Configure Intrusion Detection and Prevention

For supported software information, click here.

A security vulnerability is an unintended flaw that allows malicious users to surreptitiously attack a network. Attackers can exploit such vulnerabilities to break into and damage the network by changing, destroying, or stealing secured or confidential information, or by installing malware.

To protect a network against security vulnerabilities, the Versa Operating System^{TM} (VOS^{TM}) unified threat management (UTM) capabilities include intrusion detection and prevention (IDP). IDP is a preemptive approach to network security that identifies potential threats and responds to them based on user-defined policy. IDP comprises two components:

- Intrusion detection system (IDS) is the process of examining the network for indications of vulnerabilities and for detecting inappropriate or anomalous activity.
- Intrusion prevention system (IPS) is the process of stopping vulnerabilities by responding to inappropriate or anomalous activity. Responses can include dropping data packets and disconnecting connections that are transmitting unauthorized data.

Security analysts can use network IDS systems to examine network traffic and the network protocols, applications, and operating systems running on the network. To inspect and process the desired traffic, an IDS system can be placed inline. However, they are commonly connected to a switch's spanning port or attached to a hub, or they make use of network taps.

You commonly place an IPS system at the perimeter of a corporate network.

IPS performs the following types of vulnerability detection to help prevent attacks, including zero-day attacks such as worms or viruses:

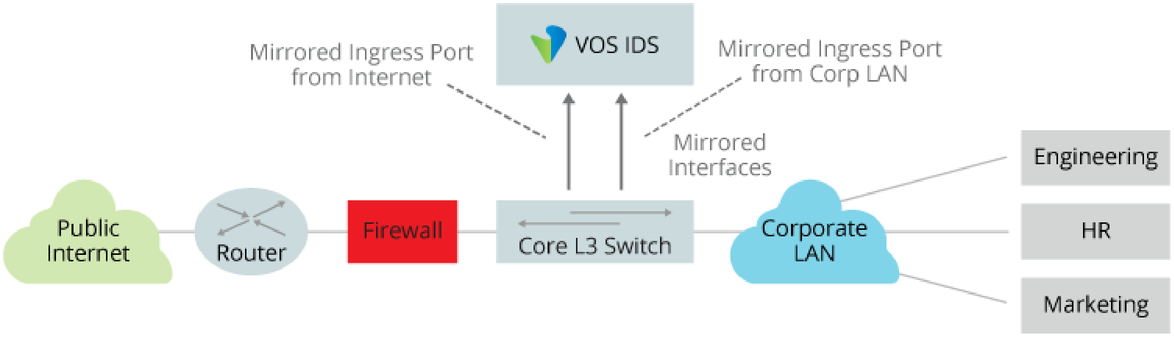
- Signature-based detection—Signatures are a set of rules that a vulnerability profile uses to detect intrusive activities. With signature-based detection, a security profile compares a software or application pattern with a database of signatures, identifying malicious activity by matching patterns to those in the database. Versa security packs (SPacks) provide a set of predefined signatures, and you can also create custom signatures.
- Anomaly detection—Anomaly detection monitors a network for unusual events or trends. You configure the vulnerability profile that compares an observed event with the baseline of the normal traffic. Anomaly detection detects patterns that are normally not present in the traffic, so it is useful for detecting new attacks.

Implementing a properly tuned and managed IPS solution at all corporate ingress and egress points helps to ensure that new and previously identified threats are dropped at the perimeter, while allowing legitimate traffic to pass.

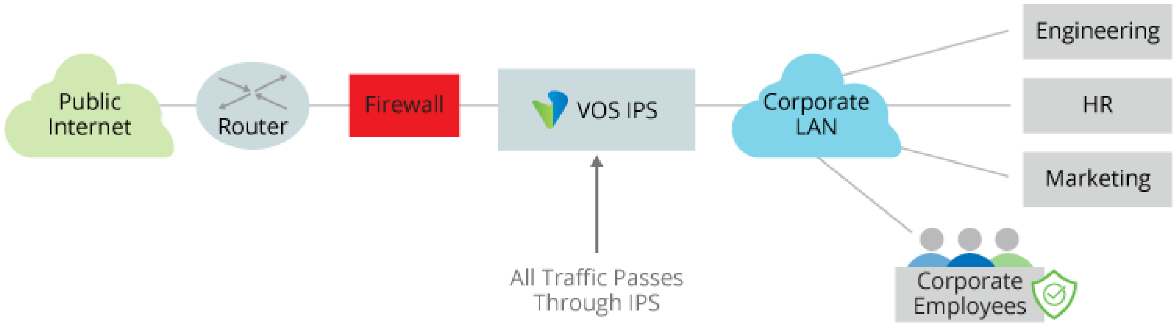
Having an IPS deployment at the edges of the network provides the preventative measures and control needed to combat new and existing threats, and including an IDS inside the firewall and at critical internal network nodes provides visibility into internal activity.

The following figures illustrate how an IDS/IPS solution can be deployed within an enterprise:

The first figure illustrates how traffic travels between an enterprise corporate network and the public internet. An edge router, a firewall, and a Layer 3 switch are positioned between the internet and the corporate network. The switch connects to a VOS device that is configured as an IDS security device. This switch has four ports, two regular network ports (one on the WAN side and one on the LAN side) and two mirror ports that connect to the VOS device. The two mirror ports send copies of the packets they receive to the VOS device for IDS processing and analysis. The green mirror port (on the left) mirrors packets received from the public internet, and the blue mirror port (on the right) mirrors packets received from the corporate LAN. Having two mirror ports allows the Layer 3 switch to process incoming and outgoing data streams concurrently on separate paths, thus ensuring that all traffic flowing across the network is monitored by the VOS IDS capability. In this type of deployment, a keepalive session is maintained between the Layer 3 switch and the VOS device to prevent network outages.



In the following figure, traffic between an enterprise corporate network and the public internet passes through a VOS device that is configured as an IPS security device. The IPS system analyzes data traffic for vulnerabilities before the traffic is forwarded towards its destination. In this scenario, if the VOS device goes down and the IPS system is no longer available, a network outage can occur.



To use IDP, you configure IDS and IPS vulnerability profiles, as described in this article. It is recommended that you use the predefined vulnerability profiles, or you can create custom vulnerability profiles. You then associate the vulnerability profiles with a next-generation firewall (NGFW) security profile (also called an access policy profile) in an NGFW policy, as described in Configure a Security Access Policy. In the policy you define the traffic to match based on various parameters, such as zones and applications, and you configure the policy to enforce the action defined in vulnerability profile.

This article discusses how to configure and use IDP:

- Install the Versa IDP signature database
- Use predefined vulnerability profiles
- Create custom vulnerability profiles
- View vulnerability statistics and logs

Install the Versa IDP Database

The Versa security research team provides an IDP signature database, and provides regular updates to the database in security packages (SPacks). To obtain the current signature database, download the latest SPack. For more information, see Use Security Packages.

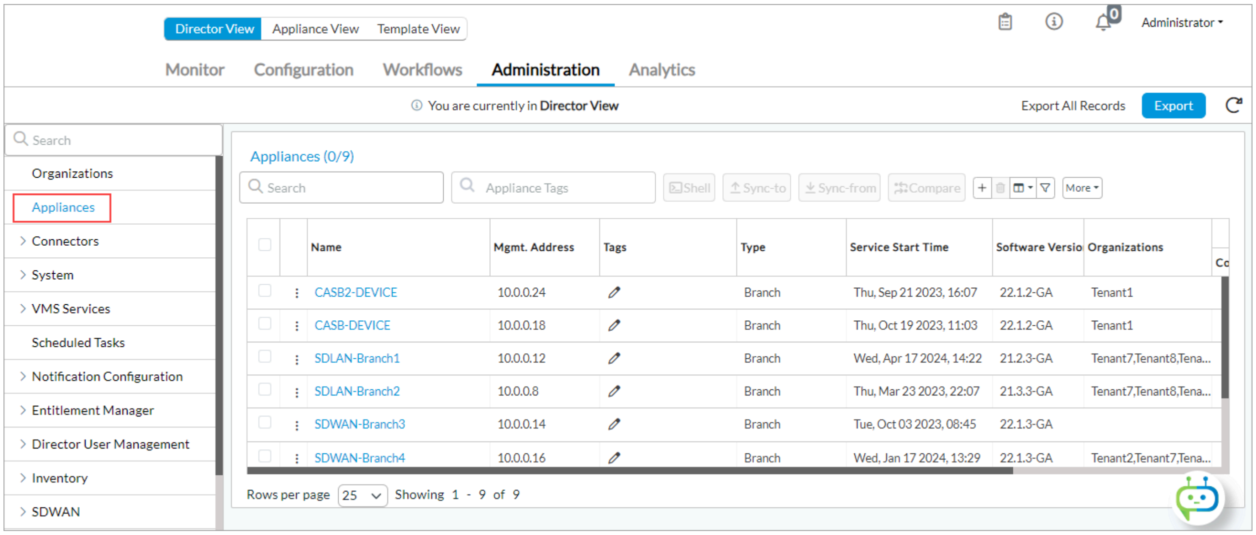
Use Predefined Vulnerability Profiles

View Predefined Vulnerability Profiles

Versa provides a set of predefined vulnerability profiles, including the Versa Recommended Profile, which detect vulnerabilities against servers and clients.

To view the predefined profiles:

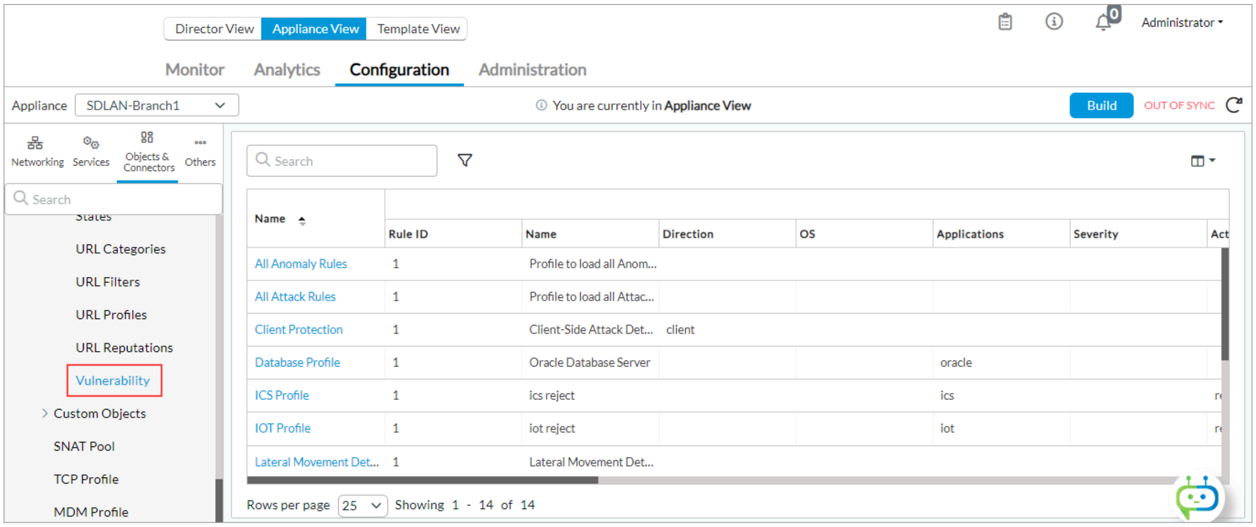
1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliance in the left menu bar.
    c. Select an appliance in the main pane. The view changes to Appliance view.



Name	Mgmt. Address	Tags	Type	Service Start Time	Software Versio	Organizations	Co
CASB2-DEVICE	10.0.0.24		Branch	Thu, Sep 21 2023, 16:07	22.1.2-GA	Tenant1	
CASB-DEVICE	10.0.0.18		Branch	Thu, Oct 19 2023, 11:03	22.1.2-GA	Tenant1	
SDLAN-Branch1	10.0.0.12		Branch	Wed, Apr 17 2024, 14:22	21.2.3-GA	Tenant7,Tenant8,Tena...	
SDLAN-Branch2	10.0.0.8		Branch	Thu, Mar 23 2023, 22:07	21.3.3-GA	Tenant7,Tenant8,Tena...	
SDWAN-Branch3	10.0.0.14		Branch	Tue, Oct 03 2023, 08:45	22.1.3-GA		
SDWAN-Branch4	10.0.0.16		Branch	Wed, Jan 17 2024, 13:29	22.1.3-GA	Tenant2,Tenant7,Tena...	

Rows per page 25 Showing 1 - 9 of 9

2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Predefined > Vulnerability in the left menu bar. The main pane lists the predefined vulnerability profiles, which are explained in the following table.



Name	Rule ID	Name	Direction	OS	Applications	Severity	Act
All Anomaly Rules	1	Profile to load all Anom...					
All Attack Rules	1	Profile to load all Attac...					
Client Protection	1	Client-Side Attack Det...	client				
Database Profile	1	Oracle Database Server			oracle		
ICS Profile	1	ics reject			ics		r
IOT Profile	1	iot reject			iot		r
Lateral Movement Det...	1	Lateral Movement Det...					

Rows per page 25 Showing 1 - 14 of 14

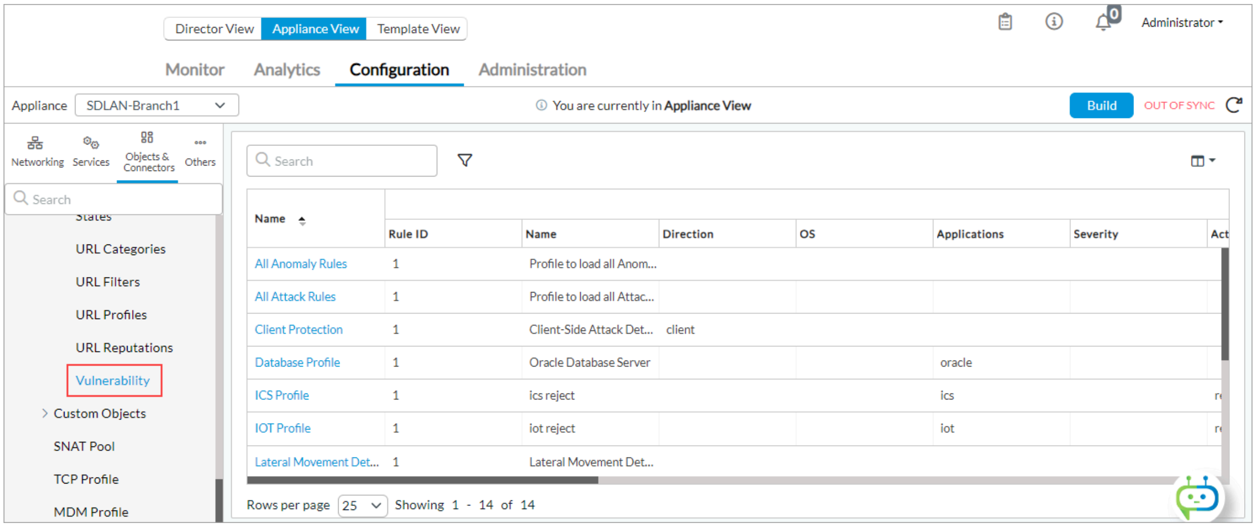
Vulnerability Profile	Description
All Anomaly Rules	Load all the anomaly signatures. Anomaly rules have threshold values; to change anomaly, see Configure Security Scanners.
All Attack Rules	Load all attack signatures.
Client Protection	Load all client-side attacks.

Database Profile	Load the Oracle database server vulnerability signatures.
ICS Profile	Load the industrial control system (ICS) vulnerability signatures.
Lateral Movement Detection	Detect post-exploitation activities in Windows OS.
Linux OS Profile	Detect all attacks specific to Linux OS.
Mac OS Profile	Detect all attacks specific to Mac OS.
Malware Profile	Detect all antivirus attacks.
Server Protection	Detect server-side attacks.
Windows OS Profile	Detect attacks specific to all Windows OSs.
Versa Branch Profile	Enable rules to detect vulnerabilities against servers and client, but by using less r common vulnerability scoring system (CVSS) range 6 through 10 vulnerabilities fo through 10 for the last 10 years. The Versa Branch Profile requires a minimum of
Versa Recommended Profile	Enable rules to detect vulnerabilities against servers and clients. These profiles co vulnerabilities for the last 10 years and critical vulnerabilities older than 10 years. requires a minimum of 16 GB of RAM. It is recommended that you use the Versa-

View Filter Values for Predefined Vulnerability Profiles

Each predefined vulnerability rule consists of a rule or a set of rules that define filter values such as action, CVSS score, and rule type. To view the filter values:

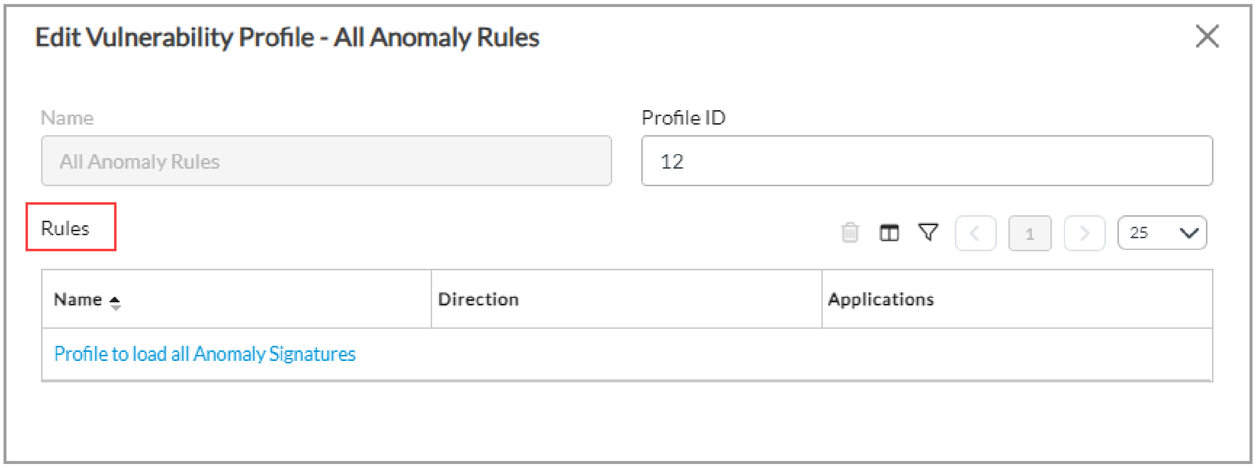
1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliance in the left menu bar
    c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Predefined > Vulnerability in the left menu bar.



Name	Rule ID	Name	Direction	OS	Applications	Severity	Act
All Anomaly Rules	1	Profile to load all Anom...					
All Attack Rules	1	Profile to load all Attac...					
Client Protection	1	Client-Side Attack Det...	client				
Database Profile	1	Oracle Database Server			oracle		
ICS Profile	1	ics reject			ics		r
IOT Profile	1	iot reject			iot		r
Lateral Movement Det...	1	Lateral Movement Det...					

Rows per page 25 Showing 1 - 14 of 14

4. Select a Predefined Vulnerability profile in the main pane.
5. Select the Rules tab, and and then select a rule to view the profile's filter values.



Edit Vulnerability Profile - All Anomaly Rules

Name: All Anomaly Rules

Profile ID: 12

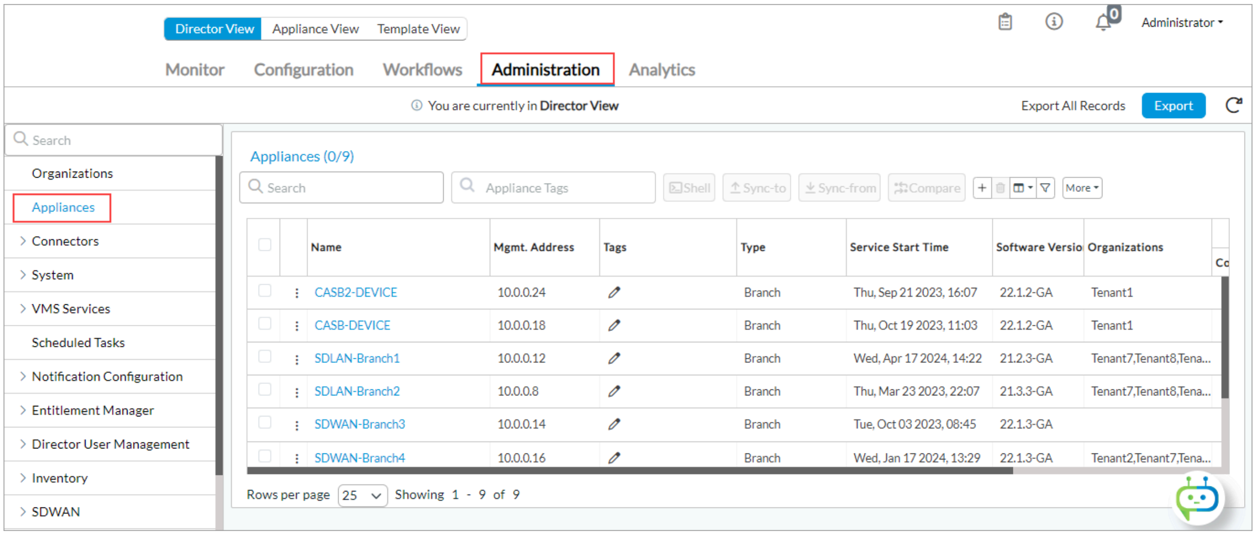
Rules

Name	Direction	Applications
Profile to load all Anomaly Signatures		

Modify a Predefined Vulnerability Profile

To modify the parameters in a predefined vulnerability profile, you create an override profile:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliance in the left menu bar.
   c. Select an appliance in the main pane. The view changes to Appliance view.

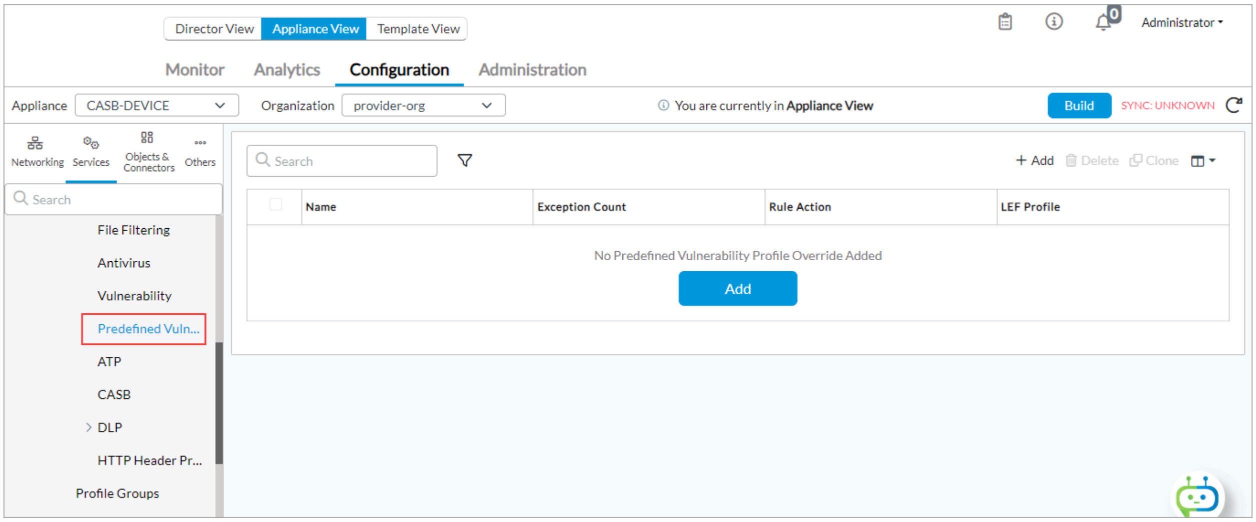


You are currently in Director View

Name	Mgmt. Address	Tags	Type	Service Start Time	Software Versio	Organizations	Co
CASB2-DEVICE	10.0.0.24		Branch	Thu, Sep 21 2023, 16:07	22.1.2-GA	Tenant1	
CASB-DEVICE	10.0.0.18		Branch	Thu, Oct 19 2023, 11:03	22.1.2-GA	Tenant1	
SDLAN-Branch1	10.0.0.12		Branch	Wed, Apr 17 2024, 14:22	21.2.3-GA	Tenant7,Tenant8,Tena...	
SDLAN-Branch2	10.0.0.8		Branch	Thu, Mar 23 2023, 22:07	21.3.3-GA	Tenant7,Tenant8,Tena...	
SDWAN-Branch3	10.0.0.14		Branch	Tue, Oct 03 2023, 08:45	22.1.3-GA		
SDWAN-Branch4	10.0.0.16		Branch	Wed, Jan 17 2024, 13:29	22.1.3-GA	Tenant2,Tenant7,Tena...	

Rows per page 25 Showing 1 - 9 of 9

2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Security > Profiles > Predefined Vulnerability Profile Override in the left menu bar.



Appliance CASB-DEVICE

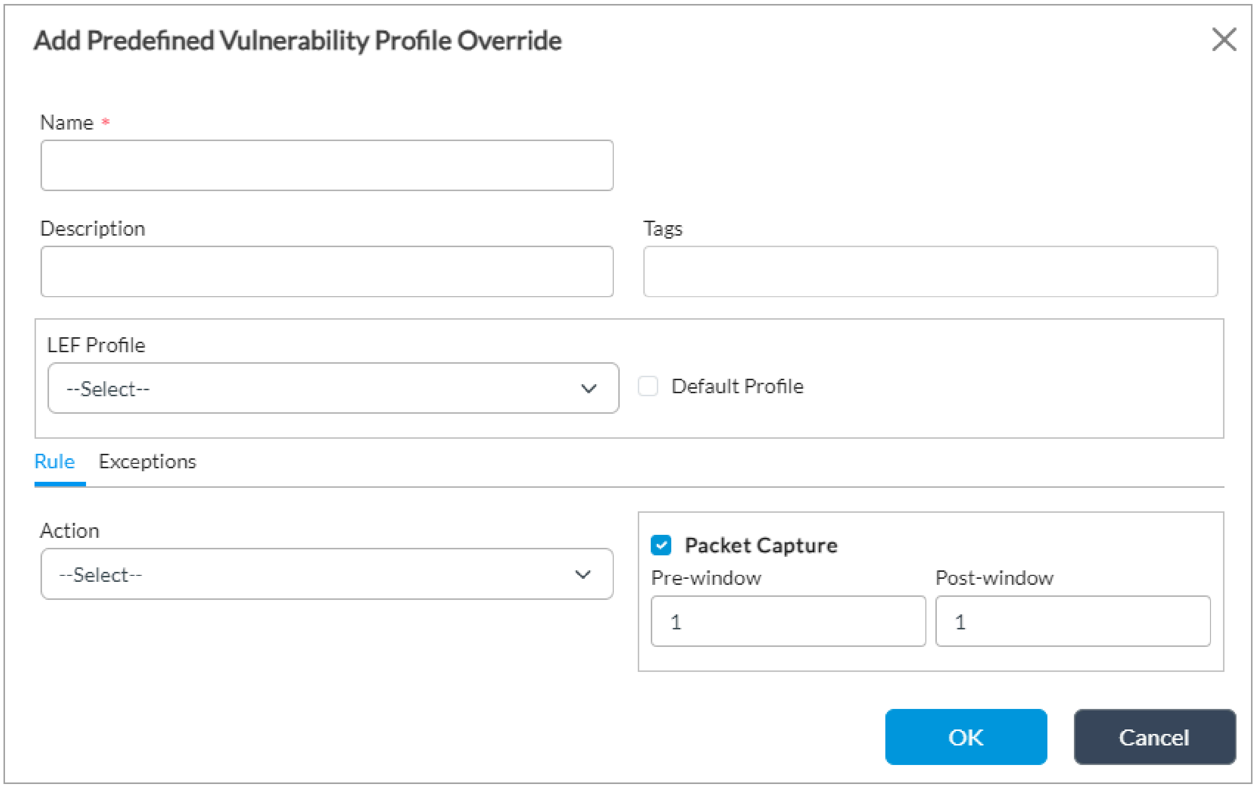
Organization provider-org

You are currently in Appliance View

Name	Exception Count	Rule Action	LEF Profile

No Predefined Vulnerability Profile Override Added

4. Click the + Add icon. In the Add Predefined Vulnerability Profile Override popup window, enter information for the following fields.



Add Predefined Vulnerability Profile Override

Name *

Description

Tags

LEF Profile: --Select--

□ Default Profile

Rule | Exceptions

Action: --Select--

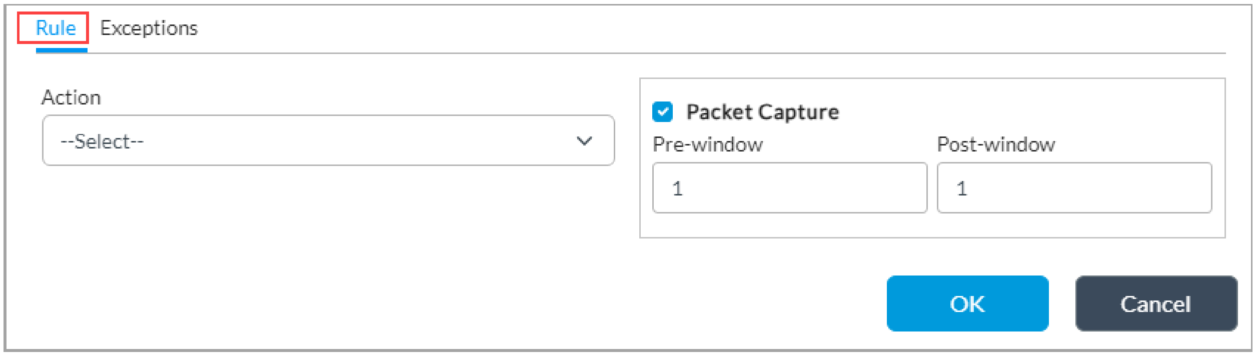
☑ Packet Capture

Pre-window: 1

Post-window: 1

Field	Description
Name (Required)	Enter a name for the modified vulnerability profile.
Description	Enter a text description for the vulnerability profile.
Tags	Enter a keyword or phrase that allows you to filter the profile name. This is useful when yo that are tagged with a particular keyword.
LEF Profile	Select a log export functionality (LEF) profile to use to record logs for the profile. For infor Configure Log Export Functionality. For information about associating a LEF profile with a Functionality.
Default Profile	Select to send logs to the default LEF profile. For information about configuring a default l Functionality.

5. Select the Rule tab to configure a vulnerability profile rule. In the popup window, enter information for the following fields.



Action: --Select--

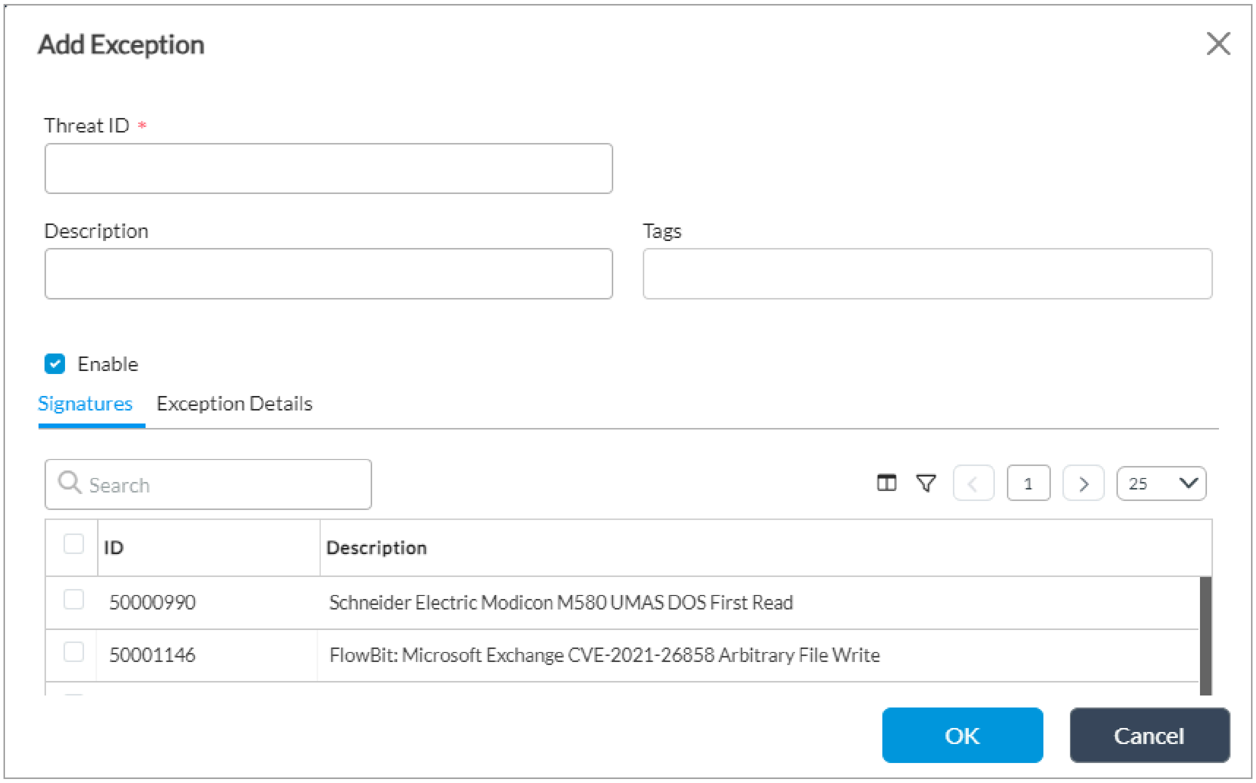
☑ Packet Capture

Pre-window: 1

Post-window: 1

Field	Description
Action	Select an action. This action overrides the action in the predefined vulnerability profile.
Packet Capture (Group of Fields)	Click to enable packet capture. Packet capture information is automatically sent to the Ana download it. For more information, see View Packet Capture Logs, below.
◦ Pre-window	Enter the number of packets immediately preceding the attacked packet that you want to
◦ Post-window	Enter the number of packets immediately following the attacked packet that you want to ca

6. Select the Exceptions tab to configure a vulnerability profile exception. Click the + Add icon, and in the Add Exception popup window, enter information for the following fields.



□	ID	Description
□	50000990	Schneider Electric Modicon M580 UMAS DOS First Read
□	50001146	FlowBit: Microsoft Exchange CVE-2021-26858 Arbitrary File Write

Field	Description
Threat ID (Required)	Enter the threat ID.
Description	Enter a text description for the threat.
Tags	Enter a keyword or phrase that allows you to filter the threat exception. This is usefu want to view those that are tagged with a particular keyword.
Signatures (Tab)	Select the vulnerability signatures to add to the vulnerability profiles exception rule.
Exception Details (Tab)	
◦ Exempt IP Address	Click the + Add icon to enter IP addresses that are exempt from the vulnerability ru
◦ Threshold (Group of fields)	Select the threshold application on the exempted IP address: ◦ Track By—Select the threshold tracking based on either source address, destin addresses.

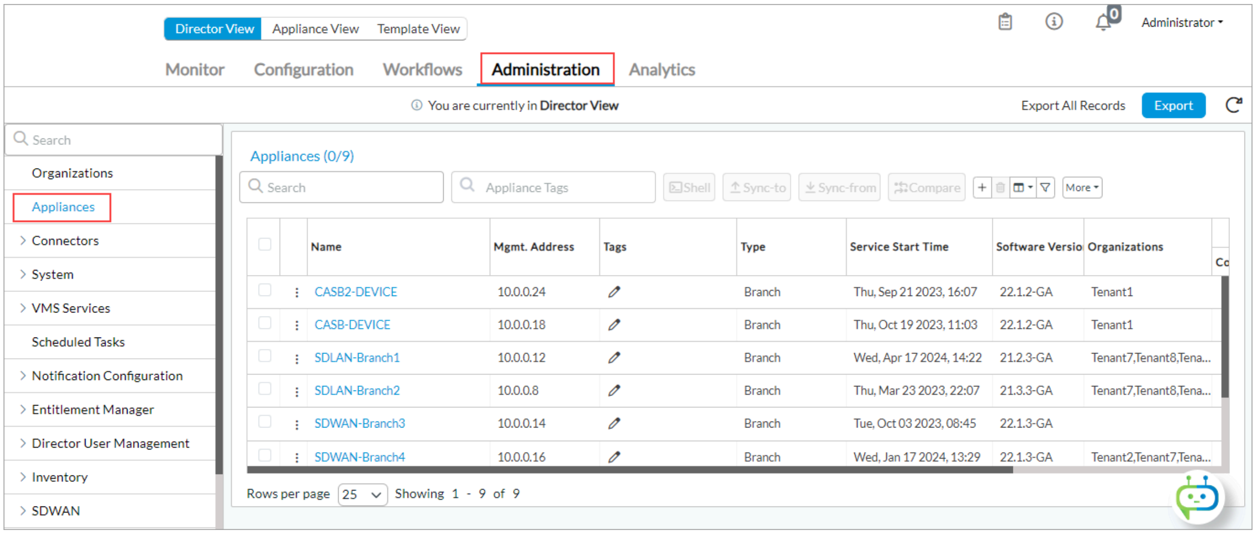
	◦ Interval—Enter an interval, in seconds. ◦ Threshold—Enter the number of hits per interval based on the traffic direction.
◦ Action	Select the action to take: ◦ Allow ◦ Alert ◦ Drop packet ◦ Drop session ◦ Reject ◦ Reset client ◦ Reset server
◦ Packet Capture (Group of Fields)	Click to enable packet capture: ◦ Pre-window—Enter the number of packets immediately preceding the attacked ◦ Post-window—Enter the number of packets immediately following the attacked

7. Click OK.

After you override a predefined vulnerable profile, you must re-apply it to the security access policy rule, as described in the Associate Vulnerability Profiles with Access Policy Profiles section, below.

Create Custom Vulnerability Profiles

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliance in the left menu bar.
    c. Select an appliance in the main pane. The view changes to Appliance view.



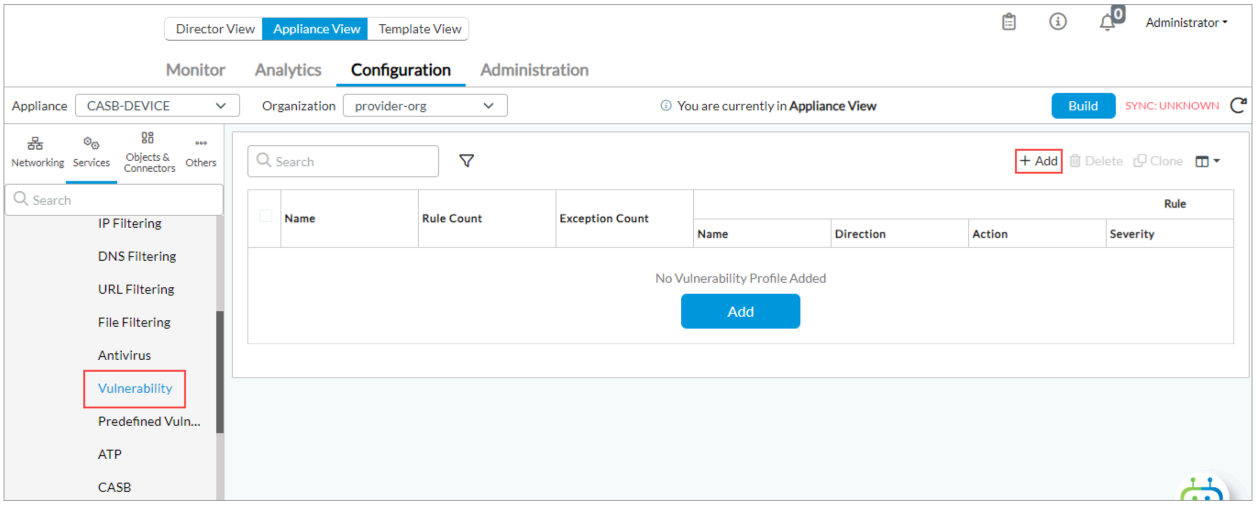
You are currently in Director View

Appliances (0/9)

Name	Mgmt. Address	Tags	Type	Service Start Time	Software Versio	Organizations	Co
CASB2-DEVICE	10.0.0.24		Branch	Thu, Sep 21 2023, 16:07	22.1.2-GA	Tenant1	
CASB-DEVICE	10.0.0.18		Branch	Thu, Oct 19 2023, 11:03	22.1.2-GA	Tenant1	
SDLAN-Branch1	10.0.0.12		Branch	Wed, Apr 17 2024, 14:22	21.2.3-GA	Tenant7,Tenant8,Tena...	
SDLAN-Branch2	10.0.0.8		Branch	Thu, Mar 23 2023, 22:07	21.3.3-GA	Tenant7,Tenant8,Tena...	
SDWAN-Branch3	10.0.0.14		Branch	Tue, Oct 03 2023, 08:45	22.1.3-GA		
SDWAN-Branch4	10.0.0.16		Branch	Wed, Jan 17 2024, 13:29	22.1.3-GA	Tenant2,Tenant7,Tena...	

Rows per page 25 Showing 1 - 9 of 9

2. Select the Configuration tab in the top menu bar.
3. Select Services > Next Gen Firewall > Security > Profiles > Vulnerability in the left menu bar
4. Click the + Add icon to create a new vulnerability profile.



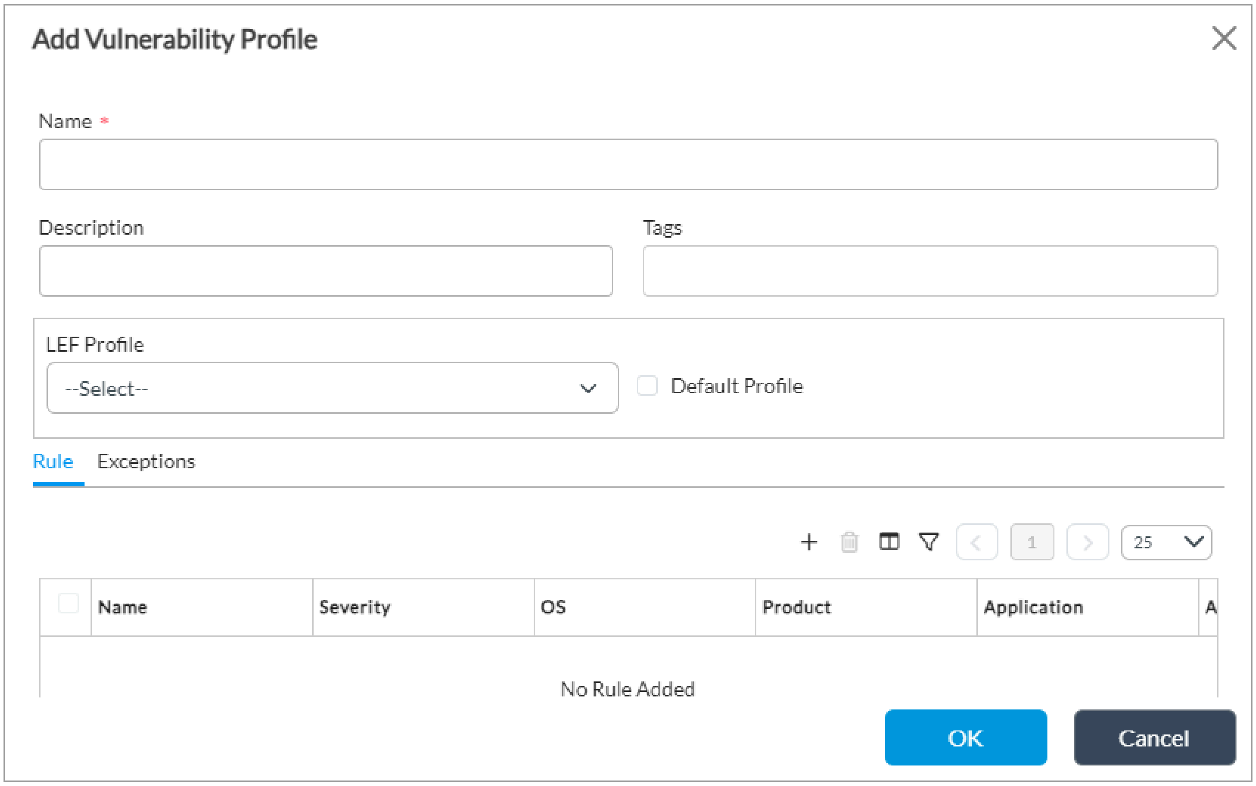
Appliance: CASB-DEVICE
Organization: provider-org

You are currently in Appliance View

Name	Rule Count	Exception Count	Rule			
			Name	Direction	Action	Severity

No Vulnerability Profile Added

5. In the Add Vulnerability Profile popup window, enter information for the following fields.


Add Vulnerability Profile

Name *

Description

Tags

LEF Profile

--Select--

□ Default Profile

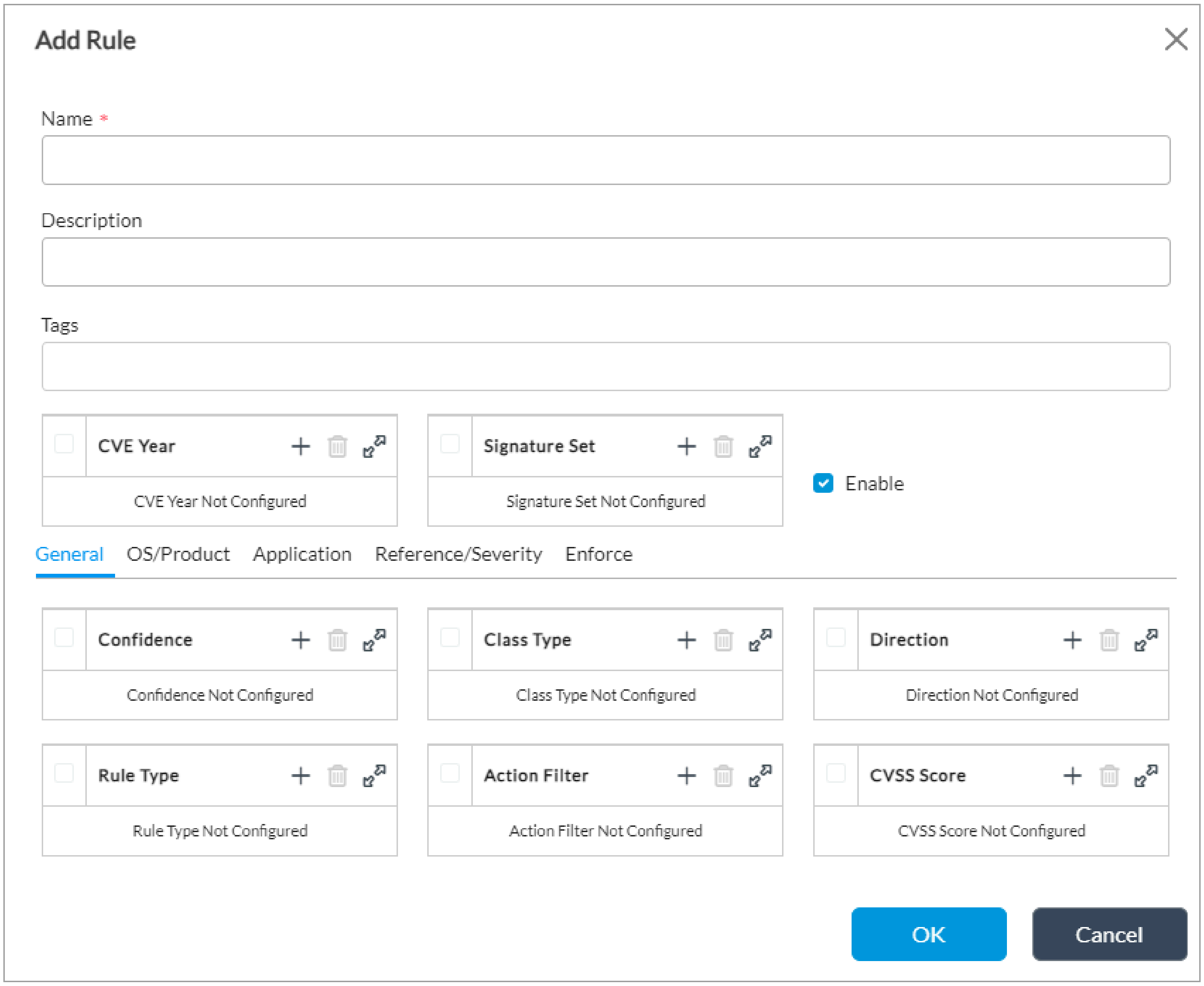
Rule Exceptions

□	Name	Severity	OS	Product	Application	A

No Rule Added

Field	Description
Name (Required)	Enter a name for the vulnerability profile.
Description	Enter a text description for the vulnerability profile.
Tags	Enter a keyword or phrase that allows you to filter the profile name. This is useful when you that are tagged with a particular keyword.
LEF Profile	Select a log export functionality (LEF) profile to use to record logs for the vulnerability profil profile, see Configure Log Export Functionality.
Default Profile	Click to send logs to the default LEF profile. For information about configuring a default LEF Functionality.

6. Select the Rule tab to configure a vulnerability profile rule. Click the + Add icon, and in the Add Rule popup window, enter information for the following fields. You can add one or more rules in a single vulnerability profile. After you have created a rule, you can modify and save it without altering the functionality of the existing vulnerability profile.



Add Rule

Name *

Description

Tags

□ CVE Year — CVE Year Not Configured

□ Signature Set — Signature Set Not Configured

☑ Enable

General | OS/Product | Application | Reference/Severity | Enforce

□ Confidence — Confidence Not Configured

□ Class Type — Class Type Not Configured

□ Direction — Direction Not Configured

□ Rule Type — Rule Type Not Configured

□ Action Filter — Action Filter Not Configured

□ CVSS Score — CVSS Score Not Configured

Field	Description
Name (Required)	Enter a name for the vulnerability profile rule.
Description	Enter a text description for the vulnerability profile rule.
Tags	Enter a keyword or phrase that allows you to filter the profile rule name. This is useful wh those that are tagged with a particular keyword.
CVE Year	Click the + Add icon and select the common vulnerabilities and exposures (CVE) year. T database and identifies the attacks. For example, select 2016 to block attacks for CVE 20

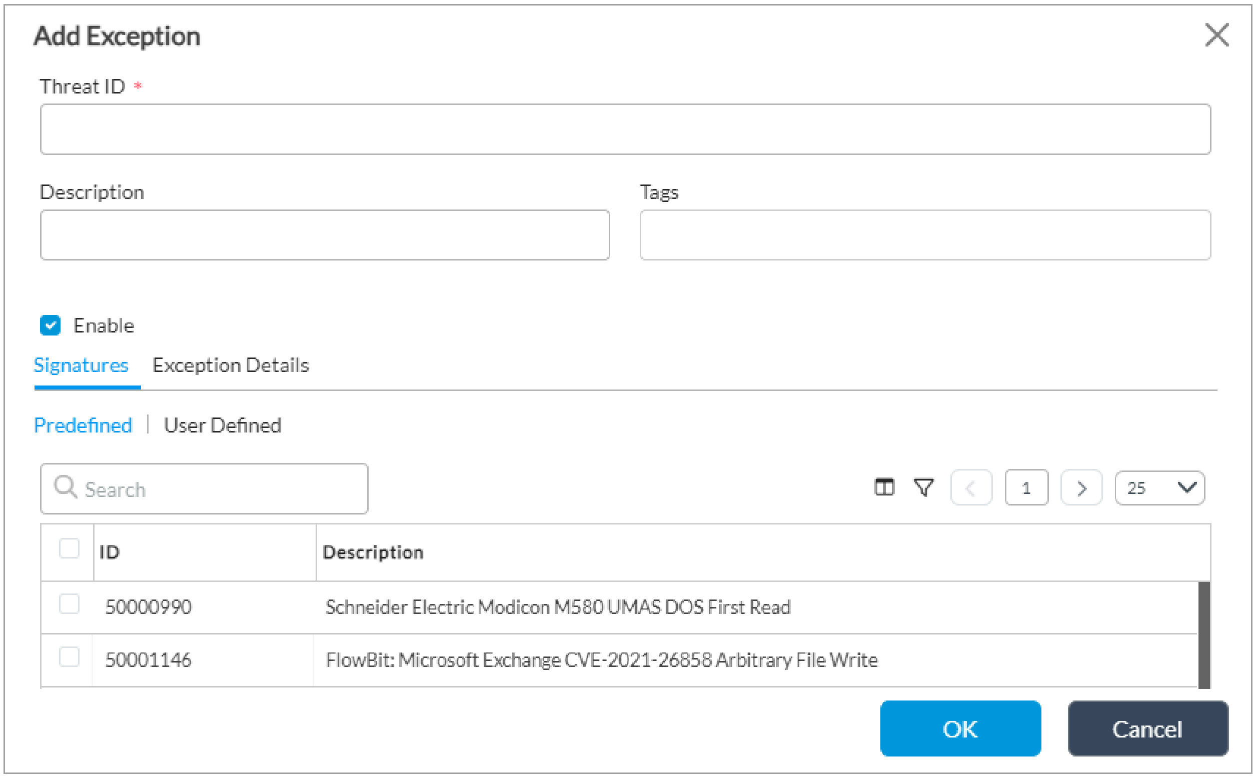
Signature Set	Click the + Add icon and select predefined, user-defined, or both types of signatures.
Enable	Click to enable the vulnerability profile rule.
General (Tab)	Configure general parameters for signatures to match.
◦ Confidence	Click the + Add icon and select the confidence level to match. Confidence indicates the vulnerability. In certain cases, Versa has deliberately kept confidence levels lower to mitig performance concerns. Signatures match if the confidence level is greater than or equal t *Value*: 0 through 9, Unspecified. The higher the value, the higher is the confidence. For e 0 is the lowest. It is recommended to choose a signature value from 6 through 9.
◦ Class Type	Click the + Add icon and select a class type to match.
◦ Direction	Click the + Add icon and select the traffic direction for applying the rule to signatures: ◦ Both ◦ Client ◦ Server
◦ Rule Type	Click the + Add icon and select a rule type to match: ◦ All rules ◦ Anomaly rules ◦ Signature rules
◦ Action Filter	Click the + Add icon and select the action to take if the signatures match the rule: ◦ Alert

	◦ Drop session ◦ Reject
◦ CVSS Score	Click the + Add icon and select the CVSS score for the signatures to match.
OS/Product (Tab)	Configure operating system and product parameters for signatures to match.
◦ OS Name (Required)	Select the name of the operating system to match and click the + Add icon.
◦ OS Version	Select the version of the operating system to match and click the + Add icon.
◦ Product Name (Required)	Select the name of the product to match and click the + Add icon.
◦ Product Version	Select the version of the product to match and click the + Add icon.
Application (Tab)	Configure application for signatures to match.
◦ Applications	Click the + Add icon and select the application to match.
Reference/Severity (Tab)	
◦ Reference Type (Required)	Select and use signatures that match a specific reference type, as specified in the databa reference type to the rule.
◦ Reference Value	Select and use signatures that match a specific reference value, as specified in the datab reference value to the rule.
◦ Severity	Click a severity to limit signatures to those that match that severity type: ◦ Any

	◦ Critical ◦ High ◦ Informational ◦ Low ◦ Medium ◦ Unspecified
Enforce (Tab)	
◦ Action	Select an action to take on matching traffic. The action applies to both predefined and cus ◦ Default ◦ Predefined ▪ Allow ▪ Alert ▪ Drop packet ▪ Drop session ▪ Reject ▪ Reset client ▪ Reset server ◦ Predefined Persistent ▪ Versa action block SIP ▪ Versa action block SP ▪ Versa action block DIP ▪ Versa action block DP ▪ Versa action block SIP SP ▪ Versa action block DIP DP ▪ Versa action block SIP SP DIP DP ▪ Versa action block SIP SP DIP DP Protocol
◦ Packet Capture (Group of Fields)	Click to enable packet capture: ◦ Pre-window—Enter the number of packets immediately preceding the attacked packe ◦ Post-window—Enter the number of packets immediately following the attacked packe

7. Select the Exceptions tab to configure a vulnerability profile exception. Click the + Add icon, and in the Add

Exception popup winter, enter information for the following fields.



□	ID	Description
□	50000990	Schneider Electric Modicon M580 UMAS DOS First Read
□	50001146	FlowBit: Microsoft Exchange CVE-2021-26858 Arbitrary File Write

Field	Description
Threat ID (Required)	Enter a name for the threat ID.
Description	Enter a text description for the threat ID.
Tags	Enter a keyword or phrase that allows you to filter the threat ID. This is useful when y those that are tagged with a particular keyword.
Enable	Click to enable the exception.
Signatures (Tab)	Select the predefined or custom vulnerability signatures to add in the vulnerability pr
◦ Predefined (Tab)	Select the predefined vulnerability signatures to add in the vulnerability profiles exce
◦ User-defined (Tab)	Select the custom vulnerability signatures to add in the vulnerability profiles exceptio
Exception Details (Tab)	

◦ Exempt IP Address	Click the + Add icon and enter IP addresses to exempt from the vulnerability rule.
◦ Threshold (Group of Fields)	Configure the thresholds for the exempted IP address: ◦ Track By—Select how to track the IP address: ▪ Destination address ▪ Source address ▪ Source and destination addresses ◦ Interval—Enter a time interval, in seconds. ◦ Threshold—Enter the number of hits per interval based on the traffic direction.
◦ Action	Select the action to take: ◦ Predefined ▪ Allow ▪ Alert ▪ Drop packet ▪ Drop session ▪ Reject ▪ Reset client ▪ Reset server
◦ Packet Capture	Click to enable packet capture: ◦ Pre-window (Required)—Enter the number of packets immediately preceding th ◦ Post-window—Enter the number of packets immediately following the attacked

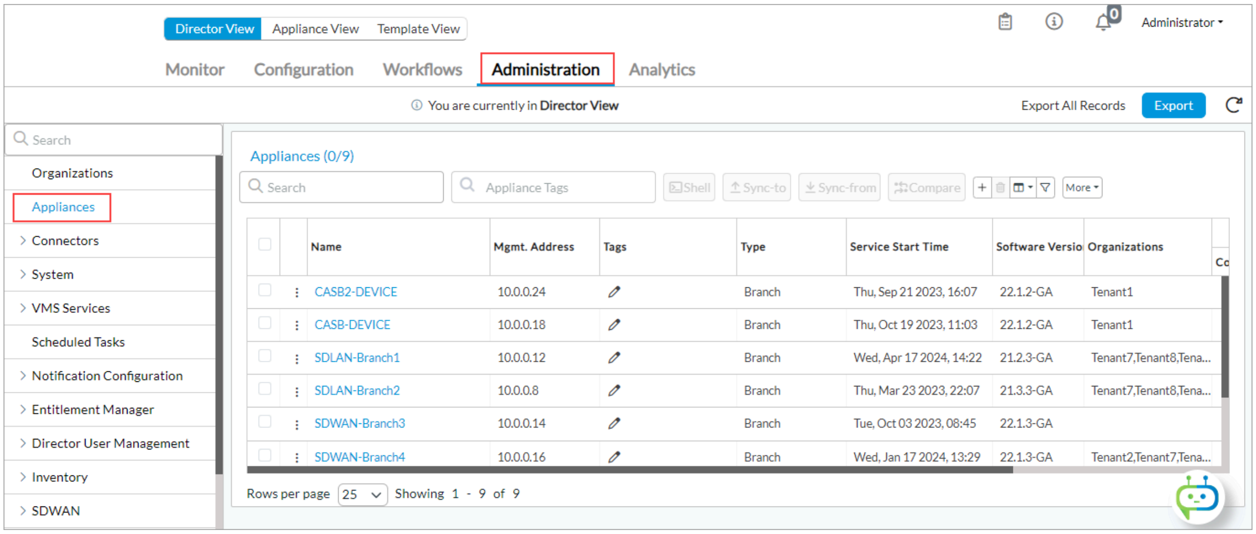
8. Click OK.

Associate Vulnerability Profiles with Access Policy Profiles

To perform intrusion detection and prevention on incoming traffic, you associate a vulnerability profile with an access policy:

1. In Director view:

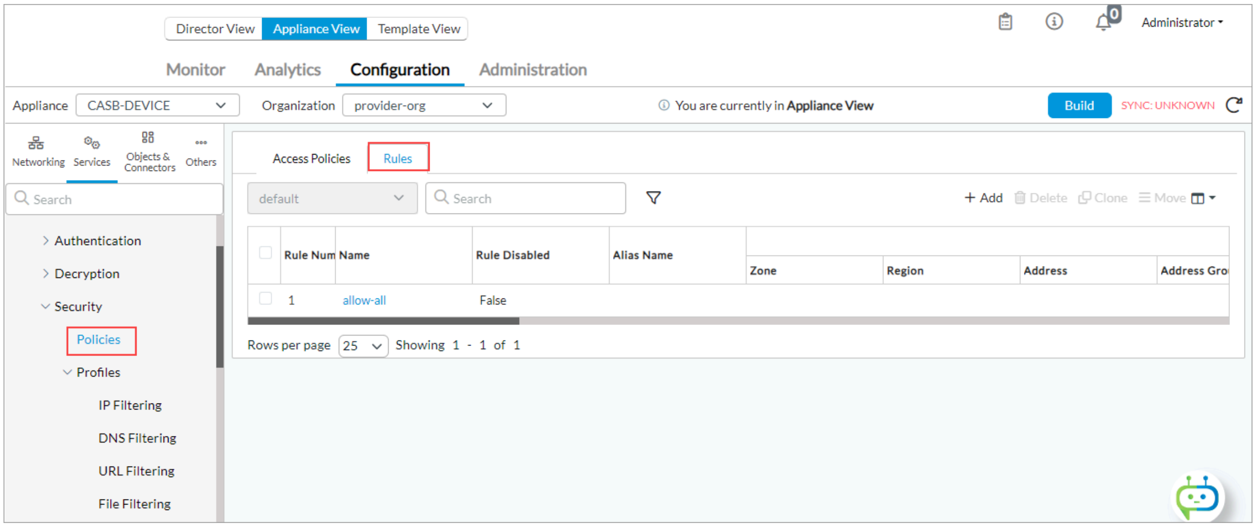
a. Select the Administration tab in the top menu bar.
b. Select Appliance in the left menu bar.
c. Select an appliance in the main pane. The view changes to Appliance view.



		Name	Mgmt. Address	Tags	Type	Service Start Time	Software Versio	Organizations	Co
□	⋮	CASB2-DEVICE	10.0.0.24	✎	Branch	Thu, Sep 21 2023, 16:07	22.1.2-GA	Tenant1	
□	⋮	CASB-DEVICE	10.0.0.18	✎	Branch	Thu, Oct 19 2023, 11:03	22.1.2-GA	Tenant1	
□	⋮	SDLAN-Branch1	10.0.0.12	✎	Branch	Wed, Apr 17 2024, 14:22	21.2.3-GA	Tenant7,Tenant8,Tena...	
□	⋮	SDLAN-Branch2	10.0.0.8	✎	Branch	Thu, Mar 23 2023, 22:07	21.3.3-GA	Tenant7,Tenant8,Tena...	
□	⋮	SDWAN-Branch3	10.0.0.14	✎	Branch	Tue, Oct 03 2023, 08:45	22.1.3-GA		
□	⋮	SDWAN-Branch4	10.0.0.16	✎	Branch	Wed, Jan 17 2024, 13:29	22.1.3-GA	Tenant2,Tenant7,Tena...	

Rows per page 25 Showing 1 - 9 of 9

2. Select Configuration in the top menu bar.
3. Select Services > Next Gen Firewall > Security > Policies in the left menu bar.
4. Click the Rules tab to display the access policy rules.



Appliance CASB-DEVICE

Organization provider-org

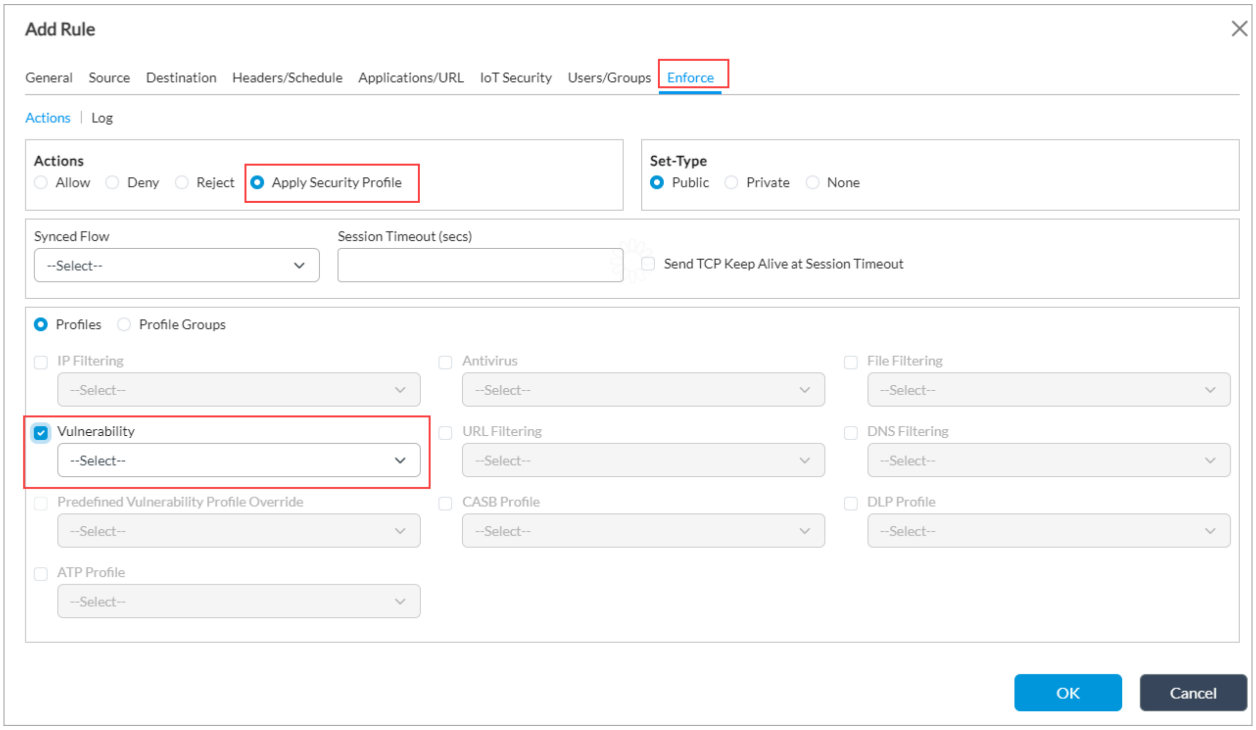
You are currently in Appliance View

default

	Rule Num	Name	Rule Disabled	Alias Name	Zone	Region	Address	Address Gro
□	1	allow-all	False					

Rows per page 25 Showing 1 - 1 of 1

5. Select the desired access policy rule. The Add Rule popup window displays.
6. Select the Enforce tab.
   a. In the Actions section, select Apply Security Profile. When you select this field, the Profiles section, on the lower part of the popup window, is then selected.
   b. Click Vulnerability and select the vulnerability profile to associate with the security access policy rule. The drop-down includes both predefined and custom vulnerability profiles.



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: --Select--

□ URL Filtering: --Select--

□ DNS Filtering: --Select--

□ Predefined Vulnerability Profile Override: --Select--

□ CASB Profile: --Select--

□ DLP Profile: --Select--

□ ATP Profile: --Select--

c. If you select a predefined vulnerability profile, the Predefined Vulnerability Profile Override field is selected, and you must select an override profile. For more information, see Modify a Predefined Vulnerability Profile, above.

d. Click OK.

7. Check the compilation state of the vulnerability profile. For more information, see View Signature Compilation Status and Loaded Signatures.

To disable the vulnerability profile for an access profile, unselect the Vulnerability field.

For more information about access policies, see Configure a Security Access Policy.

Configure Custom Vulnerability IPS Signatures

You can configure a custom vulnerability IPS signature that includes with both predefined and custom signatures. A VOS device scans the network traffic for both predefined and custom vulnerabilities and enforces the configured security action if a match is found.

You can import and use your own custom IPS signatures. To do this, upload the signatures to the Director node and then push the IDS signatures to any VOS device that is managed by the Director node. Then, you can enable and configure a vulnerability profile that includes the custom IPS signature.

Create Custom IPS Signatures

When you create custom IPS signatures, they must be in the snort rule format. For more information, see www.snort.org and the documentation at https://suricata.readthedocs.io.

The following is an example of a snort rule:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"Directory Traversal"; flow:to_server;
content:"GET"; depth:3; nocase; http_method; content:"|2e 2e 5c|"; http_uri; classtype:web-application-
attack; sid:1910000001; )
```

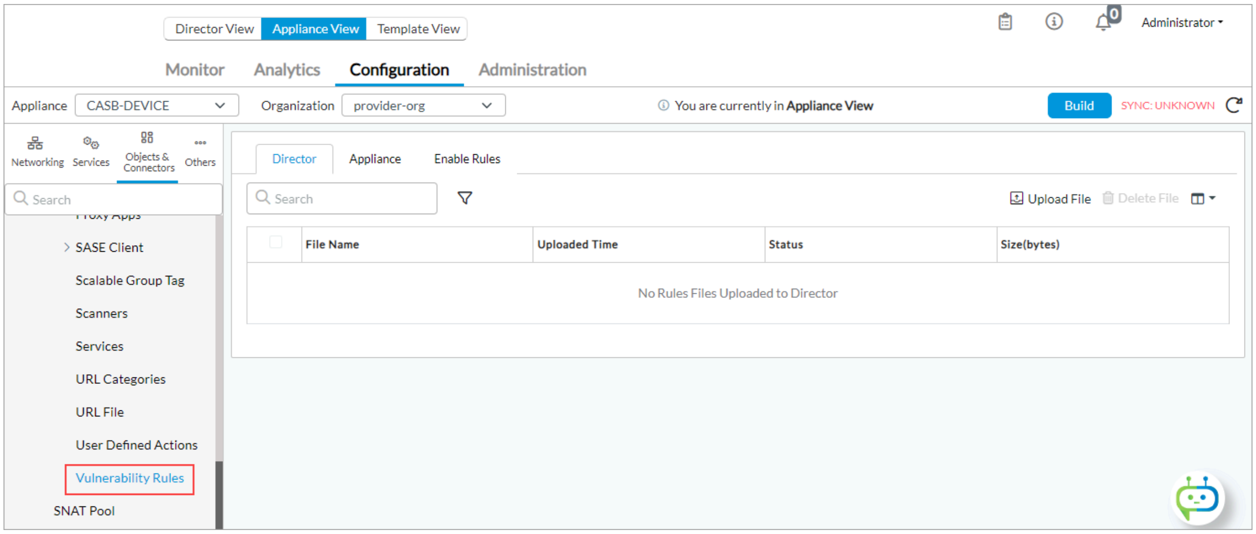
Currently, VOS devices do not support the following keywords in custom signatures: hash, protected_content, http_encode, and byte_math.

It is recommended that a custom signature be in the SID range 4293000000 through 4294000000.

Configure Custom IPS Signatures

An IPS signature file contains vulnerability rules. To configure a custom IPS signature file:

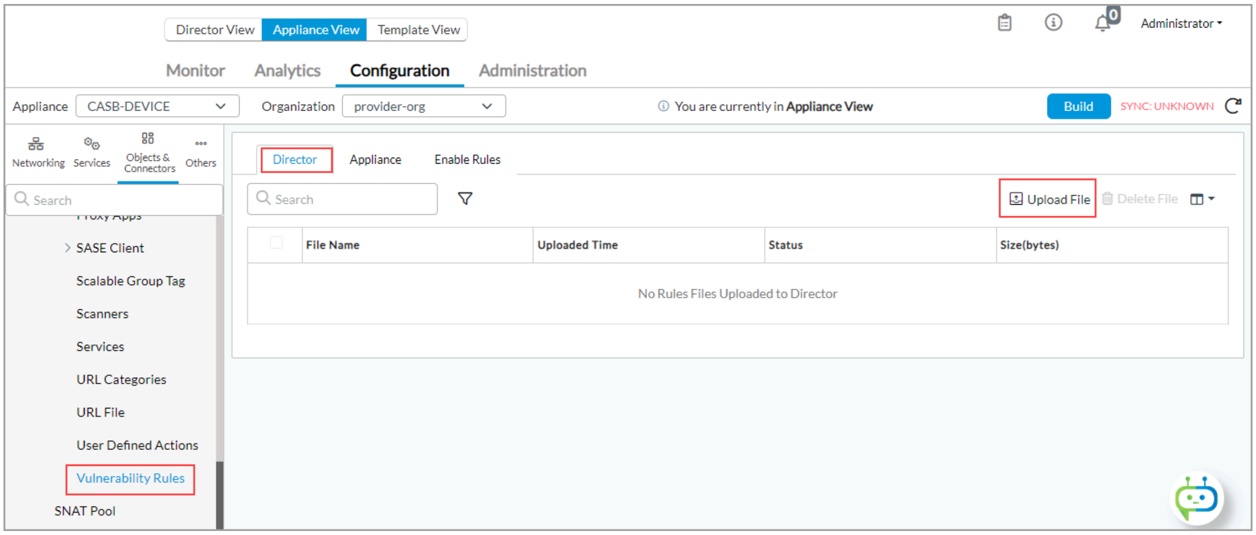
1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliance in the left menu bar.
    c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Objects > Custom Objects > Vulnerability Rules in the left menu bar.



□	File Name	Uploaded Time	Status	Size(bytes)

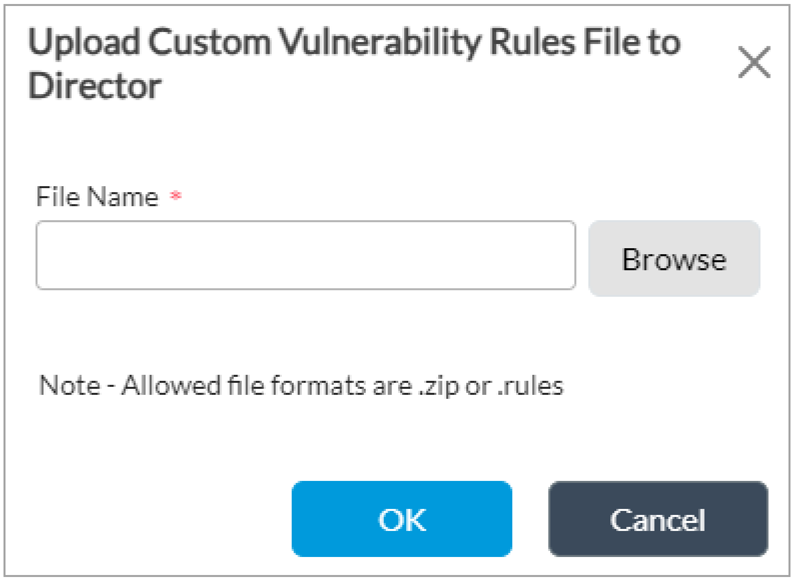
No Rules Files Uploaded to Director

4. In the main pane, select the Director tab.
5. To upload a custom vulnerability rules file to the Director from a local folder:
    a. Select the Upload icon.



No Rules Files Uploaded to Director

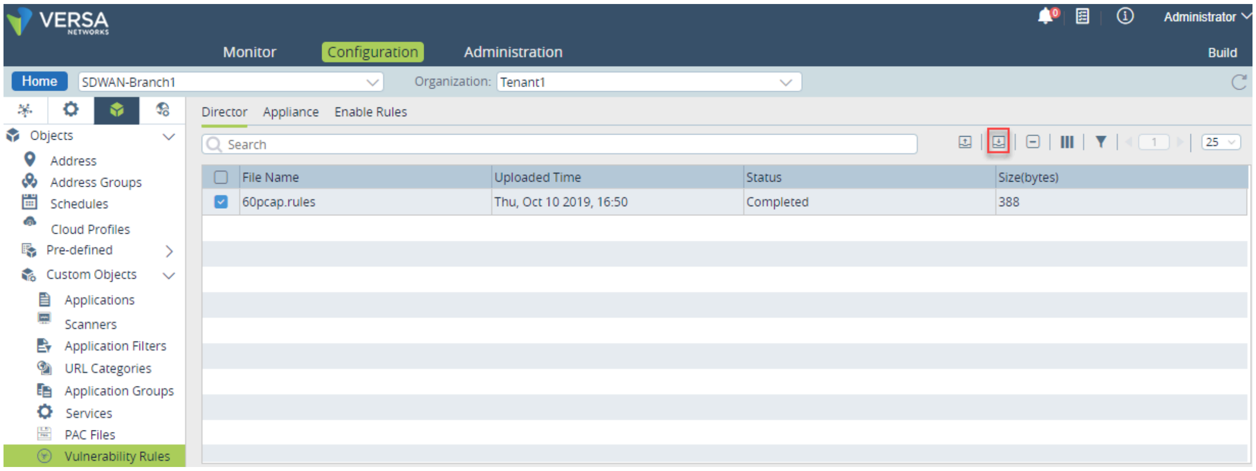
b. Click Browse, select the desired file from a local folder, and then click OK.


Upload Custom Vulnerability Rules File to Director

Note - Allowed file formats are .zip or .rules

6. (For Releases 21.2 and earlier.) To download a custom vulnerability rules file from the Director to a local folder:

   a. Select the file in the main panel and click the Download icon.

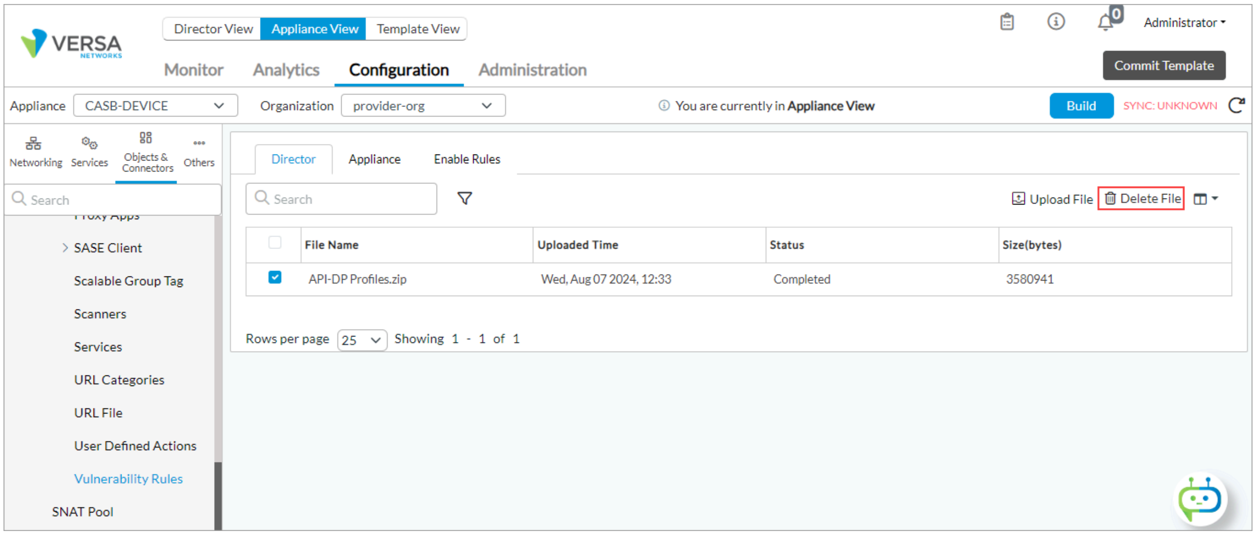


SDWAN-Branch1 Organization: Tenant1

	File Name	Uploaded Time	Status	Size(bytes)
☑	60pcap.rules	Thu, Oct 10 2019, 16:50	Completed	388

b. Enter a name for the file and click Save.

7. To delete a custom vulnerability rules file, select the file in the main pane and then click the Delete icon.



Appliance CASB-DEVICE Organization provider-org

You are currently in Appliance View

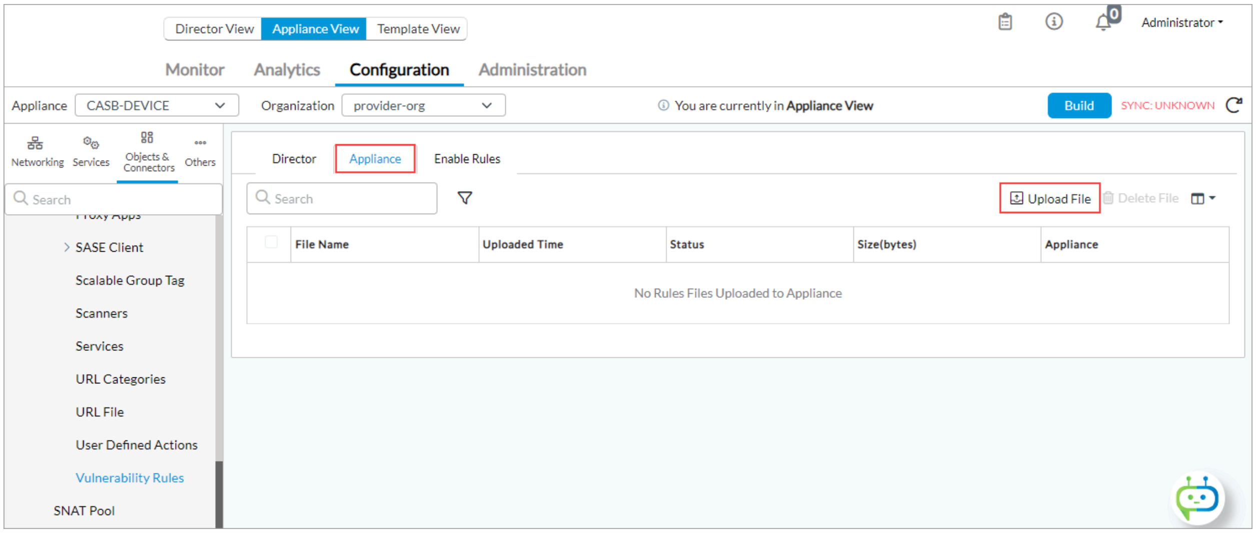
	File Name	Uploaded Time	Status	Size(bytes)
☑	API-DP Profiles.zip	Wed, Aug 07 2024, 12:33	Completed	3580941

Rows per page 25 Showing 1 - 1 of 1

8. To associate a VOS device with a custom vulnerability rules file, select the Appliance tab.

9. To upload a custom vulnerability rules file to the Director node from a local folder:

   a. Select the Upload icon.



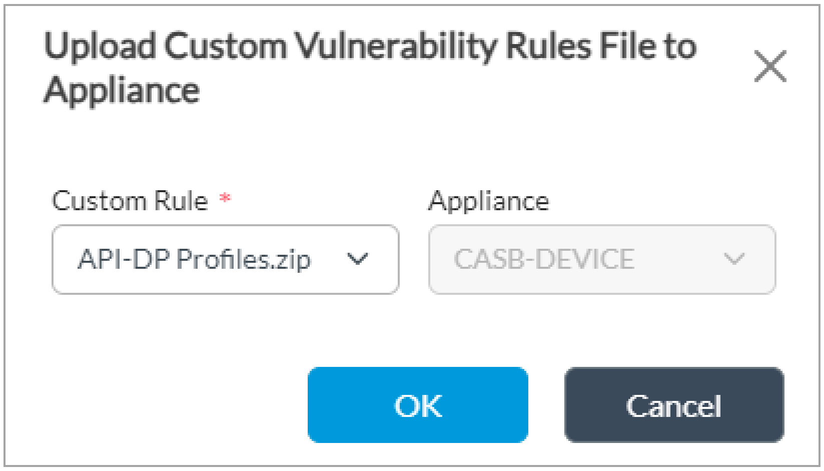
Appliance: CASB-DEVICE

Organization: provider-org

File Name	Uploaded Time	Status	Size(bytes)	Appliance

No Rules Files Uploaded to Appliance

b. Select a rule in the Custom Rule field and click OK.

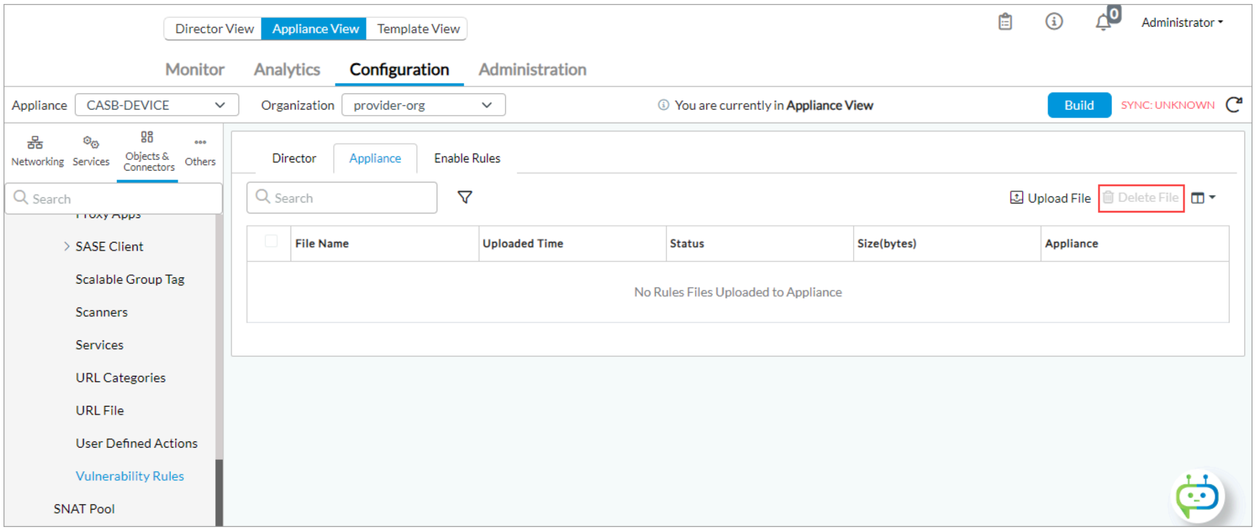


Upload Custom Vulnerability Rules File to Appliance

Custom Rule *: API-DP Profiles.zip

Appliance: CASB-DEVICE

10. To delete custom vulnerability rules file, select the file in the main pane and then select the 🗑 Delete icon.

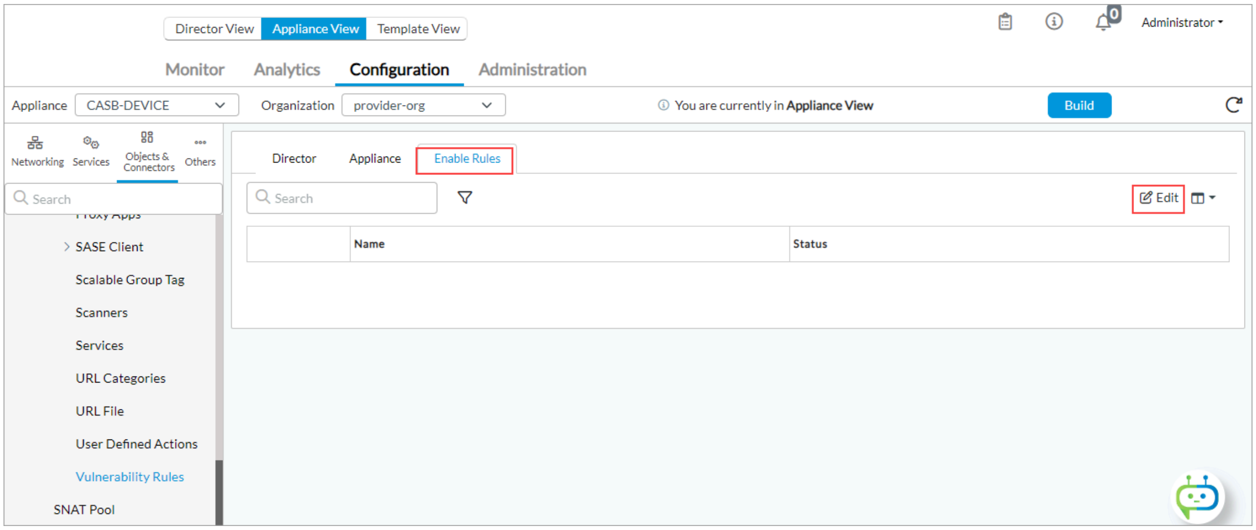


File Name	Uploaded Time	Status	Size(bytes)	Appliance

No Rules Files Uploaded to Appliance

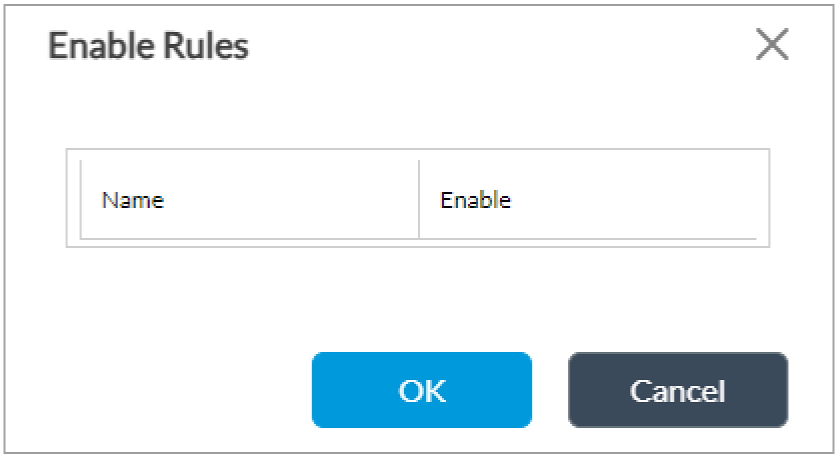
11. To enable the custom IPS signature for vulnerability profiles on a tenant:

    a. Select the Enable Rules tab, select the rule from the main pane, and click the Edit icon.



	Name	Status

    b. Click the Enable checkbox to enable a rule for the custom IPS signature.



Enable Rules

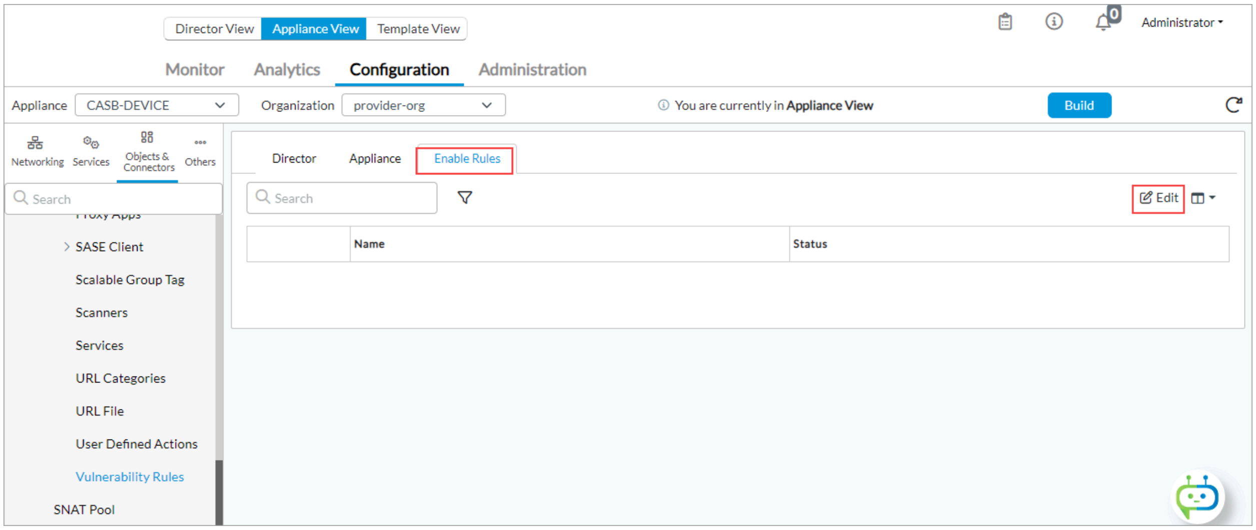
Name	Enable

c. Click OK.

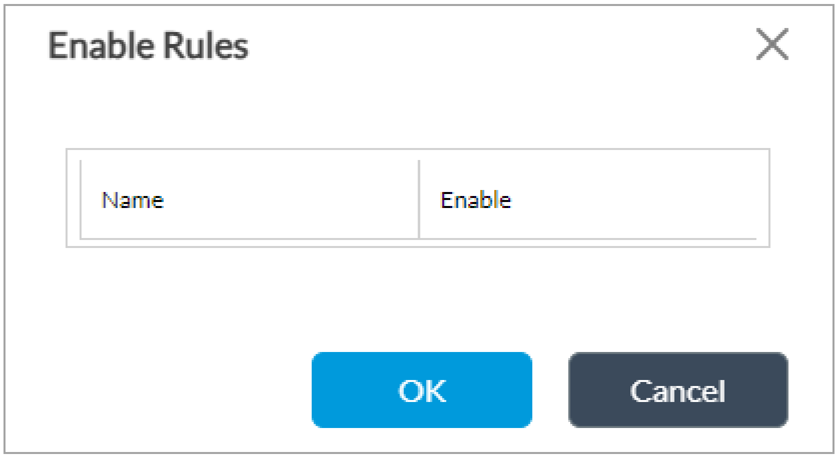
Deactivate Custom IPS Signatures for Custom Vulnerability

To deactivate a custom IPS signature for custom vulnerability:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliance in the left menu bar.
   c. Select an appliance 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 > Vulnerability Rules in the left menu bar.
4. Click the Enable Rules tab.
5. Click the 📝 Edit icon in the main pane to edit the setting in Enable Rules window.



6. Deselect the Enable checkbox.



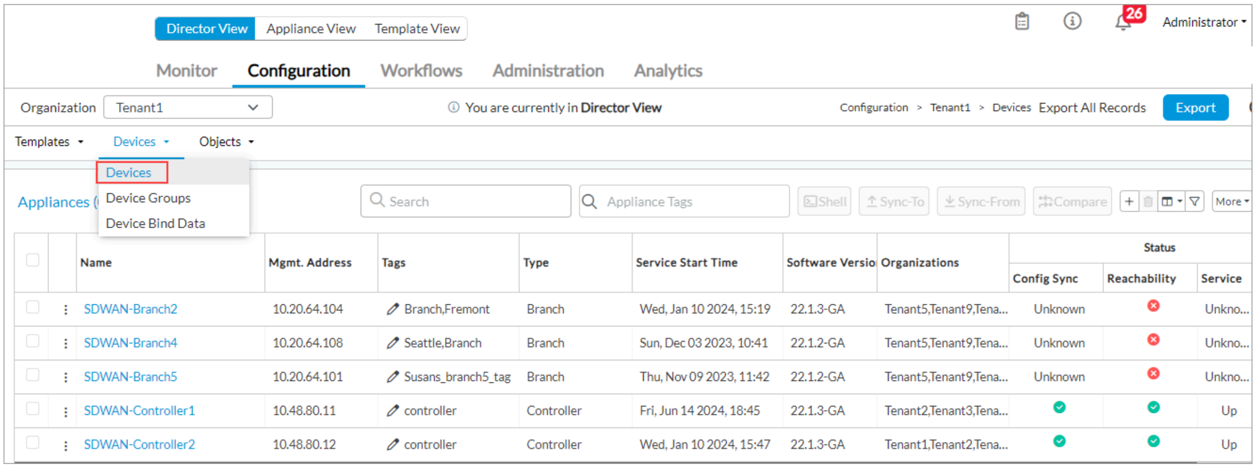
7. Click OK.

View Signature Compilation Status and Loaded Signatures

If you change the vulnerability profile in an existing access policy rule, the database is recompiled and it takes some time for the new vulnerability profile to take effect. During this transition, you can view the status of the profile from the time you change the profile to time a profile takes effect.

To check the compilation status:

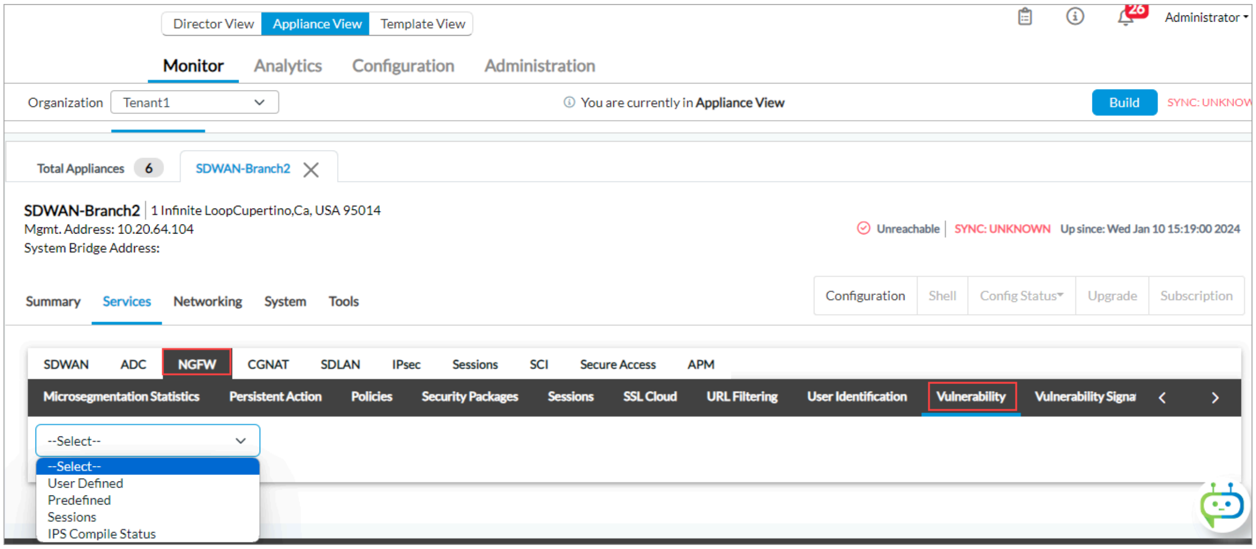
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.



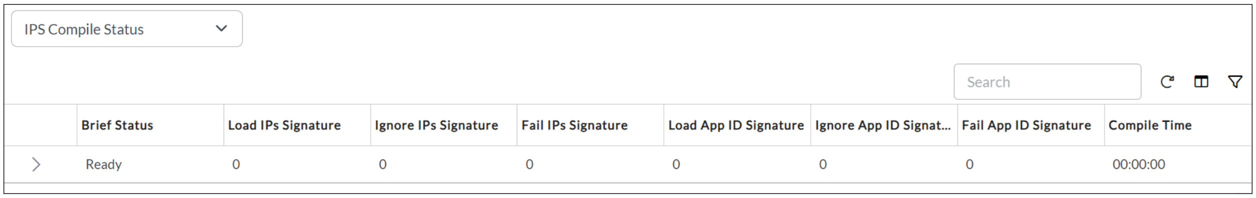
	Name	Mgmt. Address	Tags	Type	Service Start Time	Software Versio	Organizations	Status		
								Config Sync	Reachability	Service
□	SDWAN-Branch2	10.20.64.104	Branch,Fremont	Branch	Wed, Jan 10 2024, 15:19	22.1.3-GA	Tenant5,Tenant9,Tena...	Unknown	✗	Unkno...
□	SDWAN-Branch4	10.20.64.108	Seattle,Branch	Branch	Sun, Dec 03 2023, 10:41	22.1.2-GA	Tenant5,Tenant9,Tena...	Unknown	✗	Unkno...
□	SDWAN-Branch5	10.20.64.101	Susans_branch5_tag	Branch	Thu, Nov 09 2023, 11:42	22.1.2-GA	Tenant5,Tenant9,Tena...	Unknown	✗	Unkno...
□	SDWAN-Controller1	10.48.80.11	controller	Controller	Fri, Jun 14 2024, 18:45	22.1.3-GA	Tenant2,Tenant3,Tena...	✓	✓	Up
□	SDWAN-Controller2	10.48.80.12	controller	Controller	Wed, Jan 10 2024, 15:47	22.1.3-GA	Tenant1,Tenant2,Tena...	✓	✓	Up

2. Select the Monitor tab in the top menu bar.

3. Select Services > NGFW > Vulnerability in the left menu bar.



4. Select IPS Compile Status from the drop-down. The extended window displays the details of the profile.



	Brief Status	Load IPs Signature	Ignore IPs Signature	Fail IPs Signature	Load App ID Signature	Ignore App ID Signat...	Fail App ID Signature	Compile Time
>	Ready	0	0	0	0	0	0	00:00:00

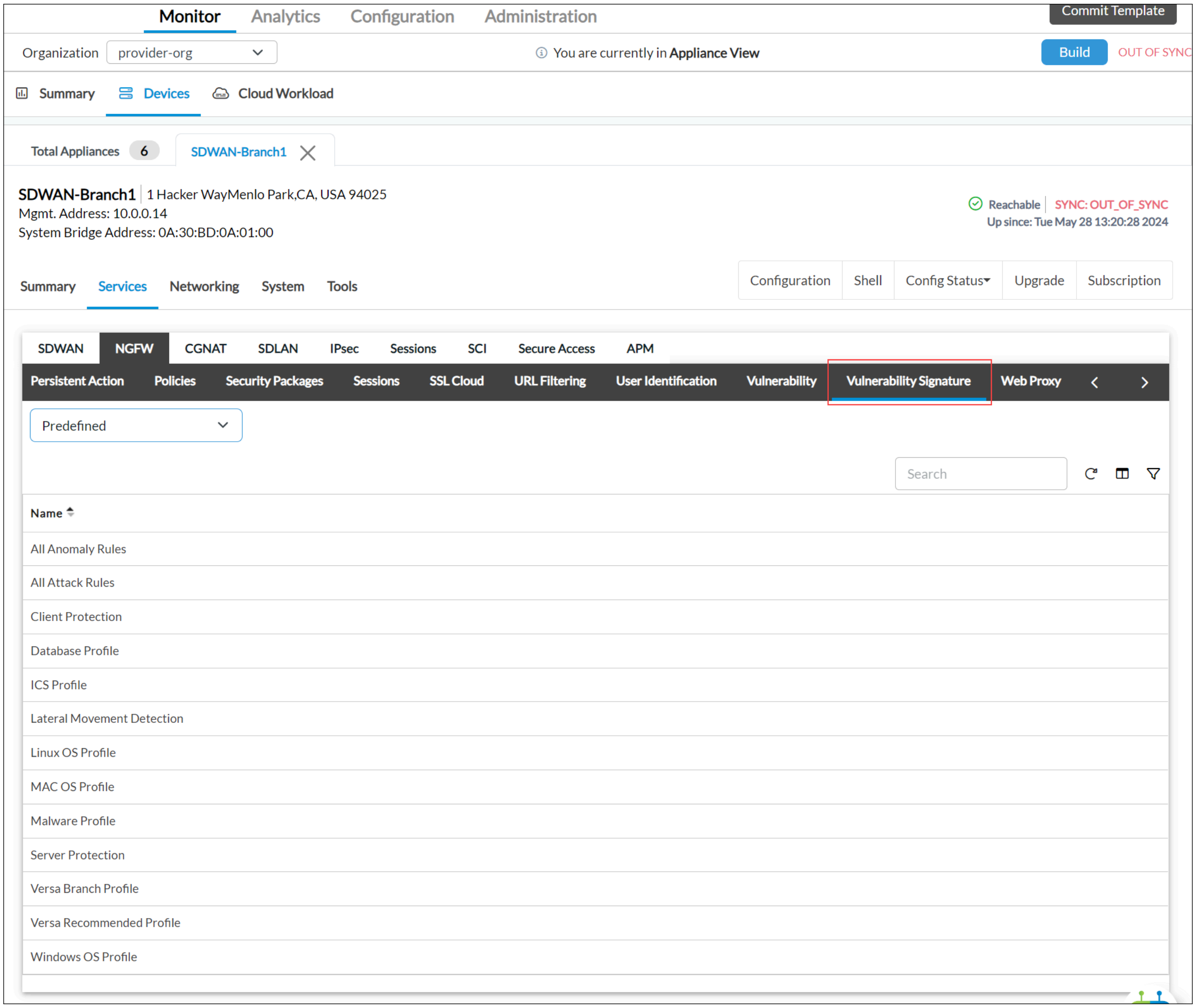
The following table explains the fields in the output:

Field	Description
Brief Status	Status of the compilation: ◦ Ready—IPS signature compilation is done. ◦ Compiling—IPS signature is being compiled. ◦ Abort-LowMem—If you enable the vulnerability profile in an access policy profile a traffic is dropped. You must disable the vulnerability profile in the access policy pr
Load IPS Signature	Number of loaded signatures.
Ignore IPS Signature	Number of ignored IPS signatures.
Fail IPS Signature	Number of failed IPS signatures.
Load App ID Signature	Number of loaded Application ID signatures.
Ignore App ID Signature	Number of ignored Application ID signatures.

Fail App ID Signature	Number of failed Appli ID signatures.
Compile Time	Time taken for the compilation. process

To check the compilation status:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select Services > NGFW > Vulnerability in the left menu bar.
4. Select the Vulnerability Signatures tab.
5. Select an option from the drop-down, and click view for the vulnerability profile you loaded.



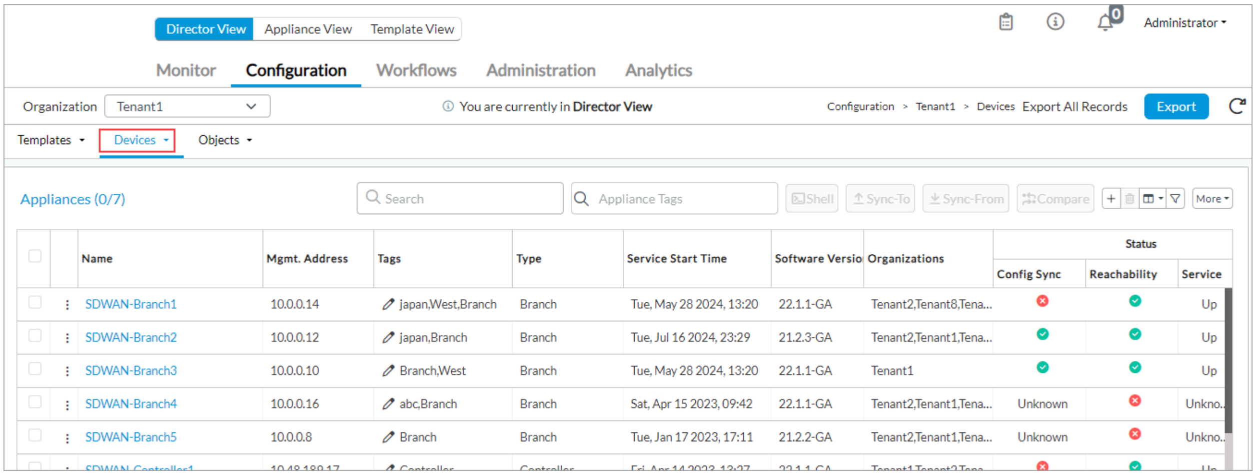
SDWAN-Branch1 | 1 Hacker WayMenlo Park,CA, USA 94025
Mgmt. Address: 10.0.0.14
System Bridge Address: 0A:30:BD:0A:01:00

Name
All Anomaly Rules
All Attack Rules
Client Protection
Database Profile
ICS Profile
Lateral Movement Detection
Linux OS Profile
MAC OS Profile
Malware Profile
Server Protection
Versa Branch Profile
Versa Recommended Profile
Windows OS Profile

Modify IPS System Parameters

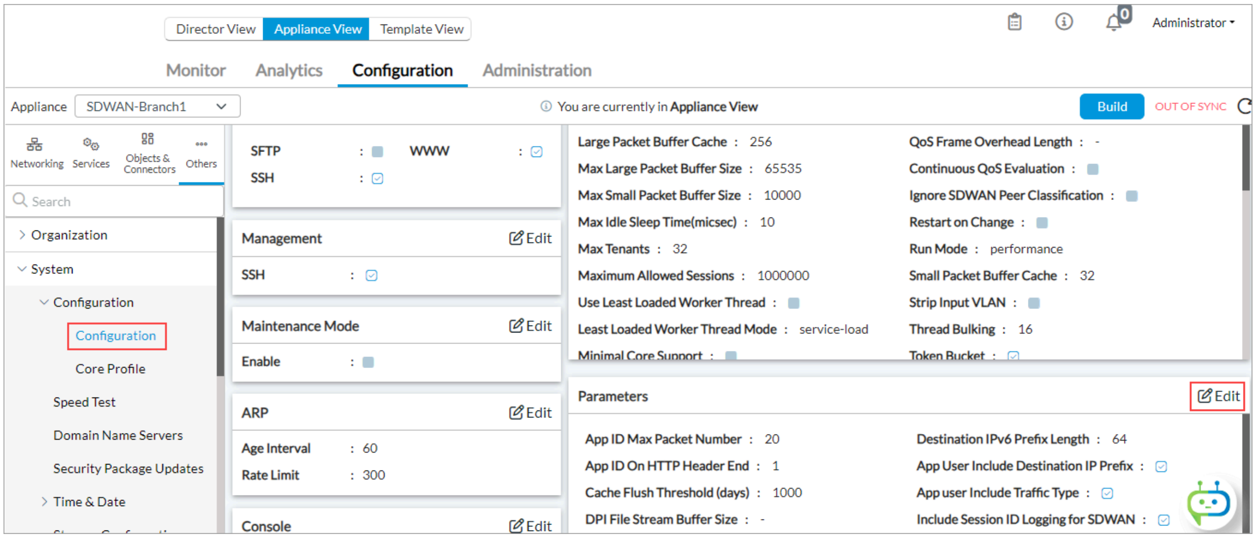
To change the IPS system parameters:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.
   c. Select a device from the main pane. The view changes to Appliance view.



Name	Mgmt. Address	Tags	Type	Service Start Time	Software Versio	Organizations	Status		
							Config Sync	Reachability	Service
SDWAN-Branch1	10.0.0.14	japan,West,Branch	Branch	Tue, May 28 2024, 13:20	22.1.1-GA	Tenant2,Tenant8,Tena...	✗	✓	Up
SDWAN-Branch2	10.0.0.12	japan,Branch	Branch	Tue, Jul 16 2024, 23:29	21.2.3-GA	Tenant2,Tenant1,Tena...	✓	✓	Up
SDWAN-Branch3	10.0.0.10	Branch,West	Branch	Tue, May 28 2024, 13:20	22.1.1-GA	Tenant1	✓	✓	Up
SDWAN-Branch4	10.0.0.16	abc,Branch	Branch	Sat, Apr 15 2023, 09:42	22.1.1-GA	Tenant2,Tenant1,Tena...	Unknown	✗	Unkno...
SDWAN-Branch5	10.0.0.8	Branch	Branch	Tue, Jan 17 2023, 17:11	21.2.2-GA	Tenant2,Tenant1,Tena...	Unknown	✗	Unkno...
SDWAN-Controller1	10.48.189.17	Controller	Controller	Fri, Apr 14 2023, 13:27	22.1.1-GA	Tenant1,Tenant2,Tena...	✗	✓	Up

2. Select Configuration in the top menu bar.
3. Select Others > System > Configuration > Configuration in the left menu bar.



SFTP : □ WWW : ☑
SSH : ☑

Management
SSH : ☑

Maintenance Mode
Enable : □

ARP
Age Interval : 60
Rate Limit : 300

Console

Large Packet Buffer Cache : 256
Max Large Packet Buffer Size : 65535
Max Small Packet Buffer Size : 10000
Max Idle Sleep Time(micsec) : 10
Max Tenants : 32
Maximum Allowed Sessions : 1000000
Use Least Loaded Worker Thread : □
Least Loaded Worker Thread Mode : service-load
Minimal Core Support : □

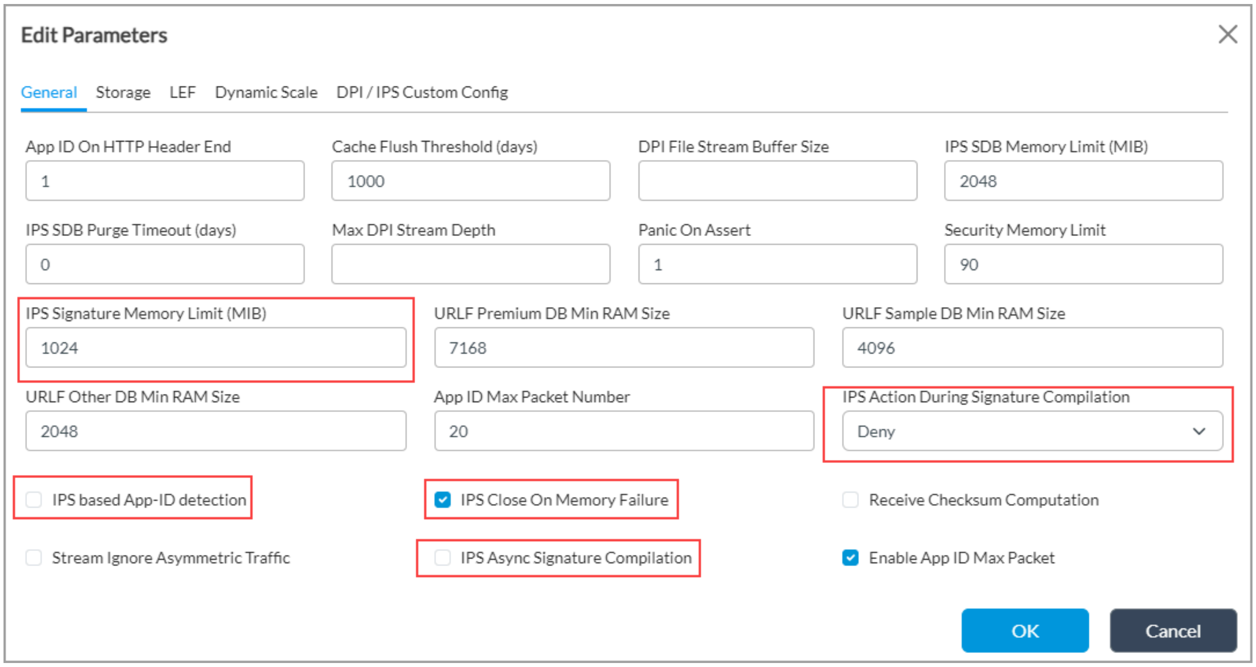
QoS Frame Overhead Length : -
Continuous QoS Evaluation : □
Ignore SDWAN Peer Classification : □
Restart on Change : □
Run Mode : performance
Small Packet Buffer Cache : 32
Strip Input VLAN : □
Thread Bulking : 16
Token Bucket : ☑

Parameters

App ID Max Packet Number : 20
App ID On HTTP Header End : 1
Cache Flush Threshold (days) : 1000
DPI File Stream Buffer Size : -

Destination IPv6 Prefix Length : 64
App User Include Destination IP Prefix : ☑
App user Include Traffic Type : ☑
Include Session ID Logging for SDWAN : ☑

4. In the Parameters pane, click the ✎ Edit icon to edit the IPS parameters. In the Edit Parameters popup window, select General tab and enter information for the following fields.



App ID On HTTP Header End: 1

Cache Flush Threshold (days): 1000

DPI File Stream Buffer Size:

IPS SDB Memory Limit (MIB): 2048

IPS SDB Purge Timeout (days): 0

Max DPI Stream Depth:

Panic On Assert: 1

Security Memory Limit: 90

IPS Signature Memory Limit (MIB): 1024

URLF Premium DB Min RAM Size: 7168

URLF Sample DB Min RAM Size: 4096

URLF Other DB Min RAM Size: 2048

App ID Max Packet Number: 20

IPS Action During Signature Compilation: Deny

□ IPS based App-ID detection

☑ IPS Close On Memory Failure

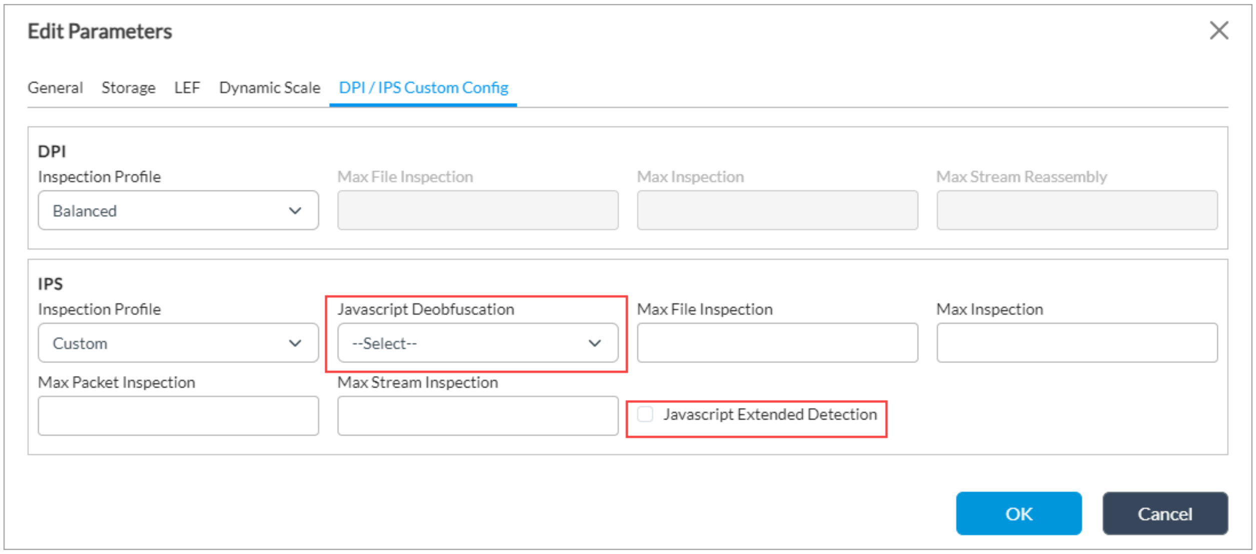
□ Receive Checksum Computation

□ Stream Ignore Asymmetric Traffic

□ IPS Async Signature Compilation

☑ Enable App ID Max Packet

5. Select DPI/IPS Custom Config tab and enter information for the following fields.



DPI

Inspection Profile: Balanced

Max File Inspection:

Max Inspection:

Max Stream Reassembly:

IPS

Inspection Profile: Custom

Javascript Deobfuscation: --Select--

Max File Inspection:

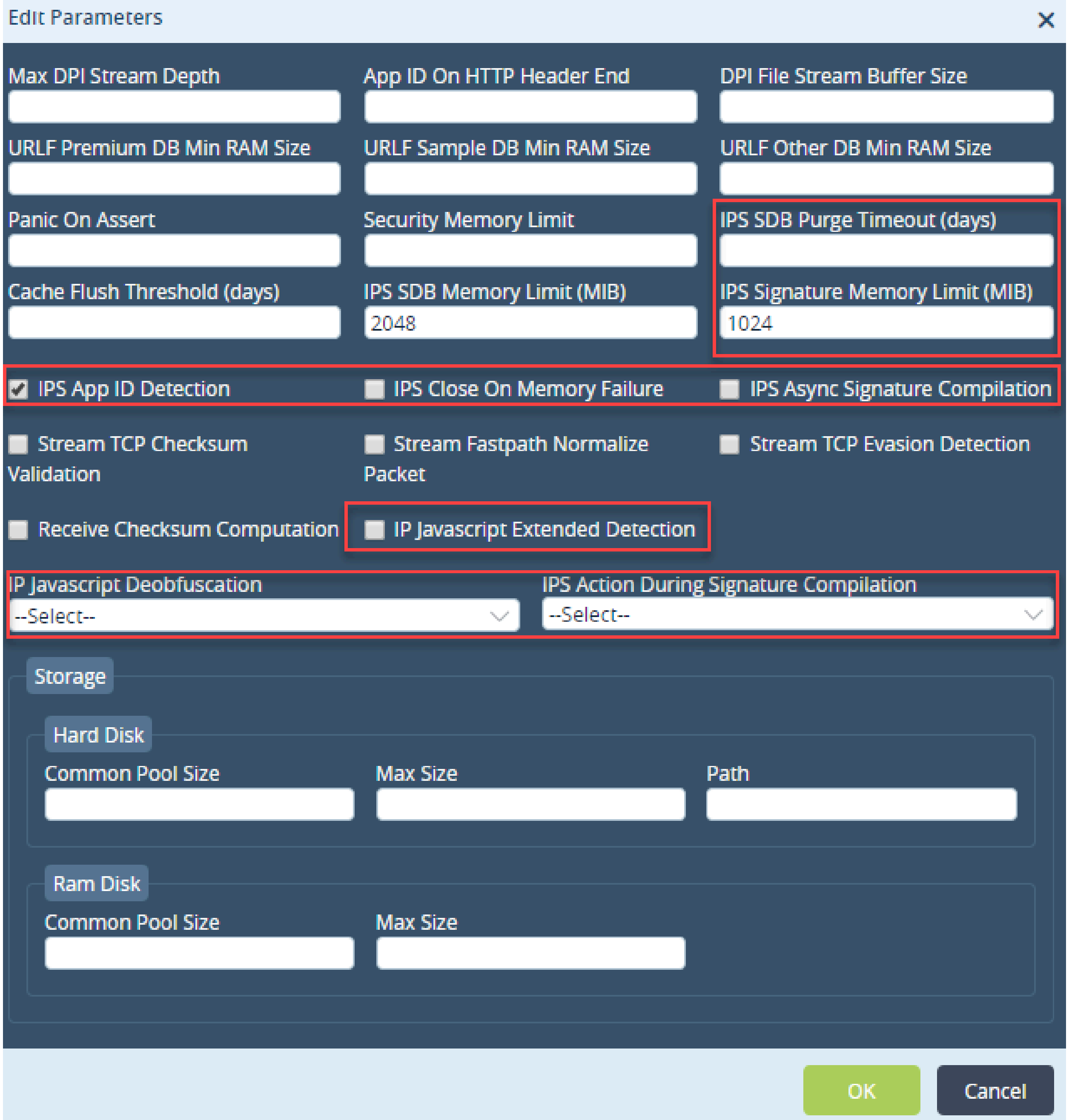
Max Inspection:

Max Packet Inspection:

Max Stream Inspection:

□ Javascript Extended Detection

For Releases 21.2 and earlier:



Edit Parameters

Max DPI Stream Depth

App ID On HTTP Header End

DPI File Stream Buffer Size

URLF Premium DB Min RAM Size

URLF Sample DB Min RAM Size

URLF Other DB Min RAM Size

Panic On Assert

Security Memory Limit

IPS SDB Purge Timeout (days)

Cache Flush Threshold (days)

IPS SDB Memory Limit (MIB): 2048

IPS Signature Memory Limit (MIB): 1024

☑ IPS App ID Detection

□ IPS Close On Memory Failure

□ IPS Async Signature Compilation

□ Stream TCP Checksum Validation

□ Stream Fastpath Normalize Packet

□ Stream TCP Evasion Detection

□ Receive Checksum Computation

□ IP Javascript Extended Detection

IP Javascript Deobfuscation: --Select--

IPS Action During Signature Compilation: --Select--

Storage

Hard Disk

Common Pool Size

Max Size

Path

Ram Disk

Common Pool Size

Max Size

Field Name	Description
IPS SDB Purge Timeout	Enter how long to save the compilation details in the IPS signature database when y This file is deleted after the specified number of days, and a new file is generated the *Range:* 0 through 65535 days

IPS SDB Memory Limit	Enter the memory limit of the signature database. If system RAM is below this value, file.
IPS Signature Memory Limit	Enter the memory limit of the IPS signature database. If the memory of the IPS datal fail to load. *Default:* 1024 MB
IPS App ID Detection	Click to have both the IPS engine and the application engine perform application ide *Default:* Enabled
IPS Close On Memory Failure	Click to drop a session if memory is not available. *Default:* Disabled
IPS Async Signature Compilation	(For Releases 22.1.3 and later.) Click to have the IPS signature compilation occur in compilation then takes place in a separate thread without blocking the other ongoing IPS signature is being compiled, traffic is processed using the previous version of IP
IPS Javascript Extended Detection	Click to perform extended Javascript detection after deobfuscation completes.
IPS Javascript Deobfuscation	Select an option to convert a Javascript or an HTML program to a simple, understan
IPS Action During Signature Compilation	Select the action to take when a signature compilation is in progress. You can either

6. Click OK.

Note: You can set other IPS parameters from the CLI.

View Vulnerability Information

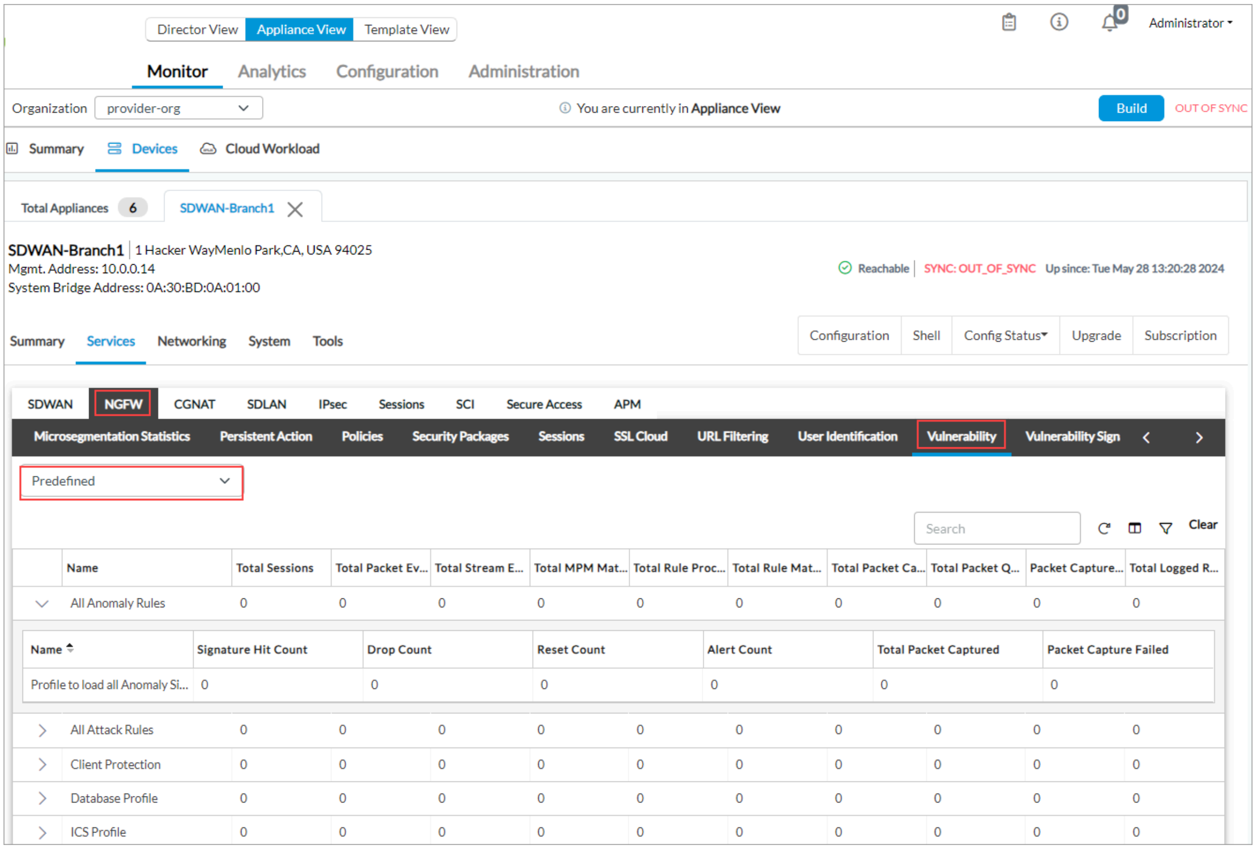
To view information about a VOS device's vulnerability, you can do the following:

- View vulnerability profile statistics and logs
- View vulnerability threats and logs
- View packet capture logs

Display Vulnerability Profile Statistics and Logs

To view profile statistics for predefined profiles:

1. In Appliance view, select the Monitor tab in the top menu bar.
2. Select Services > NGFW > Vulnerability.
3. In the drop-down menu, select Predefined.



Organization provider-org

You are currently in Appliance View

SDWAN-Branch1 | 1 Hacker WayMenlo Park,CA, USA 94025
Mgmt. Address: 10.0.0.14
System Bridge Address: 0A:30:BD:0A:01:00

Up since: Tue May 28 13:20:28 2024

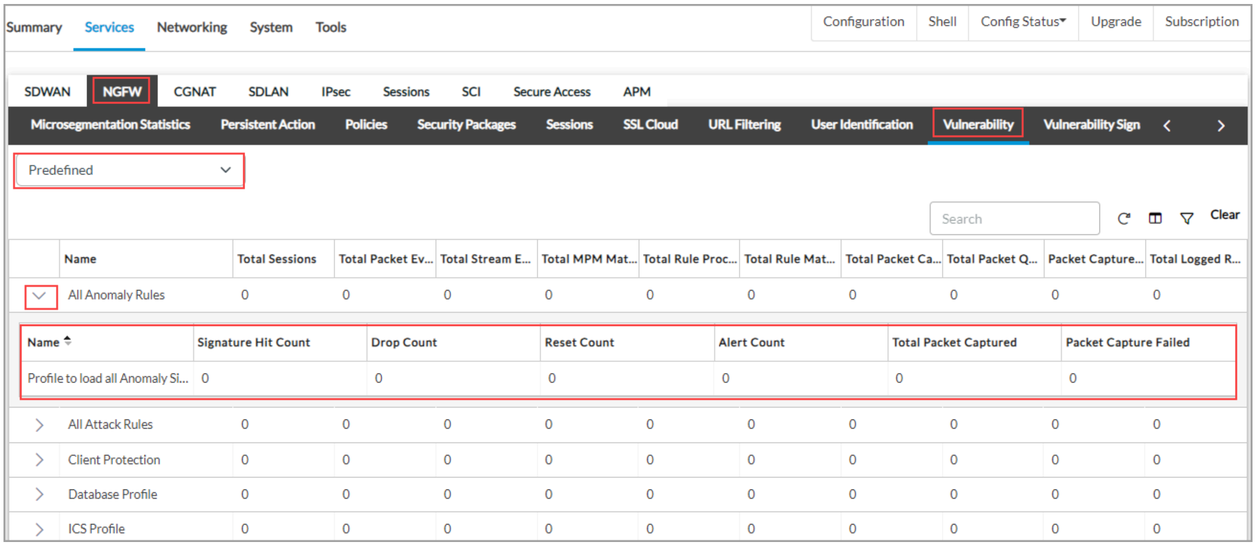
Predefined

Name	Total Sessions	Total Packet Ev...	Total Stream E...	Total MPM Mat...	Total Rule Proc...	Total Rule Mat...	Total Packet Ca...	Total Packet Q...	Packet Capture...	Total Logged R...
All Anomaly Rules	0	0	0	0	0	0	0	0	0	0

Name	Signature Hit Count	Drop Count	Reset Count	Alert Count	Total Packet Captured	Packet Capture Failed
Profile to load all Anomaly Si...	0	0	0	0	0	0

Name	Total Sessions	Total Packet Ev...	Total Stream E...	Total MPM Mat...	Total Rule Proc...	Total Rule Mat...	Total Packet Ca...	Total Packet Q...	Packet Capture...	Total Logged R...
All Attack Rules	0	0	0	0	0	0	0	0	0	0
Client Protection	0	0	0	0	0	0	0	0	0	0
Database Profile	0	0	0	0	0	0	0	0	0	0
ICS Profile	0	0	0	0	0	0	0	0	0	0

4. Click the > right arrow next to the name of the predefined profile.



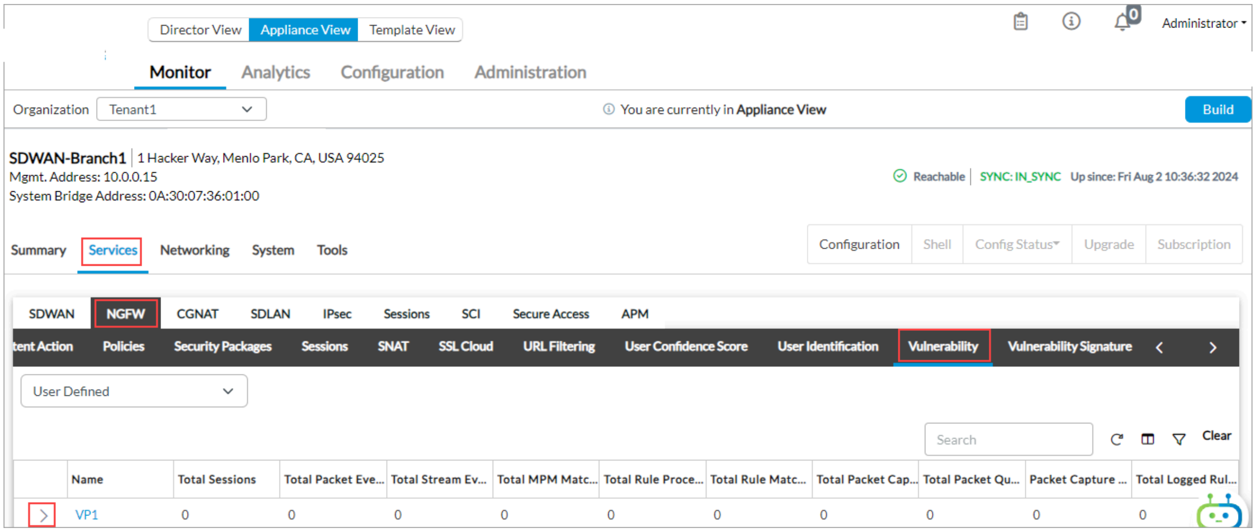
Name	Total Sessions	Total Packet Ev...	Total Stream E...	Total MPM Mat...	Total Rule Proc...	Total Rule Mat...	Total Packet Ca...	Total Packet Q...	Packet Capture...	Total Logged R...
All Anomaly Rules	0	0	0	0	0	0	0	0	0	0

Name	Signature Hit Count	Drop Count	Reset Count	Alert Count	Total Packet Captured	Packet Capture Failed
Profile to load all Anomaly Si...	0	0	0	0	0	0

Name	Total Sessions	Total Packet Ev...	Total Stream E...	Total MPM Mat...	Total Rule Proc...	Total Rule Mat...	Total Packet Ca...	Total Packet Q...	Packet Capture...	Total Logged R...
All Attack Rules	0	0	0	0	0	0	0	0	0	0
Client Protection	0	0	0	0	0	0	0	0	0	0
Database Profile	0	0	0	0	0	0	0	0	0	0
ICS Profile	0	0	0	0	0	0	0	0	0	0

To view profile statistics for custom profiles:

1. In Appliance view, select the Monitor tab in the top menu bar.
2. Select Services > NGFW > Vulnerability.



Organization Tenant1

You are currently in Appliance View

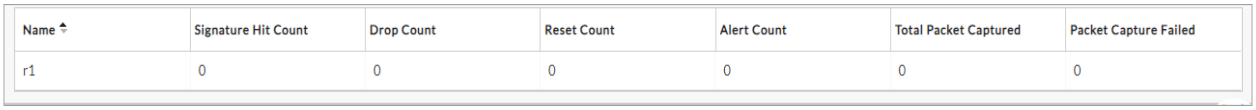
SDWAN-Branch1 | 1 Hacker Way, Menlo Park, CA, USA 94025
Mgmt. Address: 10.0.0.15
System Bridge Address: 0A:30:07:36:01:00

Reachable | SYNC: IN_SYNC Up since: Fri Aug 2 10:36:32 2024

Name	Total Sessions	Total Packet Eve...	Total Stream Ev...	Total MPM Matc...	Total Rule Proce...	Total Rule Matc...	Total Packet Cap...	Total Packet Qu...	Packet Capture ...	Total Logged Rul...
VP1	0	0	0	0	0	0	0	0	0	0

3. In the drop-down menu, select User Defined .

4. Click the > right arrow next to the name of the custom profile. The extended window displays the statistics.



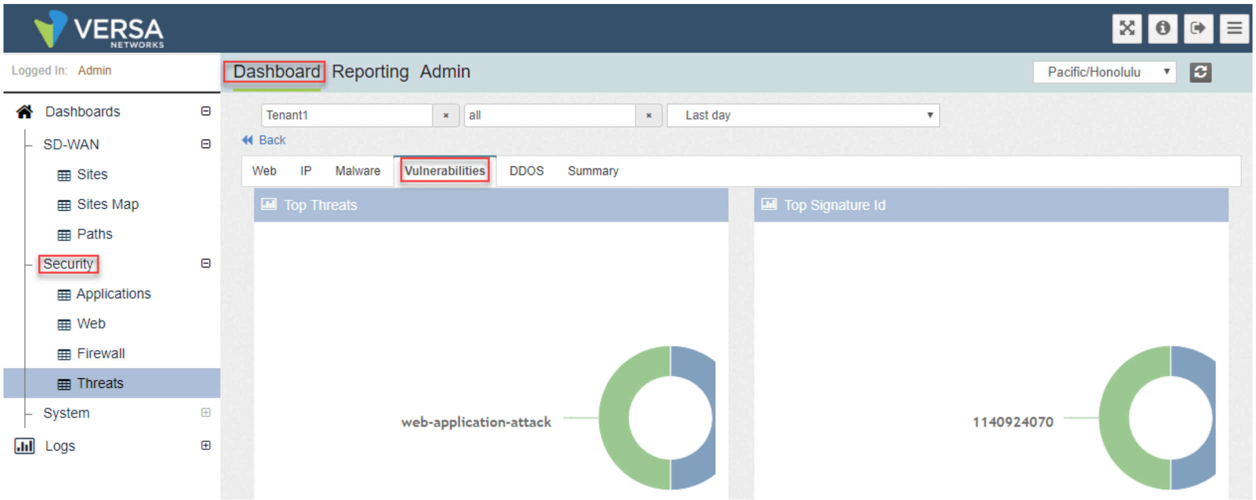
Name	Signature Hit Count	Drop Count	Reset Count	Alert Count	Total Packet Captured	Packet Capture Failed
r1	0	0	0	0	0	0

View Vulnerability Threats and Logs

When an attack is detected, the IPS engine blocks the traffic, and the Director node logs the details on the Analytics node.

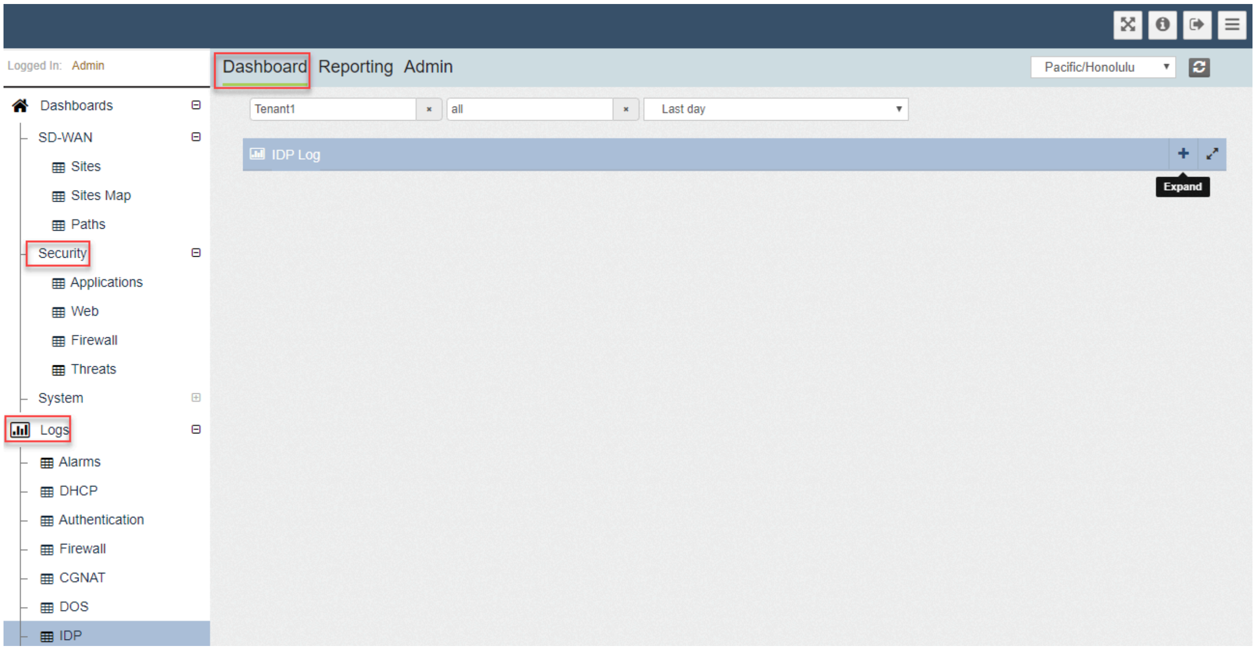
To view the vulnerability threats:

1. Log in to the Analytics node that is integrated with the Director node.
2. Select Dashboard in the top menu bar.
3. Select Security > Threats in the left navigation bar. The following window displays, showing the security panes with top data.

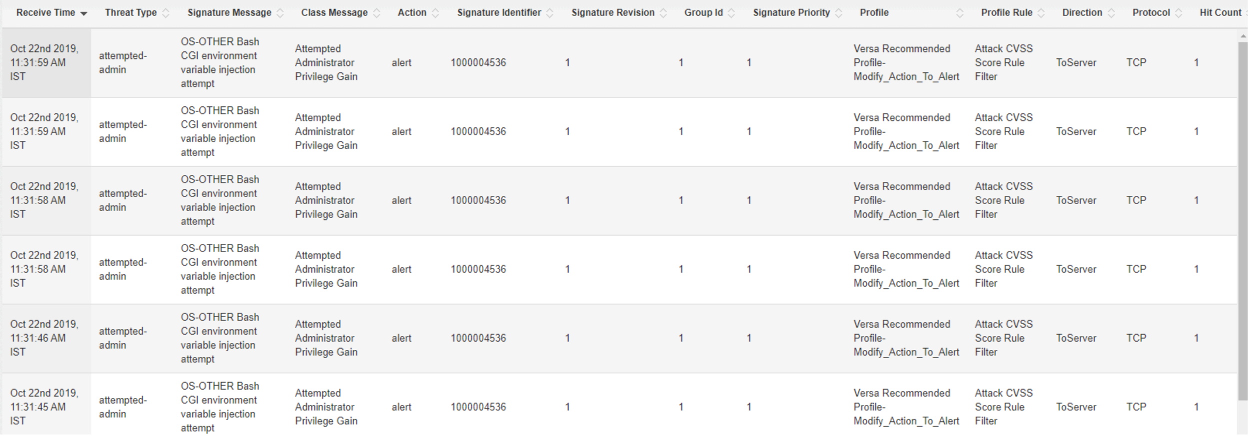


To view the vulnerability logs:

1. Log in to the Analytics node that is integrated with the Director node.
2. Select Dashboard in the top menu bar.



3. Select Logs> IDP in the left navigation bar. The following window displays, listing the detailed logs.

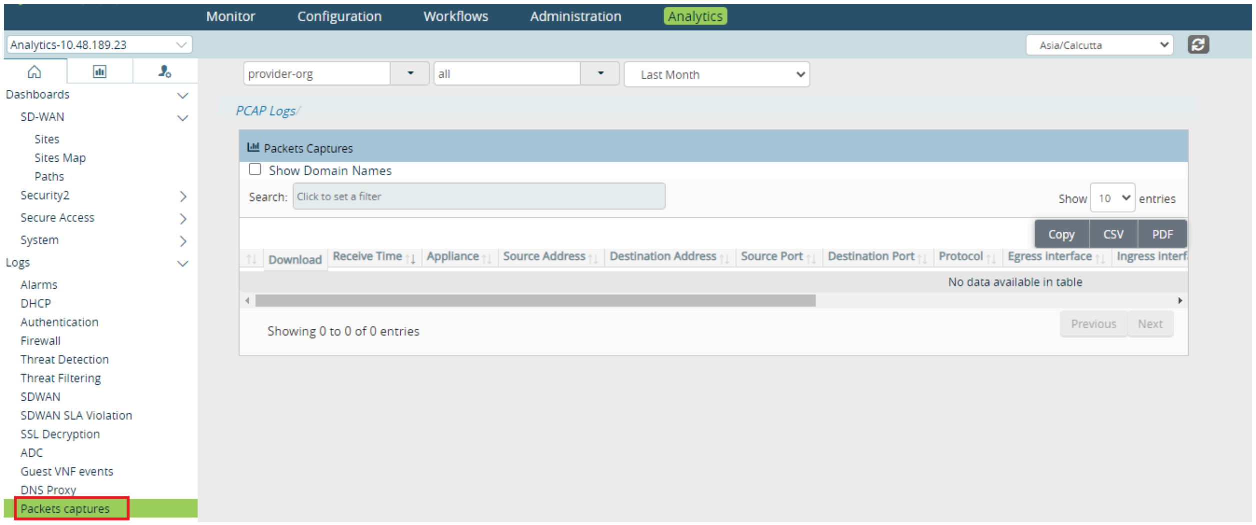


Receive Time	Threat Type	Signature Message	Class Message	Action	Signature Identifier	Signature Revision	Group Id	Signature Priority	Profile	Profile Rule	Direction	Protocol	Hit Count
Oct 22nd 2019, 11:31:59 AM IST	attempted-admin	OS-OTHER Bash CGI environment variable injection attempt	Attempted Administrator Privilege Gain	alert	1000004536	1	1	1	Versa Recommended Profile-Modify_Action_To_Alert	Attack CVSS Score Rule Filter	ToServer	TCP	1
Oct 22nd 2019, 11:31:59 AM IST	attempted-admin	OS-OTHER Bash CGI environment variable injection attempt	Attempted Administrator Privilege Gain	alert	1000004536	1	1	1	Versa Recommended Profile-Modify_Action_To_Alert	Attack CVSS Score Rule Filter	ToServer	TCP	1
Oct 22nd 2019, 11:31:58 AM IST	attempted-admin	OS-OTHER Bash CGI environment variable injection attempt	Attempted Administrator Privilege Gain	alert	1000004536	1	1	1	Versa Recommended Profile-Modify_Action_To_Alert	Attack CVSS Score Rule Filter	ToServer	TCP	1
Oct 22nd 2019, 11:31:58 AM IST	attempted-admin	OS-OTHER Bash CGI environment variable injection attempt	Attempted Administrator Privilege Gain	alert	1000004536	1	1	1	Versa Recommended Profile-Modify_Action_To_Alert	Attack CVSS Score Rule Filter	ToServer	TCP	1
Oct 22nd 2019, 11:31:46 AM IST	attempted-admin	OS-OTHER Bash CGI environment variable injection attempt	Attempted Administrator Privilege Gain	alert	1000004536	1	1	1	Versa Recommended Profile-Modify_Action_To_Alert	Attack CVSS Score Rule Filter	ToServer	TCP	1
Oct 22nd 2019, 11:31:45 AM IST	attempted-admin	OS-OTHER Bash CGI environment variable injection attempt	Attempted Administrator Privilege Gain	alert	1000004536	1	1	1	Versa Recommended Profile-Modify_Action_To_Alert	Attack CVSS Score Rule Filter	ToServer	TCP	1

View Packet Capture Logs

To view the packet capture logs:

1. Log in to the Analytics node that is integrated with the Director node.
2. Select Dashboards in the left menu bar.
3. Select Logs > Packet Captures in the left menu bar. The following window displays, showing details of the packets captured.



☐ Show Domain Names

Search: Click to set a filter

Show 10 entries

Download	Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Protocol	Egress interface	Ingress interf
No data available in table									

Showing 0 to 0 of 0 entries

Troubleshoot IDS/IPS

Run these CLI commands to troubleshoot vulnerability-based security issues:

- **show orgs org** *tenant-name* **sessions ips brief**
- **show orgs org** *tenant-name* **sessions ips detail**
- **show orgs org-services** *tenant-name* **security ips statistics**
- **show orgs org-services** *tenant-name* **security profiles ips signature predefined-profile**
- **show orgs org-services** *tenant-name* **security profiles ips signature user-defined-profile**
- **show orgs org-services** *tenant-name* **security profiles ips statistics signature predefined-profile**
- **show orgs org-services** *tenant-name* **security profiles ips statistics signature user-defined-profile**
- **show orgs org-services** *tenant-name* **security profiles ips statistics predefined**
- **show orgs org-services** *tenant-name* **security profiles ips statistics user-defined**

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 22.1.3 makes changes to the IPS Async Signature Compilation option.

Additional Information

Apply Log Export Functionality
Configure Antivirus
Configure Log Export Functionality

Configure NGFW
Configure Security Profile Groups
Versa Analytics Scaling Recommendations