# Configure IoT Security

*For supported software information, click here.*

This article provides an overview of the Internet of Things (IoT) and Versa Operating System$^{TM}$ (VOS$^{TM}$) IoT security, and it describes how to view, configure, and monitor VOS IoT security devices.

## IoT Overview

The Internet of Things (IoT) refers to the network of interconnected physical devices that communicate and exchange data with each other through the internet. These devices are embedded with sensors and connectivity that enable them to collect and share information, leading to smarter and more efficient systems. The following are some examples of IoT devices:

- Smart home devices such as thermostats, lights, security cameras, and appliances. For example, a smart thermostat can adjust temperature settings based on occupancy and weather conditions.
- Healthcare IoT devices, including wearable fitness trackers, smart medical devices, and remote patient monitoring systems, that track health metrics, send alerts, and provide real-time data to healthcare professionals.
- Industrial IoT (IIoT) devices that perform predictive maintenance, monitor equipment health, and optimize operations. Sensors on machines can collect data on performance, enabling timely maintenance and reducing downtime.
- Smart cities use IoT devices for traffic management, waste management, and energy conservation. For example, smart traffic lights can adapt based on real-time traffic flow.
- Retailers use IoT for inventory management, customer tracking, and personalized shopping experiences. Some examples are RFID tags on products, beacons in stores, and smart shelves.
- Agricultural IoT devices, including soil sensors, drones, and connected machinery, help farmers to monitor soil conditions and crop health, and to automate irrigation systems.
- Modern cars use IoT for GPS navigation, real-time diagnostics, and driver-assistance systems.
- Smart grids and home energy management systems use smart meters to provide real-time energy consumption data, which helps users to optimize their usage and to manage the grid efficiently.

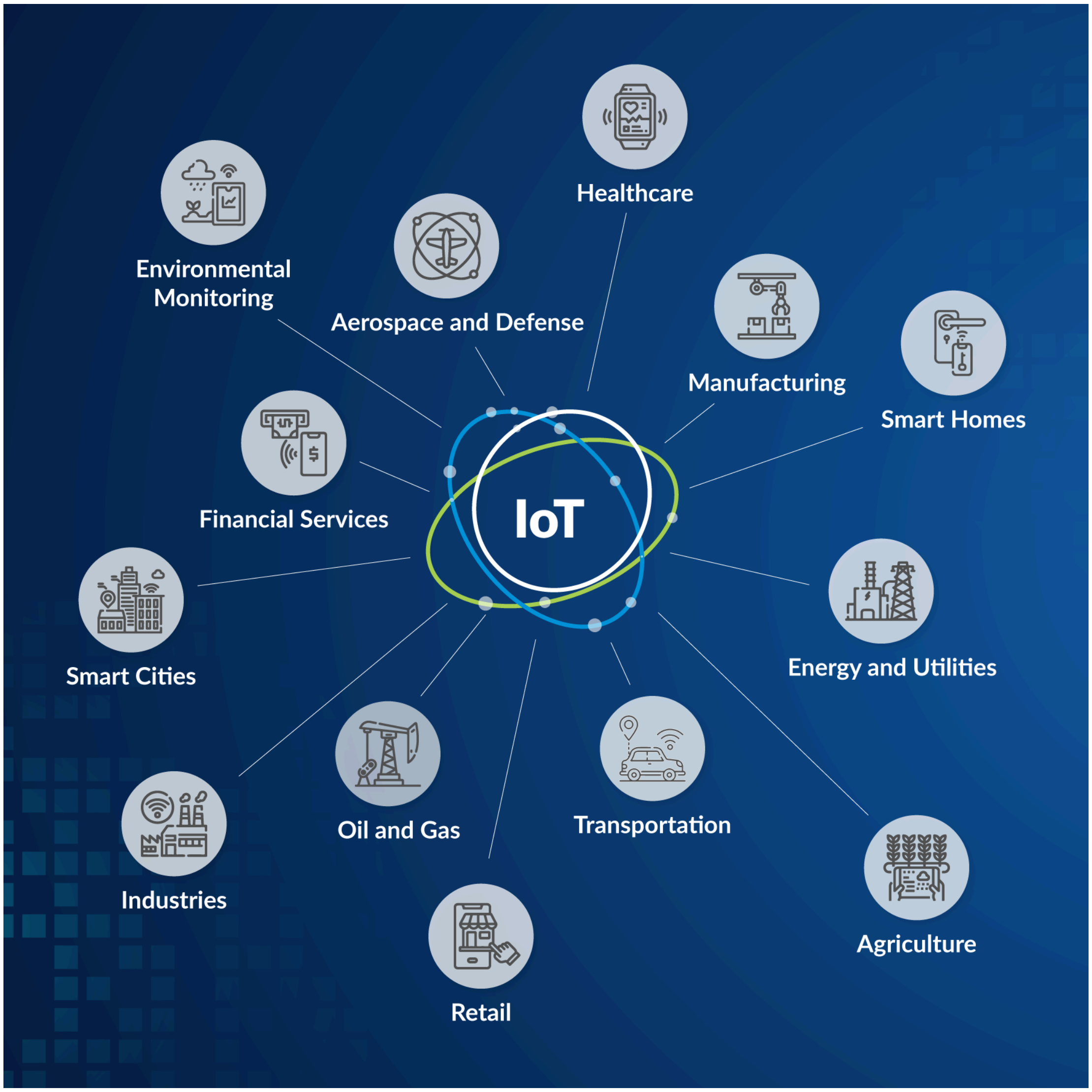
Security is foremost in the constantly expanding landscape of IoT, where an increasingly diverse range of devices connect to the internet. These device connections add to the complexity of your network. Unknown IoT devices also pose a security challenge, as many IoT endpoints have limited footprints. IoT devices are mostly unmanaged devices that do not provide a risk posture and may also lag in firmware upgrades. All these factors cause IT security blind spots that can disrupt your network.

The following are some of the common threats to IoT devices:

- Any connected and unprotected IoT device is vulnerable to being breached, compromised, and controlled by a bad actor.
- IoT devices have weak inbuilt security and this makes them vulnerable to security breaches and exploits when they connect to the internet.
- Cyber attacks are common on IoT devices and hackers target them to take control of data and tools.
- Hackers can use IoT systems to launch attacks from inside the network using remote code execution. They can use IoT devices as a base for lateral movement within the network to launch a distributed denial-of-service (DDoS) attack on the network or to exploit high value targets.

IoT security can help prevent attacks such as the Mirai Botnet (in 2016) that was used in an attempt to take Liberia offline, or the Stuxnet Worm (in 2010) that specifically aimed at disrupting supervisory control and data acquisition (SCADA) systems, which are commonly used in industrial IoT.

IoT security is crucial to various industries to protect connected devices, data, and systems. The following image displays some industries that use and require IoT security:



- Aerospace and defense—Uses IoT in defense systems, surveillance, and aerospace applications. Security is critical to protect national security interests and prevent unauthorized access.
- Agriculture—Uses IoT for precision agriculture, optimizing crop yields, and monitoring livestock. Security ensures data integrity and prevents tampering of agricultural processes.
- Energy and utilities—Employs IoT for managing smart grids, monitoring energy consumption, and optimizing resource distribution. Security prevents power grid disruptions and protects critical infrastructure.
- Environmental monitoring—Utilizes IoT to track environmental conditions such as air quality, water quality, and climate monitoring. Security is essential to ensure data accuracy and to prevent environmental disasters.
- Financial services—Uses IoT for smart ATMs, mobile banking, and payment processing. Security protects financial transactions and customer data.
- Healthcare—Uses IoT for medical implants, wearable health trackers, and hospital equipment. Security protects patient data and ensures proper functioning of these devices.
- Industrial IoT (IIoT)—Utilizes IoT for equipment monitoring, predictive maintenance, and process optimization. Security prevents production downtime and protects sensitive data.

- Manufacturing—Uses IoT for process automation, predictive maintenance, and quality control. Security prevents production disruptions and safeguards intellectual property.
- Oil and gas—Employs IoT for remote monitoring of pipelines and equipment. Security prevents environmental disasters and ensures the integrity of energy infrastructure.
- Retail—Uses IoT for inventory management, customer tracking, and to improve shopping experiences. Security protects customer data and prevents theft.
- Smart cities—Use IoT for traffic management, waste collection, and public safety. Security ensures the smooth operation of city services and protects against cyber threats.
- Smart homes—Use Iot for devices such as thermostats, cameras, and door locks. Security protects privacy and prevents unauthorized access to personal information.
- Transportation—Connected vehicles, traffic management systems, and autonomous vehicles rely on IoT. Security prevents vehicle hacks, accidents, and traffic disruptions.

These industries require IoT security solutions to scale with the growth of IoT ecosystems. The following are some of the IoT solutions in use:

- Application security—Ensures that IoT applications are developed with security in mind. It involves secure API interfaces to protect application endpoints and secure coding practices to minimize vulnerabilities.
- Cloud security—Essential for IoT solutions that involve cloud integration. It covers cloud integration security, protects data stored in the cloud, and secures communication with cloud services.
- Data security—Safeguards data during transmission and storage. Data encryption ensures that data is protected from eavesdropping and tampering, while data integrity verifies data authenticity.
- Device security—Secures IoT devices, including mechanisms for device authentication and patch management to address security vulnerabilities.
- Network security—Includes functions such as firewall protection to filter and inspect incoming and outgoing traffic. Network monitoring tools provide insights into network behavior to identify potential security threats.

## VOS IoT Security Overview

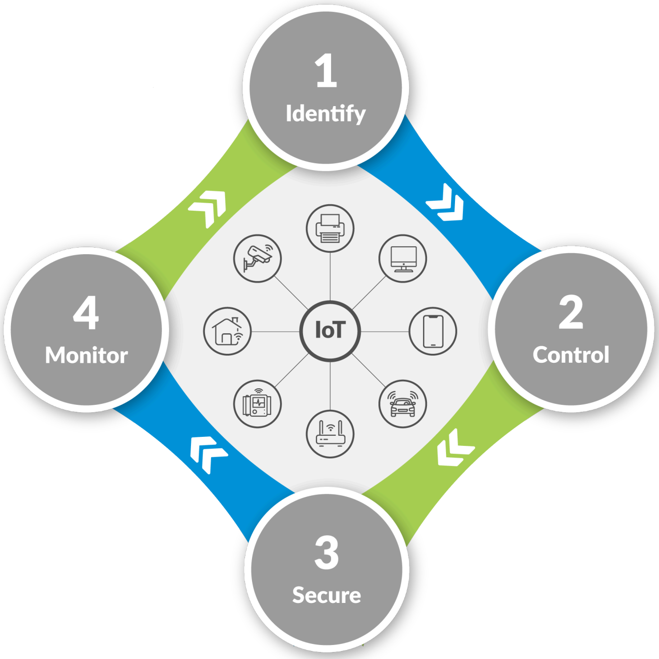
VOS IoT security uses agentless classification to identify devices based on their traffic pattern, providing real-time visibility to manage network security. VOS IoT security continuously scans data sent by IoT devices to discover devices joining the network in real-time, and evaluates their risk level. In case of a risk degradation, VOS IoT security updates the risk level of the device. Security policies can then restrict access to the network for that device, if the risk exceeds the threshold.

VOS IoT security allows you to create security and microsegmentation using the attributes of IoT devices, and to enforce these policies to prevent attacks and reduce attack surface. You also use VOS IoT in SD-WAN policies for traffic steering. VOS IoT security identifies networking devices based on their network fingerprints. When a device connects to the network and exchanges any supported control or data packets, the VOS software starts to extract signatures to discover the characteristics of the device. After collecting signatures, the VOS software checks for a match. Having a large number of fingerprints helps to correctly identify a device.

VOS IoT security provides the following:

- Visibility—For zero-trust identification of IoT devices.
- Control—For traffic analysis and segmentation based on risk.
- Security—For configuring security policy with next-generation firewall (NGFW) and unified threat management (UTM) to reduce risk exposure.
- Single pane architecture—For centralized, single policy definition for SD-WAN and security, allowing you to visualize threats and to enforce policies in real-time.
- Monitoring—For detecting behavioral anomalies and to automate enforcement.
- Analytics—For deep insight into IoT devices in the network.

The following figure illustrates the lifecycle stages in VOS IoT security.



- Identify—This stage includes device identification, categorization, and network access.
- Control—This stage involves analysis and segmentation of traffic and application of IoT security policy.
- Secure—This stage identifies and prevents vulnerabilities, attacks, exploits, and ransomware.
- Monitor—The final stage monitors event patterns based on the other stages, logs events, and allows you to monitor alerts and thresholds.

VOS IoT security includes the following functionalities:

- Agentless classification of millions of internet of secure things (IoXT) and BYOD devices. IoXT is a security standard for IoT devices.
- Comprehensive security at the Layer 2/Layer 3 boundary of the access layer and perimeter edge to protect IoT devices from inbound attacks and exploits for north-south and east-west traffic.
- Device tagging and reputation

- Microsegmentation of IoXt devices
- Detailed and in-depth device policy configuration
- Dynamic risk-based device quarantine
- Integrated device monitoring and analytics
- Centralized policy definition managed through a single pane of glass that provides visibility and enforces policies in real time.

VOS IoT security supports the following advanced identification capabilities:

- Device fingerprinting or device identification
    - Inline analysis of traffic flows for IoT devices and corporate or personal (BYOD) devices
    - Device fingerprint database for Layer 2 through Layer 7
    - Low-latency, rule-based engine
    - Match based on device class for consumption of policies and analytics
- Deep packet inspection (DPI)
    - Identification of more than 3,500 applications and protocols
    - Rich set of IoT protocol and application signatures, such as CAP, DNP3, jSCADA, MQTT, and OPC
    - User-defined applications and filters
    - Allow, block, rate-limit, and classify network traffic based on identification and policies
- URL-based traffic identification
    - Web traffic analysis of more than 460 million domains and 13 billion URLs that are scored and classified
    - Support for 83 predefined URL categories
    - URL database that is updated on a regular basis through security package (SPack) updates
    - Support for custom URL categories

This article describes the following:

- Enable IoT security in VOS
- View predefined IoT security objects
- Configure IoT security objects
- Associate IoT security objects with security policy rules
- Monitor IoT devices
- View IoT security analytics

## Configure IoT Security

To configure IoT security, you do the following:

- Enable IoT security on the VOS device and for organizations.
- Configure a cloud profile to enable cloud lookup for IoT devices.
- Modify IoT security settings to enable device identification and to select the cloud profile.

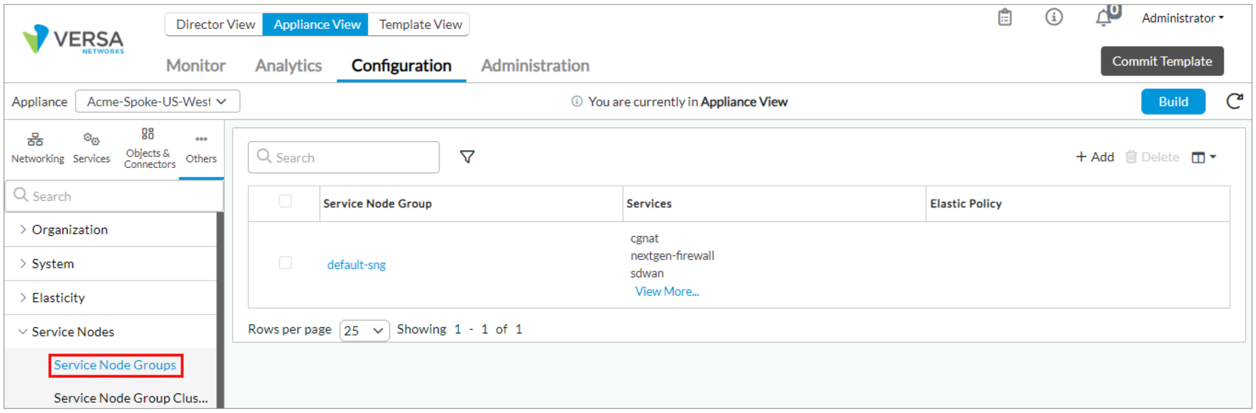
## Enable IoT Security

Before you configure IoT security, you must enable it on the VOS device. To enable IoT security, you must subscribe to IoT security license, which is an add-on in the SD-WAN licensing tier.

You can then enable IoT security globally in the service node group used by the organizations on the VOS device. After this, you enable IoT security for individual organizations, by adding IoT security to the organization limits for the provider or tenant organization, as described in this section. For information about configuring service node groups, see Configure Service Node Groups. For information about configuring organization limits, see Configure Organization Limits.

To enable IoT security globally for a VOS device:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. In the main pane, click the name of the VOS device. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > Service Nodes > Service Node Groups in the left menu bar. The main pane displays the service node groups that are already configured.



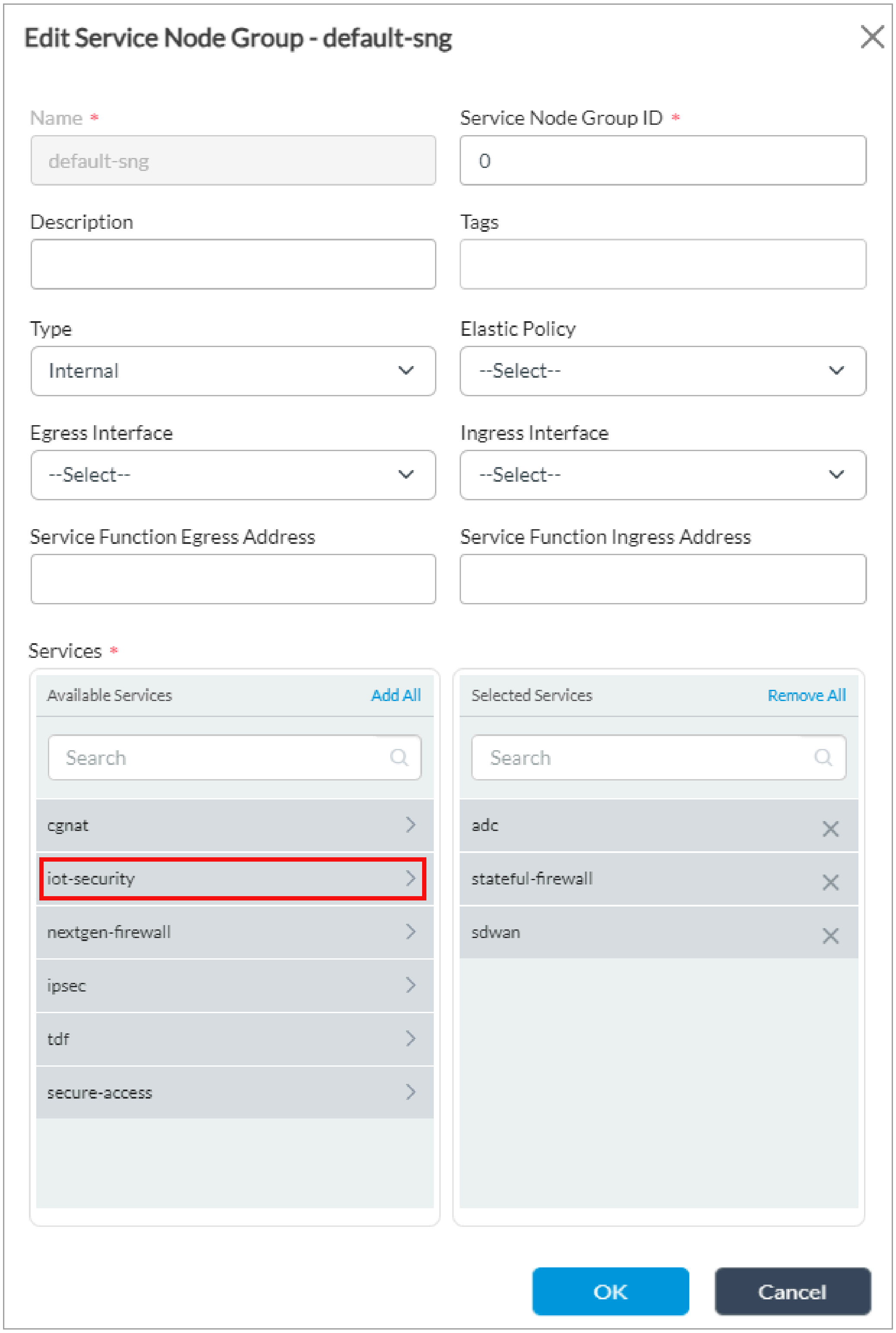
Appliance: Acme-Spoke-US-West

You are currently in Appliance View

| Service Node Group | Services | Elastic Policy |
|---|---|---|
| default-sng | cgnat<br>nextgen-firewall<br>sdwan<br>View More... | |

Rows per page 25 Showing 1 - 1 of 1

4. Click the name of the service node group. The Edit Service Node Group popup window displays.



Edit Service Node Group - default-sng

Name * default-sng

Service Node Group ID * 0

Description

Tags

Type: Internal

Elastic Policy: --Select--

Egress Interface: --Select--

Ingress Interface: --Select--

Service Function Egress Address

Service Function Ingress Address

Services *

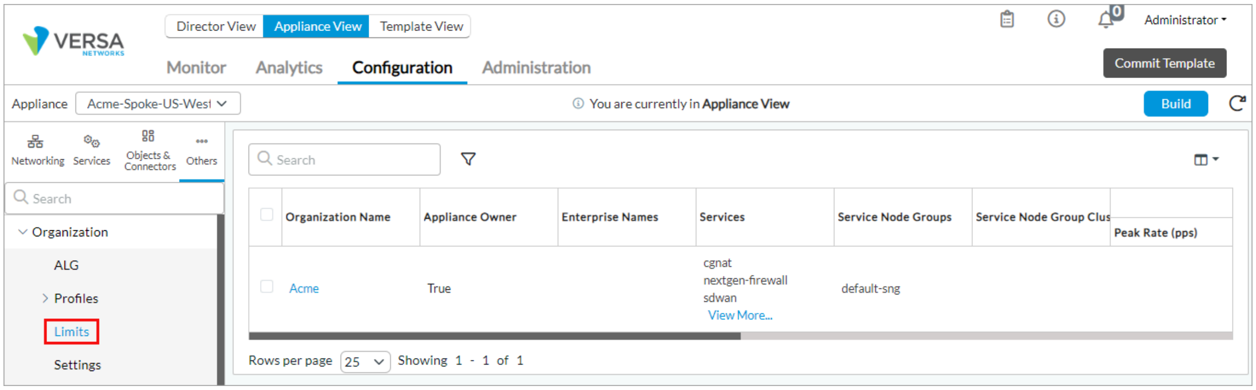
| Available Services | Selected Services |
|---|---|
| cgnat | adc |
| iot-security | stateful-firewall |
| nextgen-firewall | sdwan |
| ipsec | |
| tdf | |
| secure-access | |

5. Click iot-security in the Available Services table to move it to the Selected Services table.
6. Click OK.

7. Refresh the browser window.

To enable IoT security for an organization on a VOS device:

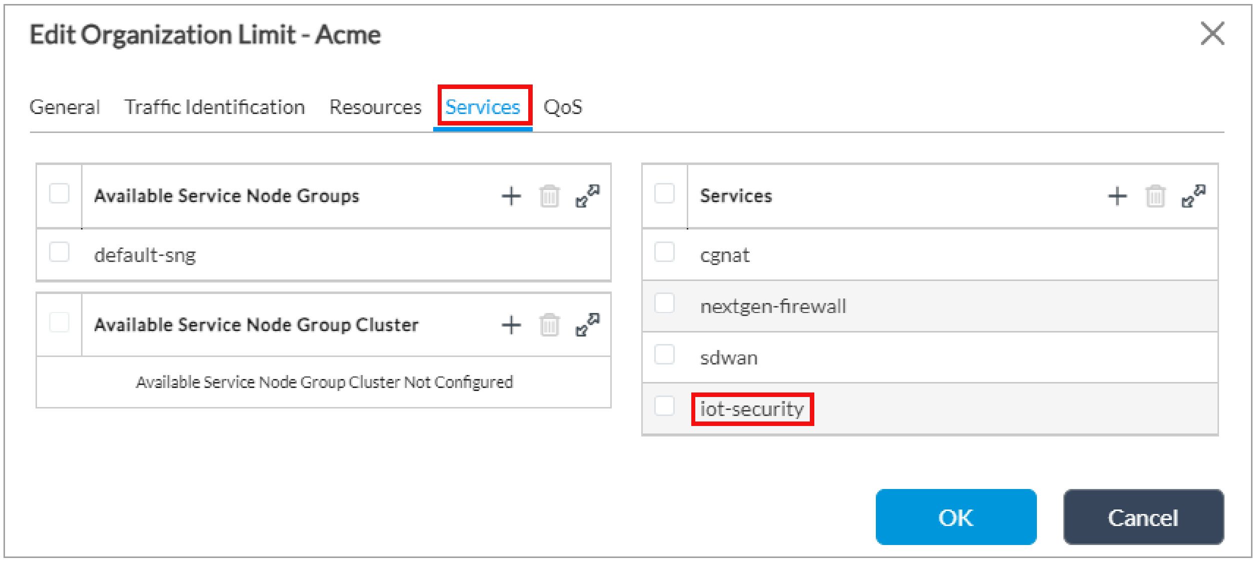
1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. In the main pane, click the name of the VOS device. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > Organization > Limits in the left menu bar. The main pane displays the organizations that are already configured.



| | Organization Name | Appliance Owner | Enterprise Names | Services | Service Node Groups | Service Node Group Clus | Peak Rate (pps) |
|---|---|---|---|---|---|---|---|
| ☐ | Acme | True | | cgnat<br>nextgen-firewall<br>sdwan<br>View More... | default-sng | | |

Rows per page 25 Showing 1 - 1 of 1

4. Click the name of the organization. The Edit Organization Limit popup window displays.
5. Select the Services tab.


Edit Organization Limit - Acme

| ☐ | Available Service Node Groups |
|---|---|
| ☐ | default-sng |

| ☐ | Available Service Node Group Cluster |
|---|---|
| | Available Service Node Group Cluster Not Configured |

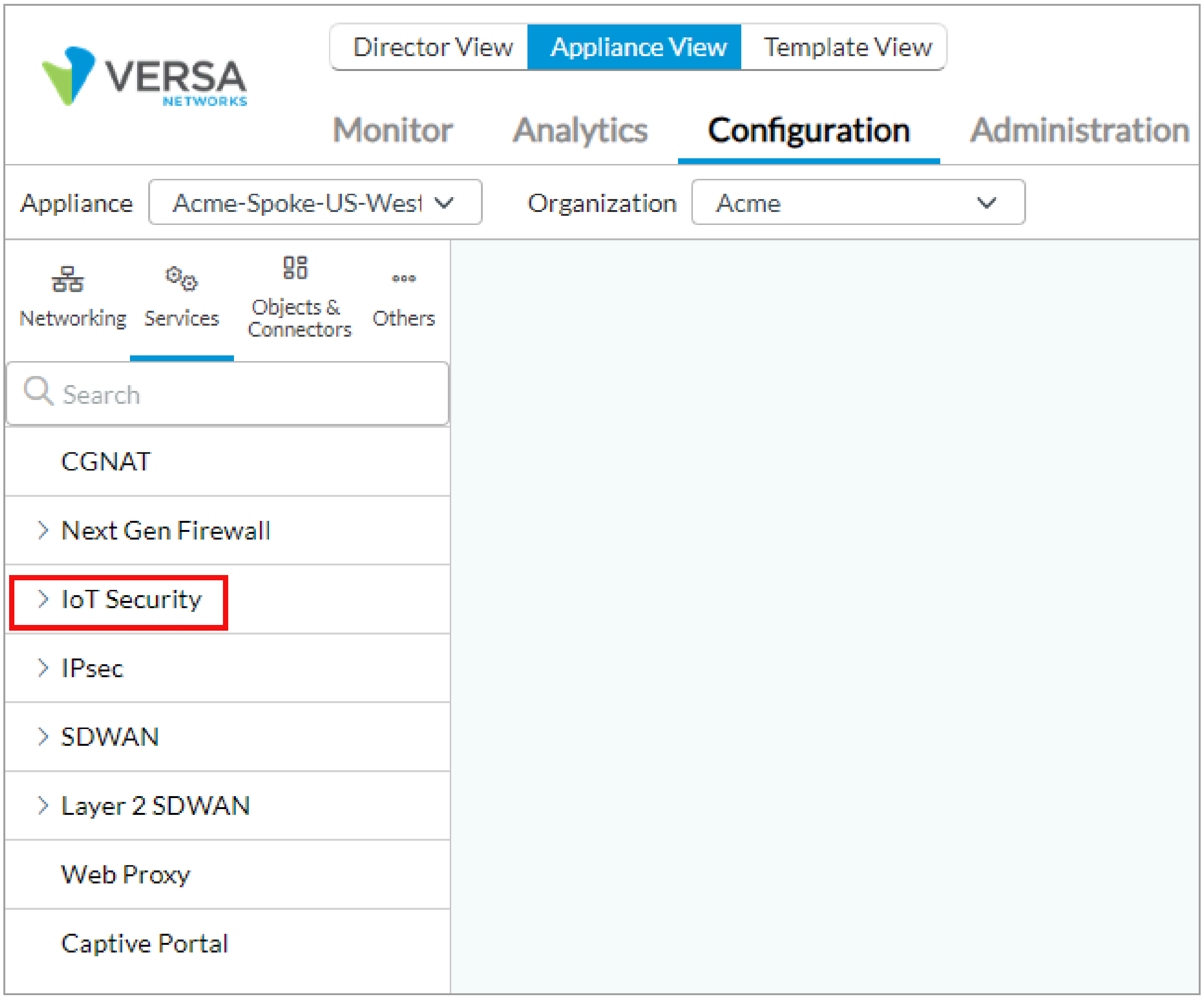
| ☐ | Services |
|---|---|
| ☐ | cgnat |
| ☐ | nextgen-firewall |
| ☐ | sdwan |
| ☐ | iot-security |

6. In the Services table, click the  Add icon and then select iot-security.
7. Click OK.

8. Refresh the browser window.

To view the IoT Security menu:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliance in the left menu bar.
   c. Select the device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > IoT Security.

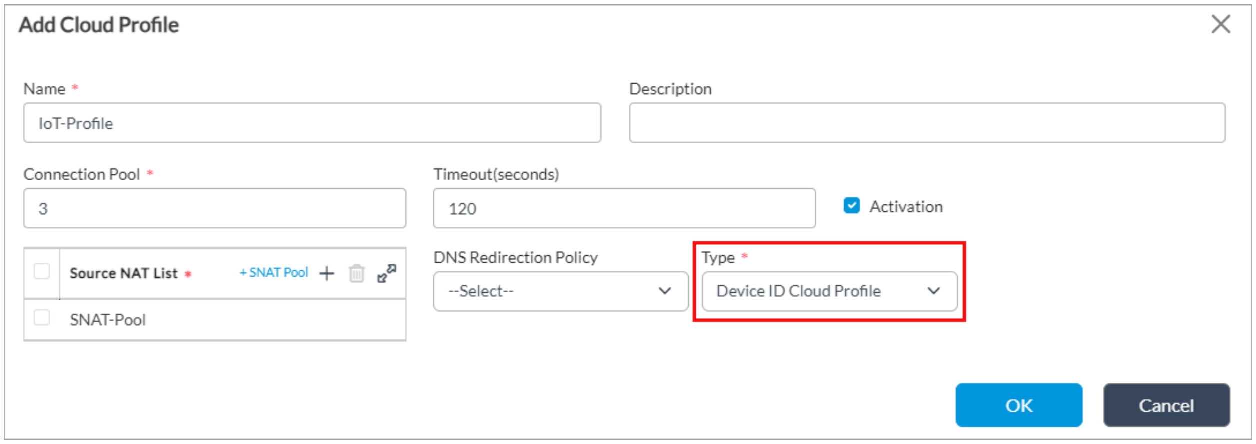


## Configure a Cloud Profile for IoT Security

To enable cloud device lookup on a VOS device, you must configure a cloud profile to look up device insights on the Versa cloud server.

To configure a cloud profile:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Cloud Profiles in the left menu bar.
4. Click the + Add icon. In the Add Cloud Profile window, enter information for the following fields.



Add Cloud Profile

Name * IoT-Profile

Description

Connection Pool * 3

Timeout(seconds) 120

☑ Activation

Source NAT List * 
SNAT-Pool

DNS Redirection Policy --Select--

Type * Device ID Cloud Profile

5. In the Name field, enter a name for the cloud profile.
6. In the Connection Pool field, enter the number of simultaneous connections to the SSL cloud server.
7. Click Activation to activate the cloud lookup profile.
8. From Source NAT List, select the SNAT pool to configure cloud lookup for IoT devices and click the + icon. The SNAT pool is linked to a routing instance that connects to the cloud server. For more information, see Configure SNAT Pools.
9. In the Type field, select Device ID Cloud Profile.
10. For information about configuring other parameters, see Configure a Cloud Profile.
11. Click OK.

## Modify IoT Security Settings

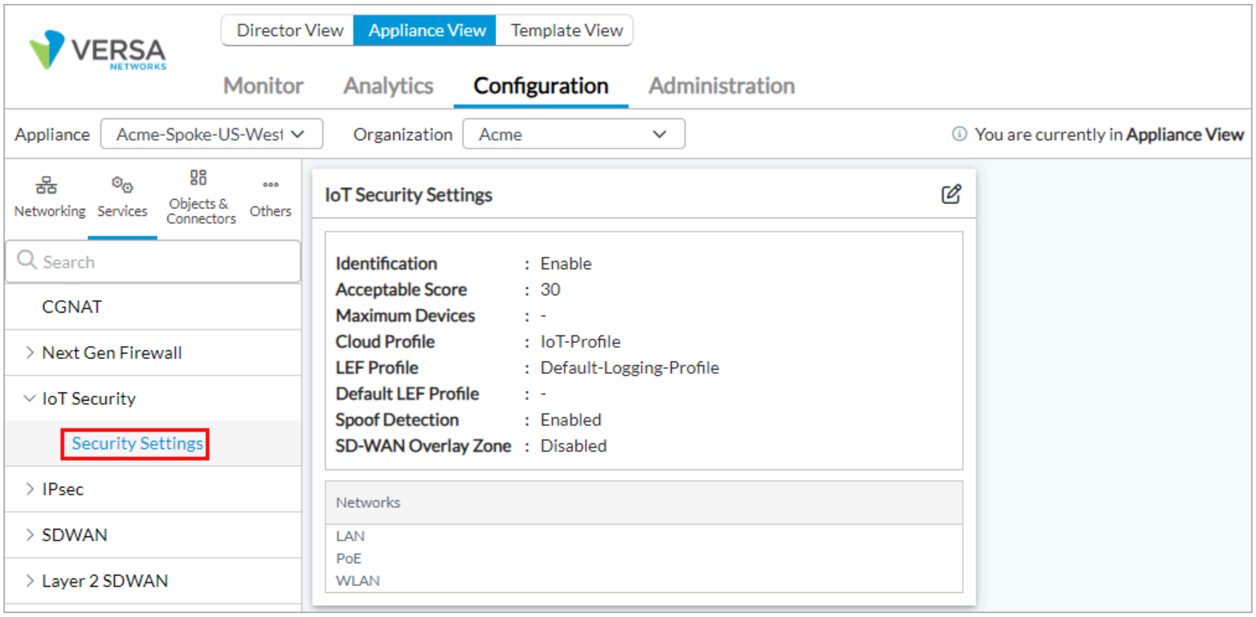
After you enable IoT security for the VOS device and organizations, you can edit the IoT security settings to enable device identification and to add a cloud profile.

To edit the IoT security settings:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliance in the left menu bar.

   c. Select the device in the main pane. The view changes to Appliance view.

2. Select the Configuration tab in the top menu bar.
3. Select Services > IoT Security > Security Settings.

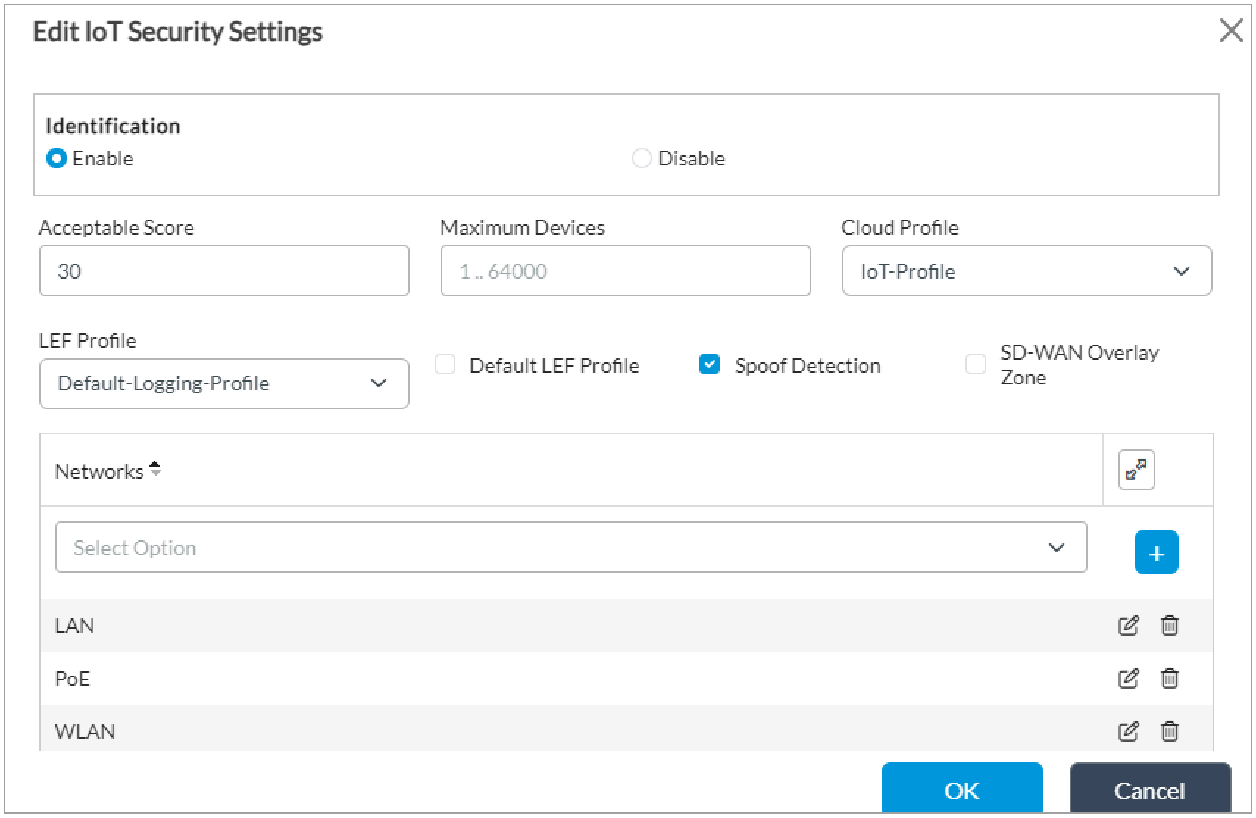


IoT Security Settings

| | |
|---|---|
| Identification | : Enable |
| Acceptable Score | : 30 |
| Maximum Devices | : - |
| Cloud Profile | : IoT-Profile |
| LEF Profile | : Default-Logging-Profile |
| Default LEF Profile | : - |
| Spoof Detection | : Enabled |
| SD-WAN Overlay Zone | : Disabled |

| Networks |
|---|
| LAN |
| PoE |
| WLAN |

4. Click the ✎ Edit icon. In the Edit IoT Security Settings window, enter information for the following fields.



Edit IoT Security Settings

Identification

● Enable ○ Disable

Acceptable Score: 30

Maximum Devices: 1 .. 64000

Cloud Profile: IoT-Profile

LEF Profile: Default-Logging-Profile

□ Default LEF Profile ☑ Spoof Detection □ SD-WAN Overlay Zone

Networks

Select Option

LAN

PoE

WLAN

| Field | Description |
|---|---|
| Identification (Group of Fields) | Enter a name for the IoT device. |
| ◦ Enable | Click to enable IoT security for the device. |
| ◦ Disable | Click to disable IoT security for the device. |
| Acceptable Score | Enter an acceptance score for device confidence. The VOS software provides a confidence score based on a scale of 0 through 100. The higher the value, the higher the device confidence.<br>*Default*: 30. It is recommended that you retain the default score of 30. |
| Maximum Devices | Enter the maximum number of devices that IoT security supports.<br>*Value*: 1 through 64000 |
| Cloud Profile | Select the cloud profile to use for cloud lookup that you configured in Configure a Cloud Profile for IoT Security, above. To add a new profile, click + Add New. For more information, see Configure a Cloud Profile. |
| LEF Profile | Select a log export functionality (LEF) profile to use to record logs for the file-filtering profile. For information about configuring a LEF profile see Configure Log Export Functionality. For information about applying a LEF profile to a feature or service, see Apply Log Export Functionality. |
| Default LEF Profile | Click to use the default LEF profile instead of the LEF profile from the previous field. |
| Spoof Detection | Click to enable spoof detection, which enables the VOS software to identify devices that spoof existing IoT devices. For example, if a device tries to spoof the MAC address and IP address of another device, the VOS software detects the device. |
| SD-WAN Overlay Zone | Click to enable device fingerprinting on the SD-WAN |

| | |
|---|---|
| | overlay. Enabling device fingerprinting on SD-WAN overlay may result in lower device confidence scores, because device insights may not translate correctly. |
| Networks | Select the networks that you want IoT security to target. For example, LAN or WLAN. If you do not specify any network, IoT security is enabled on all networks. |

5. Click OK.

## View Predefined IoT Security Objects

The VOS software provides a list of predefined IoT devices, device filters, and tags along with the Versa security package (SPack). You can view these predefined IoT objects from Versa Director. The predefined IoT security objects are updated regularly through the (SPack) updates, and you can update them at any time, by installing the latest SPack. Installing an SPack has no impact to the operation of the Director nodes and VOS devices. For more information, see Use Security Packages.

To provide feedback for adding or modifying the predefined objects, send email to support@versa-networks.com.

The VOS software classifies devices based on the following attributes:

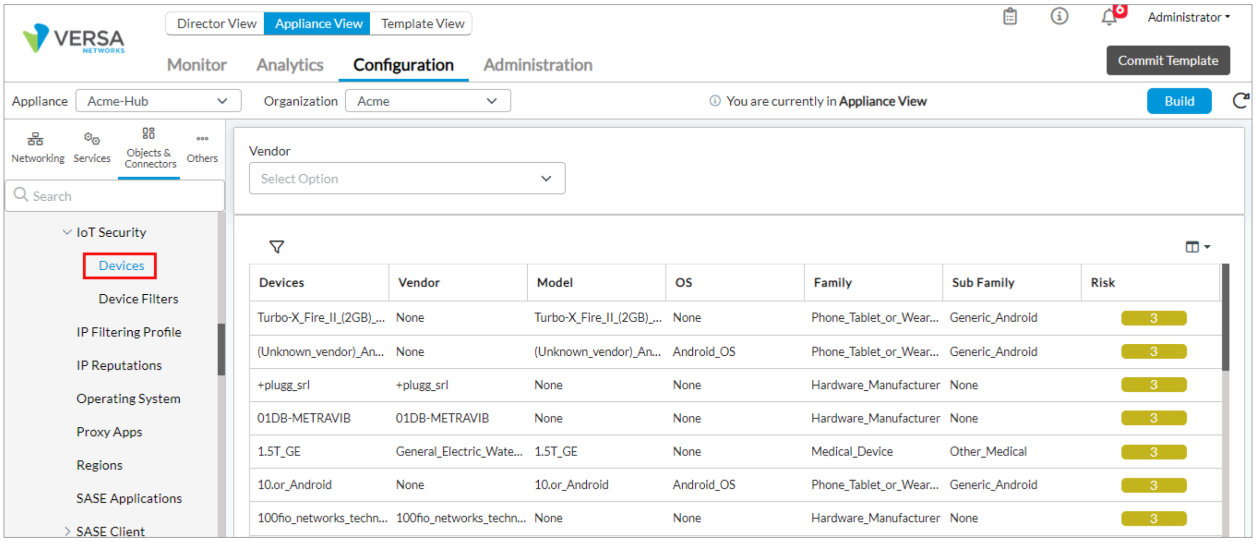
- Name—Human-readable identifier of the device.
- MAC and IP address—MAC and IP addresses of the device.
- Identified—Boolean value that indicates whether the IoT device is identified.;
- Configured—Boolean value that indicates whether the IoT device is user configured.
- Vendor—Name of the device vendor, for example, Apple.
- Model—Model of the device, for example, iPhone.
- OS—Operating system of the device, for example, iOS, Linux, and Windows.
- Family—General category of the device, such as printer or gaming console.
- Subfamily—More specific information about the device category, for example, Xiaomi printer or Xbox.
- Risk—Risk level of the device, which is a value in the range 0 through 5. A lower value indicates a lower risk level.

This section describes how to view predefined IoT security devices and device filters.

### View Predefined IoT Security Devices

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a template in the main pane. The view changes to Appliance view.

2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Objects > Predefined > IoT Security > Devices in the left menu bar.

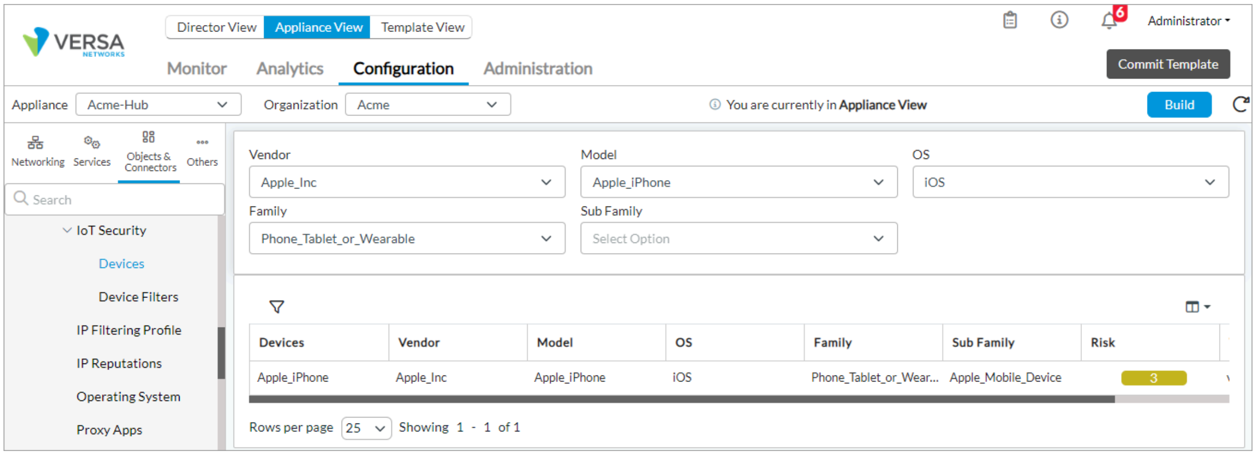


Appliance: Acme-Hub
Organization: Acme
You are currently in **Appliance View**

Vendor: Select Option

| Devices | Vendor | Model | OS | Family | Sub Family | Risk |
|---|---|---|---|---|---|---|
| Turbo-X_Fire_II_(2GB)_... | None | Turbo-X_Fire_II_(2GB)_... | None | Phone_Tablet_or_Wear... | Generic_Android | 3 |
| (Unknown_vendor)_An... | None | (Unknown_vendor)_An... | Android_OS | Phone_Tablet_or_Wear... | Generic_Android | 3 |
| +plugg_srl | +plugg_srl | None | None | Hardware_Manufacturer | None | 3 |
| 01DB-METRAVIB | 01DB-METRAVIB | None | None | Hardware_Manufacturer | None | 3 |
| 1.5T_GE | General_Electric_Wate... | 1.5T_GE | None | Medical_Device | Other_Medical | 3 |
| 10.or_Android | None | 10.or_Android | Android_OS | Phone_Tablet_or_Wear... | Generic_Android | 3 |
| 100fio_networks_techn... | 100fio_networks_techn... | None | None | Hardware_Manufacturer | None | 3 |

4. To filter the devices to display, select a vendor in the Vendor column. This displays the Model field.
5. To filter further, select a model and then the OS of the device, if applicable. For example, the following screenshot displays the options for Apple iPhone.



Appliance: Acme-Hub
Organization: Acme
You are currently in **Appliance View**

Vendor: Apple_Inc
Model: Apple_iPhone
OS: iOS
Family: Phone_Tablet_or_Wearable
Sub Family: Select Option

| Devices | Vendor | Model | OS | Family | Sub Family | Risk |
|---|---|---|---|---|---|---|
| Apple_iPhone | Apple_Inc | Apple_iPhone | iOS | Phone_Tablet_or_Wear... | Apple_Mobile_Device | 3 |

Rows per page 25 Showing 1 - 1 of 1

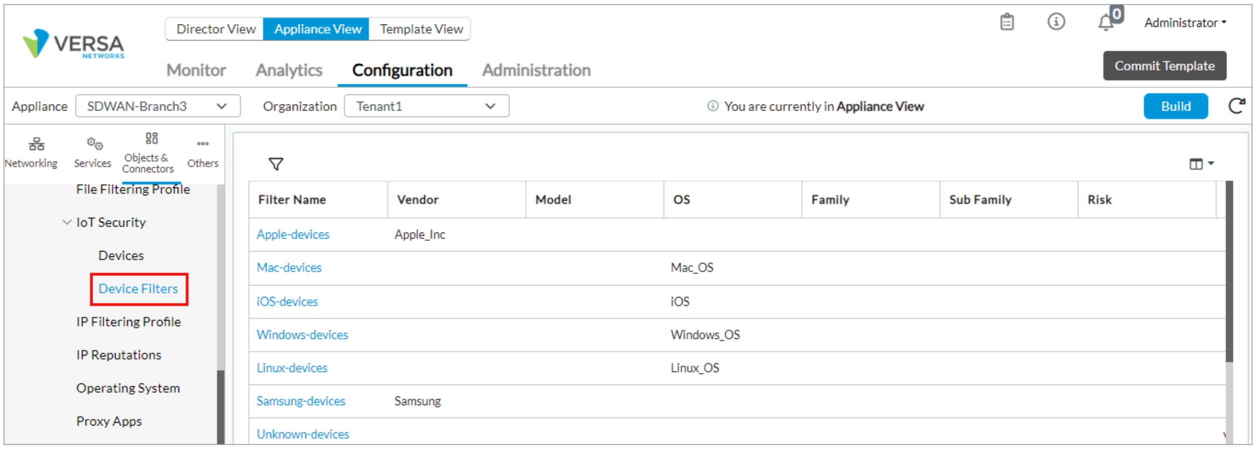
You use IoT device filters in security rules to filter traffic. You can use predefined devices in rules and also view them as examples to configure custom IoT device filters.

## View Predefined IoT Security Device Filters

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.

    d. Select a template in the main pane. The view changes to Appliance view.

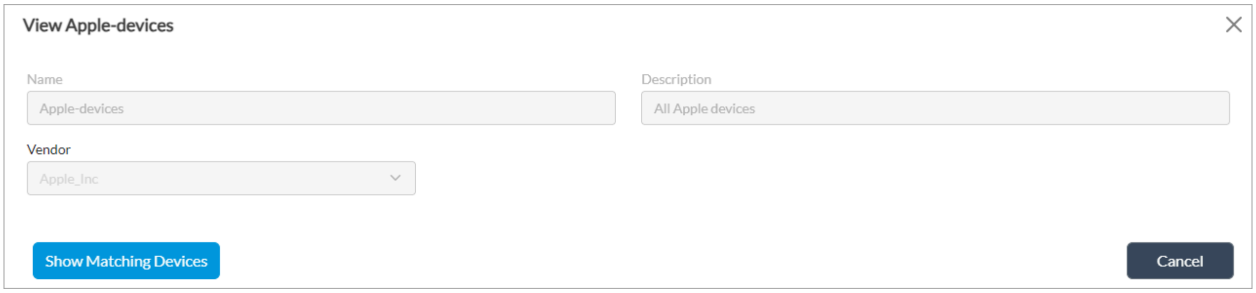
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Objects > Predefined > IoT Security > Device Filters in the left menu bar.



Appliance: SDWAN-Branch3
Organization: Tenant1
You are currently in **Appliance View**

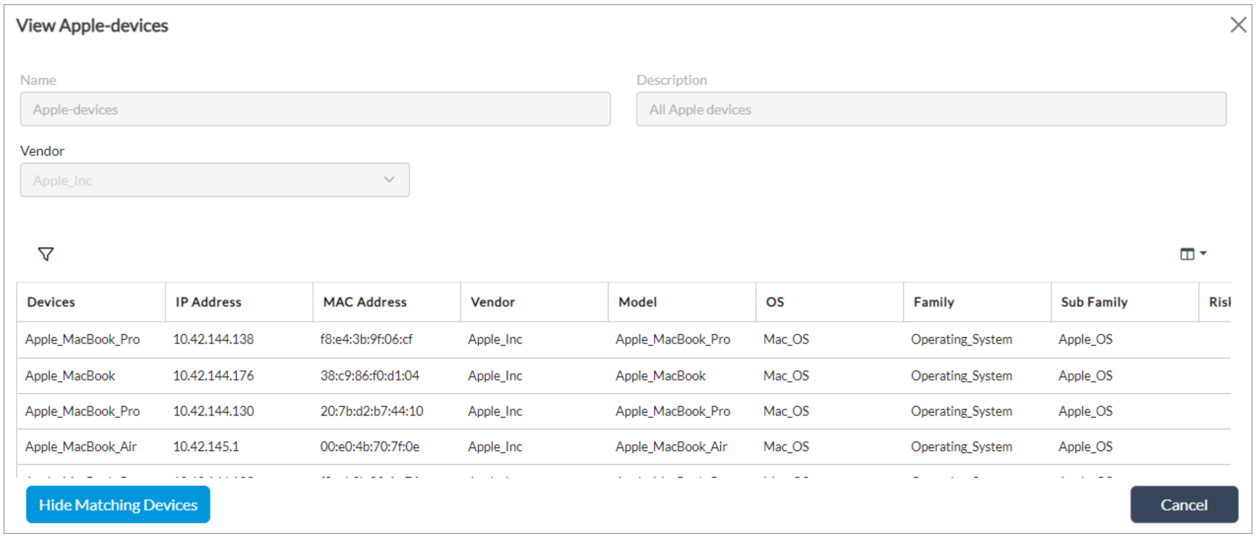
| Filter Name | Vendor | Model | OS | Family | Sub Family | Risk |
|---|---|---|---|---|---|---|
| Apple-devices | Apple_Inc | | | | | |
| Mac-devices | | | Mac_OS | | | |
| iOS-devices | | | iOS | | | |
| Windows-devices | | | Windows_OS | | | |
| Linux-devices | | | Linux_OS | | | |
| Samsung-devices | Samsung | | | | | |
| Unknown-devices | | | | | | |

4. Click a device filter name to view details.


View Apple-devices

Name: Apple-devices
Description: All Apple devices
Vendor: Apple_Inc

5. Click Show Matching Devices to view devices that match the filter. For example, the following screenshot displays the devices that belong to the device filter called Apple-devices.


View Apple-devices

Name: Apple-devices
Description: All Apple devices
Vendor: Apple_Inc

| Devices | IP Address | MAC Address | Vendor | Model | OS | Family | Sub Family | Risl |
|---|---|---|---|---|---|---|---|---|
| Apple_MacBook_Pro | 10.42.144.138 | f8:e4:3b:9f:06:cf | Apple_Inc | Apple_MacBook_Pro | Mac_OS | Operating_System | Apple_OS | |
| Apple_MacBook | 10.42.144.176 | 38:c9:86:f0:d1:04 | Apple_Inc | Apple_MacBook | Mac_OS | Operating_System | Apple_OS | |
| Apple_MacBook_Pro | 10.42.144.130 | 20:7b:d2:b7:44:10 | Apple_Inc | Apple_MacBook_Pro | Mac_OS | Operating_System | Apple_OS | |
| Apple_MacBook_Air | 10.42.145.1 | 00:e0:4b:70:7f:0e | Apple_Inc | Apple_MacBook_Air | Mac_OS | Operating_System | Apple_OS | |

# Configure Custom IoT Security Objects

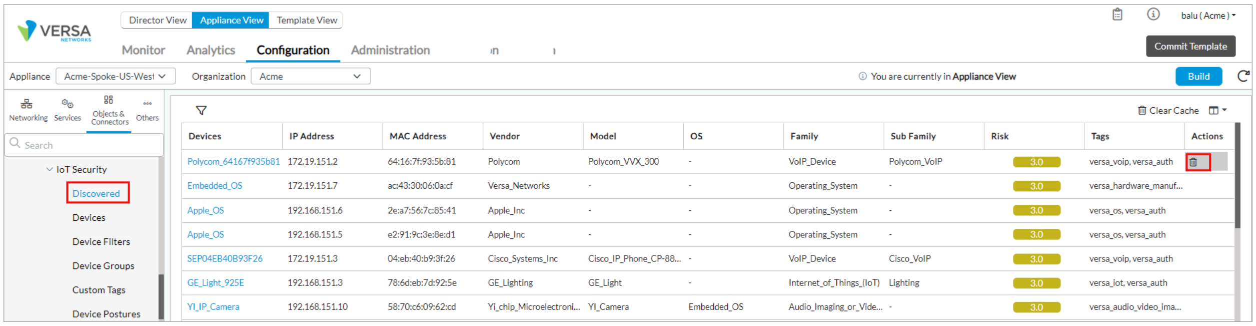
This section describes how to modify IoT devices that the VOS software discovers and identifies, and to configure custom IoT devices, device filters, device groups, and tags.

## Modify Discovered Devices

After you enable IoT security, the VOS device starts to discover and identify devices that enter your network traffic.

To view and modify discovered devices:

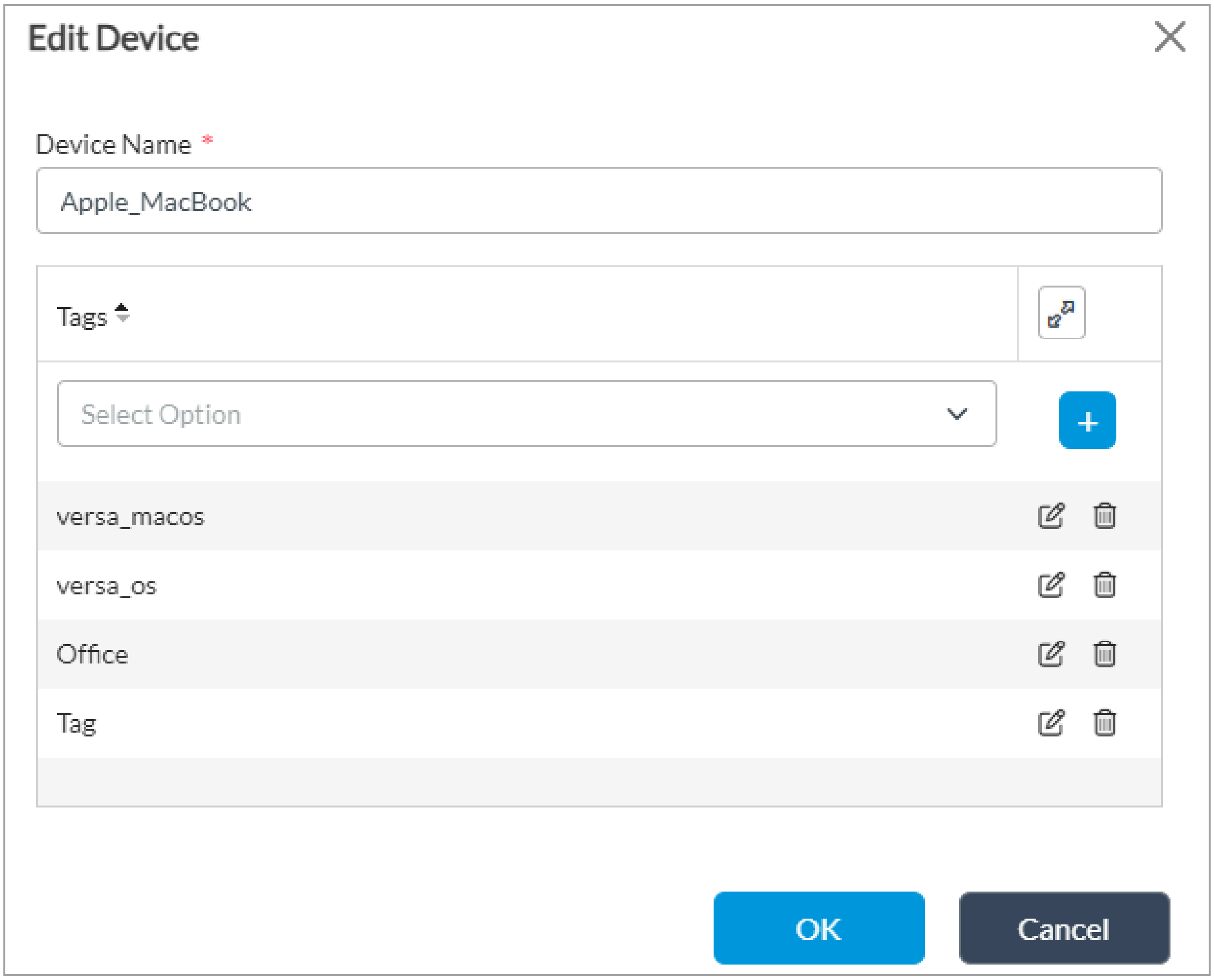
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Objects > Custom Objects > IoT Security > Discovered in the left menu bar.



| Devices | IP Address | MAC Address | Vendor | Model | OS | Family | Sub Family | Risk | Tags | Actions |
|---|---|---|---|---|---|---|---|---|---|---|
| Polycom_64167f935b81 | 172.19.151.2 | 64:16:7f:93:5b:81 | Polycom | Polycom_VVX_300 | - | VoIP_Device | Polycom_VoIP | 3.0 | versa_voip, versa_auth | 🗑 |
| Embedded_OS | 172.19.151.7 | ac:43:30:06:0a:cf | Versa_Networks | - | - | Operating_System | - | 3.0 | versa_hardware_manuf... | |
| Apple_OS | 192.168.151.6 | 2e:a7:56:7c:85:41 | Apple_Inc | - | - | Operating_System | - | 3.0 | versa_os, versa_auth | |
| Apple_OS | 192.168.151.5 | e2:91:9c:3e:8e:d1 | Apple_Inc | - | - | Operating_System | - | 3.0 | versa_os, versa_auth | |
| SEP04EB40B93F26 | 172.19.151.3 | 04:eb:40:b9:3f:26 | Cisco_Systems_Inc | Cisco_IP_Phone_CP-88... | - | VoIP_Device | Cisco_VoIP | 3.0 | versa_voip, versa_auth | |
| GE_Light_925E | 192.168.151.3 | 78:6d:eb:7d:92:5e | GE_Lighting | GE_Light | - | Internet_of_Things_(IoT) | Lighting | 3.0 | versa_iot, versa_auth | |
| YI_IP_Camera | 192.168.151.10 | 58:70:c6:09:62:cd | Yi_chip_Microelectroni... | YI_Camera | Embedded_OS | Audio_Imaging_or_Vide... | - | 3.0 | versa_audio_video_ima... | |

4. To clear all entries, click Clear Cache.

5. To clear an individual entry, hover your mouse in the Action column, and then click the 🗑 Delete icon.
6. Click on the device name to modify the discovered device. The Edit Device popup window displays. Note that you can only edit discovered devices and not custom (user-defined) devices.



Edit Device

Device Name *

Apple_MacBook

versa_macos

versa_os

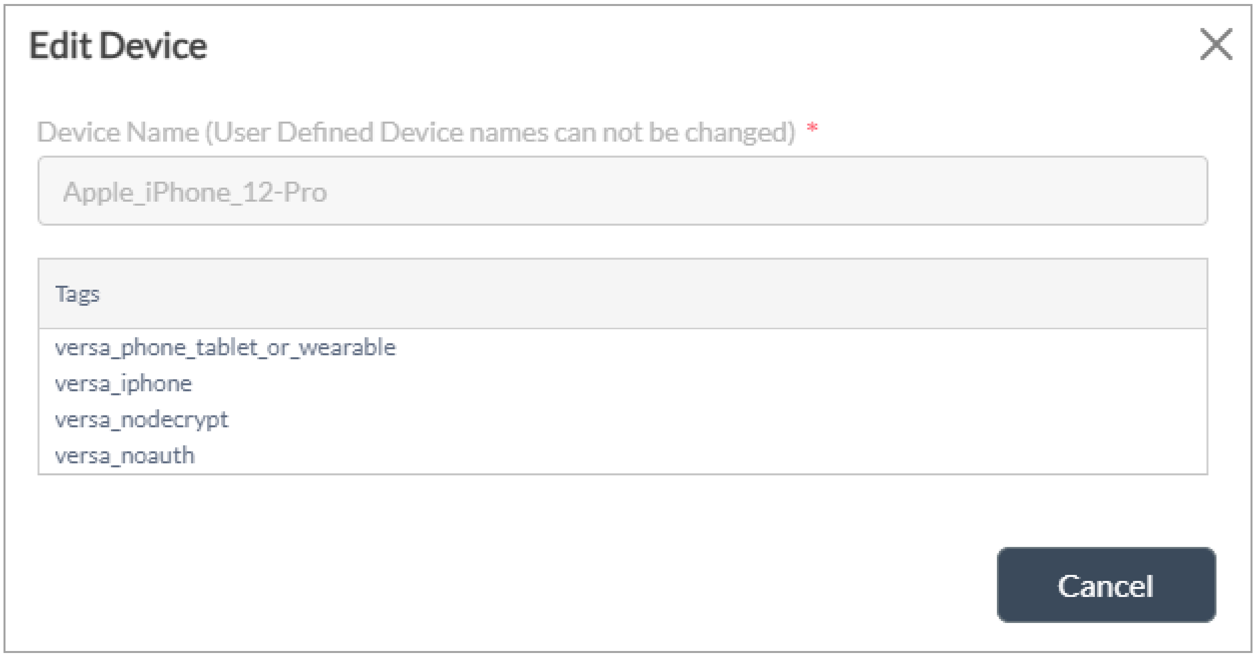
Office

Tag

7. Edit the device name, if required.

8. To add one or more tags to the device, select a tag and click the + Add icon. Note that tags preceded by 'versa_' are predefined tags.
9. Click OK.

If you select a user-defined device, the fields in the Edit Device window display as read-only, as shown in the following screenshot. For more information about user-defined or custom devices, see Configure Custom IoT Security Devices below.



Edit Device

Device Name (User Defined Device names can not be changed) *

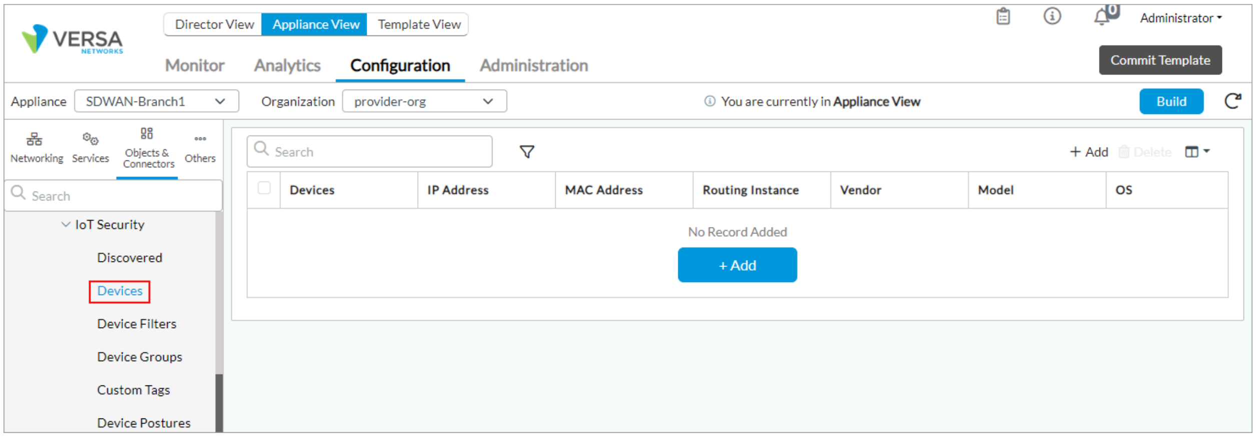
Apple_iPhone_12-Pro

Tags

versa_phone_tablet_or_wearable
versa_iphone
versa_nodecrypt
versa_noauth

## Configure Custom IoT Security Devices

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Objects > Custom Objects > IoT Security > Devices in the left menu bar.

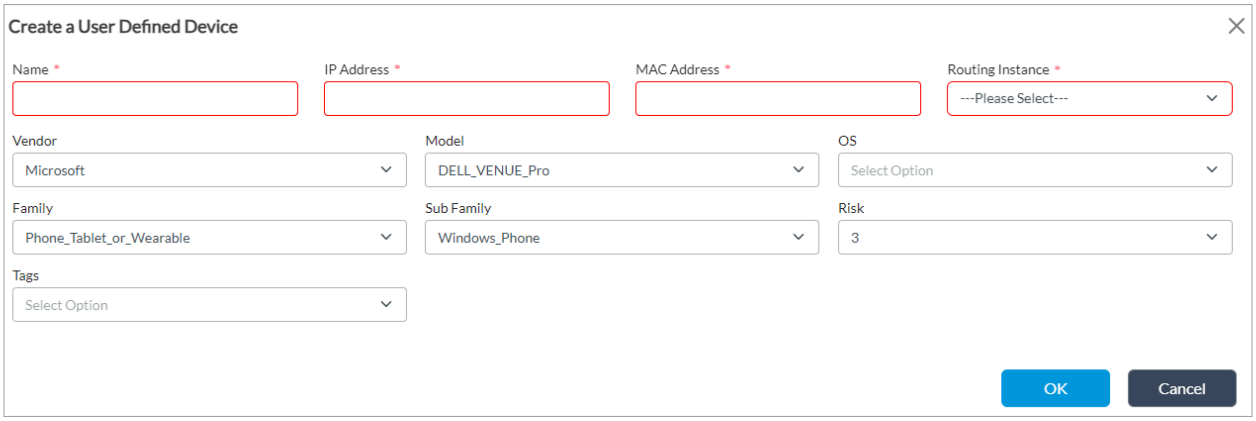


Appliance: SDWAN-Branch1
Organization: provider-org
You are currently in Appliance View

| Devices | IP Address | MAC Address | Routing Instance | Vendor | Model | OS |
|---|---|---|---|---|---|---|

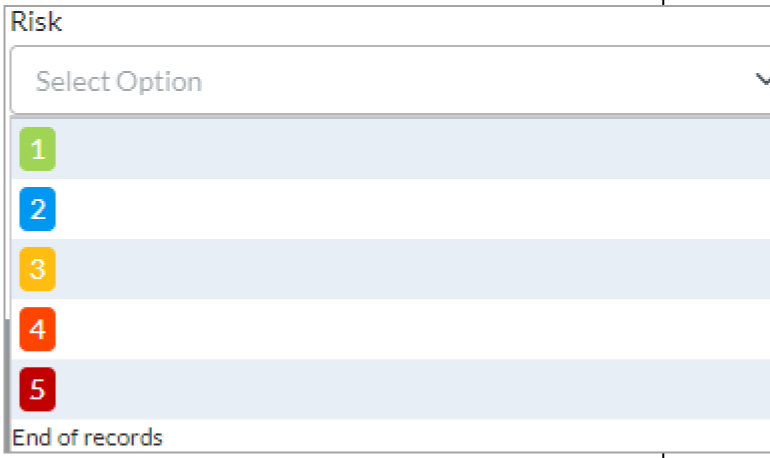
No Record Added

4. Click + Add and enter the following information in the Create a User Defined Device window.



Create a User Defined Device

| | | | |
|---|---|---|---|
| Name * | IP Address * | MAC Address * | Routing Instance * |
| | | | ---Please Select--- |
| Vendor | Model | OS | |
| Microsoft | DELL_VENUE_Pro | Select Option | |
| Family | Sub Family | Risk | |
| Phone_Tablet_or_Wearable | Windows_Phone | 3 | |
| Tags | | | |
| Select Option | | | |

| Field | Description |
|---|---|
| Name | Enter a name for the IoT device. |
| IP Address | Enter the IP address of the device. |
| MAC Address | Enter the MAC address of the device. |
| Routing Instance | Select the routing instance to associate with the device. |
| Vendor | Select a vendor associated with the device. When you select a vendor, the Model field displays. |
|  | Options for the following fields display based on the vendor you select. For example, if you select Apple_Inc as the vendor, the subsequent fields display options for Apple. |
| Model | Select the model of the IoT device. |
| OS | Select the operating system of the device. |
| Family | Select the family of the device. For example, Phone_Tablet_or_Wearable, for mobile phone, table, or a wearable smart device. |
| Sub Family | Select the sub family category such as Windows_Phone or Apple_Mobile_Device. |
| Risk | Select the risk of the device in the range of 0 through 5. A lower value indicates lower risk, as indicated in the color of each value:<br> Risk<br>Select Option<br>1<br>2<br>3<br>4<br>5<br>End of records |
| Tags | Select a predefined or custom tag to associate with the device. Use tags to group devices from different |

| | |
|---|---|
| | vendors and family into one group. |

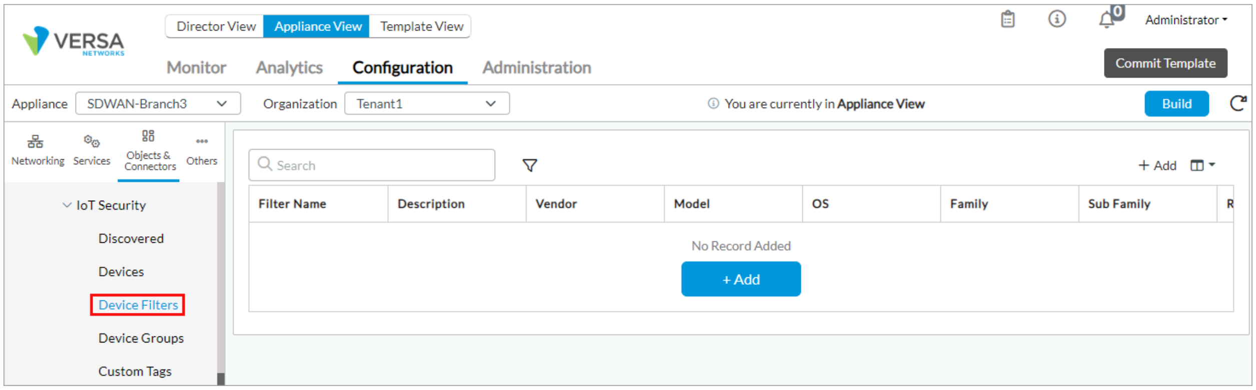
5. Click OK.

## Configure Custom IoT Security Device Filters

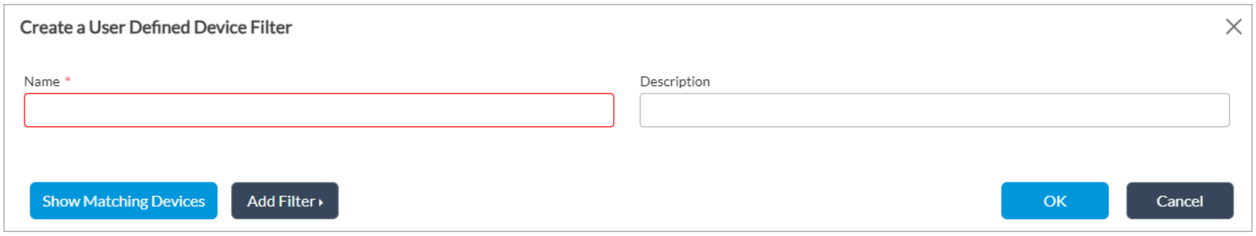
You configure device filters based on device attributes, and use them in security filter policies.

To configure an IoT security device filter:

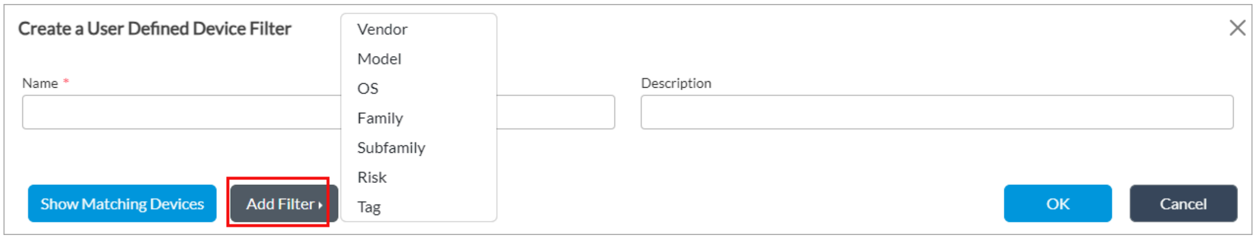
1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Templates > Device Templates in the horizontal menu bar.
    c. Select an organization in the left menu bar.
    d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Objects > Custom Objects > IoT Security > Device Filters in the left menu bar.



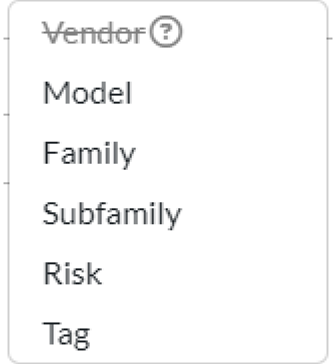
4. Click + Add and enter the following information in the Create a User Defined Device Filter window.



5. Enter a name for the device filter.
6. Enter a description for the device filter.
7. Click Add Filter and select from the options Vendor, Model, OS, Family, Subfamily, Risk, and Tag.

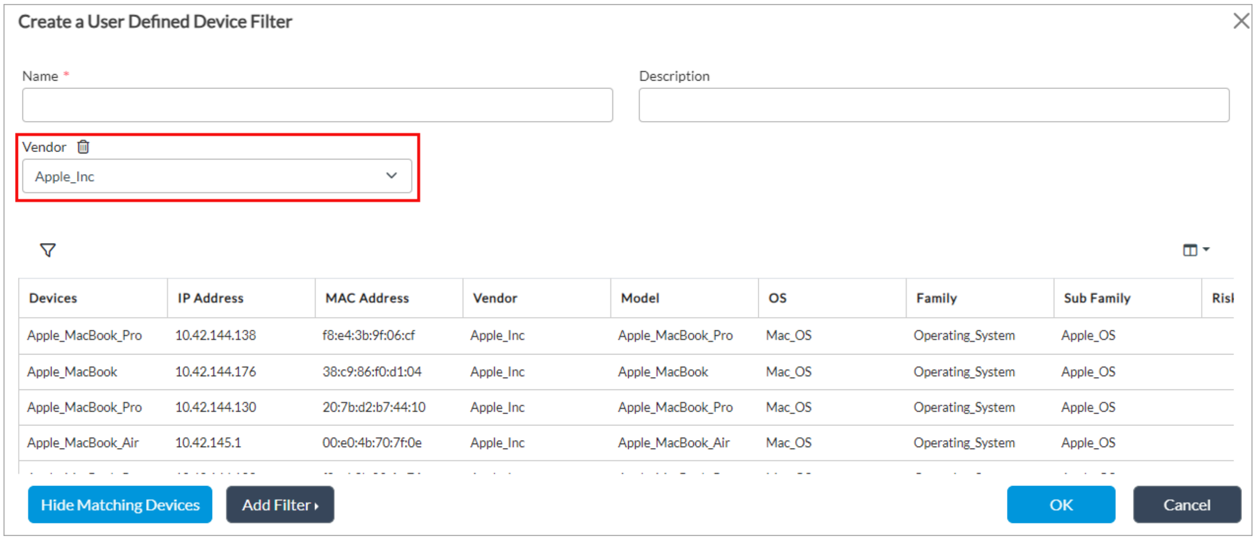


Note that if you first select an option other than Vendor, Vendor is temporarily disabled when you click Add Filter again, as shown in the following screenshot:



8. Click Show Matching Devices to display devices based on your filter. The Show Matching Devices option allows you to confirm the devices to include in your device filter. The following two screenshots display devices based on the filters Vendor and Tags:

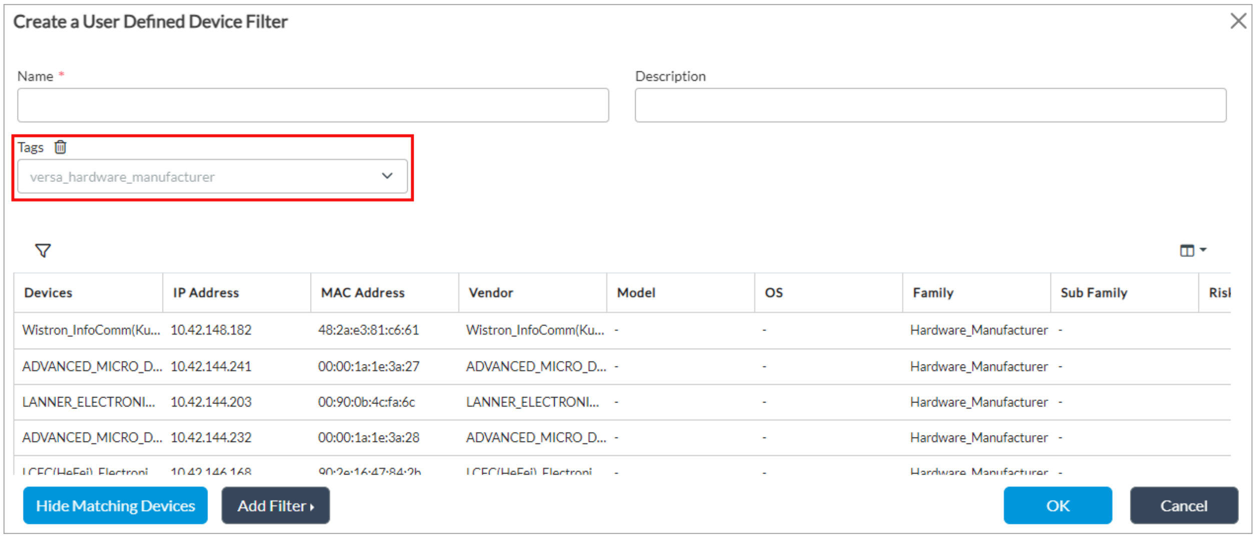
   Devices for Vendor Apple_Inc:



Vendor: Apple_Inc

| Devices | IP Address | MAC Address | Vendor | Model | OS | Family | Sub Family | Risl |
|---|---|---|---|---|---|---|---|---|
| Apple_MacBook_Pro | 10.42.144.138 | f8:e4:3b:9f:06:cf | Apple_Inc | Apple_MacBook_Pro | Mac_OS | Operating_System | Apple_OS | |
| Apple_MacBook | 10.42.144.176 | 38:c9:86:f0:d1:04 | Apple_Inc | Apple_MacBook | Mac_OS | Operating_System | Apple_OS | |
| Apple_MacBook_Pro | 10.42.144.130 | 20:7b:d2:b7:44:10 | Apple_Inc | Apple_MacBook_Pro | Mac_OS | Operating_System | Apple_OS | |
| Apple_MacBook_Air | 10.42.145.1 | 00:e0:4b:70:7f:0e | Apple_Inc | Apple_MacBook_Air | Mac_OS | Operating_System | Apple_OS | |

   Devices for Tag versa_hardware_manufacturer (predefined tag):



Tags: versa_hardware_manufacturer

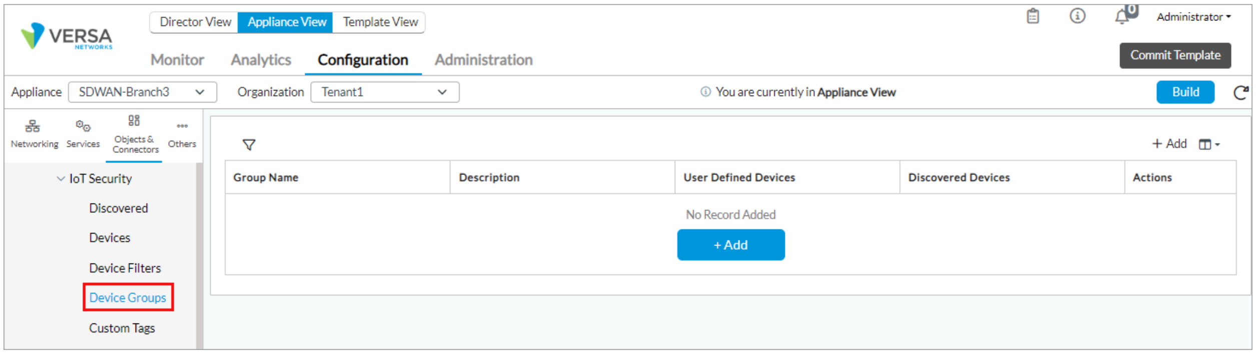
| Devices | IP Address | MAC Address | Vendor | Model | OS | Family | Sub Family | Risl |
|---|---|---|---|---|---|---|---|---|
| Wistron_InfoComm(Ku... | 10.42.148.182 | 48:2a:e3:81:c6:61 | Wistron_InfoComm(Ku... | - | - | Hardware_Manufacturer | - | |
| ADVANCED_MICRO_D... | 10.42.144.241 | 00:00:1a:1e:3a:27 | ADVANCED_MICRO_D... | - | - | Hardware_Manufacturer | - | |
| LANNER_ELECTRONI... | 10.42.144.203 | 00:90:0b:4c:fa:6c | LANNER_ELECTRONI... | - | - | Hardware_Manufacturer | - | |
| ADVANCED_MICRO_D... | 10.42.144.232 | 00:00:1a:1e:3a:28 | ADVANCED_MICRO_D... | - | - | Hardware_Manufacturer | - | |
| LCFC(HeFei) Electroni | 10.42.146.168 | 90:2e:16:47:84:2b | LCFC(HeFei) Electroni | - | - | Hardware_Manufacturer | - | |

9. Click OK.

## Configure Custom IoT Security Device Groups

Device groups allow you to group discovered and custom devices in a group. You can use these groups to configure security rules.

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Objects > Custom Objects > IoT Security > Device Groups in the left menu bar.



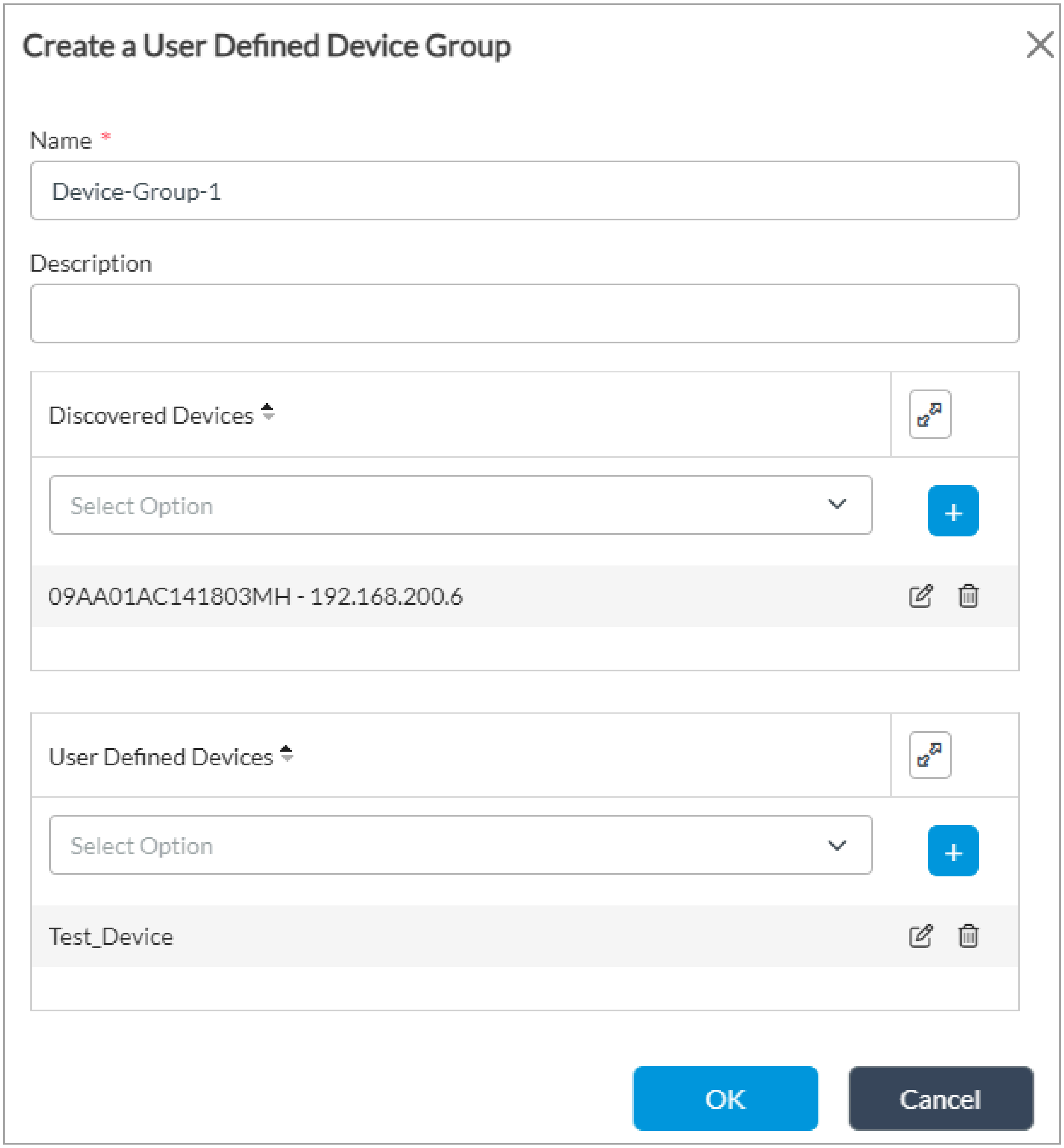
Appliance: SDWAN-Branch3 Organization: Tenant1

You are currently in **Appliance View**

| Group Name | Description | User Defined Devices | Discovered Devices | Actions |
|---|---|---|---|---|

No Record Added

4. Click + Add and enter the following information in the Create a User Defined Device Group window.



Create a User Defined Device Group

Name *

Device-Group-1

Description

Discovered Devices

Select Option

09AA01AC141803MH - 192.168.200.6

User Defined Devices

Select Option

Test_Device

| Field | Description |
|---|---|
| Name | Enter a name for the device group. |
| Description | Enter a text description for the device group. |
| Discovered Devices | Select one or more discovered devices to associate with the device group and click the + Add icon to add. For more information, see Modify Discovered Devices, above. |
| User Defined Devices | Select one or more user-defined devices to associate with the device group and click the + Add icon to add. For more information, see Configure Custom IoT Security Devices, above. |

5. Click OK.

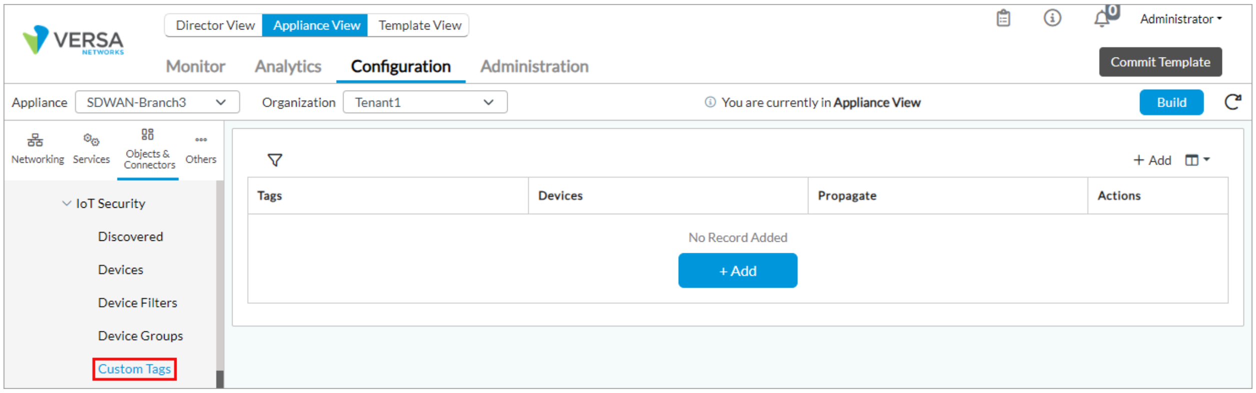
## Configure Custom IoT Security Tags

A custom tag is additional information that you can associate with a device. You can associate more than one tag with a device. Tags help group devices from different vendors and families together. For example, you can group an Apple watch and a Samsung watch in the tag "smart-watch." You can use specific custom tags to authenticate or decrypt IoT devices. For more information, see Use Custom Tags for Authentication and Decryption, below.

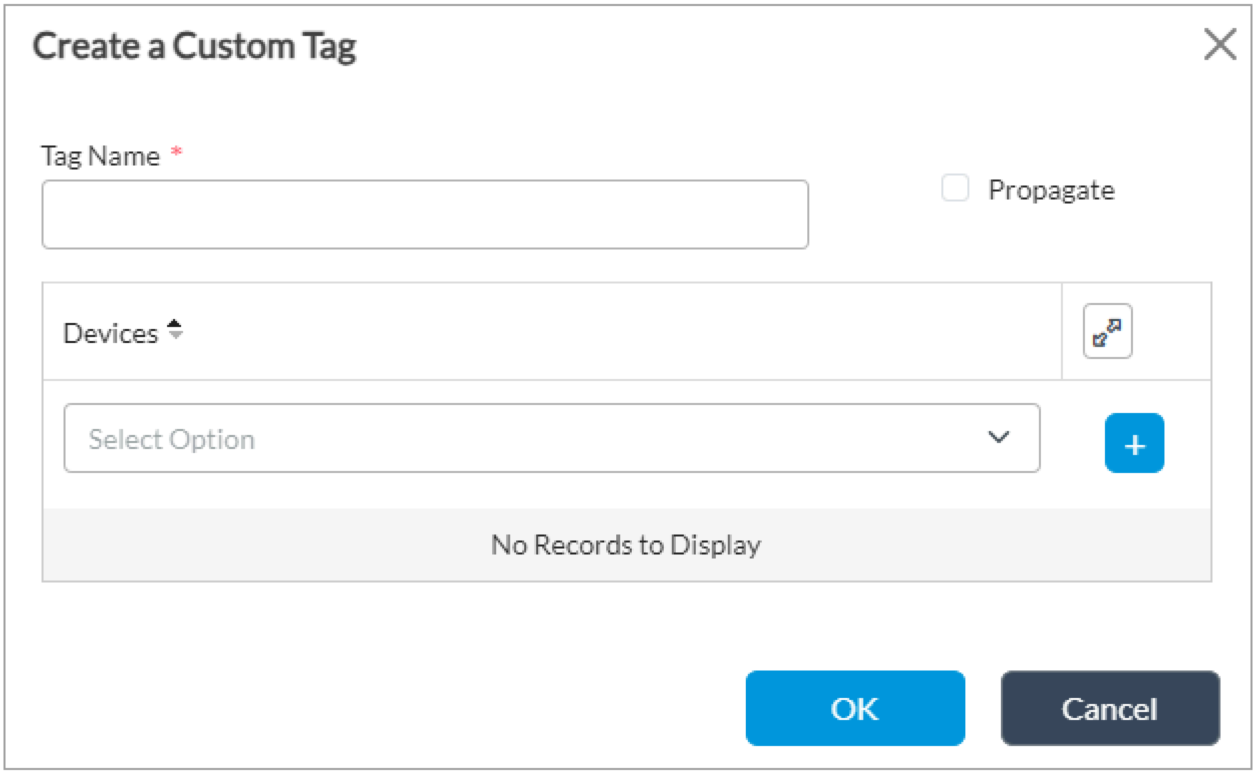
You can use tags to define custom device filters and use these filters in policy rules. You can also update the tags for a discovered device. For more information, see Modify Discovered Devices, above. The VOS software SPacks also provide predefined tags.

To configure a custom IoT security tag:

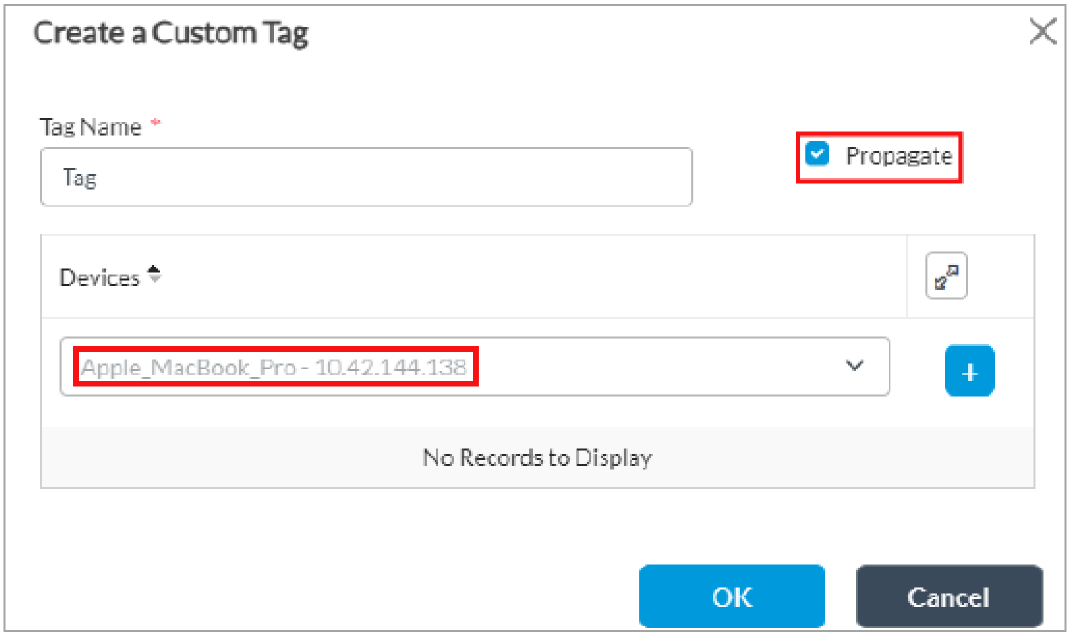
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Objects > Custom Objects > IoT Security > Custom Tags in the left menu bar.



4. Click + Add and enter the following information in the Create a Custom Tag window.



5. Enter a name for the custom device tag.
6. Click Propagate to add this tag to all devices that belong to the same category as the device you select in Devices. For example, in the following sample screenshot, you select the device, Apple_MacBook_Pro - 10.42.144.138. When you click Propagate, the tag is added to all existing MacBook devices and to the subsequent MacBook devices that the VOS software discovers:



Create a Custom Tag

Tag Name *

Tag

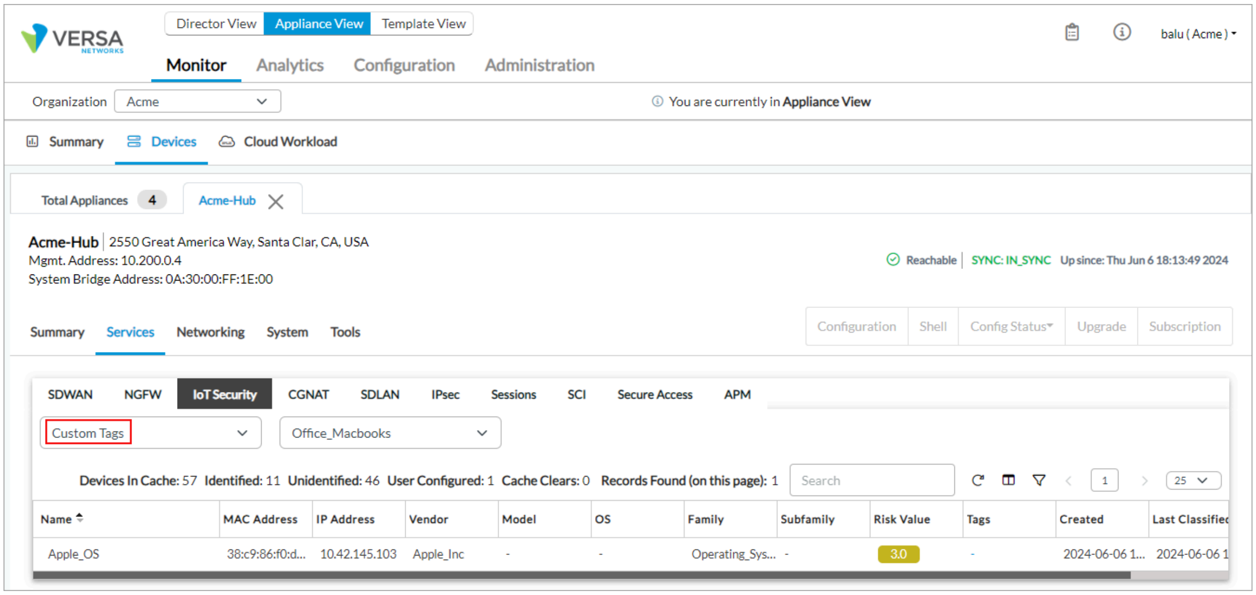
☑ Propagate

Devices

Apple_MacBook_Pro - 10.42.144.138

No Records to Display

7. From the Devices field, select a device to associate with the custom tag and click + Add icon to add.
8. Click OK.
9. To view view devices that use custom tags, select the Monitor > Services > IoT Security tab. For example:



Organization: Acme

You are currently in Appliance View

Acme-Hub | 2550 Great America Way, Santa Clar, CA, USA
Mgmt. Address: 10.200.0.4
System Bridge Address: 0A:30:00:FF:1E:00

Reachable | SYNC: IN_SYNC Up since: Thu Jun 6 18:13:49 2024

Custom Tags | Office_Macbooks

Devices In Cache: 57 Identified: 11 Unidentified: 46 User Configured: 1 Cache Clears: 0 Records Found (on this page): 1

| Name | MAC Address | IP Address | Vendor | Model | OS | Family | Subfamily | Risk Value | Tags | Created | Last Classifiec |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Apple_OS | 38:c9:86:f0:d... | 10.42.145.103 | Apple_Inc | - | - | Operating_Sys... | - | 3.0 | - | 2024-06-06 1... | 2024-06-06 1 |

For more information, see Monitor IoT Devices below.

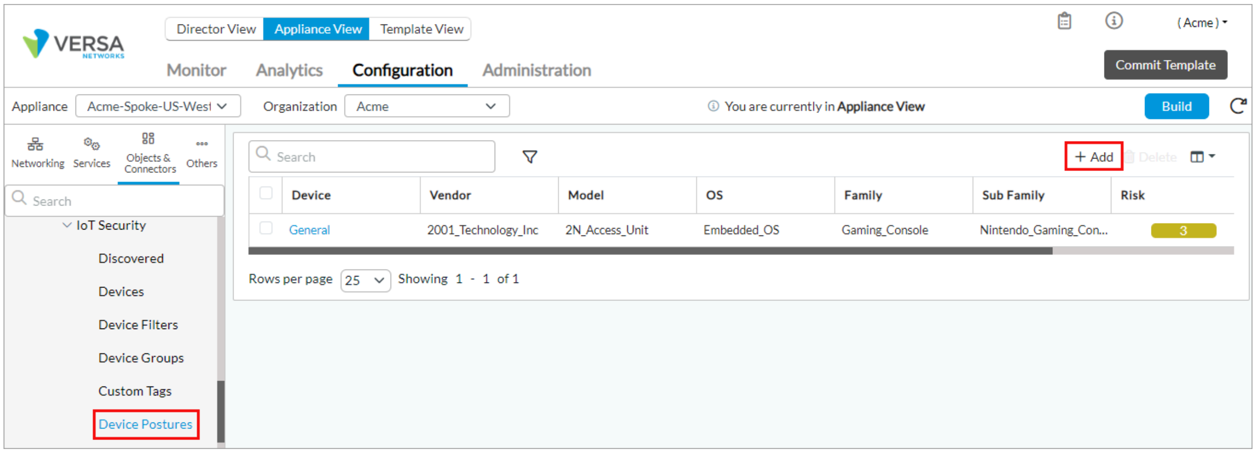
## Configure Custom Device Postures

You configure device postures to classify unidentified IoT devices. Unidentified devices are marked as opaque devices. Note that device postures are recommended only for pure IoT devices.

A device posture allows you to add information such as vendor, model, and operating system to classify opaque devices. When you configure a device posture, all matching opaque devices are automatically classified under that device posture.

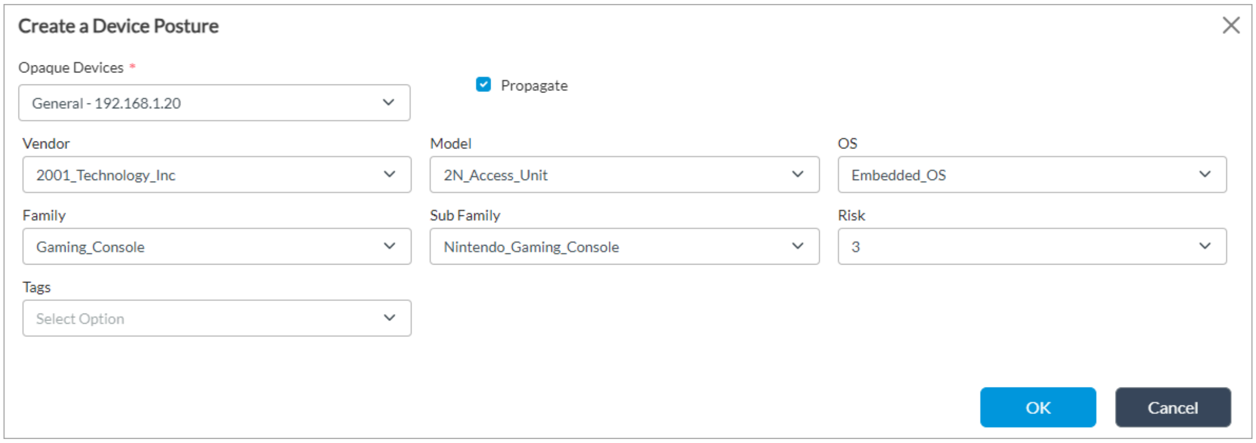
To configure a device posture:

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Templates > Device Templates in the horizontal menu bar.
    c. Select an organization in the left menu bar.
    d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Objects > Custom Objects > IoT Security > Device Postures in the left menu bar, and then click + Add.



| Device | Vendor | Model | OS | Family | Sub Family | Risk |
|---|---|---|---|---|---|---|
| General | 2001_Technology_Inc | 2N_Access_Unit | Embedded_OS | Gaming_Console | Nintendo_Gaming_Con... | 3 |

4. In the Create a Device Posture window, enter information for the following fields.



Opaque Devices *: General - 192.168.1.20

☑ Propagate

Vendor: 2001_Technology_Inc

Model: 2N_Access_Unit

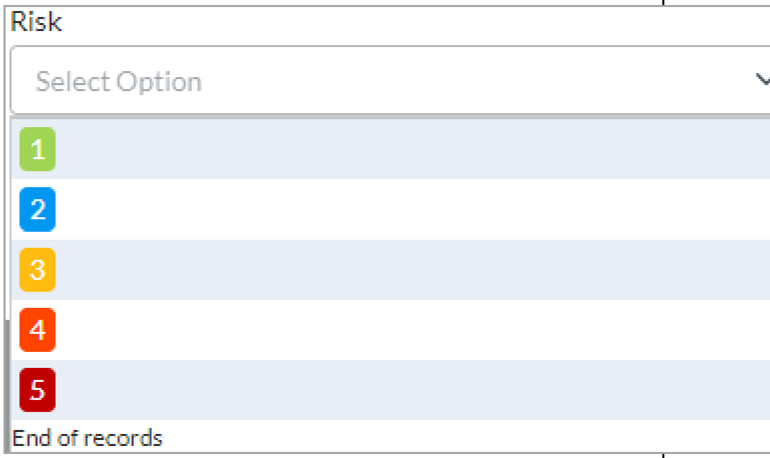
OS: Embedded_OS

Family: Gaming_Console

Sub Family: Nintendo_Gaming_Console

Risk: 3

Tags: Select Option

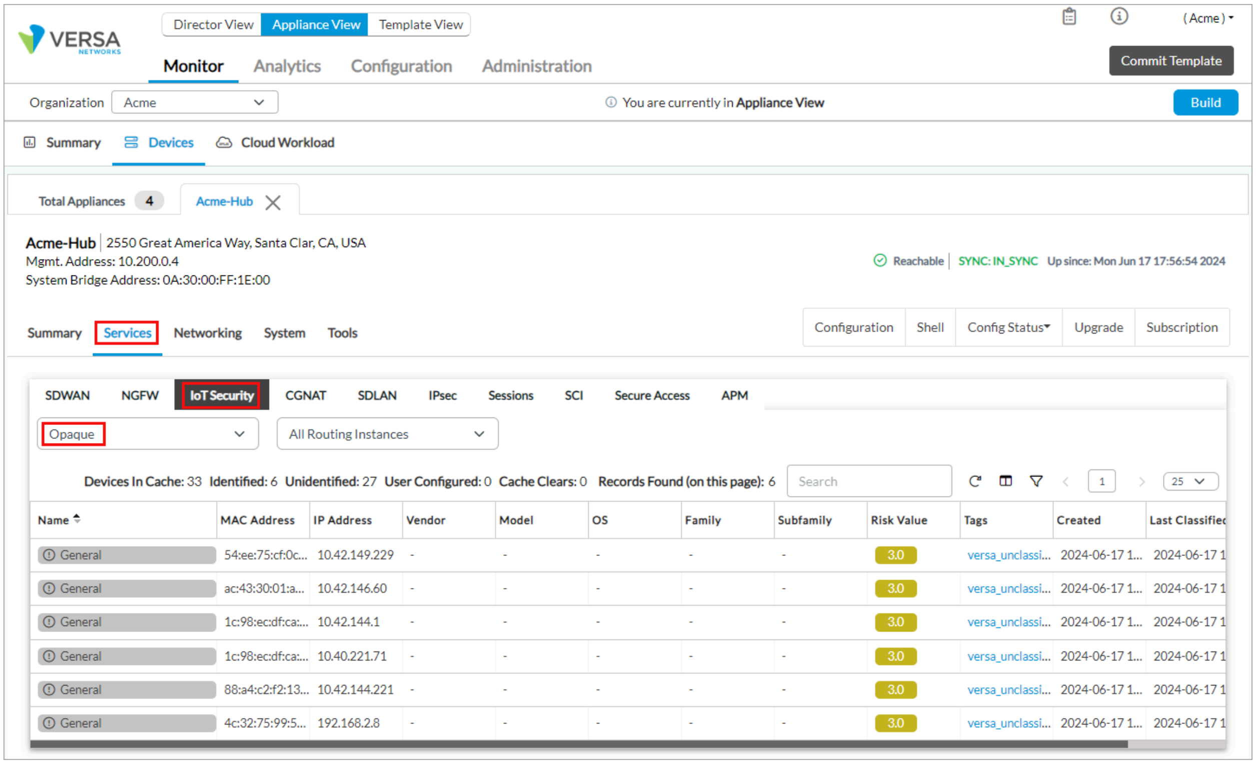
| Field | Description |
|---|---|
| Opaque Devices | Select an opaque device entry for which you want to configure a device posture. |
| Propagate | Click to classify all opaque devices with matching fingerprints under this device posture. |
| Vendor | Select a vendor to associate with the opaque device. When you select a vendor, the Model field displays. |
|  | For the following fields, the options that display are based on the vendor that you select. For example, if you select Apple_Inc as the vendor, the subsequent fields display options for Apple. |
| Model | Select a model for the device. |
| OS | Select an operating system for the device. |
| Family | Select the family of the device. For example, Gaming_Console for a gaming device. |
| Sub Family | Select the subfamily category such as Microsoft_Gaming_Console or Nintendo_Gaming_Console. |
| Risk | Select the risk of the device in the range of 0 through 5. A lower value indicates lower risk, as indicated by the color of each value.<br><br> Risk<br>Select Option<br>1<br>2<br>3<br>4<br>5<br>End of records |
| Tags | Select a predefined or custom tag to associate with the device. Use tags to group devices from different vendors or families into one group. |

5. Click OK.

You can view details of opaque devices from the Monitor tab.

To view an opaque device:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select a tenant in the left menu bar.
4. Select the Services > IoT Security tab. The IoT security statistics display.



You are currently in Appliance View

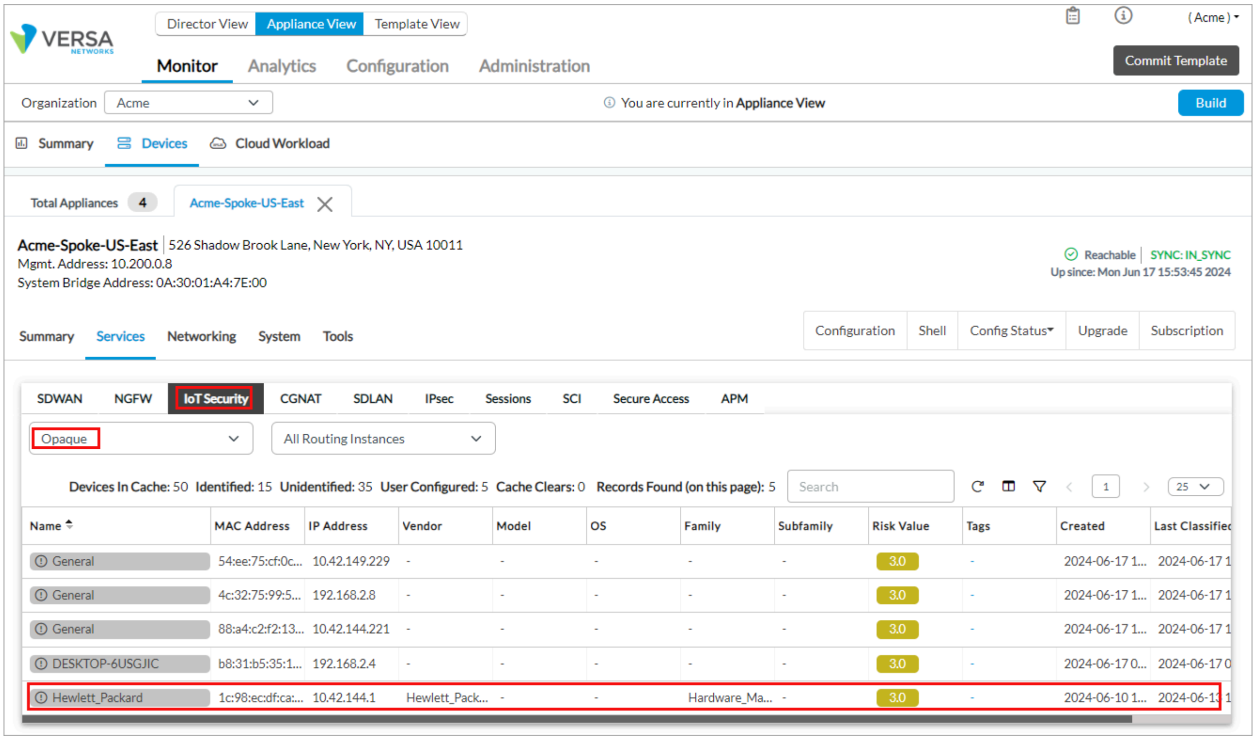
Acme-Hub | 2550 Great America Way, Santa Clar, CA, USA
Mgmt. Address: 10.200.0.4
System Bridge Address: 0A:30:00:FF:1E:00

Reachable | SYNC: IN_SYNC Up since: Mon Jun 17 17:56:54 2024

Devices In Cache: 33 Identified: 6 Unidentified: 27 User Configured: 0 Cache Clears: 0 Records Found (on this page): 6

| Name | MAC Address | IP Address | Vendor | Model | OS | Family | Subfamily | Risk Value | Tags | Created | Last Classifiec |
|---|---|---|---|---|---|---|---|---|---|---|---|
| General | 54:ee:75:cf:0c... | 10.42.149.229 | - | - | - | - | - | 3.0 | versa_unclassi... | 2024-06-17 1... | 2024-06-17 1 |
| General | ac:43:30:01:a... | 10.42.146.60 | - | - | - | - | - | 3.0 | versa_unclassi... | 2024-06-17 1... | 2024-06-17 1 |
| General | 1c:98:ec:df:ca:... | 10.42.144.1 | - | - | - | - | - | 3.0 | versa_unclassi... | 2024-06-17 1... | 2024-06-17 1 |
| General | 1c:98:ec:df:ca:... | 10.40.221.71 | - | - | - | - | - | 3.0 | versa_unclassi... | 2024-06-17 1... | 2024-06-17 1 |
| General | 88:a4:c2:f2:13... | 10.42.144.221 | - | - | - | - | - | 3.0 | versa_unclassi... | 2024-06-17 1... | 2024-06-17 1 |
| General | 4c:32:75:99:5... | 192.168.2.8 | - | - | - | - | - | 3.0 | versa_unclassi... | 2024-06-17 1... | 2024-06-17 1 |

5. From the first filtering option field, select Opaque, and then select a routing instance in the adjacent field. The Opaque devices identified for the selected tenant display as shown in the screenshot above. When an opaque device is associated with a device posture, details of the posture display in the IoT Security tab under Monitor. For example, the Hewlett_Packard entry in the screenshot below displays vendor and other details.



Organization: Acme

You are currently in Appliance View

Acme-Spoke-US-East | 526 Shadow Brook Lane, New York, NY, USA 10011
Mgmt. Address: 10.200.0.8
System Bridge Address: 0A:30:01:A4:7E:00

Reachable | SYNC: IN_SYNC
Up since: Mon Jun 17 15:53:45 2024

Opaque | All Routing Instances

Devices In Cache: 50 Identified: 15 Unidentified: 35 User Configured: 5 Cache Clears: 0 Records Found (on this page): 5

| Name | MAC Address | IP Address | Vendor | Model | OS | Family | Subfamily | Risk Value | Tags | Created | Last Classifiec |
|---|---|---|---|---|---|---|---|---|---|---|---|
| General | 54:ee:75:cf:0c... | 10.42.149.229 | - | - | - | - | - | 3.0 | - | 2024-06-17 1... | 2024-06-17 1 |
| General | 4c:32:75:99:5... | 192.168.2.8 | - | - | - | - | - | 3.0 | - | 2024-06-17 1... | 2024-06-17 1 |
| General | 88:a4:c2:f2:13... | 10.42.144.221 | - | - | - | - | - | 3.0 | - | 2024-06-17 1... | 2024-06-17 1 |
| DESKTOP-6USGJIC | b8:31:b5:35:1... | 192.168.2.4 | - | - | - | - | - | 3.0 | - | 2024-06-17 0... | 2024-06-17 0 |
| Hewlett_Packard | 1c:98:ec:df:ca:... | 10.42.144.1 | Hewlett_Pack... | - | - | Hardware_Ma... | - | 3.0 | - | 2024-06-10 1... | 2024-06-1 1 |

## Use Custom Tags for Authentication and Decryption

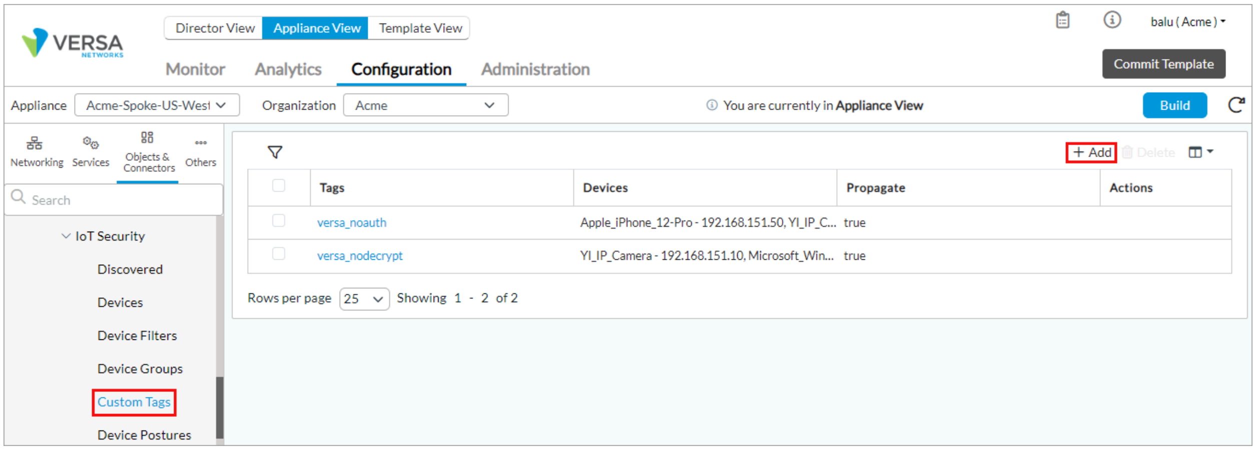
You can authenticate and decrypt IoT devices using custom IoT security tags. For more information about custom tags, see Configure Custom IoT Security Tags, above.

Use the following IoT tags to allow or bypass authentication and decryption of IoT devices:

- versa_auth—Use this tag to authenticate devices.
- versa_decrypt—Use this tag to decrypt devices.
- versa_noauth—Use this tag to bypass authentication of devices.
- versa_nodecrypt—Use this tag to bypass decryption of devices.

To use one of these custom tags for authentication or decryption:

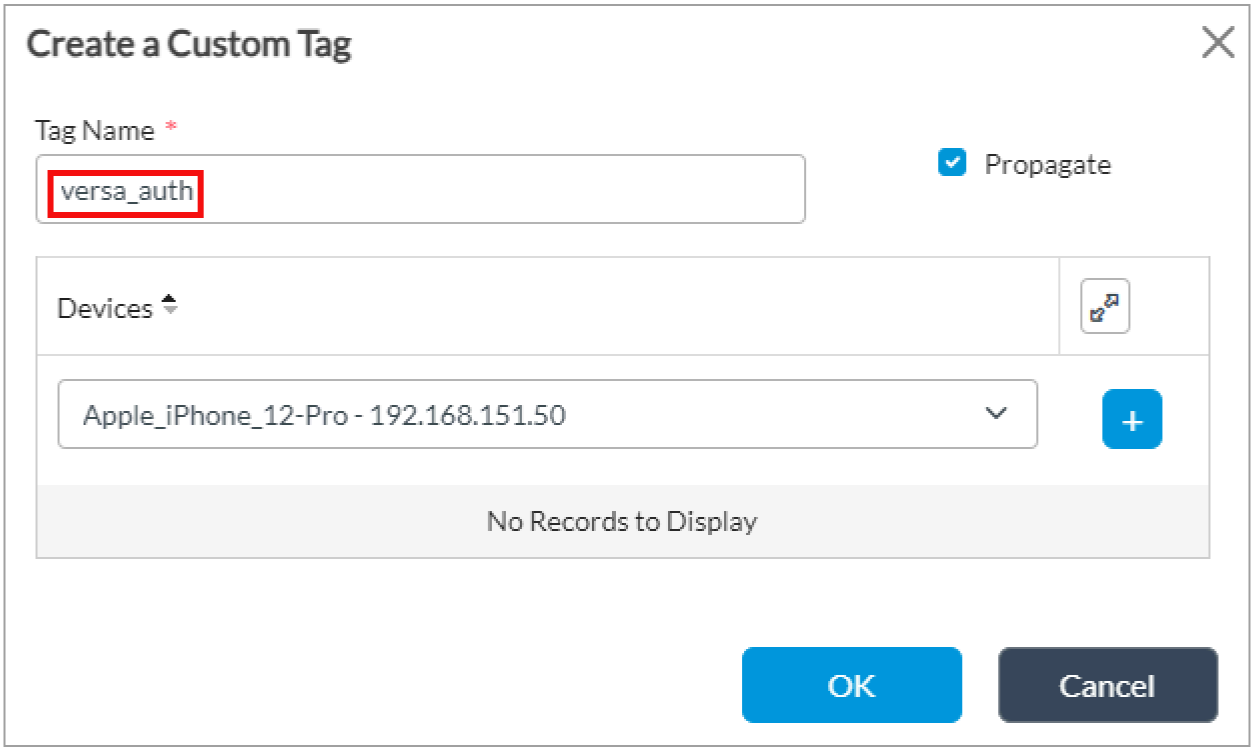
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Objects > Custom Objects > IoT Security > Custom Tags in the left menu bar.



| | Tags | Devices | Propagate | Actions |
|---|---|---|---|---|
| □ | versa_noauth | Apple_iPhone_12-Pro - 192.168.151.50, YI_IP_C... | true | |
| □ | versa_nodecrypt | YI_IP_Camera - 192.168.151.10, Microsoft_Win... | true | |

Rows per page 25 Showing 1 - 2 of 2

4. Click + Add. In the Create a Custom Tag window, enter information for the following fields.



Tag Name *

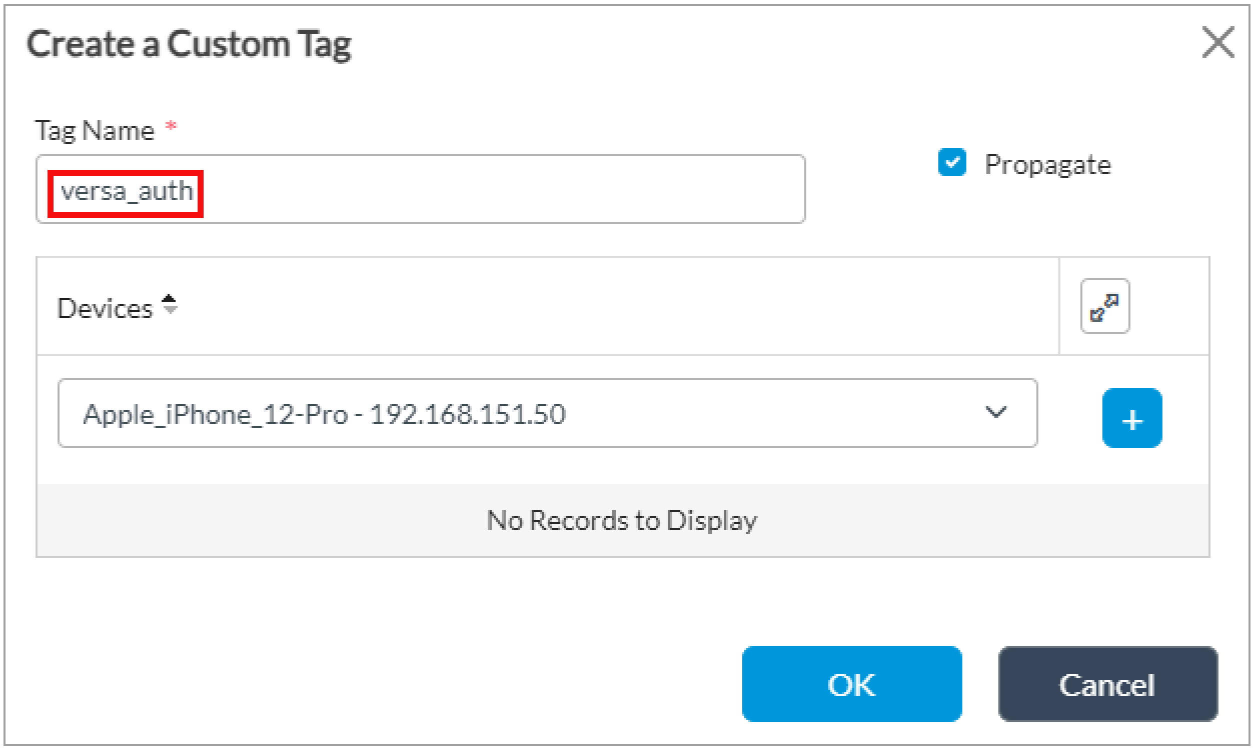
versa_auth

☑ Propagate

Devices

Apple_iPhone_12-Pro - 192.168.151.50

5. Enter the custom device tag name based on the authentication or decryption policy you want to configure. For example, versa_auth, versa_decrypt, versa_noauth, or versa_nodecrypt (here, versa_auth).



versa_auth

Apple_iPhone_12-Pro - 192.168.151.50

No Records to Display

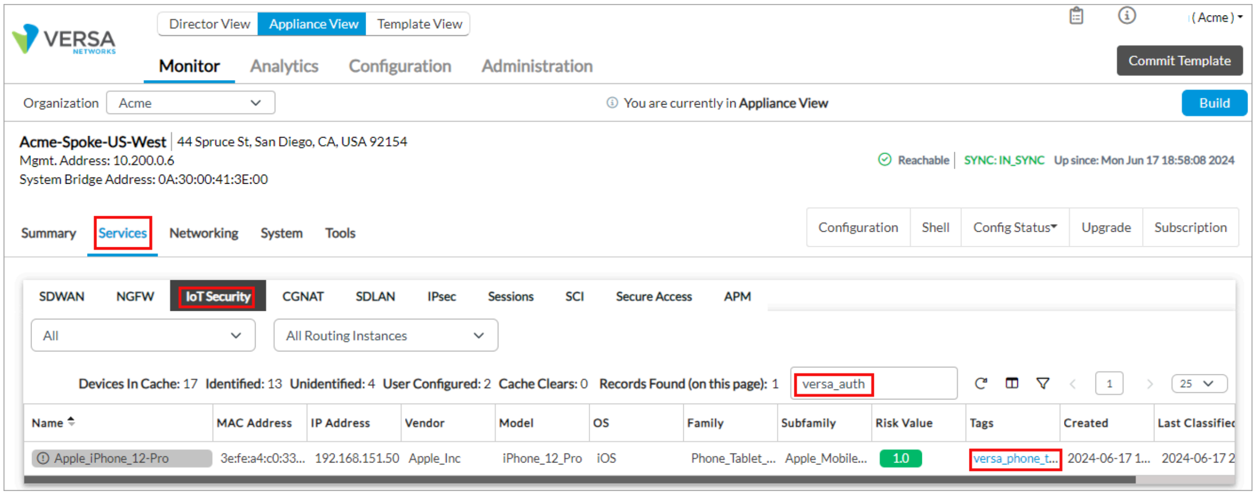
6. Click Propagate to add this tag to all devices that belong to the same category as the device you select in Devices. For example, in the screenshot above, Apple_iPhone_12-Pro - 192.168.151.50 is selected. When you click Propagate, the tag is added to authenticate all existing iPhone devices and to the subsequent iPhone devices that the VOS software discovers.

7. From the Devices field, select a device to associate with the custom tag and click the + Add icon to add.
8. Click OK.

## Monitor Devices

To monitor IoT devices that are classified under a custom tag for authentication or decryption:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select a tenant in the left menu bar.
4. Select the Services > IoT Security tab. The IoT security statistics display.
5. Use the search tab to filter records. Here, we use versa_auth to filter based on the custom tag for authentication configured in Use Custom Tags for Authentication and Decryption, above. Apple_iPhone_12-Pro displays based on the search filter.



Organization: Acme

You are currently in Appliance View

Acme-Spoke-US-West | 44 Spruce St, San Diego, CA, USA 92154
Mgmt. Address: 10.200.0.6
System Bridge Address: 0A:30:00:41:3E:00

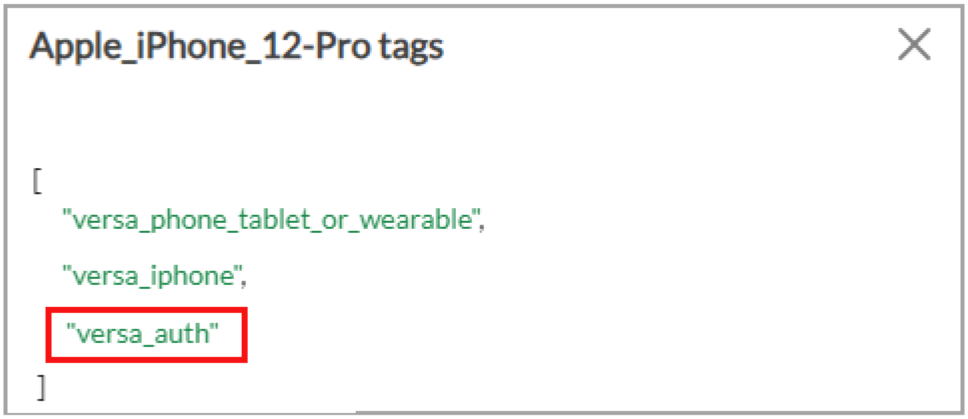
Reachable | SYNC: IN_SYNC Up since: Mon Jun 17 18:58:08 2024

All | All Routing Instances

Devices In Cache: 17 Identified: 13 Unidentified: 4 User Configured: 2 Cache Clears: 0 Records Found (on this page): 1 versa_auth

| Name | MAC Address | IP Address | Vendor | Model | OS | Family | Subfamily | Risk Value | Tags | Created | Last Classified |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Apple_iPhone_12-Pro | 3e:fe:a4:c0:33... | 192.168.151.50 | Apple_Inc | iPhone_12_Pro | iOS | Phone_Tablet_... | Apple_Mobile... | 1.0 | versa_phone_t... | 2024-06-17 1... | 2024-06-17 2 |

6. Click the value in the Tags column to display the tags associated with the device.

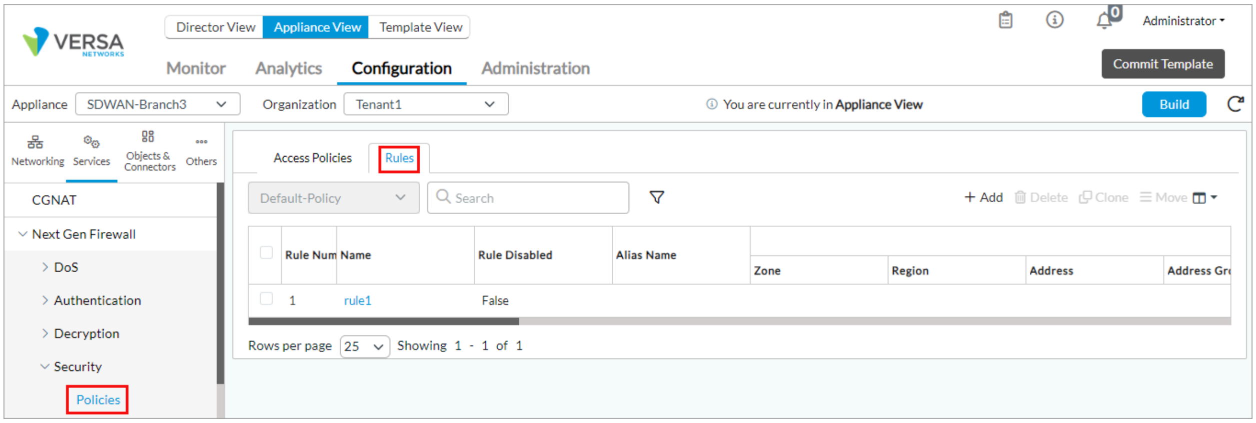

Apple_iPhone_12-Pro tags

```
[
  "versa_phone_tablet_or_wearable",
  "versa_iphone",
  "versa_auth"
]
```

## Associate IoT Security Objects with NGFW Security Rules

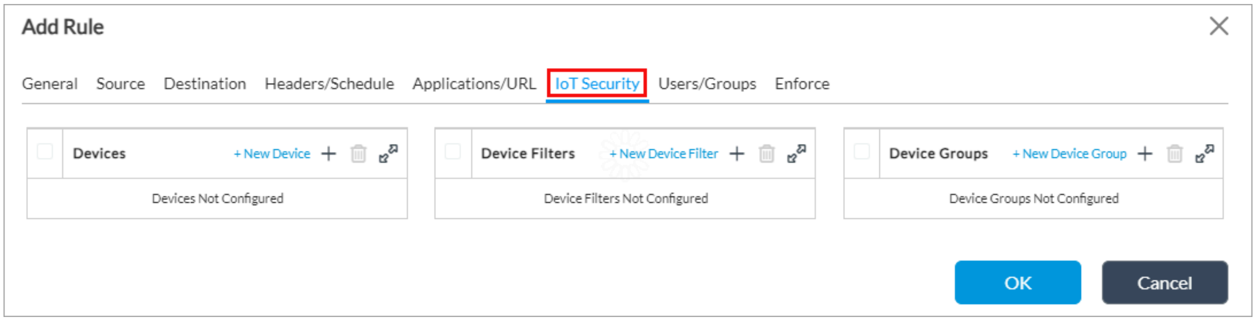
To associate IoT security devices, device filters, and device groups with an NGFW security policy rule:;

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliance in the left menu bar.
    c. Select the device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next Gen Firewall > Security > Policies in the left menu bar and select the Rules tab.

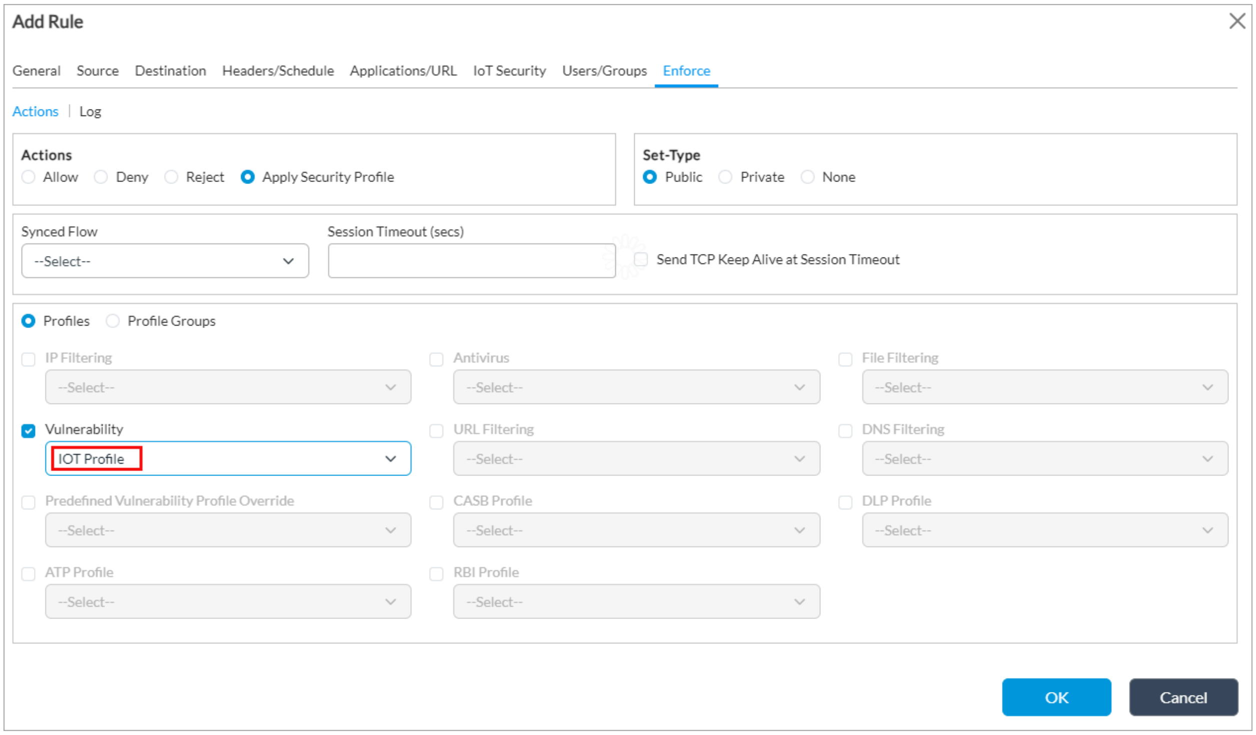


| Rule Num | Name | Rule Disabled | Alias Name | Zone | Region | Address | Address Gr |
|---|---|---|---|---|---|---|---|
| 1 | rule1 | False | | | | | |

4. Select a rule or click + Add to add a rule for the policy. The Add/Edit Rule popup window displays.
5. Select the IoT Security tab.



6. To associate an IoT security device with the NGFW security rule, click + and select a device. To add a device, click + New Device. The Create a User Defined Device window displays. For more information, see Configure Custom IoT Security Devices, above.
7. To associate an IoT security device filter with the rule, click + and then select a predefined or user-defined device filter. To add a device filter, click + New Device Filter. The Create a User Defined Device Filter window displays. For more information, see Configure Custom IoT Security Device Filters, above.
8. To associate an IoT security device group with the rule, click + and then select a device group. To add a device group, click + New Device Group. The Create a User Defined Device Group window displays. For more information, see Configure Custom IoT Security Device Groups, above.
9. Select the Enforce tab and choose the actions for the rule. Note that the IoT Profile option in the Vulnerability field is applicable only for IoT security.



Actions: ○ Allow ○ Deny ○ Reject ● Apply Security Profile

Set-Type: ● Public ○ Private ○ None

Synced Flow: --Select--

Session Timeout (secs):

□ Send TCP Keep Alive at Session Timeout

● Profiles ○ Profile Groups

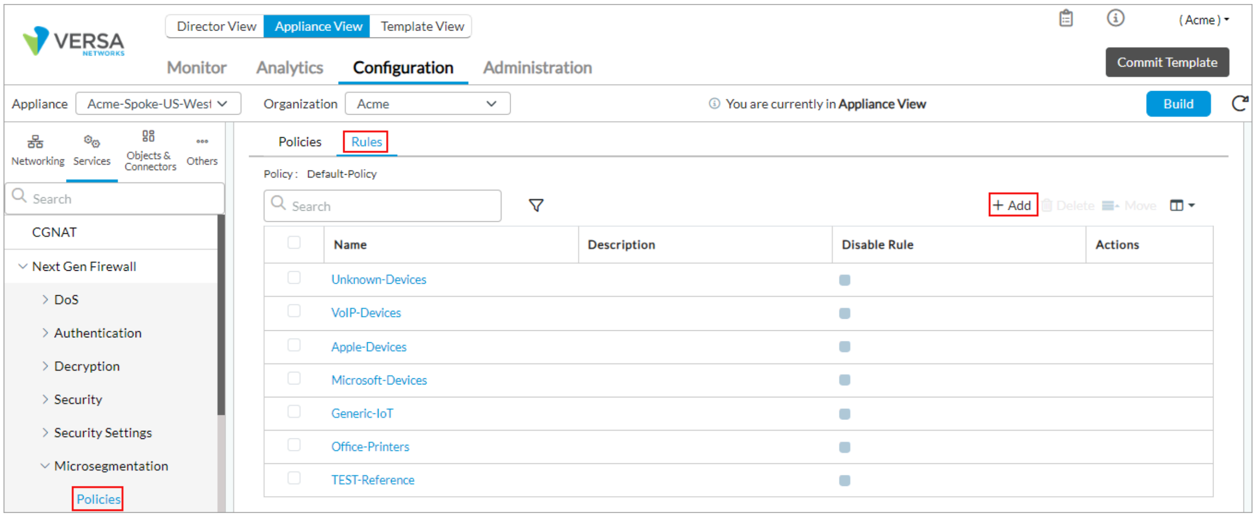
| | | |
|---|---|---|
| □ IP Filtering: --Select-- | □ Antivirus: --Select-- | □ File Filtering: --Select-- |
| ☑ Vulnerability: IOT Profile | □ URL Filtering: --Select-- | □ DNS Filtering: --Select-- |
| □ Predefined Vulnerability Profile Override: --Select-- | □ CASB Profile: --Select-- | □ DLP Profile: --Select-- |
| □ ATP Profile: --Select-- | □ RBI Profile: --Select-- | |

10. For information about configuring other parameters, see Configure SD-WAN Security Access Control Policies and Rules.
11. Click OK.

## Associate IoT Security Objects with Microsegmentation Rules

To associate IoT security devices, device filters, and device groups with microsegmentation rules:

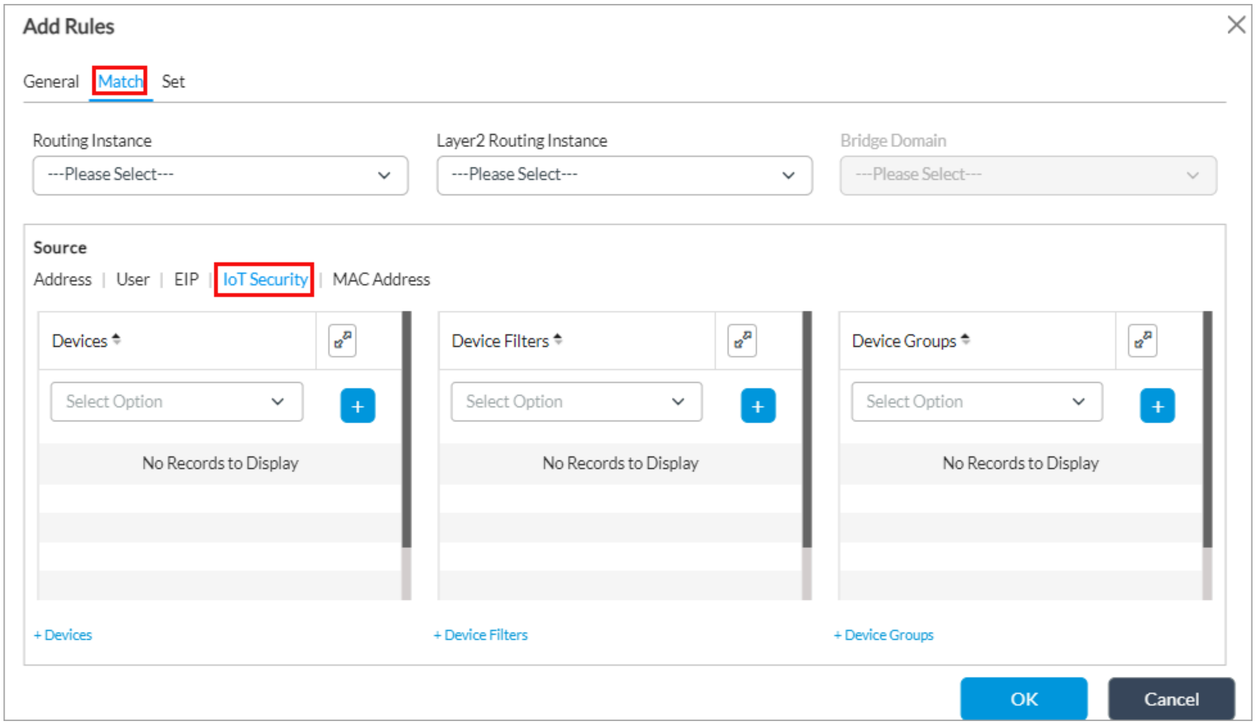
1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliance in the left menu bar.
   c. Select the device from the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Microsegmentation > Policies in the left menu bar and select the Rules tab. For more information, see Configure Microsegmentation.



Appliance: Acme-Spoke-US-West
Organization: Acme
Policy : Default-Policy

| Name | Description | Disable Rule | Actions |
|---|---|---|---|
| Unknown-Devices | | ■ | |
| VoIP-Devices | | ■ | |
| Apple-Devices | | ■ | |
| Microsoft-Devices | | ■ | |
| Generic-IoT | | ■ | |
| Office-Printers | | ■ | |
| TEST-Reference | | ■ | |

4. Select a rule or click + Add to add a rule for the policy. The Add/Edit Rules popup window displays.



Routing Instance: ---Please Select---
Layer2 Routing Instance: ---Please Select---
Bridge Domain: ---Please Select---

| Devices | Device Filters | Device Groups |
|---|---|---|
| Select Option | Select Option | Select Option |
| No Records to Display | No Records to Display | No Records to Display |

5. Select the Match tab and then select the IoT Security tab.

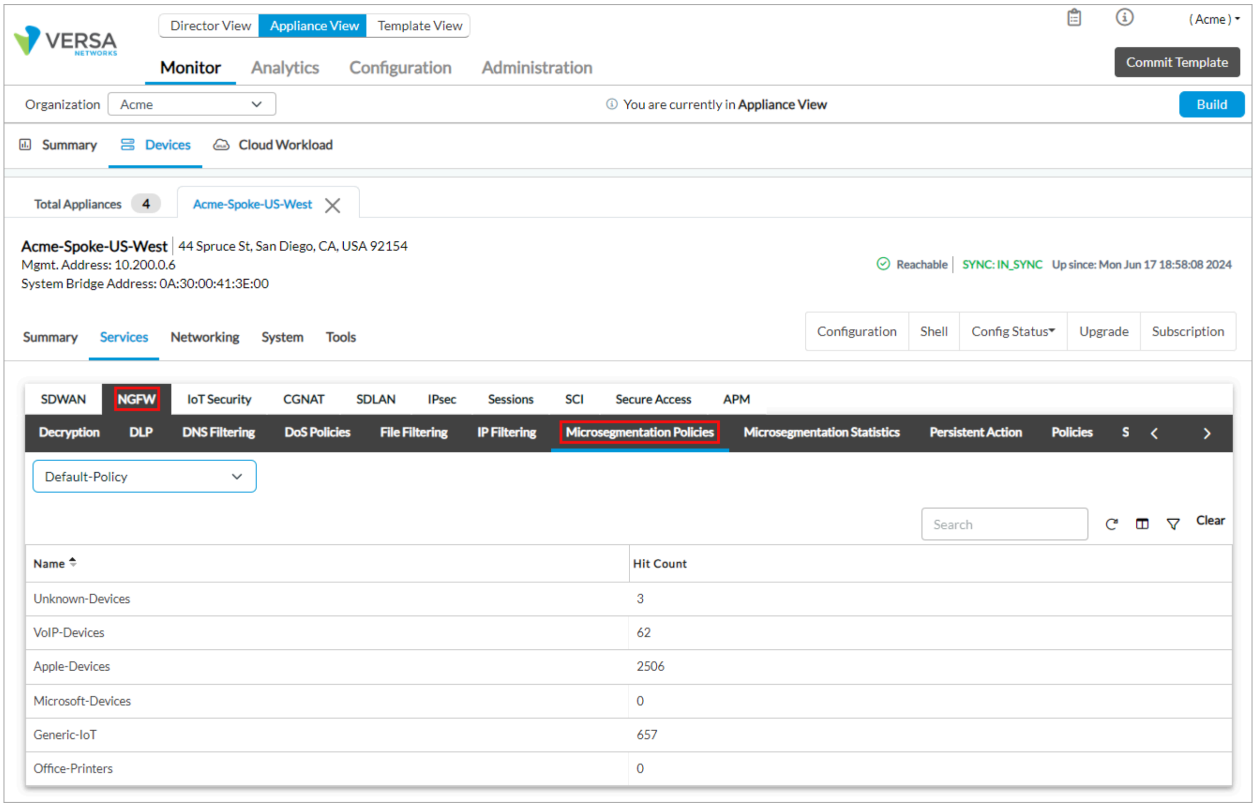
6. To associate an IoT security device with the rule, select a predefined or user-defined device and click the + Add icon. To add a device, click + Devices. The Create a User Defined Device window displays. For more information, see [Configure Custom IoT Security Devices](), above.

7. To associate an IoT security device filter with the rule, click select a predefined or user-defined device filter and filter click the + Add icon. To add a device filter, click + Device Filters. The Create a User Defined Device Filter window displays. For more information, see [Configure Custom IoT Security Device Filters](), above.

8. To associate an IoT security device group with the rule, select a device group and click the + Add icon. To add a rule, click + Device Groups. The Create a User Defined Device Group window displays. For more information, see [Configure Custom IoT Security Device Groups](), above.
9. For information about configuring other parameters, see [Configure Microsegmentation]().
10. Click OK.

To monitor the IoT devices associated with a microsegmentation policy:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select a tenant in the left menu bar.
4. Select the Services > NGFW tab, and then select Microsegmentation Policies.
5. Select the policy from the filter to view the hit count details of IoT devices.



Organization: Acme

You are currently in Appliance View

Acme-Spoke-US-West | 44 Spruce St, San Diego, CA, USA 92154
Mgmt. Address: 10.200.0.6
System Bridge Address: 0A:30:00:41:3E:00

Reachable | SYNC: IN_SYNC Up since: Mon Jun 17 18:58:08 2024

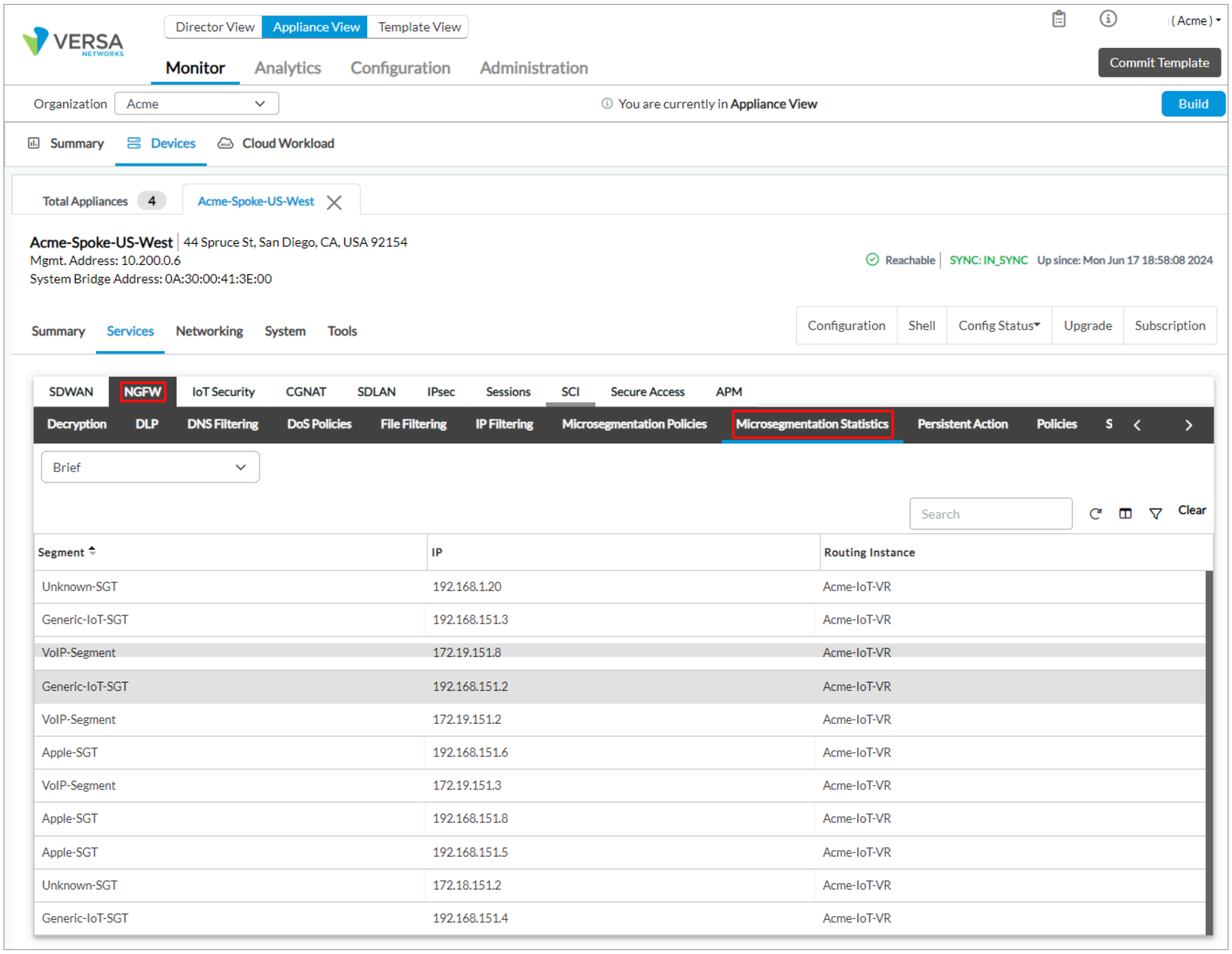
Default-Policy

| Name | Hit Count |
|---|---|
| Unknown-Devices | 3 |
| VoIP-Devices | 62 |
| Apple-Devices | 2506 |
| Microsoft-Devices | 0 |
| Generic-IoT | 657 |
| Office-Printers | 0 |

To monitor microsegmentation statistics for IoT devices:

1. Select the Monitor tab in the top menu bar.
2. Select a tenant in the left menu bar.

3. Select the Services > NGFW tab, and then select Microsegmentation Statistics.
4. Select Brief, Local Statistics, or Tunnel Statistics from the filter to view the details. For example, the following screenshot displays details for Brief.



Acme-Spoke-US-West | 44 Spruce St, San Diego, CA, USA 92154
Mgmt. Address: 10.200.0.6
System Bridge Address: 0A:30:00:41:3E:00

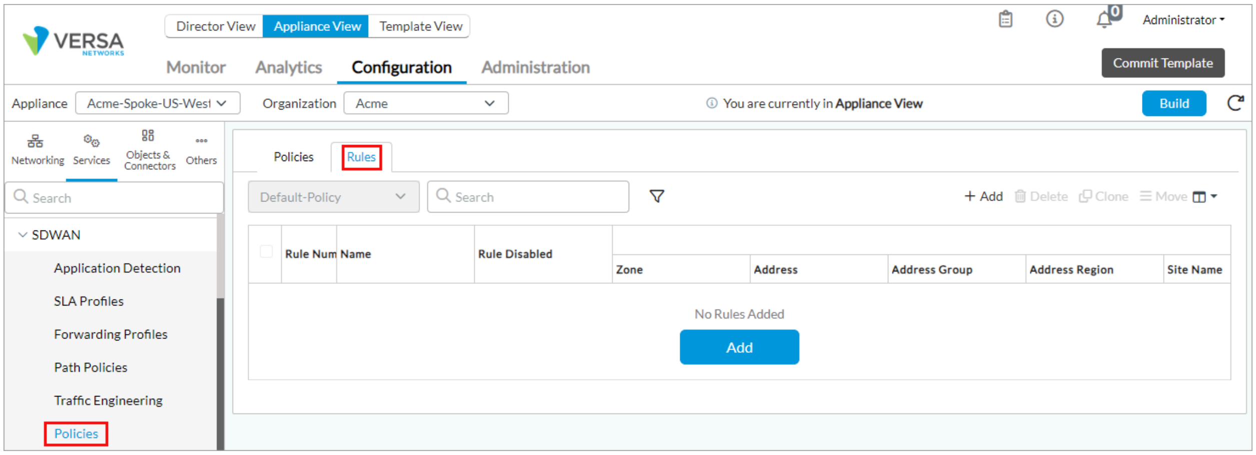
Up since: Mon Jun 17 18:58:08 2024

| Segment | IP | Routing Instance |
|---|---|---|
| Unknown-SGT | 192.168.1.20 | Acme-IoT-VR |
| Generic-IoT-SGT | 192.168.151.3 | Acme-IoT-VR |
| VoIP-Segment | 172.19.151.8 | Acme-IoT-VR |
| Generic-IoT-SGT | 192.168.151.2 | Acme-IoT-VR |
| VoIP-Segment | 172.19.151.2 | Acme-IoT-VR |
| Apple-SGT | 192.168.151.6 | Acme-IoT-VR |
| VoIP-Segment | 172.19.151.3 | Acme-IoT-VR |
| Apple-SGT | 192.168.151.8 | Acme-IoT-VR |
| Apple-SGT | 192.168.151.5 | Acme-IoT-VR |
| Unknown-SGT | 172.18.151.2 | Acme-IoT-VR |
| Generic-IoT-SGT | 192.168.151.4 | Acme-IoT-VR |

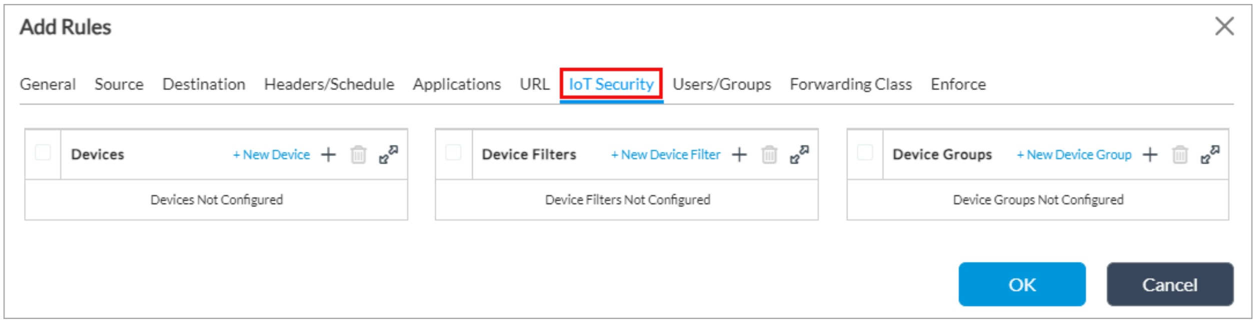
# Associate IoT Security Objects with SD-WAN Policy Rules

To associate IoT security devices, device filters, and device groups with an SD-WAN security policy rule:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliance in the left menu bar.
    c. Select the device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > SD-WAN > Policies in the left menu bar and select the Rules tab.



4. Select a rule or click + Add to add a rule for the policy. The Add/Edit Rules popup window displays.
5. Select the Match tab and then select the IoT Security tab.



6. To associate an IoT security device with the rule, select a predefined or user-defined device and click the + Add icon. To add a device, click + Devices. The Create a User Defined Device window displays. For more information, see Configure Custom IoT Security Devices, above.
7. To associate an IoT security device filter with the rule, select a predefined or user-defined device filter and filter

   click the + Add icon. To add a device filter, click + Device Filters. The Create a User Defined Device Filter window displays. For more information, see Configure Custom IoT Security Device Filters, above.

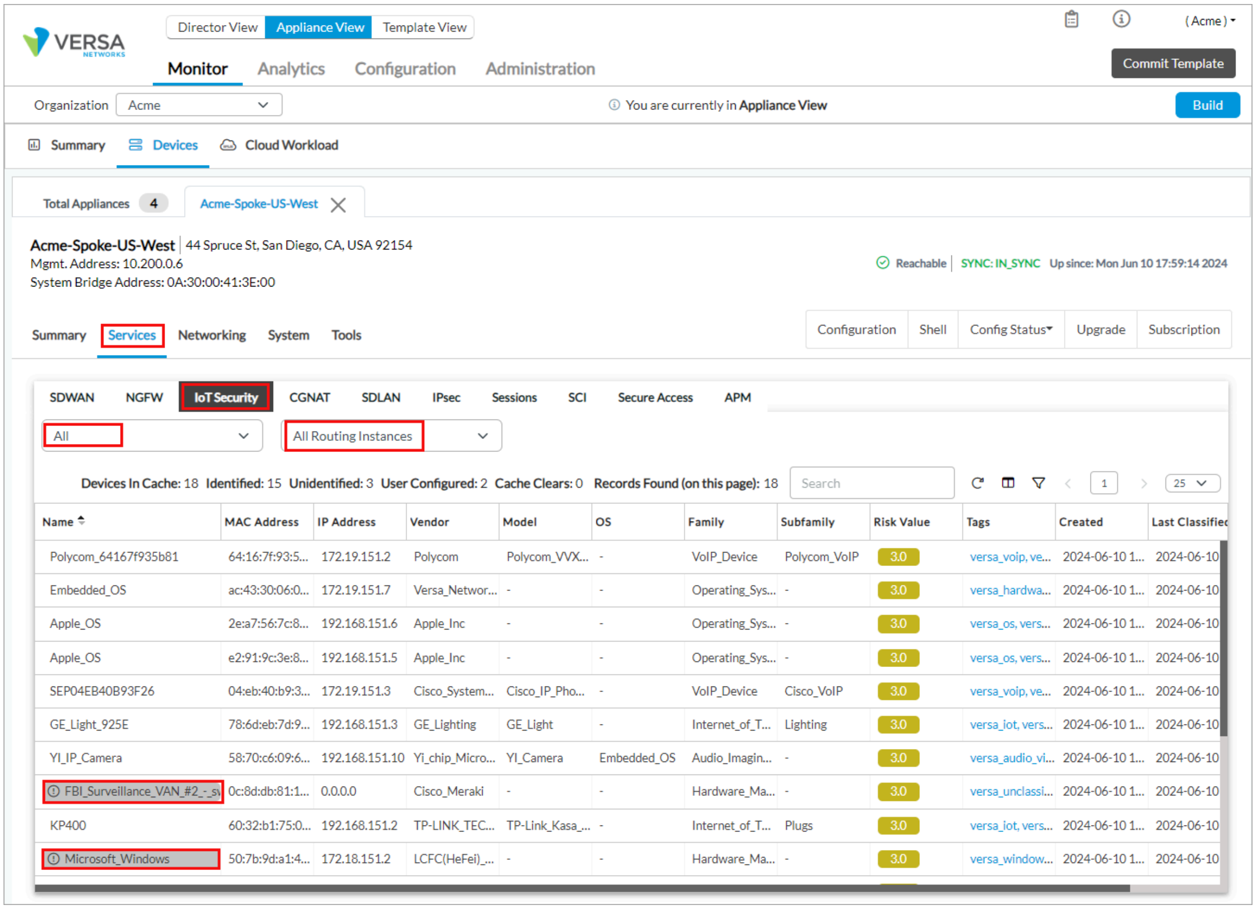
8. To associate an IoT security device group with the rule, select a device group and click the + Add icon. To add a rule, click + Device Groups. The Create a User Defined Device Group window displays. For more information, see Configure Custom IoT Security Device Groups, above.
9. Select the Enforce tab and choose the actions for the rule.
10. For information about configuring other parameters, see Configure SD-WAN Policy.
11. Click OK.

## Monitor IoT Devices

You monitor IoT devices to view details about devices that are identified, unidentified, and cached. The monitoring screen allows you to filter the display based on values such as vendor, OS, family, and tags. For more information, see Monitor Device Services.

To monitor IoT devices:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select a tenant in the left menu bar.
4. Select the Services tab.
5. Select the IoT Security tab. The IoT security statistics display.



Acme-Spoke-US-West | 44 Spruce St, San Diego, CA, USA 92154
Mgmt. Address: 10.200.0.6
System Bridge Address: 0A:30:00:41:3E:00

Up since: Mon Jun 10 17:59:14 2024

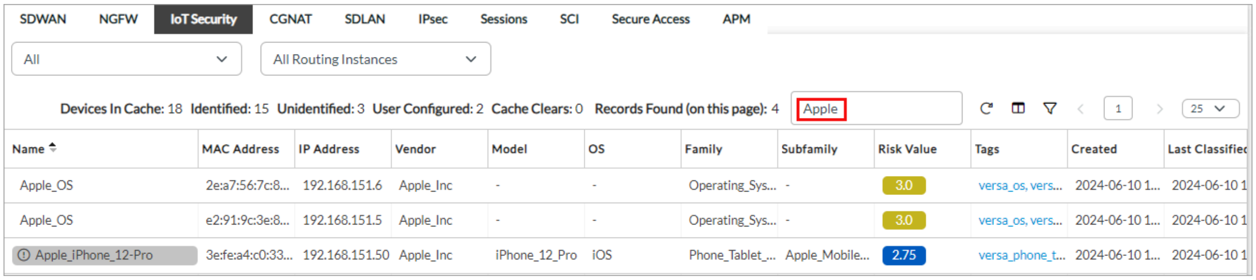
Devices In Cache: 18 Identified: 15 Unidentified: 3 User Configured: 2 Cache Clears: 0 Records Found (on this page): 18

| Name | MAC Address | IP Address | Vendor | Model | OS | Family | Subfamily | Risk Value | Tags | Created | Last Classified |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Polycom_64167f935b81 | 64:16:7f:93:5... | 172.19.151.2 | Polycom | Polycom_VVX... | - | VoIP_Device | Polycom_VoIP | 3.0 | versa_voip, ve... | 2024-06-10 1... | 2024-06-10 |
| Embedded_OS | ac:43:30:06:0... | 172.19.151.7 | Versa_Networ... | - | - | Operating_Sys... | - | 3.0 | versa_hardwa... | 2024-06-10 1... | 2024-06-10 |
| Apple_OS | 2e:a7:56:7c:8... | 192.168.151.6 | Apple_Inc | - | - | Operating_Sys... | - | 3.0 | versa_os, vers... | 2024-06-10 1... | 2024-06-10 |
| Apple_OS | e2:91:9c:3e:8... | 192.168.151.5 | Apple_Inc | - | - | Operating_Sys... | - | 3.0 | versa_os, vers... | 2024-06-10 1... | 2024-06-10 |
| SEP04EB40B93F26 | 04:eb:40:b9:3... | 172.19.151.3 | Cisco_System... | Cisco_IP_Pho... | - | VoIP_Device | Cisco_VoIP | 3.0 | versa_voip, ve... | 2024-06-10 1... | 2024-06-10 |
| GE_Light_925E | 78:6d:eb:7d:9... | 192.168.151.3 | GE_Lighting | GE_Light | - | Internet_of_T... | Lighting | 3.0 | versa_iot, vers... | 2024-06-10 1... | 2024-06-10 |
| YI_IP_Camera | 58:70:c6:09:6... | 192.168.151.10 | Yi_chip_Micro... | YI_Camera | Embedded_OS | Audio_Imagin... | - | 3.0 | versa_audio_vi... | 2024-06-10 1... | 2024-06-10 |
| ⓘ FBI_Surveillance_VAN_#2_-_sv | 0c:8d:db:81:1... | 0.0.0.0 | Cisco_Meraki | - | - | Hardware_Ma... | - | 3.0 | versa_unclassi... | 2024-06-10 1... | 2024-06-10 |
| KP400 | 60:32:b1:75:0... | 192.168.151.2 | TP-LINK_TEC... | TP-Link_Kasa_... | - | Internet_of_T... | Plugs | 3.0 | versa_iot, vers... | 2024-06-10 1... | 2024-06-10 |
| ⓘ Microsoft_Windows | 50:7b:9d:a1:4... | 172.18.151.2 | LCFC(HeFei)_... | - | - | Hardware_Ma... | - | 3.0 | versa_window... | 2024-06-10 1... | 2024-06-10 |

6. To filter the list by device type, click the first field and select from the following options: All, Configured, Custom Tags, Identified, Opaque, and Unidentified.
7. To filter the list by routing instance, click the adjacent field and select a routing instance, or select All Routing Instances.

8. To filter devices, enter a device category in the Search field and click ↻. For example, the following screenshot

shows devices filtered for the value 'Apple'.



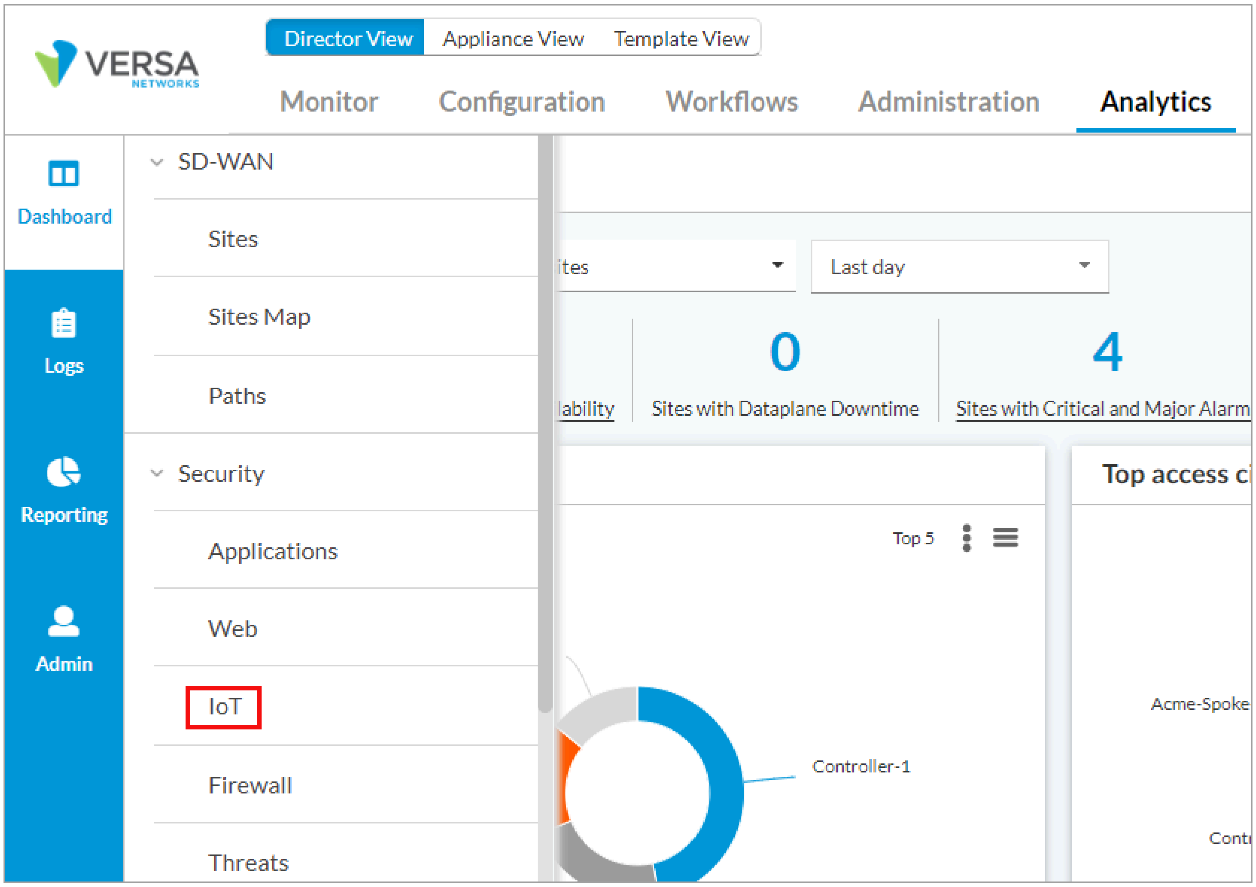
Devices In Cache: 18 Identified: 15 Unidentified: 3 User Configured: 2 Cache Clears: 0 Records Found (on this page): 4 Apple

| Name | MAC Address | IP Address | Vendor | Model | OS | Family | Subfamily | Risk Value | Tags | Created | Last Classified |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Apple_OS | 2e:a7:56:7c:8... | 192.168.151.6 | Apple_Inc | - | - | Operating_Sys... | - | 3.0 | versa_os, vers... | 2024-06-10 1... | 2024-06-10 1 |
| Apple_OS | e2:91:9c:3e:8... | 192.168.151.5 | Apple_Inc | - | - | Operating_Sys... | - | 3.0 | versa_os, vers... | 2024-06-10 1... | 2024-06-10 1 |
| Apple_iPhone_12-Pro | 3e:fe:a4:c0:33... | 192.168.151.50 | Apple_Inc | iPhone_12_Pro | iOS | Phone_Tablet_... | Apple_Mobile... | 2.75 | versa_phone_t... | 2024-06-10 1... | 2024-06-10 1 |

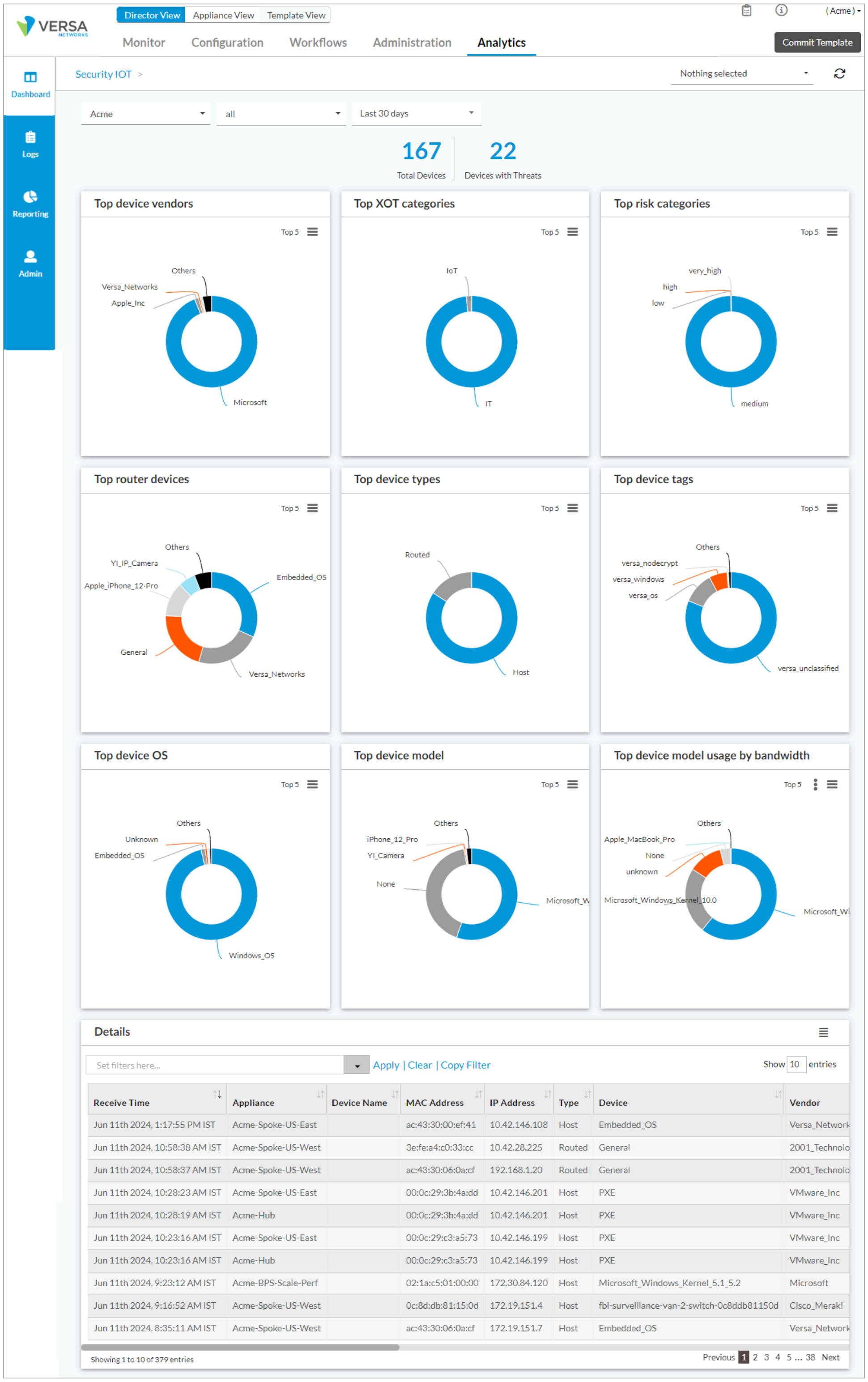
## View IoT Security Analytics

To view IoT security analytics:

1. In Director view, select the Analytics tab in the top menu bar. The view changes to Analytics view.



2. Select Dashboard > Security > IoT in the left menu bar to view the Security IoT dashboard. For more information, see Security Dashboard. The IoT Security dashboard displays.



Details

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

Show 10 entries

| Receive Time | Appliance | Device Name | MAC Address | IP Address | Type | Device | Vendor |
|---|---|---|---|---|---|---|---|
| Jun 11th 2024, 1:17:55 PM IST | Acme-Spoke-US-East | | ac:43:30:00:ef:41 | 10.42.146.108 | Host | Embedded_OS | Versa_Network |
| Jun 11th 2024, 10:58:38 AM IST | Acme-Spoke-US-West | | 3e:fe:a4:c0:33:cc | 10.42.28.225 | Routed | General | 2001_Technolo |
| Jun 11th 2024, 10:58:37 AM IST | Acme-Spoke-US-West | | ac:43:30:06:0a:cf | 192.168.1.20 | Routed | General | 2001_Technolo |
| Jun 11th 2024, 10:28:23 AM IST | Acme-Spoke-US-East | | 00:0c:29:3b:4a:dd | 10.42.146.201 | Host | PXE | VMware_Inc |
| Jun 11th 2024, 10:28:19 AM IST | Acme-Hub | | 00:0c:29:3b:4a:dd | 10.42.146.201 | Host | PXE | VMware_Inc |
| Jun 11th 2024, 10:23:16 AM IST | Acme-Spoke-US-East | | 00:0c:29:c3:a5:73 | 10.42.146.199 | Host | PXE | VMware_Inc |
| Jun 11th 2024, 10:23:16 AM IST | Acme-Hub | | 00:0c:29:c3:a5:73 | 10.42.146.199 | Host | PXE | VMware_Inc |
| Jun 11th 2024, 9:23:12 AM IST | Acme-BPS-Scale-Perf | | 02:1a:c5:01:00:00 | 172.30.84.120 | Host | Microsoft_Windows_Kernel_5.1_5.2 | Microsoft |
| Jun 11th 2024, 9:16:52 AM IST | Acme-Spoke-US-West | | 0c:8d:db:81:15:0d | 172.19.151.4 | Host | fbi-surveillance-van-2-switch-0c8ddb81150d | Cisco_Meraki |
| Jun 11th 2024, 8:35:11 AM IST | Acme-Spoke-US-West | | ac:43:30:06:0a:cf | 172.19.151.7 | Host | Embedded_OS | Versa_Network |

Showing 1 to 10 of 379 entries

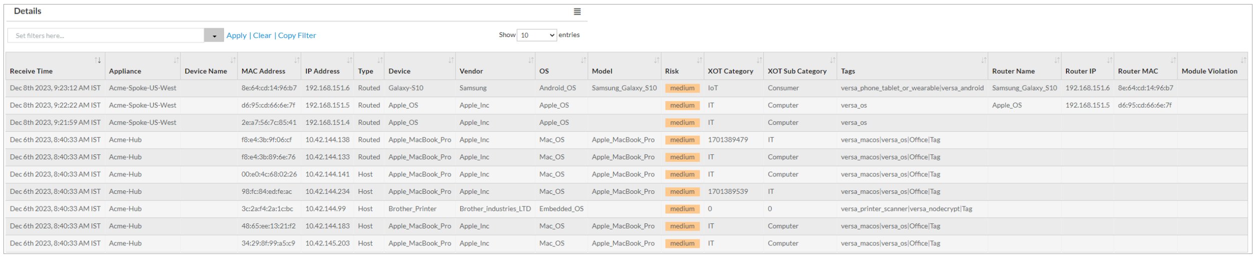
Previous 1 2 3 4 5 ... 38 Next

The top level dashboard displays the following charts:

- Total devices and devices with threats

- Top device model
- Top device model usage by bandwidth
- Top device OS
- Top device tags
- Top device types
- Top device vendors
- Top risk categories
- Top router devices
- Top XoT categories

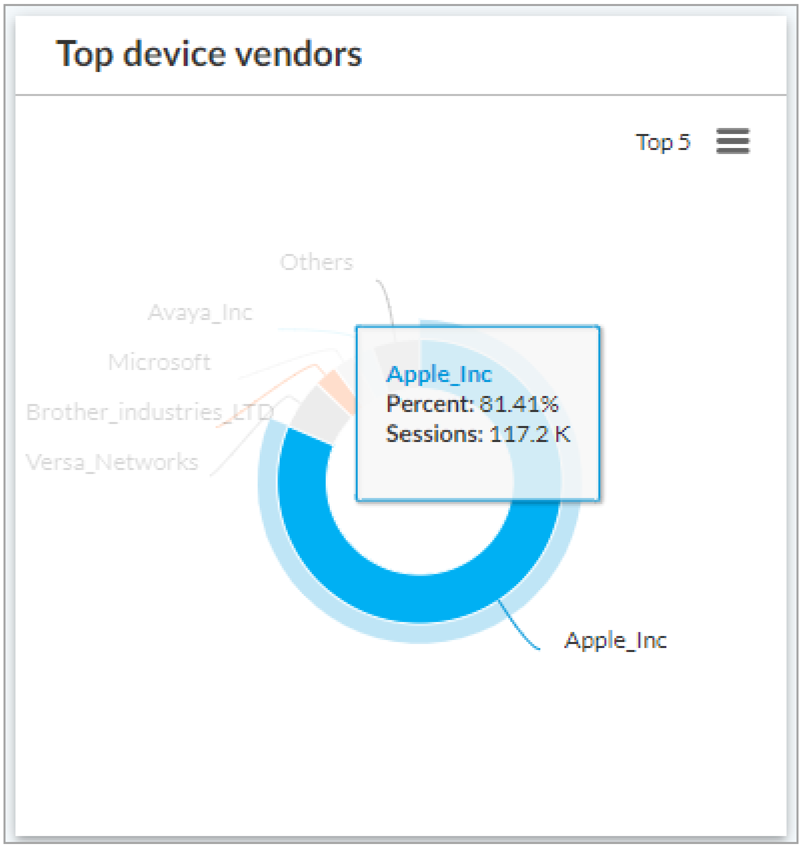
The Details section displays the following information:



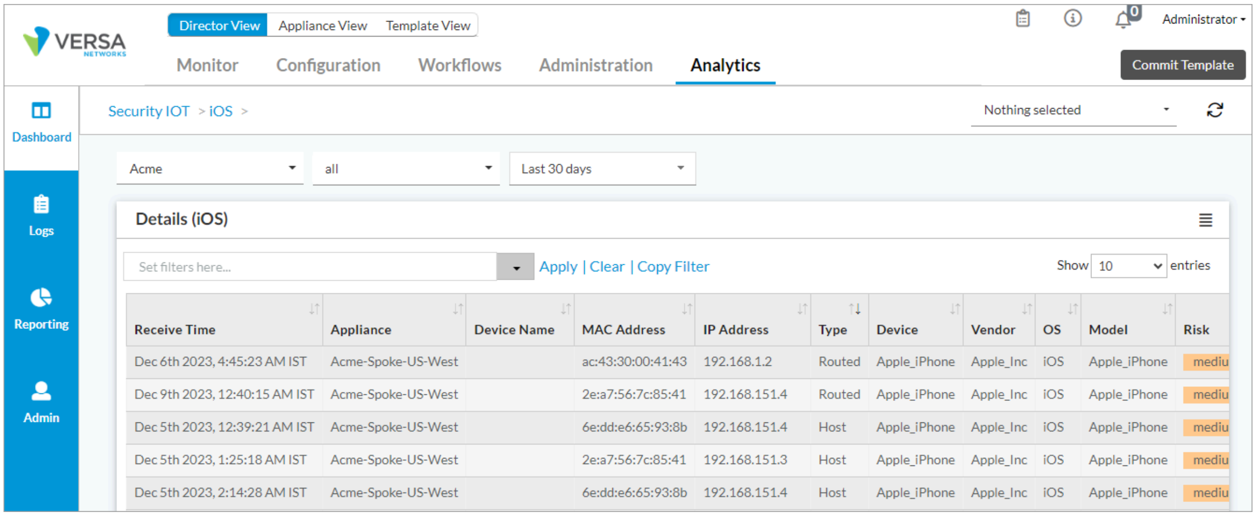
| Receive Time | Appliance | Device Name | MAC Address | IP Address | Type | Device | Vendor | OS | Model | Risk | XOT Category | XOT Sub Category | Tags | Router Name | Router IP | Router MAC | Module Violation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Dec 8th 2023, 9:23:12 AM IST | Acme-Spoke-US-West |  | 8e:64:cd:14:96:b7 | 192.168.151.6 | Routed | Galaxy-S10 | Samsung | Android_OS | Samsung_Galaxy_S10 | medium | IoT | Consumer | versa_phone_tablet_or_wearable\|versa_android | Samsung_Galaxy_S10 | 192.168.151.6 | 8e:64:cd:14:96:b7 |  |
| Dec 8th 2023, 9:22:22 AM IST | Acme-Spoke-US-West |  | d6:95:cd:66:6e:7f | 192.168.151.5 | Routed | Apple_OS | Apple_Inc | Apple_OS |  | medium | IT | Computer | versa_os | Apple_OS | 192.168.151.5 | d6:95:cd:66:6e:7f |  |
| Dec 8th 2023, 9:21:59 AM IST | Acme-Spoke-US-West |  | 2e:a7:56:7c:85:41 | 192.168.151.4 | Routed | Apple_OS | Apple_Inc | Apple_OS |  | medium | IT | Computer | versa_os |  |  |  |  |
| Dec 6th 2023, 8:40:33 AM IST | Acme-Hub |  | f8:e4:3b:9f:06:cf | 10.42.144.138 | Routed | Apple_MacBook_Pro | Apple_Inc | Mac_OS | Apple_MacBook_Pro | medium | 1701389479 | IT | versa_macos\|versa_os\|Office\|Tag |  |  |  |  |
| Dec 6th 2023, 8:40:33 AM IST | Acme-Hub |  | f8:e4:3b:89:6e:76 | 10.42.144.133 | Routed | Apple_MacBook_Pro | Apple_Inc | Mac_OS | Apple_MacBook_Pro | medium | IT | Computer | versa_macos\|versa_os\|Office\|Tag |  |  |  |  |
| Dec 6th 2023, 8:40:33 AM IST | Acme-Hub |  | 00:e0:4c:68:02:26 | 10.42.144.141 | Host | Apple_MacBook_Pro | Apple_Inc | Mac_OS | Apple_MacBook_Pro | medium | IT | Computer | versa_macos\|versa_os\|Office\|Tag |  |  |  |  |
| Dec 6th 2023, 8:40:33 AM IST | Acme-Hub |  | 98:fc:84:ed:fe:ac | 10.42.144.234 | Host | Apple_MacBook_Pro | Apple_Inc | Mac_OS | Apple_MacBook_Pro | medium | 1701389539 | IT | versa_macos\|versa_os\|Office\|Tag |  |  |  |  |
| Dec 6th 2023, 8:40:33 AM IST | Acme-Hub |  | 3c:2a:f4:2a:1c:bc | 10.42.144.99 | Host | Brother_Printer | Brother_industries_LTD | Embedded_OS |  | medium | 0 | 0 | versa_printer_scanner\|versa_nodecrypt\|Tag |  |  |  |  |
| Dec 6th 2023, 8:40:33 AM IST | Acme-Hub |  | 48:65:ee:13:21:f2 | 10.42.144.183 | Host | Apple_MacBook_Pro | Apple_Inc | Mac_OS | Apple_MacBook_Pro | medium | IT | Computer | versa_macos\|versa_os\|Office\|Tag |  |  |  |  |
| Dec 6th 2023, 8:40:33 AM IST | Acme-Hub |  | 34:29:8f:99:a5:c9 | 10.42.145.203 | Host | Apple_MacBook_Pro | Apple_Inc | Mac_OS | Apple_MacBook_Pro | medium | IT | Computer | versa_macos\|versa_os\|Office\|Tag |  |  |  |  |

- Appliance
- Device MAC address and IP address
- Device Name
- Model
- Module violation
- Receive time
- Risk
- OS
- Tags
- Type
- Router name, IP address, and MAC address
- Vendor
- XOT category and subcategory

3. Move the mouse over a chart to display details such as percentage and number of sessions. For example:



4. Drill down on a chart to display specific details.



Acme | all | Last 30 days

Details (iOS)

Show 10 entries

| Receive Time | Appliance | Device Name | MAC Address | IP Address | Type | Device | Vendor | OS | Model | Risk |
|---|---|---|---|---|---|---|---|---|---|---|
| Dec 6th 2023, 4:45:23 AM IST | Acme-Spoke-US-West | | ac:43:30:00:41:43 | 192.168.1.2 | Routed | Apple_iPhone | Apple_Inc | iOS | Apple_iPhone | mediu |
| Dec 9th 2023, 12:40:15 AM IST | Acme-Spoke-US-West | | 2e:a7:56:7c:85:41 | 192.168.151.4 | Routed | Apple_iPhone | Apple_Inc | iOS | Apple_iPhone | mediu |
| Dec 5th 2023, 12:39:21 AM IST | Acme-Spoke-US-West | | 6e:dd:e6:65:93:8b | 192.168.151.4 | Host | Apple_iPhone | Apple_Inc | iOS | Apple_iPhone | mediu |
| Dec 5th 2023, 1:25:18 AM IST | Acme-Spoke-US-West | | 2e:a7:56:7c:85:41 | 192.168.151.3 | Host | Apple_iPhone | Apple_Inc | iOS | Apple_iPhone | mediu |
| Dec 5th 2023, 2:14:28 AM IST | Acme-Spoke-US-West | | 6e:dd:e6:65:93:8b | 192.168.151.4 | Host | Apple_iPhone | Apple_Inc | iOS | Apple_iPhone | mediu |

## Supported Software Information

Releases 22.1.4 and later support all content described in this article.

## Additional Information

Apply Log Export Functionality
Configure File Filtering
Configure Log Export Functionality
Configure Microsegmentation
Configure NGFW
Configure Organization Limits
Configure SD-WAN Policy
Configure Service Node Groups
Configure SNAT Pools
Monitor Device Services
Security Dashboard
Use Security Packages