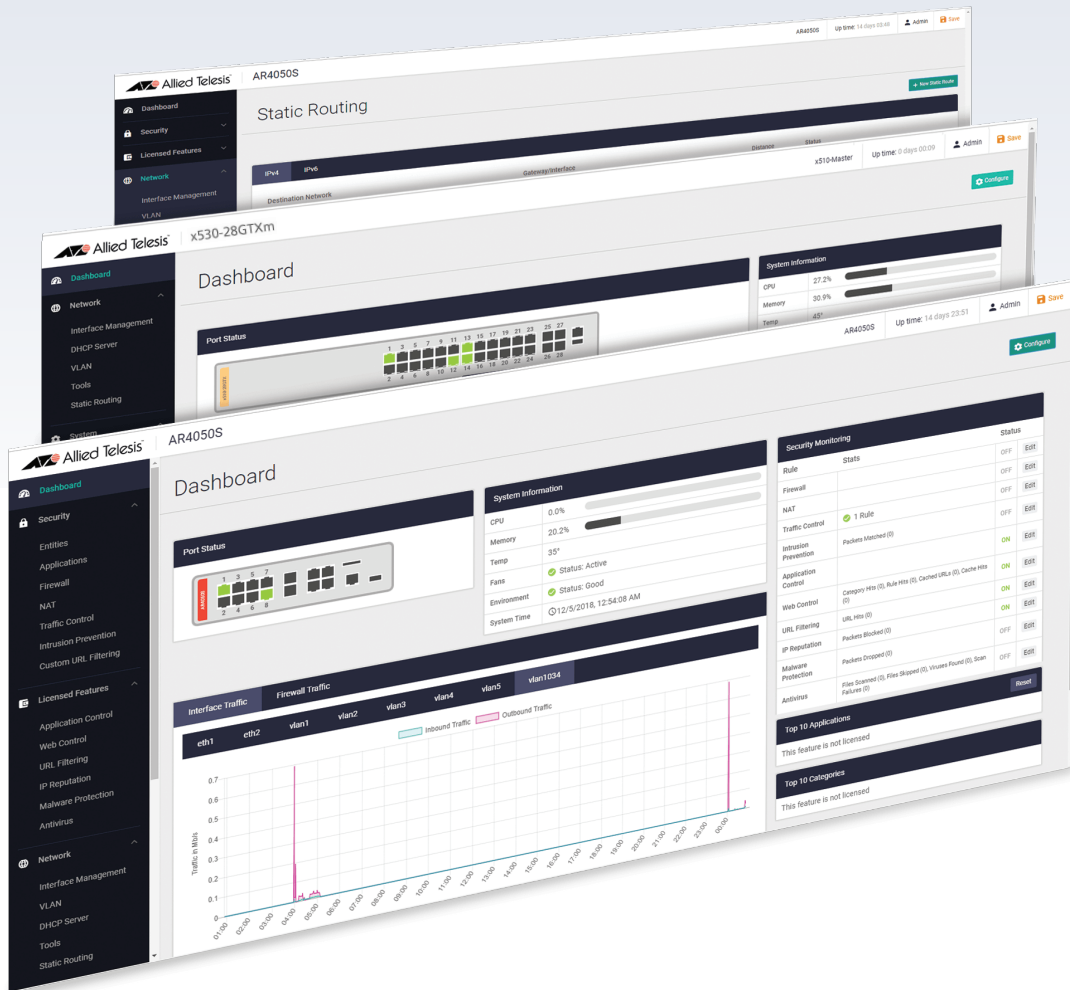


Release Note for Web-based Device GUI Version 2.11.x



» 2.11.0

AlliedWare Plus
OPERATING SYSTEM

Acknowledgments

©2022 Allied Telesis Inc. All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

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

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

Getting the most from this Release Note

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

Contents

What's New in Version 2.11.0	1
Introduction	1
New Features and Enhancements	3
Support for Native VLANs	3
Specify Fully Qualified Domain Names on Host Entities	4
Edit DHCP server pools	5
Set the GUI timeout period	5
Better display of license duration	6
Vista Manager mini: Cable-free extension of wireless networks with TQ6602 Access Points	6
Vista Manager mini: Support for TQ6602 GEN2 and TQm6602 GEN2 APs	7
Vista Manager mini: Allow guests to access only parts of your network in all Captive Portal modes.....	7
Vista Manager mini: Tech support files available for access points	9
Vista Manager mini: Enhancements to Passpoint (Hotspot 2.0)	10
Accessing and Updating the Web-based GUI.....	11

What's New in Version 2.11.0

Product families supported by this version:

AMF Cloud	XS900MX Series
SwitchBlade x8100: SBx81CFC960	GS980MX Series
SwitchBlade x908 Generation 2	GS980EM Series
x950 Series	GS980M Series
x930 Series	GS970EMX/10
x550 Series	GS970M Series
x530 Series	10G Virtual UTM Firewall
x530L Series	AR4050S
x330-10GTX	AR3050S
x320 Series	AR2050V
x230 Series	AR2010V
x220 Series	AR1050V
IE340 Series	
IE210L Series	

Introduction

This release note describes the new features in the Allied Telesis Web-based Device GUI version 2.11.0. You can run 2.11.0 with AlliedWare Plus firmware versions 5.5.0-x.x, 5.5.1-x.x, or 5.5.2-x.x, on your device, although the latest GUI features may only be supported with the latest firmware version.

For information on accessing and updating the Device GUI, see [“Accessing and Updating the Web-based GUI” on page 11](#).

The following table lists model names that support this version:

Table 1: Models and software file names

Models	Family
AMF Cloud	
SBx81CFC960	SBx8100
SBx908 GEN2	SBx908 GEN2
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930
x550-18SXQ x550-18XTQ x550-18XSPQm	x550

Table 1: Models and software file names (cont.)

Models	Family
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L
x330-10GTX	x330
x320-10GH x320-11GPT	x320
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L
x220-28GS x220-52GT x220-52GP	x220
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340
IE210L-10GP IE210L-18GP	IE210L
XS916MXT XS916MXS	XS900MX
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX
GS980EM/10H GS980EM/11PT	GS980EM
GS980M/52 GS980M/52PS	GS980M
GS970EMX/10	GS970EMX
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M
10G Virtual UTM Firewall	
AR4050S AR3050S	AR-series UTM firewalls
AR2050V AR2010V AR1050 V	AR-series VPN routers

New Features and Enhancements

This section summarizes the new features in the Device GUI software version 2.11.0.

Support for Native VLANs

Applies to devices running AlliedWare Plus 5.5.2-0.1 onwards.

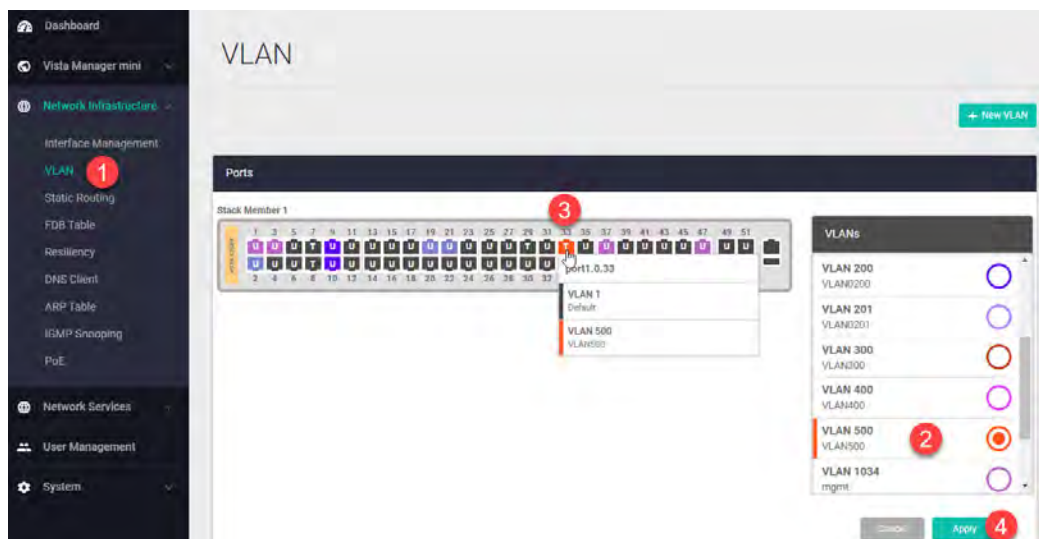
From Device GUI version 2.11.0 onwards, you can use the VLAN map to assign native VLANs to switchports.

Once a port has a native VLAN, any packets received on the switchport without a VLAN tag are placed into the native VLAN. Packets leaving a switchport on the native VLAN will not be tagged.

Different native VLANs can be assigned to different switchports on a single device. Only one native VLAN can exist per switchport.

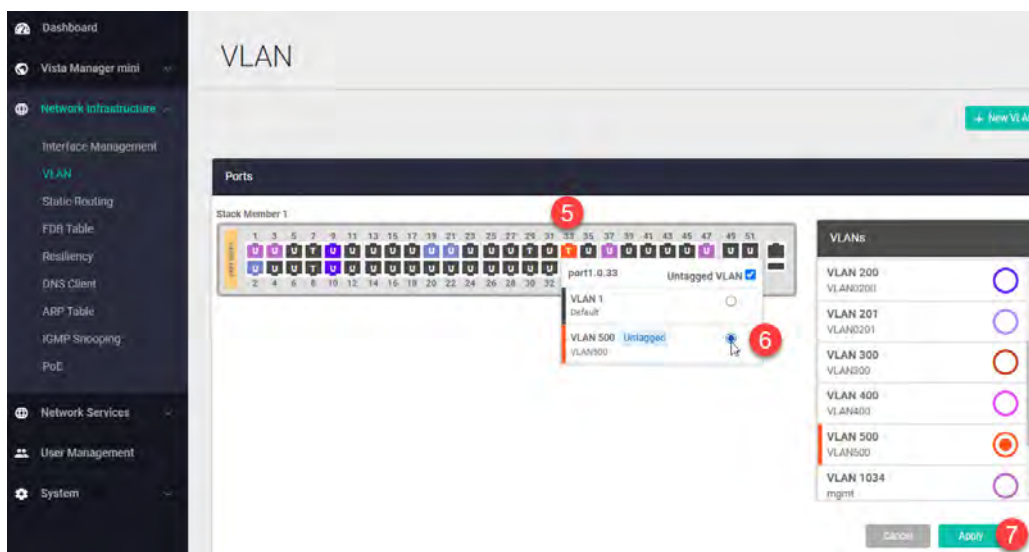
Native VLANs only apply to switchports in trunk mode, so the following procedure first uses the VLAN map to put the switchport into trunk mode, then sets the correct native VLAN:

1. Select **Network Infrastructure** > **VLAN** to open the **VLAN** page.
2. If the VLAN you want to add as a native VLAN doesn't exist, click **New VLAN** to create it. Otherwise, select the VLAN in the VLANs list.
3. Click on the **U** on the switchport until it takes on the color of your selected VLAN and changes to a **T** (for Trunk).
4. Click **Apply** to set the port mode to Trunk.



5. Hover over the switchport. A pop-up will appear, showing the current native VLAN (probably VLAN1) and the VLAN you want to add as native VLAN.
6. In the pop-up, select the VLAN that you want to make the native VLAN.

7. Click **Apply** again.

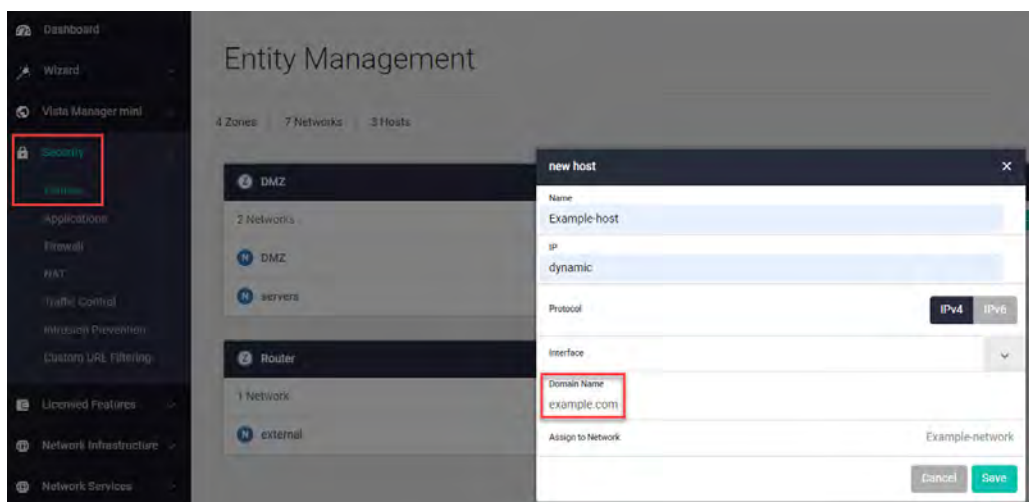


Specify Fully Qualified Domain Names on Host Entities

Applies to AR-series devices running AlliedWare Plus 5.5.2-0.1 onwards.

From version 2.11.0 onwards, you can specify one or more Fully Qualified Domain Names (FQDN) on host entities. This means you can use FQDN lookup for host entities. FQDN lookup makes it possible to match web traffic destined to a web server or cloud-based service, when the service's IP address is not fixed. Then you can create firewall rules to match that web traffic.

To specify the FQDNs, enter them in the new **Domain Name** field when creating or editing a host, in the **Security > Entities** section of the GUI. For example:



You can configure multiple FQDNs for a host, using a comma separated list. This results in multiple addresses for the host.

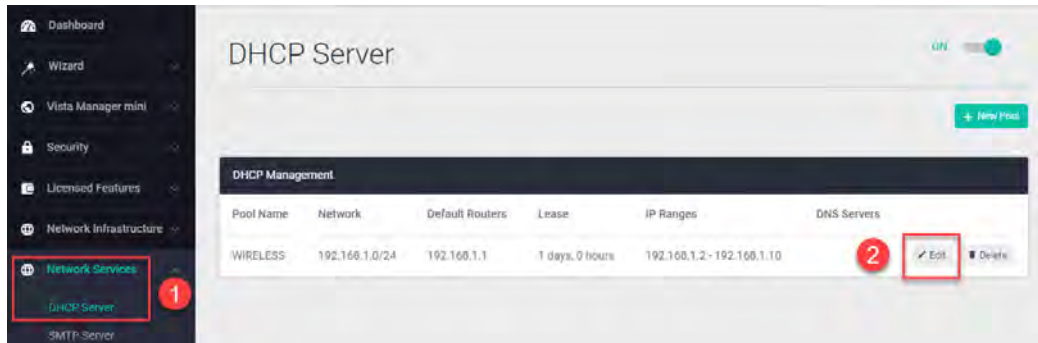
You can also configure the Interface as well as configuring FQDNs. This also results in multiple addresses for the host.

For more information about using FQDN lookup, including limitations on its use, see the [Application Awareness Feature Overview and Configuration Guide](#).

Edit DHCP server pools

Applies to devices running AlliedWare Plus 5.5.2-0.1 onwards.

From version 2.11.0 onwards, you can edit DHCP server pools. To do this, use the new **Edit** button on the **DHCP Server** page of the GUI:



Set the GUI timeout period

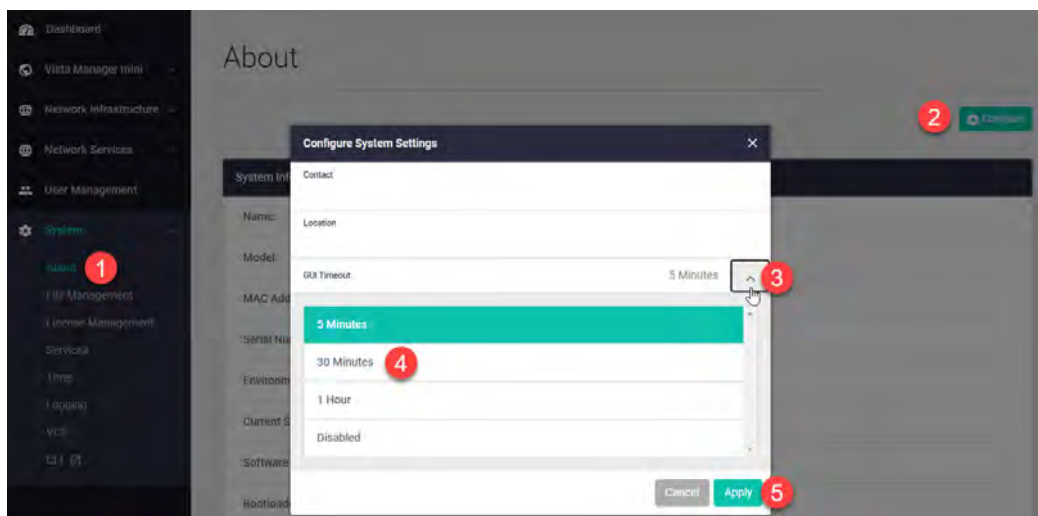
Applies to devices running AlliedWare Plus 5.5.2-0.1 onwards.

From version 2.11.0 onwards, you can set a timeout period for the GUI. The default setting is 5 minutes, meaning that after 5 minutes idle time, the GUI will log you out.

Also, some pages previously did not time out, such as the Interfaces page. These pages now time out too.

To change the timeout period:

1. Select **System** > **About** to open the **About** page.
2. Click the **Configure** button. The **Configure System Settings** dialog opens.
3. Click the arrow beside the current **GUI Timeout** value.
4. Select the new timeout value.
5. Click **Apply**.

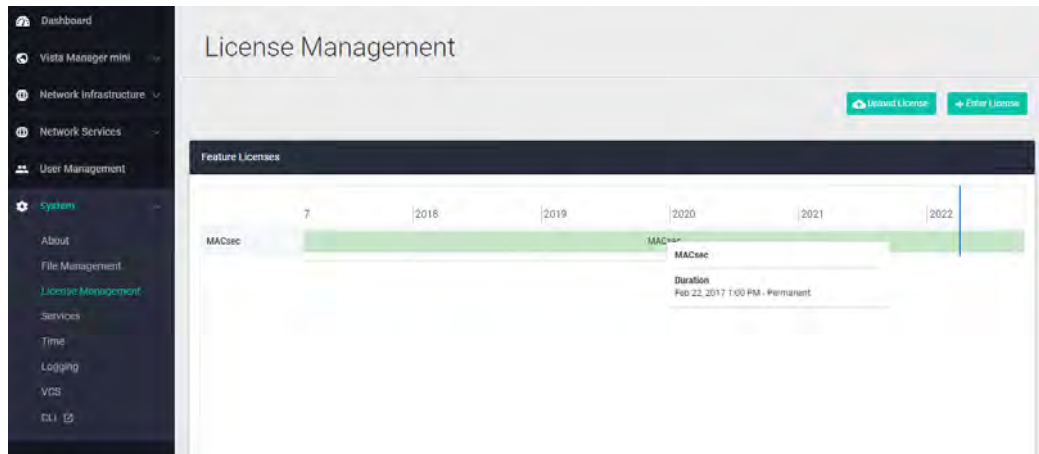


Better display of license duration

Applies to devices running AlliedWare Plus 5.5.2-0.1 onwards.

Version 2.11.0 has improved the graph on the GUI that displays information about licenses and the time until they expire. The graph is now the same as Vista Manager EX's graph.

To see the new graph, use the **System > License Management** page:



You can see details of a license by hovering over its green bar.

Vista Manager mini: Cable-free extension of wireless networks with TQ6602 Access Points

Applies to devices running AlliedWare Plus 5.5.2-0.1 onwards and TQ6602 APs running 7.0.2-0.1 onwards.

From version 2.11.0 onwards, the wireless controller in Vista Manager mini enables you to configure Autonomous Wave Control Smart Connect (AWC-SC) on TQ6602 APs. AWC-SC saves installation time and expense when adding new APs to a wireless network by removing the need to cable new APs into the network. This is particularly convenient for temporary and outdoors installations.

For more information about Smart Connect and how to configure it, see the [User Guide for Wireless management \(AWC\) with Vista Manager Mini](#).

Vista Manager mini: Support for TQ6602 GEN2 and TQm6602 GEN2 APs

Applies to AlliedWare Plus devices that support Vista Manager mini, running 5.5.2-0.1 onwards. APs must be running 8.0.1.-1.1 onwards.

From version 2.11.0 onwards, you can use the AWC Wireless Manager to manage the following additional APs in Vista Manager mini:

- TQ6602 GEN2
- TQm6602 GEN2

For these APs, note that Channel Blanket, Smart Connect and Passpoint support on Vista Manager mini will be available with a later AlliedWare Plus version.

For more information about Vista Manager mini, see the [Wireless Management \(AWC\) with Vista Manager mini User Guide](#).

Vista Manager mini: Allow guests to access only parts of your network in all Captive Portal modes

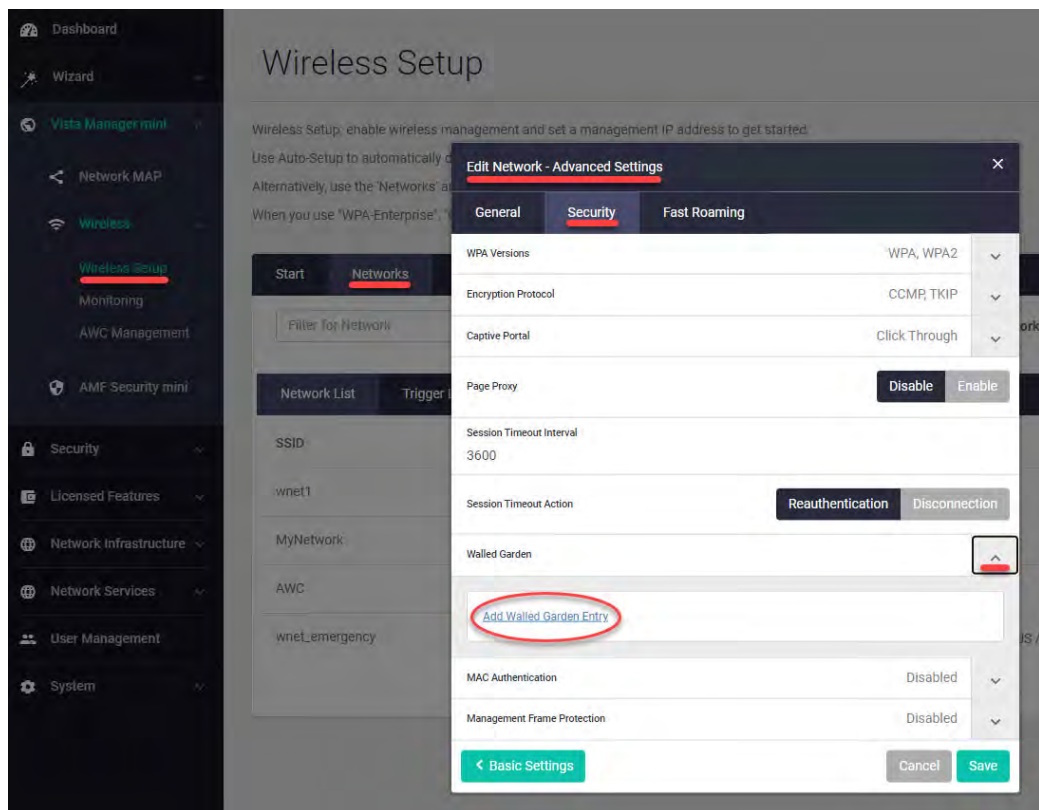
Applies to AlliedWare Plus devices that support Vista Manager mini, running 5.5.0-1.3 onwards. APs must be running:

Model	Firmware version
TQ6602 GEN2, TQm6602 GEN2	8.0.1-1.1 or later
TQ6602	7.0.1-2.1 or later
TQ5403, TQm5403, TQ5403e, TQ1402, TQm1402	6.0.1-4.1 or later

From version 2.11.0 onwards, you can use Captive Portal in the AWC Wireless Manager to allow guests to access only parts of your network in all Captive Portal modes. This is done using the Captive Portal feature called "walled garden". Previously, a walled garden was only available in the External Page Redirect mode of Captive Portal.

A walled garden limits users to accessing only a selection of web pages. A common example could be a hotel environment where unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents.

To configure a walled garden, use the AP Network's **Security** page:



1. Select **Wireless > Wireless Setup > Networks**.
2. Either create a new network by clicking + **Add Network** or edit an existing network.
3. Click **Advanced Settings**.
4. Select the **Security** tab.
5. Select the Captive Portal type: **RADIUS Server**, **Click Through**, or **External Page Redirect**.
6. In the configuration page that opens, click on the arrow beside **Walled Garden**.
7. Click **Add Walled Garden Entry**.
8. A field appears for you to enter an IP address or FQDN that you want guests to access. Add the entry.
9. If necessary, click **Add Walled Garden Entry** again and add more entries.

For more information about Captive Portal, see the [Wireless Management \(AWC\) with Vista Manager mini User Guide](#).

Vista Manager mini: Tech support files available for access points

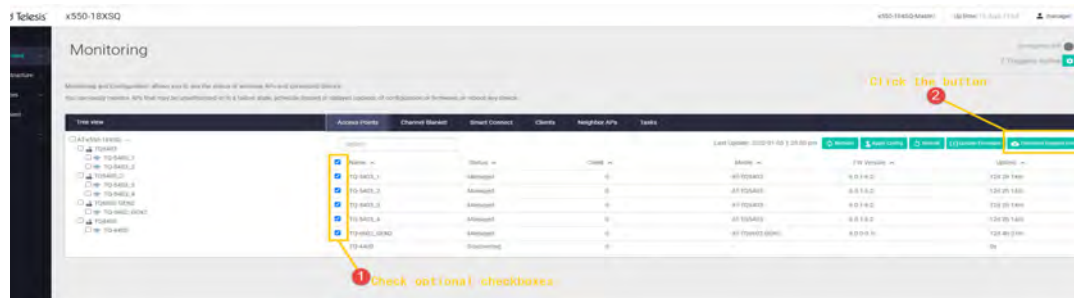
Applies to AlliedWare Plus devices that support Vista Manager mini, running 5.5.2-0.1 onwards. APs must be running:

Model	Firmware version
TQ6702 GEN2, TQm6702 GEN2	8.0.0-1.1 or later
TQ6602 GEN2, TQm6602 GEN2	8.0.1-1.1 or later
AT-TQ6602	7.0.1-2.1 or later
TQ5403 GEN2, TQm5403, TQ5403e, TQ1402, TQm1402	6.0.1-4.1 or later
TQ4600, TQ4400e	4.3.0 or later

From Device GUI 2.11.0 onwards, you can get a tech-support file via Vista Manager mini from a single managed AP or all of the APs that belong to an AWC-CB or AWC-SC group.

To access this feature, go to **Wireless > Monitoring**. Select either the Channel Blanket or Smart Connect tab. Then:

1. Select the AP or APs
2. Click **Technical Support Information**.



For more information on this feature and Vista Manager mini, see the [Wireless Management \(AWC\) with Vista Manager mini User Guide](#).

Vista Manager mini: Enhancements to Passpoint (Hotspot 2.0)

Applies to SBx908 GEN2, x950, x930, x550, x530, AR4050S, AR3050S, AR2050V, and AR2010V devices running AlliedWare Plus 5.5.2-0.1 onwards. For TQ5403, TQm5403, and TQ5403e access points running 6.0.1-5.1 or later.

Previously, TQ5403 series access points supported Hotspot 2.0 Release 1, which was based on the IEEE 802.11u standard. Release 2 (introduced in October 2014) included the standardization of credential management. The benefits of each release were:

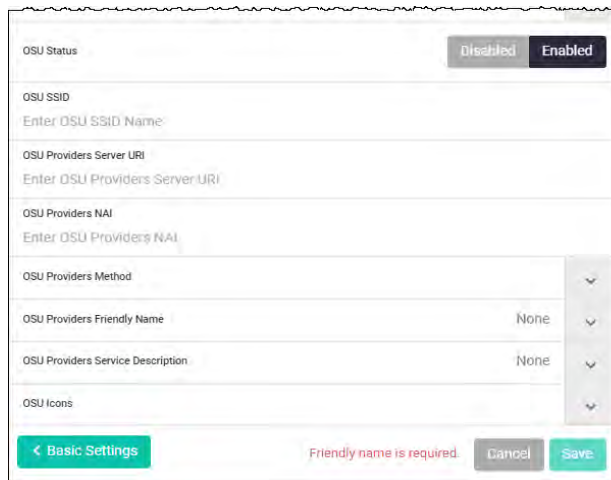
- Release 1 - effectively establishing the basic concepts of Hotspot 2.0, such as the ability to discover Passpoint enabled networks and select the optimal one.
- Release 2 - largely focused on standardizing the management of the credentials; how they are provisioned, stored on the device, used in network selection, and how long they are good for. The release incorporated an online sign-up (OSU) page to enable easy end-user device configuration provisioning.

From GUI version 2.11.0 onwards, you can use Passpoint OSU options to register a mobile device with a service provider and choose a plan to gain network access. When you sign up, your device will send you user credentials to connect to the network.

To configure OSU, go to **Wireless > Wireless Setup > Networks**

Then:

1. Network Basic Settings, select Security **WPA Enterprise**
2. Advanced Settings, **enable Passpoint**
3. The Passport tab, click **Options**
4. Passport Options, **enable OSU**
5. Complete the OSU configuration fields
6. Click **Save**



OSU Status: Disabled Enabled

OSU SSID
Enter OSU SSID Name:

OSU Providers Server URI
Enter OSU Providers Server URI:

OSU Providers NAI
Enter OSU Providers NAI:

OSU Providers Method

OSU Providers Friendly Name: None

OSU Providers Service Description: None

OSU Icons

< Basic Settings Friendly name is required. Cancel Save

For more information on this feature and Vista Manager mini, see the [Wireless Management \(AWC\) with Vista Manager mini User Guide](#).

Accessing and Updating the Web-based GUI

This section describes how to access the GUI, check the version, and update it.

Browse to the GUI

Perform the following steps to browse to the GUI.

1. If you haven't already, add an IP address to an interface. For example:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip address 192.168.1.1/24
```

Alternatively, on unconfigured devices you can use the default address, which is:

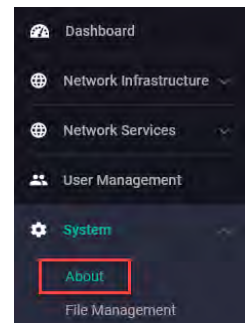
- « on switches: 169.254.42.42
- « on AR-Series: 192.168.1.1

2. Open a web browser and browse to the IP address from step 1.
3. The GUI starts up and displays a login screen. Log in with your username and password. The default username is *manager* and the default password is *friend*.

Check the GUI version

To see which version you have, open the System > About page in the GUI and check the field called **GUI version**.

If you have an earlier version than 2.11.0, update it as described in “Update the GUI on switches” on page 12 or “Update the GUI on AR-Series devices” on page 13.



Update the GUI on switches

Perform the following steps through the Device GUI and command-line interface if you have been running an earlier version of the GUI and need to update it.

1. Obtain the GUI file from our Software Download center. The filename for v2.11.0 of the GUI is `awplus-gui_552_26.gui`, `awplus-gui_551_26.gui` or `awplus-gui_550_26.gui`.

Make sure that the version string in the filename (e.g. 552) matches the version of AlliedWare Plus running on the switch. The file is not device-specific; the same file works on all devices.

2. Log into the GUI:

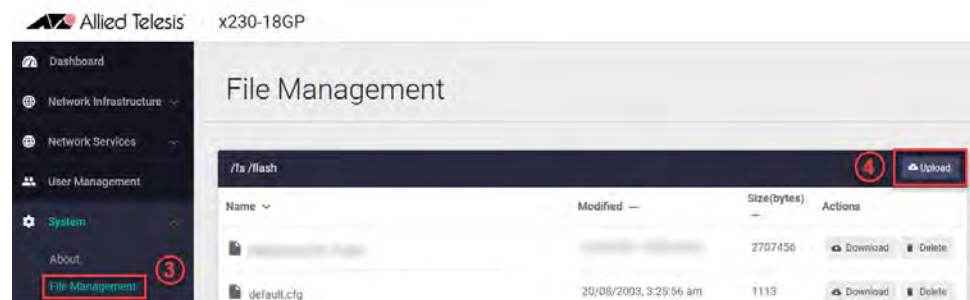
Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

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

The default username is *manager* and the default password is *friend*.

3. Go to **System > File Management**

4. Click **Upload**.



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

You can delete older GUI files, but you do not have to.

6. Reboot the switch. Or alternatively, use a Serial console connection or SSH to access the CLI, then use the following commands to stop and restart the HTTP service:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service http
awplus(config)# service http
```

To confirm that the correct file is now in use, use the commands:

```
awplus(config)# exit
awplus# show http
```

Update the GUI on AR-Series devices

Prerequisite: On AR-Series devices, if the firewall is enabled, you need to create a firewall rule to permit traffic generated by the device that is destined for external services. See the “Configuring a Firewall Rule for Required External Services” section in the [Firewall and Network Address Translation \(NAT\) Feature Overview and Configuration Guide](#).

Perform the following steps through the command-line interface if you have been running an earlier version of the GUI and need to update it.

1. Use a Serial console connection or SSH to access the CLI, then use the following commands to download the new GUI:

```
awplus> enable  
awplus# update webgui now
```

Perform the following steps if you have been running an earlier version of the GUI and need to update it.

1. Use a Serial console connection or SSH to access the CLI, then use the following commands to download the new GUI:

```
awplus> enable  
awplus# update webgui now
```

2. Browse to the GUI and check that you have the latest version now, on the System > About page. You should have v2.10.0 or later.

