# Troubleshoot Endpoint Information Profiles

Enterprise users can connect to networks and resources from a variety of locations and using a variety of endpoints, or remote computing devices. To protect the enterprise network and resources, you can create endpoint information profiles (EIPs). EIPs ensure that the endpoint devices accessing the enterprise network maintain and adhere to enterprise security standards. For more information about configuring EIP, see Configure Endpoint Information Profiles.

## Reregister Versa SASE Client

You must reregister the Versa SASE client in the following scenarios if you make any changes to an EIP agent profile:

- When you update an EIP agent profile associated with an SCA policy rule. For example, if you change a predefined EIP agent profile to a user-defined EIP agent profile in an SCA rule.
- When you update any EIP objects within a user-defined EIP agent profile. For example, if you add the AntiMalware_category_vendor to an existing user-defined EIP agent profile.
- If you update any rules of an existing user-defined EIP object. For example, if you amend the match criteria of Configured from disabled to true.

The Versa SASE client automatically reregisters at the end of Portal lifetime. To reregister the Versa SASE client manually, select Settings > *[tenant_name]* > Reregister.

## Amending the Welcome Message

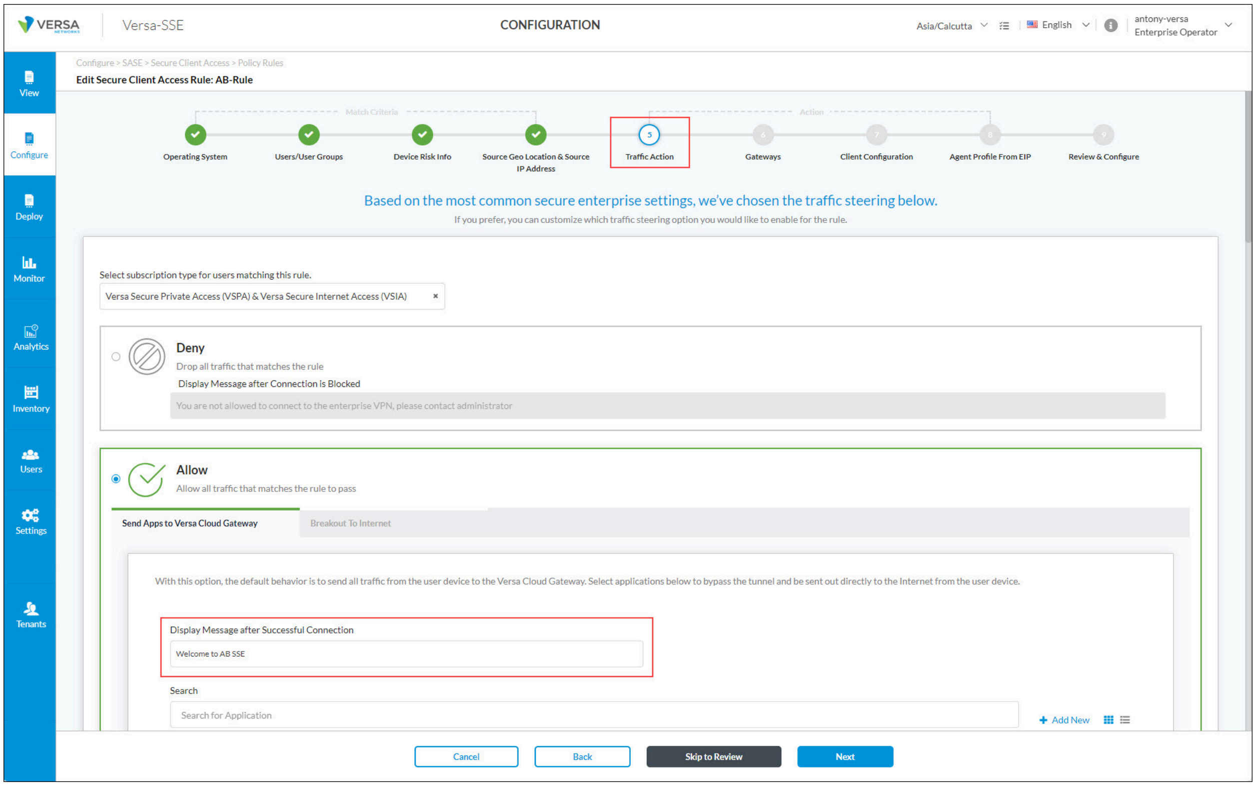
To troubleshoot EIP, you can include a reference to the SCA policy rule name in the welcome message that displays when the Versa SASE client connects to the Versa portal or Versa SASE gateway. You do this by amending the default welcome message when you configure an SCA policy rule. The default welcome message format is Welcome to <*tenant name*>. For example, if the default message is Welcome to Versa-SSE, you update the default message to Welcome to Versa-SSE (SWG_Demo), where SWG_Demo refers to the name of the matched SCA policy rule. When an enterprise device connects to the Versa SASE client, the welcome banner displays which SCA policy rule the end device matched.

Note that EIP information is used as a match criteria only when Versa SASE client connects to Versa gateways. Therefore, for troubleshooting purposes, focus on the welcome message when connecting to the Versa SASE gateway.

To update the welcome message with the SCA policy rule name:

1. Go to Configure > Secure Services Edge > Secure Access Client > Policy Rules.
2. Select the secure client access rule.
3. In the Edit Secure Client Access Rule page, select Traffic Action, and then add the SCA policy rule name to the

default text in the Display Message after Successful Connection field.



Configure > SASE > Secure Client Access > Policy Rules

Edit Secure Client Access Rule: AB-Rule

Based on the most common secure enterprise settings, we've chosen the traffic steering below.

If you prefer, you can customize which traffic steering option you would like to enable for the rule.

Select subscription type for users matching this rule.

Versa Secure Private Access (VSPA) & Versa Secure Internet Access (VSIA) ×

○ Deny

Drop all traffic that matches the rule

Display Message after Connection is Blocked

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

● Allow

Allow all traffic that matches the rule to pass

With this option, the default behavior is to send all traffic from the user device to the Versa Cloud Gateway. Select applications below to bypass the tunnel and be sent out directly to the Internet from the user device.

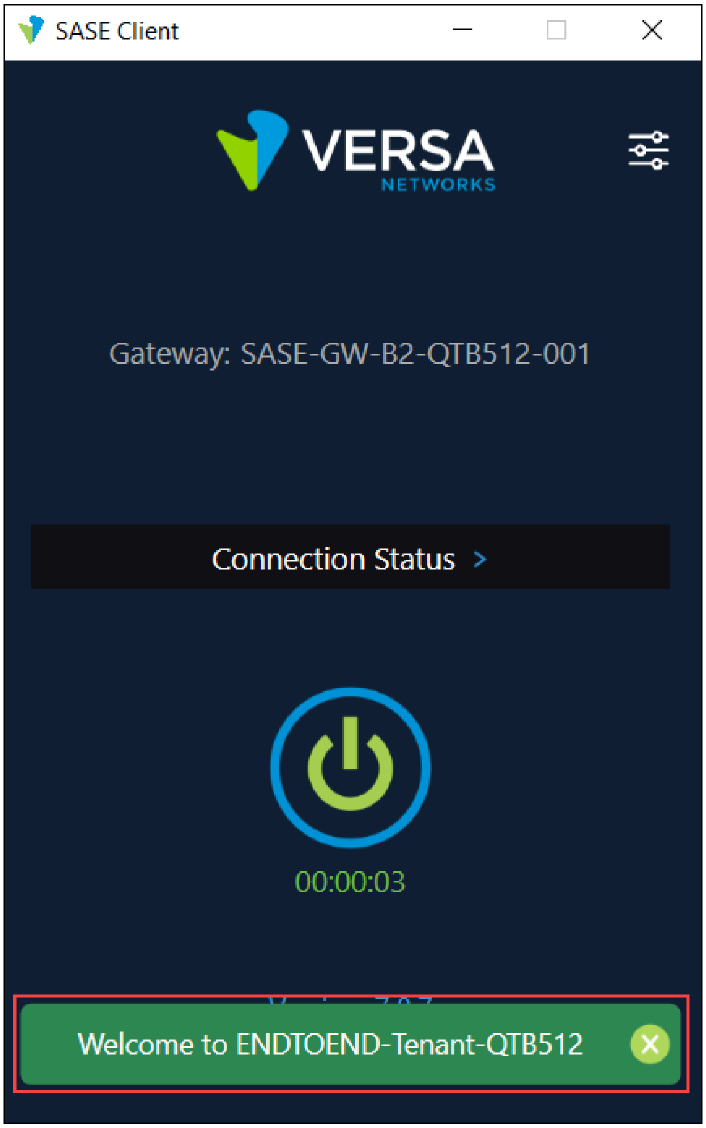
Display Message after Successful Connection

Welcome to AB SSE

Search

Search for Application

The Welcome message displays when the Versa SASE client connects to the Versa portal or Versa SASE gateway:



Gateway: SASE-GW-B2-QTB512-001

Welcome to ENDTOEND-Tenant-QTB512

# Troubleshoot EIP Profiles Using Site-to-Site Monitor

## View EIP Cache Information

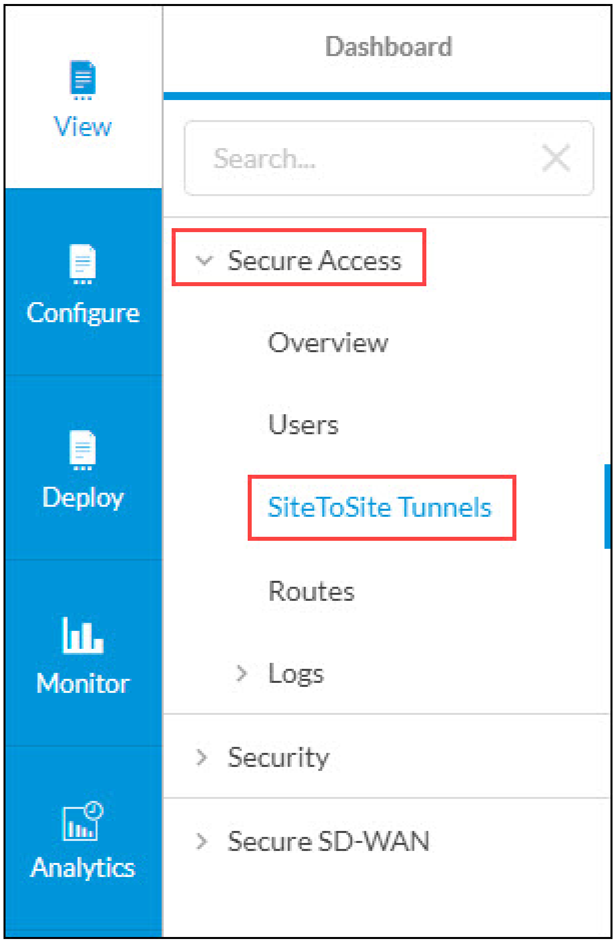
With EIPs, you collect information about the security status of the endpoint devices connecting to your networks. You then classify the endpoints based on multiple types of endpoint posture information, defining rules that allow the VOS SSE software to extract information from endpoint devices and then match the information to enforce security policy.

If you want to use EIP cache information to troubleshoot EIP, you must configure an EIP agent profile in the corresponding secure client access (SCA) for the entity and associate the EIP agent profile to an SCA rule. You configure an EIP agent profile that defines when the SSE client must extract information from endpoint devices. You associate predefined or custom EIP agent profiles with SCA rules to enforce EIP security. When you associate an EIP agent profile to an SCA policy, the entity gathers EIP information and sends it to the SSE gateway. The EIP cache information is populated with device posture details after you configure an EIP agent profile and associate it to an SCA rule. If EIP cache information is not available, check if an EIP agent profile is associated with the SCA policy.

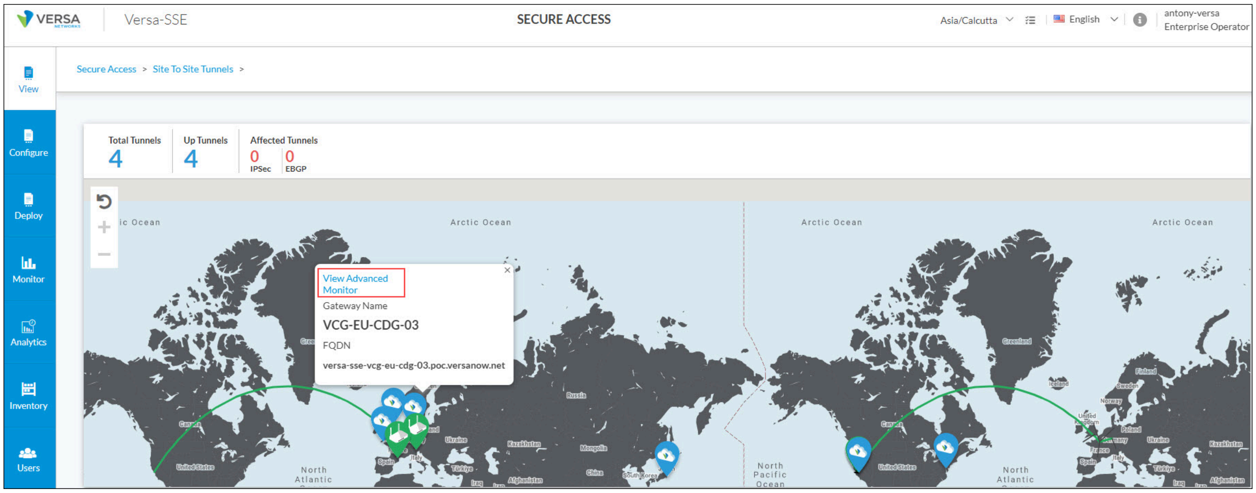
An entity can match a single EIP profile or multiple EIP profiles. By matching multiple EIP profiles, entities can be permitted or denied based on simple or complex EIP profile information. For example, all entities with Chrome installed may access the internet. However, only entities with disk encryption, anti-malware software and Chrome may access an intranet website. In this example, if an entity matches both EIP profiles, a private app protection rule can be created to match the more complex EIP profile, whereas an internet protection rule can be created to match the simple EIP profile.

To view EIP cache information:

1. Select View > Secure Access > Site-to-Site Tunnels.



2. From the list of available SSE gateways, select the SSE gateway the entity is connecting to, and then click View Advanced Monitor.

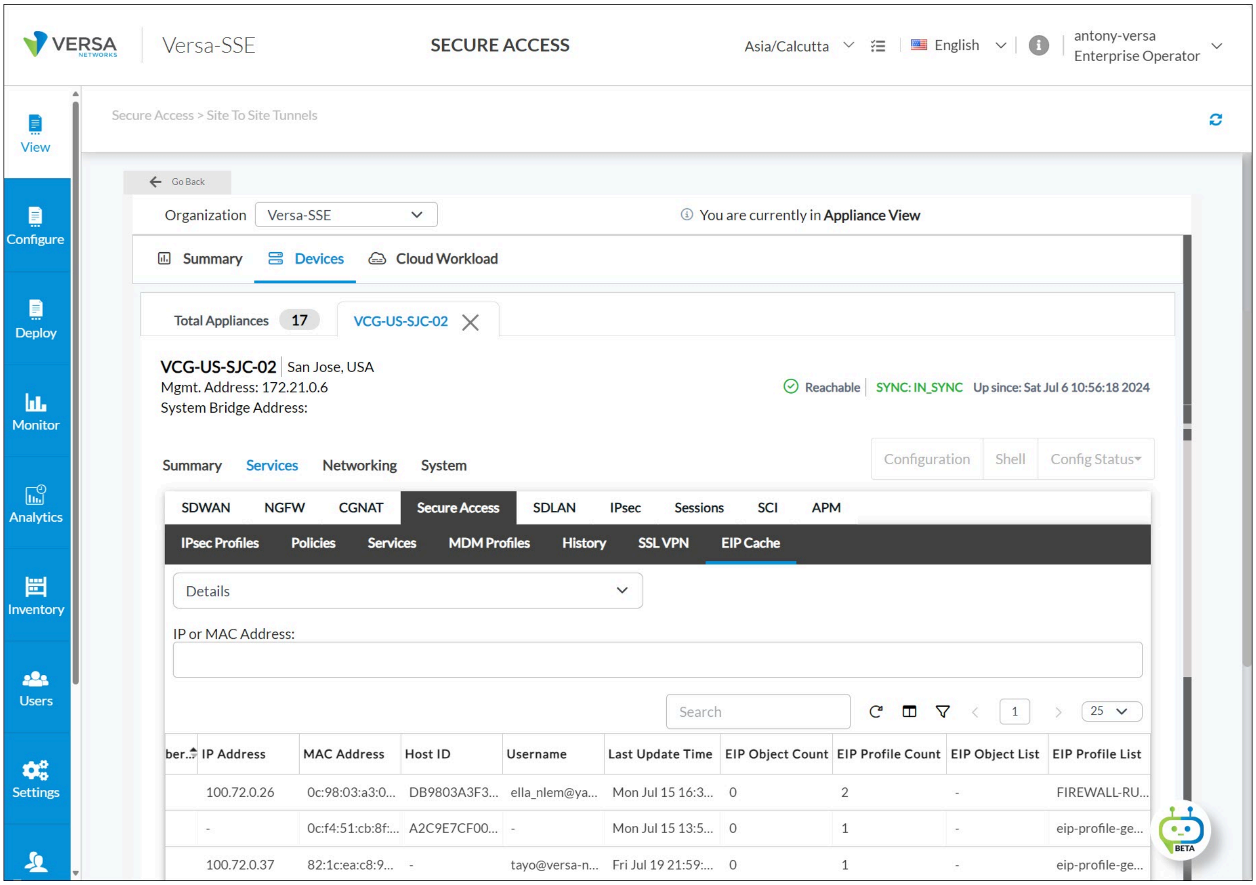


Total Tunnels 4 | Up Tunnels 4 | Affected Tunnels 0 IPSec 0 EBGP

Gateway Name: VCG-EU-CDG-03

FQDN: versa-sse-vcg-eu-cdg-03.poc.versanow.net

3. In the Devices > Services tab, select the Secure Access > EIP Cache tab.



Organization: Versa-SSE

You are currently in Appliance View

Total Appliances 17 | VCG-US-SJC-02

VCG-US-SJC-02 | San Jose, USA
Mgmt. Address: 172.21.0.6
System Bridge Address:

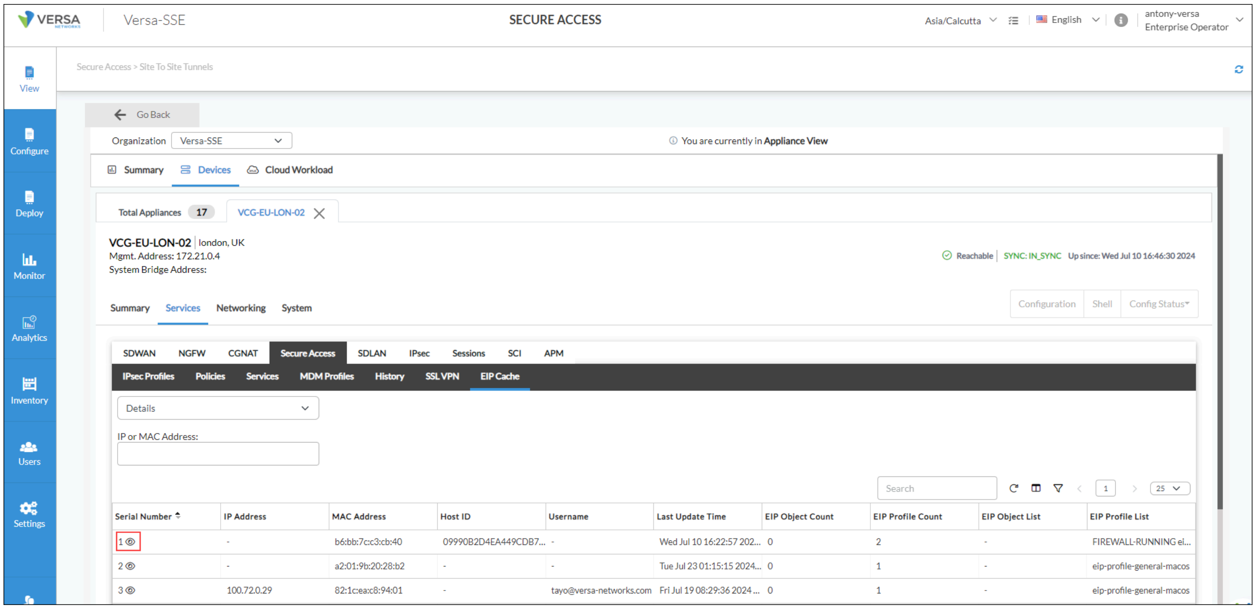
Reachable | SYNC: IN_SYNC | Up since: Sat Jul 6 10:56:18 2024

Details

IP or MAC Address:

| ber... | IP Address | MAC Address | Host ID | Username | Last Update Time | EIP Object Count | EIP Profile Count | EIP Object List | EIP Profile List |
|---|---|---|---|---|---|---|---|---|---|
| | 100.72.0.26 | 0c:98:03:a3:0... | DB9803A3F3... | ella_nlem@ya... | Mon Jul 15 16:3... | 0 | 2 | - | FIREWALL-RU... |
| | - | 0c:f4:51:cb:8f:... | A2C9E7CF00... | - | Mon Jul 15 13:5... | 0 | 1 | - | eip-profile-ge... |
| | 100.72.0.37 | 82:1c:ea:c8:9... | - | tayo@versa-n... | Fri Jul 19 21:59:... | 0 | 1 | - | eip-profile-ge... |

4. In the Serial Number column, click the ◎ Eye icon to view the EIP information that the entity sends to the SSE gateway.



Organization Versa-SSE

You are currently in **Appliance View**

VCG-EU-LON-02 | london, UK
Mgmt. Address: 172.21.0.4
System Bridge Address:

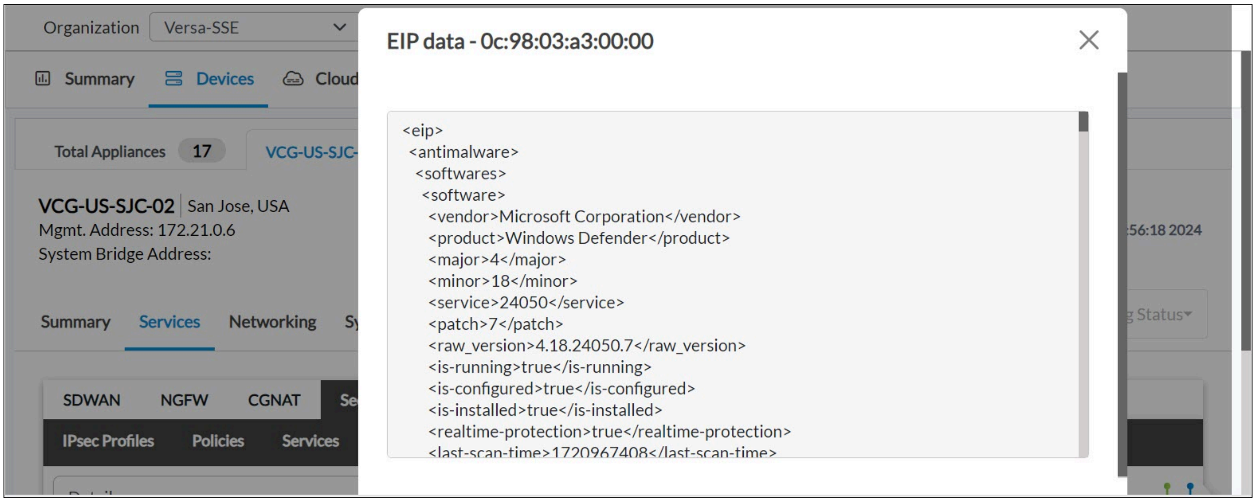
Reachable | SYNC: IN_SYNC Up since: Wed Jul 10 16:46:30 2024

Details

IP or MAC Address:

| Serial Number | IP Address | MAC Address | Host ID | Username | Last Update Time | EIP Object Count | EIP Profile Count | EIP Object List | EIP Profile List |
|---|---|---|---|---|---|---|---|---|---|
| 1 | - | b6:bb:7c:c3:cb:40 | 09990B2D4EA449CDB7... | - | Wed Jul 10 16:22:57 202... | 0 | 2 | - | FIREWALL-RUNNING ei... |
| 2 | - | a2:01:9b:20:28:b2 | - | - | Tue Jul 23 01:15:15 2024... | 0 | 1 | - | eip-profile-general-macos |
| 3 | 100.72.0.29 | 82:1c:ea:c8:94:01 | - | tayo@versa-networks.com | Fri Jul 19 08:29:36 2024 ... | 0 | 1 | - | eip-profile-general-macos |

The following screenshot shows the EIP cache information for the selected entity.



VCG-US-SJC-02 | San Jose, USA
Mgmt. Address: 172.21.0.6
System Bridge Address:

EIP data - 0c:98:03:a3:00:00

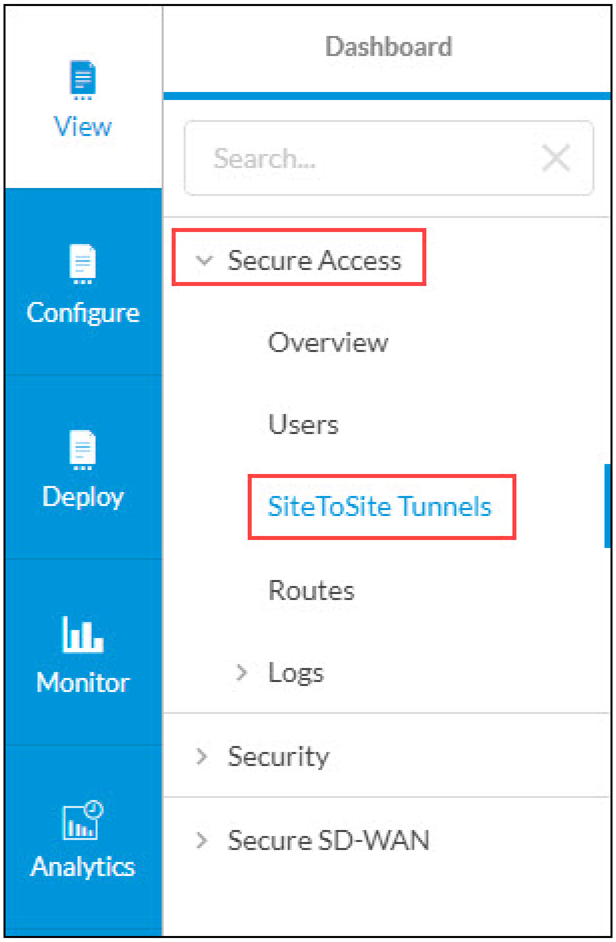
```
<eip>
 <antimalware>
  <softwares>
   <software>
    <vendor>Microsoft Corporation</vendor>
    <product>Windows Defender</product>
    <major>4</major>
    <minor>18</minor>
    <service>24050</service>
    <patch>7</patch>
    <raw_version>4.18.24050.7</raw_version>
    <is-running>true</is-running>
    <is-configured>true</is-configured>
    <is-installed>true</is-installed>
    <realtime-protection>true</realtime-protection>
    <last-scan-time>1720967408</last-scan-time>
```

## View EIP History Information

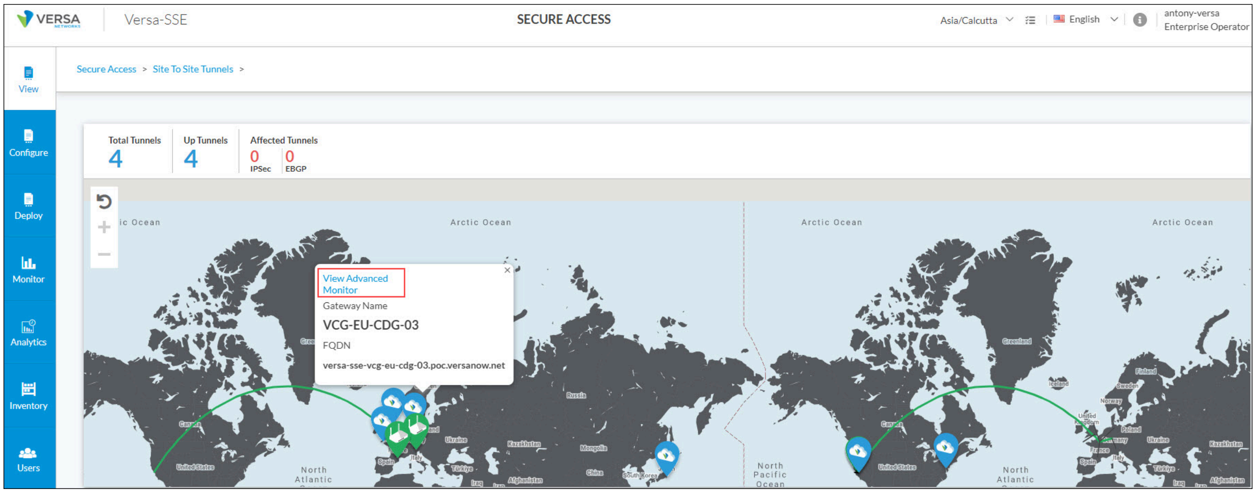
You must have an administrator privilege level to view the EIP history information. By default, entities send EIP information to the SSE gateway every 10 minutes.

To view secure access history:

1. Select View > Secure Access > Site-to-Site Tunnels.



2. From the list of available SSE gateways, select the SSE gateway the entity is connecting to, and then click View Advanced Monitor.



Total Tunnels 4

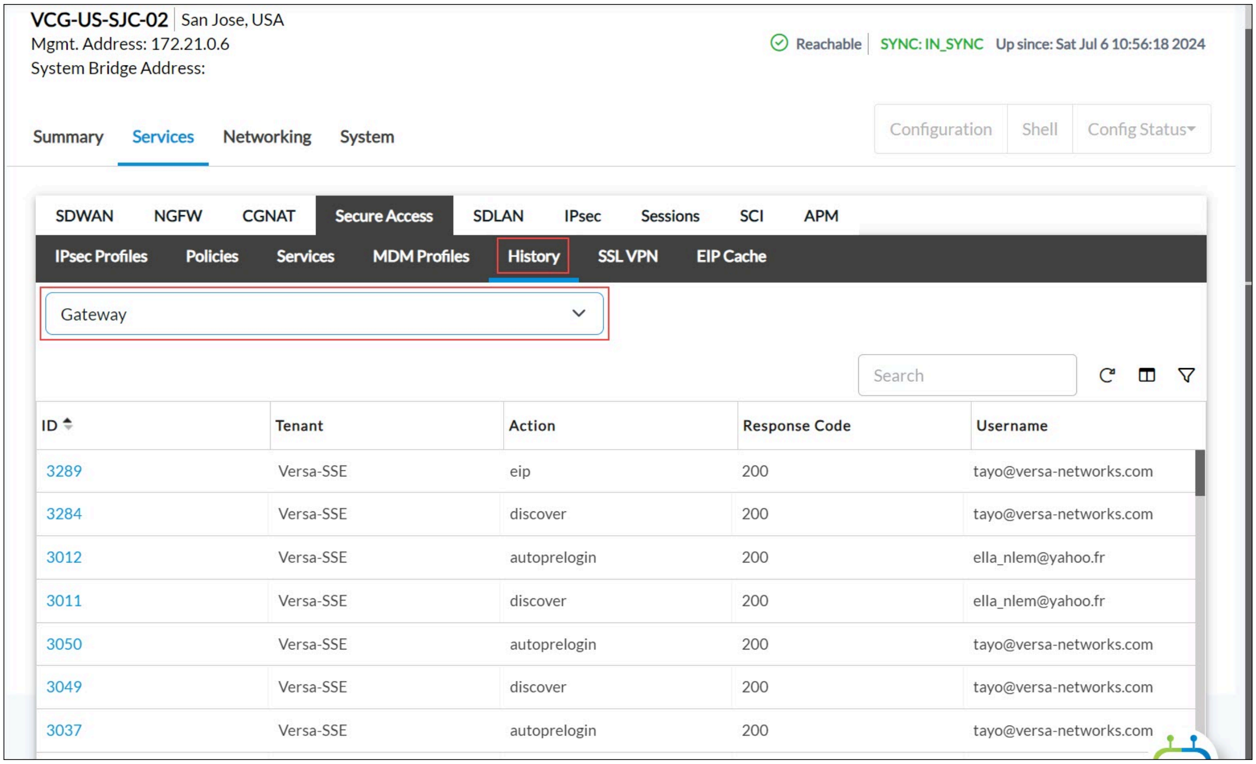
Up Tunnels 4

Affected Tunnels 0 IPSec 0 EBGP

Gateway Name
VCG-EU-CDG-03

FQDN
versa-sse-vcg-eu-cdg-03.poc.versanow.net

3. In the Devices > Services tab, select the Secure Access > History tab, and then select Gateway in the drop-down list.



VCG-US-SJC-02 | San Jose, USA
Mgmt. Address: 172.21.0.6
System Bridge Address:

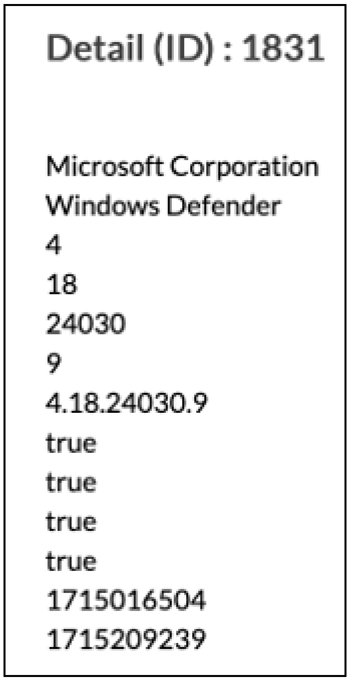
Up since: Sat Jul 6 10:56:18 2024

Gateway

| ID | Tenant | Action | Response Code | Username |
|---|---|---|---|---|
| 3289 | Versa-SSE | eip | 200 | tayo@versa-networks.com |
| 3284 | Versa-SSE | discover | 200 | tayo@versa-networks.com |
| 3012 | Versa-SSE | autoprelogin | 200 | ella_nlem@yahoo.fr |
| 3011 | Versa-SSE | discover | 200 | ella_nlem@yahoo.fr |
| 3050 | Versa-SSE | autoprelogin | 200 | tayo@versa-networks.com |
| 3049 | Versa-SSE | discover | 200 | tayo@versa-networks.com |
| 3037 | Versa-SSE | autoprelogin | 200 | tayo@versa-networks.com |

4. In the ID column, click the ID link to view the EIP history information. You can select multiple IDs.

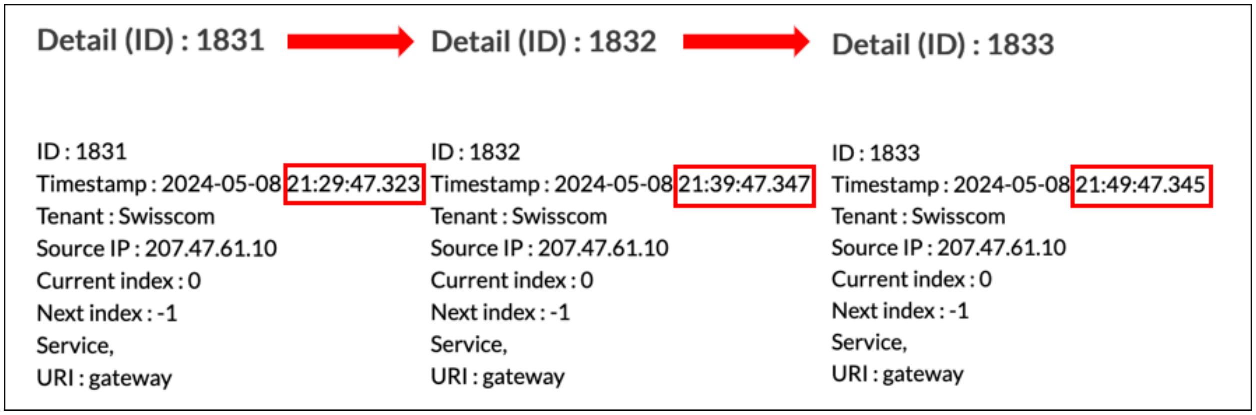
   The following screenshot shows EIP history information for the 10-minute interval.



Detail (ID) : 1831

Microsoft Corporation
Windows Defender
4
18
24030
9
4.18.24030.9
true
true
true
true
1715016504
1715209239

The following screenshot shows multiple IDs (1831 through 1833) are selected, and the Timestamp shows that the entity is sending EIP information every 10 minutes.



Detail (ID) : 1831

ID : 1831
Timestamp : 2024-05-08 21:29:47.323
Tenant : Swisscom
Source IP : 207.47.61.10
Current index : 0
Next index : -1
Service,
URI : gateway

Detail (ID) : 1832

ID : 1832
Timestamp : 2024-05-08 21:39:47.347
Tenant : Swisscom
Source IP : 207.47.61.10
Current index : 0
Next index : -1
Service,
URI : gateway

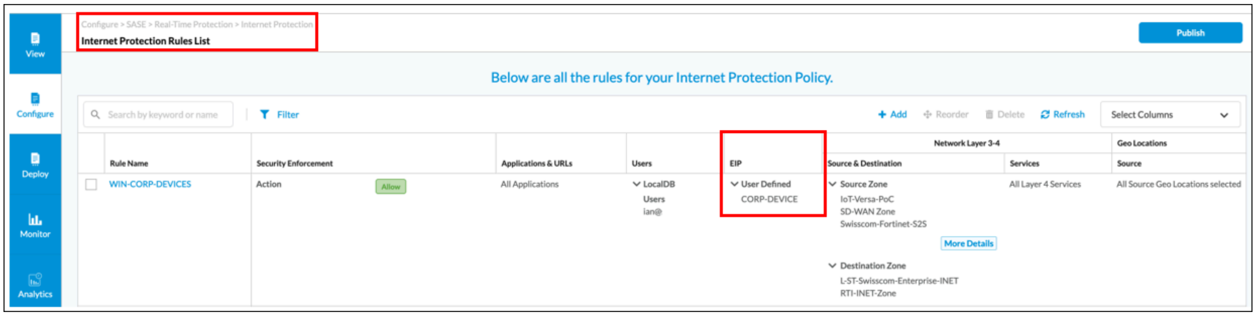
Detail (ID) : 1833

ID : 1833
Timestamp : 2024-05-08 21:49:47.345
Tenant : Swisscom
Source IP : 207.47.61.10
Current index : 0
Next index : -1
Service,
URI : gateway

## View Session Information

If an EIP is associated with real-time protection rules, you can troubleshoot EIP using the View > Devices > Services > Sessions tab. You can check the access policy associated with a session that is created for every flow of information between the source and destination.

In the following example, the internet protection rule controls the data flow from Versa SSE client to the internet. The rule matches the CORP-DEVICE EIP profile.

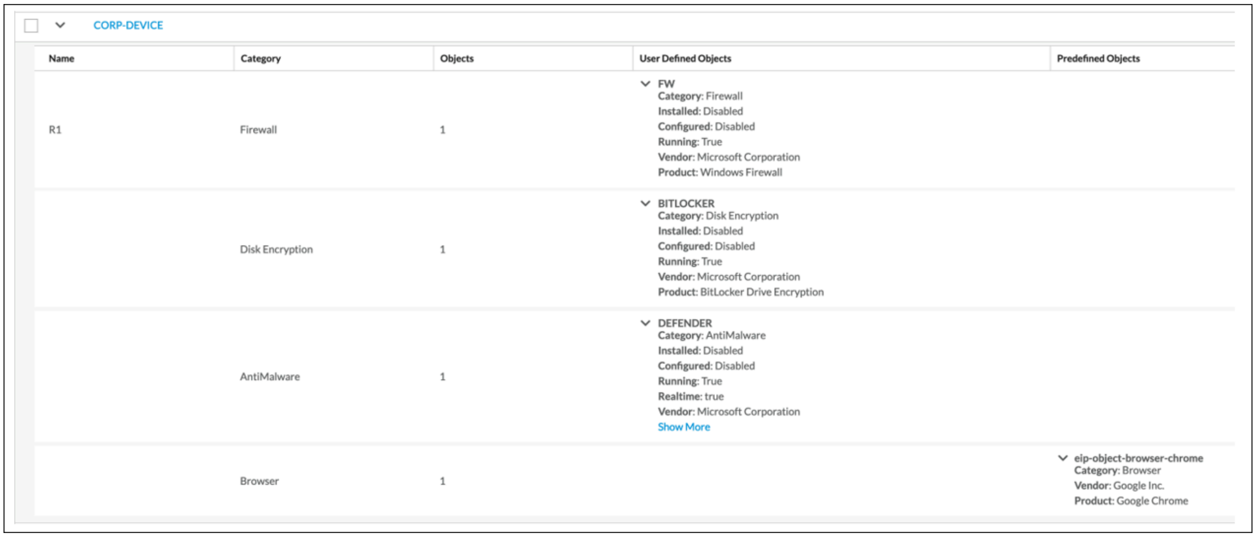


Configure > SASE > Real-Time Protection > Internet Protection
Internet Protection Rules List

Below are all the rules for your Internet Protection Policy.

| | | | | | Network Layer 3-4 | | Geo Locations |
|---|---|---|---|---|---|---|---|
| Rule Name | Security Enforcement | Applications & URLs | Users | EIP | Source & Destination | Services | Source |
| WIN-CORP-DEVICES | Action Allow | All Applications | LocalDB<br>Users<br>ian@ | User Defined<br>CORP-DEVICE | Source Zone<br>IoT-Versa-PoC<br>SD-WAN Zone<br>Swisscom-Fortinet-S2S<br>Destination Zone<br>L-ST-Swisscom-Enterprise-INET<br>RTI-INET-Zone | All Layer 4 Services | All Source Geo Locations selected |

The EIP profile matches the EIP information as shown in the following screenshot. Note that all elements in R1 must match for entities to be associated with the CORP-DEVICE EIP profile.



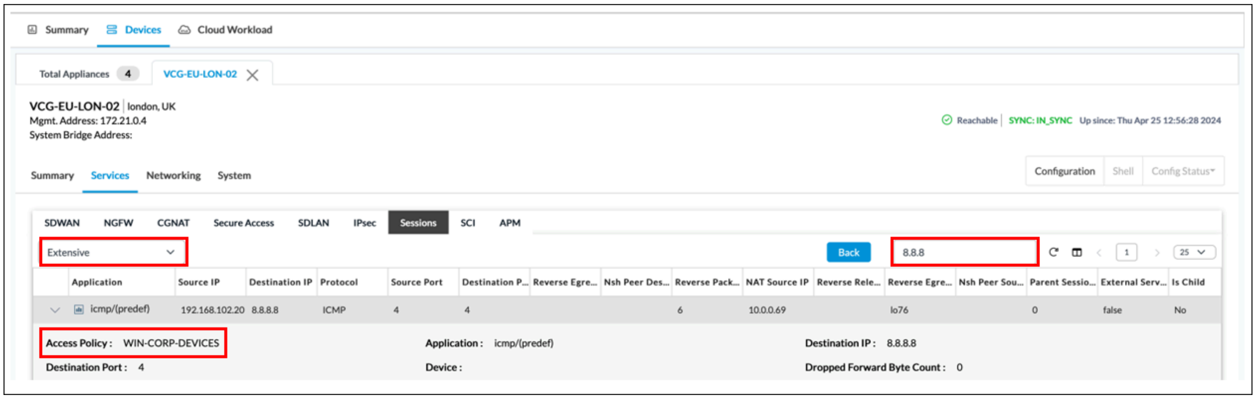
CORP-DEVICE

| Name | Category | Objects | User Defined Objects | Predefined Objects |
|---|---|---|---|---|
| R1 | Firewall | 1 | FW<br>Category: Firewall<br>Installed: Disabled<br>Configured: Disabled<br>Running: True<br>Vendor: Microsoft Corporation<br>Product: Windows Firewall | |
| | Disk Encryption | 1 | BITLOCKER<br>Category: Disk Encryption<br>Installed: Disabled<br>Configured: Disabled<br>Running: True<br>Vendor: Microsoft Corporation<br>Product: BitLocker Drive Encryption | |
| | AntiMalware | 1 | DEFENDER<br>Category: AntiMalware<br>Installed: Disabled<br>Configured: Disabled<br>Running: True<br>Realtime: true<br>Vendor: Microsoft Corporation<br>Show More | |
| | Browser | 1 | | eip-object-browser-chrome<br>Category: Browser<br>Vendor: Google Inc.<br>Product: Google Chrome |

The entity has the following objects in running state:

- Windows firewall
- Bitlocker
- Defender and realtime

When a user attempts to ping 8.8.8.8, the session table shows the access policy associated with the stream. The following screenshot shows the policy that meets the match criteria of the rule. To view the access policy, select Extensive in the drop-down list, and apply the filter to the session table to display sessions containing 8.8.8.8.



VCG-EU-LON-02 | london, UK
Mgmt. Address: 172.21.0.4
System Bridge Address:

Reachable | SYNC: IN_SYNC Up since: Thu Apr 25 12:56:28 2024

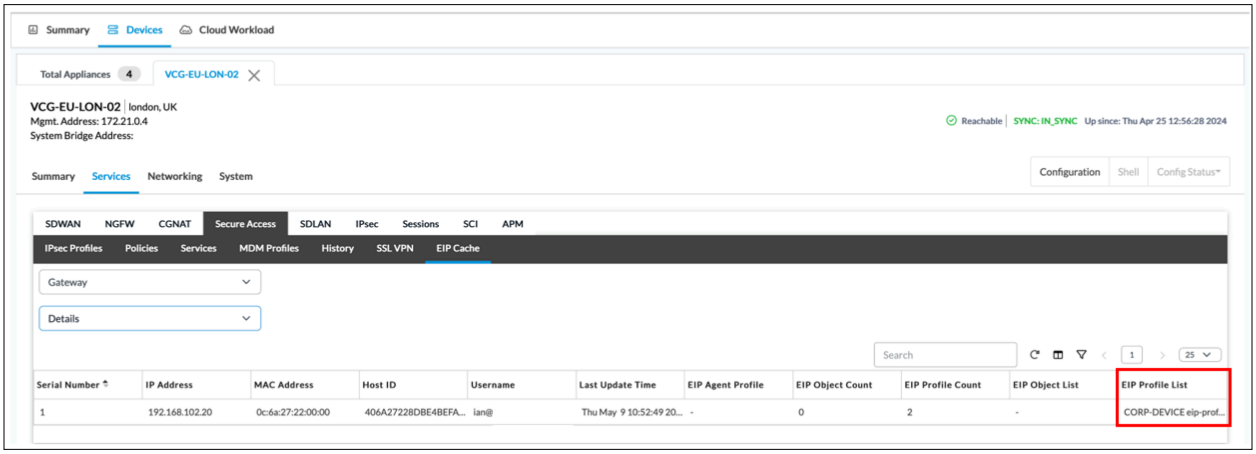
Extensive

8.8.8

| Application | Source IP | Destination IP | Protocol | Source Port | Destination P... | Reverse Egre... | Nsh Peer Des... | Reverse Pack... | NAT Source IP | Reverse Rele... | Reverse Egre... | Nsh Peer Sou... | Parent Sessio... | External Serv... | Is Child |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| icmp/(predef) | 192.168.102.20 | 8.8.8.8 | ICMP | 4 | 4 | | | 6 | 10.0.0.69 | | lo76 | | 0 | false | No |

Access Policy : WIN-CORP-DEVICES
Application : icmp/(predef)
Destination IP : 8.8.8.8
Destination Port : 4
Device :
Dropped Forward Byte Count : 0

If the session is associated with an unexpected access policy, check the EIP Profile List column. The following screenshot shows one of the EIP profiles associated with the entity is CORP-DEVICE, and this profile is used as match criteria for the internet protection rule.



VCG-EU-LON-02 | london, UK
Mgmt. Address: 172.21.0.4
System Bridge Address:

Reachable | SYNC: IN_SYNC Up since: Thu Apr 25 12:56:28 2024

Gateway

Details

| Serial Number | IP Address | MAC Address | Host ID | Username | Last Update Time | EIP Agent Profile | EIP Object Count | EIP Profile Count | EIP Object List | EIP Profile List |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 192.168.102.20 | 0c:6a:27:22:00:00 | 406A27228DBE4BEFA... | ian@ | Thu May 9 10:52:49 20... | - | 0 | 2 | - | CORP-DEVICE eip-prof... |

# Troubleshoot EIP Profiles Using Versa Analytics

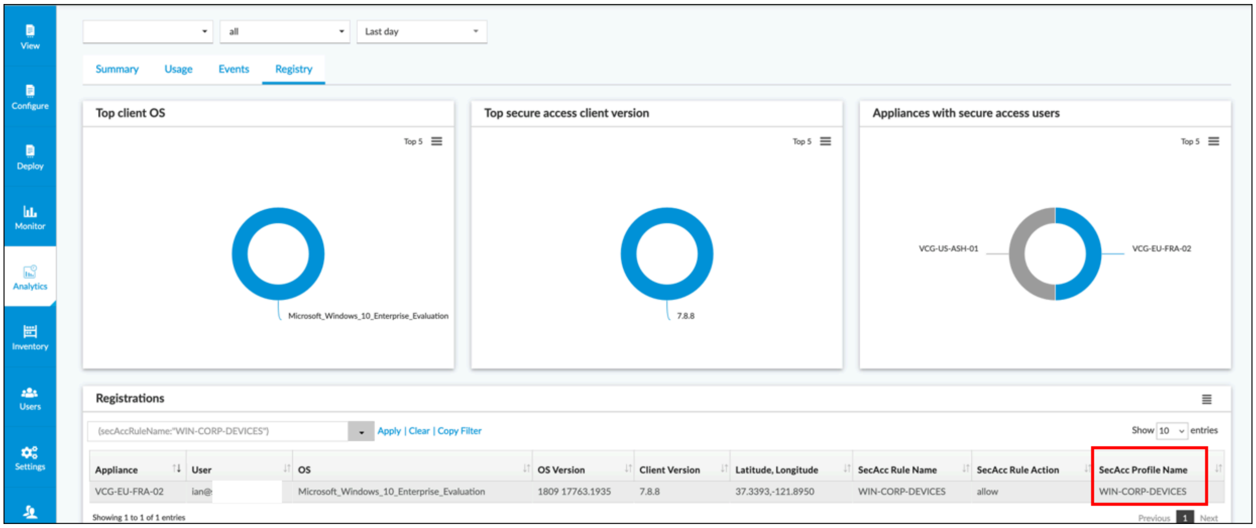
## View Entity Registration Information

You can access registration information for an entity using one of the following navigation paths in Concerto:

- Analytics > Dashboard > View > Secure Access > Users > Registry
- View > Secure Access > Users > Registry

The Registrations metrics show the secure client access profile associated with the entity during the registration to the SASE service. Note that recall EIP information is not considered as match criteria during registration, so there may be a profile name change in the output.

The following screenshot shows the SCA profile name from the registry information using the Analytics menu.



Registrations

(secAccRuleName:"WIN-CORP-DEVICES")

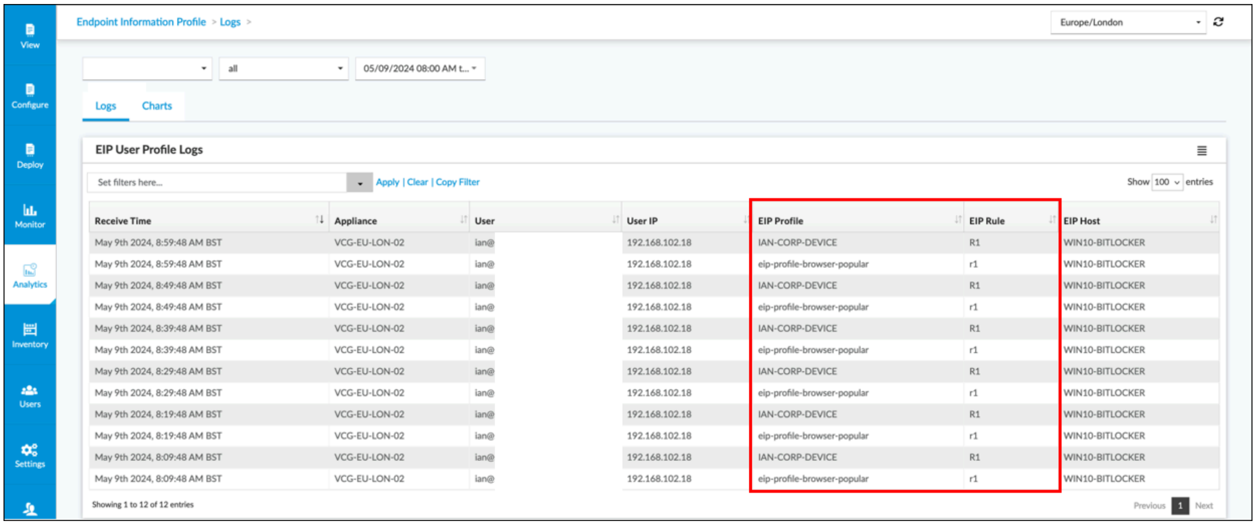
| Appliance | User | OS | OS Version | Client Version | Latitude, Longitude | SecAcc Rule Name | SecAcc Rule Action | SecAcc Profile Name |
|---|---|---|---|---|---|---|---|---|
| VCG-EU-FRA-02 | ian@[redacted] | Microsoft_Windows_10_Enterprise_Evaluation | 1809 17763.1935 | 7.8.8 | 37.3393,-121.8950 | WIN-CORP-DEVICES | allow | WIN-CORP-DEVICES |

Showing 1 to 1 of 1 entries

## View EIP Log Information

The EIP log screen shows the historical record of the EIP profile associations that the entity makes over time. You can access the EIP logs from the Analytics > Dashboard > Logs > EIP > Logs tab.

In the following screenshot, the SSE gateway associated the entity with two EIP profiles based on the information received from the Versa SASE client. You can also use the EIP rule name to troubleshoot the EIP issues.



EIP User Profile Logs

Set filters here... Apply | Clear | Copy Filter

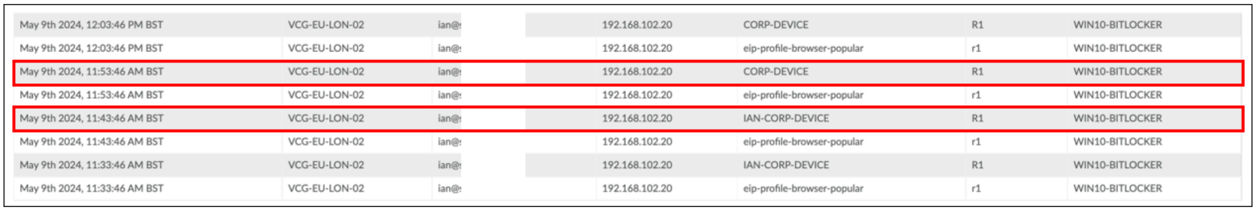
Show 100 entries

| Receive Time | Appliance | User | User IP | EIP Profile | EIP Rule | EIP Host |
|---|---|---|---|---|---|---|
| May 9th 2024, 8:59:48 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.18 | IAN-CORP-DEVICE | R1 | WIN10-BITLOCKER |
| May 9th 2024, 8:59:48 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.18 | eip-profile-browser-popular | r1 | WIN10-BITLOCKER |
| May 9th 2024, 8:49:48 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.18 | IAN-CORP-DEVICE | R1 | WIN10-BITLOCKER |
| May 9th 2024, 8:49:48 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.18 | eip-profile-browser-popular | r1 | WIN10-BITLOCKER |
| May 9th 2024, 8:39:48 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.18 | IAN-CORP-DEVICE | R1 | WIN10-BITLOCKER |
| May 9th 2024, 8:39:48 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.18 | eip-profile-browser-popular | r1 | WIN10-BITLOCKER |
| May 9th 2024, 8:29:48 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.18 | IAN-CORP-DEVICE | R1 | WIN10-BITLOCKER |
| May 9th 2024, 8:29:48 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.18 | eip-profile-browser-popular | r1 | WIN10-BITLOCKER |
| May 9th 2024, 8:19:48 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.18 | IAN-CORP-DEVICE | R1 | WIN10-BITLOCKER |
| May 9th 2024, 8:19:48 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.18 | eip-profile-browser-popular | r1 | WIN10-BITLOCKER |
| May 9th 2024, 8:09:48 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.18 | IAN-CORP-DEVICE | R1 | WIN10-BITLOCKER |
| May 9th 2024, 8:09:48 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.18 | eip-profile-browser-popular | r1 | WIN10-BITLOCKER |

Showing 1 to 12 of 12 entries

Previous 1 Next

The following screenshot shows that the entity is disassociated from the IAN-CORP-DEVICE EIP profile, and associated with the CORP-DEVICE EIP profile because of a poster change in the entity.

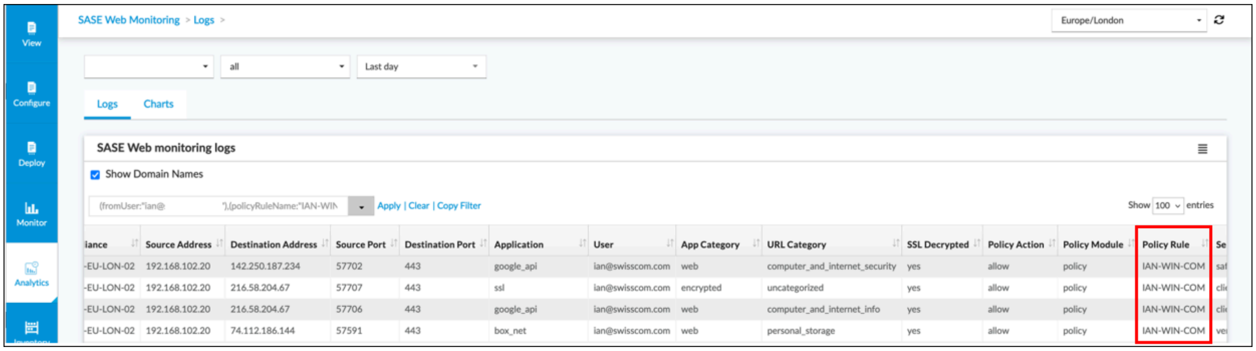


| | | | | | | |
|---|---|---|---|---|---|---|
| May 9th 2024, 12:03:46 PM BST | VCG-EU-LON-02 | ian@ | 192.168.102.20 | CORP-DEVICE | R1 | WIN10-BITLOCKER |
| May 9th 2024, 12:03:46 PM BST | VCG-EU-LON-02 | ian@ | 192.168.102.20 | eip-profile-browser-popular | r1 | WIN10-BITLOCKER |
| May 9th 2024, 11:53:46 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.20 | CORP-DEVICE | R1 | WIN10-BITLOCKER |
| May 9th 2024, 11:53:46 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.20 | eip-profile-browser-popular | r1 | WIN10-BITLOCKER |
| May 9th 2024, 11:43:46 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.20 | IAN-CORP-DEVICE | R1 | WIN10-BITLOCKER |
| May 9th 2024, 11:43:46 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.20 | eip-profile-browser-popular | r1 | WIN10-BITLOCKER |
| May 9th 2024, 11:33:46 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.20 | IAN-CORP-DEVICE | R1 | WIN10-BITLOCKER |
| May 9th 2024, 11:33:46 AM BST | VCG-EU-LON-02 | ian@ | 192.168.102.20 | eip-profile-browser-popular | r1 | WIN10-BITLOCKER |

The change is because of the automatic updates that Versa SASE client sends to the SSE gateway, and does not need the Versa SASE client to disconnect and reconnect.  This allows the SSE gateway to control access to resources based on the dynamic posture of the entity.

## View Versa SASE Web Logs

You can access the Versa SASE web logs that have session information and associations to real-time protection rules from the Analytics > Dashboard > Logs > SASE Web Monitoring > Logs tab. You can check the rule that is associated with the session and compare the rules.



SASE Web Monitoring > Logs >

Europe/London

all

Last day

Logs Charts

SASE Web monitoring logs

☑ Show Domain Names

(fromUser:"ian@ "),(policyRuleName:"IAN-WIN Apply | Clear | Copy Filter

Show 100 entries

| iance | Source Address | Destination Address | Source Port | Destination Port | Application | User | App Category | URL Category | SSL Decrypted | Policy Action | Policy Module | Policy Rule | Se |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| -EU-LON-02 | 192.168.102.20 | 142.250.187.234 | 57702 | 443 | google_api | ian@swisscom.com | web | computer_and_internet_security | yes | allow | policy | IAN-WIN-COM | saf |
| -EU-LON-02 | 192.168.102.20 | 216.58.204.67 | 57707 | 443 | ssl | ian@swisscom.com | encrypted | uncategorized | yes | allow | policy | IAN-WIN-COM | cli |
| -EU-LON-02 | 192.168.102.20 | 216.58.204.67 | 57706 | 443 | google_api | ian@swisscom.com | web | computer_and_internet_info | yes | allow | policy | IAN-WIN-COM | cli |
| -EU-LON-02 | 192.168.102.20 | 74.112.186.144 | 57591 | 443 | box_net | ian@swisscom.com | web | personal_storage | yes | allow | policy | IAN-WIN-COM | ve |

## Example: EIP Updates from a Windows Entity

The following example is an EIP update from a Windows entity based on the EIP agent profile Versa_Recommended:

```
<eip>
  <antimalware>
    <softwares>
      <software>
        <vendor>Microsoft Corporation</vendor>
        <product>Windows Defender</product>
        <major>4</major>
        <minor>18</minor>
        <service>24030</service>
        <patch>9</patch>
        <raw_version>4.18.24030.9</raw_version>
        <is-running>true</is-running>
        <is-configured>true</is-configured>
        <is-installed>true</is-installed>
        <realtime-protection>true</realtime-protection>
        <last-scan-time>1715016504</last-scan-time>
        <last-definition-update>1715189346</last-definition-update>
      </software>
    </softwares>
  </antimalware>
  <firewall>
    <softwares>
      <software>
        <vendor>Microsoft Corporation</vendor>
        <product>Windows Firewall</product>
        <major>10</major>
        <minor>0</minor>
        <service>17763</service>
        <patch>1852</patch>
        <raw_version>10.0.17763.1852</raw_version>
        <is-running>false</is-running>
        <is-configured>true</is-configured>
        <is-installed>true</is-installed>
      </software>
    </softwares>
```

```
</firewall>
<disk-backup>
  <softwares>
    <software>
      <vendor>Microsoft Corporation</vendor>
      <product>Microsoft OneDrive</product>
      <major>24</major>
      <minor>76</minor>
      <service>414</service>
      <patch>5</patch>
      <raw-version>24.076.0414.0005</raw-version>
      <is-running>true</is-running>
      <is-configured>true</is-configured>
      <is-installed>true</is-installed>
      <last-backup-time/>
    </software>
    <software>
      <vendor>Microsoft Corporation</vendor>
      <product>Windows Backup and Restore</product>
      <major>10</major>
      <minor>0</minor>
      <service>17763</service>
      <patch>1</patch>
      <raw-version>10.0.17763.1</raw-version>
      <is-running>false</is-running>
      <is-configured>true</is-configured>
      <is-installed>true</is-installed>
      <last-backup-time/>
    </software>
    <software>
      <vendor>Microsoft Corporation</vendor>
      <product>Windows File History</product>
      <major>10</major>
      <minor>0</minor>
      <service>17763</service>
      <patch>1</patch>
      <raw-version>10.0.17763.1</raw-version>
      <is-running>false</is-running>
      <is-configured>true</is-configured>
      <is-installed>true</is-installed>
      <last-backup-time/>
    </software>
  </softwares>
</disk-backup>
<disk-encryption>
  <softwares>
    <software>
      <vendor>Microsoft Corporation</vendor>
      <product>BitLocker Drive Encryption</product>
      <major>10</major>
      <minor>0</minor>
      <service>17763</service>
      <patch>1</patch>
      <raw_version>10.0.17763.1</raw_version>
```

```
        <is-running>true</is-running>
        <is-configured>true</is-configured>
        <is-installed>true</is-installed>
        <locations>
          <location>
            <path>C:\</path>
            <status>encrypted</status>
          </location>
        </locations>
      </software>
    </softwares>
  </disk-encryption>
  <data_loss_prevention>
    <softwares/>
  </data_loss_prevention>
  <patch_management>
    <softwares>
      <software>
        <vendor>Microsoft Corporation</vendor>
        <product>Windows Update Agent</product>
        <major>10</major>
        <minor>0</minor>
        <service>17763</service>
        <patch>1852</patch>
        <raw_version>10.0.17763.1852</raw_version>
        <is-running>true</is-running>
        <is-configured>true</is-configured>
        <is-installed>true</is-installed>
      </software>
    </softwares>
  </patch_management>
  <public_file_sharing>
    <softwares/>
  </public_file_sharing>
  <antiphishing>
    <softwares>
      <software>
        <vendor>Google Inc.</vendor>
        <product>Google Chrome</product>
        <major>124</major>
        <minor>0</minor>
        <service>6367</service>
        <patch>119</patch>
        <raw_version>124.0.6367.119</raw_version>
        <is-running>true</is-running>
        <is-configured>true</is-configured>
        <is-installed>true</is-installed>
      </software>
      <software>
        <vendor>Microsoft Corporation</vendor>
        <product>Internet Explorer</product>
        <major>11</major>
        <minor>1790</minor>
        <service>17763</service>
      <patch>0</patch>
      <raw_version>11.1790.17763.0</raw_version>
      <is-running>false</is-running>
      <is-configured>true</is-configured>
      <is-installed>true</is-installed>
    </software>
    <software>
      <vendor>Microsoft Corporation</vendor>
      <product>Internet Explorer</product>
      <major>11</major>
      <minor>1790</minor>
      <service>17763</service>
      <patch>0</patch>
      <raw_version>11.1790.17763.0</raw_version>
      <is-running>false</is-running>
      <is-configured>true</is-configured>
      <is-installed>true</is-installed>
    </software>
    <software>
      <vendor>Microsoft Corporation</vendor>
      <product>Microsoft Edge</product>
      <major>124</major>
      <minor>0</minor>
      <service>2478</service>
      <patch>80</patch>
      <raw_version>124.0.2478.80</raw_version>
      <is-running>true</is-running>
      <is-configured>true</is-configured>
      <is-installed>true</is-installed>
    </software>
  </softwares>
</antiphishing>
<browser>
  <softwares>
    <software>
      <vendor>Google Inc.</vendor>
      <product>Google Chrome</product>
      <major>124</major>
      <minor>0</minor>
      <service>6367</service>
      <patch>119</patch>
      <raw_version>124.0.6367.119</raw_version>
      <is-running>true</is-running>
      <is-configured>true</is-configured>
      <is-installed>true</is-installed>
    </software>
    <software>
      <vendor>Microsoft Corporation</vendor>
      <product>Internet Explorer</product>
      <major>11</major>
      <minor>1790</minor>
      <service>17763</service>
      <patch>0</patch>
      <raw_version>11.1790.17763.0</raw_version>
      <is-running>false</is-running>
      <is-configured>true</is-configured>
      <is-installed>true</is-installed>
    </software>
    <software>
      <vendor>Microsoft Corporation</vendor>
      <product>Internet Explorer</product>
      <major>11</major>
      <minor>1790</minor>
      <service>17763</service>
      <patch>0</patch>
      <raw_version>11.1790.17763.0</raw_version>
      <is-running>false</is-running>
      <is-configured>true</is-configured>
      <is-installed>true</is-installed>
    </software>
    <software>
      <vendor>Microsoft Corporation</vendor>
      <product>Microsoft Edge</product>
      <major>124</major>
      <minor>0</minor>
      <service>2478</service>
      <patch>80</patch>
      <raw_version>124.0.2478.80</raw_version>
      <is-running>true</is-running>
      <is-configured>true</is-configured>
      <is-installed>true</is-installed>
    </software>
  </softwares>
</browser>
<health_agent>
  <softwares>
    <software>
      <vendor>Microsoft Corporation</vendor>
      <product>Windows Security Health Agent</product>
      <major>10</major>
      <minor>0</minor>
      <service>17763</service>
      <patch>1</patch>
      <raw_version>10.0.17763.1</raw_version>
      <is-running>true</is-running>
      <is-configured>true</is-configured>
      <is-installed>true</is-installed>
    </software>
  </softwares>
</health_agent>
<virtual_machine>
  <softwares/>
</virtual_machine>
<cloud_storage>
  <softwares>
    <software>
      <vendor>Microsoft Corporation</vendor>
      <product>Microsoft OneDrive</product>
```

```
        <major>24</major>
        <minor>76</minor>
        <service>414</service>
        <patch>5</patch>
        <raw_version>24.076.0414.0005</raw_version>
        <is-running>true</is-running>
        <is-configured>true</is-configured>
        <is-installed>true</is-installed>
      </software>
    </softwares>
  </cloud_storage>
  <messenger>
    <softwares/>
  </messenger>
  <remote_control>
    <softwares>
      <software>
        <vendor>Microsoft Corporation</vendor>
        <product>Remote Desktop Connection</product>
        <major>10</major>
        <minor>0</minor>
        <service>17763</service>
        <patch>1</patch>
        <raw_version>10.0.17763.1</raw_version>
        <is-running>false</is-running>
        <is-configured>true</is-configured>
        <is-installed>true</is-installed>
      </software>
    </softwares>
  </remote_control>
  <management-status>false</management-status>
  <custom>
    <windows/>
    <process/>
  </custom>
  <general>
    <user-name>IEUser</user-name>
    <hostname>WIN10-BITLOCKER</hostname>
    <windows-domain>WORKGROUP</windows-domain>
    <os-major>10</os-major>
    <os-minor>0</os-minor>
    <os-service>17763</os-service>
    <os-patch>0</os-patch>
    <os-product>Microsoft Windows 10 Enterprise Evaluation</os-product>
    <os-vendor>Microsoft Corporation</os-vendor>
    <host-id>406A27228DBE4BEFA1F5A0BEA27ABED5</host-id>
    <tpm-enabled/>
  </general>
  <context>
    <generation-time>1715202751</generation-time>
    <report-time>1715202764</report-time>
    <device-tunnel-ip>192.168.104.6</device-tunnel-ip>
    <device-mac>0C-6A-27-22-00-00</device-mac>
    <vsac-version>7.8.8</vsac-version>
  <realtime-posture>false</realtime-posture>
</context>
</eip>
```

## Supported Software Information

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

## Additional Information

Configure Endpoint Information Profiles
Configure SASE Secure Client Access Rules
Use the Versa SASE Client Application