

Vista Manager Network Appliance (VST-APL)

User Guide

Introduction

The Vista Manager Network Appliance (VST-APL) includes tools to simplify and centralize management and security of your network. There are two possible ways to use the VST-APL: as a network management and monitoring device with Vista Manager, or as a firewall.

With Vista Manager, the appliance provides an integrated graphical view for monitoring and management of wired, wireless and third-party devices by combining:

- Vista Manager to provide an integrated graphical display of your network
- AMF Cloud to manage Allied Telesis wired switches and firewalls
- Wireless Controller (AWC) to manage and automatically optimize Allied Telesis wireless network devices
- SNMP or SNMP-based Trap Receiver to monitor a broad range of third-party devices
- AMF Security to defend your network from internal threats
- AT-RADgate for authentication.

As a firewall, the appliance provides:

- 10GbE UTM Firewall, a virtualized version of the AlliedWare Plus UTM Firewall.

What information will you find in this document?

The web-based GUI allows you to manage the appliance and to set up and access applications to run on it. This guide describes how to configure the VST-APL. Before using the instructions in this User Guide, you will need to connect cables, power it up, and established your initial connection with the VST-APL GUI (see [the Installation Guide](#)).

Contents

Introduction	1
Products and software versions that apply to this guide.....	4
Deploying and licensing VST-APL as a Vista Manager appliance.....	4
Deploying and licensing VST-APL as a 10GbE UTM Firewall	6
Getting connected to the VST-APL	8
Connect to the web-based Device GUI	8
Change the manager password	9
Set up network interfaces	9
Save the VST-APL configuration	11
Getting started with Vista Manager and associated applications	11
Example: activate the applications	14
Getting started with 10GbE UTM Firewall	15
Update the VST-APL Appliance base software and upload the 10GbE UTM Firewall app	16
Tidy-up and reboot	19
Final check	20
Upgrading to a new version of 10GbE UTM Firewall	20
Configuring multiple 10GbE UTM Firewall Instances	20
The VST-APL GUI Dashboard.....	21
Saving configuration and logging out	21
System Information panel	22
Deployed Applications panel	23
The Menu	24
Setting up network infrastructure	24
Interface support on the VST-APL	24
Connecting applications to the network	25
Configure Interface Management	28
Configure Static Routing	30
Configure Bonding	31
Configure Bridging	34
Configure the DNS Client.....	36
System management.....	37
Manage files	38
Generate tech support information	41
Configure system time	42
View system information	44
Configure users	46

Enable remote shutdown	47
Monitoring.....	48
View log messages	49
Monitor system CPU, memory and storage I/O.....	51
Managing applications	53
Start, stop and remove applications	53
View the Container Services page	54
Restore an application after appliance restart	55
Backing up and Restoring VST-APL.....	56
Schedule regular backups	56
Create a single backup now.....	59
Monitor backups and schedules.....	62
Manually restore the whole appliance from a backup	65
Restore a single application instance on the appliance from a back-up	69
Automatically restore the whole appliance from a backup onto new appliance hardware.....	73
Upgrading VST-APL software.....	75

Products and software versions that apply to this guide

This guide applies to the Vista Manager Network Appliances (VST-APL) running VST-APL 3.5.3 and later. For more information, see:

- The product's [Datasheet](#)
- The product's [Installation Guide](#)
- [Vista Manager Network Appliance \(VST-APL\) Technical Documents](#)—for information about how to use the VST-APL and the applications supported on it.

These documents are available on our website at alliedtelesis.com.

Deploying and licensing VST-APL as a Vista Manager appliance

The appliance comes with supported software installed, including Vista Manager EX. Add capability and capacity with subscription-based licenses for AMF-Cloud, AWC Wireless Controller, and AMF Security automation and management tools.

The VST-APL software consists of the operating system and an ISO file containing APP files for the applications. Each version of VST-APL consists of a set of supported ISO and APP files, as shown in [Table 1](#) below to [Table 3 on page 5](#). When you upgrade VST-APL, make sure you upgrade the operating system and all the applications you are using, so that they match.

[Table 4](#) below shows the activation and licensing status for the VST-APL software applications.

You can obtain the software files from the Allied Telesis [Support Portal](#). For information about licenses, see the datasheet for your appliance.

Table 1: VST-APL 3.11.x supported software and versions

Software Component	VST-APL 3.11.1	
VST-APL Operating System	Version 1.9.4: ATVSTAPL-1.9.4.iso	
VST-APL application bundle	Version 3.11.1: VST-APL-3.11.1.bundle	
Vista Manager EX	Version 3.13.1: vista-x86_64-3.13.1.app	
AMF Cloud	Version 5.5.4-2.3: AMF-x86_64-5.5.4-2.3.app	
Wireless Controller (AWC)	Version 3.13.1: awc-x86_64-3.13.1.app	
AMF Security	Version 2.6.0: sesc-x86_64-2.6.0.app	
SNMP (Full SNMP)	Version 2.12.0: fullsnmp-x86_64-2.12.0.app	
AT-RADgate	Version 1.0.0: radgate-x86_64-1.0.0.app	The AT-RADgate RADIUS server may not be available in all regions. See your Allied Telesis representative for more information

Table 2: Previous VST-APL 3.10.x and VST-APL 3.9.x supported software and versions

Software Component	VST-APL 3.10.4	VST-APL 3.10.3	VST-APL 3.10.1	VST-APL 3.9.1
VST-APL Operating System	Version 1.9.2: ATVSTAPL-1.9.2.iso	Version 1.9.2: ATVSTAPL-1.9.2.iso	Version 1.9.2: ATVSTAPL-1.9.2.iso	Version 1.9.1: ATVSTAPL-1.9.1.iso
VST-APL application bundle	Version 3.10.4: VST-APL-3.10.4.bundle	Version 3.10.3: VST-APL-3.10.3.bundle	Version 3.10.1: VST-APL-3.10.1.bundle	Version 3.9.1: VST-APL-3.9.1.bundle
Vista Manager EX	Version 3.12.3: vista-x86_64-3.12.3.app	Version 3.12.2: vista-x86_64-3.12.2.app	Version 3.12.0: vista-x86_64-3.12.0.app	Version 3.11.1: vista-x86_64-3.11.1.app
AMF Cloud	Version 5.5.4-0.5: AMF-x86_64-5.5.4-0.5.app	Version 5.5.4-0.5: AMF-x86_64-5.5.4-0.5.app	Version 5.5.4-0.1: AMF-x86_64-5.5.4-0.1.app	Version 5.5.3-2.1: AMF-x86_64-5.5.3-2.1.app
Wireless Controller (AWC)	Version 3.12.3: awc-x86_64-3.12.3.app	Version 3.12.2: awc-x86_64-3.12.2.app	Version 3.12.0: awc-x86_64-3.12.0.app	Version 3.11.1: awc-x86_64-3.11.1.app
AMF Security	Version 2.6.0: sesc-x86_64-2.6.0.app	Version 2.6.0: sesc-x86_64-2.6.0.app	Version 2.6.0: sesc-x86_64-2.6.0.app	Version 2.6.0: sesc-x86_64-2.6.0.app
SNMP (Full SNMP)	Version 2.11.1: fullsnmp-x86_64-2.11.1.app	Version 2.11.1: fullsnmp-x86_64-2.11.1.app	Version 2.11.0: fullsnmp-x86_64-2.11.0.app	Version 2.10.1: fullsnmp-x86_64-2.10.1.app

Table 3: Previous VST-APL supported software and versions 3.5.x - 3.8.x

Software Component	VST-APL 3.8.1	VST-APL 3.7.2	VST-APL 3.6.1	VST-APL 3.5.3
VST-APL Operating System	Version 1.8.3: ATVSTAPL-1.8.3.iso	Version 1.8.2: ATVSTAPL-1.8.2.iso	Version 1.7.3: ATVSTAPL-1.7.3.iso	Version 1.7.1: ATVSTAPL-1.7.1.iso
VST-APL application bundle	Version 3.8.1: VST-APL-3.8.1.bundle	Version 3.7.2: VST-APL-3.7.2.bundle	Version 3.6.1: VST-APL-3.6.1.bundle	Version 3.5.3: VST-APL-3.5.3.bundle
Vista Manager EX	Version 3.11.0: vista-x86_64-3.11.0.app	Version 3.10.3: vista-x86_64-3.10.3.app	Version 3.10.2: vista-x86_64-3.10.2.app	Version 3.9.2: vista-x86_64-3.9.2.app
AMF Cloud	Version 5.5.3-1.3: AMF-x86_64-5.5.3-1.3.app	Version 5.5.3-0.2: AMF-x86_64-5.5.3-0.2.app	Version 5.5.2-2.3: AMF-x86_64-5.5.2-2.3.app	Version 5.5.2-1.1: AMF-x86_64-5.5.2-1.1.app
Wireless Controller (AWC)	Version 3.11.0: awc-x86_64-3.11.0.app	Version 3.10.1: awc-x86_64-3.10.1.app	Version 3.10.0: awc-x86_64-3.10.0.app	Version 3.9.1: awc-x86_64-3.9.1.app
AMF Security	Version 2.6.0: sesc-x86_64-2.6.0.app	Version 2.5.1: sesc-x86_64-2.5.1.app	Version 2.5.0: sesc-x86_64-2.5.0.app	Version 2.4.0: sesc-x86_64-2.4.0.app
SNMP (Full SNMP)	Version 2.10.0: fullsnmp-x86_64-2.10.0.app	Version 2.9.1: fullsnmp-x86_64-2.9.1.app	Version 2.9.0: fullsnmp-x86_64-2.9.0.app	Version 2.8.1: fullsnmp-x86_64-2.8.1.app
Trap Receiver	—	Version 2.5.0: snmp-x86_64-2.5.0.app	Version 2.5.0: snmp-x86_64-2.5.0.app	Version 2.5.0: snmp-x86_64-2.5.0.app

Table 4: Activation and licensing of VST-APL software components

Software	Activation and license information
VST-APL Operating System	Ships with the operating system and GUI for the appliance enabled. The VST-APL operating system is pre-loaded into operating memory. It does not show in the File Management page of the GUI.
VST-APL application bundle (from 3.4.1)	The bundle file is available for upgrading from earlier versions. It is not preloaded on new devices.
Vista Manager EX	Application image preloaded. Requires activation. No license required.
AMF Cloud	Application image preloaded. Requires license and activation.
Wireless Controller (AWC)	Application image preloaded. Requires license and activation.
AMF Security	Application image preloaded. Requires license and activation.
Trap Receiver (SNMP-based, in VST-APL 3.7.2 and earlier)	Application image preloaded. Requires activation. No license required.
SNMP (Full SNMP)	Application image preloaded. Requires license and activation.
AT-RADgate	Application image preloaded. Requires license and activation.

The appliance comes with software installed.

You can obtain VST-APL software update files from the Allied Telesis [Support Portal](#).

Deploying and licensing VST-APL as a 10GbE UTM Firewall

Alternatively, you can configure VST-APL with the 10GbE UTM Firewall. This is a virtualized version of the UTM Firewall that can be run on VST-APL.

When configuring the appliance as a firewall, you need to start by replacing the installed Vista Manager software with the 10GbE UTM Firewall application. You can obtain the 10GbE UTM Firewall software files from the Allied Telesis [Support Portal](#).

The 10GbE UTM Firewall software (NFV-APL) consists of an ISO file containing the operating system, and the AW+ Firewall application. Each version of NFV-APL consists of a set including a supported ISO file and APP file, as shown in [Table 5](#). When you upgrade the software, make sure you upgrade the operating system and the AW+ Firewall application, so that they match.

Table 5: 10GbE UTM Firewall software component versions

10GbE UTM Firewall Software version	VST-APL Operating System	AW+ Firewall application
Version 5.5.4-2.3 (NFV-APL-1.12.1)	Version 1.9.4: ATVSTAPL-1.9.4.iso	Version 5.5.4-2.3 vfw-x86-64-5.5.4-2.3.app
Version 5.5.4-1.2 (NFV-APL-1.11.1)	Version 1.9.3: ATVSTAPL-1.9.3.iso	Version 5.5.4-1.2 vfw-x86-64-5.5.4-1.2.app
Version 5.5.4-0.1 (NFV-APL-1.10.1)	Version 1.9.2: ATVSTAPL-1.9.2.iso	Version 5.5.4-0.1 vfw-x86-64-5.5.4-0.1.app
Version 5.5.3-2.1 (NFV-APL-1.9.1)	Version 1.9.1: ATVSTAPL-1.9.1.iso	Version 5.5.3-2.1 vfw-x86-64-5.5.3-2.1.app
Version 5.5.3-1.3 (NFV-APL-1.8.2)	Version 1.8.3: ATVSTAPL-1.8.3.iso	Version 5.5.3-1.3 vfw-x86-64-5.5.3-1.3.app
Version 5.5.3-0.2 (NFV-APL-1.7.2)	Version 1.8.1: ATVSTAPL-1.8.1.iso	Version 5.5.3-0.2 vfw-x86-64-5.5.3-0.2.app

The 10GbE UTM Firewall application is deployed with the included base feature license. Additionally, there are advanced subscription-based feature licenses available. For more information about licenses, see the [10GbE UTM Firewall datasheet](#).

Getting connected to the VST-APL

This section describes how to get the applications on your appliances started quickly and easily in these steps:

- "Connect to the web-based Device GUI" on page 8
- "Set up network interfaces" on page 9
- "Save the VST-APL configuration" on page 11

For more detailed information about using the appliance, see the sections that follow this one.

Connect to the web-based Device GUI

Connect to the GUI with a web browser by following the steps below. These browsers are supported:

- Google Chrome™
- Mozilla Firefox™
- Microsoft Edge™
- Apple Safari™.

Step 1: Connect to the VST-APL appliance.

Connect the appliance to the network by one of the front panel Ethernet ports.

Step 2: Open a web browser and browse to the IP address for the VST-APL GUI.

From the factory, the appliance is set to accept an IP address from DHCP. If the device does not receive an IP address from a DHCP server within 10 seconds of the interface becoming active, the VST-APL uses the default IP address 192.168.1.1/24.

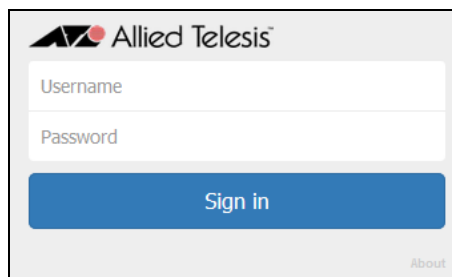
If the IP address is assigned by DHCP, you can find it from the DHCP server.

For more information on starting the initial management session, see the Installation Guide.

Step 3: Accept the security exception.

Accept the security exception for the self-signed certificate for GUI software on the appliance.

Step 4: Log in with the default username of *manager* and the default password of *friend*.

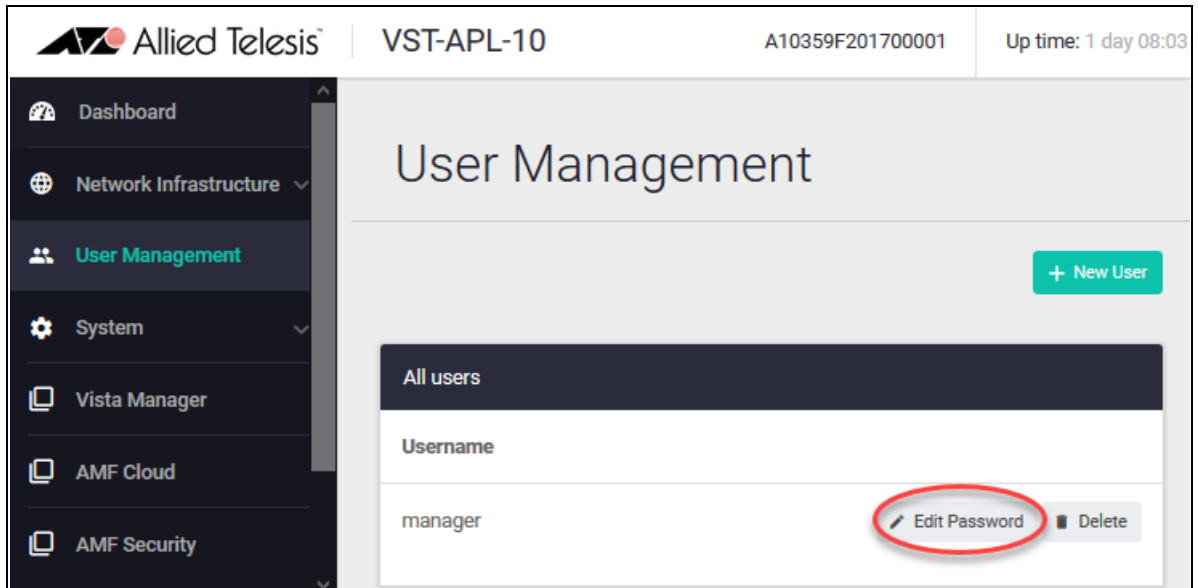


The web browser displays the VST-APL GUI dashboard.

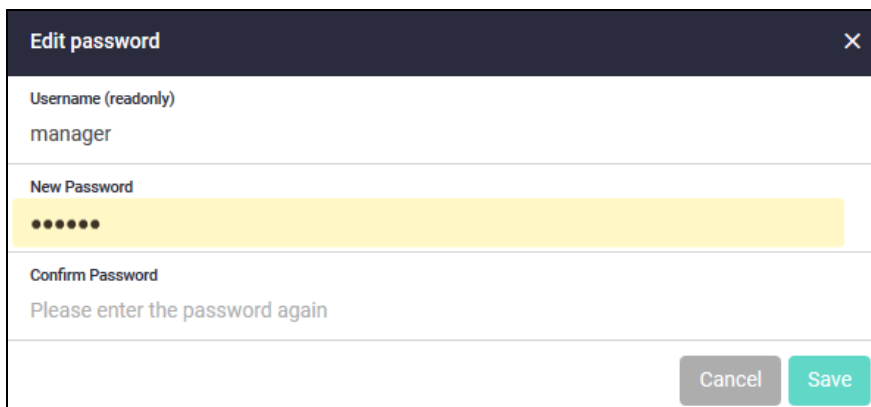
Change the manager password

In the Dashboard menu, click **User Management**.

Due to a recent design upgrade, your device's GUI may look different to this.



In the User Management page, click **Edit Password** to the right of the user 'manager'.

The 'Edit password' dialog box has a dark header with a close button. It contains three input fields: 'Username (readonly)' with the value 'manager', 'New Password' (masked with dots), and 'Confirm Password' with the placeholder text 'Please enter the password again'. At the bottom right are 'Cancel' and 'Save' buttons.

Enter the new password twice and click **Save**.

Set up network interfaces

By default, the appliance accepts IP addressing from a DHCP server, including an IP address and a default route. You can get these from the DHCP server. If a DHCP server does not supply this configuration to the appliance, you will need to manually add an IP address and a default route.

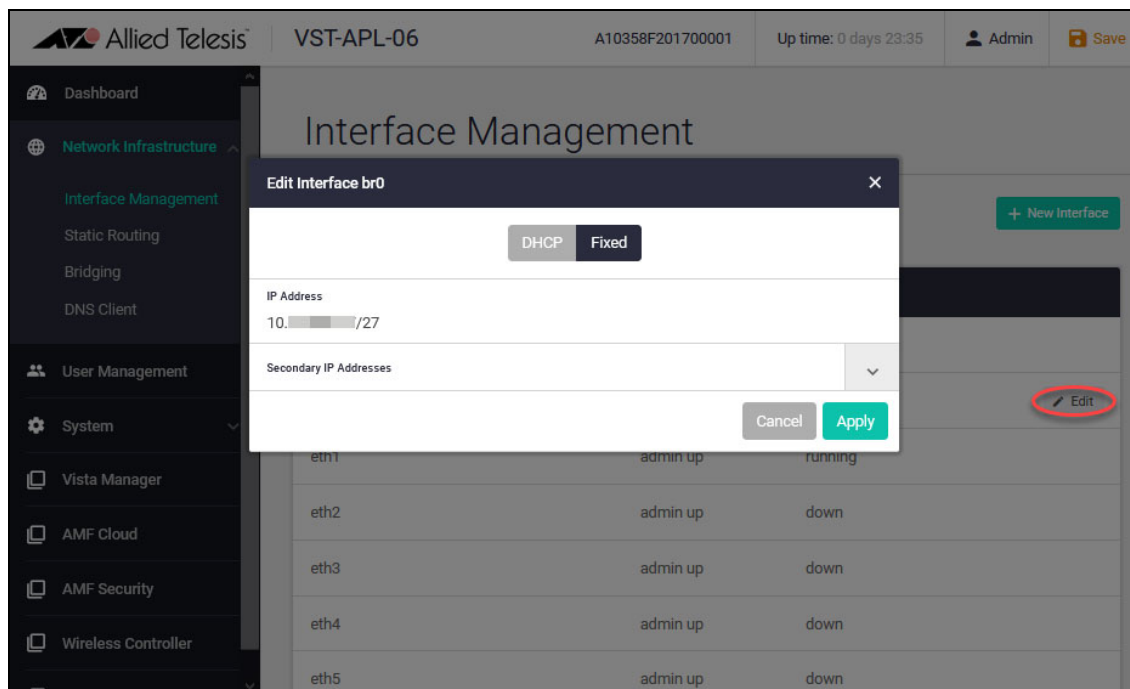
By default, all VST-APL ports are in the same L2 bridge. During the initial setup, ensure the device is connected to one port only. This prevents it from bridging multiple networks. Later, after the initial setup is complete, you will be able to assign VLANs to ports for the networks they will be connected to ("[Configure Interface Management](#)" on page 28).

1. Configure the IP address.

From the menu, navigate to the **Network Infrastructure > Interface Management** page.

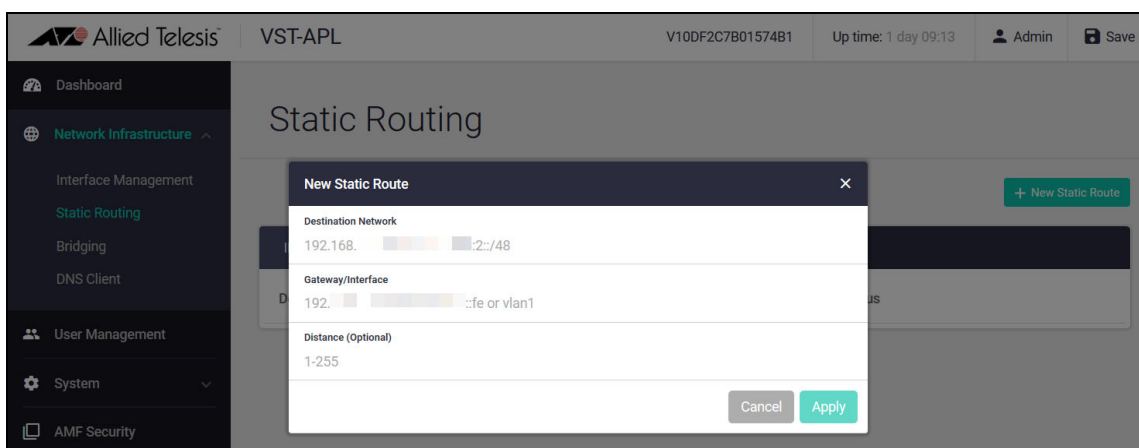
Click the **edit** button to the right of 'br0'. This is the bridge connecting interfaces.

Change the IP address of the bridge (br0) to one that you will be able to navigate to from the device you are accessing the GUI from. When you change the IP address, you will lose your browser's connection to the appliance. Point your browser to the new IP address.



2. Add a default route.

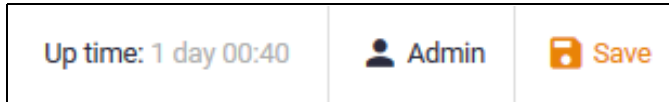
Navigate to the **Network Infrastructure > Static Route** page and click the **+ Static Route** button to add a default route.



To set up advanced network interface configuration, use the pages available under the Network Infrastructure menu item. See "[Setting up network infrastructure](#)" on page 24.

Save the VST-APL configuration

To save the VST-APL configuration, click the **Save** button at the top right of VST-APL GUI page. It is orange when there is unsaved configuration and blue otherwise. Save whenever you have VST-APL configuration you want to retain over an appliance reboot.

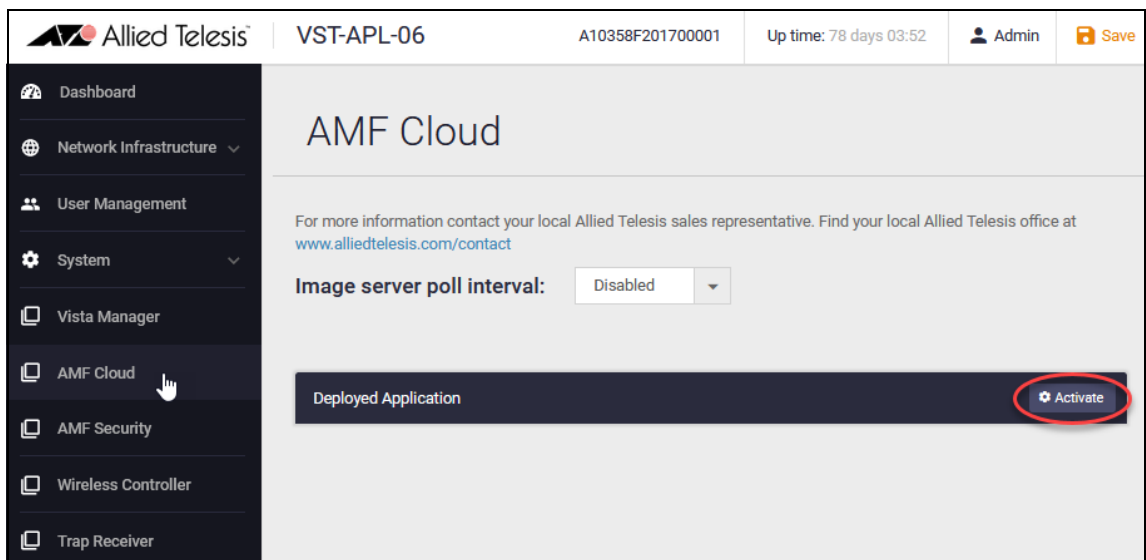


Getting started with Vista Manager and associated applications

Do this step if you are using the VST-APL for Vista Manager.

Activate each application you will use on the appliance. To activate an application, follow these steps. See also "[Example: activate the applications](#)" on page 14.

1. Click the button for the application in the **menu**. A page opens for the application.



- Click the **Activate** button. The **Application Configuration** dialog box opens automatically when you activate the application so you can configure the set up for the application container. To change this configuration later, click the **Configure** button to right of the application on this page.

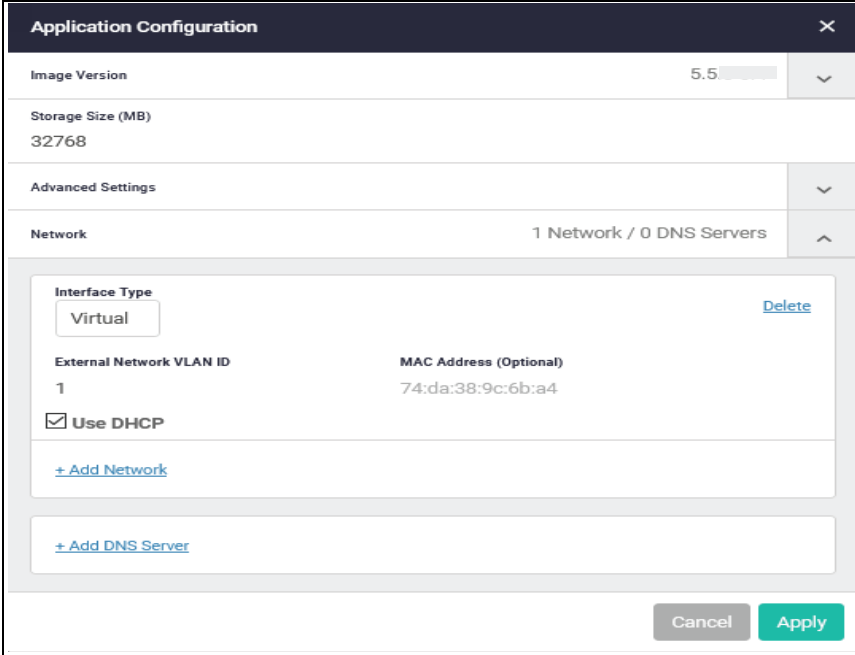
- Set up the application parameters:

Enter the storage size. We recommend entering the storage values in this table to configure the applications.

Table 6: Recommended storage limits for applications

APPLICATION	RECOMMENDED STORAGE (MB)
Vista Manager (Vista Manager EX)	204 800
AMF Cloud	32 768
AMF Security	81 920
Wireless Controller (AWC)	204 800
SNMP (Full SNMP)	102 400
Trap Receiver (SNMP-based, in VST-APL 3.7.2 and earlier)	40 960
AT-RADgate	65 536

Click the **Network** drop down list to expand it. Click **Add Network**. If there is a DHCP server on the network to assign IP addressing, select **Use DHCP**. Otherwise, specify the static IP address for the application. (Leave the Interface Type as Virtual.)




The screenshot shows the 'Application Configuration' dialog box. It has a dark header with a close button. Below the header, there are several sections: 'Image Version' with a dropdown set to '5.5'; 'Storage Size (MB)' with the value '32768'; 'Advanced Settings' with a dropdown arrow; and 'Network' with a dropdown arrow and the text '1 Network / 0 DNS Servers'. The 'Network' section is expanded, showing 'Interface Type' as 'Virtual' with a 'Delete' link. Below that, 'External Network VLAN ID' is '1' and 'MAC Address (Optional)' is '74:da:38:9c:6b:a4'. There is a checked checkbox for 'Use DHCP'. At the bottom of the network section are links for '+ Add Network' and '+ Add DNS Server'. At the very bottom of the dialog are 'Cancel' and 'Apply' buttons.

To set up advanced network interface configuration, use the pages available under the Network Infrastructure menu item. See "[Setting up network infrastructure](#)" on page 24.

Before starting any application, it must have a static or DHCP address configured.

Click **Apply** to create the container for the application with these application parameters and to start the application. This may take a few minutes. The application page displays information about the application instance.

4. To access and configure applications such as **Vista Manager EX**, **AMF Cloud**, and **AMF Security**, click the **Open** button or point your browser directly to the IP address of the application. You can access the IP address and other application configuration in the main page for the application by:
 - in VST-APL 3.5.2 and later, click the **Configure** button to the right of the application instance in the Deployed Application panel.
 - In VST-APL 3.4.1 and earlier, hover the mouse over the small instance information icon  in the left of the Deployed Application panel.

You may be asked for authentication. Use the default username 'manager' and password 'friend' the first time, then change the password for the application.

The first time you access the **AMF Cloud** application, it requires you to change the default password by using its command line interface. (The time in the password expiry message may be long ago.) Save the configuration using the 'write' command to retain the change.

5. Click the **Save** button in the VST-APL GUI to save the application set-up in the VST-APL configuration.

Example: activate the applications

The appliance has application image files preloaded into persistent storage, such as:

- Vista Manager
- AMF Cloud
- Wireless Controller (AWC)
- SNMP (full) (or Trap Receiver (SNMP-based) in VST-APL 3.7.2 and previous)
- AMF Security (also known as AMF-Sec or AT-SESC)
- RADgate (from VST-APL 3.11.1)

If you will use some or all of these applications, you can activate them in the following order. When you configure the applications, use the storage values in [Table 6 on page 12](#).

1. Log in to the VST-APL. The first time you do this, follow the steps in "[Connect to the web-based Device GUI](#)" on page 8).
2. Activate AMF Cloud if you are using AMF Cloud on the VST-APL as the AMF master, and configure your AMF network. For information about configuring an AMF network, see the [AMF Feature Overview and Configuration Guide](#).
3. Activate Vista Manager if using it to monitor your AMF and wireless network.
4. Activate Wireless Controller (AWC) if using it to manage wireless access points in your network.
5. Activate SNMP (or Trap Receiver) if using one of these to manage third-party devices.
6. Activate AMF Security if using it.
7. Activate RADgate if using it.
8. Save the appliance configuration.

After activating the applications, you may need to:

- Install licences—Vista Manager and Trap Receiver do not require a license; for other applications, you may need to install a license. See the User Guide for the application.
- Register Vista Manager EX plug-ins (the SNMP (full) plug-in or Trap Receiver (SNMP-based) plug-in and/or the AWC Wireless Controller (AWC) plug-in). See the Vista Manager EX User Guide.

For more information about using each application, see its User Guide.

Getting started with 10GbE UTM Firewall

Do this step if you are using the VST-APL for a firewall.

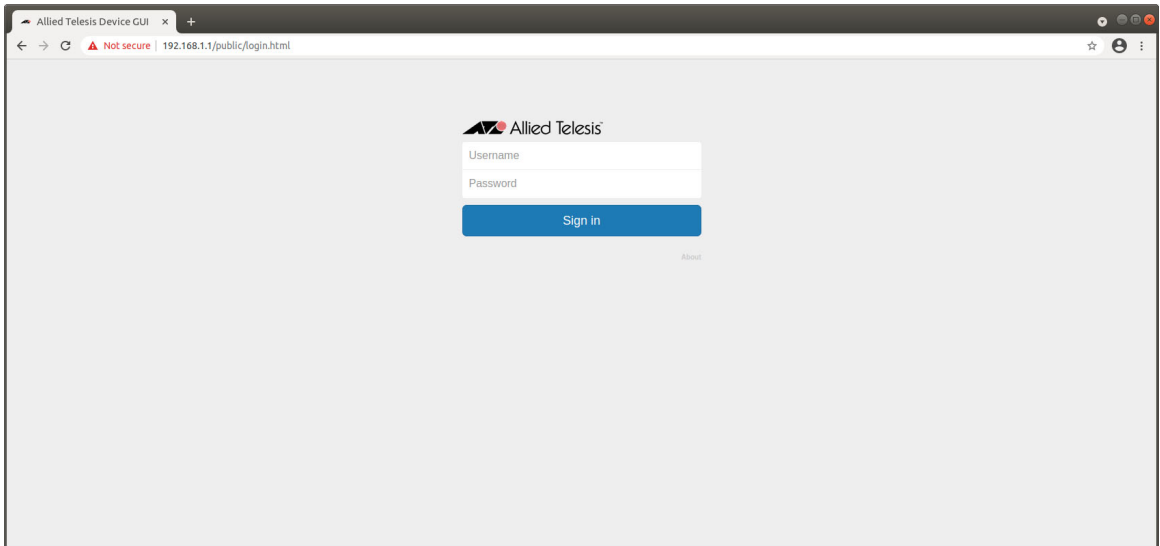
The following section will guide you through the instructions for setting up 10GbE UTM Firewall on your device.

Before you start you will need:

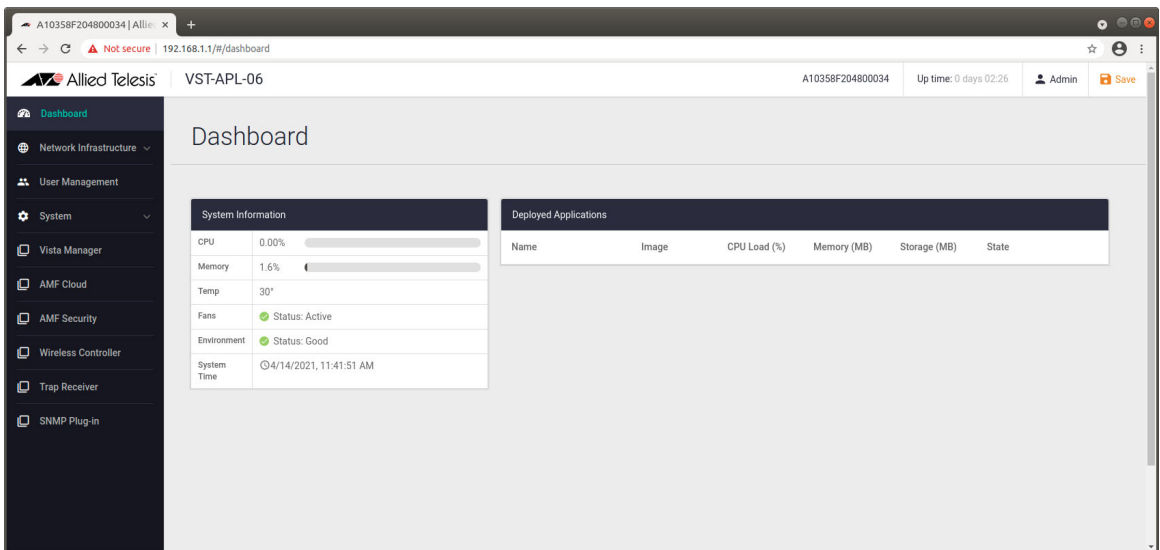
- The 10GbE UTM Firewall files. You need the following files, where **x.x.x** is the version number you are installing:
 - **ATVSTAPL-x.x.x.iso**
 - **vfw-x86_64-x.x.x.app**
- A PC with an Ethernet port, and an Ethernet cable.
- Ensure the power to the unit is switched off.
- Configure the PC with a static IP address suitable for communication with the device. The device will have the IP address 192.168.1.1/24 if no DHCP server was available at boot.

Update the VST-APL Appliance base software and upload the 10GbE UTM Firewall app

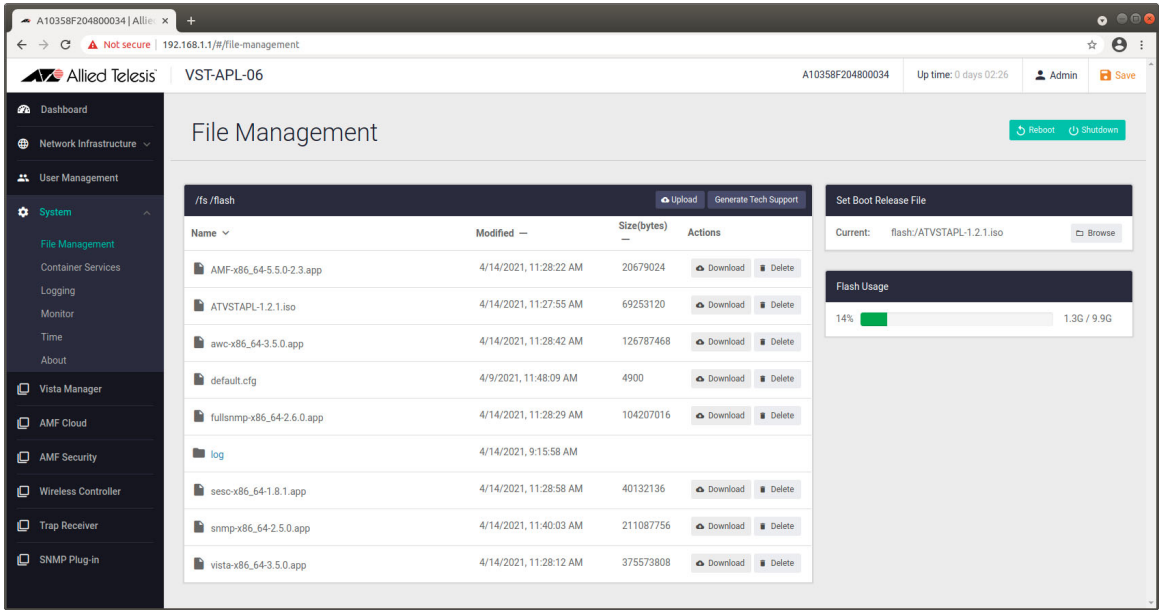
1. Connect the device to the PC using an Ethernet cable plugged into Ethernet port 1.
2. Connect to the Device GUI of the device using a web browser on the PC, using the device's IP address as described above in the “Getting started with 10GbE UTM Firewall” section.



3. Log in using the user-name **manager** and the password **friend**.



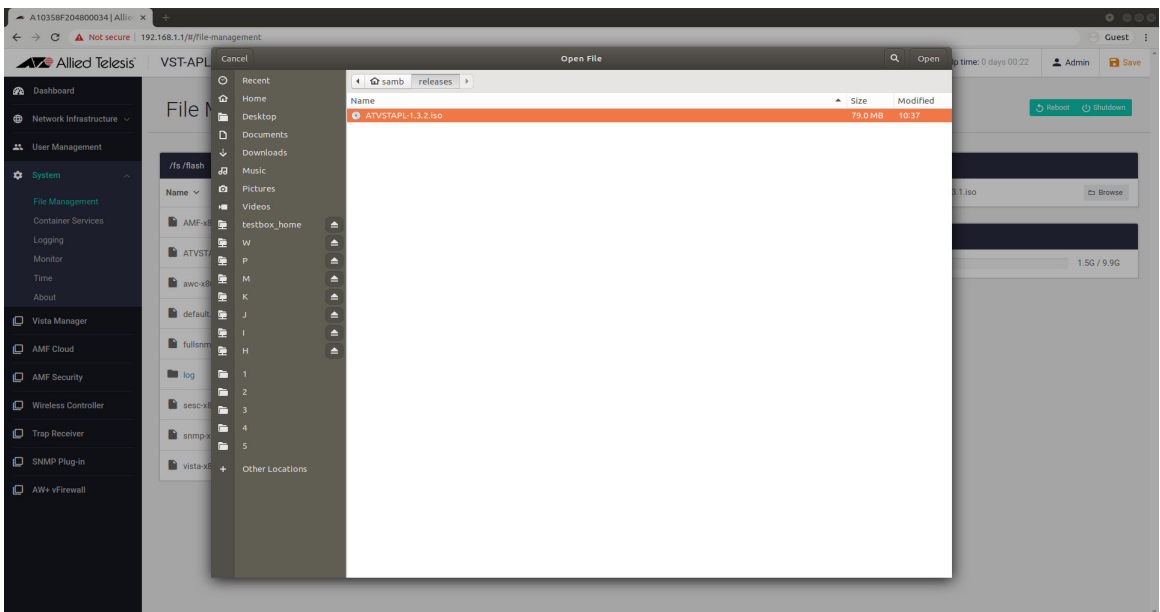
4. Navigate to the **File Management** page (**System->File Management**)



Upload the ATVSTAPL-x.x.x.iso release file

5. Click the **Upload** button, opening up the **File Upload** sub-menu shown below.

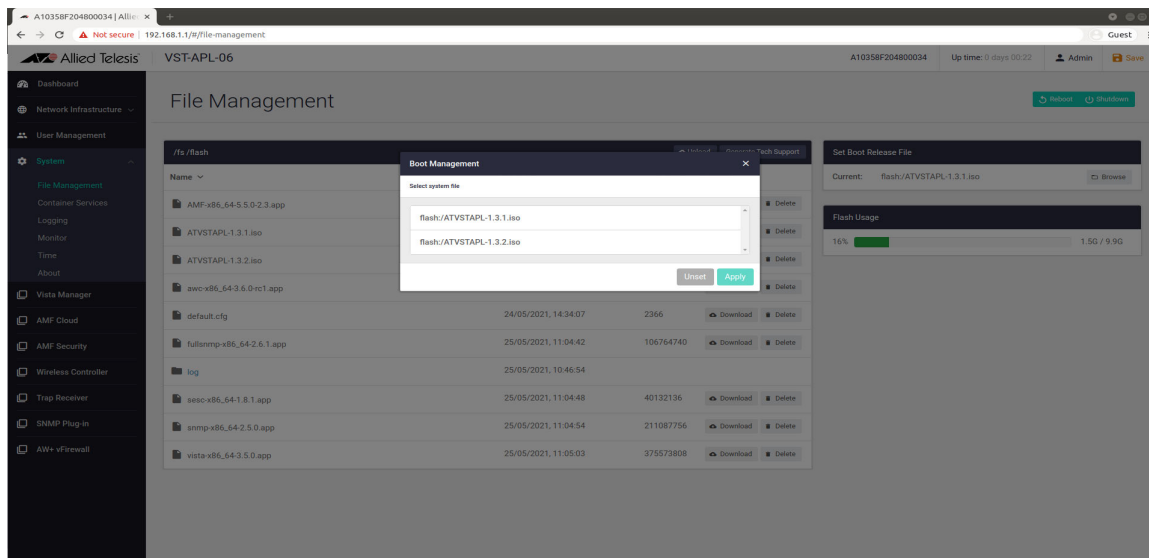
Note: The appearance of this menu may vary slightly depending on the operating system and browser you are using.



6. Navigate to the **ATVSTAPL-x.x.x.iso** release file and select it.

- Once the release file is uploaded, set it as the boot release. Under the **Set Boot Release File** panel, click on **Browse**. This will open the **Boot Management** dialog. Select the uploaded release file and click **Apply**.

Note: Only files with the correct format are displayed.



Upload the vfw-x86_64-x.x.x.app file

- Click the **Upload** button and open the **File Upload** sub-menu again.
- Navigate to the 10GbE UTM Firewall file **vfw-x86_64-x.x.x.app** and select it.

Tidy-up and reboot

1. Navigate to the **Container Services** page (**System->Container Services**)
2. Running 10GbE UTM Firewall alongside any other containers is not supported. There should be no application instances present in the **Deployed Applications** table.

The screenshot shows the 'Container Services' page in the Allied Telesis VST-APL-06 web interface. The page title is 'Container Services' and the URL is '192.168.1.1/#/container-services'. The page displays the following information:

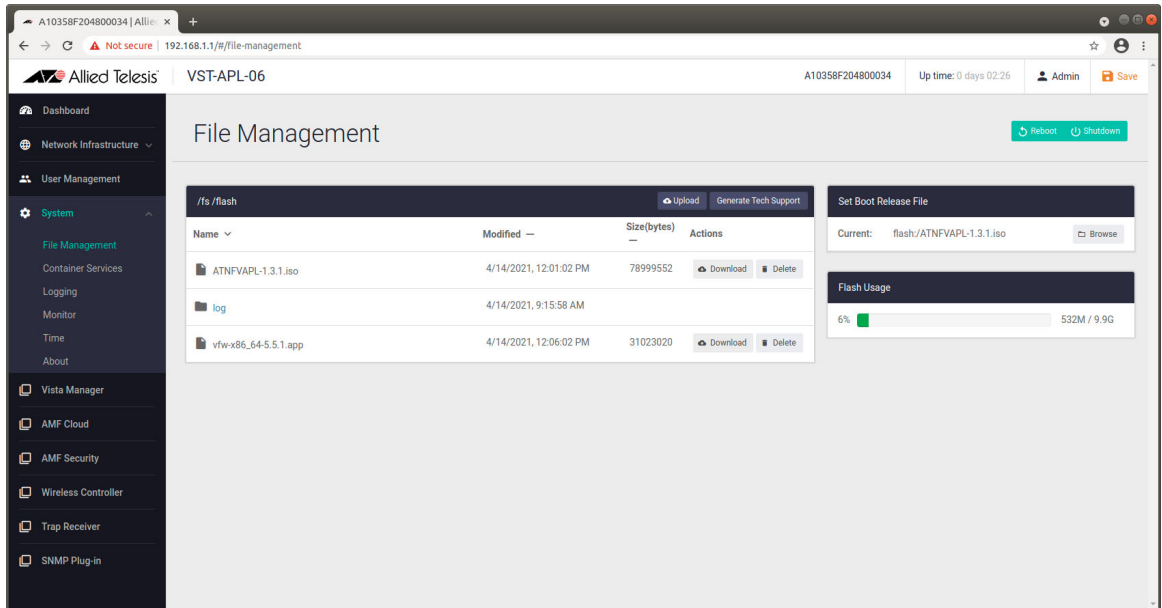
- Image server poll interval:** Disabled
- Compute Node Table:**

Compute ID	IP	Arch	CPU Load (%)	Memory (MB)	Storage (MB)	State
A10358F204800034		x86_64	0.06 / 100	278 / 83 / 1079 / 32017	12288 / 953548	Alive
- Deployed Applications Table:**

Name	Compute ID	Image	Cores	CPU Load (%)	Memory (MB)	Storage (MB)	State
AMF-Sec	Local	sesc				2000MB	Offline

If any instances are present, stop them if they are running by clicking the **Stop** button. Then destroy them by clicking the **Destroy** button next to them. The **Deployed Applications** table should now be empty.

3. Navigate to the **File Management** page (**System->File Management**). Delete the previous version of the VST-APL Appliance base software **ATVSTAPL-y.y.y.iso** (if present) by clicking on the **Delete** button next to the file on the **File Management** page.
4. Delete the VST-APL Appliance application files by using the **Delete** button next to each file on the **File Management** page. The files to delete are:
 - **vista_x86_64-x.x.x.app**
 - **AMF_x86_64-x.x.x.app**
 - **sesc_x86_64-x.x.x.app**
 - **awc_x86_64-x.x.x.app**
 - **fullsnmp-x86_64-x.x.x.app**
 - **snmp-x86_64-x.x.x.app**
 - **radgate-x86_64-x.x.x.app**



5. The only remaining files should be **ATVSTAPL-x.x.x.iso** and **vfw-x86_64-x.x.x.app**.
6. Navigate to the **File Management** page (**System->File Management**). Reboot the device by clicking on the **Reboot** button.

Final check

1. After rebooting the device, log in again using the user-name **manager** and the password **friend**.
2. Check that the correct software version is installed by navigating to the **About** page (**System->About**), and verifying the **Software Version**.

Upgrading to a new version of 10GbE UTM Firewall

For details about upgrading to a new version, refer to the [10GbE UTM Firewall Release Note](#).

Configuring multiple 10GbE UTM Firewall Instances

You can configure multiple firewall instances, which can enable you to isolate traffic in a way similar to VRF-lite. For more information, see the [Isolating Traffic with the 10GbE UTM Firewall Feature Overview and Configuration Guide](#).

The VST-APL GUI Dashboard

Log in and you'll see the VST-APL GUI dashboard. The dashboard provides an overview of the status of your appliance and the applications loaded on it.

The screenshot displays the VST-APL GUI Dashboard. At the top, the Allied Telesis logo is on the left, followed by the device name 'VST-APL-06', the serial number 'A10358F202900001', the uptime 'Up time: 3 days 03:55', and the user 'Admin' with a 'Save' button. The left sidebar contains navigation options: Dashboard (selected), Network Infrastructure, User Management, System, Vista Manager, AMF Cloud, AMF Security, Wireless Controller, Trap Receiver, and SNMP Plug-in. The main content area is titled 'Dashboard' and features two sections: 'System Information' and 'Deployed Applications'.

System Information

CPU	18.00%	<div style="width: 18%;"></div>
Memory	47.6%	<div style="width: 47.6%;"></div>
Temp	29°	
Fans	Status: Active	
Environment	Status: Good	
System Time	12/03/2021, 1:32:48 pm	

Deployed Applications

Name	Image	CPU Load (%)	Memory (MB)	Storage (MB)	State	
AMF-Sec-app	sesc	0.07/100	333 / 31977	1596 / 50000	Running	Open
AT-AMF-app	AMF	0.02/100	130 / 31977	1178 / 32768	Running	Open
AT-AWC-app	awc	0.05/100	614 / 31977	1755 / 50000	Running	Open
AT-FULLSNMP-app	fullsnmp	0.03/100	479 / 31977	1200 / 50000	Running	
AT-SNMP-app	snmp	0.05/100	359 / 31977	1165 / 50000	Running	
AT-Vista-app	vista	0.66/100	3821 / 31977	1651 / 50000	Running	Open

Saving configuration and logging out

At the top right of the screen you can see the **Uptime** for the switch, as well as the **Admin** button, which is used to log out, and the **Save** button.

Configuration changes you make become part of the running configuration on the appliance. This includes:

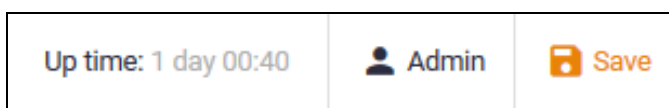
- appliance network configuration such as bridging, VLAN and IP address assignments
- user accounts
- system time configuration
- the state of applications that have been created—whether an application is running when the configuration is saved.

To make them part of the boot configuration, so they can be backed up and will survive a reboot, save these configuration changes. If an application is running when the configuration is saved, it will start up again when the appliance restarts.

Save any time there is new appliance configuration that you wish the appliance to retain. For example, we recommend saving when you have assigned an IP address to access the appliance, changed the 'manager' password, or activated and started applications.

This does not save the internal configuration and data for applications—these are managed separately by the applications themselves.

The **Save** button is colored orange any time there is unsaved configuration. If it is blue, configuration has been saved.


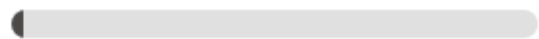




The configuration is saved to a file named "default.cfg" in persistent storage.

System Information panel

The **System Information** panel provides an overview of the current:


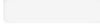
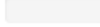



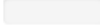
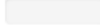



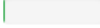
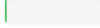



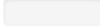
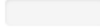


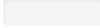
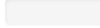


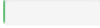
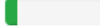


- CPU and memory usage
- environmental status
- system time (format: mm/dd/yyyy hh:mm:ss AM/PM).

System Information	
CPU	0.90% 
Memory	2.1% 
Environment	 Status: Good
System Time	 9/10/2020, 6:53:06 PM



For more detailed system information, navigate to **System > About**, and see ["Monitoring" on page 48](#).

Deployed Applications panel

The **Deployed Applications** panel provides overviews of the applications loaded on the appliance and their status.

Deployed Applications						
Name	Image	CPU Load (%)	Memory (MB)	Storage (MB)	State	
AMF-Sec-app	 sesc	 0.08/100	 333 / 31977	 1596 / 50000	Running	
AT-AMF-app	 AMF	 0.02/100	 130 / 31977	 1178 / 32768	Running	
AT-AWC-app	 awc	 0.24/100	 614 / 31977	 1755 / 50000	Running	
AT-FULLSNMP-app	 fullsnmp	 0.03/100	 479 / 31977	 1200 / 50000	Running	
AT-SNMP-app	 snmp	 0.03/100	 359 / 31977	 1165 / 50000	Running	
AT-Vista-app	 vista	 0.71/100	 3821 / 31977	 1651 / 50000	Running	

For each application, the Deployed Applications panel displays:

- the name of the application.
- the name of the image for the application. Once an application instance is created, the lock icon  to the left of the image name indicates an application authorised (signed) by Allied Telesis. If you see a warning triangle icon , this indicates an unauthorised application and may present security issues. Remove the application and/or contact your authorised Allied Telesis distributor or reseller.
- the CPU capacity it's using and how much is available to it.
- how much memory it is using and how much is available to it.
- how much storage the application is using and how much is available to it. You must configure a storage allocation as a part of activating the application.
- the state of the application. Before an application is activated, the state is 'Offline'. During normal operation, the state is 'Running'. When you activate, stop or destroy the application instance, it shows information such as 'extracting', 'creating', 'stopping', or 'destroying'.

If there is an **Open** button next to the application, you can use this to access the application.

The Menu

At the left of the dashboard are menu items for **Network Infrastructure**, **User Management** and **System**, and for each of the applications loaded on the device. You can expand **Network Infrastructure** and **System** for more menu items. The **Dashboard** item at the top of the menu returns you to this Dashboard page.

Setting up network infrastructure

This section describes network topology and interfaces on the VST-APL, how applications connect to the network, how to configure network infrastructure, default settings and recommendations.

- ["Interface support on the VST-APL" on page 24](#)
- ["Connecting applications to the network" on page 25](#)
- ["Configure Interface Management" on page 28](#)
- ["Configure Static Routing" on page 30](#)
- ["Configure Bonding" on page 31](#)
- ["Configure Bridging" on page 34](#)
- ["Configure the DNS Client" on page 36](#)

To to configure the VST-APL network configuration for an application, navigate to the application page and click the **Configure** button to the right of application.

Interface support on the VST-APL

The VST-APL provides the following interface support:

- One bridge is supported on the appliance.
- All ports attach to the bridge (br0) by default.
- For Vista Manager, AMF Cloud, Wireless Controller (AWC), SNMP, Trap Receiver, and AMF Security applications, only one network attachment (interface type) is supported per application, and that must be a virtual attachment.
- From VST-APL 3.1.1, eth interfaces can be joined by static or dynamic (LACP) bonding.

Connecting applications to the network

To connect an application instance to the network, you specify the VLAN for the network connection. This avoids binding the applications to the physical interfaces or to the underlying hardware. This means the applications can easily migrate from one piece of hardware to another without disruption to users.

To manage the VST-APL appliance, you connect to the VST-APL GUI via the bridge interface br0. This is the default management interface to the appliance's VLAN-aware bridge.

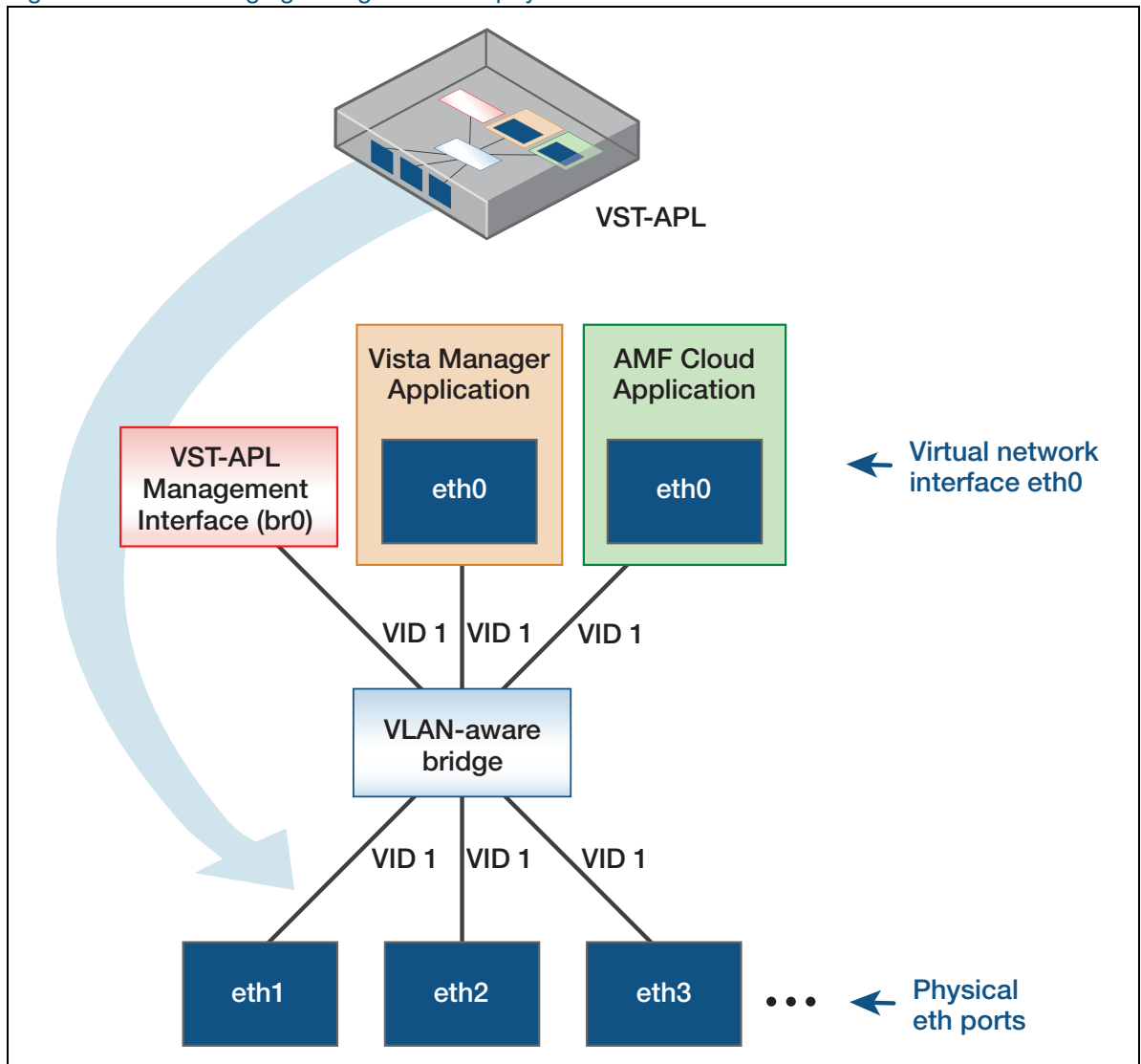
Default topology

By default, each physical Ethernet interface on the VST-APL is connected to the VLAN-aware bridge as an untagged member of the default VLAN, vlan1. In [Figure 1](#) below, eth1, eth2, and so on at the bottom of the diagram, are the physical eth ports on the appliance.

When you activate an application instance, you must assign it a network interface via which to reach it. For apps other than the firewall, the only supported interface is virtual, and the first virtual interface assigned for each application instance is eth0. As shown for the applications at the top of the diagram, eth0 is the application's virtual eth interface to the VLAN-aware bridge.

This means that by default, any interface in an application instance that is attached to vlan1 is connected to the same Layer 2 broadcast domain as all physical interfaces on the appliance.

Figure 1: Default bridging configuration for physical interfaces

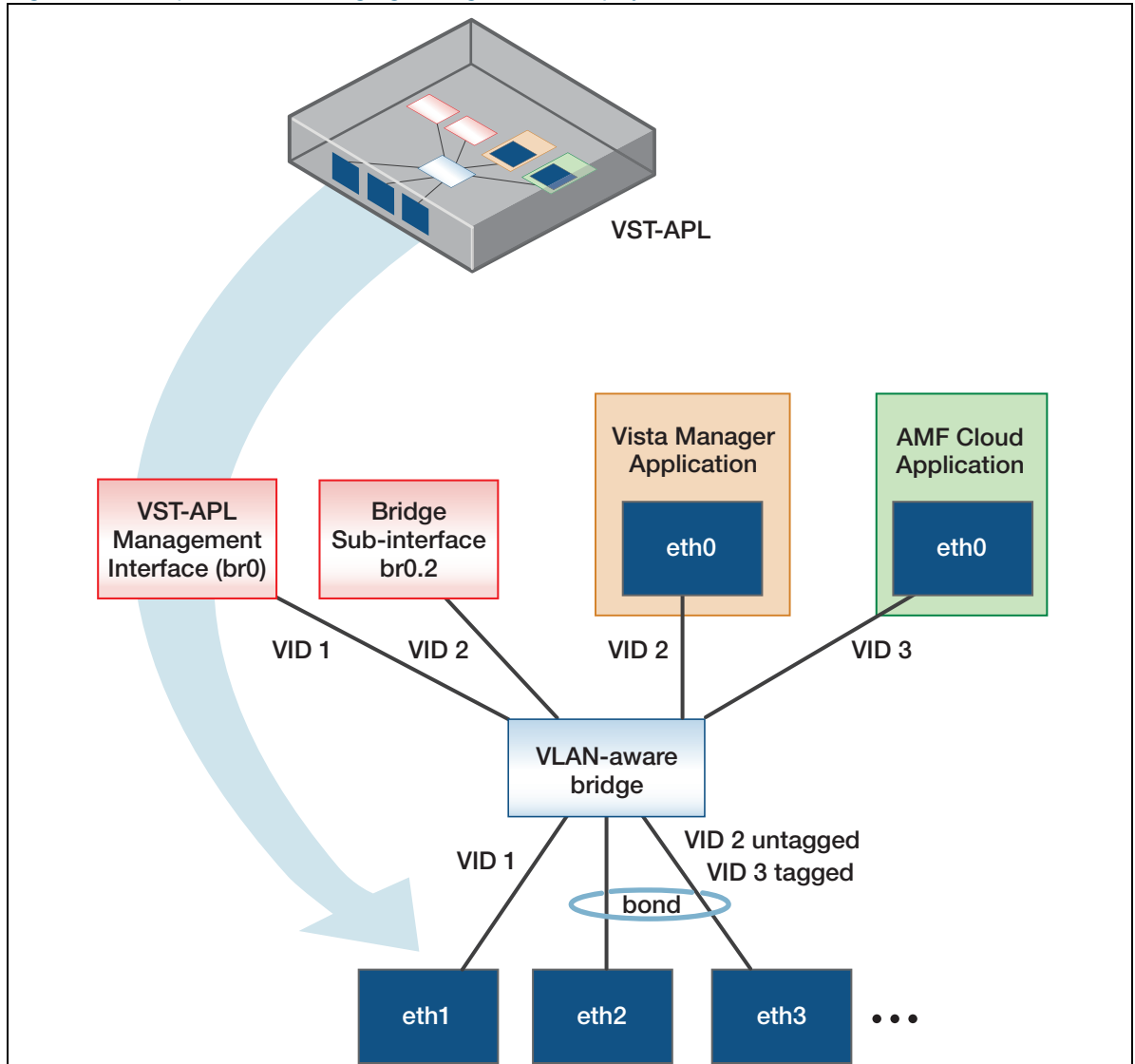


Advanced topology

You can configure the VST-APL interfaces for more complex network topologies. You can:

- connect different applications on the VST-APL to different VLANs on the network.
- join two or more physical eth links of the same speed to create bonds. This could be used to increase the bandwidth for an application's connection to another device on the network, such as an AlliedWare Plus device.

Figure 2: Example custom bridging configuration for physical interfaces

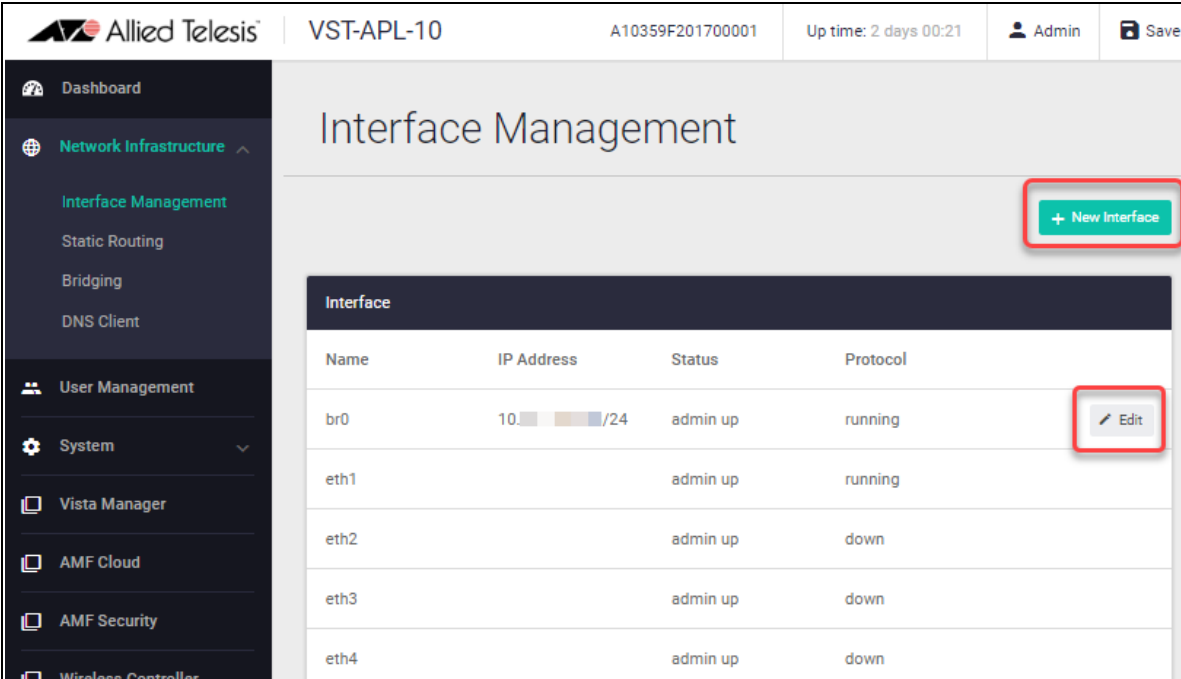


For example, some of the more advanced settings for Figure 2 are:

- AMF Cloud and Vista Manager are NOT connected internally, and would require an external device for connectivity if they needed to communicate.
- The VST-APL appliance has network connectivity to the Vista Manager application via bridge sub-interface br0.2 which is connected to vlan2.
- Eth1 is only a member of vlan1 with vlan1 as the native VLAN.
- Eth2 and eth3 are part of a bond. The bond is a member of both as an untagged member of vlan2 and a tagged member of vlan3.

Configure Interface Management

By default, the VST-APL has a number of physical eth interfaces, and one VLAN-aware bridge (br0). To view and configure interfaces, navigate to **Network Infrastructure > Interface Management**.

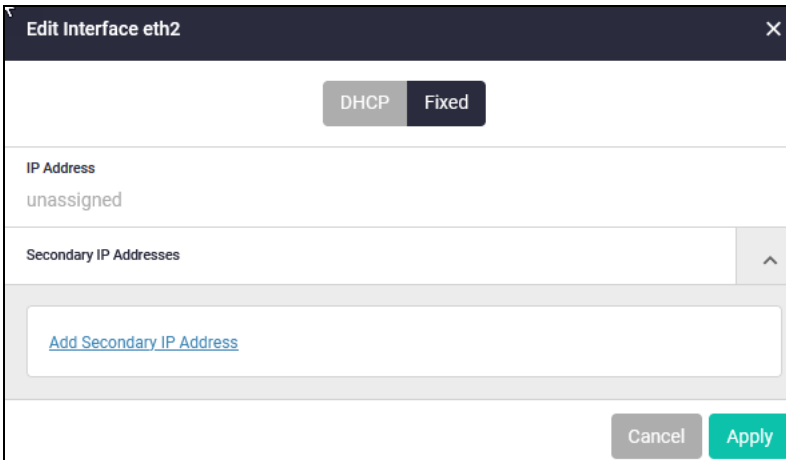


The screenshot shows the 'Interface Management' page for VST-APL-10. The page header includes the Allied Telesis logo, device name, ID (A10359F201700001), uptime (2 days 00:21), and user (Admin). The left sidebar contains navigation options: Dashboard, Network Infrastructure (selected), Interface Management (selected), Static Routing, Bridging, DNS Client, User Management, System, Vista Manager, AMF Cloud, AMF Security, and Wireless Controller. The main content area displays a table of interfaces:

Name	IP Address	Status	Protocol
br0	10.1.1.1/24	admin up	running
eth1		admin up	running
eth2		admin up	down
eth3		admin up	down
eth4		admin up	down

On the Interface Management page, you can:

- See an overview of all interfaces on the VST-APL, including the VLAN-aware bridge (br0), bridge 802.1Q sub-interfaces, physical eth ports (eth1, eth2, and so on), and bonds. For each interface, see the IP address (if assigned), the status (admin up or down), and whether the protocol is running or down.
- Assign IP addressing to the bridge, bridge 802.1Q sub-interfaces, and eth interfaces that are not attached to the bridge. Click **Edit** to its right. Either select DHCP or enter a primary and optional secondary IP address.

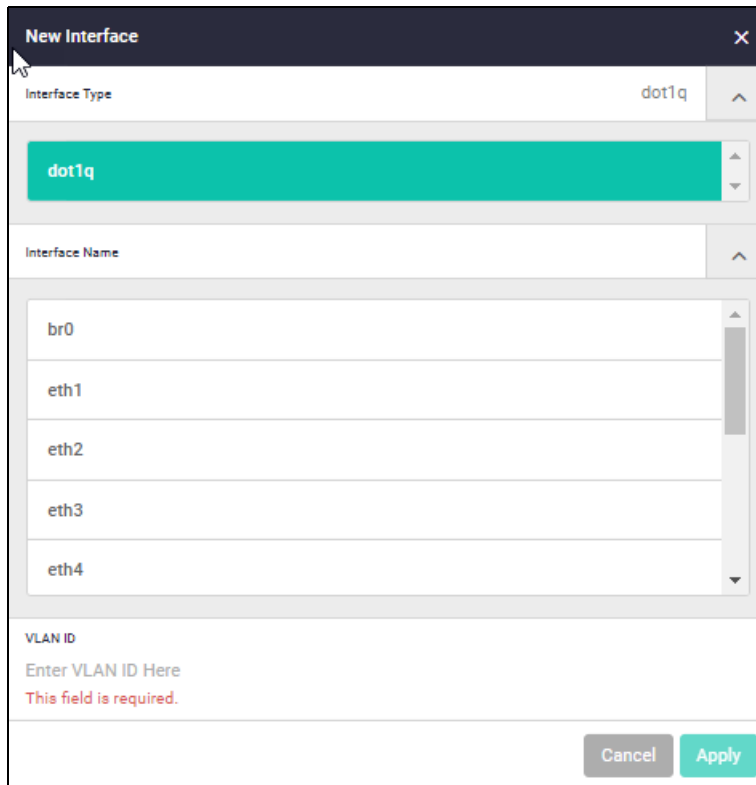


The 'Edit Interface eth2' dialog box is shown. It has a title bar with a close button. Below the title bar are two tabs: 'DHCP' and 'Fixed'. The 'Fixed' tab is selected. The 'IP Address' field is set to 'unassigned'. Below that is a section for 'Secondary IP Addresses' with an upward arrow and a button labeled 'Add Secondary IP Address'. At the bottom of the dialog are 'Cancel' and 'Apply' buttons.

- Create an 802.1Q sub-interface on an eth port or on the bridge. Click the **+ New Interface** button at the top right of the Interface table. In the **New Interface** dialog box, expand the **Interface Name** list, and select the interface. Enter a VLAN ID. Click **Apply**. The new sub-interface will show

in the **Interface** panel as the interface and the VLAN ID separated by a dot. For example, if you assign VID 300 to eth2, this is called eth2.300.

I

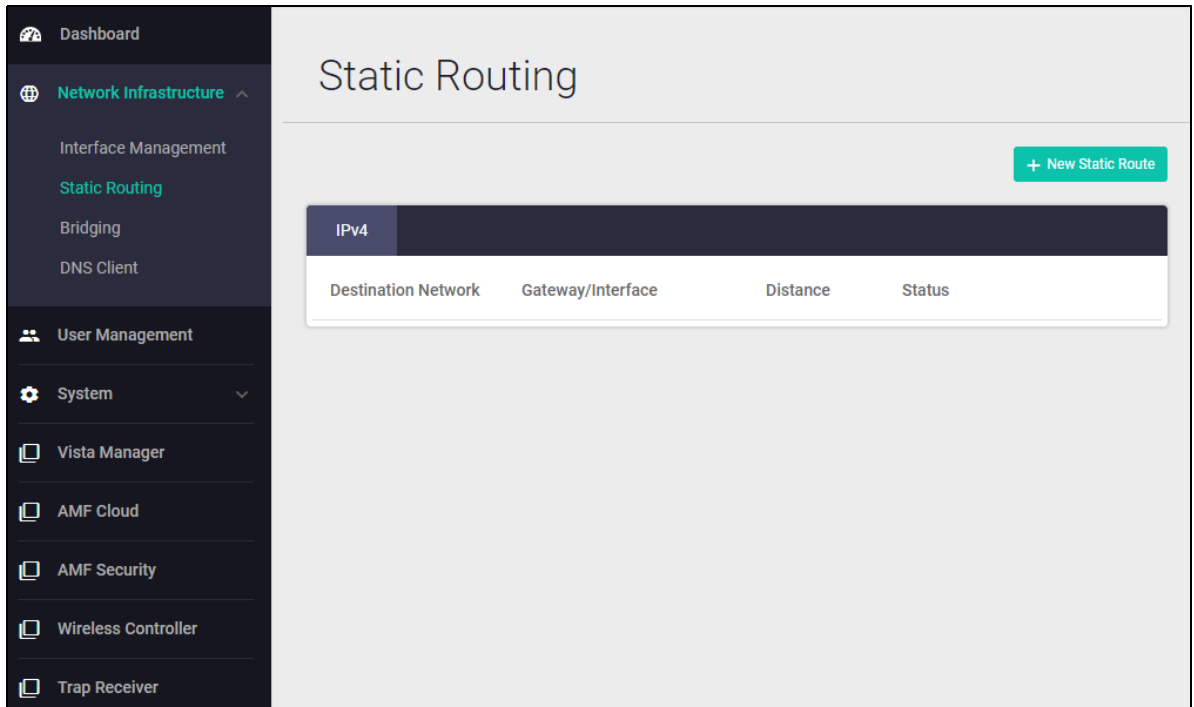


The screenshot shows a 'New Interface' dialog box with the following fields and options:

- Interface Type:** A dropdown menu currently showing 'dot1q'.
- Interface Name:** A list of interface names: br0, eth1, eth2, eth3, and eth4.
- VLAN ID:** A text input field with the placeholder text 'Enter VLAN ID Here' and a red error message 'This field is required.' below it.
- Buttons:** 'Cancel' and 'Apply' buttons at the bottom right.

Configure Static Routing

By default, the VST-APL appliance is set accept IP addressing from a DHCP server, or if none is supplied, to use the IP address 192.168.1.1. To configure and view static routes, navigate to **Network Infrastructure > Static Routing**. The default static route is not displayed.



To add a new static route, click the **+ New Static Route** button above the top right of the routes panel.

The 'New Static Route' dialog box is shown with the following fields:

Destination Network	10.1.1.0/24
Gateway/Interface	172.16.1.1
Distance (Optional)	1-255

At the bottom right of the dialog are 'Cancel' and 'Apply' buttons.

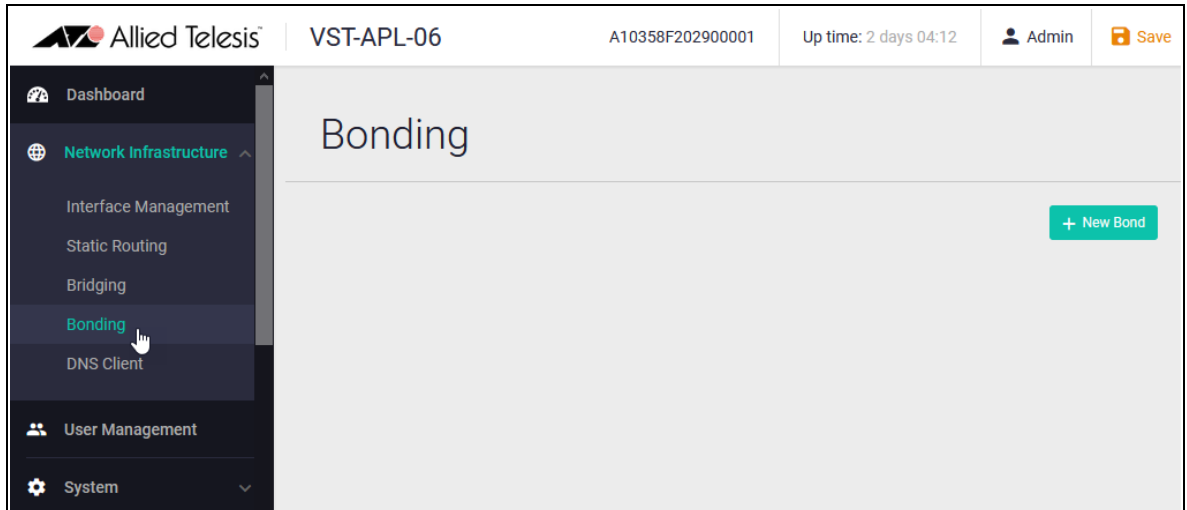
Enter the IPv4 address of the destination network. Specify the IPv4 address for the gateway, and optionally the administrative distance for the route. Click **Apply**.

To edit an existing static route, click **Edit** at its right.

Configure Bonding

You can create static or dynamic (LACP) bonds by joining multiple physical eth ports. To create, modify, or view bonds, navigate to **Network Infrastructure** > **Bonding**. You can join together in a bond any 2 or more eth links that have the same speed. For example, you can join all the 1 Gb ports into one bond.

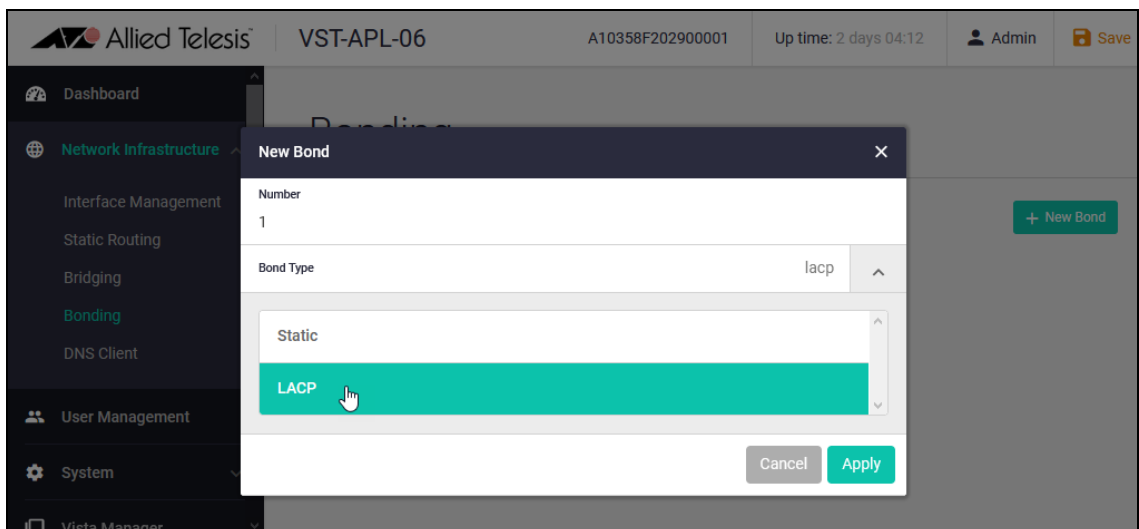
Figure 3: Bonding page



Create a bond

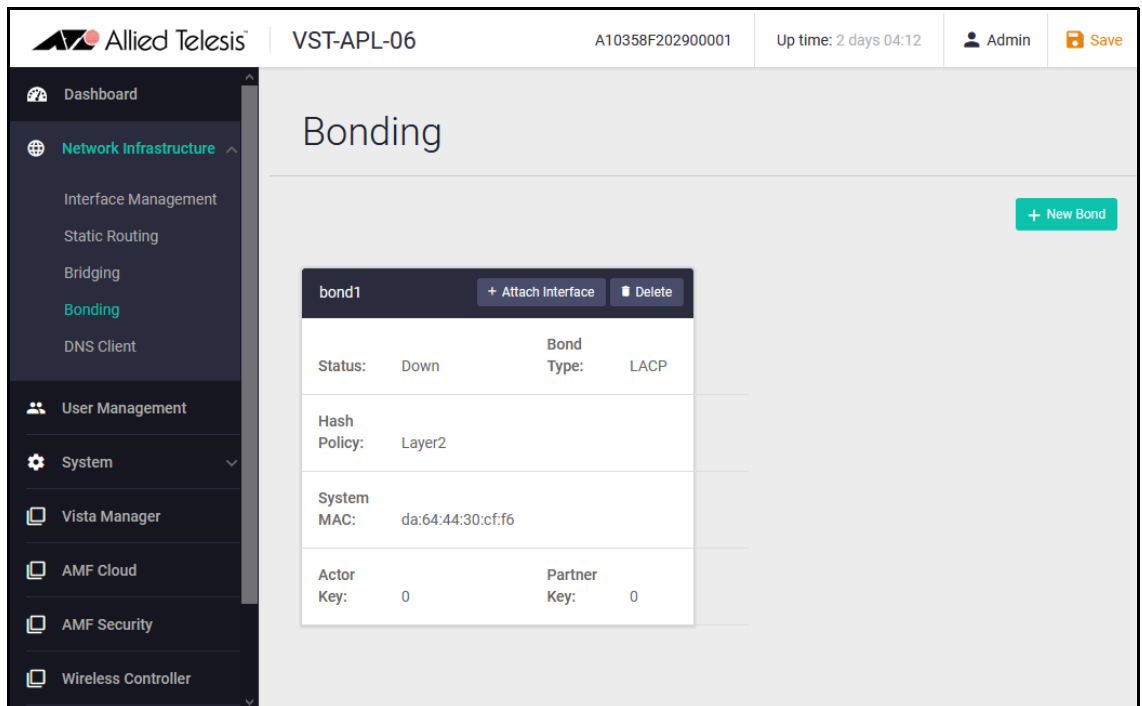
By default the appliance has no bonds. To create a bond:

1. On the **Bonding** page, click **+New Bond**.



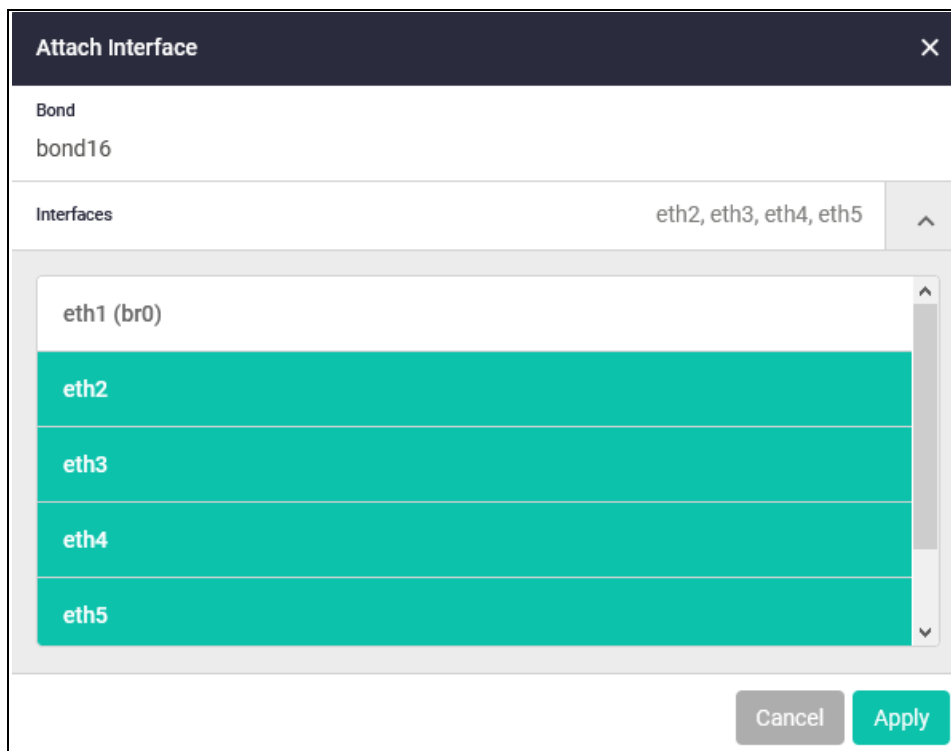
In the New Bond dialog box, enter an ID number for the bond and select whether it is to be a static bond or an LACP (dynamic) bond. Click **Apply**.

The Bonding page shows the new bond with no interfaces.



2. Click the **Attach Interface** button in the panel for the bond. Select from the list of available ports to add. An eth port is not available if it belongs to another bond. Any eth ports added to a bond are removed from the bridge.

If an interface in the list is already attached, this is shown in parentheses. Adding the interface to a bond removes it from its previous attachment. For instance “eth1 (br0)” shows that the port eth1 is attached to the bridge br0. If you add eth1 to a bond, it is removed from the bridge.



Click **Apply**.

- If you configure an LACP bond, you must ensure that the other end of the LACP connection has the appropriate LACP configuration.

The screenshot shows the Allied Telesis VST-APL-06 web interface. The sidebar menu on the left has 'Bonding' selected. The main panel displays the configuration for 'bond16'. At the top right of the bond panel are buttons for '+ Attach Interface' and 'Delete'. The configuration details are as follows:

Status:	Up	Bond Type:	LACP
Hash Policy:	Layer2		
System MAC:	8e:b1:08:ee:97:52	Partner MAC:	ec:cd:6d:d6:cf:68
Actor Key:	9	Partner Key:	1
Members:			
	Interfaces	Status	Link Partner MAC
	eth2	Up	ec:cd:6d:d6:cf:68
	eth3	Up	ec:cd:6d:d6:cf:68
	eth4	Down	unsynchronized
	eth5	Down	unsynchronized

The Bonding panel in the Bonding page shows the status of the LACP links, such as:

- **Down** (link down) and **Unsynchronised**;
 - **Up** (link partner interface is running) and **Unsynchronized** (LACP link partner is not configured correctly)
 - **Up** (link partner interface is running) and MAC address of the **Link Partner** (the link partner is synchronized).
- If required, add the bond to the bridge (**Network Infrastructure** > **Bridging** page). Bonds are not automatically attached to the bridge.

Remove an eth port from a bond

- Click on the recycle bin by the port in the bond panel on the Bonding page.
- The eth port is not automatically re-attached to the bridge. Reattach it in the **Bridging** page if required.

Remove a bond from the appliance

- Click **Delete** at the top of the bond panel in the Bonding page.
- Eth ports that were attached to the bond are not automatically re-attached to the bridge. Reattach them in the **Bridging** page if required.

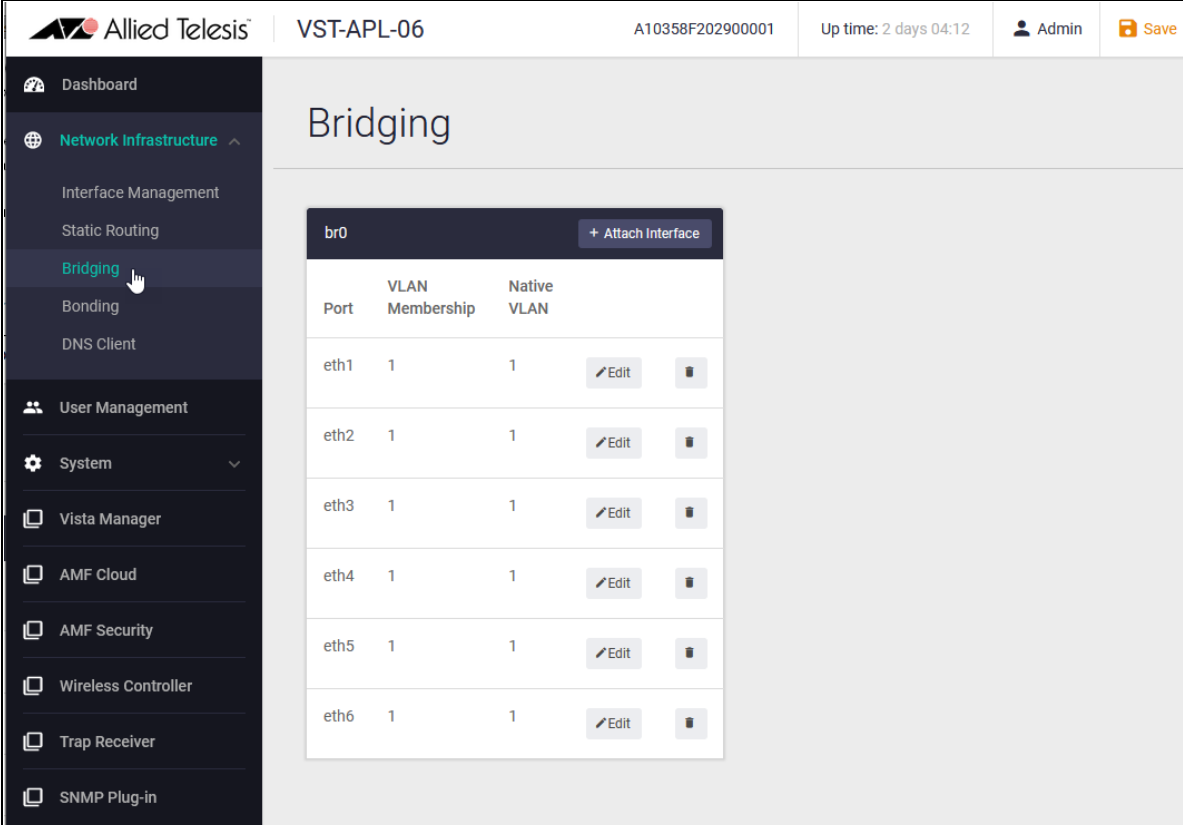
Configure Bridging

There is one VLAN-aware bridge (br0) on the appliance. By default, all physical eth interfaces are attached to the bridge. If you create bonds, they are not automatically attached to the bridge; you will need to attach them. When you activate an application, you create a virtual eth interface attachment to the bridge (eth0).

If the default configuration is suitable for your network, you don't need to change this.

To view and configure bridge connections, navigate to **Network Infrastructure > Bridging**.

Figure 4: Bridging page with default configuration



The screenshot shows the Allied Telesis VST-APL-06 web interface. The top navigation bar includes the Allied Telesis logo, the device name "VST-APL-06", the ID "A10358F202900001", the uptime "Up time: 2 days 04:12", the user "Admin", and a "Save" button. The left sidebar contains a menu with "Network Infrastructure" expanded, showing "Interface Management", "Static Routing", "Bridging" (selected), "Bonding", and "DNS Client". Below this are "User Management", "System", "Vista Manager", "AMF Cloud", "AMF Security", "Wireless Controller", "Trap Receiver", and "SNMP Plug-in". The main content area is titled "Bridging" and shows a configuration for bridge "br0". A "+ Attach Interface" button is visible. Below it is a table with the following data:

Port	VLAN Membership	Native VLAN		
eth1	1	1	Edit	
eth2	1	1	Edit	
eth3	1	1	Edit	
eth4	1	1	Edit	
eth5	1	1	Edit	
eth6	1	1	Edit	

You can use the **Bridging** page to:

- Attach a physical port or a bond to the bridge. Click the **+ Attach interface** button at the top right of the table. In the **Add Port** dialog box, select from the available interfaces (ports and bonds). Enter the VLAN membership range (a contiguous range) and the native VLAN ID. Click **Apply**.

If an interface in the list is already attached, this is shown in parentheses. Adding the interface to the bridge removes it from its previous attachment. For instance “eth2 (bond16)” shows that the port eth2 is part of bond 16. If you add eth2 to the bridge, it is removed from the bond.

The screenshot shows the 'Add Port' dialog box. The 'Name' field is set to 'br0'. The 'Ports' section contains a list of interfaces: 'bond16', 'eth2 (bond16)', 'eth3 (bond16)', 'eth4 (bond16)', and 'eth5 (bond16)'. A 'recycle bin' icon is visible to the right of the list. The 'Apply' button is highlighted in green.

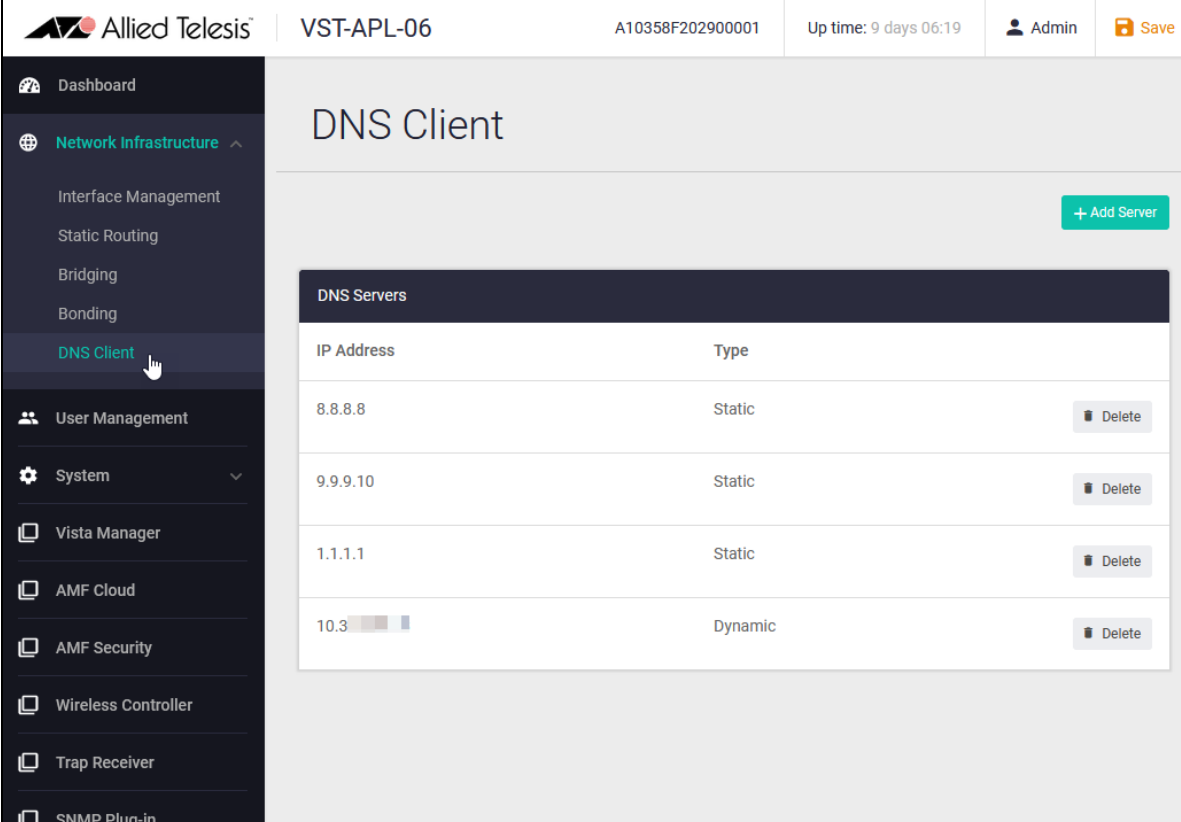
- Remove a port attachment from the bridge. Click the **recycle bin** to its right.
- Edit VLAN membership for physical eth ports and bonds attached to the bridge. Click the **Edit** button to its right. Enter the VLAN membership range (a contiguous range) and the native VLAN ID. Click **Apply**.

I

The screenshot shows the 'Edit Port' dialog box. The 'Port' field is set to 'eth6'. The 'VLAN Membership' field is set to '1'. The 'Native VLAN' field is set to '1'. The 'Apply' button is highlighted in green.

Configure the DNS Client

To view or configure DNS servers configured for the DNS client on the appliance, navigate to **Network Infrastructure > DNS Client**. Any DNS Servers assigned by DHCP are shown as dynamic entries.

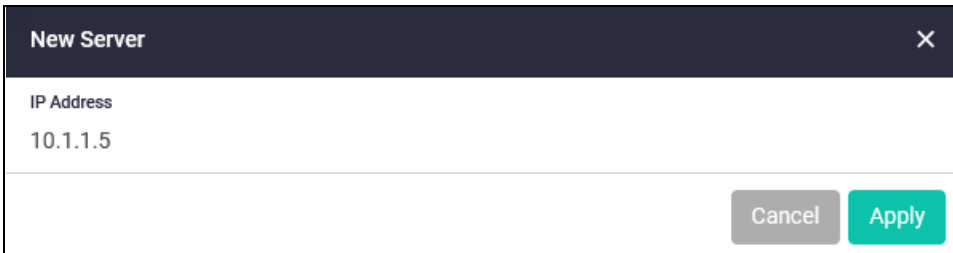


The screenshot shows the Allied Telesis VST-APL-06 DNS Client configuration page. The page title is "DNS Client". On the left is a navigation menu with "DNS Client" selected. The main content area shows a table of DNS Servers. The table has two columns: "IP Address" and "Type". There are four rows of data, each with a "Delete" button to its right. The first three rows are for static servers (8.8.8.8, 9.9.9.10, 1.1.1.1) and the last row is for a dynamic server (10.3). A "+ Add Server" button is located at the top right of the table.

IP Address	Type	
8.8.8.8	Static	Delete
9.9.9.10	Static	Delete
1.1.1.1	Static	Delete
10.3	Dynamic	Delete

In the DNS Client page:

- To add a DNS server, click the **+ Add Server** button at the top right of the table of servers. Enter the IP address of the DNS server and click **Apply**.



The screenshot shows a "New Server" dialog box. The dialog box has a title bar "New Server" and a close button. It contains a label "IP Address" and a text input field with the value "10.1.1.5". At the bottom right are "Cancel" and "Apply" buttons.

- To delete a DNS server, click **Delete** to its right.

System management

In this section, see information on how to:

- "Manage files" on page 38
- "Generate tech support information" on page 41
- "Configure system time" on page 42
- "View system information" on page 44
- "Configure users" on page 46
- "Enable remote shutdown" on page 47

Manage files

Navigate to **System > File Management**. In the File Management page, you can view and manage files in the appliance's persistent storage, manage software updates, and access troubleshooting data for tech support.

The screenshot displays the File Management interface for a VST-APL-06 appliance. The top navigation bar includes the Allied Telesis logo, the device name, a unique ID (A10358F202900001), the uptime (3 days 04:01), the user (Admin), and a Save button. The left sidebar shows the navigation menu with 'System' expanded to 'File Management'. The main content area is titled 'File Management' and includes a Reboot and Shutdown button. Below this, there are three main sections: 'Set Boot Release File' showing the current boot file as 'ATVSTAPL-1.iso' with a 'Browse' button; 'Flash Usage' showing a 75% usage bar and '7.0G / 9.9G' of space; and a file list for '/fs /flash' with columns for Name, Modified, Size(bytes), and Actions. The file list includes various application files and a default configuration file.

Name	Modified	Size(bytes)	Actions
AMF-x86_64-5.11.0.app	24/12/2020, 10:53:21 am	20679024	Download Delete
awc-x86_64-3.11.0.app	24/12/2020, 10:53:11 am	126787468	Download Delete
default.cfg	9/03/2021, 9:36:40 am	10471	Download Delete
fullsnmp-x86_64-2.5.0.app	26/01/2021, 8:56:00 am	104207016	Download Delete
log	9/03/2021, 9:38:32 am		
sesc-x86_64-3.11.0.app	7/08/2020, 9:05:12 am	40132136	Download Delete
snmp-x86_64-2.5.0.app	7/08/2020, 9:05:14 am	211087756	Download Delete
vista-x86_64-3.11.0.app	24/12/2020, 10:53:17 am	375573808	Download Delete

File system

By default this page will show that the VST-APL file system contains files for:

- each application (filename `*appname-x86_64-x.x.x.app`, where x.x.x is the version, for example, `vista-x86_64-3.11.0.app`).

Note that the operating system and application image files shown in the file system may not be the ones currently running on the appliance. The files shown here are available for activating or upgrading appliance software.

- the default configuration (filename `default.cfg`)

- a log directory for log files. The appliance stores the messages in log files (filenames “messages*”) in the log directory in the persistent storage system.
- the appliance operating system (ATVSTAPL-x.x.x.iso)

Persistent storage may also contain other files that are:

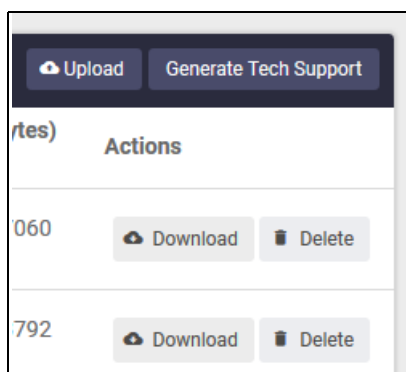
- generated by the appliance, such as tech-support files (tech-support... .tgz)
- uploaded by a user, for instance new versions of software files. Note that the image files shown in the file system may not be the ones currently running on application.

The **Flash Usage** panel shows the amount and percentage of persistent storage used.



Upload and download files

To upload a file to the appliance’s persistent storage, use the **Upload** button at the top of the file system panel. To download or delete a file from the appliance, click the **Download** or **Delete** button to the right of the file.



To navigate the file system, click on the path at the top of the file system panel, or click on a directory in the panel.

/fs /flash				Upload	Generate Tech Support
Name	Modified	Size(bytes)	Actions		
AMF-x86_64-2.3.app	24/12/2020, 10:53:21 am	20679024	Download	Delete	
awc-x86_64-3.app	24/12/2020, 10:53:11 am	126787468	Download	Delete	
default.cfg	9/03/2021, 9:36:40 am	10471	Download	Delete	
fullsnmp-x86_64-2.app	26/01/2021, 8:56:00 am	104207016	Download	Delete	
log	9/03/2021, 9:38:32 am				

USB memory device

You can insert an external USB memory device for uploading and downloading files.

To safely remove a USB device:

In the File Management page, in the **External Device Usage** panel, click the **Eject** button for the external device. Then remove it physically from the port.

External Device Usage		
/mnt/media0	98% 907GB / 931.5GB	Eject
/mnt/media1	43% 780.3GB / 1.8TB	Eject

Generate tech support information

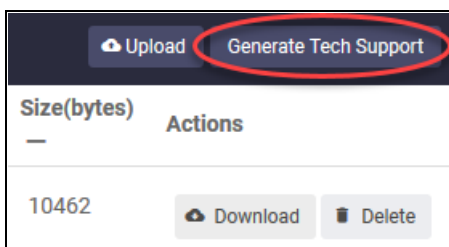
You can generate tech support output for the appliance and for each application instance that is running on it. Tech-support output can assist with troubleshooting. It includes detailed information about configuration and internal processes in the appliance. (You cannot create a tech-support file for an application when it is not running.) If you contact Allied Telesis for support, you can generate tech support files on the appliance and send them this information.

To generate a tech support output file for a single application:

1. Make sure the application is running.
2. From the VST-APL dashboard menu, navigate to the application page for the application. For instance, to generate a tech-support file for the Vista Manager application, navigate to the Vista Manager page.
3. Click the **Generate Tech Support** button. The application generates the tech support file and stores it in the appliance **/fs/flash** directory. The file name indicates the application.
4. Wait while the application generates a tech-support file. This can take up to a few minutes. The larger the tech-support data file, the longer this takes.
5. The tech support files will show in the **/fs/flash** directory in the **File Management** page. You can download them from there. You may need to refresh the page to see the new files.

To generate tech support output for the appliance, and optionally applications:

1. From the VST-APL dashboard menu, navigate to **System > File Management**.
2. Click the **Generate Tech Support** button. A pop-up opens showing the device and the running applications. By default, all of these are selected to generate tech-support data.



3. Update the selection as required and click **Generate**. The device and each application generate a tech support file and store it in the appliance **/fs/flash** directory.
4. Wait while the device and applications generate tech-support files. This can take up to a few minutes. The larger the tech-support data file, the longer this takes.
5. Navigate to the **System > File Management** page and the **/fs/flash** directory to view or download the files. You may need to refresh the page to see the new files.

Reboot or shut down

To reboot or shut down the appliance, use the green **Reboot** or **Shutdown** button buttons at the top right of this page.



Configure system time

To configure system time, navigate to **System > Time**. In the **Time** page, you can set the system time manually, or set the appliance to use NTP relationships to determine system time.

The screenshot shows the 'Time' configuration page in the Allied Telesis VST-APL-10 GUI. The page title is 'Time' and the current system time is '10 Sep 2020 04:54 PM'. The left sidebar shows the navigation menu with 'System' selected. The main content area has a 'System Time' section with a calendar and time selection controls (04:53 PM) and an 'Apply' button. Below this is an 'NTP' section with a table for adding NTP relationships. A green '+ Add NTP Relationship' button is circled in red.

Address	Type	Version	Preferred	+ Add NTP Relationship
---------	------	---------	-----------	------------------------

The system time is displayed as local time according to the time zone of the browser used to connect to the VST-APL GUI (not UTC time).

To set the time manually, set it to local time and click **Apply**.

To add an NTP server for the device to get time settings from using the Network Time Protocol, use the following steps.

1. Click the green **Add NTP Relationship** button at the top right of the NTP panel.

The screenshot shows the 'Add NTP Relationship' dialog box. The dialog has a title bar with a close button. The main content area has the following fields:

- Address (IPv4/IPv6/Hostname): 192.168.1.100: b8:: / pool.ntp.org
- Type: [Dropdown menu]
- Version: [Dropdown menu]
- Preferred: [No] [Yes]

At the bottom of the dialog are 'Cancel' and 'Apply' buttons.

2. Enter the IP address of the NTP peer.
3. Expand the **Type** options by clicking the arrow to the right. Select whether the NTP relationship is to an NTP server, peer or pool.
4. Expand the **Version** options by clicking the arrow to the right. Select the version of the NTP protocol to use with this peer.

Add NTP Relationship [X]

Address (IPv4/IPv6/Hostname)
192.16 b8:: / pool.ntp.org

Type [^]

- Server
- Peer
- Pool

Version [^]

- 1
- 2
- 3
- 4

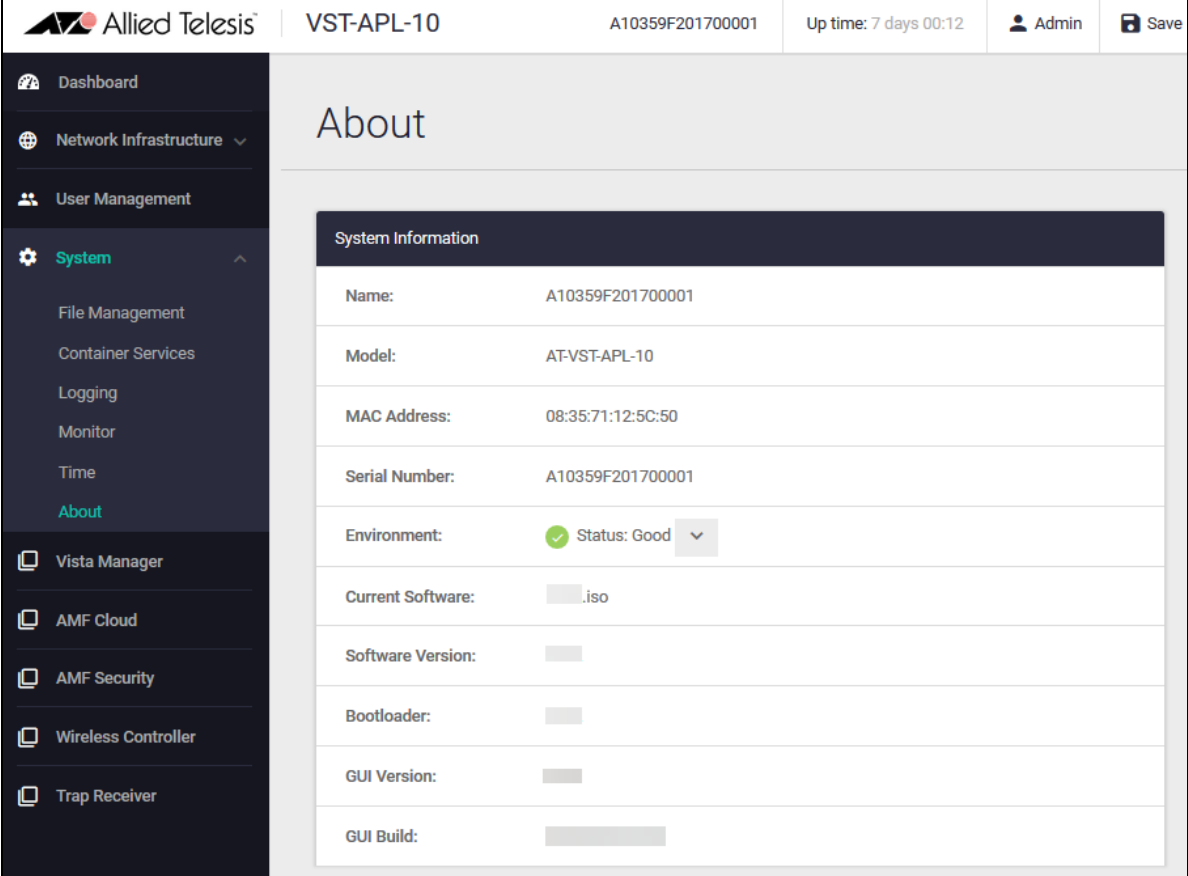
Preferred [No] [Yes]

[Cancel] [Apply]

5. Set one NTP peer to be preferred by clicking the **Yes** button. If you configure more than one NTP peer, set the others to **No**. The VST-APL will set its system time based on NTP messages it receives from the preferred peer, or from another peer if it does not receive valid messages from the preferred peer.

View system information

To see details of system hardware, operating software, and environmental indicators, navigate to **System > About**. The About page provides a good overview of your physical appliance and its current setup, and is very helpful in the event of a problem, to assist Allied Telesis support.



The screenshot shows the Allied Telesis management interface for a VST-APL-10 device. The top navigation bar includes the Allied Telesis logo, the device name 'VST-APL-10', the serial number 'A10359F201700001', the uptime 'Up time: 7 days 00:12', the user 'Admin', and a 'Save' button. A dark sidebar on the left contains a menu with items: Dashboard, Network Infrastructure, User Management, System (highlighted), File Management, Container Services, Logging, Monitor, Time, About, Vista Manager, AMF Cloud, AMF Security, Wireless Controller, and Trap Receiver. The main content area is titled 'About' and features a 'System Information' table.

System Information	
Name:	A10359F201700001
Model:	AT-VST-APL-10
MAC Address:	08:35:71:12:5C:50
Serial Number:	A10359F201700001
Environment:	✔ Status: Good ▼
Current Software:	...iso
Software Version:	...
Bootloader:	...
GUI Version:	...
GUI Build:	...

To expand details of environmental indicators, click the arrow to the right of the **Environment Status**.

Allied Telesis | VST-APL-10 | A10359F201700001

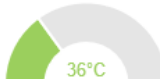





Dashboard
 Network Infrastructure
 User Management
 System
 File Management
 Container Services
 Logging
 Monitor
 Time
 About
 Vista Manager
 AMF Cloud
 AMF Security
 Wireless Controller
 Trap Receiver

About

System Information

Name:	A10359F201700001
Model:	AT-VST-APL-10
MAC Address:	08:35:71:12:5C:50
Serial Number:	A10359F201700001
Environment:	✔ Status: Good ⌵

AT-VST-APL-10

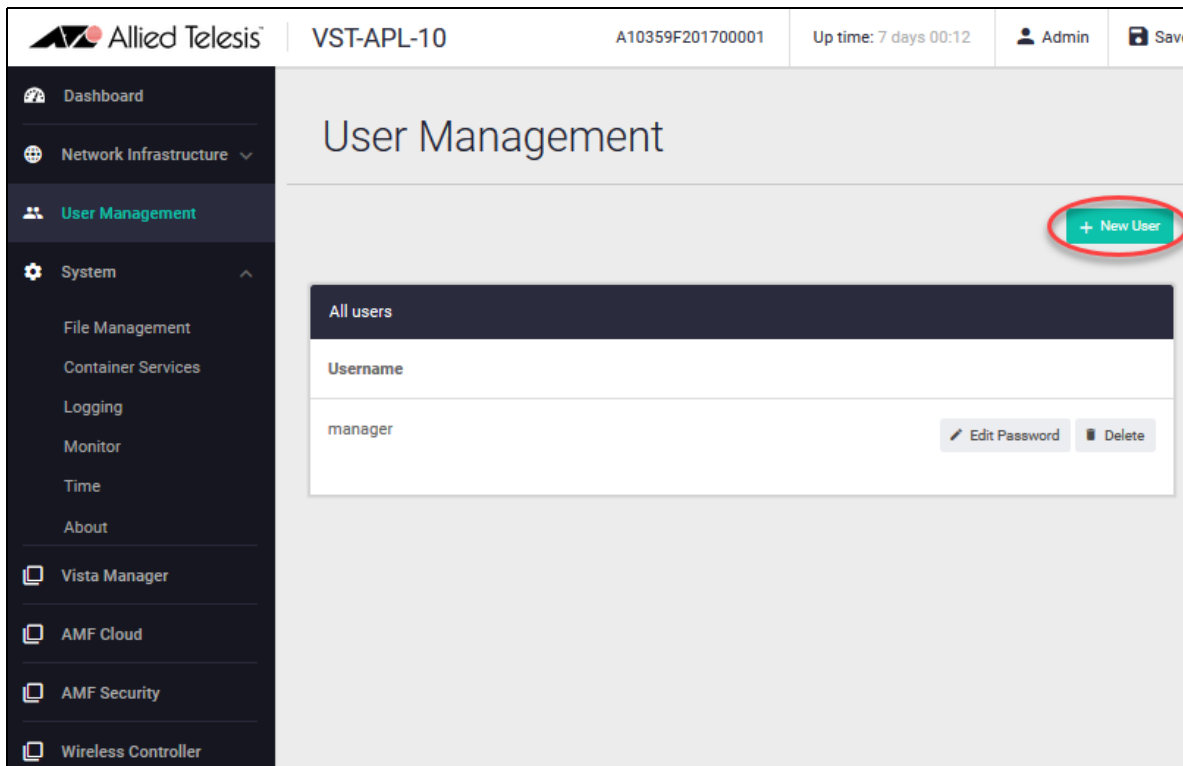
Core 0	 36°C	Core 1	 37°C
Core 3	 37°C	Core 4	 35°C
Fan1	 3479rpm	Fan2	 3479rpm

This shows detailed status for monitored components, such as the temperature of each of the CPU cores and the speed for each monitored fan.

To see the current running software version running on the appliance, see the File Management page (see "[Manage files](#)" on page 38).

Configure users

By default, the VST-APL comes with a single user account with username “manager” and password “friend”. We recommend you change this password for security. To view and configure user accounts for the appliance, select **User Management** in the Dashboard menu.



All user accounts have the same privileges as the ‘manager’ account. To add a new user, in the User Management page, click the green **+ New User** button at the top right of the All users panel and enter the username and password (twice), then click **Save**.

To change the password for a user, click the **Edit password** button to the right of the user, enter the new password, then click **Save** in the **Edit password** dialog box.

To remove a user account, click the **Delete** button to its right.

After making changes to the user accounts, click **Save** at the top right of the VST-APL window to save the appliance configuration.

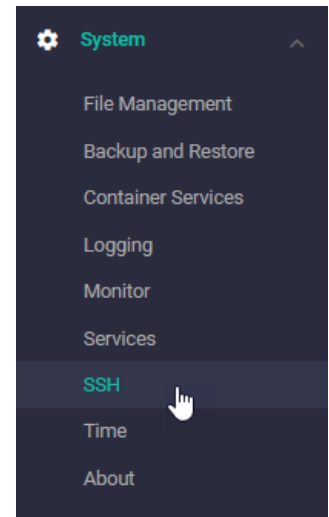
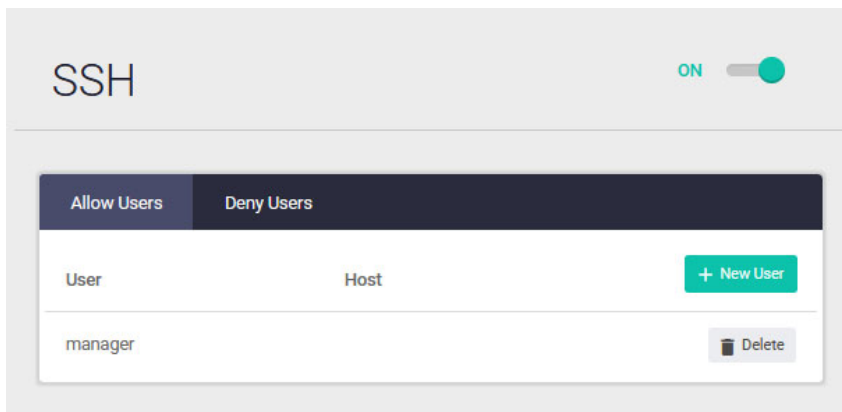
Enable remote shutdown

You can enable users to access the device command line remotely using either SSH (recommended) or Telnet to 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.

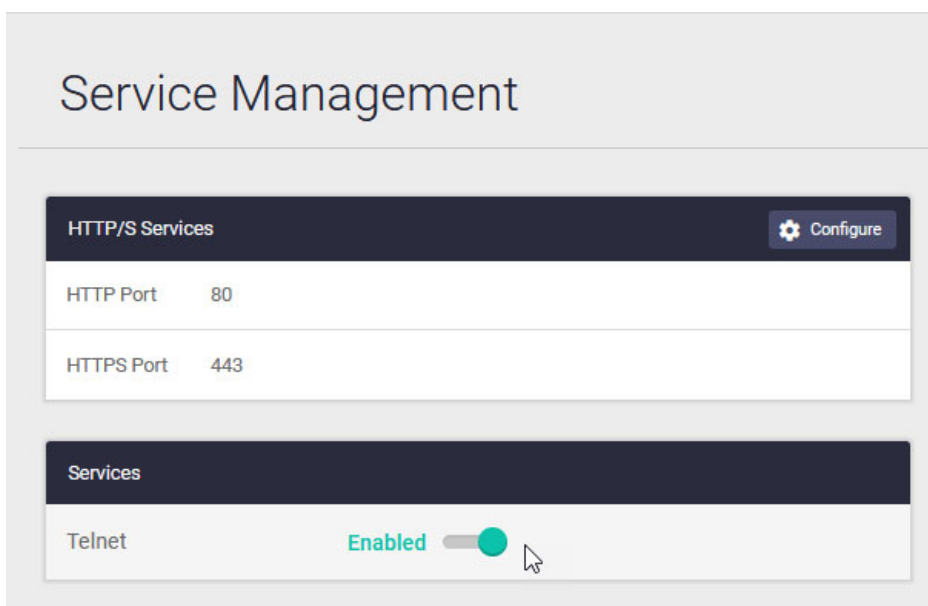
To enable a user to power down the device remotely via SSH:

1. From the VST-APL menu, navigate to **System > SSH**.
2. In the **SSH** page, enable SSH. Move 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
```

Monitoring

You can view some general information for the appliance on several pages, including the Dashboard, the File Management page (including Generate tech-support), and the About page.

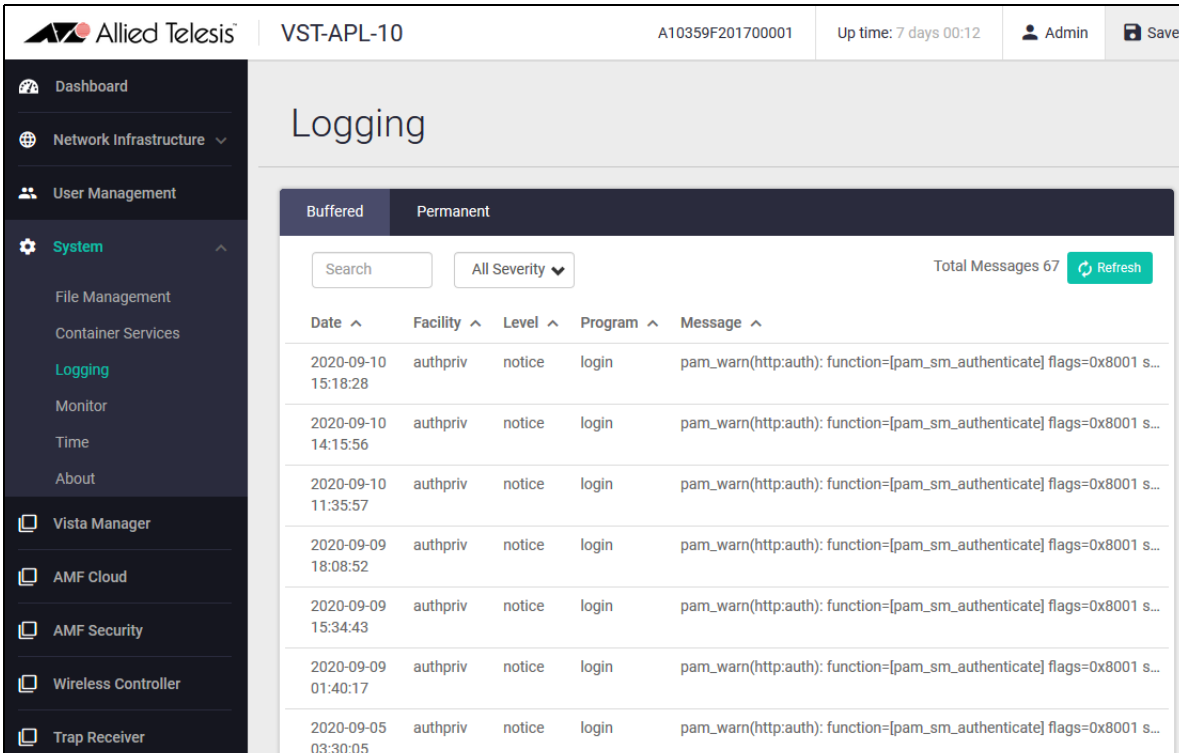
You can see an overview of the environmental status of the appliance on the Dashboard **System Information** panel ("[The VST-APL GUI Dashboard](#)" on page 21) and by navigating to the **System > About** page ("[View system information](#)" on page 44).

This section describes pages that provide more detailed monitoring information:

- "[View log messages](#)"
- "[Monitor system CPU, memory and storage I/O](#)" on page 51

View log messages

The VST-APL generates log messages related to the operation of the appliance. To view log messages, navigate to **System > Logging**.



The screenshot shows the VST-APL web interface. The top navigation bar includes the Allied Telesis logo, the device name 'VST-APL-10', a serial number 'A10359F201700001', the uptime '7 days 00:12', and user information 'Admin' with a 'Save' button. The left sidebar contains a menu with 'System' selected, and sub-items like 'File Management', 'Container Services', 'Logging', 'Monitor', 'Time', 'About', 'Vista Manager', 'AMF Cloud', 'AMF Security', 'Wireless Controller', and 'Trap Receiver'. The main content area is titled 'Logging' and has two tabs: 'Buffered' and 'Permanent'. Below the tabs is a search bar and a dropdown for 'All Severity'. A 'Total Messages 67' indicator and a 'Refresh' button are also present. A table displays log messages with columns for Date, Facility, Level, Program, and Message. The messages shown are all 'pam_warn' entries from the 'login' program, with various timestamps and severity levels.

Date	Facility	Level	Program	Message
2020-09-10 15:18:28	authpriv	notice	login	pam_warn(http:auth): function=[pam_sm_authenticate] flags=0x8001 s...
2020-09-10 14:15:56	authpriv	notice	login	pam_warn(http:auth): function=[pam_sm_authenticate] flags=0x8001 s...
2020-09-10 11:35:57	authpriv	notice	login	pam_warn(http:auth): function=[pam_sm_authenticate] flags=0x8001 s...
2020-09-09 18:08:52	authpriv	notice	login	pam_warn(http:auth): function=[pam_sm_authenticate] flags=0x8001 s...
2020-09-09 15:34:43	authpriv	notice	login	pam_warn(http:auth): function=[pam_sm_authenticate] flags=0x8001 s...
2020-09-09 01:40:17	authpriv	notice	login	pam_warn(http:auth): function=[pam_sm_authenticate] flags=0x8001 s...
2020-09-05 03:30:05	authpriv	notice	login	pam_warn(http:auth): function=[pam_sm_authenticate] flags=0x8001 s...

The appliance sends log messages to both the:

- **permanent log**

The permanent log is stored in persistent storage, and retains messages when the appliance is rebooted. Messages of severity level warning (4) and higher go to the permanent log.

To view messages in the permanent log, click **Permanent** at the top of the logging panel. If a tech-support file is generated, the contents of the permanent log are included in it.

The appliance stores the messages in log files in the log directory in the persistent storage system with file names beginning with 'messages'. To download or delete a log file, navigate to the **System > File Management** page and the **log** directory ("[Manage files](#)" on page 38).

- **buffered log**

The buffered log is in current memory. It contains the most recent log messages and discards older ones when it fills the allocated memory. These messages are lost when the appliance restarts. Messages of severity level notice (5) and higher go to the buffered log.

To view messages in the buffered log, click **Buffered** at the top of the logging panel.

The logging panel displays these components for each message:

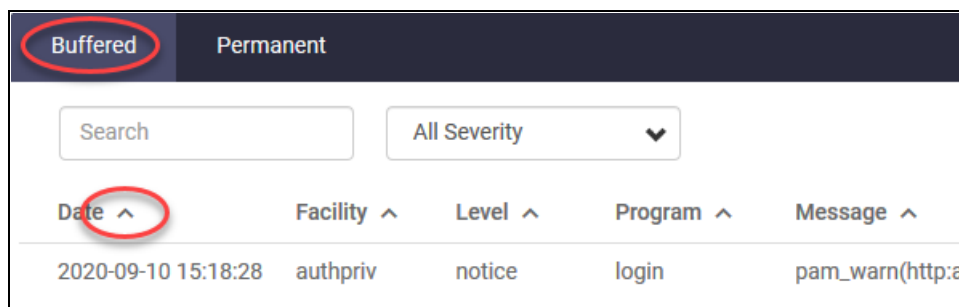
- Date—the date and time when the log message was generated, according to the device’s clock in the local time zone.
- Facility—the facility in the operating software that generated the message.
- Level—the severity level of the message, indicating how important it is. See the table below.
- Program—the particular program in the operating system that generated the message.
- Message—the content of the message.

Table 7: Severity levels in log messages

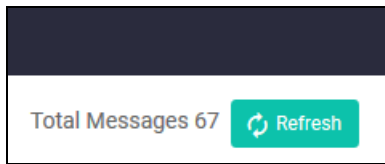
SEVERITY IN MESSAGE	SEVERITY LEVEL	MEANING
emerg	0	Emergency: the system is unusable; operation severely impaired.
alert	1	Alert: action must be taken immediately; operation has been or could be affected.
crit	2	Critical conditions; a possible problem or issue that requires manager attention.
err	3	Error: error conditions; an issue that may require manager attention.
warning	4	Warning conditions; normal notification of an event, not serious or particularly important.
notice	5	Notice: normal but significant condition; useful information that can generally be ignored during normal operation. Messages of this severity level are sent to the buffered log but not to the permanent log.
info	6	Informational messages.
debug	7	Debug level messages; extremely detailed (possibly high-volume) debugging information.

To select which messages to display:

- Show the messages in either the Buffered or the Permanent log by clicking the Buffered or Permanent button at the top of logging panel.
- To filter the messages, select a particular severity level to display or enter a search string.
- To sort the messages, click the arrow to the right of any column headings: Date, Facility, Level, Program, Message.



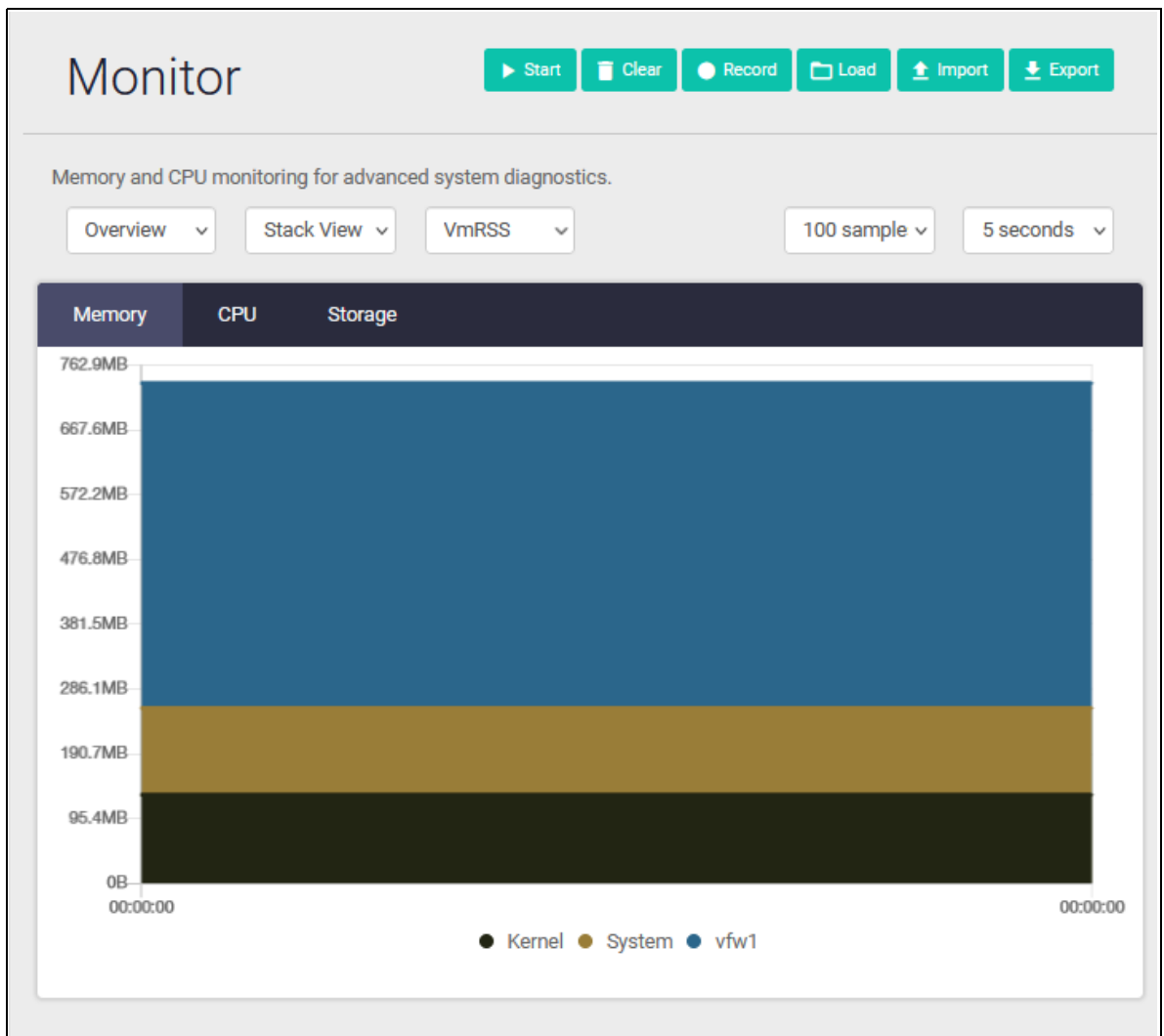
- To update the display, click the green **Refresh** button at the top right of the **Logging** panel. To the left of this button you can see how many messages match the current selection.



- Select how many messages to display at the bottom right of the page.

Monitor system CPU, memory and storage I/O

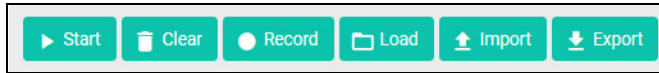
To monitor system CPU, memory use, and input/output storage processing, in the side menu, navigate to **System > Monitor**. The appliance can gather samples of memory, CPU usage or storage data for the appliance itself and for applications running on it.



Set the sampling parameters:

- Set the maximum number of data samples to gather by setting the **sample collection limit** in the drop-down list.
- Set the interval between samples by setting the **sampling period** in the drop-down list.

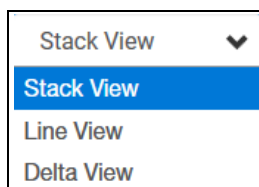
Use the green buttons to gather and record data.



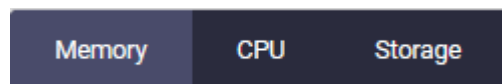
- Start the appliance collecting usage data samples by clicking the green **Start** button and stop sampling by clicking the red **Stop** button.
- Record the data in a file in the appliance persistent storage by clicking the green **Record** button
- Export the data as displayed in the GUI browser to a file in the appliance persistent storage by clicking the green **Export** button
- Reimport data from a file in persistent storage to display in the GUI **Monitoring** page by clicking the green **Load** button
- Import a data file from the file system of the device running the browser to display in the GUI **Monitoring** page by clicking the green **Import** button
- Clear the data from the browser by clicking the green **Clear** button

Select your view of the sampled data (without affecting the sampling itself) in the graph on the Monitoring page. The key below the graph shows the color for each program. You can:

- Select the type of **graph** to display from stack view, line view or delta view (values since the start of sampling, beginning at 0) from the drop-down list.



- Select whether to monitor memory, CPU usage, or storage by clicking the **Memory**, **CPU** or **Storage** tab at the top of the graph panel.



- Display the usage for a particular program by selecting it from the drop-down list. See the color-coded key for the programs below the graph.

To display more detailed memory use for a particular program, select the program in the drop-down list to the left above the graph.

Managing applications

This section describes the application pages in the VST-APL GUI, and:

- "Start, stop and remove applications" on page 53
- "View the Container Services page" on page 54
- "Restore an application after appliance restart" on page 55

From VST-APL application page you can also:

- Change the configuration for the application container in VST-APL, including the network infrastructure. Click the **Configure** button.
- Generate a tech-support file for an application by clicking the **Generate tech-support** button. See "Generate tech support information" on page 41.

Start, stop and remove applications

There is a page for each application; click on the menu item for the application to open its page.

Dashboard

Network Infrastructure

User Management

System

Vista Manager

AMF Cloud

AMF Security

Wireless Controller

Trap Receiver

AMF Security

Allied Telesis Autonomous Management Framework (AMF) simplifies and automates network management. AMF Security adds a powerful security component with an intelligent, fully-featured SDN controller. It reduces manual effort and cost in two ways: first, it reads data from business applications and automatically changes network configuration. Then, AMF Security works with security applications to instantly respond to alerts, and block the movement of threats within a wired or wireless network.

For more information contact your local Allied Telesis sales representative. Find your local Allied Telesis office at www.alliedtelesis.com/contact

Image server poll interval: Disabled

Deployed Application			
CPU Load (%)	Memory (MB)	Storage (MB)	State
		50000MB	Stopped

Destroy Start

This page displays the CPU load, the memory in MB, the storage in MB, and the state of the application, including whether it is:

- **Offline**—The application instance has not yet been activated or is not reachable.
- **Extracting, Creating**—when you activate the application, it extracts and creates an instance of the application on the appliance.
- **Running**—the application is running; normal operation.
- **Stopping or stopped**—the application stops gracefully. Before you can change the application configuration, you must stop the application. To stop an application, click the **Stop** button.
- **Destroying**—the application and its configuration is being removed from the appliance.
Caution: Destroying an application removes the application, its configuration, and all data associated with the application instance from the appliance. To destroy an application, click the **Destroy** button.

If the application has its own GUI (such as Vista Manager), then you can access it by clicking the **Open** button. You can also enter the application's IP address directly in your browser.

View the Container Services page

The underlying technology supporting the applications on this appliance is Container Services.

The System menu includes a Container Services page. In this page, you can see an overview of all the applications on the appliance. Do not use this page to configure or manage applications. Instead, use the separate application pages. Click on the menu item for the application.

Caution: The VST-APL supports one instance of each application associated with Vista Manager. Attempting to use this page to activate more instances of these applications can result in overloading the appliance's resources and unpredictable behaviour. The Container Services page is intended for advanced users who understand the systems resources. For configuration, regular users should only use the specific menu items for each application they need to configure. If you use this page, then monitor the total storage, memory and CPU items in the Compute Node section. If any of these change to red, then you are close to using all the system resources.

Note that the IP address field in the Compute Node Panel on this page is for a Network Attached Compute node. On the VST-APL appliance, this field is empty. The deployed applications run on the local device itself, not on a network attached node.

Restore an application after appliance restart

We recommend saving any appliance configuration that you want to retain as soon as you have made it, before the appliance reboots. The **Save** button is orange when there is unsaved configuration and blue when configuration has been saved. Click it to save.

However, if the VST-APL restarts after an application has been activated but before the appliance configuration has been saved, you can still restore the application and its configuration without having to begin again.

To restore one or more such applications:

1. When the appliance has restarted, navigate to the application page from the VST-APL menu.
2. In the application page, click the **Restore** button to the right of the application in the Deployed Application panel.

The screenshot shows the Allied Telesis VST-APL-06 management interface. The top header includes the Allied Telesis logo, the device name 'VST-APL-06', the ID 'A10358F201700001', the uptime 'Up time: 0 days 04:50', the user 'Admin', and a 'Save' button. The left sidebar contains a navigation menu with items: Dashboard, Network Infrastructure, User Management, System, Vista Manager (highlighted with a mouse cursor), AMF Cloud, AMF Security, Wireless Controller, and Trap Receiver. The main content area is titled 'Vista Manager' and contains a description of the tool, contact information for Allied Telesis, and a dropdown menu for 'Image server poll interval' set to 'Disabled'. Below this is a 'Deployed Application' table with the following data:

CPU Load (%)	Memory (MB)	Storage (MB)	State
		204800MB	Offline

To the right of the application row are two buttons: 'Destroy' and 'Restore'. The 'Restore' button is highlighted with a red circle.

The application is restored to the configuration it had before the restart. This may take a few minutes.

3. To start the application, click the **Start** button to its right.
4. Save the appliance configuration by clicking the **Save** button.

Backing up and Restoring VST-APL

You can create backups of the state of the VST-APL Network Appliance including some or all of the appliance configuration, application images (.app), and snapshots of application configuration and data for application instances. You can use a backup to restore either an individual application instance or all the appliance configuration, files, and application instances. (This feature does not back up application bundle files.)

Use the Backup and Restore page in the VST-APL GUI to:

- ["Schedule regular backups" on page 56](#) (VST-APL 3.7.1 and onward)
- ["Create a single backup now" on page 59](#) (VST-APL 3.4.1 and onward)
- ["Manually restore the whole appliance from a backup" on page 65](#)—use the backup file to return the device to the same state at a later date, or to replace the device with an identical back-up device (VST-APL 3.4.1 and onward)
- ["Restore a single application instance on the appliance from a back-up" on page 69](#)—restore one or more application instances on the appliance without removing other appliance configuration (VST-APL 3.4.1 and onward)
- ["Automatically restore the whole appliance from a backup onto new appliance hardware" on page 73](#) (VST-APL 3.7.1 and onward).

Schedule regular backups

You can create multiple backup schedules, for example to backup daily and weekly.

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.

To create a schedule:

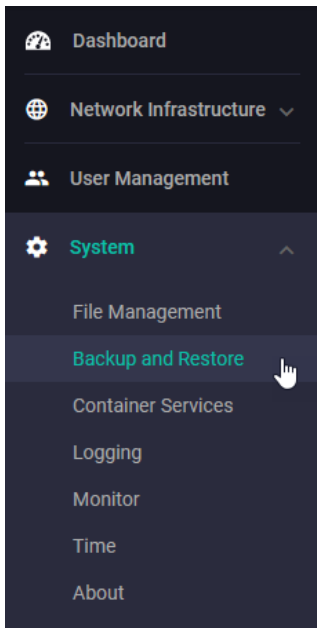
Step 1: Connect external media

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

The external media must have space for the new backup files and support sufficiently large file sizes (e.g. file system format ext4).

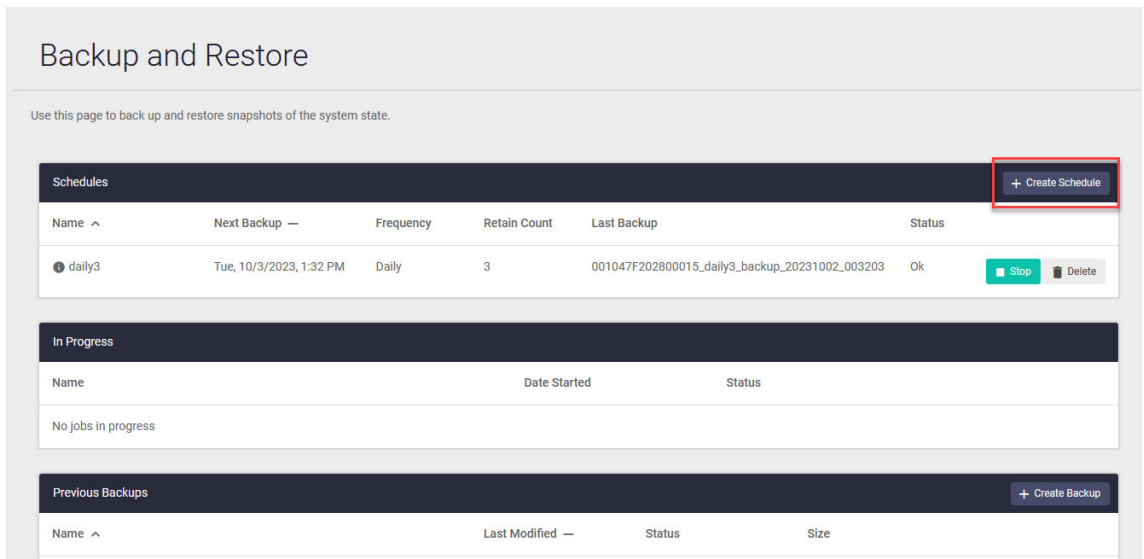
Step 2: Go to the Backup and Restore page.

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



Step 3: Open the Schedule dialog box.

Click **+ Create Schedule** at the top right of the **Schedules** panel.



Step 4: Configure the backup schedule.

In the Schedule dialog box:

- Enter a name for the schedule (A).
- Set the external media to save the backup to (B).
- Choose whether to back up the configuration file for the device (C).

- Select the files to back up (D). By default, all files are included in the backup. For example, for the 10GbE UTM Firewall, include the application file vfw-x86-x.x.x.app file. For the Vista Manager, include all the application files you are using.
- By default all application instances are included in the backup. Unselect any that you do not want to include (E). For example, to backup the main Firewall instance, make sure AT-vFW-app is included. If you have multiple firewall instances configured, include each of them.
- Set the start date and time for the first scheduled backup (F).
- Set the backup frequency (G).
- Enter the number of backup files to retain (H). Older backup files will be deleted to make space for newer ones.

Schedule
✕

Name
weekly-2 A

Select backup location B /mnt/media0 (132.8GB free) ▼

Back up configuration file? C No Yes

Files to back up D vfw-x86_... .app
vfw-x86_... .app ▼

Application instances to back up E AT-vFW-app
vfw1
vfw2 ▼

Start Date F 5/10/2023, 10:30:00 PM ▼

Backup frequency G Weekly ▼

Retain Count
3| H

Estimated free space required in backup location I 2.3GB

Cancel
Schedule

Step 5: Check free space on the external media.

As you configure the scheduled backups, the estimated free space required in the backup location displays at the bottom (I). Make sure you have enough free space on the external media (B).

Step 6: Confirm the schedule.

Click Schedule (J).

Note that backing up may take several minutes to a few hours, depending on how much data is backed up. When there is a backup in progress, you can see it in the **In Progress** panel. Once the backup is complete, see it in the **Previous Backups** panel.

Create a single backup now

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.

To create a schedule:

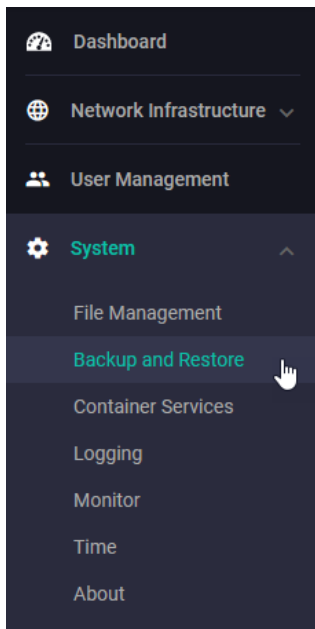
Step 1: Connect external media

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

The external media must have space for the new backup file and support sufficiently large file sizes (e.g. file system format ext4).

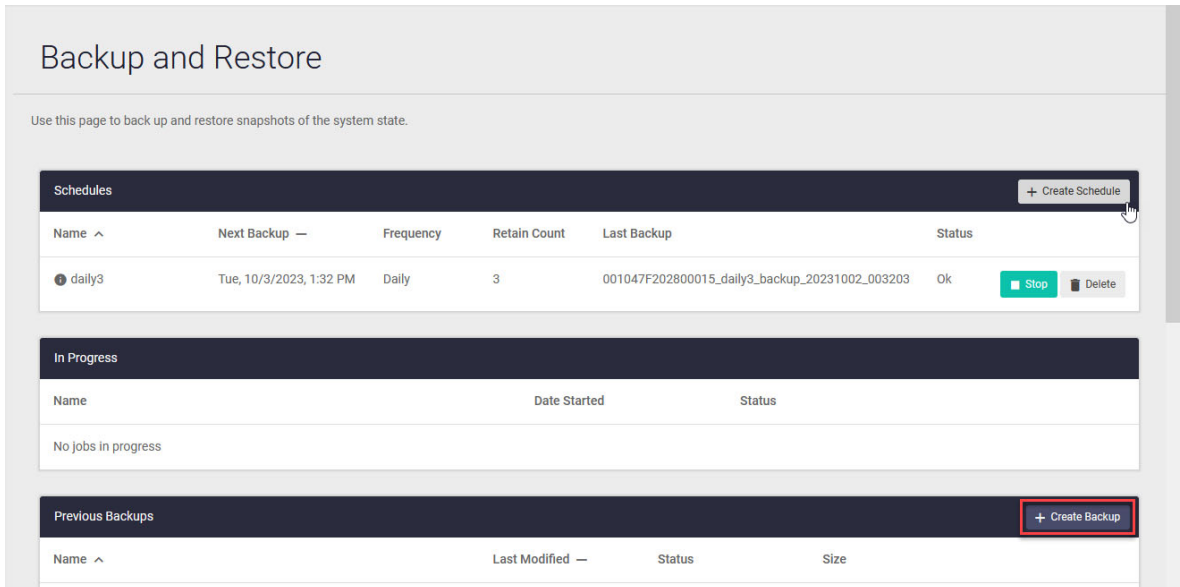
Step 2: Go to the Backup and Restore page.

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



Step 3: Open the Backup dialog box.

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



The **Backup** dialog box that opens shows 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.

Step 4: Configure the backup details.

In the **Backup** dialog box, select the external media for the backup location (A).

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 **System > File Management** in the VST-APL GUI.

Backup ✕

Select backup location
/mnt/media1
⌵

Back up configuration file?
No
Yes

Files to back up

sesc-x86_64-
vista-x86_64-

⌵

Application instances to back up

AMF-Sec-app
AT-AMF-app
AT-AWC-app
AT-FULLSNMP-app
AT-SNMP-app
AT-Vista-app

⌵

AMF-Sec-app

AT-AMF-app

AT-AWC-app

AT-FULLSNMP-app

AT-SNMP-app

Estimated free space required in backup location
18.5GB

Cancel
Back Up Now

Set the contents of the backup:

- Choose whether to back up the configuration file for the device (B).
- The default settings back up all application files stored in the device's file system. Unselect any files not to include (C).

For example, for the 10GbE UTM Firewall, include the application image vfw-x86-x.x.x.app.

For Vista Manager, include vista-x86_64-x.x.x.app and other application files being used on the appliance. (It does not backup application bundle files.)

By default, it is set to back up all application instances on the device that are running or stopped. Unselect any instances that you don't want it to back up (D).

For example, to backup the main firewall instance, make sure AT-vFW-app is included. If you have multiple firewall instances configured, include each of them.

For Vista Manager, include all the application instances being used on the appliance, such as AT-Vista-app and others.

The appliance shows the free space it estimates is required for the backup (E). Make sure there is enough free space on the external media (A).

Step 5: Start the backup.

Click **Back Up Now** (F). The current back-up shows in the **In Progress** panel. Backing up may take several minutes to a few hours, depending on how much data is backed up. Once the backup is complete, see it in the **Previous Backups** panel.

In Progress		
Name	Date Started	Status
A1C..._backup_20220113_011350	13/01/2022, 2:20:09 pm	Backup in progress

Monitor backups and schedules

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

Backup and Restore

Use this page to back up and restore snapshots of the system state.

Schedules + Create Schedule

Name ^	Next Backup --	Frequency	Retain Count	Last Backup	Status	
Monthly-A	Thu, 7/6/2023, 7:30 PM	Monthly	3		Ok	■ Stop 🗑 Delete

In Progress



Name	Date Started	Status
No jobs in progress		

Previous Backups + Create Backup


Name ^	Last Modified --	Status	Size	
00104..._weekly-2_backup_20230510_...	5/10/2023, 10:30:24 PM	Valid	444.8MB	🔄 Restore 🗑 Delete
00104..._weekly-1_backup_20230514_...	5/14/2023, 10:59:46 PM	Valid	1.5GB	🔄 Restore 🗑 Delete
00104..._weekly-1_backup_20230507_...	5/7/2023, 10:59:43 PM	Valid	1.5GB	🔄 Restore 🗑 Delete
00109..._backup_20230327_021722	3/28/2023, 4:30:39 AM	Device Mismatch	2.6GB	🗑 Delete

In the **Schedules** panel, you can see an overview of all the backup schedules configured on the device.












- You can **Stop** or **Start** a backup schedule or **Delete** it. To change a configured schedule, create a new schedule and delete the one it replaces.
- To see the details of one schedule, hover over the “i” icon to its left. This shows the name, location and contents for the backup schedule.

weekly-2	
Schedule Name	weekly-2
Location	/mnt/media0
Files	default.cfg vfw-x86_64-  .app vfw-x86_64-  .app AT-vFW-app vfw1 vfw2

In the **In Progress** panel, you can see any backup or restore process on the appliance now.

In Progress		
Name	Date Started	Status
A1C  _backup_20220113_011350	13/01/2022, 2:20:09 pm	Backup in progress

In the **Previous Backups** panel, you can see information about the backup files stored on the external media.

Previous Backups				+ Create Backup
Name ^	Last Modified —	Status	Size	
00104  _weekly-2_backup_20230510_...	5/10/2023, 10:30:24 PM	Valid	444.8MB	 Restore  Delete
00104  _weekly-1_backup_20230514_...	5/14/2023, 10:59:46 PM	Valid	1.5GB	 Restore  Delete
00104  _weekly-1_backup_20230507_...	5/7/2023, 10:59:43 PM	Valid	1.5GB	 Restore  Delete
00109  _backup_20230327_021722	3/28/2023, 4:30:39 AM	Device Mismatch	2.6GB	 Delete

- The filename are based on the device serial number, the backup name (if scheduled) and the time of backup.

- A status of **Valid** confirms that the backup has a valid checksum and that it can be used to restore the current device. Status **Invalid checksum** shows the backup failed or was corrupted. Status **Device Mismatch** means that the backup has been created on a different device model (different boardname). It cannot be used to restore this device.
- To see the files contained in a backup, hover over the instance icon “i” to its left. This shows the name, location and contents for the backup.

001047F202[redacted]_weekly-2_backup_20230510_103011	
Backup Name	001047F202[redacted]_weekly-2_backup_20230510_103011
Location	/mnt/media0 /00104[redacted]00015_weekly-2_backup_20230510_103011.abk
Date Created	5/10/2023, 10:30:11 PM
Board Name	AT-[redacted]-APL-[redacted]
Files	default.cfg vfw-x86_64-[redacted]-0.1.app vfw-x86_64-[redacted]-0.2.app AT-vFW-app vfw1 vfw2

Manually restore the whole appliance from a backup

Use this procedure to restore an existing VST-APL appliance to a previous state that you have a backup for.

If instead, you want:

- to restore one or more application instances on the appliance and leave other configuration and instances unchanged, use the procedure in "[Restore a single application instance on the appliance from a back-up](#)" on page 69.
- to replace an appliance with a factory-new appliance that has no new configuration saved, use the procedure in "[Automatically restore the whole appliance from a backup onto new appliance hardware](#)" on page 73.

Step 1: Access the VST-APL GUI. For a new device, see "[Connect to the web-based Device GUI](#)" on page 8 or the [Installation Guide for your appliance](#).

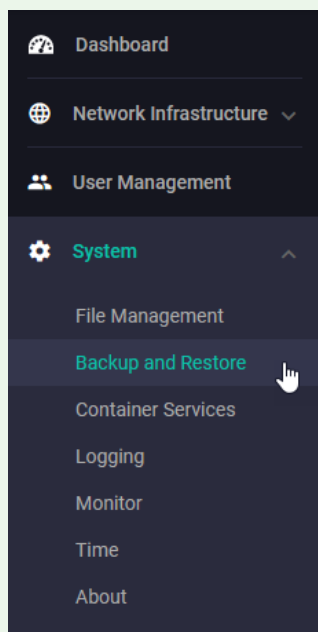
Step 2: Connect the external media containing the backup file.

Step 3: Stop all running application instances.

To do this, in the VST-APL menu, navigate to **System > Container Services**, and click **Stop** for each instance that is running.

Step 4: Open the Backup and Restore page.

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



Step 5: Select the backup to restore from.

In the **Previous Backups** panel, select the backup to restore from.

Previous Backups + Create Backup				
Name ^	Last Modified --	Status	Size	
B 00104 [redacted]_weekly-2_backup_20230510_...	5/10/2023, 10:30:24 PM	A Valid	444.8MB	C Restore Delete
00104 [redacted]_weekly-1_backup_20230514_...	5/14/2023, 10:59:46 PM	Valid	1.5GB	Restore Delete
00104 [redacted]_weekly-1_backup_20230507_...	5/7/2023, 10:59:43 PM	Valid	1.5GB	Restore Delete
00109 [redacted]_backup_20230327_021722	3/28/2023, 4:30:39 AM	Device Mismatch	2.6GB	Delete

- Check that the **Status** for the backup is **Valid** (A). This confirms that the backup has a valid checksum and that it was created on the same model of appliance—it has the same board name.
- Check that the backup has all the components you will need. To see the contents of a previous back-up, hover over the instance icon “i” to its left (B). A pop-up window displays the contents of the backup.

001047F202[redacted]_weekly-2_backup_20230510_103011	
Backup Name	001047F202[redacted]_weekly-2_backup_20230510_103011
Location	/mnt/media0 /00104[redacted]00015_weekly-2_backup_20230510_103011.abk
Date Created	5/10/2023, 10:30:11 PM
Board Name	AT-[redacted]-APL-[redacted]
Files	default.cfg vfw-x86_64-[redacted]-0.1.app vfw-x86_64-[redacted]-0.2.app AT-vFW-app vfw1 vfw2

Click the **Restore** button at the right of the backup (C).

Step 6: Configure what to restore.

In **Restore** dialog box:

- Set **Restore device configuration?** to **Yes** to restore the VST-APL configuration file, default.cfg (A).
- By default, all the application images in the back-up file are set to be restored. You can deselect any you don't need on the device at **Files to restore** (B).
- By default, all the application images in the back-up file are set to be restored. You can deselect any you don't need on the device at **Application instances to restore** (C).

Restore		✕
Backup to restore		
A10358F202900001_backup_20220113_011826 A		
Restore device configuration?	No Yes	
Files to restore	B vista-x86_64-3.8.0.app	▼
Application instances to restore	C AT-Vista-app	▼
Estimated flash space required	D 401.4MB	
Estimated storage space required	E 200GB	
		F Cancel Restore

Step 7: Check memory and storage available.

Check that the **estimated flash space required** (D) and the **estimated storage space required** (E) are available on the appliance. You can see the memory and storage available on the appliance in the VST-APL GUI Dashboard.

To free flash memory, in the VST-APL menu, navigate to **System > File Management**. Click **Delete** next to files you no longer need.

To free storage space, navigate to **System > Container Services**. Click **Destroy** next to instances you no longer need, such as the old instances that will be restored from the backup. You must stop an instance before you can destroy it.

Step 8: Begin restore.

To begin the restore job, click **Restore** (F) at the bottom of the Restore dialog box. See the current restore process in the **In Progress** panel in the Backup and Restore page. Restoring may take several minutes to a few hours, depending on how much data is being restored.

In Progress		
Name	Date Started	Status
A10359F202900001_backup_20220113_011826	13/01/2022, 2:29:30 pm	Restore in progress. Please do not reboot or power off the device.

If there is not enough space for the restored files and instances, the **Status** in the **In Progress** panel will show that the restore has failed. Free up flash and storage space—see the previous step.

Caution: You **must** restart the appliance before you save the restored appliance configuration, as in the next step. Do **not** save the appliance configuration before the next step.

Step 9: Restart the appliance.

To put the changes into effect, you need to restart the appliance. When the restore process is complete, click OK. In the VST-APL menu, navigate to **System > File Management**, and click **Reboot**. When the appliance restarts, it will use the restored configuration file to restore the state of application instances.

Step 10: Save the VST-APL configuration.

Clicking the **Save** button at the top of the VST-APL page.

Step 11: Schedule backups.

We recommend you schedule future backups if they are not already part of the configuration.

Restore a single application instance on the appliance from a back-up

Use this procedure to restore one or more individual application instances on a VST-APL appliance from a backup. This leaves the appliance configuration and other applications instances on the appliance as they were.

Caution: Make sure you follow this procedure carefully. This will replace only the required application. Failing to follow this procedure can result in permanently losing appliance configuration and data for other applications.

If instead, you want:

- to restore everything on the appliance, see "[Manually restore the whole appliance from a backup](#)" on page 65.
- to replace an appliance with a factory-new appliance that has no new configuration saved, use the procedure in "[Automatically restore the whole appliance from a backup onto new appliance hardware](#)" on page 73.

Step 1: Access the VST-APL GUI.

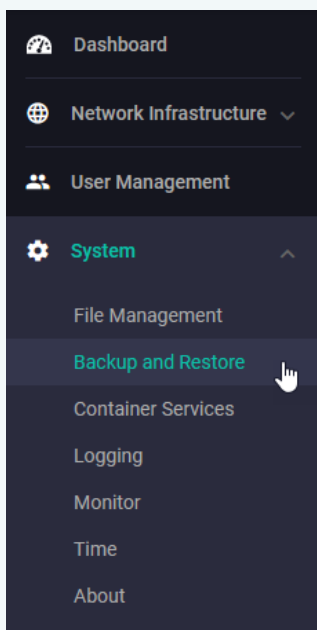
Step 2: Connect the external media containing the backup file.

Step 3: Stop the application instance.

If the application you are going to restore is running, stop it. To do this, in the VST-APL menu, navigate to **System > Container Services**, and click **Stop**.

Step 4: Open the Backup and Restore page.

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



Step 5: Select the backup to restore from.

The **Previous Backups** panel in the Backup and Restore page shows the backups available on the external media.

Previous Backups + Create Backup				
Name ^	Last Modified --	Status	Size	
B 00104 [redacted]_weekly-2_backup_20230510_...	5/10/2023, 10:30:24 PM	A Valid	444.8MB	C Restore Delete
00104 [redacted]_weekly-1_backup_20230514_...	5/14/2023, 10:59:46 PM	Valid	1.5GB	Restore Delete
00104 [redacted]_weekly-1_backup_20230507_...	5/7/2023, 10:59:43 PM	Valid	1.5GB	Restore Delete
00109 [redacted]_backup_20230327_021722	3/28/2023, 4:30:39 AM	Device Mismatch	2.6GB	Delete

Check that the backup you choose:

- has Status **Valid (A)**—this means it has a valid checksum and was created on an appliance with the same board name.
- contains a backup of the application image and instance that you want to restore. Hover over the instance icon “i” to the left of a backup to see details of which files and instances the backup contains (B).

001047F202[redacted]_weekly-2_backup_20230510_103011	
Backup Name	001047F202[redacted]_5_weekly-2_backup_20230510_103011
Location	/mnt/media0 /00104 [redacted]00015_weekly-2_backup_20230510_103011.abk
Date Created	5/10/2023, 10:30:11 PM
Board Name	AT-[redacted]-APL-[redacted]
Files	default.cfg vfw-x86_64-[redacted]-0.1.app vfw-x86_64-[redacted]-0.2.app AT-vFW-app vfw1 vfw2

Click **Restore** at the right of the backup (C). The **Restore** dialog box opens.

Step 6: Set the application to restore.

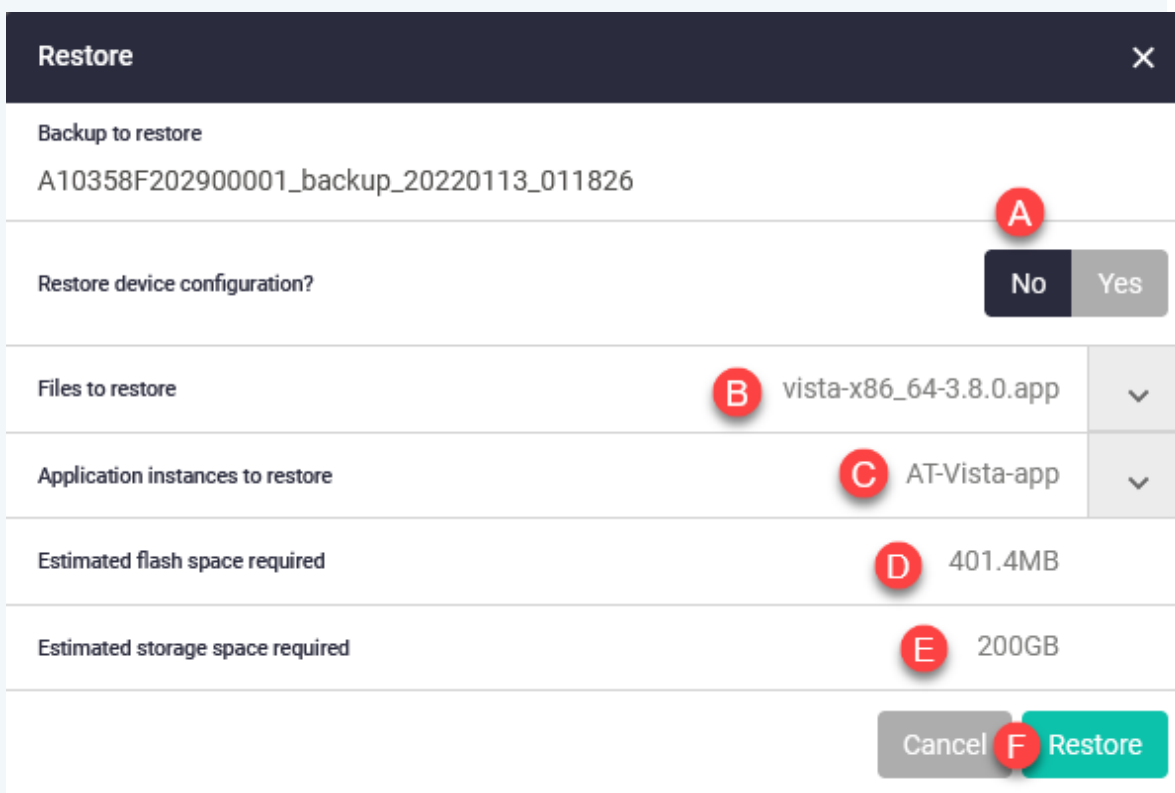
In the **Restore** dialog box, set the details of which application file and instance to restore.

By default, all the items in the back-up file are set to be restored. To make sure only the required application instance is restored from the backup, and the appliance configuration and other application instances are retained on the appliance:

- Set **Restore device configuration** to **No** (A).

Caution: It is important to set this to **No**. Otherwise the appliance configuration and application data for other application instances may be permanently lost from the appliance.

- At **Files to restore**, make sure the application file you want to restore remains selected (B). Unselect any others.
- At **Application instances to restore**, make sure the application instance you want to restore remains selected (C). Unselect any others.



Step 7: Check memory and storage available.

Check that the **estimated flash space required** (D) and the **estimated storage space required** (E) are available on the appliance. You can see the memory and storage available on the appliance in the VST-APL GUI Dashboard.

To free flash memory, in the VST-APL menu, navigate to **System > File Management**. Click **Delete** next to files you no longer need. To free storage space, navigate to **System > Container Services**. Click **Destroy** next to instances you no longer need, such as the old instance that will be restored from the backup. You must stop an instance before you can destroy it.

Step 8: Begin restore.

Click **Restore** (F) at the bottom right of the Restore dialog box. Click **OK** in the pop-up box.

In Progress		
Name	Date Started	Status
A10358F202900001_backup_20220113_011826	13/01/2022, 2:29:30 pm	Restore in progress. Please do not reboot or power off the device.

The restore shows in the **In Progress** panel in the Backup and Restore page. Restoring may take several minutes or longer, depending on the amount of data being restored for the application.

In Progress		
Name	Date Started	Status
A10358F202900001_backup_20220113_011826	13/01/2022, 2:29:30 pm	Restore in progress. Please do not reboot or power off the device.

If there is not enough space for the restored file and instance, the **Status** in the **In Progress** panel will show that the restore has failed. Free up flash and storage space—see the previous step—and retry.

Step 9: Start the application.

After restoring the application instance, it will be in a stopped state. In the VST-APL menu, navigate to **System > Container Services**. Click **Start** next to the instance.

Step 10: Save the appliance configuration.

Click the **Save** button at the top of the VST-APL page.

Step 11: Schedule future backups.

We recommend you schedule future backups if they are not already part of the configuration.

Automatically restore the whole appliance from a backup onto new appliance hardware

Use this procedure if you need to take an appliance out of the network and replace it with a factory new appliance. You can use this to restore a 10GbE UTM Firewall or a Vista Manager Network Appliance from a backup of the previous appliance.

If instead, you want:

- to restore all configuration, application files and instances on an appliance that has previously been configured, see ["Manually restore the whole appliance from a backup" on page 65](#).
- to restore one or more application instances on the appliance and leave other configuration and instances unchanged, use the procedure in ["Restore a single application instance on the appliance from a back-up" on page 69](#).

For this procedure, you need:

- a recent valid backup for the previous appliance on external media. The automatic restore process will find and use the most recent backup on the external media that is valid for the new appliance. Make sure the most recent valid backup on the media is the one you want.
- a factory new or unconfigured replacement appliance. It is important that no new VST-APL configuration has been saved on the new appliance.
- The new appliance must be the same model (that is, with the same board name) as the one being replaced, that is, the one from which the backup was created.

To automatically restore a new appliance with a backup, follow these steps:

Step 1: Physically install the new appliance.

Follow the instructions in the VST-APL Installation Guide to place the appliance in same location as the one it replaces. Do **not** save any configuration you use to connect a console. Do **not** connect the appliance to the rest of the network until after the backup has been restored.

Step 2: Insert the backup media.

Insert the external media that contains the appliance backup.

Step 3: Power on or reboot the appliance.

The appliance automatically searches the external media for the latest valid backup. Then it restores the appliance configuration (default.cfg), the application files, and the application instances from the backup onto the new appliance. Restoring may take several minutes to a few hours, depending on how much data is being restored.

While it is being restored, the appliance will send messages to the console. When the appliance has finished uploading the backup files, it will automatically restart. This puts into effect the configuration in the restored default.cfg file. This will end the connection to the console.

Step 4: Connect the ports

Connect the ports on the new appliance to the network in the same way as the old appliance.

Step 5: Log into the appliance.

Connect to the VST-APL GUI from your browser using the appliance IP address, user name and password in the restored configuration, as for the appliance it replaces.

Step 6: For a 10GbE UTM Firewall, remove the Vista Manager application files.

For a 10GbE UTM Firewall only, keep these files in the appliance memory (if present):

- vFW-x86_64-x.x.x-x.x.app—the Firewall application image file
- ATVSTAPL-x.x.x.iso —the VST-APL operating system file

Remove the Vista Manager application files.

In the VST-APL GUI, navigate to **System > File Management**. Select the files to delete and click the **Delete** button. Delete each of these application images, if present:

- vista-x86_64-x.x.x.app
- AMF-x86_64-x.x.x-x.x.app
- awc-x86_64-3.10.0.app
- sesc-x86_64-x.x.x.app
- fullsnmp-x86_64-x.x.x.app
- snmp-x86_64-x.x.x.app
- radgate-x86_64-1x.x.x.app
- VST-APL-x.x.x.bundle (if present)

Step 7: Schedule future backups.

We recommend you schedule future backups if they are not already part of the configuration.

Upgrading VST-APL software

To upgrade the VST-APL operating system and applications to use for Vista Manager or as a 10GbE UTM Firewall, see the [Vista Manager Network Appliance \(VST-APL\) Release Notes](#) for the version that you need to upgrade to.

C613-04099-00 REV N



NETWORK SMARTER

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

© 2025 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.