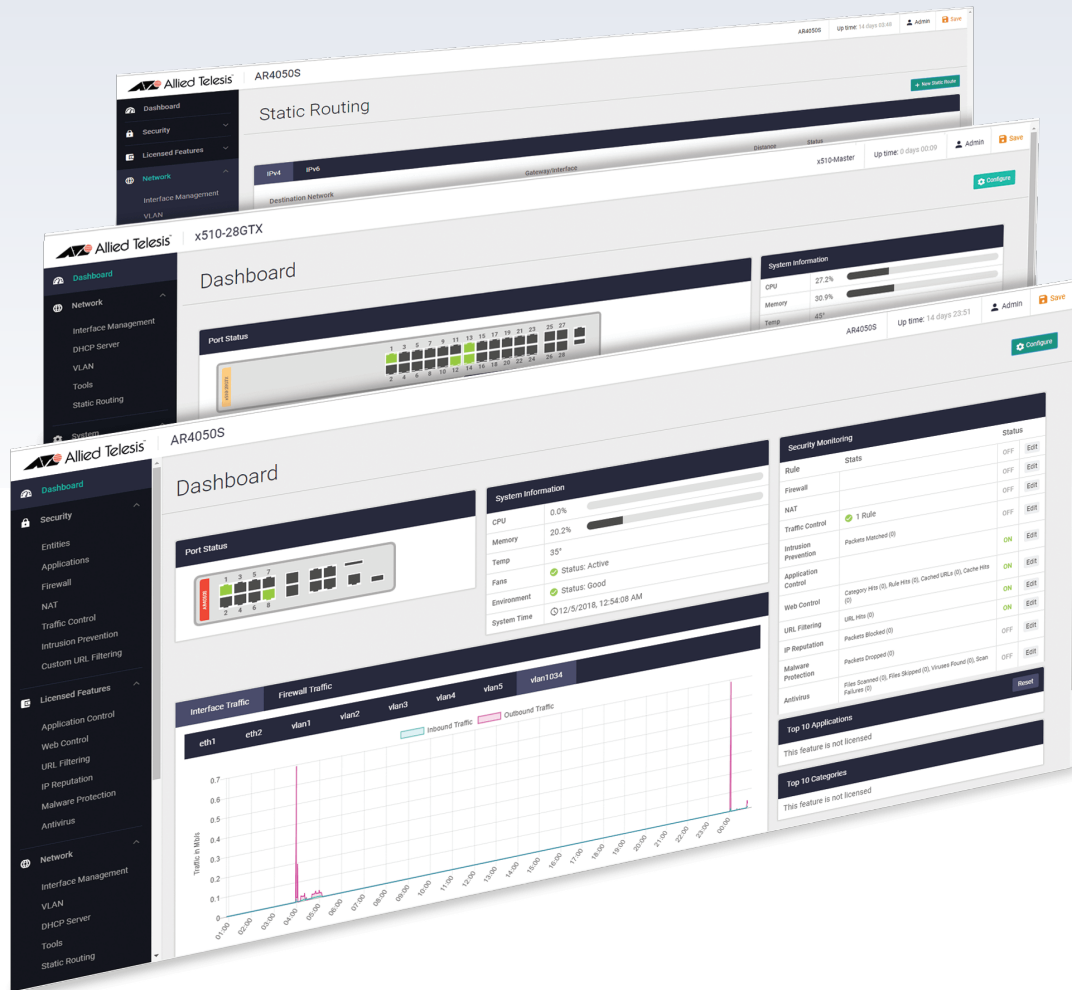


Release Note for Web-based Device GUI Version 2.7.x



» 2.7.0

AlliedWare Plus
OPERATING SYSTEM

Acknowledgments

©2021 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 2.7.0	4
Introduction	4
New Features and Enhancements	7
Wi-Fi Alliance certified Passpoint® (Hotspot 2.0) support and WiFi4EU	7
VLAN and EPSR interaction	11
Installing and Accessing the Web-based GUI on Switches.....	12
Installing and Accessing the Web-based GUI on AR-Series Devices	15

What's New in Version 2.7.0

Product families supported by this version:

SwitchBlade x908 GEN2	XS900MX Series
SwitchBlade x8100 Series	GS980M Series
x950 Series	GS980EM Series
x930 Series	GS970M Series
x550 Series	GS900MX/MPX Series
x530 Series	FS980M Series
x530L Series	AR4050S
x510 Series	AR3050S
x510L Series	AR2050V
IX5-28GPX	AR2010V
x310 Series	AR1050V
x320 Series	
x230 Series	
x230L Series	
x220 Series	
IE510-28GSX-80	
IE340 Series	
IE340L Series	
IE300 Series	
IE210L Series	
IE200 Series	

Introduction

This release note describes the new features in the Allied Telesis Web-based Device GUI version 2.7.0. You can run 2.7.0 with any AlliedWare Plus firmware version on your device. However some of the new features are only available with 5.5.0-2.2 or later.

For information on accessing and updating the Device GUI, see [“Installing and Accessing the Web-based GUI on Switches”](#) on page 12 or [“Installing and Accessing the Web-based GUI on AR-Series Devices”](#) on page 15.

The following table lists model names that support this version:

Table 1: Models

Models	Family
SBx908 GEN2	SBx908 GEN2
SBx81CFC960	SBx8100
x950-28XSQ x950-28XTQm x950-52XSQ	x950
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930

Table 1: Models (cont.)

Models	Family
x550-18SXQ x550-18XTQ x550-18XSPQm	x550
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L
IX5-28GPX	IX5
x310-26FT x310-50FT x310-26FP x310-50FP	x310
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
IE510-28GSX	IE510-28GSX
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340 and IE340L
IE300-12GT IE300-12GP	IE300
IE210L-10GP IE210L-18GP	IE210L
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200

Table 1: Models (cont.)

Models	Family
XS916MXT XS916MXS	XS900MX
GS980M/52 GS980M/52PS	GS980M
GS980EM/10H GS980EM/11PT	GS980EM
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28DP FS980M/28PS FS980M/52 FS980M/52PS	FS980M
AR4050S AR3050S	AR-series UTM firewalls
AR2050V AR2010V AR1050V	AR-series VPN routers

New Features and Enhancements

This section summarizes the new features in the Device GUI software version 2.7.0, for devices running AlliedWare Plus.

As well, version 2.7.0 includes a number of issue resolutions.

From version 2.7.0 onwards, the following new features and enhancements are available:

Wi-Fi Alliance certified Passpoint® (Hotspot 2.0) support and WiFi4EU

Applicable to Access Points: TQ5403, TQm5403, TQ5403e

Available with Alliedware Plus software version 5.5.0-2.2 or later.

Wireless > Wireless Setup > Networks

From version 2.7.0, you can enable Hotspot 2.0 on your wireless networks.

Hotspot 2.0, also known as Passpoint™ is the open standard for public Wi-Fi, introduced by the [Wi-Fi Alliance™](#). Passpoint brings seamless, secure Wi-Fi connectivity to any network employing Passpoint enabled Wi-Fi hotspots. It also provides user connections with WPA3™ security protection, enabling users to feel confident that their data is safe.

How does Passpoint work?

Passpoint lets users sign in to a Wi-Fi hotspot once, then uses their credentials as their devices hop from one access point to the next. Users' authentication occurs every time they connect. Of course, the hotspot (i.e., router) must support Passpoint for this connectivity transfer to happen.

Once a user accesses the Wi-Fi network offered at a location, the Passpoint-enabled client device will automatically connect upon subsequent visits. This eliminates the need for users to search for and choose a network, request Wi-Fi access, and re-enter authentication credentials each time they visit.

Passpoint improves the mobile user experience by offering:

- Automatic network discovery and selection
- Simplified online sign-up and instant account provisioning
- Seamless network access and cellular-like roaming between hotspots
- Enhanced security

The WiFi4EU Program

The WiFi4EU program provides funding to municipalities that want to participate in the development of a European free Wi-Fi network, so everyone has access. The program described on the WiFi4EU portal is open to any municipality that wants to provide this service.

To participate in this project, the Wi-Fi Access Points deployed within the municipality must be Passpoint certified so that interoperability with the whole system is guaranteed.

The Allied Telesis No Compromise Wi-Fi solution has been developed to support Passpoint 2.0 and is ready for WiFi4EU projects.

Enabling Hotspot 2.0

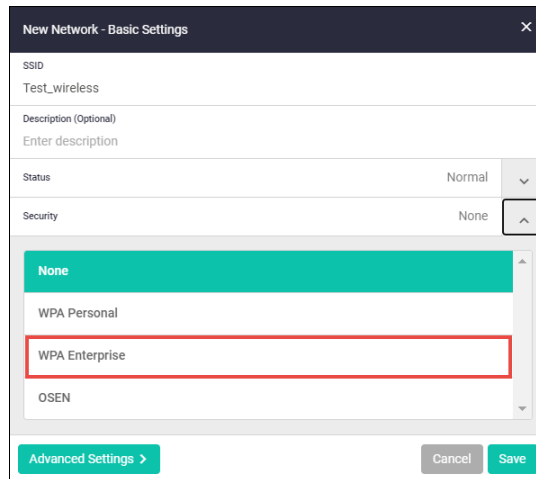
You enable Hotspot 2.0 in the wireless **Network** settings. There are two ways you can access the wireless Network settings:

- create a wireless network
- edit an existing wireless network

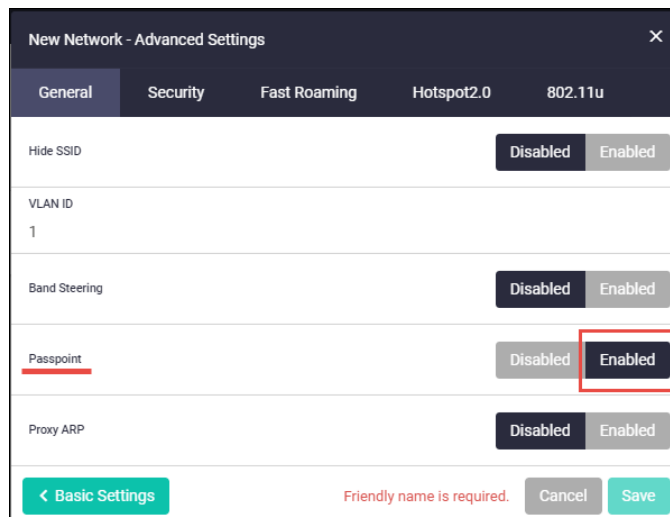
Create a wireless network

To create a wireless network:

- Select **Wireless > Wireless Setup > Networks**
- Click **+ Add Network**.
- The **Network - Basic Settings** window opens. From here you can:
 1. Enter the **SSID**, **Description**, **Status**, and **Security** details.
 2. For **Security** type, select **WPA Enterprise**.



3. Go to the **Advanced settings**.
4. Select the **General** tab and **Enable** Passpoint.



Configuring Hotspot 2.0

5. In the Advanced Settings, select the **Hotspot2.0** tab.
 - Complete the Hotspot 2.0 configuration fields:
 - ◀ The table below describes these fields.

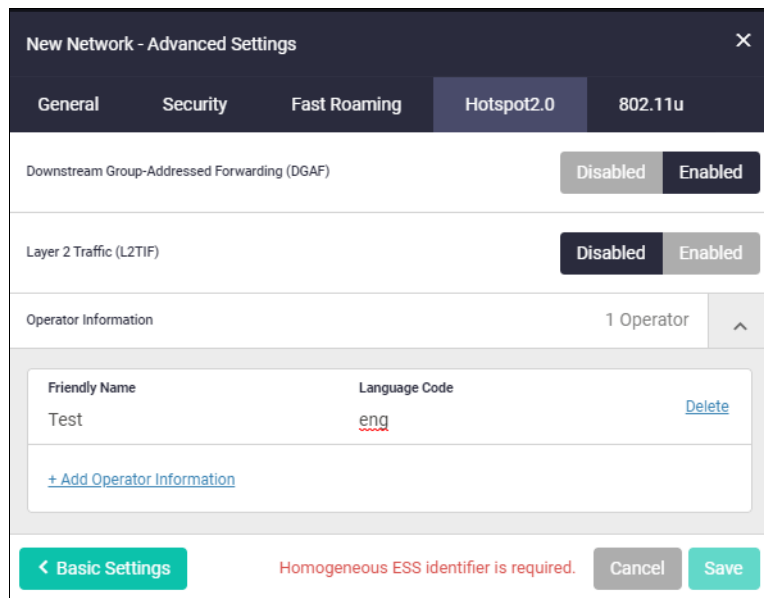


Table 2: Hotspot 2.0 configuration fields

Field	Description
Operator Friendly Name	The name of the operator you are providing. Use the language code, for example 'jpn' or 'eng', and the operator name string. <language code>:<name> For example: eng : Allied Telesis Holdings K.K. jpn : アライドテレスिस株式
Disable Downstream Group-Address Forwarding (DGAF)	Select 'Enable' to disable Downstream Group-Addressed Forwarding, change Disable Downtown Group-Addressed Forwarding (DGAF).
L2 Traffic Inspection and Filtering	If you want to discard L2 traffic between VAPs, enable L2 Traffic Injection and Filtering. The packets that TQ restricts are: ARP, ICMP, and TDLS.

Configuring 802.11u

6. Select the **802.11u** tab.
 - Complete the 802.11u configuration fields and click **Save**:
 - ◀ The table below describes these fields.

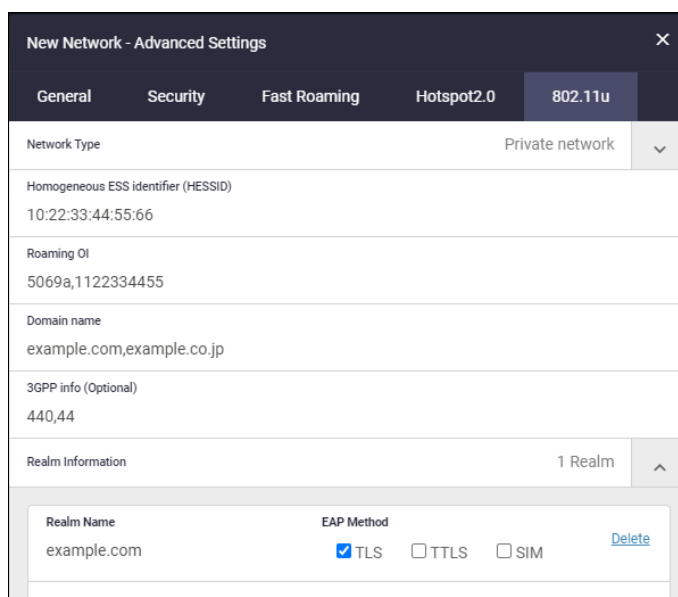


Table 3: 802.11u configuration fields

Field	Description
Network Type	<p>Specify any of the following 802.11u network types.</p> <ul style="list-style-type: none"> ■ private network — This network is accessible for authorized users only. For example, home networks or enterprise networks that require user authentication. ■ private network with guest access— This network is accessible to guest users based on guest authentication methods. For example, enterprise networks that allow guest users with captive portal authentication. ■ chargeable public network — This network provides access to the Internet based on payment. For example, a subscription-based Internet access in a coffee shop or a hotel offering chargeable in-room Internet access service. ■ free public network —This network is accessible to all without any charges applied. For example, a hotspot in airport or other public places that provide Internet access with no additional cost. ■ personal device network — This network is accessible for personal devices. For example, a laptop or camera configured with a printer for the purpose of printing. ■ emergency service only network —This network is limited to accessing emergency services only. ■ test or experimental — This network is used for test purposes only. ■ wildcard —This network indicates a wildcard network.

Field	Description
Homogeneous ESS Identifier HEISS	Homogeneous Extended Service Set Identifier. The device MAC address in a hexadecimal format separated by colons. For example, 10:22:33:44:55:66
Roaming OI	A group of subscription service providers (SSPs) having inter-SSP roaming agreements. <ul style="list-style-type: none"> ■ The Roaming Consortium list tells a mobile device which roaming consortiums or service providers are available through an AP. ■ The list must be in Hexadecimal format. For example, "506f9a, 001aeb, 1122334455"
Domain Name	Domain name of the access network operator, which is the identifier of the operated Hotspot2.0 network. For example, "example.com, example.net"
3GPP Cellular Network Information	The cellular network identifier. <ul style="list-style-type: none"> ■ This is a string concatenated Mobile Country Code (MCC) and comma(,) and Mobile Network Code (MNC). The MCC code is three digits, and the MNC is two or three digits. For example: "440,10" means "NTT DoCoMo, Inc" which is a mobile network in Japan. ■ Each "MCC, MNC" pair is separated by a semi-colon(;). For example: "440,10;440,50" ■ For more information on mobile network codes, see: Mobile Network Codes
Realm Information	The Network Access Identifier (NAI) Realm information. <ul style="list-style-type: none"> ■ The realm in the NAI format is represented after the @ symbol, which is specified as domain.com For example: user@realm.example.com <p>EAP method is the method that this NAI realm uses for authentication:</p> <ul style="list-style-type: none"> ■ TLS ■ TTLS ■ SIM

VLAN and EPSR interaction

Previously, it was possible to use the Device GUI to create and edit VLANs on ports that had EPSR configured. From version 2.7.0 onwards, EPSR ports are disabled on the VLAN editing page. Users can easily identify EPSR ports when editing VLANs and avoid misconfigurations.

Installing and Accessing the Web-based GUI on Switches

This section describes how to access the GUI to manage and monitor your AlliedWare Plus switch.

The GUI is a convenient tool for monitoring your device's status and performing basic management tasks. Its dashboard provides at-a-glance monitoring of traffic and other key metrics.

On SBx908 GEN2 switches, x950 Series, x930 Series, and x530 Series, you can also optimize the performance of your Allied Telesis APs through the Autonomous Wave Control wireless manager.

The steps for installing and accessing the GUI depend on whether the latest GUI has been pre-installed on your device in the factory.

Check if the GUI is installed

To tell if the GUI is installed on your device, simply browse to it, as described below.

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

Alternatively, you can use the default address on unconfigured devices, which is 169.254.42.42.

2. Open a web browser and browse to the IP address from step 1.
3. If you do not see a login page, you need to install the GUI, as described in ["Install the GUI if it is not installed" on page 13](#). If you see a login page, log in. The default username is *manager* and the default password is *friend*.

Check the GUI version

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

If you have an earlier version, update it as described in ["Update the GUI if it is not the latest version" on page 14](#).

Install the GUI if it is not installed

Perform the following steps through the command-line interface if your AlliedWare Plus switch does not currently have a GUI installed.

1. Obtain the GUI file from our Software Download center. The file to use is `awplus-gui_550_21.gui`.

The file is not device-specific; the same file works on all devices.

2. Copy the file into Flash memory on your switch. You can copy the file into Flash using any of the following methods:

- « TFTP server
- « USB Flash drive
- « SD card

For example, to copy the GUI file from your USB Flash drive, use the following commands:

```
awplus>enable
awplus#copy usb:awplus-gui_550_21.gui flash
```

To view all files in Flash and check that the newly installed file is there, use the following command:

```
awplus#dir
```

3. Delete any previous Java switch GUI files.

If you have been using the previous Java switch GUI, we recommend you delete the old GUI file to avoid any conflict. To do this, delete any Java files (.jar) from the switches Flash memory. For example:

```
awplus#del x510-gui_547_02.jar
```

4. If you haven't already, add an IP address to a VLAN on the switch. For example:

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

5. Make sure the HTTP service is running:

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

6. 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*.

Update the GUI if it is not the latest version

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. Obtain the GUI file from our Software Download center. The file to use is `awplus-gui_550_21.gui`.

The file is not device-specific; the same file works on all devices.

2. Copy the file into Flash memory on your switch. You can copy the file into Flash using any of the following methods:

- « TFTP server
- « USB Flash drive
- « SD card

For example, to copy the GUI file from your USB Flash drive, use the following commands:

```
awplus>enable
awplus#copy usb:awplus-gui_550_21.gui flash
```

To view all files in Flash and check that the newly installed file is there, use the following command:

```
awplus#dir
```

3. Stop and restart the HTTP service:

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

4. 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*.

Installing and Accessing the Web-based GUI on AR-Series Devices

This section describes how to access the GUI to manage and monitor your AlliedWare Plus device.

The GUI is a convenient tool for monitoring your device's status and performing basic management tasks. Its dashboard provides at-a-glance monitoring of traffic and other key metrics.

On AR4050S and AR3050S firewalls, you can use the GUI to create an advanced application-aware firewall with features such as Application control and Web control. Alternatively, you can configure real-time threat protection with URL filtering, Intrusion Prevention and Malware protection.

The steps for installing and accessing the GUI depend on whether the latest GUI has been pre-installed on your device in the factory.

Check if the GUI is installed

To tell if the GUI is installed on your device, simply browse to it, as described below.

Browse to the GUI

Perform the following steps to browse to the GUI.

Prerequisite: 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](#).

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

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

Alternatively, you can use the default address on unconfigured devices, which is 192.168.1.1.

2. Open a web browser and browse to the IP address from step 1.
3. If you do not see a login page, you need to install the GUI, as described in “[Install the GUI if it is not installed](#)” on page 16. If you see a login page, log in. The default username is *manager* and the default password is *friend*.

Check the GUI version

To see which version you have, open the About page in the GUI and check the field called **GUI version**. The version to use is 2.7.0. If you have an earlier version, update it as described in “[Install the GUI if it is not installed](#)” on page 16.

Install the GUI if it is not installed

Perform the following steps through the command-line interface if your AR-series device does not currently have a GUI installed.

1. If the device's firewall is enabled, 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](#).
2. If you haven't already, create one or more IP interfaces and assign them IP addresses, including configuring WAN connectivity. For information about configuring PPP, see the [PPP Feature Overview and Configuration Guide](#). For information about configuring IP, see the [IP Feature Overview and Configuration Guide](#).

3. Use the following command to download and install the GUI:

```
awplus# update webgui now
```

4. Make sure the HTTP service is running:

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

5. 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.

Update the GUI if it is not the latest version

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 the following command to download and install the GUI:

```
awplus# update webgui now
```

2. Stop and restart the HTTP service:

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

3. 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.