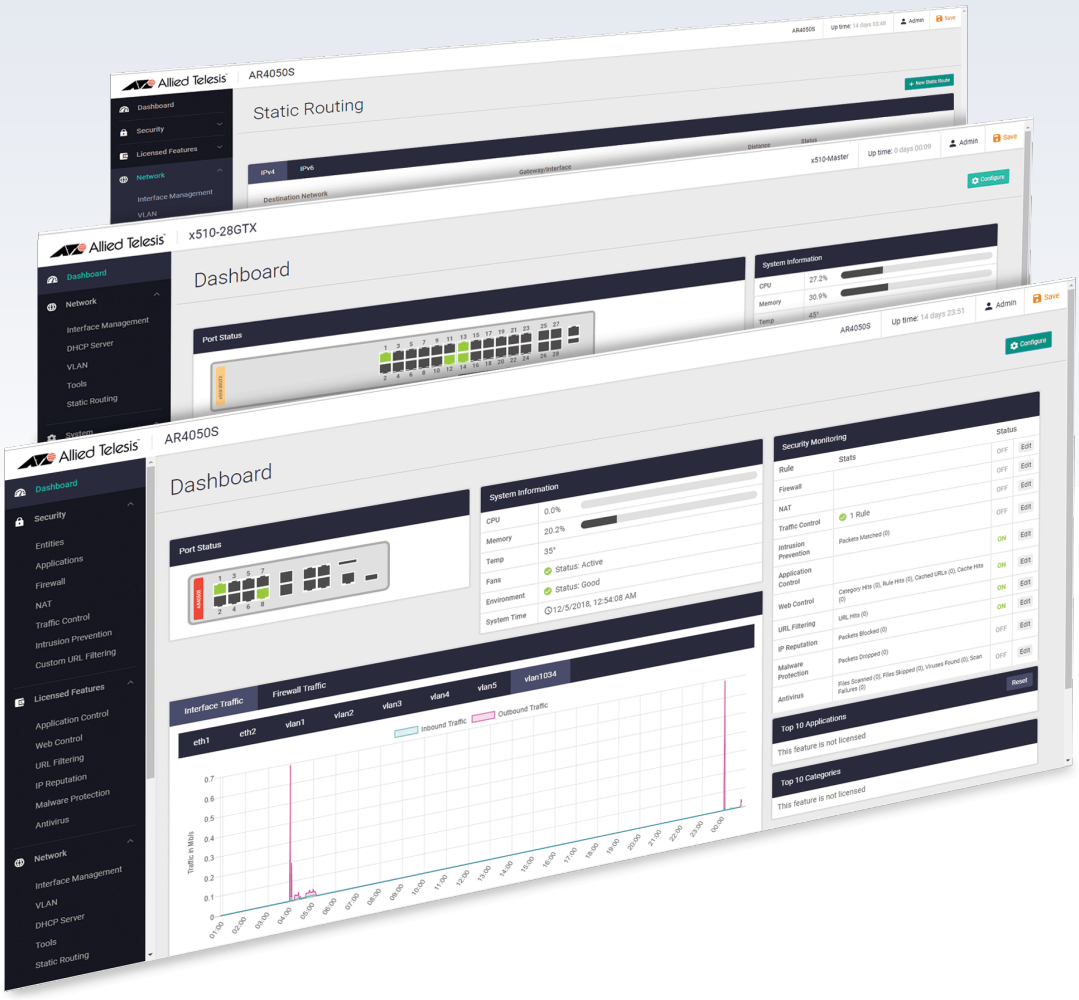
Release Note for Web-based Device GUI Version 2.18.x



» 2.18.0

AlliedWare Plus OPERATING SYSTEM

Acknowledgments

©2024 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 2.18.0

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330-10GTX
x320 Series
x230 Series
x240 Series
x220 Series
IE340 Series
IE220 Series
IE210L Series
SE240 Series[1]
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
AR4000S-Cloud
10GbE UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V[2]
AR2010V[2]
AR1050V
TQ6702 GEN2-R

1. Not available in all regions
2. Does not support all of the latest features

Introduction

This release note describes the new features in the Allied Telesis Web-based Device GUI version 2.18.0. You can run 2.18.0 with AlliedWare Plus firmware versions 5.5.4-x.x, 5.5.3-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 18.

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

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

Models	Family
x550-18SXQ x550-18XTQ x550-18XSPQm	x550
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330
x320-10GH x320-11GPT	x320
x240-10GTXm x240-10GHXm	x240
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
IE220-6GHX IE220-10GHX	IE220
IE210L-10GP IE210L-18GP	IE210L
SE240-10GTXm[1] SE240-10GHXm[1]	SE240
XS916MXT XS916MXS	XS900MX
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX
GS980EM/10H GS980EM/11PT	GS980EM
GS980M/52 GS980M/52PS	GS980M

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

Models	Family
GS970EMX/10 GS970EMX/20 GS970EMX/28 GS970EMX/52	GS970EMX
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M
10GbE UTM Firewall	
AR4000S Cloud	
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls
AR2050V[2] AR2010V[2] AR1050V	AR-series VPN routers
TQ6702 GEN2-R	Wireless AP Router

1. Not available in all regions
2. Does not support all of the latest features

New Features and Enhancements

This section summarizes the new features in the Device GUI software version 2.18.0.

Improvements to design of Device GUI

Available on: all devices

From version 2.18.0 onwards, the visual design of the Device GUI has been improved. GUI functionality was not affected by these improvements.

Firewall

Available on: devices that support the firewall

From version 2.18 onwards, you can apply firewall rules to tunnel and PPP interfaces. Do this by selecting the tunnel or PPP interface when creating or editing the relevant entity. See Getting Started with the TQ6702 GEN2-R Wireless Router using the Device GUI for information about creating and using entities.

IPsec VPNs

Available on: devices that support IPsec

From version 2.18.0 onwards, IPsec tunnels have the following enhancements.

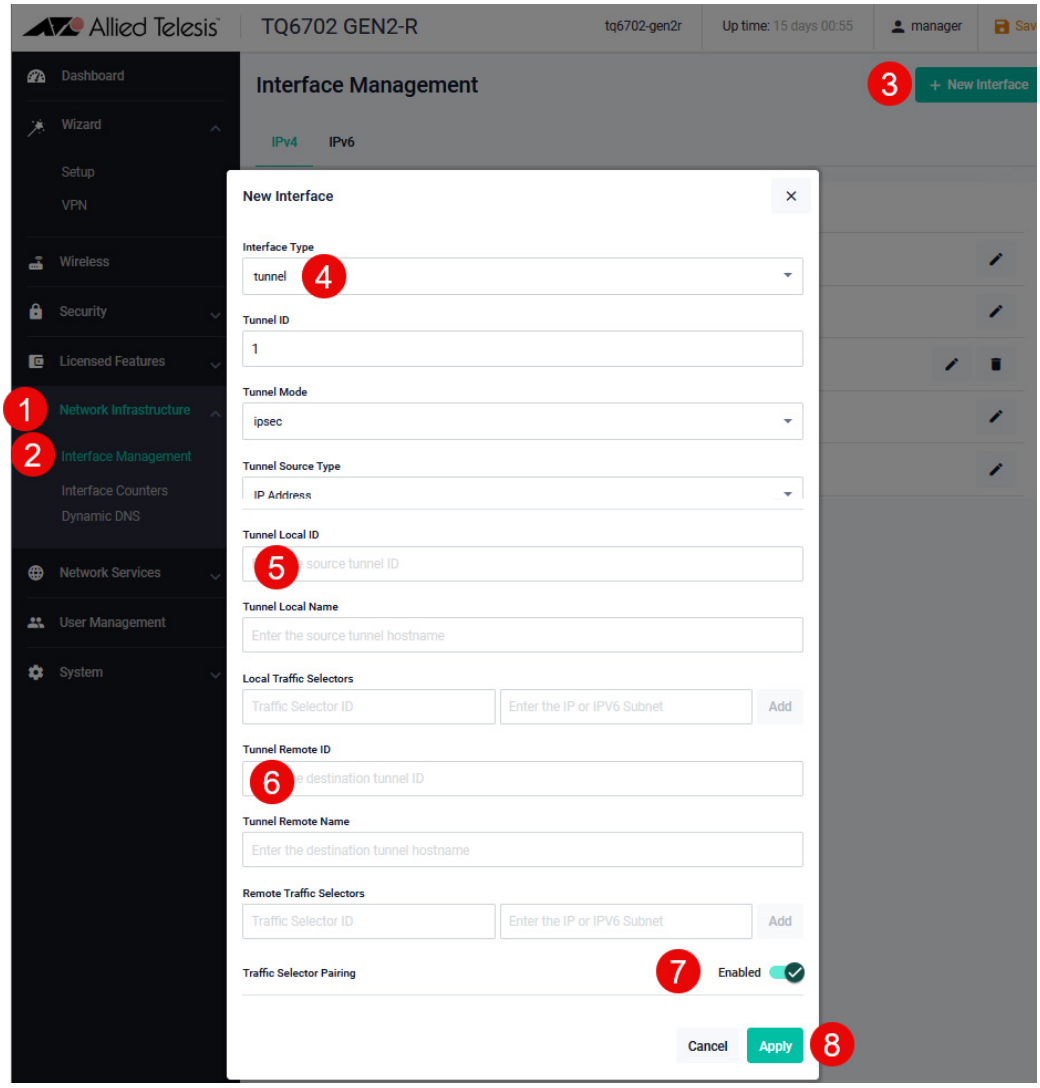
Local and remote ID and Traffic Selector Pairing

You can now configure a local and remote ID for IPsec tunnels in new tunnels. To do this, select **Network Infrastructure** in the lefthand menu, then **Interface Management**. Then add a new tunnel interface, and enter the **Tunnel Local ID** and **Tunnel Remote ID**.

You can also enable Traffic Selector Pairing in new tunnels. When this feature is disabled, if you specify address selectors, the tunnel can permit any combination of matching sources and/or destinations. While this conforms to the RFC, it may not be the expected behavior and may cause the IPsec SA to either fail negotiation or fail to pass traffic correctly.

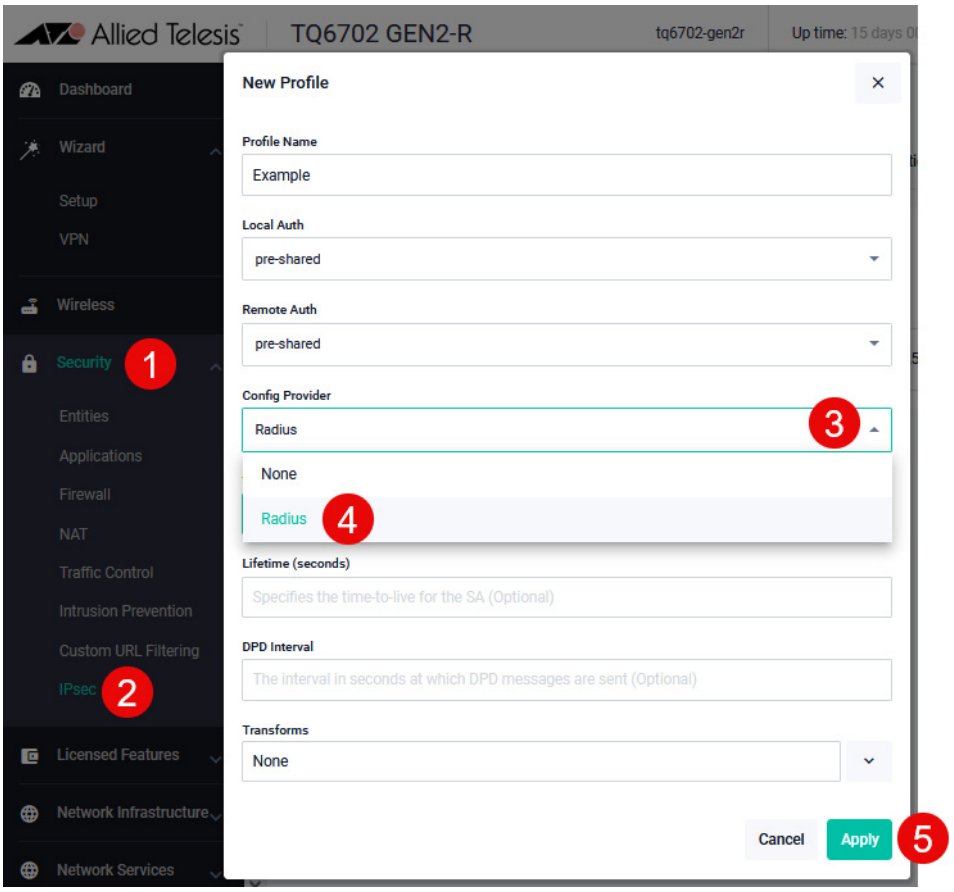
Enabling Traffic Selector Pairing forces ISAKMP to create individual IPsec SAs for each pair of source and destination selectors that have the same selector ID. Only traffic that matches a selector pair is permitted to flow via the associated SA.

To enable it, select **Network Infrastructure** in the lefthand menu, then **Interface Management**. Then add a new tunnel interface, and change the **Traffic Selector Pairing** to **Enabled**.


Allied Telesis
TQ6702 GEN2-R
tq6702-gen2r
Up time: 15 days 00:55
manager
Dashboard
Wizard
Setup
VPN
Wireless
Security
Licensed Features
Network Infrastructure
Interface Management
Interface Counters
Dynamic DNS
Network Services
User Management
System
Interface Management
+ New Interface
IPv4
IPv6
New Interface
Interface Type
tunnel
Tunnel ID
1
Tunnel Mode
ipsec
Tunnel Source Type
IP Address
Tunnel Local ID
source tunnel ID
Tunnel Local Name
Enter the source tunnel hostname
Local Traffic Selectors
Traffic Selector ID
Enter the IP or IPV6 Subnet
Add
Tunnel Remote ID
destination tunnel ID
Tunnel Remote Name
Enter the destination tunnel hostname
Remote Traffic Selectors
Traffic Selector ID
Enter the IP or IPV6 Subnet
Add
Traffic Selector Pairing
Enabled
Cancel
Apply
1
2
3
4
5
6
7
8

Configuration provided by RADIUS server

In ISAKMP, you can choose to have a RADIUS server provide configuration for clients. To do this, specify "Radius" as the **Config Provider** in the ISAKMP profile:

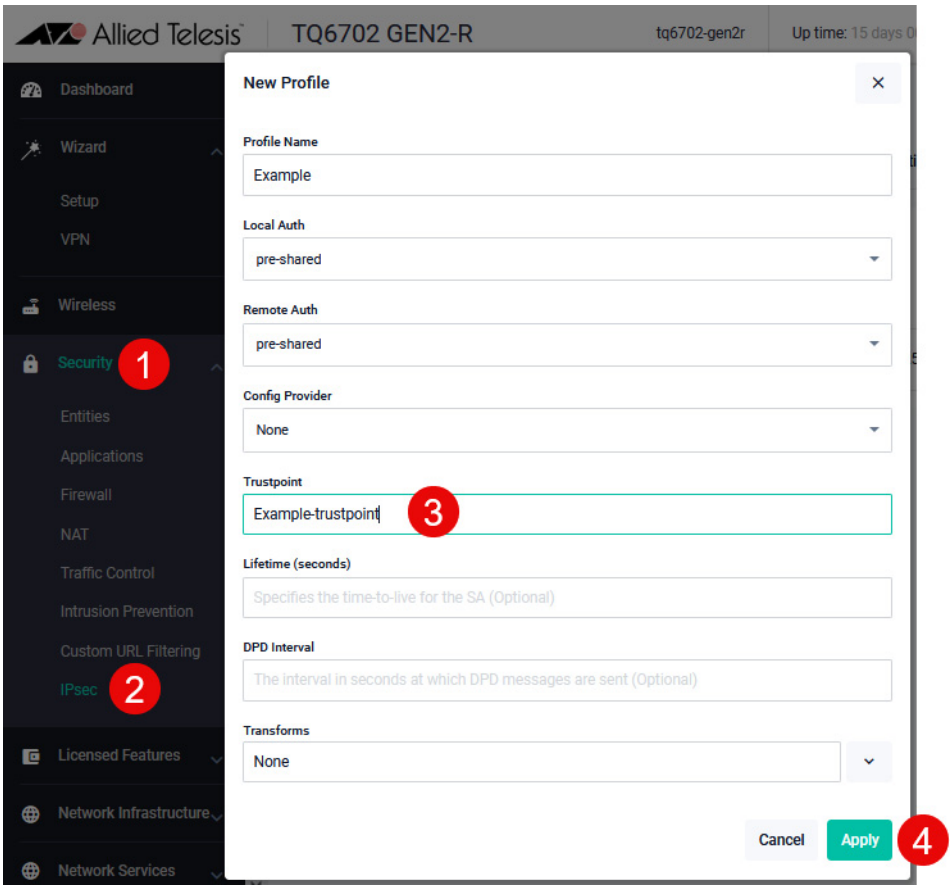


The following attributes are supported:

ID	ATTRIBUTE	TYPE	SPECIFICATION	EXAMPLE	USAGE
8	Framed-IP-Address	ipaddr	RFC2865	10.10.10.50	IP address to be pushed to the client.
9	Framed-IP-Netmask	ipaddr	RFC2865	255.255.255.0	IP netmask to be pushed to the client
MS-28	Microsoft-Primary-DNS-Server	ipaddr	RFC2548	10.10.10.1	Primary DNS to push to client. If multiple primary DNS servers are provided, only the first one will be used.
MS-29	Microsoft-Secondary-DNS-Server	ipaddr	RFC2548	10.10.10.2	Secondary DNS to push to client. If no primary address provided, this will be ignored.
168	Framed-IPv6-Address	ipv6addr	RFC6911	fc00:2::2	IPv6 address to be pushed to the client.
169	DNS-Server-IPv6-Address	ipv6addr	RFC6911	fc00:2::1	IPv6 DNS address to be pushed to the client (without NH).

Trustpoint

In ISAKMP, you can specify a trustpoint to use. To do this, specify it in the ISAKMP profile:

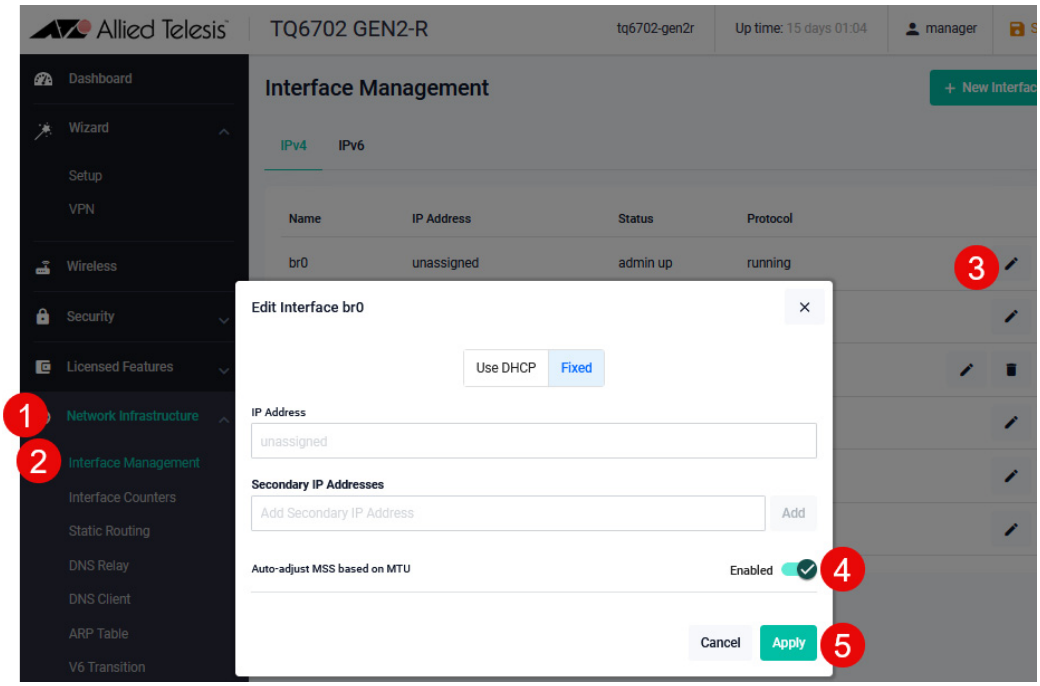


Automatically determine MSS

Available on: devices that support tunnels, PPP, eth and bridge interfaces

From version 2.18.0 onwards, on tunnels, PPP, eth and bridge interfaces, you can choose to automatically determine the MSS (maximum segment size) based on the MTU (maximum transmission unit). This feature is disabled by default. When it is disabled, you can enter an MSS value manually.

To enable it, select **Network Infrastructure** in the lefthand menu, then **Interface Management**. Then edit an existing interface, and change **Auto-adjust MSS based on MTU** to **Enabled**.

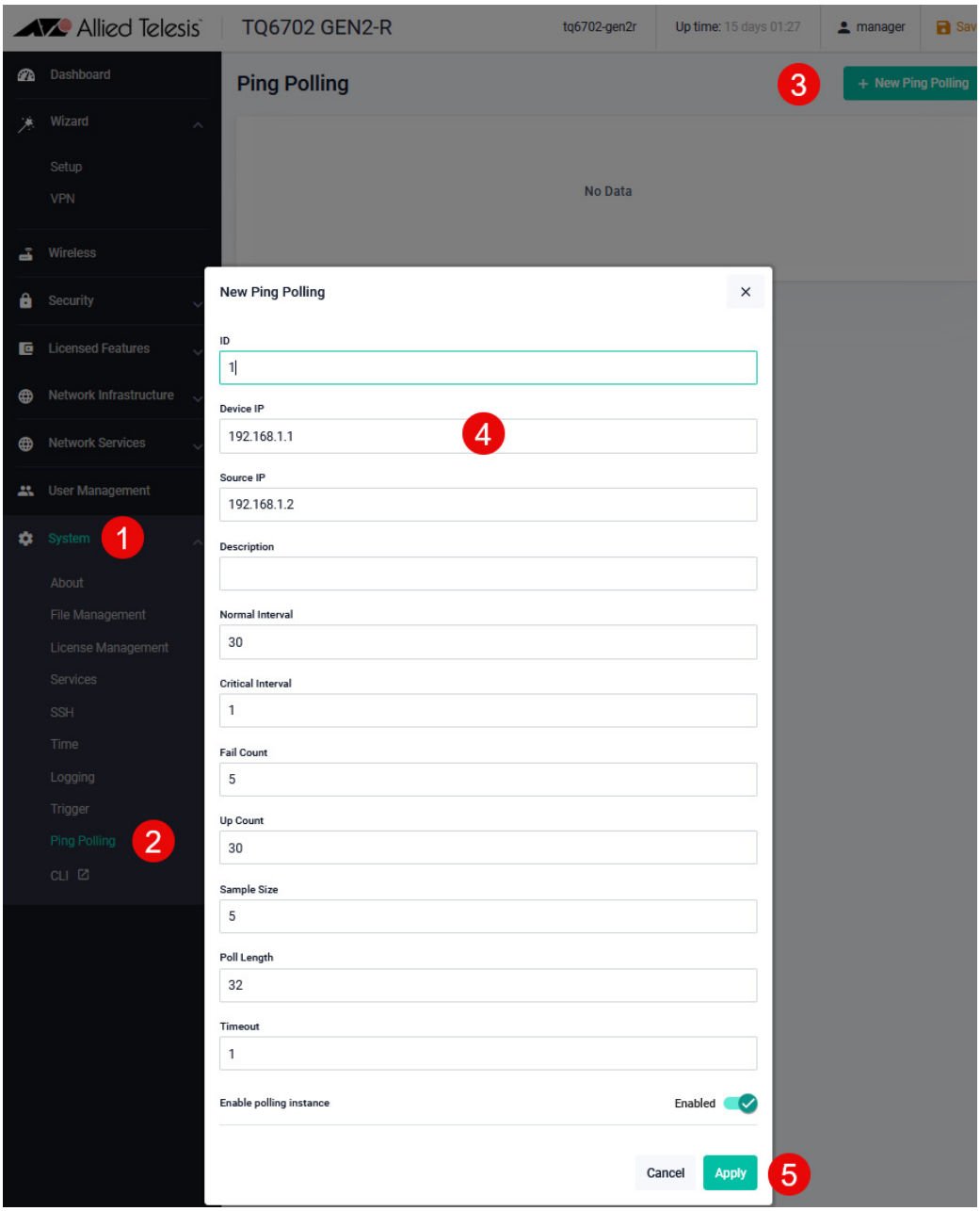


Ping Polling

Available on: all devices

From version 2.18.0 onwards, you can use Ping Polling to monitor whether a device is up or not. See the Ping Polling Feature Overview and Configuration Guide for information about ping polling.

To configure it, select **System** in the lefthand menu, then **Ping Polling**. Then create a new Ping Poll instance.



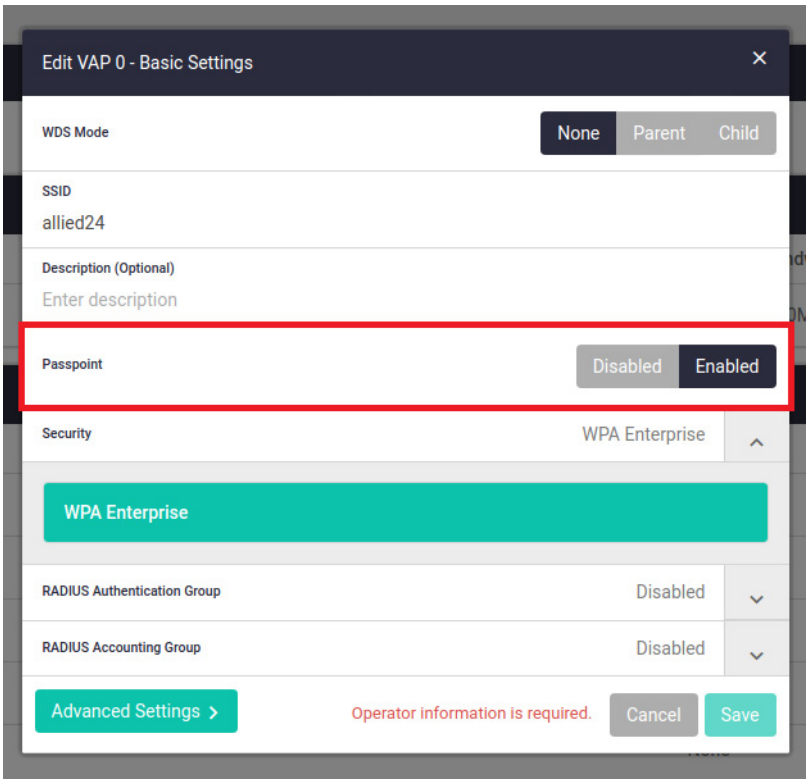
TQ6702 GEN2-R enhancements

From version 2.18.0 onwards, the Device GUI on TQ6702 GEN2-R wireless AP routers supports the following enhancements.

Most of these features require AlliedWare Plus version 5.5.4-1.1 onwards.

Passpoint

Version 2.18.0 onwards supports configuration of Passpoint™, also known as Hotspot 2.0. 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.



Edge Security

Version 2.18.0 onwards supports Edge Security. Once Edge Security has been configured on a TQ6702 GEN2-R, you become able to use Vista Manager EX to:

- Allow and deny specific clients to connect to the TQ6702 GEN2-R.
- Record all the clients which attempt to connect to the TQ6702 GEN2-R.

To configure Edge Security in the Device GUI on the TQ6702 GEN2-R, select Security > MAC Authentication from the lefthand menu.

Then select RADIUS, MAC Filter + External RADIUS, or External RADIUS. The following options will become available:

- **Unassociated Client List Acquire**

When enabled, this allows unauthenticated client information to be acquired and added to the Vista Manager EX topology map.

- **MAC Auth RADIUS Send Service-Type**

  When enabled, this adds the Service-Type attribute value 'Call-Check (10)' on the Access-Request when the device is RADIUS authenticated.

  Based on the request, the device's authentication mode will be either MAC Authentication or WPA-Enterprise.

- **MAC Auth RADIUS Dynamic Authorization Client**

  This lets you specify the client's IP address and shared key of Vista Manager EX.

More Radio mode options

Version 2.18.0 onwards supports configuring the following additional radio modes and bandwidth options:

Radio modes

- Radio1 - b/g/n
- Radio2 - a/n, a/n/ac

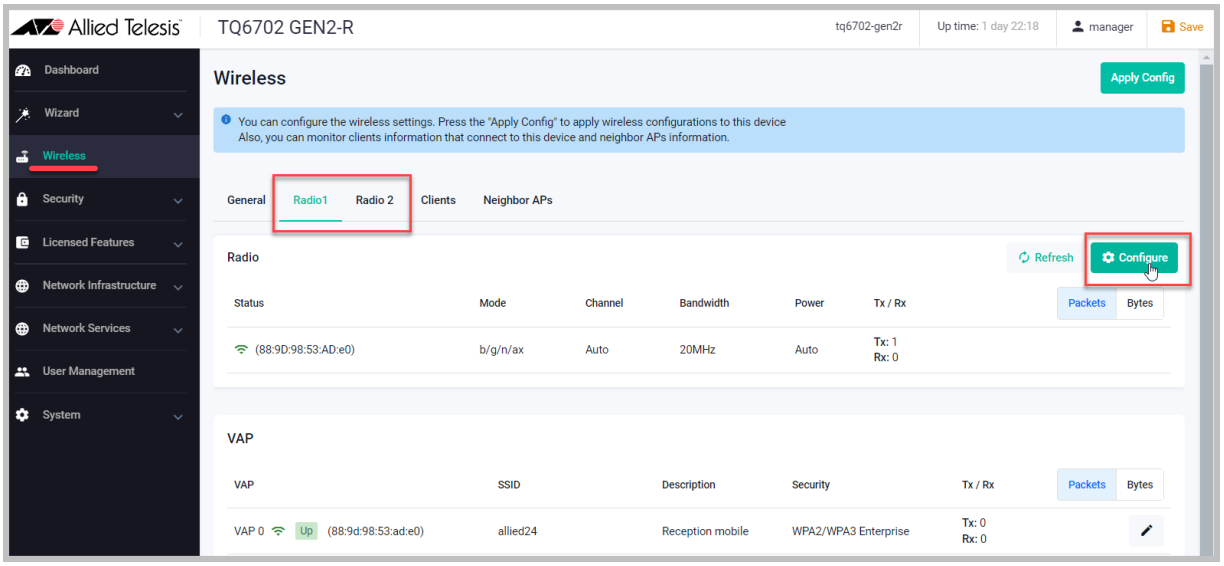
Bandwidth options

Radio1:

- b/g/n: 20 MHz, 40 MHz

Radio2:

- a/n: 20 MHz, 40 MHz
- a/n/ac: 20 MHz, 40 MHz, 80 MHz, 80+80 MHz



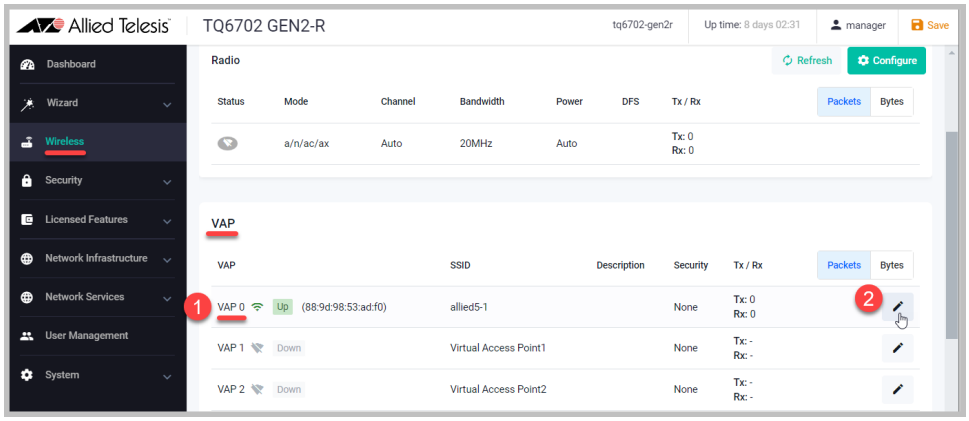
Multicast to Unicast conversion

From version 2.18.0 onwards, you can configure an Access Point (AP) to convert multicast packets into unicast packets destined for the client connected to the VAP. This conversion allows each client to receive data at the highest possible rate it supports.

To configure this feature:

1. Select **Wireless** from the left menu, and then select the Radio you want to configure. Find the VAP you want to edit (for example, VAP0).

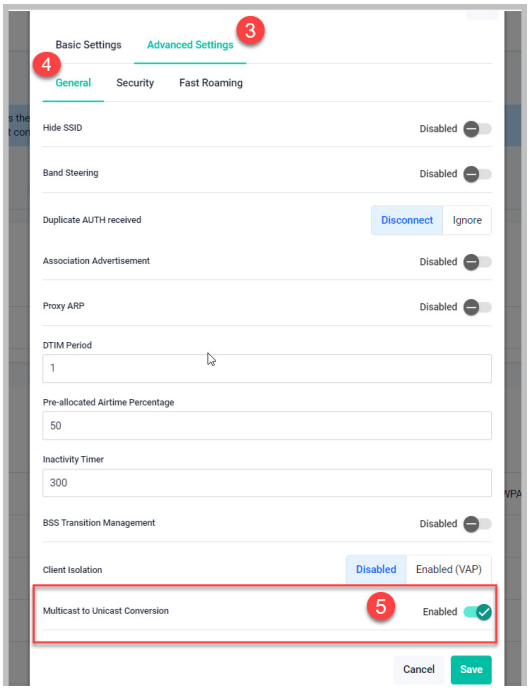
2. Click **Edit** VAP0.



3. Click **Advanced Settings**.

4. Select the **General** tab.

5. Enable **Multicast to Unicast Conversion**.



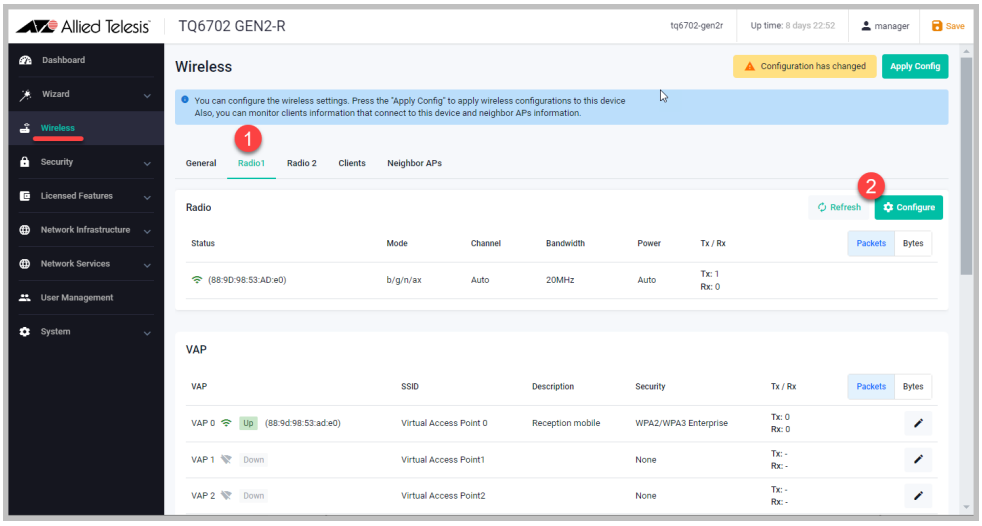
Airtime Fairness for each VAP

Version 2.18.0 adds the ability to set each VAP's Airtime Fairness percentage **manually**.

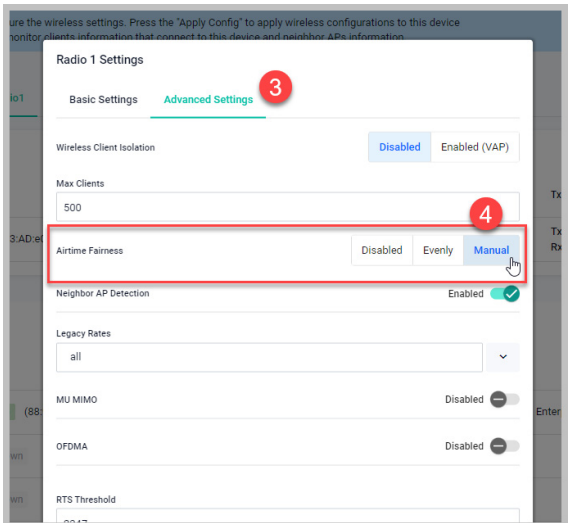
Airtime fairness is a concept and feature designed to ensure that all devices on a wireless network receive a fair share of the available airtime. This is particularly important in environments where devices with varying capabilities and data rates are connected to the same wireless access point.

To set Airtime Fairness to Manually:

1. Select **Wireless** from the menu on the left, and then select the **Radio** you want to configure.
2. Click **Configure**.



3. Click **Advanced Settings**.
4. Select the desired **Airtime Fairness** setting to **Manual**.

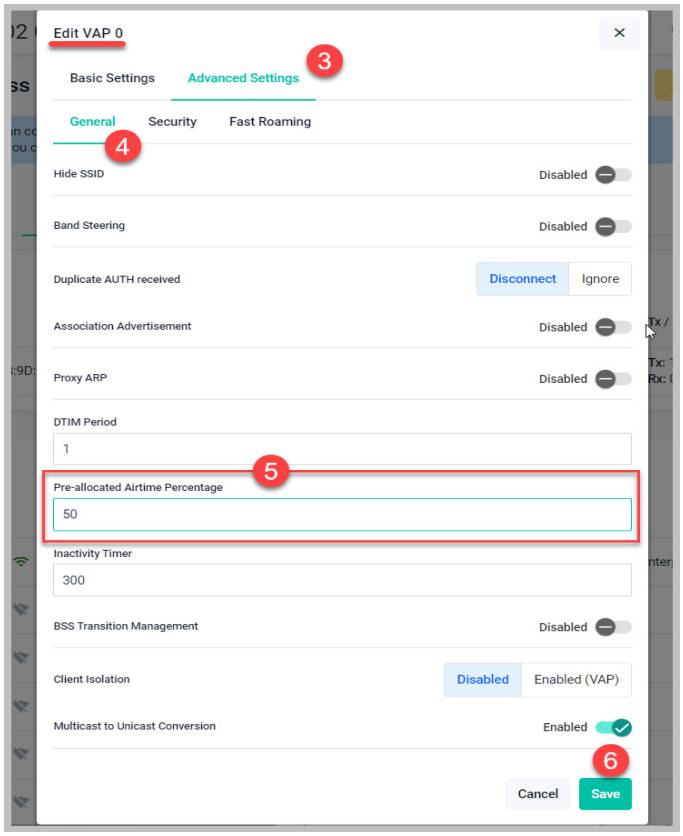


5. Click **Apply**.

You can now configure the VAP's **Pre-allocated Airtime Percentage**.

From the **Wireless** window:

1. Select the **VAP** you want to configure.
2. Click **Edit**.
3. Select **Advanced Settings**.
4. Select **General**.
5. Type in the **Pre-allocated Airtime Percentage** value, for example 50 (percent).
6. Click **Save**.



Accessing and Updating the Web-based GUI

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

Important Note: Very old browsers may not be able to access the Device GUI. From AlliedWare Plus version 5.5.2-2.1 onwards, to improve the security of the communication for the Device GUI, ciphersuites which use RSA or CBC based algorithms have been disabled, as they are no longer considered secure. Note that the removal of ciphersuites using those algorithms may prevent some old versions of browsers from communicating with the device using HTTPS.

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 and TQ6702 GEN2-R: 192.168.1.1

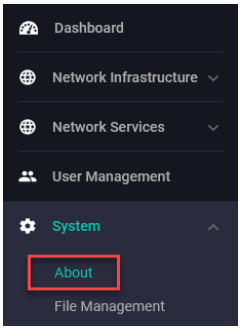
2. Open a web browser and browse to the IP address from step 1.

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 2.18.0, update it as described in "Update the GUI on switches" on page 19 or "Update the GUI on AR-Series devices" on page 20.



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 v2.18.0 of the GUI is:

   - awplus-gui_554_34.gui
   - awplus-gui_553_34.gui, or
   - awplus-gui_552_34.gui

   Make sure that the version string in the filename (e.g. 554) 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:

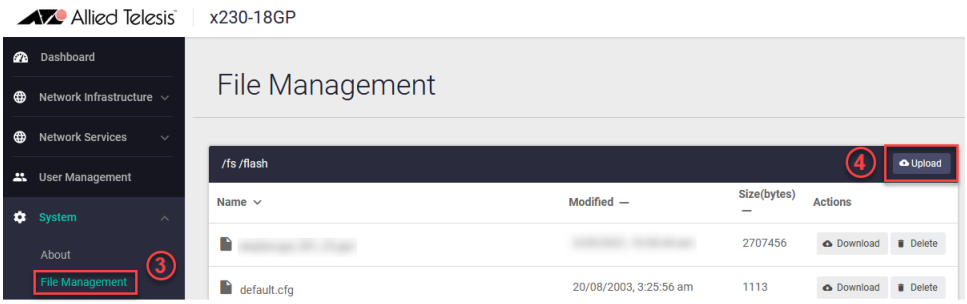
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   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

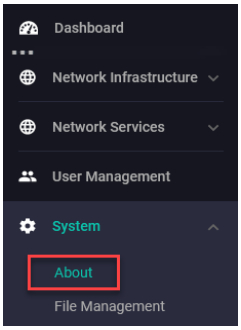
Prerequisite: On AR-Series devices, if the firewall is enabled, you need to create a firewall rule to permit traffic generated by the device that is destined for external services. See the "Configuring a Firewall Rule for Required External Services" section in the Firewall and Network Address Translation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

Perform the following steps 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 v2.18.0 or later.



Verifying the GUI File

On devices that support crypto secure mode, to ensure that the GUI file has not been corrupted or interfered with during download, you can verify the GUI file. To do this, enter Global Configuration mode and use the command:

```
awplus(config)#crypto verify gui <hash-value>
```

Where <*hash-value*> is the known correct hash of the file.

This command compares the SHA256 hash of the release file with the correct hash for the file. The correct hash is listed in the table of Hash values below or in the release's sha256sum file, which is available from the Allied Telesis Download Center.

Caution

If the verification fails, the following error message will be generated:
"% Verification Failed"
In the case of verification failure, please delete the release file and contact Allied Telesis support.

If you want the device to re-verify the file when it boots up, add the **crypto verify** command to the boot configuration file.

Table: Hash values

Firmware Version	GUI File	Hash
5.5.4-x.x	awplus-gui_554_32.gui	b3750b7c5ee327d304b5c48e860b6d71803544d8e06fc454c14be25e7a7325f4
5.5.3-x.x	awplus-gui_553_32.gui	b3750b7c5ee327d304b5c48e860b6d71803544d8e06fc454c14be25e7a7325f4
5.5.2-x.x	awplus-gui_552_32.gui	b3750b7c5ee327d304b5c48e860b6d71803544d8e06fc454c14be25e7a7325f4