
Configure SD-WAN Malware Protection Policies

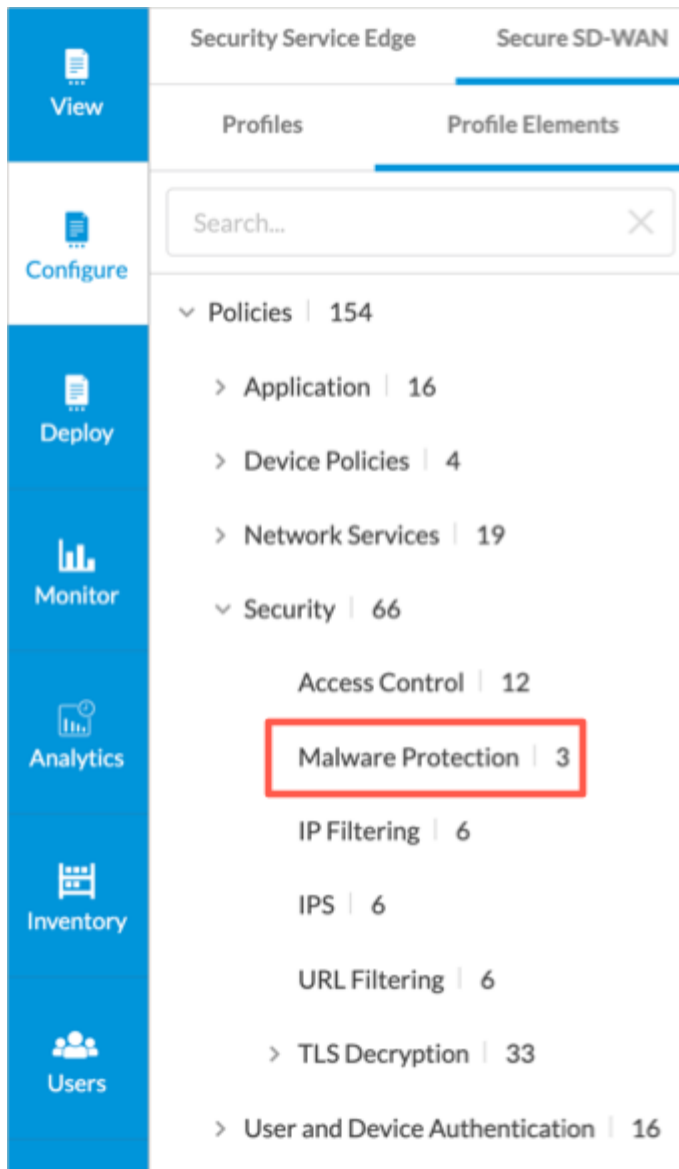
 For supported software information, click [here](#).

You can configure malware protection policies to detect and prevent malware threats. You then associate the policies with basic or standard master profiles. For more information, see [Configure Profiles](#).

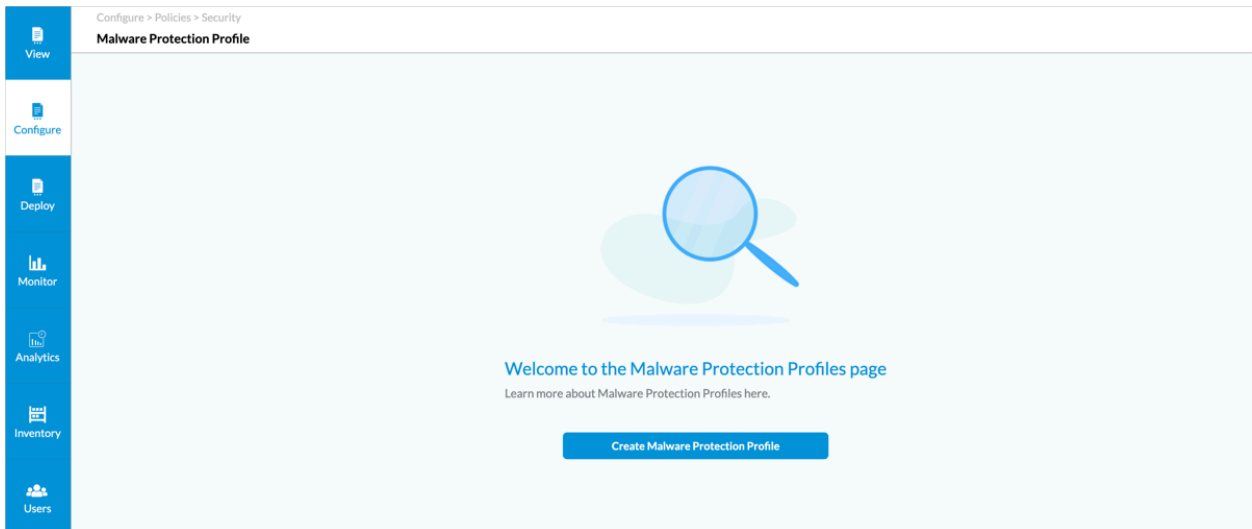
Note that when you configure master profiles and subprofiles, malware protection policies are referred to as antivirus policies.

To configure a malware protection policy:

1. In Tenant view, go to the Configure lifecycle in the left menu bar.



2. Select Secure SD-WAN > Profile Elements > Policies > Security > Malware Protection.
 - If you have not yet configured a malware protection policy, the following screen displays. Click Create Malware Protection Profile to display the Add Malware Protection Profile screen. Continue with [Step 4](#).



- If you have configured one or more malware policies, the Malware Protection Profile screen displays the policies that are already configured.

Configure > Policies > Security

Malware Protection Profile

Malware Protection Profile (3)

Search By Name

+ Add

Clone

Delete

Refresh

More Actions >

Select Columns

			Match Criteria							
	Name	Version	File Types				Protocols	Direction	Action	Last Modified
<input type="checkbox"/>	AutoDelete	1	avi, bat, bmp, cab, c, dll, doc, docx, dwg, coff, xml, appleplist, cpp, php, mach_o, wav, jar, targa, exe, flv, gif, gzip, class, iso, jpeg, lha, lnk, lzh, mdb, mdi, mov, mpeg, msi, msoffice, android, pdf, png, ppg, plf, pl, ppt, pptx, psd, rar, reg, rm, rtf, sh, tar, ttf, torrent, wmf, wmv, xls, txt, elf, xlsx, mp3, zip, html, 7zip, dmg, bz2, deb, db, gpg, ace, arj, xz, wim, py, inf, svg, xlb, com, odp, eml, evtx, mht, pst, chm, midi, swf, avif, webp, visio, any				IMAP	Download and Upload	Deny	4/4/2024, 11:33:32 AM Administrator
<input type="checkbox"/>	asd	1	avi				FTP, SMTP			11/22/2023, 12:04:10 PM Administrator
<input type="checkbox"/>	AnitVirus	1								6/1/2023, 4:42:10 PM Administrator

Showing 1-3 of 3 results

10 Rows per Page

Go to page 1

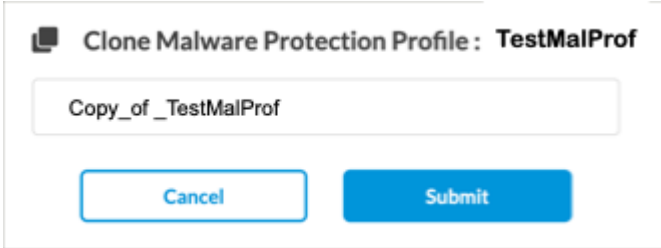
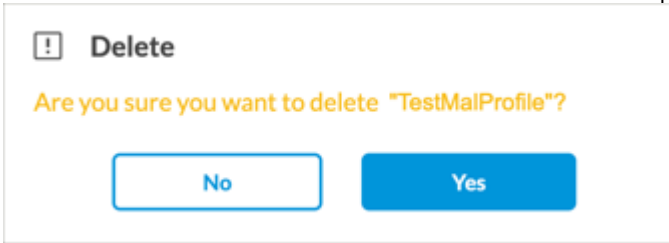
< Previous

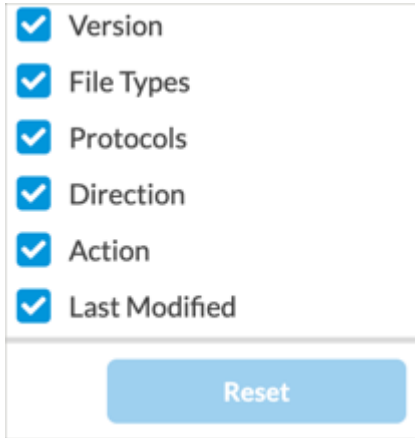
1


Next >

3. In the horizontal menu bar, you can select one of the following operations.

Operation	Description
+ Add	Create a new malware protection policy. This button is active when no existing profile is selected.
Clone	Clone the selected malware protection policy. A popup window similar to the following displays.

Operation	Description
	 <p>Rename the default name of the cloned policy (here, Copy_of_TestMalProf), if needed, and then click Submit.</p>
Delete	<p>Delete the selected malware protection policy. A popup window similar to the following displays.</p>  <p>Click Yes to delete the policy, or click No to retain the profile.</p>
Refresh	Refresh the list of existing policies.
More Actions	<p>Perform an action on the selected malware protection policy:</p> <ul style="list-style-type: none"> ◦ Compare Versions—View the differences between two versions of a policy. ◦ Disable Auto Delete—Disable the automatic deletion of the policy (auto deletion is enabled by default). For more information, see Configure

Operation	Description
	<p>Automatic Deletion of SD-WAN Object Versions.</p> <ul style="list-style-type: none"> ◦ Propagate—Propagate changes made to a profile to any entities that use the policy. For more information, see Propagate Object Configuration Changes. ◦ View References—View the objects that refer to the selected policy. For more information, see View References to Objects in the Configuration Hierarchies.
Select Columns	<p>To select the columns that you want to display, click the down arrow. To return to the default column selection, click Reset.</p>  <p>The column headings are:</p> <ul style="list-style-type: none"> ◦ Action ◦ Direction ◦ File Types ◦ Last Modified ◦ Protocols ◦ Version

4. Click  Add to create a new malware protection policy. A policy consists of one or more match criteria, an action, and permissions. The following screen displays.

Add Malware Protection Profile

Match Criteria: 1 File Type & Protocol, 2 Enforcement, 3 Permissions, 4 Review & Submit

By default, all fields are configured. Otherwise, you can choose which actions to enforce for your malware protection. If traffic is matched in both deny and allow, then the deny action takes precedence.

Select the type of protocols to scan for malware.

☐ Select All

HTTP FTP SMTP IMAP POP3 MAPI SMB

Select the type of files to scan for malware.

☐ Select All

AVI BAT BMP cab C DLL

Cancel Skip to Review Next

- In Step 1, File Type and Protocol, select the protocols to scan for malware. Use the search box to find specific protocol types. Check the Select All box to select all protocol types.

Add Malware Protection Profile

Match Criteria: 1 File Type & Protocol, 2 Enforcement, 3 Permissions, 4 Review & Submit

HTTP FTP SMTP IMAP POP3 MAPI

Select the type of files to scan for malware.

☐ Select All

avi bat bmp cab c dll

Select the direction of the traffic on which to perform the malware scan.

Download and Upload Download Upload

Cancel Skip to Review Next

- Select the types of files to scan for malware. Use the search box to find specific file types. Check the Select All box to select all file types.

Select the direction of the traffic on which to perform the malware scan.

Download and Upload ☒ Download ☐ Upload ☐

Cancel Skip to Review Next

7. Scroll to the bottom of the screen, and then click the direction of the traffic on which to perform the malware scan.
8. Click Next to go to Step 2, Enforcement. You can define the default enforcement actions to take on traffic that meets the previously selected match conditions. The following screen displays the available enforcement actions.

Add Malware Protection Profile

Match Criteria ☒ Action ☒ ☐ ☐

File Type & Protocol Enforcement Permissions 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.

Specify the action to enforce when traffic matches the profile.

Alert ☐ Allow ☐ Deny ☒ Recommended Action ☐ Reject ☐

Cancel Back Skip to Review Next

9. Select the action to enforce when traffic matches the protocols, file types, and traffic direction you selected in Step 1, File Types and Protocol:
 - Alert—Allow the file to pass and log the action.
 - Allow—Allow the file to pass without logging the action.
 - Deny—Do not allow the file to pass and log the action. This is the default.
 - Recommended Action—FTP and HTTP traffic is set to Deny. Email traffic (SMTP, IMAP, POP3, and MAPI) is set to Alert.
 - Reject—Reset the connection to the server and client, and log the action.
10. Click Next to go to Step 3, Permissions. You can select malware protection policy permissions for each Concerto role.

Add Malware Protection Profile

Match Criteria

Action

3

4

File Type & Protocol

Enforcement

Permissions

Review & Submit

We have preselected the permissions for the roles, below You can change the permission for each of the roles.

Role	Permissions
Enterprise Administrator (Inherited)	<div>Edit</div>
Service Provider Administrator (Inherited)	<div>Edit</div>
Service Provider Operator (Inherited)	<div>Read</div>
Enterprise Operator (Inherited)	<div>Read</div>

Cancel

Back


Skip to Review

Next

11. Enter information for the following fields.

Field	Description
Enterprise Administrator	<p>Select a malware policy permission for user accounts with the Enterprise Administrator role:</p> <ul style="list-style-type: none"> Edit—User can view and change malware policies. Hide—User cannot view malware policies. Read—User can view malware policies. <p><i>Default:</i> Edit</p>
Service Provider Administrator	<p>Select a malware policy permission for user accounts with the Service Provider Administrator role:</p> <ul style="list-style-type: none"> Edit—User can view and change malware policies. Hide—User cannot view malware policies. Read—User can view malware policies. <p><i>Default:</i> Edit</p>

Field	Description
Service Provider Operator	<p>Select a malware policy permission for user accounts with the Service Provider Operator role:</p> <ul style="list-style-type: none"> ◦ Edit—User can view and change malware policies. ◦ Hide—User cannot view malware policies. ◦ Read—User can view malware policies. <p><i>Default:</i> Read</p>
Enterprise Operator	<p>Select a malware policy permission for user accounts with the Enterprise Administrator role:</p> <ul style="list-style-type: none"> ◦ Edit—User can view and change malware policies. ◦ Hide—User cannot view malware policies. ◦ Read—User can view malware policies. <p><i>Default:</i> Read</p>

12. Click Next to go to Step 4, Review and Submit.
13. In the General box, enter a name for the malware protection policy. You can also enter a text description for the policy and one or more tags. A tag is an alphanumeric text descriptor with no spaces or special characters. You can specify multiple tags added for the same object. The tags are used for searching the objects.
14. Review the settings you have selected. Click the  Edit icon to change a setting, as needed.
15. Click Save to create the malware protection policy.

Supported Software Information

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

Additional Information

[Configure Automatic Deletion of SD-WAN Object Versions](#)

[Configure Profiles](#)

[Propagate Object Configuration Changes](#)

[Versa Concerto Overview](#)

[View References to Objects in the Configuration Hierarchies](#)