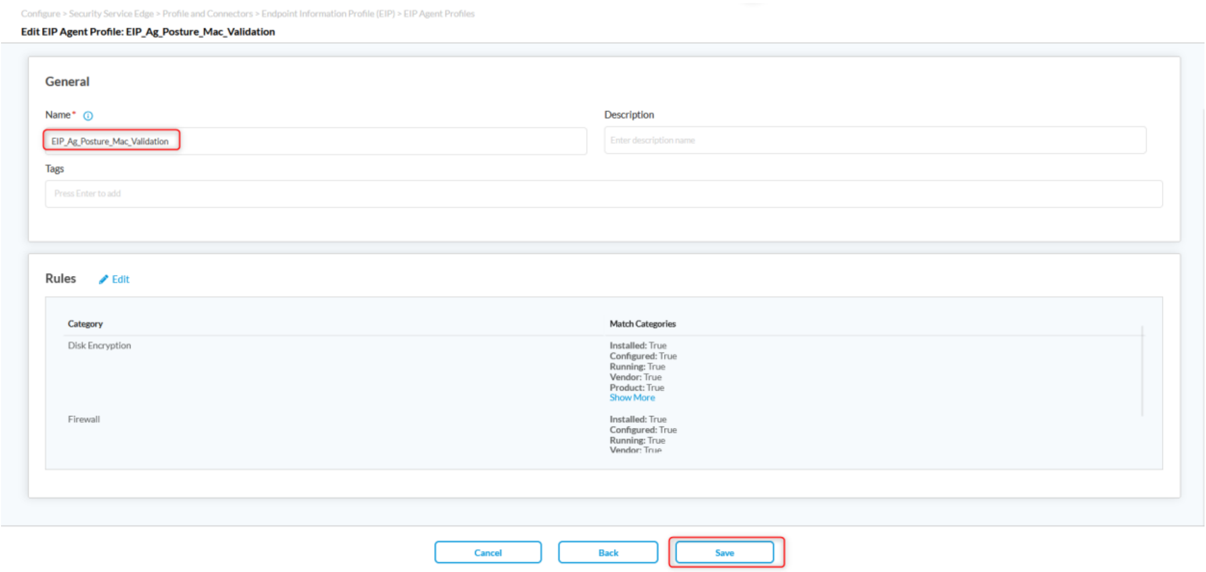


Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Edit EIP Agent Profile: EIP_Ag_Posture_Mac_Validation

	Category	Match Categories
□	Disk Encryption	Installed : True Configured : True Running : True Vendor : True Product : True Show More
□	Firewall	Installed : True Configured : True Running : True Vendor : True Product : True Show More

Showing 1-2 of 2 results 10 Rows per Page Go to page 1 Previous 1 Next



Configure > Security Service Edge > Profile and Connectors > Endpoint Information Profile (EIP) > EIP Agent Profiles

Edit EIP Agent Profile: EIP_Ag_Posture_Mac_Validation

General

Name*: EIP_Ag_Posture_Mac_Validation

Description: Enter description name

Tags: Press Enter to add

Rules

Category	Match Categories
Disk Encryption	Installed: True Configured: True Running: True Vendor: True Product: True Show More
Firewall	Installed: True Configured: True Running: True Vendor: True

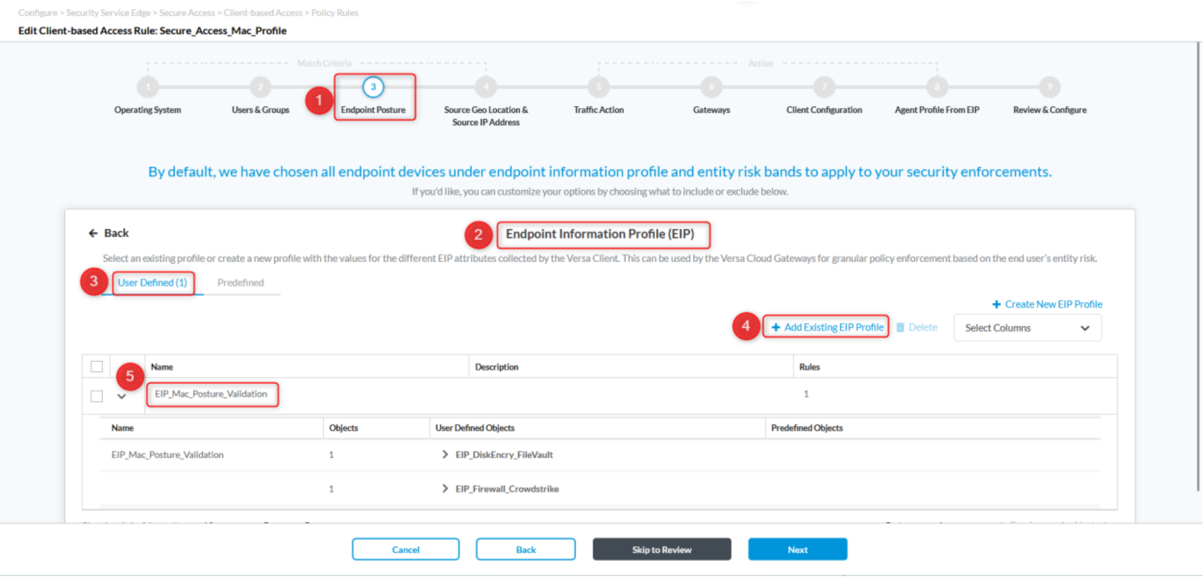
Step 6: Configure Secure Client Access Rule

Navigate to:

Configure > Security Service Edge > Secure Access > Client-based Access > Rules.

Click “**+ Add**” to create a new Secure Access Client rule or edit an existing rule.

In the Match Criteria configuration, go to the ***Endpoint Posture*** section. Under the *Endpoint Information Profile (EIP)* panel, select the desired profile by navigating to the ***User Defined*** tab and clicking on *Add Existing EIP Profile*. Then, choose the EIP profile you previously created. Example EIP_Mac_Posture_Validation).



Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure_Access_Mac_Profile

By default, we have chosen all endpoint devices under endpoint information profile and entity risk bands to apply to your security enforcements.

If you'd like, you can customize your options by choosing what to include or exclude below.

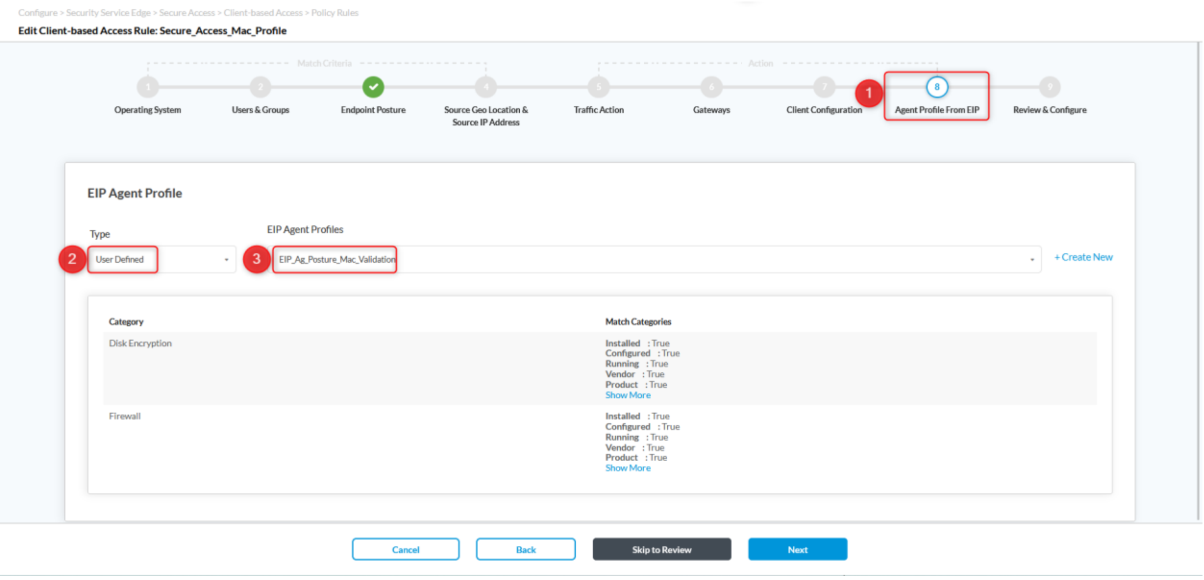
Endpoint Information Profile (EIP)

Select an existing profile or create a new profile with the values for the different EIP attributes collected by the Versa Client. This can be used by the Versa Cloud Gateways for granular policy enforcement based on the end user's entity risk.

Name	Description	Rules
EIP_Mac_Posture_Validation		1

Name	Objects	User Defined Objects	Predefined Objects
EIP_Mac_Posture_Validation	1	EIP_DiskEncry_FileVault	
	1	EIP_Firewall_Crowdstrike	

In action configuration, under the **Agent Profile From EIP** section, set the Type to **User Defined** and select the **EIP Agent Profile** you previously created. Example **EIP_Ag_Posture_Mac_Validation**. *The Match Categories panel will display the defined validation criteria, such as registry paths or process checks, ensuring that the selected EIP Agent Profile is applied for endpoint posture verification*.



Configure > Security Service Edge > Secure Access > Client-based Access > Policy Rules

Edit Client-based Access Rule: Secure_Access_Mac_Profile

EIP Agent Profile

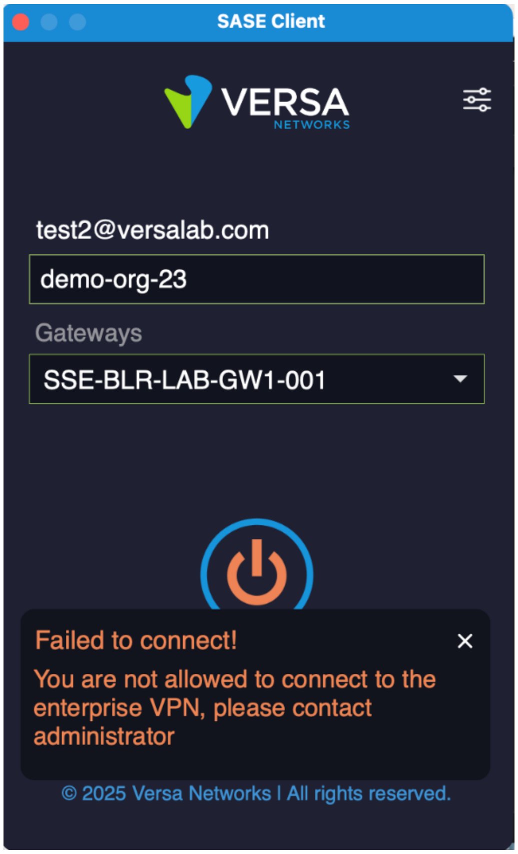
Type: User Defined

EIP Agent Profiles: EIP_Ag_Posture_Mac_Validation

Category	Match Categories
Disk Encryption	Installed : True Configured : True Running : True Vendor : True Product : True Show More
Firewall	Installed : True Configured : True Running : True Vendor : True Product : True Show More

Verification

At this time, the macOS device has FileVault disk encryption installed, configured; and running. When the Versa SASE Client attempts to connect, the authentication fails due to the EIP policy that requires Crowdstrike Falcon Firewall is running.



test2@versalab.com

demo-org-23

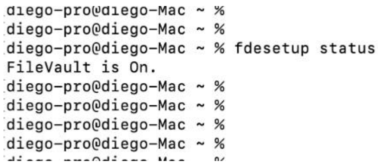
SSE-BLR-LAB-GW1-001

Failed to connect!
You are not allowed to connect to the enterprise VPN, please contact administrator

© 2025 Versa Networks | All rights reserved.

To confirm the posture on the endpoint, you would check whether FileVault is enabled and running by executing the following command in Terminal:

fdesetup status

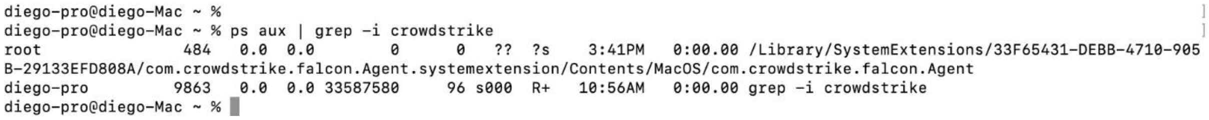


```
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ % fdesetup status
FileVault is On.
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
```

The command output shows that FileVault is active, which validates that disk encryption is running on the device. However, to verify Firewall (CrowdStrike Falcon:

- ps aux | grep -i crowdstrike

The command output shows that **CrowdStrike Falcon** agent is installed, however firewall feature is not running on the device.



```
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ % ps aux | grep -i crowdstrike
root               484   0.0  0.0        0      0   ??  ?s    3:41PM   0:00.00 /Library/SystemExtensions/33F65431-DEBB-4710-905
B-29133EFD808A/com.crowdstrike.falcon.Agent.systemextension/Contents/MacOS/com.crowdstrike.falcon.Agent
diego-pro         9863   0.0  0.0 33587580     96 s000  R+   10:56AM   0:00.00 grep -i crowdstrike
diego-pro@diego-Mac ~ % 
```

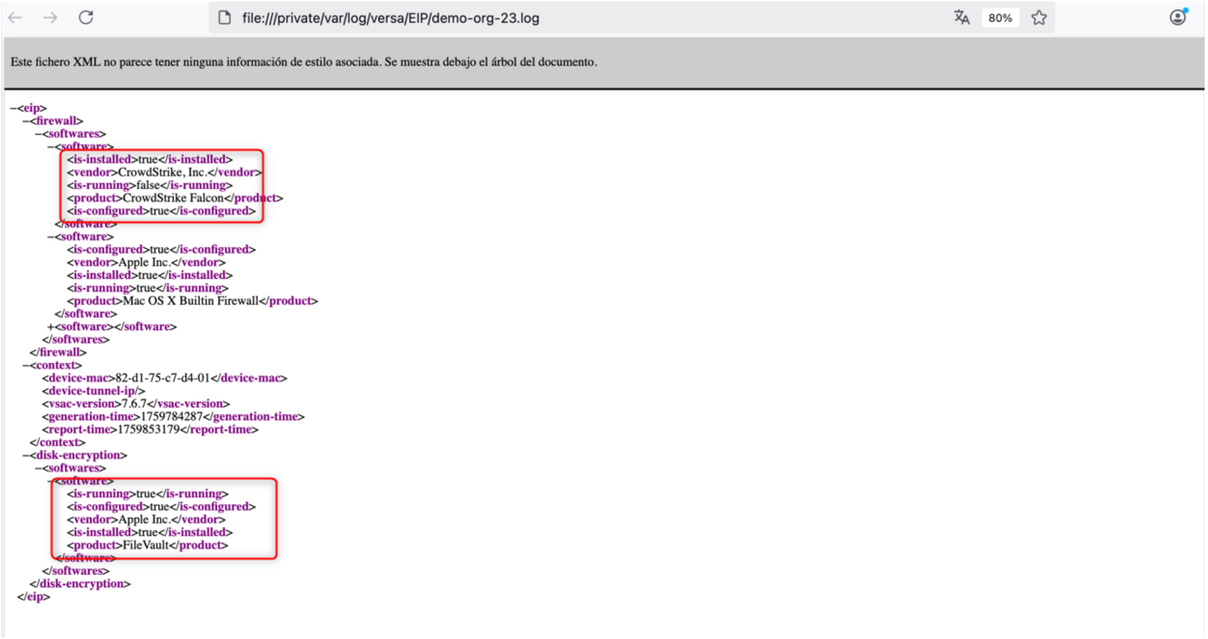
In addition, reviewing the EIP posture log collected from the device confirms that **FileVault disk encryption** is detected with the following attributes:

- **Vendor:** Apple Inc.
- Installed: True
- Configured: True
- Running: True

And that **CrowdStrike Falcon** as well is detected with the following attributes:

- Vendor: CrowdStrike.
- Installed: True
- Configured: True
- Running: False

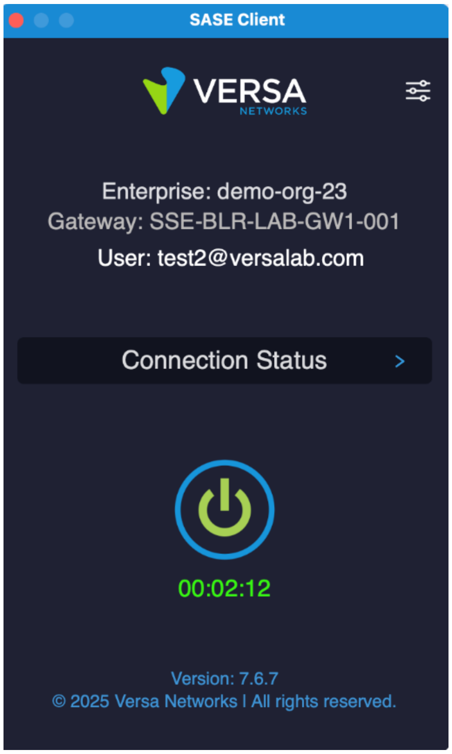
Logs show that **CrowdStrike Falcon** is installed. However, it is not running this means that while disk encryption is active and compliant, the firewall requirement is not met. As a result, the macOS device does not fully satisfy the EIP policy, since both controls — disk encryption and firewall — must be enabled to achieve compliance.



Este fichero XML no parece tener ninguna información de estilo asociada. Se muestra debajo el árbol del documento.

```
–<eip>
  –<firewall>
    –<softwares>
      –<software>
          <is-installed>true</is-installed>
          <vendor>CrowdStrike, Inc.</vendor>
          <is-running>false</is-running>
          <product>CrowdStrike Falcon</product>
          <is-configured>true</is-configured>
        </software>
      –<software>
          <is-configured>true</is-configured>
          <vendor>Apple Inc.</vendor>
          <is-installed>true</is-installed>
          <is-running>true</is-running>
          <product>Mac OS X Builtin Firewall</product>
        </software>
      +<software></software>
      </softwares>
    </firewall>
  –<context>
      <device-mac>82-d1-75-c7-d4-01</device-mac>
      <device-tunnel-ip/>
      <vsac-version>7.6.7</vsac-version>
      <generation-time>1759784287</generation-time>
      <report-time>1759853179</report-time>
    </context>
  –<disk-encryption>
    –<softwares>
      –<software>
          <is-running>true</is-running>
          <is-configured>true</is-configured>
          <vendor>Apple Inc.</vendor>
          <is-installed>true</is-installed>
          <product>FileVault</product>
        </software>
      </softwares>
    </disk-encryption>
  </eip>
```

After enabling Firewall **Crowdstrike Falcon** and it is running, the Versa SASE Client is able to authenticate successfully and establish a secure connection to the enterprise VPN.

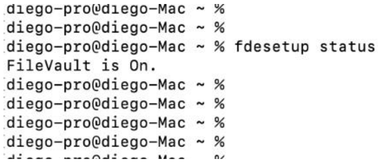


Enterprise: demo-org-23
Gateway: SSE-BLR-LAB-GW1-001
User: test2@versalab.com

Version: 7.6.7
© 2025 Versa Networks I All rights reserved.

To confirm the posture on the endpoint, you would check again whether **FileVault** disk encryption is enabled and running by executing the following command in Terminal:

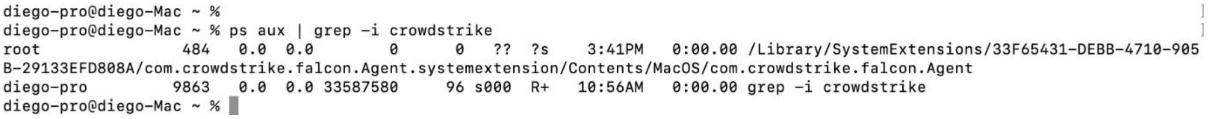
fdesetup status



```
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ % fdesetup status
FileVault is On.
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ %
```

The command output shows **"FileVault is On"**, which validates that disk encryption is enabled and actively protecting the macOS device.

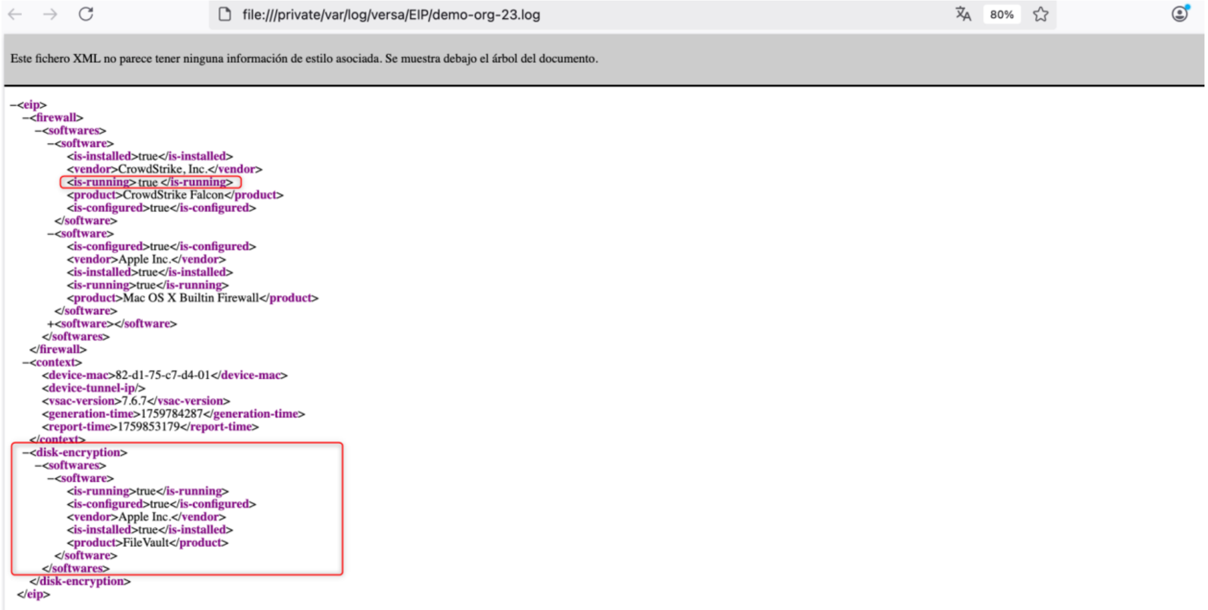
And to confirm if CrowdStrike Falcon is installed ps aux | grep -i crowdstrike



```
diego-pro@diego-Mac ~ %
diego-pro@diego-Mac ~ % ps aux | grep -i crowdstrike
root               484   0.0  0.0        0      0   ??  ?s    3:41PM   0:00.00 /Library/SystemExtensions/33F65431-DEBB-4710-905
B-29133EFD808A/com.crowdstrike.falcon.Agent.systemextension/Contents/MacOS/com.crowdstrike.falcon.Agent
diego-pro         9863   0.0  0.0 33587580     96 s000  R+   10:56AM   0:00.00 grep -i crowdstrike
diego-pro@diego-Mac ~ %
```

The command output shows that **CrowdStrike Falcon** agent is installed and actively protecting the macOS device.

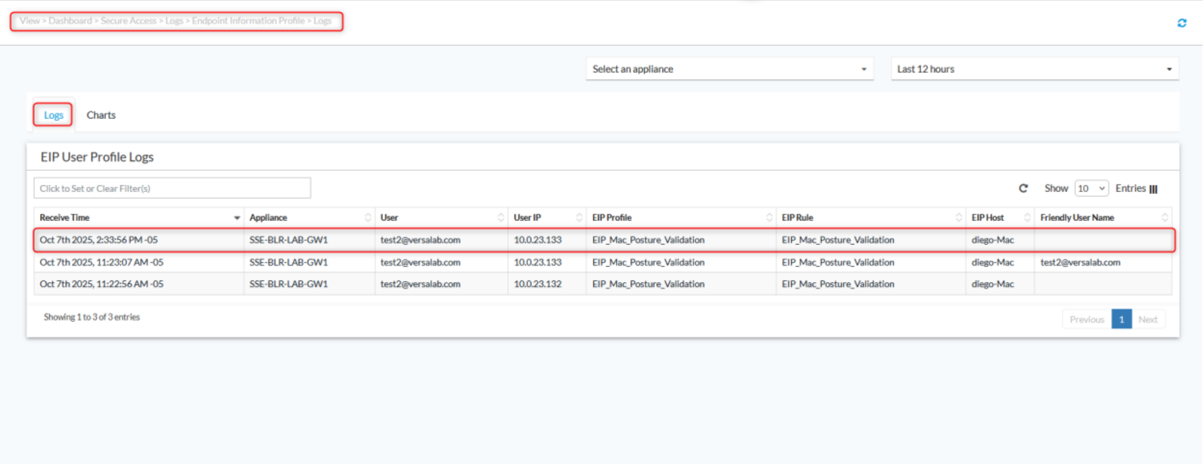
You are able to check the disk encryption and firewall status directly in the EIP posture logs located under /private/var/log/versa/EIP/demo-org-23.log.



Este fichero XML no parece tener ninguna información de estilo asociada. Se muestra debajo el árbol del documento.

```
−<eip>
  −<firewall>
    −<softwares>
      −<software>
          <is-installed>true</is-installed>
          <vendor>CrowdStrike, Inc.</vendor>
          <is-running> true </is-running>
          <product>CrowdStrike Falcon</product>
          <is-configured>true</is-configured>
        </software>
      −<software>
          <is-configured>true</is-configured>
          <vendor>Apple Inc.</vendor>
          <is-installed>true</is-installed>
          <is-running>true</is-running>
          <product>Mac OS X Builtin Firewall</product>
        </software>
      +<software></software>
      </softwares>
    </firewall>
  −<context>
      <device-mac>82-d1-75-c7-d4-01</device-mac>
      <device-tunnel-ip/>
      <vsac-version>7.6.7</vsac-version>
      <generation-time>1759784287</generation-time>
      <report-time>1759853179</report-time>
    </context>
  −<disk-encryption>
    −<softwares>
      −<software>
          <is-running>true</is-running>
          <is-configured>true</is-configured>
          <vendor>Apple Inc.</vendor>
          <is-installed>true</is-installed>
          <product>FileVault</product>
        </software>
      </softwares>
    </disk-encryption>
 </eip>
```

You check the Concerto logs to validate that the EIP authentication profile matches the expected profile. In Concerto From the log view (**View > Dashboard > Secure Access > Logs > Endpoint Information Profile > Logs**).



View > Dashboard > Secure Access > Logs > Endpoint Information Profile > Logs
Select an appliance
Last 12 hours
Logs
Charts
Click to Set or Clear Filter(s)
Show 10 Entries
Previous
1
Next

EIP User Profile Logs

Receive Time	Appliance	User	User IP	EIP Profile	EIP Rule	EIP Host	Friendly User Name
Oct 7th 2025, 2:33:56 PM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.133	EIP_Mac_Posture_Validation	EIP_Mac_Posture_Validation	diego-Mac	
Oct 7th 2025, 11:23:07 AM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.133	EIP_Mac_Posture_Validation	EIP_Mac_Posture_Validation	diego-Mac	test2@versalab.com
Oct 7th 2025, 11:22:56 AM -05	SSE-BLR-LAB-GW1	test2@versalab.com	10.0.23.132	EIP_Mac_Posture_Validation	EIP_Mac_Posture_Validation	diego-Mac	

Showing 1 to 3 of 3 entries

Entry show that the endpoint matches the **EIP_Mac_Posture_Validation** profile and rule after DiskEncryption and Firewall are running. The appliance, user, and host details confirm that the macOS device, associated with user, is evaluated against the correct profile. This confirms that the endpoint is recognized as compliant, the EIP profile and rule are enforced, and secure access is granted according to the posture policy.

About Versa

Versa, the global leader in SASE, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE Platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while delivering a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users, trust Versa with their mission critical networks and security. Versa is privately held and funded by investors such as Sequoia Capital, Mayfield, and BlackRock. For more information, visit https://www.versa-networks.com and follow Versa on LinkedIn and X (Twitter) @versanetworks.