
Configure Advanced Threat Protection

 For supported software information, click [here](#).

Antivirus software is typically installed on endpoint machines. When new malware outbreaks occur, antivirus software vendors update their definition or data file for the antivirus software so that the software detects new malware. This scenario has the following limitations:

- Because of the volume of malware files and evasion techniques, such as polymorphism, packers, and encryption, signature-based detection of malware is ineffective.
- In case of a malware infection, the impact of the malware is quite significant.

Addressing these scenarios requires real-time, zero-day threat detection that does not require waiting for signature updates to detect and protect against threats.

Versa advanced threat protection (ATP) provides advanced detection mechanisms that detect and prevent organizations from zero-day threats. ATP includes the following detection mechanisms:

- Artificial intelligence (AI) and machine learning (ML)
- MITRE ATT&CK framework
- Multiple sandboxes and dynamic analysis
- Multiple antivirus engines
- Reputation-based matches
- Signature-based matches
- Static analysis

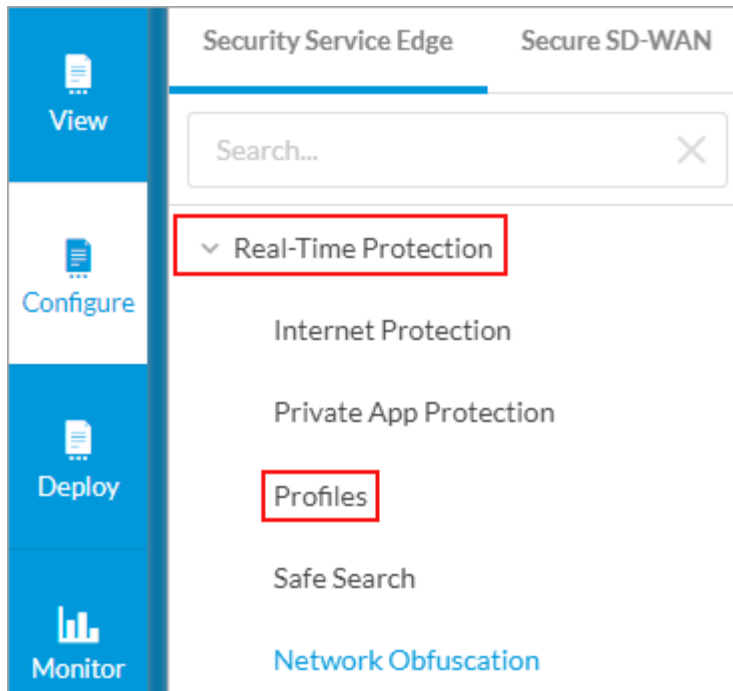
You can configure Versa ATP using sandboxing profiles. Then, in a security policy, you associate an ATP profile with the policy action so that the profile is applied to traffic that matches the policy's match criteria.

When you enable sandboxing, files extracted from matching traffic are submitted to Versa ATP for threat detection. If Versa ATP detects any malware, policy enforcement actions are taken to alert, block, or remediate the affected devices.

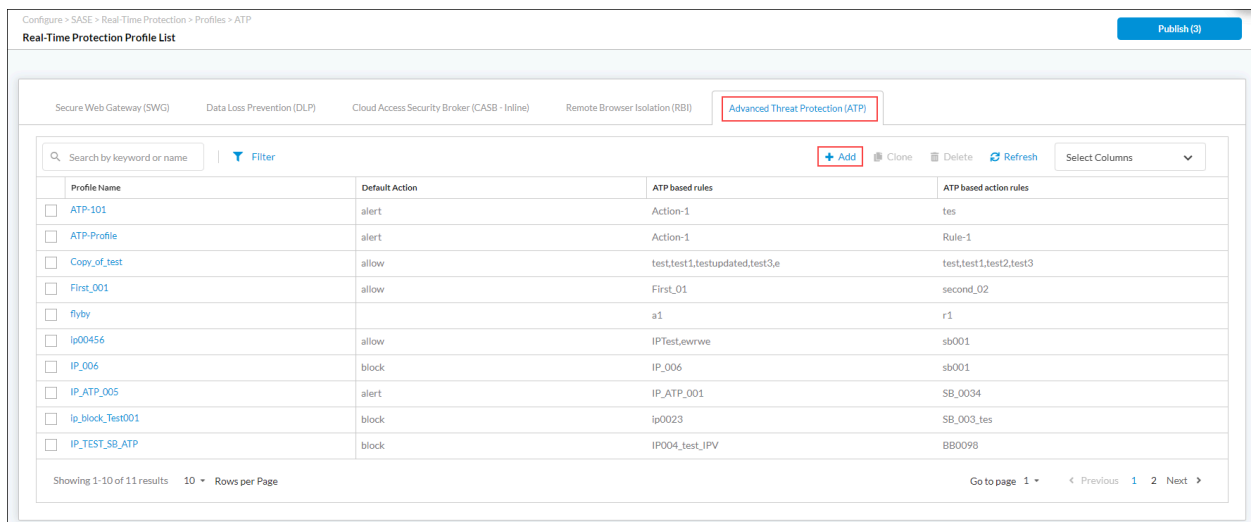
To enable ATP in Concerto, you configure ATP profiles to define ATP actions, sandbox rules, and default actions.

Configure ATP Profiles

1. Go to Configure > Secure Services Edge > Real-Time Protection > Profiles.



2. Select the Advanced Threat Protection (ATP) tab.



3. Click + Add. The Create ATP Profile screen displays.

Configure > SASE > Real-Time Protection > Profiles > ATP

Create ATP Profile

1
ATP ACTIONS

2
SANDBOX RULES

3
DEFAULT ACTIONS

4
REVIEW & SUBMIT

Configure ATP actions that will be used for your sandbox rules..

+ Add Delete Select Columns

NAME	PENDING ATP ACTION	SANDBOX ACTIONS		
		CLEAN	SUSPICIOUS	MALICIOUS
No Data				

Cancel

Back

Skip to Review

Next

4. In Step 1, ATP Action screen, click + Add to configure ATP actions. In the Add ATP Action screen, enter information for the following fields.

Add ATP Action

Choose which configurations to enforce for your action.

Action Name

Pending ATP Action

<input checked="" type="checkbox"/> Allow and scan first time	<input checked="" type="checkbox"/> block	<input checked="" type="checkbox"/> Wait until timeout
--	--	---

Sandbox Actions

Specify the actions for the following

Clean

Suspicious

Malicious

Cancel

Save

Field	Description
Action Name	Enter a name for the ATP action.
Pending ATP Actions	<p>Select the action to take on the file until the sandbox results are available from the cloud:</p> <ul style="list-style-type: none"> ◦ Allow and Scan First Time—Allow the file download while the file is submitted to the cloud for scanning. The sandbox results received from the cloud are cached on the device. ◦ Block—Block the file download. The sandbox results from the cloud are cached on the device. ◦ Wait Until Timeout—Pause the file download as the last packet is held by the Versa Operating System™ (VOS™) device until the timeout, in seconds, which is configured in the Default Actions tab. The action to take on the file depend on the results available within this timeout value. If timeout time occurs before results are available, the timeout action is taken.
Sandbox Actions	<p>Select the actions to take for the different file reputations, clean, suspicious, and malicious:</p> <ul style="list-style-type: none"> ◦ Alert ◦ Allow ◦ Block

5. Click Save. The saved ATP action displays in the main pane.

Configure > SASE > Real-Time Protection > Profiles > ATP

Create ATP Profile

1

ATP Actions

2

Sandbox Rules

3

Default Actions

4

Review & Submit

Configure ATP actions that will be used for your sandbox rules..

+ Add

Delete

Select Columns

Name	Pending ATP Action	Clean	Sandbox Actions	Suspicious	Malicious
<input type="checkbox"/> AllowCleanFiles	Allow and scan first time	allow	alert	block	

Showing 1-1 of 1 results

10

Rows per Page

Go to page

< Previous

Next >

Cancel

Back

Skip to Review

Next

6. Click Next to go to Step 2, Sandbox Rules.

Configure > SASE > Real-Time Protection > Profiles > ATP

Create ATP Profile

✓

ATP ACTIONS

2

SANDBOX RULES

3

DEFAULT ACTIONS

4

REVIEW & SUBMIT

Configure sandbox rules that will be used for your ATP profile.

+ Add

Delete

Select Columns

NAME	ATP ACTION	DIRECTION	PROTOCOL	FILE TYPE
No Data				

Cancel

Back

Skip to Review

Next

7. Click + Add. In the Add Sandbox Rule screen, enter information for the following fields.

Add Sandbox Rule

Choose which configurations to enforce for your rule.

Rule Name








Description

☒ Rule is Enabled

ATP Action



















[+ Add New](#)

Select the type of protocol to detect and analyze.

 HTTP	 FTP	 SMTP	 IMAP	 POP3	 MAPI
 SMB					

Select the type of files to detect and analyze

 ☐ Select All

 avi	 bat	 bmp	 cab	 c	 dll
 doc	 docx	 dwg	 coff	 xml	 applelist
					

Select type of file action.

Download and Upload <input checked="" type="checkbox"/>	Download <input type="checkbox"/>	Upload <input type="checkbox"/>
---	-----------------------------------	---------------------------------

Notification Profile

Cancel

Save

Field	Description																																																																																										
Rule Name	Enter a name for the rule.																																																																																										
Description	Enter a text description for the rule.																																																																																										
ATP Actions	Select the ATP action that you added in Step 4, or Click Add New to create a new ATP action.																																																																																										
Protocol	Select the protocols to enable extracting and scanning of files. To select all files, click Select All.																																																																																										
File Types	<p>Select the types of files to enable for sandbox analysis. The supported file types are:</p> <table border="1"> <tbody> <tr> <td>7zip</td><td>ace</td><td>android</td><td>apple</td><td>arj</td><td>avi</td><td>avif</td><td>bat</td><td>bmp</td></tr> <tr> <td>bzip2</td><td>cab</td><td>c</td><td>chm</td><td>class</td><td>coff</td><td>com</td><td>cpp</td><td>csv</td></tr> <tr> <td>db</td><td>deb</td><td>dll</td><td>dmg</td><td>doc</td><td>docx</td><td>dwg</td><td>elf</td><td>eml</td></tr> <tr> <td>evtx</td><td>exe</td><td>flv</td><td>gif</td><td>gpg</td><td>gzip</td><td>html</td><td>inf</td><td>iso</td></tr> <tr> <td>jar</td><td>jpeg</td><td>lha</td><td>lnk</td><td>lzh</td><td>mach_o</td><td>mdb</td><td>mdi</td><td>mht</td></tr> <tr> <td>midi</td><td>mov</td><td>mp3</td><td>mpeg</td><td>msi</td><td>msoffdocp</td><td>pdf</td><td>pem</td><td></td></tr> <tr> <td>pgp</td><td>php</td><td>pif</td><td>pl</td><td>png</td><td>ppk</td><td>ppt</td><td>pptx</td><td>psd</td></tr> <tr> <td>pst</td><td>py</td><td>rar</td><td>reg</td><td>rm</td><td>rtf</td><td>sh</td><td>svg</td><td>swf</td></tr> <tr> <td>tar</td><td>targa</td><td>tiff</td><td>torrent</td><td>txt</td><td>visio</td><td>vsf</td><td>wav</td><td>webp</td></tr> <tr> <td>wim</td><td>wmf</td><td>wmv</td><td>xlb</td><td>xls</td><td>xlsx</td><td>xml</td><td>xz</td><td>zip</td></tr> </tbody> </table>	7zip	ace	android	apple	arj	avi	avif	bat	bmp	bzip2	cab	c	chm	class	coff	com	cpp	csv	db	deb	dll	dmg	doc	docx	dwg	elf	eml	evtx	exe	flv	gif	gpg	gzip	html	inf	iso	jar	jpeg	lha	lnk	lzh	mach_o	mdb	mdi	mht	midi	mov	mp3	mpeg	msi	msoffdocp	pdf	pem		pgp	php	pif	pl	png	ppk	ppt	pptx	psd	pst	py	rar	reg	rm	rtf	sh	svg	swf	tar	targa	tiff	torrent	txt	visio	vsf	wav	webp	wim	wmf	wmv	xlb	xls	xlsx	xml	xz	zip
7zip	ace	android	apple	arj	avi	avif	bat	bmp																																																																																			
bzip2	cab	c	chm	class	coff	com	cpp	csv																																																																																			
db	deb	dll	dmg	doc	docx	dwg	elf	eml																																																																																			
evtx	exe	flv	gif	gpg	gzip	html	inf	iso																																																																																			
jar	jpeg	lha	lnk	lzh	mach_o	mdb	mdi	mht																																																																																			
midi	mov	mp3	mpeg	msi	msoffdocp	pdf	pem																																																																																				
pgp	php	pif	pl	png	ppk	ppt	pptx	psd																																																																																			
pst	py	rar	reg	rm	rtf	sh	svg	swf																																																																																			
tar	targa	tiff	torrent	txt	visio	vsf	wav	webp																																																																																			
wim	wmf	wmv	xlb	xls	xlsx	xml	xz	zip																																																																																			
Direction	<p>Select the direction to enable the scanning of files:</p> <ul style="list-style-type: none"> ◦ Download ◦ Download and upload ◦ Upload 																																																																																										

Notification Profile

(For Releases 12.1.1 and later.) Select a notification profile. To configure a notification profile, see [Configure SASE User-Defined Objects](#).

- Click Save. The saved sandbox rule displays in the main pane.

Configure > SASE > Real-Time Protection > Profiles > ATP

Create ATP Profile

1 ATP Actions

2 Sandbox Rules

3 Default Actions

4 Review & Submit

Configure sandbox rules that will be used for your ATP profile.

+ Add Delete Select Columns

	Name	ATP Action	Direction	Protocol	File Type
<input type="checkbox"/>	ATP-Sandbox-Rule1	AllowCleanFiles	Download and Upload	HTTP,FTP,SMTP,IMAP,POP3,MAP	all

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

Cancel

Back

Skip to Review

Next

- Click Next to go to Step 3, Default Actions, and then enter information for the following fields.

Configure > SASE > Real-Time Protection > Profiles > ATP

Create ATP Profile

✓

ATP ACTIONS

✓

SANDBOX RULES

3

DEFAULT ACTIONS

4

REVIEW & SUBMIT

By default, we will allow all files that do not match any criteria specified. Otherwise, you can choose which default action to enforce if there are no criteria matched.

Select the default action to enforce if there are no criteria matched.

Default Action

Timeout Action

Duration to wait before timeout

Cloud Lookup ⓘ

☐ Cloud Lookup State

Cancel

Back

Skip to Review

Next

Field	Description
Default Action	<p>Select the default action. This action applies when there is no match for protocol or file type.</p> <ul style="list-style-type: none"> Alert Allow Block
Timeout Action	Select the action to apply when a timeout occurs.
Timeout	<p>Enter timeout value, in seconds.</p> <p><i>Range:</i> 1 through 600 seconds</p>
Cloud Lookup State	Check to enable cloud lookup for file reputation.

10. Click Next to go to Step 4, Review and Submit. Click Edit next to any section to make changes

Configure > SASE > Real-Time Protection > Profiles > ATP

Create ATP Profile

ATP Actions

Sandbox Rules

Default Actions

4
Review & Submit

Review your ATP configuration below

General

Name *

AtpProfile1

Description

ATP profile for Test

Tags

Press Enter to add

Logging is Disabled

ATP Action

Name

ATP-ACTION1

Pending ATP Action

Allow and scan first time

Sandbox Actions

Clean: Allow
Suspicious: Alert
Malicious: Reject

Sandbox Rules

Name	ATP Action	Direction	Protocol	File Type
Sandbox-rule1	ATP-ACTION1	Download and Upload	HTTP,FTP	avi,cab,bmp,bat,c,dll,applelist,xml,coff,dwg,docx,doc

Default Actions

Default Action:

Alert

Timeout Action:

Reject

Duration to wait before timeout:

30

Cloud Lookup:

true

Cancel

Back

Save

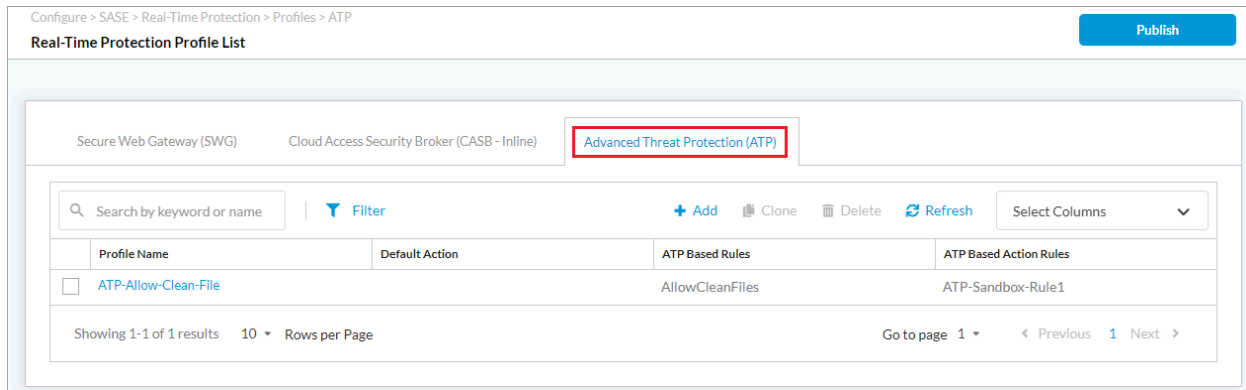
11. Click Save. The ATP profile displays in the Advanced Threat Protection (ATP) tab.

https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Advanced_Threat_...

Updated: Wed, 23 Oct 2024 08:40:56 GMT

Copyright © 2024, Versa Networks, Inc.

11



Associate an ATP Profile with a SASE Internet Protection Rule

To enforce Versa ATP detection mechanisms for internet traffic, you associate an ATP profile with a SASE internet protection rule:

1. Go to Configure > Real-Time Protection > Internet Protection.
2. In the Internet Protection Rules List screen, click + Add to create a rule. The Create Internet Protection Rule screen displays. For more information, see [Configure SASE Internet Protection Rules](#).
3. Select the Security Enforcement screen, and then select Profiles.
4. Select the Advanced Threat tab, and then click the slider to enable ATP.

Configure > SASE > Real-Time Protection > Internet Protection

Create Internet Protection Rule

✓

Applications & URLs

✓

Users & Groups

✓

Endpoint Information Profile (EIP)

✓

GEO Locations

✓

Network Layer 3-4

6

Security Enforcement

7

Review & Deploy

We have preselected your security enforcements, below

You can unselect and customize any configuration you'd like to enforce.

☐

✓

Allow

Allow all traffic that matches the rule to pass

☐

✗

Deny

Drop all traffic that matches the rule

☐

✗

Reject

Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

✓

Profiles

Choose one or more predefined or user defined security enforcements which include criteria to allow or reject traffic.

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB - Inline)

Advanced Threat Protection (ATP)

Advanced Threat Protection

+ Create New

Advanced Threat Protection ATP-2

The following sandbox rules will be used in if malware is found

Sandbox Rules	ATP Action	Protocols	File Types
ATP-Sandbox-Rule1	AllowCleanFiles	HTTP,FTP,SMTP,IMAP,POP3,MAPI	all

Cancel

Back

Skip to Review

Next

- Select the ATP profile to associate with the internet protection rule.
- To create a new ATP profile, click + Create New. The Create ATP Profile screen displays. For more information, see [Configure ATP Profiles](#), above.

7. Review the internet protection rule, and then deploy it.

Software Release Information

Releases 11.4.1 and later support all content described in this article, except:

- Release 12.1.1 supports notification profile selection for ATP rules.

Additional Information

[Configure SASE Internet Protection Rules](#)