Arista VeloCloud Edge Threat Management Guide

Version 7.0.1

Arista.com

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA +1-408-547-5500	+1-408-547-5502 +1-866-476-0000	+1-408-547-5501 +1-866-497-0000
www.arista.com/en/	support@arista.com	sales@arista.com

© Copyright 2026 Arista Networks, Inc. All rights reserved. The information contained herein is subject to change without notice. The trademarks, logos, and service marks ("Marks") displayed in this documentation are the property of Arista Networks in the United States and other countries. Use of the Marks is subject to the Arista Networks Terms of Use Policy, available at www.arista.com/en/terms-of-use. Use of marks belonging to other parties is for informational purposes only.

Contents

Chapter 1: Edge Threat Management Overview..... 1

Chapter 2: Prerequisites.....2

Chapter 3: Access Edge Threat Management.....3

Chapter 4: Monitor Edge Threat Management.....5

4.1 Security Overview.....5
4.2 Edge Reports.....6
4.3 Alerts.....9
4.4 Audit.....10
4.5 Notifications..... 11
4.6 Tasks..... 11

Chapter 5: Configure Policy Manager.....13

5.1 Configure Security Profiles.....13
Create a Security Profile.....14
Provision Security Profiles.....16
Export and Import Profiles.....16
5.2 Configure Policies.....16
Create New Policy..... 16
5.3 Configure Rules and Conditions..... 19
Create Rules..... 19
Create Conditions.....23
5.4 Configure Templates..... 24
Create New Template.....25
Manage Templates.....26
5.4.1 Template Configuration Examples.....27
5.5 Configure Objects.....39
Create New Object.....39
Manage Objects and Object Groups..... 40
5.5.1 Object Type Configurations..... 40

Chapter 6: Provision Edge Threat Management.....48

Chapter 7: Service Settings..... 51

7.1 Alert Rules.....51
7.2 Notification Profiles.....52

Chapter 1

Edge Threat Management Overview

Edge Threat Management (ETM) provides an integrated, AI-powered security solution for secure SD-Branch networking. The service evolves the Enhanced Firewall Service (EFS) by introducing advanced policy management, dynamic blocklists, and dedicated operational dashboards.

Edge Threat Management (ETM) vs Enhanced Firewall Service (EFS)

ETM is a new Enterprise application within Orchestrator that manages Security Profiles and provides a dedicated dashboard for security operations. It builds on the existing EFS features, including IDS/IPS, Web Filtering, and threat-reputation services, by adding greater configuration flexibility and extending security capabilities.

Within each SD-WAN Profile, the administrator can choose between Edge Threat Management or Enhanced Firewall Services. New deployments use ETM as the default, while existing deployments based on EFS may continue using EFS and can upgrade to ETM at any time.

Supported Edge Platforms

The following Edge platforms support ETM for VeloCloud:

- Edge 710W / 710-5G
- Edge 720
- Edge 740
- Edge 4100
- Edge 5100
- Virtual / Cloud

Chapter 2

Prerequisites

Configuring Edge Threat Management requires the following prerequisites.

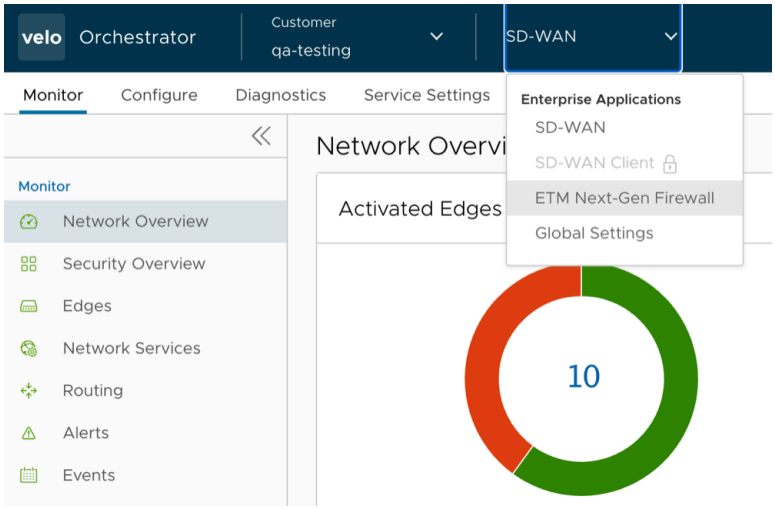
- **Activate ETM Next-Gen Firewall feature**: Only an Operator can activate the ETM feature for the Customers and Partners. Hence, to activate this feature, contact your Operator.
- **Provision a new Edge**: In the **SD-WAN** service of the Enterprise portal, go to **Configure** > **Edges**, and then click **Add Edge**. For more information, see the topic *Provision a New Edge* in the *Arista VeloCloud Administration Guide.*

Access Edge Threat Management

VeloCloud Orchestrator hosts Edge Threat Management (ETM) within a dedicated Enterprise application. This enables security operations administrators to focus on building security-specific profiles and monitoring the network's overall security health.

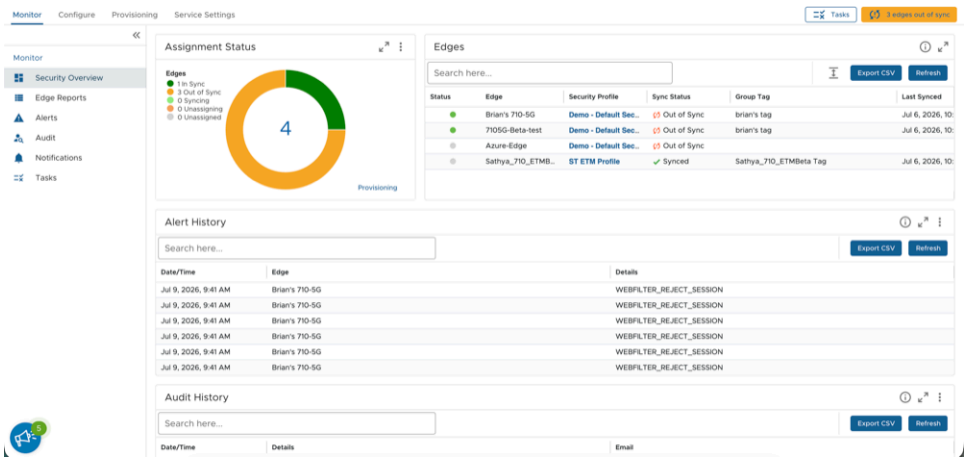
To access the ETM application from the VeloCloud Orchestrator, go to the **Enterprise Applications** drop-down menu and select **ETM Nex-Gen Firewall**.

Figure 3-1: ETM Nex-Gen Firewall



The ETM dashboard appears:

Figure 3-2: ETM Dashboard



The following are some of the common features across all of the ETM Dashboard screens:

- **Export CSV**: Click this button to export the data into a CSV file.

- **Refresh**: Click this button to refresh the data.
- **Search**: Enter a text to locate a specific item.
- **Tasks**: Click this button to review all the active tasks.
- **Column Options**: Each column in a data grid includes a three-line menu that allows users to refine the data in the columns.

Table 1: Column Options

Option	Description
Filter	Apply filters to the list of entries as required.
Pin	Pin/unpin a column to either the left or the right.
Columns	Select/clear columns to be displayed on the screen.
Toolbar	Move or hide the toolbar.
Refresh	Refresh the data.
Export CSV	Export data to a CSV file.



Note: The **Refresh** and **Export CSV** options are also located at the top right of all ETM screens.

The various configuration options available on the ETM dashboard are explained in the following sections.

- Monitor Edge Threat Management
- Configure Security Profiles
- Provision Edge Threat Management
- Service Settings

Chapter 4

Monitor Edge Threat Management

The Edge Threat Management dashboard displays the **Monitor** screen by default.

The **Monitor** screen allows monitoring the following functions:

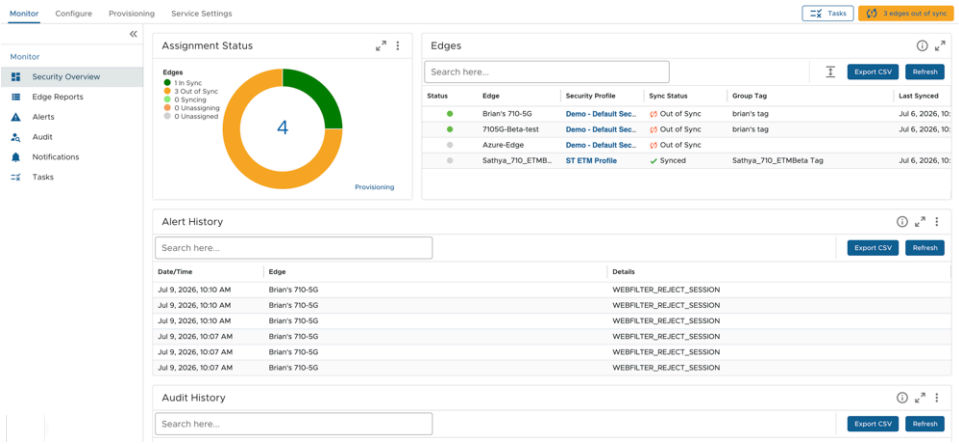
- Security Overview
- Edge Reports
- Alerts
- Audit
- Notifications
- Tasks

4.1 Security Overview

The **Monitor Security Overview** screen provides a quick review of the security health of the user's network. This helps the security administrator identify Edges that lack the latest Security Profile and prioritize urgent security events.

The ETM dashboard displays the **Monitor** > **Security Overview** screen by default.

Figure 4-1: Monitor Security Overview



The following primary features are available on this screen:

Table 2: Monitor Security Overview

Feature	Description
Assignment Status	Displays the Edge assignment status. Example: In Sync, Out of Sync, Syncing, Unassigned, and so on. Users can directly access the **Provisioning** screen from this section.
Edges	Displays the list of Edges along with their Security Profiles, Sync details, Group Tag, Serial Numbers, and Locations. Clicking on a Security Profile directs users to the **Configure** > **Security Profile** screen.
Alert History	Displays the list of alerts generated by the Edges along with Date/Time details. Similar alerts are grouped into 15-minute intervals. Select an entry to view additional information.
Audit History	Displays the list of account activities. Select an entry to view additional information.
Policy Analytics	Displays the analytics information for the security policy. Users can view the Issue, Severity, Recommendation, and Date Created. Clicking the **Review** arrow in the **Action** column opens the **Edit Rule** screen. Click the delete icon to remove an issue from the list. To initiate the analysis, click the **Analyze** button. To check the status of the analysis, click the **Tasks** option located at the top right of the **Monitor** screen.

Click the double arrow located at the top right of each section to expand it for a better view.

4.2 Edge Reports

The **Monitor Edge Reports** screen monitors consolidated bandwidth usage, web activities, and security events across all managed networks. It helps analyze aggregated data from all Edges or review site-specific reports to evaluate precise network flows.

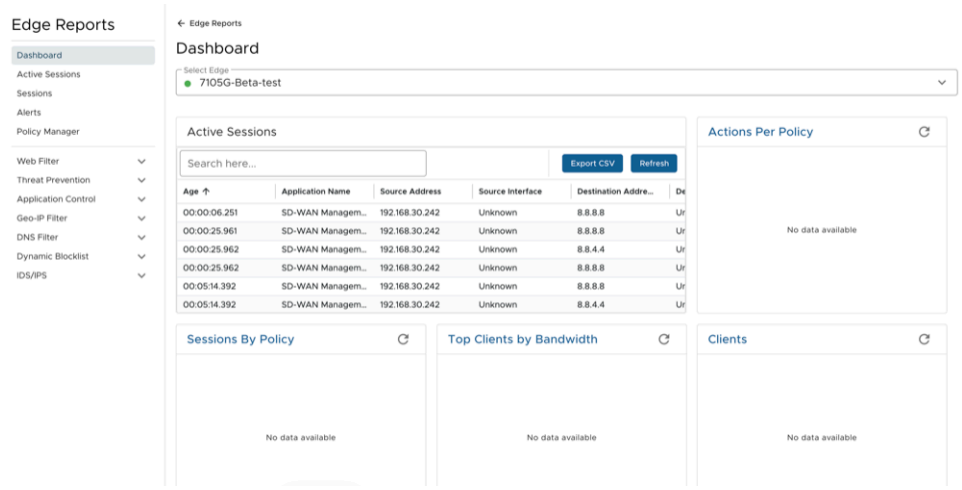
To access the **Edge Reports** screen, select **Monitor** > **Edge Reports** on the ETM dashboard.

Figure 4-2: Monitor Edge Reports



Select a report to review security events and flows occurring on the network managed by that Edge. The **Dashboard** view appears by default.

Figure 4-3: Edge Report Details



Filter the view by either of the following options:

- **Active Sessions**: Displays the details for active Edge sessions only.
- **Sessions**: Displays the details for all the sessions. Select the **From** and **To** dates, and then click **Apply** to retrieve data from a particular time period for all sessions. Users can also refine this data based on **Reject**, **Block**, and **Alert** action filters.
- **Alerts**: Select the **From** and **To** dates, and then click **Apply** to retrieve alert details from a particular time period.
- **Policy Manager**: Select the **From** and **To** dates, and then click **Apply** to retrieve Security Policy details from a particular time period.

Some additional filter types for viewing the reports include:

Table 3: Edge Reports - Filter Types and Subtypes

Filter Type	Subtype	Description
Web Filter	Summary	Displays the list of Clients, Sites, and Categories. Users can also refine this data based on **Reject**, **Block**, and **Alert** action filters.
	Visited Sites	Select a reason (Block Category, Block List, Pass Category, Pass List, or All) from the **Reason** drop-down menu to display site information such as Time Stamp, Site, Source and Destination Addresses, Verdict, Action, and Category. Users can also refine this data based on **Reject**, **Block**, and **Alert** action filters.
IP Reputation	Summary	Displays the list of IP addresses by Time and the top addresses by Count. Users can also refine this data based on **Reject**, **Block**, and **Alert** action filters.
	Sessions	Select a direction (All, Inbound or Outbound) from the **Direction** drop-down menu to display session information such as Time Stamp, Direction, Source and Destination Addresses, Host, Reputation Score, Verdict, Reason, and Action. Users can also refine this data based on **Reject**, **Block**, and **Alert** action filters.
URL Threat Prevention	Blocked Summary	Displays the list of Blocked IP addresses / Domains by Time and Top Addresses By Blocked Count.
	Blocked Addresses	Displays information such as Time Stamp, Direction, Source Address, Blocked Address, and Reputation Score.
	Rejected Summary	Displays the list of Rejected IP addresses by Time and Top Addresses By Rejected Count.
Application Control	Applications	Displays information such as Time Stamp, Name, Verdict, Action, Source and Destination Addresses, Source Port, and Destination Port. Users can also refine this data based on **Reject**, **Block**, and **Alert** action filters.
Geo-IP Filter	Sessions	Select a direction (All, Inbound, or Outbound) from the **Direction** drop-down menu to display session information such as Time Stamp, Direction, Source and Destination Addresses, Source and Destination Countries, Destination DNS Cache, Verdict, and Action. Users can also refine this data based on **Reject**, **Block**, and **Alert** action filters.
	Outbound Blocked Countries	Displays the list of Blocked Countries by Time and Countries by Blocked Count.
	Inbound Blocked Countries	Displays the list of Blocked Countries by Time and Countries by Blocked Count.
	Distribution Map	Displays the Distribution Map, Outbound Blocked Sessions, and Inbound Blocked Sessions.
DNS Filter	Summary	Displays DNS Filter Top Blocked Domains, DNS Filter Top Visited Domains, DNS Filter Top Clients by Blocked Domains, and DNS Filter Top Clients by Visited Domains.
	Visited Domains	Displays information such as Time Stamp, Verdict, Action, Domain, Source and Destination Addresses. Users can also refine this data based on **Reject**, **Block**, and **Alert** action filters.
Dynamic Blocklist	Blocked Summary	Displays Blocked IP addresses / Domains by Time, Top Addresses By Blocked Count, and Top Domains By Blocked Count.
	Blocked Addresses	Displays information such as Time Stamp, Verdict, Action, Source and Destination Addresses, Host, and Blocklist Entry. Users can also refine this data based on **Reject**, **Block**, and **Alert** action filters.
IDS/IPS	Summary	Displays Signature information, Total IDPS Triggers, IDPS Events by Time, IDPS Events by Client, and IDPS Triggers by Class Type.
	IDS/IPS Events	Displays information such as Time Stamp, Verdict, Action, Source and Destination Addresses, Client and Server Ports, Severity, Signature, SID, and IPS Action.

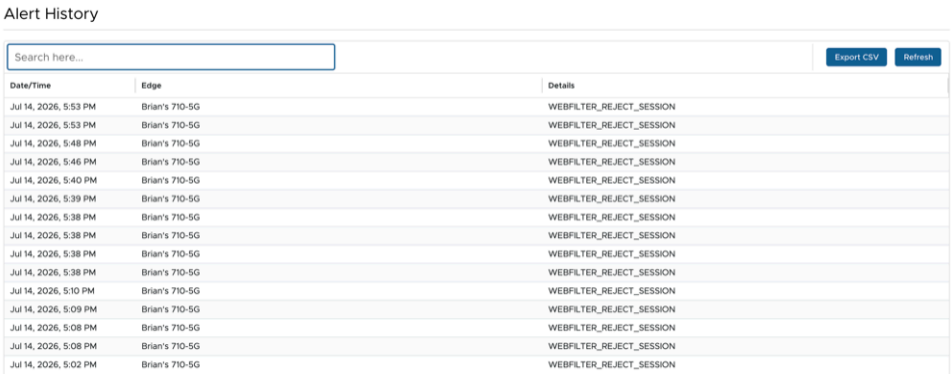
Note: All these filter subtypes also include **From** and **To** date options to retrieve data for a specific time period.

4.3 Alerts

The **Monitor Alerts** screen displays activities from Edge Threat Management appliances connected to the user's account.

To access the **Alerts** screen, select **Monitor** > **Alerts** on the ETM dashboard.

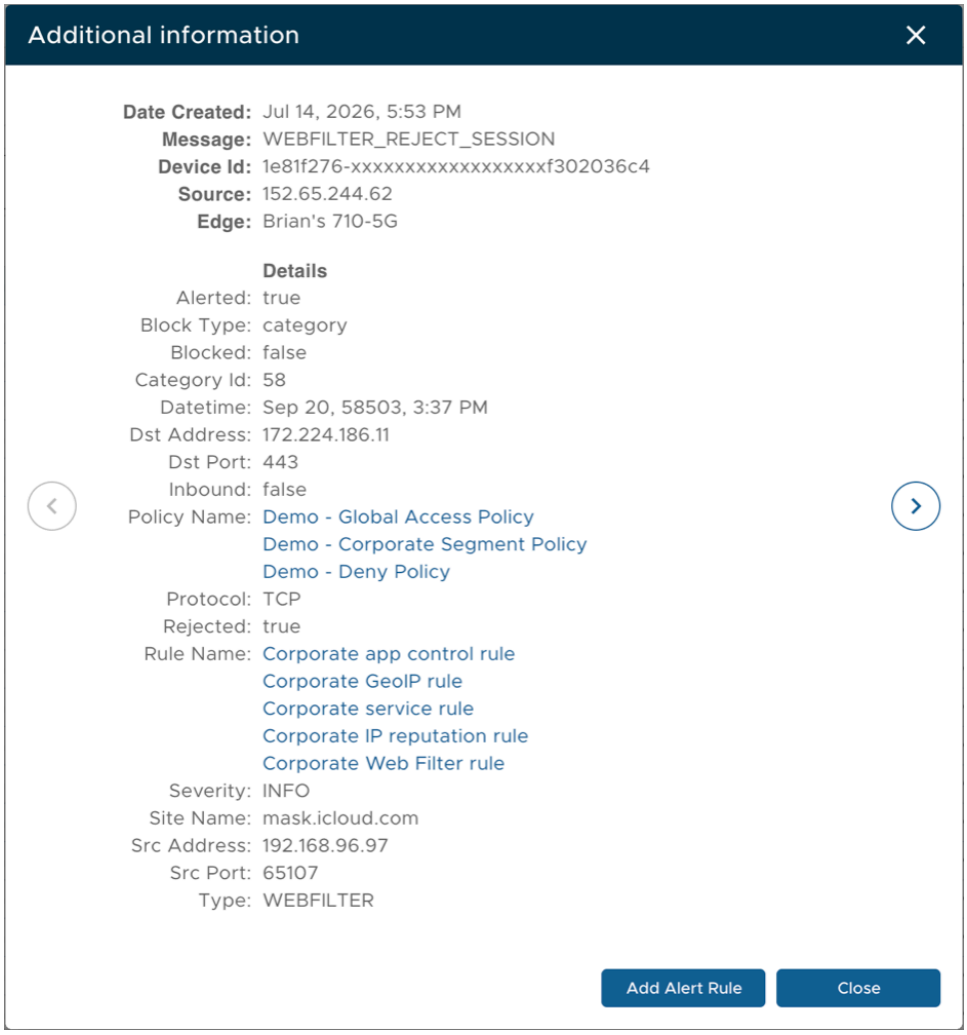
Figure 4-4: Monitor Alerts



The **Alert History** provides a log of security events and other types of built-in ETM processing activities. For example, a blocked session due to Geo-IP Filtering or Web Filter may generate an alert. Security Rules and Templates have individual settings to enable alerting for related events.

Select an Alert event to view additional alert information.

Figure 4-5: Additional Alert Information



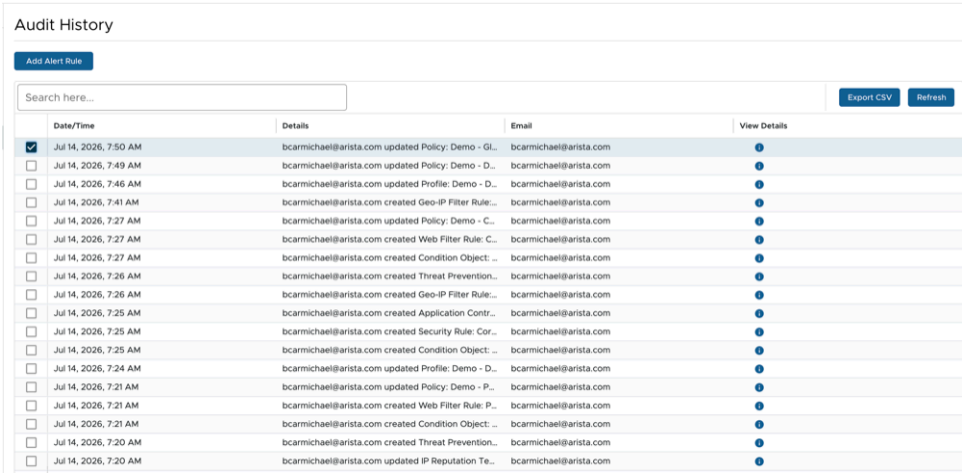
The **Add Alert Rule** button creates rules for receiving alerts. This helps in determining which events route to the selected Notification Profiles. For more information, see Service Settings. Click **Close** to close the **Additional Information** window.

4.4 Audit

The **Monitor Audit** screen displays activities such as logins or configuration changes to appliances. This allows other users to manage appliances in the account and enables auditing of their activities.

To access the **Audit** screen, select **Monitor** > **Audit** on the ETM dashboard.

Figure 4-6: Monitor Audit



The **Audit History** provides a log of ETM audit events, such as template updates or policy assignments to Security Profiles.

Select an audit event and click **Add Alert Rule** to configure custom notifications for that event. For more information, see Service Settings.

Click the link under the **View Details** column to view additional audit information.

4.5 Notifications

The **Monitor Notifications** screen displays a list of all processed notifications.

To access the **Notifications** screen, select **Monitor** > **Notifications** on the ETM dashboard.

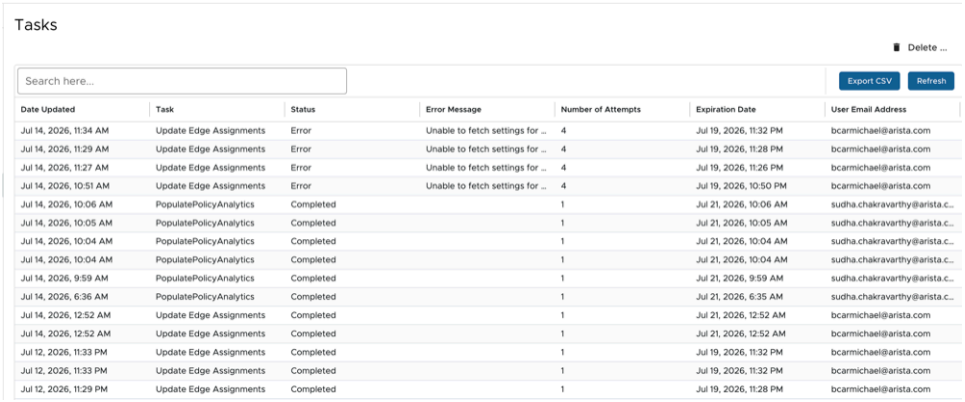
The **Notification Log** reports when each alert message occurs and which **Notification Profile** it uses. This information confirms whether the account sends alerts and delivers them successfully.

4.6 Tasks

The **Monitor Tasks** screen displays a list of user-initiated tasks, along with information such as Date, Status, Error Message, Number of Attempts, and more.

To access the **Tasks** screen, select **Monitor** > **Tasks** on the ETM dashboard.

Figure 4-7: Monitor Tasks



Note: The **Tasks** screen can also be accessed by clicking the **Tasks** button at the top right of the **Monitor** screen.

Click the **Delete** button to delete one or more tasks.

Chapter 5

Configure Policy Manager

Configure Policy Manager to define, manage, and enforce network security and access rules across the infrastructure.

The ETM Security configuration process starts with analyzing network flows to ensure the firewall has clear visibility into each flow's context. Next, users can create objects and templates, which serve as the foundation for policy rules. After these objects and templates are defined, the next step is to configure the policies. These policies specify the rules that determine what is permitted on the network. After the policies are configured, users can compile them into a Security Profile. This Security Profile organizes all the rules and templates that constitute the complete security configuration. The final step involves associating Edges with the Security Profile and provisioning them according to the established configuration.

This topic contains the following sections:

- Configure Security Profiles
- Configure Policies
- Configure Rules and Conditions
- Configure Templates
- Configure Objects

5.1 Configure Security Profiles

A Security Profile is a grouping of one or more Policy Objects, including Policies, Rules, and Templates. A Security Profile is configured entirely in the ETM Dashboard and enables the Enterprise Admin to configure Security Profiles to assign Policies and Templates to one or more Edges.



Note: An Edge device can belong to only one Security Profile.

Security Profiles bring together all the security configurations provisioned for all Edges associated with the Profile. Users must add a Security Profile to provision any ETM configuration to Edges. For more information, see Provision Edge Threat Management.

Security Profiles enable users to:

- Add policies
- View the complete collection and order of rules
- Assign Security Profile templates
- Confirm all Edges that the Profile provisions

- Obtain answers about the profile using the Ask AVA AI assistant

Create a Security Profile

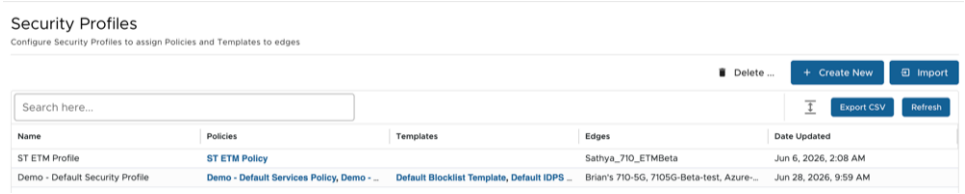
To create a Security Profile, perform the following steps:

1. Log in to the VeloCloud Orchestrator as an Enterprise User.
2. To access the ETM application from the VeloCloud Orchestrator, go to the **Enterprise Applications** drop-down menu and select **ETM Nex-Gen Firewall**.
3. Navigate to **Configure** > **Security Profiles**.

   The **Security Profiles** page appears.

   The **Security Profiles** page displays a listing of all Security Profiles and details which policies and templates each contains, and the Edges the Profile is assigned to, and its last edited date. Users can also create a new Security Profile using the **Create New** button. The table's contents can be refreshed or exported as a comma-separated (CSV) file using the buttons along the top.

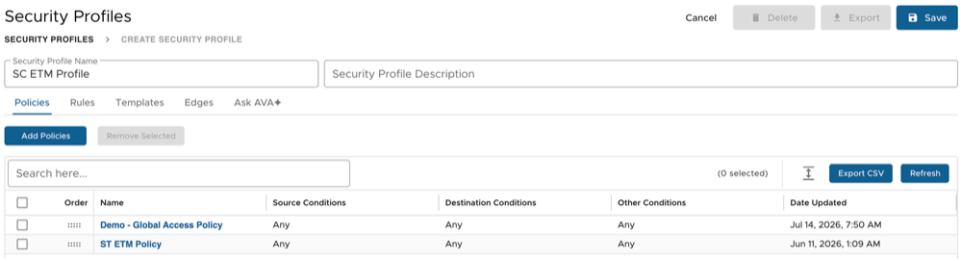
   Figure 5-1: Security Profiles



4. To create a Security Profile, click **Create New**.

   The **Create Security Profile** page appears.

   Figure 5-2: Create Security Profile - Policies Tab

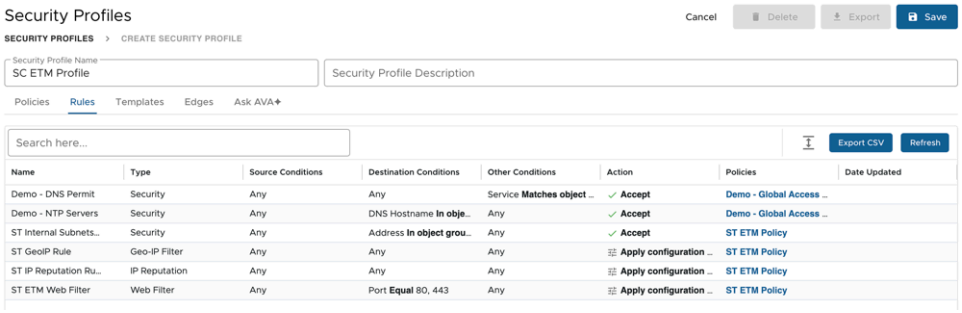


5. In the **Security Profile Name** field, enter a unique name for the Profile.
6. In the **Security Profile Description** field, describe the Security Profile.
7. The **Policies** tab enables users to view, add, reorder, or remove policies in the Profile. In the **Policies** tab, click **Add Policies** to choose one or more policies to associate with this Profile. When combining multiple policies in a Profile, the order of the policies is important because the rules are evaluated from top to bottom, and users can confirm this when viewing rules.

   For more information on creating a Policy, see Configure Policies.

8. The **Rules** tab automatically populates all the rules across all the policies in the Profile.

Figure 5-3: Create Security Profile - Rules Tab

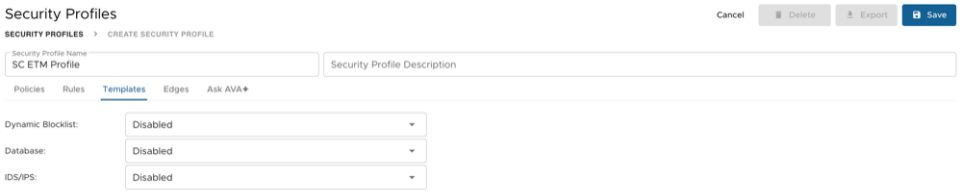


For more information on creating rules, see Configure Rules and Conditions.

9. The **Templates** tab enables users to assign Security Profile templates. This includes Dynamic Blocklist, Database, and IDS/IPS templates configuration. By default, *Disabled* is selected. If users have configured any custom templates, they appear as options in the respective Templates drop-down.

   These types of Profile templates apply unconditionally to all traffic. For example, if users apply an IPS template, it will affect all traffic.

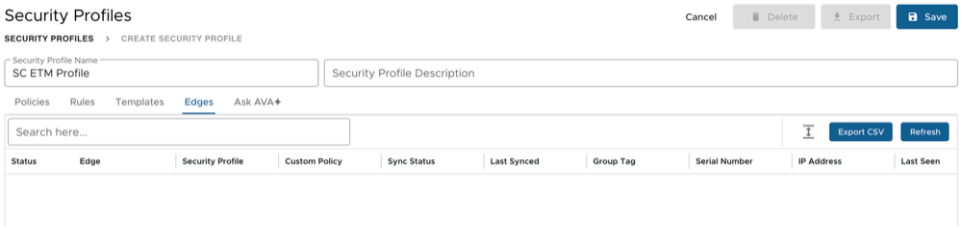
Figure 5-4: Create Security Profile - Templates Tab



For more information about Objects and Templates, see Configure Templates and Configure Objects.

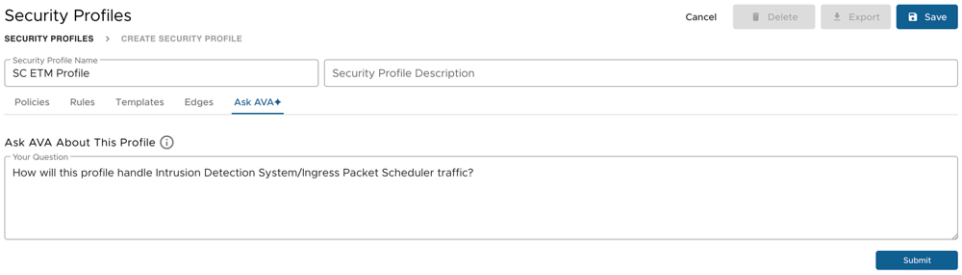
10. The **Edges** tab displays all Edges assigned to the Security Profile. The grid provides details about each Edge, including the online status, the last time the Security Profile was updated, and the status of the most recent Profile push. The **Search here** field enables to find specific Edges assigned to the Security Profile.

Figure 5-5: Create Security Profile - Edges Tab



11. Click **Ask AVA** to ask any questions about this Profile. The **Ask AVA** feature enables the admin to ask questions about the Security Profile to quickly obtain information about the Profile, rather than attempting to interpret the Policy from a list of rules.

Figure 5-6: Create Security Profile - Ask AVA Tab



12. Click **Save** to finish creating a Security Profile.

Provision Security Profiles

Profiles are pushed to Edges via the **Provisioning** feature. For more details, refer to Provision Edge Threat Management.

Export and Import Profiles

Profiles can be exported via the **Export** button in the configuration screen for the desired Profile, creating a JavaScript Object Notation (JSON) configuration file that can be imported via the **Import** button in the main **Profiles** tab.

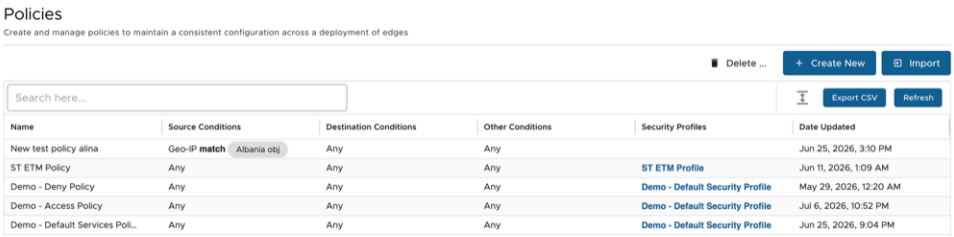
5.2 Configure Policies

Create and manage policies in the ETM Dashboard to maintain consistent configurations across multiple Edge deployments. Apply these policies to synchronize network settings and minimize initial setup time.

A Policy can be used to apply or synchronize network or service settings; to ensure new deployments are activated with minimal initial configuration time; and to enforce consistency across an environment with multiple Edge deployments.

The **Policies** page displays a listing of all current Policies and the **Create New** option. The table's contents can be refreshed or exported as a comma-separated (CSV) file using the buttons at the top.

Figure 5-7: Policies



Create New Policy

Admin users can create a new Policy to create exceptions, Policies specific to certain deployments or situations, or other instances.

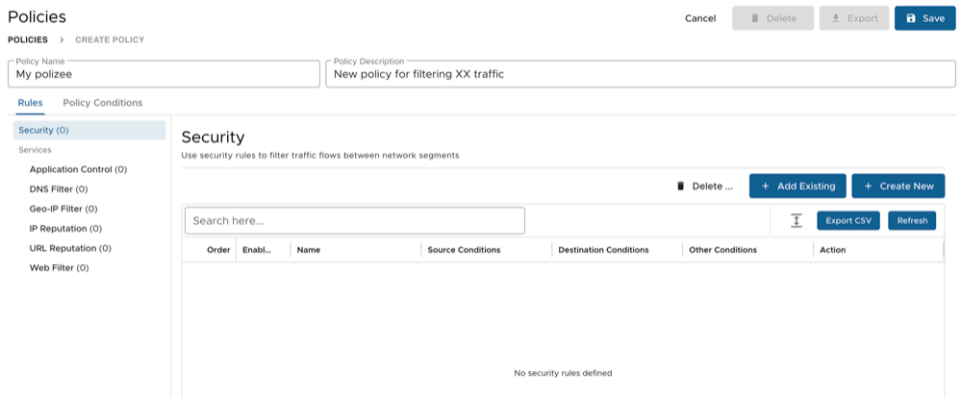
To create a Security Policy, perform the following steps:

1. Log in to the VeloCloud Orchestrator as an Enterprise User.
2. To access the ETM application from the VeloCloud Orchestrator, go to the **Enterprise Applications** drop-down menu and select **ETM Nex-Gen Firewall**.
3. Navigate to **Configure** > **Policies**.

   The **Policies** page appears.
4. To create a new Security Policy, click **Create New**.

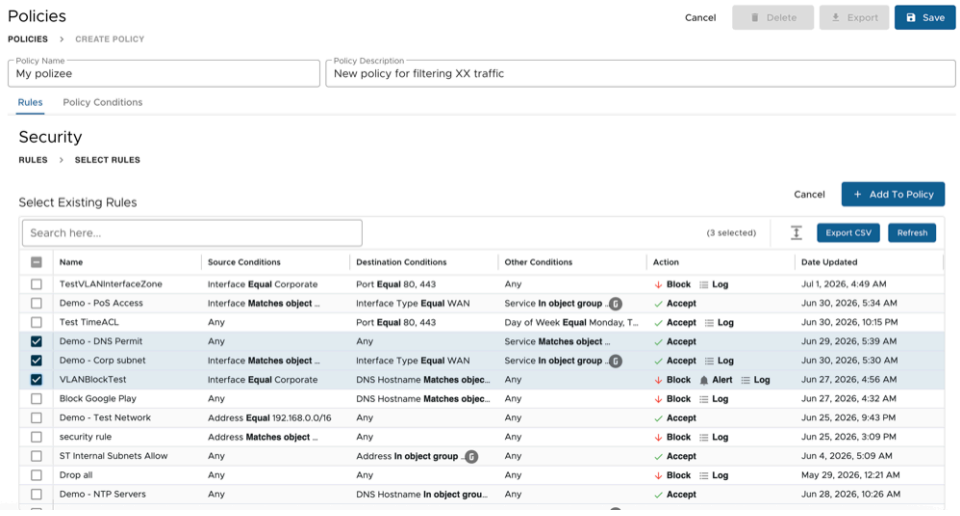
   The **Create Policy** page appears.

   Figure 5-8: Create Policy



5. In the **Policy Name** field, enter a unique name for the Policy.
6. In the **Policy Description** field, describe the Security Policy.
7. In the **Rules** tab, users can add **Security** and **Services** rules to the Policy to filter traffic flows between network segments.
8. To add Security rules to the Policy, click **Security** and then select **Add Existing**. The **Select Existing Rules** page appears.

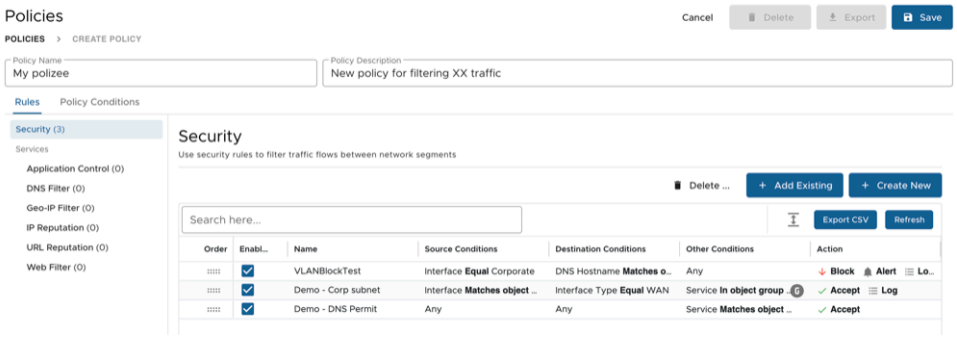
   Figure 5-9: Select Existing Security Rules



9. Select one or more existing Security rules and click **Add To Policy** to associate the rules with the Policy. You can also choose to create a new Security rule. For more information, see Configure Rules and Conditions.

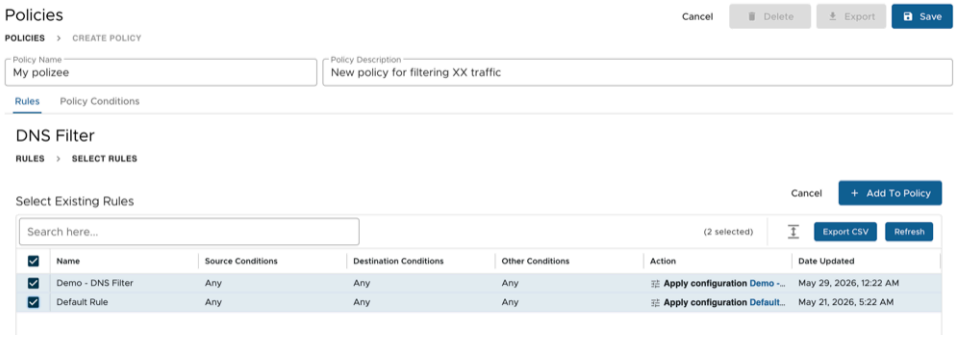
The selected rules get added to the **Security Rules** grid.

Figure 5-10: Security Rules Grid



10. Users can also add Service rules to the Policy. Service rules apply policy templates to Policies. To add Service rules to the Policy, under **Services** click the Service filter (for example, DNS Filter) and then select **Add Existing**. The **Select Existing Rules** page appears.

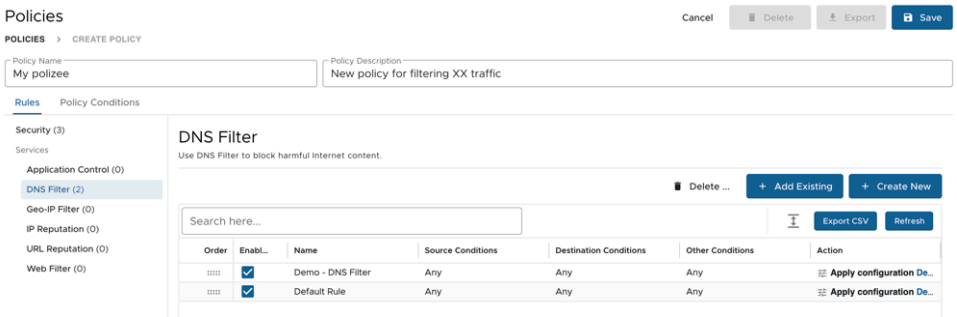
Figure 5-11: Select Existing Services Rules



11. Select one or more existing Service rules and click **Add To Policy** to associate the rules with the Policy. You can also choose to create a new Service rule. For more information, see Configure Rules and Conditions.

    The selected rules get added to the **Services Rules** grid.

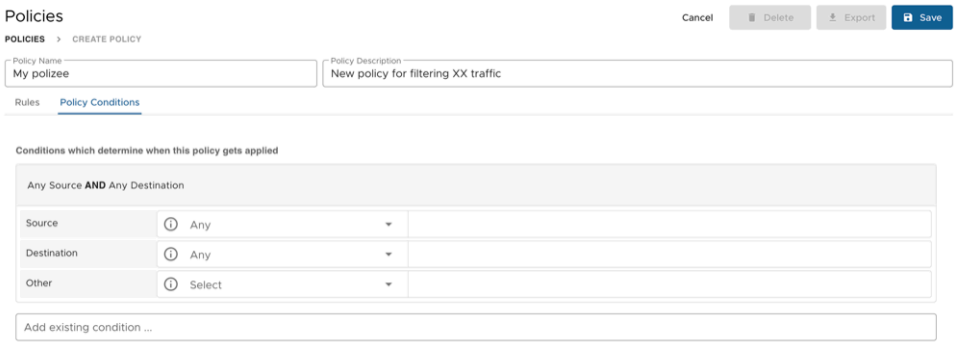
Figure 5-12: DNS Filter Rules Grid



12. Click the **Policy Conditions** tab to define a global condition that the firewall engine evaluates before any rules in the Policy are evaluated. This adds a layer of flexibility, allowing users to exclude an entire Policy if a specific condition is not met.

ETM supports many conditions that may be applied to either the source or destination of a session, or generally to both. Users can add multiple types of conditions to a Policy rule, and the summary at the top of the Policy provides a simplified explanation of the rule logic.

Figure 5-13: Policy Conditions



For more information about Policy Condition types, see Configure Rules and Conditions.

13. Click **Save** to finish creating a Security Policy.

5.3 Configure Rules and Conditions

The Edge Thread Management (ETM) Dashboard enables the Admin to create and manage rules and conditions to use in policies.

There are two types of rules:

- **Security Rule** - Determines what traffic is permitted across the user's network based on rule conditions and corresponding actions.
- **Service Rule** - Processes traffic that is permitted by Security rules and maintains its own set of conditions. For example, to block malicious web content based on URL categories, users need to add a Web Filter service rule in their policy.

> **Note:** Service rules apply policy templates as actions into policies.

Create Rules

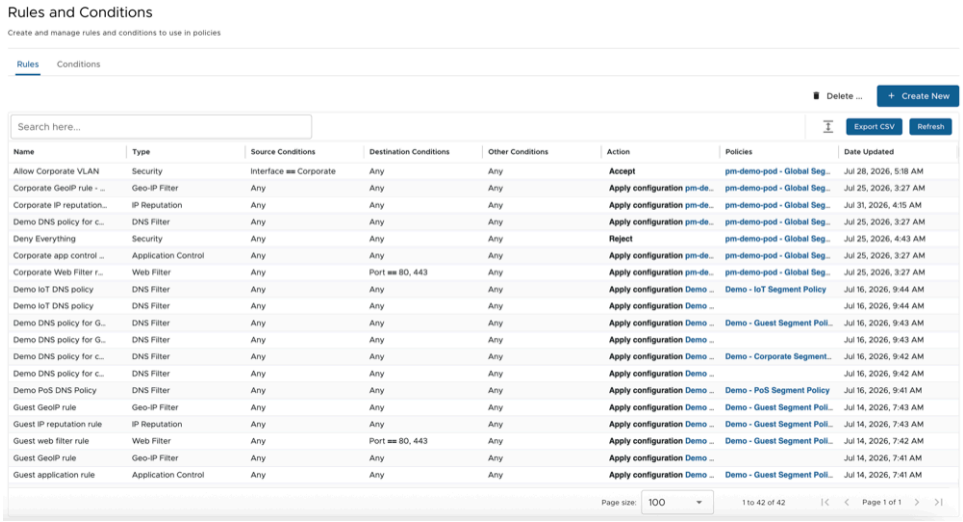
Users can create a **Security** and **Services** rules to use in a policy to filter traffic flows between network segments.

To create a new rule, perform the following steps:

1. Log in to the VeloCloud Orchestrator as an Enterprise User.
2. To access the ETM application from the VeloCloud Orchestrator, go to the **Enterprise Applications** drop-down menu and select **ETM Nex-Gen Firewall**.
3. Navigate to **Configure** > **Rules and Conditions**.

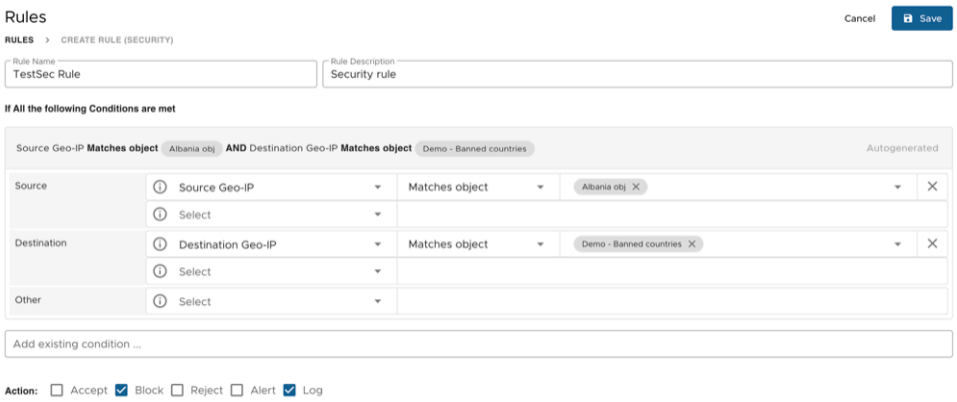
The **Rules and Conditions** screen appears.

Figure 5-14: Rules and Conditions - Rules Tab



4. To create a new **Security** Rule, click **Create New** > **Security Rule**.
   The **Create Rule - Security** screen appears.

   Figure 5-15: Create Rule - Security



5. In the **Rule Name** field, enter a unique name for the rule.
6. In the **Rule Description** field, describe the rule.
7. Define the rule's conditions and actions. ETM supports many conditions that may be applied to either the source or destination of a session, or generally to both. Users can add multiple types of conditions to a policy rule, and the summary at the top of the policy provides a simplified explanation of the rule logic.

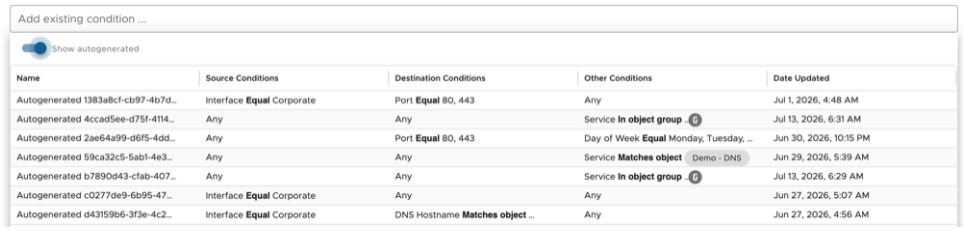
   The following table describes each condition type.

Table 4: Policy Condition Types and Descriptions

Type	Description
Source/Destination	
Address	A custom list of IPs, ranges, or CIDR notated subnets or a defined IP address object.
Custom Application	A selection from the defined Custom application objects.
DNS	A single hostname or a defined hostname object.
Geo-IP	A selection from the list of built-in countries or a Geo-IP object.
Interface	A specific physical/virtual interface by name or a defined interface zone object.
Interface Type	A selection from the list of built-in interface types.
Port	A custom list of ports or ranges.
Service	A selection from a defined service object.
VLAN Id	A comma separated list of VLAN IDs.
VLAN Type	A selection of built-in options (Local or Remote).
Other	
Application Category	An application category from the list of built-in classifications.
Application Name	An application from the list of built-in classifications.
Custom Application	A selection from the defined Custom application objects.
Day of Week	A selection of days of the week.
DSCP	A selection from the list of built-in Differentiated Services Code Point (DSCP) values.
IP Protocol	A selection from the list of built-in protocols (e.g. ICMP, GRE, L2TP, and so on).
MAC Address	A single MAC address.
Segment	A segment name or defined segment object.
Service	A selection from a defined service object.
Time of Day	A selection of the time of day.

Users can also select and add an existing condition to the rule by clicking **Add existing condition**.

Figure 5-16: Add Existing Conditions



8. The action depends on the type of rule (Security or Service). Service rules apply a policy template as the action. When assigning a policy template, users can edit the selected template or create a new one. The following actions apply to Security rules.

Table 5: Security Rule Actions

Action	Description
Accept	Permit the session.
Block	Drop the session without sending any denial response. This causes the client application to time out.
Reject	Deny the session by sending an ICMP “Port Unreachable” message. This causes the client application to report a connection error to the user immediately.
Alert	Include the session event as an alert.
Log	Record the session event in the reports.

9. Users can also create **Service** Rules. Service rules process traffic permitted by Security rules and maintain their own set of conditions.

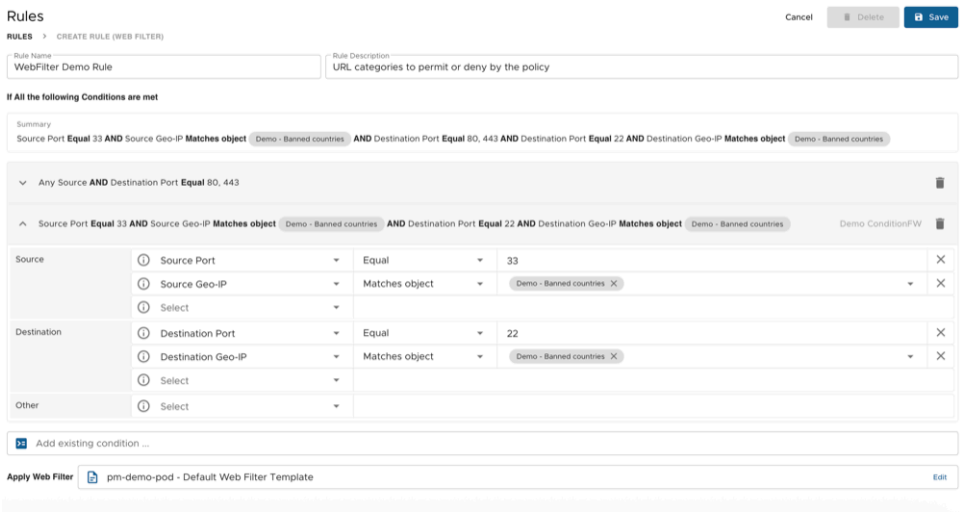
   The Edge Threat Management (ETM) feature supports the following Service filter templates:

   - Application Control - Use an Application Control template to define which applications the policy permits or denies.
   - DNS Filter - Use DNS Filter to block harmful Internet content.
   - Geo-IP Filter - Use a Geo-IP Filter template to define which countries to block or allow by the policy.
   - IP Reputation - Use IP Reputation to block high-risk IPs with a poor reputation.
   - URL Reputation - Use URL Reputation to block high-risk sites with a poor reputation.
   - Web Filter - Use a Web Filter template to define which URL categories to permit or deny by the policy.

10. For example, to create a new Web Filter Service rule, click **Create New** > **Services** > **Web Filter**.

    The **Create Rule - Web Filter** page appears.

    Figure 5-17: Create Rule - Web Filter



11. Enter a rule name and description, and define the rule conditions for the source or destination of a session, or both, that must be met to apply a specified filter.

    Optionally, users can select and apply an existing condition to the rule by clicking **Add existing condition**. To apply a Web Filter Template to the rule, click **Apply Web Filter** and from the list of available templates select a filter template to associate to the rule.

12. Click **Save**.

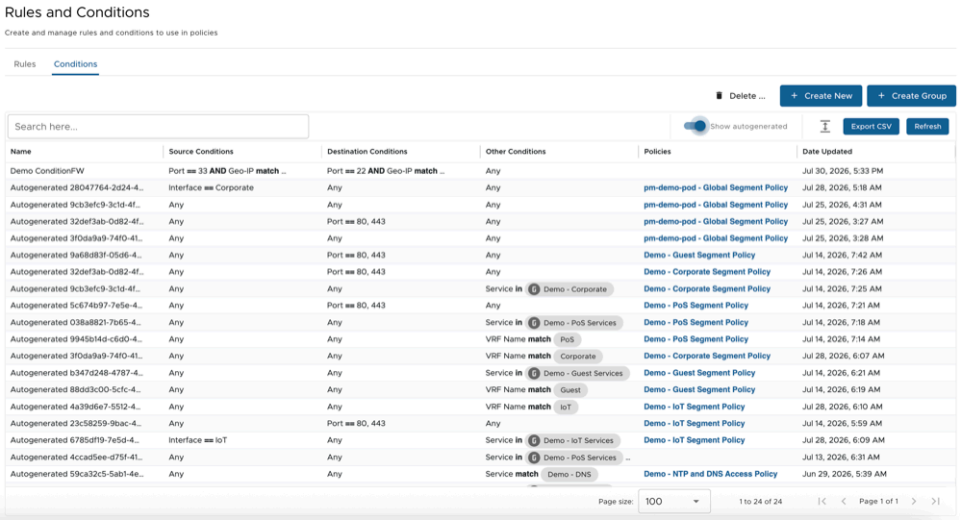
Create Conditions

Users can create conditions to use across multiple policy rules.

To create a new Condition, perform the following steps:

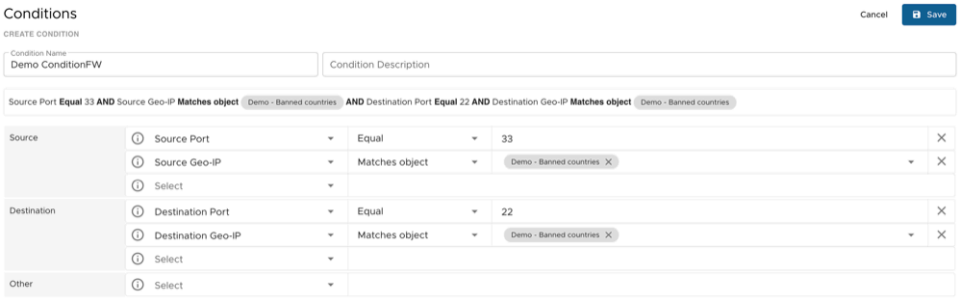
1. Navigate to **Configure** > **Rules and Conditions** > > **Conditions**. The **Conditions** screen displays a list of all current conditions and the **Create New** option.

   Figure 5-18: Rules and Conditions - Conditions Tab



2. To create a new Condition, click **Create New**.

   Figure 5-19: Create Conditions



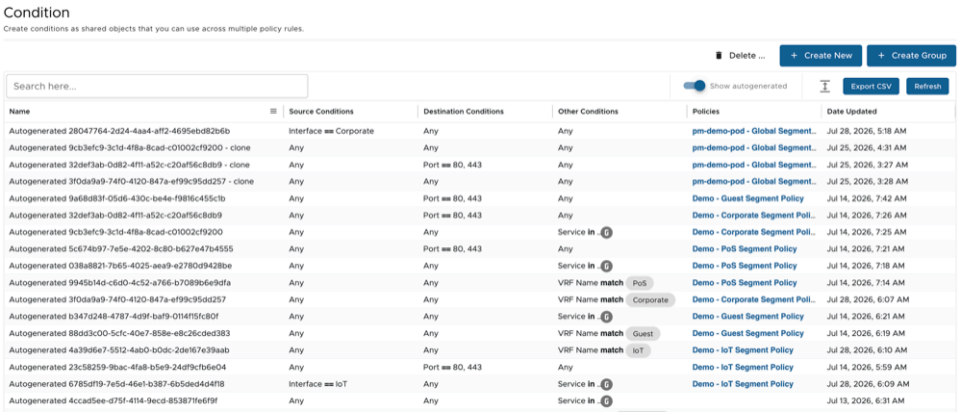
3. Provide a Name and Description for the Condition and configure the following required parameters:
   - From the **Source** drop-down menu, select the Source parameters and define the conditions to use in policy rules.
   - From the **Destination** drop-down menu, select the Destination parameters and define the conditions to use in policy rules.
   - From the **Other** drop-down menu, select the other parameters and define the conditions to use in policy rules.

   After configuring all the necessary conditions to use in policy rules, click **Save**.
4. To create a new Condition Group, click **Create Group**. Provide a Name and Description for the Condition Group and click **Save**.

5. To view the auto-generated conditions, turn on the **Show autogenerated** button.

> **Note:** The autogenerated conditions are created each time a new rule is created.

Figure 5-20: Show Autogenerated Conditions



5.4 Configure Templates

A Template is a complete set of configuration options for a specific service or feature. Templates are useful when deploying an identical configuration across multiple Edge devices, such as branch offices or backup units.

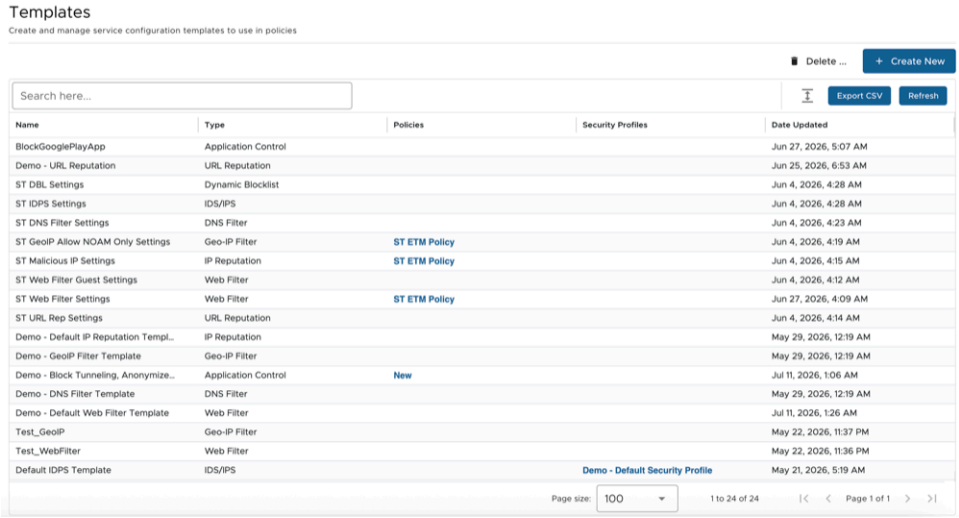
The ETM Dashboard enables the Admin to create and manage service configuration templates to use in policies. There are two types of templates:

- **Policy Template** - Policy templates include Application Control Filter, DNS Filter, Geo-IP Filter, IP Reputation, URL Reputation, and Web Filter. This type of configuration typically includes a large set of categories or individual items that are easier to maintain as a collection. Policy templates are effective only when applied by a Policy Service rule. The Edge Threat Management (ETM) supports the following Policy templates:
  - Application Control - Use an Application Control template to define which applications the policy permits or denies.
  - DNS Filter - Use DNS Filter to block harmful Internet content.
  - Geo-IP Filter - Use a Geo-IP Filter template to define which countries to block or allow by the policy.
  - IP Reputation - Use IP Reputation to block high-risk IPs with a poor reputation.
  - URL Reputation - Use URL Reputation to block high-risk sites with a poor reputation.
  - Web Filter - Use a Web Filter template to define which URL categories to permit or deny by the policy.
- **Security Profile Template** - Security Profile templates include External Databases, Dynamic Blocklists, and Intrusion Detection and Prevention (IDS/IPS). These templates are applied to Security Profiles and do not support any condition. After applying the template to a profile, it is unconditionally applicable to all sessions. The ETM supports the following Security Profile templates:
  - Database - Use the Database template to persist reporting events.
  - Dynamic Blocklists - Add an IP/FQDN block list source to block IP/FQDN addresses listed in it.

- IDS/IPS - Use Intrusion Prevention to scan, detect, and block attacks and suspicious traffic using signatures

The **Templates** page displays a list of all current templates and the **Create New** option. The table's contents can be refreshed or exported as a comma-separated (CSV) file using the buttons at the top.

Figure 5-21: Templates



Create New Template

To create a new template, perform the following steps:

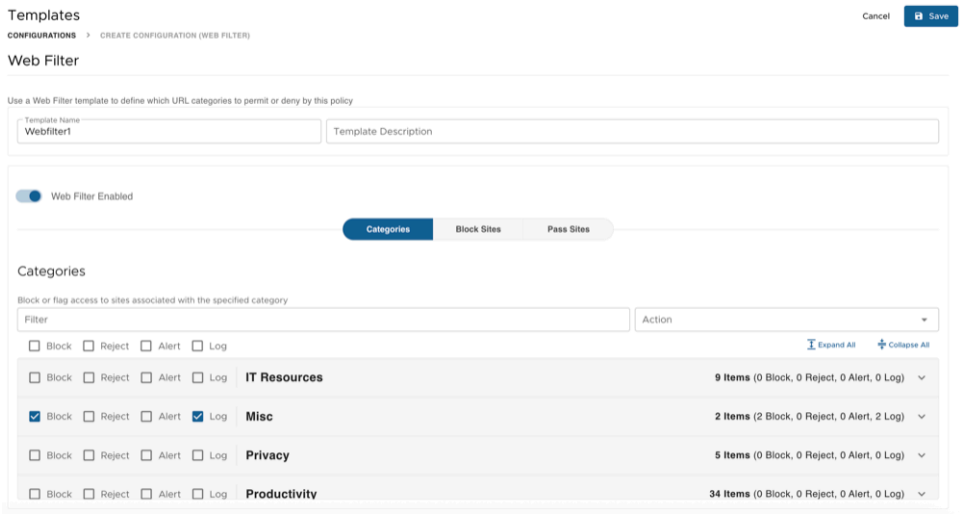
1. Log in to the VeloCloud Orchestrator as an Enterprise User.
2. To access the ETM application from the VeloCloud Orchestrator, go to the **Enterprise Applications** drop-down menu and select **ETM Nex-Gen Firewall**.
3. Navigate to **Configure** > **Templates**.

   The **Templates** page appears.
4. To create a new template, click **Create New** and select the appropriate type of template from the drop-down list that appears.

   Each template will have its own options and configuration settings, configured as you would in an individual Edge.

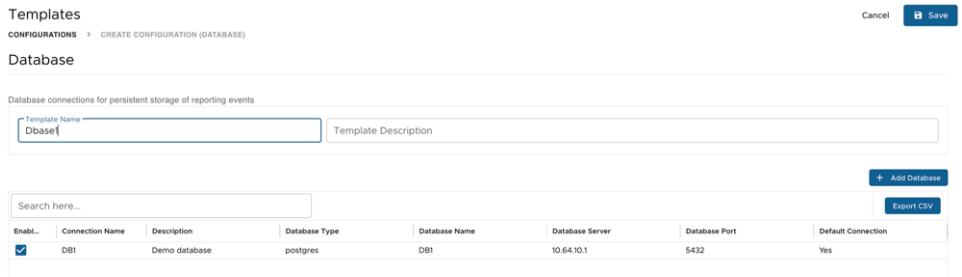
5. To configure a Policy Template (for example, Web Filter), provide a Name and Description for the template, configure settings to block or flag access to sites associated with the specified Categories, and configure Block Sites and Pass Sites.

Figure 5-22: Templates - Web Filter



6. To configure a Security Profile Template (for example, Database), provide a Name and Description for the template, add database connections, and configure the database to persist reporting events.

Figure 5-23: Templates - Database



7. After configuring all the necessary configuration settings, click **Save** to finish creating a template.

   For more information about how to configure the various supported templates, see Template Configuration Examples.

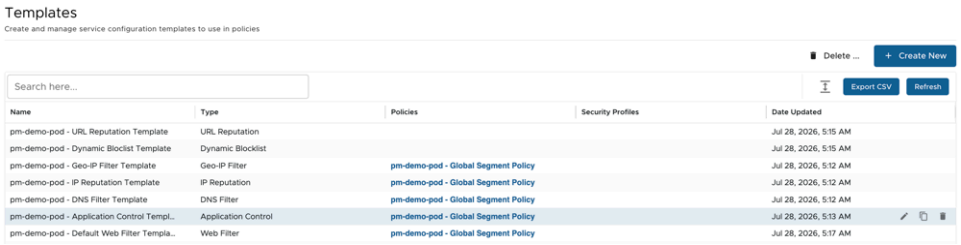
Manage Templates

From the main table of templates, click any template to open its settings. Hovering over the template will reveal additional option buttons in the **Policies** column:

- The pencil icon opens the policy settings for editing.
- The duplicate icon creates a copy of the highlighted policy and opens it for editing.

- The trash can icon deletes the highlighted policy.

Figure 5-24: Manage Templates



The table also provides the following global option buttons:

- **Export CSV** exports a comma-separated list of rules.
- **Refresh** refreshes the list of templates.
- **Delete …** enables bulk deletion of templates.

5.4.1 Template Configuration Examples

The ETM Dashboard enables the Admin to create and manage service configuration Templates to use in policies. This topic provides details about configuring the various policies and Security Profile Templates with examples.

Configure Application Control Template

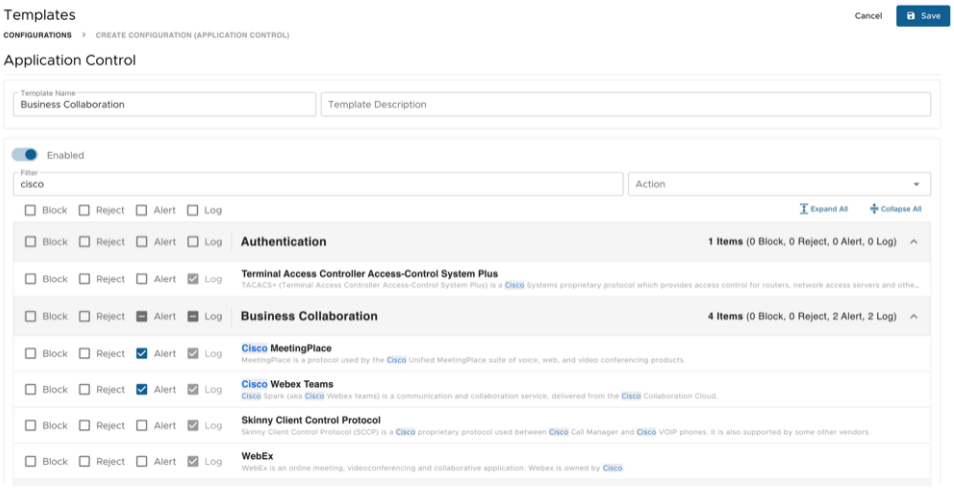
Application Control defines which applications to permit or deny by the policy.

To create a new Application Control Template, perform the following steps:

1. In the **Templates** screen, click **Create New** > **Application Control**.
2. In the **Application Control** screen, provide a Name and Description for the Template.

3. From the list of available filters, search for a specific filter by filter name and action type (Block, Reject, Alert, and Log) to apply to the Template, and click **Save**.

Figure 5-25: Create Application Control Template



Configure DNS Filter Template

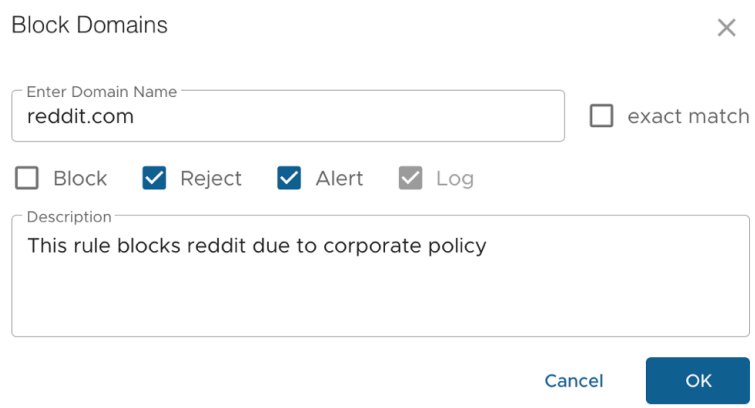
DNS Filter enables Admins to view all DNS requests on the network and define Domains to block by preventing them from resolving.

To create a new DNS Filter Template, perform the following steps:

1. In the **Templates** screen, click **Create New** > **DNS Filter**.
2. In the **DNS Filter** screen, provide a Name and Description for the Template.
3. Under **Block Domains**, click **Add Domain** to configure a new block domain rule and apply it to the Template.

   The **Block Domains** dialog appears.

Figure 5-26: Block Domains

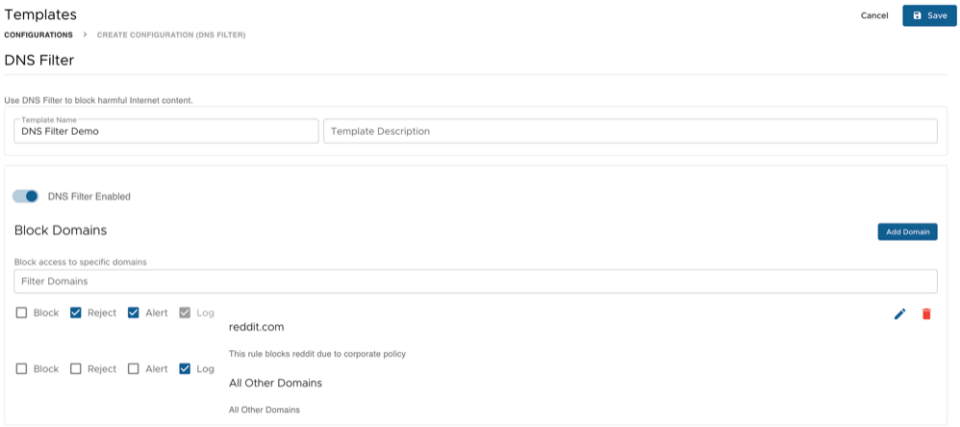


- In the **Block Domains** dialog, enter the domain name you want to block access to and select the "Exact Match" check box to create a rule that matches the specified domain name exactly.

- Configure the filter actions as needed and click **OK**.
  - **Block** - Drop the session without sending any denial response.
  - **Reject** - Deny the session by sending an ICMP “Port Unreachable” message.
  - **Log** - Record the session event in the reports.
  - **Alert** - Include the session event as an alert.

4. Use the **Filter Domains** search field to search for and find a specific domain to block access to from the configured domains.
5. For all other domains, configure the filter action as needed and click **Save**.

Figure 5-27: Create DNS Template



Configure Geo-IP Filter Template

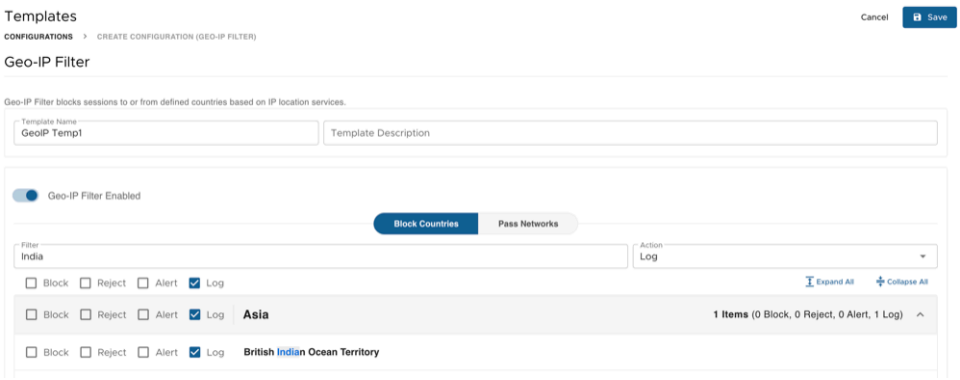
Geo-IP Filter blocks sessions to or from defined countries based on IP location services.

To create a new Geo-IP Filter Template, perform the following steps:

1. In the **Templates** screen, click **Create New** > **Geo-IP Filter**.
2. In the **Geo-IP Filter** screen, provide a Name and Description for the Template.

3. Under **Block Countries**, click the **Filter** field to search for the countries to block, by country name and action type, and apply to the Template.

Figure 5-28: Create Geo-IP Filter Template - Block Countries



4. Under **Pass Networks**, users can allow access to specific external networks by adding them to the Geo-IP Template. Click **Add Network** to configure an external network. Use the **Search here...** field to find and add the network to allow access.

Figure 5-29: Add Network

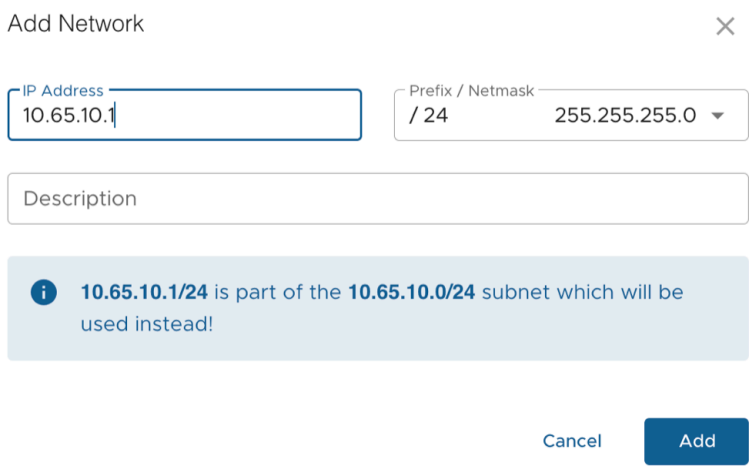
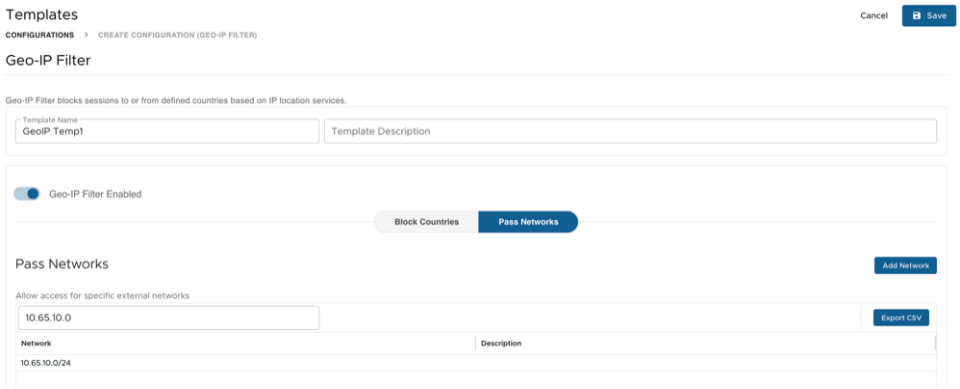


Figure 5-30: Create Geo-IP Filter Template - Pass Networks



5. After configuring Pass Networks and Block Countries, click **Save**.

Configure IP Reputation Template

IP Reputation blocks high-risk IPs that have a poor reputation.

To create a new IP Reputation Template, perform the following steps:

1. In the **Templates** screen, click **Create New** > **IP Reputation**.
2. In the **IP Reputation** screen, provide a Name and Description for the Template.
3. Under **Settings**, configure the action types (Block, Reject, Alert, and Log) for the IP Reputation parameters (Malicious and Non-Malicious).

   Figure 5-31: Create IP Reputation Template - Settings



4. Under the **Pass List**, users can grant access to specific CIDR networks by adding them to the IP Reputation Template. Click **Add Network** to configure a CIDR network. Use the **Search here...** field to find and add the network to allow access.

Figure 5-32: Add Network - IP Reputation

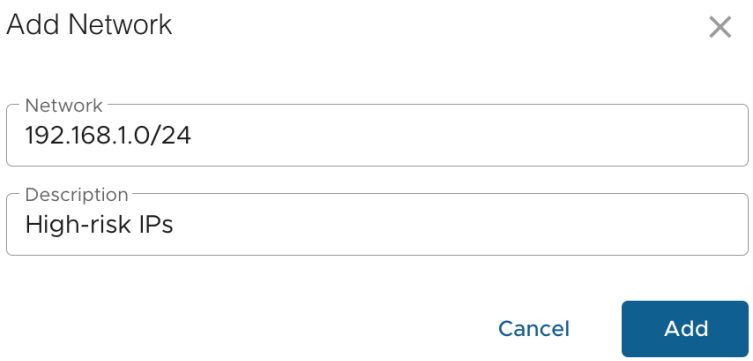
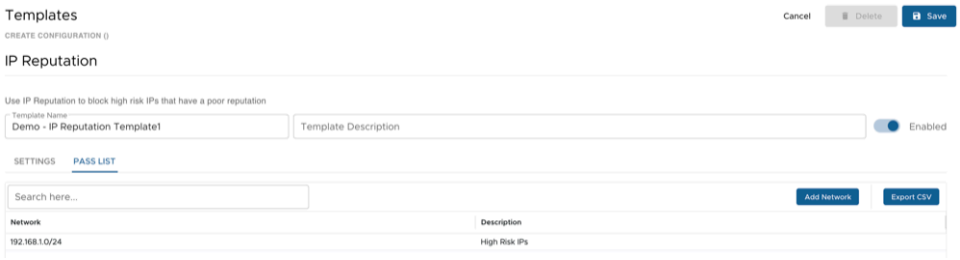


Figure 5-33: Create IP Reputation Template - Pass List



5. After configuring the required settings and passed networks, click **Save**.

Configure URL Reputation Template

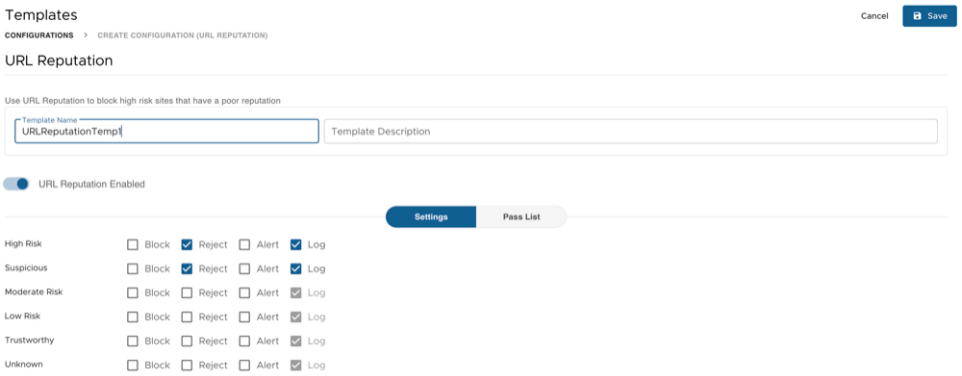
URL Reputation blocks high-risk sites that have a poor reputation.

To create a new URL Reputation Template, perform the following steps:

1. In the **Templates** screen, click **Create New** > **URL Reputation**.
2. In the **URL Reputation** screen, provide a Name and Description for the Template.

3. Under **Settings**, configure the action types (Block, Reject, Alert, and Log) for each URL Reputation parameter (High Risk, Suspicious, Moderate Risk, Low Risk, Trustworthy, and Unknown).

Figure 5-34: Create URL Reputation Template - Settings



4. Under **Pass List**, click **Add Host** to configure specific hosts to allow access to. Use the **Search here...** field to find and add the host to allow access.

Figure 5-35: Add Host - URL Reputation

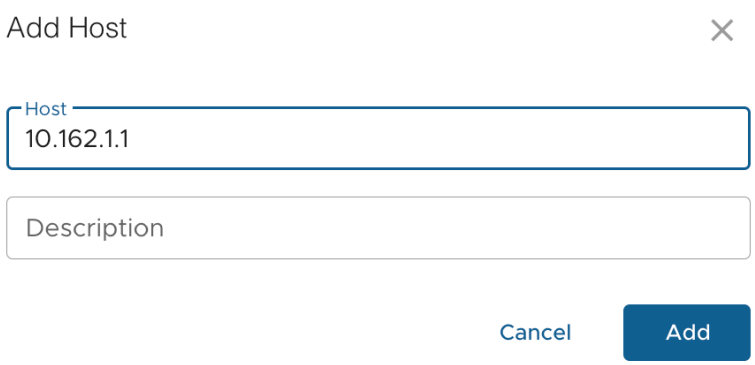
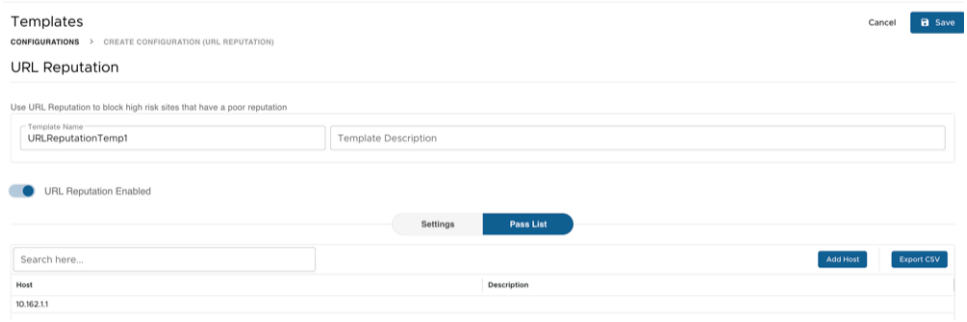


Figure 5-36: Create URL Reputation Template - Pass List



5. After configuring the required settings and passed hosts, click **Save**.

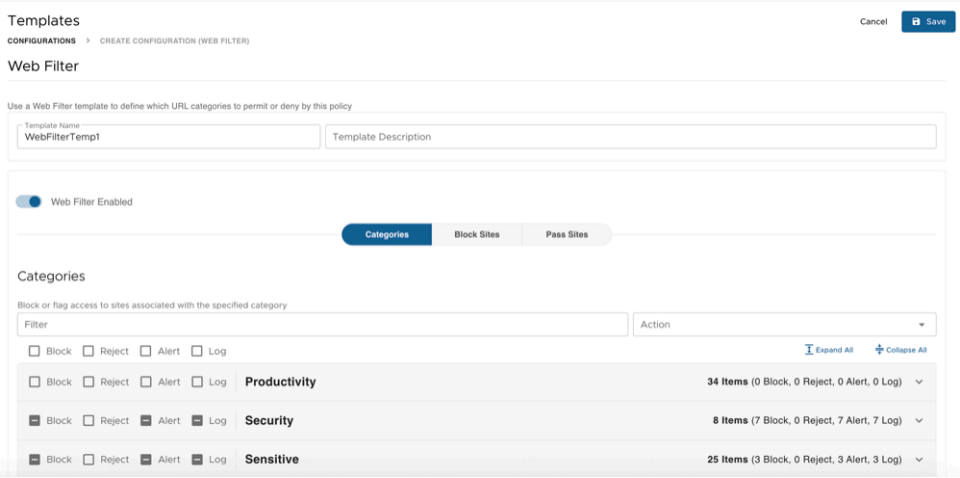
Configure Web Filter Template

Web Filter defines which URL categories to permit or deny by the policy. The default configuration of the Web Filter template restricts access to several categories classified under Security and Sensitive.

To create a new Web Filter Template, perform the following steps:

1. In the **Templates** screen, click **Create New** > **Web Filter**.
2. In the **Web Filter** screen, provide a Name and Description for the Template.
3. Under **Categories**, configure block or flag access to sites associated with the specified category.

Figure 5-37: Create Web Filter Template - Categories



4. Under **Block Sites**, click **Add Site** to configure specific sites to block access.

Figure 5-38: Add Block Site

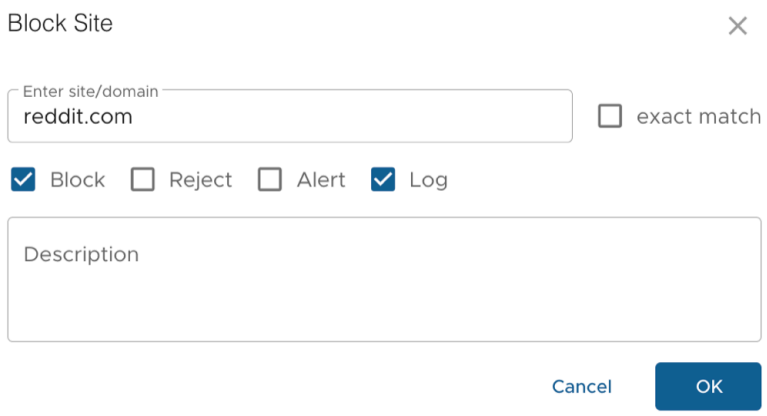
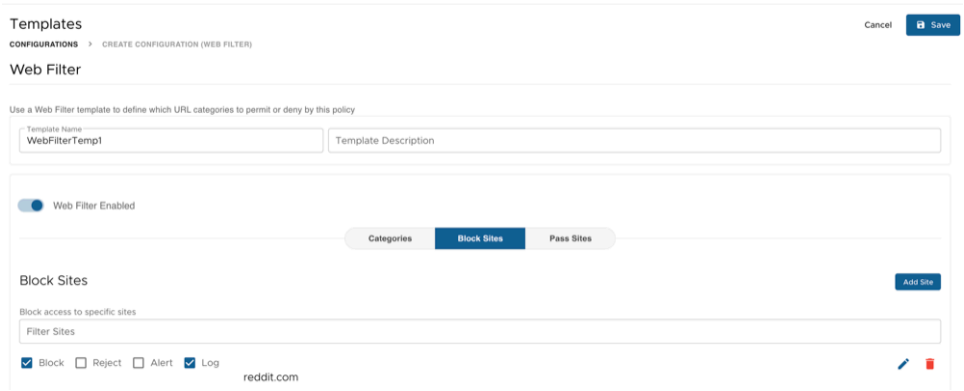


Figure 5-39: Create Web Filter Template - Block Sites



5. Under **Pass Sites**, click **Add Site** to configure specific sites to allow access.

Figure 5-40: Add Pass Site

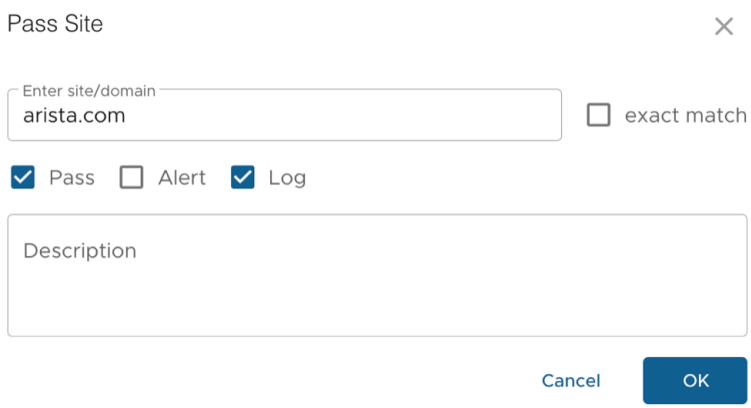
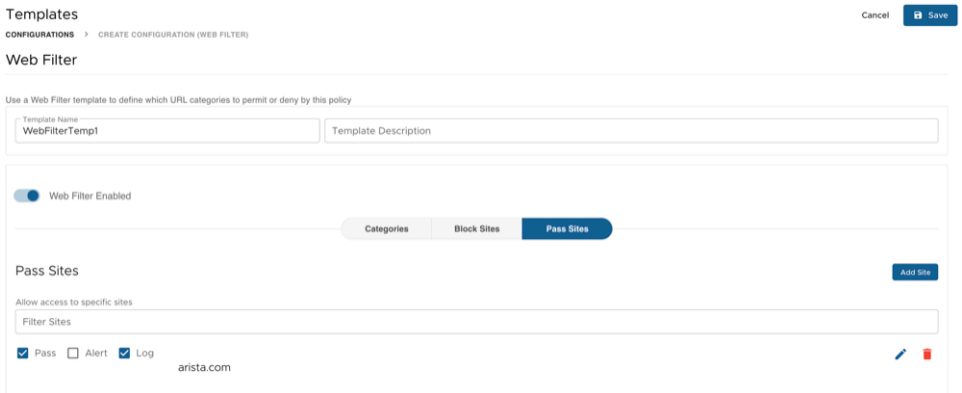


Figure 5-41: Create Web Filter Template - Pass Sites



6. After configuring the required, blocked, and passed sites, click **Save**.

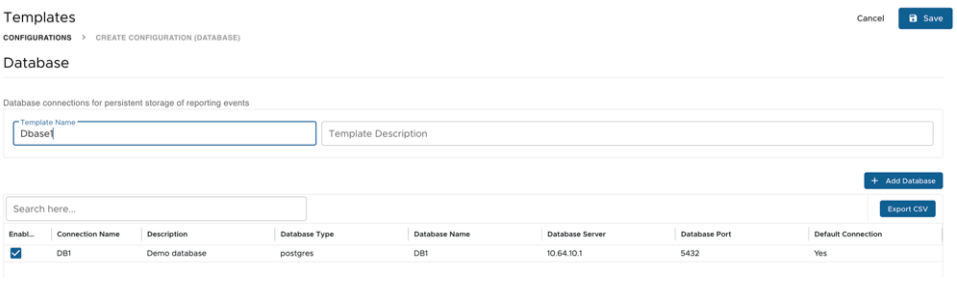
Configure Database Template

The database Template allows for the persistent storage of reporting events.

To create a new Database Template, perform the following steps:

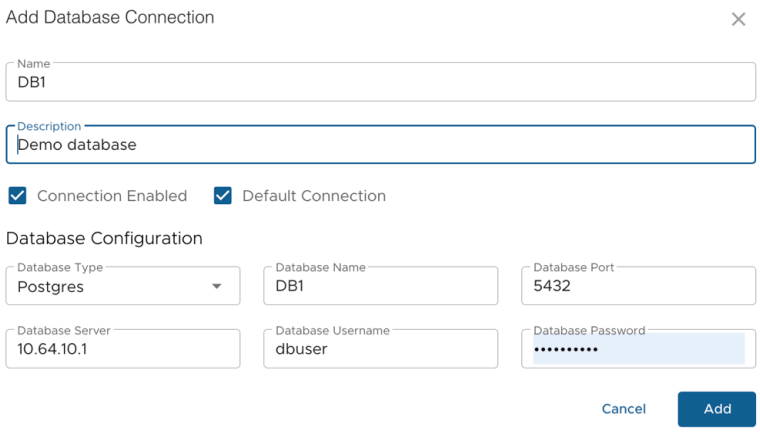
1. In the **Templates** screen, click **Create New** > **Database**.
2. In the **Database** screen, provide a Name and Description for the Template.

   Figure 5-42: Create Database Template



3. To add a new Database Connection, click **Add Database**.
4. In the **Add Database Connection** dialog, provide the database name, description, and the required database configuration details (like Type, Port, Server, Username, and Password). Also, users can select the following checkboxes, and click **Add**.
   - **Connection Enabled** - When the Database Connection is enabled, the Edge will stream events to the database.
   - **Default Connection** - If Database Connection is set as the default option, it will use that default database for viewing Edge reports. If no database is designated as the default, the system will utilize the local database on the Edge.

   Figure 5-43: Add Database Connection



   Use the **Search here...** field to find a database that the users want to edit or enable/disable.
5. After configuring the required database connection details, click **Save**.

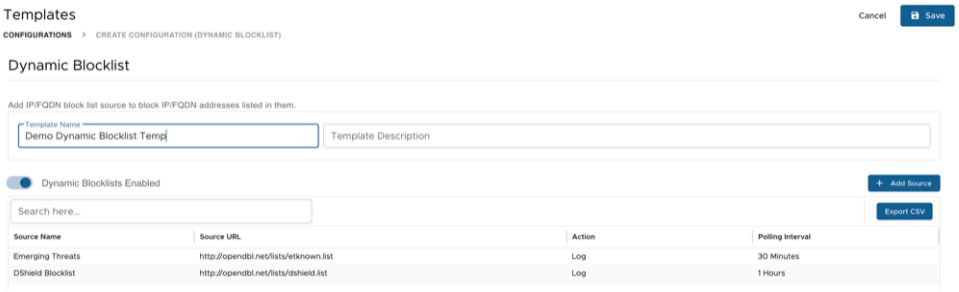
Configure Dynamic Blocklist Template

Dynamic Blocklist allows adding an IP/FQDN block list source to block IP/FQDN addresses listed in it. If Dynamic Blocklist template is configured then the Edge will fetch the remote list directly from the source.

To create a new Dynamic Blocklist Template, perform the following steps:

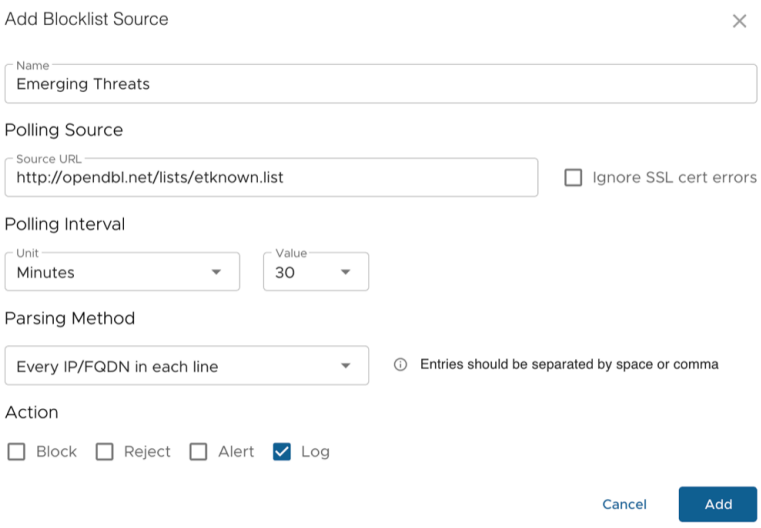
1. In the **Templates** screen, click **Create New** > **Dynamic Blocklist**.
2. In the **Dynamic Blocklist** screen, provide a Name and Description for the Template.

   Figure 5-44: Create Dynamic Blocklist Template



3. To add a new Blocklist Source, click **Add Source**.
4. In the **Add Blocklist Source** dialog, provide the Source name, Source URL, polling interval, parsing method, and rule action, and click **Add**.

   Figure 5-45: Add Blocklist Source



   Use the **Search here...** field to find and add the dynamic blocklist sources to the Template.

5. After configuring the required details, click **Save**.

Configure IDS/IPS Template

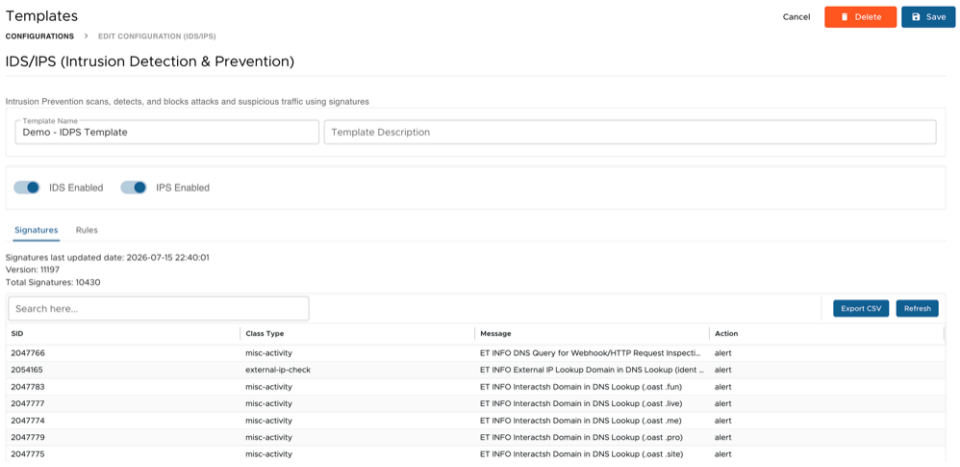
Intrusion Detection and Prevention (IDS/IPS) scans, detect, and block attacks and suspicious traffic using signatures.

To create a new IDS/IPS Template, perform the following steps:

1. In the **Templates** screen, click **Create New** > **IDS/IPS**.

2. In the **IDS/IPS** screen, provide a Name and Description for the Template. By default, IDS is enabled. To enable IPS, turn on the **IPS Enabled** button.

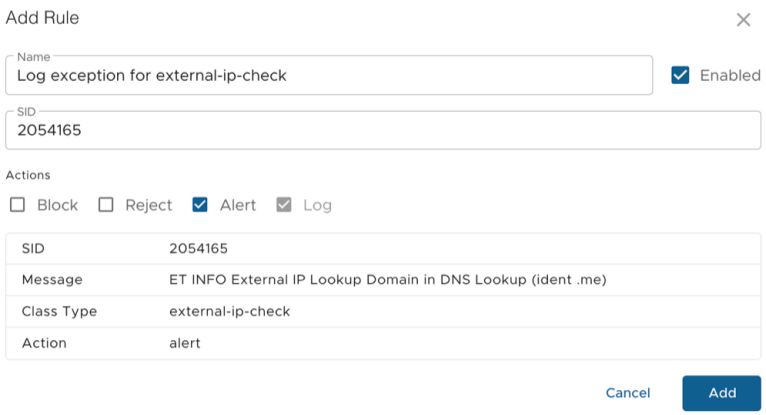
   Figure 5-46: Create IDS/IPS Template - Signatures



3. In the **Signatures** tab, use the **Search here...** field to find and add specific signatures to the Template. This enables the Admin to override the signature's default actions. For example, if there is a false positive, then the Admin can change the action from reject to log.

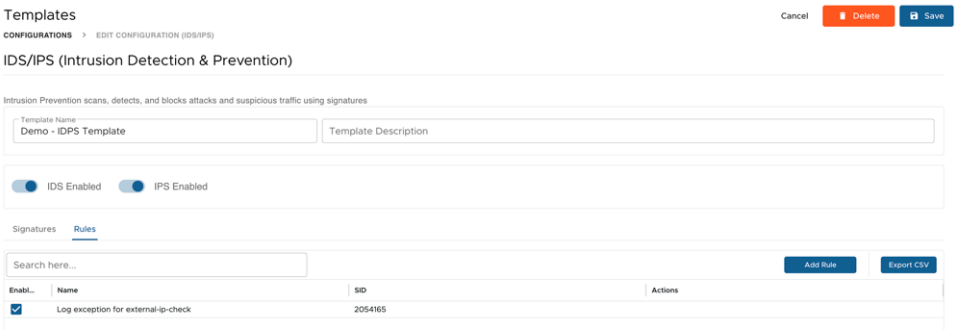
4. To add a new Rule to the Template, go to **Rules** > **Add Rule**.

   Figure 5-47: Add Rule



5. In the **Add Rule** dialog, provide the Rule name, System ID (SID), and rule action, and click **Add**. The **Rules** list displays the newly added rule.

   Figure 5-48: Create IDS/IPS Template - Rules



6. After configuring the required details, click **Save**.

5.5 Configure Objects

An Object is a grouping of one or more traits: IP addresses, interfaces, application identifications, user or VLAN tag groups, and so on. Group these traits into named objects to streamline policy and rule configuration.

The ETM Dashboard enables the Admin to create and manage the following Object types to use in policies:

- Custom Applications
- Domains
- GeoIP Locations
- Interfaces
- IP Addresses
- Segments
- Services

Create New Object

To create a new Object, perform the following steps:

1. Log in to the VeloCloud Orchestrator as an Enterprise User.
2. To access the ETM application from the VeloCloud Orchestrator, go to the **Enterprise Applications** drop-down menu and select **ETM Nex-Gen Firewall**.
3. Navigate to **Configure** > **Objects**.
4. From the left navigation menu, select the appropriate Object type to create; for example, to create a Custom Applications Object, select **Custom Applications**.
5. To create a new Object, click **Create New**. Provide a Name and Description for the Object and configure the required parameters.

Each type of Object has different configuration options, based on what details the Object will contain. For example, when creating a Custom Applications Object, provide the port(s) and IP address(es) used by the application.

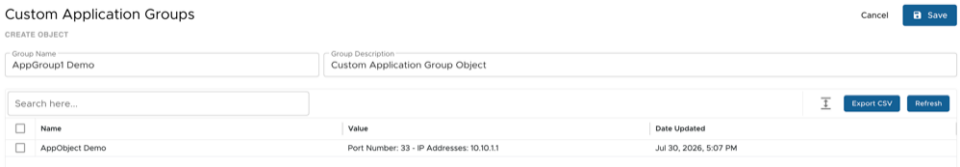
Figure 5-49: Create Custom Applications Object



After configuring all the necessary configuration settings, click **Save** to finish creating an Object.

6. To create a new Object Group, click **Create Group**. Provide a Name and Description for the Object Group and click **Save**.

Figure 5-50: Create Custom Application Groups



For more information about how to configure the various supported Object types, see Object Type Configurations.

Manage Objects and Object Groups

From the main table of Objects and Object Groups, hover over any Object or Group to edit, clone, or delete the Object or Group.

- The pencil icon opens the Object settings for editing.
- The duplicate icon creates a copy of the highlighted Object and opens it for editing.
- The trash can icon deletes the highlighted Object.

The table also provides the following global option buttons:

- **Export CSV** exports a comma-separated list of Objects.
- **Refresh** refreshes the list of Objects and Groups.
- **Delete …** enables bulk deletion of Objects and Groups.

5.5.1 Object Type Configurations

The ETM Dashboard enables the Admin to create and manage Objects and Object Groups to use in policies and rules. This topic provides details about configuring the various Objects with examples.

Configure Custom Applications Object

Create custom applications based on IP and port information to use across multiple policy rules.

To create a new Custom Applications Object, perform the following steps:

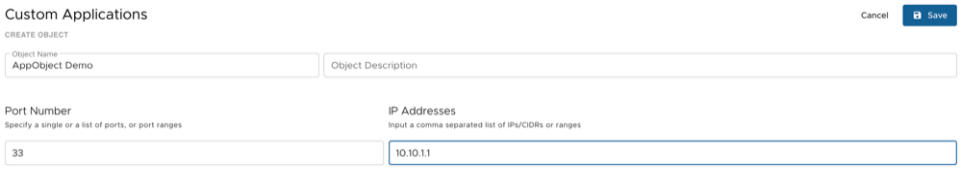
1. Navigate to **Configure** > **Objects** > **Custom Applications**. The **Custom Applications** screen appears.

   Figure 5-51: Custom Applications Screen



2. To create a new Object, click **Create New**.

   Figure 5-52: Create Custom Applications Object



3. Provide a Name and Description for the Object and configure the following required parameters:
   - In the **Port Number** field, specify a single port or a list of ports, or port ranges.
   - In the **IP Addresses** field, input a comma-separated list of IPs/CIDRs or ranges.

   After configuring all the necessary parameters, click **Save**.

4. To create a new Object Group, click **Create Group**. Provide a Name and Description for the Object Group and click **Save**.

Configure Domains Object

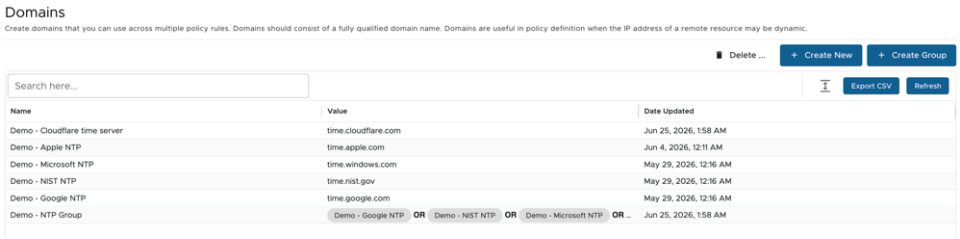
Create domains to use across multiple policy rules. Domains should consist of a fully qualified domain name. Domains are useful in policy definition when the IP address of a remote resource may be dynamic.

> **Note:** The **Domains** screen displays Domains configured in the SD-WAN Object Groups.

To create a new Domains Object, perform the following steps:

1. Navigate to **Configure** > **Objects** > **Domains**. The **Domains** screen appears.

   Figure 5-53: Domains Screen



2. To create a new Domain, click **Create New**.

   Figure 5-54: Create Domains



3. Provide a Name, Description, and Hostname for the Object and click **Save**.

4. To create a new Domains Group, click **Create Group**. Provide a Name and Description for the Domains Group and click **Save**.

Configure GeoIP Locations Object

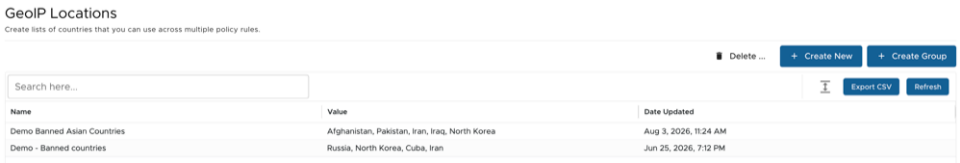
Create lists of countries to use across multiple policy rules.

> **Note:** The GeoIP Locations Template may be easier to manage and blocks traffic in either direction, while the GeoIP Locations object provides more granular configuration.

To create a new GeoIP Location Object, perform the following steps:

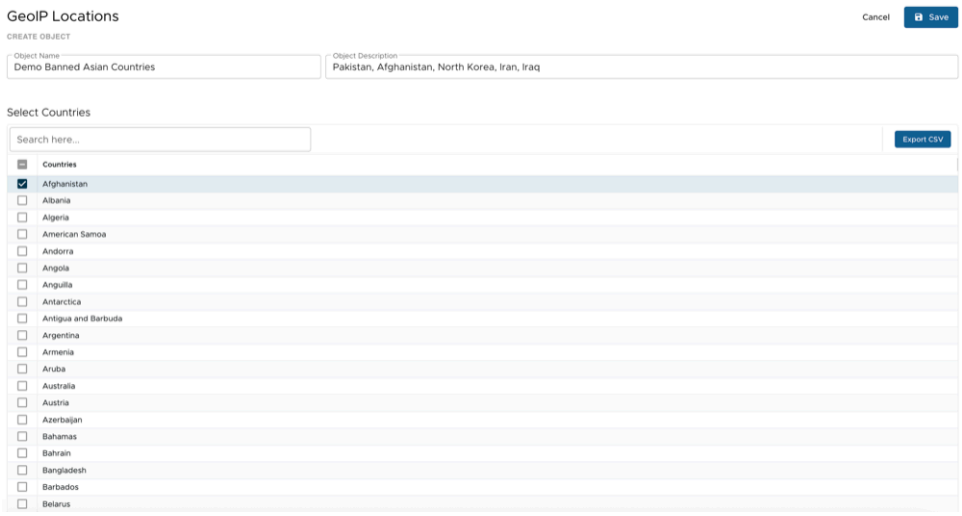
1. Navigate to **Configure** > **Objects** > **GeoIP Locations**. The **GeoIP Locations** screen appears.

   Figure 5-55: GeoIP Locations Screen



2. To create a new GeoIP Locations object, click **Create New**.

Figure 5-56: Create GeoIP Locations Object



3. Provide a Name and Description for the Object and select the lists of countries to use in policy rules.

   After configuring all the necessary details to use in policy rules, click **Save**.

4. To create a new GeoIP Locations Group, click **Create Group**. Provide a Name and Description for the GeoIP Locations Group and click **Save**.

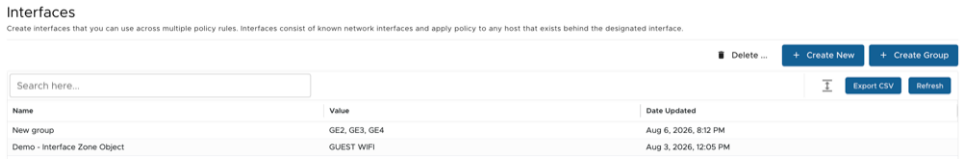
Configure Interfaces Object

Create Interfaces to use across multiple policy rules. Interfaces consist of known network interfaces and apply policy to any host that exists behind the designated interface.

To create a new Interfaces Object, perform the following steps:

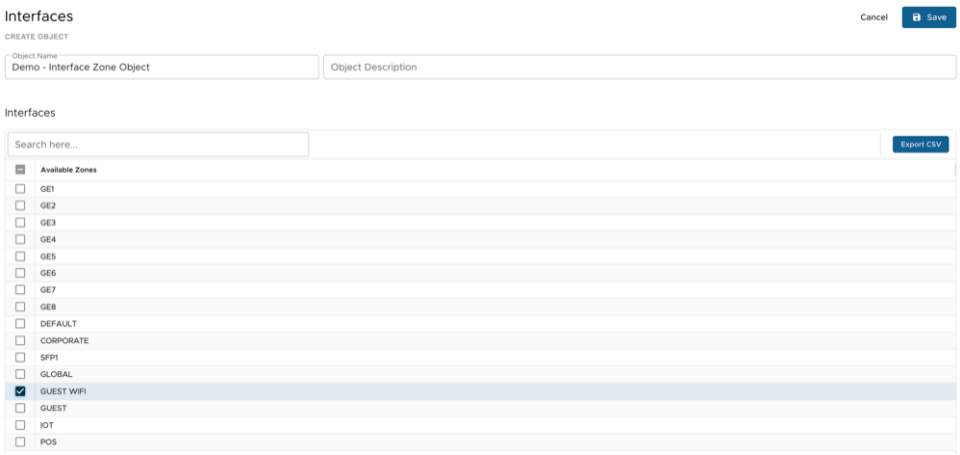
1. Navigate to **Configure** > **Objects** > **Interfaces**. The **Interfaces** screen appears.

Figure 5-57: Interfaces Screen



2. To create a new Interface object, click **Create New**.

Figure 5-58: Create Interfaces Object



3. Provide a Name and Description for the Object.

4. From the list of **Available Zones**, select the Interfaces to use in policy rules, and click **Save**.

   To configure a custom interface to use in policy rules, enter the Interface name and click **Add**. The Custom Interface appears under **Available Zones**.

5. To create a new Interfaces Group, click **Create Group**. Provide a Name and Description for the Interface Group and click **Save**.

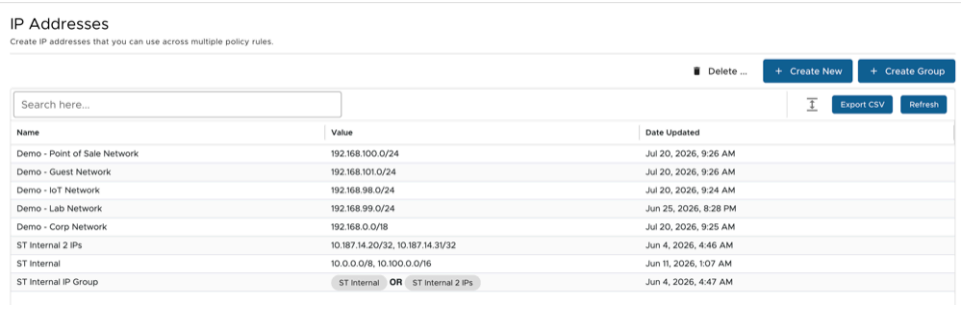
Configure IP Addresses Object

Create lists of IP Addresses to use across multiple policy rules.

To create a new IP Address, perform the following steps:

1. Navigate to **Configure** > **Objects** > **IP Addresses**. The **IP Addresses** screen appears.

Figure 5-59: IP Addresses Screen



The screen displays the IP Address Objects created from SD-WAN configuration.

2. To create a new IP Address, click **Create New**.

Figure 5-60: Create IP Addresses Object



3. Provide a Name and Description for the Object.
4. In the **IP Addresses** field, enter a comma-separated list of IP addresses/CIDRs or ranges, and click **Save**.
5. To create a new Object Group, click **Create Group**. Provide a Name and Description for the Object Group and click **Save**.

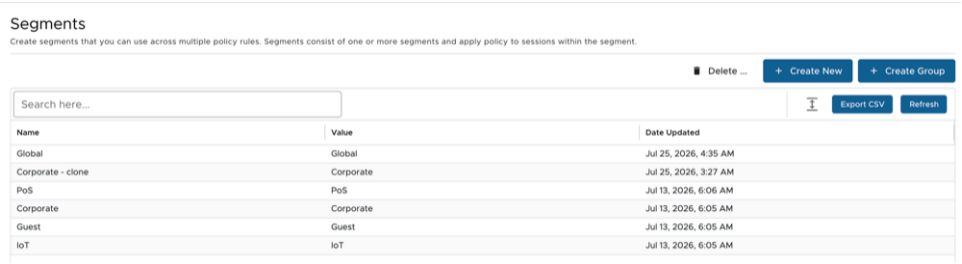
Configure Segments Object

Create Segments to use across multiple policy rules. Users can apply a policy to sessions within the Segment.

To create a new Segment, perform the following steps:

1. Navigate to **Configure** > **Objects** > **Segments**. The **Segments** screen appears.

Figure 5-61: Segments Screen



The screen displays the Segment Objects created from SD-WAN configuration.

2. To create a new Segment, click **Create New**.

Figure 5-62: Create Segments Object



3. Provide a Name and Description for the Object.
4. In the **Segments** field, enter either one or a comma-separated list of Segment names (Examples: Global, Corporate, Guest, IoT, and so on).

5. Click **Save**.

6. To create a new Object Group, click **Create Group**. Provide a Name and Description for the Object Group and click **Save**.

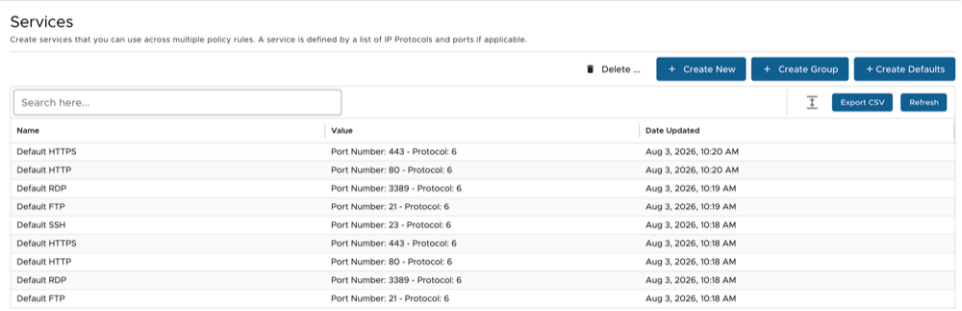
Configure Services Object

Create Services to use across multiple policy rules. A Service is defined by a list of IP Protocols and ports, if applicable.

To create a new Service, perform the following steps:

1. Navigate to **Configure** > **Objects** > **Services**. The **Services** screen appears.

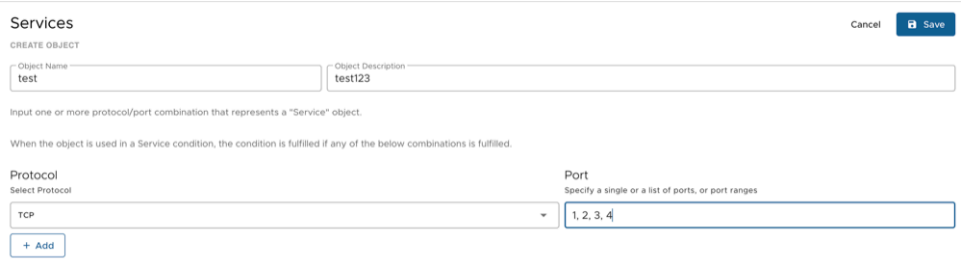
   Figure 5-63: Services Screen



   The screen displays Service Group Objects created from SD-WAN configuration.

2. To create a new Service, click **Create New**.

   Figure 5-64: Create Services Object



3. Provide a Name and Description for the Object.

4. Select a protocol from the **Protocol** drop-down menu.

5. In the **Port** field, enter a single port or a list of ports, or port ranges.

> **Note:** Users can add or delete Protocols as required.

6. Click **Save**.

7. To create a new Object Group, click **Create Group**. Provide a Name and Description for the Object Group and click **Save**.

8. To create a Service Object with default values, click **Create Defaults**.

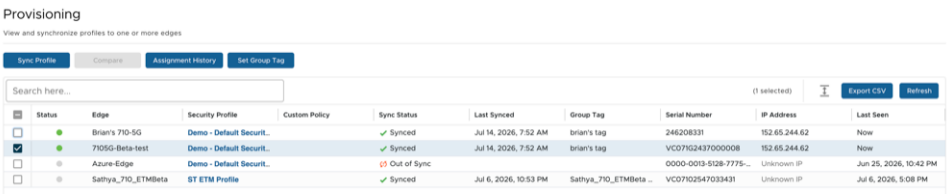
Chapter 6

Provision Edge Threat Management

Provisioning the ETM security configuration is independent of SD-WAN configuration. This enables security administrators to assign and activate Security Policies independently of SD-WAN Policies.

The **Provisioning** screen displays a list of provisioned Edges, including details such as Security Profile, Custom Policy, Sync details, Group Tag, and more. To access this screen, click **Provisioning** on the ETM dashboard.

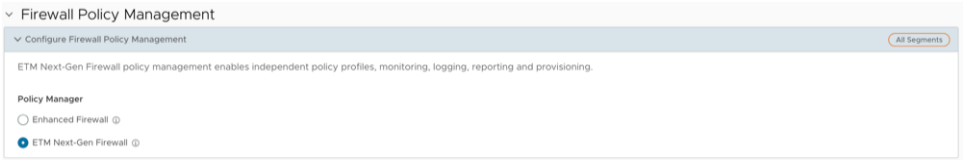
Figure 6-1: Provision Edge Threat Management



Perform the following steps to provision Edge Threat Management:

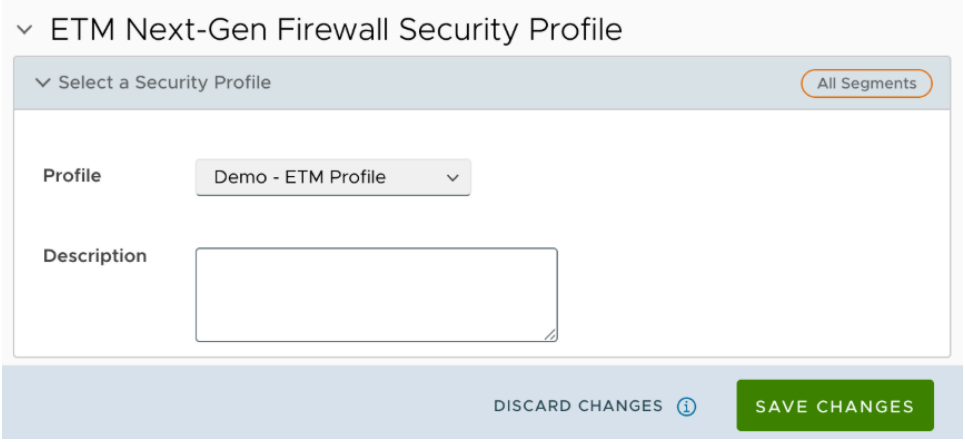
1. Follow the steps in Configure Security Profiles to create a Security Profile.
2. After creating a Security Profile, assign it to the SD-WAN Profile.
   a. In the **SD-WAN** service of the **Enterprise** portal, go to **Configure** > **Profiles** > **Firewall** > **Firewall Policy Management**.
   b. Under **Policy Manager**, select **ETM Next-Gen Firewall**.

   Figure 6-2: Firewall Policy Management



Selecting **ETM Next-Gen Firewall** introduces a new section, **ETM Next-Gen Firewall Security Profile**, on this screen.

Figure 6-3: ETM Next-Gen Firewall Security Profile



c. Choose an ETM Security Profile from the drop-down menu and add a description (optional).

d. Click **Save Changes**.

Note: Assigning a Security Profile does not immediately apply it to Edges. Users must synchronize the Security Policy with Edges, as explained in the next step.

3. To synchronize Security Profiles, go to the **ETM Next-Gen Firewall** Enterprise Application, and click **Provisioning** on the ETM Dashboard.

a. Select the Edges to synchronize the Security Profile. Use the filter option to display only the Edges affected by the Security Profile. Alternatively, select only the **Out-of-Sync** Edges.

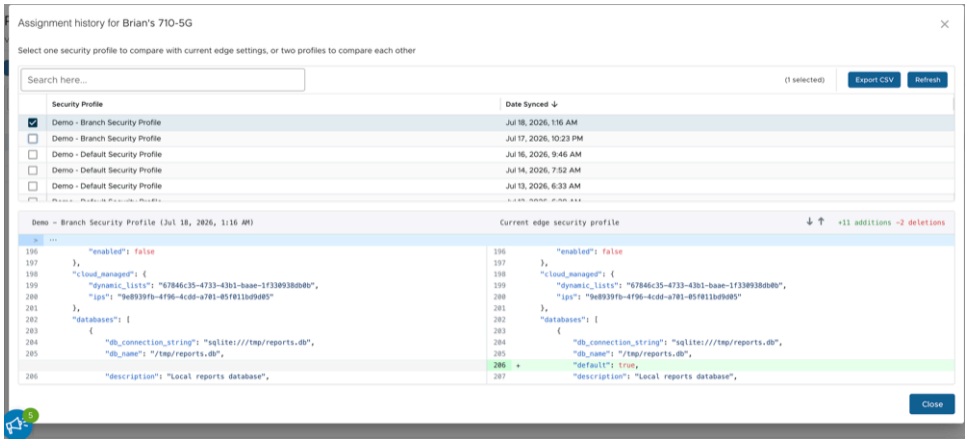
b. Click **Sync Profile** to initiate the synchronization.

c. Click **Compare** to view a side-by-side difference between the current Security Profile and the previously synchronized version.

d. To check the synchronization status, click the **Tasks** button located at the top right of the **Provisioning** screen.

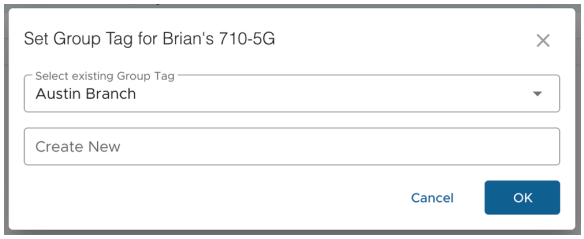
e. Clicking **Assignment History** displays the following screen. Select at least one Security Profile to compare with the current Edge settings.

Figure 6-4: Assignment History



f. To set a Group Tag for an Edge, click **Group Tag**.

Figure 6-5: Set Group Tag



g. Either select an existing Group Tag or create a new one to assign it to the Edge.

h. Click **OK**.

Note: Synchronizing Security Profiles may take approximately 1 minute. Click the **Refresh** button to confirm the synchronization status. To review the active tasks, click the **Tasks** button at the top right of the **Provisioning** screen.

Chapter 7

Service Settings

The **Service Settings** allow the user to view and manage Alert Rules and Notification Profiles.

To access this screen, click **Service Settings** on the ETM dashboard.

The **Service Settings** offers the following functions:

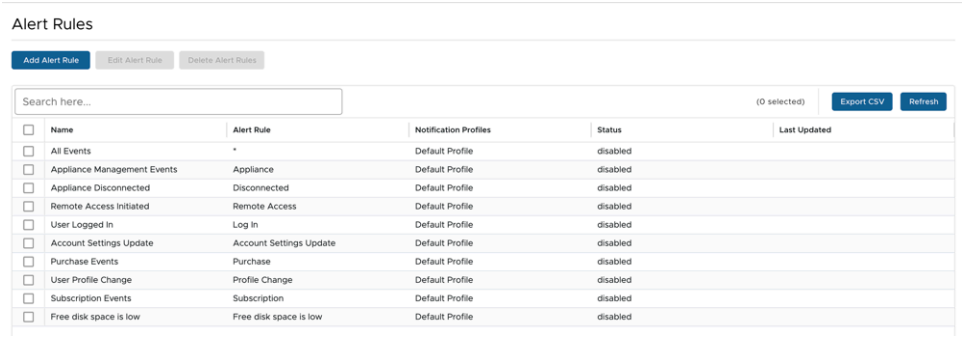
- Alert Rules
- Notification Profiles

7.1 Alert Rules

Alert Rules determine which events flow through Notification Profiles.

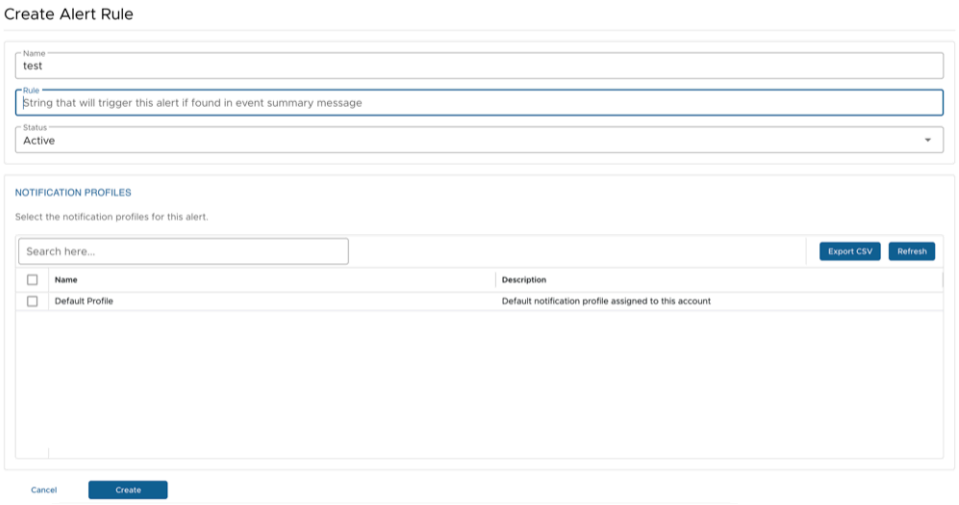
To access this screen, go to **Service Settings** > **Alert Rules**.

Figure 7-1: Alert Rules



1. To create a new Alert Rule, click **Add Alert Rule**.

   Figure 7-2: Create Alert Rule



   a. Enter a name for the new Alert Rule.

   b. Specify the Rule. This is the text string the Alert Rule looks for to trigger the Alert.

   c. Select the Alert Status as either **Active** or **Disabled**.

   > **Note:** All default rules are set to **Disabled** to prevent excessive email notifications from the ETM Dashboard.

   d. Select an existing Notification Profile from the list or create a new one. For more information, see Notification Profiles.

   e. Click **Create**.

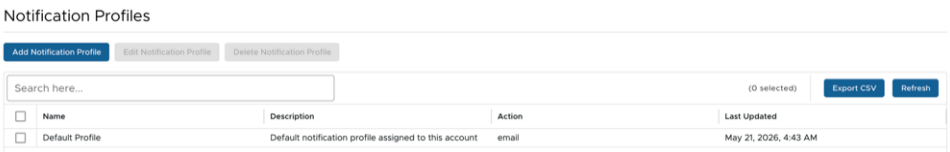
2. To edit an existing Alert Rule, click **Edit Alert Rule** and edit the required fields. Click **Update**.
3. To delete Alert Rules, select one or more Alert Rules, and then click **Delete Alert Rules**. On the delete confirmation screen, click **Yes**.

7.2 Notification Profiles

Notification Profiles specify the delivery methods for Alerts. All Alert Rules require a Notification Profile to send alerts. The Notification Profile specifies how users receive alerts and view information.

To access this screen, go to **Service Settings** > **Notification Profiles**.

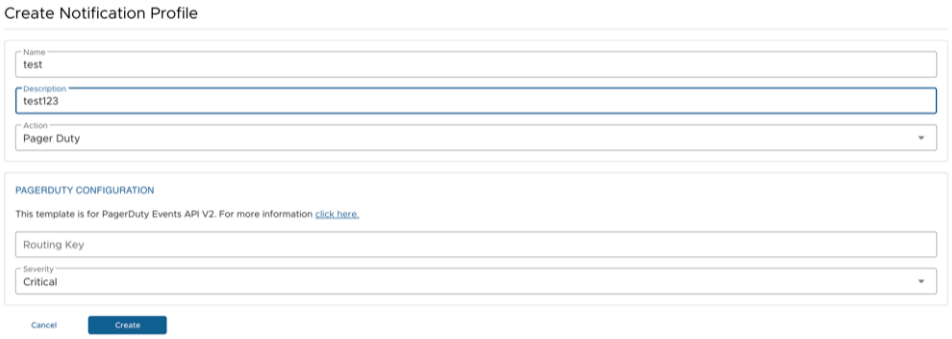
Figure 7-3: Notification Profiles



Note: Every account in the ETM Dashboard has a default Notification Profile that delivers alerts via email to the email address associated with the account. The default set of Alert Rules uses this Profile to send alerts.

1. To create a new Notification Profile, click **Add Notification Profile**.

Figure 7-4: Create Notification Profile



   a. Type a name for the new Notification Profile.

   b. Enter a description.

   c. Select an appropriate action from the **Action** drop-down menu to define alert delivery preferences.

      The available options are Email, Webhook, Slack, Pager Duty, VictorOps, and Untangle Go (Mobile). The configuration options vary depending on the selected action.

Table 6: Actions

Option	Description
Email	• Enter the **To**, **CC**, and **BCC** addresses separated by commas. **Note:** Only the **From** and **To** addresses are required • Enter a Subject and Body. **Note:** The area above these options displays usable message variables. Refer to the default Notification Profile for formatting.
Webhook	• Enter the Endpoint URL designated for ETM Dashboard notifications. • Click **Add Header** and enter a Name and Value if the custom integration requires custom headers. • Select an HTTP **Method**: GET, POST, or PUT.
Slack	Enter the target **Endpoint URL** to connect the application.
Pager Duty	• Enter the **Routing Key** designated for ETM Dashboard notifications. • Select a severity level: Critical, Error, Warning, or Info.
VictorOps	• Enter the **Endpoint URL** designated for ETM Dashboard notifications. • Select a **Message Type**: Critical, Warning, or Info.
Untangle Go (Mobile)	From the list, select the Untangle Go application target for notifications. Connecting Untangle Go from multiple mobile devices displays a list of all available options.

d. Click **Create**.

Note: After creating a Notification Profile, users can assign it to Alert Rules. For more information, see Alert Rules.

2. To edit an existing Notification Profile, click **Edit Notification Profile** and edit the required fields. Click **Update**.
3. To delete a Notification Profile, select it and then click **Delete Notification Profile**.

Note: Notification Profiles that are associated with Alert Rules cannot be deleted.