Configure API-Based Data Protection Policy for IaaS

For supported software information, click here.

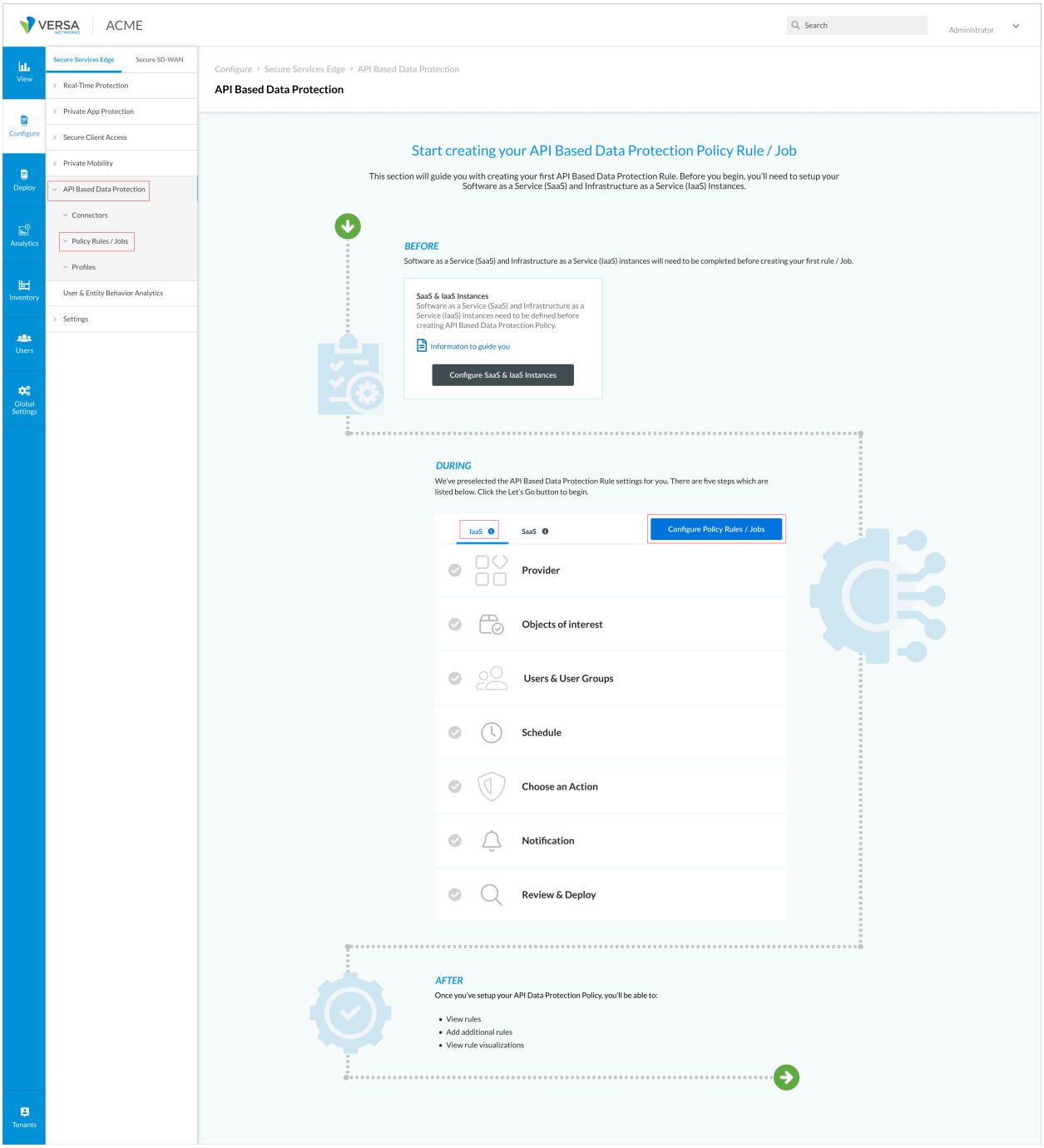
Versa Networks API-based data protection protects and secures organization data that resides in software as a service (SaaS) and infrastructure as a service (IaaS) applications. You create an API data protection policy under a tenant in Concerto to configure API data protection. The policy contains a 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.

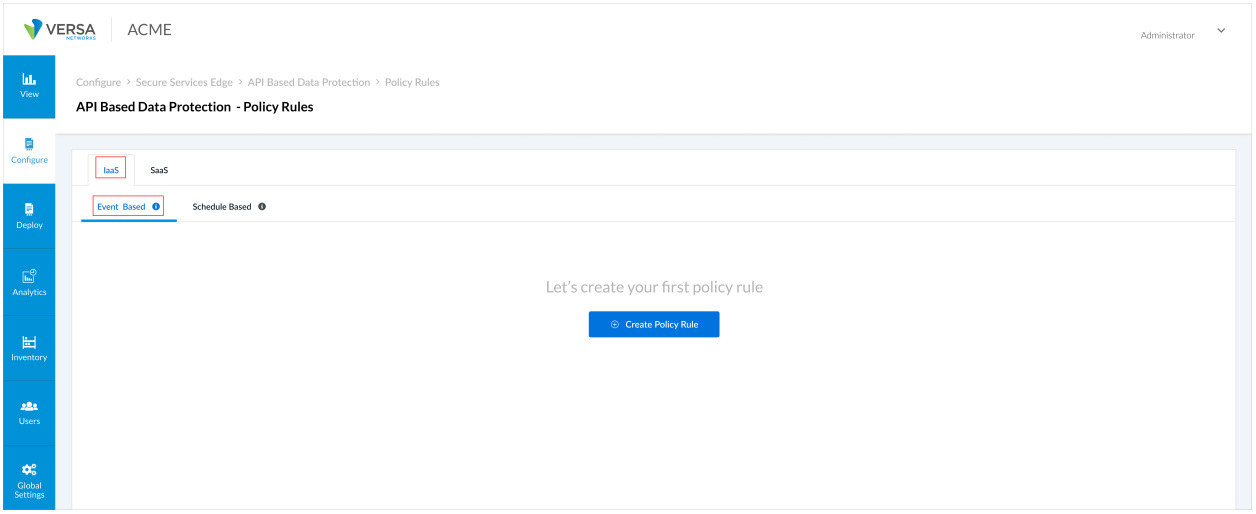
This article describes how to create event-based and schedule-based API data protection policy rules for IaaS.

Configure an Event-Based IaaS API Data Protection Policy Rule

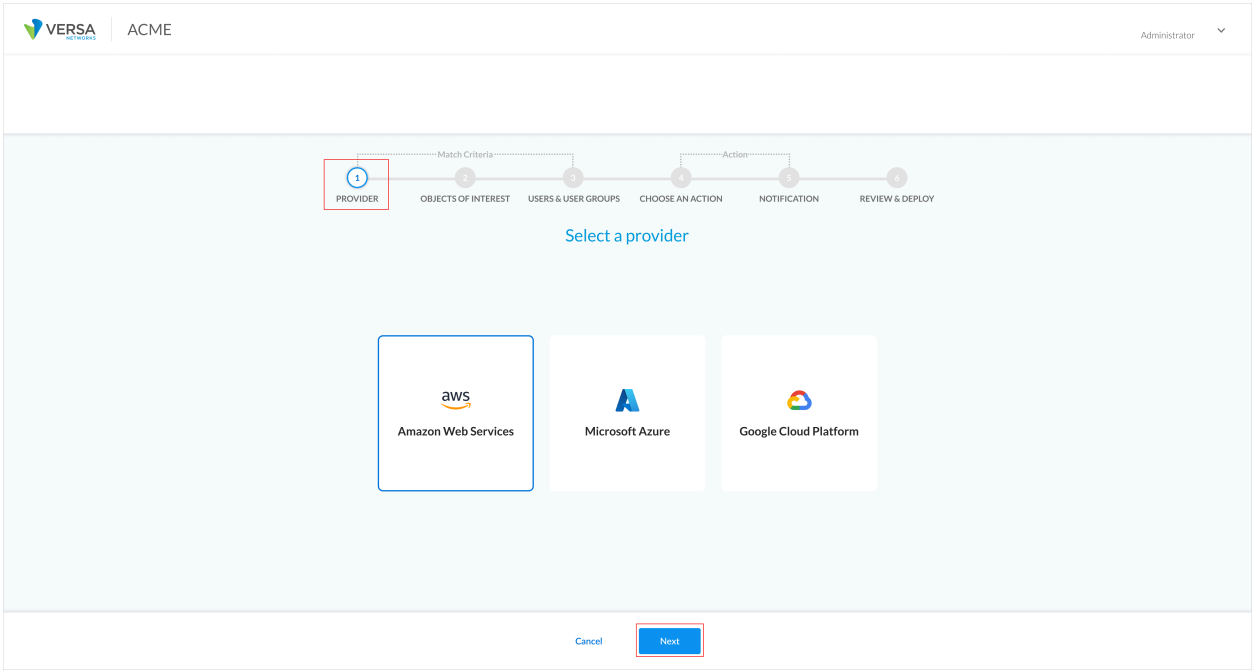
1. Go to Configure > Secure Service Edge > API-Based Data Protection > Policy Rules.



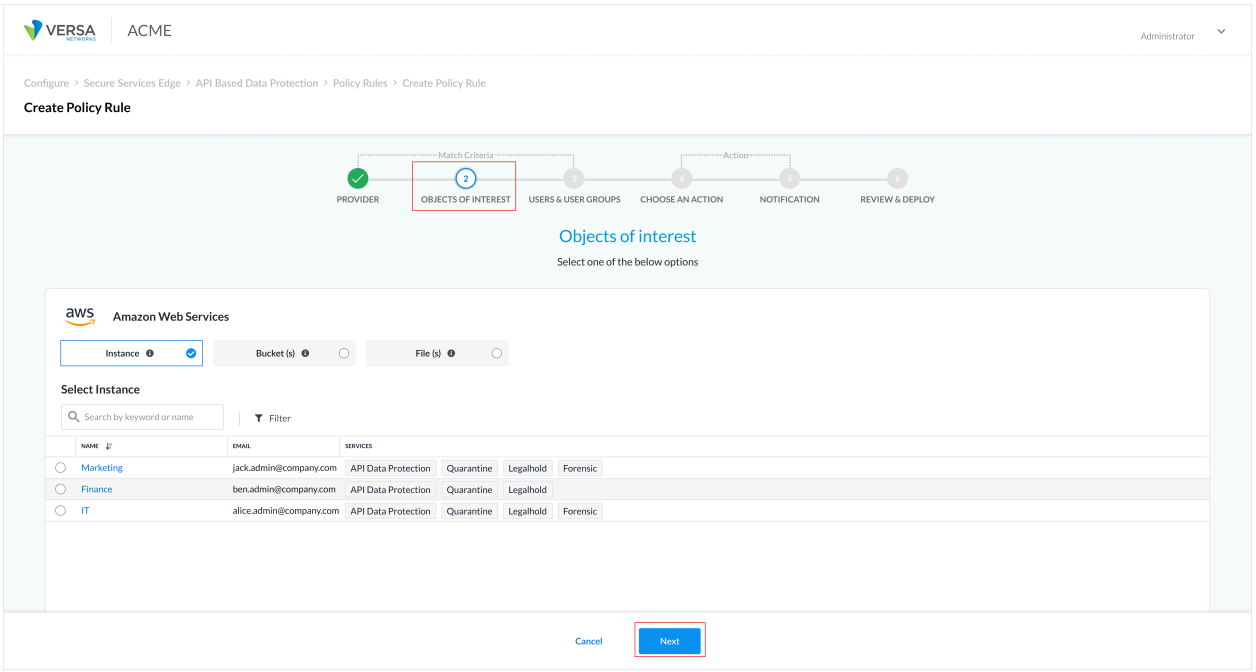
2. Select IaaS, and then click Configure Policy Rules/Jobs. The API-Based Data Protection - Policy Rules screen displays.



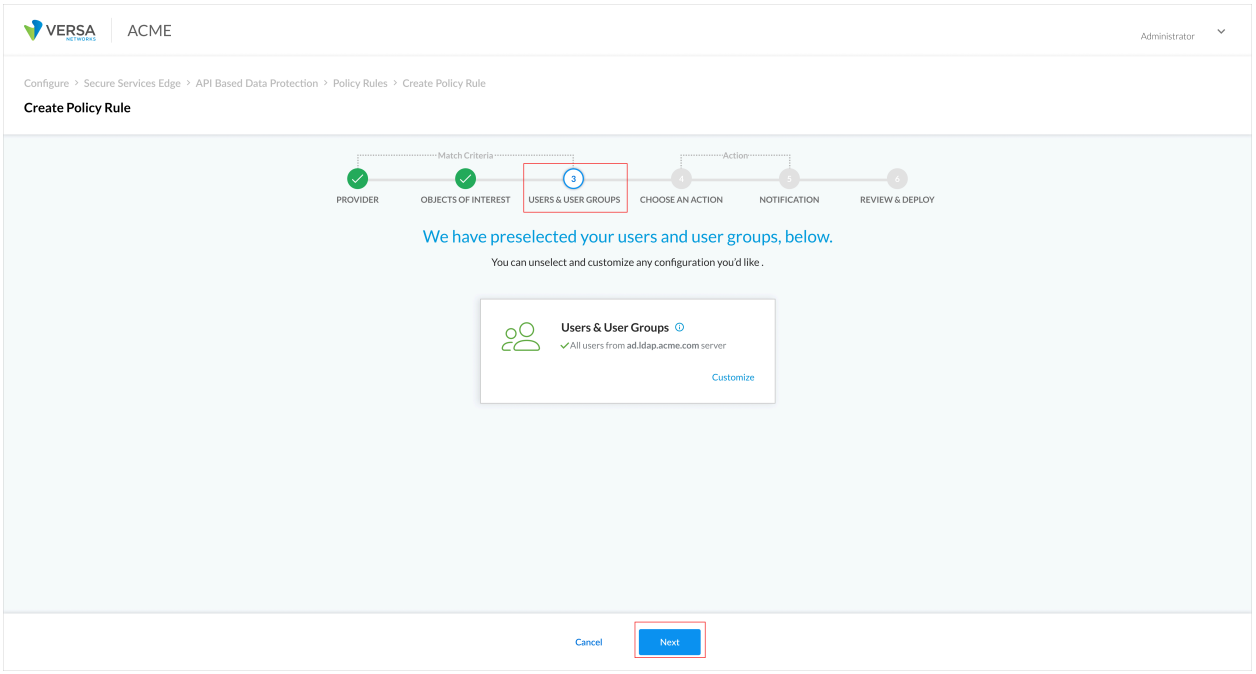
3. Select the Event-Based tab and click Create Rule Policy. The Create Policy Rule screen displays.



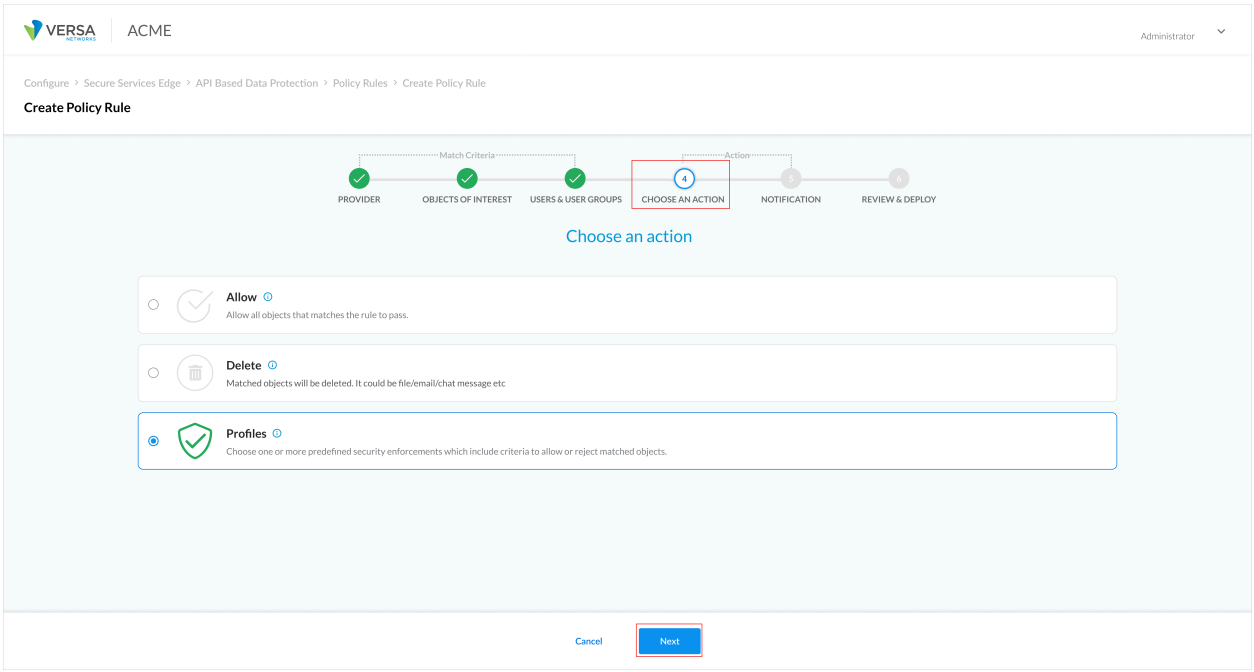
4. Go to Step 1, Provider. Select the IaaS provider for which to apply the rule.
5. Click Next to go to Step 2, Objects of Interest. Select the objects of interest for the IaaS provider—instance, buckets, or files.



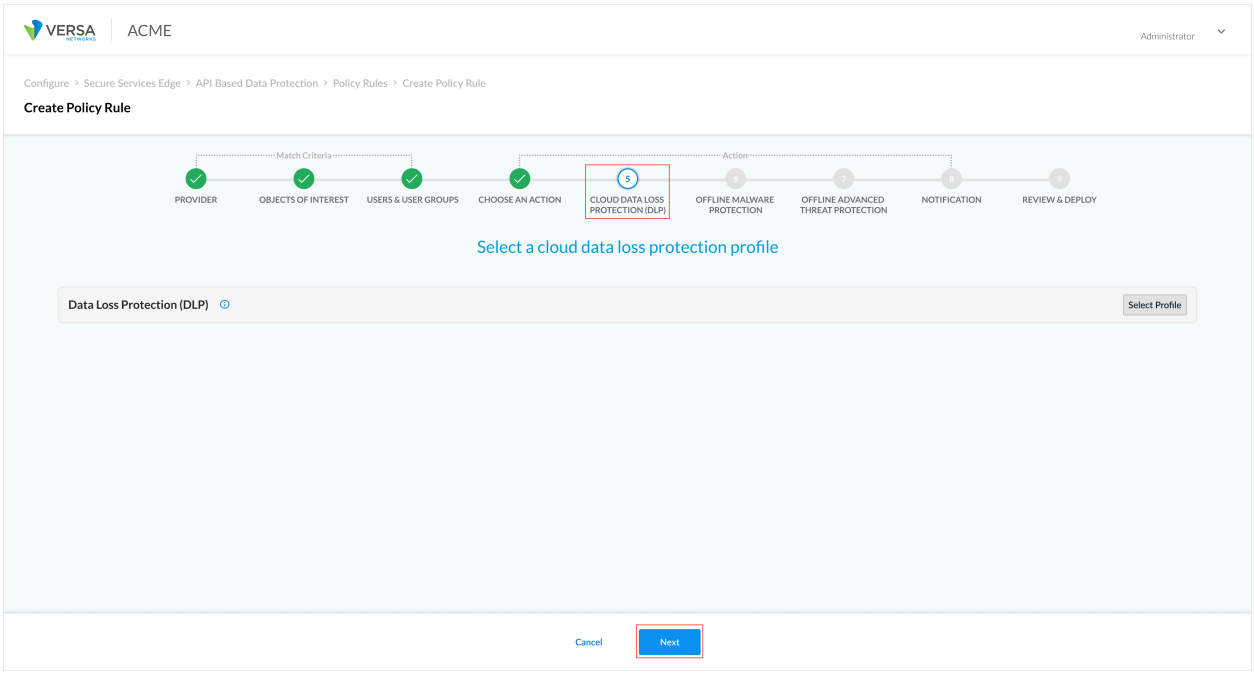
6. Click Next to go to Step 3, User and User Groups. Select the users or user groups to match the policy.



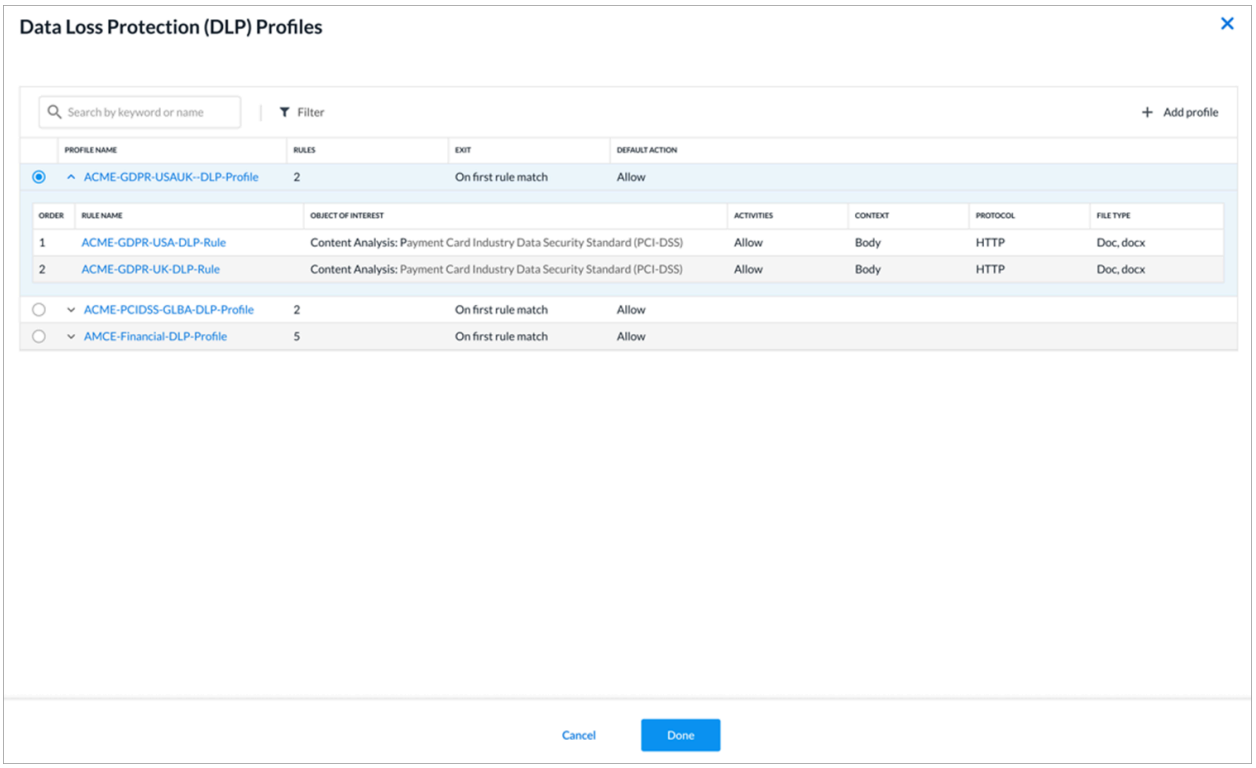
7. Click Next to go to Step 4, Choose an Action. Select an appropriate action to assign security policy profiles, allow list, and disallow list. To use offline DLP, malware, and advanced threat protection (ATP) profiles, select Profiles.



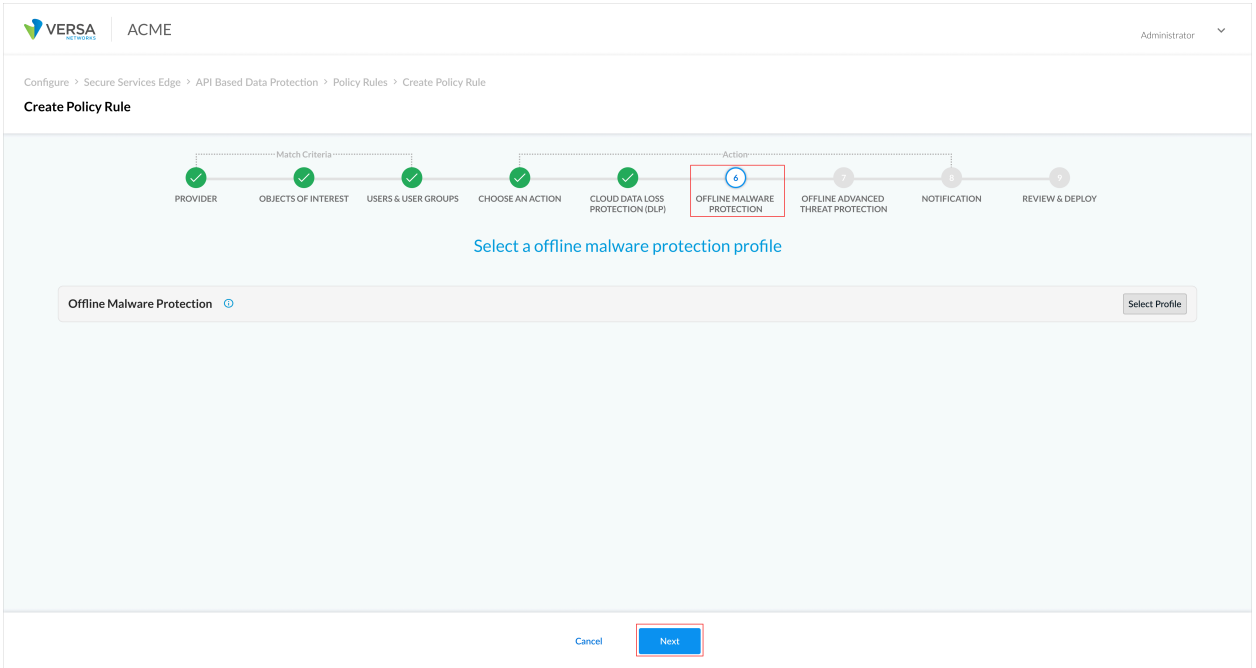
8. Click Next to go to Step 5, Offline Data Loss Protection (DLP).



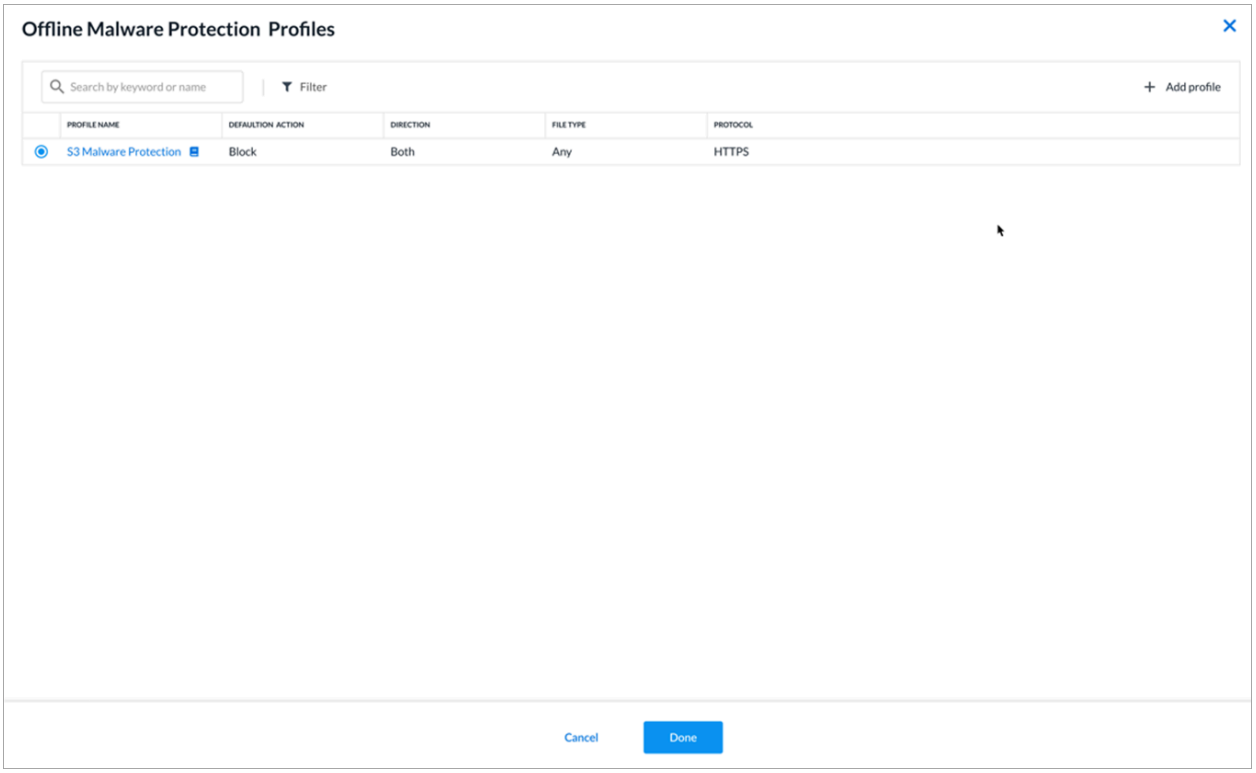
9. Click Select Profile. The Data Loss Protection (DLP) Profiles screen displays.



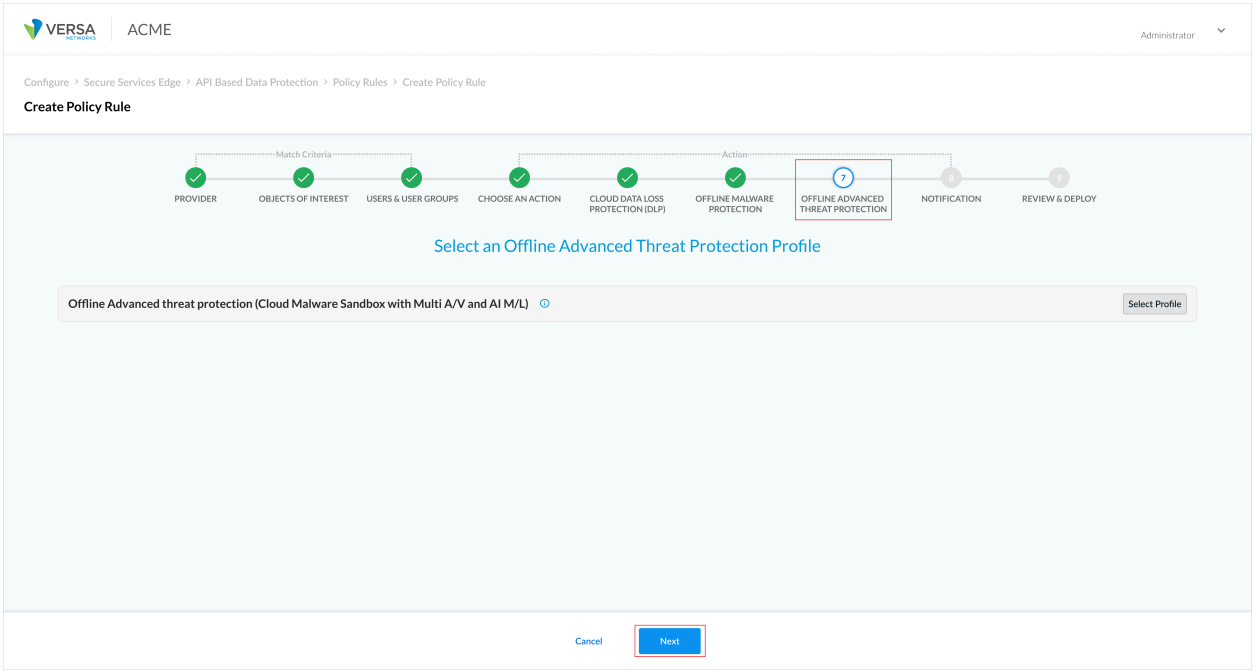
10. Select a DLP profile. To add a profile, click + Add Profile. For more information, see Configure Offline Data Loss Prevention.
11. Click Done.
12. Click Next to go to Step 6, Offline Malware Protection.



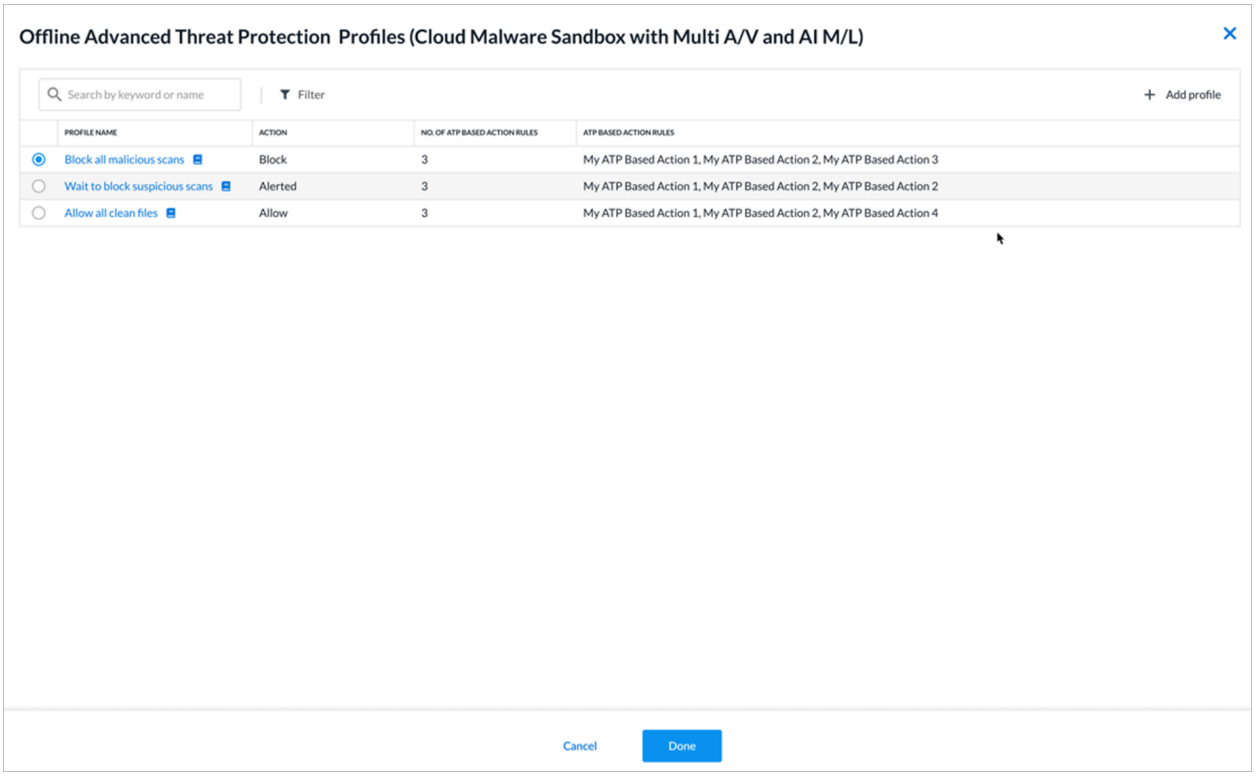
13. Click Select Profile. The Offline Malware Protection Profile screen displays.



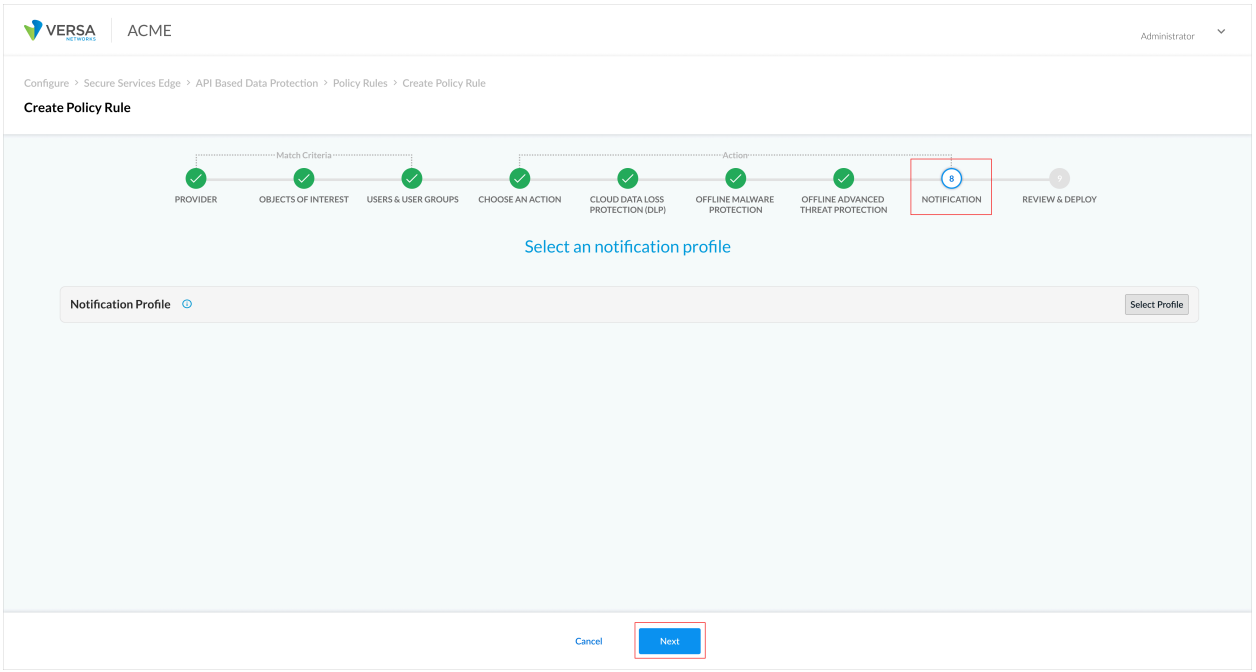
14. Select a malware profile. To add a profile, click + Add Profile. For more information, see Configure Offline Custom Malware Protection Profiles.
15. Click Done.
16. Click Next to go to Step 7, Offline Advanced Threat Protection.



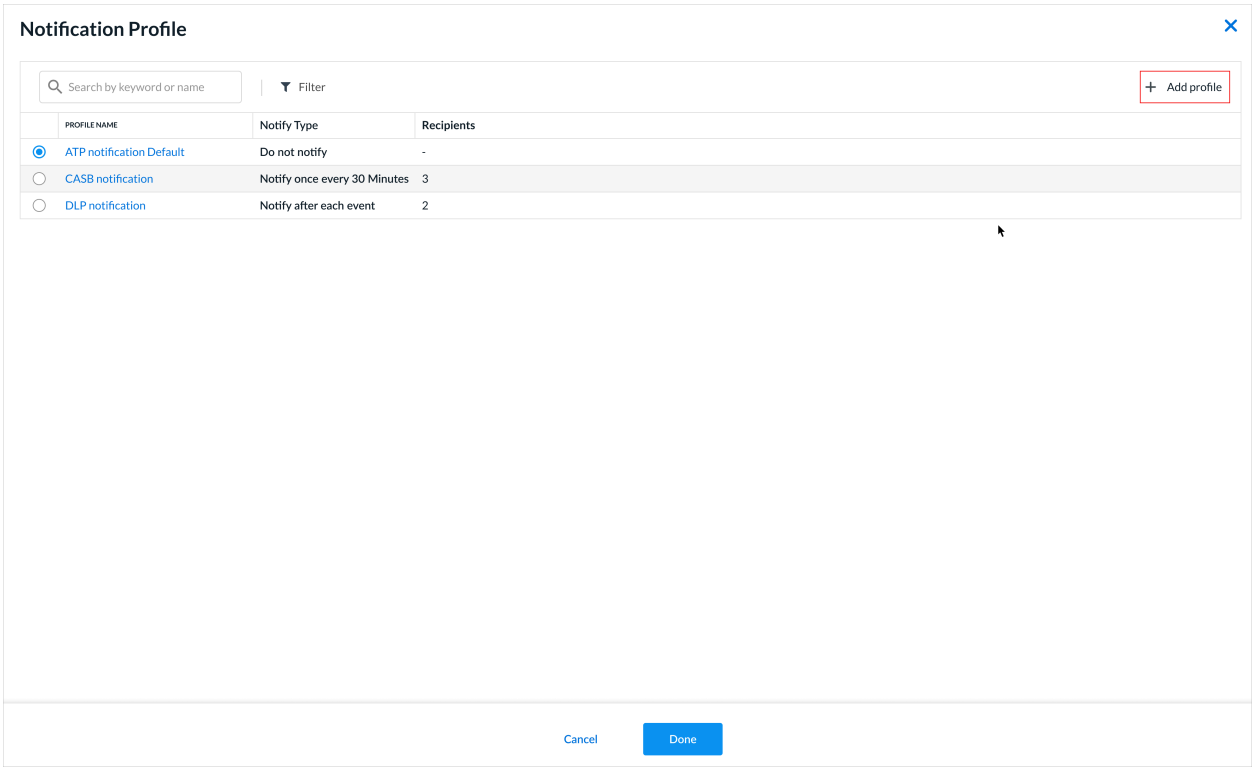
17. Click Select Profile. The Offline Advanced Threat Protection Profiles (Cloud Malware Sandbox with Multi A/V and AI M/L) screen displays.



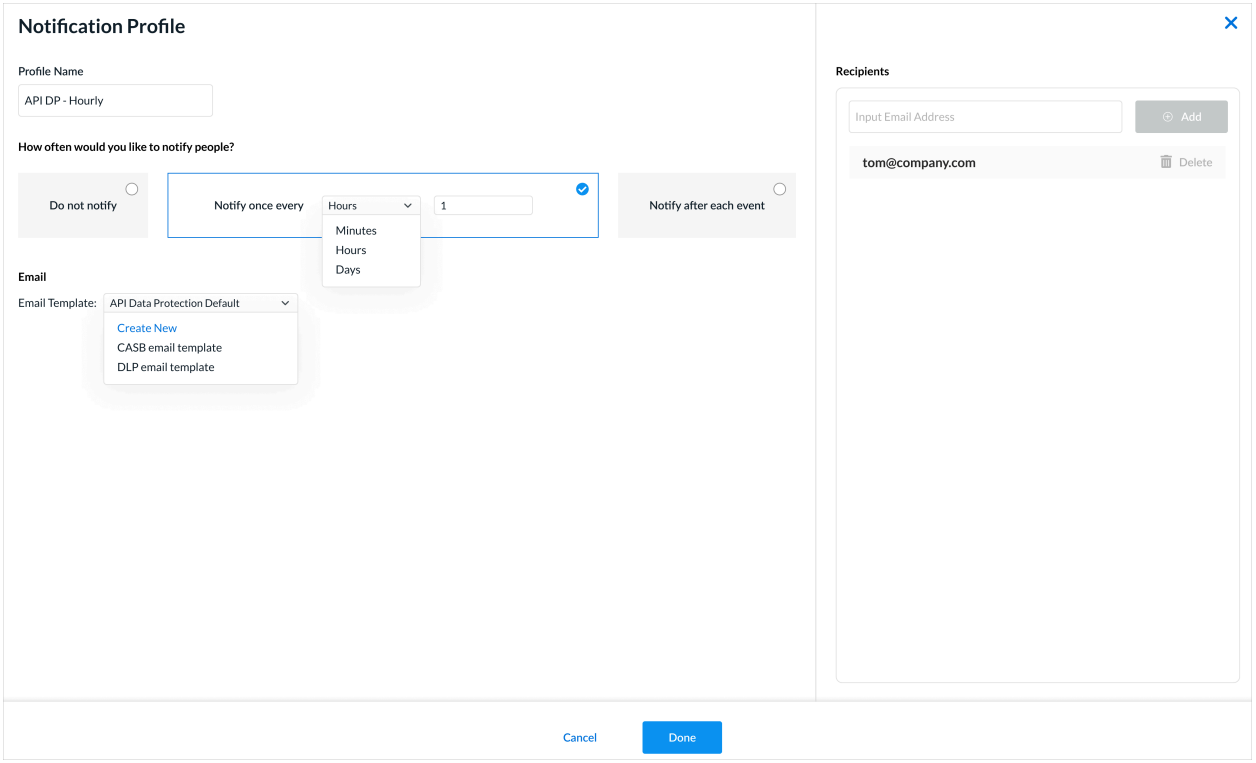
18. Select an ATP profile. To add a profile, click + Add Profile. For more information, see Configure Offline Advanced Threat Protection.
19. Click Done.
20. Click Next to go to Step 8, Notification. You can use a notification profile to send logs to Versa Analytics.



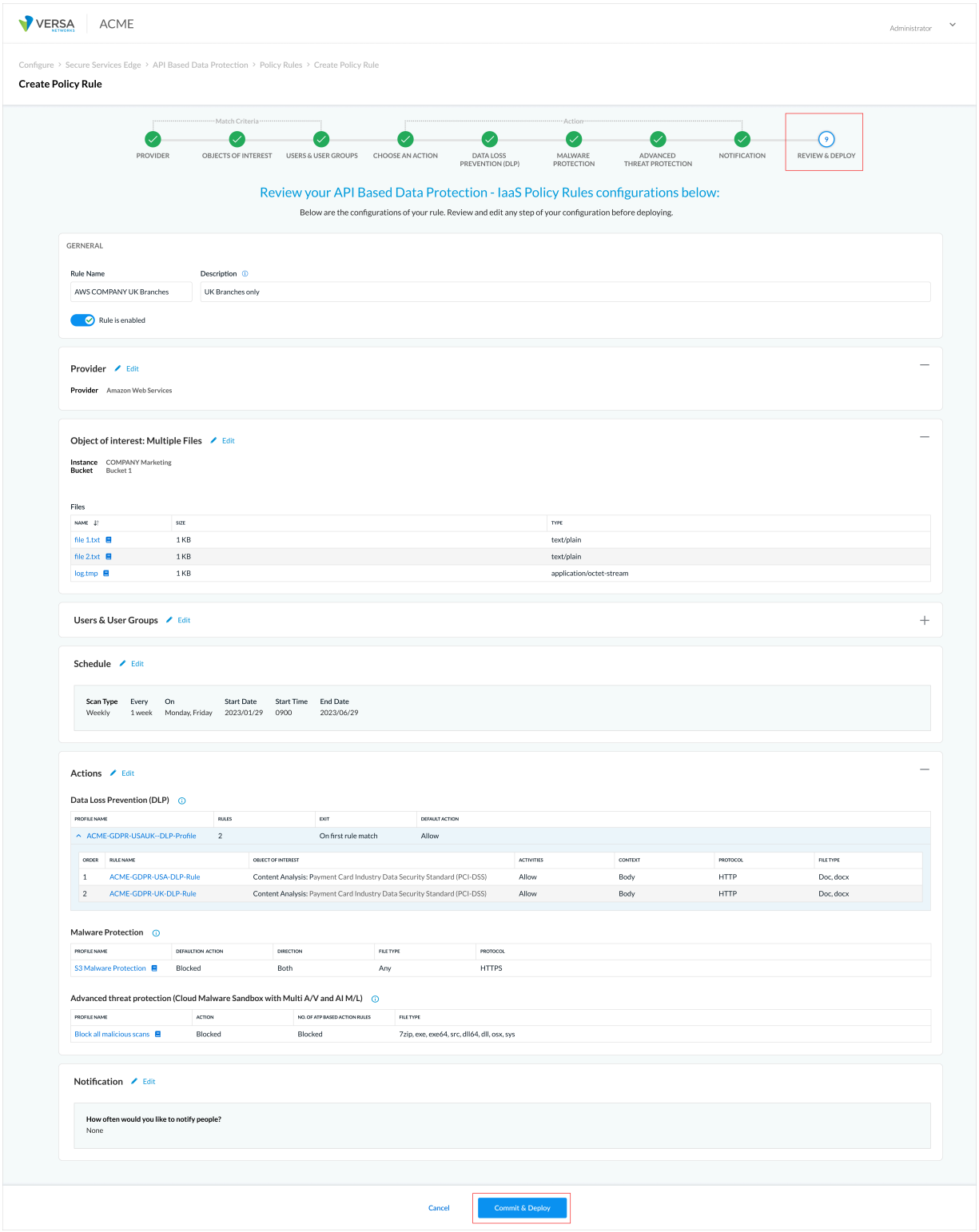
21. Click Select Profile. The Notification Profiles screen displays.



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



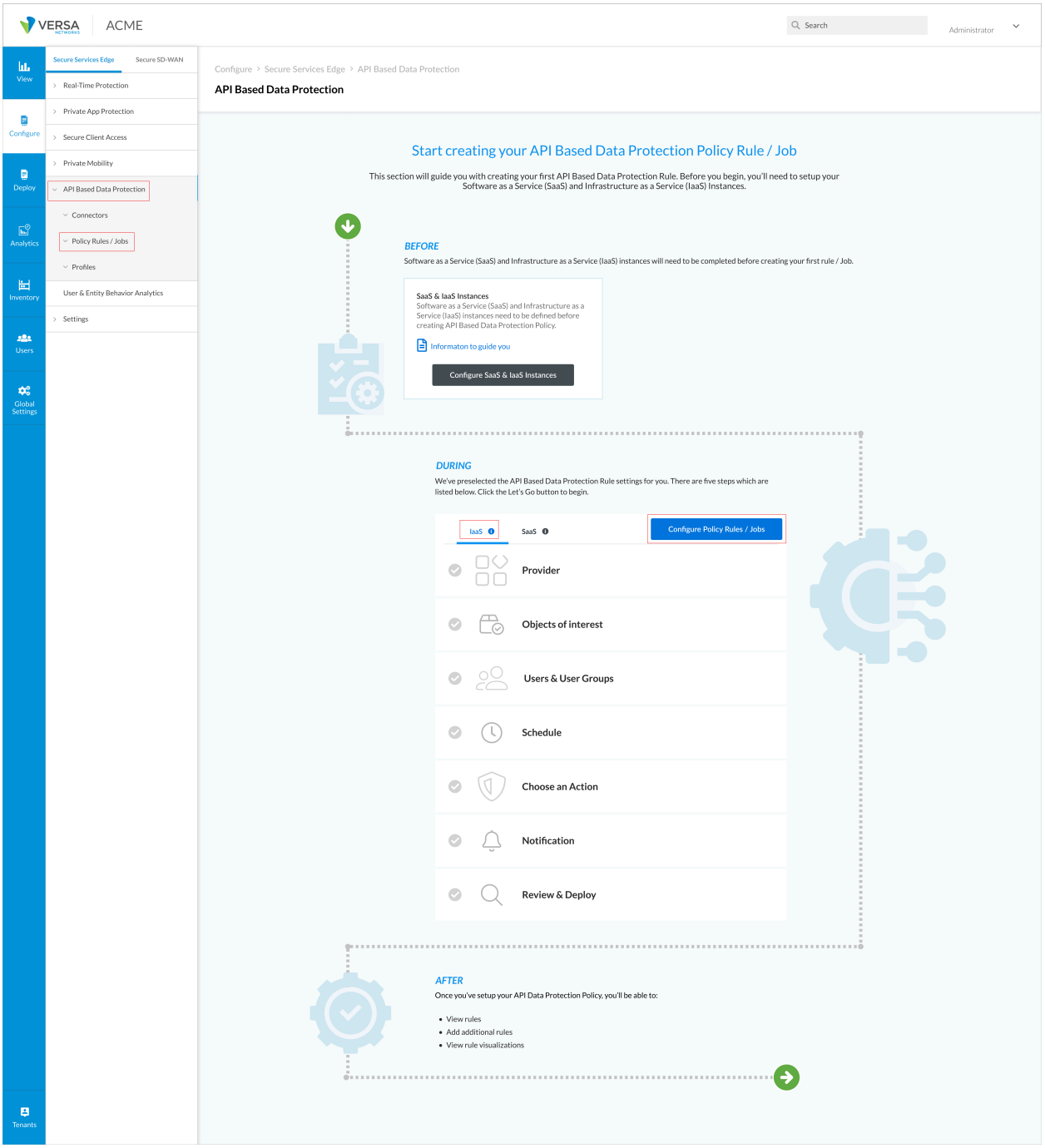
23. In the Profile Name field, enter a notification profile name to use for Analytics.
24. Select the option to notify for Analytics - Do not notify, Notify once every (select the duration), or Notify after each event.
    a. If you select to notify, select the duration.
    b. Select an email template 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.



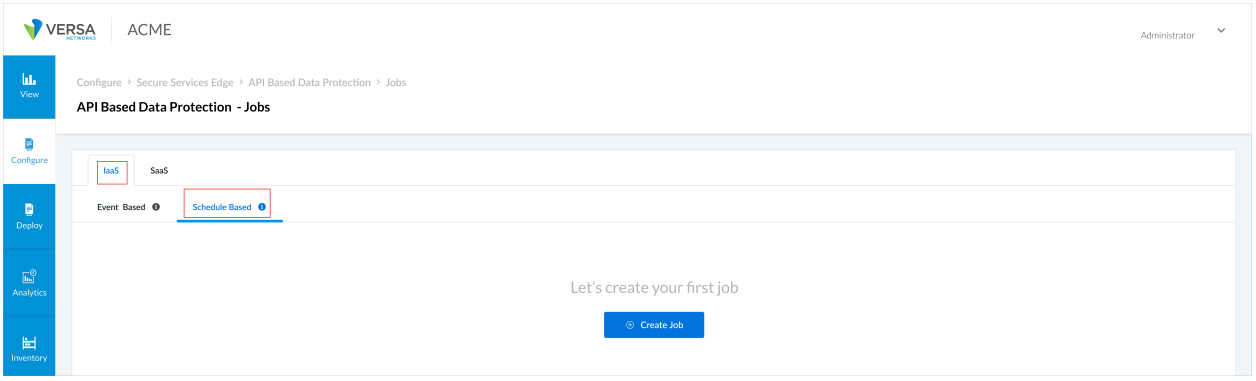
26. Click Commit and Deploy.

Configure a Schedule-Based IaaS API Data Protection Policy Rule

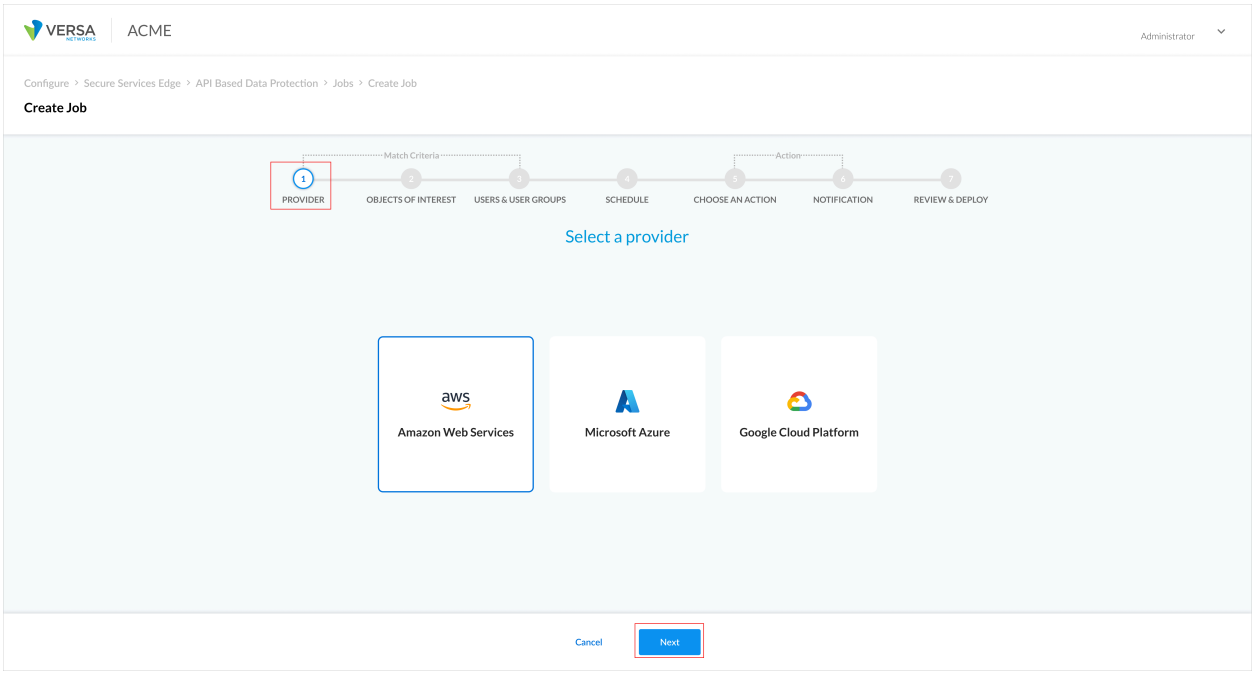
1. Go to Configure > Secure Service Edge > API Based Data Protection > Policy Rules.



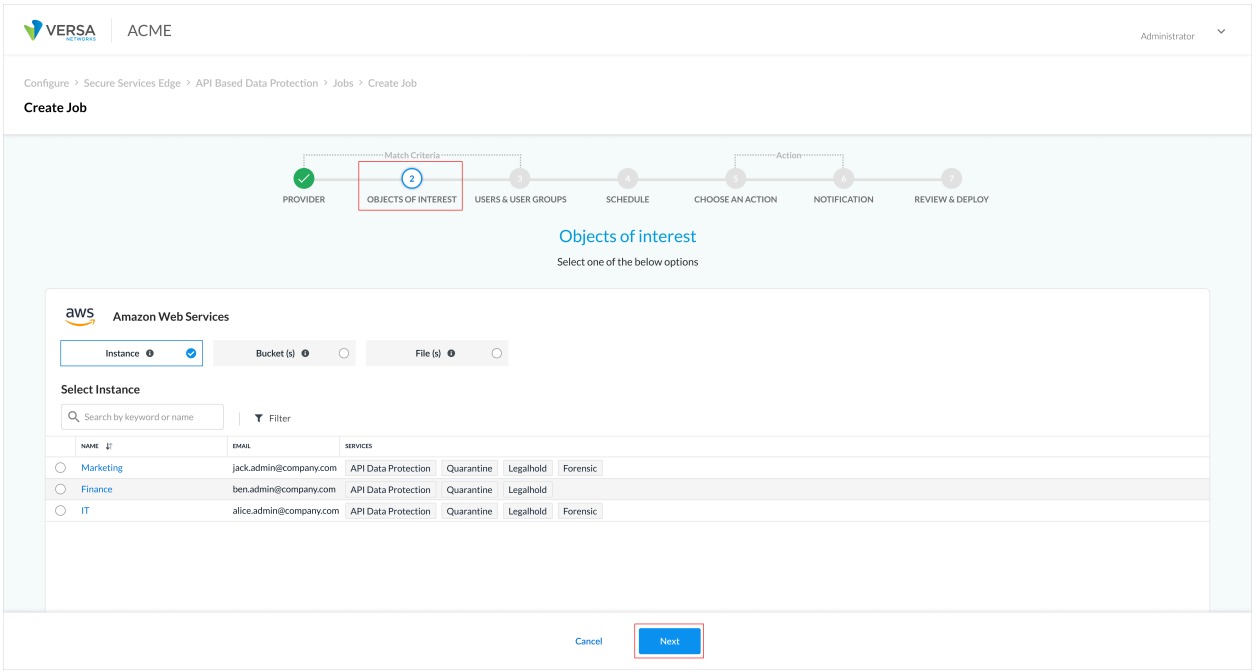
2. Select IaaS, and then click Configure Policy Rules/Jobs. The following screen displays.



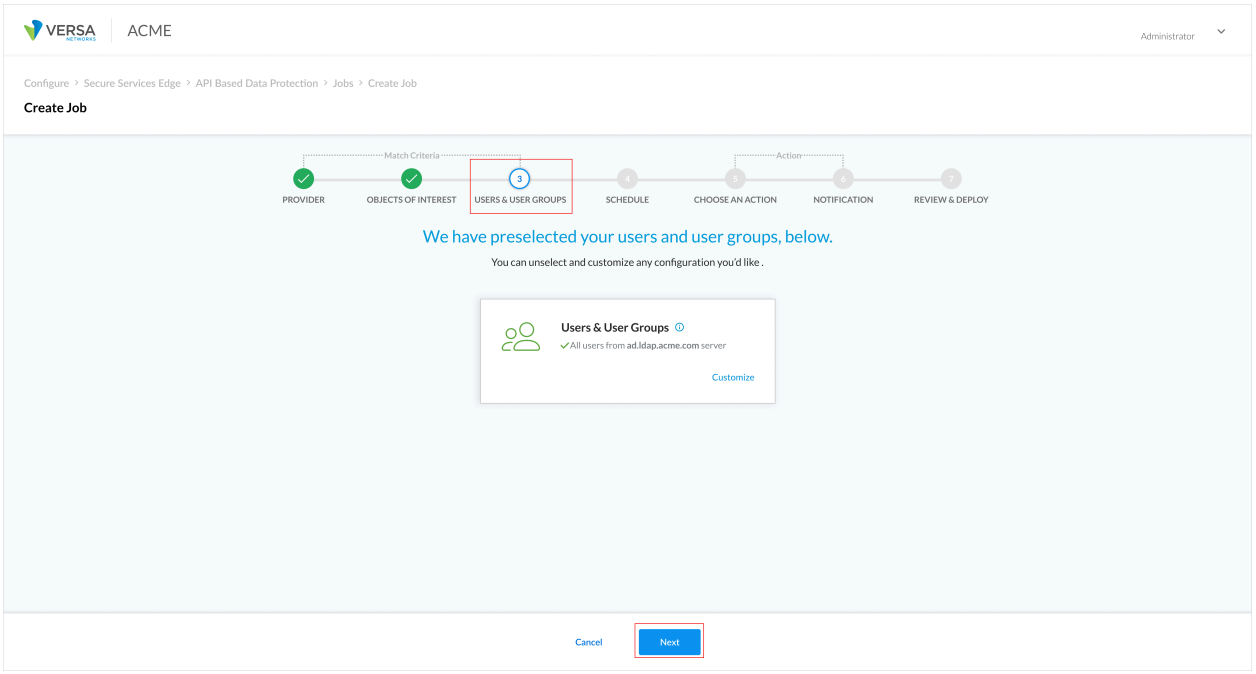
3. Select IaaS, select the Schedule-Based tab, and then click Create a Job. The Create Job screen displays.



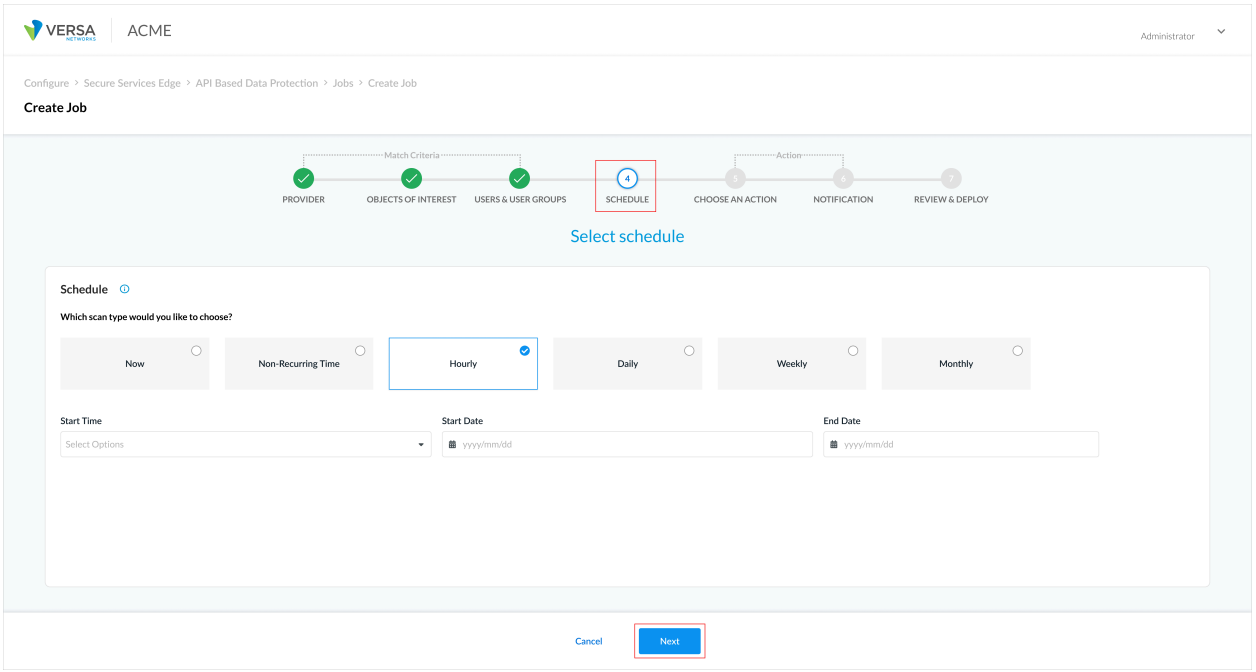
4. Go to Step 1, Provider. Select the IaaS provider for which to apply the rule.
5. Click Next to go to Step 2, Objects of Interest. Select the objects of interest for the IaaS provider—Instance, buckets, or files.



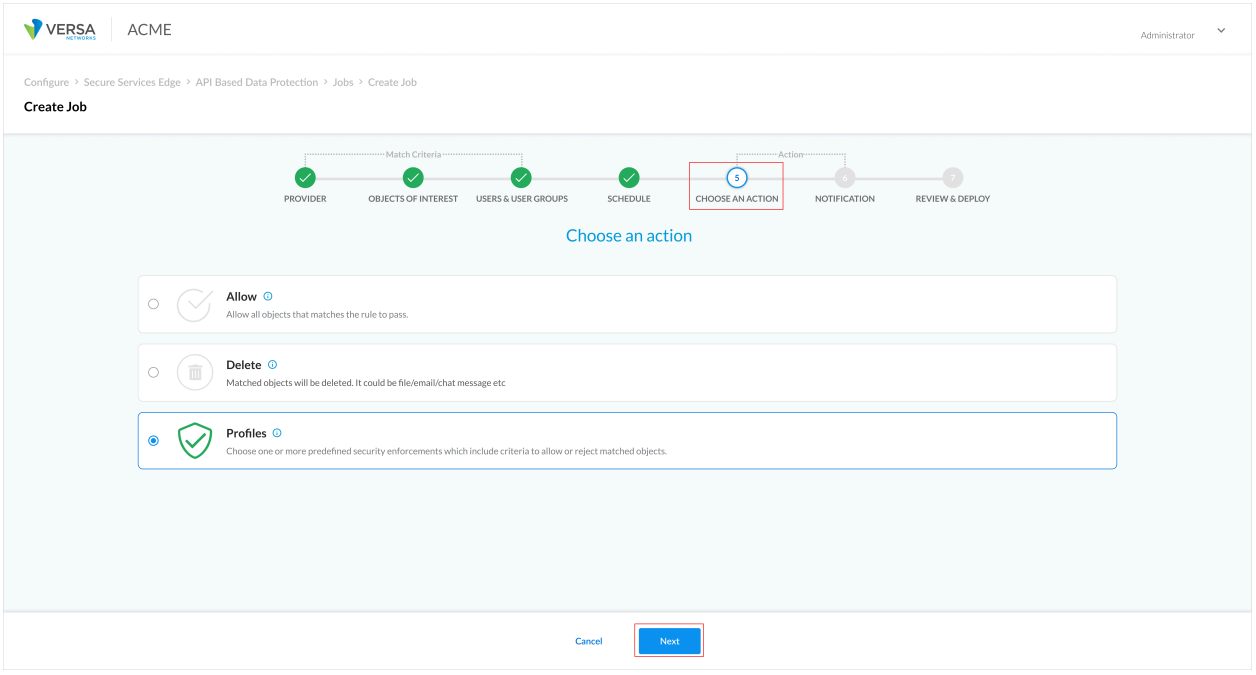
6. Click Next to go to Step 3, User and User Groups. Select the users or user groups to match the policy.



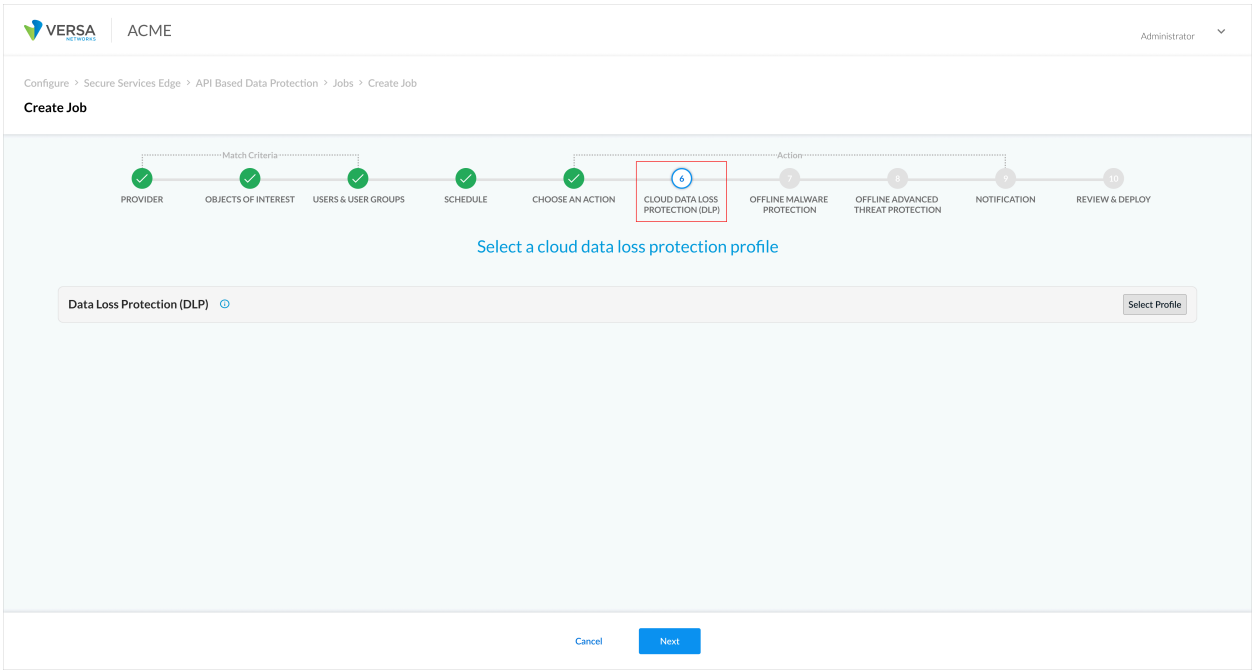
7. Click Next to go to Step 4, Schedule. You can select the scan frequency options - Now, Non-Recurring Time, Hourly, Daily, Weekly, Monthly.



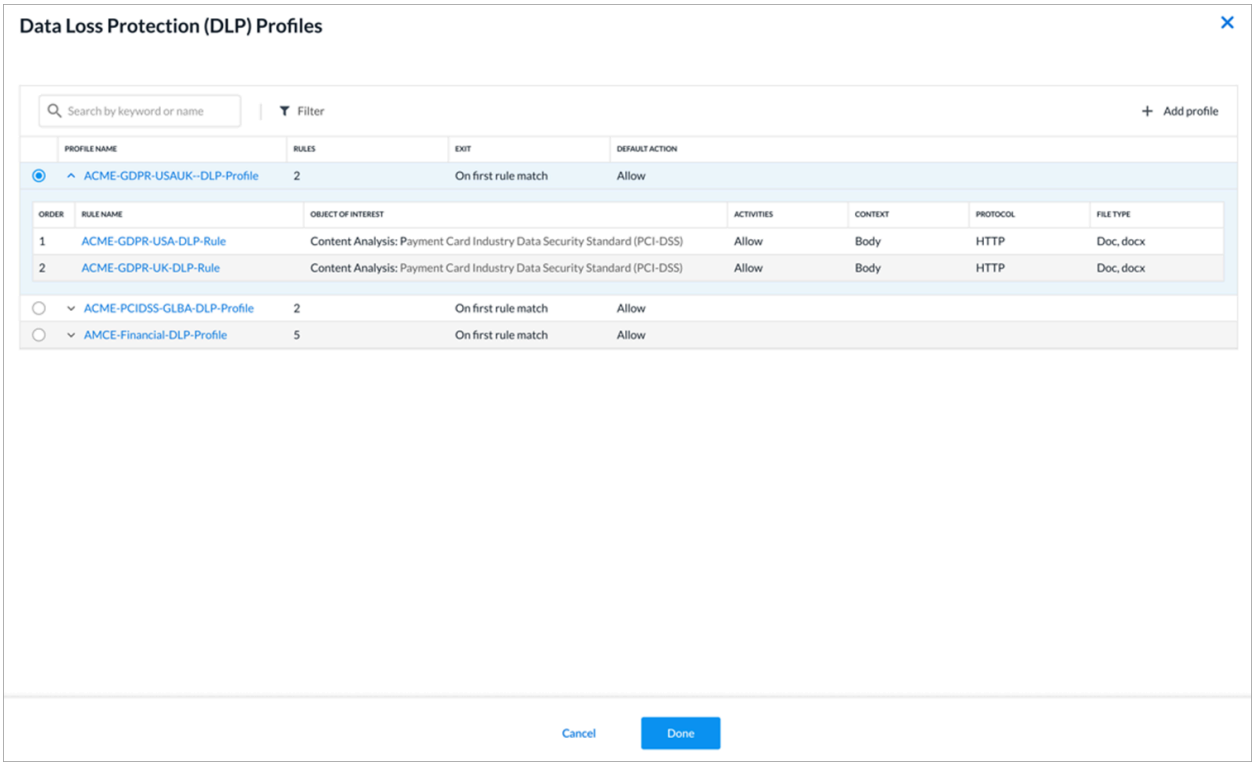
8. Click Next to go to Step 5, Choose an Action. Select an appropriate action to assign security policy profiles, allow list, and disallow list. To use offline DLP, malware, and ATP profiles, select Profiles.



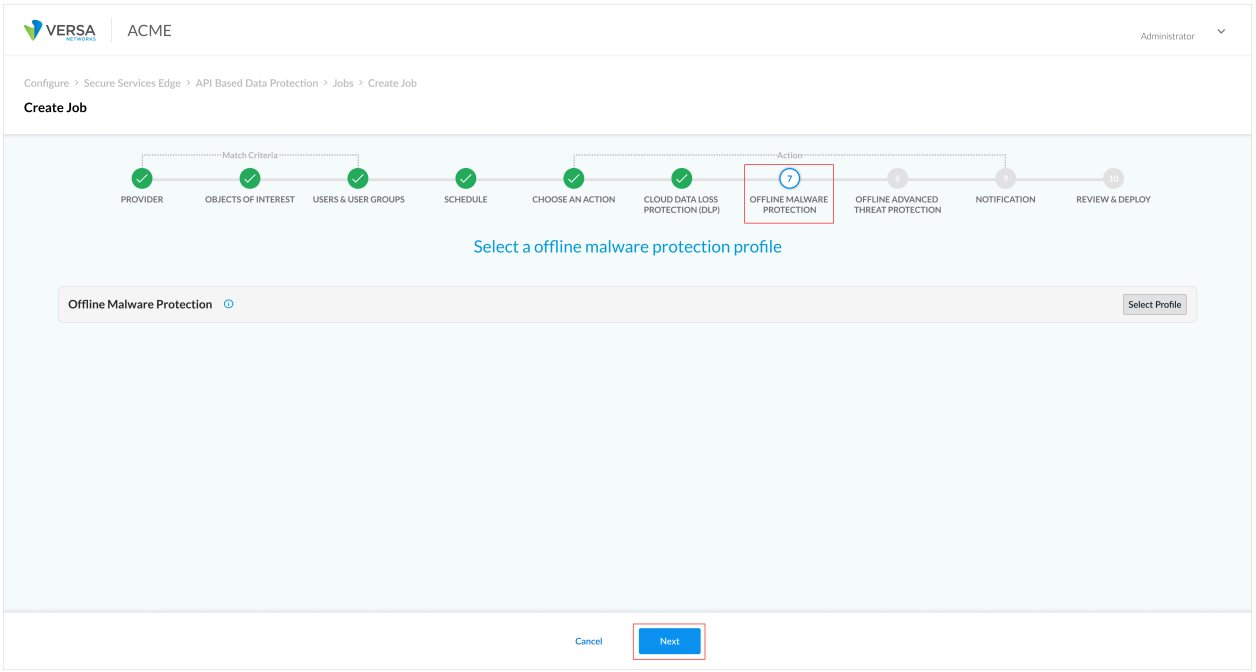
9. Click Next to go to Step 6, Offline Data Loss Protection (DLP) Profile.



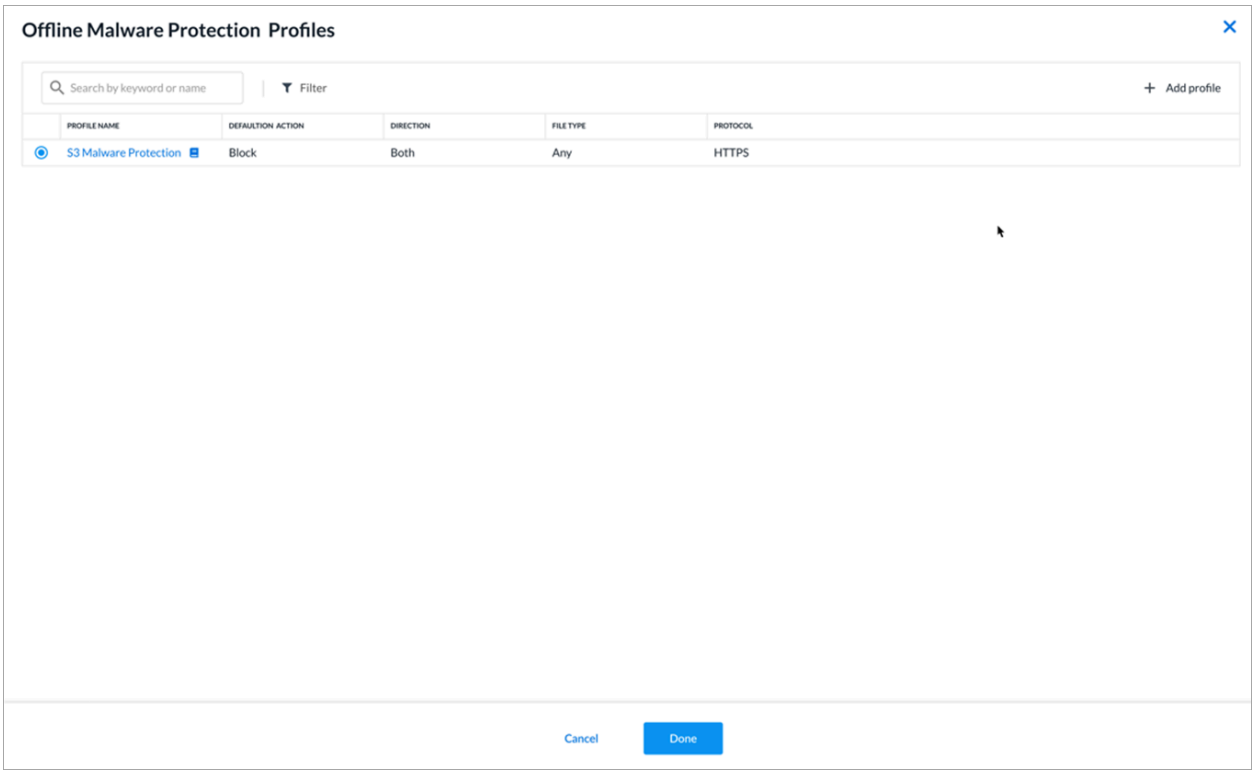
10. Click Select Profile. The Data Loss Protection (DLP) Profiles screen displays.



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.

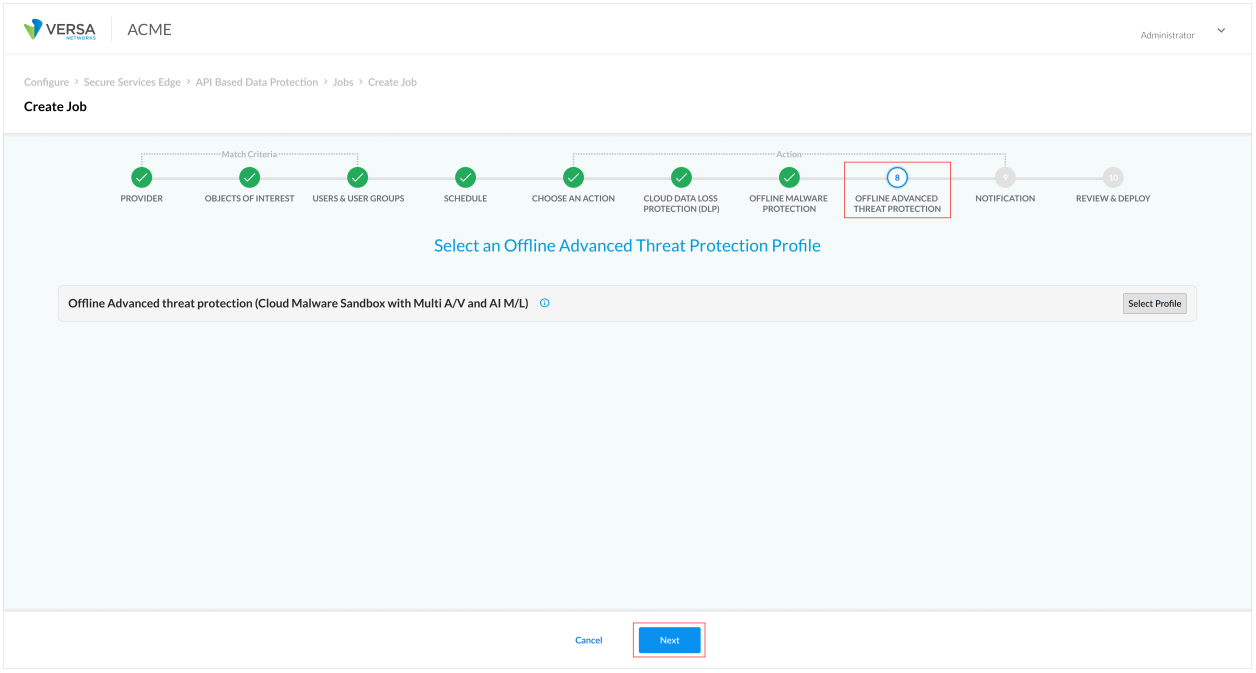


14. Click Select Profile. The Offline Malware Protection Profile screen displays.

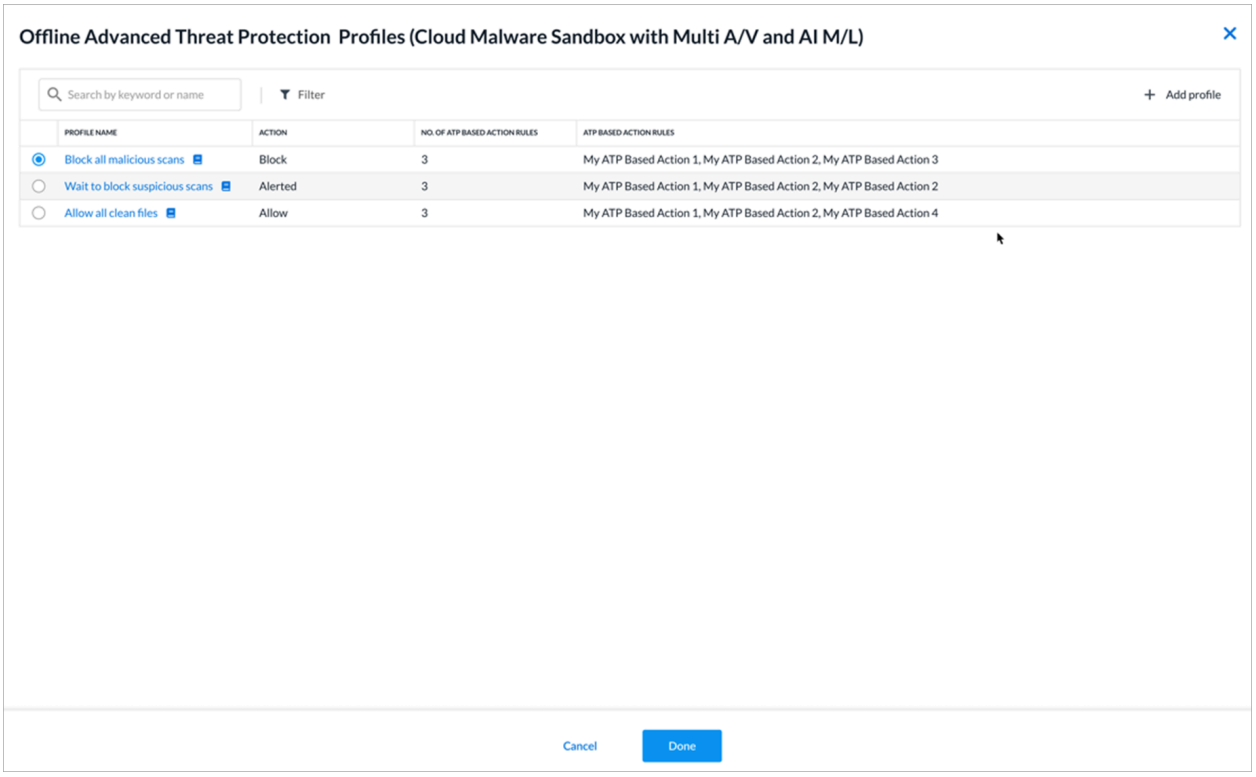


15. Select a malware profile. To add a profile, click + Add Profile. For more information, see Configure Offline Custom Malware Protection Profiles.
16. Click Done.

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



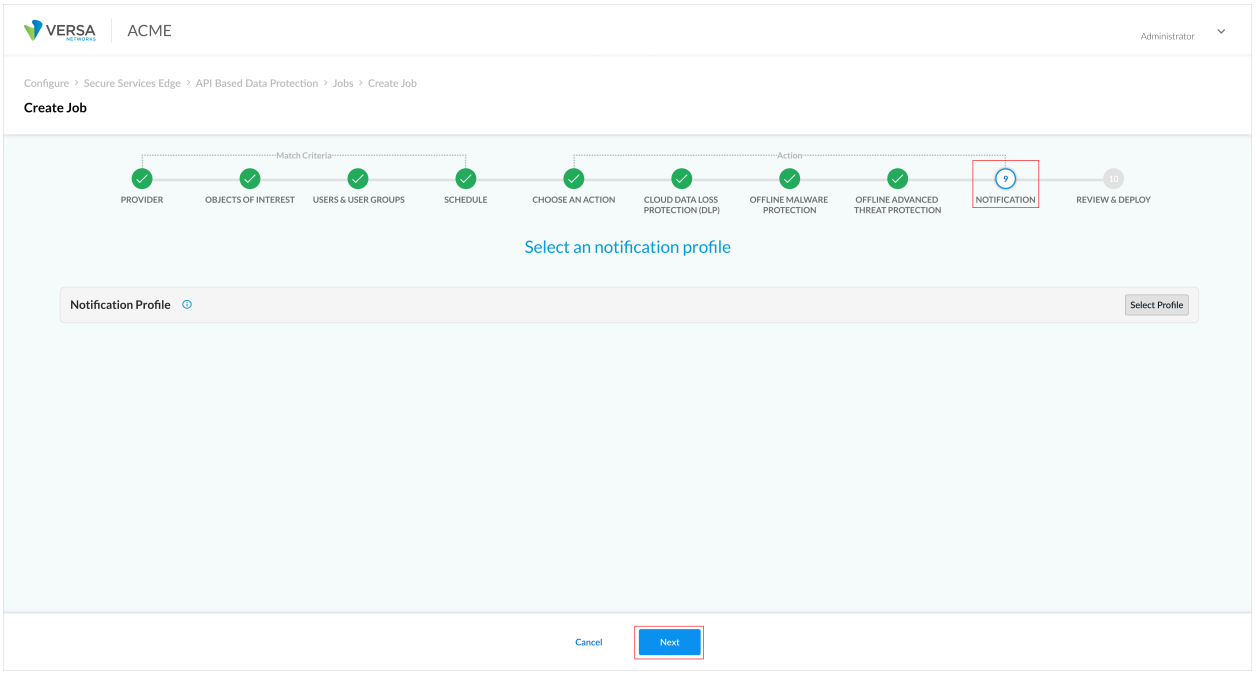
18. Click Select Profile. The Offline Advanced Threat Protection Profiles (Cloud Malware Sandbox with Multi A/V and AI M/L) screen displays.



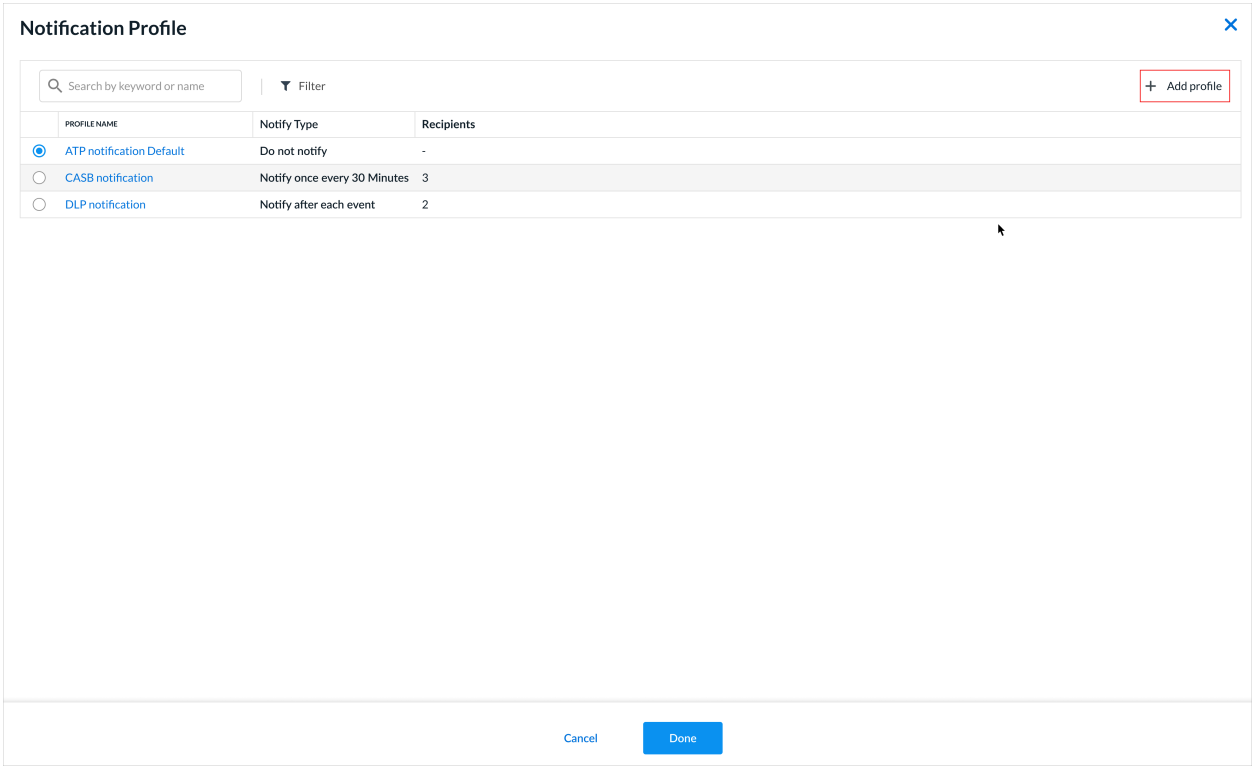
19. Select an ATP profile. To add a profile, click + Add Profile. For more information, see Configure Offline Advanced

Threat Protection.

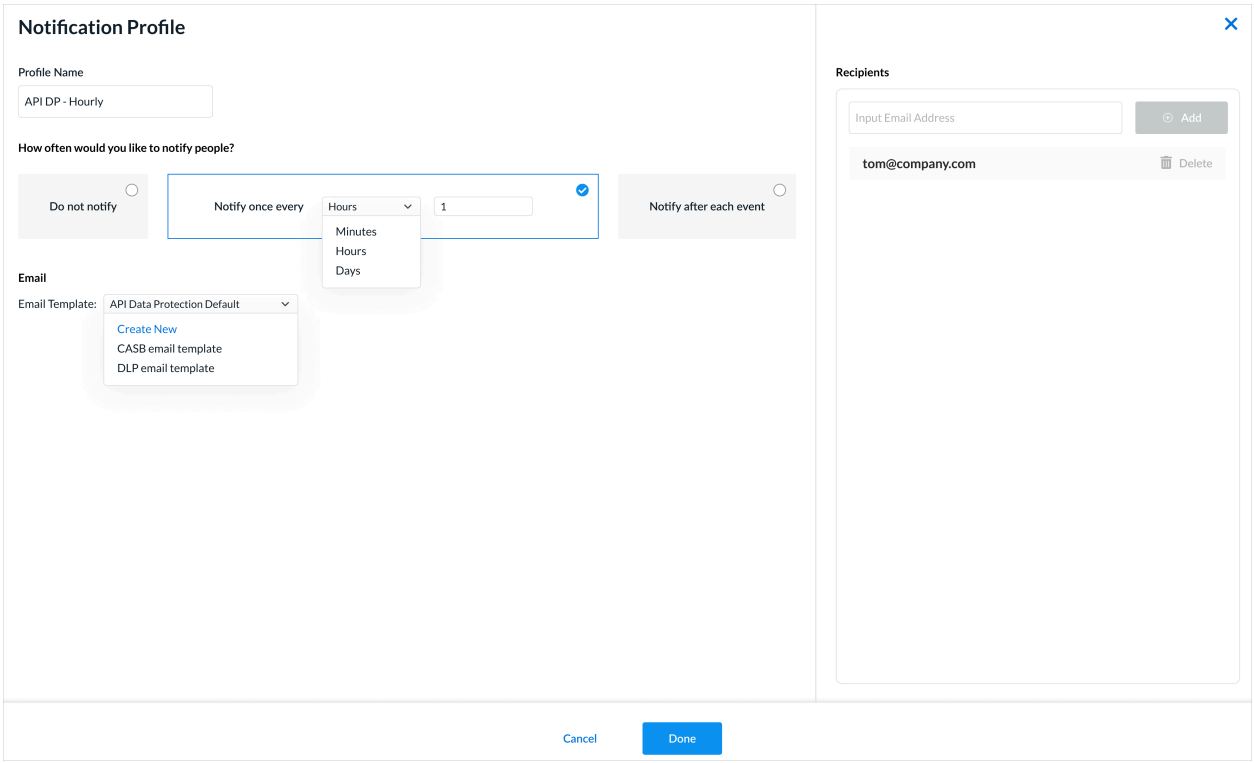
20. Click Done.
21. Click Next to go to Step 9, Notification. You can use a notification profile to send logs to Versa Analytics.



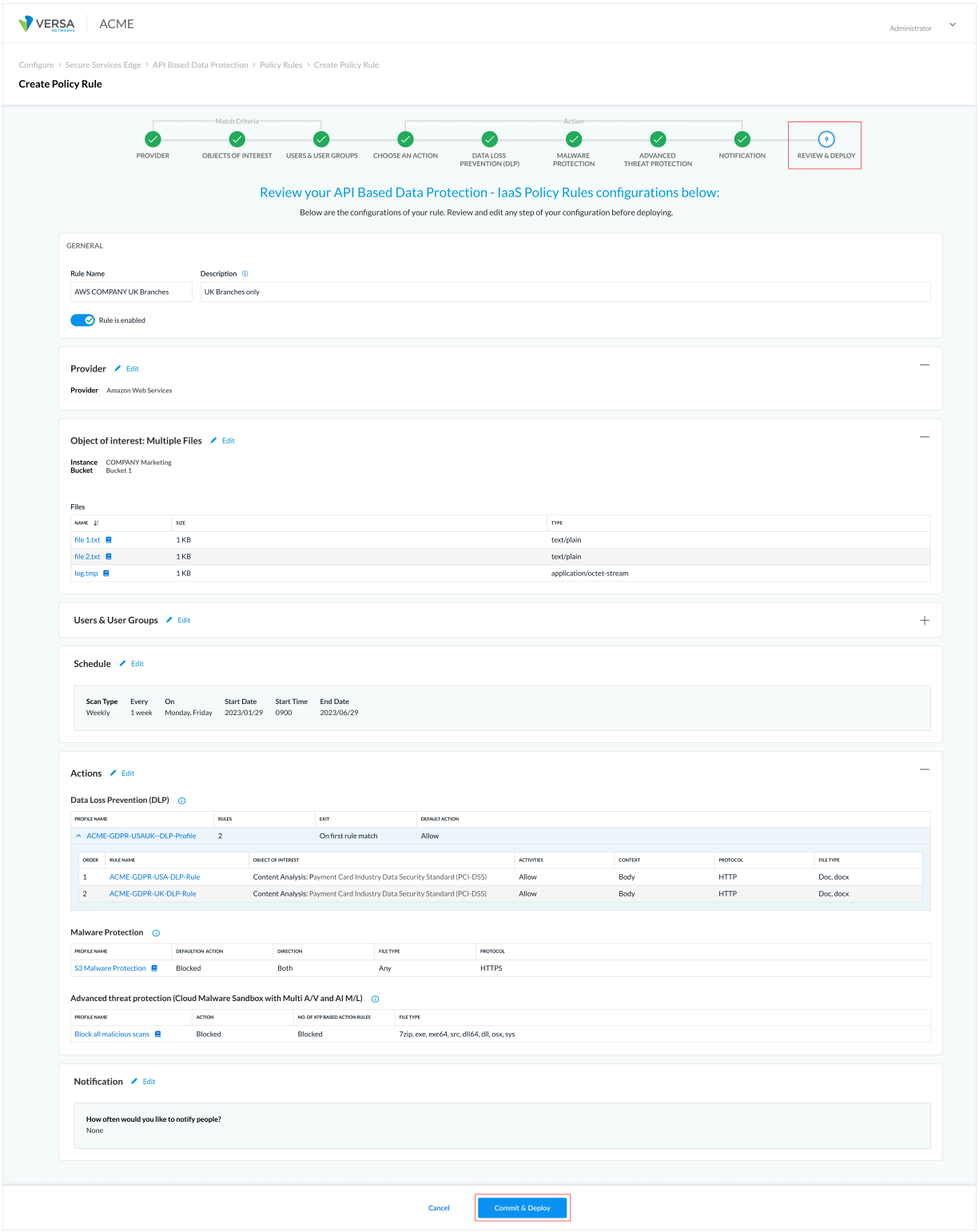
22. Click Select Profile. The Notification Profiles screen displays.



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



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



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