Configure SD-WAN IPS-Filtering Policies

For supported software information, click here.

The intrusion prevention system (IPS) mitigates security vulnerabilities by responding to inappropriate or anomalous activity. Responses can include dropping data packets and disconnecting connections that are transmitting unauthorized data.

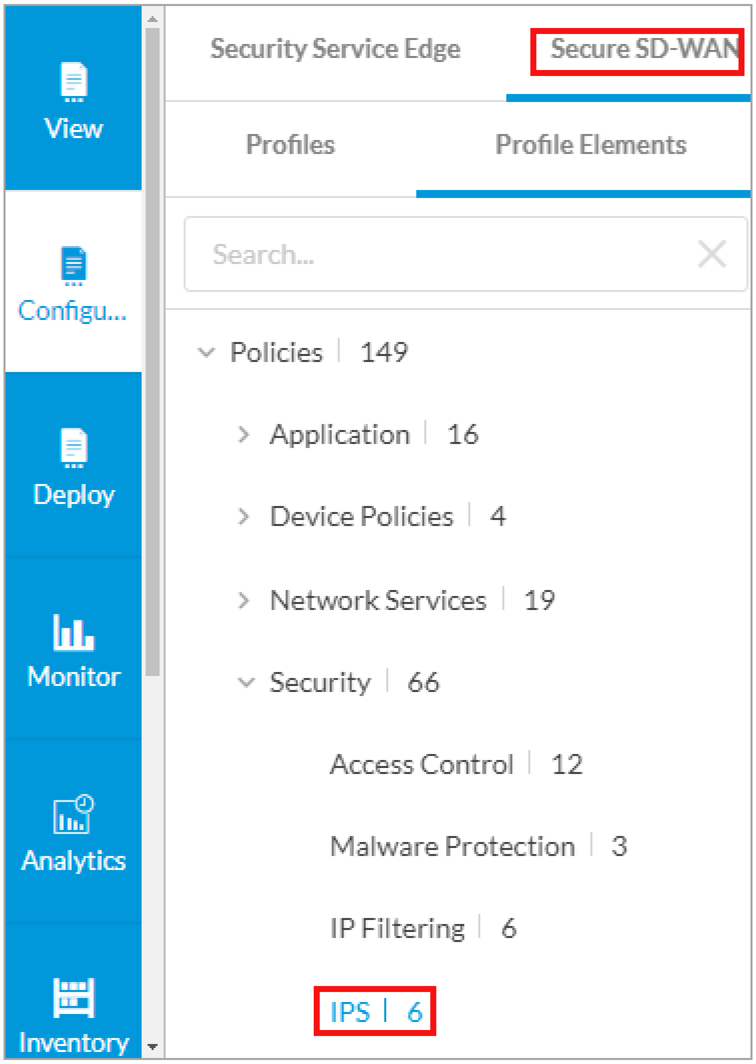
You commonly place an IPS system at the perimeter of a corporate network. IPS performs the following types of vulnerability detection to help prevent attacks, including zero-day attacks such as worms or viruses:

- 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

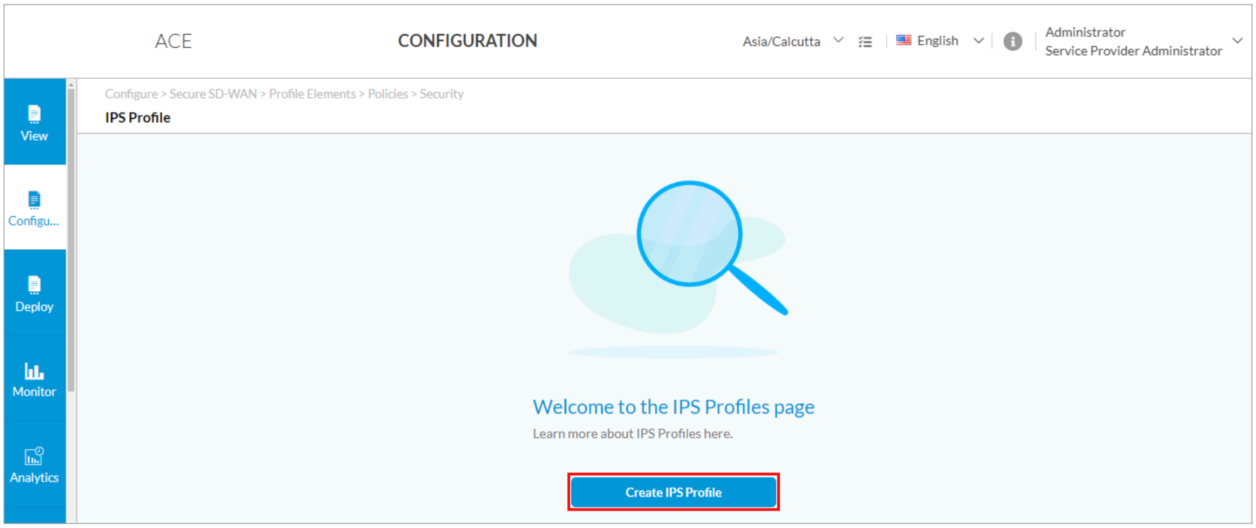
By default, Versa SASE provides a predefined IPS enforcement policy. This article describes how you can configure custom IPS-filtering policies.

To configure an IPS-filtering profile:

1. Go to Configure > Secure SD-WAN > Profile Elements > Policies > Security > IPS.



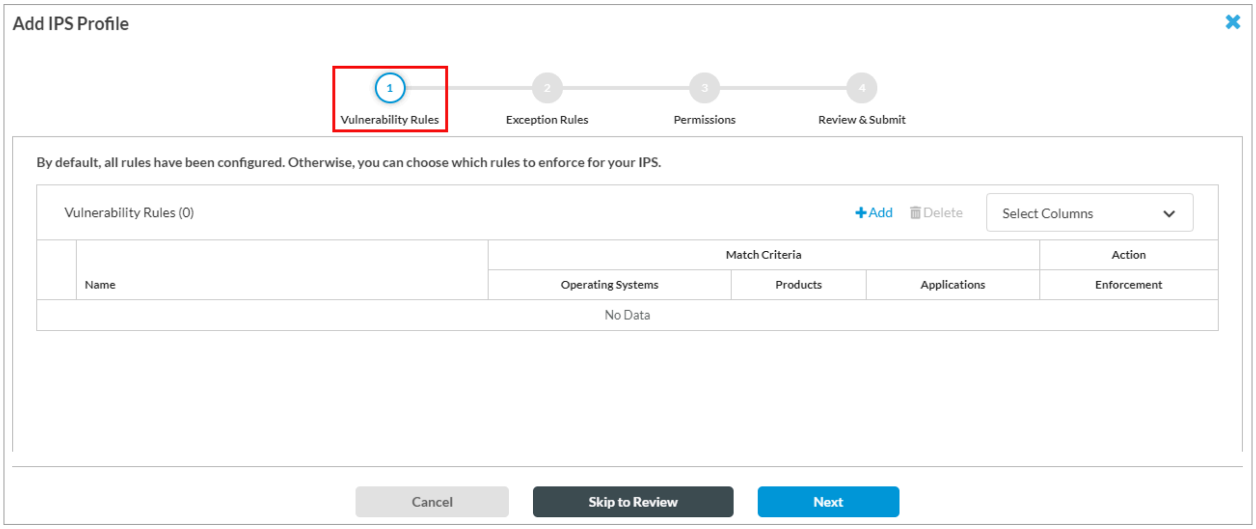
If there is no existing IPS policy, the following screen displays.


ACE
CONFIGURATION
Asia/Calcutta
English
Administrator
Service Provider Administrator
View
Configu...
Deploy
Monitor
Analytics
Configure > Secure SD-WAN > Profile Elements > Policies > Security
IPS Profile

Welcome to the IPS Profiles page

Learn more about IPS Profiles here.

2. Click Create IPS Policy or + Add to add a new IPS-filtering policy. The Add IPS Policy screen displays, and Step 1, Vulnerability Rules, is selected.



Add IPS Profile

1 Vulnerability Rules — 2 Exception Rules — 3 Permissions — 4 Review & Submit

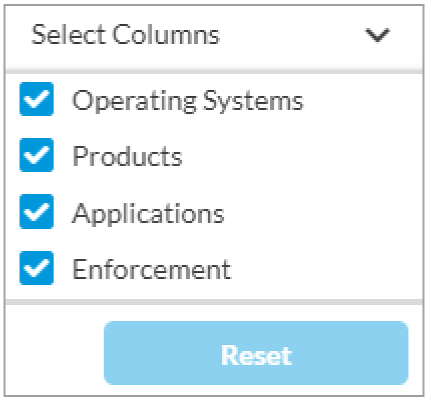
By default, all rules have been configured. Otherwise, you can choose which rules to enforce for your IPS.

Vulnerability Rules (0)   + Add   Delete   Select Columns

		Match Criteria			Action
	Name	Operating Systems	Products	Applications	Enforcement
	No Data				

Cancel   Skip to Review   Next

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



Select Columns

☑ Operating Systems

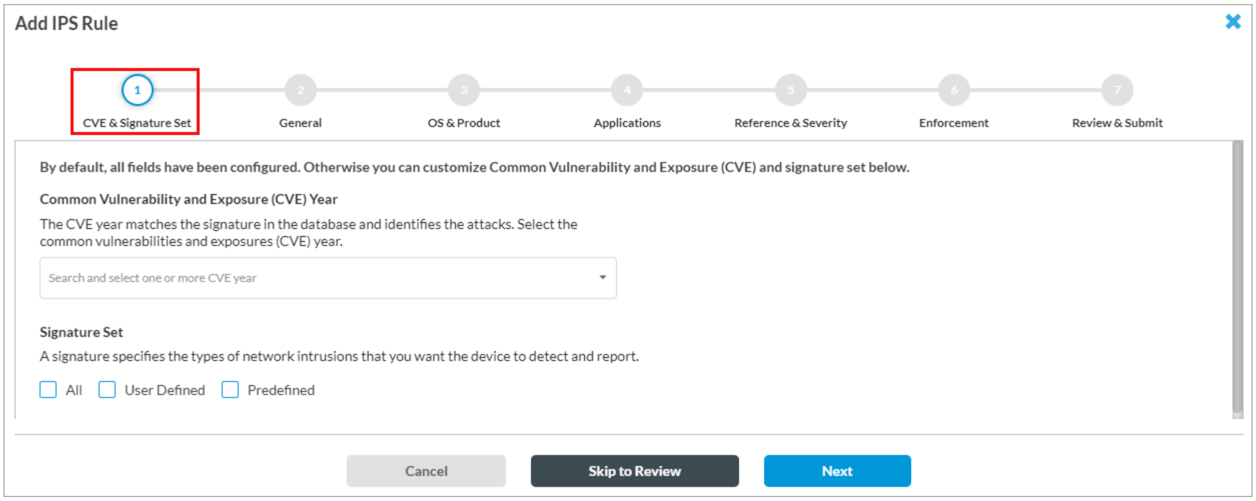
☑ Products

☑ Applications

☑ Enforcement

Reset

4. Click + Add to add a vulnerability rule. The Add Vulnerability Rule screen displays. In the Step 1, CVE and Signature Set screen, enter information for the following fields.



Add IPS Rule

By default, all fields have been configured. Otherwise you can customize Common Vulnerability and Exposure (CVE) and signature set below.

Common Vulnerability and Exposure (CVE) Year

The CVE year matches the signature in the database and identifies the attacks. Select the common vulnerabilities and exposures (CVE) year.

Search and select one or more CVE year

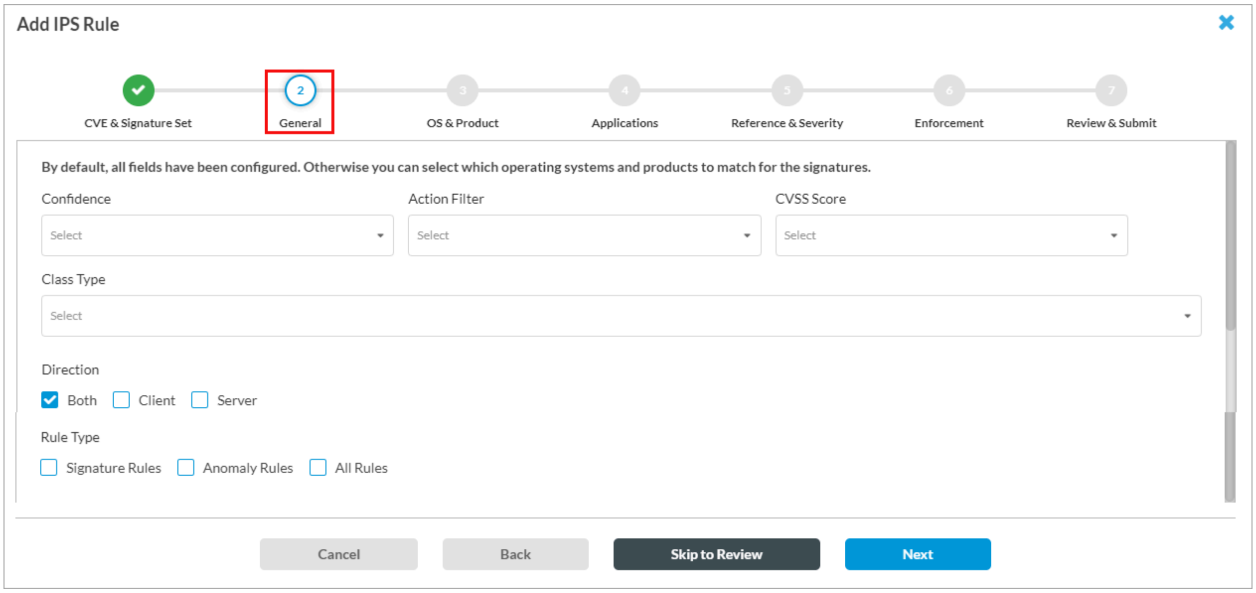
Signature Set

A signature specifies the types of network intrusions that you want the device to detect and report.

□ All □ User Defined □ Predefined

Field	Description
Common Vulnerabilities and Exposures (CVE) Year	Select one or more CVE years. The CVE year matches the signature in the database and identifies the attacks.
Signature Set	Select the signature set to use for the rule: ◦ All ◦ Predefined ◦ User Defined

5. Click Next. In the Step 2, General screen, enter information for the following fields.



By default, all fields have been configured. Otherwise you can select which operating systems and products to match for the signatures.

Confidence: Select

Action Filter: Select

CVSS Score: Select

Class Type: Select

Direction

☑ Both □ Client □ Server

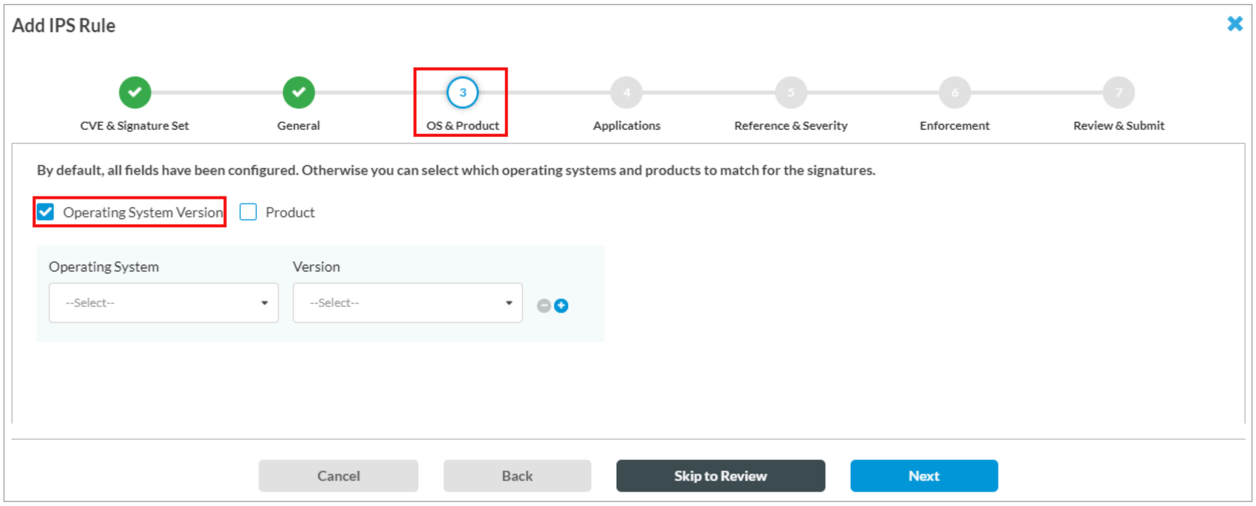
Rule Type

□ Signature Rules □ Anomaly Rules □ All Rules

Field	Description
Confidence	Select one or more confidence levels to use to match the signatures. *Range*: 0 through 9, Unselected *Default*: None
Action Filter	Select one or more action filters to use to match the signatures: ◦ Alert ◦ Drop Packet ◦ Drop Session ◦ Reject
CVSS Score	Select one or more common vulnerability scoring system scores to use to match the signatures. *Range*: 1 through 10
Class Type	Select one or more class types of vulnerabilities to use to match the signatures.
Direction	Click to select the traffic direction for applying the rule

Field	Description
	to signatures: ◦ Both ◦ Client ◦ Server
Rule Type	Click to select the rule type to use to match the signatures: ◦ All Rules ◦ Anomaly Rules ◦ Signature Rules

6. Click Next. In the Step 3, OS and Product screen, click Operating System Version, and then select an operating system and operating system version to match for signatures. Click the ⊕ Plus icon to add an operating system. Click the ⊖ Minus icon to remove an operating system.

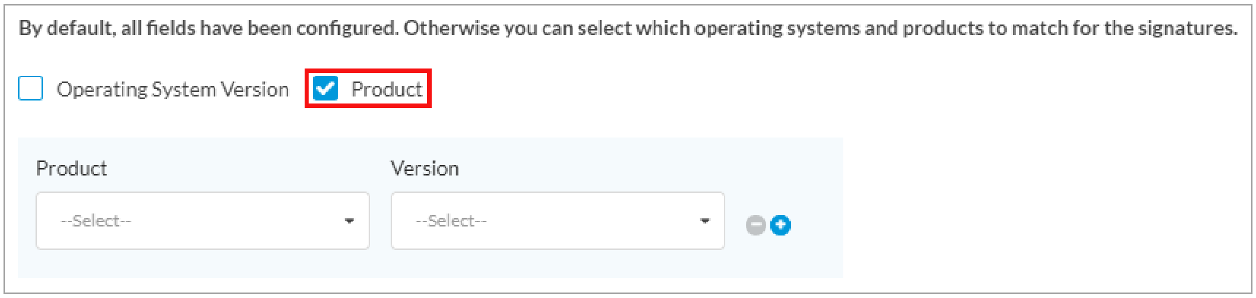


By default, all fields have been configured. Otherwise you can select which operating systems and products to match for the signatures.

☑ Operating System Version ☐ Product

Operating System: --Select--
Version: --Select-- ⊖ ⊕

7. Click Product, and then select a product and a product version to match for signatures. Click the ⊕ Plus icon to add an operating system. Click the ⊖ Minus icon to remove an operating system.



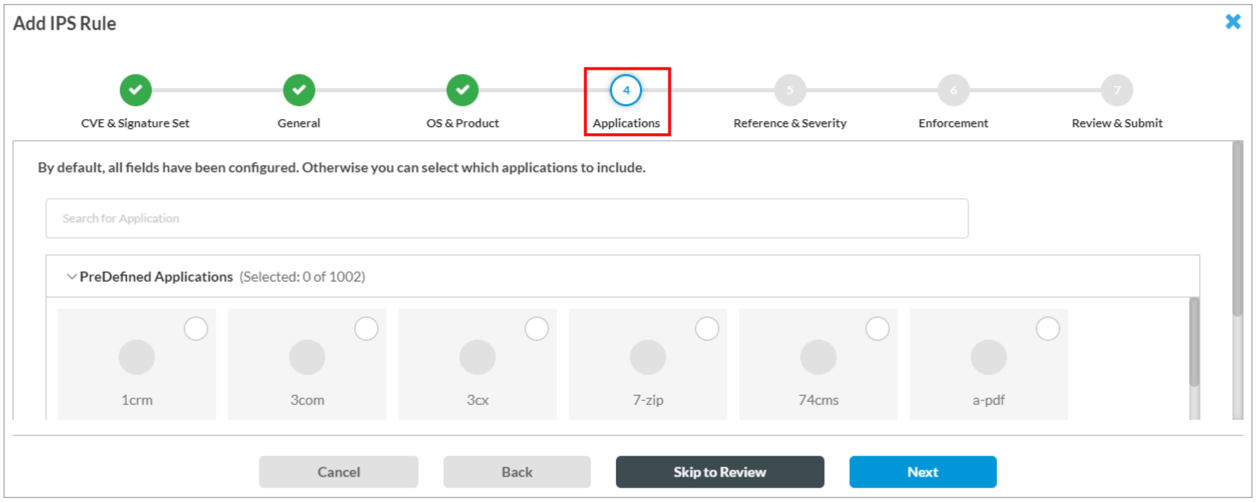
By default, all fields have been configured. Otherwise you can select which operating systems and products to match for the signatures.

□ Operating System Version ☑ Product

Product: --Select--

Version: --Select--

8. Click Next. The Step 4, Application screen displays all predefined applications. Click an application to add it to the list of applications to match. Use the search box to find specific applications. You can include or exclude the selected applications by clicking its checkbox.



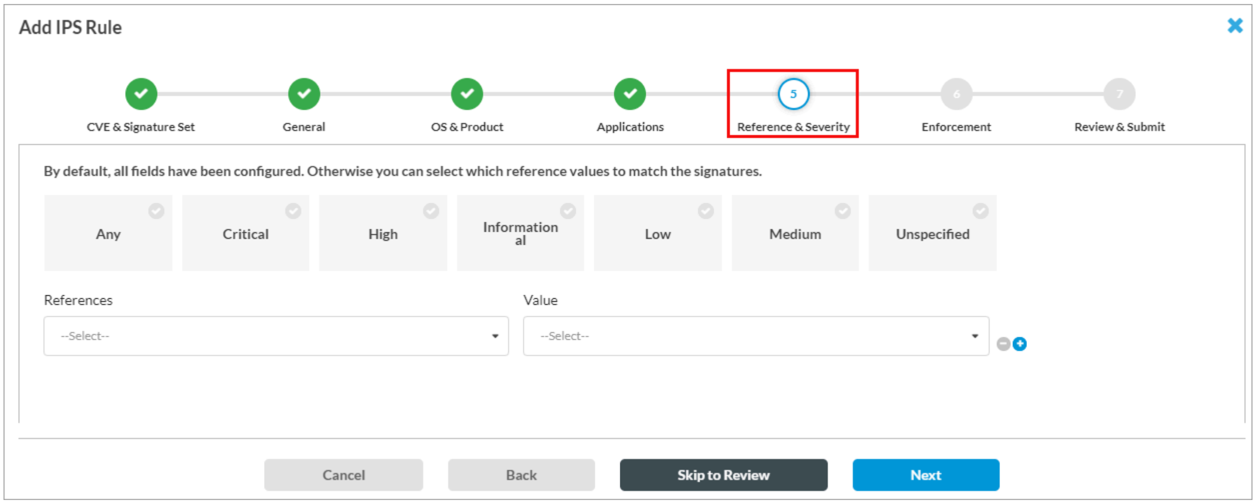
Add IPS Rule

By default, all fields have been configured. Otherwise you can select which applications to include.

Search for Application

PreDefined Applications (Selected: 0 of 1002)

9. Click Next, and in the Step 5, Reference and Severity screen, enter information for the following fields.



Add IPS Rule

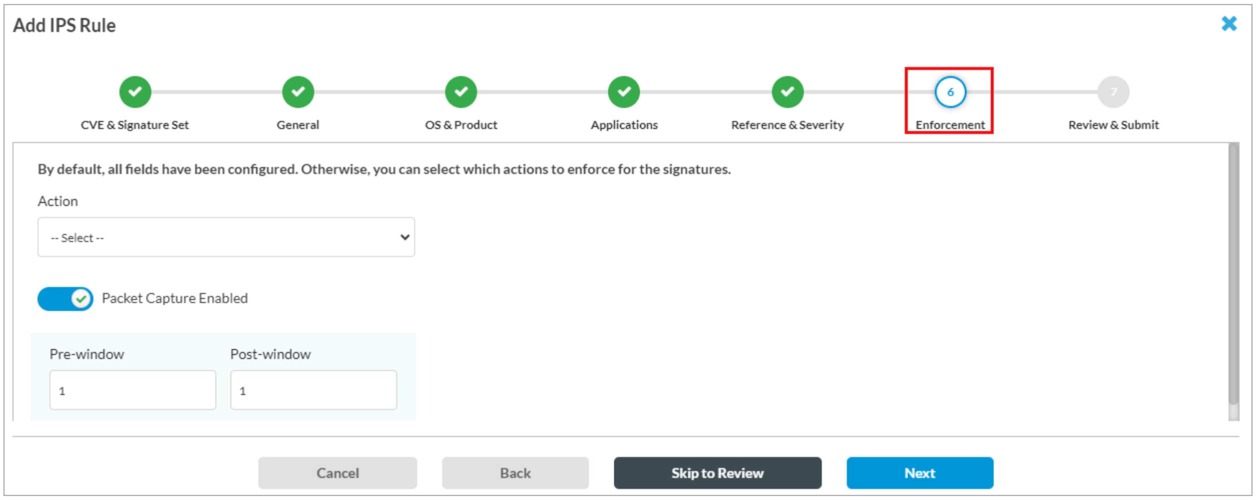
By default, all fields have been configured. Otherwise you can select which reference values to match the signatures.

References: --Select--

Value: --Select--

Field	Description
Severity	Select one or more severity-level match criteria: ◦ Any ◦ Critical ◦ High ◦ Informational ◦ Low ◦ Medium ◦ Unspecified
References	Select and use signatures that match a specific reference type. Click the ⊕ Add icon to add the reference type to the rule.
Value	Select and use signatures that match a specific reference value. Click the ⊕ Add icon to add the reference value to the rule.

10. Click Next. In the Step 6, Enforcement screen, enter information for the following fields.



By default, all fields have been configured. Otherwise, you can select which actions to enforce for the signatures.

Action: -- Select --

Packet Capture Enabled

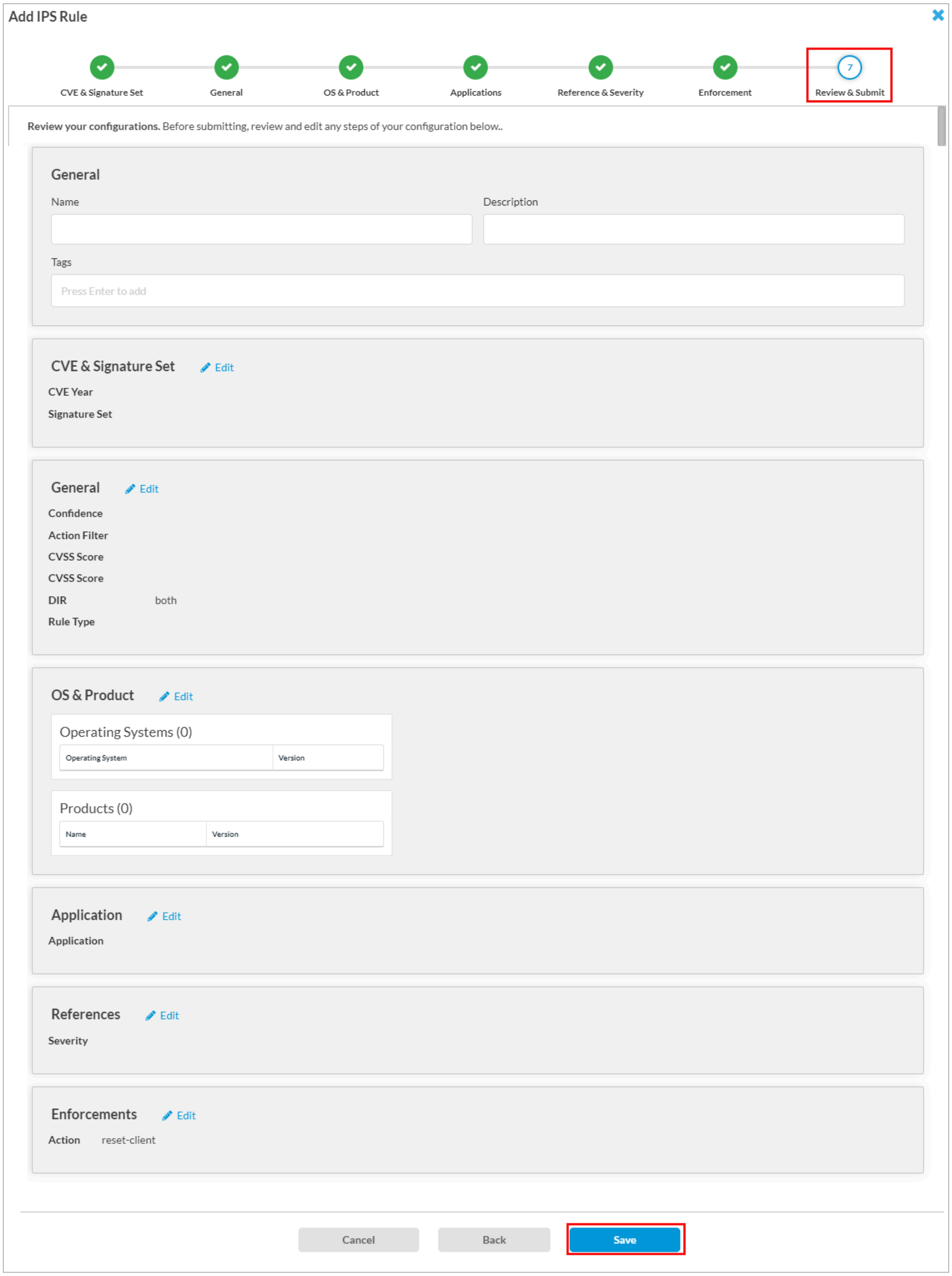
Pre-window: 1

Post-window: 1

Field	Description
Action	Select an enforcement action to apply to the signatures: ◦ Default ◦ Predefined ▪ Allow ▪ Alert ▪ Deny ▪ Drop Packet ▪ Drop Session ▪ Reset Client ▪ Reset Server ▪ Reject ◦ 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
Enable Packet Capture (Group of Fields)	Click to enable packet capture. When enabled, packet capture logs are sent to Versa Analytics.
◦ Pre-window	Enter the number of packets immediately preceding the attacked packet that you want to capture. *Range*: 0 through 10 *Default*: 1
◦ Post-window	Enter the number of packets immediately following the attacked packet that you want to capture. *Range*: 0 through 10

	Default: 1

11. Click Next, and in the Step 7, Review and Submit screen, enter a name for the IPS profile. Optionally, enter a description and one or more tags. A tag is an alphanumeric descriptor, with no white spaces or special characters, that you can use to search the objects.



Add IPS Rule

Review your configurations. Before submitting, review and edit any steps of your configuration below..

General

Name

Description

Tags

Press Enter to add

CVE & Signature Set

CVE Year

Signature Set

General

Confidence

Action Filter

CVSS Score

CVSS Score

DIR both

Rule Type

OS & Product

Operating Systems (0)

Operating System	Version

Products (0)

Name	Version

Application

Application

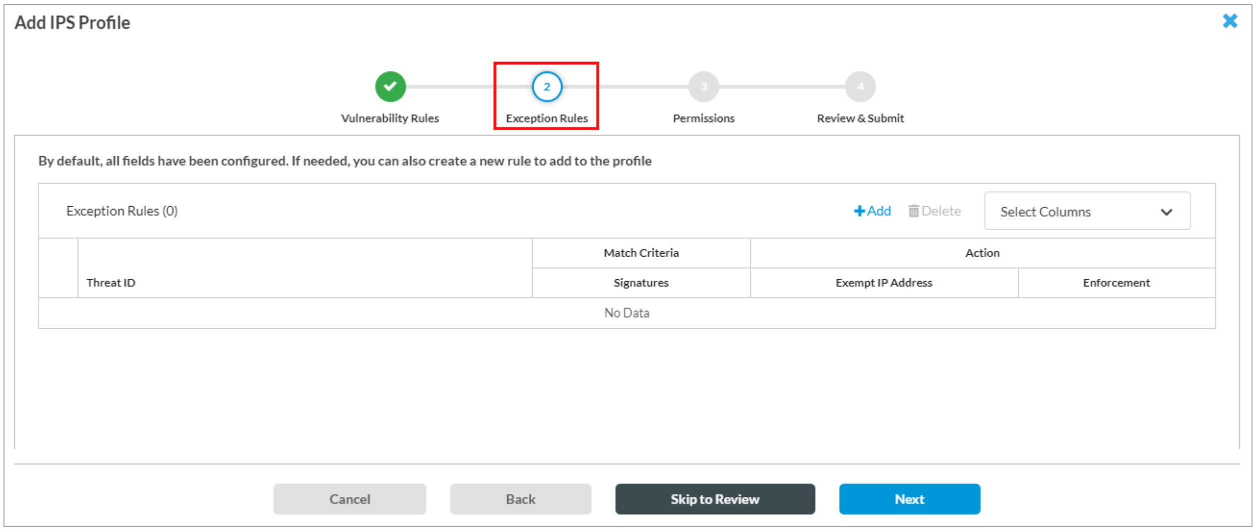
References

Severity

Enforcements

Action reset-client

12. For all other sections, review the information. If you need to make changes, click the Edit icon.
13. In the Add IPS Profile screen, click Next to go to Step 2, Exceptions Overrules.

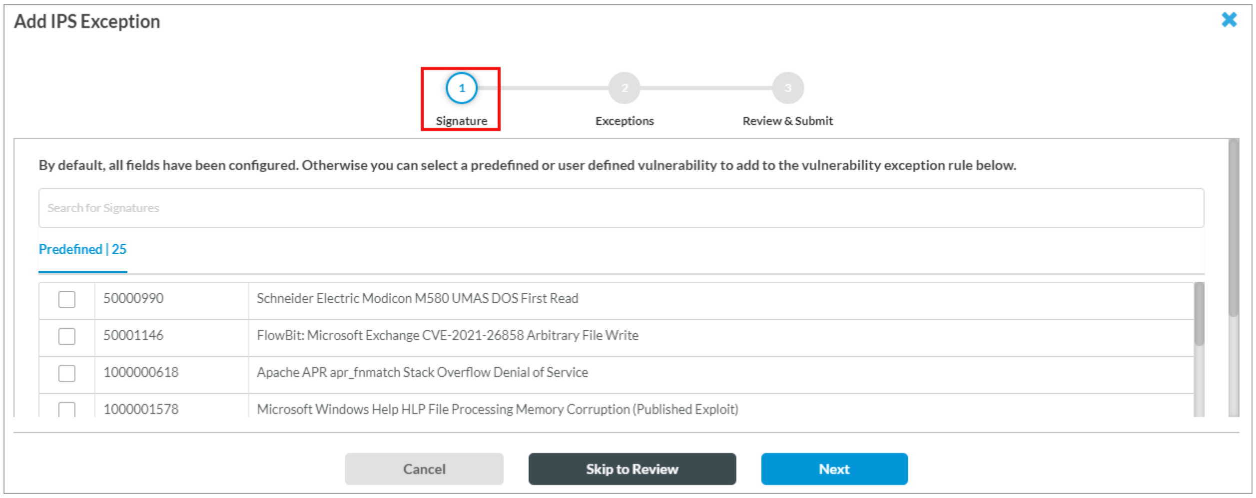


By default, all fields have been configured. If needed, you can also create a new rule to add to the profile

Exception Rules (0)

	Match Criteria	Action	
Threat ID	Signatures	Exempt IP Address	Enforcement
No Data			

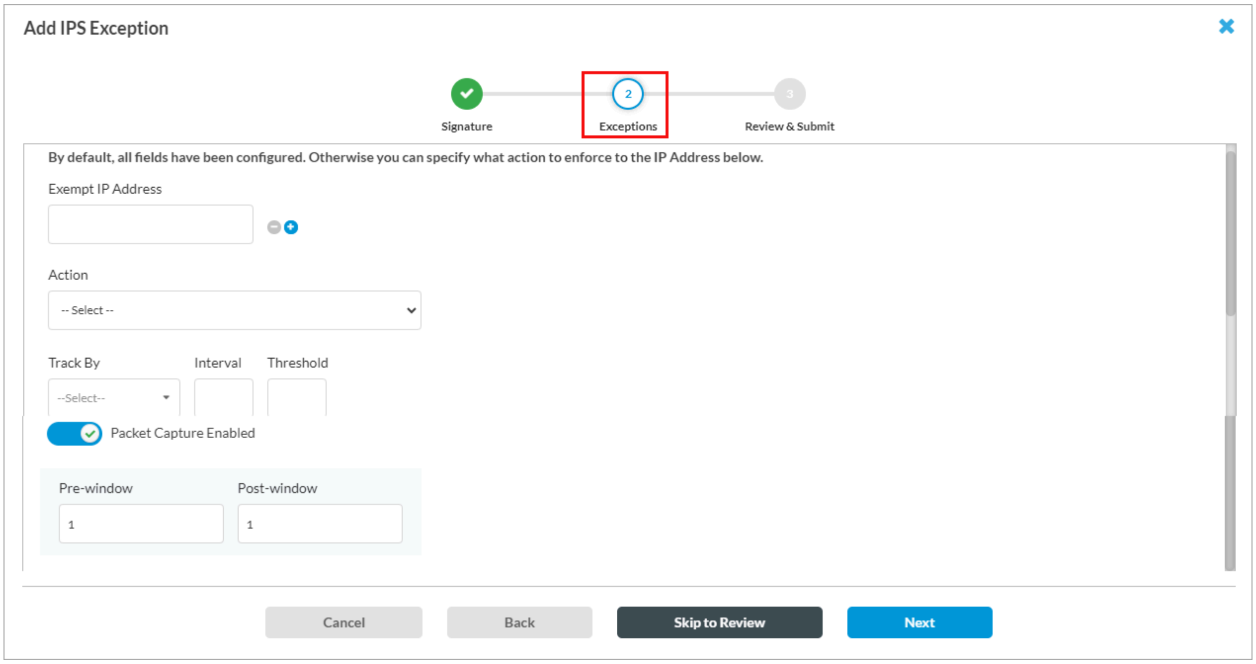
14. Click + Add. The Add IPS Exception screen displays.



By default, all fields have been configured. Otherwise you can select a predefined or user defined vulnerability to add to the vulnerability exception rule below.

□	50000990	Schneider Electric Modicon M580 UMAS DOS First Read
□	50001146	FlowBit: Microsoft Exchange CVE-2021-26858 Arbitrary File Write
□	1000000618	Apache APR apr_fnmatch Stack Overflow Denial of Service
□	1000001578	Microsoft Windows Help HLP File Processing Memory Corruption (Published Exploit)

15. In the Signatures screen, select the vulnerability signatures to add to the vulnerability profiles exception rule.
16. Click Next. In the Exception screen, enter information for the following fields.



Add IPS Exception

By default, all fields have been configured. Otherwise you can specify what action to enforce to the IP Address below.

Exempt IP Address:

Action: -- Select --

Track By: --Select--

Interval:

Threshold:

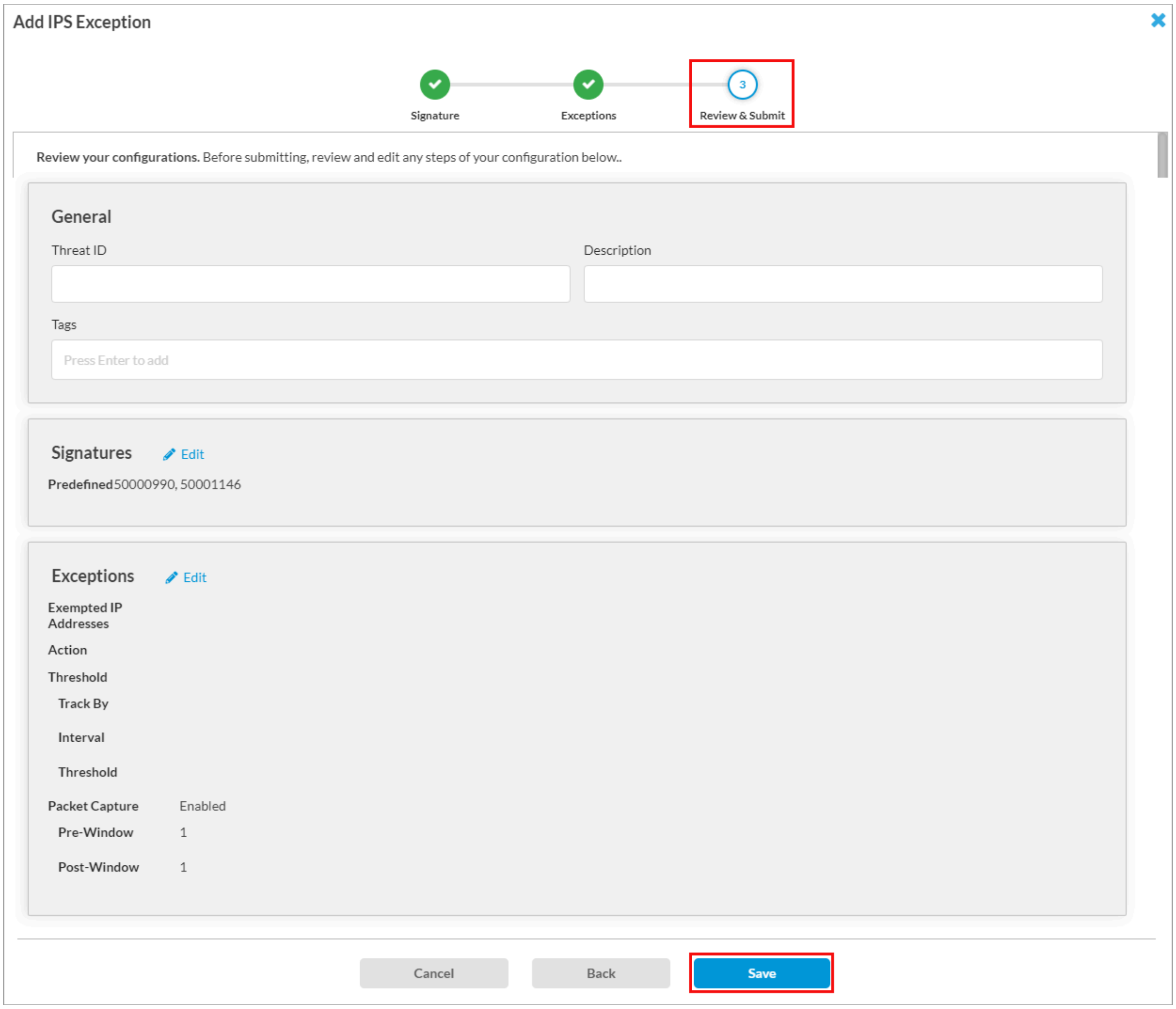
Packet Capture Enabled

Pre-window: 1

Post-window: 1

Field	Description
Exempt IP Address	Click the + Add icon to enter the IP addresses that are exempt from the vulnerability rule.
Action	Select the action to take: ◦ Allow ◦ Alert ◦ Drop packet ◦ Drop session ◦ Reject ◦ Reset client ◦ Reset server
Threshold	Select the threshold application on the exempted IP address: ◦ Interval—Enter an interval, in seconds. ◦ Threshold—Enter the number of hits per interval based on the traffic direction. ◦ Track By—Select the threshold tracking based on either source address, destination address, or both source and destination addresses.
Packet Capture Enabled	Click this, and then enter the following information: ◦ Pre-window—Enter the number of packets immediately preceding the attacked packet that you want to capture. ◦ Post-window—Enter the number of packets immediately following the attacked packet that you want to capture.

17. Click Next to go to Step 3, Review and Submit.



Review your configurations. Before submitting, review and edit any steps of your configuration below..

General

Threat ID

Description

Tags

Press Enter to add

Signatures

Predefined50000990, 50001146

Exceptions

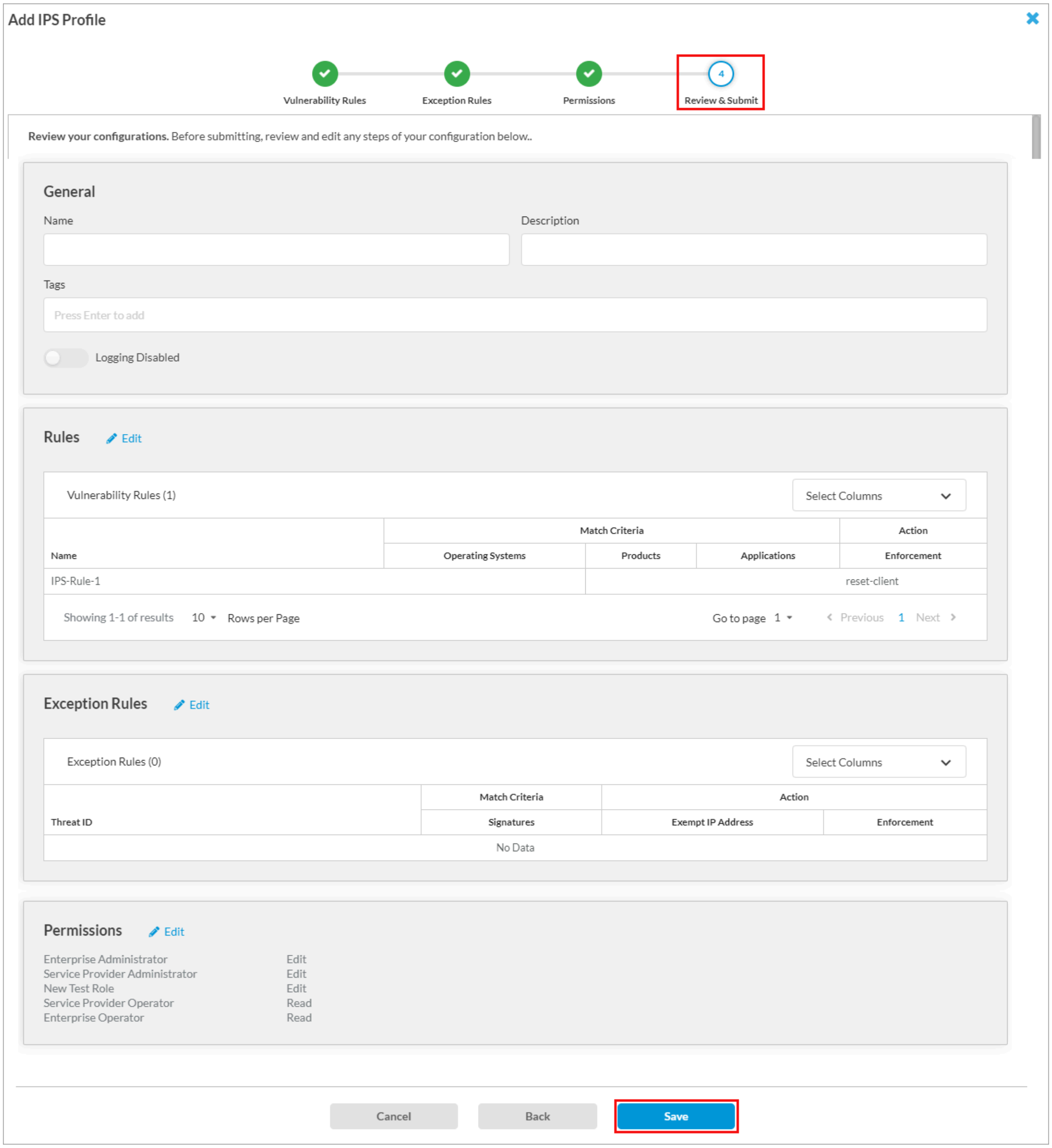
Exempted IP Addresses	
Action	
Threshold	
Track By	
Interval	
Threshold	
Packet Capture	Enabled
Pre-Window	1
Post-Window	1

a. In the General section, enter a name for the IPS exception, optionally, a description and tags.

b. For all other sections, review the information. To make changes, click the ✎ Edit icon.

c. Click Save.

18. In the Add IPS Profile screen, click Next to go to Step 3, Permissions screen to set or update the permission for each role. The roles are Enterprise Administrator, Enterprise Operator, Service Provider Administrator, and Service Provider Operator. The permission for each role is selected by default, and you can update it. The role permissions are Edit, Hide, and Read.



Review your configurations. Before submitting, review and edit any steps of your configuration below..

General

Name:

Description:

Tags: Press Enter to add

○ Logging Disabled

Rules ✏ Edit

Vulnerability Rules (1) — Select Columns

	Match Criteria			Action
Name	Operating Systems	Products	Applications	Enforcement
IPS-Rule-1				reset-client

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

Exception Rules ✏ Edit

Exception Rules (0) — Select Columns

	Match Criteria	Action	
Threat ID	Signatures	Exempt IP Address	Enforcement
No Data			

Permissions ✏ Edit

Enterprise Administrator	Edit
Service Provider Administrator	Edit
New Test Role	Edit
Service Provider Operator	Read
Enterprise Operator	Read

19. Click Next to go to Step 3, Review and Submit.
20. In the General section, enter a name for the IPS policy, optionally, a description and tags.
21. For all other sections, review the information. To make changes, click the ✏ Edit icon.
22. Click Save.

Supported Software Information

Releases 12.1.1 and later support all content described in this article.

Additional Information

Configure Custom IPS-Filtering Profiles
Versa Concerto Overview