



Configure API-Based Data Protection Policy for SaaS



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 SaaS.

Configure an Event-Based SaaS API Data Protection Policy Rule

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

- Select SaaS, 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 08:40:17 GMT

Copyright © 2024, Versa Networks, Inc.

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

4. Go to Step 1, SaaS Application screen. Select the SaaS application for which to apply the rule.
5. Click Next to go to Step 2, Instances. Select the instances of the SaaS application(s). To add an instance, click + Add Instance.

Select Instance Selected Files: 1 out of 3

NAME	APPLICATION	ADMIN EMAIL	SERVICES
<input checked="" type="checkbox"/> Marketing	box Box	ben.admin@company.com	API Data Protection Quarantine Legalhold Malware Forensic
<input type="checkbox"/> Finance	box Box	jack.admin@company.com	API Data Protection Quarantine Legalhold Malware Forensic
<input type="checkbox"/> IT	Google Drive	sales.admin@company.com	API Data Protection Malware Forensic

Showing 1 - 3 of 3 entries 10 rows < Previous 1 2 3 4 Next >

Cancel Next

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

We have preselected your users and user groups, below.
You can unselect and customize any configuration you'd like.

Users & User Groups ⓘ
 ✓ All users from ad ldap.acme.com server
Customize

Cancel Next

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 CASB, 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 08:40:17 GMT

Copyright © 2024, Versa Networks, Inc.

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

Create Policy Rule

Match Criteria

- SaaS Application
- INSTANCES
- USERS & USER GROUPS

Action

- CHOOSE AN ACTION
- NOTIFICATION
- REVIEW & DEPLOY

Choose an action

- Allow ⓘ Allow all that matches the rule to pass.
- Delete ⓘ Matched objects will be deleted. It could be file/email/chat message etc
- Profiles ⓘ Choose one or more predefined security enforcements which include criteria to allow or reject matched objects.

Cancel **Next**

8. Click Next to go to Step 5, Offline Cloud Access Security Broker (CASB).

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

Create Policy Rule

Match Criteria

- SaaS Application
- INSTANCES
- USERS & USER GROUPS
- CHOOSE AN ACTION

Action

- OFFLINE CLOUD ACCESS SECURITY BROKER (CASB)
- OFFLINE DATA LOSS PROTECTION (DLP)
- MALWARE PROTECTION
- OFFLINE ADVANCED THREAT PROTECTION
- NOTIFICATION
- REVIEW & DEPLOY

Configure Offline Cloud Access Security Broker (CASB) Profile

On Offline Cloud Access Security Broker (CASB)

PROFILE NAME	RULES	ACTIONS				
ACME Box GoogleDrive	2	<input type="button" value="Select Profile"/> <input type="button" value="Edit"/>				
ORDER	RULE NAME	RULE ACTION	EMAIL PROFILE	RISK LEVEL	PREDEFINED APPLICATIONS	ACTIVITIES
1	Box	Allow	Marketing User	Low	Word Online	Login, Download
2		Allow	Marketing User	Low	Evernote	Login

Cancel **Next**

9. Click Select Profile. The Offline Cloud Access Security Broker (CASB) Profiles screen displays.

Offline Cloud Access Security Broker (CASB) Profiles

PROFILE NAME	RULES				
ACME Box GoogleDrive	2				
Box	Allow	Marketing User	Low	Word Online	Login, Download
Google Drive	Allow	Marketing User	Low	Evernote	Login
ACME Amazon aws	2	On first rule match	Allow		
ACME Outlook	5	On first rule match	Allow		

Cancel **Done**

10. Select a CASB profile. To add a profile, click + Add Profile.
11. Click Done.
12. Click Next to go to Step 6, Offline Data Loss Protection (DLP).

ACME

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

Create Policy Rule

Select a cloud data loss protection profile

Data Loss Protection (DLP)

Select Profile

Cancel

13. Click Select Profile. The Data Loss Protection (DLP) Profiles 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 08:40:17 GMT
 Copyright © 2024, Versa Networks, Inc.

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

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

VERSA Networks ACME

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

Create Policy Rule

Match Criteria

- SaaS Application
- Instances
- Users & User Groups

Action

- OFFLINE CLOUD ACCESS SECURITY BROKER (CASB)
- OFFLINE DATA LOSS PROTECTION (DLP)
- MALWARE PROTECTION (7)
- OFFLINE ADVANCED THREAT PROTECTION
- NOTIFICATION
- REVIEW & DEPLOY

Select an Offline Malware Protection Profile

Malware Protection (7) Select Profile

Cancel Next

17. 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 08:40:17 GMT
 Copyright © 2024, Versa Networks, Inc.

The screenshot shows a table with columns: PROFILE NAME, DEFAULT ACTION, DIRECTION, FILE TYPE, and PROTOCOL. One row is selected, showing:

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

Buttons at the bottom include 'Cancel' and 'Done'.

18. Select a malware profile. To add a profile, click + Add Profile. For more information, see [Configure Offline Custom Malware Protection Profiles](#).
19. Click Done.
20. Click Next to go to Step 8, Offline Advanced Threat Protection.

The screenshot shows a 'Create Policy Rule' interface. The 'Action' section includes steps: OFFLINE CLOUD ACCESS SECURITY BROKER (CASB), OFFLINE DATA LOSS PROTECTION (DLP), MALWARE PROTECTION, and OFFLINE ADVANCED THREAT PROTECTION (highlighted with a red box). A dropdown menu for 'Select an Offline Advanced Threat Protection Profile' lists 'Advanced threat protection (Cloud Malware Sandbox with Multi A/V and AI M/L)'.

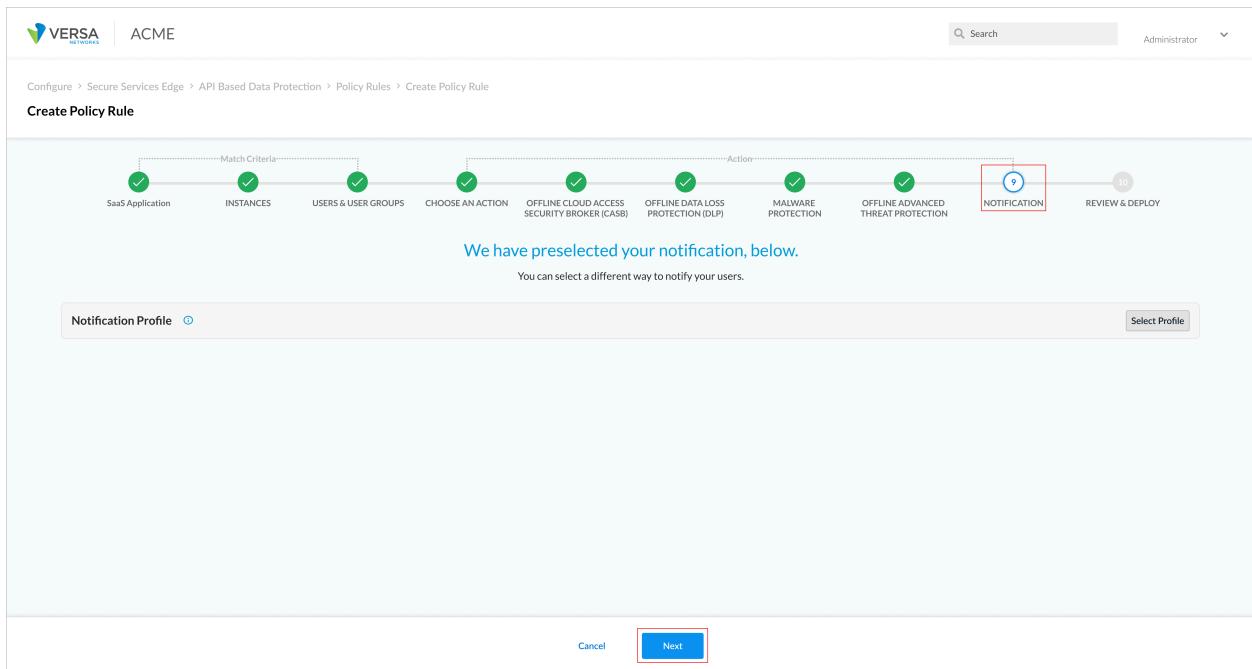
21. Click Select Profile. The Offline Advanced Threat Protection Profiles (Cloud Malware Sandbox with Multi A/V and AI M/L) screen displays.

The screenshot shows a dialog box titled "Offline Advanced Threat Protection Profiles (Cloud Malware Sandbox with Multi A/V and AI M/L)". At the top right is a close button (X). Below the title is a search bar labeled "Search by keyword or name" and a filter icon. On the right side, there is a "+ Add profile" button. The main area is a table with four columns: PROFILE NAME, ACTION, NO. OF ATP BASED ACTION RULES, and ATP BASED ACTION RULES. There are three rows:

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

At the bottom left are "Cancel" and "Done" buttons.

22. Select an ATP profile. To add a profile, click + Add Profile. For more information, see [Configure Offline Advanced Threat Protection](#).
23. Click Done.
24. Click Next to go to Step 9, Notification. You can use a notification profile to send logs to Versa Analytics.



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

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

At the top right is a '+ Add profile' button with a red box around it. At the bottom are 'Cancel' and 'Done' buttons.

26. 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 08:40:17 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 Notify after each event

Notify once every: Hours: 1

Email

Email Template: API Data Protection Default

- Create New
- CASB email template
- DLP email template

Recipients

Input Email Address: tom@company.com

Add Delete

Cancel Done

27. In the Profile Name field, enter a notification profile name to use for Analytics.
28. 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.
29. Click Next to go to Step 10, Review and Deploy. Click Edit next to any section to make changes.

30. Click Commit and Deploy.

Configure a Schedule-Based SaaS API Data Protection Policy Rule

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

ACME

Secure Services Edge Secure SD-WAN

View Configure Deploy Analytics Inventory Users Global Settings Tenants

Secure Services Edge > API Based Data Protection

API Based Data Protection - Policy Rules

Start creating your API Based Data Protection Policy Rule / Job

This section will guide you with creating your first API Based Data Protection Rule. Before you begin, you'll need to setup your Software as a Service (SaaS) and Infrastructure as a Service (IaaS) Instances.

BEFORE

Software as a Service (SaaS) and Infrastructure as a Service (IaaS) instances will need to be completed before creating your first rule / Job.

SaaS & IaaS Instances
Software as a Service (SaaS) and Infrastructure as a Service (IaaS) instances need to be defined before creating API Based Data Protection Policy.

Information to guide you

Configure SaaS & IaaS Instances

DURING

We've preselected the API Based Data Protection Rule settings for you. There are five steps which are listed below. Click the Let's Go button to begin.

		Configure Policy Rules / Jobs
<input checked="" type="radio"/>	SaaS Application	
<input checked="" type="radio"/>	Instance	
<input checked="" type="radio"/>	Users & User Groups	
<input checked="" type="radio"/>	Schedule	
<input checked="" type="radio"/>	Choose an Action	
<input checked="" type="radio"/>	Notification	
<input checked="" type="radio"/>	Review & Deploy	

AFTER

Once you've setup your API Data Protection Policy, you'll be able to:

- View rules
- Add additional rules
- View rule visualizations

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

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

- Go to Step 1, SaaS Application. Select the SaaS application for which to apply the rule.
- Click Next to go to Step 2, Instances. Select the instances for the SaaS application(s). To add an instance, click + Add Instance.

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

Create Job

Match Criteria

SaaS Application

INSTANCES

USERS & USER GROUPS

SCHEDULE

CHOOSE AN ACTION

NOTIFICATION

REVIEW & DEPLOY

Select your Instance

Select Instance Selected Files: 1 out of 3

Search by keyword or name Filter

NAME	APPLICATION	ADMIN EMAIL	SERVICES
<input checked="" type="checkbox"/> Marketing	box Box	ben.admin@company.com	API Data Protection Quarantine Legalhold Malware Forensic
<input type="checkbox"/> Finance	box Box	jack.admin@company.com	API Data Protection Quarantine Legalhold Malware Forensic
<input type="checkbox"/> IT	Google Drive	sales.admin@company.com	API Data Protection Malware Forensic

Showing 1 - 3 of 3 entries 10 rows

Cancel Next

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

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

Create Job

Match Criteria

SaaS Application

INSTANCES

USERS & USER GROUPS

SCHEDULE

CHOOSE AN ACTION

NOTIFICATION

REVIEW & DEPLOY

We have preselected your users and user groups, below.

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

Customize

Cancel Next

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

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

Create Job

Match Criteria

- SaaS Application (Green checkmark)
- INSTANCES (Green checkmark)
- USERS & USER GROUPS (Green checkmark)
- SCHEDULE** (Red box)
- CHOOSE AN ACTION
- NOTIFICATION
- REVIEW & DEPLOY

Select schedule

Schedule 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** (Red box)

- 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 CASB, DLP, malware, and ATP profiles, select Profiles.

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

Create Job

Match Criteria

- SaaS Application (Green checkmark)
- INSTANCES (Green checkmark)
- USERS & USER GROUPS (Green checkmark)
- SCHEDULE
- CHOOSE AN ACTION** (Red box)
- NOTIFICATION
- REVIEW & DEPLOY

Choose an action

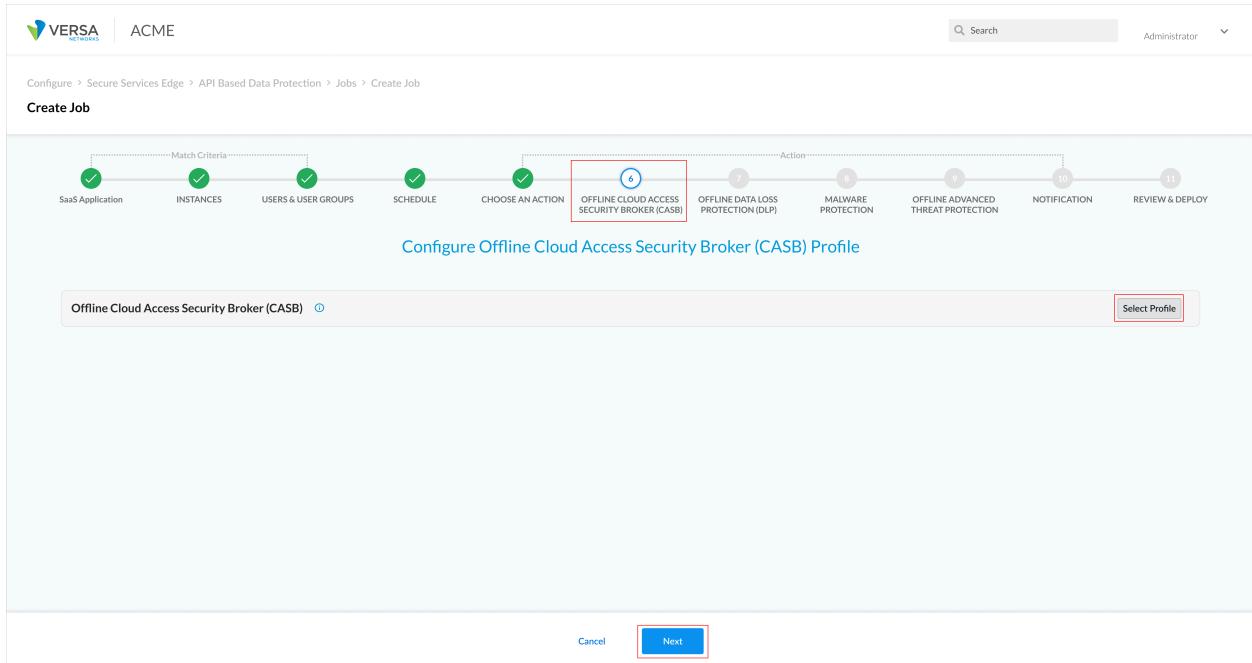
Allow Allow all that matches the rule to pass.

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

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

Cancel **Next** (Red box)

- Click Next to go to Step 6, Offline Cloud Access Security Broker (CASB).



- Click Select Profile. The Offline Cloud Access Security Broker (CASB) Profiles screen displays.

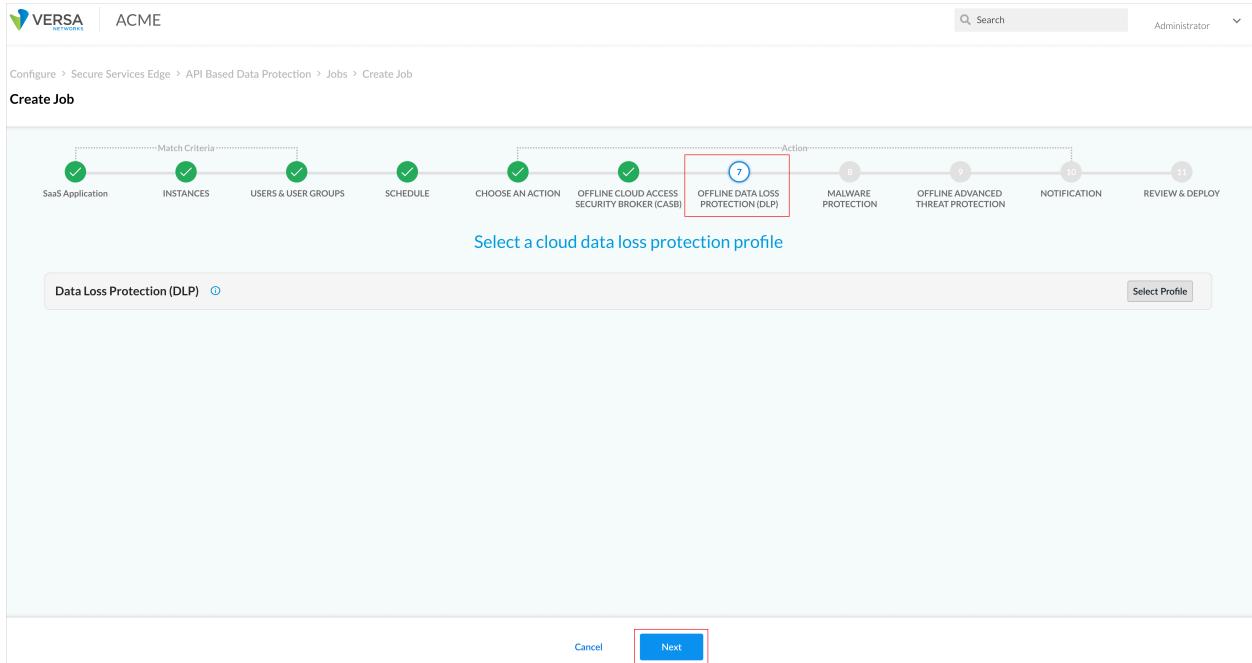
Offline Cloud Access Security Broker (CASB) Profiles							
PROFILE NAME		RULES					
<input checked="" type="radio"/> ACME Box GoogleDrive	2						
ORDER	RULE NAME	RULE ACTION	EMAIL PROFILE	RISK LEVEL	PREDEFINED APPLICATIONS	ACTIVITES	
1	Box	Allow	Marketing User	Low	Word Online	Login, Download	
2	Google Drive	Allow	Marketing User	Low	Evernote	Login	
<input type="radio"/>	ACME Amazon aws	2	On first rule match	Allow			
<input type="radio"/>	ACME Outlook	5	On first rule match	Allow			

- Select a CASB profile. To add a profile, click + Add Profile.
- Click Done.
- Click Next to go to Step 7, Offline Data Loss Protection (DLP) Profile.

[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 08:40:17 GMT

Copyright © 2024, Versa Networks, Inc.



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

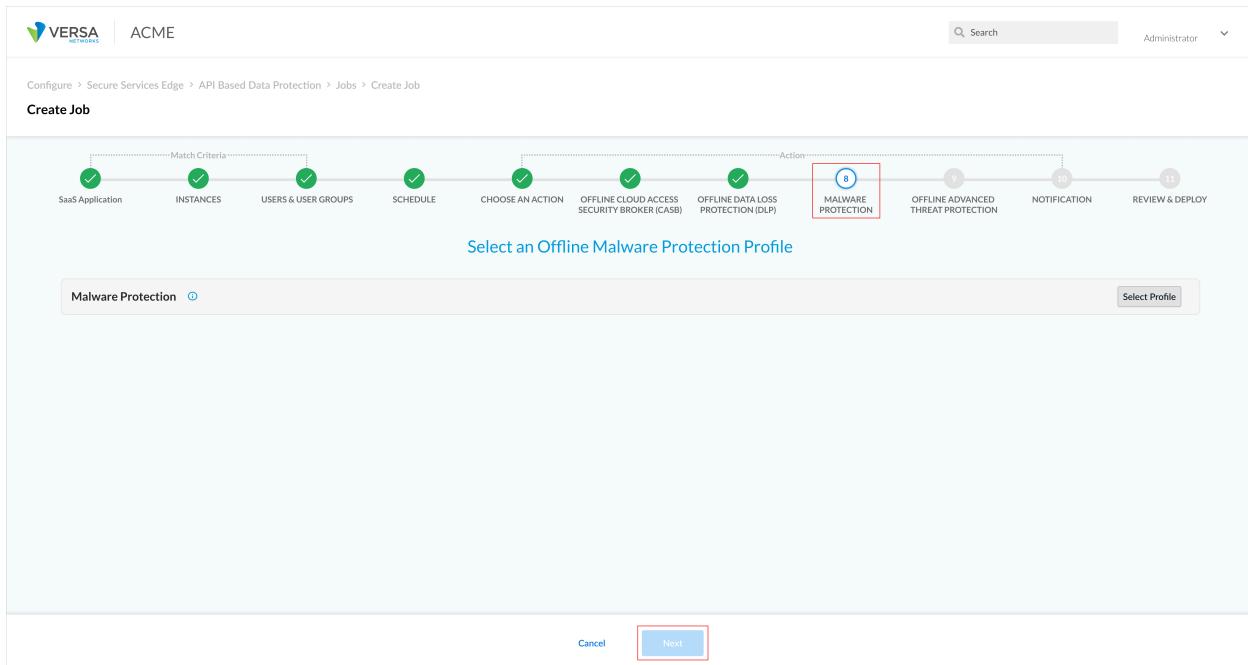
PROFILE NAME	RULES	EXIT	DEFAULT ACTION			
<input checked="" type="radio"/> ACME-GDPR-USAUK-DLP-Profile	2	On first rule match	Allow			
ORDER	RULE NAME	OBJECT OF INTEREST	ACTIVITIES	CONTEXT	PROTOCOL	FILE TYPE
1	ACME-GDPR-USA-DLP-Rule	Content Analysis: Payment Card Industry Data Security Standard (PCI-DSS)	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		

15. Select a DLP profile. To add a profile, click + Add Profile. For more information, see [Configure Offline Data Loss Prevention](#).
16. Click Done.
17. Click Next to go to Step 8, 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 08:40:17 GMT

Copyright © 2024, Versa Networks, Inc.



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

PROFILE NAME	DEFUALT ACTION	DIRECTION	FILETYPE	PROTOCOL
<input checked="" type="radio"/> S3 Malware Protection	Block	Both	Any	HTTPS

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

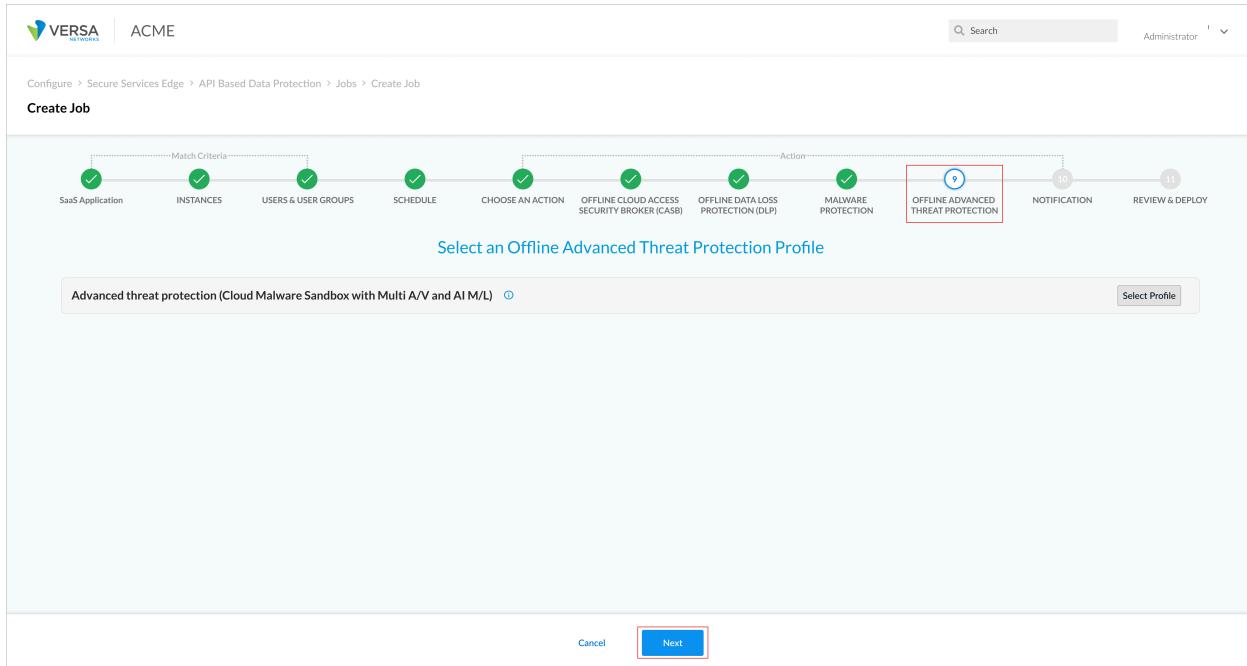
- Click Done.

[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 08:40:17 GMT

Copyright © 2024, Versa Networks, Inc.

21. Click Next to go to Step 9, Offline Advanced Threat Protection (ATP).



22. 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	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	Alerted	3	My ATP Based Action 1, My ATP Based Action 2, My ATP Based Action 2
<input type="radio"/> Allow all clean files	Allow	3	My ATP Based Action 1, My ATP Based Action 2, My ATP Based Action 4

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

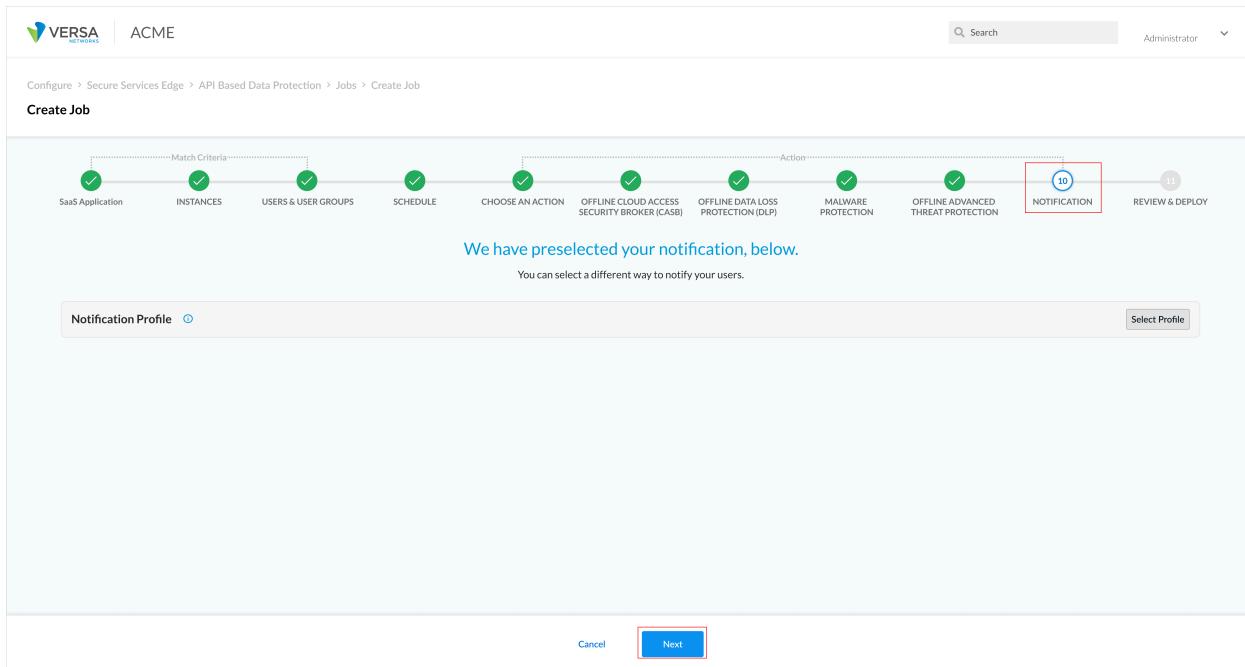
[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_API-Based_Data_P...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_API-Based_Data_P...)

Updated: Wed, 23 Oct 2024 08:40:17 GMT

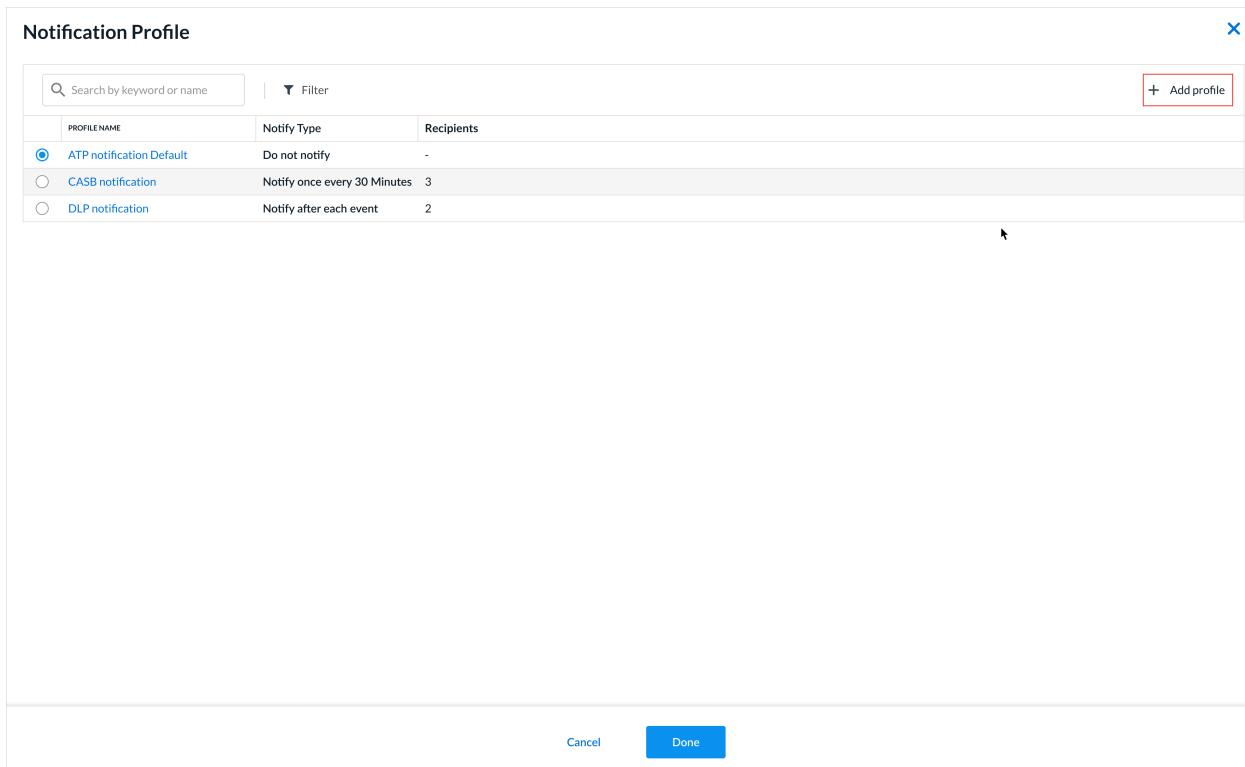
Copyright © 2024, Versa Networks, Inc.

Threat Protection.

24. Click Done.
25. Click Next to go to Step 10, Notification. You can use a notification profile to send logs to Versa Analytics.



26. Click Select Profile. The Notification Profiles 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 08:40:17 GMT

Copyright © 2024, Versa Networks, Inc.

27. 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' entered into an input field, with a 'Delete' button next to it. At the bottom are 'Cancel' and 'Done' buttons.

28. In the Profile Name field, enter a notification profile name to use for Analytics.
29. 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.
30. Click Next to go to Step 11, Review and Deploy. Click Edit next to any section to make changes.

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

Create Job

31. Click Commit and Deploy.

[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 08:40:17 GMT
 Copyright © 2024, Versa Networks, Inc.

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 IaaS](#)

[Configure Offline Advanced Threat Protection](#)

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

[Configure Offline Custom Malware Protection Profiles](#)

[Configure Offline Data Loss Prevention](#)