Configure Offline Custom Malware Protection Profiles

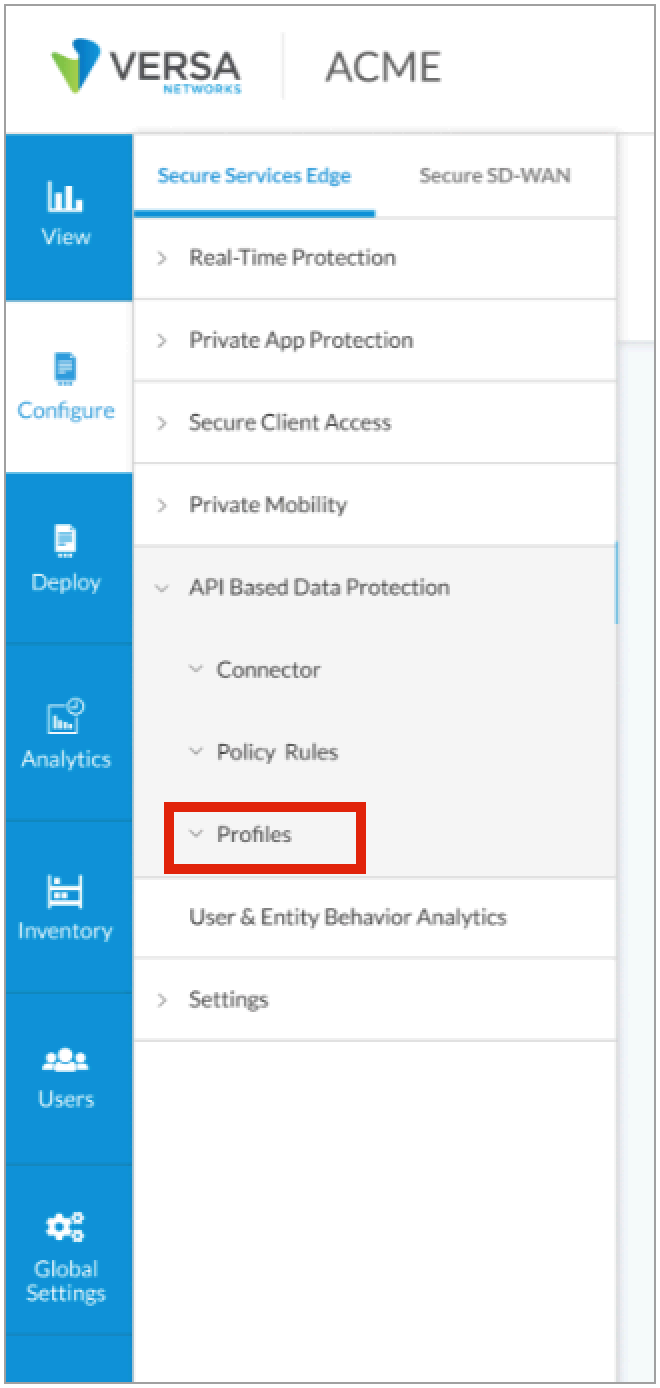
For supported software information, click here.

Offline malware is malicious software that is specifically designed to disrupt computers and computer systems. There are many types of malware, including computer viruses, worms, Trojan viruses, spyware, adware, and ransomware. Among the things malware can do is leak private information, gain unauthorized access to information or systems, and deprive users of access to information.

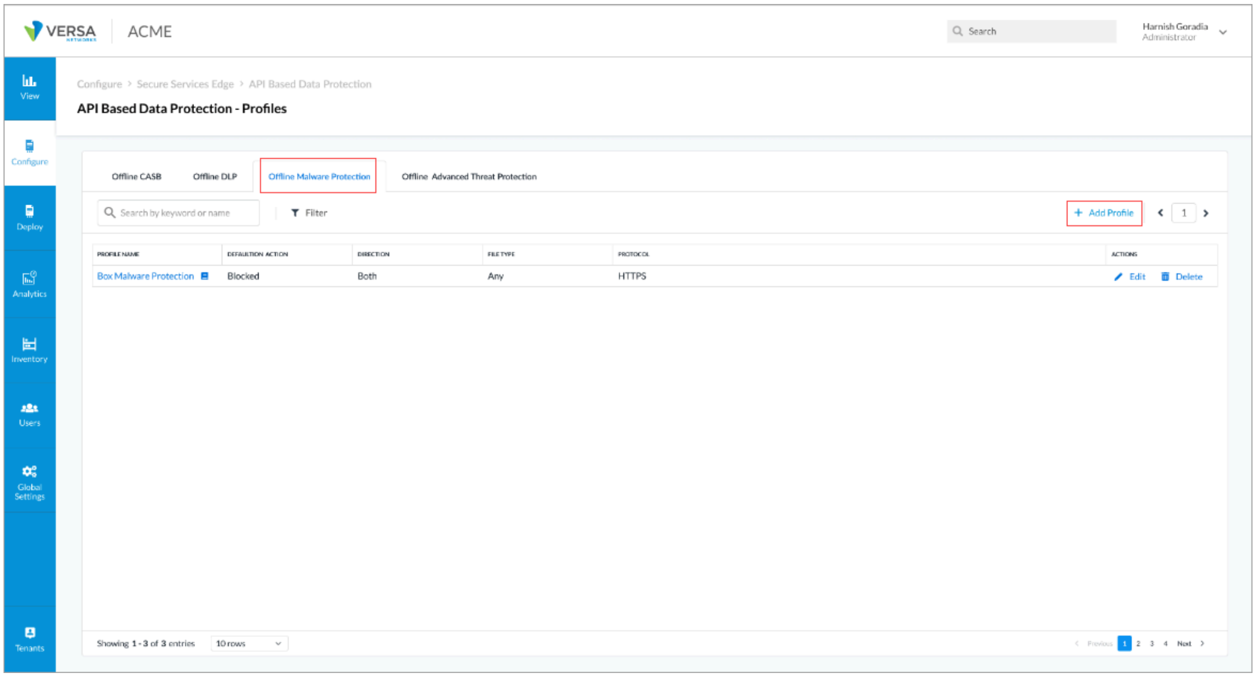
By default, Versa SASE provides a predefined security enforcement policy to protect against malware. This article describes how you can configure custom malware protection profiles.

To configure a custom offline malware-filtering profile:

1. Go to Configure > API Based Data Protection > Profiles.

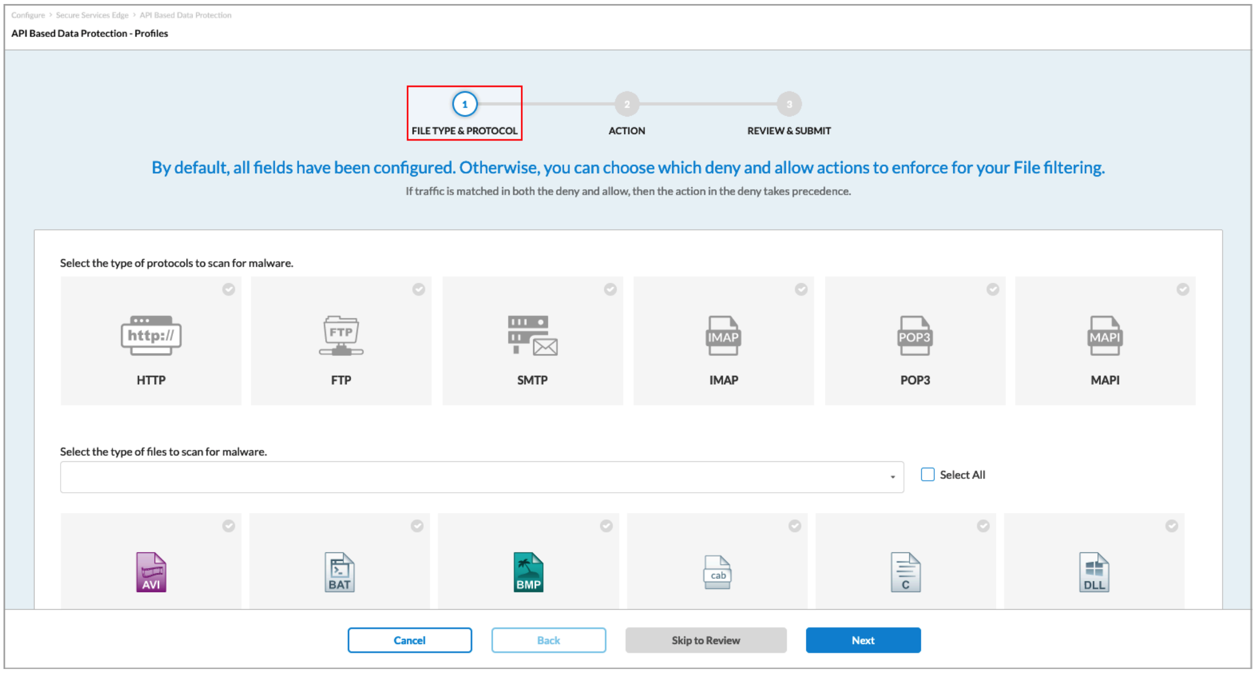


The following screen displays.


VERSA
ACME
Search
Harnish Goradia
Administrator
View
Configure
Deploy
Analytics
Inventory
Users
Global Settings
Tenants
Configure > Secure Services Edge > API Based Data Protection
API Based Data Protection - Profiles
Offline CASB
Offline DLP
Offline Malware Protection
Offline Advanced Threat Protection
Search by keyword or name
Filter
+ Add Profile
Showing 1 - 3 of 3 entries
10 rows

PROFILE NAME	DEFAULT ACTION	DIRECTION	FILE TYPE	PROTOCOL	ACTIONS
Box Malware Protection	Blocked	Both	Any	HTTPS	Edit Delete

2. Select the Secure Web Gateway (SWG) tab, and then select the Malware Protection subtab.
3. Click + Add to add a new offline malware-filtering profile. The API Based Data Protection-Profiles screen displays.


Configure > Secure Services Edge > API Based Data Protection
API Based Data Protection - Profiles
1
FILE TYPE & PROTOCOL
2
ACTION
3
REVIEW & SUBMIT

By default, all fields have been configured. Otherwise, you can choose which deny and allow actions to enforce for your File filtering.

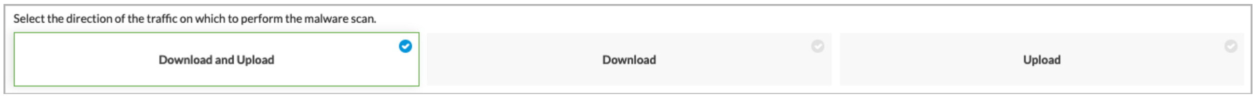
If traffic is matched in both the deny and allow, then the action in the deny takes precedence.

Select the type of protocols to scan for malware.

Select the type of files to scan for malware.

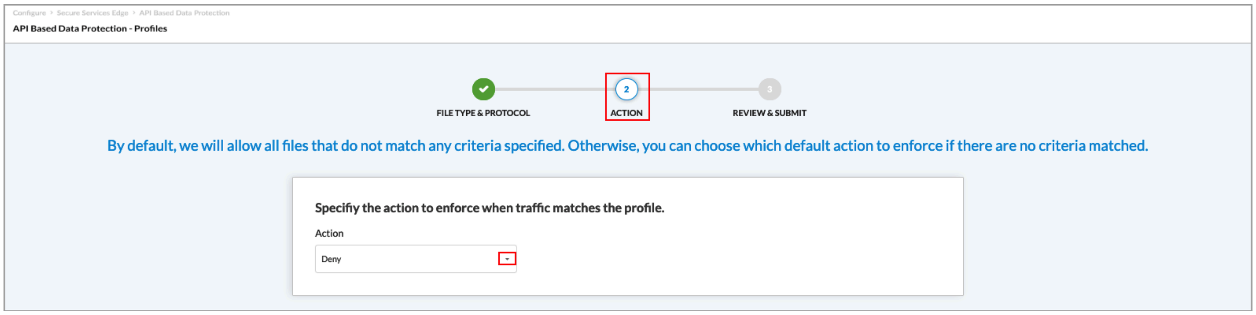
4. Select the protocols to scan for offline malware:
   - FTP
   - HTTP
   - IMAP

    - MAPI
    - POP3
    - SMTP
5. Select the types of files to scan for offline malware. Use the search box to find specific file types. Check the Select All box to select all file types.
6. Scroll to the bottom of the screen, and then select the direction of the traffic on which to perform the malware scan. By default, the Download and Upload option.



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

7. Click Next to go to the Action screen.



Configure > Secure Services Edge > API Based Data Protection
API Based Data Protection - Profiles
FILE TYPE & PROTOCOL
2
ACTION
3
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.

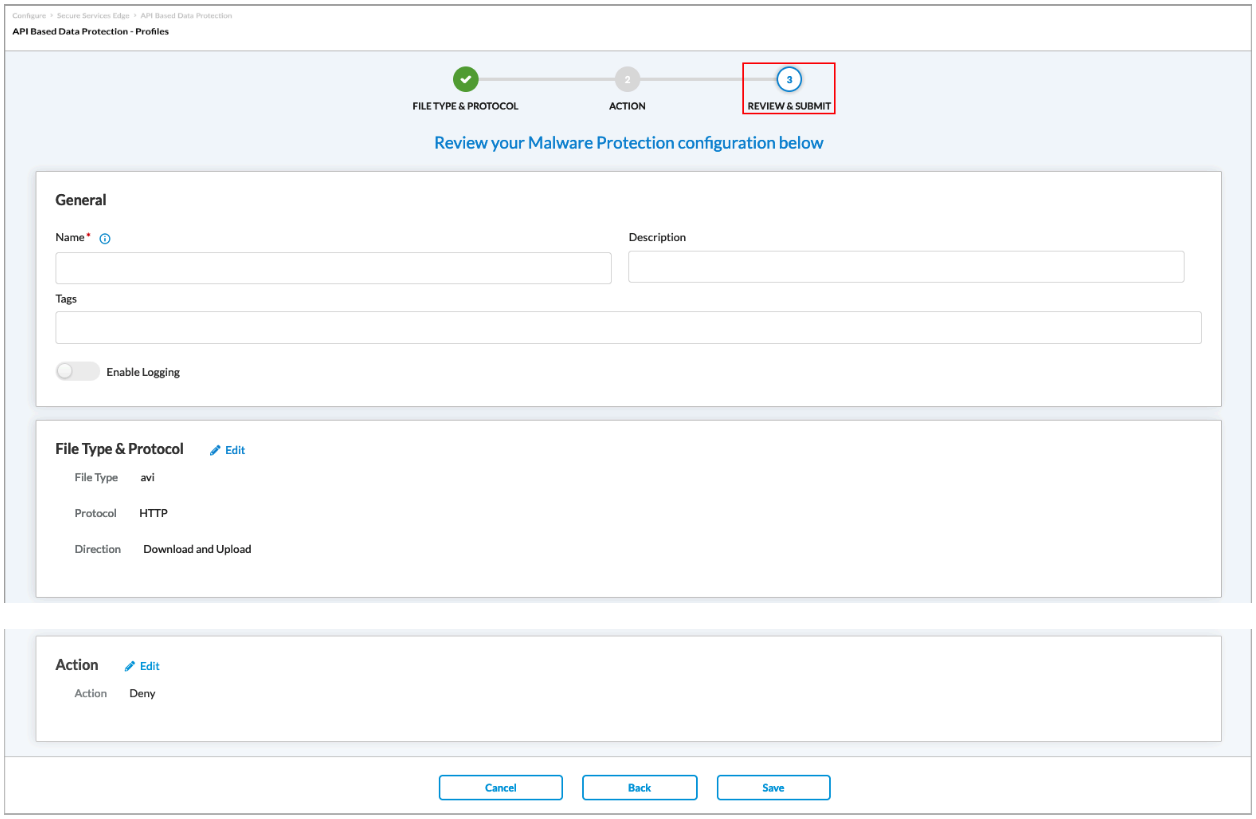
Specifiy the action to enforce when traffic matches the profile.

Action

Deny

8. Select the enforcement action to take when traffic matches the offline malware profile:
    - Alert
    - Allow
    - Deny (default)
    - Recommended Action
    - Reject

    Note that if traffic matches both the Allow and Deny actions, the Deny action takes precedence over the Allow action.
9. Click Next.
10. In the Review and Submit screen, enter a name for the offline malware protection profile and, optionally, 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.


Configure > Secure Services Edge > API Based Data Protection
API Based Data Protection - Profiles
FILE TYPE & PROTOCOL
2
ACTION
3
REVIEW & SUBMIT
Cancel
Back
Save

Review your Malware Protection configuration below

General

Name*

Description

Tags

Enable Logging

File Type & Protocol Edit

File Type avi

Protocol HTTP

Direction Download and Upload

Action Edit

Action Deny

11. Click the Enable Logging slider to send logs to Versa Analytics.

12. Review the remaining entries. To make changes, click the ✎ Edit Edit icon.

13. Click Save to add the malware protection profile.

Supported Software Information

Releases 11.1.1 and later support all content described in this article.

Additional Information

[Configure Custom Malware Protection Profiles](#)
[Configure Profiles](#)