Technical Guide

Getting Started on the Device GUI for UTM Firewalls

Feature Overview and Configuration Guide

Introduction

Allied Telesis Unified Threat Management (UTM) Firewalls are the ideal integrated security platform for modern businesses. Our UTM firewalls have an integrated architecture built on the AlliedWare Plus™ OS, bringing its verified and superior operation to the security needs of today's networks. As well as Allied Telesis' advanced feature set, and powerful VPN connectivity options for remote network access, the firewalls utilize best of breed security providers, for up-to-the-minute protection from all known threats.

This guide covers the following products:

- AR-Series UTM Firewalls (AR3050S, AR4050S, and AR4050S-5G)
- 10GbE UTM Firewall
- AR4000S-Cloud
- ARX200S-GTX
- ARX200S-GT
- TQR Series (TQ6702 GEN2-R, TQ6702e GEN2-R, TQ7403-R)

The 10GbE UTM Firewall is a virtualized version of the UTM Firewall that can be run on the Vista Manager Network Appliance (VST-APL).

The AR4000S-Cloud is a virtual router product that provides functions such as VPN and firewall that can be run in an Amazon Web Services (AWS) cloud environment or Microsoft Hyper-V virtual environment.

The screenshots in this guide were made with a AR4050S UTM Firewall running AlliedWare Plus software version **5.5.5-2.x** and Device GUI version **2.22.0**. To replicate this setup, please use these versions.

What information will you find in this document?

The Device GUI provides graphical management and monitoring for switches, UTM firewalls, and VPN routers running the AlliedWare Plus operating system.

This guide shows how to configure a UTM Firewall using the Device GUI. You can use the Device GUI to setup the firewall and configure entities (zones, networks and hosts). You can then create the firewall NAT and traffic-control rules for managing traffic between these entities.

You can enable, configure, and customize advanced firewall features such as Application control and Web control. For an even more comprehensive security solution, you can configure threat management features such as Intrusion Prevention, Malware protection, and Antivirus.

The GUI also supports a number of other features such as interface, VLAN, file, log, and wireless network management, as well as a CLI window and a Dashboard for network monitoring. The Dashboard shows interface and firewall traffic, system and environmental information, and the security monitoring widget lets you manage which security features are enabled, as well as providing statistics. The top 10 applications and top 10 categories widgets indicate which applications are consuming the most firewall bandwidth. You can configure rules in response to this monitoring.

You can configure the complete AlliedWare Plus feature-set by utilizing the built-in industry standard Command Line Interface (CLI) window within the Device GUI.

Contents

Introduction 1

Getting Started on the Device GUI for UTM Firewalls 1

- What information will you find in this document? 2
- Products and software version that apply to this guide 5
- Related documents 6
- 10GbE UTM Firewall documents 7
- AR4000S-Cloud documents 7

Updating the GUI 8

- Using the CLI to update the GUI version 8
- Using the GUI to update the GUI version 8

Using the wizard to configure Internet and VPN connections 11

- Setup an Internet connection 11
- Configuring a VPN connection 21

What is a firewall? 24

What are entities? 24

- Zones, networks, and hosts 25

Using rules 26

Configuring the firewall 27

- Part 1: Configure a standard 3-zone network 27
- Part 2: Configure the firewall for Update Manager 42
- Part 3: Configure free security features 46
- Part 4: Configure licensed Advanced Firewall security features 50
- Part 5: Configure licensed Advanced Threat Protection (ATP) security features 56
- Part 6: Advanced IPS 57

The Dashboard 61

The Network Map 69

- Network map features 69
- Viewing device information 71
- Configuring the topology view 72
- Customizing device icons 74
- Accessing the Device GUI from the Network map 76

Wireless management 78

Other features 79

- File management 80
- License management 81
- Logging management 83

AMF Security mini on the AR4050S Series 87
5G Mobile on the AR4050S-5G 87

Products and software version that apply to this guide

This guide applies to:

All AR-Series UTM Firewalls running version **5.4.7-x.x or 5.4.8-x.x** or later.
Supported models include:

- AR3050S
- AR4050S
- AR4050S-5G from version **5.5.1-1.3** onwards.

The 10GbE UTM Firewall, running version **5.5.1-2.x** or later.

The AR4000S-Cloud, running version **5.5.2-2.x** or later.

The 10GbE UTM Firewall is supported running on the Vista Manager Network Appliance (VST-APL).

The AR4000S-Cloud is supported running on the Amazon Web Services (AWS) cloud environment, and Microsoft Hyper-V virtual environment.

Note: The screen shots in this guide were made with a router running AlliedWare Plus software version **5.5.5-2.x** and Device GUI version **2.22.0**. To replicate this setup, please use these versions.

Feature support may change in later software versions. For the latest information, see the following documents:

- The product's Datasheet
- The AlliedWare Plus Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

Related documents

You also may find the following AlliedWare Plus Feature Overviews useful:

- Firewall and Network Address Translation (NAT)
- Advanced Network Protection

  This document describes the Advanced Network Security features on the AR4050S, AR4050S-5G and AR3050S, how to configure them, and the logging available for:

  - Intrusion Prevention System
  - Anti-virus
  - Malware Protection
  - IP Reputation
  - Web Control
  - URL Filtering

  It also provides information about: choosing a firewall and features to meet the security and performance needs of your network using Unified Threat Management (UTM) Offload with the AR4050S for sharing the processing load with a second physical or virtual device.

To configure an Allied Telesis VPN Router or switch using the Device GUI see the following guides:

- Getting Started with the Device GUI for VPN Routers Guide
- Getting Started with the Device GUI on Switches

For detailed documentation on wireless configuration, see:

- User Guide: Wireless Controller using the Device GUI.

10GbE UTM Firewall documents

The following documents contain additional information about configuring the 10GbE UTM Firewall on VST-APL.

- 10GbE UTM Firewall Product Information Datasheet
- Installation Guide: Vista Manager Appliance (VST-APL)
- Release Notes: Vista Manager Network Appliance (VST-APL)
- Release Notes for 10GbE UTM Firewall
- User Guide: Vista Manager Network Appliance (VST-APL)

AR4000S-Cloud documents

The following documents contain additional information about configuring the AR4000S-Cloud on AWS.

- AR4000S-Cloud Product Information Datasheet
- Installation Guide: AR4000S-Cloud on Amazon Web Services (AWS)

Updating the GUI

Note: This section details how to upgrade for the AR3050 and AR4050 series devices.

- To upgrade your 10GbE UTM Firewall, refer to the 10GbE UTM Firewall Release Note.
- To upgrade your AR4000S-Cloud, refer to the AR4000S-Cloud documentation.

As new versions of the Device GUI become available with additional functionality, they will also be made available on the update server to be downloaded and installed on the firewall. You can update the GUI version using the CLI or use the File Management menu in the firewall's GUI.

Using the CLI to update the GUI version

To check if there is a new version of the Device GUI, and install it on your firewall, firstly ensure that the firewall can contact the update server and then enter the following command from the CLI window:

```
update webgui now
```

Using the GUI to update the GUI version

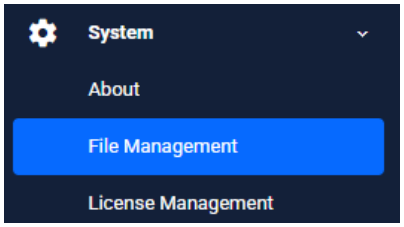
If you would like to use the GUI to update the GUI version, use the following steps:

1. Obtain the GUI file from our Support Portal centre. The filename ends in '.gui'. The file is not device-specific; the same file works on all AlliedWare Plus devices.
2. Log into the GUI:

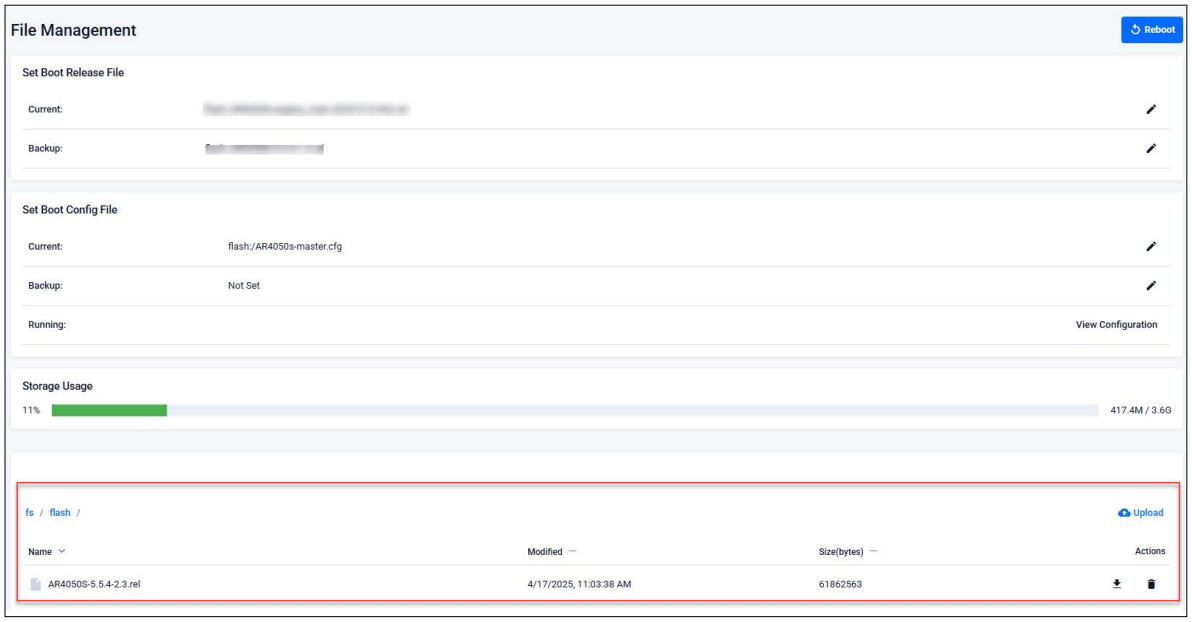
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   The GUI starts up and displays a login screen. Log in with your username and password.

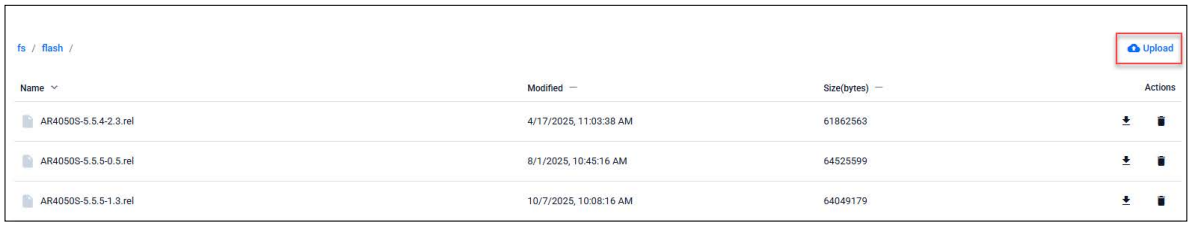
   The default username is ***manager*** and the default password is ***friend.***
3. Go to **System** > **File Management**



4. Scroll down to the Flash section



5. Click **Upload** to upload a GUI file

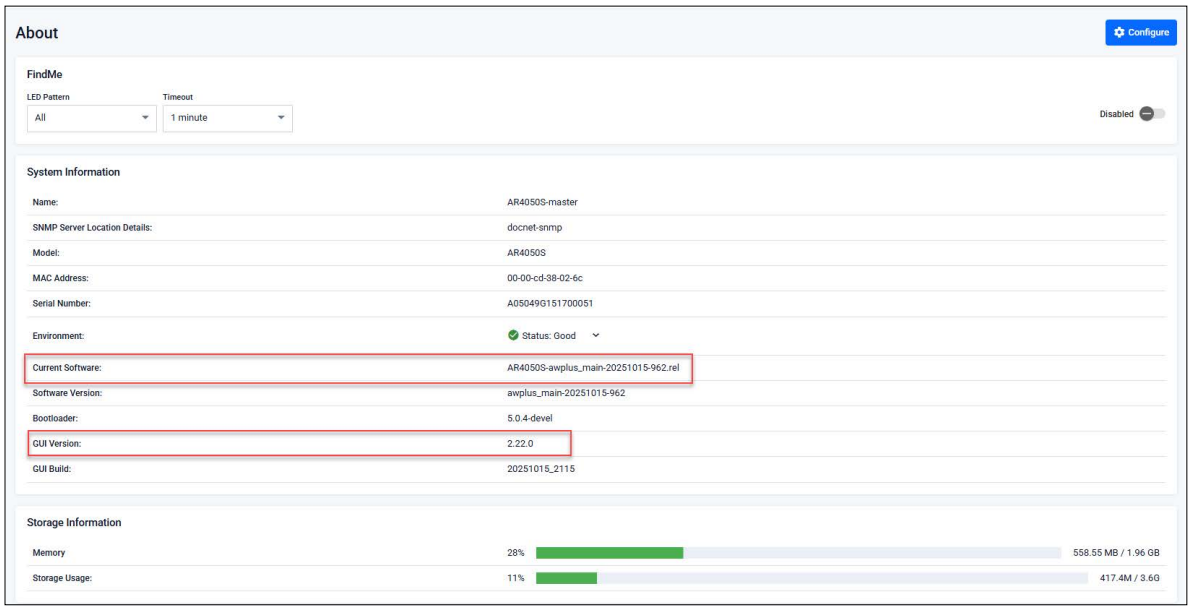


6. Locate and select the GUI file you downloaded from our Software Download centre. The new GUI file is added to the **File Management** window.

7. Use a Serial console connection, Telnet, or SSH to access the CLI, then enter the following commands. These commands configure the device to use GUI files that are stored in Flash, and then stop and restart the HTTP service:

```
awplus# configure terminal
awplus(config)# gui preference flash
awplus(config)# no service http
awplus(config)# service http
```

8. In the Device GUI, go to **System** > **About** to check that the latest file has been successfully added to the device. Look for the GUI Version and GUI Build entries. The first part of the GUI Build entry is the GUI build date.



The device GUI service expects a GUI resource file with a .gui extension. If there is more than one .gui file then it will pick up the one with the highest number in its name.

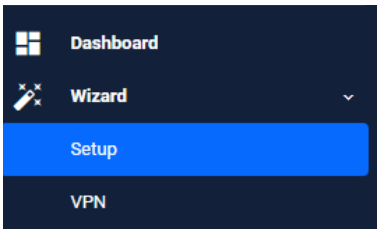
For example, if the following two files are present:

- awplus-gui_555_27.gui
- awplus-gui_555_28.gui

The GUI service will use the '.gui' file with the 28 in its name, as this is the highest number.

Using the wizard to configure Internet and VPN connections

This section describes how to use the wizard to setup an Internet and VPN connection.



Setup an Internet connection

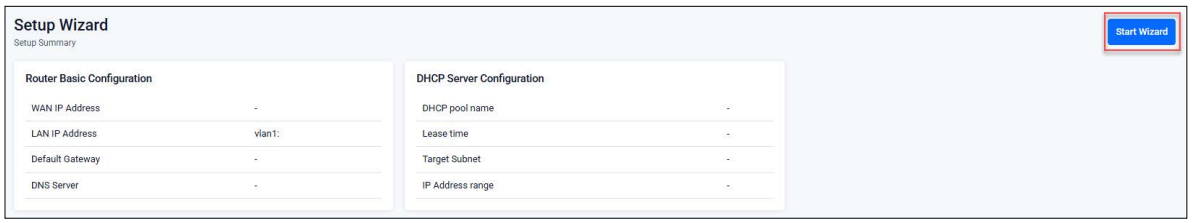
Use the wizard to setup a router's WAN interface along with creating a basic configuration for a LAN. There are three IPv4 methods available: DHCP, Fixed IP, and PPPoE, and two IP version methods available: IPoE and V6 Transition (IPv4 over IPv6).

Once the wizard has run, the **Setup Summary** page displays the current configuration. You can change other things in the GUI after having run the setup wizard, however if you choose to go back and run the wizard again, all your previous configuration will be removed.

The configuration steps are as follows:

Step 1: **Go to Wizard** > **Setup**

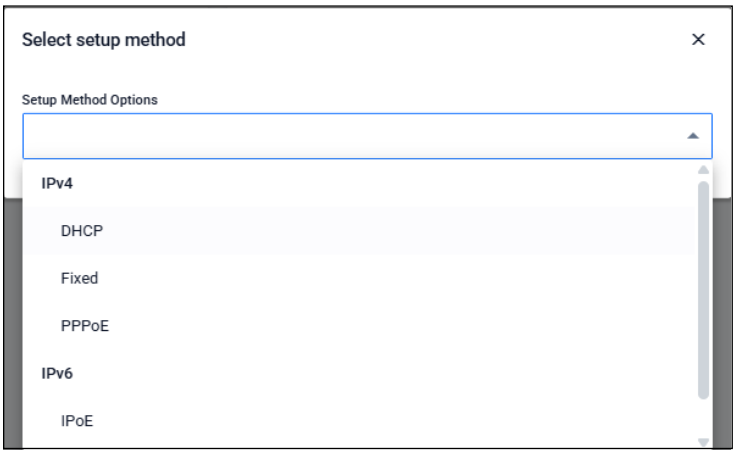
Step 2: **Start the Wizard**



- Click **Start Wizard**
  - If you do have an Internet connection configured, then you'll see those details displayed in the **Setup Summary** screen. Click the **Start Wizard** button in that same screen to reconfigure your current Internet connection settings:
  - If you do not have an Internet connection configured, you'll see a blank **Setup Summary** screen.

Step 3: **Choose a connection method**

- Select a method to connect to the Internet



Step 4: **Configure the connection method**

The following section describes the configuration settings for each connection method.

Note: If you turn on the DHCP server, it will assign clients addresses that are in the same subnet as the LAN interface's default address. This will not work if you have changed the LAN interface's address. In that case, select OFF for DHCP Server and manually configure the DHCP server from the **Network Services** menu after the Wizard is complete.

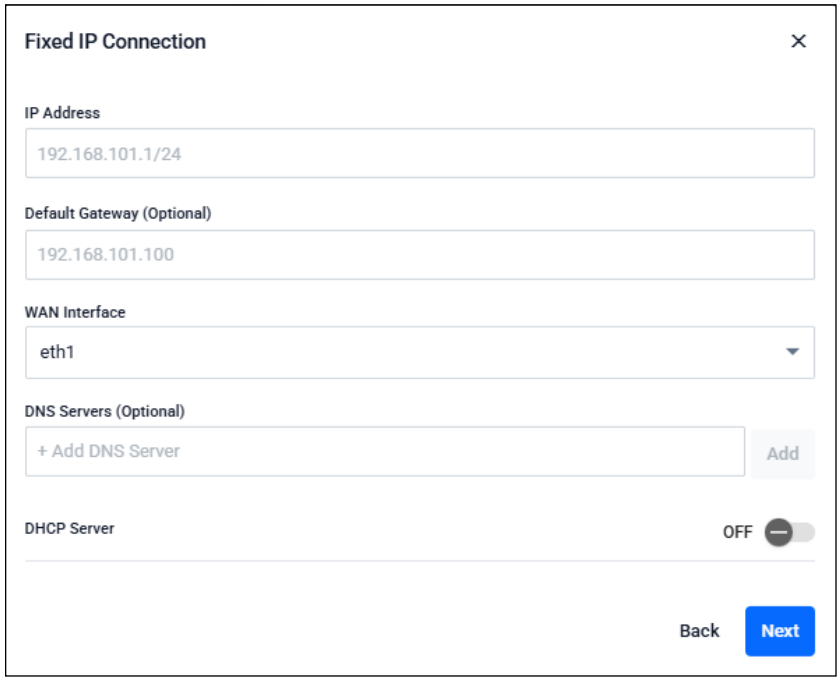
IPv4 - DHCP Connection

Configure the IPv4 DHCP connection:

Field	Description
WAN Interface	Select the interface used to connect to the Internet, for example eth1.
DNS Servers	Specify the DNS server to use for name resolution. ■ If you want DHCP to automatically obtain a DNS server address, use the default **Auto**. ■ If fixed settings are required, click the down arrow on the right, click **+ Add DNS Server**, and enter the IP address of the DNS server.
DHCP Server	Select: ■ **Enabled** to operate the DHCP server function on the LAN-side interface of the device and provide IP addresses etc. to the LAN-side terminals. ■ **Disabled** if you do not want to use the DHCP server function.

IPv4 - Fixed IP Connection

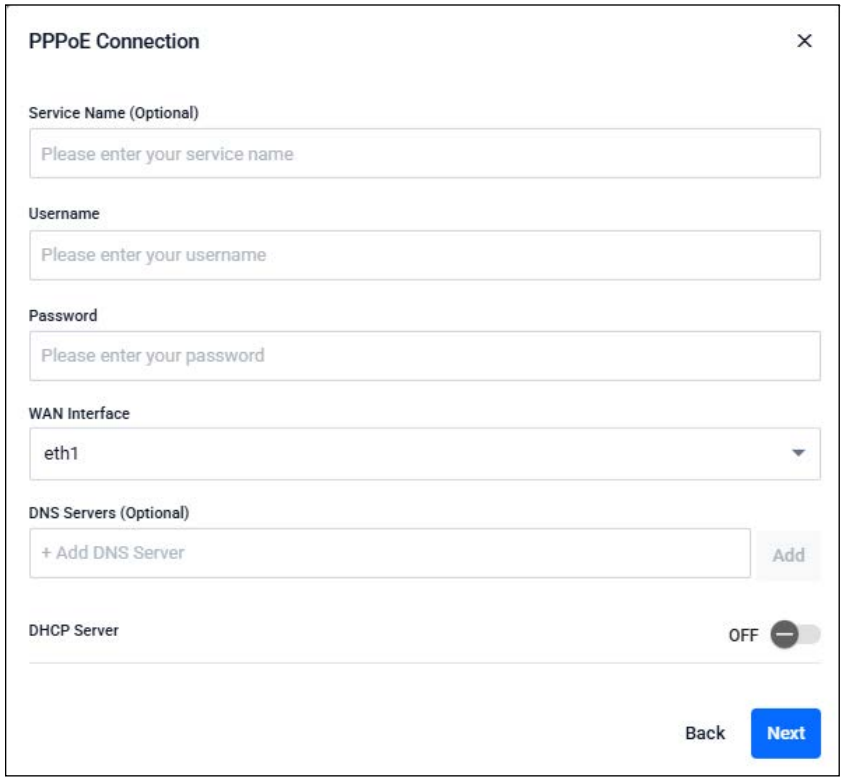
Configure the IPv4 fixed IP connection:



Field	Description
IP Address	Enter the IP address of the WAN-side interface.
Default Gateway	Enter the IP address of the default gateway used to connect to the Internet.
WAN Interface	Select the interface used to connect to the Internet.
DNS Servers	Specify the DNS server to use for name resolution. Click the down arrow on the right, click **+ Add DNS Server**, and enter the IP address of the DNS server.
DHCP Server	Select: ■ **Enabled** to operate the DHCP server function on the LAN-side interface of the device and provide IP addresses etc. to the LAN-side terminals. ■ **Disabled** if you do not want to use the DHCP server function.

IPv4 - PPPoE Connection

Configure the IPv4 PPPoE connection:



Field	Description
Service Name	This is the PPPoE service name. You can usually leave it blank. Enter the PPPoE service name only if your Internet service provider (ISP) has specified it.
Username	PPP user name. Enter the user name for the Internet connection notified by your ISP.
Password	PPP password. Enter the password for the Internet connection provided by your ISP.
WAN Interface	Select the interface used to connect to the Internet.
DNS Servers	Specify the DNS server to use for name resolution. ■ If you want IPCP to automatically obtain the DNS server address when connecting to PPPoE, you can leave it as the default. ■ If fixed settings are required, click the down arrow on the right, click **+ Add DNS Server**, and enter the IP address of the DNS server.
DHCP Server	Select: ■ **Enabled** to operate the DHCP server function on the LAN-side interface of the device and provide IP addresses etc. to the LAN-side terminals. ■ **Disabled** if you do not want to use the DHCP server function.

IPv6 - IPoE Connection

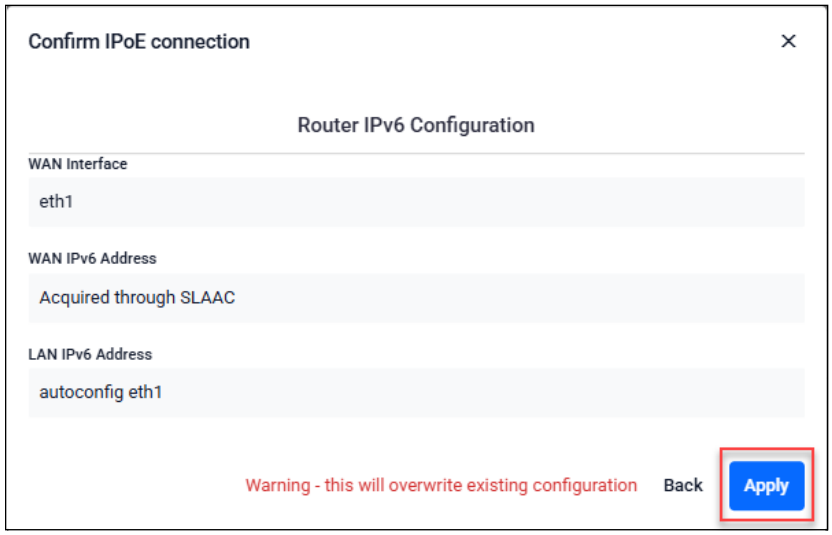
Configure the IPv6 IPoE connection. There are two tabs in this panel, SLAAC (Stateless Address Auto-Configuration) and DHCPv6 PD (Prefix Delegation).

1. SLAAC number (RA method)

Field	Description
WAN Interface	The interface used to connect to the Internet, for example eth1.

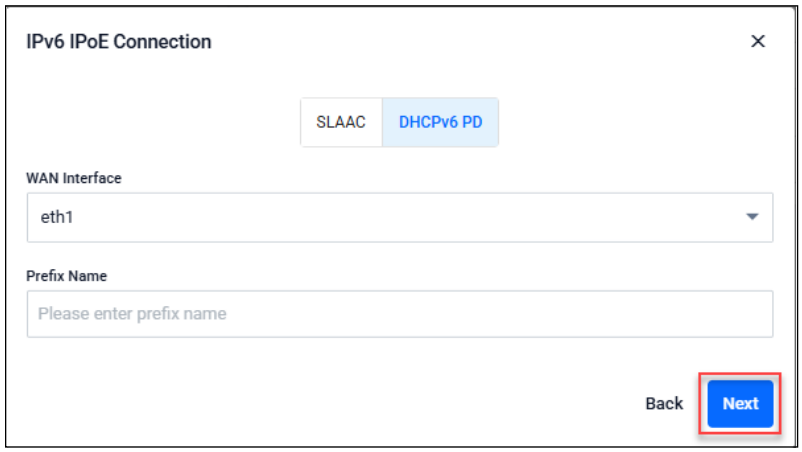
- Click the drop down arrow to select the WAN interface
- Click **Next**

  The following confirmation panel appears:



- Click **Apply** to continue

2. DHCPv6 PD (Prefix Delegation)



Field	Description
WAN interface	Select the interface used to connect to the Internet, for example eth1.
Prefix Name	Enter a name to refer to the retrieved prefix. ■ This is the IPv6 prefix name advertised on the router advertisement message sent from the device. ■ The IPv6 prefix name is delegated from the DHCPv6 Server configured for DHCPv6 Prefix-Delegation.

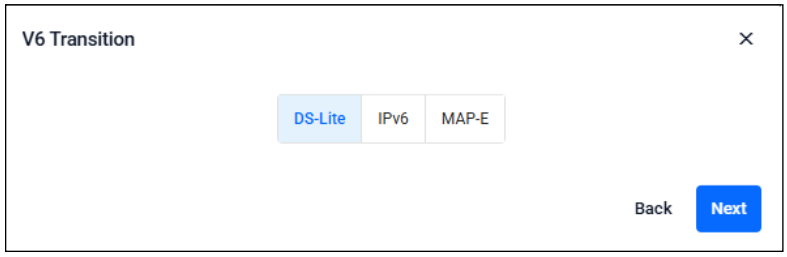
- Click the drop down arrow to select the WAN interface
- Enter a **Prefix Name**
- Click **Next**
- Check the **Confirm IPoE connection** dialog and click **Apply**

V6 Transition (IPv4 over IPv6)

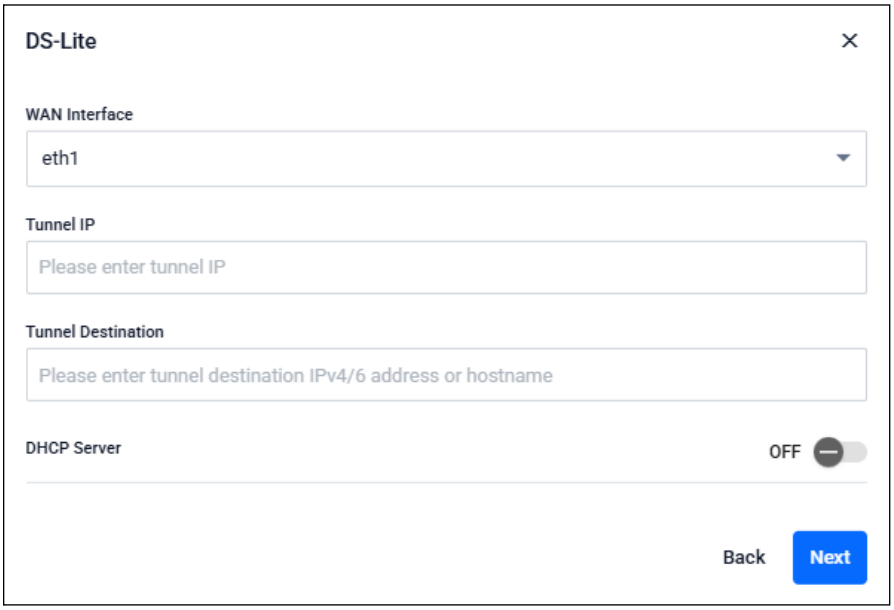
Configure the V6 transition options. There are three tabs in this panel:

1. DS-Lite
2. IPv6
3. MAP-E

Select a tab, then click **Next**:

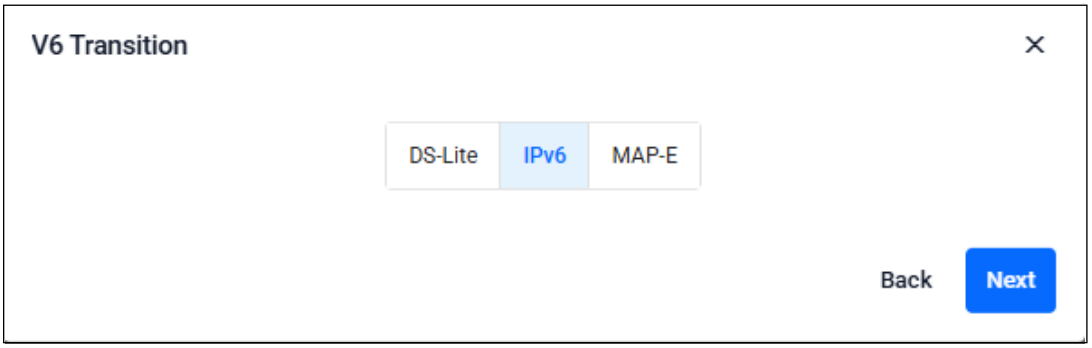


1. DS-Lite tab



Field	Description
WAN Interface	Select the interface used to connect to the Internet.
Tunnel IP	Enter the IPv4 adders for the tunnel interface.
Tunnel Destination	Enter the destination address for packets sent over the tunnel.
DHCP Server	Select: ■ **Enabled** to operate the DHCP server function on the LAN-side interface of the device and provide IP addresses etc. to the LAN-side terminals. ■ **Disabled** if you do not want to use the DHCP server function.

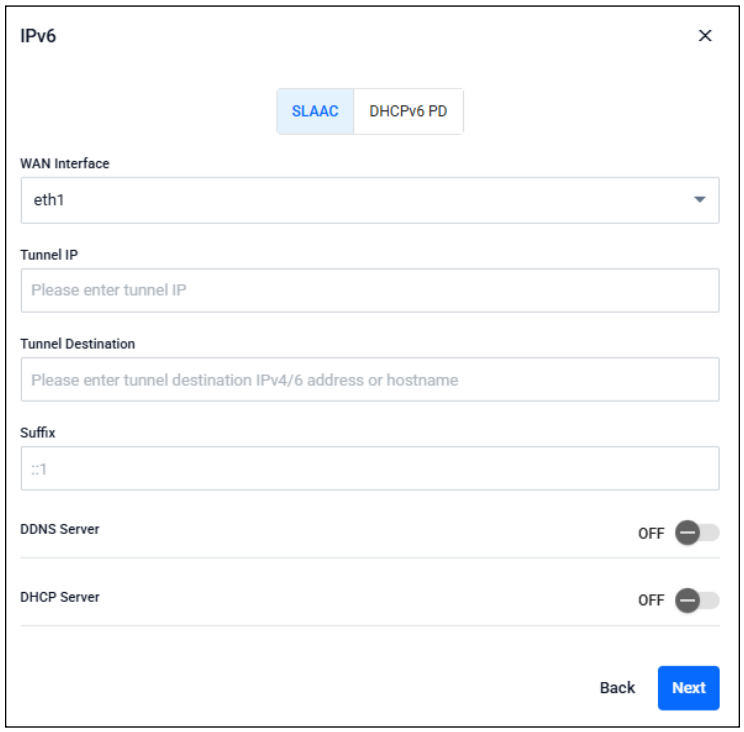
2. IPv6 tab



There are two tabs here, SLAAC and DHCPv6 PD:

- IPv6 - SLAAC

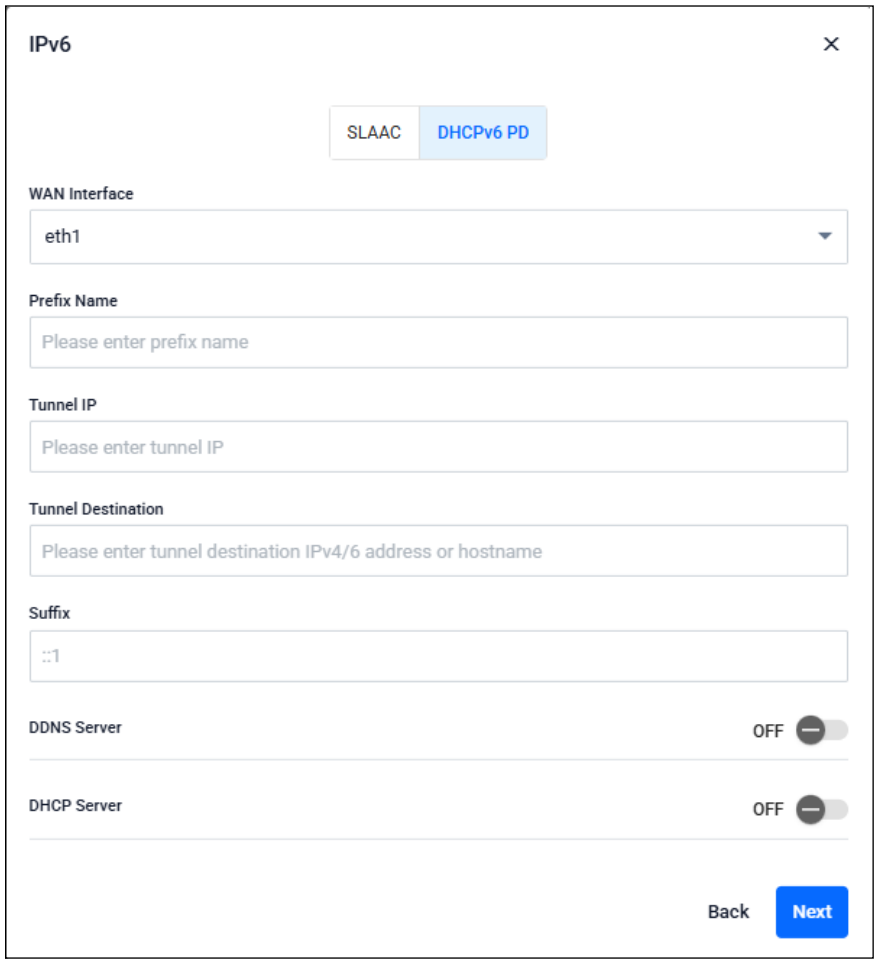
Configure the IPv4 connections with IPv6 IPoE connections (RA method) and IPv6 tunnels (fixed):



Field	Description
WAN Interface	Select the interface used to connect to the Internet.
Tunnel IP	Enter the address for the tunnel interface.
Tunnel Destination	Enter the destination address for packets traversing the tunnel.
Suffix	Enter the interface ID specified in advance by your ISP.
DDNS Server	Use the dynamic DNS client feature to notify the update server of the IPv6 address updates.
DHCP Server	Select: ■ **Enabled** to operate the DHCP server function on the LAN-side interface of the device and provide IP addresses etc. to the LAN-side terminals. ■ **Disabled** if you do not want to use the DHCP server function

- IPv6 - DHCPv6 PD

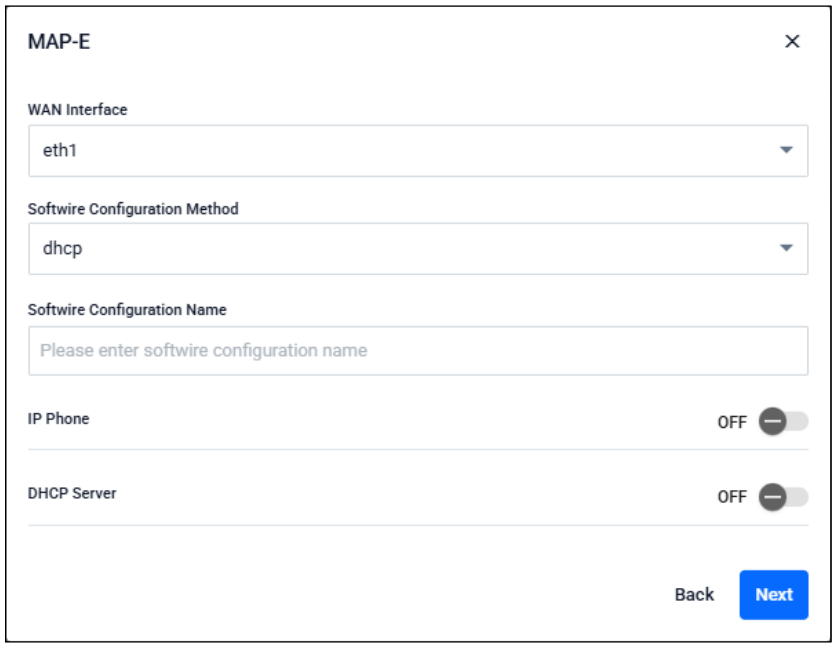
Configure IPv4 connections with IPv6 IPoE connections (DHCPv6 PD method) and IPv6 tunnels (fixed).



Field	Description
WAN Interface	Select the interface used to connect to the Internet.
Prefix Name	Enter a name to refer to the retrieved prefix.
Tunnel IP	Enter the IPv4 address that you want to configure for the tunnel interface.
Tunnel Destination	Enter the end point (on-the-go device: operator router (BR)) address of the delivery packet sent from the tunnel interface.
Suffix	Enter the interface ID specified in advance by your ISP.
DDNS Server	Use the dynamic DNS client feature to notify the update server of IPv6 address updates. When enabled, the fields ‘DDNS update URL’, ‘DDNS user name’, and ‘DDNS password’ are displayed.
DHCP Server	Select: ■ **Enabled** to operate the DHCP server function on the LAN-side interface of the device and provide IP addresses etc. to the LAN-side terminals. ■ **Disabled** if you do not want to use the DHCP server function.

3. MAP-E

Configure IPv6 IPoE and MAP-E IPv4 connections:



Field	Description
WAN Interface	Select the interface used to connect to the Internet, for example eth1.
Softwire Configuration Method	Select the softwire method: DHCP, Proprietary, or Static
Softwire Configuration Name	Enter a name to create a new soft wire configuration.
IP Phone	Select: ■ **Enabled** to use an IP phone. When enabled, the **Prefix Name** field is displayed. ■ **Disabled** if you do not want to use the IP Phone function.
DHCP Server	Select: ■ **Enabled** to operate the DHCP server function on the LAN-side interface of the device and provide IP addresses etc. to the LAN-side terminals. ■ **Disabled** if you do not want to use the DHCP server function.

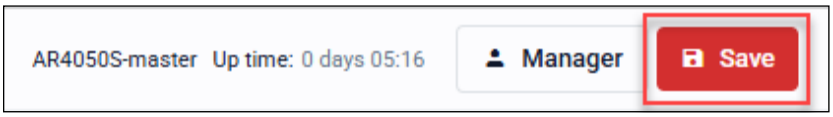
Step 5: **Check and save the configuration**

- Check your configuration is correct and click **Next** to continue

Step 6: **Save the settings to the startup configuration**

A summary screen of the connection status is displayed once the configuration save is complete.

- The contents set in the simple setting are stored in the running configuration and reflected in the operation, but are **not** automatically saved in the startup configuration.
- After confirming that there are no problems with the settings, manually save the settings to the startup configuration using the **Save** button in the navigation bar.
- You can run the wizard again to make changes to your connection method settings.



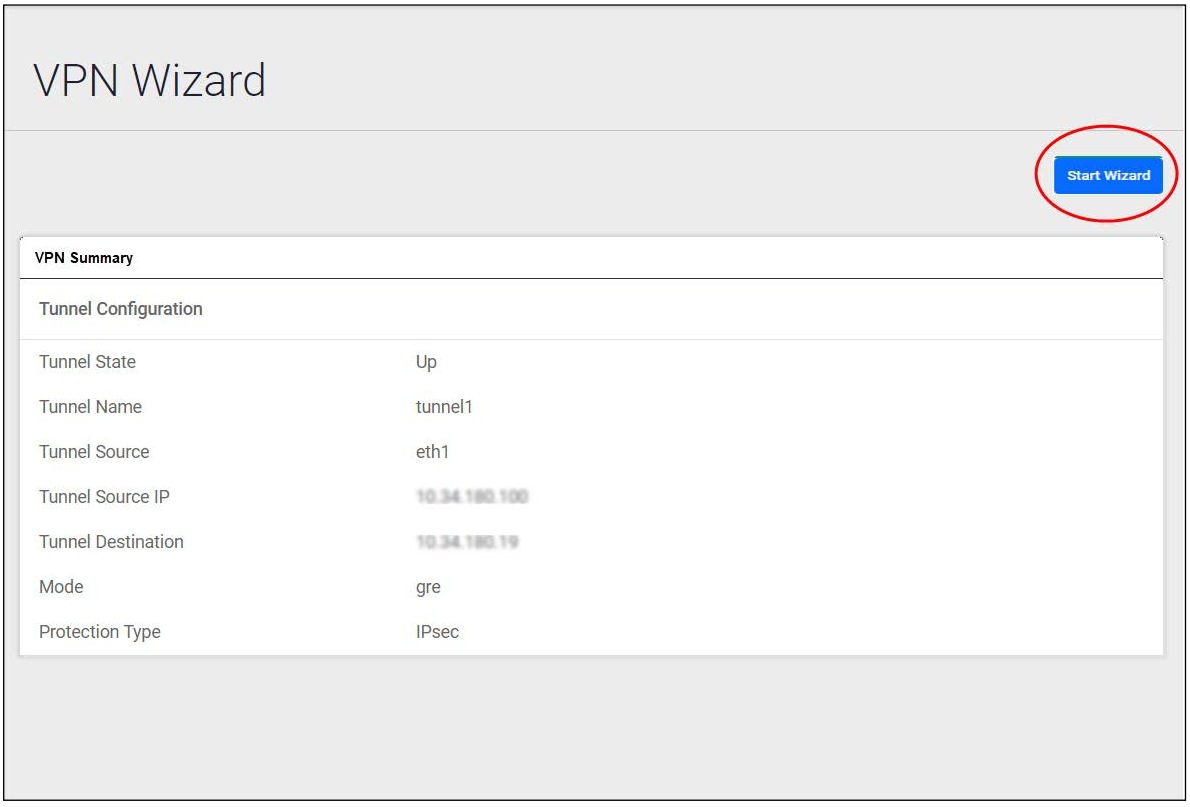
Configuring a VPN connection

To configure a secure VPN connection, first make sure you have an Internet connection, and then use the following steps:

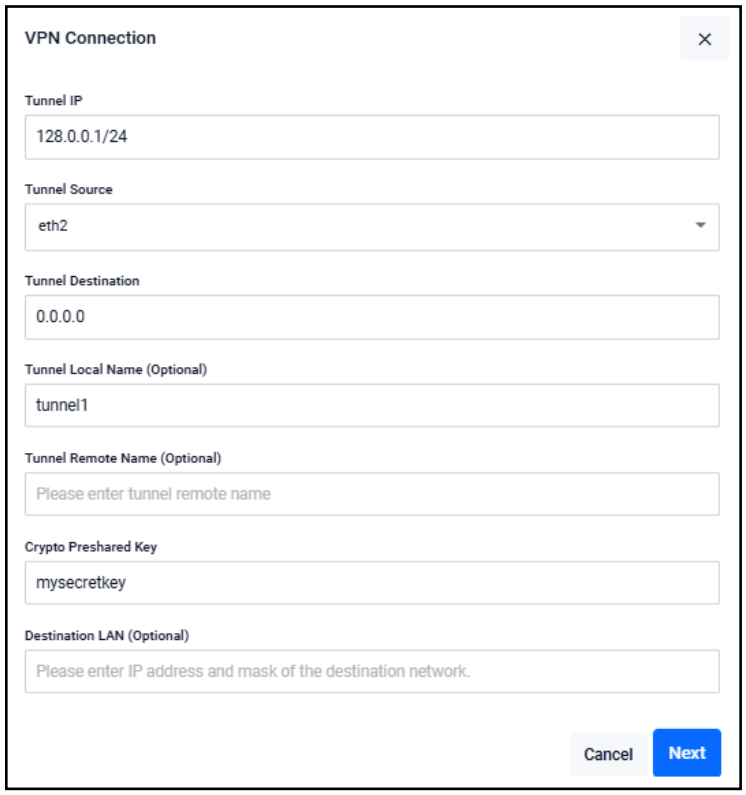
Step 1: **Go to Wizard** > **VPN**

Step 2: **Click the Start Wizard button**

- If you don't have an existing VPN connection, you'll see a blank **VPN Summary** screen like the one above.
- If you do have an existing VPN connection, then you'll see those details displayed in the **VPN Summary** screen. Click the **Start Wizard** button on that same screen to reconfigure your current VPN connection settings:

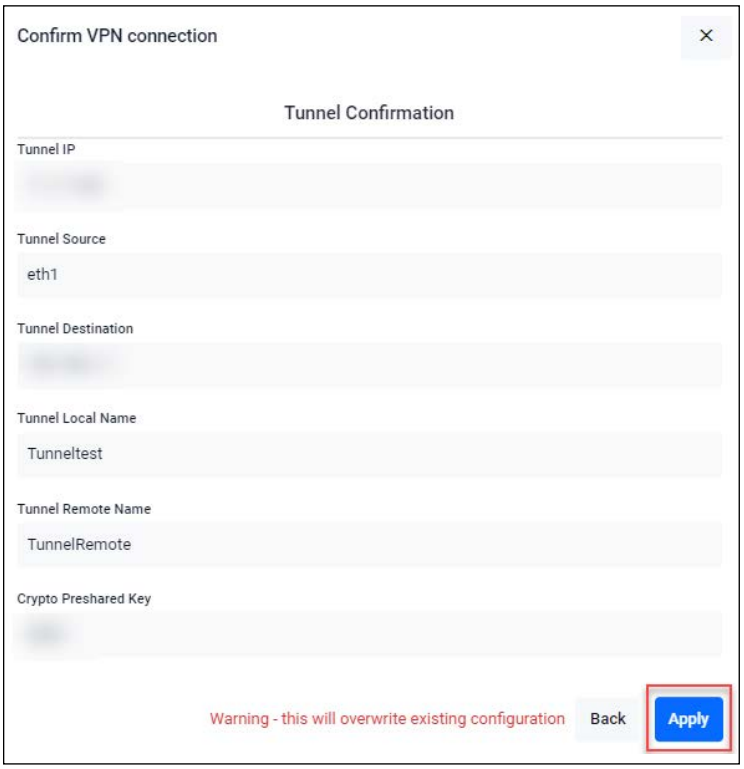


Step 3: **Enter the VPN connection information**



Field	Description
Tunnel IP	Enter the IPv4 address of the tunnel interface.
Tunnel Source	Select the interface for the VPN connection.
Tunnel Destination	Enter the end IP address or host name of the VPN destination.
Tunnel Local Name	Enter the ISAKMP IP (local ID) for the local router.
Tunnel Remote Name	Enter the ISAKMP IP (remote ID) for the remote router.
Crypto Pre-shared Key	Enter the password (ISAKMP pre-shared key) for the VPN connection.
Destination LAN	Enter the LAN-side IPv4 address of the destination network.

Step 4: **Confirm VPN tunnel connection**



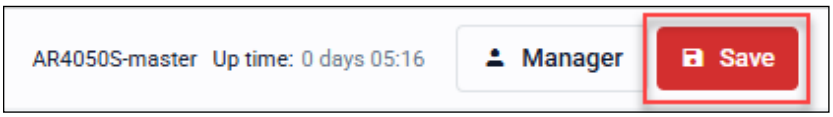
Step 5: **Review and save your settings**

- Check your configuration is correct and click **Apply** to continue.
- If you click **Apply** with a VPN connection already set up, the existing settings on the running configuration will be erased and replaced with the newly configured content.

Step 6: **Save the settings to the startup configuration**

When the configuration save is complete, a summary screen of the connection status is displayed.

- The contents set in the simple setting are stored in the running configuration and reflected in the operation, but are **not** automatically saved in the **startup** configuration.
- After confirming that there are no problems with the settings, manually save the settings to the **startup** configuration using the **Save** button in the navigation bar.
- You can always run the wizard again to make changes to your VPN connection settings.



What is a firewall?

A firewall, at its simplest level, controls traffic flow between a trusted network (such as a corporate LAN) and an untrusted or public network (such as the Internet). Previous generations of firewalls were port-based or used packet filtering. These traditional firewalls determined whether traffic is allowed or disallowed based on characteristics of the packets, including their destination and source IP addresses and TCP/ UDP port numbers. However, traditional firewalls have failed to keep pace with the increased use of modern applications and network security threats.

Allied Telesis firewalls use a **Deep Packet Inspection** (DPI) engine that provides real-time, Layer 7 classification of network traffic. Rather than being limited to filtering packets based on protocols and ports, the firewall can determine the **application** associated with the packet, for example social networking, instant messaging, file sharing, or streaming. This allows Enterprises to accurately differentiate business-critical from non-critical applications, and enforce security and acceptable-use policies for applications in ways that make sense for the business.

This comprehensive application, content, and user identification provides full visibility into network activity, to allow intelligent control of network traffic. Visibility and control, partnered with advanced threat protection, together provide comprehensive online security.

What are entities?

The firewall questions where streams are coming from, and where they are going to be sent.

To help answer those questions, the firewall must have a logical map of the network environment, so that it can categorize the sources and destinations of the flows that it is managing.

Allied Telesis firewalls map out the network environment into regions, using three separate levels. The divisions into which the firewall cuts up its environment is called **entities.** These entities, in order of scale, include zones, networks, and hosts. You can use these hierarchical groups to apply security policies over different company networks, separate departments, or on individual client devices.

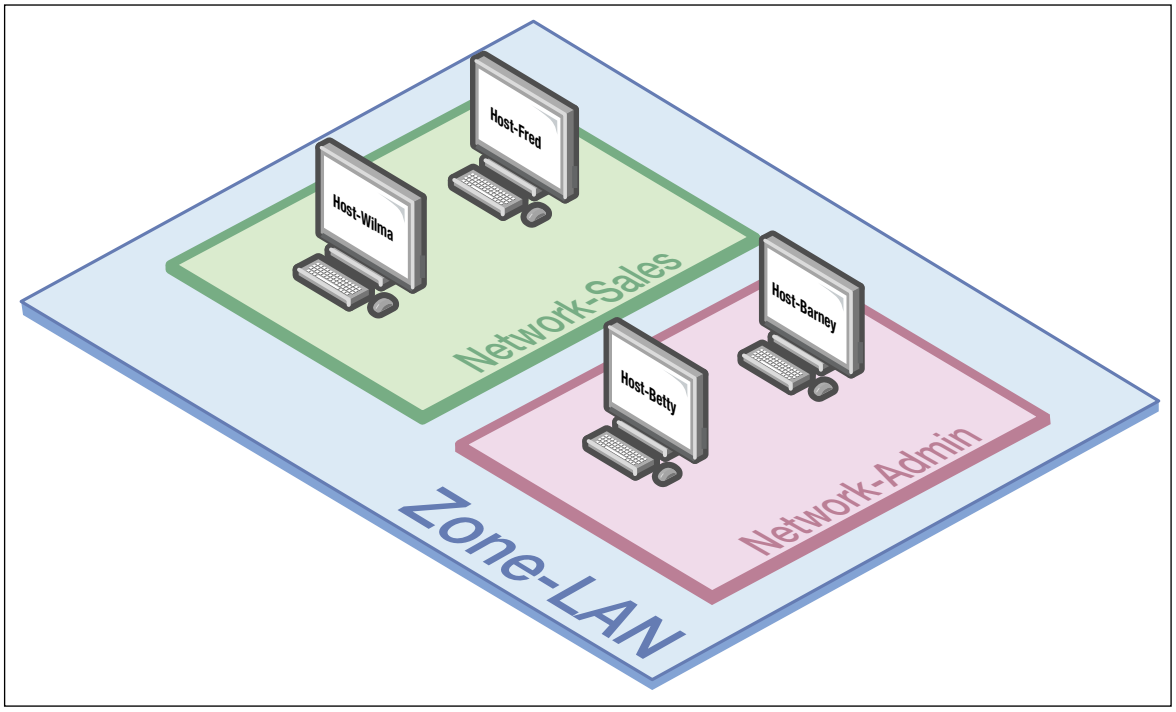
The next sections describe the AlliedWare Plus firewall and how to configure it.

Zones, networks, and hosts

A **zone** is the highest level of division within the network, and defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of your network. A typical network environment might contain a public (WAN) zone representing the Internet, a private (LAN) zone behind the firewall, and a Demilitarized zone (DMZ) containing publicly accessible web servers. Zones are divided up into networks, which in turn contain hosts.

A **network** is a logical grouping of hosts within a zone, for example, the sales network within the LAN zone. Networks consist of the IP subnets and interfaces over which they are reachable. The allocating of networks to zones is the core activity in dividing the network up into logical regions to which different security policies apply. A zone has no real meaning in itself until it has one or more networks allocated to it. Once networks have been allocated to a zone, the zone is then the entity that collectively represents that set of networks. Then rules can be applied to the zone as a whole, or to individual networks within the zone.

A **host** is a single node in a network, for example, the PC of a specific employee. The diagram below shows PC Wilma is a host within the sales network within the LAN zone. Host entities are defined so that specific rules can be applied to those particular hosts - e.g. a server to which certain types of sessions may be initiated.



Using rules

Rules allow the advanced control of users, and the applications they use on the network.

Firewall rules: are used to filter traffic, allowing or denying, between any two entities. This allows for granular control, as rules can be based on traffic sources that might be zones, networks, or hosts, and traffic destinations that might be zones, networks, or hosts.

For example, an organization may choose to block Skype™ company-wide (i.e. from ANY zone to ANY zone), or allow it only for the marketing department (i.e. allow Skype from the Marketing network to ANY zone, but block it from any other network, zone, or host).

Traffic control rules: are used to control the bandwidth that applications use. For example, Spotify™ music streaming may be allowed, but limited in bandwidth due to an acceptable use policy ensuring company Internet connectivity is prioritized for business traffic.

Network Address Translation (NAT) rules: are used to hide private network addresses for traffic bound for the Internet. All company traffic leaving the corporate office can share a public network address for routing through the Internet to its destination.

The firewall supports:

- NAT with IP Masquerade, where private source addresses are mapped to a public source address with source port translation to identify the association. The single public IP address masquerades as the source IP on traffic from the private addresses as it goes out to the Internet.
- Port forwarding, to provide public access to internal servers. Port forwarding redirects traffic to a specific host, e.g. forwarding HTTP traffic to a web server in the DMZ.

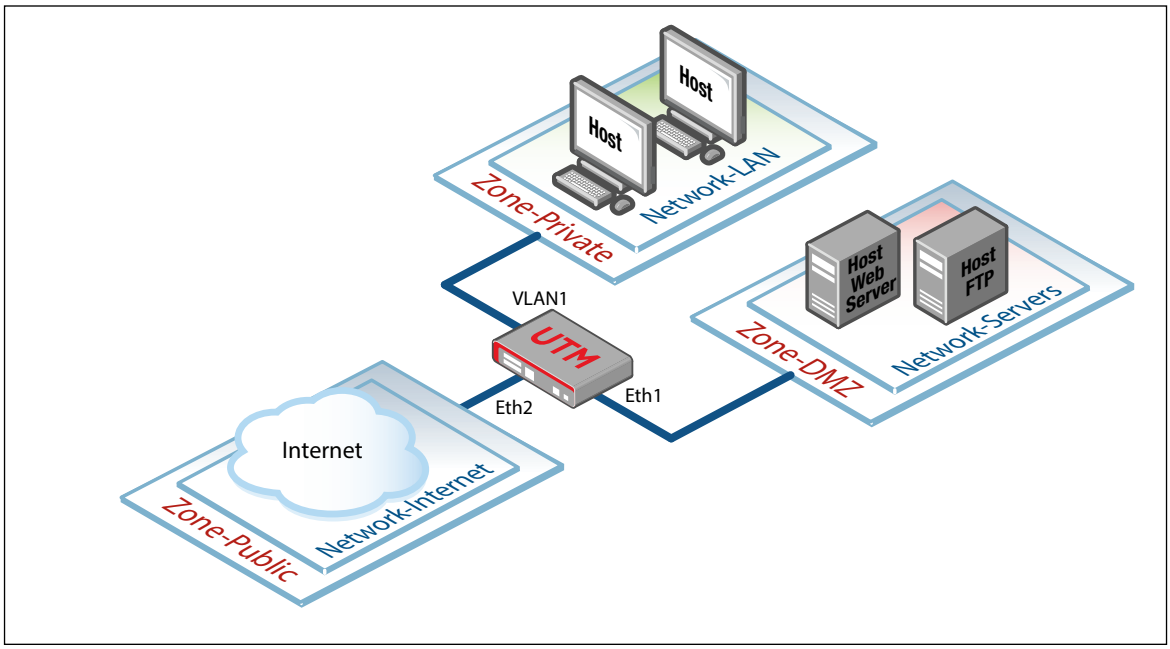
Configuring the firewall

This section comprises of six parts, and describes how to configure an example network scenario, including free and licensed features to create a robust network solution.

The six parts are as follows:

- "Part 1: Configure a standard 3-zone network" on page 27
- "Part 2: Configure the firewall for Update Manager" on page 42
- "Part 3: Configure free security features" on page 46
- "Part 4: Configure licensed Advanced Firewall security features" on page 50
- "Part 5: Configure licensed Advanced Threat Protection (ATP) security features" on page 56
- "Part 6: Advanced IPS" on page 57

Part 1: Configure a standard 3-zone network



Step 1: **Configure firewall interfaces**

Connect to any switch port and browse to **192.168.1.1** to start.

For your virtual firewall, the IP address will be specified when you configure the 10GbE UTM Firewall in VST-APL, or the AR4000S-Cloud in AWS.

If your physical firewall is new and unused, it will already have:

- The GUI installed from the factory,
- the IP address 192.168.1.1 on VLAN1,
- and the HTTP service enabled.

To use the Device GUI, you need to add an IP address to an interface over which you will connect with a browser, once the Device GUI resource file has been loaded onto the firewall.

- You will also need to add IP addresses to the other interfaces that are used in the network.
- Alternatively, you can just add an IP address to the interface over which you will connect with your browser, and then add the other two IP addresses using the GUI Interface Management page.

From the CLI, add the following interface addresses:

IP address for **eth2:**

```
awplus(config)# interface eth2
awplus(config-if)# ip address 128.0.0.1/24
awplus(config-if)# exit
```

IP address for **eth1:**

```
awplus(config-if)# interface eth1
awplus(config-if)# ip address 172.16.0.1/24
awplus(config-if)# exit
```

For **physical devices**, IP address for **VLAN 1**:

```
awplus(config)# interface vlan1
awplus(config-if)# ip address 192.168.1.1/24
awplus(config-if)# exit
```

Or, for **10GbE UTM Firewall** and **AR4000S-Cloud**, IP address for **eth3**:

```
awplus(config)# interface eth3
awplus(config-if)# ip address 192.168.1.1/24
awplus(config-if)# exit
```

Step 2: **Enable the Web server**

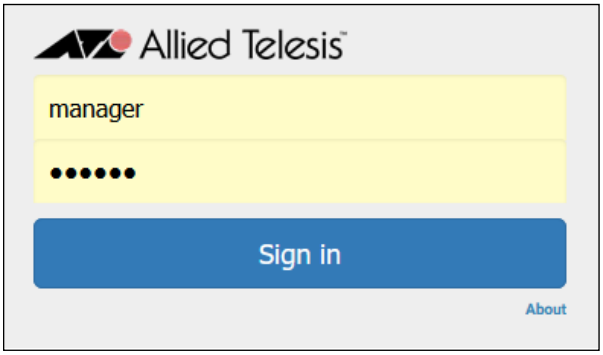
Enable HTTP so the firewall will serve the Device GUI pages:

```
awplus(config)# service http
```

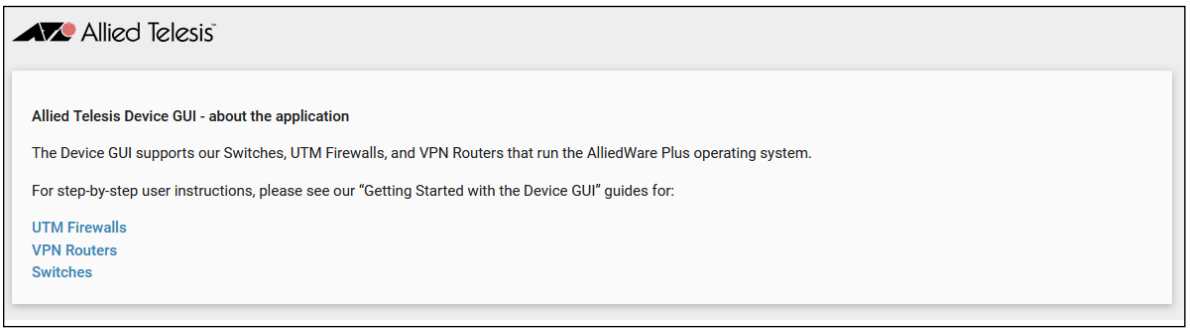
Step 3: **Login to the firewall GUI**

Browse to the IP address of the firewall on the interface you are connecting to - e.g. 192.168.1.1 for VLAN1.

The GUI login page similar to the one below displays:



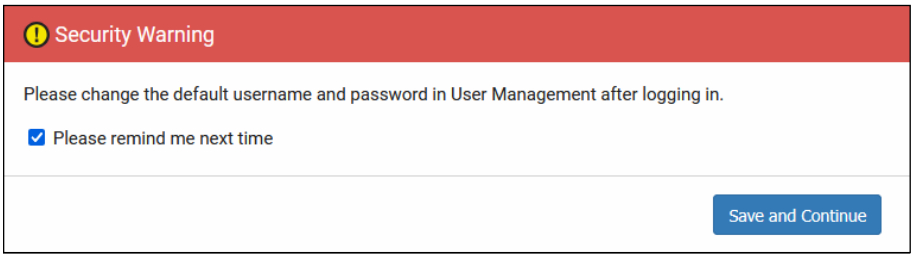
Before you log in, you can click on **About** to display a information about the Device GUI and other Getting Started guide links.



Clicking About opens in a new tab. Close the new tab to return to the login screen.

You can log in using any valid username/password combination that has been configured, or use the default username/password (**manager/friend**), if that has not been changed.

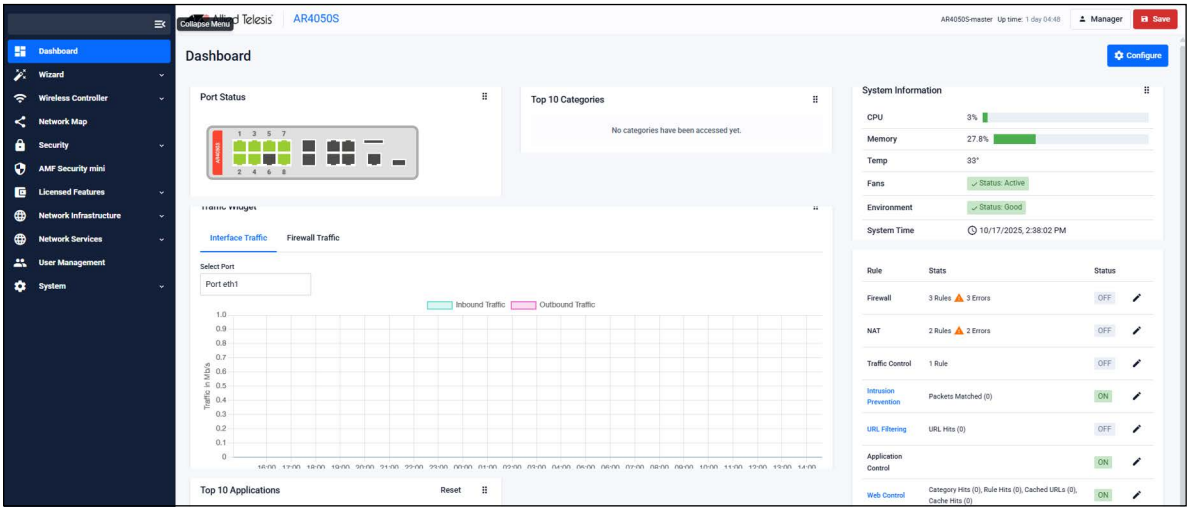
When you log in, you are prompted to change your password. We recommend you change this password in the User Management section for security.



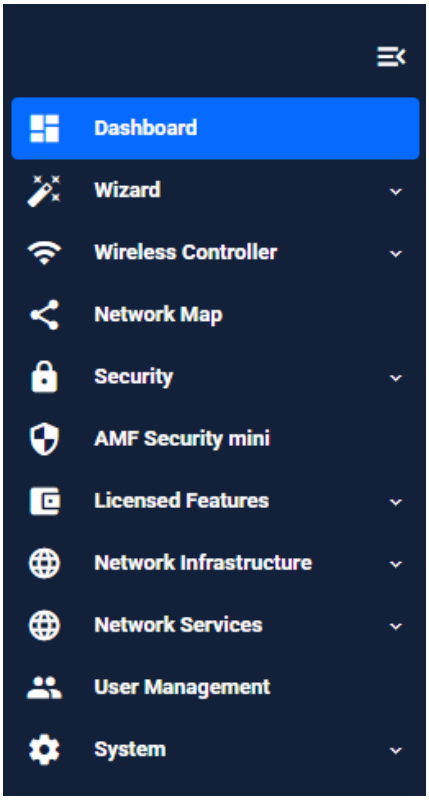
You can tick the check box to choose to be reminded to do this at a later time.

Click **Save and Continue**

Once logged in you will arrive at your device's Dashboard.



The **Dashboard** has a number of useful widgets for monitoring the state of your firewall. We'll look closer at the various Dashboard widgets later, after we've configured the firewall.



The left side of the GUI menu provides the **Wizard**, **Wireless Controller**, **Network Map, Security**, **LAMF Security mini, Licensed Features**, **Network Infrastructure**, **Network Services**, **User Management** and **System** menus.

Note: Not all menu items are available for the 10GbE UTM Firewall and AR4000S-Cloud.

Step 4: **Configure entities**

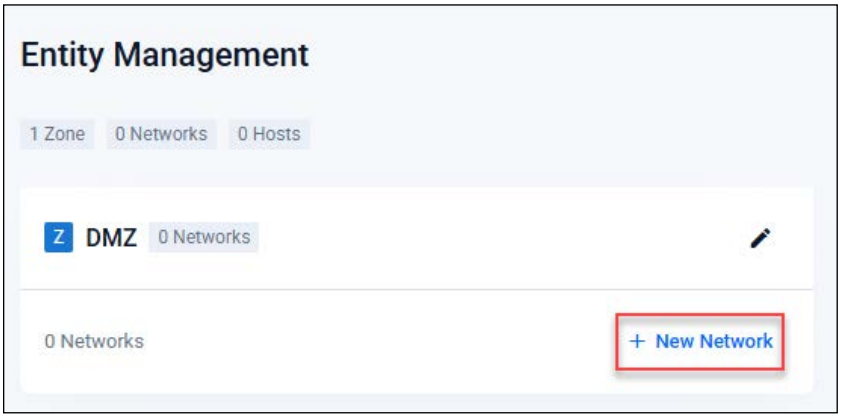
To configure the firewall, we'll first create entities to which rules can be applied. Entities are made up of zones, networks, and hosts. First you create a zone, then you assign the zone a network and then add hosts to that network.

- Go to **Security** > **Entities**

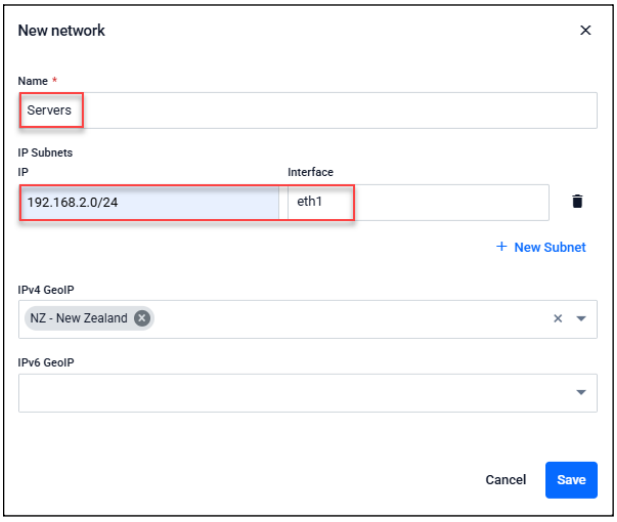
Click the **+ New Zone** button to add a zone

- The first zone we will add is the **DMZ** zone to be used for company servers that we want to be accessible from the Internet.
- Click **Apply**

- Click **+ New Network** in the DMZ zone panel.

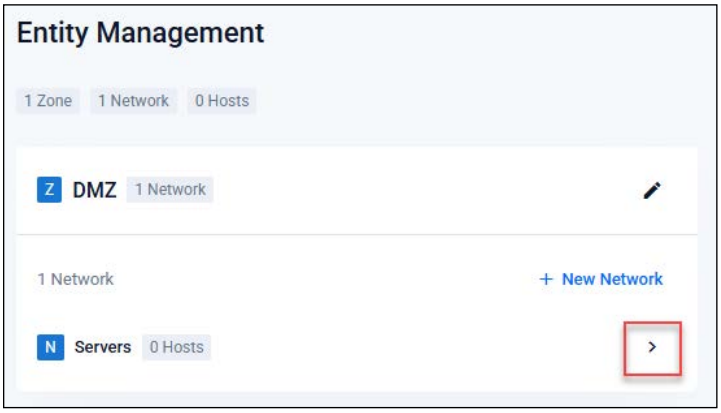


- Name the new network '**servers**'. Add an IP subnet and eth1 as the interface over which this network will be reachable.



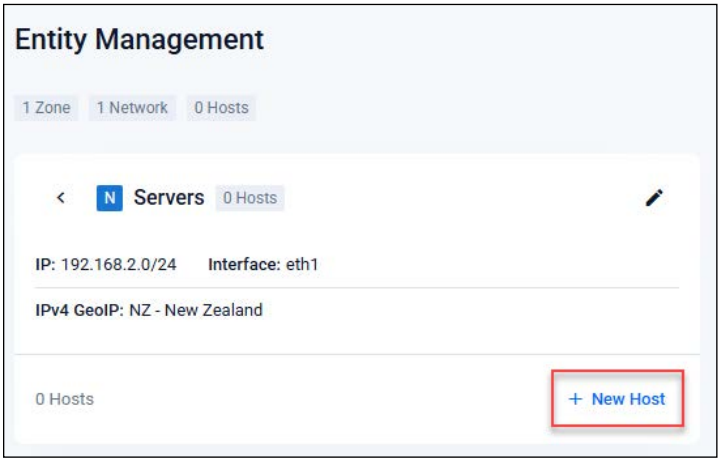
- We can now add specific **hosts** (servers in this case)
- Click on the arrow to add a host to the ‘servers’ network

.

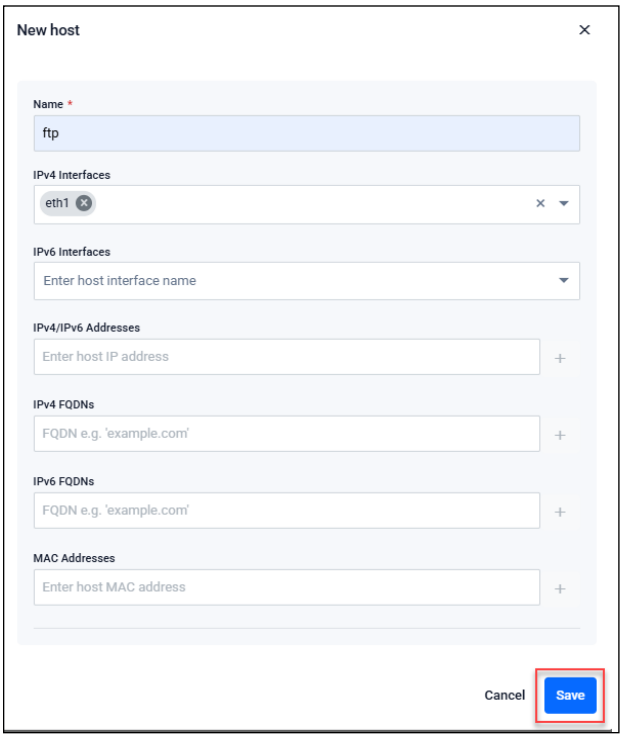


- Click the **+New Host** button

.



- Add the host Name **‘ftp’** and its IP address, and save it

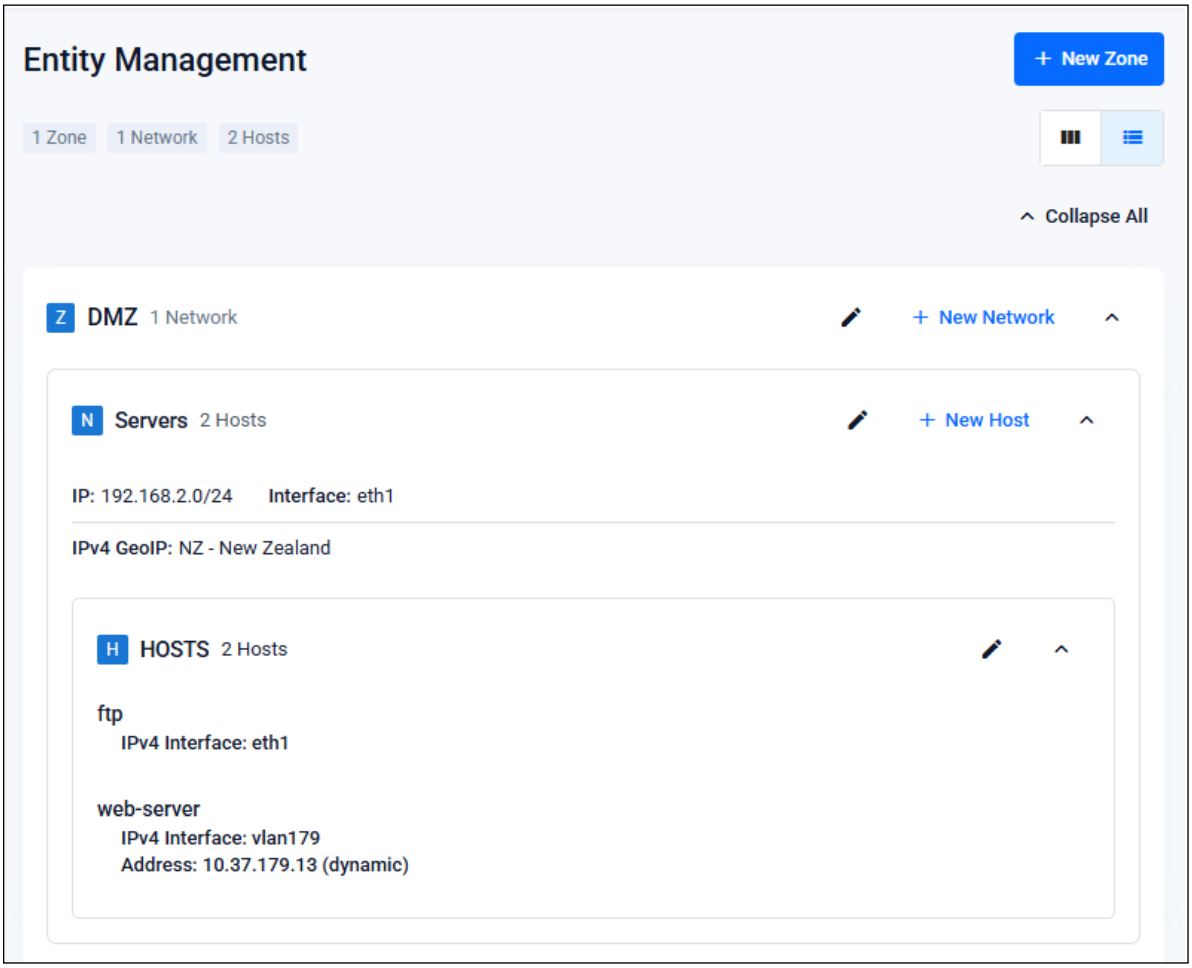


- Add a second host named **web-server** with an IP address, and save it

  The DMZ zone now contains a network named **servers** with two hosts:

  - web-server
  - ftp

.



- Repeat the same steps to create private and public zones/networks with the following details:

  Private zone:

  - Zone name = private
  - Network name = lan
  - Network subnet and interface = (IP address), VLAN1

  Or, for a 10GbE UTM Firewall and AR4000S-Cloud:

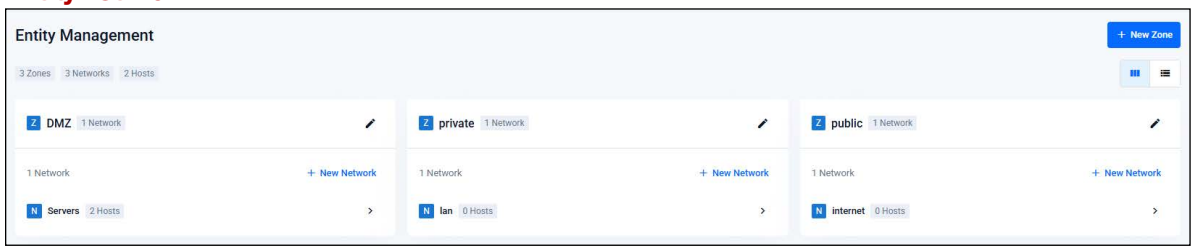
  - Network subnet and interface = (IP address), eth3

  Public zone:

  - Zone name = public
  - Network name = internet
  - Network subnet and interface = 0.0.0.0/0, eth2

The **Entity Management** page now contains a 3-zone network.

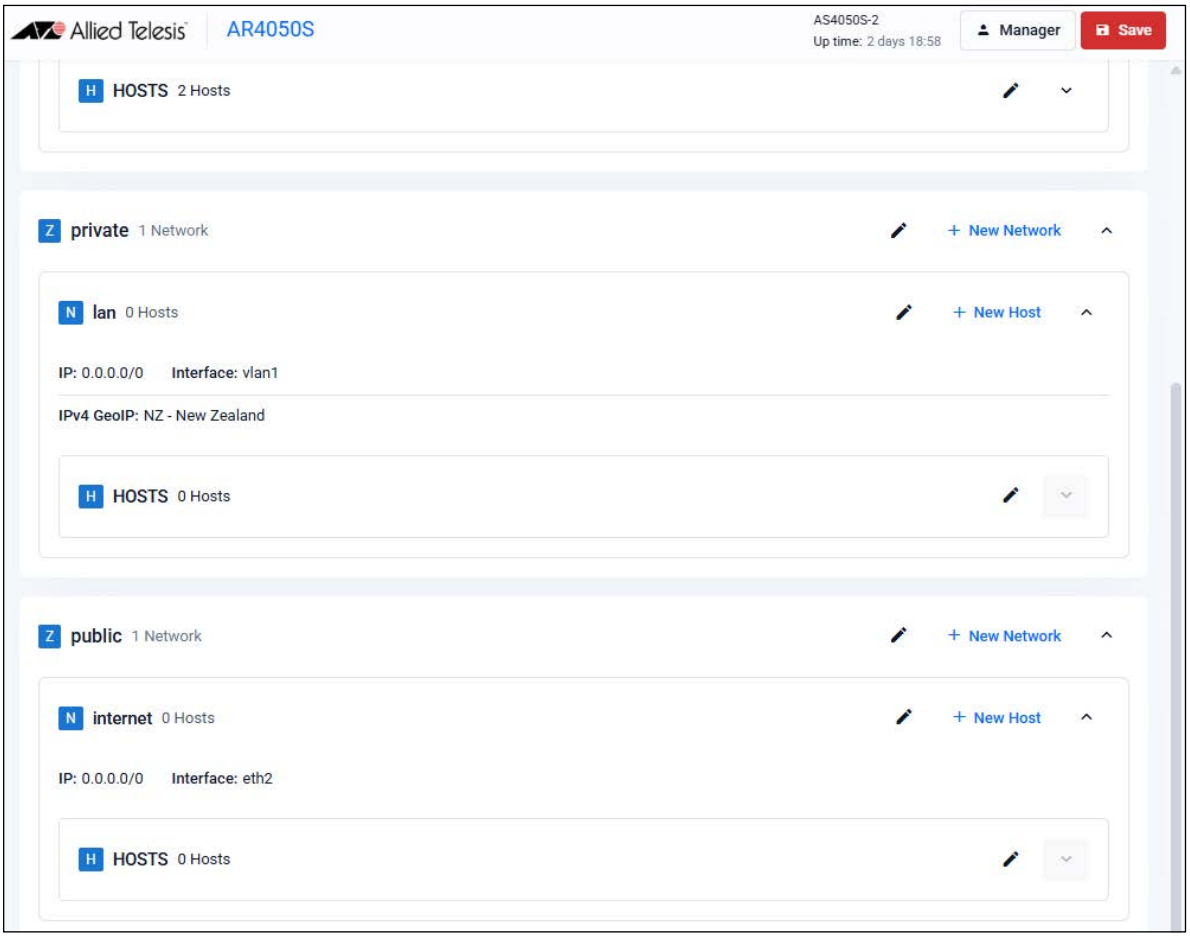
Entity list view



To view and manage entities in list view, click on the list icon on the right side of the page.

The list view is a good option for an overall entity view. Click **Expand All** (on the right side of the page) to display all entities and their interfaces, IP addresses, and so on.

.



If you'd like to view changes as added to the firewall configuration file:

- Select **CLI** under the **System** menu. This opens a CLI tab
- Type **ena** to access Privileged Exec mode, then use the CLI commands:

show running-config entity and **show entity**.

```
AlliedWare Plus (TM) 5.4.6 11/10/16 03:51:21

awplus>ena
awplus#show running-config entity
zone dmz
 network servers
  ip subnet 172.16.0.0/24 interface Eth1
  host ftp
   ip address 172.16.0.2
  host web-server
   ip address 172.16.0.10
!
zone private
 network LAN
  ip subnet 192.168.1.0/24 interface VLAN1
!
zone public
 network Internet
  ip subnet 0.0.0.0/0 interface Eth2
!
awplus#
awplus#show entity
Zone:         dmz
 Network:     dmz.servers
  Subnet:     172.16.0.0/24 via Eth1
  Host:       dmz.servers.ftp
   Address:   172.16.0.2
  Host:       dmz.servers.web-server
   Address:   172.16.0.10

Zone:         private
 Network:     private.LAN
  Subnet:     192.168.1.0/24 via VLAN1

Zone:         public
 Network:     public.Internet
  Subnet:     0.0.0.0/0 via Eth2

awplus#
```

Note the syntax that is used for identifying a network or host entity.

The syntax for naming a **network** entity is:

```
<Parent Zone Name>.<network name>
```

- For example, `private.LAN`

The syntax for identifying a **host** entity is:

```
<Parent Zone name>.<Parent Network Name>.<Host Name>
```

- For example, `dmz.servers.ftp`

So, the hierarchy is included in the identifier of a second-tier or bottom-tier entity.

- For example, **dmz.servers.web-server** indicates that this host named **web-server** is part of the **servers** network within the **dmz** domain.

Step 5: **Configure firewall rules**

We now have a 3-zone network (Public, Private, and DMZ), so next let's configure the firewall rules to manage the traffic between these entities.

- Go to **Security** > **Firewall**

WARNING: Don't enable the firewall yet. Enabling the firewall with the **Enabled/Disabled** switch will block all applications between all entities by default - no traffic will flow. It is therefore

important to create firewall rules to allow application usage as desired **prior** to enabling the firewall.

- Click **+ New Rule** and create a rule to allow **Ping** traffic from the Public zone to the Private zone. This will allow us to test connectivity through the firewall.

Note: To select an application, simply start typing in the application field. Available options will be filtered down until you select the desired application.

- You can see the new rule added to the firewall:

Create further new firewall rules with these details:

Further Ping rules to allow connectivity checking:

- Permit Ping from Public to DMZ
- Permit Ping from Private to DMZ
- Permit Ping from DMZ to Private

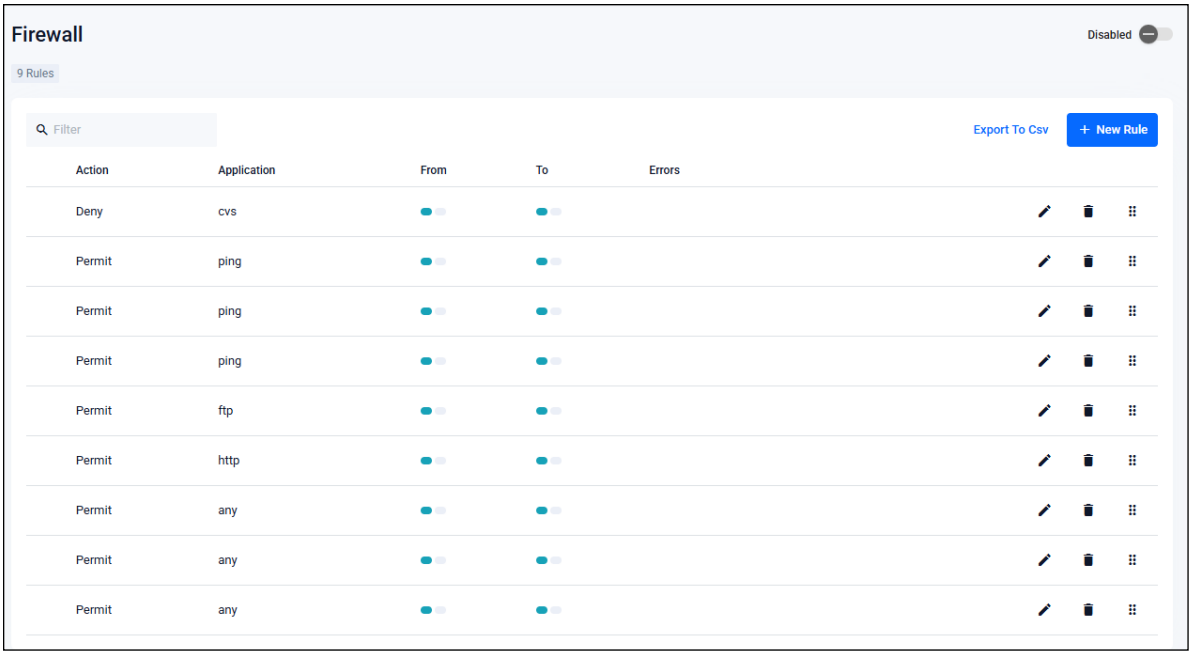
Allow public traffic from the Internet to our DMZ servers:

- Permit ftp from Public to dmz/servers/ftp
- Permit http from Public to dmz/servers/web-server

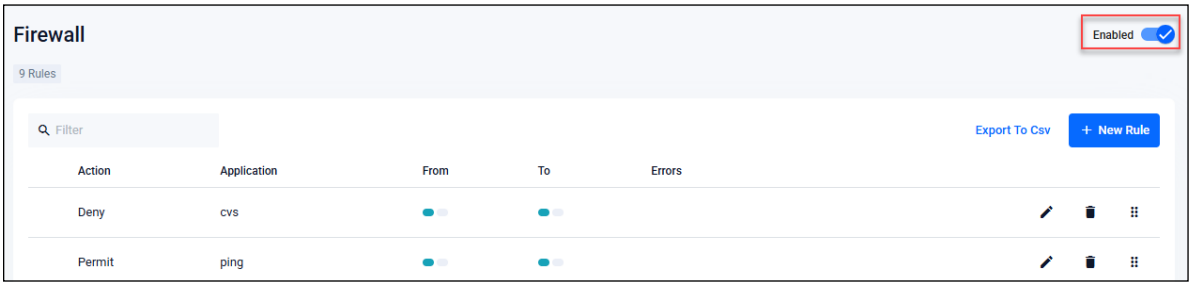
Allow private side firewall zones to initiate traffic flows with each other and out to the Internet:

- Permit Any from Private to Private
- Permit Any from DMZ to DMZ
- Permit Any from Private to Public
- Permit Any from DMZ to Public

We can now see these firewall rules displayed:

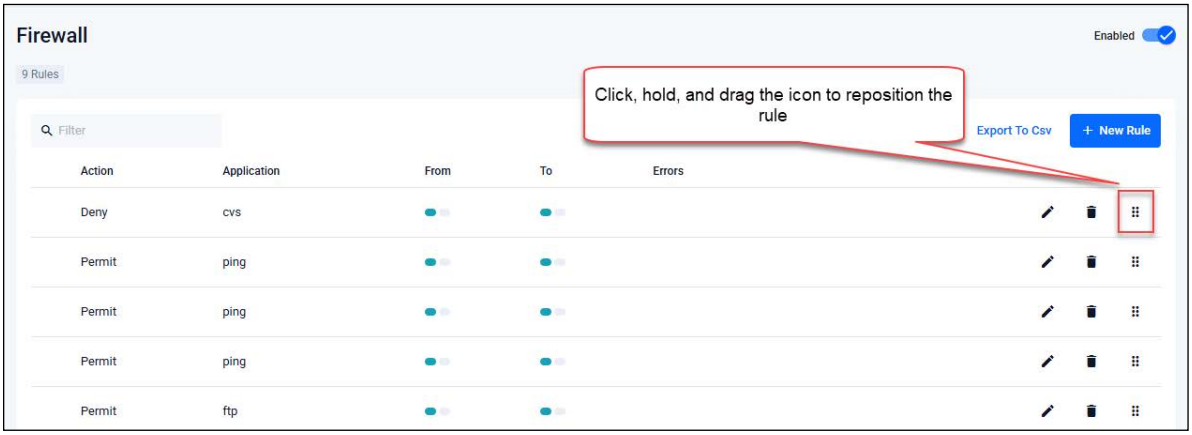


- Now that the firewall rules are created, you can turn the firewall on using the button at the top right of the Firewall page.



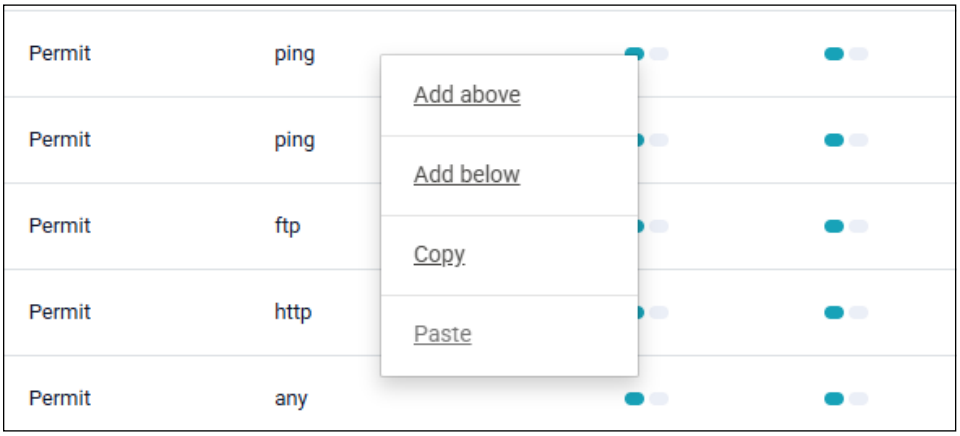
Firewall rule placement

The firewall rules are displayed in the order they were created, which is also the order in which they will be actioned by the firewall. If you need to change the order of any specific rule, click and drag it into a new position.



There are two other options for placing new rules:

- **Right-click** on any firewall rule and the menu gives you the option to create a new rule above or below that rule. This allows new rules to be immediately placed in the desired location, and order of processing.
- The **right-click** menu also has a copy-and-paste function, so you can copy an existing rule that is similar to the new rule you wish to create, and paste it into a different location. It can then be edited to suit.



These right-click options are very useful when you have a large number of firewall rules. The same right-click options are also available when creating new NAT and Traffic Control rules.

If you'd like to see the updated firewall configuration, use the CLI window and the commands: **show firewall rule**, **show running-config firewall** and **show firewall**.

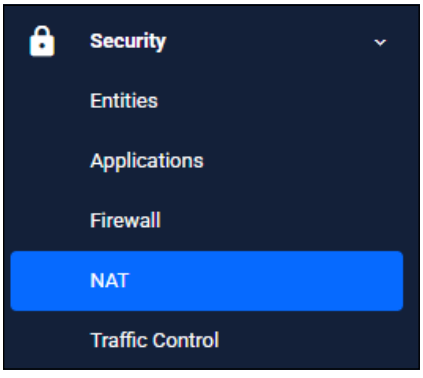
```
AlliedWare Plus (TM) 5.4.6 11/10/16 03:51:21

awplus>ena
awplus#show firewall rule

[* = Rule is not valid - see "show firewall rule config-check"]
  ID     Action  App        From                To                  Hits
-------------------------------------------------------------------------------
* 10     permit  ping       public              private             0
* 20     permit  ping       public              dmz                 0
* 30     permit  ping       private             dmz                 0
* 40     permit  ping       dmz                 private             0
* 50     permit  ftp        public              dmz.servers.ftp     0
* 60     permit  http       public              dmz.servers.web-server
                                                                    0
* 70     permit  any        private             private             0
* 80     permit  any        dmz                 dmz                 0
* 90     permit  any        private             public              0
* 100    permit  any        dmz                 public              0
awplus#
awplus#show running-config firewall
firewall
 rule 10 permit ping from public to private log
 rule 20 permit ping from public to dmz log
 rule 30 permit ping from private to dmz log
 rule 40 permit ping from dmz to private log
 rule 50 permit ftp from public to dmz.servers.ftp log
 rule 60 permit http from public to dmz.servers.web-server log
 rule 70 permit any from private to private log
 rule 80 permit any from dmz to dmz log
 rule 90 permit any from private to public log
 rule 100 permit any from dmz to public log
!
awplus#
awplus#show firewall
Firewall protection is disabled
Active connections: 13
awplus#
```

Note that the firewall rules are numbered in the order in which they will be actioned (e.g. 10, 20, 30, and so on). If a rule is dragged to a different location in the list displayed by the GUI, the rules will be renumbered to reflect the change in order of operation.

Step 6: **Configure NAT rules**

Now let's configure NAT rules to manage IP address translation between the Internet and our internal networks.

- Go to **Security** > **NAT**

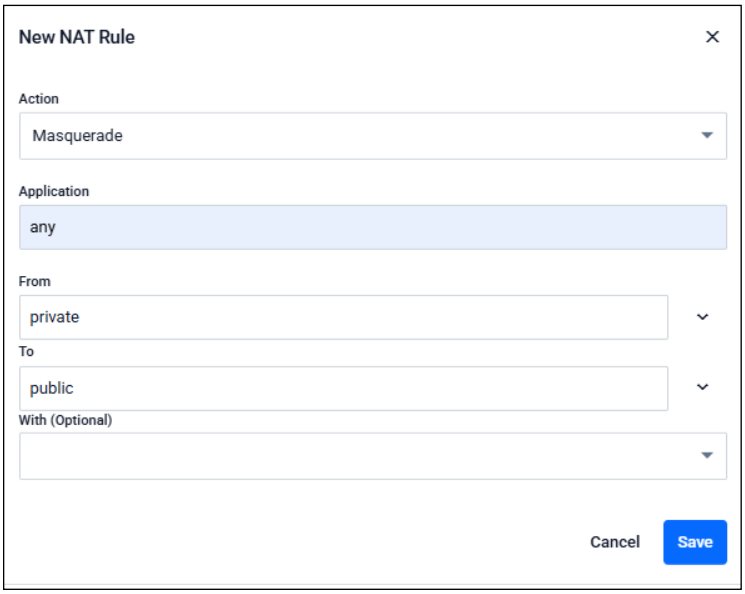


We need two NAT masquerade rules for private to public address translation, which are:

- Any traffic going from the Private zone out to the Public zone will have NAT applied, so that it appears to have come from the IP address of the eth2 interface.
- Any traffic going from the DMZ zone out to the Public zone will have NAT applied, so that it appears to have come from the IP address of the eth2 interface.

Click **+ New Rule** to create the first rule for Private to Public traffic:

- Action = Masquerade
- Application = any
- From = Private
- To = public



Click **+ New Rule** again and create the second NAT masquerade rule in the same way for DMZ to Public traffic with these details:

- Action = Masquerade, Application = any, From = DMZ, To = public

We now need to create two NAT port-forwarding rules to enable access to the FTP and Web servers to be delivered to the right destinations. To users in the Public zone, both servers will appear to have

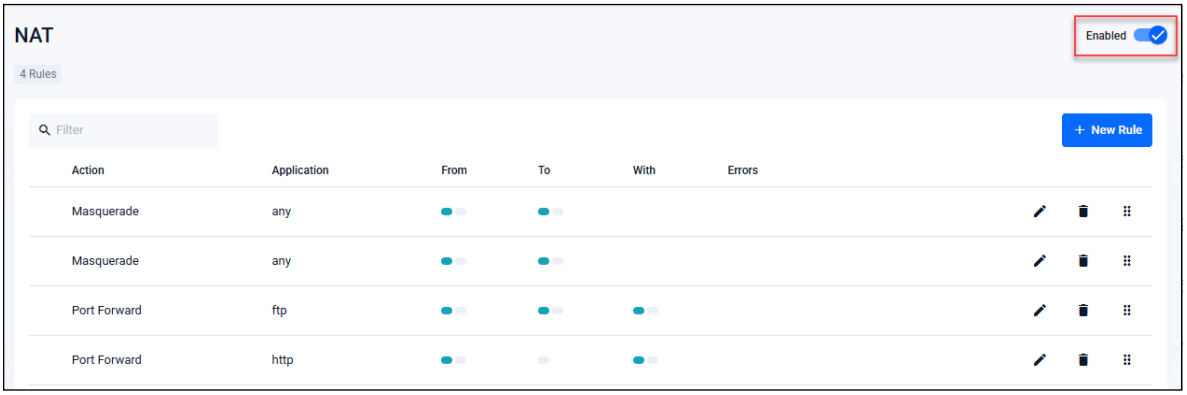
the IP address that is on the eth2 interface, so sessions towards those servers will be initiated to that address. The firewall must then forward those sessions to the actual addresses of the servers.

Click **+ New Rule** and create the two NAT port-forward rules with the following details:

- Action = Port Forward, Application = ftp, From = public, With = dmz/servers/ftp
- Action = Port Forward, Application = http, From = public, With = dmz/servers/web-server

Now, click the **Enable/Disable** button at the top right of the Dashboard page to enable NAT.

You can see the four new NAT rules:



Open the CLI window to see these new NAT rules. Enter the command **show nat rule**.

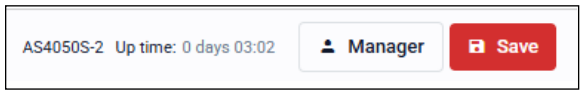
```
AlliedWare Plus (TM) 5.4.6 11/10/16 03:51:21

awplus>ena
awplus#show nat rule

[* = Rule is not valid - see "show nat rule config-check"]
-------------------------------------------------------------------------------
  ID     Action      From                  With (dst/src) Entity   Hits
         App         To                    With dport
-------------------------------------------------------------------------------
* 10     masq        private               -                       0
         any         public                -
* 20     masq        dmz                   -                       0
         any         public                -
* 30     portfwd     public                dmz.servers.web-server  0
         ftp         -                     -
* 40     portfwd     public                dmz.servers.web-server  0
         http        -                     -
awplus#
```

Step 7: **Save configuration changes**

The configuration we have made so far is part of the **running-configuration** on the firewall.

Save these configuration changes to make them part of the boot configuration, so they can be backed up and will survive a reboot of the firewall.

- Click the **Save** button at the top right of the GUI screen. The **Save** button will be orange anytime there is unsaved configuration.



Part 2: Configure the firewall for Update Manager

Modern security devices require regular updates to keep rule-sets and threat signature databases up to date, ensuring effective protection for business networks. Features such as IP Reputation, Malware Protection, and Antivirus (which we'll configure in parts 5 and 6), monitor network traffic and detect malicious activity in real-time by comparing the threats' characteristics and patterns against known lists and databases.

The leading third-party security providers employed by the firewall keep their databases regularly updated with the very latest **threat signatures**, so security scanning of firewall traffic catches the latest malicious threats. The firewall utilizes **Update Manager** to contact the Allied Telesis update server and download the latest components at pre-defined intervals, or at specific user request.

You must configure entities and rules to allow connectivity between Update Manager and the Update Server.

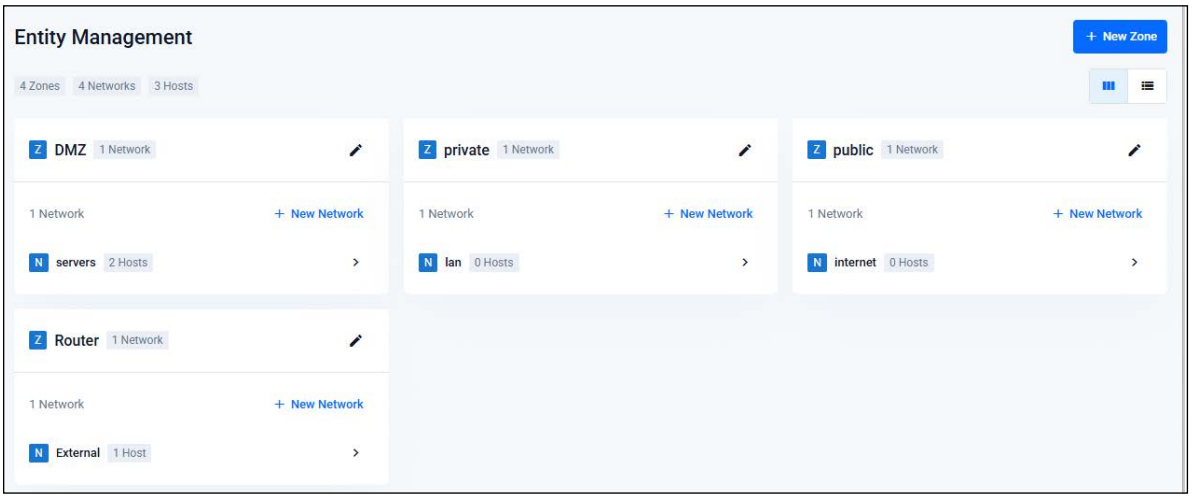
Step 1: **Create appropriate entities**

Update Manager retrieves files using sessions initiated from the firewall unit itself. This means that firewall rules are required that permit these sessions. So, a zone needs to be created that represents the firewall itself, and the public interface of the firewall has to exist as a host within this zone.

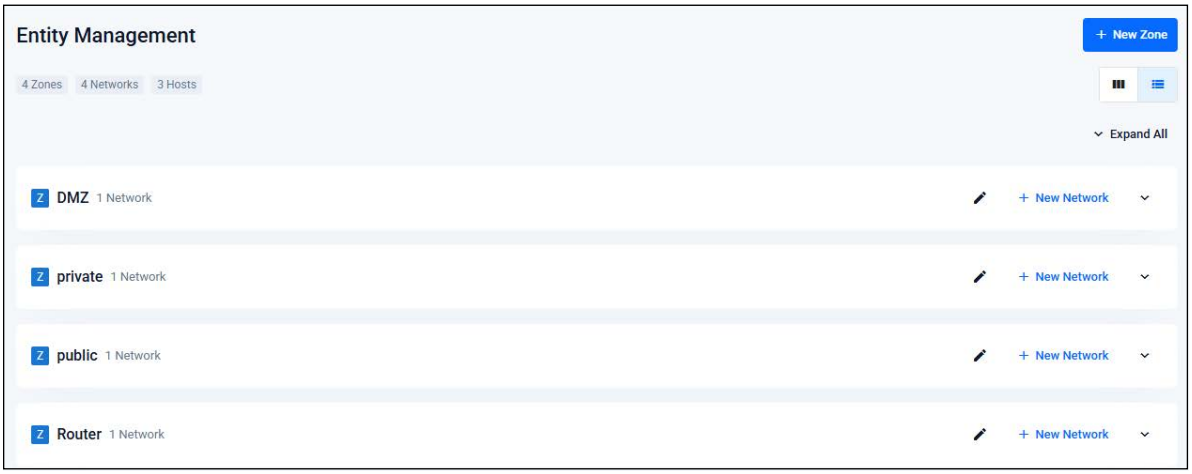
Create zone/network/host entities for Update Manager source traffic with the following details:

- Zone name = Router
- Network name = External
- Network subnet and interface = 192.168.52.0/24, Eth2
- Host name = External_Int
- Host IP address = 192.168.52.20

The updated **Entity Management** page looks like this:



Or in **List View** (with just the new zone expanded) like this:

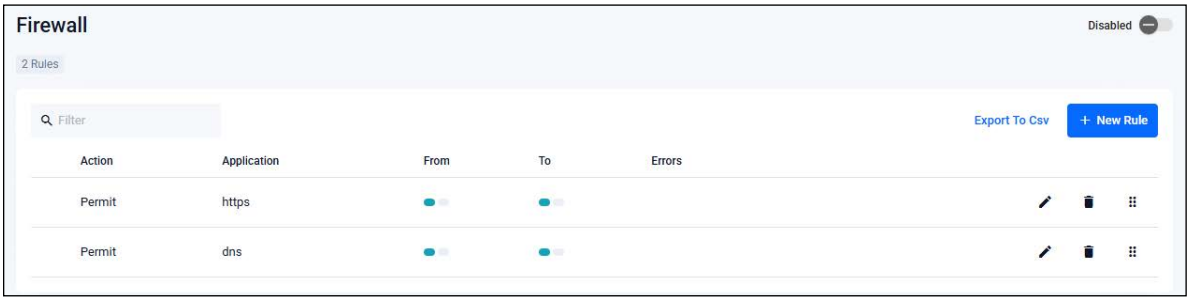


Step 2: **Create firewall rules for the Update Manager traffic**

The Update Manager uses HTTPS for secure connectivity, so we'll create a firewall rule with the following details to allow HTTPS traffic out to the update server.

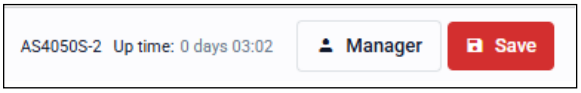
Also create a rule to allow DNS resolution of the update server's URL.

These new rules can be seen added to the firewall rule set.



Step 3: **Save configuration changes**

Once again click the **Save** button on the GUI top bar to save the Update Manager configuration to the boot configuration file.



Part 3: Configure free security features

Allied Telesis firewalls have a number of security features that can be configured to manage application and website usage, as well as provide comprehensive threat protection.

This section explains configuring the following free security features:

- Intrusion Prevention System (IPS), and
- Custom URL Filtering.

Parts 4 and 5 of this guide includes configures licensed firewall and threat protection features:

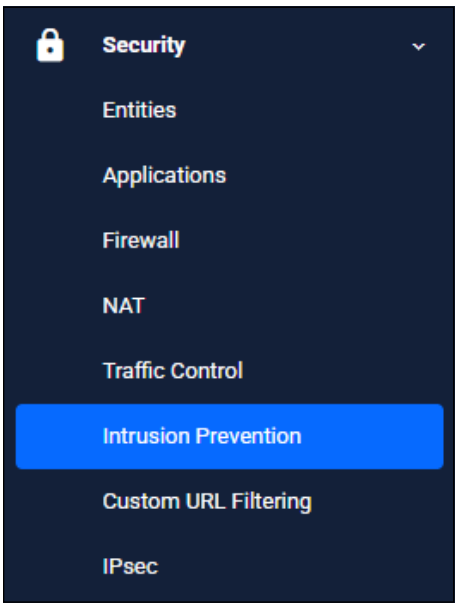
- "Part 4: Configure licensed Advanced Firewall security features"
- "Part 5: Configure licensed Advanced Threat Protection (ATP) security features"

Enable and configure Intrusion Prevention System (IPS) actions

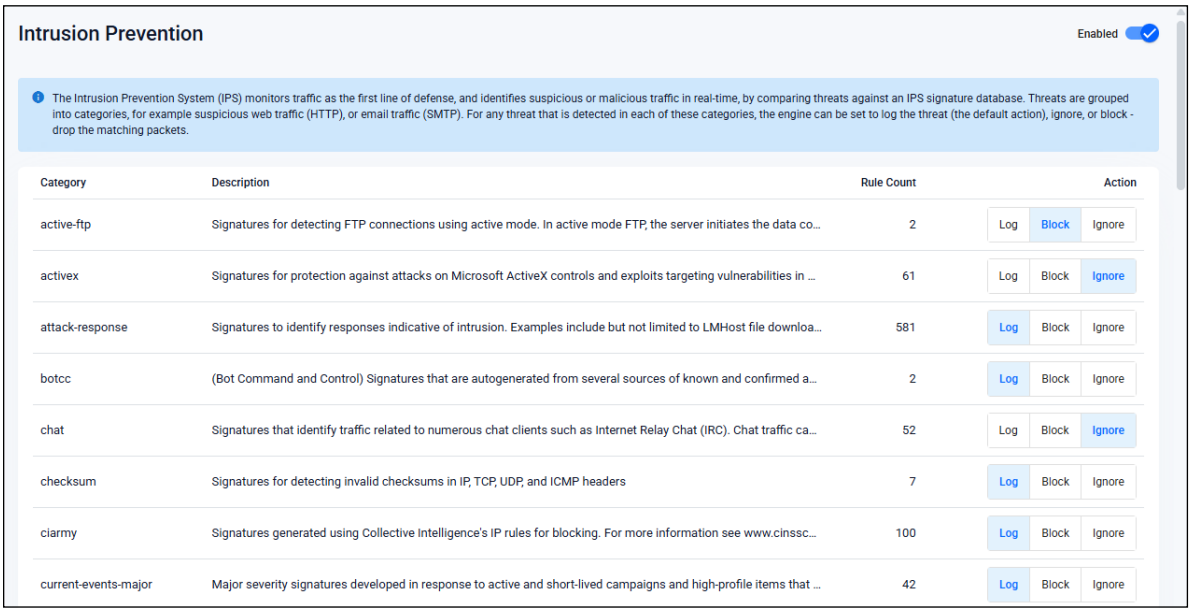
IPS monitors inbound and outbound traffic as the first line of defense, and identifies suspicious or malicious traffic in real-time by comparing threats against an IPS known signature database.

Step 1: **Enable IPS**

Go to **Security** > **Intrusion Prevention**



- Click the **Enabled/Disabled** switch on the top right of the page to enable IPS.

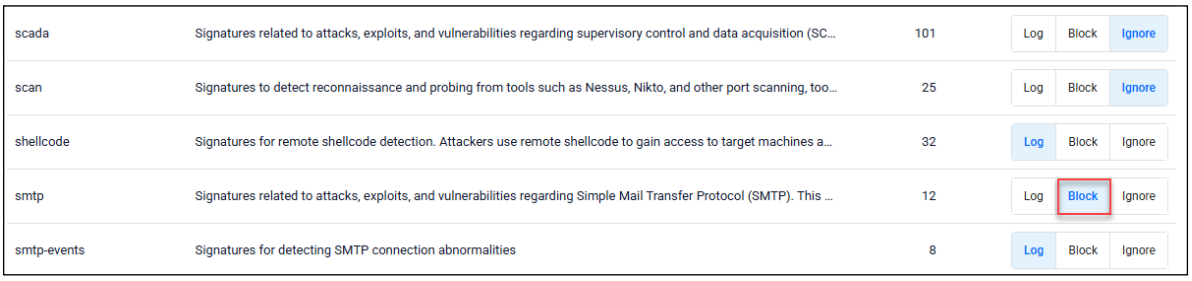


Note: You may have to refresh the page to see the IPS toggles.

Step 2: **Configure IPS actions**

Threats are grouped into categories, for example suspicious web traffic (HTTP), or email traffic (SMTP). For any threat that is detected in each of these categories, the engine can be set to log the threat (which is the default action), ignore, or block - drop the matching packets.

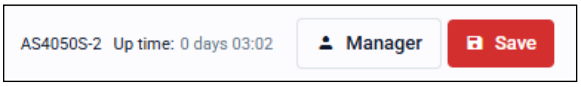
To drop suspicious SMTP traffic, set the action to **Block**.



Note: You can monitor IPS matches using the Dashboard's security monitoring widget.

Step 3: **Save configuration changes**

Save the IPS configuration changes to make them part of the boot configuration file.



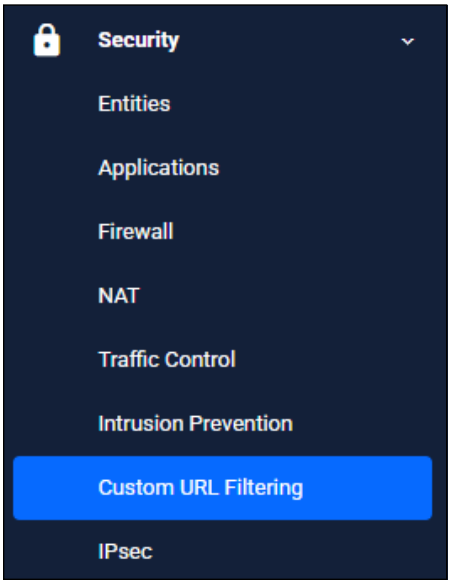
Custom URL Filtering

URL Filtering is a fast efficient (stream-based) method to allow or block employee's website access. You can specify a user-defined list of websites to allow (whitelist) and/or block (blacklist) on the free-to-use Custom URL Filtering page.

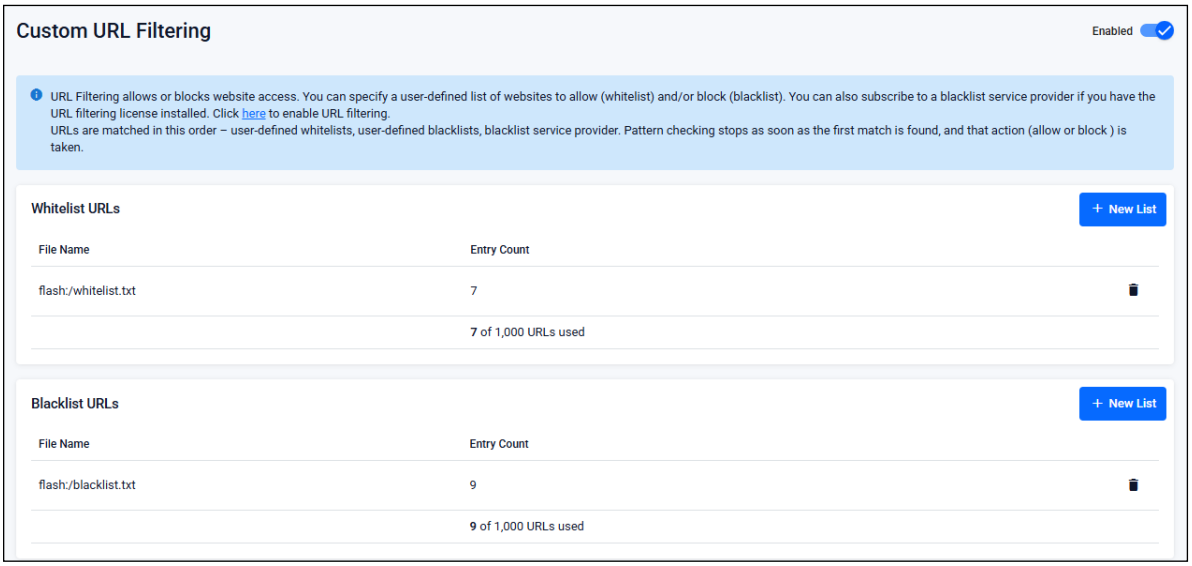
URLs are matched in this order – user-defined whitelists then user-defined backlists. Pattern checking stops as soon as the first match is found, and that action (allow or block) is taken. If no match is found, website access will be allowed.

Step 1: **Configure custom URL filtering**

- Go to **Security** > **Custom URL Filtering**



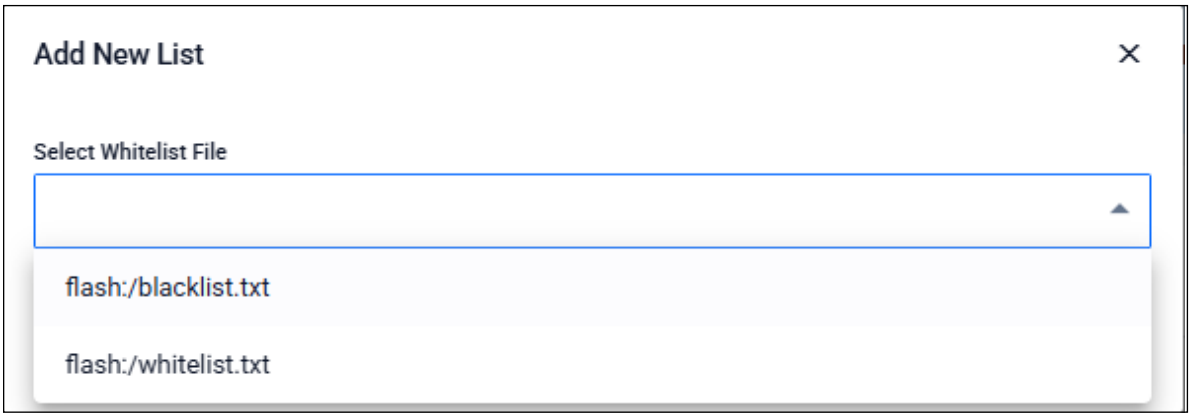
You can add user-defined whitelists of URLs to allow, and/or blacklists of URLs to block. You can add multiple lists, and these can have a total maximum of 1000 whitelist URLs and 1000 blacklist URLs. The GUI page lets you know how many URLs are in each list and the total URLs used.



Click on the **+New list** button to add a new whitelist or blacklist.

The custom URL list must be a text file (.txt). All of your '.txt' files in flash, USB, or SD card are shown. You can select and save them for the Custom URL Filtering feature to use.

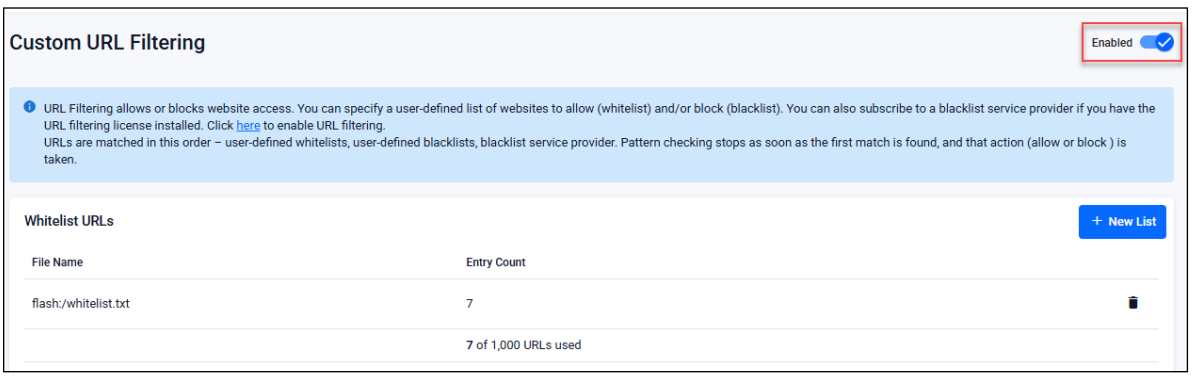
See the URL Filtering Feature Overview Guide for more information about creating user-defined URL Filtering lists.



- Any whitelists and blacklists that have been selected are now shown on the Custom URL Filtering page, with the entry count showing the number of URLs used:

Step 2: **Enable URL Filtering**

- Enable URL Filtering with the **Enable/Disable** switch at the top of the page:

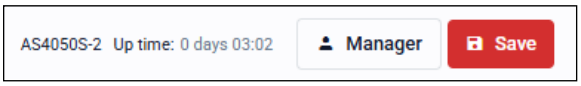


The firewall will now match any website URLs that users try to browse to against the provider's whitelist/s, then the blacklist/s. Pattern checking stops as soon as the first match is found, and that action (allow or block) is taken. If no match is found, website access will be allowed.

Note: You can monitor URL Filtering hits using the Dashboard's security monitoring widget.

Step 3: **Save configuration changes**

Save your Custom URL Filtering changes to make them part of the boot configuration.



Part 4: Configure licensed Advanced Firewall security features

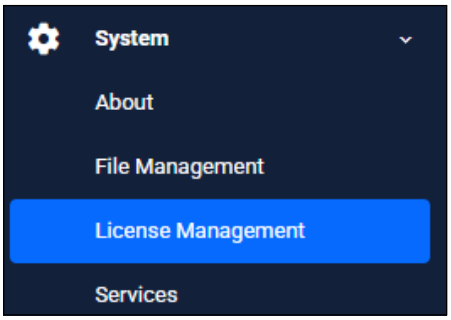
Online business activity is now based around applications that enable people to interact with services such as collaborative document creation, social networking, video conferencing, cloud-based storage, and much more. Organizations need to be able to control the applications that their people use, and how they use them, as well as managing website traffic.

Allied Telesis firewalls are application aware, and so provide the visibility and control necessary to safely navigate the increase in online applications and web traffic that are used for effective business today.

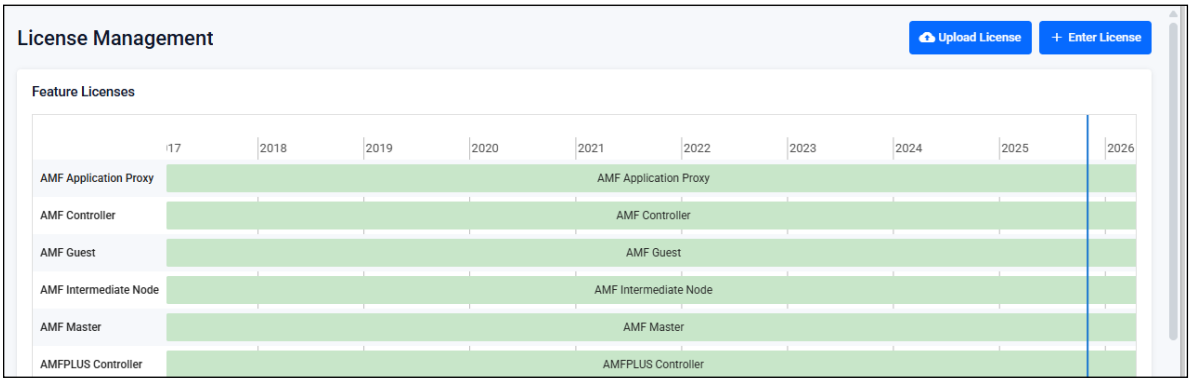
The **Advanced Firewall Security license** includes **Application Control** and **Web Control**, and is available in 1, 3, and 5 year subscriptions. For information on licensing for your device, see the product's Datasheet.

You can view current license status on your device by navigating to the **System** > **License Management** page. For more information about license management in the Device GUI, refer to "License management" on page 81.

- Go to **System** > **License Management**



The License Management page is displayed:

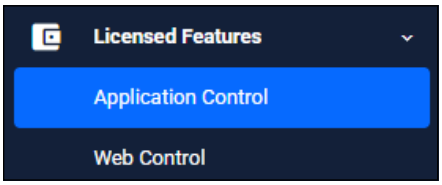


Application Control

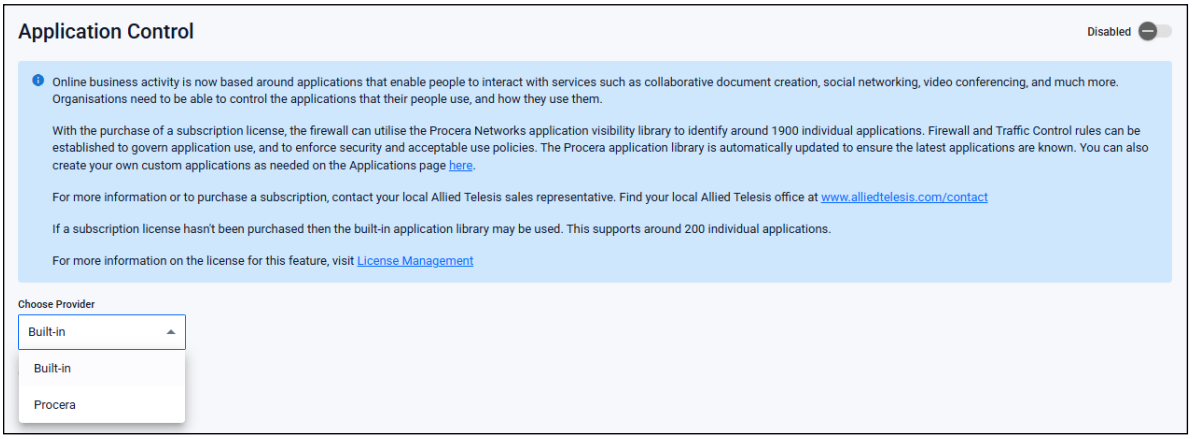
The Deep Packet Inspection (DPI) firewall engine allows fine-grained application control. Reliable identification of the individual applications means that rules can be established to govern application use, and to enforce security and acceptable use policies. For example, Skype chat may be allowed company wide, while Skype video calls can only be made by the sales department.

Step 1: Configuring application control

Go to **Licensed Features** > **Application Control**



1. Click the **Enabled/Disabled** switch to enable Application Control.
2. Choose a **Provider** to ensure the latest applications are known.



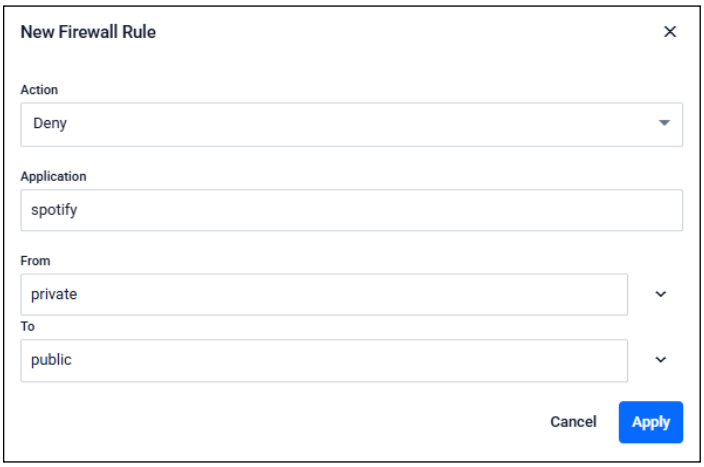
The provider options are:

- **Built-in** - if a subscription license hasn't been purchased then the built-in application library may be used. This supports around 200 individual applications.
- **Procera** - the Procera Networks application visibility library identifies around 1400 individual applications. The firewall will update the library from the Allied Telesis update server at the specified interval to ensure the latest applications are known.

Step 2: Add rules to manage applications

You can now create firewall or traffic shaping rules to manage how applications are allowed to be used on the network. Add rules from the **Security** > **Firewall** menu.

For example, to block the use of Spotify™ (a music streaming service) company-wide, create a firewall rule denying the Spotify application from the Public (Internet) zone to the Private (LAN) zone.

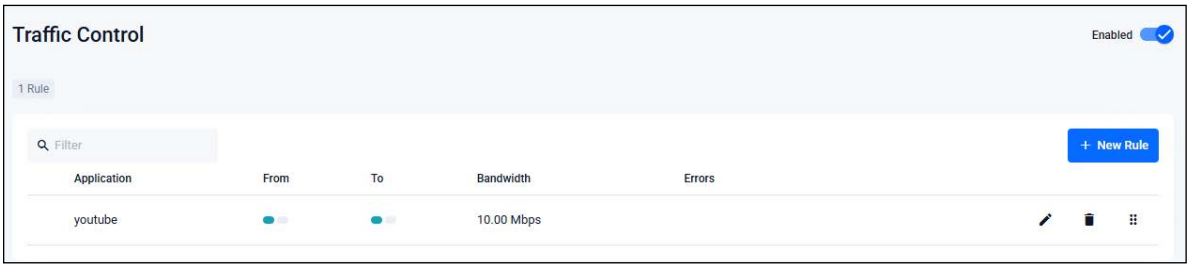


Step 3: **Add rules to manage application bandwidth**

As well as using the firewall to block undesired traffic, you can also use the **Traffic Control** page to manage the bandwidth that certain applications are able to use on the firewall.

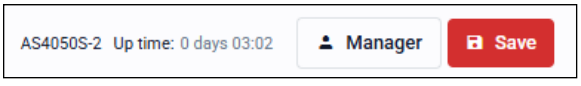
For example, to limit Youtube traffic through the firewall to 10Mbps, go to the **Traffic Control** page and add a new rule from the Public (Internet) zone to the Private (LAN) zone.

You can see the new Traffic Control rule applied with a bandwidth limit of 10Mbps for the application **youtube**.



Step 4: **Save configuration changes**

Save the Application Control configuration changes to make them part of the boot configuration.



Web Control

Note: As well as Web Control, the UTM firewalls also support Web Categorization, which is a more flexible solution and can be configured using the firewall's CLI. See the Advanced Network Protection Feature Overview and Configuration Guide for details.

Web Control provides enterprises with an easy means to monitor and control their employees' web traffic for productivity, legal, and security purposes. The Web Control feature uses the following providers:

- OpenText
- and Digital Arts

Choose a provider for active rating systems for comprehensive and dynamic URL coverage. Websites are accurately assigned to around 100 categories, which can be allowed or blocked.

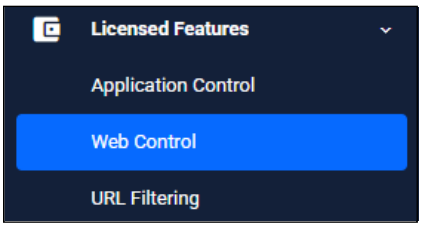
When a user tries to browse to a website, the http request is intercepted and sent to the classifier engine, which queries the provider's constantly updated URL database for the category that the website belongs to.

From software version 5.5.4-1.x onwards, Web Control utilizes Deep Packet Inspection.

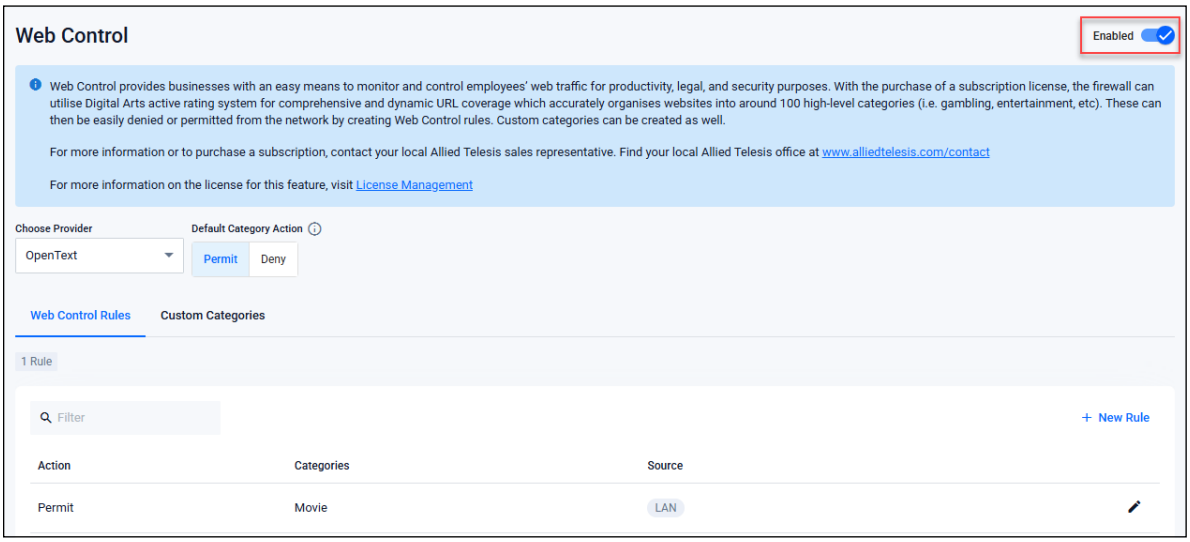
Once a particular URL has been categorized, the result is cached in the firewall so that any subsequent requests with the same URL can be immediately processed.

Step 1: **Configure Web Control**

- Go to **Licensed Features** > **Web Control**



- Click on the **Enabled/Disabled** switch to enable **Web Control**.
- Choose a provider (Digital Arts or OpenText).
- Select the **Default Action** - deny or permit, for web pages that do not match any specific rules, but match a Web Control category.



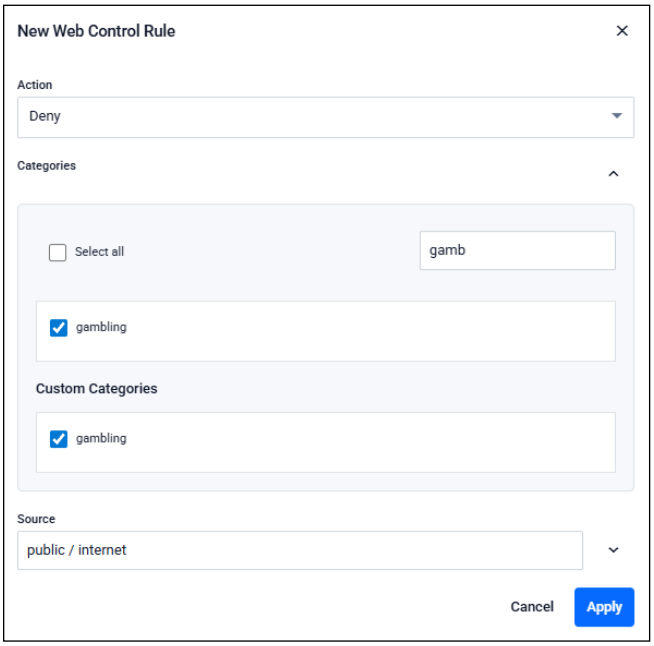
Note: You can monitor URL Filtering and Web Control hits using the Dashboard's security monitoring widget.

Step 2: **Add rules to manage website categories**

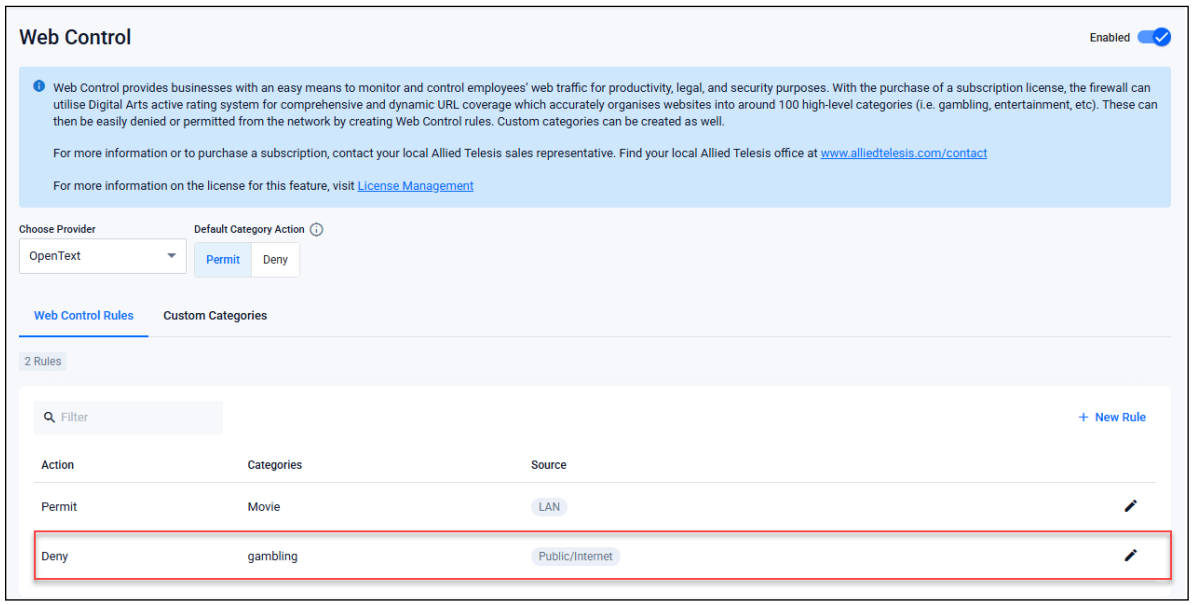
The Web Control feature has its own set of rules, which are separate to the firewall rules. The Web Control rules are created on the Web Control configuration page.

For example, to block gambling websites, create a rule that applies to the Internet network.

- Click **+ New Rule**



You can see the new rule applied to the Internet network in the Public zone:

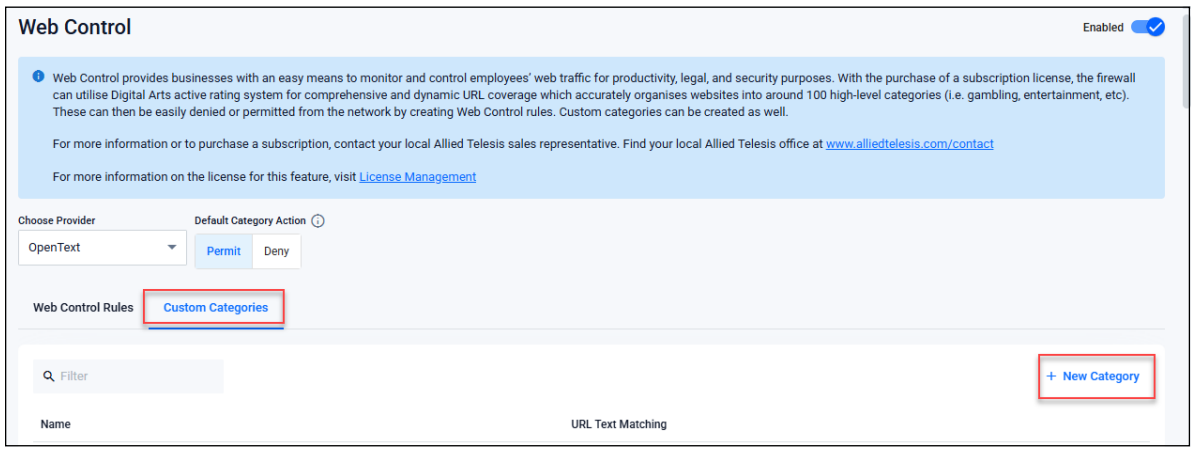


Step 3: **Create custom categories**

As well as using the predefined website categories, you can also create your own custom categories which match text strings you enter against website URLs. These custom categories can then have rules applied (as we did for gambling websites above).

For example, to create a custom 'Movie' category which contains the IMDB and Rotten Tomatoes websites:

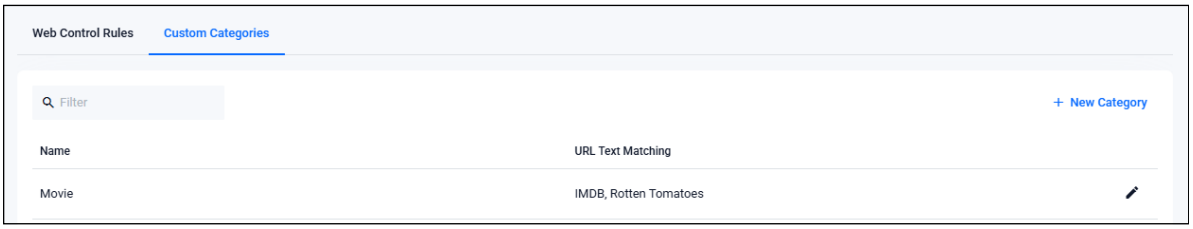
1. Go to the **Custom Categories** tab
2. Click the **+ New Category** button



3. Create a new 'Movie' category, and add text string matches for any website addresses containing IMDB or Rotten Tomatoes.

4. Click **Apply**

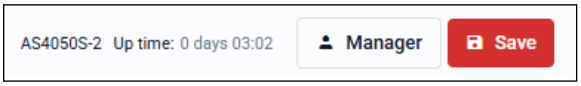
You can see the new category and its website matches below:



Use the Web Control Rules tab to add more rules for this category as desired.

Step 4: **Save configuration changes**

Save the Web Control configuration changes to make them part of the boot configuration file.



Note: You can monitor category and rule hits using the Dashboard's security monitoring widget.

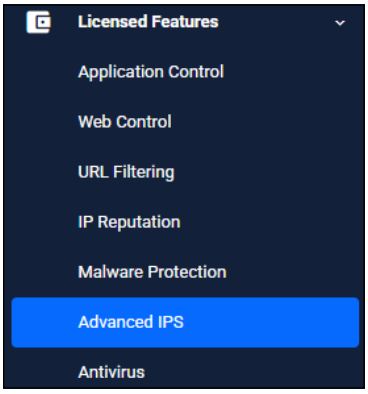
Part 5: Configure licensed Advanced Threat Protection (ATP) security features

Application use provides businesses with increased efficiency and improved collaboration, along with new ways to manage customer interaction. However, it has also opened the door for greater security concerns. Business data is potentially vulnerable, and the rapid development of new services and technologies have introduced new types of cyber threats. Allied Telesis firewalls provide comprehensive threat protection, utilizing security engines and threat signature databases from the industry's leading vendors for implementation of a robust intrusion prevention system. The consistent monitoring ensures up-to-date protection against cyber attacks.

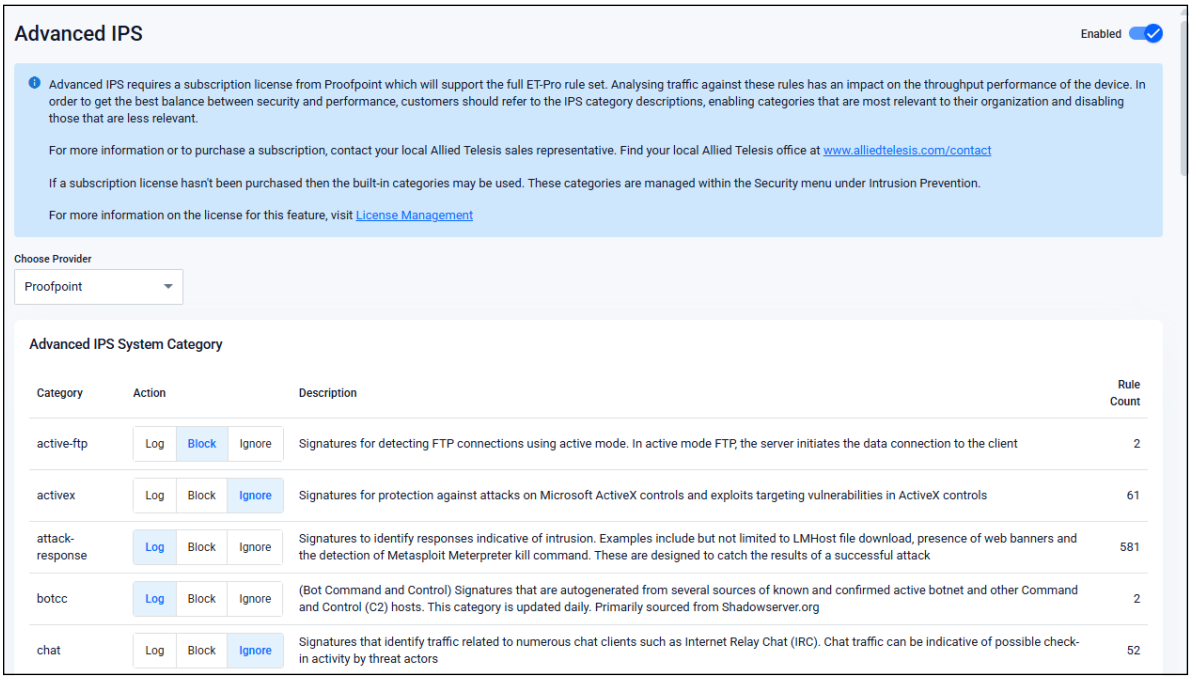
The **Advanced Threat Protection (ATP) license** enables **IP Reputation** and **Advanced IPS**, and is also available in 1, 3, and 5 year subscriptions. For information on licensing for your device, see the product's Datasheet. Both features enable realtime threat protection.

You can view current license status on your device by navigating to the **System** > **License** page. For more information about license management in the Device GUI, refer to "License management" on page 81.

- Go to **Licensed Features** > **Advanced IPS**



The **Advanced IPS** page is displayed:



Part 6: Advanced IPS

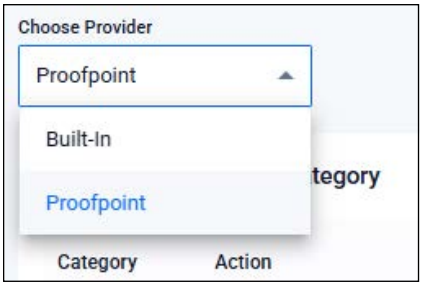
From version 5.5.2-2.2 onwards, AlliedWare Plus provides Advanced IPS (Intrusion Prevention System) functionality.

This is made possible by the addition of the third-party vendor Proofpoint's ET Pro Ruleset. The Proofpoint ET Pro Ruleset detects and blocks advanced threats. Updated daily, it covers malware delivery, command and control, attack spread, in-the-wild exploits and vulnerabilities, and credential phishing. It also detects and blocks distributed denial-of-service attacks (DDoS), protocol and application anomalies, exploit kits, and supervisory control and data acquisition (SCADA) attacks.

Advanced IPS requires a license, which is available in the bundle pack: AT-AR4-UTM-02-1/3/5YR. Contact your authorized Allied Telesis support center to obtain a license.

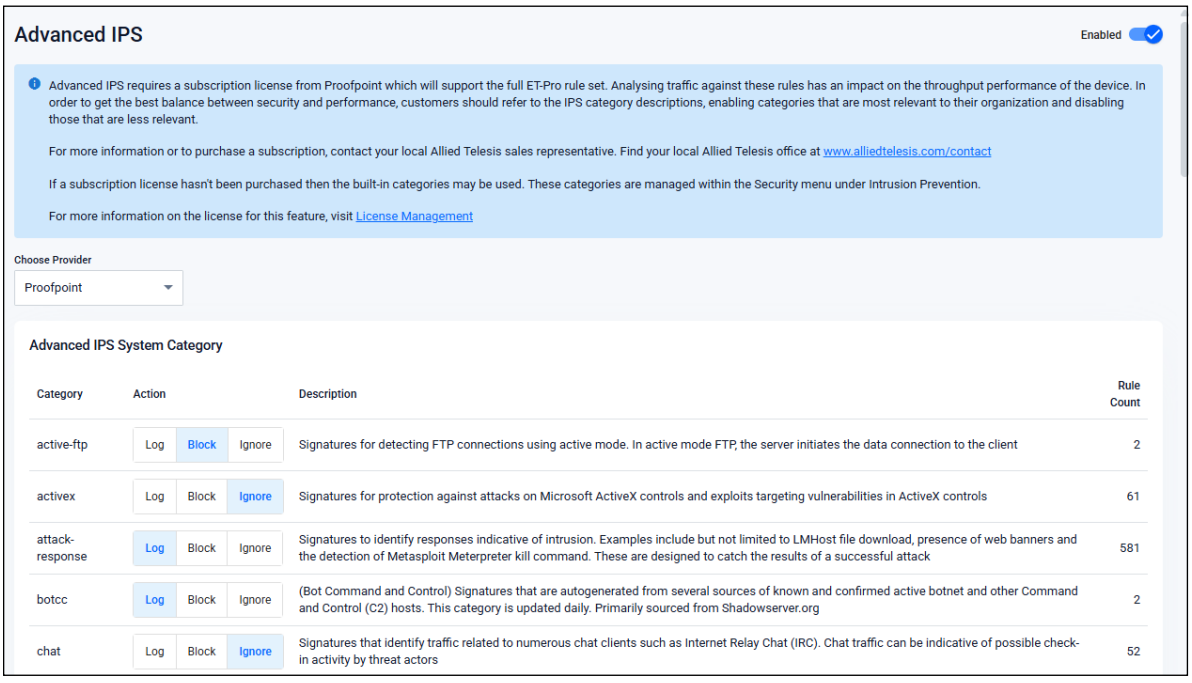
Step 1: **Enable Advanced IPS**

- Go to **Licensed Features** > **Advanced IPS**
- Click the **Enable/Disable** switch on the top right of the page to enable Advanced IPS
- From the drop-down, select the **Proofpoint** provider



Step 2: **Configure IPS actions**

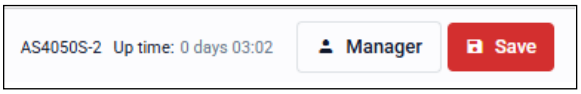
Threats are grouped into categories. For any threat that is detected in each of these categories, the engine can be set to log the threat (which is the default action), ignore, or block - drop the matching packets.



For example, to drop UDP decoder events, scroll down to the category and set the action to **Block**.

Step 3: **Save configuration changes**

Save the Advanced IPS configuration changes to make them part of the boot configuration file.

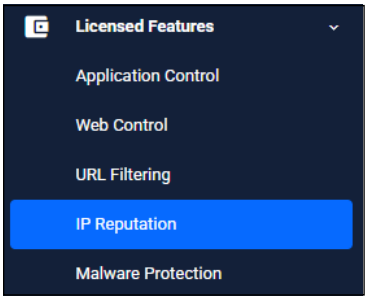


IP Reputation

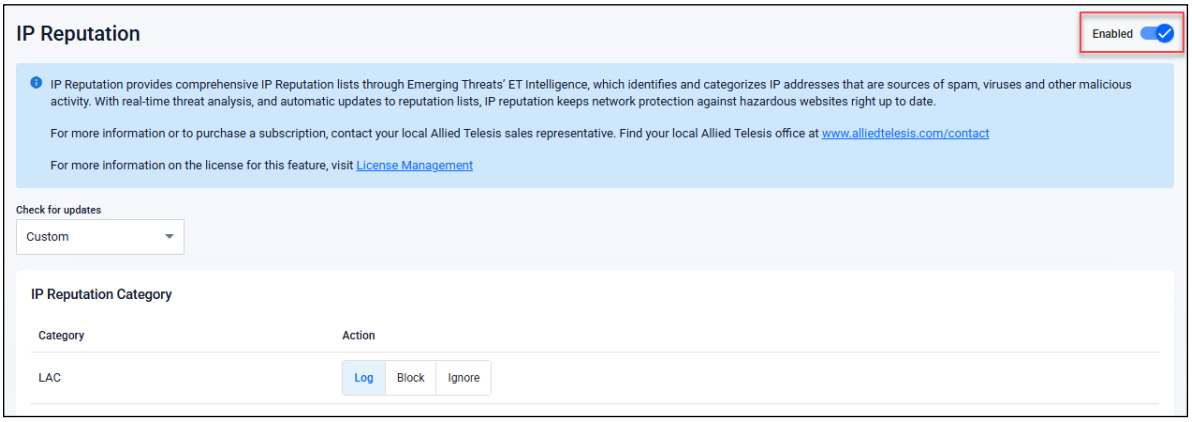
IP Reputation provides comprehensive IP reputation lists through Emerging Threat (ET) Intelligence™ (provided by Proofpoint™), which identifies and categorizes IP addresses that are sources of Spam, viruses and other malicious activity. With real-time threat analysis, and regular updates to reputation lists, IP Reputation keeps network protection against hazardous websites right up to date.

Step 1: **Enable IP Reputation**

- Go to **Licensed Features** > **IP Reputation**



- Click the **Enabled/Disabled** switch to enable IP Reputation
- Set an **Update interval** to contact the Update Server for IP Reputation list updates

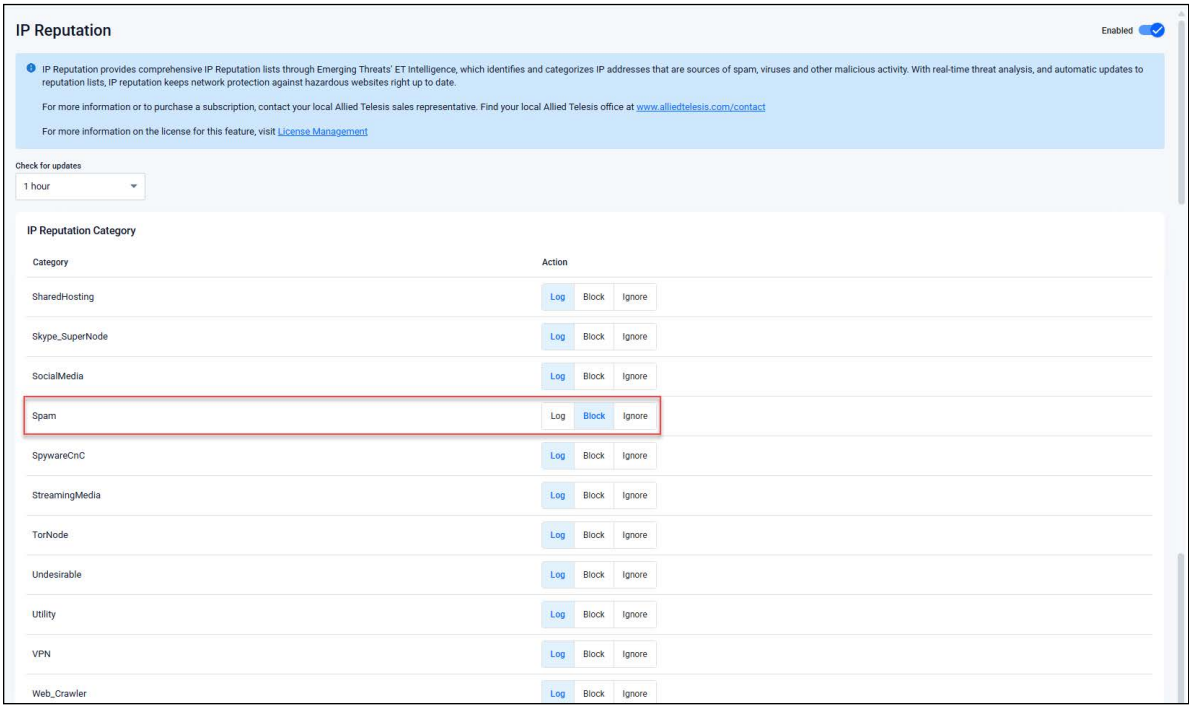


Step 2: **Configure IP Reputation categories**

IP Reputation uses categories to classify the nature of a host's bad reputation. For example, IP addresses known to be sources of Spam will be added to the **Spam** category.

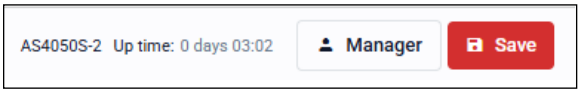
For any category, IP Reputation can be set to log the threat (which is the default action), ignore, or block/drop the matching packets.

To drop traffic from websites known as sources of Spam, set the **Spam** category to **Block**.



Step 3: **Save configuration changes**

Save the IP Reputation configuration changes to be part of the boot configuration file.

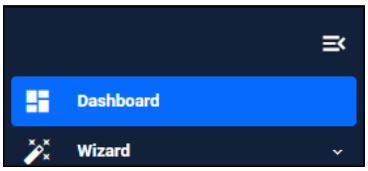


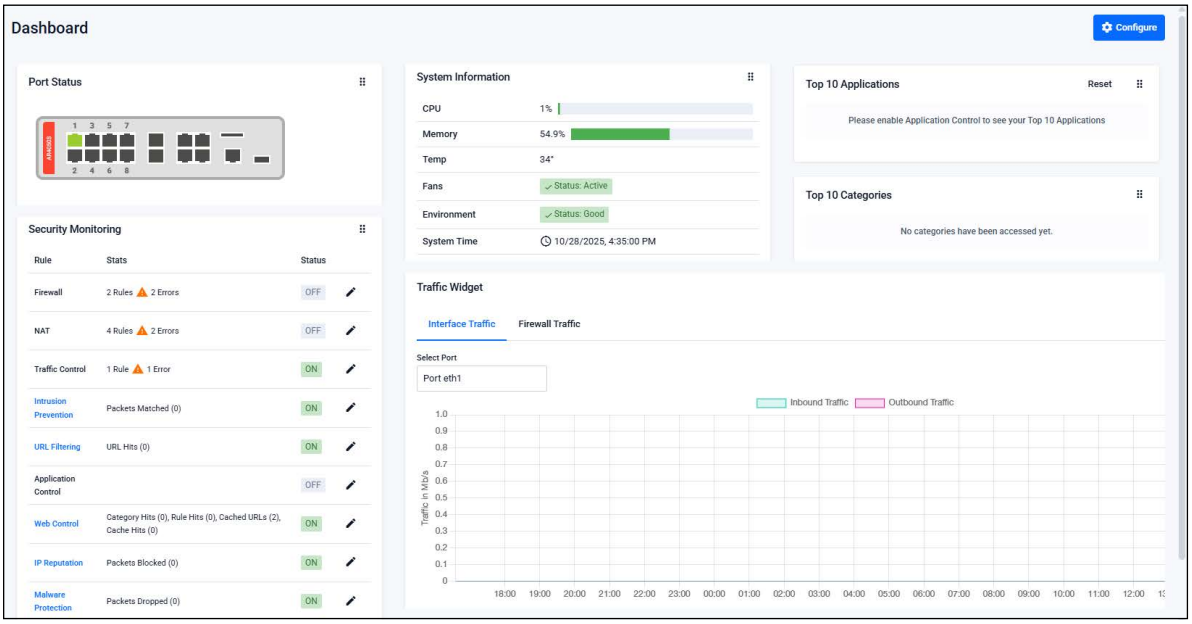
Note: You can monitor IP Reputation blocked packets using the Dashboard's security monitoring widget.

The Dashboard

Now that we have configured the firewall, application control, web control, and threat protection features, let's take a look at the Dashboard of the GUI, and what information is provided in the various widgets (applications).

- Go to **Dashboard** from the main menu:





Currently, the widgets are:

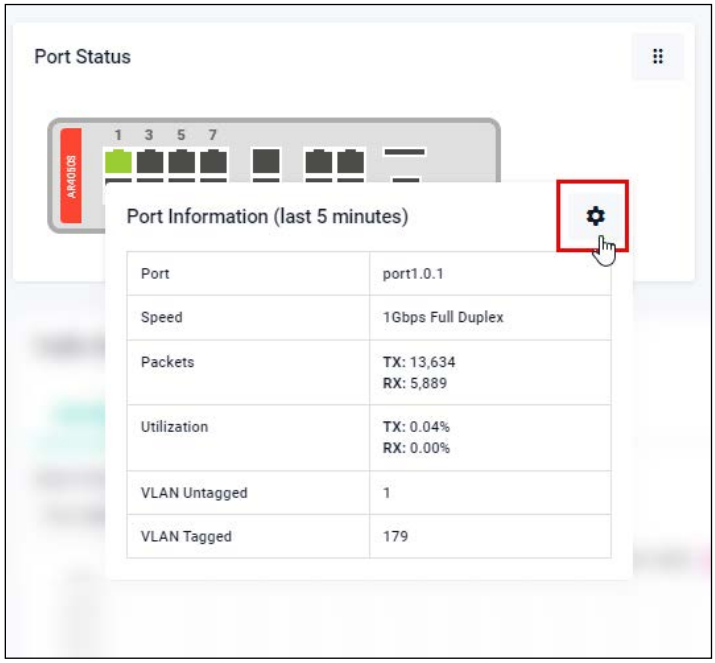
- **Port Status** (not available for the 10GbE UTM Firewall and AR4000S-Cloud)
- **System Information**
- **Traffic** (not available for the 10GbE UTM Firewall and AR4000S-Cloud)
- **Security Monitoring**
- **Top 10 Applications**
- **Top 10 Categories**

The next section provides a brief summary of their functionality.

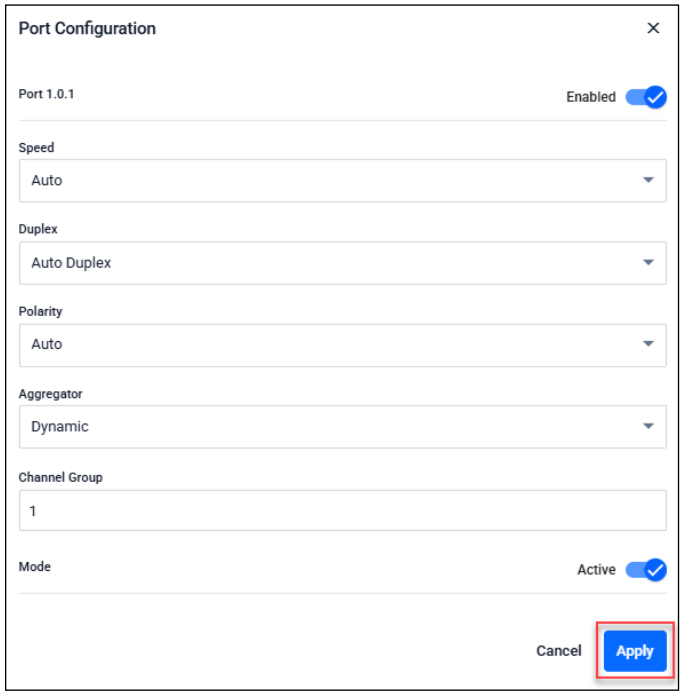
Port Status The Port Status widget displays the front panel ports of the device.

Any ports that are currently ‘up’ are shown in green. **Hovering your mouse** over any port that is ‘up’ displays the Port Information panel, with statistics over the last 5 minutes. The panel lists the port’s number, speed, packet transmit and receive counts, utilization percentages, and VLAN associations and aggregation options. For example, display status information for port 1.0.1:

- Click on the **Configure** button to access port options.



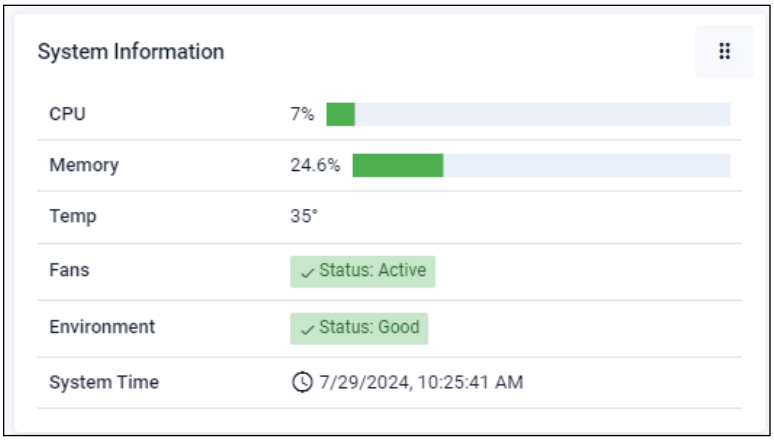
- From the Port Configuration panel, you can enable or disable the port, or configure its speed, duplex mode, polarity, and aggregator status.
- Click **Apply** to save changes.



Note: The Port Status widget is not available for the 10GbE UTM Firewall and AR4000S-Cloud.

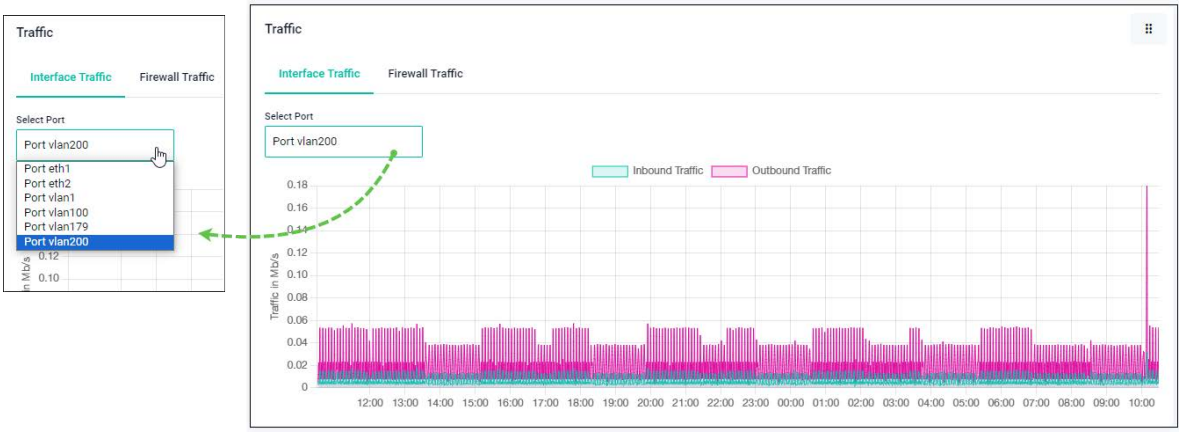
System Information

This widget shows CPU and memory use, as well as device health.



Interface Traffic

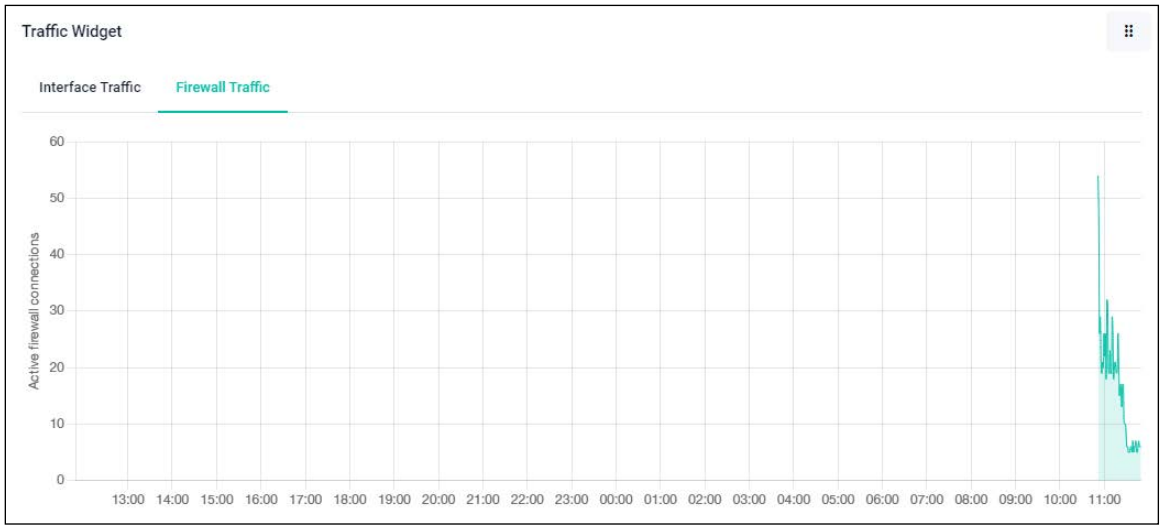
The **Interface Traffic** widget shows traffic passing through a chosen interface in both directions over a 24 hour period.



Note: The Interface Traffic widget is not available for the 10GbE UTM Firewall and AR4000S-Cloud.

Firewall Traffic

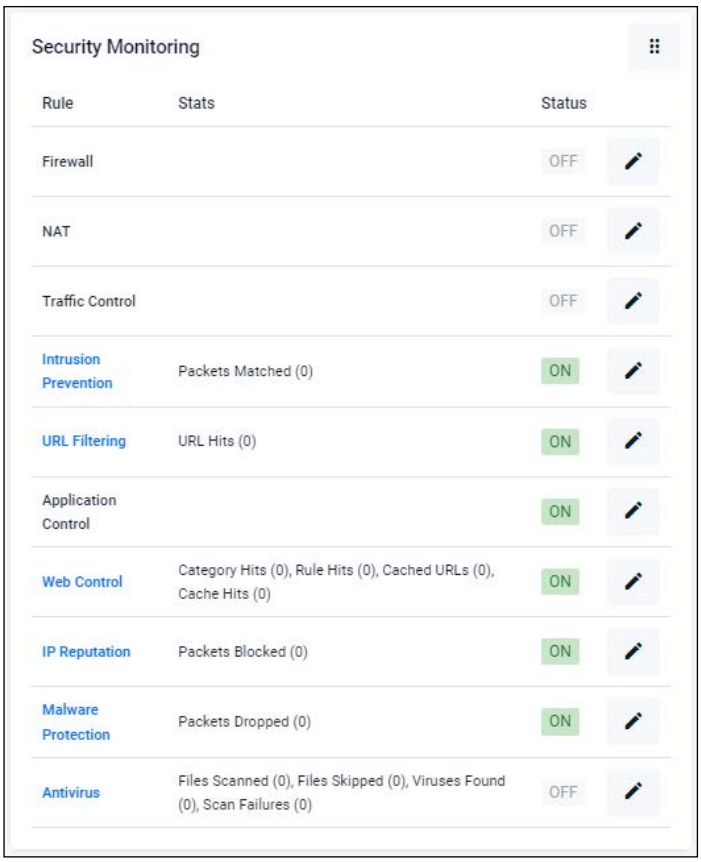
When you have Firewall Traffic enabled, the **Firewall Traffic** widget shows traffic passing through the firewall over a 24 hour period.



Note: The Firewall Traffic widget is not available for the 10GbE UTM Firewall and AR4000S-Cloud.

Security monitoring

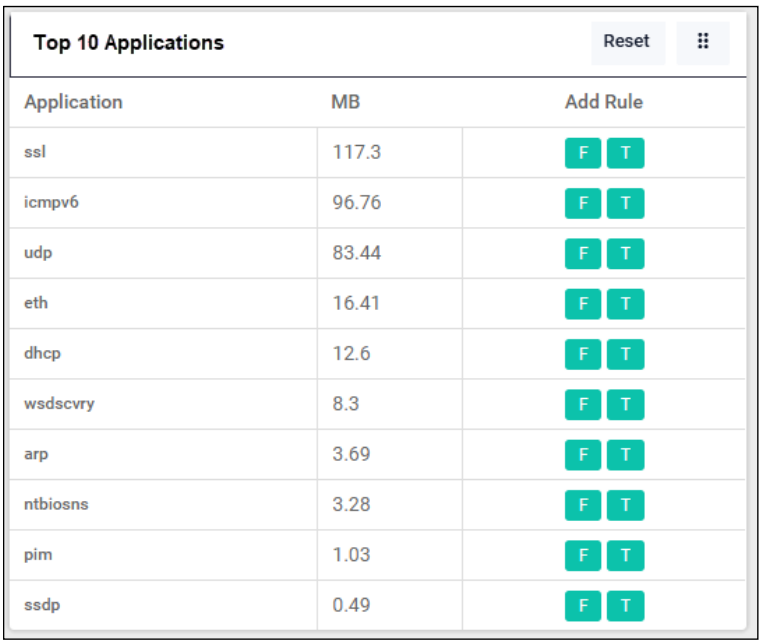
The **Security Monitoring** widget shows the main security and threat protection features of the firewall in one handy location. You can see which are currently enabled and which are not. You can select **edit** to go to that feature's dedicated page to configure it further.



You can also see how many rules are configured for the various features, and statistics for each of the security features, for example: URL rules hit, packets blocked, and viruses found.

Top 10 Applications

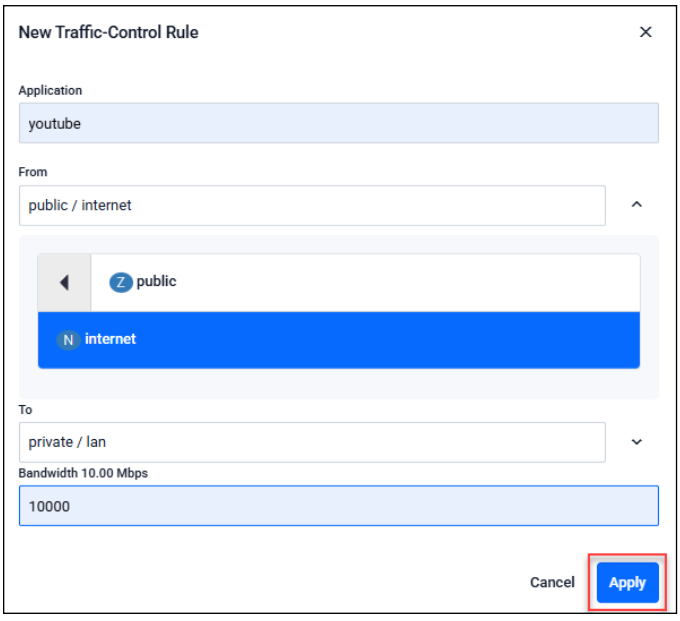
The **Top 10 Applications** widget shows the top 10 applications using firewall bandwidth. You have the ability to take action based on this reporting, by adding a new firewall or traffic control rule. To add a new firewall or traffic control rule, simply click on the **'F'** or **'T' Add Rule** buttons.



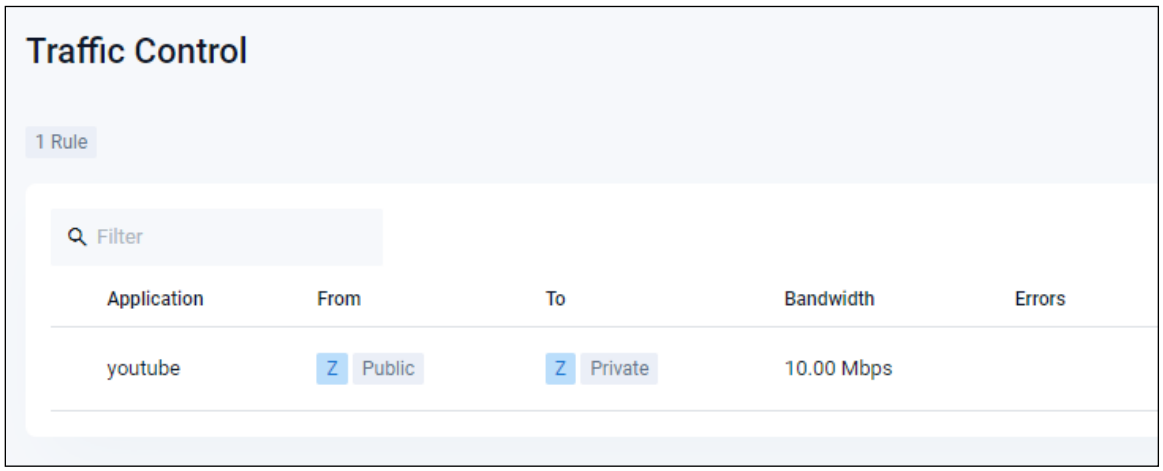
Application	MB	Add Rule
ssl	117.3	F T
icmpv6	96.76	F T
udp	83.44	F T
eth	16.41	F T
dhcp	12.6	F T
wsdscvry	8.3	F T
arp	3.69	F T
ntbiosns	3.28	F T
pim	1.03	F T
ssdp	0.49	F T

The Top 10 Applications table shows cumulative totals, and is live, so the **MB** used will change and applications will move position in the table. Clicking the **reset** button will zero all totals and start to display the top used applications from that time onwards.

Here is an example of creating a new traffic control rule. Click the **Apply** button to apply the rule:

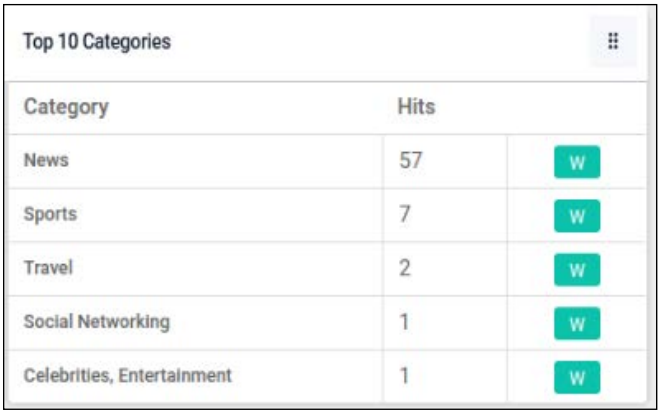


Once you have created the rule it appears in this dialog from where you can view and edit it:



Top 10 Categories

Similar to the Top 10 Applications widget, the **Top 10 Categories** widget shows the top 10 Web control website categories that are using firewall bandwidth. Click on the 'W' button to create a new Web control rule from the widget in response to this reporting.

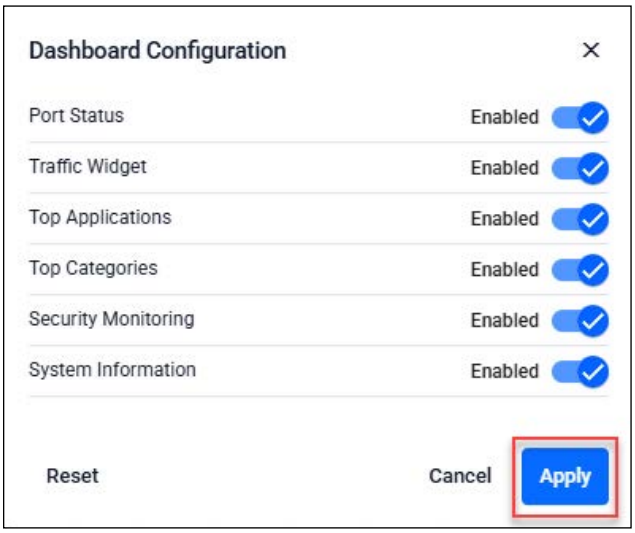


Configure

The Dashboard **Configure** button (top right) allows you to turn on or off: Port Status, Traffic Widget, Top Applications, Top Categories, Security Monitoring, and System Information. Click the **Apply** button to apply the configuration changes. Click the **Cancel** button to backout without making any changes. Click the **Reset** button to put the settings back to their default values.

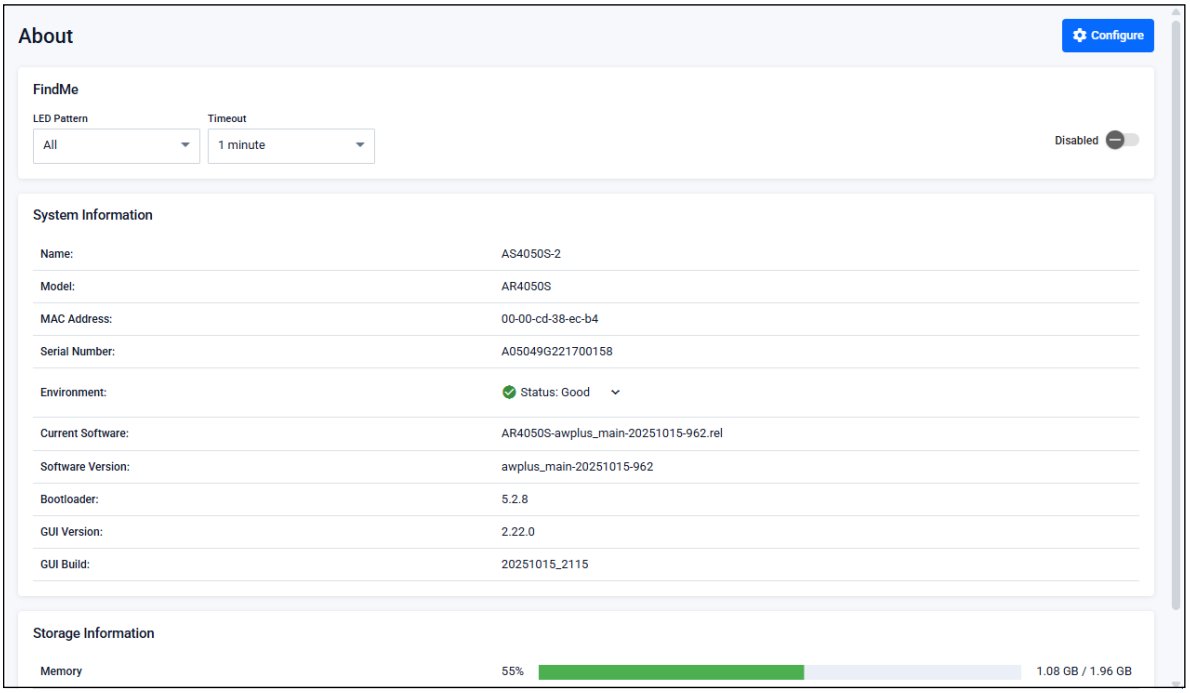
Click **Configure** to show the Dashboard Configuration options:

Click **Apply** to set the Dashboard display:



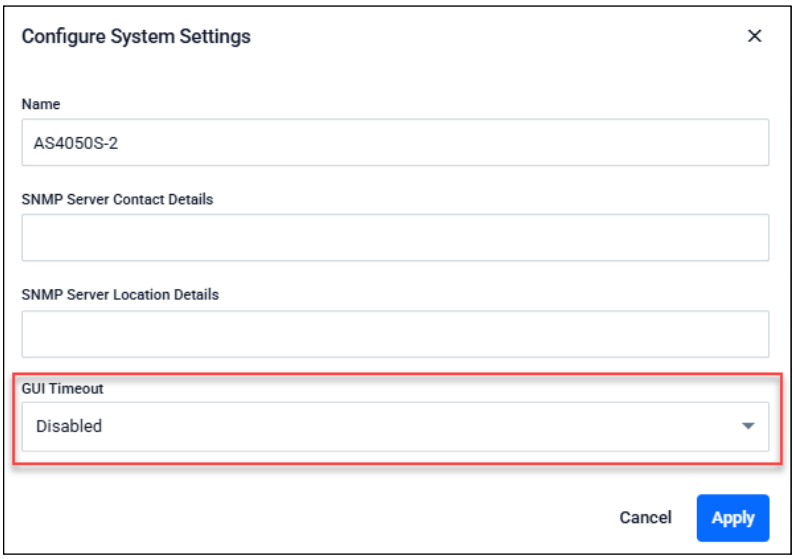
System Page

Further system information is available on the **About** page, under the **System** menu, such as model, MAC address, serial number, firmware, GUI versions, and so on.



GUI timeout

To change the GUI time out parameters, from the **System** menu, click **Configure**.



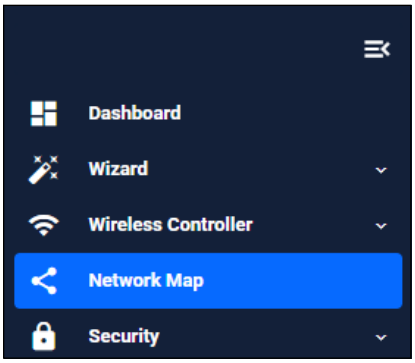
Select a parameter from the drop down list. From here you can also edit Name, SNMP Server Contact Details and SNMP Server Location Details.

Note: Vista Manager mini and the network map are not available for the 10GbE UTM Firewall and AR4000S-Cloud.

The Network Map

Under the main menu, there is a network topology map. To view the Network map, click the **Network MAP** menu item.

- Go to **Network Map** from the main menu:



The Network map shows details of the devices connected to your switch or firewall. You can use it to see your:

- Wired devices
- APs
- Wireless deployment and coverage.

This section begins with a brief description of the network map, and the tasks you can perform there. The section ends with a look at configuring the network topology view and customizing node icon images.

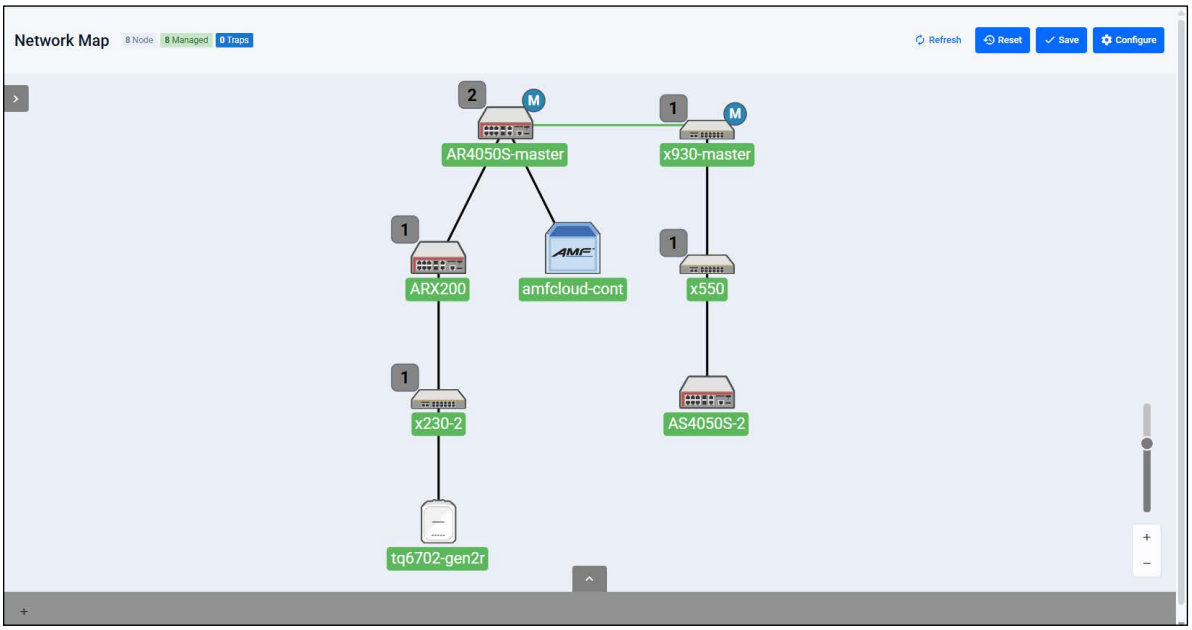
Note that the screenshots in this section show an x930 Series switch, but the functionality is the same for all devices that include the Wireless Controller.

Network map features

When you access the Network map from your device's GUI, the Network map displays details of your device, and other wired connections made to your device in a graphical display.

From the **Network MAP** page, you can:

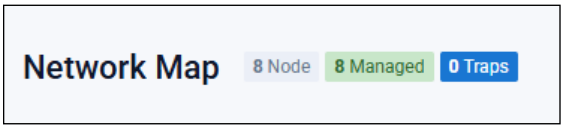
- Customize network icon images by clicking on them from the Node List.
- See a visual list of network nodes, including individual node details.
- Configure the topology view, SNMP, and Device Discovery settings.
- Create a heat map by clicking the + icon in the footer
- View stored heat maps



Use the network map to check the status of a node at a glance.

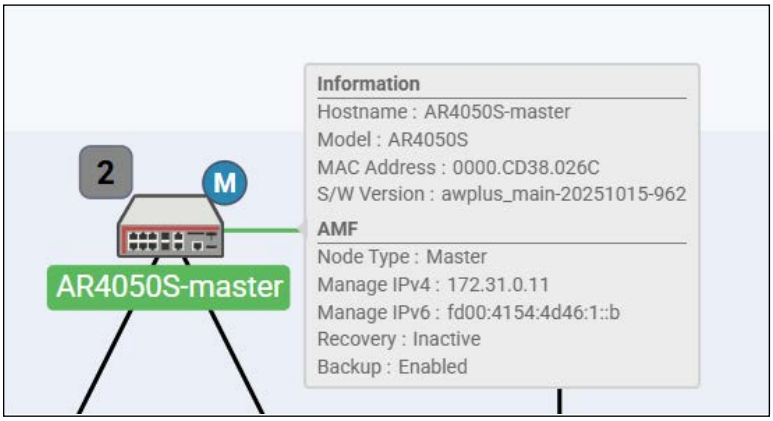
Node status is indicated by the node title background color:

- abnormal is red,
- managed is green,
- blue indicates an unmanaged node.



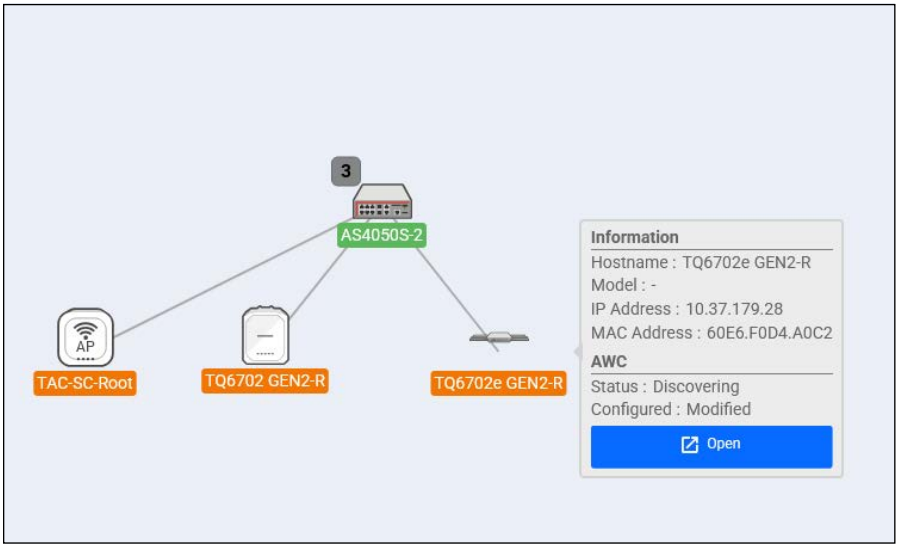
Viewing device information

In the network topology map view, your main device and any connected devices are displayed. Click on a device to see information about the Hostname, Model, MAC address, and Software Version.



Device information from AMF nodes are gathered by SNMP and Device Discovery. The Device GUI uses this information to display the devices on the Network map. For information about Device Discovery and SNMP, see the Device Discovery and Monitoring using SNMP Feature Overview and Configuration Guide.

When you click on various devices in your network, depending on the security that has been set up, you may be able to Open it as well, so you can log into it directly from the map.

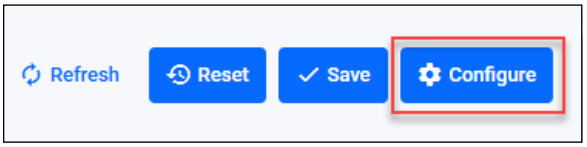


Configuring the topology view

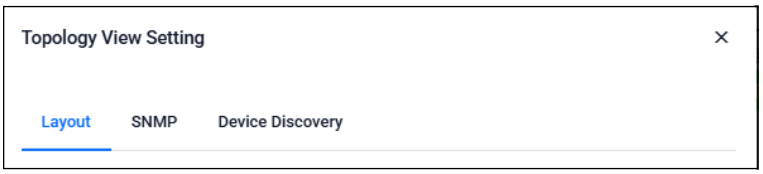
The Device GUI automatically creates a complete topology map from an AMF network of switches, firewalls, and wireless access points (APs), showing areas and multiple levels of connected nodes and devices.

From the Configure menu, you can configure a variety of settings related to the Network Map. These include layout settings, SNMP settings, and Device Discovery settings.

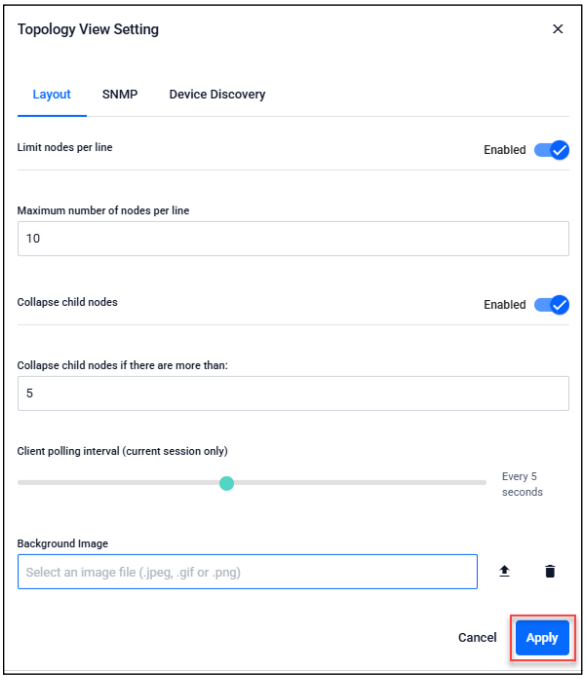
To change the topology view settings:
Click the **Configure** button in the top-right of the Network MAP page.



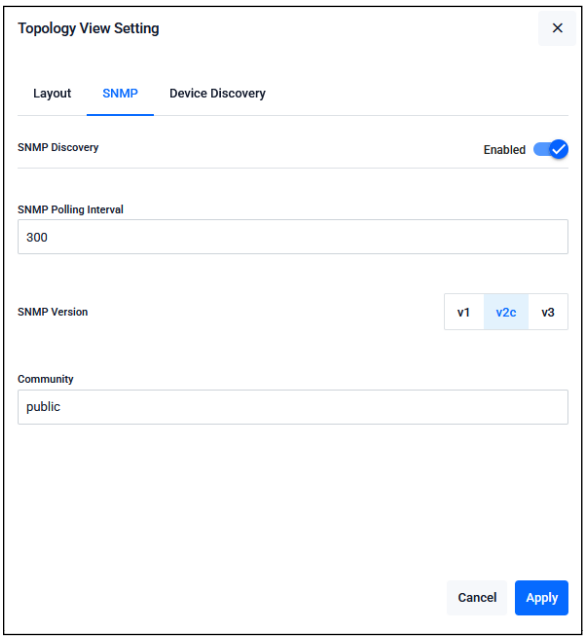
Select the tab you wish to view, this includes **Layout**, **SNMP**, or **Device Discovery** settings.



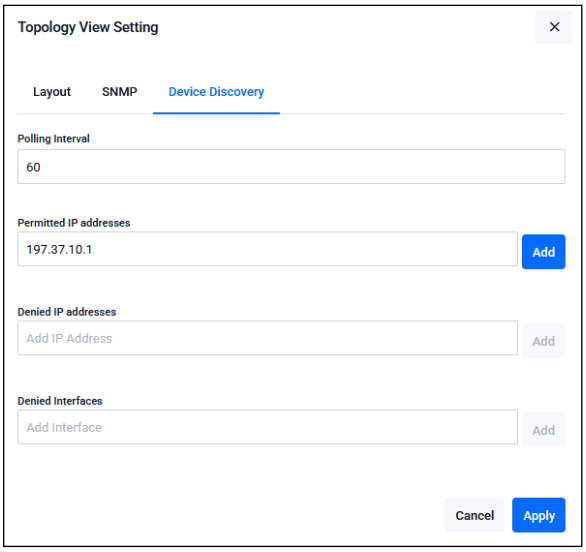
These are the **Layout** options:



These are the **SNMP** options:



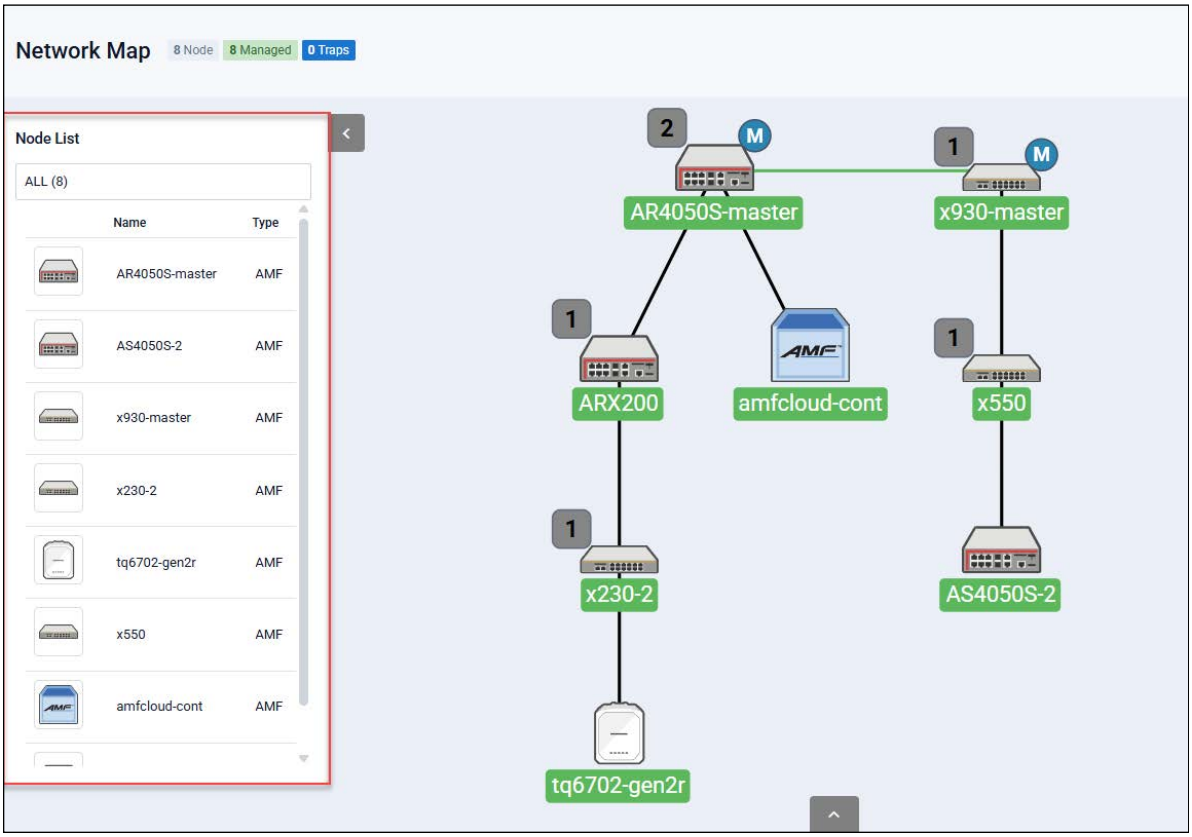
These are the **Device Discovery** options:



1. Change the settings you wish to edit, and click **Apply** to save your changes.
2. Save the changes to your configuration.

Customizing device icons

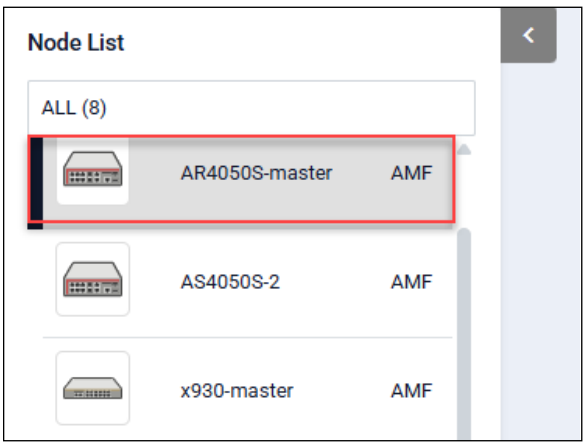
You can customize the look of your network nodes with icon images. For example, you can add access point, switch, and router images to make the network map easier to understand.



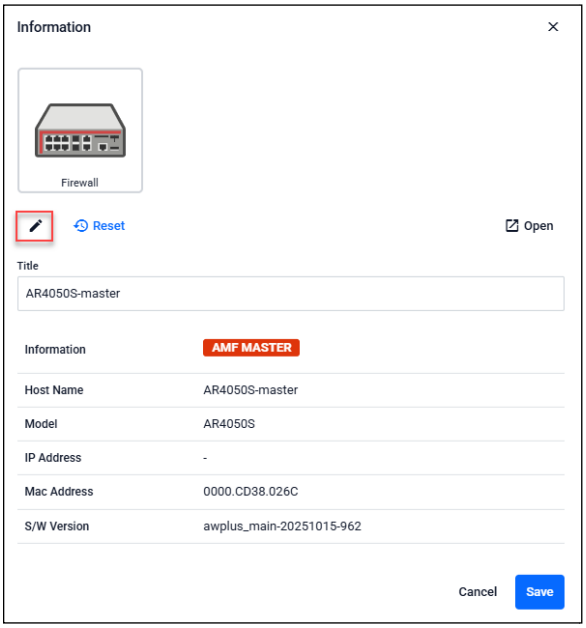
To customize a device icon:

1. From the Network map, open the Node List by clicking the arrow on the left.

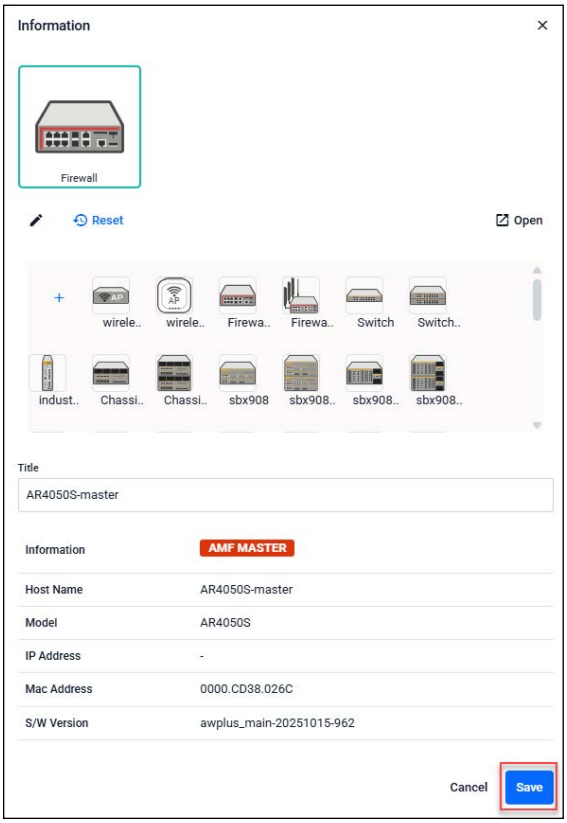
2. Click on a node's icon image in the list to open the settings.



Click on the **device icon**, or the **edit pencil icon** to open the icon menu.



3. Scroll and select an image from the library or click the '+' sign to add a custom image from.

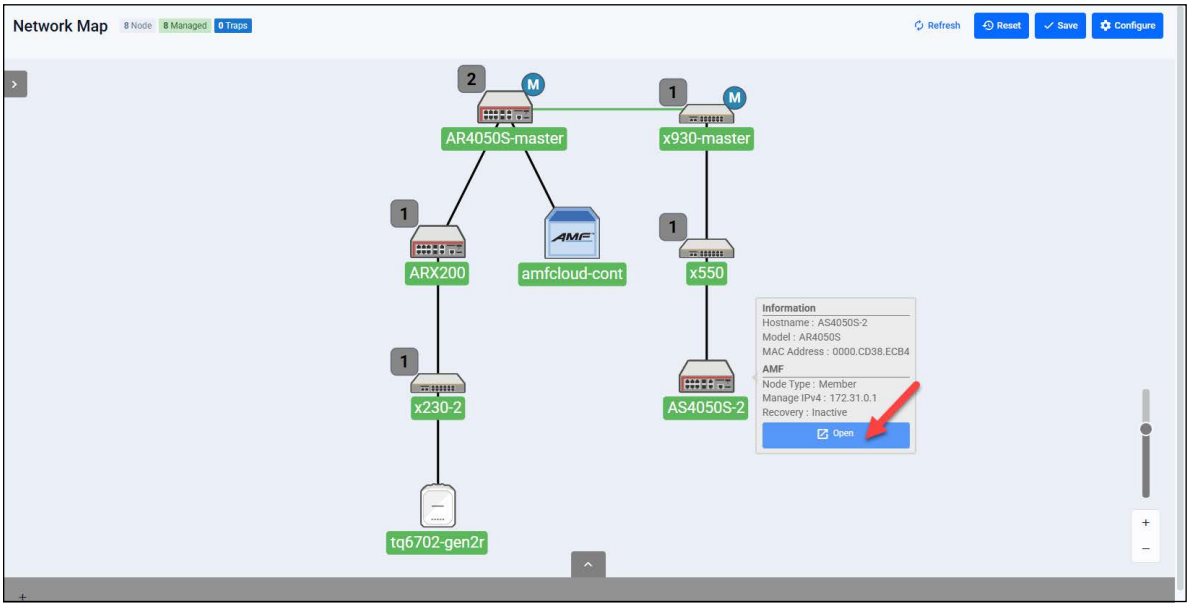


4. Click **Save**.

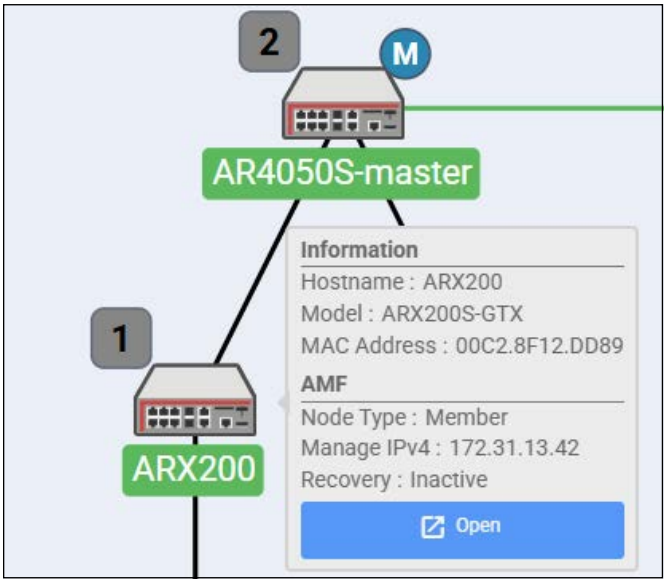
5. Save your configuration.

Accessing the Device GUI from the Network map

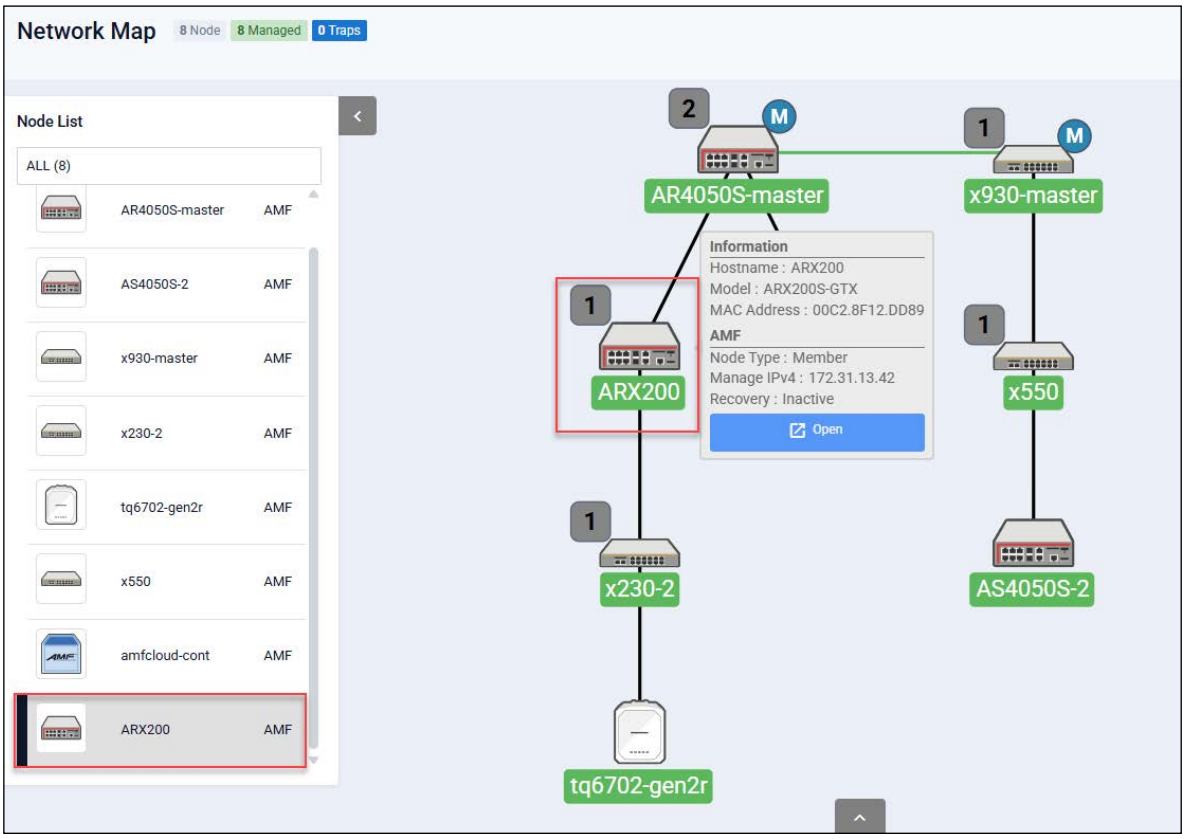
You can access another device's GUI instance from the Network map by clicking the open button on the information panel. For example, the screenshot below shows an x230 that is a client device of an AR4050S. Clicking on the open button will open the x230 switch's Device GUI in another browser tab.



When you double-click a device's icon on the Network Map, the node information is displayed. In the node information window, click on the **Open** button to access the device's GUI.



You can use the **Node List** to help you locate a device in the network map. Simply click the device in the Node List to see its **Information** details.



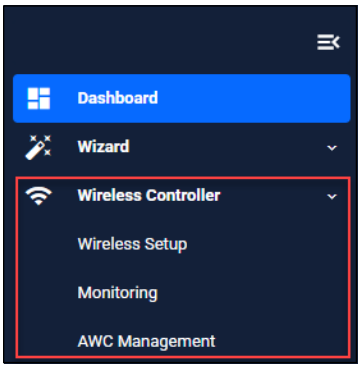
Wireless management

Allied Telesis UTM Firewalls incorporate Autonomous Wave Control (AWC) wireless management, allowing your wireless access points (APs) to be setup and managed from the Device GUI on your security appliance. AWC uses wireless intelligence to constantly model AP location and signal strength information. It then automatically optimizes wireless output and channel selection for optimum performance.

Note: The Vista Manager mini settings are not available for the 10GbE UTM Firewall and AR4000S-Cloud.

The device GUI includes a Wireless Controller menu, which enables you to set up your wireless network, monitor and configure the network, and manage AWC:

- Go to **Wireless Controller** from the main menu:



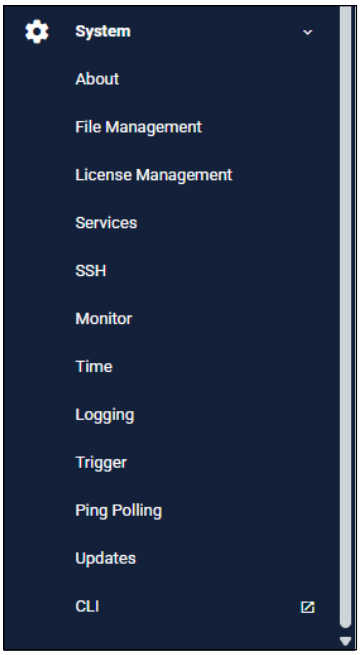
The device GUI also displays heat maps for managed APs on the network map.

Other features

The Device GUI has a number of other great features. The **Network Infrastructure** menu includes interface management, VLAN management, DNS management, and various other tools.

The **Network Services** menu allows you to configure the firewall as a DHCP server for the network. There are configuration options for SMTP, RADIUS, Tools, and AAA here too. These will not be detailed here, but are easy and intuitive to use.

The **System** menu includes information about the device's model name, MAC address, and firmware/software etc. You can also manage your files, licenses, and logging here.



Note: The Time settings are not available for the 10GbE UTM Firewall. Its time settings are managed through the VST-APL menu.

Let's look at a few important features:

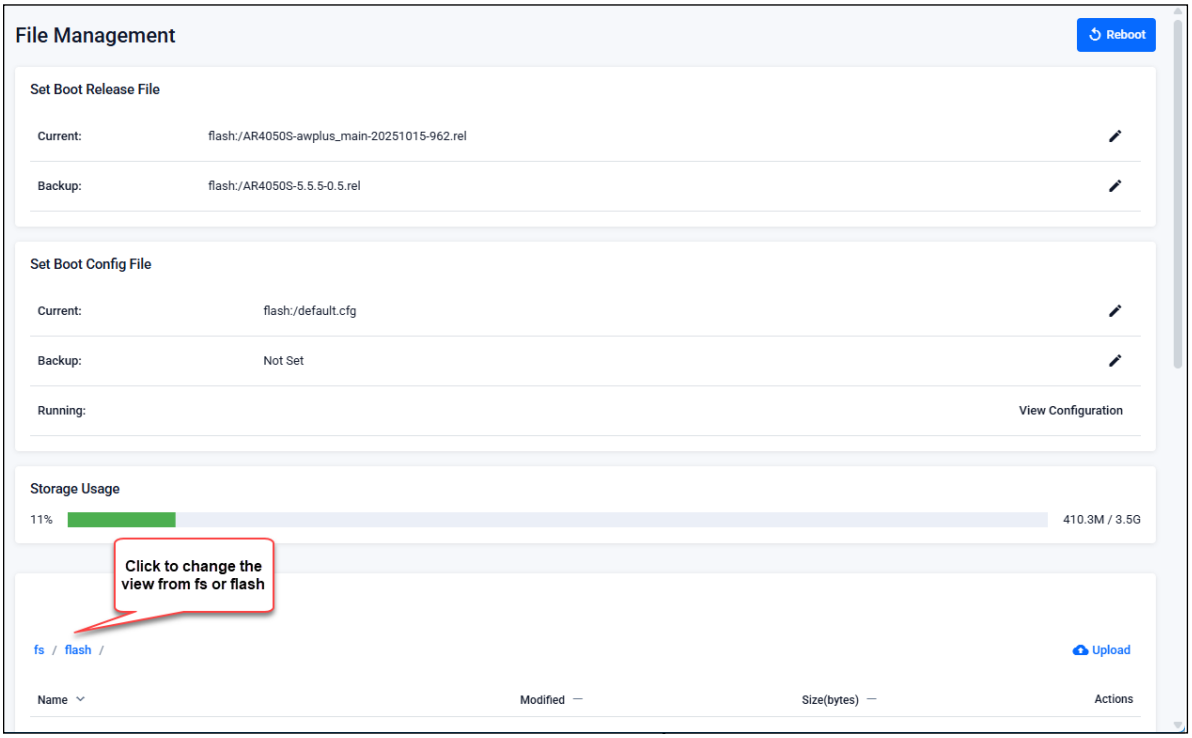
- "File management" on page 80
- "License management" on page 81
- "Logging management" on page 83
- "AMF Security mini on the AR4050S Series" on page 87

File management

The **File Management** page is located under the **System** menu. Use this page to view all files stored on the device, as well as any USB device or SD card that is plugged in.

The upload and download functions provide an easy way to add new files such as firmware, configurations, scripts, or URL lists to the device.

You can use this page to set the device's software release or upgrade its firmware and reboot.

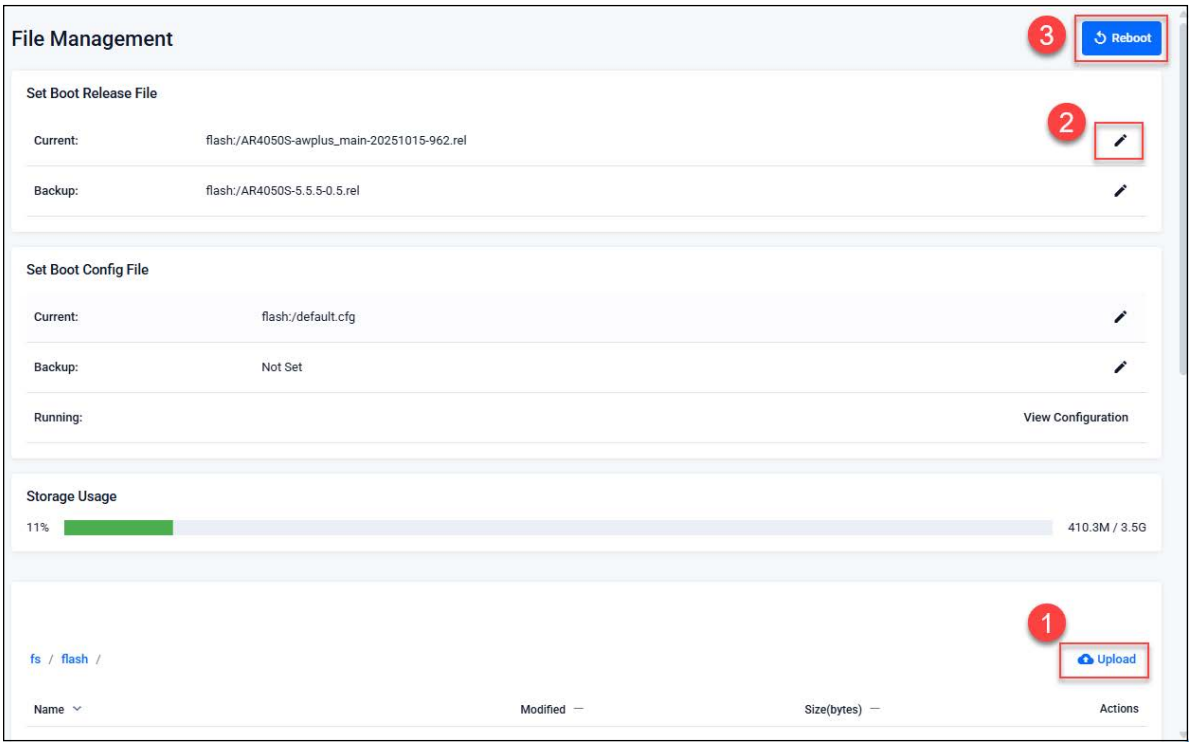


- By default, the **flash** system files are shown as above.
- To view files on a USB device, navigate back to the main **file system (fs)**, and choose USB: Load some files on a USB and plug it in to reproduce this screen shot. Check it is available for all routers.

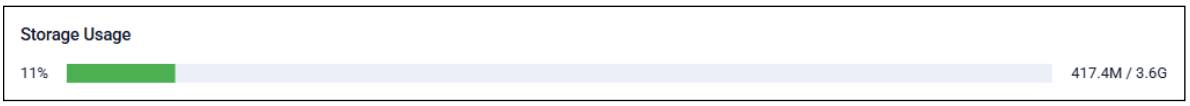
Use the **upload** option to browse and locate the file you wish to add to the firewall. From here it is easy to add more files and change the release and configuration files to be used.

For example, for an easy 3-click firmware upgrade, simply:

1. Browse to the new firmware file using the **upload** option
2. Set the new firmware file to be the boot release
3. Re-boot the device.



Tip The **Storage Usage** panel provides details on the percentage used and total available flash.

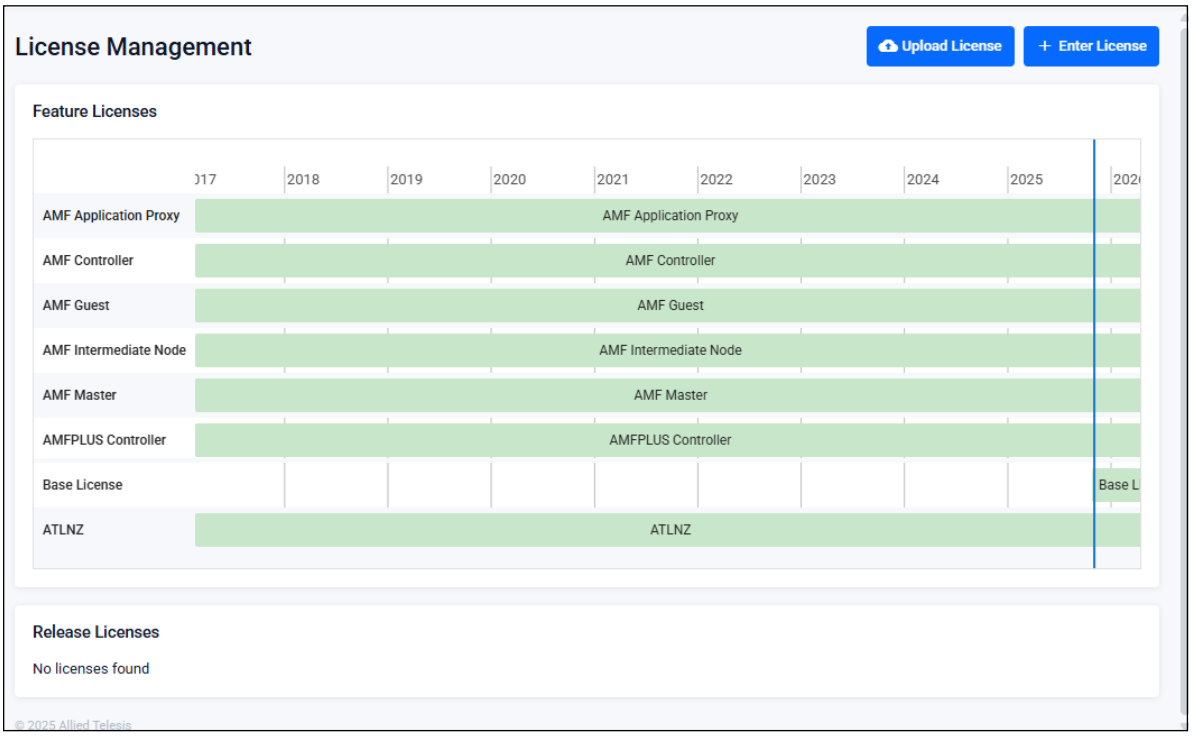


License management

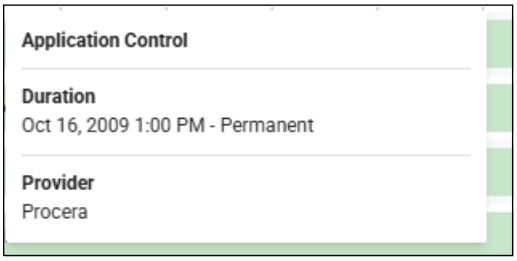
You can use feature licenses to unlock advanced functionality on UTM firewalls.

Licenses such as advanced firewall, and advanced threat protection, enable additional security features as described in **Part 4** on page 50 and **Part 5** on page 56 of this guide. You can purchase AMF Master and AWC wireless licenses to manage your wired and wireless network devices. All of the licenses are available in 1 or 5-year subscriptions.

The License Management page shows the licenses you currently have on your device. You can add new purchased licenses from this page too.



Hover your mouse over a green license bar to show its details, such as duration and other relevant feature information.

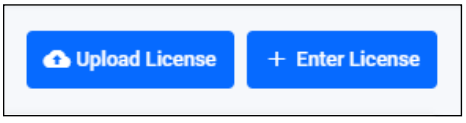


Adding a new subscription feature license

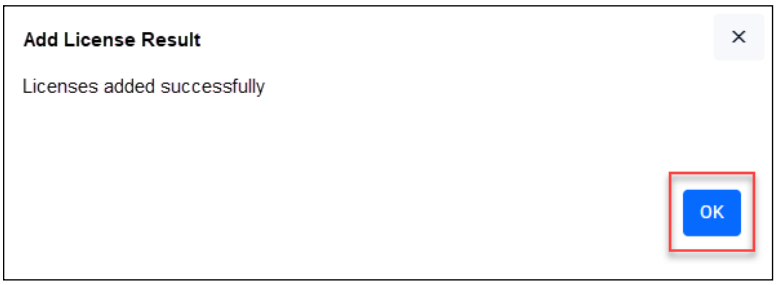
Subscription feature license files are in the '.bin' file format. The '.bin' file format is a file that stores data in a compressed binary format. Once you have purchased your new subscription license you should add it to your firewall.

For example, to add a 1 year Advanced Threat Protection (ATP) subscription license:

1. Go to **System** > **License Management**
2. Click the **Upload License** button.



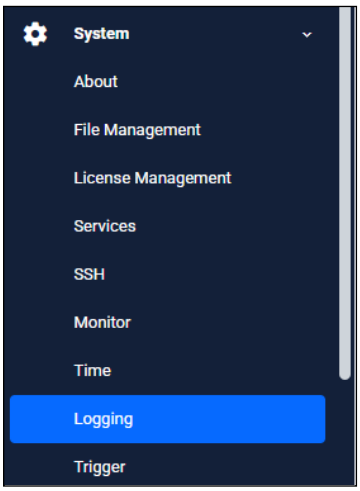
3. Browse and select the '.bin' file you purchased. Once selected, the '.bin' file will be uploaded and the subscription license added to your device.



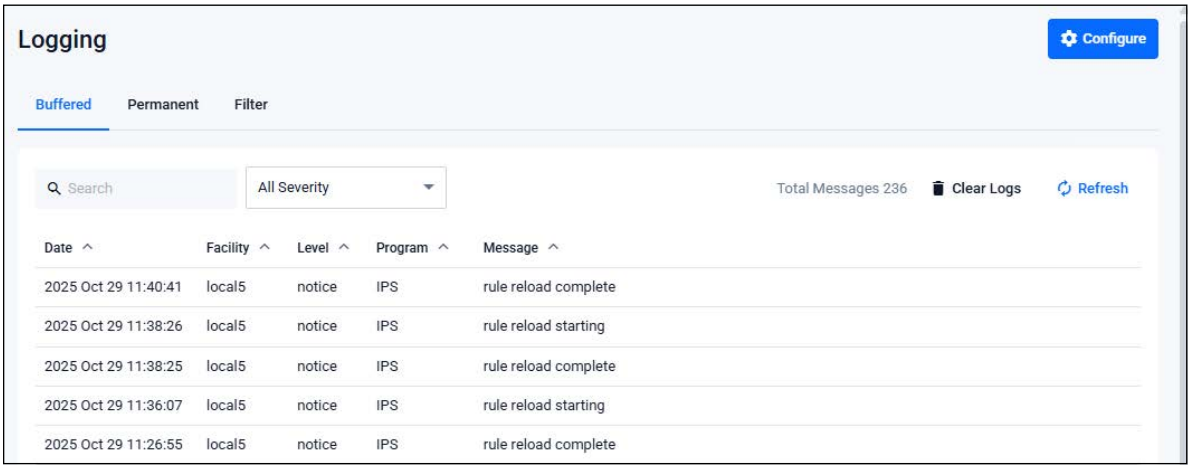
Logging management

The **Logging** page shows buffered and permanent log messages stored on the device. There are two tabs, Buffered and Permanent.

- Go to **System > Logging** from the main menu:

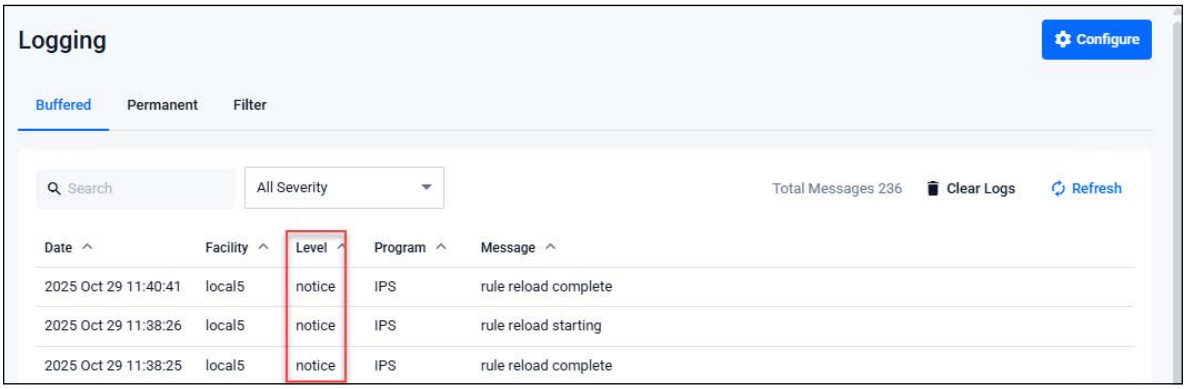


The Buffered tab is displayed by default:

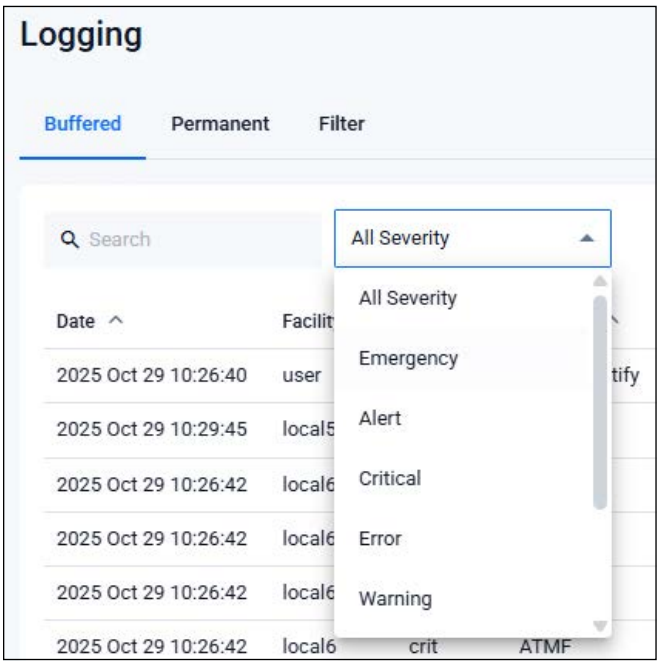


You can filter logs in 3 different ways to focus your view and support easy analysis:

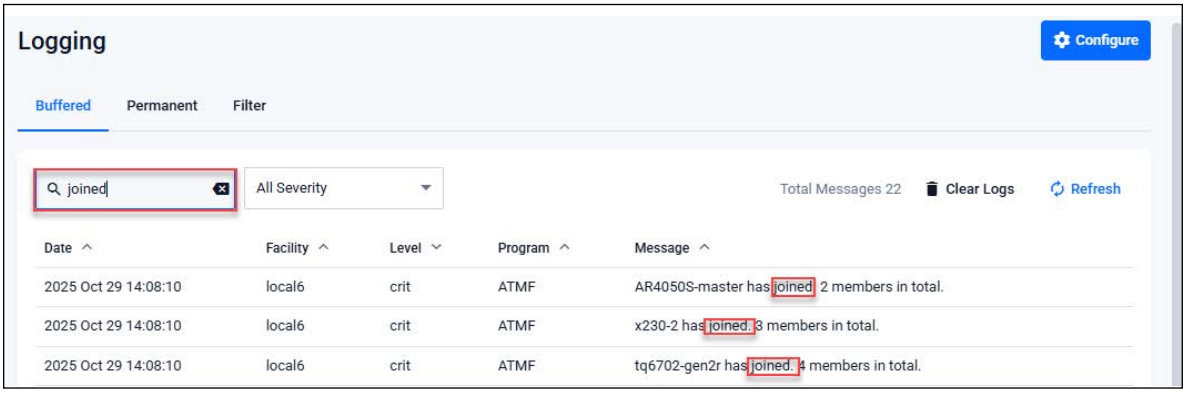
1. sort columns in ascending or descending order.



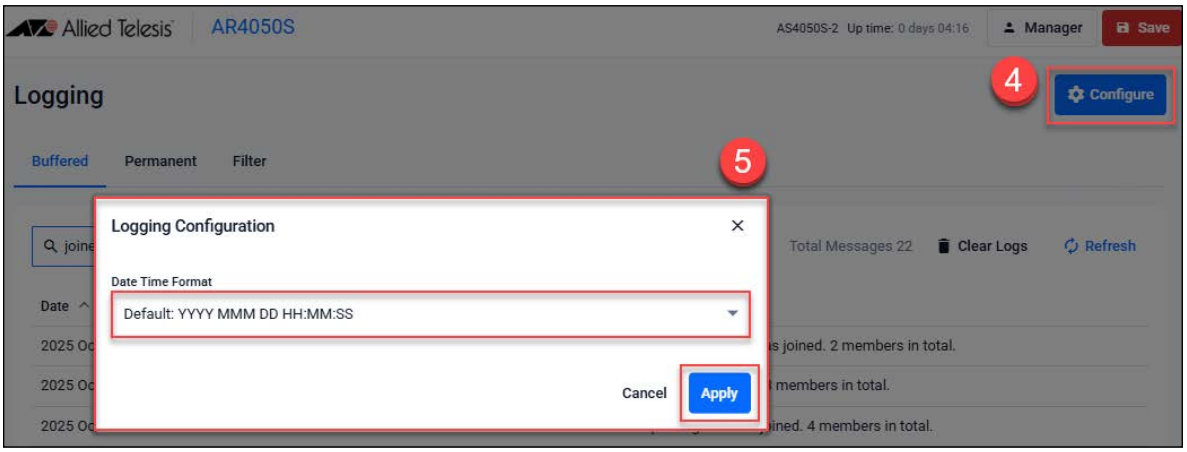
2. select the severity of logs to display, e.g Critical, Warning, Error etc.



3. search for any text string found in the logs.



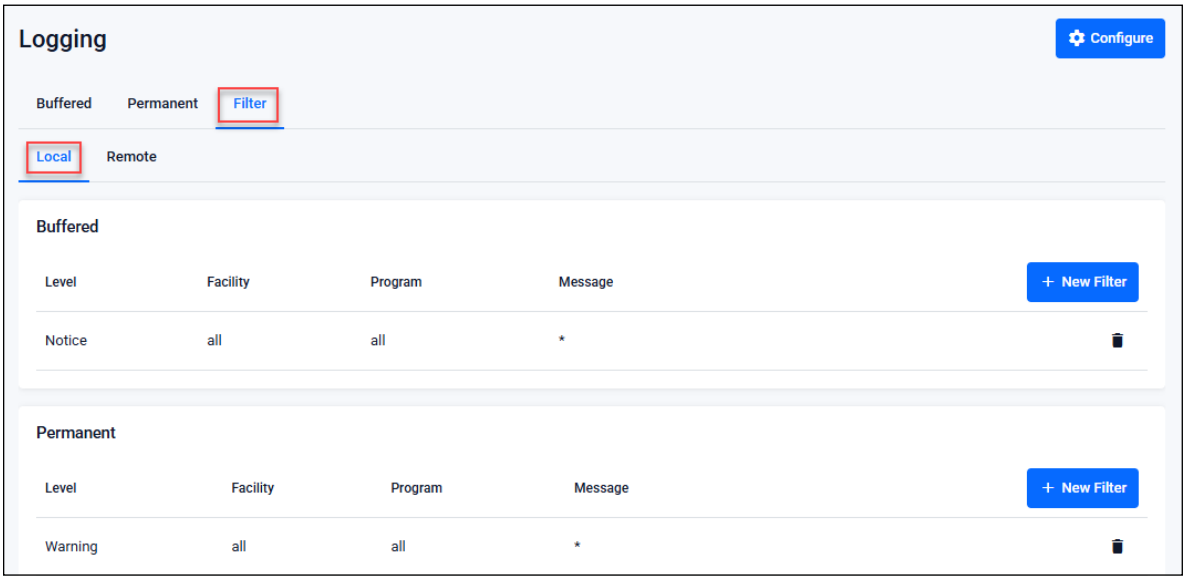
4. Click the **Configure** button to access the Logging Configuration settings:



5. Select the **Date Time Format** from the drop-down list, and click **Apply**.

From the Filter tab on the **Logging** page, you can create filters to manage which logs are stored on the device and also set up a Syslog server(s) for remote log storage.

The Filter tab has a further two tabs: **Local** and **Remote** (i.e. syslog server).

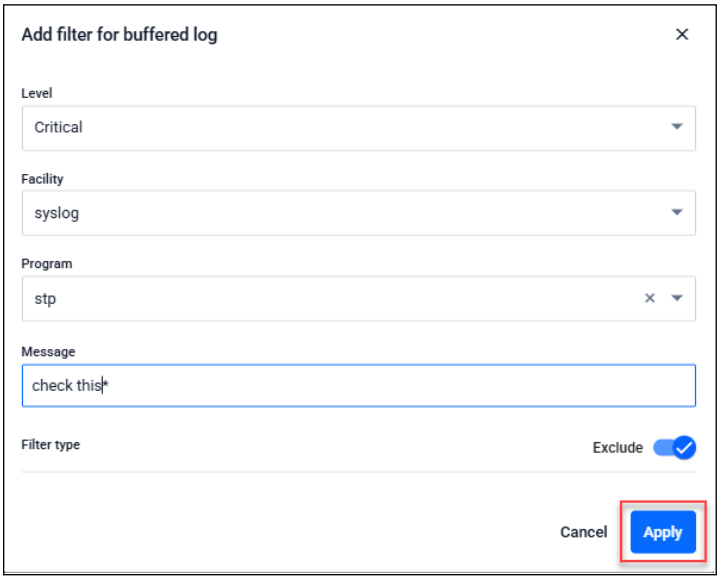


- Use the **Local** tab (default) to create filters to manage the level of logs that are stored in the buffered and permanent logs on the device. You can also delete the buffered or permanent logs using the **Clear Logs** button.

To create a new log filter:
Click **+New Filter**

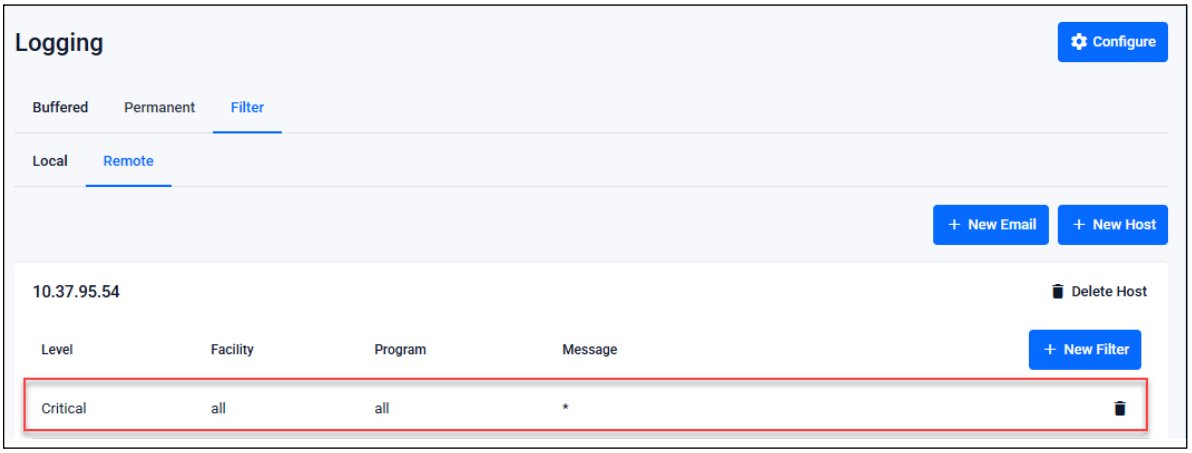
1. Select a **Notice** level: All, Emergency, Alert, Critical, Error, Warning, Notice, Info, or Debug.
2. Select the **Facility** and **Program** - a drop-down list appears when you begin typing in these fields.
3. Type in the log 'message'.

4. Select **Included** or **Excluded**.
5. Click **Apply**.



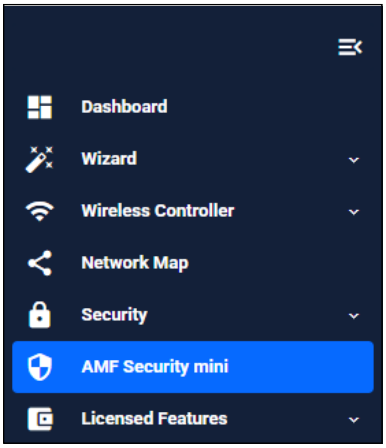
This enables log storage on the device to be configured exactly as desired.

Use the **Remote** tab and the **+New Host** button to set up a syslog server to send log messages to for storage and analysis.



AMF Security mini on the AR4050S Series

The main menu supports AMF Security mini (AMF-Sec mini) on the AR4050S Series. Allied Telesis Autonomous Management Framework (AMF) simplifies and automates network management. AMF Security mini adds a powerful security component with an intelligent SDN controller that works with firewalls and other security devices to instantly respond to alerts, and block the movement of malware threats within a wired or wireless network.



For more information on using AMF-Sec mini, see the User Guide: AMF Security mini.

5G Mobile on the AR4050S-5G

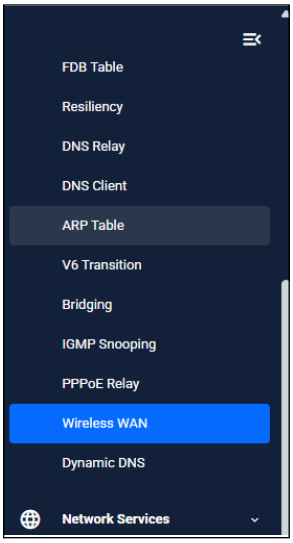
The 5G feature uses an internal cellular modem that supports 5th generation mobile communication. This modem supports configuration of carrier information used to connect to mobile carrier networks. This modem can also connect to 3G and 4G wireless networks automatically. The router connects to the fastest available wireless technology. Dual SIM card slots support resilient mobile connectivity, with the ability to use SIM cards from two different carriers.

5G refers to the internal Sierra Wireless EM9191 modem. It features a higher speed wireless connection that creates two WWAN interfaces. The interface '**wwan0**' is used for the internal EM9191 modem. The interface '**wwan1**' is available for external USB 3G and 4G cellular modems.

The **Wireless WAN** menu enables you to set up, monitor, and configure your 5G connections. For detailed documentation on 5G mobile broadband configuration, see 5G Mobile UTM Firewall Feature Overview and Configuration Guide.

Wireless WAN

From the main menu, go to **Network Infrastructure** > **Wireless WAN**:

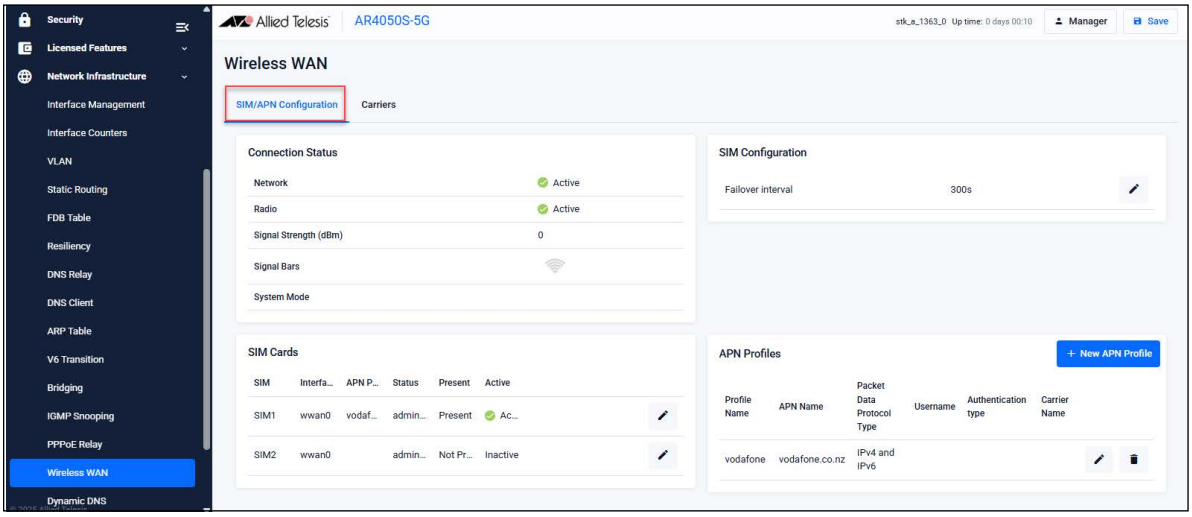


From the **Network Infrastructure** menu, select **Wireless WAN.** There are two tabs:

- **SIM/APN Configuration**
  From this tab you can display connection information, SIM information and add, edit or delete APN profiles.
- **Carriers**
  From this tab you can display or edit firmware and carrier information and files, for example, upgrade to a later version of firmware and carrier.

SIM/APN Configuration

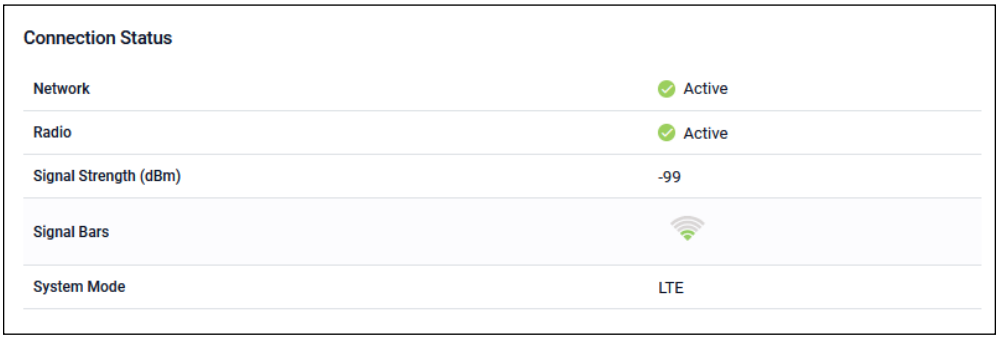
Click on the **SIM/APN Configuration** tab to view the connection status, view and edit the SIM configuration failover interval, view and edit SIM card information and APN profiles:



Connection Status

The **Connection Status** dialog shows the following:

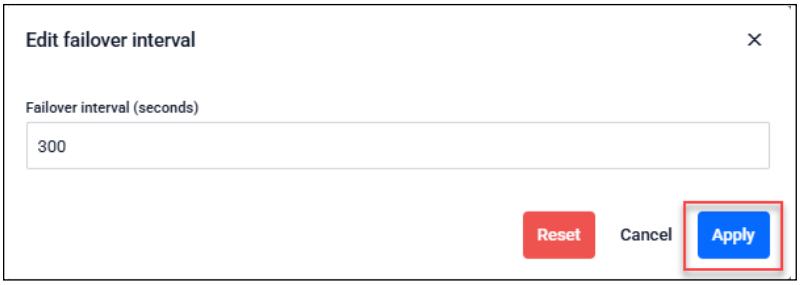
- If the network is active
- If the radio signal is active
- The signal strength
- The signal bars
- What system mode the network is operating in. For example, LTE (4G):



SIM Config

The **SIM Configuration** dialog enables you to edit the failover interval time in seconds. Click the **Edit** button to change the time:

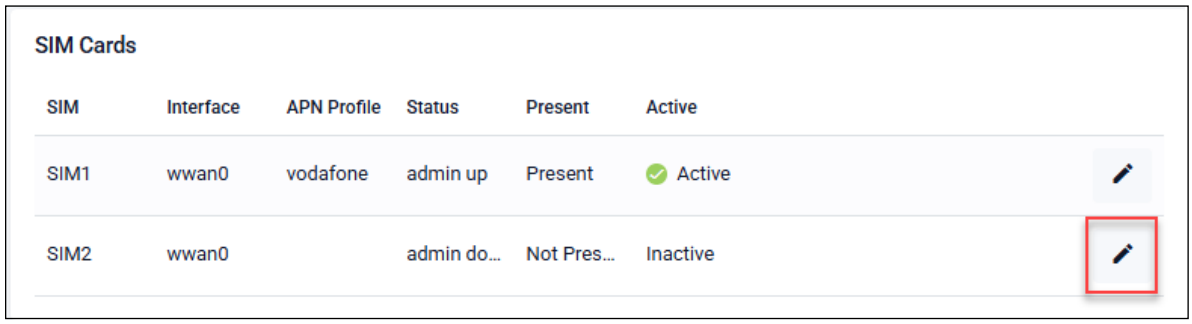
The failover interval in seconds can be from the range 60 to 3600. Enter the number of seconds for the interval in the **Edit failover interval** dialog:



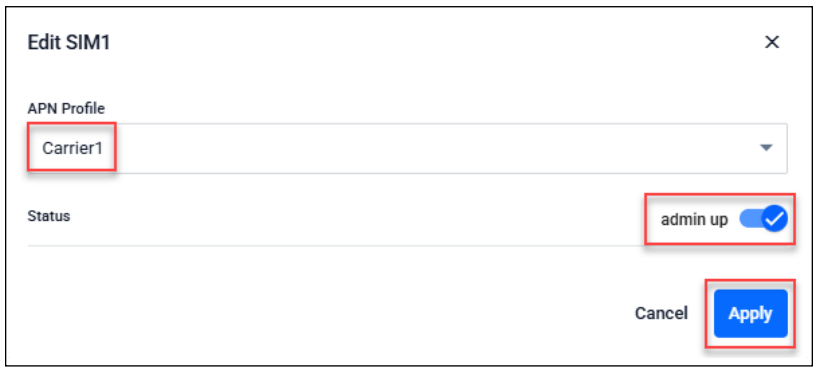
Click the **Apply** button to make the change. The default is 300 seconds. If you click the **Reset** button the interval is set back to the default. The **Cancel** button allows you to backout without making any changes.

SIM Cards

The **SIM Cards** dialog displays information about the SIM cards and their slots, for example, the SIM slot number, the interface, the APN profile, status, if the network is present or not and if 5G is active or not:



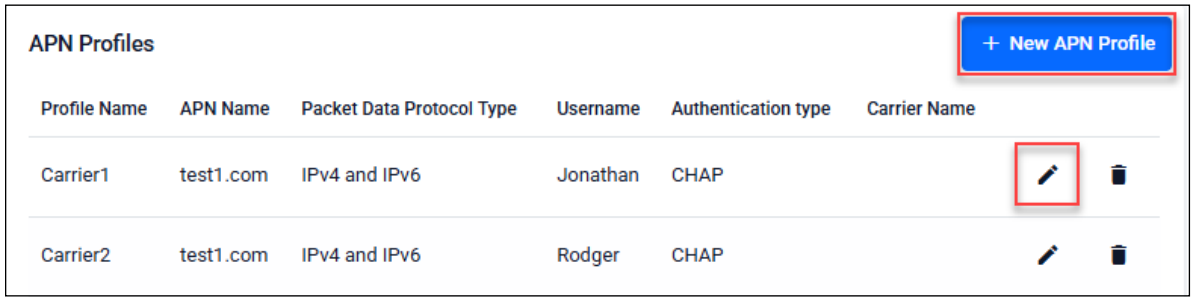
Click on the **Edit** button to select a SIM card to edit:



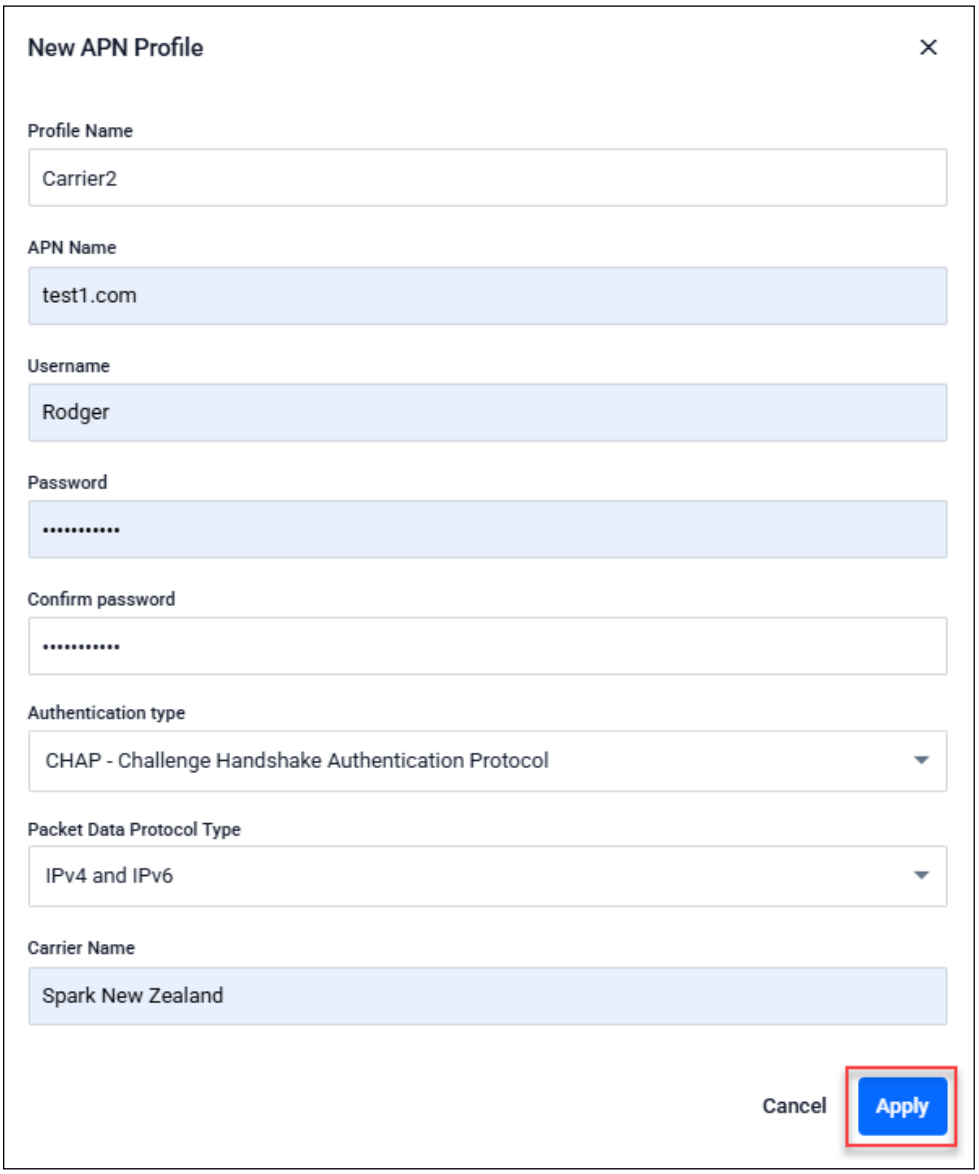
You can adjust the SIM card state and force it to be **admin down** or **admin up**. Click the **Apply** button to make the change or **cancel** to back out without changing anything.

APN Profiles

An APN profile must have a minimum configuration that includes the APN Name. The name field accepts any string. Some carriers do not require any configuration and will allow you to connect to their network as long as you have a valid SIM card. From the **APN Profiles** dialog you can edit, delete or add APN profiles:



Either click the **Edit** button to change an existing APN profile, or click **+New APN Profile** to add a new one:

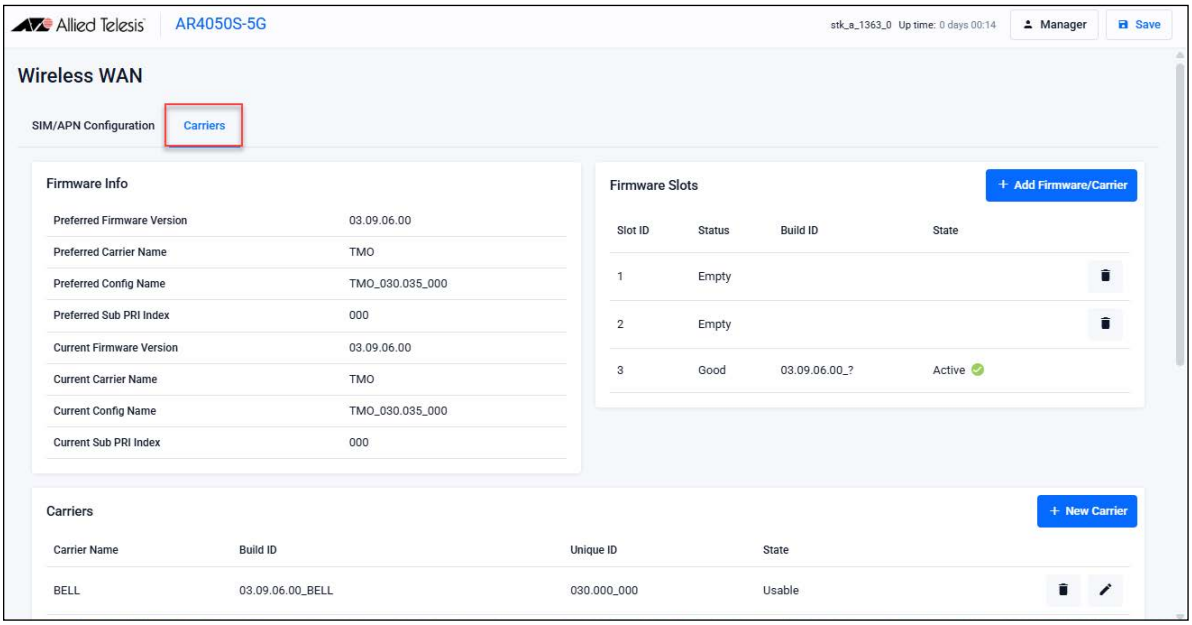


Information for these fields is supplied by your carrier. From this dialog you can change the APN Name, Username, Password, Packet Data Protocol Type and Carrier Name.

If you add a Username you are required to enter a Password and authentication method. An APN profile PDP (Packet Data Protocol) type defaults to IPv4 and IPv6. Some carriers only support IPv4. You can get the details from your carrier.

Carriers

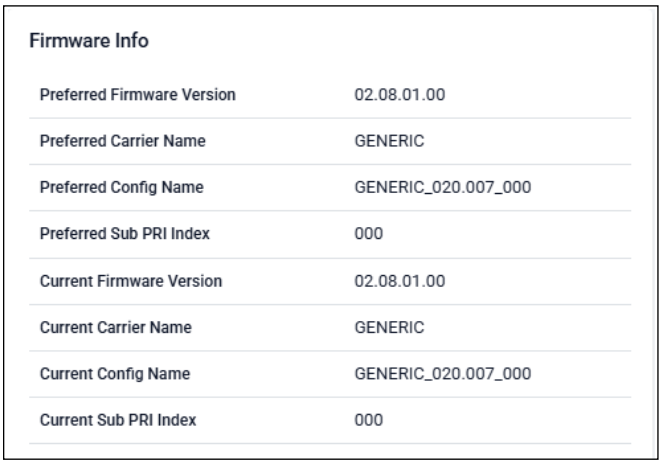
From the **Carriers** tab you can display firmware and Carrier information:



Firmware Info

The **Firmware Info** dialog displays the following information:

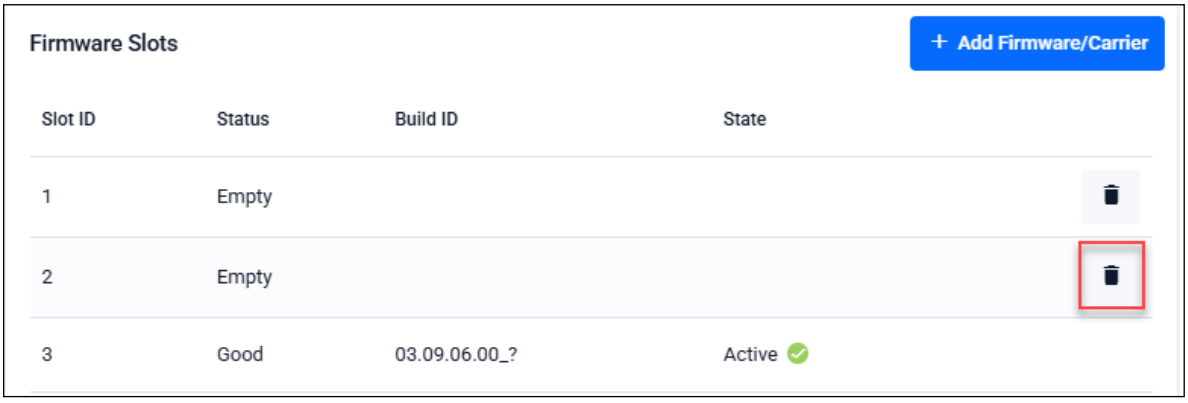
Preferred firmware version, preferred carrier name, preferred configuration file name as well as the current version, configuration file name and carrier name. It also displays the sub PRI index for both preferred and current versions.



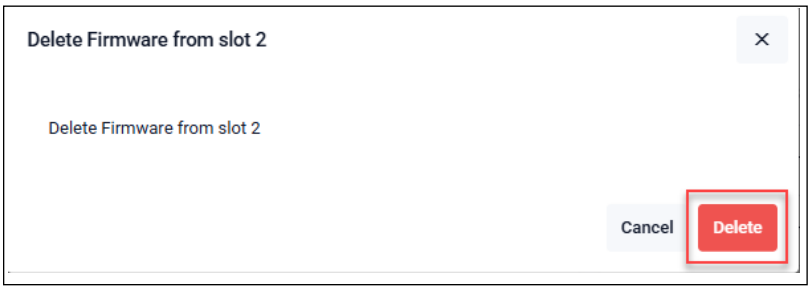
Firmware Slots

The **Firmware Slots** dialog displays the slot ID, status and build ID as well as the state of the slot. For example, if the firmware slot is good, or empty and is usable or active:

If you want to delete some firmware, click on the **Delete** button beside the Slot ID for the firmware version that you no longer want:

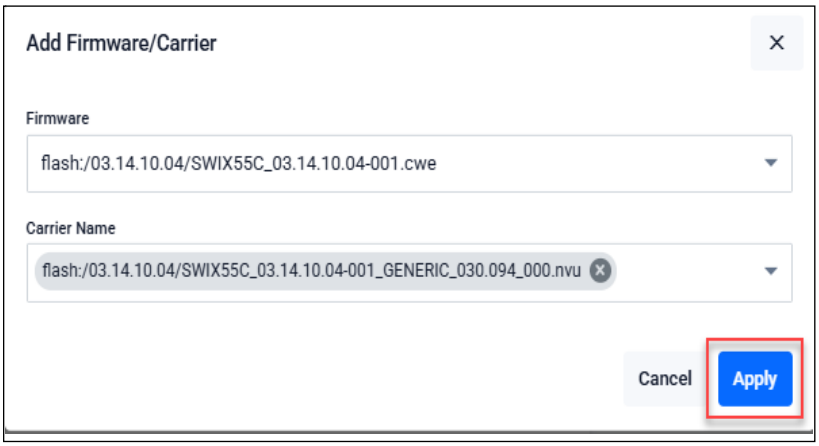


Confirm that you have selected the correct firmware version and slot, click the **Delete** button to proceed:

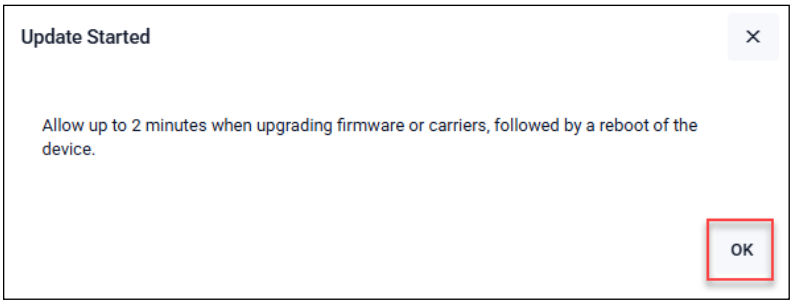


To add firmware and carriers click on the **+ Add Firmware/Carrier** button:

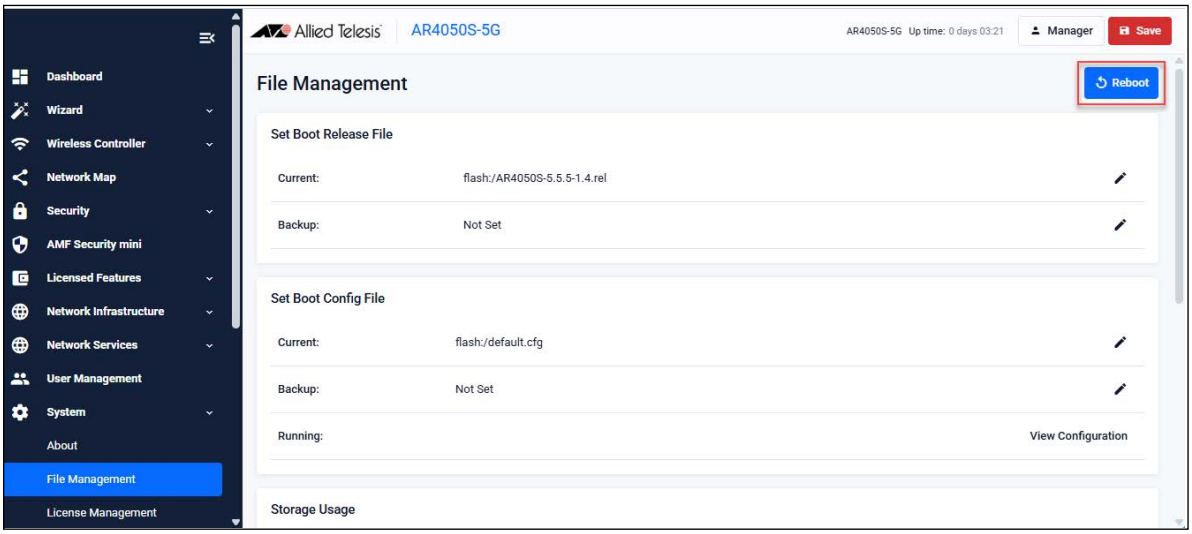
From the **Add Firmware/Carrier** dialog, select the required firmware file and the matching carrier name file (PRI) from their correct locations and click **Apply**: Get some data in here?



The following **Update Started** dialog appears, click the **OK** button to proceed:



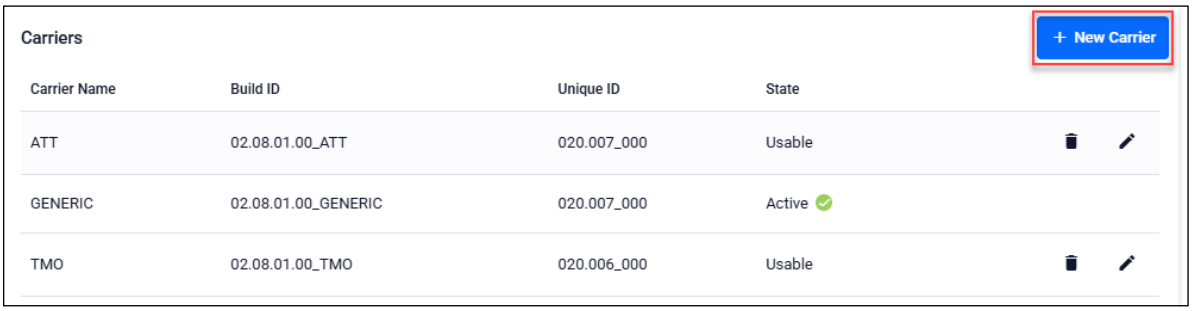
After allowing for a period of at least two minutes, you can then reboot your device. To reboot your router, from the **main menu**, select **System** > **File Management**:



Click the **Reboot** button and wait for the router to come back up.

From the **Carriers** tab, check the **Firmware Info** dialog to confirm that the firmware and carrier files you have upgraded are the preferred and current versions. Also check the **Firmware Slots** dialog and the **Carriers** dialog to confirm that the correct version is active.

Carriers The **Carriers** dialog displays the carrier name, which build version it is, the unique file name ID and its current state:



You can also delete PRI files using the **Delete** button. The **Set Active** button allows you to select which carrier you want as the active carrier.

If you need to add a new carrier PRI file, then you can click the **+New Carrier** button and then select which file you want to add. Click the **Apply** button to select the file: