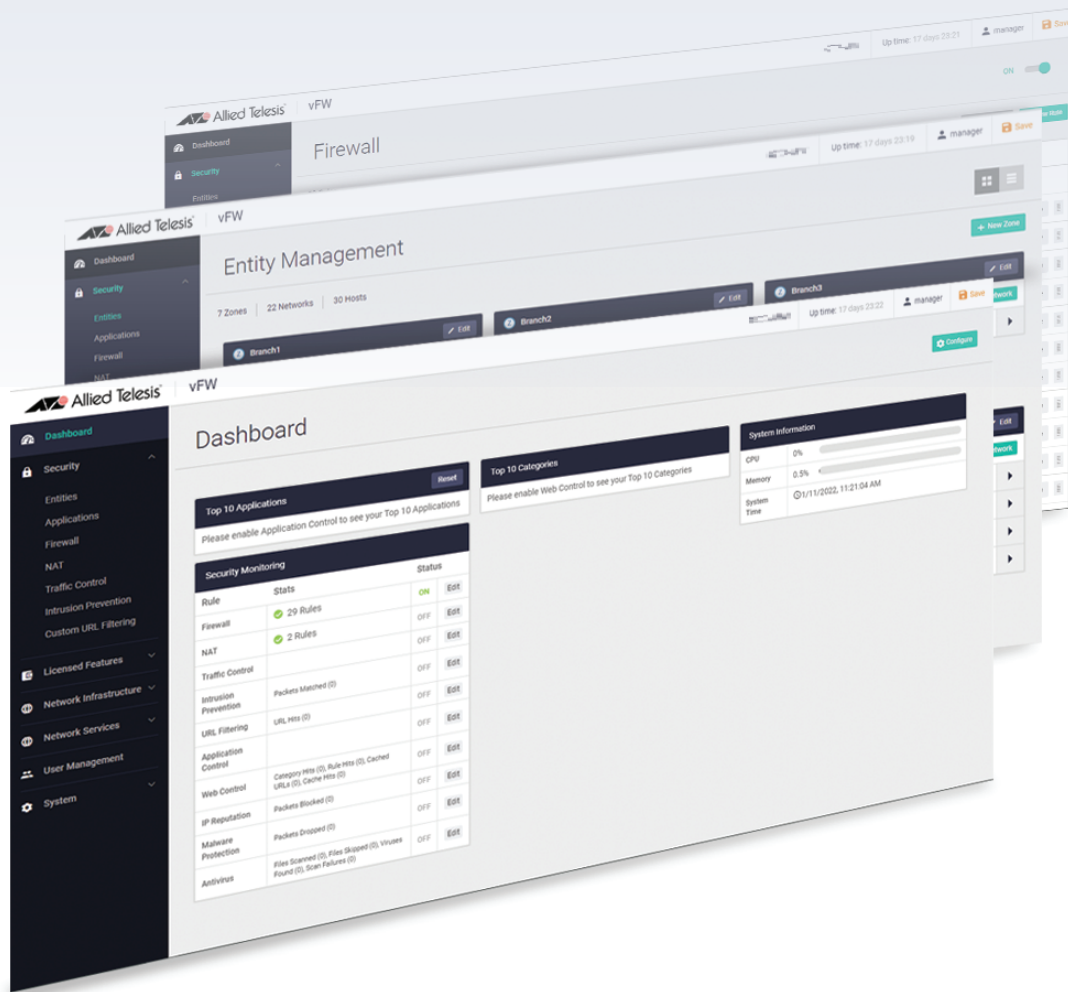


Release Note for 10GbE UTM Firewall 5.5.3-2.x



» 5.5.3-2.1 (NFV-APL-1.9.1)

AlliedWare Plus
OPERATING SYSTEM

Acknowledgments

©2023 Allied Telesis Inc. All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Allied Telesis, AlliedWare Plus, Allied Telesis Management Framework, EPSRing, SwitchBlade, VCStack and VCStack Plus are trademarks or registered trademarks in the United States and elsewhere of Allied Telesis, Inc. Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Additional brands, names and products mentioned herein may be trademarks of their respective companies.

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 v5.5.3-2.1 (NFV-APL-1.9.1).....	4
Important Considerations Before Upgrading	8
Obtaining User Documentation	8
Upgrading the VST-APL appliance and the firewall app.....	9

What's New in 10GbE UTM Firewall v5.5.3-2.1 (NFV-APL-1.9.1)

Introduction

This release note describes the new features in 10GbE UTM Firewall v5.5.3-2.1.

You can obtain the software files from the [Software Download area of the Allied Telesis website](#). Log in using your assigned email address and password.

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-1.9.1 Software component versions

Software Component	Version
VST-APL Operating System	Version 1.9.1: ATVSTAPL-1.9.1.iso
AW+ Firewall application	Version 5.5.3-2.1 vfw-x86-64-5.5.3-2.1.app

New features in 5.5.3-2.1

This version adds:

- “Support remote shutdown using SSH or Telnet”
- “USB unmount button” on page 6
- “Disk storage input/output process monitoring” on page 7
- “Increase log storage” on page 7
- new features and enhancements as described in the [AlliedWare Plus Release Note](#).

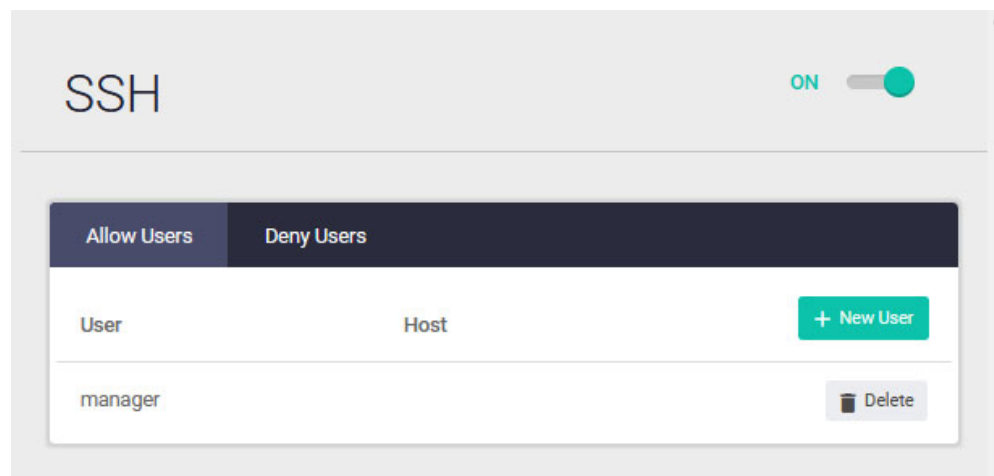
Support remote shutdown using SSH or Telnet

You can now enable users to access the device command line remotely using either SSH (recommended) or Telnet and power down the VST-APL. Where there is a risk of power overload or loss of power, this can protect the storage hardware in the device from physical damage.

Note that enabling Telnet or SSH allows remote control of the device. It is important to ensure that the device is secured both by network access control (firewall) and by strong credentials.

To enable a user to power down the device remotely via SSH:

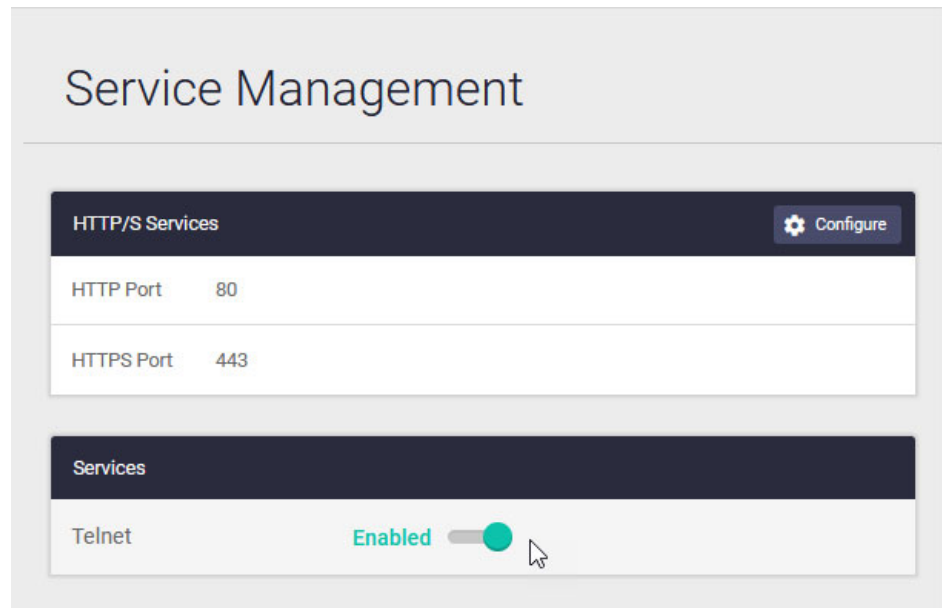
1. From the VST-APL menu, navigate to **System > SSH**.
2. In the **SSH** page, enable SSH. Drag the toggle at the top right to **ON**. This makes SSH available on port 22.
3. In the **Allow Users** tab, click **+ New User**. Type in the username to allow.



To enable users to power down the device remotely using Telnet:

1. In the VST APL menu, navigate to **System > Services**.

2. In the Services panel in the Service Management page, move the Telnet toggle to **Enabled**. This makes Telnet available on port 23.



To power down the VST-APL device remotely:

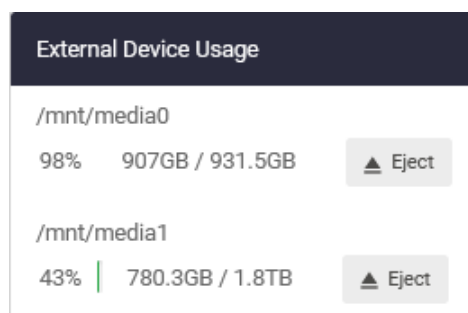
1. Connect remotely to the device CLI by using SSH (port 22) or Telnet (port 23).
2. Enter the username and password for the device.
3. Power it down by using the command:

```
AT-VST-APL-10# poweroff
```

USB unmount button

You can now safely unmount a specific USB memory device by using a new **Eject** button in the appliance GUI. To remove a USB device:

1. From the side menu, navigate to **System > File Management**.
2. On the File Management page, in the **External Device Usage** panel, click the **Eject** button for the external USB memory device.

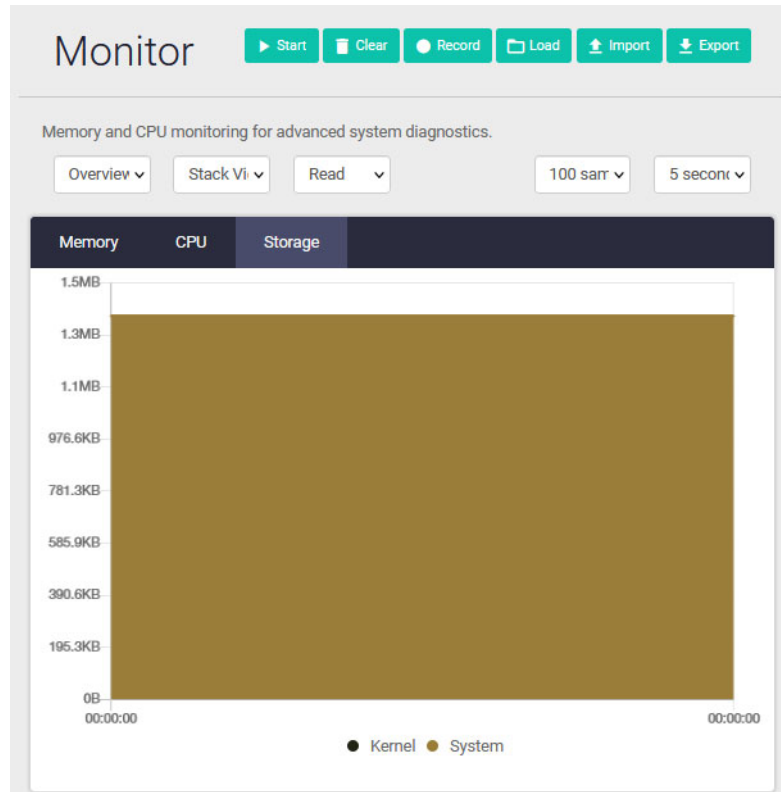


3. Remove the USB device physically from its port.

Disk storage input/output process monitoring

The appliance GUI now supports monitoring the Input/Output for the internal device storage. To access this monitoring:

1. From the side menu, navigate to **System** > **Monitor**.
2. Click the **Storage** tab.



For more information about how to use Monitoring on the device, see the “Vista Manager Network Appliance (VST-APL) User Guide”.

Increase log storage

From this version, the size of the buffered and permanent logs has increased from 50KB to 5MB.

For more information about Logging, see the “Vista Manager Network Appliance (VST-APL) User Guide”, available from [Vista Manager Network Appliance \(VST-APL\) Technical Documents](#).

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:

- “Backup the system” on page 9
- “Backup application data” on page 11
- “Download component software” on page 11
- “Upgrade the 10GbE UTM Firewall app” on page 13
- “Remove obsolete files from memory” on page 14

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.

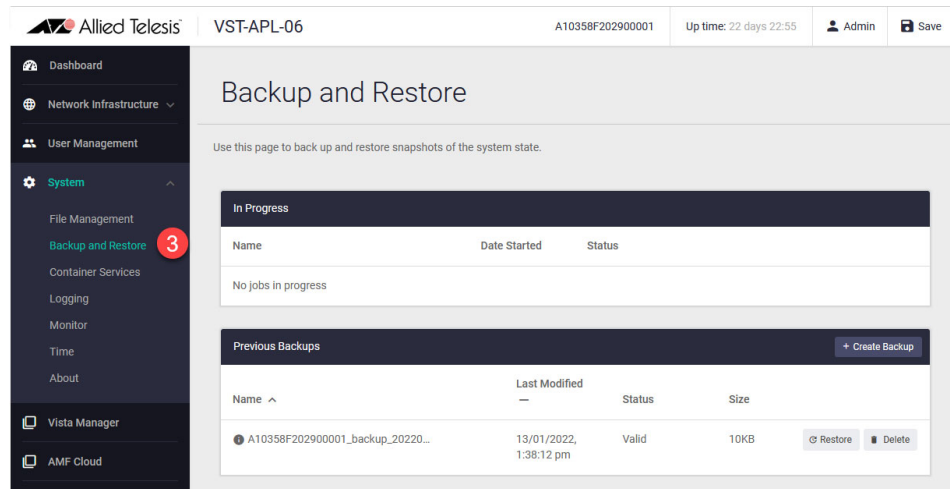
Backup and restore: back up the appliance

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.

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



- 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.

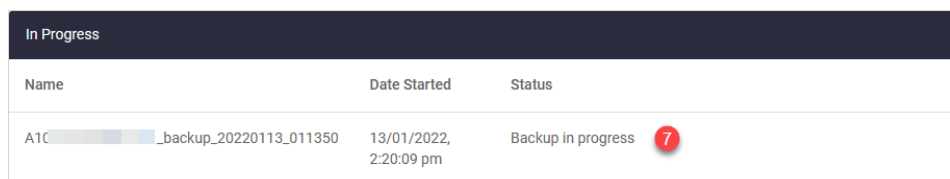
- In the **Backup** dialog box, click the down-arrow at the right of **Select backup location** and from the locations available, choose the external media connected previously.

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.

- 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).

- Click the green **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.



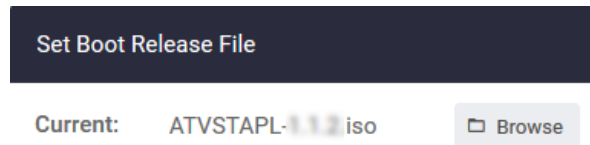
Upgrade the operating system

Before upgrading the operating system, make sure to:

- “Backup the system” on page 9
- “Download component software” on page 11

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

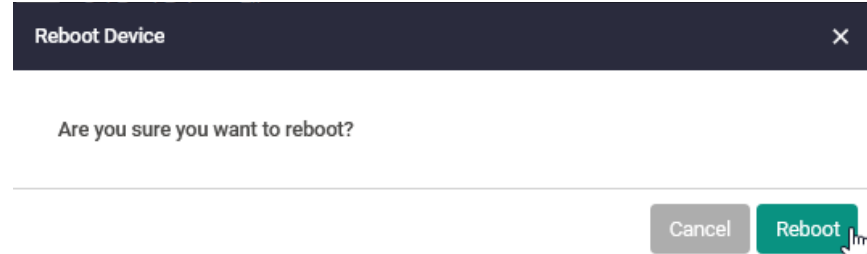
1. In the **File Management** page **Set Boot Release File** panel, click **Browse**.



2. Select the new software version and click **Apply**.
3. Reboot the appliance by clicking the green **Reboot** button at the top right of the **File Management** page.



4. 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.

5. When the upgrade has completed, you will need to re-authenticate to access the appliance.
6. To verify the currently running software version, log in to your VST-APL Web GUI, and navigate to the **System > About** page. The **Software Version** should agree with the VST-APL Web GUI version.

Upgrade the 10GbE UTM Firewall app

The following section will guide you through the instructions for upgrading 10GbE UTM Firewall on your device.

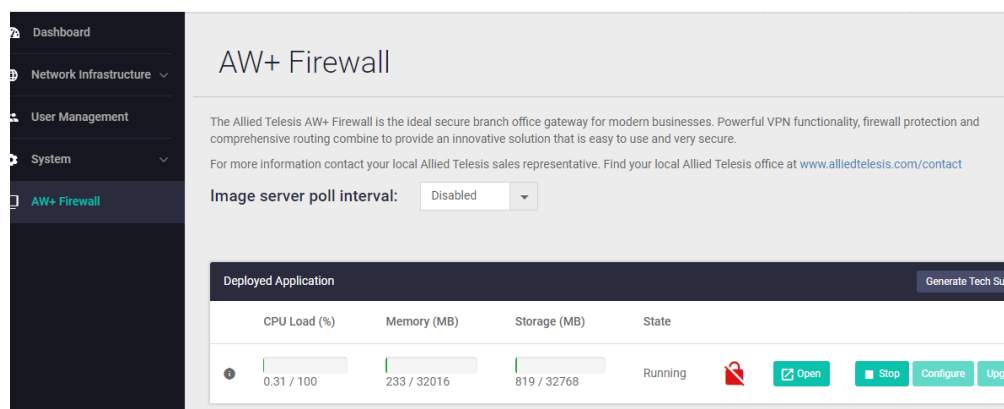
Before upgrading the firewall app, you need the image file for the app:

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

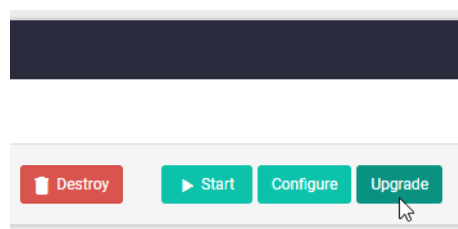
where **x.x.x** is the new version number you are installing.

Upload the new version and update the 10GbE UTM Firewall app

1. Log in to the Device GUI.
2. Navigate to the **File Management** page (**System->File Management**).
1. Click the **Upload** button, opening up the **File Upload** sub-menu.
2. Navigate to the **vfw-x86_64-x.x.x.app** file and select it.
3. Once the file is uploaded, select **AW+ Firewall** from the main menu.



4. If the AW+ Firewall is running, click on the **Stop** button.
5. Once the AW+ Firewall has stopped running, click on the **Upgrade** button.



- Click on the arrow to open the drop-down, select the new version, and click **Apply**.

Application Configuration

This provides the ability to upgrade the Application Instance when a new version is released.

Image Version 5.5.2-0.1

vfw-5.5.1-2.1

vfw-5.5.2-0.1

Cancel Apply

- 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.

- From the VST-APL dashboard, navigate to the **System > File Management** page.
- Click the **Delete** button to the right of the obsolete files you want to remove.