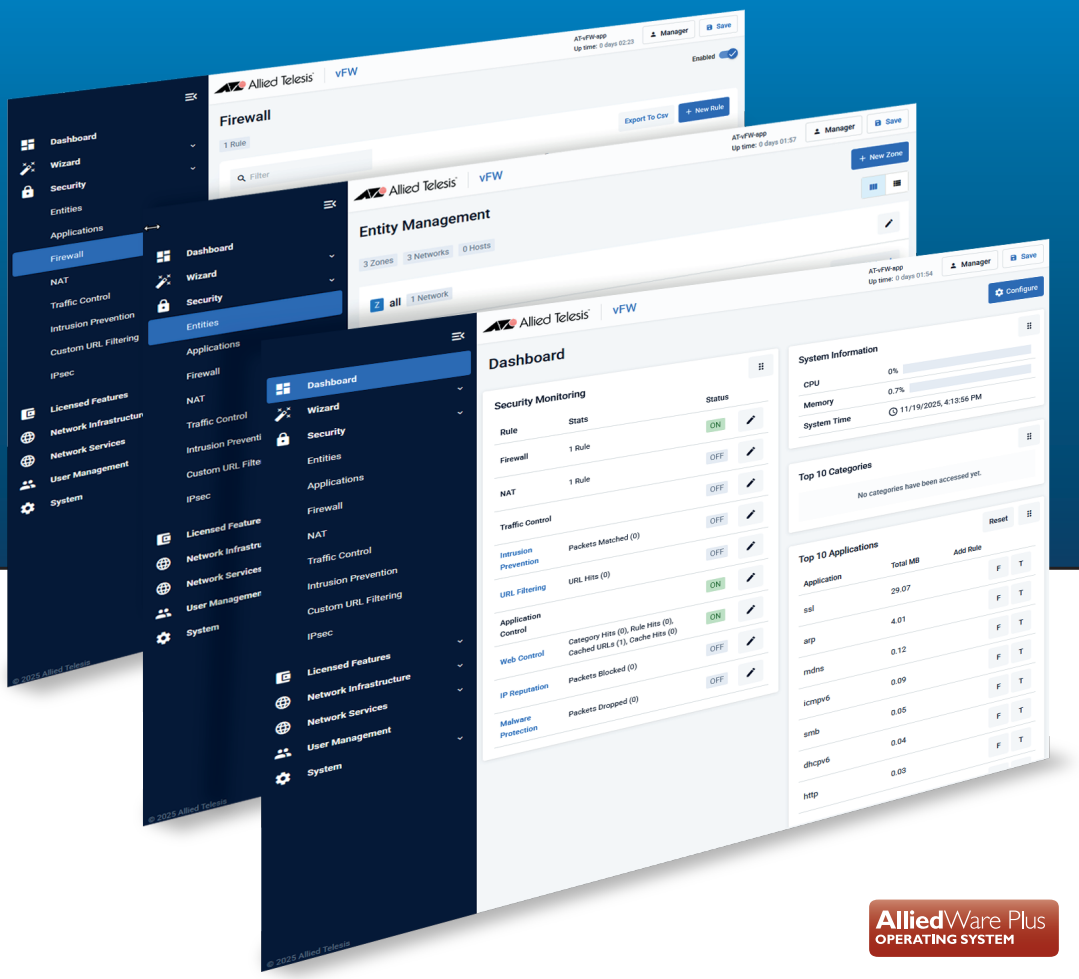
Release Notes

Allied Telesis™



AlliedWare Plus OPERATING SYSTEM

10GbE UTM Firewall 5.5.5-2.x

- 5.5.5-2.1 (NFV-APL-1.15.1)

Acknowledgments

Getting the most from this Release Note

To get the best from this release note, we recommend using Adobe Acrobat Reader version 8 or later. You can download Acrobat free from **www.adobe.com/**

Contents

What's New in 10GbE UTM Firewall v5.5.5-2.1 (NFV-APL-1.15.1)

Introduction

This release note describes the new features in 10GbE UTM Firewall v5.5.5-2.1.

You can obtain the software files from the Allied Telesis Support Portal.

Contact your authorized Allied Telesis support center to obtain licenses.

Caution: Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc.

While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

10GbE UTM Firewall

The Allied Telesis 10GbE Unified Threat Management (UTM) Firewall is an ideal integrated security platform for modern businesses. A powerful 10G firewall and threat protection is combined with comprehensive VPN capability. Easily and securely connect the head-office to branch-offices for an innovative high performance business solution.

It is a virtualized version of the AlliedWare Plus Next Generation Firewall and runs on the Vista Manager Network Appliance (AT-VST-APL-6 or VST-APL-10).

The software on the VST-APL consists of an ISO file containing the operating system, and an APP file for the 10GbE UTM Firewall application. When you upgrade, you must upgrade both the VST-APL operating system and the application to a supported set of versions, as shown in the following table:

Table 1: NFV-APL 1.15.1 software component versions

Software Component	Version
VST-APL Operating System	Version 1.13.1 ATVSTAPL-1.13.1.iso
AW+ Firewall application	Version 5.5.5-2.1 vfw-x86_64-5.5.5-2.1.app

New features in AW+ Firewall 5.5.5-2.1

This version includes new features and enhancements:

- "IPv6 management"
- "Remote Logging"
- "Host networking mode for application instances" on page 11
- and as described in the AlliedWare Plus Release Note.

IPv6 management

This version supports IPv6 management of the device.

All configuration and fields in the VST-APL GUI that previously supported IPv4 addresses now also support IPv6 addresses.

Note that if the VST-APL is set to accept DHCP addressing (this is the default), DHCP will accept an IPv6 address if offered. You can then manage the device completely using IPv6 addressing.

If an IPv6 address is not offered via DHCP, you will initially need to access the device via IPv4. You can then configure IPv6 addresses as required and manage the device via IPv6 from then on.

Remote Logging

From version 5.5.5-1.3 (NFV-APL1.14.3), you can configure the device to send log messages to:

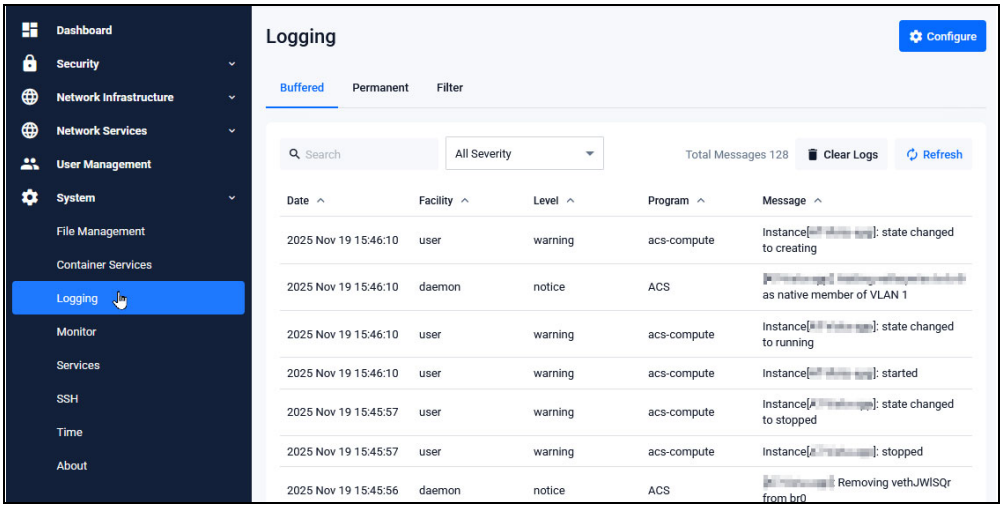
- a remote syslog server
- an email address.

You can use this to monitor the device and to alert a user to serious issues.

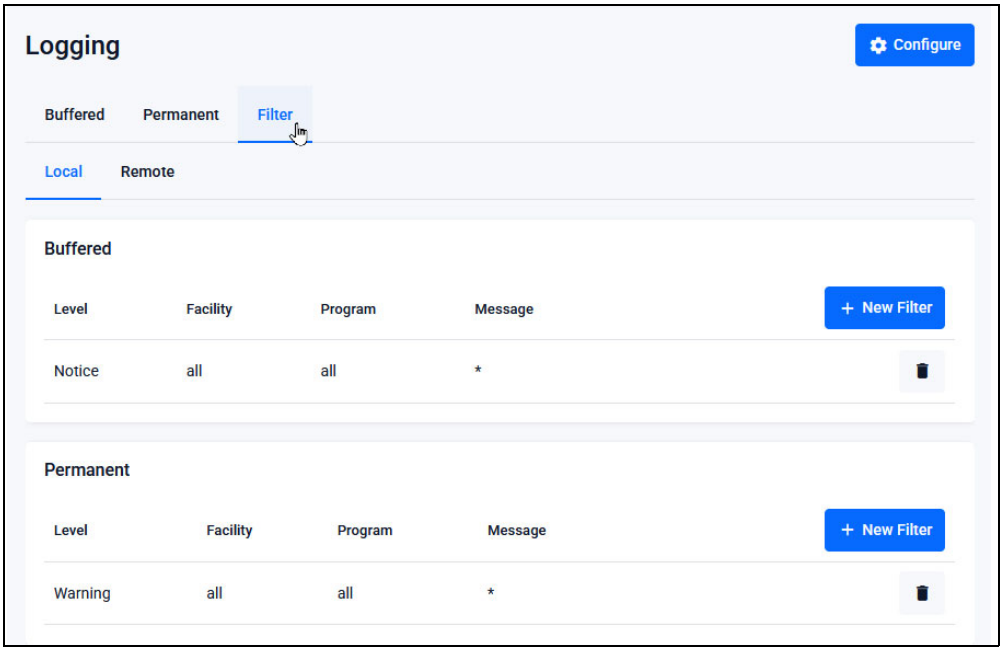
As in previous versions, the device also sends log messages to the permanent and buffered logs on the local device.

Send log messages to a remote syslog server

1. In the VST-APL menu, click **System** > **Logging**.

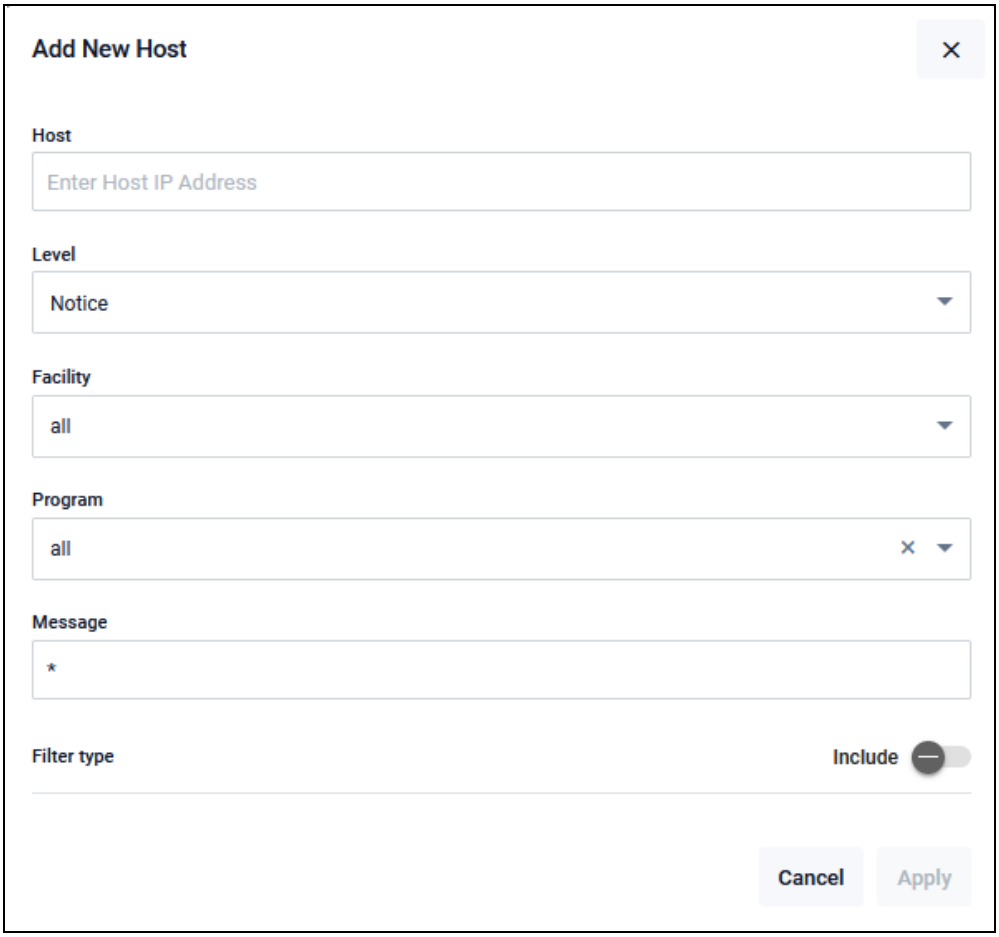


2. In the Logging page, click **Filter**.



3. Click **Remote**.

4. Click **+ New Host**.



5. Enter the IP address of the syslog **Host** to send log messages to.

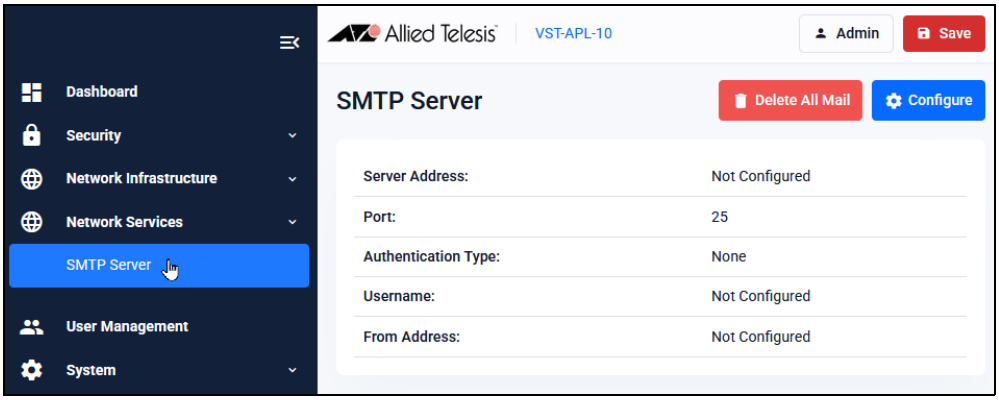
6. Set the filter parameters to select which messages to send ("Filter the messages to send" on page 10).

7. Click **Apply**.

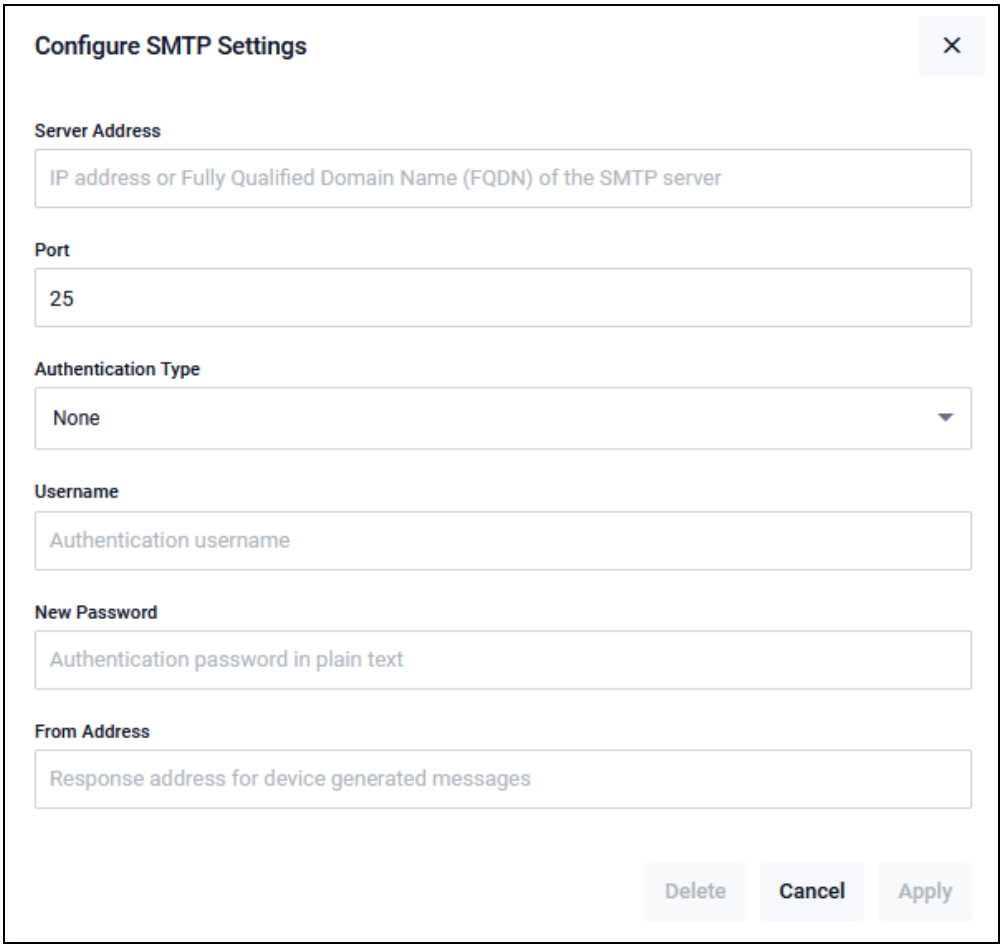
Configure an SMTP server.

To send messages by email, you must configure an SMTP server.

1. In the VST-APL menu, click **Network Services** > **SMTP Server**.



2. Click the **Configure** button at the top of the SMTP Server page.

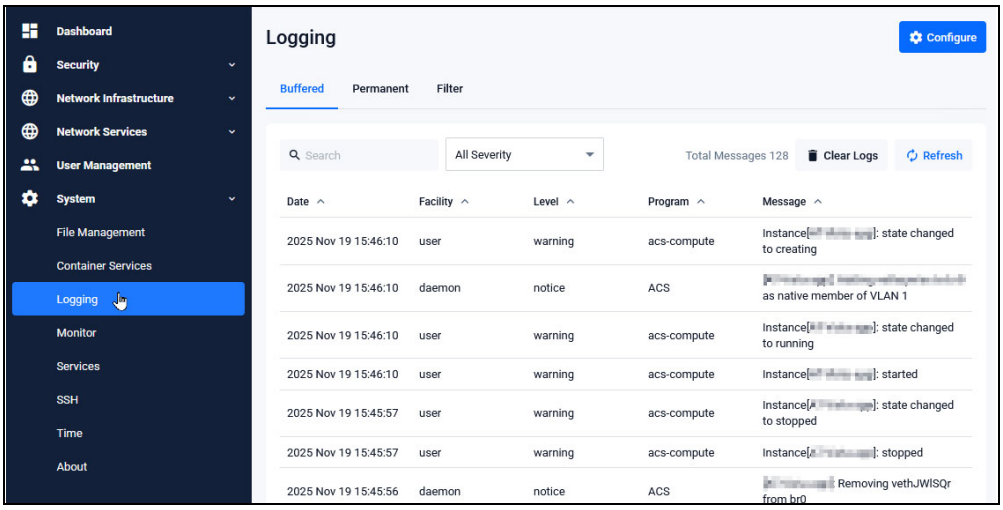


3. Configure SMTP settings based on your mail server configuration:
   - Enter the **Server Address**—the IP address or domain name of the SMTP server.
   - Enter the **Port** to use for the SMTP server (port 25 by default).
   - Select the **Authentication Type** to apply (None, Login, CRAM-MD5, or Plain).
   - Enter your user name and password for the SMTP server if required for authentication.
   - Enter the **From Address**. Log message emails will show that they were sent from this address.

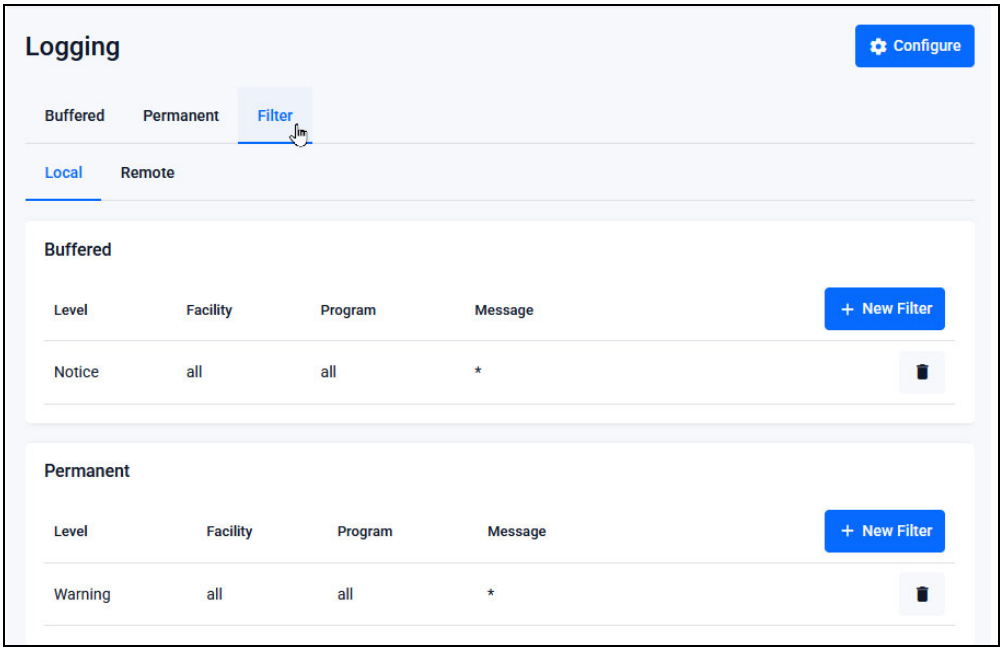
4. Click **Apply**.

Send log messages to an email address

1. In the VST-APL menu, click **System** > **Logging**.

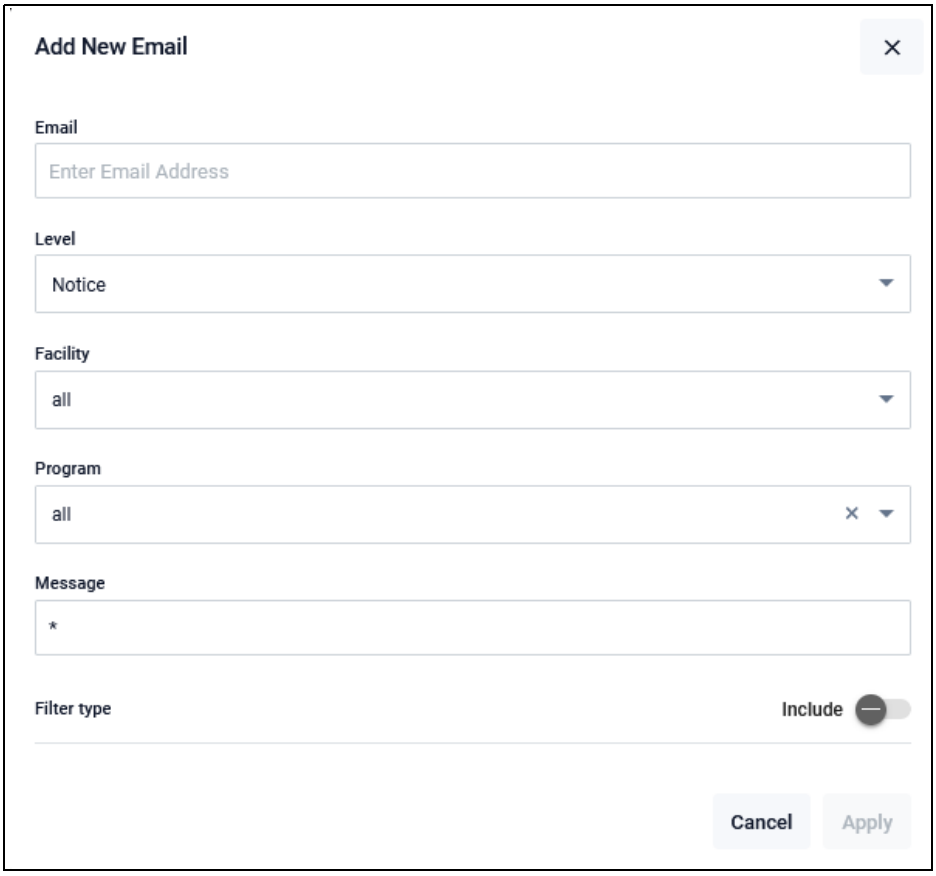


2. In the Logging page, click **Filter**.



3. Click **Remote**.

4. Click + **New Email**.



5. Enter the **Email** address to send log messages to.

6. Set the filter parameters to select which messages to send ("Filter the messages to send" below).

Filter the messages to send

By default, the device will send all messages with severity level Notice or higher. To change which messages it sends, specify filter parameters. You can add more filters after the syslog or email receiver has been set up. You can also create filters for the permanent and buffered logs on the device.

1. Select the **Level** (**Notice** by default). Messages at or above this severity level match the filter.

2. Select the **Facility** or match messages from all facilities.

3. Select the **Program** or match messages from all programs.

4. Enter a text string in the **Message** field to send only messages that include this string. Wild cards are implicit.
   By default, set with an asterisk "*", all message strings are included.

5. When you first set up remote logging, set the filter to **Include**. This sets it to send all the messages that match the filtering fields above.
   Once you have created this initial filter, you can refine the filtering by setting up additional filters to include or exclude particular messages.

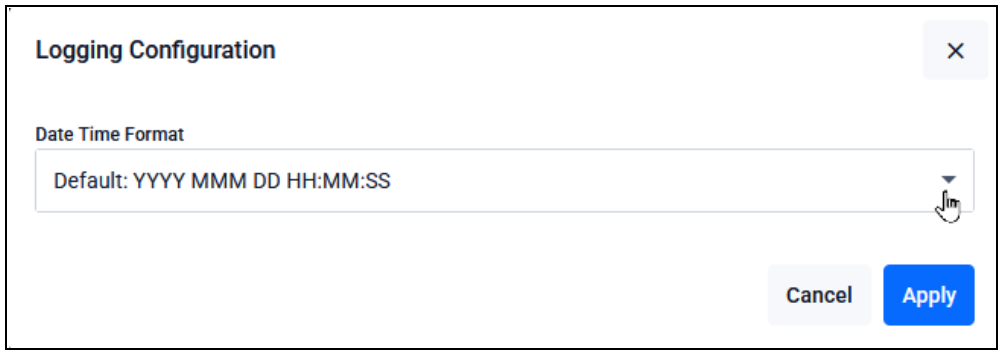
6. Click **Apply**.

Set the date-time format for log messages

The date and time when a log message is generated will be included in all log messages in one of these formats:

- YYYY MMM DD HH:MM:SS (default)
- YYYY-MM-DDThh:mm:ssTZD (ISO standard)

To set this, click **Configure** at the top right of the Logging page, and select the format required. Click **Apply**.



Host networking mode for application instances

This version supports network mode **Host** in addition to the previous network mode **Private**.

In Private mode, you must configure the network, including routing to and from the application. The advantage is that multiple services, for instance web servers, can run via a single network port. This suits many networks.

In Host mode, you do not need to configure the private network and routing. However, multiple services cannot use the same network port, so you must configure each service to use a different port. For instance, you cannot have two web servers running on port 443, and must configure each web server to use a different port.

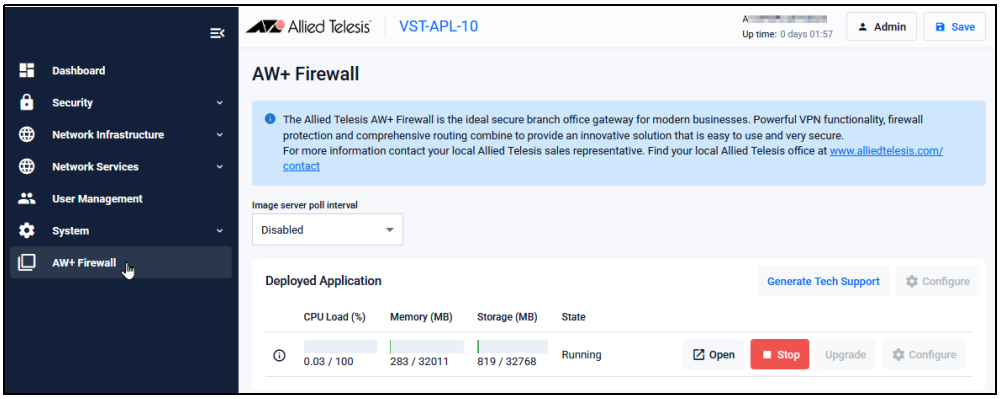
Configure network mode Host

You can configure network mode Host:

- when you create the Firewall application instance, or
- by stopping the app instance, reconfiguring it, and starting it again.

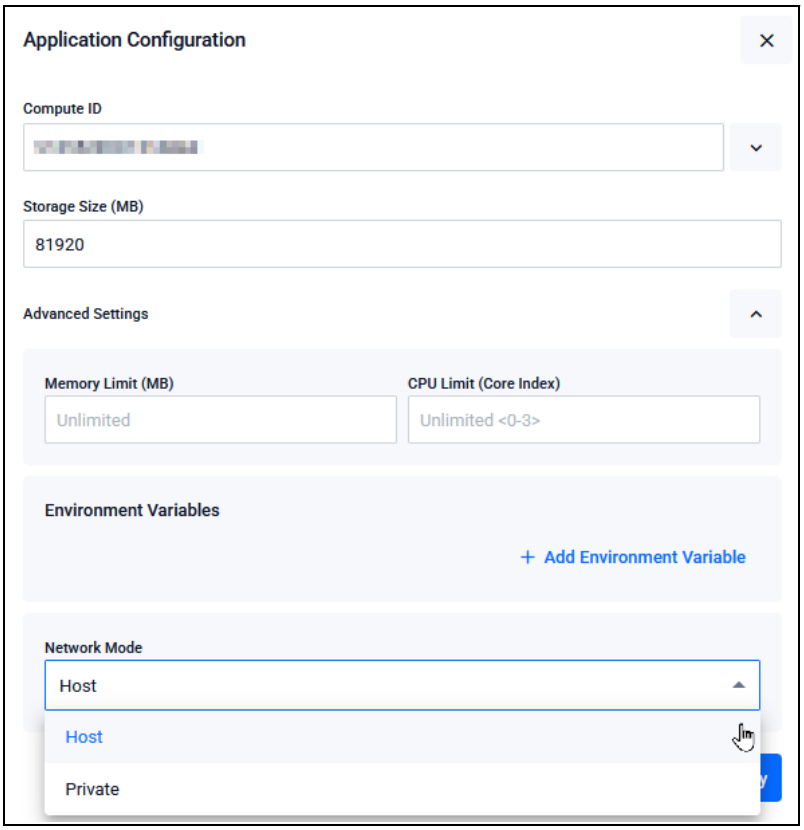
The default setting is Private.

1. From the VST-APL menu, select **AW+ Firewall**.



2. In the AW+ Firewall page, if the app instance is running, click **Stop** and wait for it to stop. Click **Configure**.

3. In the Application Configuration dialog box, expand **Advanced Settings**. In the **Network Mode** drop down list, select **Host**.



4. Click **Apply**.

Important Considerations Before Upgrading

This section describes changes that may affect the VST-APL appliance, the Firewall application, or your network's behavior if you upgrade. Please read it carefully before upgrading.

Web Control

Interface matching in Web Control is not supported in the Firewall app from version 5.5.3-2.1 onwards.

In a web control entity configuration like the one below, the **interface eth** portion of the **ip subnet** command will have no effect.

```
awplus(config-web-control)#exit
awplus(config)#zone private
awplus(config)#network engineering
awplus(config-network)#ip subnet 192.168.1.0/24 interface eth1
```

If you configure a rule using the **rule (web control)** command, the device sends this message to the command line and to the log:

```
% Entity "private.engineering" contains interface matches - only
the subnet portion is used by Web Control
```

Obtaining User Documentation

10GbE UTM Firewall documentation

The Datasheet, Installation Guide, User Guide, and Release Notes for 10GbE UTM Firewall are available from:

- 10GbE UTM Firewall Datasheet
- Vista Manager Appliance (VST-APL) Installation Guide.
- 10GbE UTM Firewall Release Note
- AlliedWare Plus Release Note
- Isolating Traffic with the 10GbE UTM Firewall Feature Overview and Configuration Guide
- Getting Started with the Device GUI on UTM Firewalls
- Vista Manager Network Appliance (VST-APL) User Guide

AlliedWare Plus documentation

For full AlliedWare Plus documentation, see our online documentation library on our website, alliedtelesis.com.

Upgrading the VST-APL appliance and the firewall app

To upgrade, you need to:

Note that some elements of the following screenshots may not match recent design updates.

Backup the system

You can use the Backup and Restore feature to create a back-up file for a VST-APL Network Appliance.

The back-up file records, and can restore:

- the appliance configuration
- the APP file stored in the appliance persistent memory.
  These contain the image of the application software.
- snapshots of the application instance. This is a snapshot of the configuration and application data of an application instance on the device.

Backup and restore: back up the appliance

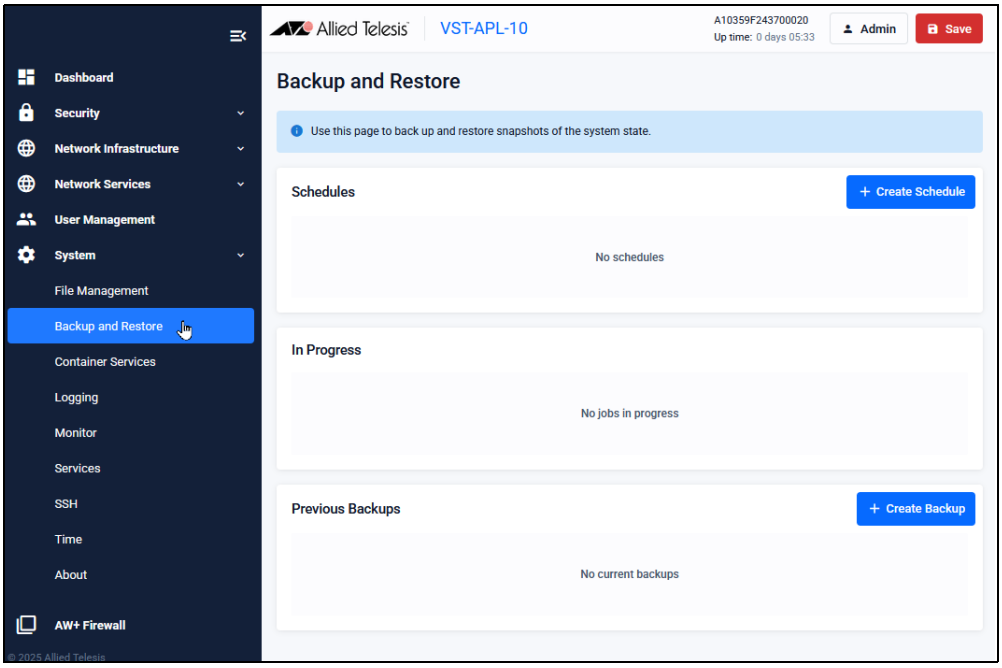
To back up all the appliance configuration, any application image files (.app) and the application data for the application instance, follow these steps. This provides a backup that can later be used to restore the application instance or the application configuration and application instance.

1. If there is unsaved appliance configuration that you want to include in the back-up, click the **Save** button at the top of the VST-APL GUI page.

2. Connect external media for storing the back-up to the appliance's USB port. The external media must have one of the following supported formats: FAT32, exFAT, ext2, ext3 or ext4.

   Note that if the external media file system format does not support a sufficiently large file size, the backup will fail. Choose a different external media with a file system format that supports a larger maximum file size, such as ext4.

3. In the VST-APL menu, navigate to **System** > **Backup and Restore**.



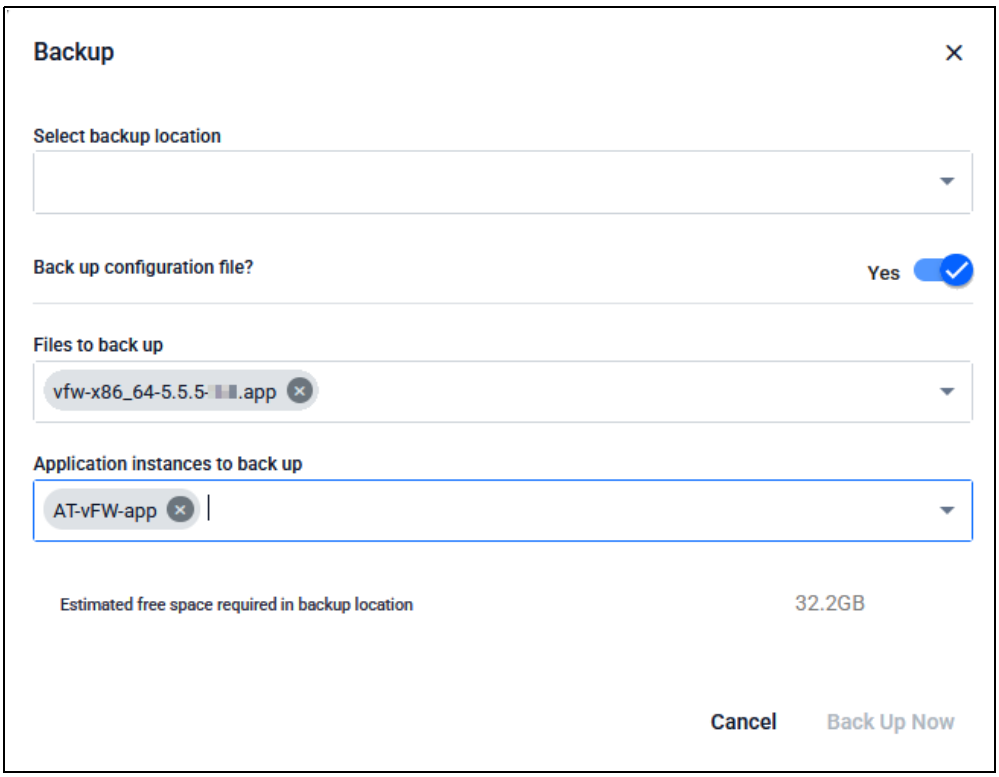
4. On the **Backup and Restore** page, click **+ Create Backup** at the top right of the **Previous Backups** panel.

   The **Backup** dialog box opens, showing the default settings for the back-up you are about to create, and the storage space it estimates that you need to have free on the external media.

5. In the **Backup** dialog box, click the down-arrow at the right of **Select backup location** and from the locations available, choose the external media connected previously.

   Check that the backup location has sufficient free space for the new back-up file. You can see the free space available on the backup media in this panel. You can also see the file system of the external media by navigating to the **System** > **File**

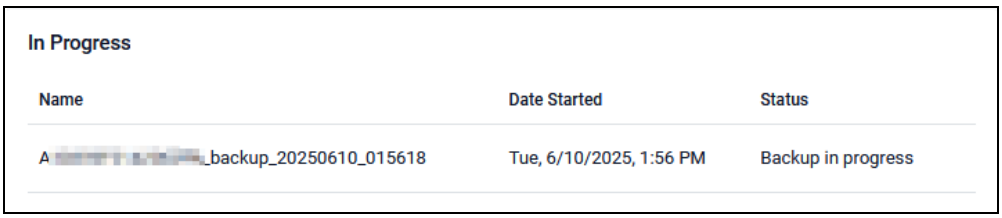
Management page and then clicking in the file path at the top of the **File System** (fs) panel.



6. By default, the back-up configuration sets the device to back up everything it can. Check that the following are selected for backup:

- **Back up configuration file?** is set to **Yes**. This sets the file default.cfg to back up.
- the application image file stored in the device's file system: **vfw-x86_64-x.x.x.app**
- the firewall application instance on the device.
  If an application instance to back up does not show the firewall app, then make sure it is Running or Stopped. (To check this, from the VST-APL menu, navigate to the VST-APL page for the application or to System > Container Services).

7. Click the **Back Up Now** button at the bottom right. The backup dialog box closes, and the current back-up job shows in the **In Progress** panel in the Backup and Restore page. Backing up may take several minutes.



The backup filename will have a format like this:

`<device-serial-number>_backup_YYYYMMDD_HHMMSS.abk`

for example:

`A103590000000000_backup_20220113_011350.abk.`

If the appliance estimates that the space required for the back-up is close to the free space available on the external media, a pop-up window with a warning message

appears after clicking Back Up Now. Consider providing more free space on the external media.

When the backup is complete, it disappears from the In Progress panel, and shows in the **Previous Backups** panel. Here you can see the time (Last Modified) and file size of the back-up. Status **Valid** confirms that the backup file has been stored successfully with a valid checksum file.

For more information about the Backup and Restore feature and how to restore a VST-APL system or application, see the Vista Manager Network Appliance Technical Document page on our website.

Backup application data

We recommend backing up application data regularly. You should also backup the application data before following this upgrade procedure. See the relevant application's user manual for information on how to backup an application.

Download component software

You need the new image file in the appliance persistent storage to change the running software. Make sure to upgrade the operating system and the application, so that they match.

To see which version of the VST-APL operating system the appliance is currently running, use the VST-APL GUI to navigate to the **System** > **About** page. To see the application files loaded in the appliances memory, navigate to the **System** > **File Management** page. To see the current version of an application running on the appliance, go to the GUI page for the application by clicking on its menu item, and hover over the instance information icon in the Deployed Application panel.

Caution: Ensure you obtain the software image files from Allied Telesis. If you try to install software that is not provided by Allied Telesis, there is risk of corrupting the installation.

1. Download the following software files from the Allied Telesis Support Portal. Save them to a directory that the appliance can access, such as the device your GUI browser is running on.
   - **ATVSTAPL-x.x.x.iso** —the appliance software operating system, where **x.x.x** is the new version number of the operating system.
   - **vfw-x86_64-x.x.x.app**—the application image file for the new version of the 10GbE UTM Firewall app, where **x.x.x** is the new version number of the app you are installing.

Upgrade the operating system and Firewall application

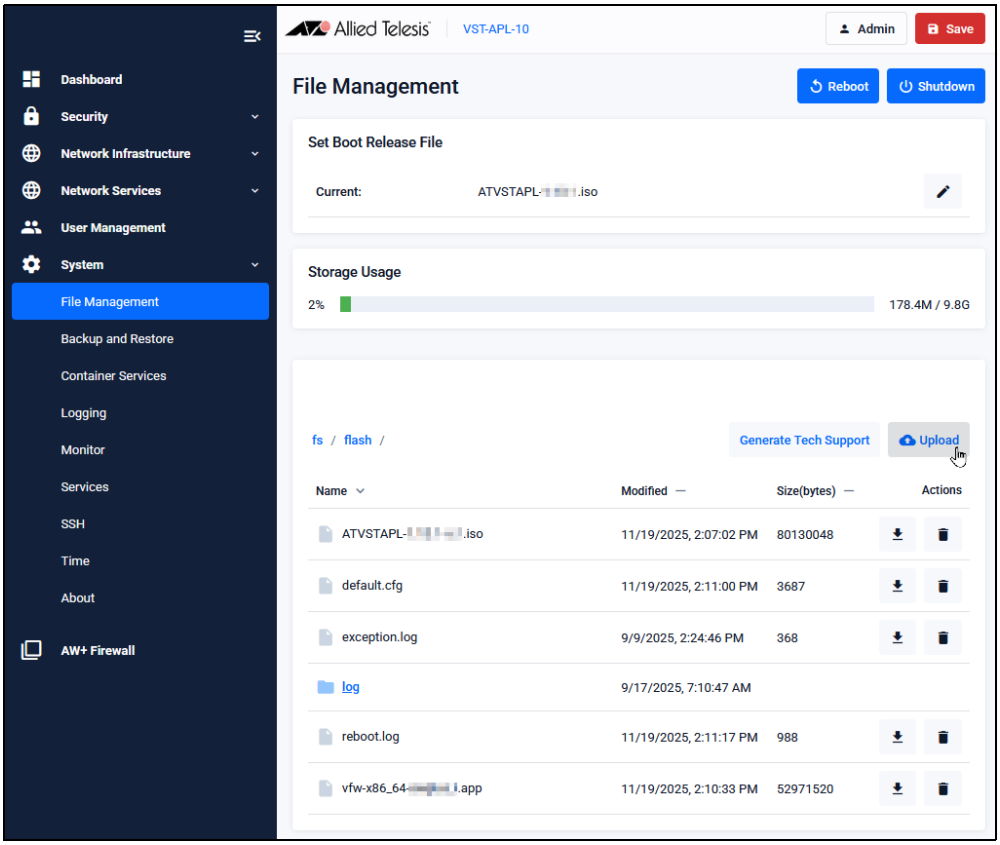
Before upgrading the operating system, make sure to:

- "Backup the system" on page 14
- "Download component software" on page 17

To upgrade the VST-APL operating system, follow these steps.

Upload the new software version files

1. Log in to the VST-APL GUI.
2. Navigate to the **File Management** page (**System**->**File Management**).



3. Click the **Upload** button, opening up the **File Upload** sub-menu.
4. Navigate to the **ATVSTAPL-x.x.x.iso** file, select and upload it.
5. Upload the **vfw-x86_64-x.x.x.app** file in the same way.

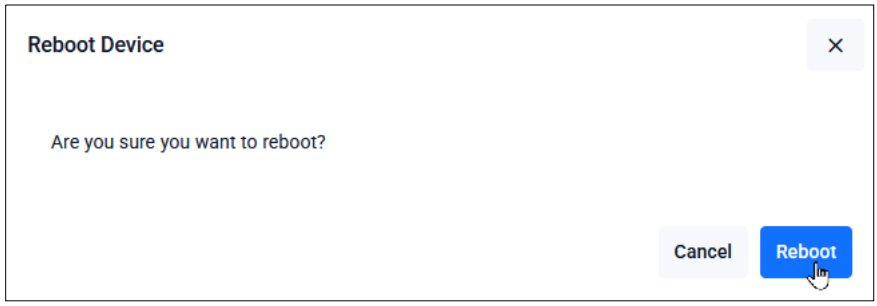
Upgrade the operating system

1. In the **File Management** page **Set Boot Release File** panel, browse to select the new software version file.

Click **Apply**.

2. Reboot the appliance by clicking the **Reboot** button at the top right of the **File Management** page.

3. Click **Reboot** again to confirm.



The appliance will shut down any applications that are running, install the new version of the VST-APL operating system, and restart any applications that were running when the appliance configuration was last saved. This may take several minutes. The appliance configuration, including IP addressing, is retained from the last time it was saved.

4. When the upgrade has completed, you will need to re-authenticate to access the appliance.

5. To verify the currently running software version, log in to the VST-APL Web GUI and navigate to the **System > About** page. The **Software Version** (the.iso file version) should agree with the VST-APL operating system version.

Upgrade the 10GbE UTM Firewall app

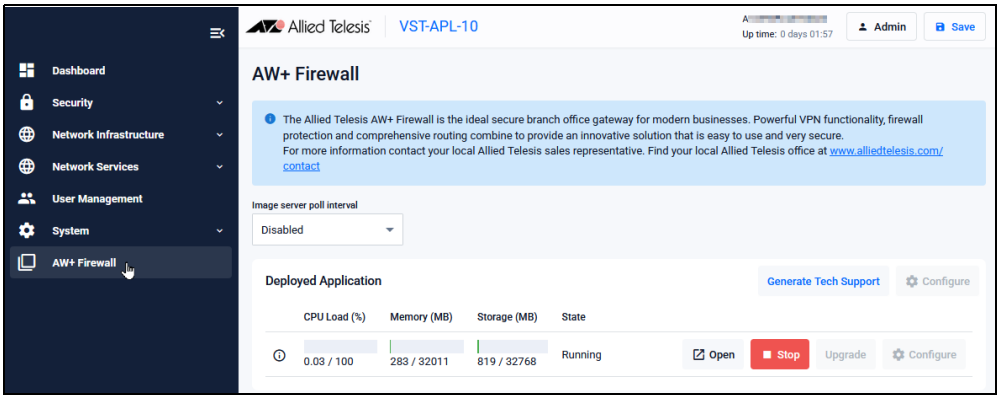
Before upgrading the firewall app, you need the image file for the app on your appliance ("Upload the new software version files" on page 18):

- **vfw-x86_64-x.x.x.app**

where **x.x.x** is the new version number you are installing.

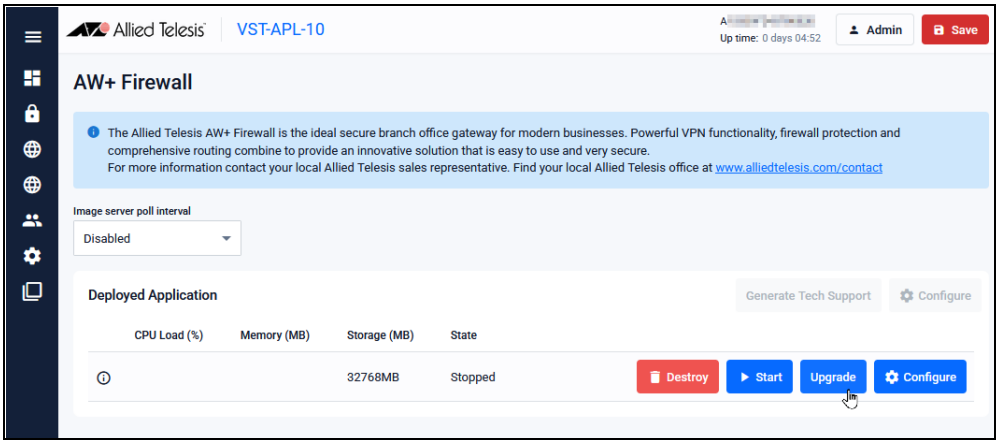
1. Log in to the VST-APL GUI.

2. Select **AW+ Firewall** from the main menu.

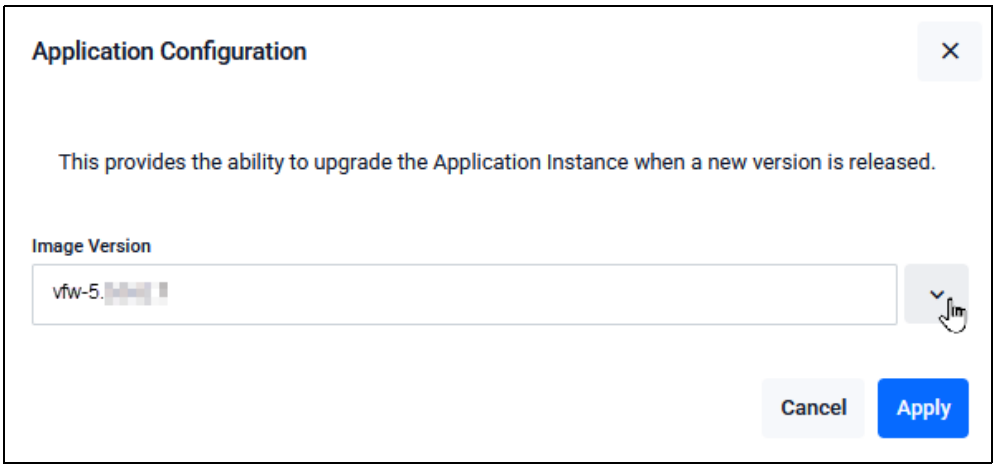


3. If the AW+ Firewall is running, click on the **Stop** button.

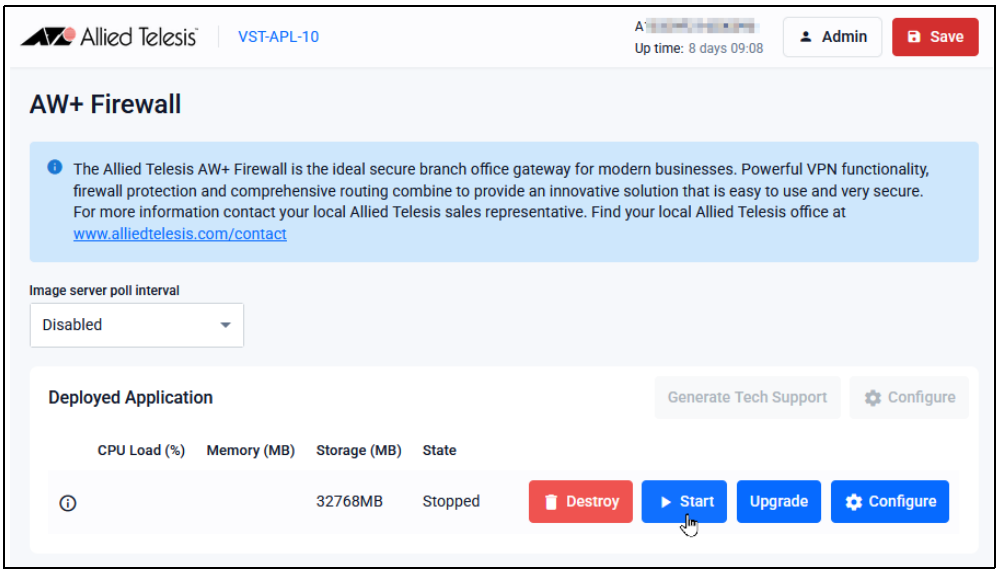
4. Once the AW+ Firewall app has stopped running, click the **Upgrade** button.



5. In the **Application Configuration** dialog box, expand the Image Version, select the new version, and click **Apply**.



6. Click on the **Start** button to restart the AlliedWare Plus Firewall.



Remove obsolete files from memory

You can make more space available in the device's persistent memory by removing obsolete files. We recommend removing the .iso file for the previous version of the operating system. Keep the current versions.

1. From the VST-APL dashboard, navigate to the **System** > **File Management** page.

2. Click the **Delete** button to the right of the obsolete files you want to remove.

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com