



Configure API-Based Data Protection Policy for IaaS



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

Versa Networks API-based data protection protects and secures organization data that resides in software as a service (SaaS) and infrastructure as a service (IaaS) applications. You create an API data protection policy under a tenant in Concerto to configure API data protection. The policy contains a set of rules, and you can configure event-based rules (based on an event generated by the SaaS or IaaS applications) or schedule-based rules (the rule triggers on a specific date or time). A scheduled-based rule scans the objects at rest (referred to as a retro scan).

Each rule contains two parts. The first part of the rule categorizes the SaaS or IaaS object on which to apply the policy. The second part defines the actions to take on the SaaS or IaaS objects that match the rules.

This article describes how to create event-based and schedule-based API data protection policy rules for IaaS.

Configure an Event-Based IaaS API Data Protection Policy Rule

1. Go to Configure > Secure Service Edge > API-Based Data Protection > Policy Rules.

The screenshot shows the VERSA Networks ACME interface. The left sidebar has a blue header with the VERSA logo and 'ACME'. Below it are several sections: View, Configure, Deploy, Analytics, Inventory, Users, Global Settings, and Tenants. Under 'Configure', 'Secure Services Edge' is selected, and 'API Based Data Protection' is highlighted. The main content area is titled 'API Based Data Protection' and contains the following steps:

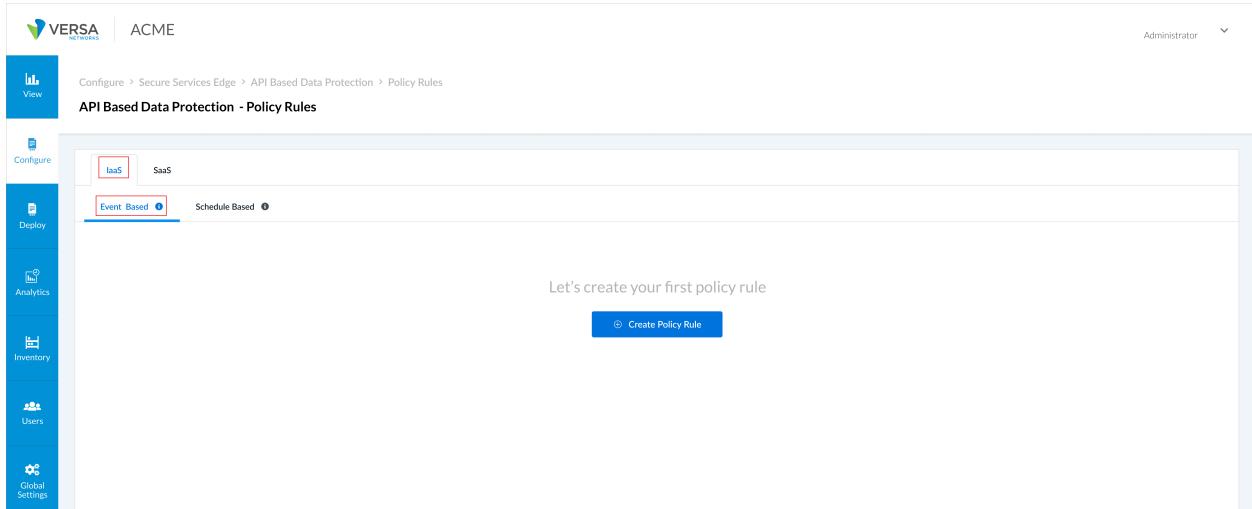
- Start creating your API Based Data Protection Policy Rule / Job**: A note says this section will guide you with creating your first API Based Data Protection Rule. It mentions setting up Software as a Service (SaaS) and Infrastructure as a Service (IaaS) instances.
- BEFORE**: A note states that Software as a Service (SaaS) and Infrastructure as a Service (IaaS) instances need to be defined before creating the API Based Data Protection Policy. A button 'Configure SaaS & IaaS Instances' is shown.
- DURING**: A note says we've preselected the API Based Data Protection Rule settings for you. There are five steps listed below: Provider, Objects of interest, Users & User Groups, Schedule, Choose an Action, Notification, and Review & Deploy. The 'IaaS' tab is selected in the top navigation bar.
- AFTER**: Once you've setup your API Data Protection Policy, you'll be able to:
 - View rules
 - Add additional rules
 - View rule visualizations

1. Select 'Secure Services Edge' from the left sidebar, then 'API Based Data Protection' under 'Configure'.
2. Select IaaS, and then click 'Configure Policy Rules/Jobs'. The API-Based Data Protection - Policy Rules screen displays.

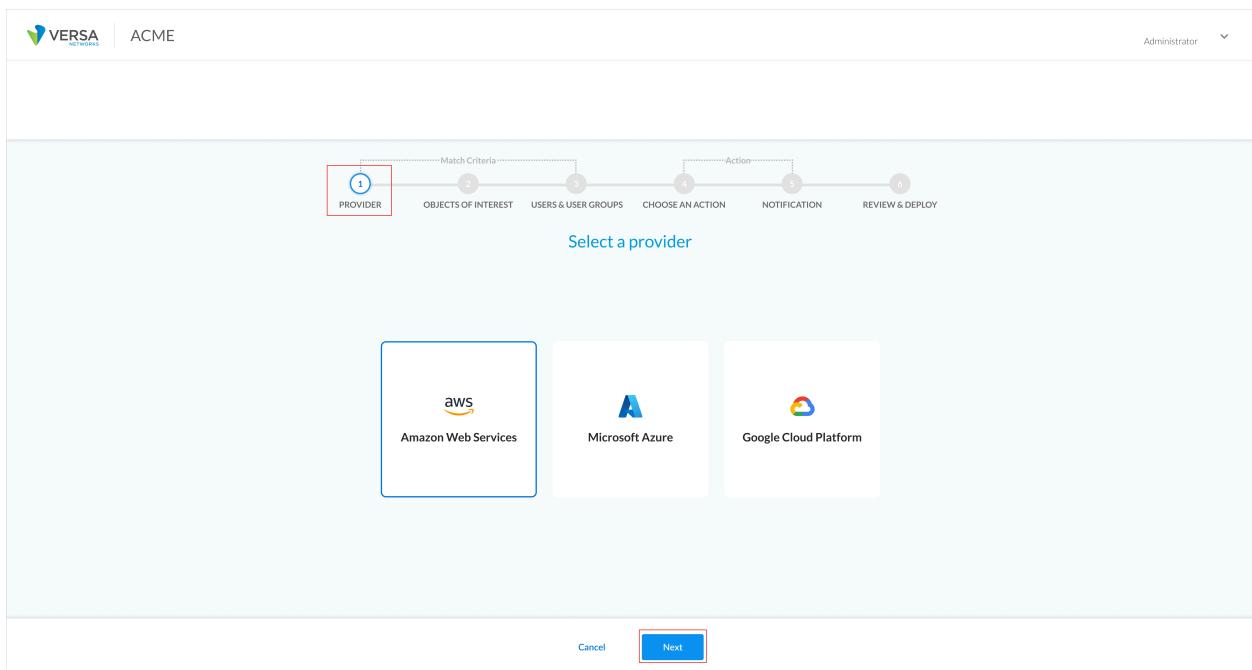
[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_API-Based_Data_P...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_API-Based_Data_P...)

Updated: Wed, 23 Oct 2024 08:36:36 GMT

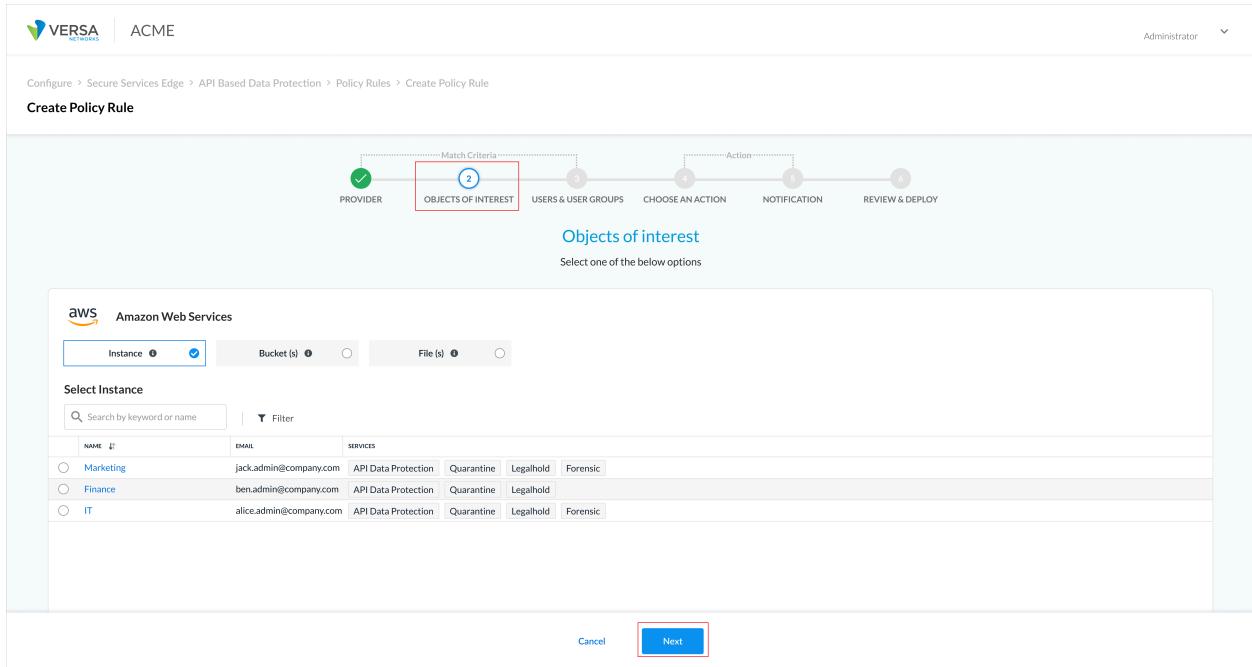
Copyright © 2024, Versa Networks, Inc.



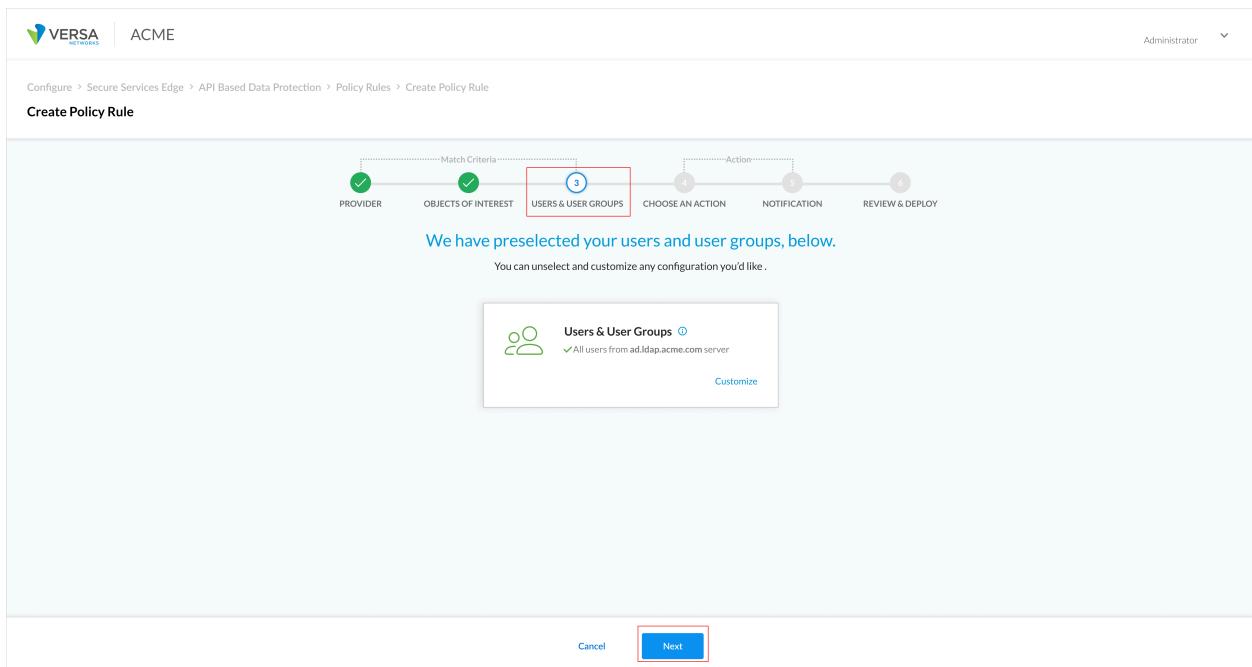
3. Select the Event-Based tab and click Create Rule Policy. The Create Policy Rule screen displays.



4. Go to Step 1, Provider. Select the IaaS provider for which to apply the rule.
5. Click Next to go to Step 2, Objects of Interest. Select the objects of interest for the IaaS provider—instance, buckets, or files.



6. Click Next to go to Step 3, User and User Groups. Select the users or user groups to match the policy.

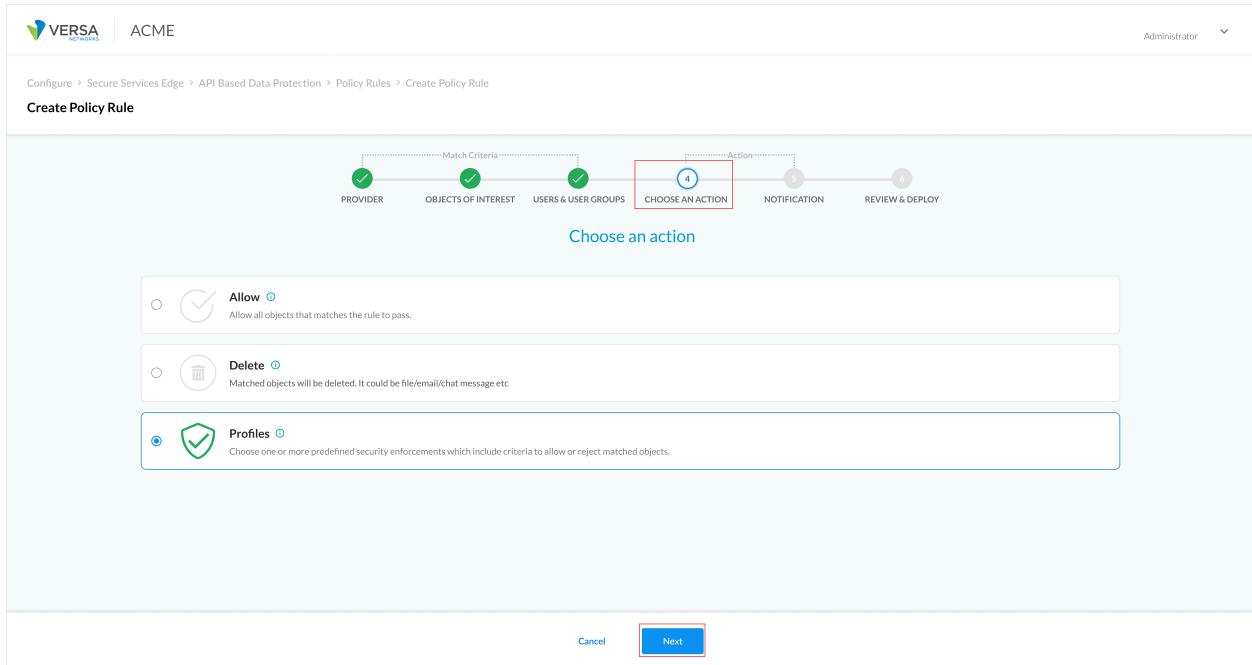


7. Click Next to go to Step 4, Choose an Action. Select an appropriate action to assign security policy profiles, allow list, and disallow list. To use offline DLP, malware, and advanced threat protection (ATP) profiles, select Profiles.

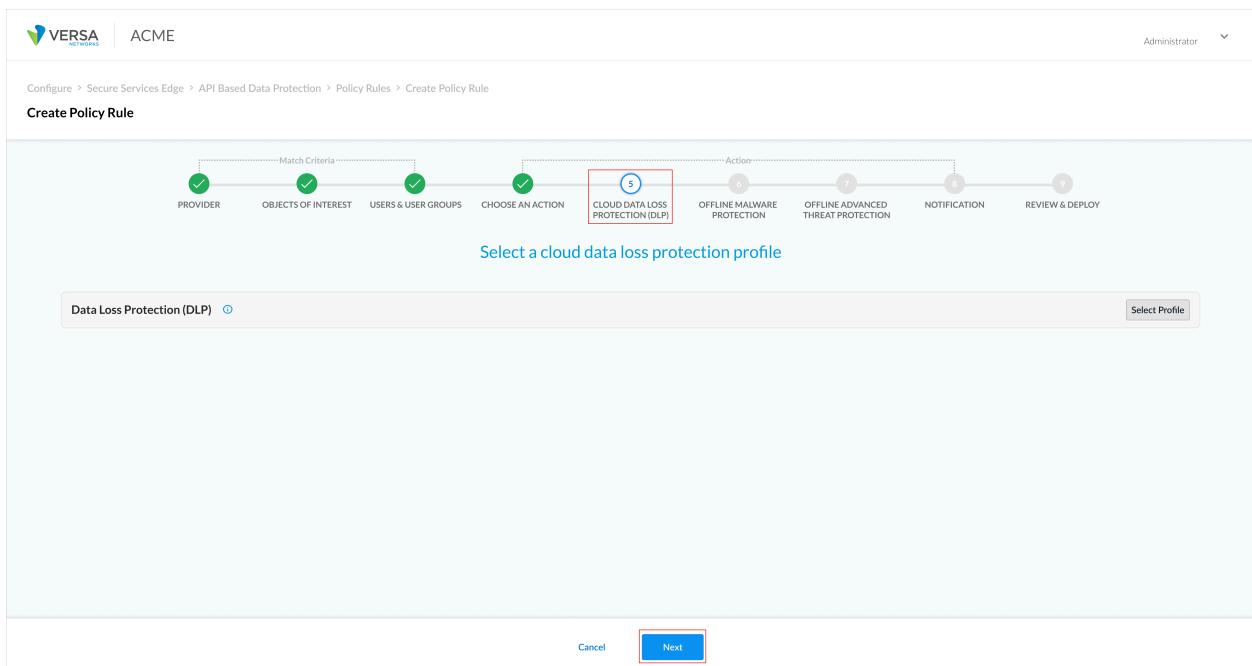
[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_API-Based_Data_P...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_API-Based_Data_P...)

Updated: Wed, 23 Oct 2024 08:36:36 GMT

Copyright © 2024, Versa Networks, Inc.



8. Click Next to go to Step 5, Offline Data Loss Protection (DLP).



9. Click Select Profile. The Data Loss Protection (DLP) Profiles screen displays.

Data Loss Protection (DLP) Profiles

PROFILE NAME	RULES	EXIT	DEFAULT ACTION
ACME-GDPR-USAUK-DLP-Profile	2	On first rule match	Allow
ACME-PCIDSS-GLBA-DLP-Profile	2	On first rule match	Allow
AMCE-Financial-DLP-Profile	5	On first rule match	Allow

Cancel Done

10. Select a DLP profile. To add a profile, click + Add Profile. For more information, see [Configure Offline Data Loss Prevention](#).
11. Click Done.
12. Click Next to go to Step 6, Offline Malware Protection.

VERSA Networks ACME

Administrator

Configure > Secure Services Edge > API Based Data Protection > Policy Rules > Create Policy Rule

Create Policy Rule

Select a offline malware protection profile

Offline Malware Protection Select Profile

Cancel Next

13. Click Select Profile. The Offline Malware Protection Profile screen displays.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_API-Based_Data_P...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_API-Based_Data_P...)
 Updated: Wed, 23 Oct 2024 08:36:36 GMT
 Copyright © 2024, Versa Networks, Inc.

The screenshot shows a table with columns: PROFILE NAME, DEFAULT ACTION, DIRECTION, FILE TYPE, and PROTOCOL. There is one row selected, labeled 'S3 Malware Protection' with a Block action, Both direction, Any file type, and HTTPS protocol.

PROFILE NAME	DEFAULT ACTION	DIRECTION	FILE TYPE	PROTOCOL
S3 Malware Protection	Block	Both	Any	HTTPS

14. Select a malware profile. To add a profile, click + Add Profile. For more information, see [Configure Offline Custom Malware Protection Profiles](#).
15. Click Done.
16. Click Next to go to Step 7, Offline Advanced Threat Protection.

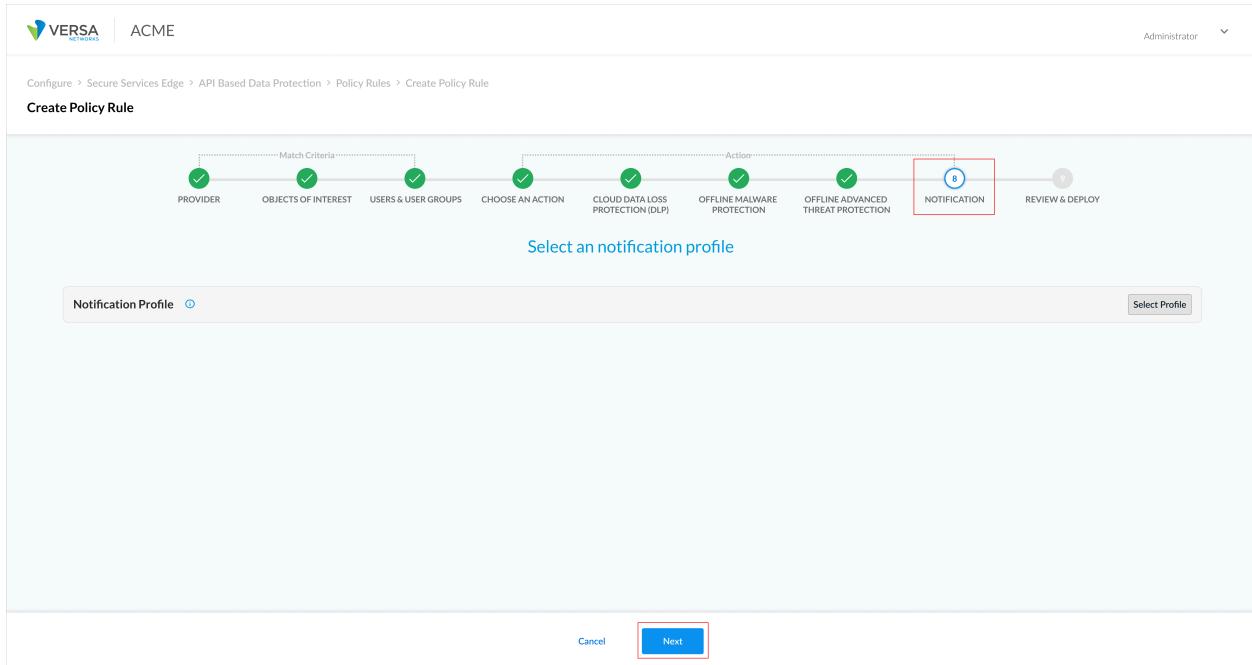
The screenshot shows a flow diagram with steps: PROVIDER, OBJECTS OF INTEREST, USERS & USER GROUPS, CHOOSE AN ACTION, CLOUD DATA LOSS PROTECTION (DLP), OFFLINE MALWARE PROTECTION, OFFLINE ADVANCED THREAT PROTECTION (highlighted with a red box), NOTIFICATION, and REVIEW & DEPLOY. Below the steps, a dropdown menu displays 'Offline Advanced threat protection (Cloud Malware Sandbox with Multi A/V and AI M/L)' with a 'Select Profile' button.

17. Click Select Profile. The Offline Advanced Threat Protection Profiles (Cloud Malware Sandbox with Multi A/V and AI M/L) screen displays.

PROFILE NAME	ACTION	NO. OF ATP BASED ACTION RULES	ATP BASED ACTION RULES
<input checked="" type="radio"/> Block all malicious scans [edit]	Block	3	My ATP Based Action 1, My ATP Based Action 2, My ATP Based Action 3
<input type="radio"/> Wait to block suspicious scans [edit]	Alerted	3	My ATP Based Action 1, My ATP Based Action 2, My ATP Based Action 2
<input type="radio"/> Allow all clean files [edit]	Allow	3	My ATP Based Action 1, My ATP Based Action 2, My ATP Based Action 4

Cancel Done

18. Select an ATP profile. To add a profile, click + Add Profile. For more information, see [Configure Offline Advanced Threat Protection](#).
19. Click Done.
20. Click Next to go to Step 8, Notification. You can use a notification profile to send logs to Versa Analytics.



21. Click Select Profile. The Notification Profiles screen displays.

The "Notification Profile" screen displays the following profiles:

PROFILE NAME	Notify Type	Recipients
<input checked="" type="radio"/> ATP notification Default	Do not notify	-
<input type="radio"/> CASB notification	Notify once every 30 Minutes	3
<input type="radio"/> DLP notification	Notify after each event	2

Buttons at the bottom include "Cancel", "Done", and a red-bordered "+ Add profile" button.

22. Select a notification profile. To add a profile, click + Add Profile. Enter the following information in the Create Notification Profile screen.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_API-Based_Data_P...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_API-Based_Data_P...)

Updated: Wed, 23 Oct 2024 08:36:36 GMT

Copyright © 2024, Versa Networks, Inc.

Notification Profile

Profile Name: API DP - Hourly

How often would you like to notify people?

Do not notify Notify once every Hours: 1 Notify after each event

Email Template: API Data Protection Default

Recipients

tom@company.com

23. In the Profile Name field, enter a notification profile name to use for Analytics.
24. Select the option to notify for Analytics - Do not notify, Notify once every (select the duration), or Notify after each event.
 - a. If you select to notify, select the duration.
 - b. Select an email template for notifications. Click Create New to add an email template.
 - c. Under Recipients, enter the email addresses to receive notifications and click Add.
 - d. Click Done.
25. Click Next to go to Step 9, Review and Deploy. Click Edit next to any section to make changes.

VERSAs | ACME

Administrator ▾

Configure > Secure Services Edge > API Based Data Protection > Policy Rules > Create Policy Rule

Create Policy Rule

Review your API Based Data Protection - IaaS Policy Rules configurations below:

Below are the configurations of your rule. Review and edit any step of your configuration before deploying.

GENERAL

Rule Name	Description ⓘ
AWS COMPANY UK Branches	UK Branches only

Rule is enabled

Provider ⓘ Edit

Provider Amazon Web Services

Object of interest: Multiple Files ⓘ Edit

Instance COMPANY Marketing
Bucket Bucket 1

Files

NAME ⓘ	SIZE	TYPE
file 1.txt ⓘ	1 KB	text/plain
file 2.txt ⓘ	1 KB	text/plain
log.tmp ⓘ	1 KB	application/octet-stream

Users & User Groups ⓘ Edit

Schedule ⓘ Edit

Scan Type	Every	On	Start Date	Start Time	End Date
Weekly	1 week	Monday, Friday	2023/01/29	0900	2023/06/29

Actions ⓘ Edit

Data Loss Prevention (DLP) ⓘ

PROFILE NAME	RULES	EXIT	DEFAULT ACTION
ACME-GDPR-USAUK-DLP-Profile	2	On first rule match	Allow

ORDER	RULE NAME	OBJECT OF INTEREST	ACTIVITIES	CONTEXT	PROTOCOL	FILETYPE
1	ACME-GDPR-USA-DLP-Rule	Content Analysis: Payment Card Industry Data Security Standard (PCI-DSS)	Allow	Body	HTTP	Doc, docx
2	ACME-GDPR-UK-DLP-Rule	Content Analysis: Payment Card Industry Data Security Standard (PCI-DSS)	Allow	Body	HTTP	Doc, docx

Malware Protection ⓘ

PROFILE NAME	DEFINITION ACTION	DIRECTION	FILETYPE	PROTOCOL
S3 Malware Protection ⓘ	Blocked	Both	Any	HTTPS

Advanced threat protection (Cloud Malware Sandbox with Multi A/V and AI M/L) ⓘ

PROFILE NAME	ACTION	NO OF ATP BASED ACTION RULES	FILETYPE
Block all malicious scans ⓘ	Blocked	Blocked	7zip, exe, exe64, src, dll64, dll, osx, sys

Notification ⓘ Edit

How often would you like to notify people?
None

Commit & Deploy

26. Click Commit and Deploy.

Configure a Schedule-Based IaaS API Data Protection Policy Rule

1. Go to Configure > Secure Service Edge > API Based Data Protection > Policy Rules.

The screenshot shows the Versa Networks interface for configuring an API Based Data Protection Policy Rule. The left sidebar navigation includes: View, Secure Services Edge (selected), Secure SD-WAN, Configure, Deploy (with API Based Data Protection selected), Analytics, Inventory, Users, Global Settings, and Tenants. The main content area is titled "API Based Data Protection" and displays a "Start creating your API Based Data Protection Policy Rule / Job". It includes sections for "BEFORE" (informing about SaaS & IaaS instances setup), "DURING" (a five-step configuration process: Provider, Objects of interest, Users & User Groups, Schedule, Choose an Action, and Notification), and "AFTER" (a list of actions like View rules, Add additional rules, and View rule visualizations). A large gear icon is present on the right side of the configuration steps.

2. Select IaaS, and then click Configure Policy Rules/Jobs. The following screen displays.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_API-Based_Data_P...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_API-Based_Data_P...)

Updated: Wed, 23 Oct 2024 08:36:36 GMT

Copyright © 2024, Versa Networks, Inc.

VERSACLOUD
ACME

Configure > Secure Services Edge > API Based Data Protection > Jobs

API Based Data Protection - Jobs

IaaS SaaS

Event Based Schedule Based

Let's create your first job

Create Job

3. Select IaaS, select the Schedule-Based tab, and then click Create a Job. The Create Job screen displays.

VERSACLOUD
ACME

Configure > Secure Services Edge > API Based Data Protection > Jobs > Create Job

Create Job

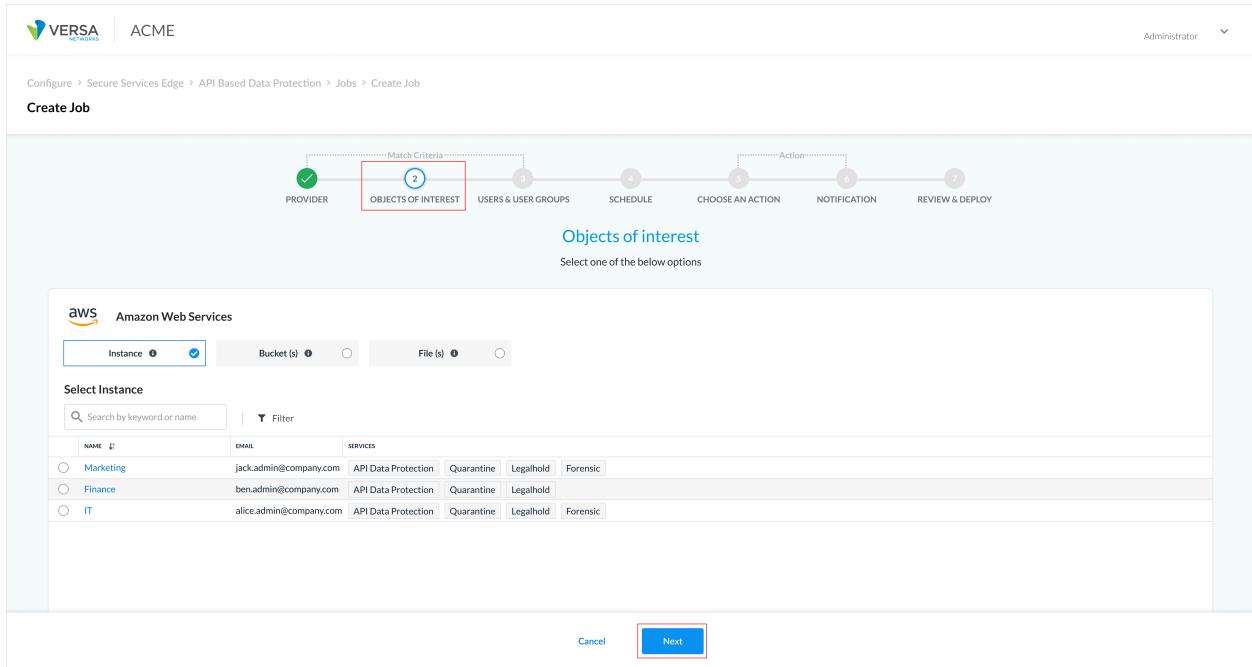
1 PROVIDER 2 OBJECTS OF INTEREST 3 USERS & USER GROUPS 4 SCHEDULE 5 CHOOSE AN ACTION 6 NOTIFICATION 7 REVIEW & DEPLOY

Select a provider

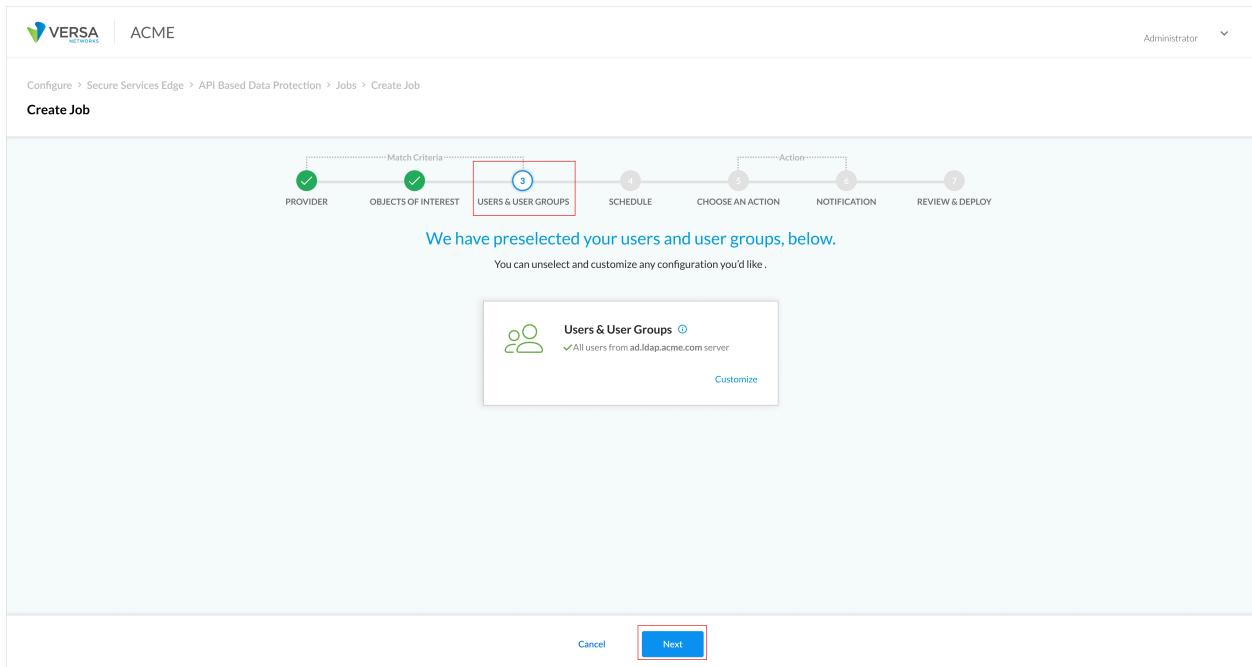
AWS Amazon Web Services Microsoft Azure Google Cloud Platform

Cancel Next

4. Go to Step 1, Provider. Select the IaaS provider for which to apply the rule.
5. Click Next to go to Step 2, Objects of Interest. Select the objects of interest for the IaaS provider—Instance, buckets, or files.



6. Click Next to go to Step 3, User and User Groups. Select the users or user groups to match the policy.



7. Click Next to go to Step 4, Schedule. You can select the scan frequency options - Now, Non-Recurring Time, Hourly, Daily, Weekly, Monthly.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_API-Based_Data_P...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_API-Based_Data_P...)

Updated: Wed, 23 Oct 2024 08:36:36 GMT

Copyright © 2024, Versa Networks, Inc.

Configure > Secure Services Edge > API Based Data Protection > Jobs > Create Job

Create Job

Match Criteria

SCHEDULE

Action

CHOOSE AN ACTION

NOTIFICATION

REVIEW & DEPLOY

Select schedule

Schedule (1)

Which scan type would you like to choose?

Now Non-Recurring Time Hourly Daily Weekly Monthly

Start Time: Select Options

Start Date: yyyy/mm/dd

End Date: yyyy/mm/dd

Cancel Next

- Click Next to go to Step 5, Choose an Action. Select an appropriate action to assign security policy profiles, allow list, and disallow list. To use offline DLP, malware, and ATP profiles, select Profiles.

Configure > Secure Services Edge > API Based Data Protection > Jobs > Create Job

Create Job

Match Criteria

SCHEDULE

CHOOSE AN ACTION

NOTIFICATION

REVIEW & DEPLOY

Choose an action

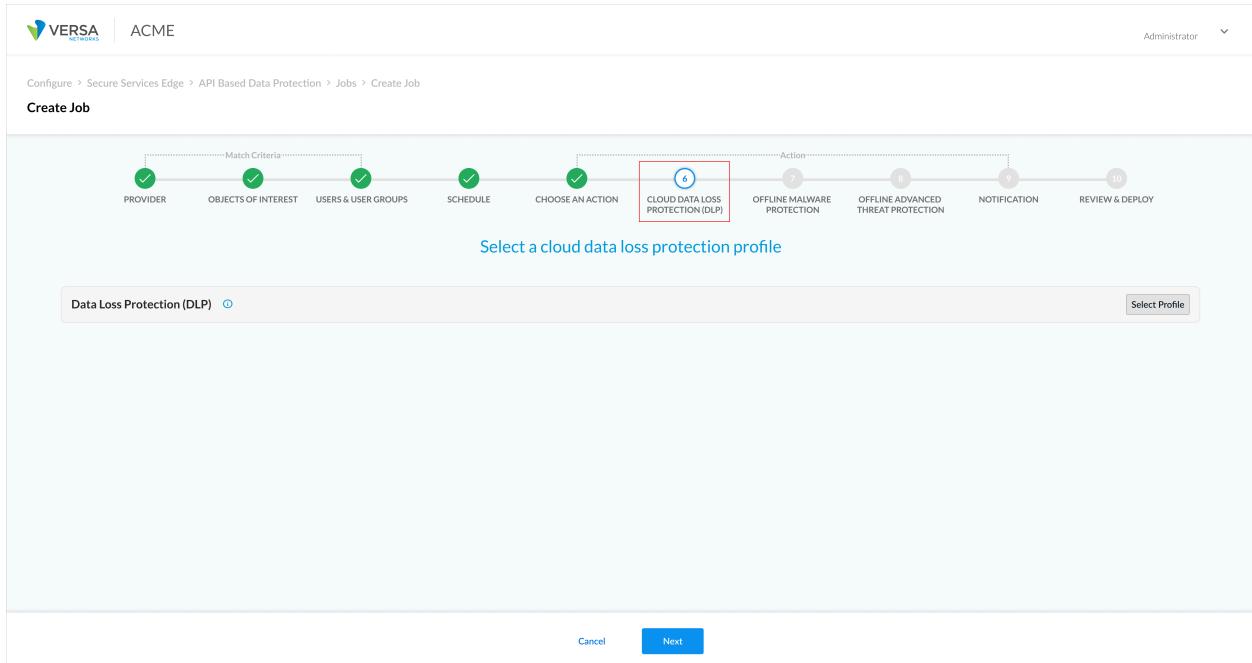
Allow (1)
Allow all objects that matches the rule to pass.

Delete (1)
Matched objects will be deleted. It could be file/email/chat message etc.

Profiles (1)
Choose one or more predefined security enforcements which include criteria to allow or reject matched objects.

Cancel Next

- Click Next to go to Step 6, Offline Data Loss Protection (DLP) Profile.



10. Click Select Profile. The Data Loss Protection (DLP) Profiles screen displays.

Data Loss Protection (DLP) Profiles					
Search by keyword or name		Filter	+ Add profile		
PROFILE NAME	RULES	EXIT	DEFAULT ACTION		
<input checked="" type="radio"/> ACME-GDPR-USAUK-DLP-Profile	2	On first rule match	Allow		
1 ACME-GDPR-USA-DLP-Rule	Content Analysis: Payment Card Industry Data Security Standard (PCI-DSS)	Allow	Body	HTTP	Doc, docx
2 ACME-GDPR-UK-DLP-Rule	Content Analysis: Payment Card Industry Data Security Standard (PCI-DSS)	Allow	Body	HTTP	Doc, docx
<input type="radio"/> ACME-PCIDSS-GLBA-DLP-Profile	2	On first rule match	Allow		
<input type="radio"/> AMCE-Financial-DLP-Profile	5	On first rule match	Allow		

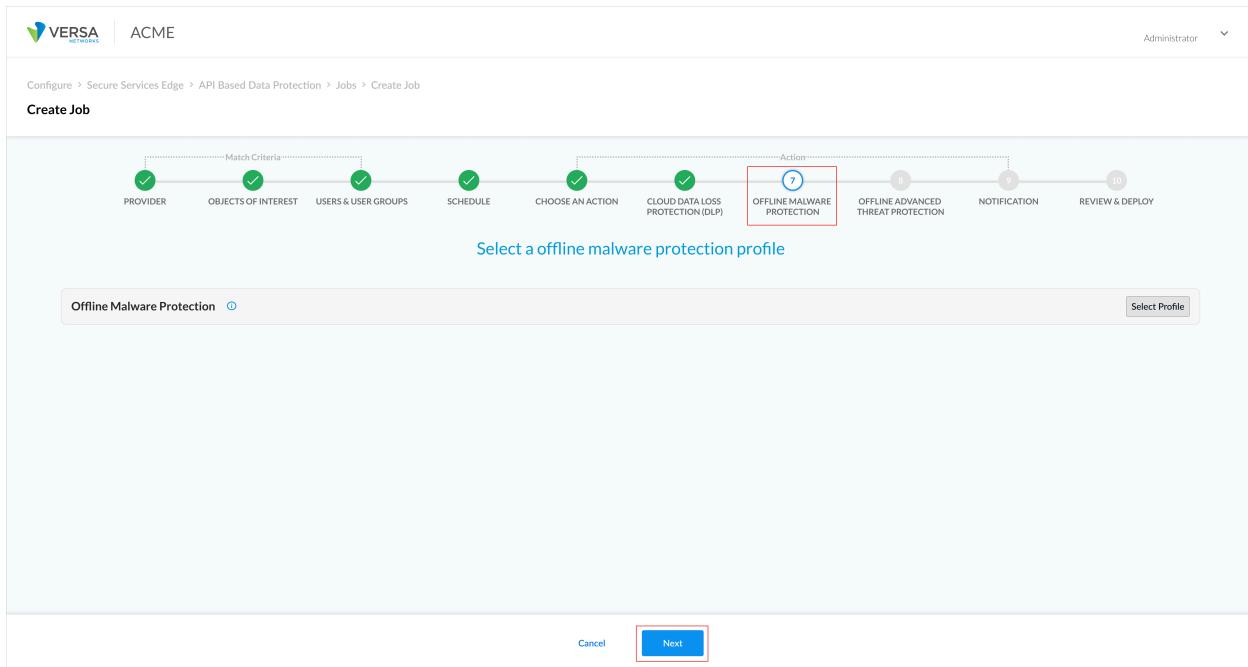
Cancel Done

11. Select a DLP profile. To add a profile, click + Add Profile. For more information, see [Configure Offline Data Loss Prevention](#).
12. Click Done.
13. Click Next to go to Step 7, Offline Malware Protection.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_API-Based_Data_P...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_API-Based_Data_P...)

Updated: Wed, 23 Oct 2024 08:36:36 GMT

Copyright © 2024, Versa Networks, Inc.



14. Click Select Profile. The Offline Malware Protection Profile screen displays.

PROFILE NAME	DEFUALT ACTION	DIRECTION	FILETYPE	PROTOCOL
S3 Malware Protection	Block	Both	Any	HTTPS

Cancel Done

15. Select a malware profile. To add a profile, click + Add Profile. For more information, see [Configure Offline Custom Malware Protection Profiles](#).

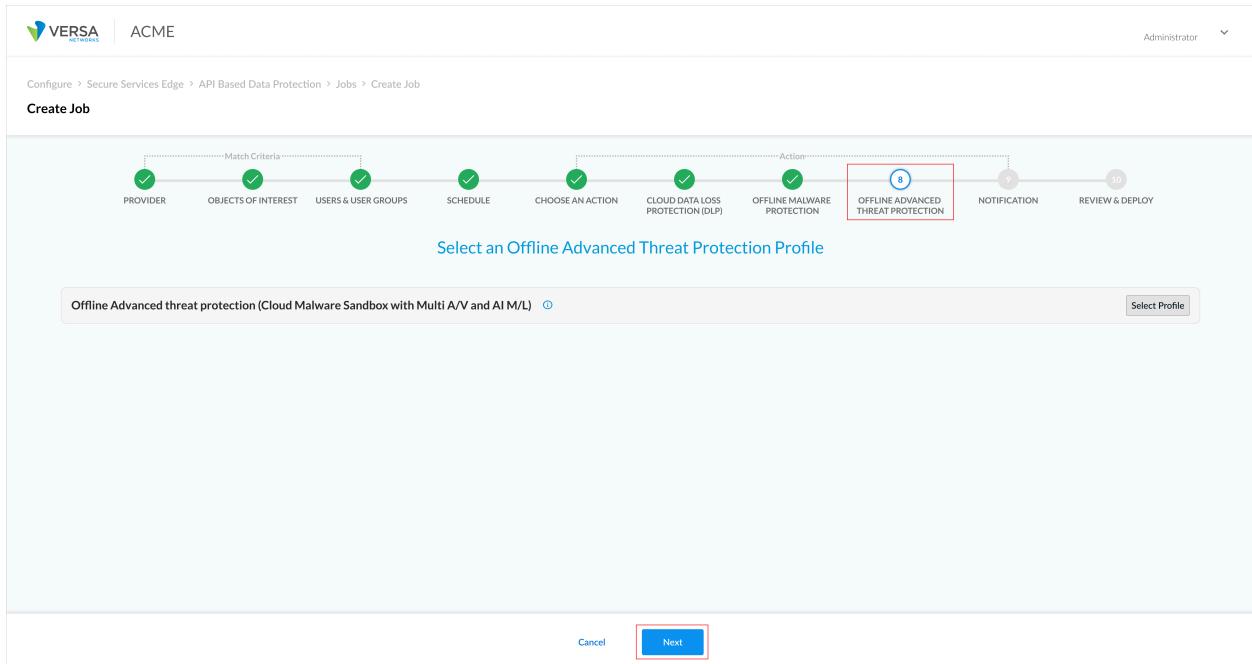
16. Click Done.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_API-Based_Data_P...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_API-Based_Data_P...)

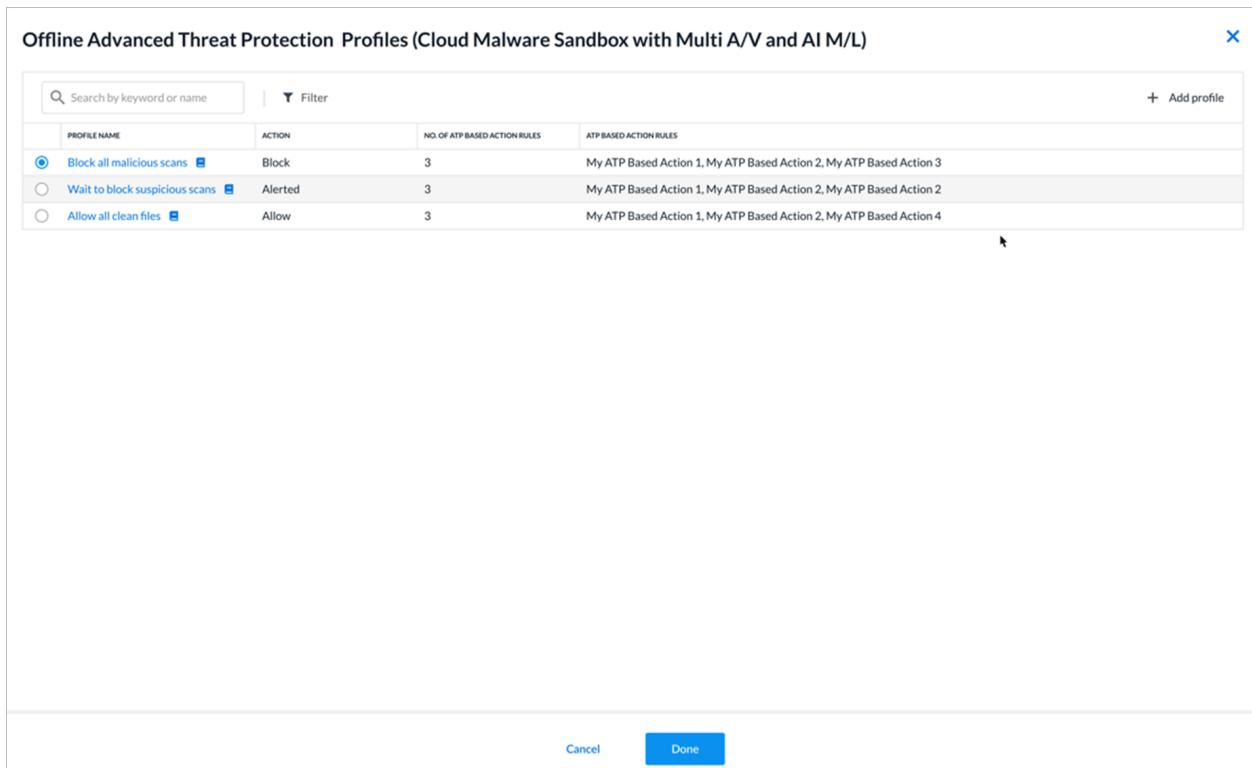
Updated: Wed, 23 Oct 2024 08:36:36 GMT

Copyright © 2024, Versa Networks, Inc.

17. Click Next to go to Step 8, Offline Advanced Threat Protection (ATP).



18. Click Select Profile. The Offline Advanced Threat Protection Profiles (Cloud Malware Sandbox with Multi A/V and AI M/L) screen displays.



19. Select an ATP profile. To add a profile, click + Add Profile. For more information, see [Configure Offline Advanced](#)

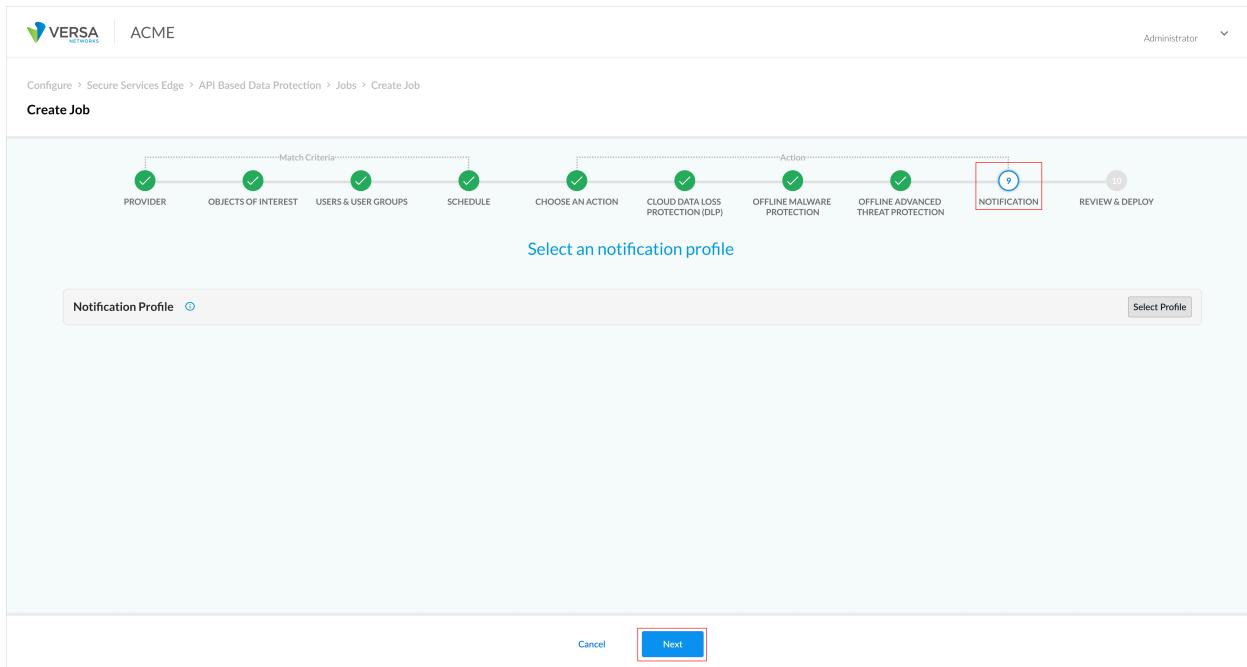
[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_API-Based_Data_P...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_API-Based_Data_P...)

Updated: Wed, 23 Oct 2024 08:36:36 GMT

Copyright © 2024, Versa Networks, Inc.

Threat Protection.

20. Click Done.
21. Click Next to go to Step 9, Notification. You can use a notification profile to send logs to Versa Analytics.



22. Click Select Profile. The Notification Profiles screen displays.

The screenshot shows the 'Notification Profile' dialog box. It lists three profiles:

- ATP notification Default (selected, Do not notify)
- CASB notification (Notify once every 30 Minutes, 3 recipients)
- DLP notification (Notify after each event, 2 recipients)

A red box highlights the '+ Add profile' button. At the bottom are 'Cancel' and 'Done' buttons.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_API-Based_Data_P...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_API-Based_Data_P...)

Updated: Wed, 23 Oct 2024 08:36:36 GMT

Copyright © 2024, Versa Networks, Inc.

23. Select a notification profile. To add a profile, click + Add Profile. Enter the following information in the Create Notification Profile screen.

The screenshot shows the 'Notification Profile' configuration screen. The 'Profile Name' field contains 'API DP - Hourly'. Under 'How often would you like to notify people?', the 'Notify once every' option is selected, with 'Hours' set to 1. In the 'Email' section, the 'Email Template' dropdown is set to 'API Data Protection Default' and includes options for 'Create New', 'CASB email template', and 'DLP email template'. The 'Recipients' panel on the right shows an email address 'tom@company.com' listed with a delete icon. At the bottom are 'Cancel' and 'Done' buttons.

24. In the Profile Name field, enter a notification profile name to use for Analytics.
25. Select the option to notify for Analytics - Do not notify, Notify once every (select the duration), or Notify after each event.
- If you select to notify, select the duration.
 - Select an email template for notifications. Click Create New to add an email template.
 - Under Recipients, enter the email addresses to receive notifications and click Add
 - Click Done.
26. Click Next to go to Step 10, Review and Deploy. Click Edit next to any section to make changes.

VERSAs | ACME

Administrator ▾

Configure > Secure Services Edge > API Based Data Protection > Policy Rules > Create Policy Rule

Create Policy Rule

Match Criteria

Provider: PROVIDER

Objects of Interest: OBJECTS OF INTEREST

Users & User Groups: USERS & USER GROUPS

Choose an Action: CHOOSE AN ACTION

Action: DATA LOSS PREVENTION (DLP), MALWARE PROTECTION, ADVANCED THREAT PROTECTION, NOTIFICATION

Review your API Based Data Protection - IaaS Policy Rules configurations below:

Below are the configurations of your rule. Review and edit any step of your configuration before deploying.

GENERAL

Rule Name: AWS COMPANY UK Branches

Description: UK Branches only

Rule is enabled

Provider [Edit](#)

Provider: Amazon Web Services

Object of interest: Multiple Files [Edit](#)

Instance: COMPANY Marketing

Bucket: Bucket 1

NAME	SIZE	TYPE
file 1.txt	1 KB	text/plain
file 2.txt	1 KB	text/plain
log.tmp	1 KB	application/octet-stream

Users & User Groups [Edit](#)

Schedule [Edit](#)

Scan Type	Every	On	Start Date	Start Time	End Date
Weekly	1 week	Monday, Friday	2023/01/29	0900	2023/06/29

Actions [Edit](#)

Data Loss Prevention (DLP) [Edit](#)

PROFILE NAME	RULES	EXIT	DEFAULT ACTION		
ACME-GDPR-USAUK-DLP-Profile	2	On first rule match	Allow		
ACME-GDPR-USA-DLP-Rule	Content Analysis: Payment Card Industry Data Security Standard (PCI-DSS)	Allow	Body	HTTP	Doc, docx
ACME-GDPR-UK-DLP-Rule	Content Analysis: Payment Card Industry Data Security Standard (PCI-DSS)	Allow	Body	HTTP	Doc, docx

Malware Protection [Edit](#)

PROFILE NAME	DEFINITION ACTION	DIRECTION	FILE TYPE	PROTOCOL
S3 Malware Protection	Blocked	Both	Any	HTTPS

Advanced threat protection (Cloud Malware Sandbox with Multi A/V and AI M/L) [Edit](#)

PROFILE NAME	ACTION	NO OF ATP BASED ACTION RULES	FILE TYPE
Block all malicious scans	Blocked	Blocked	7zip, exe, exe64, src, dll64, dll, osx, sys

Notification [Edit](#)

How often would you like to notify people?
None

27. Click Commit and Deploy.

Supported Software Information

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

Additional Information

[Configure API-Based Data Protection Policy for SaaS](#)

[Configure Cloud Applications to use with API-Based Data Protection](#)

[Configure Offline Advanced Threat Protection](#)

[Configure Offline Custom Malware Protection Profiles](#)

[Configure Offline Data Loss Prevention](#)