

# ARISTA

## User Guide

## Edge Threat Management (ETM) Dashboard



<b>Headquarters</b>	<b>Support</b>	<b>Sales</b>
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
<a href="http://www.arista.com/en/">www.arista.com/en/</a>	<a href="mailto:support@arista.com">support@arista.com</a>	<a href="mailto:sales@arista.com">sales@arista.com</a>

© Copyright 2024 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](http://www.arista.com/en/terms-of-use). Use of marks belonging to other parties is for informational purposes only.

# Contents

- Chapter 1: Getting Started..... 1**
  - 1.1 Which Option to Use when Downloading NG Firewall Software..... 1
  - 1.2 Edge Threat Management Dashboard Overview..... 1
  - 1.3 Logging into the Arista Edge Threat Management Dashboard..... 2
  - 1.4 The Edge Threat Management Dashboard..... 3
  - 1.5 Getting Started with Edge Threat Management Mobile App..... 4
  
- Chapter 2: Networks..... 7**
  - 2.1 Managing Networks in ETM Dashboard..... 7
  - 2.2 Setting up Software-defined Networks in the ETM Dashboard..... 10
  
- Chapter 3: Appliances..... 14**
  - 3.1 Managing Appliances in the ETM Dashboard..... 14
  - 3.2 Adding Edge Threat Management Appliances to the ETM Dashboard..... 15
  - 3.3 Upgrading Appliances via the ETM Dashboard..... 15
  - 3.4 Assigning a Location to Appliances in the ETM Dashboard..... 16
  - 3.5 Managing Backup Configurations in ETM Dashboard..... 17
  - 3.6 Labeling Appliances in the ETM Dashboard..... 19
  - 3.7 How to Remove an Appliance from the ETM Dashboard..... 21
  
- Chapter 4: Hosts..... 22**
  - 4.1 Managing Hosts in the ETM Dashboard..... 22
  - 4.2 Managing Endpoints via Bitdefender GravityZone Integration..... 27
  - 4.3 Managing Endpoints via Webroot Integration..... 29
  - 4.4 Managing Endpoints via Malwarebytes Integration..... 30
  
- Chapter 5: Events and Alerts..... 31**
  - 5.1 Managing Tasks in the ETM Dashboard..... 31
  - 5.2 Viewing Events in the ETM Dashboard..... 32
  - 5.3 Managing Alert Rules..... 33
  - 5.4 Creating an Alert Rule from an Event..... 34
  - 5.5 Managing Notification Profiles..... 35
  
- Chapter 6: Policies..... 38**
  - 6.1 Assigning or Synchronizing a Common Configuration to the NG Firewall Appliances..... 38
  
- Chapter 7: Reports..... 41**
  - 7.1 The ETM Dashboard Reports..... 41
  
- Chapter 8: Licensing and Subscriptions..... 45**
  - 8.1 How to Assign a Subscription to an Appliance..... 45
  - 8.2 Upgrading an Appliance Subscription..... 46

8.3 How to Remove/Unassign a Subscription from an Appliance.....	48
8.4 How to Share a Subscription to a Different Account.....	49
8.5 How to Transfer a Subscription to Another Appliance.....	49
8.6 How to Renew a Subscription.....	50
8.7 Redeeming a Voucher.....	51
8.8 How to Create a Subscription Renewal Quote.....	52
8.9 Enabling or Disabling Auto-Renewal.....	53
<b>Chapter 9: Account and Organization Management.....</b>	<b>54</b>
9.1 Configuring SAML, OAuth2, or OpenID Login in the ETM Dashboard.....	54
9.2 ETM Dashboard Organization.....	57
9.3 Enabling or Disabling Automatic Sign-on to Appliances.....	57
9.4 Enabling and Disabling Dashboard Widgets on the ETM Dashboard.....	57
9.5 Switching Themes on the ETM Dashboard.....	58
9.6 Two-Factor Authentication on the ETM Dashboard.....	59
9.7 General Data Protection Regulation (GDPR).....	61
9.8 Request a Copy of your Data.....	61
9.9 Deleting an ETM Dashboard Account.....	62

## Getting Started

This section discusses the following topics:

- [Which Option to Use when Downloading NG Firewall Software](#)
- [Edge Threat Management Dashboard Overview](#)
- [Logging into the Arista Edge Threat Management Dashboard](#)
- [The Edge Threat Management Dashboard](#)
- [Getting Started with Edge Threat Management Mobile App](#)

### 1.1 Which Option to Use when Downloading NG Firewall Software

The NG Firewall software is free to download and works on multiple platforms. But how do I know which download I need?

Your choice of download format depends on the method you intend to use to install the software:

- Select the *Serial Installer* version if you intend to install using a serial console connection. Here are more details on the serial console: [Managing wSeries and eSeries appliances via Serial Console](#).
- Select the *ISO Installer* version for all other install types (hardware or virtual environment).

### 1.2 Edge Threat Management Dashboard Overview

Arista's Edge Threat Management (ETM) Dashboard is a cloud-based central management platform that lets you centrally manage your Micro Edge and NG Firewall deployments from a browser. All features of ETM Dashboard are available to licensed Micro Edge and NG Firewall deployments.

The screenshot shows the Arista ETM Dashboard interface. The left sidebar contains navigation options: DASHBOARD, ALERTS, APPLIANCES, HOSTS, REPORTS, TOOLS, DOWNLOAD, MY ACCOUNT, and MY ORGANIZATION. The main content area is divided into several sections:

- Information:** Shows login details for 'etm-agent@arista.com' and account owner 'Arista ETM [etm-agent@arista.com]'. It indicates 9 appliances online and 6 offline. Summary statistics include 15 appliances, 2 active hosts, and 3 blocked threats. The user is logged in from IP 93.184.216.34 in Hyperborea.
- Appliance Map:** A map of the United States with red location pins.
- Appliances Table:** A table listing appliance details.
 

Status	License	Appliance	Version	Serial Number	Network	Host Count	Location	Last Seen
●	▲	ec2-52-52-20-106.us-west-1.compute.amazon...	16.6.2	Not Found	Not Assigned	0	San Jose, CA	Now
●	▲	qfial.demo.arista.com	4.3	1019FLA001014	ACME Auto Parts	2	Jacksonville, FL	Now
●	▲	plcoos1.pluethunetworks.com	4.2	Not Found	Not Assigned	0	Santa Clara, CA	Now
●	▲	duz2f.sj.aristanetworks.com	16.6.2	1018ADA001045	Not Assigned	0	San Jose, CA	Now
●	▲	Q1.example.com	16.5.2	CTW22380002	Not Assigned	0	Bend, OR	Now
●	▲	duz12.sj.aristanetworks.com	16.5.2	020180A9999900	ACME Auto Parts	0	Las Vegas, NV	Now
●	▲	Q6.example.com	16.6.2	0201ADA0000000	Not Assigned	0	Miami, FL	Now
●	▲	zfa-demo.example.com	16.5.2	0201DWA0001001	ACME Auto Parts	0	Fair, MI	Now
- Audit History:** A log of events including logins and network rule pushes.
- Top Applications (by bandwidth) - Last 30 Days:** A pie chart showing traffic distribution for applications like APPLE 6.0% and SQL 29.4%.
- Recent Hosts:** A table listing active hosts with columns for hostname, appliance, IP address, and active status.
- Total Bandwidth - Last 30 Days:** A line graph showing bandwidth usage over time.
- Top Domains (by request):** A pie chart showing domain traffic distribution.

---

Critical features of the ETM Dashboard include:

- Slack, PagerDuty, VictorOps, or email notifications based on essential activities.
- Mobile app to manage appliances and subscriptions from a mobile device.
- Central reporting of Micro Edge and NG Firewall deployments.
- Secure remote access via Single Sign-On to any of your Edge Threat Management appliances.
- License management of your Edge Threat Management appliances.
- Automatic daily backup and optional configuration restore.
- Configuration templates with real-time sync.
- Host and device management with integration to Bitdefender, Malwarebytes, and Webroot.

To log in or to create a free ETM Dashboard account, navigate to <https://edge.arista.com/cmd>.

## 1.3 Logging into the Arista Edge Threat Management Dashboard

You can manage all of your networks using Arista's cloud-based ETM Dashboard.

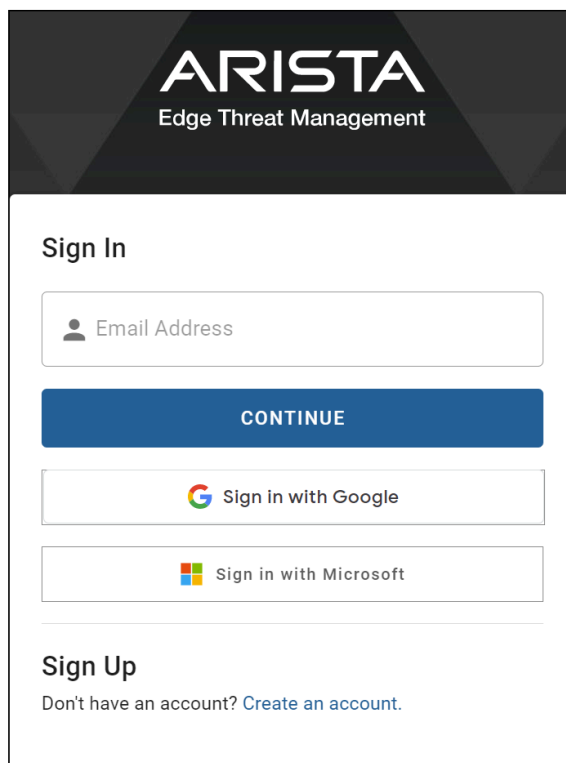
### Creating an Account

To log into the ETM Dashboard, you must have a login account. If you do not have an account yet, click **Create an Account** at the bottom of the page to set one up.

### Logging into the ETM Dashboard

To log into your account:

1. Go to <https://launchpad.edge.arista.com>.
2. Enter your email address in the **Email Address** field and click **Continue** to log in with an ETM Dashboard account.



The screenshot shows the login interface for the Arista Edge Threat Management Dashboard. At the top, the Arista logo is displayed with the text "ARISTA Edge Threat Management". Below the logo, the "Sign In" section contains an input field for "Email Address" with a person icon, a blue "CONTINUE" button, and two social login options: "Sign in with Google" and "Sign in with Microsoft". At the bottom, the "Sign Up" section includes the text "Don't have an account? [Create an account.](#)"

3. A **Password** field appears on the page. Enter your password and click **Log In** to enter your account.



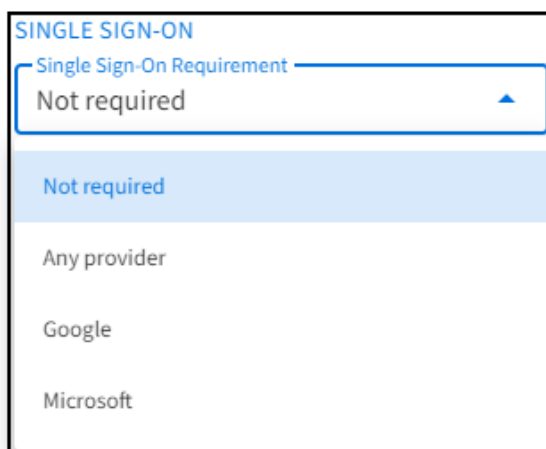
**Note:** If you do not know your account password, click **Forgot your Password?** to send an email containing a password reset link.

### Logging into ETM Dashboard using Single Sign-On with Google or Microsoft Accounts

If you have an existing Google or Microsoft account and want to Single Sign-On (SSO) to log into your ETM Dashboard account, you can do so by clicking the appropriate button (below the **Log In** button). This redirects you to the service provider's login page. If your SSO account requires multi-factor authentication (MFA), you will receive the code via your usual method and complete the MFA through the SSO login page.

Once logged into that service, you are logged into your ETM Dashboard account.

You can also require SSO to access your ETM Dashboard account. This option is located in **My Organization > Settings**:



Not required	SSO is available, but it is not required to log into this ETM Dashboard account.
Any provider	You must use SSO to access this ETM Dashboard account, but either Google or Microsoft SSO is allowed.
Google	You must select Google SSO to log into this ETM Dashboard account.
Microsoft	You must select Microsoft SSO to log into this ETM Dashboard account.

### Logging into ETM Dashboard using SAML, OAuth2, or OpenID Single Sign-On Accounts

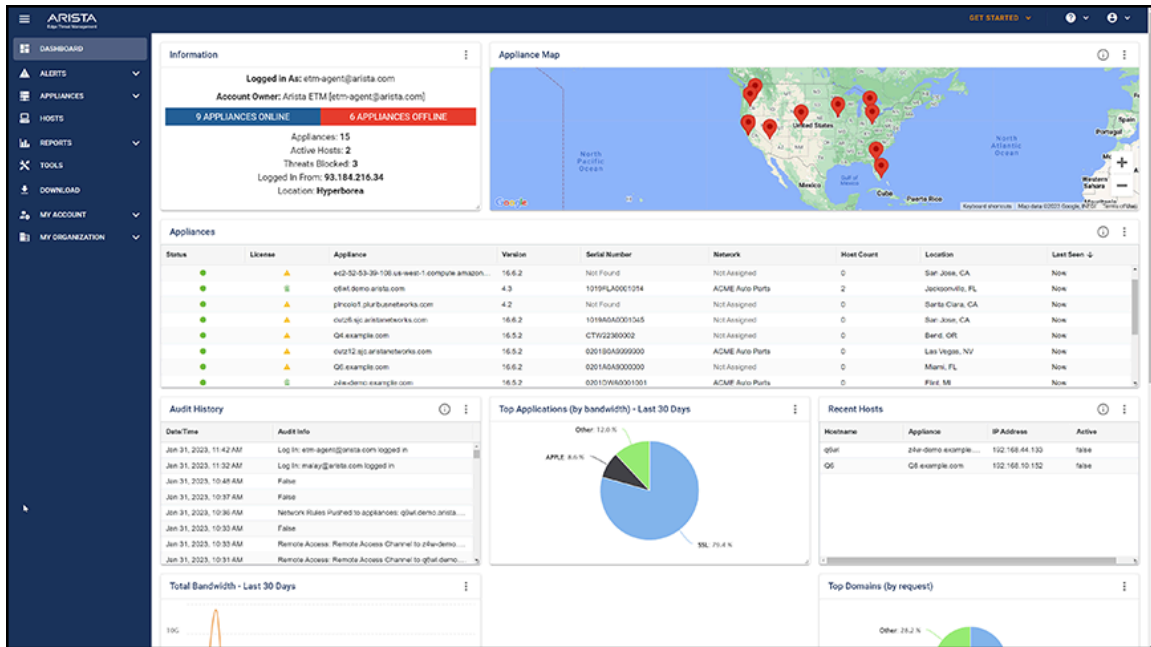
Refer to this article to configure these Identity Provider connections: [Configuring SAML, OAuth2, or OpenID Login in the ETM Dashboard](#).

Enter your Organization Name in the **Email or Organization** field to log into your account.

Click **Continue** to be redirected to your Identity Provider's SSO login page, where you will complete your login. When you successfully log into your IdP's system, you will be logged in and redirected to your ETM Dashboard account.

## 1.4 The Edge Threat Management Dashboard

The Edge Threat Management (ETM) Dashboard is a high-level view of all networks and appliances associated with your Arista ETM Dashboard account.



## Viewing the Dashboard

When logging into the ETM Dashboard, you are directed to the Dashboard. From the Dashboard, you can see the status and locations of your managed networks. You can also view reports, audit histories, recent threats, and more via the Dashboard Widgets.

By default, the ETM Dashboard shows all Dashboard Widgets. You can configure which Widgets to see in your **Preferences**. See [Enabling and Disabling Dashboard Widgets](#) for more details.

## 1.5 Getting Started with Edge Threat Management Mobile App

Arista Go is a mobile app for Android and iOS-based devices that extends ETM Dashboard functionality to your mobile device, enabling you to manage your networks and Edge Threat Management appliances from anywhere.

Arista Go enables you to:

- Review recent alerts related to your Edge Threat Management appliances and managed networks.
- Review the connection status and details of your Edge Threat Management appliances.
- Review the subscriptions associated with your Edge Threat Management appliances.

### Installing Arista Go

Arista Go is accessible through the Google Play and Apple app stores. To install the app:

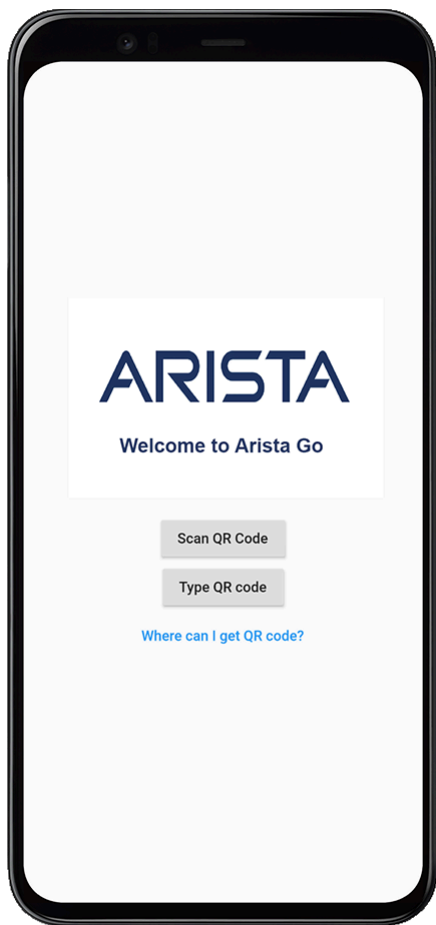
1. On your mobile device, open the browser and navigate to <https://play.google.com/store/apps/details?id=com.untangle.go> (Android) or <https://apps.apple.com/us/app/untangle-go/id1561237778> (Apple iOS). Alternatively, open your Google Play or Apple App Store app and search for "Untangle Go."
2. Review the app details to ensure they meet your device's requirements.
3. Click **Install** or **Get**, depending on your device.

### Pairing the app to your ETM Dashboard Account

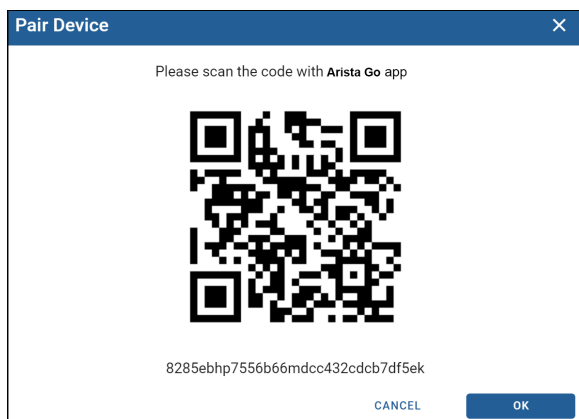
1. After Arista Go installs, launch the app.



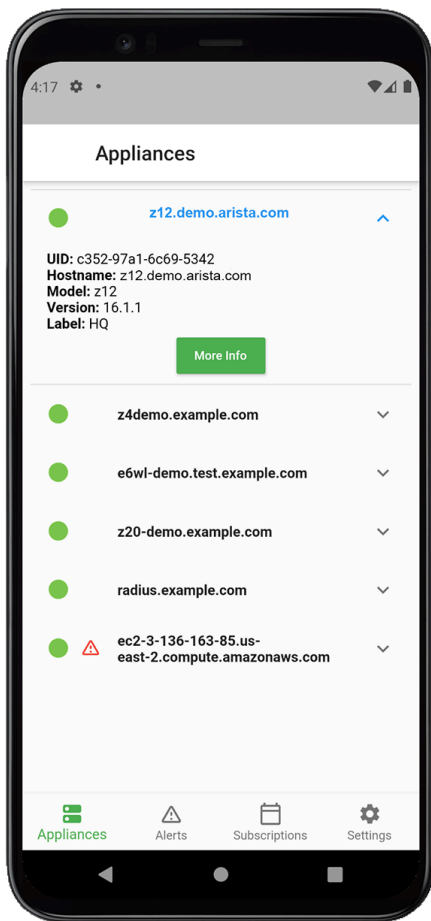
2. If you want to receive ETM Dashboard alerts, allow notifications when prompted.
3. On the next screen, choose how to pair your device. If you decide to **Scan the QR code**, the app asks permission to use your phone's camera. If you prefer not to consent to your camera, choose **Type QR code**.



4. To obtain your QR code, log into your ETM Dashboard account and navigate to **My Account** > **Arista Go**.
5. Click **Pair Device**.



6. Direct your phone's camera at the QR image, or type the QR code below the image if you prefer not to use the camera.
7. After your account is paired, you can manage your appliances using the app.



## Unpairing your Device

To disconnect the app from your account:

1. Open the app and navigate to **Settings**.
2. Click **Unpair device**.

## Networks

This section discusses the following topics:

- [Managing Networks in ETM Dashboard](#)
- [Setting up Software-defined Networks in the ETM Dashboard](#)

### 2.1 Managing Networks in ETM Dashboard

ETM Dashboard enables you to group Edge Threat Management NG Firewall and Micro Edge appliances into a network. By grouping appliances, you can obtain information specific to the collection of appliances in the Network. You can also apply a standard set of WAN Routing Rules to all Micro Edge appliances that belong to the same Network.



**Note:** NG Firewall appliances require a complete subscription to add to a network.

#### Creating a Network

To create a Network:

1. Click the **Networks** tab. The Networks screen shows a list of your Networks.
2. Click **Create Network**.
3. Select the NG Firewall and Micro Edge appliances to add to your Network.
4. Click **Next** to review the summary of your Network.
5. Click **Create**.

The screenshot displays the ARISTA ETM Dashboard interface. The left sidebar contains navigation options: DASHBOARD, ALERTS, APPLIANCES, HOSTS, REPORTS, TOOLS, DOWNLOAD, MY ACCOUNT, and MY ORGANIZATION. The main content area is divided into several sections:

- Information:** Shows the user is logged in as 'etm-agent@arista.com' with account owner 'Arista ETM [etm-agent@arista.com]'. It displays '9 APPLIANCES ONLINE' and '6 APPLIANCES OFFLINE'. Summary statistics include: Appliances: 15, Active Hosts: 2, Threats Blocked: 3, Logged In From: 93.184.216.34, and Location: Hyperborea.
- Appliance Map:** A map of the United States with red location pins indicating the positions of various appliances.
- Appliances Table:** A table listing individual appliances with columns for Status, License, Appliance, Version, Serial Number, Network, Host Count, Location, and Last Seen.
 

Status	License	Appliance	Version	Serial Number	Network	Host Count	Location	Last Seen
●	▲	4c2-52-53-39-106.us-east-1.compute.amazonaws.com	16.6.2	Not Found	Not Assigned	0	San Jose, CA	Now
●	▲	qfai.demo.arista.com	4.3	1019PLA0001014	ACME Auto Ports	2	Jacksonville, FL	Now
●	▲	pkrc0f1.pluribusnetworks.com	4.2	Not Found	Not Assigned	0	Santa Clara, CA	Now
●	▲	cu2f6.gp.aristanetworks.com	16.6.2	1018MA0001545	Not Assigned	0	San Jose, CA	Now
●	▲	Q6.example.com	16.5.2	CTW2280002	Not Assigned	0	Beard, OR	Now
●	▲	cu2f12.gp.aristanetworks.com	16.5.2	02015AA0000000	ACME Auto Ports	0	Las Vegas, NV	Now
●	▲	Q6.example.com	16.6.2	02015AA0000000	Not Assigned	0	Miami, FL	Now
●	▲	zha-demo.example.com	16.5.2	02017AA0001001	ACME Auto Ports	0	Fort, MI	Now
- Audit History:** A log of events such as 'etm-agent@arista.com logged in' and 'Network Rules Pushed to appliances: qfai.demo.arista.com'.
- Top Applications (by bandwidth) - Last 30 Days:** A pie chart showing traffic distribution: SSL (75.4%), Other (12.6%), and APPLE (8.6%).
- Recent Hosts:** A table listing recent hosts with columns for Hostname, Appliance, IP Address, and Active status.
 

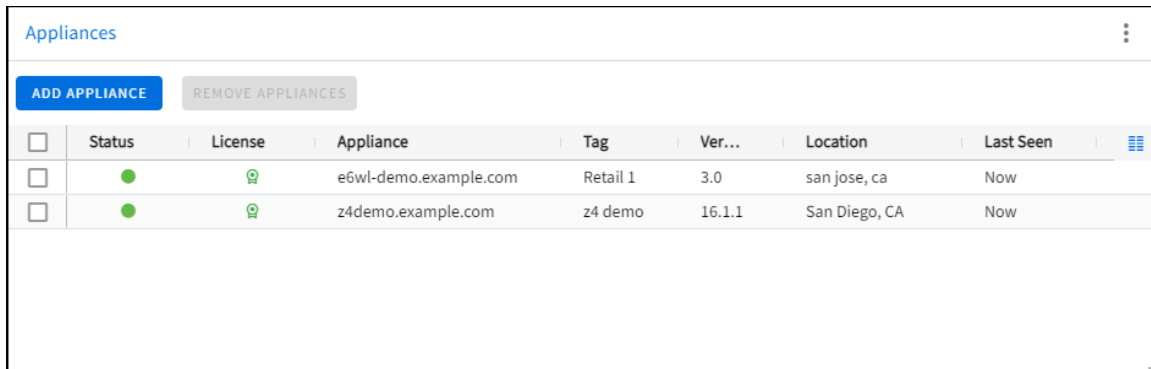
Hostname	Appliance	IP Address	Active
qfai	zha-demo.example.com	192.168.44.133	1994
Q6	Q6.example.com	192.168.10.152	1994
- Total Bandwidth - Last 30 Days:** A line graph showing bandwidth usage over time.
- Top Domains (by request):** A pie chart showing traffic distribution: Other (78.2%), and a small portion for another category.

## Managing Appliances in your Network

Your Networks appear in the **Networks** panel of the Networks screen. Select a Network to manage its associated appliances.

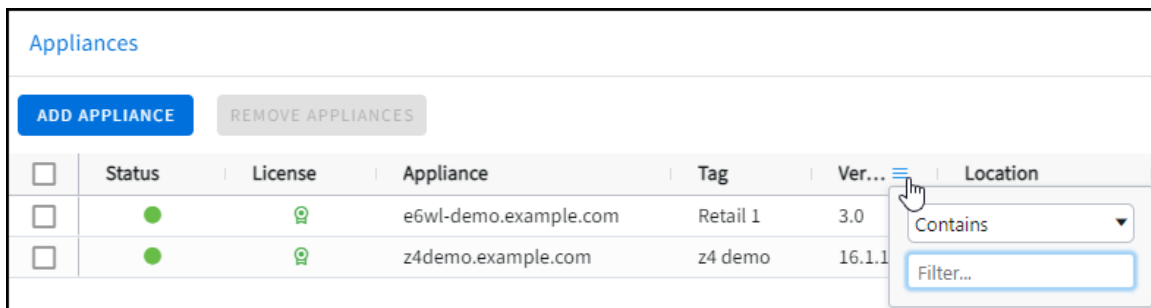
### Appliances Widget

The Appliances widget shows the status, software version, location, IP address, and other relevant details of each appliance in your Network. You can add or remove appliances from your Network using the **Add Appliance** and **Remove Appliance** buttons at the bottom of the widget.



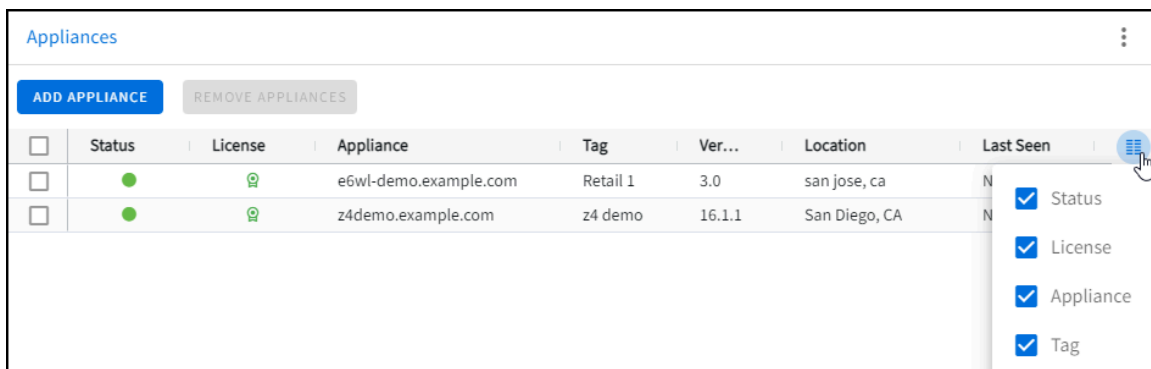
<input type="checkbox"/>	Status	License	Appliance	Tag	Ver...	Location	Last Seen	
<input type="checkbox"/>	●	🔒	e6wl-demo.example.com	Retail 1	3.0	san jose, ca	Now	
<input type="checkbox"/>	●	🔒	z4demo.example.com	z4 demo	16.1.1	San Diego, CA	Now	

Select the filter options to locate an appliance in the list by clicking the three horizontal lines in any column header.



<input type="checkbox"/>	Status	License	Appliance	Tag	Ver...	Location	Last Seen	
<input type="checkbox"/>	●	🔒	e6wl-demo.example.com	Retail 1	3.0			
<input type="checkbox"/>	●	🔒	z4demo.example.com	z4 demo	16.1.1			

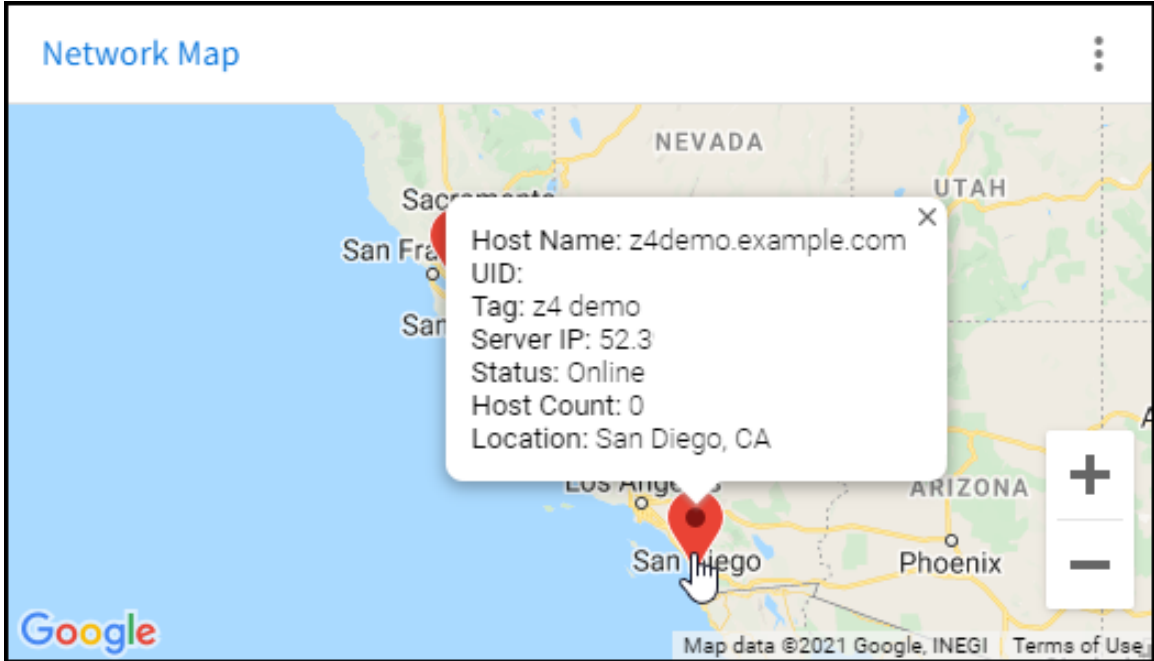
The grid menu provides additional options, including sorting and choosing columns to show or hide appliance properties.



<input type="checkbox"/>	Status	License	Appliance	Tag	Ver...	Location	Last Seen	
<input type="checkbox"/>	●	🔒	e6wl-demo.example.com	Retail 1	3.0	san jose, ca	N	
<input type="checkbox"/>	●	🔒	z4demo.example.com	z4 demo	16.1.1	San Diego, CA	N	

### Map Widget

The Network Map widget displays the physical location of each appliance in your network. Hover over a marker to view additional details about the appliance, or click the marker to open the dashboard. If you enable appliances in Software-defined Networks, the map draws green or red lines between the markers to indicate the link status between each location.



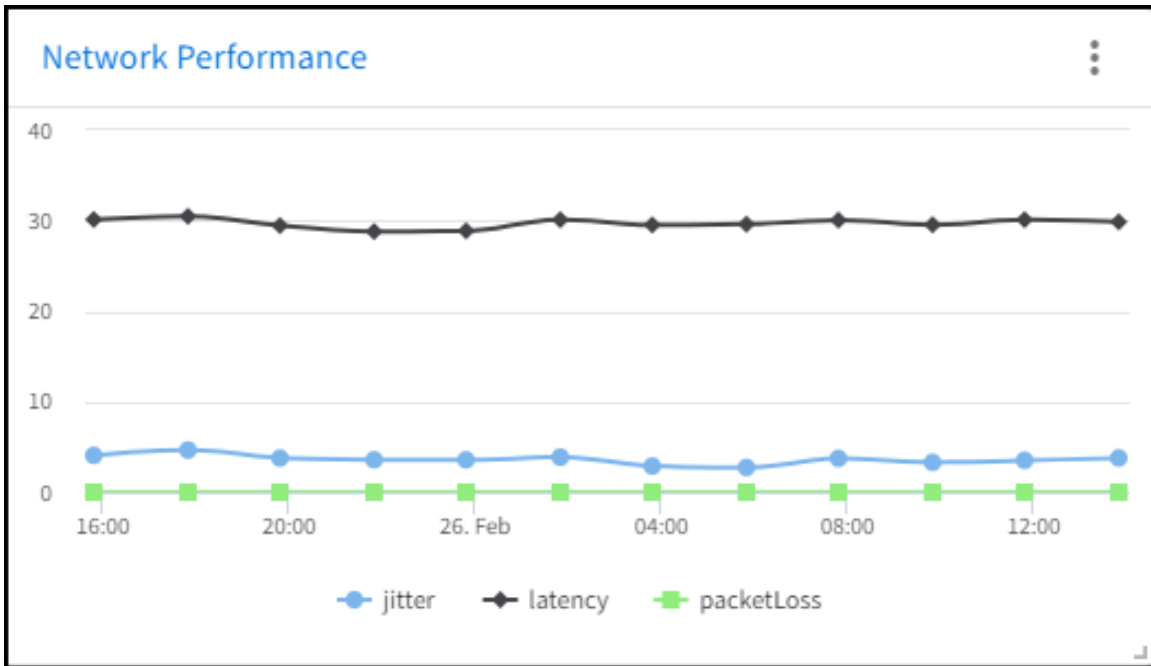
### Software-defined Networks Widget

The Software-defined Networks widget enables you to configure a Virtual Private Network for appliances in the network. For more information on this widget, see [Setting up Software-defined Networks in ETM Dashboard](#).

Software-defined Networks				
CONFIGURATION				
SYNC VPN SETTINGS				
RESET TO DEFAULTS				
Status	License	Appliance	IP Address	Shared Subnets
●	🔒	z4w-demo.example.com	104.2.147.129	192.168.44.0/24
●	⚠️	dutz12.sjc.aristanetworks.com	162.210.130.3	192.168.2.0/24
●	🔒	q6wl.demo.arista.com	162.210.130.3	172.16.25.0/24

### Network Performance Widget

The Network Performance widget displays the average jitter, latency, and packet loss across all Micro Edge appliances in your Network. Click any of the performance metrics in the legend to show or hide its view in the line chart.



### WAN Rules Widget

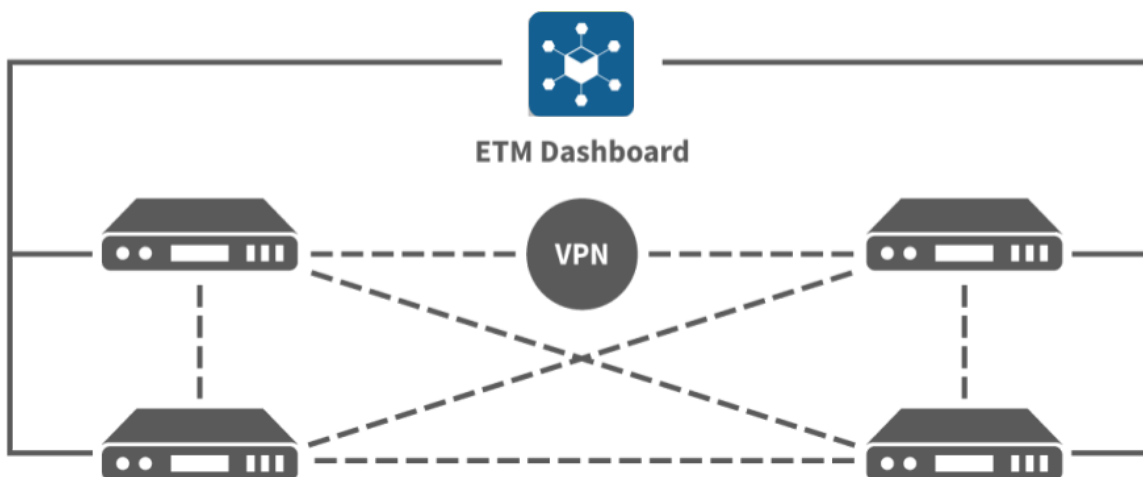
The WAN Rules widget establishes a common WAN Routing strategy for all Micro Edge appliances in your Network; for more information, see [Configuring WAN Rules for Micro Edge in the ETM Dashboard](#).

The Configuration interface includes buttons for 'ADD WAN RULE', 'EDIT WAN RULE', 'DELETE WAN RULES', and 'SYNC RULES TO APPLIANCES'. Below is a table of configured WAN rules.

<input type="checkbox"/>	Name	Summary	WAN Policy
<input type="checkbox"/>	☰ Prioritize Secondary Link For File Transfers	Application Category == File Transfer	Specific WAN - WAN1
<input type="checkbox"/>	☰ Primary WAN For Productivity Apps	Undefined == 5	Specific WAN - WAN0
<input type="checkbox"/>	☰ Lowest Latency Zoom		Lowest Latency - Any WAN
<input type="checkbox"/>	☰ Lowest Latency For Salesforce		Lowest Latency - Any WAN

## 2.2 Setting up Software-defined Networks in the ETM Dashboard

You can automatically set up one or more software-defined networks to connect remote office networks managed by Micro Edge and NG Firewall. The ETM dashboard controls each software-defined network and uses [WireGuard VPN](#) tunnels to route traffic between each network in a site-to-site mesh topology. Managing your software-defined networks via ETM Dashboard reduces the complexity of manually configuring VPN tunnels.



### Prerequisites

Before configuring your Software-defined network, confirm that your appliances meet the following requirements:

#### Micro Edge

- Version **3.1** or newer

#### NG Firewall

- Version **16.1** or newer.
- IPsec and OpenVPN must be disabled or uninstalled.
- NG Firewall Complete or Trial License.
- You must install the WireGuard app.

### Setting up the Software-defined Network

To set up your software-defined network, you must first create one. See [Managing Software-defined Networks in ETM Dashboard](#) for steps to create your Software-defined Network.

After your Software-defined Network is set up with at least two appliances, you can configure the Software-defined Network.

1. From the **Networks** list, select your network.
2. Locate the **Software Defined Network** widget containing the appliances in your network.



3. Select each appliance and click **Configuration**.
4. Turn on the **Enable** option to activate VPN access for this appliance and the networks behind it.
5. After enabling access, choose the local subnets you want to make accessible to other appliances in this network.
6. You can also specify a new Endpoint Address if you would like to choose the WAN IP address used when other appliances connect to this appliance. You can enable the 'Automatic' option to allow the ETM Dashboard to determine the appropriate endpoint address.

configuration - e6wl.demo.example.com
✕

Enabling VPN Access will add tunnels with all VPN enabled appliances in the current network.

Enable

ENDPOINT ADDRESS

Automatic (162.210.130.3)

The VPN Tunnel endpoint will be configured using the Internet IP address registered to ETM Dashboard.

SHARED SUBNETS

Select subnets behind this appliance that must be accessible to all other peered networks in this VPN. An empty selection means the appliance will be in client mode.

192.168.10.0/24

192.168.99.99/32

CANCEL
SAVE

### Notes regarding shared subnets:

- Selecting shared subnets is optional. If no local subnets are enabled, this appliance network acts in client mode and can access resources of remote networks but not vice versa.
- If a local subnet conflicts with a shared subnet from a different appliance, you cannot enable VPN access, which may result in routing issues.

### Synchronizing the Software-defined Network

After you enable access to your appliances and specify shared subnets, you must synchronize your changes. This action adds, removes, or updates VPN tunnels for each appliance in the network.

By clicking **Sync VPN Settings**, the ETM Dashboard queues the request for processing, which may take several minutes. You can review the [Audit History](#) to check the status of your sync request.

Software Defined Network

CONFIGURATION
SYNC VPN SETTINGS
Last sync initiated at Aug 2, 2021, 4:53 PM. View status in [Audit History](#).

After synchronization, you can review the tunnels and their status by logging into each appliance.



**Note:** For NG Firewall appliances, the ETM Dashboard creates a tunnel for each remote appliance in the network. The ETM Dashboard only has a single tunnel interface for Micro Edge appliances. However, all remote networks are serviced via this tunnel interface.



**Important:** You may view the tunnels managed by the ETM Dashboard for status information and other relevant details. However, it would help if you did not edit these tunnels, as the ETM Dashboard will overwrite the changes during the next synchronization.

### Troubleshooting

You confirm that the VPN tunnels are synchronized to an NG Firewall appliance; you can view the *Enabled Tunnels* grid on the [WireGuard VPN Status](#) page. The *Last Handshake* confirms the most recent successful transfer, and the *Bytes In* and *Bytes Out* ensure that data flows in both directions.



Enabled Tunnels

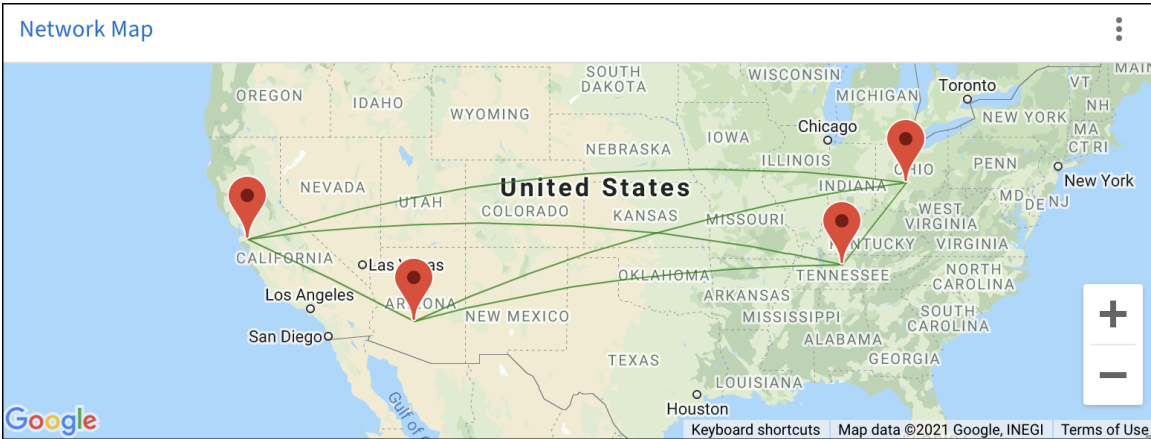
Description	Remote Endpoint	Remote Networks	Last Handshake	Bytes In	Bytes Out
CCTunnel1	10.111.0.124	192.168.102.0/25,192.168.10.0/2...	2021-08-23 10:53:49 am	244.63 KB	429.12 KB
CCTunnel2	192.168.10.185	192.168.222.0/24,172.16.2.1/32	No recent activity	148 B	5.36 MB

Refresh Reset View

You can view the [Interfaces](#) screen to confirm that VPN tunnels are synchronized to a Micro Edge appliance. The **Connected** and **Online** statuses confirm that the tunnel is up, and the arrows confirm that data flows in both directions.

**CCTunnel**  
● connected | ● online | ↓ 0.086 KBps ↑ 0.154 KBps  
Type: WIREGUARD | Device: CCTunnel  
IPv4: 172.21.161.1/24 (wireguard)

You can check the status of your Centrally Managed Network tunnels from the Network Dashboard. The Network Map shows the links between each peer in the network.



If there is a specific reason that an appliance cannot sync, the Software Defined Network widget provides information in the **Notes** column next to the associated appliance.

# Appliances

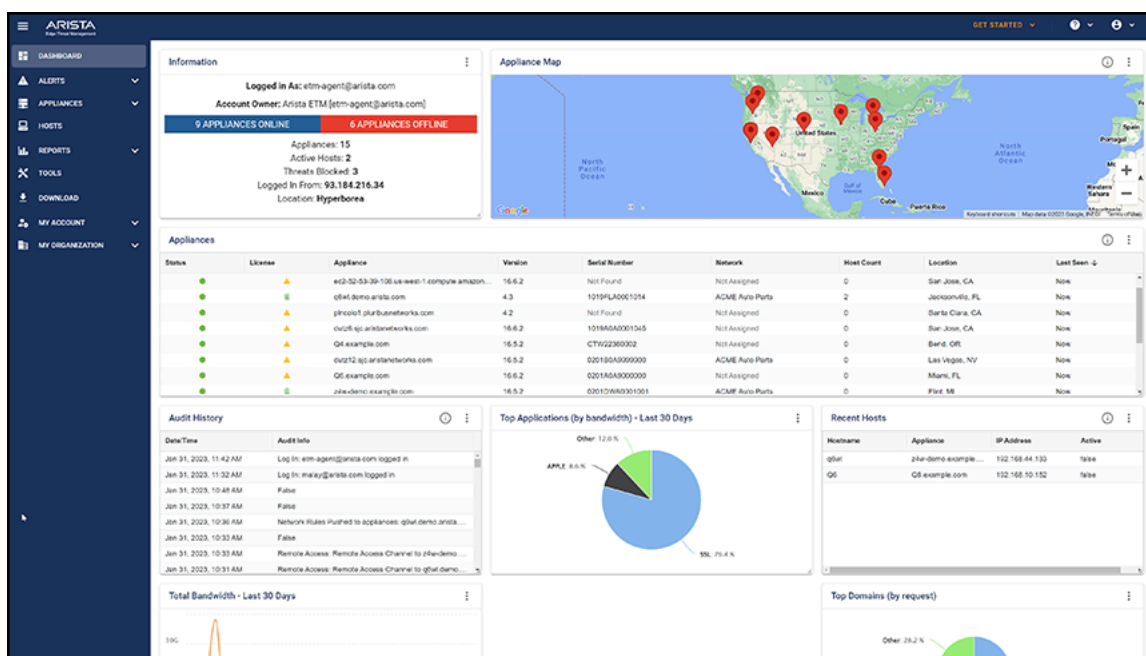
This section discusses the following topics:

- [Managing Appliances in the ETM Dashboard](#)
- [Adding Edge Threat Management Appliances to the ETM Dashboard](#)
- [Upgrading Appliances via the ETM Dashboard](#)
- [Assigning a Location to Appliances in the ETM Dashboard](#)
- [Managing Backup Configurations in ETM Dashboard](#)
- [Labeling Appliances in the ETM Dashboard](#)
- [How to Remove an Appliance from the ETM Dashboard](#)

## 3.1 Managing Appliances in the ETM Dashboard

The ETM Dashboard is a cloud-based service for managing Edge Threat Management appliances. For example, you can perform the following appliance management tasks using the ETM Dashboard:

- See the status of all your deployments in a single dashboard view.
- Remotely connect to your appliances without logging in.
- Push shared configuration profiles to multiple appliances.
- Backup and restore configuration.
- Apply or transfer a license subscription.
- Set up notifications to your email, Arista Go mobile app, Slack, PagerDuty, or VictorOps accounts
- Review consolidated alerts and reports.



**Requirements:**

To use ETM Dashboard with your Edge Threat Management deployments, you must meet the following requirements:

- NG Firewall version **12.2** or higher. No minimum version of Micro Edge is required to connect to the ETM Dashboard.
- Registered account in ETM Dashboard. You can create an account [here](#).
- **Connect to ETM Dashboard** option in NG Firewall must be enabled. You can find this option in **Config > System > Support**.

The ETM Dashboard is a free service. However, for full functionality, you must assign your appliance a subscription. Features that require an appliance subscription include [Policies](#), [Alerts](#), [Reports](#), and [Networks](#).

**Adding an Appliance to your ETM Dashboard Account**

You can add NG Firewall and Micro Edge appliances to ETM Dashboard: [Adding Edge Threat Management appliances to ETM Dashboard](#).

**3.2 Adding Edge Threat Management Appliances to the ETM Dashboard**

You can remotely manage and access your NG Firewall and Micro Edge appliances by adding them to your ETM Dashboard account. If the appliance is online but not configured, you can add it based on its serial number by a process referred to as Zero Touch Provisioning. Alternatively, you can add the appliance using its UID if you do not know the serial number.

**3.3 Upgrading Appliances via the ETM Dashboard**

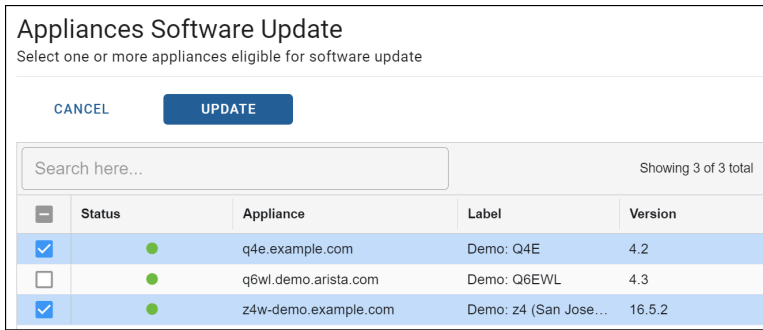
The ETM Dashboard enables the admin to upgrade multiple appliances simultaneously without connecting to each one. You can also configure schedules for automatic upgrades in the ETM Dashboard.

**Upgrading Multiple Appliances**

1. Go to the **Appliances** page. The Appliances grid displays the software version of each device.
2. Click the blue **Update Software** button at the top of the list.

Status	Appliance	Label	Version
●	q4e.example.com	Demo: Q4E	4.3
●	ec2-52-53-39-108.us-...	Demo: AWS	16.6.2
●	q6wl.demo.arista.com	Demo: Q6EWL	4.3

3. The list of appliances is filtered only to include those that can be upgraded.
4. Select the appliances you want to upgrade and click the **Update** button.



The update process is initiated for all selected appliances.

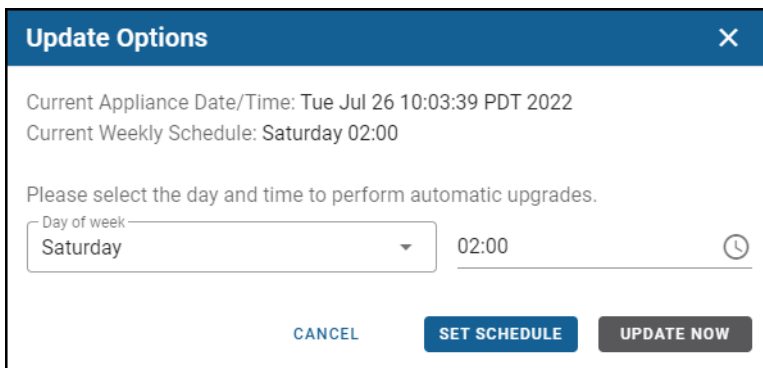
### Configuring Scheduled Automatic Upgrades

1. Go to **Appliances** and select the appliance to set the scheduling policy.
2. Click the **Update Software** button.



Select the day and time you want the appliance updated in the menu that pops up.

3. Click **Set Schedule** to apply the schedule.



## 3.4 Assigning a Location to Appliances in the ETM Dashboard

The ETM Dashboard and Appliance detail screens display a map showing the geographic location of your appliances. These detail screens help you identify which appliance you want to manage or see from a single view where all your appliances are geographically located. The ETM Dashboard uses IP-based geo-location technology to estimate the location of your appliances. You can assign a precise address in the appliance details if you prefer to define a precise address.

### Updating an Appliance Location

Select an appliance to view the current assigned location data in the Appliances view. The appliance location appears in the Appliance Map widget.

z4w-demo.example.com - Demo: z4 (San Jose office)

REMOTE ACCESS SET LABEL ADD LICENSE UPDATE SOFTWARE REBOOT REMOVE APPLIANCE

**Information**

z4w-demo.example.com  
Version: 16.5.2  
203d 1h 5m 34s  
CPU Count: 4  
Architecture: x86\_64  
Host Count: 0  
IP Address: 93.184.216.34  
Network Name: ACME Auto Parts

**Appliance Map**

Flint, MI  
MICHIGAN  
Detroit  
Ann Arbor  
Grand Rapids  
Traverse City  
Green Bay  
Appleton  
Milwaukee  
Chicago  
Mississauga  
Toronto  
Hamilton

To update the location of your appliance or network:

1. Click **Edit**.
2. Enter the new address.
3. Click **Save**.

**Edit Location**

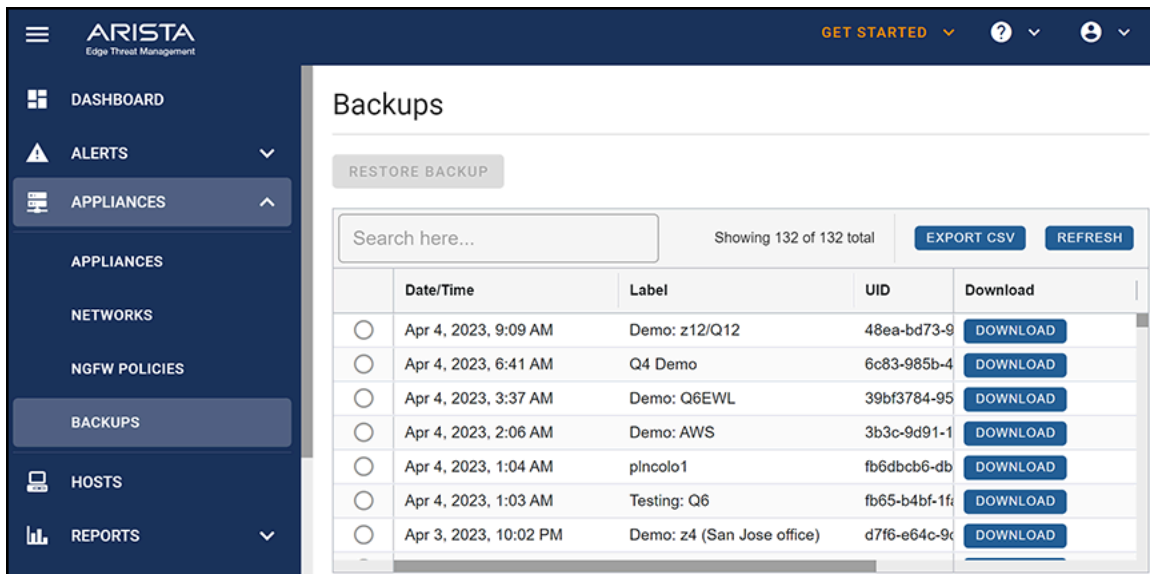
Enter an address for your appliance

Location  
Kokomo, IN

CANCEL SAVE

## 3.5 Managing Backup Configurations in ETM Dashboard

The ETM Dashboard enables you to automatically backup configuration data from appliances connected to your account. After an appliance performs at least one backup to the ETM Dashboard, you can select the backup file as a [Configuration Template](#) or restore it to the source appliance or any other appliance connected to this account.



## Requirements

This functionality requires the [Configuration Backup](#) for the NG Firewall.

This feature operates automatically in Micro Edge: no special settings or configurations are required.

## Notes Regarding Restoring Backups

A backup file can only be restored to the same version it was drawn from or one newer version. For example, an NG Firewall backup taken on **16.5** can be restored to **16.5** or **16.6**. A backup taken on Micro Edge **4.2** can be restored to **4.2** or **4.3**.

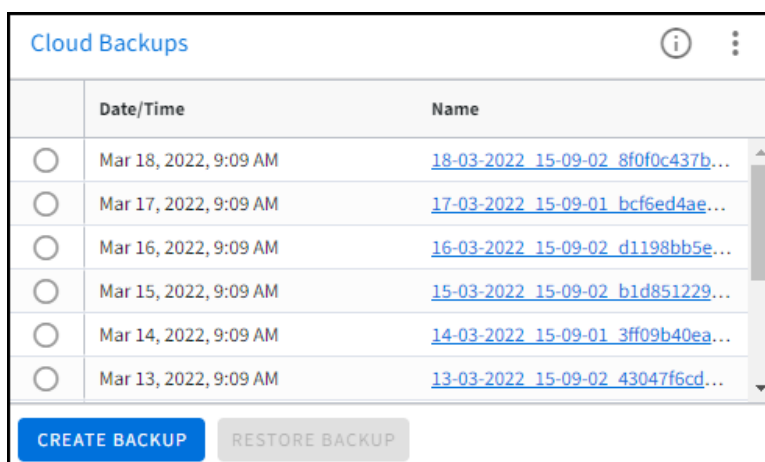
Backup files are not "backwards compatible," meaning that a backup file cannot be used on an older version of the software than the one it was taken on. For example, NG Firewall **16.5** cannot be restored to an NG Firewall running version **16.4** or older.

NG Firewall backups can only be restored to the NG Firewall. Micro Edge backups can only be restored to Micro Edge.

## Restoring a Configuration Backup to the Source Appliance

Select this option to restore an appliance using its backup config settings.

1. Go to the **Appliances** heading along the left-hand side of the page and select the **Appliances** tab.
2. Select the appliance from the appliances list.
3. Find the **Cloud Backups** Widget.
4. Select a backup file by date and click **Restore Backup**.
5. Click **Yes** to confirm.



	Date/Time	Name
<input type="radio"/>	Mar 18, 2022, 9:09 AM	<a href="#">18-03-2022 15-09-02 8f0f0c437b...</a>
<input type="radio"/>	Mar 17, 2022, 9:09 AM	<a href="#">17-03-2022 15-09-01 bcf6ed4ae...</a>
<input type="radio"/>	Mar 16, 2022, 9:09 AM	<a href="#">16-03-2022 15-09-02 d1198bb5e...</a>
<input type="radio"/>	Mar 15, 2022, 9:09 AM	<a href="#">15-03-2022 15-09-02 b1d851229...</a>
<input type="radio"/>	Mar 14, 2022, 9:09 AM	<a href="#">14-03-2022 15-09-01 3ff09b40ea...</a>
<input type="radio"/>	Mar 13, 2022, 9:09 AM	<a href="#">13-03-2022 15-09-02 43047f6cd...</a>

CREATE BACKUP RESTORE BACKUP

### Restoring a Backup to a Different Appliance

This option is useful when upgrading or replacing hardware or after a reinstall of the appliance.

Select to push common configurations that you would like shared amongst multiple appliances.

1. Go to the **Appliances** heading along the left-hand side of the page and select the **Backups** tab.
2. Select the backup configuration you would like to restore. The **UID** and **Label** columns identify the NG Firewall from which these settings were taken.
3. Click the **Restore Backup** button.
4. The *Restore Backup* menu opens, displaying all eligible NG Firewall appliances in your account. Select one or more appliances to push the config and click **Restore Backup**.
5. A confirmation menu displays your chosen backup file and the appliances you will restore to. Verify your selections and click **Confirm Restore** to initiate the backup.

### Creating a Backup File Manually

Click the **Create Backup** button in the **Cloud Backups** widget on the **Appliances** page to force an immediate backup of the selected appliance.

### Downloading a Backup File

You can download a copy of the backup settings file to your local computer in two ways:

- From the **Cloud Backups** widget on the **Appliances** page, click the link in the **Name** column.
- From the **Backups** page, click the **Download** button on the right-hand side.

## 3.6 Labeling Appliances in the ETM Dashboard

You can assign a label to appliances in the ETM Dashboard to help you identify them in a list. By default, the appliance displays its hostname first, then its label. In the following screenshot, the label is **Demo: z4**, in grey.

z4w-demo.example.com - Demo: z4

REMOTE ACCESS SET LABEL ADD LICENSE

Information

**z4w-demo.example.com**  
Version: 16.5.2

203d 1h 5m 34s

CPU Count: 4  
Architecture: x86\_64  
Host Count: 0  
IP Address: 93.184.216.34  
Network Name: ACME Auto Parts

**To Assign a Label:**

1. Click the **Appliances** option in the top bar.
2. Select the appliance from the list.
3. Click the **Set Label** button.

**Set Label** X

Please enter a label for your appliance

Label  
Miami, FL Office

CANCEL SAVE

4. Enter your label and click **Save**.



**Note:** A label is required when adding new appliances to the ETM Dashboard.



## 3.7 How to Remove an Appliance from the ETM Dashboard

In some situations, you may need to remove an appliance from your ETM Dashboard account. For example, you want to move your appliance to another account, or you reinstalled the NG Firewall, and the appliance has a new UID.



**Important:** removing an appliance from the ETM Dashboard will permanently delete any cloud backups for that appliance.

It is also removed if the appliance is part of an SD Network. However, tunnel configurations created on the appliance will remain and should be removed manually.

### Removing an Appliance

To remove an appliance from your account:

1. Navigate to **Appliances**.
2. Select the appliance to be removed.
3. Click the **Remove Appliance** button.
4. Confirm that you want to remove the appliance from your account.

The screenshot shows the ETM Dashboard interface for an appliance. At the top, the URL is 'q6wl.demo.arista.com - Demo: Q6EWL'. Below the URL, there is a row of action buttons: 'REMOTE ACCESS', 'SET LABEL', 'ADD LICENSE', 'UPDATE SOFTWARE', 'REBOOT', and 'REMOVE APPLIANCE'. The 'REMOVE APPLIANCE' button is highlighted in blue. Below the buttons, there is an 'Information' section with a vertical ellipsis menu icon on the right. The information displayed includes: 'q6wl.demo.arista.com', 'Version: 4.3', a status bar with a clock icon and '17d 23h 57m', a server icon, 'CPU Count: 4', 'Architecture: x86\_64', 'Host Count: 2', 'IP Address: 93.184.216.34', and 'Network Name: ACME Auto Parts'.

## Hosts

This section discusses the following topics:

- [Managing Hosts in the ETM Dashboard](#)
- [Managing Endpoints via Bitdefender GravityZone Integration](#)
- [Managing Endpoints via Webroot Integration](#)
- [Managing Endpoints via Malwarebytes Integration](#)

### 4.1 Managing Hosts in the ETM Dashboard








The Hosts view in the ETM Dashboard lets you view the Internet activity of host devices on your networks. You can view additional details of hosts that [Webroot Endpoint Protection](#) or [Malwarebytes](#) protect.

To view additional host details, you must configure a connection with the Webroot or Malwarebytes Cloud Management system. See [Managing Endpoints Via Malwarebytes Integration](#) and [Managing Endpoints via Webroot Integration](#) for more details.

This information is queried and updated daily.

#### Viewing Hosts

To view activities and other details of host devices, click **Hosts**. The Hosts table in the left pane provides details about each host.

Hosts				
Search here...				
	Hostname ▾ ↓	IP Address	MAC Address Vendor	Operating System
	desktop-td4942m	192.168.0.153		Windows 10 Home
	desktop-smlc4ln	192.168.1.66		Windows 10 Home
	desktop-sjr6ge6	10.0.0.242		Windows 10 Home
	desktop-ro33p2n	192.168.1.42		Windows 10 Home
	DESKTOP-P8UNBGN	104.2.147.129		Windows 10.0 (Build 17763) 64bit
	desktop-0a0ln6f	172.17.0.50		Windows 10 Home
	desktop-0a0ln6f	192.168.100.5		Windows 10 Home

You can hide columns, sort, or filter any details by clicking the three stacked horizontal lines at the right-hand side of each column header and choosing an action.

Hostname	IP Address
desktop-td4942m	
desktop-smlc4ln	
desktop-sjr6ge6	
desktop-ro33p2n	
DESKTOP-P8UNBGN	
desktop-oa0ln6f	
desktop-oa0ln6f	
desktop-oa0ln6f	
desktop-gsabrhp	
desktop-g2pjc9l	
desktop-fvjgea5	

Filter CLEAR

desk

Pin >

Columns >

Toolbar >

Refresh

Export CSV

The available columns for each host include:

- **Endpoint Security Association icon**
- **Hostname**
- **IP address**
- **Mac Address**
- **Mac Address vendor**
- **Appliance**
- **UID**
- **Operating System**
- **Quota and Quota usage**
- **License entitlement**
- **Date creation**
- **Date updated**

Click a specific host to view additional details.

### Summary

By selecting a host, you can view a summary of the host in the **Host Details** panel at the bottom. The summary includes the same information as the details in the host's table.

## Host Details: desktop-td4942m

ANTIVIRUS SCAN

Summary

Endpoint Security

Installed Software

Sessions

Web Events

Applications

### Network Details

Hostname	desktop-td4942m
IP Address	192.168.0.153
MAC Address	8c:c6:81:1f:9e:60
MAC Address Vendor	-
Captive Portal User	-
HTTP User Agent	-
Last Session	-
Domain	-
Appliance	-
Tags	-
License Entitled	-

### System Details

Platform	Windows
Operating System	Windows 10 Home

### Endpoint Security Details

The **Endpoint Security** tab shows details related to the endpoint security software, including the engine version and when it was last seen on the network.

You can click the link at the top of the screen to launch the web console for the corresponding endpoint management system for more details and actions.

### Host Details: desktop-td4942m

**ANTIVIRUS SCAN**

Summary **Endpoint Security** Installed Software Sessions Web Events Applications

**B** [Go to my bitdefender console](#)

#### Last Scan Results

Scan Type	normal	Engine Version	6.6.24.337
Start Time	Mar 5, 2021, 2:53 AM	Last Seen	
Scan Duration	0	First Seen	
Threats	0	Endpoint Id	5f6cf.
Quarantined	0		
Deleted	0		
Total Count	0		

### Installed Software

You can see software installed on the endpoint using the **Installed Software** tab.

Summary Endpoint Security **Installed Software** Sessions Web Events Applications

Search here...

Name	Version	Date Installed
Microsoft Edge	79.0.309.71	Feb 6, 2020, 7:00 AM
Word	1.0	Feb 6, 2020, 7:00 AM
Excel	1.0	Feb 6, 2020, 7:00 AM
PowerPoint	1.0	Feb 6, 2020, 7:00 AM
Outlook	1.0	Feb 6, 2020, 7:00 AM
Microsoft OneDrive	19.222.1110.0006	Feb 6, 2020, 7:00 AM
Mozilla Firefox 72.0.2 (x64 en-US)	72.0.2	Feb 6, 2020, 7:00 AM
Mozilla Maintenance Service	72.0.2	Feb 6, 2020, 7:00 AM
Malwarebytes Endpoint Agent	1.1.2.0	Feb 6, 2020, 7:00 AM

### Sessions

You can click **Sessions** at the bottom of the **Host Details** panel to view all active sessions from that host.

Summary   Endpoint Security   Installed Software <b>Sessions</b> Web Events   Applications					
Search here...					
Timestamp	Server	Server Port	Server Country	Is Entitled	Is Bypassed
Mar 5, 2021, 1:50 PM	184.27.30.29	443	US	true	false
Mar 5, 2021, 1:50 PM	192.168.10.1	53	XU	true	false
Mar 5, 2021, 1:50 PM	192.168.10.1	53	XU	true	false
Mar 5, 2021, 1:50 PM	34.214.159.27	443	US	true	false

The available details for each session include the following:

- **Timestamp**
- **Protocol**
- **Hostname**
- **Client Port**
- **Server**
- **Server Port**
- **Server Country**
- **End Time**
- **License entitlement**
- **Bypass status**
- **Tags**

You can hide columns and sort any details by clicking the three stacked horizontal lines at the right-hand side of each column header and choosing an action.

### Web Events

By clicking **Web Events**, you can view all URLs currently visited by the selected host.

Summary   Endpoint Security   Installed Software   Sessions <b>Web Events</b> Applications			
Search here...			
Timestamp	Hostname	Is Blocked	Is Flagged
Mar 5, 2021, 1:52 PM	untangle	false	false
Mar 5, 2021, 1:52 PM	untangle	false	false
Mar 5, 2021, 1:52 PM	untangle	false	false
Mar 5, 2021, 1:52 PM	untangle	false	false

The available details for each web event include:

- **Timestamp**
- **Hostname**
- **Client Port**
- **Server**

- **Server Port**
- **Domain**
- **Host**
- **URI**
- **Method**
- **Category**
- **Blocked**
- **Flagged**
- **Reason**

You can hide columns and sort any details by clicking the three stacked horizontal lines at the right-hand side of each column header and choosing an action.

Summary   Endpoint Security   Installed Software   Sessions   Web Events   Applications					
Search here...					
Application	Server	Category	Sent	Received	Is Blocked
REDDIT	151.101.1.140	Social Networking	444.854 KB	17.554 MB	false
CNN	151.101.1.67	Web Services	421.66 KB	15.319 MB	false
CNN	151.101.193.67	Web Services	319.51 KB	12.928 MB	false
YOUTUBE	216.58.194.206	Streaming Media	173.516 KB	8.417 MB	false
GOOGLE	172.217.5.109	Web Services	154.865 KB	7.078 MB	false
MICROSOFT	204.79.197.203	Web Services	206.575 KB	5.959 MB	false

The available details for each application connection include:

- **Application** - The detected application is based on the connection characteristics.
- **Server** - The IP address of the remote server.
- **Server Country** - The inferred location of the remote server is based on the IP address.
- **Category** - The application category.
- **Confidence** - A confidence level related to the accuracy of the detection.
- **Details** - Identifiable metadata associated with the network traffic.
- **Sent** - The amount of transferred data during the connection.
- **Received** - The amount of received data during the connection.
- **Total** - The total volume of transferred data during the connection.
- **Is Bypassed** - Was the connection excluded from app management?
- **Is Blocked** - Whether the connection was blocked.
- **Is Flagged** - Was the connection flagged?
- **Tags** - Any tags that may be associated with the connection.

## 4.2 Managing Endpoints via Bitdefender GravityZone Integration

The ETM Dashboard integrates with [Bitdefender GravityZone](#) to extend the host management capabilities in the ETM Dashboard. In the [Hosts](#) screen in the ETM Dashboard, you can see additional information about each host and perform specific actions.

---

## Connecting your GravityZone Account

To connect your GravityZone account, you need the following details:

- **Access URL** - The Access URL defines the region of your account.
- **API Key** - An API Key allows the ETM Dashboard to authenticate to your account to retrieve information about the endpoints you manage.

To obtain an API key and the Access URL from your GravityZone account:

1. Log in to [GravityZone Control Center](#).
2. Go to **My Account**.
3. Under **Control Center API**, locate your **Access URL**.
4. Under the API keys section, click **Add**.
5. Choose **Licensing API** and **Network API** permissions.
6. Click **Save**.

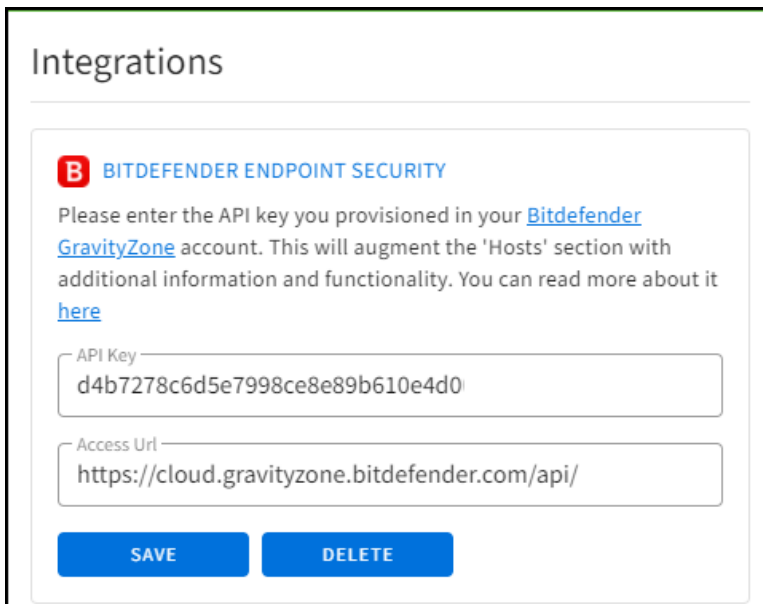
For easy reference, the Access URLs for US and EU regions are provided below:

- US - <https://cloud.gravityzone.bitdefender.com/api/>.
- EU - <https://cloudgz.gravityzone.bitdefender.com/api/>.

## Configuring your API Key in the ETM Dashboard

To select Bitdefender integration, connect your ETM Dashboard account to your GravityZone account.

1. Log in to ETM Dashboard.
2. Go to **My Organization**.
3. Click **Integrations > Bitdefender Endpoint Security**.
4. Enter your GravityZone Access URL.
5. Enter your GravityZone API Key.
6. Click **Save**.



The screenshot shows the 'Integrations' section of the ETM Dashboard. It features a card for 'BITDEFENDER ENDPOINT SECURITY' with a red 'B' logo. The card contains the following text: 'Please enter the API key you provisioned in your [Bitdefender GravityZone](#) account. This will augment the 'Hosts' section with additional information and functionality. You can read more about it [here](#)'. Below the text are two input fields: 'API Key' with the value 'd4b7278c6d5e7998ce8e89b610e4d0' and 'Access Url' with the value 'https://cloud.gravityzone.bitdefender.com/api/'. At the bottom of the card are two buttons: 'SAVE' and 'DELETE'.

After you connect your GravityZone account, you can manage endpoints from the [Hosts](#) screen. Hosts which have Bitdefender endpoint security software installed display the Bitdefender logo.



B	cloudeng5-pc	192.168.20.116	Windows 7 Professional
B	cloudeng6-pc	192.168.20.118	Windows 7 Professional
B	macbook-pro-heather.local...	192.168.1.70	macOS Catalina 10.15.5

## 4.3 Managing Endpoints via Webroot Integration

The ETM Dashboard integrates with [Webroot Endpoint Protection](#) to extend the host management capabilities in the ETM Dashboard. In the [Hosts](#) screen in the ETM Dashboard, you can see additional information about each host and perform specific actions.

### Connecting your Webroot Account

Connect your ETM Dashboard account to your [Webroot account](#) to select Webroot integration. This requires a Parent keycode that you can locate in your Webroot account.

To obtain your Parent keycode:

1. Log in to your Webroot account and select your site.
2. Navigate to **Settings > Account Information**.
3. Copy the **Parent Keycode**.

After you obtain the keycode, you can set up your Webroot account connection in the ETM Dashboard.

To configure your Webroot account connection:

1. Log in to ETM Dashboard.
2. Go to **My Organization > Integrations**.
3. Enter your Webroot account credentials and the Parent keycode.
4. Click **Save**.

**W WEBROOT ENDPOINT SECURITY**

Please enter your credentials for [Webroot SecureAnywhere](#) account. This will augment the 'Hosts' section with additional information and functionality. You can read more about it [here](#).

User Name

Password

Webroot Parent Keycode

**SAVE** **DELETE**

After connecting your account, you can manage your Webroot endpoints in the [Hosts](#) screen.


## 4.4 Managing Endpoints via Malwarebytes Integration

The ETM Dashboard integrates with [Malwarebytes](#) to extend the host management capabilities in the ETM Dashboard. In the [Hosts](#) screen in ETM Dashboard, you can see additional information about each host and perform specific actions.

### Connecting your Malwarebytes Account


To select Malwarebytes integration, you must connect your ETM Dashboard account to your Malwarebytes account.

1. Log in to ETM Dashboard.
2. Go to **My Organization**.
3. Click **Integrations**.
4. Enter your Malwarebytes account information.
5. Click **Save**.

 **MALWAREBYTES ENDPOINT SECURITY**

Please enter your credentials for [Malwarebytes Nebula Console](#) account. This will augment the 'Hosts' section with additional information and functionality.






User Name  
arista-etm@arista.com

Password  
..... 

**SAVE** **DELETE**

### Managing Endpoints

After you connect your Malwarebytes account, you can manage endpoints from the [Hosts](#) screen. Hosts which have Malwarebytes endpoint security software installed display the Malwarebytes logo.

	cloudengWin7-1	192.168.20.110	Microsoft Windows 7 Professional
	cloudengWin7-2	192.168.20.108	Microsoft Windows 7 Professional
	DESKTOP-BK6COGR	192.168.21.150	Microsoft Windows 10 Pro
	cloudeng4-PC	192.168.20.114	Microsoft Windows 7 Professional
	Boulder-VMWare-Win10-Malware...	192.168.2.159	Microsoft Windows 10 Pro

## Events and Alerts

This section discusses the following topics:

- [Managing Tasks in the ETM Dashboard](#)
- [Viewing Events in the ETM Dashboard](#)
- [Managing Alert Rules](#)
- [Creating an Alert Rule from an Event](#)
- [Managing Notification Profiles](#)

### 5.1 Managing Tasks in the ETM Dashboard

Centralized management through the ETM Dashboard allows the admin to push various configuration items to their appliances directly from the ETM Dashboard: backup configs, software-defined networks and VPN connections, application policies, and more. The Tasks feature enables the admin to view those pushes in one listing.

<input type="checkbox"/>	Date Updated	Task	Status	Error Message	Retry Count	Expiration Date	User Email Address
<input type="checkbox"/>	Jan 31, 2023, 10:38 AM	Synchronize WAN Rules	Queued		0	Jan 31, 2023, 10:51 AM	jsmith@arista.com
<input type="checkbox"/>	Jan 31, 2023, 10:38 AM	Synchronize VPN Info...	Completed		1	Jan 31, 2023, 10:50 AM	etm-agent@arista.com

#### Viewing Tasks

This view displays information about pushes initiated from the ETM Dashboard.

Column	Description
Date Updated	The date and time the task was initiated.
Task	A description of the task.
Status	The current state of the task: queued, error, or completed.
Error Message	If an error is encountered, the message will be displayed here.
Retry Count	The number of times the task has automatically retried to complete.
Expiration Date	The time at which ETM Dashboard will stop automatically retrying in the event of failures.
User Email Address	The email address of the ETM Dashboard login that initiated the task.

## Removing Tasks

To remove a task from the list, select it and click the **Remove Task** button.

Any task in "queued" or "error" status will be canceled, preventing attempts to complete the push. Completed tasks are only removed from the listing.

## 5.2 Viewing Events in the ETM Dashboard

You can view event logs in the Alerts section of the ETM Dashboard. The logs include:

- Audits
- Alerts
- Notifications

### Audit History

The Audit History reports ETM Dashboard activities such as logins or appliance configuration changes. This is useful, for example, if you allow other users to manage appliances in your account and you need to audit their activities.

### Alerts Received

The Alerts Received log reports activities from Edge Threat Management appliances connected to your account. For example, when an appliance disconnected or upgraded automatically.

Alerts provide important information that may require immediate attention. Therefore, you can create rules to receive alerts to your email, Slack, or Arista Go app. More details are available in [Managing Alert Rules](#).

	Date/Time	Appliance	Details	Label
<input type="radio"/>	Jan 27, 2023, 7:44 PM	Q6.example.com	Appliance Update: Appliance updated from build 16.6.1...	Testing: Q6
<input type="radio"/>	Jan 27, 2023, 4:39 PM	ec2-52-53-39-108.us-west-1.compute.amazonaws.com	Appliance Update: Appliance updated from build 16.6.1...	Demo: AWS
<input type="radio"/>	Jan 27, 2023, 11:40 AM	dutz6.sjc.aristanetworks.com	Appliance Update: Appliance updated from build 16.6.1...	Demo: z6
<input type="radio"/>	Jan 18, 2023, 7:33 AM	mfw.example.com	Appliance Disconnected [Occurred 1 time(s)]	ME Performance Test
<input type="radio"/>	Jan 10, 2023, 10:55 AM	Q8.example.com	Appliance Disconnected [Occurred 1 time(s)]	Demo: Q8
<input type="radio"/>	Jan 10, 2023, 10:36 AM	Q6.example.com	Appliance Disconnected [Occurred 1 time(s)]	Testing: Q6
<input type="radio"/>	Jan 10, 2023, 9:51 AM	w8-test.example.com	Appliance Disconnected [Occurred 1 time(s)]	Testing: w8
<input type="radio"/>	Jan 10, 2023, 8:10 AM	ec2-52-53-39-108.us-west-1.compute.amazonaws.com	Appliance Update: Appliance updated from build 16.5.2...	Demo: AWS
<input type="radio"/>	Jan 10, 2023, 8:03 AM	ec2-52-53-39-108.us-west-1.compute.amazonaws.com	Appliance Disconnected [Occurred 1 time(s)]	Demo: AWS
<input type="radio"/>	Jan 9, 2023, 12:36 PM	ec2-54-183-150-46.us-west-1.compute.amazonaws.com	Appliance Disconnected [Occurred 1 time(s)]	Testing: ipsec-perftest

## Notification Log

The Notification Log reports when each alert message and via which notification profile. This is useful to confirm whether your account is sending alerts and if they are delivered successfully.

## 5.3 Managing Alert Rules

Your ETM Dashboard account includes several default alert rules to notify you about important events related to your appliances, subscriptions, and account. For example, an Alert Rule can trigger a notification when an appliance in your account goes offline or when an infected computer is discovered on the network.

### Managing Alerts

1. Log in to the ETM Dashboard.
2. Click the **Alerts** tab at the top of the screen.
3. Click **Alert Rules** from the menu on the left pane.

<input type="checkbox"/>	Name	Alert Rule	Notification Profiles	Status	Last Updated
<input type="checkbox"/>	appliance update	Appliance Update: Appliance updated		active	Nov 17, 2020, 10:24 AM
<input type="checkbox"/>	Config sync notification	Appliance Restoration		active	Aug 19, 2020, 3:13 PM
<input type="checkbox"/>	Partner Test Alert	If someone logs in, ping me		active	May 9, 2019, 11:40 AM
<input type="checkbox"/>	All Events	*		disabled	
<input type="checkbox"/>	Appliance Disconnected	Disconnected		active	Sep 21, 2020, 5:27 PM
<input type="checkbox"/>	Account Settings Update	Account Settings Update		disabled	
<input type="checkbox"/>	Subscription Events	Subscription		disabled	
<input type="checkbox"/>	Remote Access Initiated	Remote Access		active	Sep 21, 2020, 5:28 PM
<input type="checkbox"/>	User Logged In	Log In		disabled	
<input type="checkbox"/>	Appliance Management Events	Appliance		disabled	
<input type="checkbox"/>	Purchase Events	Purchase		disabled	

### Enabling Default Rules

All default rules are disabled to prevent excessive email notifications from the ETM Dashboard. To enable a rule:

1. Select a rule and click the **Edit Alert Rule** button.
2. Set the rule status to **Active**.
3. Confirm that your preferred [notification profile](#) is set and click **Update**.

### Edit Alert Rule

Name

Rule

Status

**NOTIFICATION PROFILES**

Select the notification profiles for this alert.

Showing 4 of 4 total
[EXPORT CSV](#)
[REFRESH](#)

<input type="checkbox"/>	Name	Description
<input checked="" type="checkbox"/>	Default Profile	Default notification profile assigned to this account
<input type="checkbox"/>	Critical Alerts	Critical
<input type="checkbox"/>	Test	Demo Profile
<input type="checkbox"/>	Alert Demo	Demo

[CANCEL](#)
[UPDATE](#)

### Adding an Alert Rule

You can add alert rules by [creating an alert rule from an event](#), or you can add an alert rule manually.

To manually add an alert rule:

1. Click **Add Alert Rule**.
2. Enter a **Name** for the rule.
3. Specify the **Rule**. This is the text string the Alert Rule will look for to trigger the Alert. You can view some example text strings under the Events report in the Command Center. Alternatively, entering "\*" (without quotes) will trigger all events.
4. Set the **Status** as **Disabled** or **Active**.
5. Select your preferred [notification profile](#) and click **Create**.

## 5.4 Creating an Alert Rule from an Event

Alert rules are conditions based on events that trigger a notification. You can [manually configure alert rules](#) or create a rule from an event in the **Audit History** or **Alerts Received**.

### Creating a Rule from an Event or Alert

1. Log in to ETM Dashboard.
2. Click the **Alerts** tab at the top of the screen.
3. Click the **Audit History** or **Alerts Received**.
4. Select an event from which you want to make a rule.

Alert Rules

ADD ALERT RULE EDIT ALERT RULE DELETE ALERT RULES

Search here... Showing 16 of 16 total EXPORT CSV REFRESH

<input type="checkbox"/>	Name	Alert Rule	Notification Profiles	Status	Last Updated
<input type="checkbox"/>	appliance update	Appliance Update: Appliance updated		active	Nov 17, 2020, 10:24 AM
<input type="checkbox"/>	Config sync notification	Appliance Restoration		active	Aug 19, 2020, 3:13 PM
<input type="checkbox"/>	Partner Test Alert	If someone logs in, ping me		active	May 9, 2019, 11:40 AM
<input type="checkbox"/>	All Events	*		disabled	
<input type="checkbox"/>	Appliance Disconnected	Disconnected		active	Sep 21, 2020, 5:27 PM
<input type="checkbox"/>	Account Settings Update	Account Settings Update		disabled	
<input type="checkbox"/>	Subscription Events	Subscription		disabled	
<input type="checkbox"/>	Remote Access Initiated	Remote Access		active	Sep 21, 2020, 5:28 PM
<input type="checkbox"/>	User Logged In	Log In		disabled	
<input type="checkbox"/>	Appliance Management Events	Appliance		disabled	
<input type="checkbox"/>	Purchase Events	Purchase		disabled	

5. Click **Add Alert Rule**.
6. The view switches to the Create Alert Rule screen with the **Rule** populated by the event.

Edit Alert Rule

Name: Appliance Disconnected

Rule: Disconnected

Status: Active

NOTIFICATION PROFILES

Select the notification profiles for this alert.

Search here... Showing 4 of 4 total EXPORT CSV REFRESH

<input type="checkbox"/>	Name	Description
<input checked="" type="checkbox"/>	Default Profile	Default notification profile assigned to this account
<input type="checkbox"/>	Critical Alerts	Critical
<input type="checkbox"/>	Test	Demo Profile
<input type="checkbox"/>	Alert Demo	Demo

CANCEL UPDATE

7. Enter a **Name** for the rule.
8. Confirm the Notification profile and click **Create**.

## 5.5 Managing Notification Profiles

The ETM Dashboard [alert rules](#) require a notification profile to send you alerts. The notification profile specifies how you want to receive alerts and how to present the information. You can manage notification profiles in **Alerts > Notification Profiles**.

## Default Notification Profile

Your account in ETM Dashboard has a default notification profile that delivers alerts via email to the email address associated with your account. The default set of alert rules uses this profile to send you alerts.

<input type="checkbox"/>	Name	Description	Action	Last Updated
<input type="checkbox"/>	Untangle GO	Untangle Go notifications	mobile	Jan 20, 2022, 10:17 AM
<input type="checkbox"/>	Default Profile	Default notification profile assigned to this account	email	Oct 22, 2021, 4:18 PM
<input type="checkbox"/>	Critical Alerts	Critical	mobile	Mar 21, 2022, 10:44 AM
<input type="checkbox"/>	Test	Demo Profile	slack	Mar 27, 2018, 7:26 AM
<input type="checkbox"/>	Alert Demo	Demo	slack	Apr 19, 2019, 9:05 AM

If you want to change how you receive alerts, you can edit this profile by selecting the profile and clicking **Edit Notification Profile**.

**EMAIL CONFIGURATION**

To: arista-etm-notifications@arista.com

CC

BCC

You can use the following variables in the field(s) below:

- **%event%** - JSON body of the entire event object including envelope info
- **%event.HTML%** - body of the entire event object including envelope info converted to HTML
- **%eventstring%** - body of the entire event object including envelope info encoded as escaped JSON string
- **%event.message%** - event message string containing summary of the event
- **%event.body%** - JSON event payload excluding envelope info

## Notification Types

ETM Dashboard supports the following delivery services:

Email	Standard email delivery to the email address you specify.
Slack	Delivery via a <a href="#">Slack webhook</a> .
Pagerduty	Delivery via a <a href="#">Pagerduty webhook</a> .
VictorOps	Delivery via a <a href="#">VictorOps webhook</a> .
Webhook	Delivery via a custom <a href="#">webhook</a> .
Arista Go (Mobile)	Delivery via <a href="#">Untangle Go</a> mobile app.



## Adding a Notification Profile

Depending on the alert, you can add notification profiles to receive alerts to other addresses or types of delivery services. After you add a notification profile, you can configure alert rules to select the new profile.

To add a notification profile:

1. Click **Add Notification Profile**.
2. Specify a **name** and **description**.
3. Select an **action** to define how you want to receive the alert.
  - For an **Email** action:
    - a. Specify a **From** address and the **To**, **CC**, and **BCC** addresses separated by commas. Note that only the **From** and **To** addresses are required.
    - b. Enter a Subject and Body. The table above these values provides variables you can use in the message. Refer to the default notification profile as a formatting guide.
  - For a **Slack** action:
    - a. Enter the endpoint URL of your app.
  - For a **Pagerduty** action:
    - a. Enter the **routing key** you designed for ETM Dashboard notifications.
    - b. Select a severity level.
  - For a **VictorOps** action:
    - a. Enter the **Endpoint URL** you designate for ETM Dashboard notifications.
    - b. Select a message type.
  - For a **Webhook** action:
    - a. Enter the Endpoint URL you designate for ETM Dashboard notifications.
    - b. Click **Add Header** and enter a name and value if your custom integration requires custom headers.
    - c. Select an HTTP **Method**.
  - For a **Mobile** action:
    - a. From the list under **Mobile Configuration**, select the Arista Go app in which you would like to receive notifications. You will see a list of all available devices if you have connected Arista Go from multiple mobile devices.

MOBILE CONFIGURATION

Please select mobile devices you want to receive the notifications.

Showing 4 of 4 total
EXPORT CSV REFRESH

<input type="checkbox"/>	Device Type	Last Login	Date Paired
<input type="checkbox"/>	iPad6,7-iOS-14.4.2		Apr 14, 2021, 4:36 PM
<input type="checkbox"/>	iPhone12,1-iOS-14.4.2		Apr 20, 2021, 8:26 AM
<input type="checkbox"/>	iPhone9,1-iOS-14.4.2		Apr 28, 2021, 4:40 PM
<input type="checkbox"/>	OnePlus-ONEPLUS A5000-7.1.1		Oct 11, 2021, 8:28 AM

4. Click **Create**.

## Policies

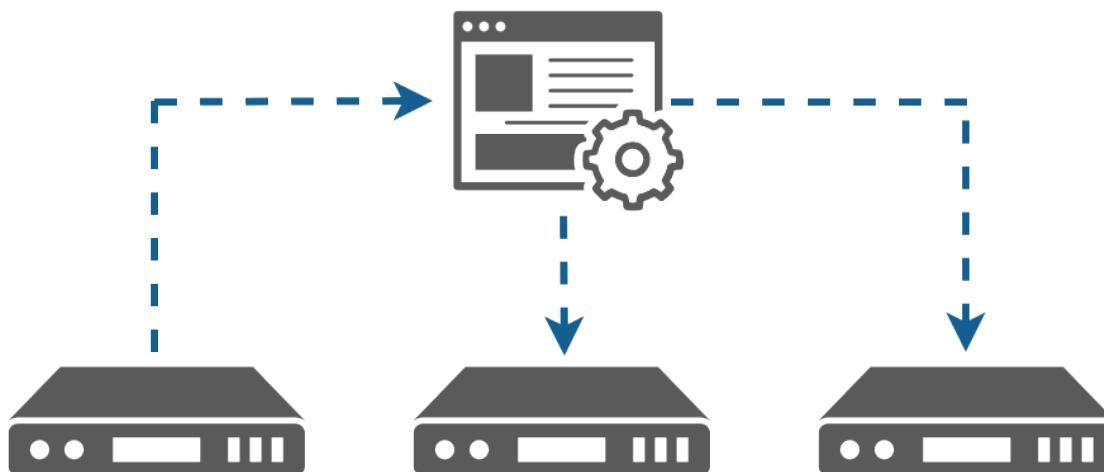
This section discusses the following topics:

- [Assigning or Synchronizing a Common Configuration to the NG Firewall Appliances.](#)

The ETM Dashboard Configuration Templates enable you to replicate a configuration across multiple NG Firewall appliances. These are useful, for example, if you want a standby failover system or manage multiple deployments that select an identical configuration. Configuration replication works in combination with [Configuration Backup](#).

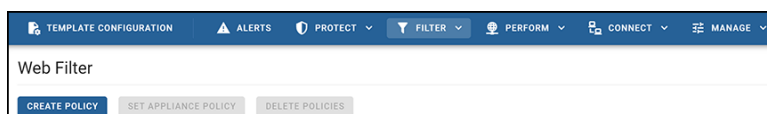
### 6.1 Assigning or Synchronizing a Common Configuration to the NG Firewall Appliances

The ETM Dashboard Configuration Templates enable you to replicate a configuration across multiple NG Firewall appliances. This is useful, for example, if you want to have a standby failover system or manage multiple deployments that use an identical configuration. Configuration replication works in combination with [Configuration Backup](#).



NG Firewall configuration replication can include a complete configuration or specific sections. You can manage both options in the **Appliances > NGFW > Policies** area of the ETM Dashboard.

- To push the complete configuration, select **Templates**. Note that the network configuration is excluded from the template.
- To push specific types of configuration, such as Firewall rules or Captive Portal settings, use the application grouping options at the top of the **Policies** menu.



## Prerequisites

- Appliances must meet the requirements for [managing appliances in the ETM Dashboard](#).
- Configuration templates are based on backups. Therefore, you must install and enable [Configuration Backup](#).
- Each NG Firewall appliance must be running version **13.2** and earlier.



**Note:** If you select Policy Manager to create custom policies, you must create the same policy names on each appliance. Otherwise, only the default policy synchronizes to each appliance.

## Creating Templates

To create a template:

1. Navigate to the **Appliances > NGFW > > Policies** tab in the ETM Dashboard.
2. In the menu bar at the top of the table, click **Template Configuration**.
3. Click **Add Template** to open the template configuration wizard.
4. Choose an appliance you want to use as the configuration master and click **Next**.
5. Choose a recent backup and click **Next**.
6. Choose appliances to sync from the master.

Select the Template appliance

Step 1 of 3

Select the Arista ETM appliance that you would like to use as the master appliance. Only licensed appliances

	Status	License	Appliance	Label
<input type="radio"/>	<span style="color: green;">●</span>	<span style="color: green;">🔑</span>	ec2-3-136-163-85.us-east-2.compute.amazon...	aws
<input checked="" type="radio"/>	<span style="color: green;">●</span>	<span style="color: green;">🔑</span>	ngfw-test.arista.com	Arista Test Device
<input type="radio"/>	<span style="color: green;">●</span>	<span style="color: green;">🔑</span>	dutz12.sjc.aristanetworks.com	z12demo

7. If you want the appliances to synchronize when you change to the master, enable **Keep in Sync** and set a schedule.

**Keep in Sync**

If this setting is enabled, target appliances will be automatically synced with the master appliance whenever

Sync frequency

Daily ▼

Time of Day (UTC)

02:30 AM ▼

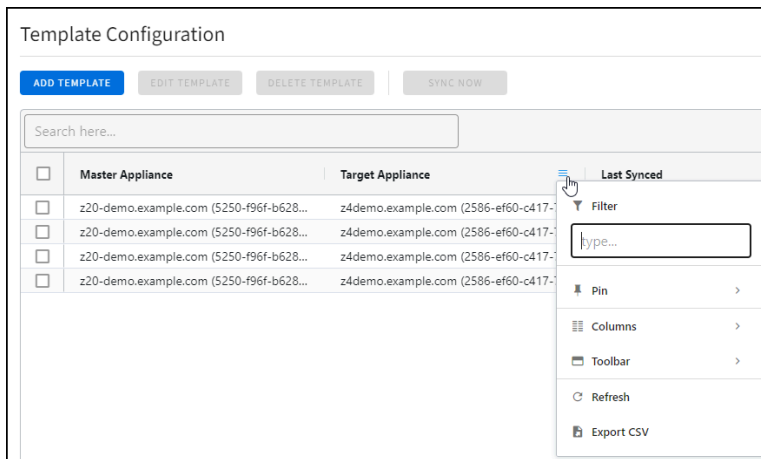
BACK
NEXT

8. Click **Next**.
9. In the final step, click **Create Template** to apply the configuration template.

## Managing Templates

### Sorting and Filters

The **Template Configuration** grid displays your templates and relevant details in sortable and filterable columns. You can manage these options and show or hide columns by clicking the three horizontal lines to the right of any column header to access the menu.



## Sync options

**Sync Now** - You can manually initiate a configuration sync by selecting one or more templates and clicking **Sync Now**. You can also configure appliances to synchronize automatically.

**Keep in Sync**- You can set a sync schedule as Immediate, Daily, or Weekly. You can configure the **Keep in Sync** option when creating a new configuration template or by selecting the template and clicking **Manage Template** afterward.

### Notes regarding synchronization:

- If a template is configured for immediate synchronization and the target appliance is offline, the target appliance retries every 12 hours for up to 7 days.
- You can check the status of the synchronized appliances in the [Event Log](#). Audit History.

## Target Appliances

**Target Appliances** inherit the configuration of the **Master Appliance** based on the sync options. You configure target appliances when creating a new configuration template or afterward by selecting the template and clicking **Manage Template**.



**Note:** Each NG Firewall appliance must be on the same version. The configuration does not sync unless the version of the appliance matches the version of the master appliance.

## Deleting Templates

To delete one or more templates, select the template and click **Delete Templates**.

## Reports

This section discusses the following topic:

- [The ETM Dashboard Reports](#)

The ETM Dashboard lets you view consolidated reports from all networks managed through your account. The reporting data includes bandwidth usage and web activities.

### 7.1 The ETM Dashboard Reports

The ETM Dashboard lets you view consolidated reports from all networks managed through your account. The reporting data includes bandwidth usage and web activities.

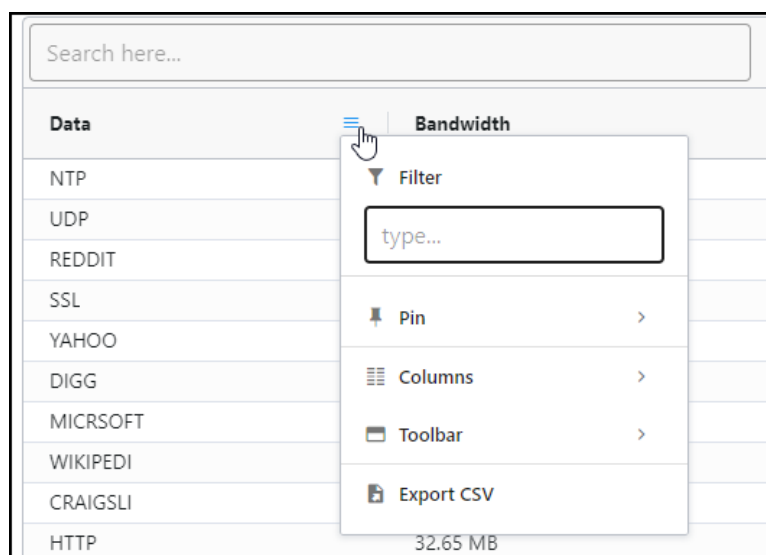
#### Viewing Reports

To view reports:

1. Log in to ETM Dashboard.
2. Navigate to the **Reports** tab.
3. Select the report you want to view.

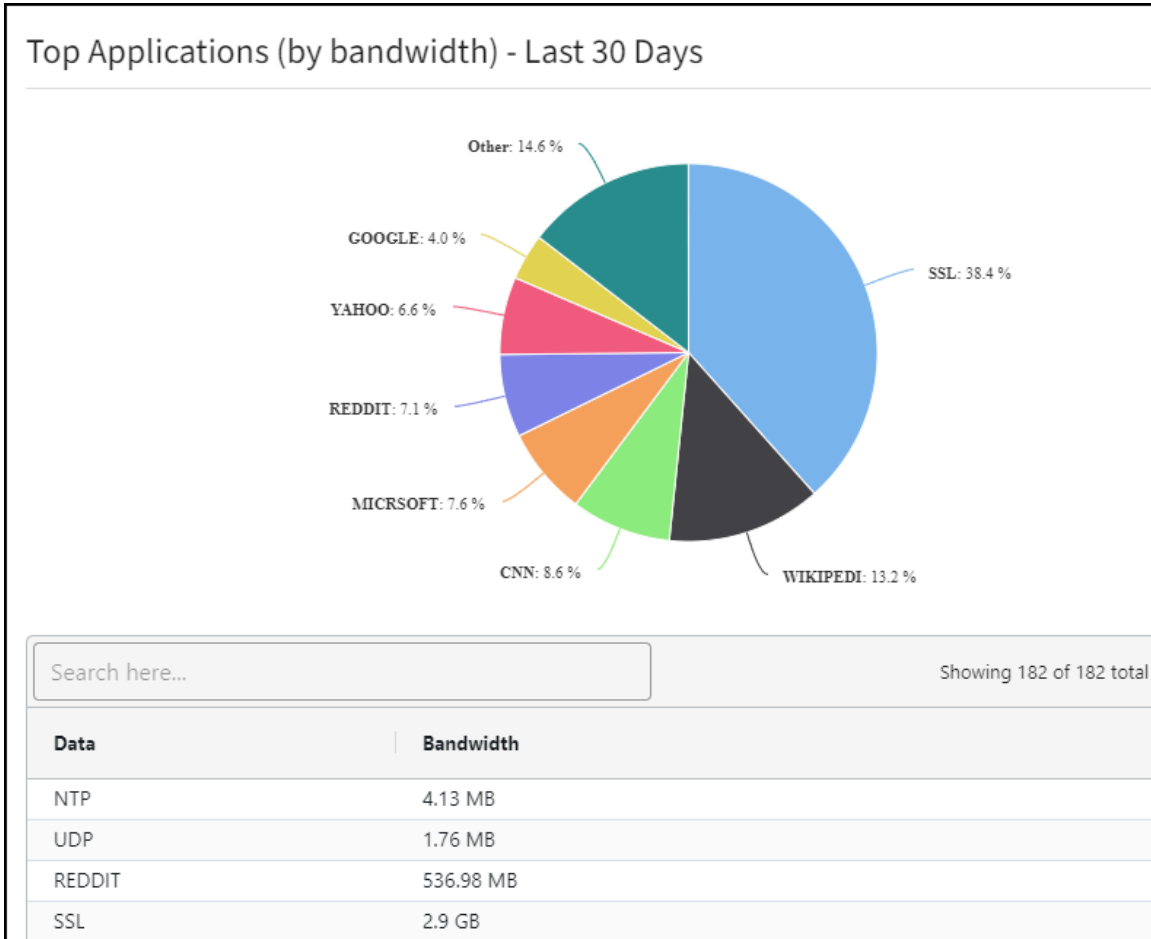
#### Filtering and sorting data

You can refine the data in the grids below the charts. For example, if you want to view reporting data only from a specific appliance. To sort columns or filter the data, click the three horizontal lines at the right-hand side of the header to expose the menu.

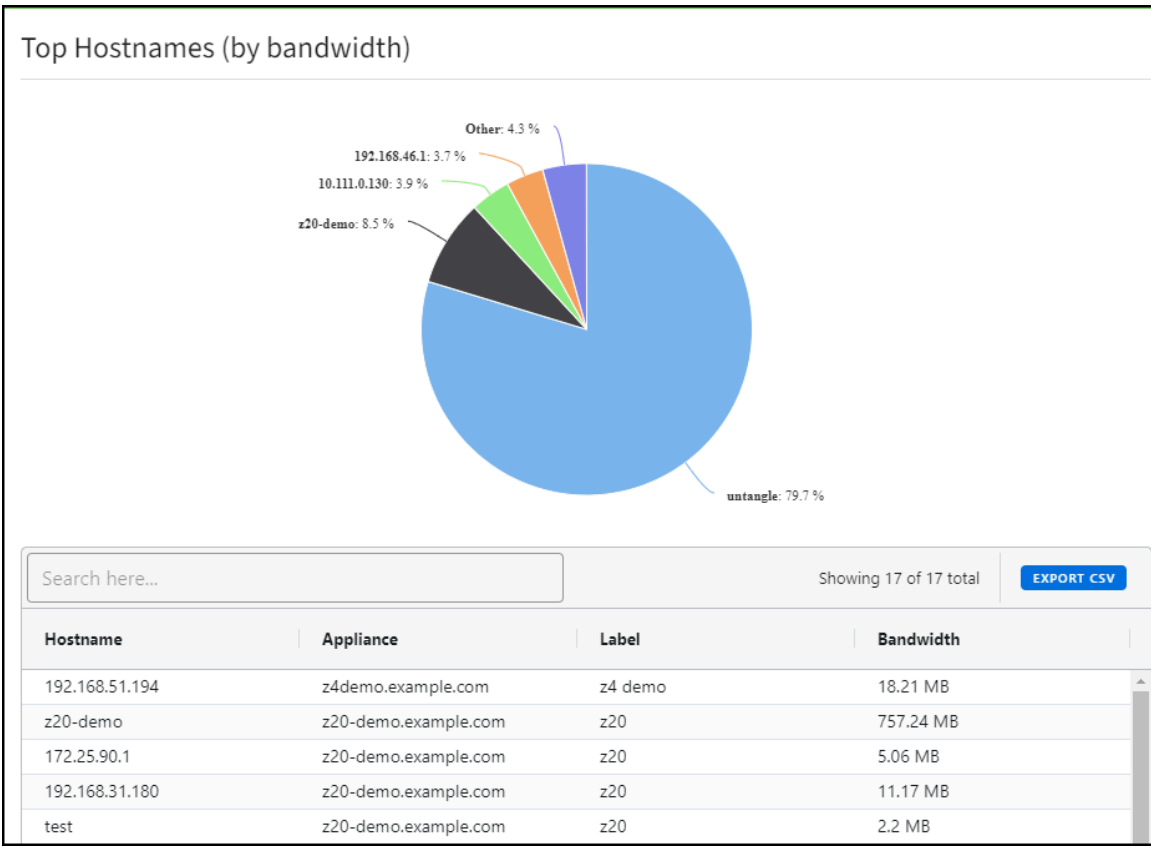


## Report Types

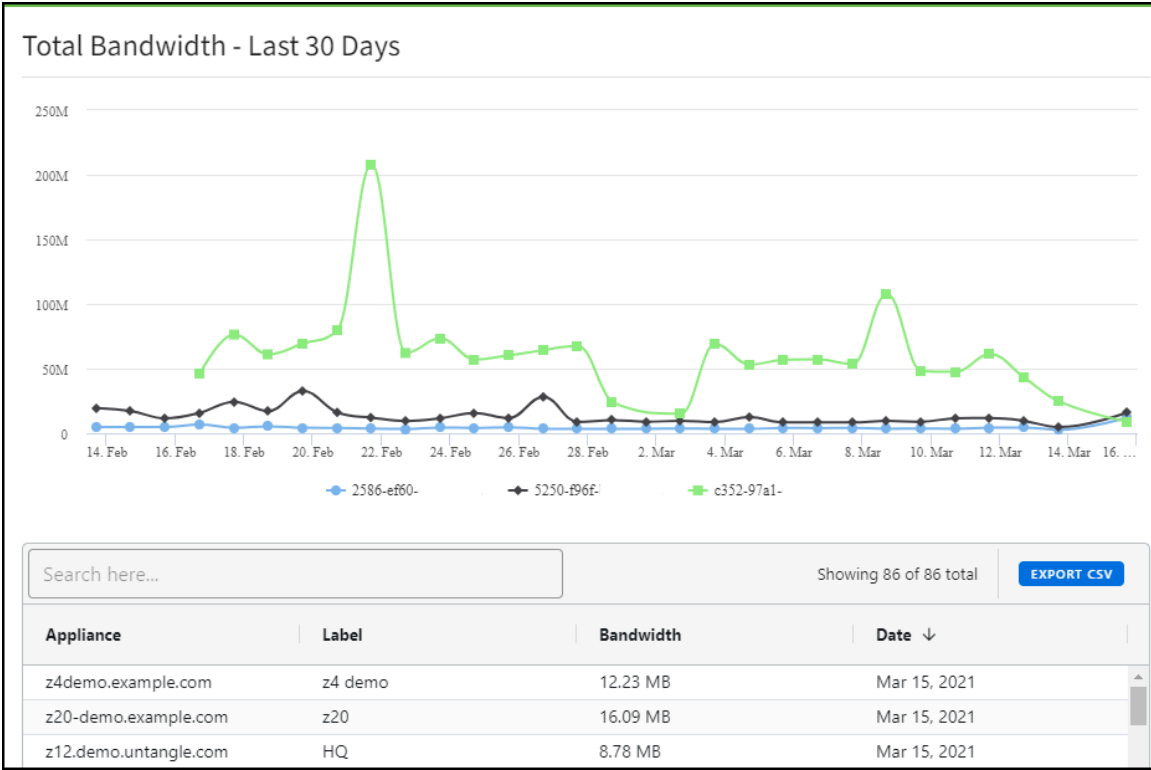
**Bandwidth Control - Top Application (by bandwidth)** provides you with the applications that are using the most bandwidth.



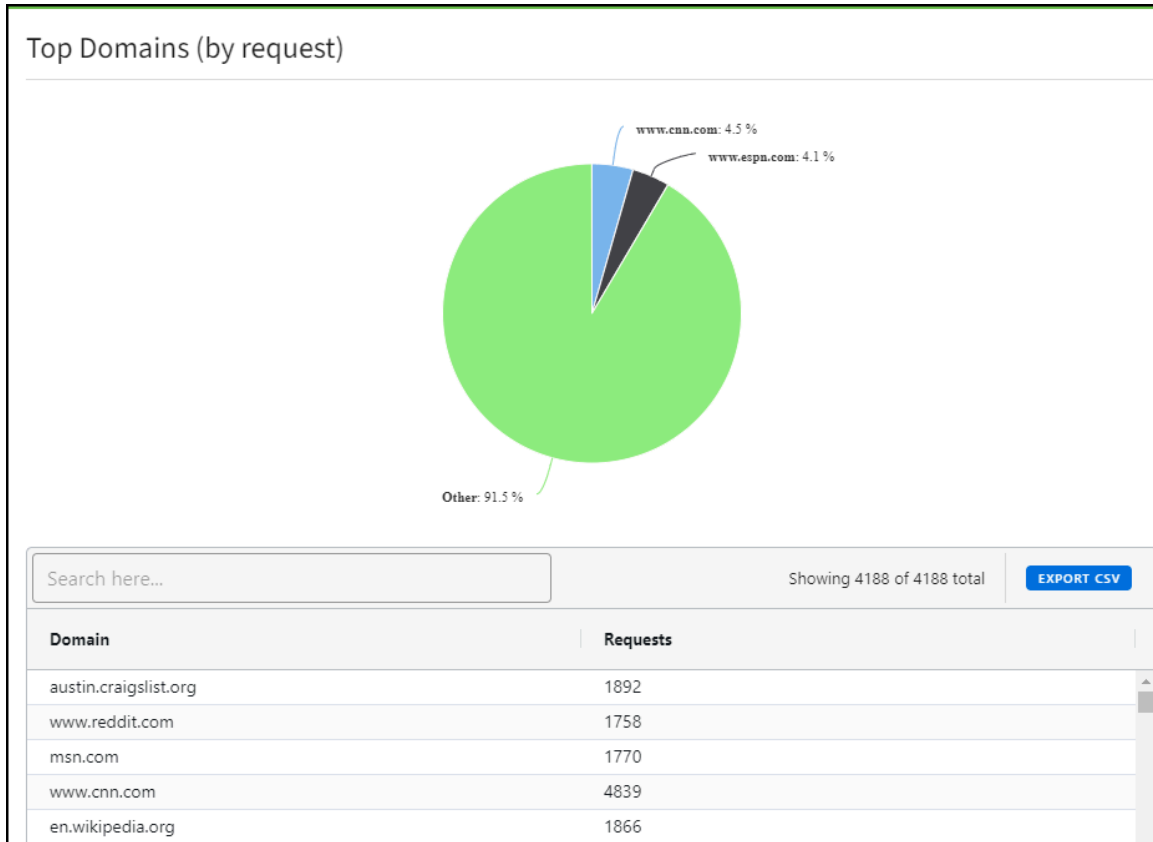
**Hosts - Top Hostnames (by bandwidth)** This report displays information about hosts that use the most bandwidth.



**Network - Total Bandwidth - Last 30 Days** provides a glance at the total bandwidth passing through this appliance over the last 30 days.



**Web Filter - Top Domains (by request)** provides the top requested domains, blocked categories, sites, and hostnames.





## Licensing and Subscriptions

This section discusses the following topics:

- [How to Assign a Subscription to an Appliance](#)
- [Upgrading an Appliance Subscription](#)
- [How to Remove/Unassign a Subscription from an Appliance](#)
- [How to Share a Subscription to a Different Account](#)
- [How to Transfer a Subscription to Another Appliance](#)
- [How to Renew a Subscription](#)
- [Redeeming a Voucher](#)
- [How to Create a Subscription Renewal Quote](#)
- [Enabling or Disabling Auto-Renewal](#)

### 8.1 How to Assign a Subscription to an Appliance

Edge Threat Management appliances require a license for full functionality.

#### Prerequisites

- You must have an ETM Dashboard account.
- Your appliance must be registered to your ETM Dashboard account. See [How to register an Edge Threat Management appliance in the ETM Dashboard](#).

#### Assigning a Subscription

You can assign a subscription from the appliance dashboard or the subscriptions area.

To assign a subscription from the appliance dashboard:

1. Login to ETM Dashboard.
2. Click **Appliances**.
3. Select the appliance you want to license from the list on the left.
4. Locate the Appliance Licenses widget and click **Add license**.
5. Select the subscription to assign to this appliance.
6. Click **Add**.

Number	Product Name	Band/Tier	Status	Label	Term	Auto Renew
<input checked="" type="radio"/> A-S00127252	NG Firewall Complete	100	Active	Label Not Set	1 Year	Will Renew

To assign a subscription from the subscriptions area:


1. Login to ETM Dashboard.
2. Click **My Organization** in the menu on the left.
3. Select **Subscriptions**.
4. Select the subscription you want to assign.
5. Select the **manage** button.
6. Choose Assign subscription to an appliance.
7. Select an appliance and click **Save**.

Manage Subscription A-S00092600

Assign subscription to an appliance  
 Unassign subscription from c352-97a1-6c69-5342  
 Allow another user to view and assign/unassign this subscription.

Quick Filter REFRESH EXPORT CSV

	Appliance	Tag	Version	Last Seen	
<input checked="" type="checkbox"/>	ec2-3-136-163-85.us-east-2.compute...	Tag not assigned	16.1.1	Never	
<input type="checkbox"/>	radius.example.com	Tag not assigned	16.2.0	Never	
<input type="checkbox"/>	z20-demo.example.com	z20	16.2.2	Never	

 **WARNING:** Subscription will be unassigned from c352-97a1-6c69-5342.

CANCEL SAVE

## 8.2 Upgrading an Appliance Subscription

You can upgrade your software subscriptions from the ETM Dashboard. For example, if you need to add users or convert to an NG Complete subscription. Before upgrading your subscription, make sure your billing information is accurate. See [How to Update Billing / Shipping Address for details](#).

### To upgrade your subscriptions

1. Login to ETM Dashboard.
2. Click **My Organization** in the menu on the left.
3. Select the **Subscriptions**.
4. Check the box for each subscription(s) to upgrade.



**Note:** you'll only be able to update one Complete package subscription at a time.

5. Click the **Upgrade** button.
6. Fill in the relevant information to upgrade your subscription and click **Review**.

### Subscription Upgrade ×

**CURRENT PRODUCT**

Current Product: NG Firewall Complete  
Band/Tier: 12  
Renewal Period: 1 Year

**SELECT NEW PRODUCT**

Upgrade Product  
NG Firewall - Complete

Licensed Devices  
Up To 25

Renewal Period  
1 Year

Purchase Order Number

Coupons

[CANCEL](#) [REVIEW](#)

7. Review the upgrade charges and payment method and click **Upgrade**.

Subscription Upgrade
✕

**CURRENT PRODUCT**

Current Product: NG Firewall Complete  
 Band/Tier: 12  
 Renewal Period: 1 Year

**NEW PRODUCT**

New Product: NG Firewall Complete  
 Band/Tier: Up To 25  
 Renewal Period: 1 Year

New Subscription Charge	\$540.00
Discount	-\$135.00
<b>Total Cost</b>	<b>\$405.00</b>

Subscription term: Jan 10, 2023 - Jan 10, 2024

i Your current subscription(s) will be cancelled and a new one will be created. Are you sure you want to proceed with the upgrade?

BACK
UPGRADE

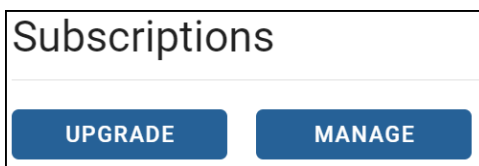
8. You'll receive a message that the subscription has been successfully upgraded.

### 8.3 How to Remove/Unassign a Subscription from an Appliance

This section walks you through removing a subscription from an Edge Threat Management appliance.

#### Removing a Subscription

1. Login to ETM Dashboard.
2. Click **My Organization** in the menu on the left.
3. Click **Subscriptions**.
4. Check the box for each subscription(s) to be removed/unassigned.
5. Click the **Manage** button.



6. A pop-up will appear giving you three options - select the option to "Unassign subscription from [UID#]" button and click **OK**.

Now that you have unassigned the subscription, if you would like to assign it to another UID, here is how:

[How to assign/transfer a subscription](#)

[How to allow users to manage subscriptions](#)

## 8.4 How to Share a Subscription to a Different Account

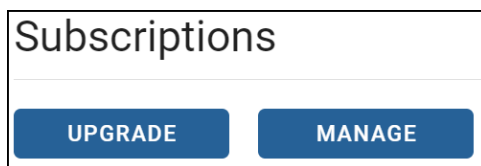
You can share a subscription to a different ETM Dashboard user account. For example, user Bob purchases a subscription and needs to assign it to an appliance that belongs to Sally's account. In this case, Bob owns the subscription, and he can share it with Sally so that she can assign it to an appliance that belongs to her account.



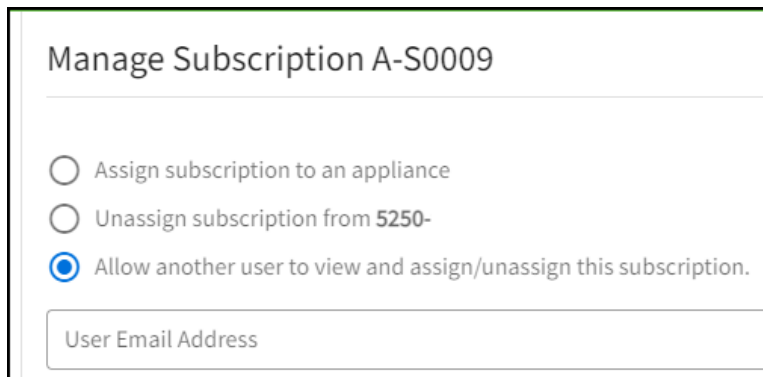
**Note:** When sharing a subscription, the delegated user does not see the subscription price and cannot upgrade or renew the subscription. The shared subscription remains in the owner's account, and all billing aspects of the subscription are managed exclusively by the owner.

### To Share a Subscription

1. Login to ETM Dashboard.
2. Click **My Organization** in the menu on the left.
3. Click **Subscriptions**.
4. Select the subscription you want to share.
5. Click the **Manage** button.



6. Choose **Allow another user to view and assign/unassign this subscription** and enter the email address of another account.



7. Click **Save**.
8. The other user receives an email confirming access to the subscription. The other user can [assign the subscription](#) to one of their appliances at that point.

## 8.5 How to Transfer a Subscription to Another Appliance

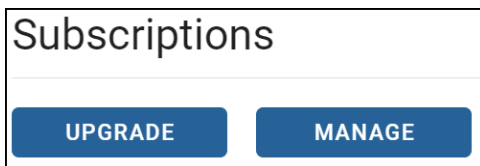
If you need to move a subscription to another appliance, you can do so at any time in the Subscriptions area of your account.

---

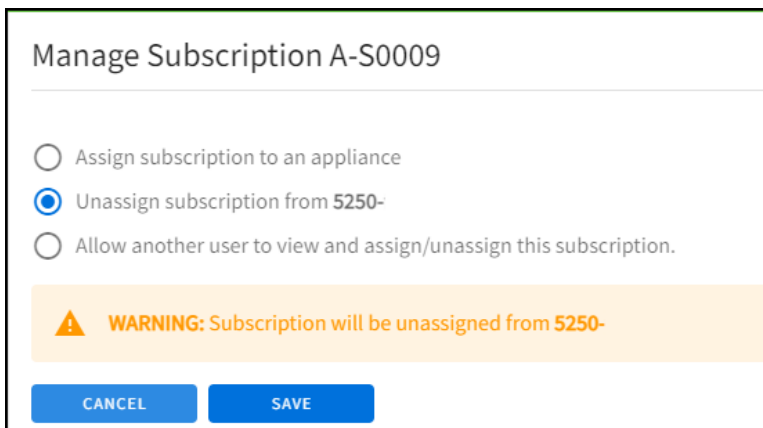
## Reassigning a Subscription

First, you must unassign a license from the current appliance to reassign a license to a different one. To unassign a subscription:

1. Login to the ETM Dashboard.
2. Click **My Organization** in the menu on the left.
3. Click **Subscriptions**.
4. Select the subscription you want to unassign.
5. Click the **Manage** button.



6. Choose the option "Unassign subscription from ...".
7. Click **Save**.



After unassigning the subscription, you can [assign it to an appliance](#) in your account or an appliance managed in a different ETM Dashboard account.

To assign a subscription to another account, see [How to share a subscription to another account](#).

## 8.6 How to Renew a Subscription

You can renew a subscription using your ETM Dashboard account without making a new purchase or contacting the Sales team.

### Renewing a Subscription

1. Login to the ETM Dashboard.
2. Click **My Organization** in the menu on the left.
3. Click **Subscriptions**.
4. Select the checkboxes for the subscriptions that are to be renewed.
5. Click **Renew Now**.

Subscriptions			
<input type="button" value="UPGRADE"/>		<input type="button" value="MANAGE"/>	
<input type="button" value="RENEW NOW"/>		<input type="button" value="RENEWAL QUOTE"/>	
<input type="text" value="Search here..."/>			
<input type="checkbox"/>	Number	Product Name	Band/Tier
<input type="checkbox"/>	A-S00092600	NG Firewall Complete	12
<input checked="" type="checkbox"/>	A-S00092601	NG Firewall Complete	12
<input type="checkbox"/>	A-S00092602	NG Firewall Complete	12

- A dialog box will appear showing your current balance, if any.
- Upon clicking the "Renew" button, the subscription will be renewed for an additional period (depending on the subscription, this could be monthly, yearly, or multi-year).

#### Notes regarding subscription renewal:

- Only subscriptions within 30 days of expiration are eligible for renewal. If the subscription renewal is further away and you want to renew it, we recommend enabling **auto-renewal** on the subscription. [CLICK HERE](#) to learn how to toggle Auto Renewal.
- After a subscription reaches the expired state, it is automatically unassigned from the appliance.
- An expired subscription can be renewed for up to 14 days. After 14 days, a new subscription must be purchased.
- The anniversary date of a subscription remains the same whether it is renewed before or after the expiration date.

#### Related topics:

[How to assign a subscription to a server.](#)

## 8.7 Redeeming a Voucher

A voucher is a transferable license that becomes an active subscription after you redeem the code and assign it to an instance of NG Firewall. A voucher is a "gift certificate" for a specific NG Firewall software package. The voucher key is a unique alphanumeric code that you redeem in the ETM Dashboard to create the subscription.

A voucher provides you a way to delay the activation of your subscription. If you are a Partner, purchasing a set of vouchers using one transaction and redeeming them as you deploy NG Firewalls is efficient. If you do not intend to install the NG Firewall yourself, you can simplify the installation process by sending the voucher to your customer.



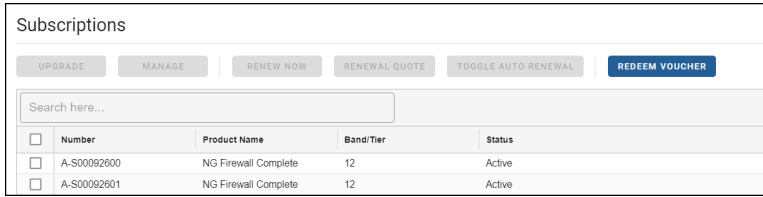
**Important:** If you do not redeem the voucher for a subscription within 30 days, it will convert automatically to a subscription.

#### Redeeming a Voucher

To redeem a voucher:

- Log in to the Edge Threat Management Dashboard at <https://launchpad.edge.arista.com/>
- If you do not have an account, click **Create an account** on the login page.
- After logging in, click **My Organization** from the menu on the left-hand side of the page.
- Click **Subscriptions**.

5. Click **Redeem Voucher**.



6. Enter your voucher code and click **Redeem**.

7. Review your list of subscriptions and confirm that a new subscription appears.

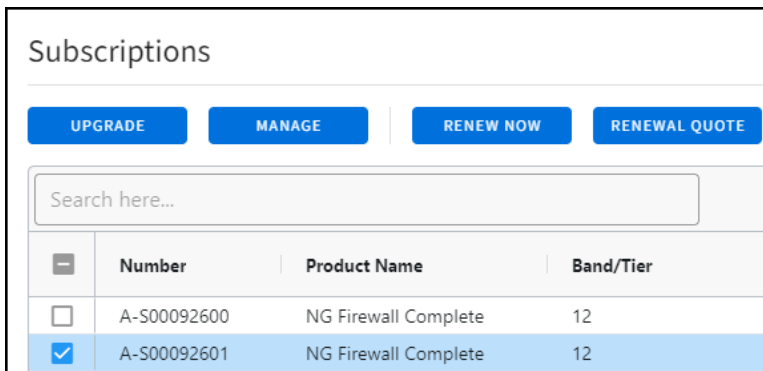
After you redeem your voucher, you can [assign your new subscription to an appliance](#).

## 8.8 How to Create a Subscription Renewal Quote

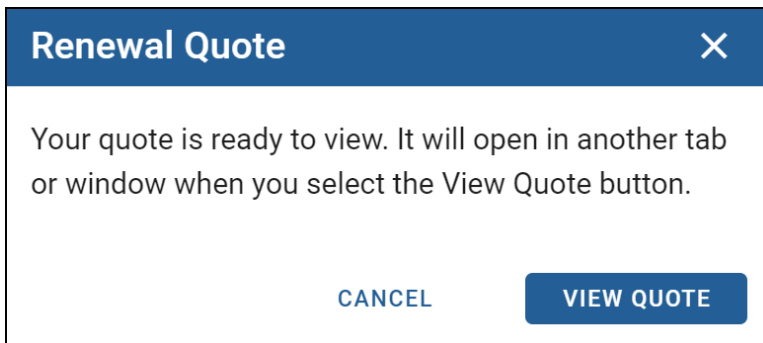
You can use the ETM Dashboard to generate a renewal quote for a subscription without contacting the Edge Threat Management Sales team directly.

### Generating your Quote

1. Login to ETM Dashboard.
2. Click **My Organization**.
3. Select **Subscriptions**.
4. Select the checkbox on the subscription where a renewal quote is needed.



5. Click the **Renewal Quote** button. You'll receive a message that the quote is ready. Click the **View Quote** button.



6. The quote will open in a new tab. Select that tab to view the quote.



- You can save or print the quote using the browser's print or save feature. To print using the Chrome browser, Select **File > Print**.

[How to assign a subscription to a server.](#)

## 8.9 Enabling or Disabling Auto-Renewal

This process lets you turn on or off the auto-renew feature on an appliance subscription.

### Toggle Auto-Renew State

- Login to ETM Dashboard.
- Click **My Organization** from the menu on the left-hand side of the screen.
- Select **Subscriptions**.
- To change the auto-renew setting for a subscription, select the checkbox for the subscription and click the **Toggle Auto Renewal** button. Depending on the current state of that subscription, auto-renewal will be enabled or disabled.

	Number	Product Name	Band/Tier	Status	Term
<input checked="" type="checkbox"/>	A-S00092600	NG Firewall Complete	12	Active	1 Year
<input type="checkbox"/>	A-S00092601	NG Firewall Complete	12	Active	1 Year

### Other Resources Relating to Subscription Management

- [How to upgrade a subscription.](#)
- [How to manually renew a subscription.](#)
- [How to assign a subscription.](#)

---

## Account and Organization Management

---

This section discusses the following topics:

- [Configuring SAML, OAuth2, or OpenID Login in the ETM Dashboard](#)
- [ETM Dashboard Organization](#)
- [Enabling or Disabling Automatic Sign-on to Appliances](#)
- [Enabling and Disabling Dashboard Widgets on the ETM Dashboard](#)
- [Switching Themes on the ETM Dashboard](#)
- [Two-Factor Authentication on the ETM Dashboard](#)
- [General Data Protection Regulation \(GDPR\)](#)
- [Request a Copy of your Data](#)
- [Deleting an ETM Dashboard Account](#)

### 9.1 Configuring SAML, OAuth2, or OpenID Login in the ETM Dashboard

Single Sign-On (SSO) provided by an Identity Provider (IdP) is an increasingly common, security-focused practice.

Single Sign-On (SSO) is common in Zero-Trust Network Access security policies because it enables the admin to:

- Centralize control of user login policies and credentials.
- Consolidate user accounts that require access to multiple cloud-based services.
- Enforce stringent password policies and multi-factor authentication
- Simplify user login to reduce password fatigue.
- Reduce the threat of data breaches by moving authentication off-site.

The ETM Dashboard supports login using SAML, OAuth2, or OpenID federated accounts. To select these options, you must have an existing account with an Identity Provider (or IdP) such as Okta, Duo, or OneLogin.

Single Sign-on is configured in **My Organization > SSO**.

#### Who is Affected?

- The account owner.
- Anyone who has been invited to manage the account as a user.

#### Before you Begin

The **Organization Name** attribute identifies and initiates this specific SAML or OAuth2 login process; you can think of it as a username. It can include letters, numbers, or punctuation. You can use capital letters when configuring the Organization Name, but it is not case-sensitive at the login point. For example, you could enter "Example Company" as your organization and still log in with "example company."

Your Organization Name must be unique. You will receive an error message if a given name is not available for use.

This Organization Name is specific to this SSO option and does not need to match the name associated with your ETM Dashboard organization.

## Configuring SAML Login

Set the **Organization Login Type** to "SAML."

### Provider attributes

The attributes under the **Configuration** heading inform the ETM Dashboard about connecting to and authenticating against your SAML provider.

The *Login URL*, *Entity Id*, and *Encryption Certificate* fields are required. The *Signing Certificate* field is only used when the provider gives you a different certificate.

### Testing SAML login

The **Test SAML** button will appear after you have saved your settings. This will validate that the ETM Dashboard can connect to your provider.

### Downloading SP Metadata

The **Download SP Metadata** button will appear after you have saved your settings. The resulting data is uploaded to your Identity Provider to authorize ETM Dashboard to use their SSO login.

## Removing SAML

Click the **Delete** button to remove this configuration. This option can change the SAML connection or switch to a different provider.

To disable this authentication method, set the **Organization Login Type** to "Disabled" instead.

**ORGANIZATION SSO LOGIN**

Organization Name

Organization Login Type  
SAML ▼

**CONFIGURATION**

Login URL (HTTP-REDIRECT)

Entity Id

Encryption Certificate

Signing Certificate (if different from the encryption certificate)

i You must save the SAML settings before running a test or downloading SP metadata

## Configuring OAuth2 / OpenID Login

Set the **Organization Login Type** to "OAuth2 / OpenID".

### Provider Attributes

The attributes under the **Configuration** heading inform the ETM Dashboard about connecting to and authenticating against your OAuth2 or OpenID provider.

All fields are required.

## Sign-in Redirect URI's

If your OAuth2 provider requires sign-in redirects, they can be found following the configuration fields. Those URIs are also provided here for your convenience:

1. <https://launchpad.edge.arista.com/account/sso>
2. <https://launchpad.edge.arista.com/oauth2/signon/fc05796533944dff9e19b3c76621cda1>

## Testing OAuth2 or Open ID

The **Test OAuth2** button becomes available after you save your OAuth2 / OpenID settings. This will validate that the ETM Dashboard can connect to your provider.

## Removing OAuth2 / OpenID

Click the **Delete** button to remove this configuration. You can use this option to change to the OAuth2 / OpenID connection or switch to a different provider.

To disable this authentication method, set the **Organization Login Type** to "Disabled" instead.


**ORGANIZATION SSO LOGIN**

Organization Name

Organization Login Type  
OAuth2 / OpenID ▼

**CONFIGURATION**

Client Id

Client Secret\*  

Authorization Endpoint URL

Token Endpoint URL

User Info Endpoint URL

Client Authentication Method ▼

**i** Your OAuth2 provider may require sign-in redirect URIs for the application. The following URIs will need to be allowed:  
<https://launchpad.edge.arista.com/account/sso>  
<https://launchpad.edge.arista.com/oauth2/signon/fc05796533944dff9e19b3c76621cda1>

**i** You must save the OAuth2 settings before running a test.

**SAVE OAUTH2** **DELETE** **TEST OAUTH2 SETTINGS**

## Logging into the ETM Dashboard using Identity Provider SSO

1. Go to the ETM Dashboard login page at <https://launchpad.edge.arista.com>.
2. Enter your Organization Name.
3. Click **Continue**.
4. You are redirected to your IdP's login page to authenticate.
5. You are redirected to your ETM Dashboard account when your login is complete.

## 9.2 ETM Dashboard Organization

Your ETM Dashboard account may be invited to other ETM Dashboard accounts and permitted to manage Edge Threat Management appliances or subscriptions owned by the inviting account. This additional account access is called an *Organization*.

## 9.3 Enabling or Disabling Automatic Sign-on to Appliances

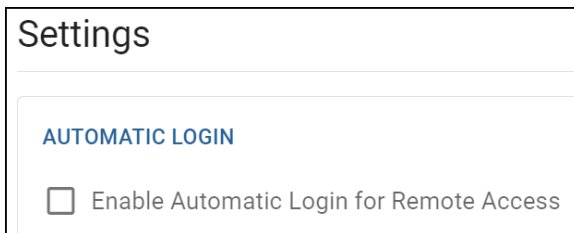
The ETM Dashboard enables you to remotely connect to the administration GUI of your NG Firewall and Micro Edge deployments. This remote connection uses a secure proxy that does not require exposing any ports on your firewall. By default, this proxy connection authenticates you automatically, so you do not need to provide credentials to access the web administration.

### Disabling Automatic Sign-On for Remote Access

Sometimes, you may prefer to authenticate using local firewall user database credentials.

To enforce authentication using the local firewall administration account:

1. Log in to ETM Dashboard.
2. Go to **My Organization**.
3. Click **Settings**.
4. Uncheck **Enable Automatic Login For Remote Access**. Click **Save** to apply the change.



## 9.4 Enabling and Disabling Dashboard Widgets on the ETM Dashboard

The ETM Dashboard gives you a high-level overview of your managed networks and appliances. This information is presented through a variety of small windows called Widgets. Based on your preference, you can modify the default set of Widgets you see on the main Dashboard and Appliances dashboard.



**Note:** Your Dashboard Widget layout is unique to each organization you belong to. This means you see the complete set of default Widgets when switching to another organization. Repeat the steps below for each organization based on your preference.

### Managing Dashboard Widgets

To turn Widgets on or off:

1. Go to **My Account**.
2. Click **Preferences**.
3. In the **Dashboard Widgets** section, select the Widgets you want to see on the Dashboard.
4. Click **Save**.

Preferences

---

**CHANGE PASSWORD**

New Password\*

Confirm New Password\*

**SAVE**

---

**DASHBOARD WIDGETS**

You can select the widgets you want to be displayed. Use drag & drop to specify the order you want them to be shown.

- Appliances Map
- Appliances
- Alert History
- Recent Hosts
- Audit History
- Threat History
- Total Bandwidth
- Top Applications
- Top Domains

**RESET TO DEFAULTS**

---

**APPLIANCE WIDGETS**

You can select the widgets you want to be displayed. Use drag & drop to specify the order you want them to be shown.

- Appliance Model
- Location
- Link Information

## 9.5 Switching Themes on the ETM Dashboard

The ETM Dashboard supports different themes you can select based on your preference. A theme defines the color scheme of the ETM Dashboard, including buttons, grids, headings, and so on.

### Switching Themes

To set a different theme:

1. Go to **My Organization > Settings**.
2. In the **Choose Theme** settings, select a different theme.
3. Click **Save**.

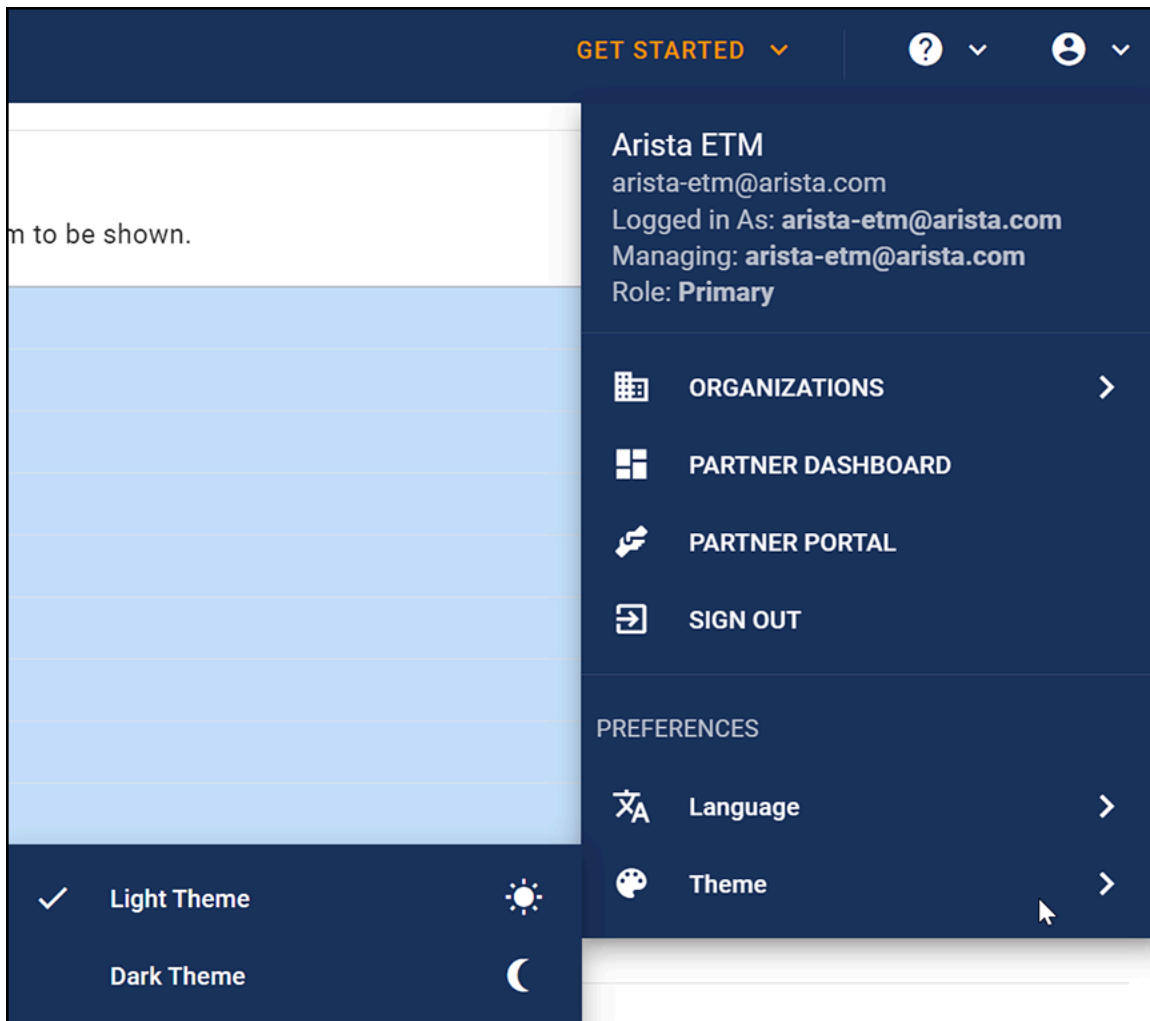
**CHOOSE THEME**

Choose Theme

Light Theme

**SAVE**

You can also select themes directly in the **Account** menu:



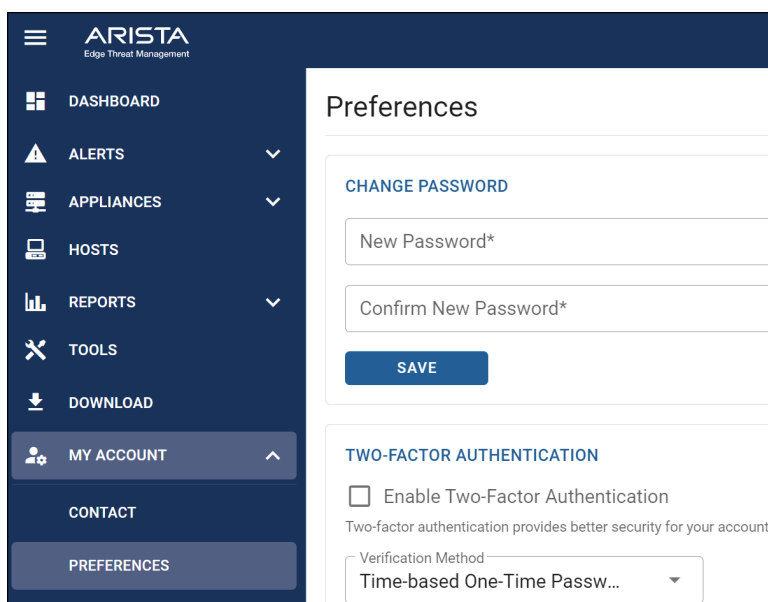
## 9.6 Two-Factor Authentication on the ETM Dashboard

You can enable two-factor authentication to secure your ETM Dashboard account. If enabled, the system requires the user to enter a one-time-use verification code before logging onto the ETM Dashboard. The code allows you to access your account after you authenticate with your regular username and password.

If enabled, two-factor authentication requires PIN confirmation upon each login. If you frequently connect using the same system and browser, you can opt to "remember me" during PIN verification. This option uses a secure cookie to authenticate your browser after login. The cookie is valid for 30 days.

### Enabling Two-Factor Authentication

1. On the ETM Dashboard, click **My Account** in the menu along the left-hand side of the page.
2. Click **Preferences**.
3. In the Two-Factor Authentication section, select **Enable Two-Factor Authentication**.
4. Select your preferred delivery method under the *Verification Method*. See the following for more information on delivery methods.
5. Click **Save** to apply the change.



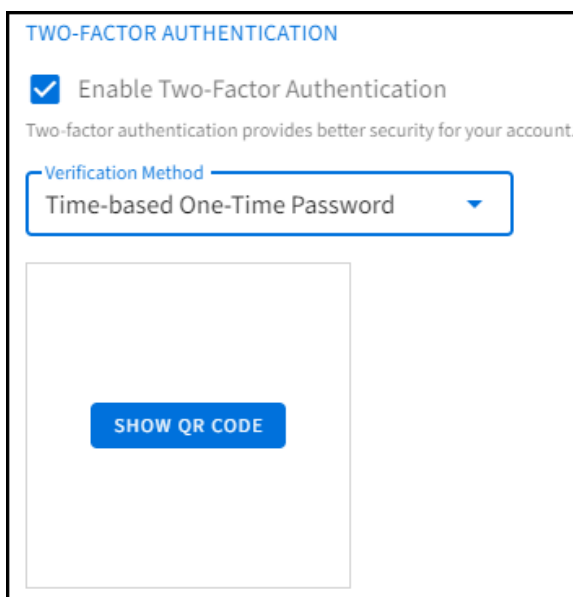
## Delivery Method Options

ETM Dashboard provides two options to receive your one-time code.

- *Email* will send the code to the account's primary email address.
- A *time-based one-time password* (or "TOTP") will send the code to a TOTP application of your choice, such as Google Authenticator.

## Pairing a TOTP application with ETM Dashboard

Selecting the *Time-based One-Time Password* delivery option will reveal the **show QR code** button. Click that button to display the QR code. On your mobile device, open the TOTP authentication app you want to pair with the ETM Dashboard and select its **pair** or **scan** feature. Scan the code on your screen to complete pairing.

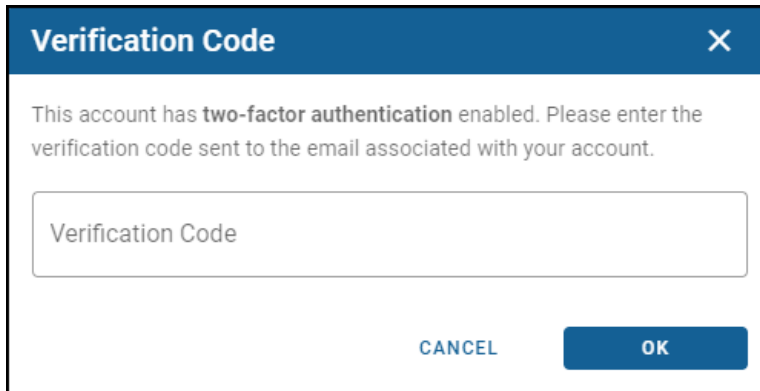




After you have paired an app with the ETM Dashboard, that app is a necessary part of the login procedure. If you uninstall the app or remove the paired account and fail to disable two-factor authentication in the ETM Dashboard, you will lose access to your account. In that instance, contact Support for assistance.

### Logging onto the ETM Dashboard

During the login process, after entering your email address and password, you will be prompted to enter your verification code. Open the paired TOTP app to retrieve the code.

A screenshot of a 'Verification Code' dialog box. The title bar is blue with the text 'Verification Code' and a close button (X). The main content area is white and contains the text: 'This account has two-factor authentication enabled. Please enter the verification code sent to the email associated with your account.' Below this text is a text input field with the placeholder text 'Verification Code'. At the bottom of the dialog, there are two buttons: 'CANCEL' and 'OK'.

On the Verification Code pop-up, you will have the option to remember the device from which you are logging in. Enable this option to postpone further verification requests for 30 days.

## 9.7 General Data Protection Regulation (GDPR)

We have recently made changes to comply with the EU's General Data Protection Regulation (GDPR). As per the GDPR, the following articles will help guide you through deleting your account and all associated data or requesting a copy of all data.

You can view Arista Edge Threat Management's Privacy Policy here:

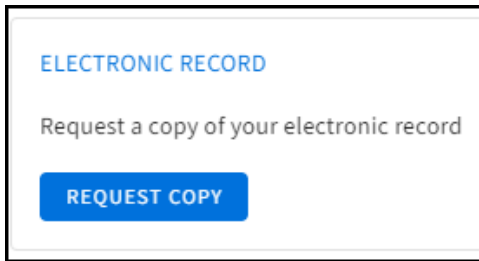
<https://www.arista.com/en/privacy-policy>.

## 9.8 Request a Copy of your Data

You can select this process to request a copy of all data stored by your ETM Dashboard account. This excludes data from any NG Firewall or Micro Edge appliances associated with the account, such as settings or Reports data.

### Requesting your Data

1. Login to the ETM Dashboard.
2. Click **My Organization** in the menu along the left-hand side.
3. Select **Settings**.
4. Click the blue **Request Copy** button at the bottom of the **Settings** page.



5. You should then receive a message acknowledging the request. A copy of the data will be sent to the account owner's email address.

## 9.9 Deleting an ETM Dashboard Account

Follow the process outlined in this article to remove your ETM Dashboard account and all associated data altogether.



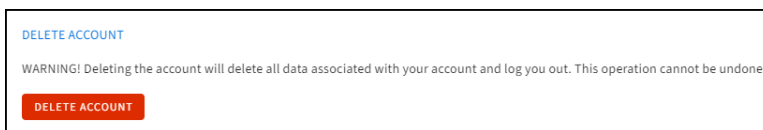
**Important:** Account deletion is permanent and cannot be undone! Arista Edge Threat Management cannot restore accounts deleted by accident.



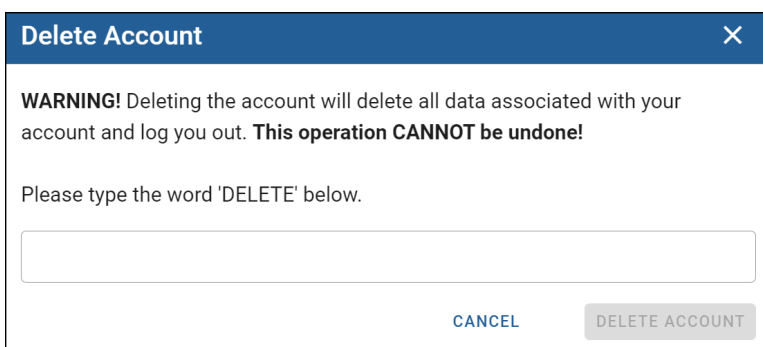
**Note:** Removing a user under your account is not the process. [CLICK HERE](#) for those steps.

### Deleting your ETM Dashboard Account

1. Login to ETM Dashboard.
2. Click **My Organization** in the menu at the left-hand side of the page.
3. Click **Settings**.
4. At the bottom of the Settings page is an option labeled **Delete Account**.



5. Click the red **Delete Account** button.
6. A confirmation dialogue will appear asking that the word DELETE be entered before proceeding.



7. Click the **Delete Account** button.
8. You will then be logged out of the ETM Dashboard, and your account will no longer exist.