Allied Telesis

New and enhanced features in AlliedWare Plus 5.4.5 major and minor versions (5.4.5-x.x)

AlliedWare Plus
OPERATING SYSTEM

» SBx8100 Series » SBx908 » DC2552XS » x930 Series
» x610 Series » x510 Series » IX5 » x310 Series » x230 Series
» x210 Series » AR3050S NGFW » AR4050S NGFW » VAA
» 5.4.5-2.x » 5.4.5-1.x » 5.4.5-0.x

Acknowledgments

Getting the most from this manual

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

Contents

AlliedWare Plus Version 5.4.5-2.x

for SwitchBlade x8100 Series, SwitchBlade x908, DC2552XS/L3, x930 Series, x610 Series, x510 Series, IX5-28GPX, x310 Series, x230 Series, and x210 Series Switches, the VAA (Virtual AMF Appliance), and AR3050S and AR4050S Next-Generation Firewalls

Contents

Introduction

This release note describes the new features and enhancements in AlliedWare Plus software version 5.4.5-2.x. For more information, see the Command Reference for your switch or AR-series firewall. Software file details for this version are listed in Table 1 below.

Caution: Software version 5.4.5 requires a release license for the SBx908 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.5 license certificate before you upgrade.

If an SBx908 or SBx8100 switch already has a version 5.4.5 license installed, that license also covers 5.4.5-2.x versions. Such switches do not need a new license before upgrading to version 5.4.5-2.x.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 28 and
- "Licensing this Software Version on a Control Card for an SBx8100 Series Switch" on page 30.

The first 5.4.5-2.x software version is numbered 5.4.5-2.1. The following table lists model names and software files for this version.

Table 1: Models and software file names

Models	Family	Software File	Date	GUI File
x210-9GT x210-16GT x210-24GT	x210 Series	x210-5.4.5-2.1.rel	11/2015	x210-gui_545_10.jar
x230-10GP x230-18GP x230-28GP	x230 Series	x230-5.4.5-2.1.rel	11/2015	x230-gui_545_11.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310 Series	x310-5.4.5-2.1.rel	11/2015	x310-gui_545_10.jar
IX5-28GPX		IX5-5.4.5-2.1.rel	11/2015	IX5-gui_545_06.jar
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 Series	x510-5.4.5-2.1.rel	11/2015	x510-gui_545_10.jar
x610-24Ts x610-24Ts-PoE+ x610-24Ts/X x610-24Ts/X-PoE+ x610-24SPs/X x610-48Ts x610-48Ts-PoE+ x610-48Ts/X x610-48Ts/X-PoE+	x610 Series	x610-5.4.5-2.1.rel	11/2015	x610-gui_545_10.jar

Table 1: Models and software file names

Models	Family	Software File	Date	GUI File
SwitchBlade x908 (see Table 2)	SBx908	SBx908-5.4.5-2.1.rel	11/2015	SBx908-gui_545_09.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930 Series	x930-5.4.5-2.1.rel	11/2015	x930-gui_545_11.jar
DC2552XS/L3		dc2500-5.4.5-2.1.rel	11/2015	n/a
SBx81CFC400 SBx81CFC960	SBx8100 Series	SBx81CFC400-5.4.5-2.1.rel SBx81CFC960-5.4.5-2.1.rel	11/2015	SBx81CFC400-gui_545_09.jar SBx81CFC960-gui_545_09.jar
AR3050S AR4050S	AR-series firewall	AR3050S-5.4.5-2.1.rel AR4050S-5.4.5-2.1.rel	11/2015	n/a
VAA (Virtual AMF Appliance)		vaa-5.4.5-2.1.iso	11/2015	n/a

Under version 5.4.5, not all models of XEM are supported in the SwitchBlade x908. The following table lists which XEMs are and are not supported under version 5.4.5.

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.5-x.x

Product	Supported in version 5.4.5-x.x
XEM-1XP	No
XEM-2XP	Yes
XEM-2XS	Yes
XEM-2XT	Yes
XEM-12S	No
XEM-12T	No
XEM-12Sv2	Yes
XEM-12Tv2	Yes
XEM-24T	Yes

Caution: Using a software version file for the wrong switch or AR-series firewall model may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

New Products

AlliedWare Plus version 5.4.5-2.x supports the following recently-released products.

Virtual AMF Appliance (VAA)

Virtual AMF Appliance (VAA) is a virtualized implementation of Allied Telesis Management Framework (AMF) that allows you to install AMF Masters and/or Controllers on a server. Having AMF Masters and Controllers available as virtual machines adds flexibility to the options available for AMF network designs.

For more information and installation instructions, see the "Virtual AMF Appliance (VAA) Installation and Technical Guidelines" later in this release note.

10G copper Ethernet expansion module for x930 Series switches

The AT-x9EM/XT4 features four 10GBASE-T ports, adding to the flexibility of the x930 series of advanced Layer 3+ switches. The x930 series have 24 or 48 1Gbps and 4 x 10Gbps SFP+ ports on the base unit. Now additional deployment options are supported with the ability to add 4 x 10Gbps copper ports (x9EM/XT4 module) or 2 x 40Gbps QSFP+ ports (StackQS module).

For more information, see the *x930 Series Data Sheet,* available from our website at **alliedtelesis.com/switches/x930**.

New Features and Enhancements

This section describes the new features in 5.4.5-2.x.

For a list of all new and modified commands, see "Licensing this Software Version on an SBx908 Switch" on page 28. For more information about all features on the switch or AR-series firewall, see the Command Reference for your switch or AR-series firewall.

Unless otherwise stated, all new features and enhancements are available on all switch and AR-series firewall models running this version of AlliedWare Plus.

AMF 20-Node Master License for x510 Series switches

A 20-node AMF Master feature license is now available for x510 Series switches, including x510DP and x510L Series switches. The license model name is AT-FL-x510-AM20.

Active Fiber Monitoring

For SwitchBlade x8100 Series, SwitchBlade x908, x930 Series, x610 Series, x510 Series, IX5-28GPX, x310 Series, x230 Series, and x210 Series Switches.

The active fiber monitoring feature monitors fiber ports to see if the received optical power drops below a configurable baseline by a threshold amount. This may indicate physical bending of the fiber cable, which could arise when there is a physical intrusion. If this happens, the device can perform a configurable action.

For step-by-step configuration instructions, see the "Active Fiber Monitoring Feature Overview and Configuration Guide" later in this release note.

For command details, see "Active Fiber Monitoring Commands" later in this release note.

Policy-based routing (PBR) on AR-series firewalls and SBx8100 Series switches

Policy-based routing is a way to direct any traffic (no matter its destination IP address) to a particular next-hop based on a rule. Traffic that matches the rule is routed via a next-hop defined on the rule, and is not routed by looking up a route in the normal IP route table.

Policy-based routing lets you specifically direct particular traffic streams down particular paths. There are various reasons for wanting to do this, including:

- Security: you may want traffic from certain parts of your network to traverse the Internet via a VPN, but traffic from other parts of the network can go openly via the Internet.
- Performance: you might have a dedicated link that you want voice traffic to go over, and a different link for all other traffic, to ensure that voice traffic has sufficient bandwidth.
- Multi-tenancy: Different subnets behind a switch might belong to different tenants, where each tenant has their own Internet gateway. In this situation, the switch needs to direct the different tenants' Internet- destined traffic via a different gateway device.

Earlier AlliedWare Plus versions supported policy-based routing on many x-series switches. This version adds support on SBx8100 Series and AR-series firewalls.

Policy-based routing for SBx8100 Series

On the SBx8100 Series, policy-based routing is configured in the same way as it is on other x-series switches: by creating class maps and policy maps to match the desired traffic, and then using the **set ip next-hop** command to apply a next-hop to the policy map.

Policy-based routing must be explicitly enabled on SBx8100 Series switches. To enable policy-based routing, use the new command:

```
awplus#platform pbr-enable
```

You need to reboot the switch after entering this command.

Note that enabling policy-based routing reduces the size of the conventional route table by 512 routes.

Policy-based routing for AR-series firewalls

On the AR-series firewalls, policy-based routing specifies which next-hop the firewall will use to route traffic from specified applications and entities. Configuring it is a two-step process.

First, create the application and entities that specify the traffic you want to route. To create an application, use the **application** command. To create entities, use the **zone**, **network**, and **host** commands. To see existing applications and entities, use the **show application** and **show entity** commands.

Then create policy routes to specify the next-hop for traffic that matches the desired application and entities. You can specify the route's next-hop by specifying the next-hop device's IPv4 or IPv6 address or egress interface. You can also list alternative next-hops to use if your first choice is down. To create policy routes, use the new commands listed below.

Commands

Policy-based routing introduces the new commands in the following table. For command details, see "Policy-based Routing Commands for AR-series Firewalls" later in this release note.

IPv4/IPv6	Command	Purpose
Both	policy-based-routing	Enter config-pbr mode
	policy-based-routing enable	Enable policy-based routing
	debug policy-based-routing	Turn on debugging for Policy-based routing
IPv4	dscp	Add DSCP values to an application
	ip policy-route	Create a policy route
	show ip pbr route	View the routes
IPv6	ipv6 policy-route	Create a policy route
	show ipv6 pbr route	View the routes

Example

In this example, external voice calls need to be routed via a next-hop of 10.37.236.65. Voice calls are identified by their UDP ports. To configure this, use the following commands:

Step 1: Create the application

```
awplus#configure terminal
awplus(config)#application voice
awplus(config-application)#protocol udp
awplus(config-application)#sport 3000 to 3010
awplus(config-application)#exit
```

Step 2: Create internal and external zones

```
awplus(config)#zone inside
awplus(config-zone)#network lan1
awplus(config-network)#ip subnet 192.168.1.0/24
awplus(config-network)#exit
awplus(config)#zone outside
awplus(config-zone)#network lan2
awplus(config-network)#ip subnet 10.37.119.0/27
awplus(config-network)#exit
```

Step 3: Create the policy route

```
awplus(config)#policy-based-routing
awplus(config-pbr)#policy-based-routing enable
awplus(config-pbr)#ip policy-route 10 match voice from inside
to outside nexthop 10.37.236.65
```

Step 4: Verify the route details

```
awplus(config-pbr)#exit
awplus(config)#exit
awplus#show ip pbr route
```

NAT support for VPN pass-through

For the AR-series firewalls only.

In addition to supporting network address translation for TCP and UDP traffic, AR-series firewalls also support VPN pass-through. Network services that use the following protocols can traverse a NAT device.

- ESP (Encapsulation Security Payload)
- PPTP (Point to Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)
- GRE (Generic Routing Encapsulation)

No commands have been updated or newly introduced as a result of this software update.

NAT enhancements

For the AR-series firewalls only.

The previous release of AlliedWare Plus supported two basic modes of NAT: Masquerading and Port Forwarding.

NAT enhancements have introduced the following extensions to these features:

- The ability to configure the global address used in Masquerading and Port Forwarding. Previously NAT used whatever IP address was configured on the egress interface. The enhancements make it possible to specify a different address to use.
- The ability to perform port translations in Port Forwarding configurations.

Therefore, AlliedWare Plus now supports the following methods of network address translation.

- Static NAT: This is a one-to-one, address-only translation. For packets originating in the private zone and destined for the public zone, the source IP address is translated. For packets originating in the public zone and destined for the NAT device's globally routable address, the destination address is translated.
- Static Enhanced NAT (ENAT): This is a one-to-one address and port translation for packet flows initiated by a host in a public zone that is mapped through to a host in a private zone. This has a number of possible uses. For example, a difference in destination port, with the same address in the public zone can be used to distinguish between two different servers in the private zone. For whatever reason, the server in the private zone may be listening on a different port to the one advertised in the public zone.
- Dynamic ENAT: This is a many-to-one address translation where multiple hosts in the private zone share a globally routable address in the public zone. Source-port translation is used to provide uniqueness in the connect tracking so that return packets can be forwarded to the correct host in the private zone.

With the above software updates, the **rule (NAT)** command has been updated, as described in the following section.

rule (NAT)

Overview Use this command to create a NAT rule.

Use the **no** variant of this command to remove a rule or all rules.

Syntax

```
rule [<1-65535>] {masq <application_name> from <source_entity> to
   <destination_entity>}|{portfw <application_name> from
   <source_entity> with dst <destination_host_entity>}

no rule {<1-65535>|all}
```

Parameter	Description
<1-65535>	Rule ID is an integer in the range <1-65535>. If you do not designate a rule ID, a rule ID will be automatically generated and it will be greater than the current highest rule ID.
`masq`	NAT with IP Masquerade is a case where all or a range of addresses are mapped to a single address with source port translation to identify the association. This single address masquerades as the public source address for the private addresses.
<application_name>	Application name. Application is a high level abstraction of application packets being transported by network traffic. You can configure source port, destination port, protocol, DSCP, ICMP code and ICMP type for the application. There are 40 predefined applications with protocols, source and destinations ports.You can use the **show application** command to show the detail of these applications.
`masq` *<source_entity>*	Source entity name. A entity represents a logical grouping of subnets, hosts or interfaces. The source entity defines the private side of the router. You assign private IP addresses (RFC 1918) to hosts on the private side of the router. When those hosts send traffic, the router translates the private addresses to one or more publicly valid addresses before routing the traffic. When the router receives traffic that is destined for those hosts, it translates the public addresses back to the appropriate private addresses.
<destination_entity>	Destination entity name. The destination entity defines the pool of public-valid IP addresses.
`portfw`	Allow remote hosts to connect to a specific host or service within a private LAN. This will forward IPv4 packets on to another device, for example, forward HTTP traffic to an internal web server.

Parameter	Description
<application_name>	Application name. You can configure source port, destination port, protocol, DSCP, ICMP code and ICMP type for the application. There are 40 predefined applications with protocols, source and destinations ports.You can use the **show application** command to show the detail of these applications.
`portfw` *<source_entity>*	Source entity name. An entity represents a logical grouping of subnets, hosts or interfaces. The source entity may be an entity outside your private network.
<destination_host_entity>	Target entity name. The target entity must be a host with one IP address.
<1-65535>	Remove a specific rule identified by its rule ID. You can change the rule order by using the **move rule (NAT)** command.
`all`	Remove all rules.

Mode NAT Configuration

Usage The device uses the AR-series firewall in conjunction with NAT. Portfwd and masq rules do not implicitly permit packets. Portfwd rules (actions) are applied before any other firewall and masq rules (actions) are applied after any other firewall rules. When firewall protection is enabled, all traffic is blocked by default. You should use the **rule (Firewall)** command to configure firewall rules which allow the same application, source and destination entities you configure for the NAT rules.

Entities should have valid interfaces on which inbound and outbound traffic can be properly translated. You can use the **ip subnet** command and the **ipv6 subnet** command to configure the interfaces.

Removing the NAT rule for an actively translated flow does not stop translating immediately. This means subsequent packets in the flow continue to be translated.

Example To perform network address translation and port forward application **http** from entity **public** to **any** with target destination **dmz.servers.web_server**, use the command:

```
awplus(config-nat)# rule 10 portfw http from public with dst
dmz.servers.web_server
```

To perform network address translation and masquerade application **http** from entity **lan** to **wan**, use the command:

```
awplus(config-nat)# rule masq http from lan to wan
```

To remove NAT rule 10, use the command:

```
awplus(config-nat)# no rule 10
```

IPsec custom profiles

For the AR-series firewalls only.

The previous release of the IPsec feature only supported default IPsec profiles and default ISAKMP profiles.

The IPsec custom profiles feature allows the AR-series firewalls to interoperate with routers running AlliedWare. You can use the new **crypto IPsec profile** command to configure a custom IPsec profile and then configure the required IPsec protocols, algorithms and parameters. You can also use the new **crypto isakmp profile** command to configure a custom ISAKMP profile and then configure the required IPsec protocols, algorithms and parameters.

For details about new and updated IPsec commands, see "IPsec Commands" later in this release note.

PPP IP Borrow

For the AR-series firewalls only.

PPP IP Borrow is a new feature in this release. PPP IP borrow involves processing IP packets on an PPP interface without explicitly assigning an IP address. This action can be performed by borrowing an IP address from another interface. The PPP interface which borrows the IP address is called the unnumbered interface. This feature is especially useful to save scarce IPv4 addresses.

You can use the new **ip unnumbered** command to borrow the primary IPv4 address from a specified interface, such as a VLAN, loopback, ethernet, or bridge interface. The IP address will be borrowed from the specified interface, regardless of the interface's operational state. For example, a VLAN or Ethernet interface can be in the "up" or the "down" state, and the address will still be borrowed. Packets originating from the AR-series firewall's unnumbered PPP interface have the borrowed IP address as their source IP address.

ip unnumbered

Overview Use this command to borrow an IP address from the specified interface, on an unnumbered PPP interface.

Use the **no** variant of this command to remove the borrowed IP address.

Syntax

```
ip unnumbered <interface_name>
no ip unnumbered
```

Parameter	Description
<interface_name>	Name of the Interface from which the IP address is to be borrowed. Valid interface types from which the IP address can be borrowed from are: VLAN, ethernet, loopback and bridge.

Default IP unnumbered is disabled by default.

Mode Interface Configuration for a PPP interface

Usage An unnumbered PPP interface can process IP packets without explicitly assigning an IP address. This is achieved by borrowing the primary IP address from the specified interface. Valid interface types from which the IP address can be borrowed from are VLAN, ethernet, loopback and bridge.

Example To borrow an IP address on unnumbered PPP from vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip address 6.6.6.6/24
awplus(config-if)# exit
awplus(config)# interface ppp0
awplus(config-if)# ip unnumbered vlan2
```

To remove the borrowed IP address, use the below commands:

```
awplus(config)# interface ppp0
awplus(config-if)# no ip unnumbered
```

PPP Dial on Demand

For the AR-series firewalls only.

PPP Dial on Demand is a new feature in this release. PPP Dial on Demand is used when a network connection is established only as required. Using PPP with this technique, a direct connection between two nodes can be established based on certain criteria, generally when the data needs to be sent.

On AlliedWare Plus devices, PPP links can be established over L2TP and PPPoE and can transport both IPv4 and IPv6 protocols.

An idle timer will disconnect the connection after a certain number of seconds determined by the configured device. This would be reset upon either ingress or egress user traffic. Non-user traffic such as Link Control Protocol (LCP) keepalives and Network Control Protocol (NCP) negotiation packets do not reset the idle timer. You can use the new **ppp timeout idle** command to enable the PPP Dial on Demand feature by specifying an idle time when a ppp connection is disconnected.

ppp timeout idle

Overview Use this command to specify an idle time when a PPP connection is disconnected.

Use the **no** variant of this command to reset the idle time to the default of 60 seconds.

Syntax

```
ppp timeout idle <0-99999>
no ppp timeout idle
```

Parameter	Description
<0-99999>	The time in seconds before the idle timeout disconnects. If this is not specified the default value of 60 seconds is used.

Default PPP timeout idle is not set and the PPP Dial on Demand feature is disabled. If no idle time is set, the default value of 60 seconds is used.

Mode Interface Configuration

Usage This command allows an idle timer to disconnect a PPP connection after a specified time. The timer is reset upon either ingress or regress user traffic. Non-user traffic such as Link Control Protocol (LCP) keepalives and Network Control Protocol (NCP) negotiation packets do not reset the idle timer.

Example To set the idle time to 30 seconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp timeout idle 30
```

To disable the use of the timer and disable the PPP Dial on Demand feature, enter the following commands:

```
awplus(config)# interface ppp0
awplus(config-if)# no ppp timeout idle 30
```

DNS Domain Name Matching

For the AR-series firewalls only.

DNS Domain Name Matching is a new feature in this release. DNS domain name matching allows you to specify a domain name suffix to match on when a client does a DNS lookup. When a match is detected the appropriate name server is used for resolving the address. For example, you might want to do the following:

- For all general DNS lookups such as www.example.com, use name server 1.2.3.4.
- For internal domain names such as example.lc, use the name server received on interface ppp1.

Note that this feature will only work for DNS lookups from a down-stream host that are relayed via the device, which is enabled by using the **ip dns forwarding** command. The feature functionality does not apply to DNS lookups originating from the device itself, for example "ping hostname" executed on the device.

For details about the new and updated commands, see "DNS Domain Name Matching Commands" later in this release note.

Supplicant MAC now supports MAC/Mask and IP/Mask

AlliedWare Plus Port Authentication offers the ability to authenticate supplicants (client devices) based on their MAC address. This allows users to configure authentication parameters of a supplicant with a specific MAC address.

Previously, this functionality could only match individual supplicant MAC addresses, and required a separate configuration entry for each supplicant. This functionality has now been extended to enable users to configure a masked MAC address so that a range of supplicants can be authorized, or unauthorized, based on their Organizationally Unique Identifier (OUI).

For example, you can force the interface state to authorized for any SCE (Sony) client device with a MAC address that includes an OUI of fc0f.e600.0000 by using the following command:

```
auth supplicant-mac fc0f.e600.0000 mask ffff.ff00.0000 port-control force-authorized
```

The existing **auth supplicant-mac** command has been updated to reflect this new behavior.

You can optionally use the `mask <mac-addr>` parameter of this command to add a mask to the MAC address of the supplicant.

For example, to add the supplicant MAC address 0009.41A4.0001 with mask ffff.ffff.0000 with force-authorized port control on interface port1.0.2, you can use the following commands:

```
awplus(config)# interface port1.0.2
```

```
awplus(config-if)# auth supplicant-mac 0009.41A4.5943 mask ffff.ffff.0000 port-control force-authorized
```

This enhancement also enables users to authorize or unauthorize supplicants by IP address and subnet mask. This is covered in the following section through the new **auth supplicant-ip** command.

auth supplicant-ip

Overview Use this command to add a supplicant (client device) IP address on a given interface.

Use the **no** variant of this command to delete the supplicant IP address, and reset to the default for the supplicant parameter.

Syntax

```
auth supplicant-ip <ip-addr>
[max-reauth-req <1-10>]
[port-control {auto | force-authorized | force-unauthorized}]
[quiet-period <1-65535>]
[reauth-period <1-4294967295>]
[supp-timeout <1-65535>]
```

```
[server-timeout <1-65535>][reauthentication]

no auth supplicant-ip <ip-addr> [reauthentication]
```

Parameter	Description
<ip-addr>	IP address of the supplicant entry in A.B.C.D/M format
`max-reauth-req`	Number of reauthentication attempts before becoming unauthorized (default 2).
<1-10>	Count of reauthentication attempts
`auto`	Allow port client to negotiate authentication
`force-authorized`	Force port state to authorized
`force-unauthorized`	Force port state to unauthorized
`quiet-period`	Quiet period in the HELD state (default 60 seconds).
<1-65535>	Seconds for quiet period.
`reauth-period`	Seconds between reauthorization attempts (default 3600 seconds).
<1-4294967295>	Seconds for reauthorization attempts (reauth-period).
`supp-timeout`	Supplicant response timeout (default 30 seconds).
<1-65535>	Seconds for supplicant response timeout.
`server-timeout`	Authentication server response timeout (default 30 seconds).
<1-65535>	Seconds for authentication server response timeout
`reauthentication`	Enable reauthentication on a port.

Default No supplicant IP address for port authentication exists by default until first created with this command. The defaults for parameters applied are as shown in the parameter table.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, a switch port, or Auth Profile.

Example To add the supplicant IP address 192.168.10.0/24 with force authorized port control for interface port1.0.2, use the following commands:

```
awplus# configure terminal

awplus(config)# interface port1.0.2

awplus(config-if)# auth supplicant-ip 192.168.10.0/24 port-
control force-authorized
```

To delete the supplicant IP address 192.168.10.0/24 for interface port1.0.2, use the following commands:

```
awplus# configure terminal

awplus(config)# interface port1.0.2

awplus(config-if)# no auth supplicant-ip 192.168.10.0/24
```

To reset reauthentication to disable for the supplicant(s) IP address 192.168.10.0/24, for interface port1.0.2 use the following commands:

```
awplus# configure terminal

awplus(config)# interface port1.0.2

awplus(config-if)# no auth supplicant-ip 192.168.10.0/24
reauthentication
```

To add the supplicant IP address 192.168.10.0/24 to force authorized port control for auth profile 'student', use the following commands:

```
awplus# configure terminal

awplus(config)# auth profile student

awplus(config-auth-profile)# auth supplicant-ip 192.168.10.0/
24 port-control force-authorized
```

To delete the supplicant IP address 192.168.10.0/24 for auth profile 'student', use the following commands:

```
awplus# configure terminal

awplus(config)# auth profile student

awplus(config-auth-profile)# no auth supplicant-ip
192.168.10.0/24
```

To reset reauthentication to disable for the supplicant IP address 192.168.10.0/24, for auth profile 'student', use the following commands:

```
awplus# configure terminal

awplus(config)# auth profile student

awplus(config-auth-profile)# no auth supplicant-ip
192.168.10.0/24 reauthentication
```

Web-auth for AR-series firewalls (ETH ports only)

For the AR-series firewalls only.

Web authentication is supported for routers on ETH ports. It is a mechanism to authenticate a client by using HTTP or HTTPS.

If the AR-series firewall detects an unauthorized user web browsing, then they are re-directed to a Web-authentication login page. The client enters their username and password into the login page, and the device then sends the credentials to a RADIUS server for checking. If the RADIUS server accepts the client's credentials, the device then allows the client's traffic to enter the network.

For more information about Web-authentication, see the Web-authentication Feature Overview and Configuration Guide document which is available on our website.

For more information about Authentication commands, see "Authentication Commands" later in this release note. For more information about AAA commands, see "AAA Commands" later in this release note.

Web-auth language localization

Previously, Web authentication pages were presented in English. Now Web authentication pages can be presented in Japanese. Web authentication pages are presented in English by default and you can use the **auth-web-server page language** command to set the presentation language of Web authentication pages.

auth-web-server page language

Overview Use this command to set the presentation language of Web authentication pages. Titles and subtitles of Web authentication pages will be set accordingly.

Use the **no** variant of this command to set the presentation language of Web authentication pages to its default (English).

Syntax

```
auth-web-server page language {english|japanese}
no auth-web-server page language
```

Parameter	Description
`english`	Web authentication pages are presented in English.
`japanese`	Web authentication pages are presented in Japanese.

Default Web authentication pages are presented in English by default.

Mode Global Configuration

Example To set Japanese as the presentation language of Web authentication pages, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page language japanese
```

To set English as the presentation language of Web authentication pages, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page language english
```

To unset the presentation language of Web authentication pages and use English as the default presentation language, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page language
```

Support for Service-Type(6) and NAS-Identifier(32) RADIUS attributes

For AlliedWare Plus switches (not AR-series firewalls).

This enhancement enables the switch to include the following attributes in RADIUS authentication requests:

- the Service-Type(6) RADIUS attribute.
- the NAS-Identifier(32) RADIUS attribute for VLAN notification.

To configure the Service-Type RADIUS attribute, use the command:

```
awplus(config)# auth radius send service-type
```

To configure the NAS-Identifier RADIUS attribute, use the command:

```
awplus(config)# auth radius send nas-identifier [<name>|
<vlan-id>]
```

The following sections give detailed information about these new commands.

auth radius send service-type

Overview Use this command to enable the switch to include the Service-Type attribute in RADIUS authentication requests. The Service-Type attribute has a value of:

- Framed(2) for 802.1x
- Call-Check(10) for MAC authentication
- Unbound(5) for Web authentication.

Use the **no** variant of this command to stop including the Service-Type attribute.

Syntax

```
auth radius send service-type
```

```
no auth radius send service-type
```

Mode Global Configuration

Examples To send the Service-Type attribute, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# auth radius send service-type
```

To stop sending the Service-type attribute, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no auth radius send service-type
```

auth radius send nas-identifier

Overview Use this command to enable the switch to include the NAS-Identifier attribute in RADIUS authentication requests.

Use the **no** variant of this command to stop including the NAS-Identifier attribute.

Syntax

```
auth radius send nas-identifier [<name>|vlan-id]
no auth radius send nas-identifier
```

Parameter	Description
<name>	Send this user-defined text as the NAS-Identifier. You can specify up to 253 characters.
`vlan-id`	Send the VLAN ID of the authentication port as the NAS-Identifier. This is the configured VLAN ID, not the dynamic VLAN ID or guest VLAN ID.

Mode Global Configuration

Examples To use a user-defined identifier of NASID100 as the NAS-Identifier attribute, use the commands:

```
awplus# configure terminal
awplus(config)# auth radius send nas-identifier NASID100
```

To use the VLAN ID as the NAS-Identifier attribute, use the commands:

```
awplus# configure terminal
awplus(config)# auth radius send nas-identifier vlan-id
```

To stop sending the NAS-Identifier attribute, use the commands:

```
awplus# configure terminal
awplus(config)# no auth radius send nas-identifier
```

Flow-based Equal-Cost Multi-Path (ECMP) routing

For the AR-series firewalls only.

ECMP enables a router to vary the path that traffic takes, so that if multiple paths have the same routing cost, traffic is split between those paths. This significantly improves bandwidth by utilizing all available paths of equal cost.

Previously, ECMP calculations were done on a per-packet basis. This meant that the packets in a flow could take different paths.

On AR-series firewalls, ECMP routing is now flow-based. This means that packets from the same flow will always be sent on the same path.

Note that ECMP routing has not changed on AlliedWare Plus switches; it is still packet-based.

ECMP is enabled by default. You can use the **maximum-paths** command to turn it off or to change the maximum number of paths over which the router can split traffic.

Flexible LAG configuration for x210 Series switches

For x210 Series switches only.

Previously, on x210 switches you could create up to 4 static channel groups and up to 4 dynamic (LACP) channel groups.

You can now create up to 8 channel groups, in any combination of static channel groups and dynamic (LACP) channel groups. For example, you can create 6 LACP groups and 2 static groups, or 3 LACP groups and 5 static groups, or any other combination to a maximum of 8 groups.

Increased number of ACLs on x930 Series switches

For x930 Series switches only.

AlliedWare Plus now supports up to 2038 ACLs on x930 Series switches.

Note that QoS entries share the same area of dedicated ASIC memory, so increasing the number of ACLs reduces the number of QoS class-maps and policy-maps available. ASIC memory is allocated in “groups” of 256 entries. The switch automatically allocates the correct number of groups to ACLs and QoS as you create more ACLs or QoS class-maps and policy-maps.

To see how many entries are allocated and used, use the command:

```
awplus# show platform classifier statistics utilization brief
```

The following example output is for a switch where:

- 758 entries are allocated to ACLs, of which 702 entries are used, and
- 1024 entries are allocated to QoS, of which 850 entries are used, and
- 256 entries are unallocated (2038 - 1024 - 758 = 256)

```
[Instance 4]
Capacity: 2038
Number of Entries:
Policy Type Group ID Used / Allocated
-------------------------------------------
ACL 1476395009 702 / 758 ( 92%)
DoS Inactive 0 / 0 ( 0%)
VLAN Counter
Group-Octet Inactive 0 / 0 ( 0%)
Group-Packet Inactive 0 / 0 ( 0%)
QoS 850 / 1024 ( 83%)
Group-0 1 250 / 256 ( 97%)
Group-1 2 250 / 256 ( 97%)
Group-2 3 250 / 256 ( 97%)
Group-3 4 100 / 256 ( 39%)
```

Increased number of VRRPv3 limits

Previously, VRRPv3 on AlliedWare Plus was limited to 32 IPv4 VRRP instances and 32 IPv6 VRRP instances.

It is now possible to configure up to 255 IPv4 and 255 IPv6 VRRP instances.

Note that configuring a high number of instances may adversely affect the device's performance, depending on the device CPU and the other protocols running on the device.

Storm event notifications: traps, log messages and flashing LEDs

For AlliedWare Plus switches.

The methods to alert users of the existence of network storms have been enhanced. The following methods are now available.

findme trigger

Overview When this command is enabled, the LED flashing functionality of the **findme** command is applied whenever any or all of the selected parameter conditions is detected.

Use the **no** variant to remove the findme trigger function for the selected parameter function.

Syntax

```
findme trigger {all|loopprot|thrash-limit|qsp}
no findme trigger {all|loopprot|thrash-limit|qsp}
```

Parameter	Description
`all`	Enable the find-me function whenever any of the listed parameter functions is detected.
`loopprot`	Enable the find-me function whenever loop protection is detected.
`thrash-limit`	Enable the find-me function whenever thrash-limiting is detected.
`qsp`	Enable the find-me function whenever a QSP (QoS Storm Protection) event is detected.

Default The findme trigger function is disabled.

Mode Global Configuration

Example To enable the findme function whenever loop protection condition is detected:

```
awplus# findme trigger loopprot
```

snmp-server trap

This command now includes a QSP (QoS Storm Protection) parameter. With this parameter selected, an SNMP notification and log message will be generated whenever a QSP event is detected.

Overview Use this command to enable the switch to transmit the specified notifications (traps).

Note that the SNMP environmental monitoring traps defined in AT-ENVMONv2-MIB are enabled by default.

Use the **no** variant of this command to disable the transmission of the specified notifications (traps).

Syntax

```
snmp-server enable trap
   {[atmf][atmflink][atmfnode][atmfrr][auth][bgp]
   [dhcpsnooping] [epsr] [lldp] [loopprot] [mstp] [nsm] [ospf]
   [pim] [power-inline] [qsp] [rmon] [thrash-limit]
   [vcs][vrrp][wireless]}
```

Increased feature support for DC2552XS/L3 switches

AlliedWare Plus now supports the following additional commands on DC2552XS/L3 switches. For information about each command, see the switch's Command Reference, which is available from our website at alliedtelesis.com.

Command	Feature
atmf backup server	AMF
atmf backup synchronize	AMF
atmf cleanup	AMF
atmf distribute firmware	AMF
atmf provision	AMF
atmf provision node clone	AMF
atmf provision node configure boot config	AMF
atmf provision node configure boot system	AMF
atmf provision node create	AMF
atmf provision node delete	AMF
atmf provision node license-cert	AMF
atmf provision node locate	AMF
atmf recover led-off	AMF
show atmf provision nodes	AMF
aaa login fail-delay	Authentication
auth guest-vlan forward	Authentication
auth-web forward	Authentication
auth-web-server login-url	Authentication
auth-web-server page logo	Authentication
auth-web-server page sub-title	Authentication
auth-web-server page success-message	Authentication
auth-web-server page title	Authentication
auth-web-server page welcome-message	Authentication
auth-web-server ssl	Authentication
show auth	Authentication
show auth diagnostics	Authentication

Command	Feature
show auth sessionstatistics	Authentication
show auth statistics	Authentication
show auth supplicant	Authentication
show auth-web-server page	Authentication
bgp damp-peer-oscillation	BGP
ip dhcp-relay agent-option subscriber-id-auto-mac	DHCP relay
ip tftp source-interface	File management
ipv6 tftp source-interface	File management
mac address-table ageing-time	L2 switching
lacp global-passive-mode enable	Link aggregation
static-channel-group	Link aggregation
linkflap action	Link management
loop-protection action-delay-time	Loop protection
clear ip mroute	Multicast
ip igmp snooping routermode	Multicast
ip igmp snooping routermode address	Multicast
ip igmp trusted	Multicast
platform multicast-ratelimit	Multicast
show ip igmp snooping routermode	Multicast
clear port-security intrusion	Port security
mls qos map premark-dscp	QoS
show mls qos maps premark-dscp	QoS
trust dscp	QoS
snmp-server enable trap	SNMP
snmp-server legacy-ifadminstatus	SNMP
ssh server max-auth-tries	SSH
virtual-ipv6	VRRP

Important Considerations Before Upgrading to this Version

Licensing

From software version 5.4.4-0.4 onwards, AlliedWare Plus software releases need to be licensed for SBx908 and SBx8100 switches.

If you are upgrading to 5.4.5-2.x on your SBx908 or SBx8100 switch, please ensure you have a 5.4.5 license on your switch. To obtain a license, contact your authorized Allied Telesis support center. You will need to provide the MAC addresses of the switches you want to license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 28 and
- "Licensing this Software Version on a Control Card for an SBx8100 Series Switch" on page 30.

Upgrading a VCStack

This version supports VCStack "reboot rolling" upgrades. With the **reboot rolling** command, you can reduce downtime when upgrading a VCStack.

You can use the **reboot rolling** command to upgrade to any 5.4.5-2.x version from 5.4.5-1.x, 5.4.5-0.x or any 5.4.4-x.x version.

You cannot use rolling reboot to upgrade directly to 5.4.5-2.x from 5.4.3-x.x releases. If you wish to use rolling reboot, you must first use it to upgrade from 5.4.3-0.0 to 5.4.4-0.x, then from 5.4.4-0.x to 5.4.5-2.x.

Forming or extending a VCStack

If you create a VCStack from switches that are running different software versions, auto-synchronization ensures that all members will run the same software version when they boot up.

Auto-synchronization is supported between all versions of 5.4.5-2.x, 5.4.5-1.x, 5.4.5-0.x and 5.4.4-2.x or later. It is not supported between 5.4.5-x.x and earlier versions of 5.4.4 (5.4.4-1.x or 5.4.4-0.x).

Before you add a new switch to a stack, make sure the new switch's software version is compatible with the stack's version. If the new switch is running an incompatible version, it cannot join the stack until you have manually upgraded it.

AMF software version compatibility

We strongly recommend that all switches in an AMF network run the same software release.

If this is not possible, switches running version 5.4.5-2.x, 5.4.5-1.x and 5.4.5-0.x are compatible with switches running version 5.4.3-2.6 and later, or any 5.4.4 version.

Upgrading all switches in an AMF network

This version supports upgrades across AMF networks. There are two methods for upgrading firmware on an AMF network:

- Reboot-rolling, which upgrades and reboots each switch in turn
- Distribute firmware, which upgrades each switch, but does not reboot them. This lets you reboot the switches at a minimally-disruptive time.

You can use either of these methods to upgrade to this software version.

You can use these methods to upgrade to this version from 5.4.3-2.6 and later.

In summary, the process for upgrading firmware on an AMF network is:

1. Copy the release .rel files for each switch family to the media location you intend to upgrade from (Flash memory, SD card, USB stick etc).
2. Decide which AMF upgrade method is most suitable.
3. Initiate the AMF network upgrade using the selected method. To do this:
    a. create a working-set of the switches you want to upgrade
    b. enter the command **atmf reboot-rolling <*location*>** or **atmf distribute-firmware <*location*>** where **<*location*>** is the location of the .rel files.
    c. Check the console messages to make sure that all switches are “release ready”. If they are, follow the prompts to perform the upgrade.

ISSU (In-Service Software Upgrade) on SBx8100 with CFC960

ISSU is available on standalone SBx8100 Series switches with dual CFC960 control cards, and on switches using VCStack Plus™ to create a single virtual unit out of two chassis (where each chassis has a pair of CFC960 control cards). ISSU allows you to upgrade the software release running on the CFCs with no disruption to network traffic passing through the chassis.

This minor release cannot be upgraded from any previous release using ISSU.

For each software change on these platforms, the change will take effect as indicated when:

- CFCs upgraded: The change will apply once all CFCs have rebooted and are running the same SW version.
- ISSU Complete: The change will apply once all cards in the system are running the same SW version.

Please refer to the ISSU compatibility matrix below to determine ISSU release compatibility. In the matrix:

- "C" (compatible) indicates that you **can** use ISSU to upgrade from the "FROM" release to the "TO" release.
- "I" (incompatible) indicates that you **cannot** use ISSU to upgrade from the "FROM" release to the "TO" release.

		TO							
	RELEASE	**5.4.5-0.2**	**5.4.5-0.3**	**5.4.5-0.4**	**5.4.5-1.1**	**5.4.5-1.2**	**5.4.5-1.3**	**5.4.5-1.4**	**5.4.5-2.1**
FROM	**5.4.5-0.1**	C	C	I	I	I	I	I	I
	5.4.5-0.2		C	I	I	I	I	I	I
	5.4.5-0.3			I	I	I	I	I	I
	5.4.5-0.4				I	I	I	I	I
	5.4.5-1.1					C	I	I	I
	5.4.5-1.2						I	I	I
	5.4.5-1.3							C	I
	5.4.5-1.4								I
	5.4.5-2.1								

Licensing this Software Version on an SBx908 Switch

Release licenses are applied with the **license certificate** command, then validated with the **show license** or **show license brief** commands. Follow these steps:

- Obtain the MAC address for a switch
- Obtain a release license for a switch
- Apply a release license on a switch
- Confirm release license application

Step 1: Obtain the MAC address for a switch

A release license is tied to the MAC address of the switch.

Switches may have several MAC addresses. Use the **show system mac license** command to show the switch MAC address for release licensing:

```
awplus# show system mac license
MAC address for licensing:
eccd.6d9d.4eed
```

Step 2: Obtain a release license for a switch

Contact your authorized Allied Telesis support center to obtain a release license.

Step 3: Apply a release license on a switch

Use the **license certificate** command to apply a release license to your switch.

Note the license certificate file can be stored on internal flash memory, or an external SD card, or on a server accessible by the TFTP, SCP or HTTP protocols.

Entering a valid release license changes the console message displayed about licensing:

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus#license certificate demo1.csv
A restart of affected modules may be required.
Would you like to continue? (y/n): y
11:58:14 awplus IMI[1696]: SFL: The current software is licensed. Exiting
unlicensed mode.

Stack member 1 installed 1 license

1 license installed.
```

Step 4: Confirm release license application

On a stand-alone switch, use the commands **show license** or **show license brief** to confirm release license application.

On a stacked switch, use the command **show license member** or **show license brief member** to confirm release license application.

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus switches:

```
awplus# show license
OEM Territory : ATI USA
Software Licenses
------------------------------------------------------------------------
Index                          : 1
License name                   : Base License
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Mar-2015
License expiry date            : N/A
Features included              : EPSR-MASTER, IPv6Basic, MLDSnoop, OSPF-64,
                                 RADIUS-100, RIP, VRRP

Index                          : 2
License name                   : 5.4.5-rl
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Mar-2015
License expiry date            : N/A
Release                        : 5.4.5
```

Licensing this Software Version on a Control Card for an SBx8100 Series Switch

Release licenses are applied with the **license certificate** command, then validated with the **show license** or **show license brief** commands. Follow these steps:

- Obtain the MAC address for a control card
- Obtain a release license for a control card
- Apply a release license on a control card
- Confirm release license application

If your control card is in a stacked chassis, you do not need to perform these steps on each chassis in the stack, only on the stack master.

If your license certificate contains release licenses for each control card present in a stacked chassis, entering the **license certificate** command on the stack master will automatically apply the release licenses to all the control cards within the stack.

Step 1: Obtain the MAC address for a control card

A release license is tied to the control card MAC address in a chassis.

Chassis may have several MAC addresses. Use the **show system mac license** command to show the control card MAC address for release licensing. Note the MAC addresses for each control card in the chassis. The chassis MAC address is not used for release licensing. Use the card MAC address for release licensing.

```
awplus#show system mac license

MAC address for licensing:


Card                MAC Address
-----------------------------------
1.5                 eccd.6d9e.3312
1.6                 eccd.6db3.58e7

Chassis MAC Address eccd.6d7b.3bc2
```

Step 2: Obtain a release license for a control card

Contact your authorized Allied Telesis support center to obtain a release license.

Step 3: Apply a release license on a control card

Use the **license certificate** command to apply a release license to each control card installed in your chassis or stack.

Note the license certificate file can be stored on internal flash memory, a USB drive, or on a server accessible by the TFTP, SCP or HTTP protocols.

Entering a valid release license changes the console message displayed about licensing:

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus# license certificate demo1.csv
A restart of affected modules may be required.
Would you like to continue? (y/n): y
11:58:14 awplus IMI[1696]: SFL: The current software is licensed. Exiting
unlicensed mode.

Stack member 1 installed 1 license

1 license installed.
```

Step 4: Confirm release license application

On a stand-alone chassis, use the commands **show license** or **show license brief** to confirm release license application.

On a stacked chassis, use the command **show license member** or **show license brief member** to confirm release license application.

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus chassis:

```
awplus# show license
OEM Territory : ATI USA
Software Licenses
------------------------------------------------------------------------
Index                          : 1
License name                   : Base License
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Mar-2015
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                                 Virtual-MAC, VRRP

Index                          : 2
License name                   : 5.4.5-rl
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Mar-2015
License expiry date            : N/A
Release                        : 5.4.5
```

Installing this Software Version

Caution: Software versions 5.4.5-x.x require a release license for the SBx908 and SBx8100 switches. Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 28 and
- "Licensing this Software Version on a Control Card for an SBx8100 Series Switch" on page 30.

To install and enable this software version, use the following steps:

1. Copy the software version file (.rel) onto your TFTP server.

2. If necessary, delete or move files to create space in the switch's Flash memory for the new file. To see the memory usage, use the command:

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

   ```
   awplus# del <filename>
   ```

   You cannot delete the current boot file.

3. Copy the new release from your TFTP server onto the switch.

   ```
   awplus# copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.

4. Move from Privileged Exec mode to Global Configuration mode, using:

   ```
   awplus# configure terminal
   ```

   Then set the switch to reboot with the new software version. For example, for 5.4.5-2.1, use one of the following commands:

Switch	Command
x210 series	`awplus(config)# boot system x210-5.4.5-2.1.rel`
x230 series	`awplus(config)# boot system x230-5.4.5-2.1.rel`
x310 series	`awplus(config)# boot system x310-5.4.5-2.1.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.4.5-2.1.rel`
x510 series	`awplus(config)# boot system x510-5.4.5-2.1.rel`
x610 series	`awplus(config)# boot system x610-5.4.5-2.1.rel`
SBx908	`awplus(config)# boot system SBx908-5.4.5-2.1.rel`
x930 series	`awplus(config)# boot system SBx930-5.4.5-2.1.rel`
SBx8100 with CFC400	`awplus(config)# boot system SBx81CFC400-5.4.5-2.1.rel`
SBx8100 with CFC960	`awplus(config)# boot system SBx81CFC960-5.4.5-2.1.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.4.5-2.1.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.4.5-2.1.rel`

5. Return to Privileged Exec mode and check the boot settings, using:

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

6. Reboot using the new software version.

```
awplus# reload
```

Installing the GUI

This section describes how to install and set up the AlliedWare Plus GUI using an SD card, a USB storage device, or a TFTP server. The version number in the GUI Java applet filename (**.jar)** gives the earliest version of the software file (**.rel**) that the GUI can operate with.

To install and run the AlliedWare Plus GUI requires the following system products and setup:

- PC Platform:
  Windows XP SP2 and up / Windows Vista SP1 and up
- Browser: (must support Java Runtime Environment (JRE) version 6)
  Microsoft Internet Explorer 7.0 and up / Mozilla Firefox 2.0 and up

To install the GUI on your switch, use the following steps:

1. Copy to the GUI Java applet file (**.jar** extension) onto your TFTP server, SD card or USB storage device.

2. Connect to the switch's management port, then log into the switch.

3. If necessary, delete or move files to create space in the switch's Flash memory for the new file.

   To see the memory usage, use the command:

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

   ```
   awplus# del <filename>
   ```

   You cannot delete the current boot file.

4. Assign an IP address for connecting to the GUI. Use the commands:

   ```
   awplus# configure terminal
   awplus(config)# interface vlan1
   awplus(config-if)#ip address <address>/<prefix-length>
   ```

   Where <*address*> is the IP address that you will subsequently browse to when you connect to the GUI Java applet. For example, to give the switch an IP address of 192.168.2.6, with a subnet mask of 255.255.255.0, use the command:

   ```
   awplus(config-if)# ip address 192.168.2.6/24
   ```

5. If required, configure a default gateway for the switch.

   ```
   awplus(config-if)# exit
   awplus(config)# ip route 0.0.0.0/0 <gateway-address>
   ```

   Where <*gateway-address*> is the IP address for your gateway device. You do not need to define a default gateway if you browse to the switch from within its own subnet.

6. Copy the GUI file onto your switch from the TFTP server, SD card, or USB storage device.

   TFTP server: Use the command:

   ```
   awplus# copy tftp://<server-address>/<filename.jar> flash:/
   ```

   SD card: use the command:

   ```
   awplus# copy card:/<filename.jar> flash:/
   ```

   USB storage device: use the command:

   ```
   awplus# copy usb:/<filename.jar> flash:/
   ```

   where <*server-address*> is the IP address of the TFTP server, and where <*filename.jar*> is the filename of the GUI Java applet.

7. Ensure the HTTP service is enabled on your switch. Use the commands:

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

   The HTTP service needs to be enabled on the switch before it accepts connections from a web browser. The HTTP service is enabled by default. However, if the HTTP has been disabled then you must enable the HTTP service again.

8. Create a user account for logging into the GUI.

   ```
   awplus(config)# username <username> privilege 15 password
                   <password>
   ```

   You can create multiple users to log into the GUI. For information about the **username** command, see the AlliedWare Plus Command Reference.

9. Start the Java Control Panel, to enable Java within a browser

   On your PC, start the Java Control Panel by opening the Windows Control Panel from the Windows Start menu. Then enter Java Control Panel in the search field to display and open the Java Control Panel.

   Next, click on the 'Security' tab. Ensure the 'Enable Java content in the browser' checkbox is selected on this tab.

10. Enter the URL in the Java Control Panel Exception Site List

    Click on the 'Edit Site List' button in the Java Control Panel dialog Security tab to enter a URL in the Exception Site List dialog. In the 'Exception Site List' dialog, enter the IP address you configured in Step 4, with a http:// prefix.

    After entering the URL click the Add button then click OK.

11. Log into the GUI.

    Start a browser and enter the switch's IP address. The GUI starts up and displays a login screen. Log in with the username and password specified in the previous step.

Technical Guide

Virtual AMF Appliance (VAA) Installation and Technical Guidelines

Introduction

Virtual AMF Appliance (VAA) is a virtualized implementation of Allied Telesis Management Framework (AMF) that allows you to install AMF Masters and/or Controllers on a server. Having AMF Masters and Controllers available as virtual machines adds flexibility to the options available for AMF network designs.

What is AMF virtualization?

AMF is a suite of features that combine to simplify network management across all supported network equipment from the core to the edge.

AMF provides simplified device recovery and firmware upgrade management. The primary function of AMF is to reduce the management and maintenance overhead on a network, while improving on responsiveness and handling of equipment failures within the network.

With a non-virtual situation, the AMF nodes that manage the network need to reside on Allied Telesis routers or switches. **Virtualization** of AMF removes this limitation and allows the management to be done from a server-hosted virtual machine which is running a special version of AlliedWare Plus dedicated to AMF.

This gives greater flexibility for where the AMF management devices can physically reside as they can be in remote locations away from other parts of the network.
AMF virtualisation has many other benefits common to virtual machines, such as excellent disaster recovery and rapid deployment.

The AlliedWare Plus software for the virtual machine is known as the Virtual AMF Appliance, or VAA. The VAA is an ISO image that is loaded onto the virtual machine at boot up time. Once the VAA has loaded, the familiar AlliedWare Plus command-line interface (CLI) is available and network engineers can then use this CLI to configure and manage the virtual AMF Master Controller.

Audience for this guide

This guide is intended for computer system administrators and network engineers. Moderate expertise in the field of hypervisors and virtual machine (VM) creation and configuration is highly recommended, at least to the level where the installer already knows how to create virtual machines.

This guide describes how to create a virtual machine for AMF Virtualisation. For further documentation of AMF configuration, including examples and command references, please see the links provided in the "Related documents" section below.

Related documents

The following documents give more information about AMF:

- AMF Feature Overview and Configuration Guide
- AMF Solution - reducing the cost and complexity of enterprise network management
- AMF Solution - a simple powerful, cost-effective SDN solution

These documents are available from the links above or on our website at alliedtelesis.com

Contents

How do I obtain a VAA and Configure it?

To obtain and configure a VAA you need to:

Step 1. **Purchase a support agreement and license.**

- Purchasing VAA is explained more in the section: "Purchasing a VAA License" on page 39.

Step 2. **Install a Hypervisor, the Operating System that Virtual Machines run on.**

- Prerequisites and installation of Hypervisor is described in the section: "Prerequisites" on page 39

Step 3. **Create and configure the Virtual Machine on a Hypervisor.**

- Configuring a virtual machine is detailed in the section: "Configuring a Virtual Machine Using VMware vSphere" on page 40

Purchasing a VAA License

Licensing for the VAA is subscription-based. The type of license will depend on how extensive the network is that you need to manage.

Network engineers in charge of managing AMF need to consider how many:

- AMF Masters throughout the network are linked to an AMF Controller
- nodes in each AMF Area are linked to the area's AMF Master.

Each VAA acting as an AMF Controller or AMF Master will need it's own unique license file that is based on the unique serial number of the VAA.

Please contact Allied Telesis customer support to establish licenses options.

Planning an AMF network is beyond the scope of this installation guide. Please refer to the AMF Feature Overview and Configuration Guide for more detail.

Providing the Hypervisor that the VA Runs On

Prerequisites

Allied Telesis' VAA supports the VMware hypervisor **VMware vSphere v6.0** or above, to create and configure virtual machines (VMs) and manage virtual infrastructures.

This guide assumes that the customer knows either how to install VMware vSphere, or already has a VMware vSphere host ready to install virtual machines for VAA.

Physical Ethernet ports

One Ethernet port on the host machine will be configured for access from the VM Client. The addition of network interface cards (NICs) for VAA networking is recommended.

Hypervisor clock

Virtual machines are synced to the main hypervisor clock by default. As the VAA licenses are time-based, it is critical that the hypervisor clock is synchronized to UTC.

Memory and disk space

Each virtual machine for a VAA has a minimum set of hardware requirements. This implicates how large the physical RAM and physical hard drive storage space needs to be on the host machine.

For each VM, Allied Telesis recommends that you allocate:

- 1GB physical disk space for storage
- 1GB physical RAM

Configuring a Virtual Machine Using VMware vSphere

Uploading a Virtual AMF Appliance ISO image

Before you begin, you will first need to upload a VAA ISO image to a data store on your ESXi server. For the complete set of instructions on uploading a VAA ISO image, please refer to the VMware vSphere 6.0 Documentation Centre.

Creating a VAA virtual machine

Using **VMware vSphere client 6.0**, follow these steps:

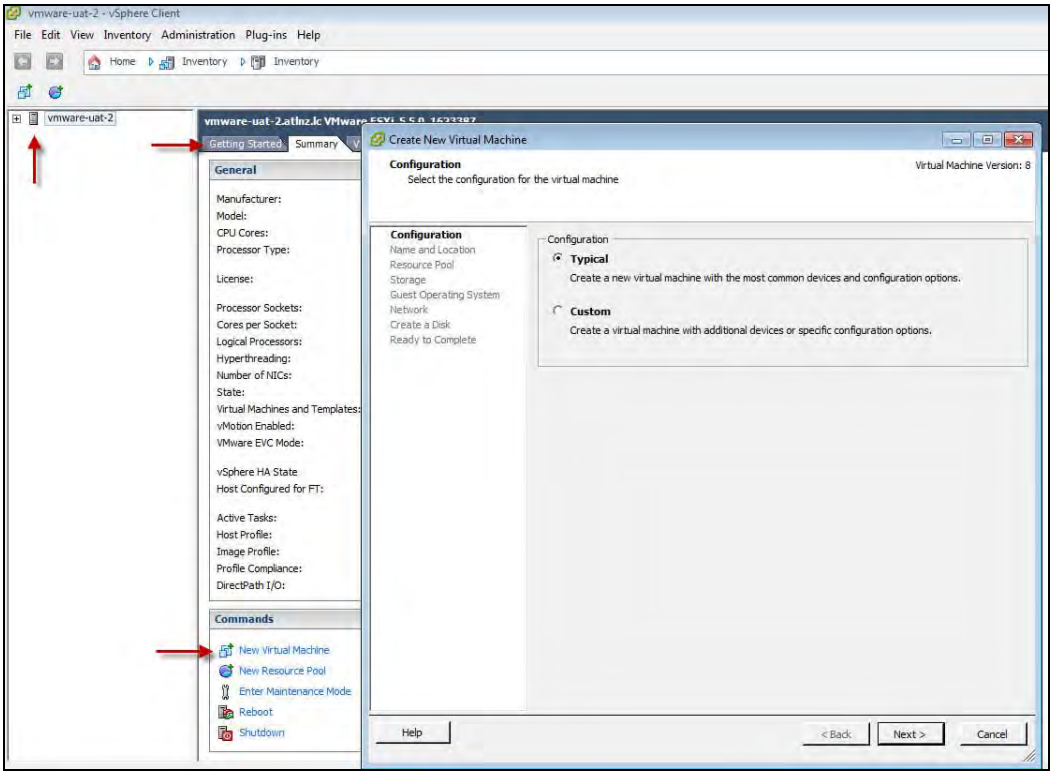
1. Select your **ESXi server** in the list on the left.
2. Select the **Getting Started** tab.
3. Click on the **Create New Virtual Machine** link.

This opens a configuration wizard, that guides you through the following process:

Configuration

In the **Configuration** window:

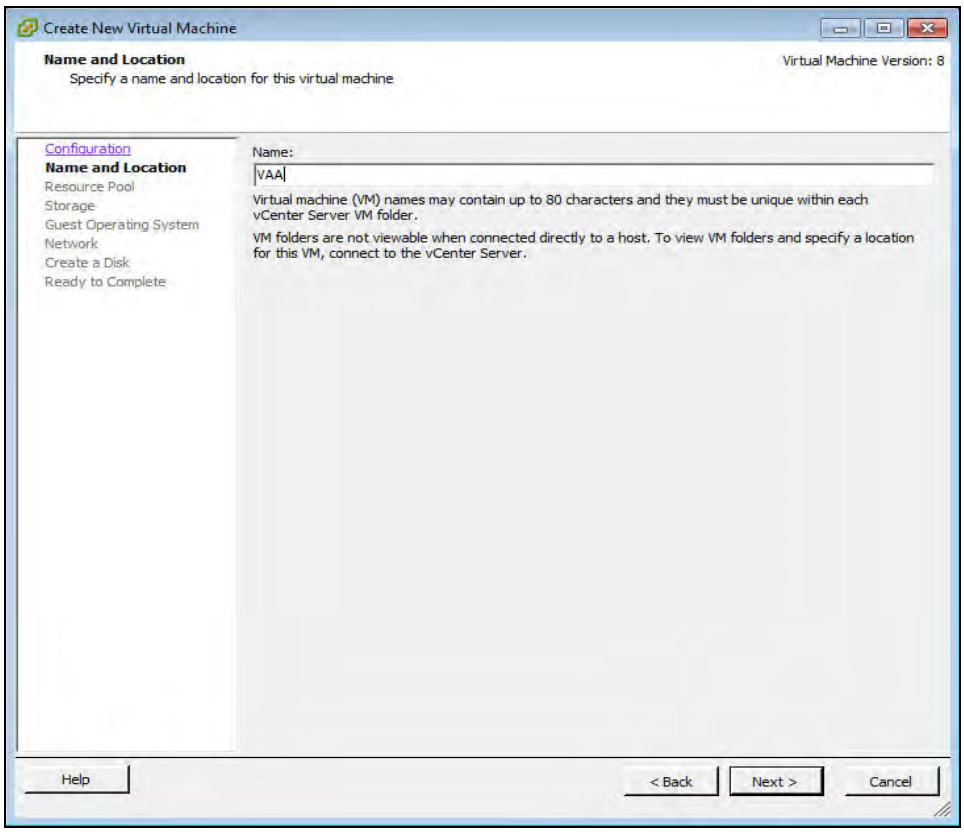
- Select **Typical**
- Click **Next >**



Name and Location

In the **Name and Location** window:

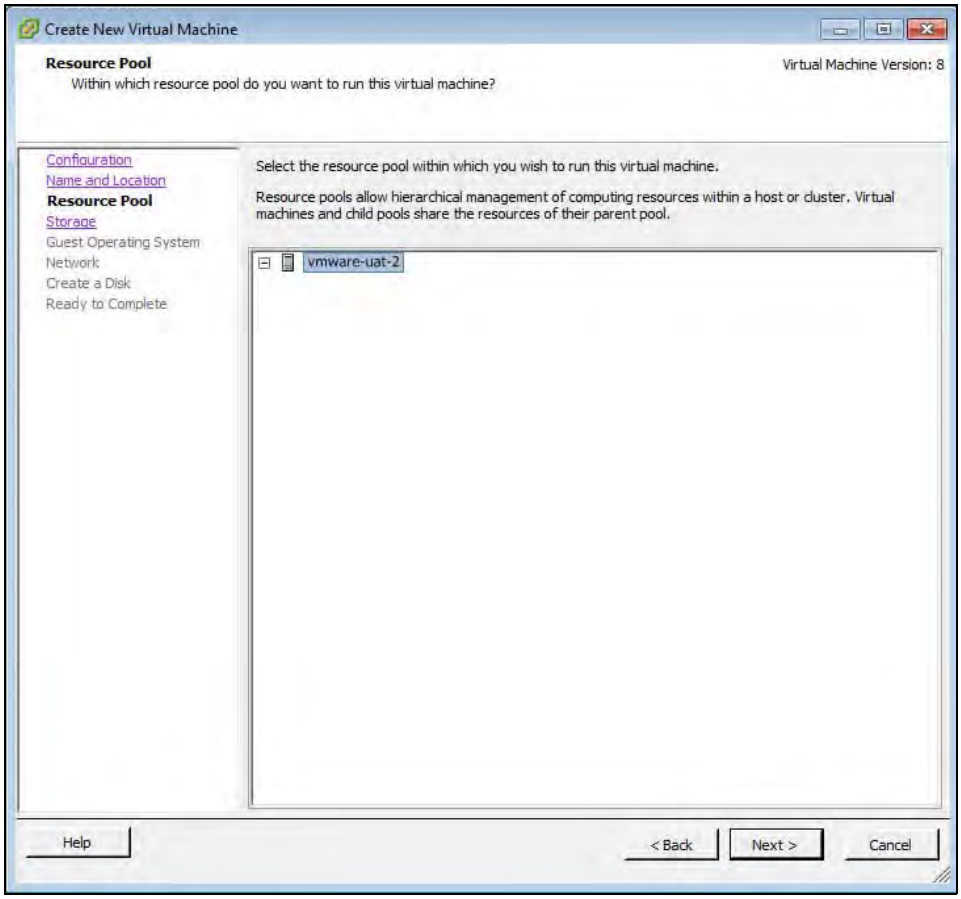
- Enter a **Name** of your choosing.
- Click **Next >**



Resource Pool

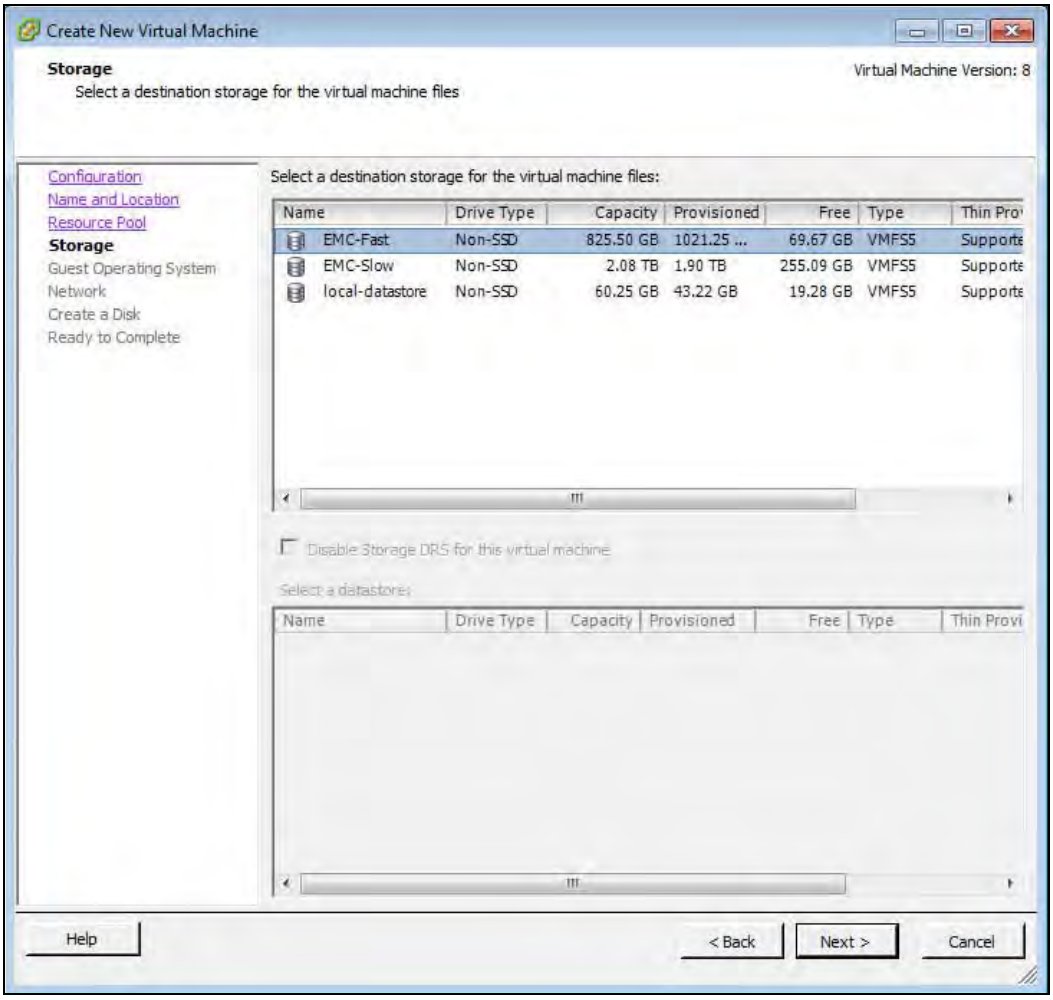
In the **Resource Pool** window:

- Select the **HostGroup** to run on.
- Click **Next>**



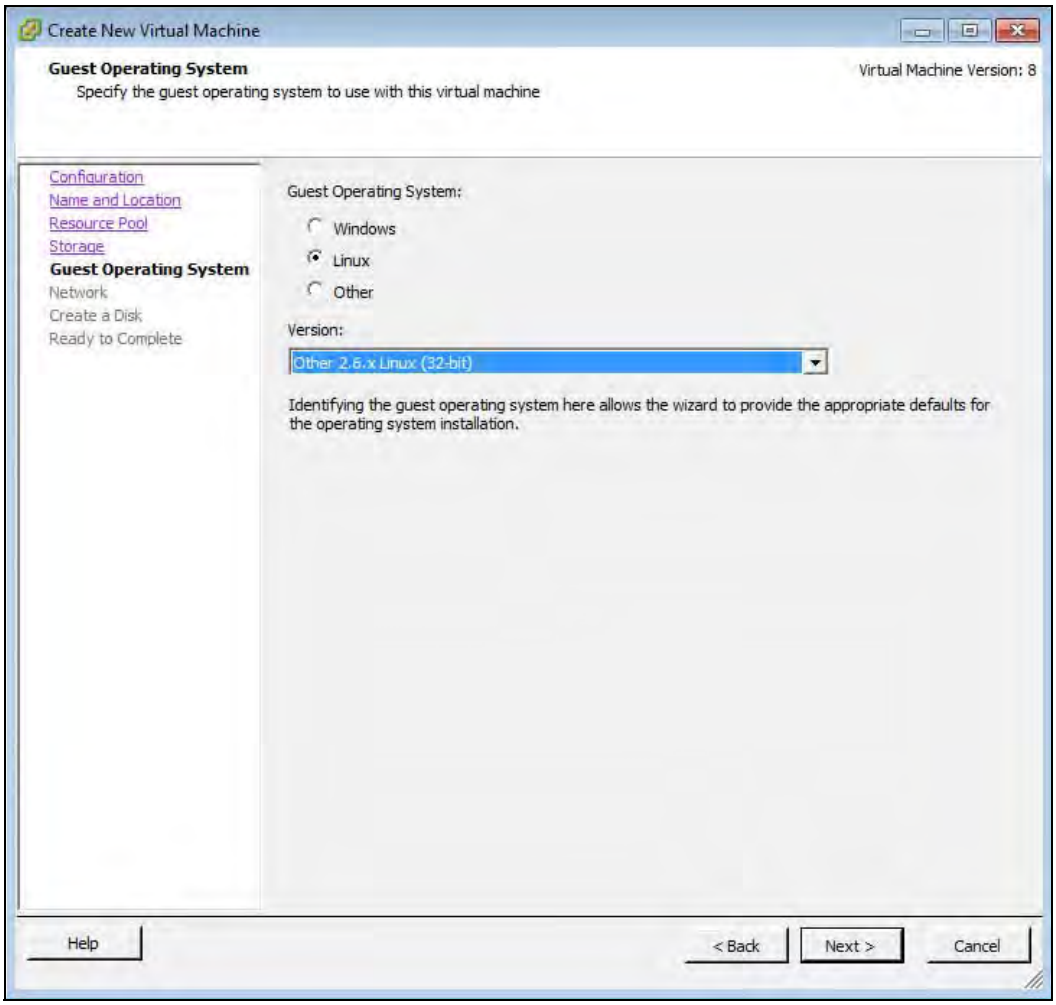
Storage

Select an appropriate destination data store for the virtual machine files. The appropriate choice depends on your specific ESXi configuration.



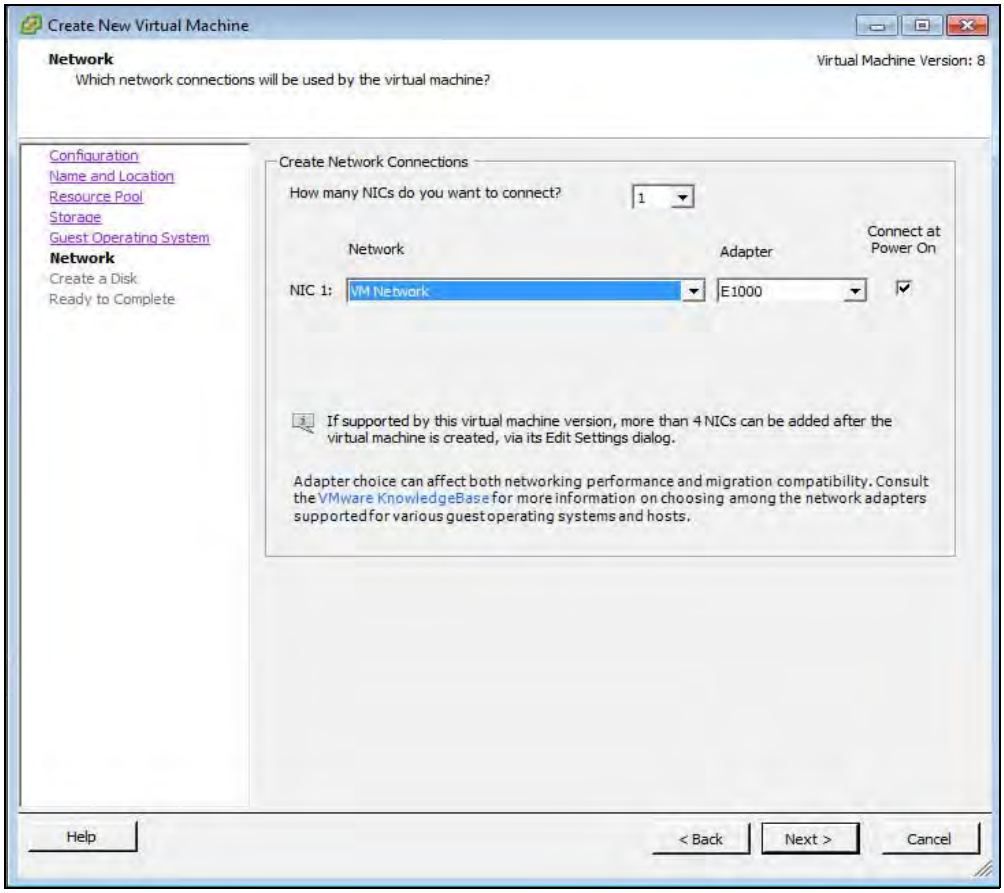
- Click **Next >**

Guest Operating System



- Select the **Linux** radio button.
- Select **Version** Other 3.x Linux (32-bit). If this version is not available, such as on earlier versions of vSphere, you should select Other 2.6x Linux (32-bit).
- Click **Next >**

Network



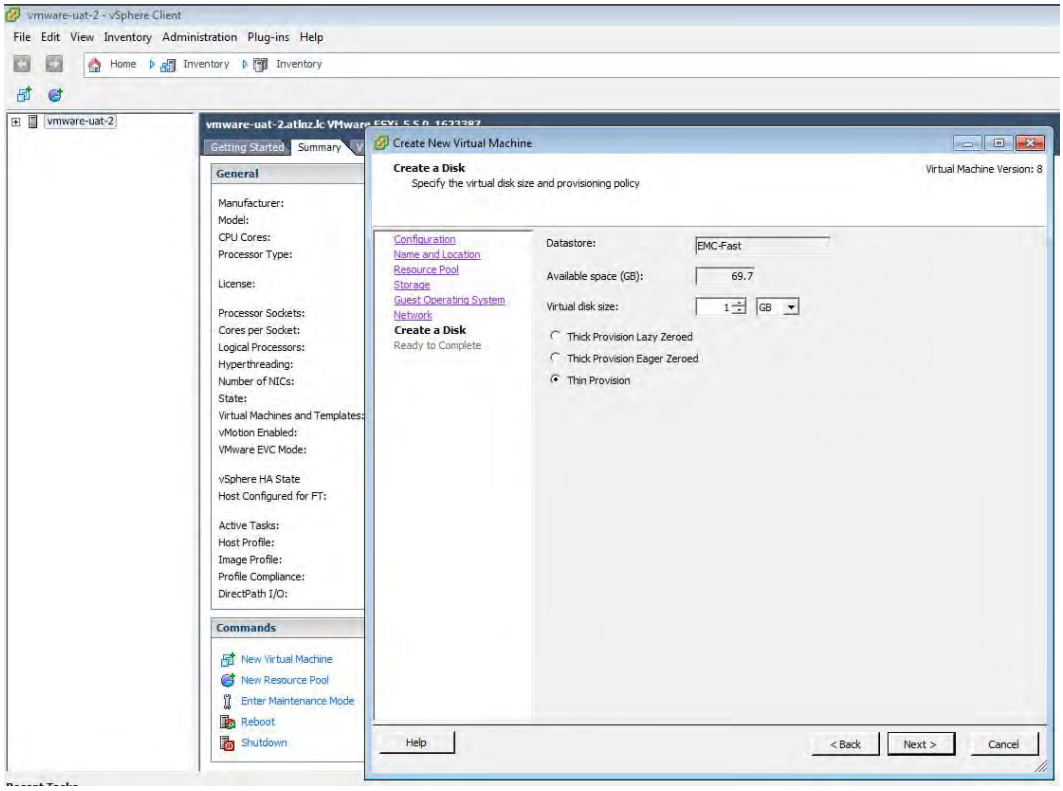
- Specify the number of interfaces the VAA will require, one interface for every VMware network you need to connect to.
- For each NIC select the appropriate network.
- **Adapter** type can be E1000 or VMXNET3, with VMXNET3 possibly offering better performance.
    - For information on the E1000 or VMXNET3, please see the VMware Knowledge Base article: Choosing a network adapter for your virtual machine (1001805).
- Ensure **Connect at Power On** is ticked.
- Click **Next >**

VLAN configuration

It is recommended that you create an AMF specific network using either a VLAN, or a dedicated NIC.

If you wish to use VLAN sub-interfaces in the Virtual AMF Appliance, you will need to set "VLAN ID: All (4095)" in the VMware port group settings. This in effect tags a port to allow all VLAN IDs to pass through it.

Create a Disk

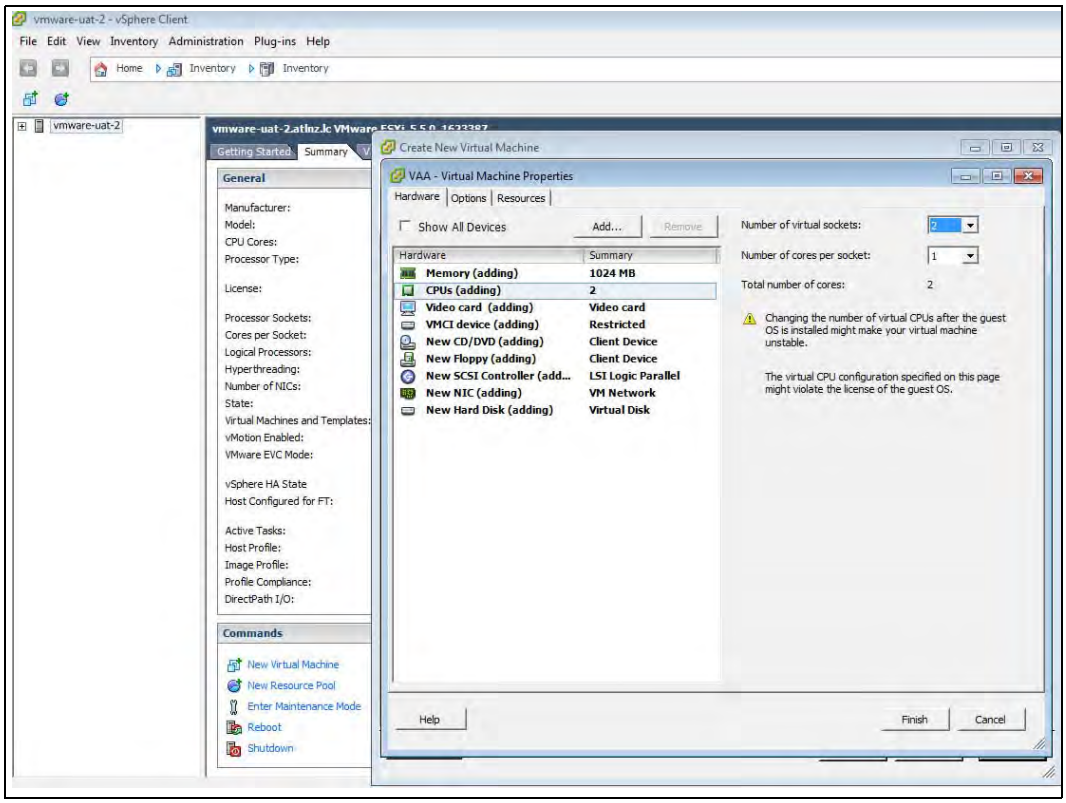


- Virtual disk size must be between 1GB and 2TB, **32GB** is recommended.
- Click **Next >**

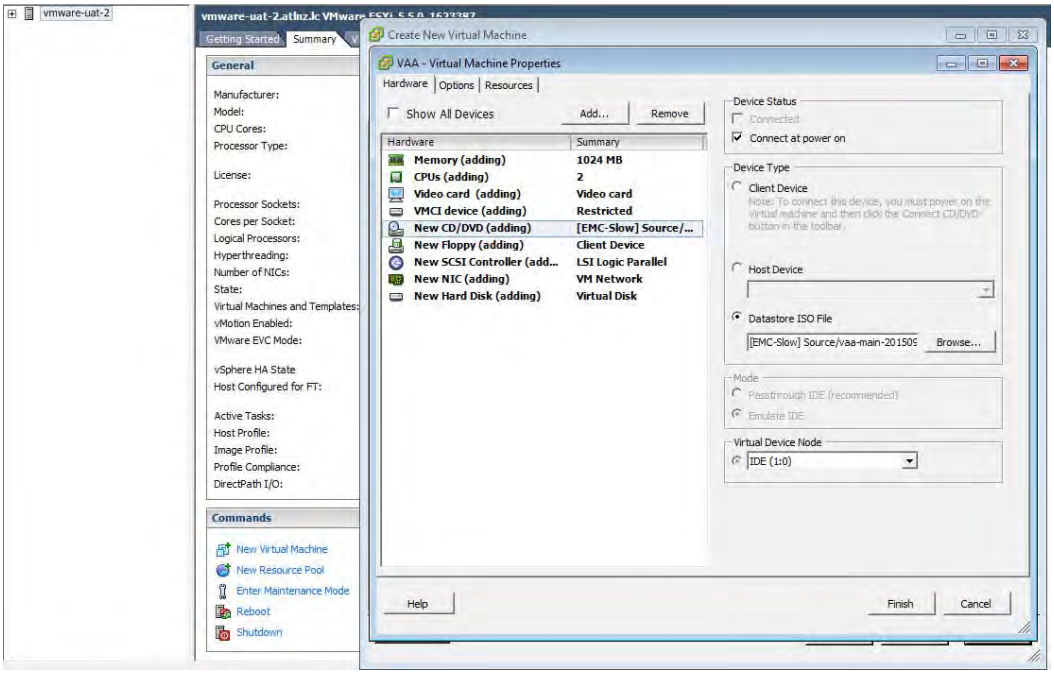
Ready to Complete

- Double check the virtual-machine configuration is correct.
- Tick the **Edit virtual machine settings before completion** check-box.
- Click **Finish**

Virtual Machine Properties



- Select the **Memory** item and set memory to **1024 MB**
- Select the **CPUs** item and set the number of CPUs to **2**
- Select the **CD/DVD** Drive 1 item.



- Ensure that **Connect at power on** check-box is ticked.
- Select the **Datastore ISO File** radio button.
- **Browse** for the VAA ISO image you uploaded earlier.
- Click **Finish**.

Operating a VAA

Start a VAA

In the vSphere Client:

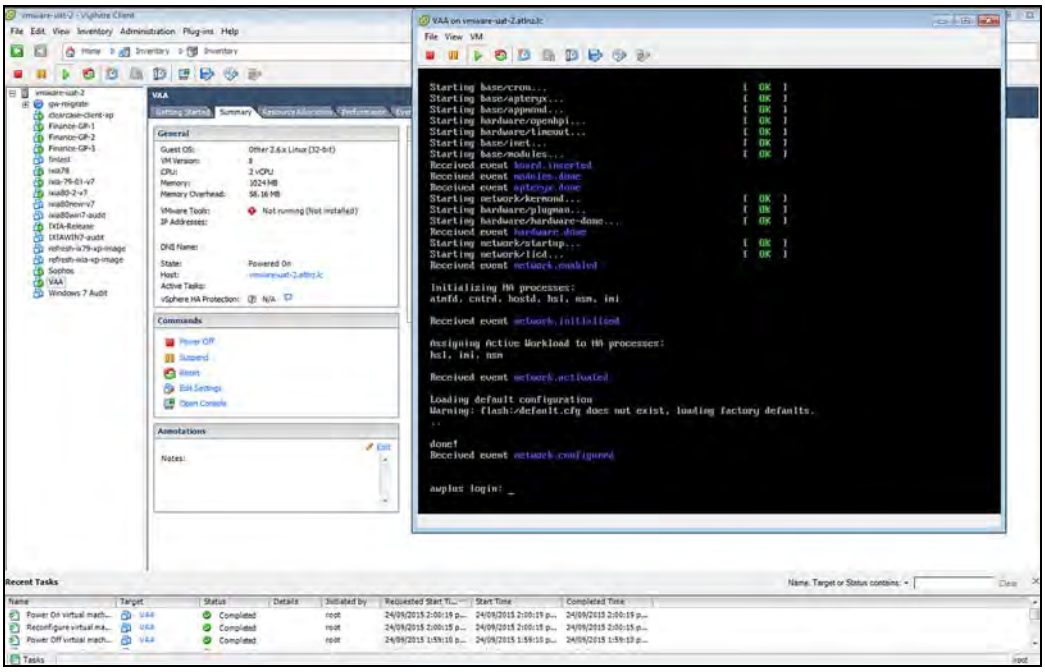
- Select **VAA** from the inventory list on the left.
- **Right click** the virtual appliance, opening the context menu.
- In the **Commands** sub-menu, click **Power On**.

View Console

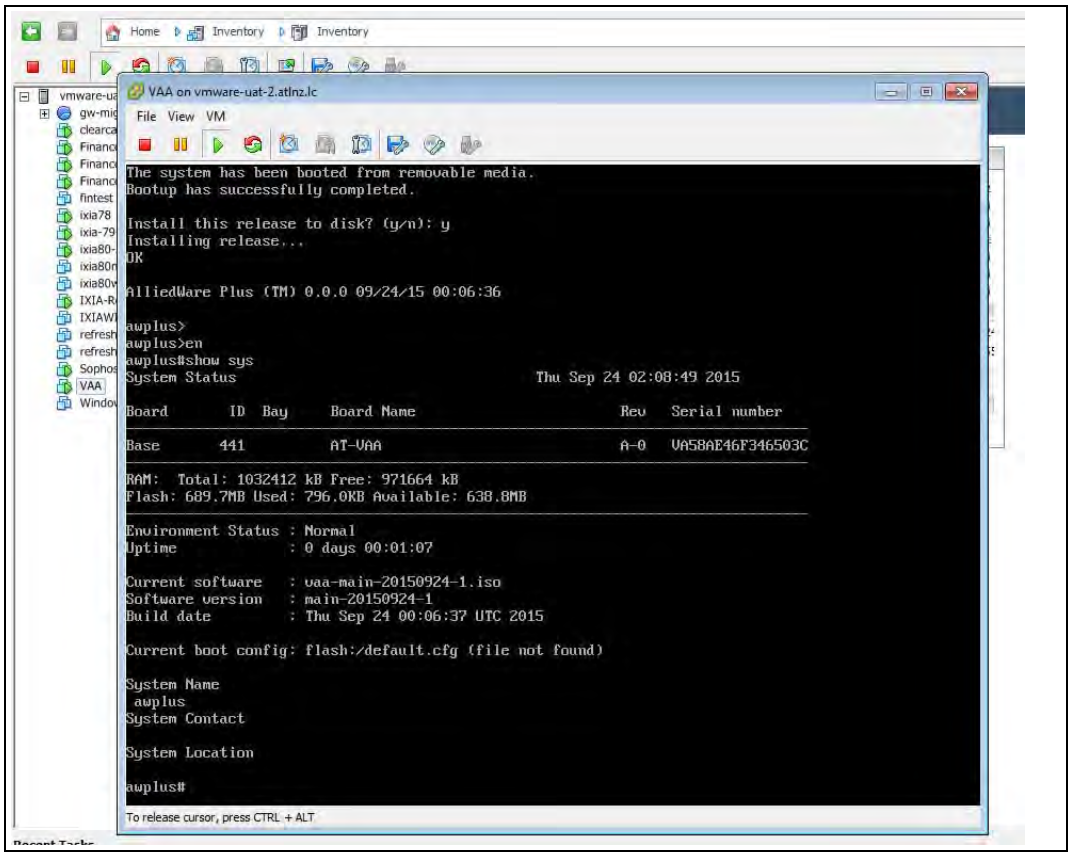
- Select **VAA** from the inventory list on the left side of vSphere Client.
- **Right click** the virtual appliance, opening the context menu.
- Click **Open Console**

Install

- The install login prompt displays: *Do you want to install this release to disc?*
- Type in **Yes** to Install.



The following screenshot shows the first run.



Stop a VAA

- Select **VAA** from the inventory list on the left side of vSphere Client.
- **Right click** the virtual appliance, opening the context menu.
- In the **Power** sub-menu, click **Power Off**.

Upgrading and Downgrading the Software of a VAA

First upload the new VAA ISO image to a data store, as detailed in "Configuring a Virtual Machine Using VMware vSphere" on page 40. To upgrade or downgrade the current installed image, you will need to change the current.iso software image in the virtual-machine configuration, then reboot the virtual-machine.

To change the current .iso software image:

- Power off the virtual-machine you wish to upgrade/downgrade.
- Edit the settings of the virtual-machine.
- Select CD/DVD Drive 1 item
- Ensure that **Connect at power on** check-box is ticked.
- Select the **Datastore ISO File** radio button.
- **Browse** for the desired VAA iso image.

Now start the virtual machine, during boot you will see a menu that looks like this:

```
Alliedware+
Boot from CD
```

- Select the **Boot from CD** option.

Note: You will only have 5 seconds to select "Boot from CD" before the boot continues with the previously installed release.

This will boot using the new .iso software image, and next time you login using the console you will be presented with the "*Install this release to disk? (y/n)*" option.

Migrate a running VAA to a different physical host

If you need to take a host offline for maintenance, you can move the virtual machine to another host. Migration with vMotion™ allows virtual machine processes to continue working throughout a migration.

Requirements: Both physical hosts must have:

- the same network configuration.
- access to the same network(s) to which the interfaces of the VAA are mapped.
- access to the data-store that the VAA uses.

Refer to the VMotion documentation for instructions on how to migrate the virtual machine.

Accessing the CLI of the VAA

When the VAA is powered on, and is being viewed via the console, and has completed its bootup sequence, it will offer a login prompt: Login as *manager/friend*.

You now have access to the familiar AlliedWare Plus CLI, and can configure the AMF Master/Controller as described in the AMF Feature Overview and Configuration Guide.

License installation for AMF

License files are a binary file known as a license Response file. This is a binary-encoded file that defines the number and type of nodes allowed throughout the AMF network. To install a license Response file, the file must be transferred to the VAA and visible on the virtual Flash.

Step 1. On the VAA CLI, ensure the license Response file exists in Flash.

```
London_Mast#dir
     16384 drwx Oct 28 2017 01:55:02  lost+found/
       907 -rw- Nov  5 2015 15:20:47  Mast20-response.bin
       826 -rw- Nov  5 2015 15:18:16  default.cfg
       270 -rw- Nov  5 2015 13:42:35  reboot.log
      4096 drwx Oct 30 2015 03:00:00  atmf/
```

Step 2. Enter the license command on the CLI, giving the license response bin file as the parameter.

- For example, if the response file is called "Master20-response.bin"

```
London_Mast#license update Mast20-response.bin
London_Mast#15:21:15 London_Mast ATMF[667]: The number of nodes allowed
on this ATMF network is 20
```

Step 3. Confirm the license has been applied.

```
London_Mast#show license external
Licensed features:
London_Mast#license update Mast20-response.bin
London_Mast#15:21:15 London_Mast ATMF[667]: The number of nodes allowed
on this ATMF network is 20

London_Mast#show license external
Licensed features:

AMF Master
       Start date                    : 05-Nov-2015 12:00AM
       Expiry date                   : 03-Nov-2016 11:59PM
       Total Nodes Allowed           : 20
```

AMF license expiry

AMF licenses on VAA are time based. Warnings of a pending license expiry will be displayed in the log at the following times: 28 days, 21 days, 14 days, 7 days and 1 day prior to a license expiring. Users can set up appropriate syslog monitoring to look for these messages.

An expiration date of '0' means the license is permanent and will not expire.

Technical Guide

Active Fiber Monitoring Feature Overview and Configuration Guide

Key concepts

The active fiber monitoring feature monitors fiber ports to see if the received optical power drops below a configurable baseline by a threshold amount. This may indicate physical bending of the fibre cable, which could arise when there is a physical intrusion. If this happens, the device can perform a configurable action.

Configuring active fiber monitoring

Step 1: Enable active fiber monitoring

To configure a port to monitor received power at the default intervals and sensitivity, use the commands:

```
awplus(config)# interface port1.0.1
awplus(config-if)# fiber-monitoring enable
```

By default, the interval is once every 5 seconds, the baseline value is calculated from the average of the last 12 readings, and the action is to generate a log message if the received power drops below the threshold by more than 1dB.

Step 2: Configure actions

By default, the device will generate a log message when the alarm threshold is exceeded in either direction for a port. Additional actions may be configured.

To send a notification to the configured SNMP trap host when the alarm threshold is crossed, use the commands:

```
awplus(config)# interface port1.0.1
awplus(config-if)# fiber-monitoring action trap
```

AlliedWare Plus™ OPERATING SYSTEM

To shut down the port when the alarm threshold is crossed, use the commands:

```
awplus(config)# interface port1.0.1
awplus(config-if)# fiber-monitoring action shutdown
```

To both send a trap and shutdown the port, use the commands:

```
awplus(config)# interface port1.0.1
awplus(config-if)# fiber-monitoring action trap shutdown
```

The actions can be configured in the same command or in separate commands and in any order.

Step 3: Configure polling interval

The interval for polling received optical power is 5s by default, and can be configured from 2 - 60s. To poll the received power every 2 seconds instead of every 5 seconds (configurable from 2-60), use the commands:

```
awplus(config)# interface port1.0.1
awplus(config-if)# fiber-monitoring interval 2
```

Step 4: To configure how the baseline is calculated

To calculate the baseline values based on the average on the last 30 readings instead of the last 12 readings (configurable from 12-150), use the commands:

```
awplus(config)# awplus(config)# interface port1.0.1
awplus(config-if)# fiber-monitoring baseline average 30
```

Note: Setting a **fixed value is not recommended** because gradual change over time caused by temperature fluctuations, etc. could lead to unnecessary alarms.

However, if you decide to use a fixed baseline value (e.g. with a value of 1000) rather than calculating an average, you can set it to a value in the range 1-65535), using the commands:

```
awplus(config)# interface port1.0.1
awplus(config-if)# fiber-monitoring baseline fixed 1000
```

Step 5: Configure sensitivity

To configure the sensitivity of the alarm threshold. (A value that is too sensitive could cause unnecessary alarms).

```
awplus(config)# interface port1.0.1
awplus(config-if)# fiber-monitoring sensitivity high
```

The sensitivity can be configured as a dB value (effectively a percentage change in power) or a fixed value and there are a number of pre-defined options. We do not recommend setting sensitivity to**highest** for multi-mode SFPs and **high** should be used with caution. The values indicate the difference from the baseline value.

Table 1: Configurable values for optical power sensitivity

CONFIG VALUE	DB	FIXED (0.0001MW)	COMMENTS
low	2dB	-	
medium	1dB	-	default value
high	0.5dB	25	(whichever is larger)
highest	-	25	
fixed 50	-	50	configurable from 25-65535
relative 0.75	0.75dB	-	configurable from 0.00-10.00 dB

Step 6: Review configuration and status

To display the configuration and current status of active fiber monitoring, use the command:

```
awplus# show system fiber-monitoring
```

```
Fiber Monitoring Status
  Reading units 0.0001mW

Stack member 1:

Interface port1.0.1
Status:           enabled
Supported:        Supported pluggable
Debugging:        disabled
Interval:         2 seconds
Sensitivity:      1.00dB
Baseline type:    average of last 35 values greater than 50
Status:
 Baseline value:   496
 Alarm threshold:  393
 Alarm:            no
 Last 12 Readings: 498 498 498 498 498 498 498 498 498 498 498 498
 Minimum reading: 486
 Maximum reading: 498
```

Table 2: Parameters in the output from **show system fiber-monitoring**

PARAMETER	Description
Reading units	The units for optical power readings in the rest of the display, e.g. 0.0001mW.
Status	Whether active fiber monitoring is enabled or disabled for this port.
Supported	Whether the pluggable inserted in this port supports active fiber monitoring.
Debugging	Whether debugging of active fiber monitoring is enabled or disabled for this port.
Interval	The configured interval between readings of optical power on this port.

Table 2: Parameters in the output from **show system fiber-monitoring**

PARAMETER	Description
Sensitivity	The configured sensitivity threshold for optical power changes on this port.
Baseline type	How the baseline optical power level is calculated: either the average of the specified number of previous readings or a specified fixed value in 0.0001mW.
Status	Current values for the following parameters.
Baseline value	The baseline value, calculated according to the configured baseline method, in 0.0001mW.
Alarm threshold	The current threshold for a change in optical power, calculated according to the configured sensitivity method, that will result in action.
Alarm	Whether the optical power at the most recent reading has exceeded the threshold.
Last 12 readings	The last 12 optical power values measured, in 0.0001mW, with oldest value first.
Minimum reading	The lowest optical power reading since the fiber pluggable was last inserted, or since active fiber monitoring was last enabled on the port.
Maximum reading	The highest optical power reading since the fiber pluggable was last inserted, or since active fiber monitoring was last enabled on the port.

Step 7: View optical power readings as they happen

Debugging can be enabled to show each optical power reading as it happens. To enable debugging for an interface, use the commands:

```
awplus# terminal monitor
awplus# debug fiber-monitoring interface port2.0.1
```

Example console output:

```
% Warning: Console logging enabled
awplus#01:42:50 awplus Pluggable[522]: Fiber-monitor port2.0.1:
Channel:1 Reading:1748 Baseline:1708 Threshold:1356
01:42:52 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1
Reading:1717 Baseline:1709 Threshold:1357
01:42:54 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1
Reading:1780 Baseline:1709 Threshold:1357
01:42:56 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1
Reading:1685 Baseline:1710 Threshold:1358
01:42:58 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1
Reading:1701 Baseline:1710 Threshold:1358
```

Disabling active fiber monitoring

Step 1: Disable active fibre monitoring

To disable fiber-monitoring on a port, use the commands:

```
awplus# interface port1.0.1
awplus(config-if)# no fiber-monitoring enable
```

The latest state information will be kept, and will still be available in **show fiber-monitoring** command.

Step 2: Remove configuration and status

To remove all fiber-monitoring configuration and state information for a port, use the commands:

```
awplus# interface port1.0.1
awplus(config-if)# no fiber-monitoring
```

3 Active Fiber Monitoring Commands

Overview This chapter provides an alphabetical reference of commands used to configure Active Fiber Monitoring, for detecting changes in optical power received over fiber cables.

debug fiber-monitoring

Overview Use this command to enable debugging of active fiber monitoring on the specified ports.

Use the **no** variant of this command to disable debugging on all ports or the specified ports.

Syntax

```
debug fiber-monitoring interface <port-list>
no debug fiber-monitoring [interface <port-list>]
```

Parameter	Description
<port-list>	The list of fiber ports to enable or disable debugging for, as a single port, a comma separated list or a hyphenated range.

Default Debugging of active fiber monitoring is disabled by default.

Mode User Exec/Privileged Exec

Usage While debugging is enabled by this command for a port, all the optical power readings for the port are sent to the console.

Example To enable debugging messages for active fiber monitoring of port 1.0.2 to be sent to the console, use the commands:

```
awplus# debug fiber-monitoring interface port 1.0.2
awplus# terminal monitor
```

To disable debugging messages for active fiber monitoring on port 1.0.2, use the command:

```
awplus# no debug fiber-monitoring interface port 1.0.2
```

Output Figure 3-1: Example output from **debug fiber-monitoring**

```
awplus#debug fiber-monitoring interface port2.0.1
awplus#terminal monitor
% Warning: Console logging enabled
awplus#01:42:50 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1
Reading:1748 Baseline:1708 Threshold:1356
01:42:52 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1 Reading:1717
Baseline:1709 Threshold:1357
01:42:54 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1 Reading:1780
Baseline:1709 Threshold:1357
01:42:56 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1 Reading:1685
Baseline:1710 Threshold:1358
01:42:58 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1 Reading:1701
Baseline:1710 Threshold:1358
01:43:01 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1 Reading:1733
Baseline:1709 Threshold:1357
```

Related Commands show system fiber-monitoring

fiber-monitoring action

Overview Use this command to specify an action to be taken if the optical power received on the port changes from the baseline by the amount specified in the **fiber-monitoring sensitivity** command.

Use the **no** variant of this command to remove the specified action or all actions from the port.

Syntax

```
fiber-monitoring action {trap|shutdown}
no fiber-monitoring action [trap|shutdown]
```

Parameter	Description
`trap`	Send an SNMP notification.
`shutdown`	Shutdown the port.

Default By default a log message is generated, but no additional action is performed.

Mode Interface Configuration mode for a fiber port.

Usage If fiber monitoring is enabled and this command is not used to set an action, the only result of a change in received power on a fiber port is to generate a log message.

Example To set the device to send an SNMP notification when ports 1.0.1 or 1.0.2 receive reduced power, use the commands:

```
awplus(config)# interface port1.0.1-1.0.2
awplus(config-if)# fiber-monitoring action trap
```

To set the device not to send an SNMP notification when ports 1.0.1 or 1.0.2 receive reduced power, use the commands:

```
awplus(config)# interface port1.0.1-1.0.2
awplus(config-if)# no fiber-monitoring action trap
```

To set the device not to perform any action when it receives reduced power on ports 1.0.1 or 1.0.2, use the commands:

```
awplus(config)# interface port1.0.1-1.0.2
awplus(config-if)# no fiber-monitoring action
```

Related Commands fiber-monitoring sensitivity

show system fiber-monitoring

fiber-monitoring baseline

Overview Use this command to configure how the baseline value for comparison is calculated for active fiber monitoring on the port.

Note that alarm generation will not commence until the link has been up for a full averaging period.

Use the **no** variant of this command to set the fiber-monitoring baseline to its default value.

Syntax

```
fiber-monitoring baseline (average <12-150>|fixed <1-65535>)
no fiber-monitoring baseline
```

Parameter	Description
`average`	Set the baseline optical power received to be based on the moving average of the specified number of most recent (non-zero) values. Default.
<12-150>	The number of most recent values to average for the baseline. Default: 12.
`fixed`	Set the baseline to a fixed level of received optical power. Not recommended—see Usage below.
<1-65535>	The fixed baseline value of received optical power in 0.0001mW.

Default The default is a moving average of the last 12 values. If the **fiber-monitoring interval** is set to its default (5s), the **fiber-monitoring baseline** default will be the average over the last minute.

Mode Interface Configuration for a fiber port

Usage Setting a fixed value is not recommended because gradual change over time caused by temperature fluctuations, etc. could lead to unnecessary alarms.

There are two ways to configure the baseline. The first is to choose a number of readings to average. This is the default and recommended method. The second is to set a fixed value in units of x0.0001mW.

If a fixed value is required, the easiest way is to enable fiber monitoring on the port and use the **show system fiber-monitoring** command to see what readings can be expected.

Example To set the baseline optical power to a moving average of the last 30 readings, use the command:

```
awplus(config-if)# fiber-monitoring baseline average 30
```

To set the baseline to its default, averaging the last 12 readings, use the command:

```
awplus(config-if)# no fiber-monitoring baseline
```

Related Commands

fiber-monitoring interval

fiber-monitoring sensitivity

fiber-monitoring enable

Overview Use this command to enable active fiber monitoring on a fiber port. If the port can support fiber monitoring but does not have the correct SFP or fiber type installed, the configuration will be saved, and monitoring will commence when a supported SFP is inserted. Disabling and re-enabling fiber monitoring on a port resets the baseline calculation.

Use the **no** variants of this command to disable active fiber monitoring on the interface, or to remove all the configuration and state for the ports, respectively.

Syntax

```
fiber-monitoring enable
no fiber-monitoring enable
no fiber-monitoring
```

Default Active fiber monitoring is disabled by default.

Mode Interface Configuration mode for a fiber port

Examples To enable active fiber monitoring on ports 1.0.1 and 1.0.2, use the commands:

```
awplus(config)# interface port1.0.1-1.0.2
awplus(config-if)# fiber-monitoring enable
```

To disable fiber monitoring on the ports, use the commands:

```
awplus(config)# interface port1.0.1-1.0.2
awplus(config-if)# no fiber-monitoring enable
```

To remove all fiber-monitoring configuration and state for the ports, use the commands:

```
awplus(config)# interface port1.0.1-1.0.2
awplus(config-if)# no fiber-monitoring
```

Related Commands

fiber-monitoring action

fiber-monitoring sensitivity

show system fiber-monitoring

fiber-monitoring interval

Overview Use this command to configure the fiber monitoring polling interval in seconds for the port. The optical power will be read every <interval> seconds and compared against the calculated threshold values to see if a log message or other action is required.

Use the **no** variant of this command to reset the polling interval to the default (5 seconds).

Syntax

```
fiber-monitoring interval <2-60>
no fiber-monitoring interval
```

Parameter	Description
<2-60>	Optical power polling interval in seconds.

Default The interval is set to 5 seconds by default.

Mode Interface configuration mode for a fiber port.

Example To set the fiber monitoring polling interval for port 1.0.2 to 30 seconds, use the commands:

```
awplus(config)# interface port1.0.2
awplus(config-if)# fiber-monitoring interval 30
```

To reset the fiber monitoring polling interval back to the default (5s), use the commands:

```
awplus(config)# interface port1.0.2
awplus(config-if)# no fiber-monitoring interval
```

Related Commands fiber-monitoring baseline

show system fiber-monitoring

fiber-monitoring sensitivity

Overview Use this command to configure the sensitivity of the alarm thresholds on the port for active fiber monitoring.

Use the **no** variant of this command to reset the sensitivity to the default.

Syntax

```
fiber-monitoring sensitivity (low|medium|high|highest|fixed <25-65535>)|relative <0.01-10.0>
no fiber-monitoring sensitivity
```

Parameter	Description
`low`	Low sensitivity (+/-2dB)
`medium`	Medium sensitivity (1dB) (default)
`high`	High sensitivity (the greater of 0.5dB and 0.0025mW)
`highest`	The highest sensitivity available: 0.0025mW
`fixed` *<25-65535>*	Fixed sensitivity at the specified level in 0.0001 mW.
`relative` *<0.01-10.0>*	Relative sensitivity at the specified level in dB.

Default The default is medium sensitivity.

Mode User Exec/Privileged Exec

Usage A log message is generated and configured actions are taken if the received optical power drops below the baseline value by the sensitivity configured with this command.

The sensitivity can be configured to one of four pre-defined levels in decibels or to a fixed absolute delta in units of 0.0001mW. The alarm thresholds can be seen in the **show system fiber-monitoring** output. The maximum absolute sensitivity configurable is 0.0025mW. Note that 0.0025mW equates to a reduction of approximately 1dB at the maximum attenuation of an AT-SPLX10/1.

Example To set the fiber monitoring sensitivity for port 1.0.2 to a relative sensitivity of 0.1 dB, use the commands:

```
awplus(config)# interface port1.0.2
awplus(config-if)# fiber-monitoring sensitivity relative 0.1
```

To reset the fiber monitoring sensitivity to the default (medium), use the commands:

```
awplus(config)# interface port1.0.2
awplus(config-if)# no fiber-monitoring sensitivity
```

Related Commands

fiber-monitoring action

fiber-monitoring baseline

show system fiber-monitoring

show system fiber-monitoring

Overview Use this command to display settings and current status for Active Fiber Monitoring.

Syntax

```
show system fiber-monitoring
```

Mode User Exec/Privileged Exec

Example To display configuration and status for active fiber monitoring on ports., use the command:

```
awplus# show system fiber-monitoring
```

Output Figure 3-2: Example output from **show system fiber-monitoring**

```
awplus#show sys fiber-monitoring
Fiber Monitoring Status
  Reading units 0.0001mW

Stack member 1:

Interface port1.0.1
Status:           enabled
Supported:        Supported pluggable
Debugging:        disabled
Interval:         2 seconds
Sensitivity:      1.00dB
Baseline type:    average of last 35 values greater than 50
Status:
 Baseline value:   496
 Alarm threshold:  393
 Alarm:            no
 Last 12 Readings: 498 498 498 498 498 498 498 498 498 498 498 498
 Minimum reading: 486
 Maximum reading: 498

Interface port1.0.2
Status:           enabled
Supported:        Supported pluggable
Debugging:        disabled
Interval:         2 seconds
Sensitivity:      1.00dB
Baseline type:    average of last 30 values greater than 50
Status:
 Baseline value:   0
 Alarm threshold:  0
 Alarm:            no
 Last 12 Readings: 0 0 0 0 0 0 0 0 0 0 0 0
 Minimum reading: 0
 Maximum reading: 0
```

Table 3-1: Parameters in the output from **show system fiber-monitoring**

Parameter	Description
`Reading units`	The units for optical power readings in the rest of the display, e.g. 0.0001mW.
`Status`	Whether active fiber monitoring is enabled or disabled for this port.
`Supported`	Whether the pluggable inserted in this port supports active fiber monitoring.
`Debugging`	Whether debugging of active fiber monitoring is enabled or disabled for this port.
`Interval`	The configured interval between readings of optical power on this port.
`Sensitivity`	The configured sensitivity threshold for optical power changes on this port.
`Baseline type`	How the baseline optical power level is calculated: either the average of the specified number of previous readings or a specified fixed value in 0.0001mW.
`Status`	Current values for the following parameters.
`Baseline value`	The baseline value, calculated according to the configured baseline method, in 0.0001mW.
`Alarm threshold`	The current threshold for a change in optical power, calculated according to the configured sensitivity method, that will result in action.
`Alarm`	Whether the optical power at the most recent reading has exceeded the threshold.
`Last 12 readings`	The last 12 optical power values measured, in 0.0001mW, with oldest value first.
`Minimum reading`	The lowest optical power reading since the fiber pluggable was last inserted, or since active fiber monitoring was last enabled on the port.
`Maximum reading`	The highest optical power reading since the fiber pluggable was last inserted, or since active fiber monitoring was last enabled on the port.

Related Commands

debug fiber-monitoring

fiber-monitoring action

fiber-monitoring baseline

fiber-monitoring enable

fiber-monitoring interval

fiber-monitoring sensitivity

4 Policy-based Routing Commands for AR-series Firewalls

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure policy-based routing.

debug policy-based-routing

Overview Use this command to enable policy-based routing debugging. This will cause messages containing detailed debugging information to be displayed and logged at the "debugging" level.

Use the **no** variant of this command to disable policy-based routing debugging.

Syntax
```
debug policy-based-routing
no debug policy-based-routing
```

Default Policy-based routing debugging is disabled by default.

Mode Privileged Exec

Examples To enable policy-based routing debugging, use the command:

```
awplus# debug policy-based-routing
```

To disable policy-based routing debugging, use the command:

```
awplus# no debug policy-based-routing
```

Related Commands
ip policy-route

ipv6 policy-route

policy-based-routing

show ip pbr route

show ipv6 pbr route

ip policy-route

Overview Use this command to configure IP policy routes. These routes specify how the device will route traffic from specified applications and entities. You can specify the route's next-hop by specifying the next-hop device's IP address or the egress interface. You can also list alternative next-hops to use if your first choice is down.

Use the **no** variant of this command to remove a policy route.

Syntax

```
ip policy-route [<1-128>] [match <application-name>] [from
<source-entity>] [to <destination-entity>] nexthop
{<interface-list>|<ip-add-list>}
```

```
no ip policy-route <1-128>
```

Parameter	Description
<1-128>	The policy route ID number. If you do not specify an ID number, the device assigns the new policy route the next available number, in multiples of 10. For example, if the highest numbered policy route is 81, the next policy route would be given an ID of 90. Policy routes are checked in order of ID number, starting with the lowest ID number. The device applies the policy route as soon as it finds a matching route; it does not check the remaining policy routes.
<application-name>	An application name.
<source-entity>	A source entity name.
<destination-entity>	A destination entity name.
<interface-list>	The name of the egress interface or interfaces. You can list up to 8 interfaces per policy route; the device sends the traffic out the first interface in the list that is up.
<ip-add-list>	The IP address of the next-hop. You can list up to 8 next-hop addresses per policy route; the device sends the traffic to the first address in the list that is reachable.

Default No policy routes

Mode Policy-based-routing

Usage You must specify at least one of the **match**, **from** or **to** parameters. Packets will be routed to the specified next-hop if they match the application, come from the source entity, and are destined for the destination entity.

Before creating a policy route, you need to create the application and entities that specify the traffic you want to route. To create an application, use the application command. To create entities, use the zone, network, and host commands. To see existing applications and entities, use the show application and show entity commands.

Examples

To create a policy route to route traffic that matches an application called "voice", comes from the entity called "inside", and is destined for the entity called "outside", use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# policy-based-routing enable
awplus(config-pbr)# ip policy-route 10 match voice from inside
to outside nexthop 10.37.236.65
```

To delete the policy route created above, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# no ip policy-route 10
```

To route the above traffic via ppp0 if ppp0 is up, or ppp1 if ppp0 is down, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# policy-based-routing enable
awplus(config-pbr)# ip policy-route 20 match voice from inside
to outside nexthop ppp0 ppp1
```

To delete the policy route created above, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# no ip policy-route 20
```

Related Commands

policy-based-routing

policy-based-routing enable

show application

show entity

show ip pbr route

ipv6 policy-route

Overview Use this command to configure IPv6 policy routes. These routes specify how the device will route traffic from specified applications and entities. You can specify the route's next-hop by specifying the next-hop device's IPv6 address or the egress interface. You can also list alternative next-hops to use if your first choice is down.

Use the **no** variant of this command to remove a policy route.

Syntax

```
ipv6 policy-route [<1-128>] [match <application-name>] [from
<source-entity>] [to <destination-entity>] nexthop
{<interface-list>|<ipv6-add-list>}
```

```
no ipv6 policy-route <1-128>
```

Parameter	Description
<1-128>	The policy route ID number. If you do not specify an ID number, the device assigns the new policy route the next available number, in multiples of 10. For example, if the highest numbered policy route is 81, the next policy route would be given an ID of 90. Policy routes are checked in order of ID number, starting with the lowest ID number. The device applies the policy route as soon as it finds a matching route; it does not check the remaining policy routes.
<application-name>	An application name.
<source-entity>	A source entity name.
<destination-entity>	A destination entity name.
<interface-list>	The name of the egress interface or interfaces. You can list up to 8 egress interfaces per policy route; the device sends the traffic out the first interface in the list that is up.
<ipv6-add-list>	The IPv6 address of the next-hop, specified in the form X:X::X:X. You can list up to 8 next-hop addresses per policy route; the device sends the traffic to the first address in the list that is reachable.

Default No policy routes

Mode Policy-based-routing

Usage You must specify at least one of the **match**, **from** or **to** parameters. Packets will be routed to the specified next-hop if they match the application, come from the source entity, and are destined for the destination entity.

Before creating a policy route, you need to create the application and entities that specify the traffic you want to route. To create an application, use the application command. To create entities, use the zone, network, and host commands. To see

existing applications and entities, use the show application and show entity commands.

Examples

To create a policy route to route traffic that matches an application called "voice", comes from the entity called "inside", and is destined for the entity called "outside", use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# policy-based-routing enable
awplus(config-pbr)# ipv6 policy-route 10 match voice from
inside to outside nexthop 2001:100::1
```

To delete the policy route created above, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# no ipv6 policy-route 10
```

To route the above traffic via ppp0 if ppp0 is up, or ppp1 if ppp0 is down, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# policy-based-routing enable
awplus(config-pbr)# ipv6 policy-route 20 match voice from
inside to outside nexthop ppp0 ppp1
```

To delete the policy route created above, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# no ipv6 policy-route 20
```

Related Commands

policy-based-routing

policy-based-routing enable

show application

show entity

show ipv6 pbr route

policy-based-routing

Overview Use this command to enter Policy-based-routing mode. Policy-based routing lets you determine how the device will route traffic from specified applications and entities.

Use the **no** variant of this command to remove the whole policy-based routing configuration.

Syntax
```
policy-based-routing
no policy-based-routing
```

Default n/a

Mode Global configuration

Usage Once you have entered policy-based-routing mode, use the policy-based-routing enable command to turn on policy-based routing, and the ip policy-route or ipv6 policy-route commands to create policy routes.

Example To enter policy-based-routing mode, use the commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)#
```

Related Commands
ip policy-route

ipv6 policy-route

policy-based-routing enable

policy-based-routing enable

Overview Use this command to enable policy-based routing (PBR). Policy-based routing lets you determine how the device will route traffic from specified applications and entities.

Use the **no** variant of this command to disable policy-based routing.

Syntax

```
policy-based-routing enable
no policy-based-routing enable
```

Default Policy-based routing is disabled by default

Mode Policy-based-routing

Examples To enable Policy-based routing use the following commands.

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# policy-based-routing enable
```

To disable Policy-based routing use the following commands.

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# no policy-based-routing enable
```

Output Figure 4-1: Example output from **show pbr rules**

```
awplus#show pbr rules
Policy based routing is enabled
Rule Match        From             To               Valid Nexthop
-------------------------------------------------------------------------------
  10 udp          inside           any              Yes   10.37.236.65
  20 udp          inside           any              Yes   2001:100::2
```

Related Commands ip policy-route

ipv6 policy-route

show ip pbr route

Overview Use this command to display the installed IPv4 routes for policy-based routing.

Syntax

```
show ip pbr route [<1-128>]
```

Parameter	Description
<1-128>	The policy route ID. If you specify a policy route ID, the output only lists routes for that ID. If you do not specify an ID, the output also lists the ordinary static and dynamic routes, in the table called "main".

Mode User Exec/Privileged Exec

Usage If you do not specify a policy routeID, the output starts by listing the ordinary static and dynamic routes, in a table called "main".

Example To show all the IPv4 routes, use the following command:

```
awplus# show ip pbr route
```

Output Figure 4-2: Example output from **show ip pbr route**

```
awplus#show ip pbr route
Route table: main
    10.33.11.0/24 via 10.37.236.65, eth1
    10.37.236.64/27 is directly connected, eth1
    172.31.0.0/17 is directly connected, vlan4092
    192.168.1.0/24 is directly connected, vlan2

Route table: policy-route 10

Route table: policy-route 20
    default via 10.37.236.65, ppp0
```

If you do not specify a policy routeID, the output starts by listing the ordinary static and dynamic routes, in the route table called "main".

Then it lists the routes for each policy route.

For each route, the output lists the route's next-hop IP address and/or the egress interface.

Example To show only the routes for policy-route 20, use the following command:

```
awplus# show ip pbr route 20
```

Output

Figure 4-3: Example output from **show ip pbr route** for a specified policy-route

```
awplus#show ip pbr route 20

Route table: policy-route 20
    default via 10.37.236.65, ppp0
```

For each route, the output lists the route's next-hop IP address and/or the egress interface.

Related Commands

ip policy-route

policy-based-routing

show ipv6 pbr route

Overview Use this command to display the installed IPv6 routes for policy-based routing.

Syntax `show ipv6 pbr route [<1-128>]`

Parameter	Description
<1-128>	The policy route ID. If you specify a policy route ID, the output only lists routes for that ID. If you do not specify an ID, the output also lists the ordinary static and dynamic routes, in the table called "main".

Mode User Exec/Privileged Exec

Usage If you do not specify a policy routeID, the output starts by listing the ordinary static and dynamic routes, in a table called "main".

Example To show all the IPv6 routes, use the following command:

```
awplus# show ipv6 pbr route
```

Output Figure 4-4: Example output from **show ipv6 pbr route**

```
awplus#show ipv6 pbr route
Route table: main
    2001:100::/64 dev eth1
    fe80::/64 dev eth1

Route table: policy-route 10

Route table: policy-route 20
    default via 2001:100::2, eth1
```

If you do not specify a policy routeID, the output starts by listing the ordinary static and dynamic routes, in the route table called "main".

Then it lists the routes for each policy route.

For each route, the output lists the route's next-hop IPv6 address and/or the egress interface.

Example To show only the routes for policy-route 20, use the following command:

```
awplus# show ip pbr route 20
```

Output Figure 4-5: Example output from **show ipv6 pbr route** for a specified policy-route

```
awplus#show ipv6 pbr route 20

Route table: policy-route 20
    default via 2001:100::2, eth1
```

For each route, the output lists the route's next-hop IPv6 address and/or the egress interface.

Related Commands

ipv6 policy-route

policy-based-routing

show pbr rules

Overview Use this command to display the configured IPv4 and IPv6 policy routes. It also shows the validity of the policy routes.

Syntax

```
show pbr rules
```

Mode User Exec/Privileged Exec

Example To show information about the policy routes, use the command:

```
awplus# show pbr rules
```

Output Figure 4-6: Example output from **show pbr rules**

```
awplus#show pbr rules
Policy based routing is enabled
Rule Match    From            To                Valid  Nexthop
-----------------------------------------------------------------
10   any      entities.any    entities.outside  Yes    10.10.20.2
20   udp      any             any               Yes    2001:100::2
```

Table 4-1: Parameters in the output from **show pbr rules**

Parameter	Description
`Rule`	The policy route ID number. Policy routes are checked in order of ID number, starting with the lowest ID number. The device applies the policy route as soon as it finds a matching route; it does not check the remaining policy routes.
`Match`	The name of an application. Packets will be routed to the specified next-hop if they match this application, come from the source entity, and are destined for the destination entity.
`From`	The name of the source entity. Packets will be routed to the specified next-hop if they match the application, come from this source entity, and are destined for the destination entity.
`To`	The name of the destination entity. Packets will be routed to the specified next-hop if they match the application, come from the source entity, and are destined for this destination entity.

Table 4-1: Parameters in the output from **show pbr rules** (cont.)

Parameter	Description
`Valid`	Whether the application and entities are valid.
`Nexthop`	The IPv4 or IPv6 address of the next-hop, or the egress interface. You can list up to 8 next-hop addresses or up to 8 interface names per policy route; the device sends the traffic to the first address in the list that is reachable or the first interface that is up and running.

Related Commands

ip policy-route

ipv6 policy-route

policy-based-routing

show ip pbr route

show ipv6 pbr route

5 IPsec Commands

crypto ipsec profile

Overview Use this command to configure a custom IPsec profile.

An IPsec profile comprises one or more transforms that can be configured by using the transform (IPsec Profile) command.

Use the **no** variant to delete a previously created profile.

Syntax

```
crypto ipsec profile <profile_name>
no crypto ipsec profile <profile_name>
```

Parameter	Description
<profile_name>	Profile name. Profile names are case insensitive and can be up to 64 characters long composed of printable ASCII characters. Profile names can have only letters from a to z and A to Z, numbers from 0 to 9, - (dash), or _ (underscore).

Default The default IPsec profile with transforms in order of preference is listed in the following table. Which IPsec profile will actually be used depends on how the negotiation between the peers is carried out when establishing the connection. Note that you cannot delete or edit the default profile. Expiry time of 8 hours applies to the default IPsec profile.

Table 5-1: IPsec default profile

Attribute	Transform 1	Transform 2	Transform 3	Transform 4	Transform 5	Transform 6
Protocol	ESP	ESP	ESP	ESP	ESP	ESP
Encryption (all CBC)	AES256	AES256	AES128	AES128	3DES	3DES
Integrity (all HMAC)	SHA256	SHA1	SHA256	SHA1	SHA256	SHA1

Mode Global Configuration

Examples To configure a custom IPsec profile for establishing IPSec SAs with a remote peer, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto ipsec profile my_profile
awplus(config-ipsec-profile)# transform 2 protocol esp
integrity sha1 encryption 3des
```

To delete a custom profile, use the following commands:

```
awplus# configure terminal
awplus(config)# no crypto ipsec profile my_profile
```

Related Commands lifetime (IPsec Profile)

transform (IPsec Profile)

Validation Commands show ipsec profile

lifetime (IPsec Profile)

Overview Use this command to specify a lifetime for an IPsec SA.

Lifetime measures how long the IPsec SA can be maintained before it expires. Lifetime prevents a connection from being used too long.

Use the **no** variant to set the lifetime to default (28800 seconds).

Syntax

```
lifetime seconds <300-31449600>
no lifetime seconds
```

Parameter	Description
<300-31449600>	Lifetime in seconds.

Default If you do not specify a lifetime, the default lifetime of 28800 seconds (8 hours) applies.

Mode IPsec Profile Configuration

Examples To specify a lifetime for an IPsec SA, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile
awplus(config-ipsec-profile)# lifetime seconds 400
```

To set the lifetime to its default, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile
awplus(config-ipsec-profile)# no lifetime seconds
```

Related Commands crypto ipsec profile

transform (IPsec Profile)

Overview Use this command to create an IPsec profile transform which specifies the encryption and authentication algorithms used to protect data.

Use the **no** variant to delete a previously created transform.

Syntax

```
transform <1-255> protocol esp integrity {sha1|sha256|sha512}
encryption {3des|aes128|aes192|aes256}
```

```
no transform <1-255>
```

Parameter	Description
<1-255>	Transform priority (1 is the highest)
`sha1`	Secure Hash Standard with 160-bit digest size
`sha256`	Secure Hash Standard with 256-bit digest size
`sha512`	Secure Hash Standard with 512 bit digest size
`3des`	Triple DES symmetric key block cipher with a 168-bit key
`aes128`	Advanced Encryption Standard symmetric key block cipher with a 128-bit key
`aes192`	Advanced Encryption Standard symmetric key block cipher with a 192-bit key
`aes256`	Advanced Encryption Standard symmetric key block cipher with a 256-bit key

Default By default, an IPsec profile has no transforms and so will not be active.

Mode IPsec Profile Configuration

Examples To configure an IPsec profile transform, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile
```

```
awplus(config-ipsec-profile)# transform 2 protocol esp
integrity sha1 encryption 3des
```

To delete a created transform, use the following command:

```
awplus(config-ipsec-profile)# no transform 2
```

Related Commands crypto ipsec profile

Validation Commands show ipsec profile

pfs

Overview Use this command to enable PFS and set a Diffie-Hellman group for PFS in an IPsec profile.

Use the **no** variant to disable PFS.

Syntax

```
pfs {14|15|16|18|2|5}
no pfs
```

Parameter	Description
14	2048-bit MODP Group
15	3072-bit MODP Group
16	4096-bit MODP Group
18	8192-bit MODP Group
2	1024-bit MODP Group
5	1536-bit MODP Group

Default PFS is disabled.

Mode IPsec Profile Configuration

Usage Perfect Forward Secrecy (PFS) ensures generated keys, for example IPsec SA keys are not compromized if any other keys, for example, ISAKMP SA keys are compromized.

The specified PFS group must match the PFS group setting on the peer - especially when IKEv2 is used for ISAKMP SA negotiation. With IKEv2, if there is a PFS group mismatch an IPsec SA will be established and the tunnel will come up because PFS is not required for the initial child SA negotiation. However, when the IPsec SA rekeys it will fail due to the PFS group mismatch, and upon IPsec SA expiry the tunnel will no longer be able to carry traffic.

Examples To enable PFS and set a Diffie-Hellman group for PFS, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile
awplus(config-ipsec-profile)# pfs 15
```

To disable PFS, use the following command:

```
awplus(config-ipsec-profile)# no pfs
```

Related Commands crypto ipsec profile

Validation Commands show ipsec profile

crypto isakmp profile

Overview Use this command to configure a custom ISAKMP profile.

An ISAKMP profile comprises one or more transforms that can be configured by using the transform (ISAKMP Profile) command.

Use the **no** variant to delete a previously created profile.

Syntax

```
crypto isakmp profile <profile_name>
no crypto isakmp profile <profile_name>
```

Parameter	Description
<profile_name>	Profile name. Profile names are case insensitive and can be up to 64 characters long composed of printable ASCII characters. Profile names can have only letters from a to z and A to Z, numbers from 0 to 9, - (dash), or _ (underscore).

Default Which ISAKMP profile transform will actually be used depends on how the negotiation between the peers is carried out when establishing the connection. For more information about default ISAKMP profiles, see the following table. Note that you cannot delete or edit the default profile. Expiry time of 24 hours applies to the default profile.

Table 5-2: ISAKMP default profile

Attribute	Encryption	Integrity	Group	Authentication
Transform 1	AES256	SHA256	14	Pre-shared
Transform 2	AES256	SHA256	16	Pre-shared
Transform 3	AES256	SHA1	14	Pre-shared
Transform 4	AES256	SHA1	16	Pre-shared
Transform 5	AES128	SHA256	14	Pre-shared
Transform 6	AES128	SHA256	16	Pre-shared
Transform 7	AES128	SHA1	14	Pre-shared
Transform 8	AES128	SHA1	16	Pre-shared
Transform 9	3DES	SHA256	14	Pre-shared
Transform 10	3DES	SHA256	16	Pre-shared
Transform 11	3DES	SHA1	14	Pre-shared
Transform 12	3DES	SHA1	16	Pre-shared

Mode Global Configuration

Examples

To configure a custom ISAKMP profile for establishing ISAKMP SAs with a remote peer, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp profile my_profile
awplus(config-isakmp-profile)# transform 2 integrity sha1
encryption 3des group 5
```

To delete a custom profile, use the following commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp profile my_profile
```

Related Commands

dpd-interval

dpd-timeout

lifetime (ISAKMP Profile)

transform (ISAKMP Profile)

version

Validation Commands

show isakmp profile

version

Overview Use this command to set the ISAKMP protocol version.

Use the **no** variant to set the protocol version to default (IKEv2).

Syntax

```
version {1 mode {aggressive|main}|2}
no version
```

Parameter	Description
1	IKEv1
main	IKEv1 Main mode. An IKE session begins with the initiator and recipient sending three two-way exchanges to define what encryption and authentication protocols are acceptable, how long keys should remain active, and whether perfect forward secrecy should be enforced. Main mode uses more packets for the process than Aggressive mode, but Main mode is considered more secure.
aggressive	IKEv1 Aggressive mode. The initiator and recipient accomplish the same objectives, but in only two exchanges.
2	IKEv2

Default If you do not specify the version, the default version is IKEv2

Mode IPsec ISAKMP Configuration

Examples To set the ISAKMP protocol version of profile "my_profile" to IKEv1 main mode, use the following commands:

```
awplus(config)# configure isakmp profile my_profile
awplus(config-isakmp-profile)# version 1 mode main
```

To set the version to its default, use the following command:

```
awplus# no version
```

Related Commands crypto isakmp profile

Validation Commands show isakmp profile

lifetime (ISAKMP Profile)

Overview Use this command to specify a lifetime for an ISAKMP SA.

Lifetime measures how long the ISAKMP SA can be maintained before it expires. Lifetime prevents a connection from being used too long.

Use the **no** variant to set the lifetime to default (86400 seconds).

Syntax

```
lifetime <600-31449600>
no lifetime
```

Parameter	Description
<600-31449600>	Lifetime in seconds.

Default If you do not specify a lifetime, the default lifetime of 86400 seconds (8 hours) applies.

Mode ISAKMP Profile Configuration

Examples To specify a lifetime for an ISAKMP SA, use the following commands:

```
awplus(config)# configure isakmp profile my_profile
awplus(config-isakmp-profile)# lifetime 700
```

To set the lifetime to its default, use the following commands:

```
awplus(config-isakmp-profile)# no lifetime
```

Related Commands crypto isakmp profile

dpd-interval

Overview Use this command to specify the Dead Peer Detection (DPD) interval for an ISAKMP profile.

DPD is an IKE mechanism using a form of keep-alive to determine if a tunnel peer is still active.

The interval parameter specifies the amount of time the device waits for traffic from its peer before sending a DPD acknowledgment message.

Use the **no** variant to set the interval to its default (30 seconds).

Syntax

```
dpd-interval <10-86400>
no dpd-interval
```

Parameter	Description
<10-86400>	Interval expressed in seconds.

Default If you do not specify an interval, the default interval of 30 seconds applies.

Mode ISAKMP Profile Configuration

Examples To specify a DPD interval, use the following commands:

```
awplus(config)# crypto isakmp profile my_profile
awplus(config-isakmp-profile)# dpd-interval 20
```

To set the interval to its default, use the following commands:

```
awplus(config-isakmp-profile)# no dpd-interval
```

Related Commands crypto isakmp profile

Validation Commands show isakmp profile

dpd-timeout

Overview Use this command to specify a Dead Peer Detection (DPD) timeout for IKEv1.

DPD is an IKE mechanism using a form of keep-alive to determine if a tunnel peer is still active.

DPD timeout defines the timeout interval after which all connections to a peer are deleted in case of inactivity. This only applies to IKEv1, in IKEv2 the default retransmission timeout applies as every exchange is used to detect dead peers.

Use the **no** variant to set the timeout to its default (150 seconds).

Syntax

```
dpd-timeout <10-86400>
no dpd-timeout
```

Parameter	Description
<10-86400>	Timeout in seconds.

Default If you do not specify a timeout, the default timeout of 150 seconds applies.

Mode ISAKMP Profile Configuration

Examples To specify a DPD timeout for IKEv1, use the following commands:

```
awplus(config)# crypto isakmp profile my_profile
awplus(config-isakmp-profile)# dpd-timeout 200
```

To set the timeout to its default, use the following command:

```
awplus(config-isakmp-profile)# no dpd-timeout
```

Related Commands crypto isakmp profile

Related Commands show isakmp profile

transform (ISAKMP Profile)

Overview Use this command to create an ISAKMP profile transform which specifies the encryption and authentication algorithms used to protect data in the tunnel.

Use the **no** variant to delete a previously created transform.

Syntax

```
transform <1-255> integrity {sha1|sha256|sha512} encryption
{3des|aes128|aes192|aes256} group {2|5|14|15|16|18}

no transform <1-255>
```

Parameter	Description
<1-255>	Transform priority (1 is the highest)
sha1	Secure Hash Standard with 160-bit digest size
sha256	Secure Hash Standard with 256-bit digest size
sha512	Secure Hash Standard with 512 bit digest size
3des	Triple DES symmetric key block cipher with a 168-bit key
aes128	Advanced Encryption Standard symmetric key block cipher with a 128-bit key
aes192	Advanced Encryption Standard symmetric key block cipher with a 192-bit key
aes256	Advanced Encryption Standard symmetric key block cipher with a 256-bit key
group	Diffie-Hellman group
2	1024-bit MODP Group
5	1536-bit MODP Group
14	2048-bit MODP Group
15	3072-bit MODP Group
16	4096-bit MODP Group
18	8192-bit MODP Group

Default By default, an ISASMP profile has no transforms and so will not be active.

Mode ISAKMP Profile Configuration

Examples To create an ISAKMP profile transform, use the following commands:

```
awplus(config)# crypto isakmp profile my_profile
awplus(config-isakmp-profile)# transform 2 integrity sha1
encryption 3des group 5
```

To delete a created transform, use the following command:

```
awplus(config-isakmp-profile)# no transform 2
```

Related Commands crypto isakmp profile

crypto isakmp peer

Overview Use this command to configure a peer to use a specific ISAKMP profile.

Use the **no** variant to set the peer back to using the default profile.

Syntax

```
crypto isakmp peer {dynamic|address {<ipv4-addr>|<ipv6-addr>}}
profile <profile_name>
```

```
no crypto isakmp peer {dynamic|address
{<ipv4-addr>|<ipv6-addr>}} profile
```

Parameter	Description
`dynamic`	Remote endpoint with a dynamic IP address.
<ipv4-addr>	Destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<ipv6-addr>	Destination IPv6 address. The IPv4 address uses the format X:X::X:X.
<profile-name>	Profile name.

Default By default, all peers use the default profile.

Mode Global Configuration

Examples To configure a profile for a peer with a dynamic IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp peer dynamic profile peer_profile
```

To configure a profile for a peer with IPv4 address, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp peer address 192.168.1.2 profile
peer_profile
```

To set the profile for the peer back to default, use the following commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp peer dynamic profile
```

Validation Commands show isakmp peer

tunnel protection ipsec

Overview Use this command to enable IPsec protection for packets encapsulated by this tunnel.

Use the **no** variant to disable IPsec protection.

Syntax

```
tunnel protection ipsec [profile <profile_name>]
no tunnel protection ipsec
```

Default IPsec protection for packets encapsulated by tunnel is disabled. If no custom profile is specified, the default profile is used.

Parameter	Description
<profile_name>	Custom profile name. You can use the crypto ipsec profile command to create custom profiles.

Mode Interface Configuration

Usage IPsec mode tunnels (IPv4 and IPv6) require this command for them to work. GRE IPv6 and L2TPv3 IPv6 tunnel have IPsec protection as an option.

Examples To enable IPsec protection by using default profile, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel14
awplus(config-if)# tunnel protection ipsec
```

To enable IPsec protection by using a custom profile, use the following commands:

```
awplus(config)# interface tunnel14
awplus(config-if)# tunnel protection ipsec profile
my_profile
```

To disable IPsec protection for packets encapsulated by `tunnel14`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel14
awplus(config-if)# no tunnel protection ipsec
```

Related Commands crypto ipsec profile

tunnel destination (IPsec)

Overview Use this command to specify a destination IPv4 or IPv6 address or destination network name for the remote end of the tunnel.

Use the **no** variant of this command to remove a configured tunnel destination address.

Syntax

```
tunnel destination {<WORD>|<ipv4-address>|<ipv6-address>}
no tunnel destination {<WORD>|<ipv4-address>|<ipv6-address>}
```

Parameter	Description
<WORD>	Destination network name or "dynamic". The "dynamic" parameter allows you to specify a dynamic IP address for the remote endpoint. The dynamic IP address can be obtained, for example, via DHCP.
<ipv4-address>	Destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<ipv6-address>	Destination IPv6 address. The IPv4 address uses the format X:X::X:X.

Mode Interface Configuration

Examples To configure a destination IPv4 address for IPsec `tunnel145`, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel145
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if# tunnel destination 192.0.3.1
```

To configure a destination IPv6 address for IPsec `tunnel145`, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel145
awplus(config-if)# tunnel mode ipsec ipv6
awplus(config-if# tunnel destination 2001:0db8::
```

To configure a destination network name for IPsec `tunnel145`, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel145
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if# tunnel destination www.z.com
```

To configure a dynamic IP address for the tunnel destination, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel145
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if# tunnel destination dynamic
```

To remove the destination address of IPSec `tunnel145`, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel145
awplus(config-if)# no tunnel destination 192.0.3.1
```

Related Commands tunnel source (IPSec)

tunnel local selector

Overview Use this command to specify a source address as the traffic selector. A traffic selector is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote addresses.

Use the **no** variant of this command to remove the source address and traffic selector.

Syntax

```
tunnel local selector {<ipv4-address>|<ipv6-address>}
no tunnel local selector
```

Parameter	Description
<ipv4-address>	IPv4 address in the format of A.B.C.D/M
<ipv6-address>	IPv6 address in the format of X:X::X:X/M

Default No traffic selector is specified.

Mode Interface Configuration

Usage The Security Policy Database (SPD) stores the static IPsec configuration on how to process different types of traffic entering and leaving the device. The SPD is a list of selectors that define the matching criteria for packets that must be protected. For GRE based tunnels these selectors specify the source and destination addresses of the tunnels and IP protocol type 47 (GRE). If outgoing packets match these selectors, then the packet is marked for IPsec processing using the SA or SA's linked to from the policy entry.

Examples To specify a source address as the traffic selector for the traffic to match for `tunnel0`, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel source eth1
awplus(config-if)# tunnel destination 10.0.0.2
awplus(config-if)# tunnel local name office
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel local selector 192.168.1.0/24
awplus(config-if)# tunnel remote selector 192.168.2.0/24
```

To remove the source address from `tunnel0`, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel local selector
```

Related Commands tunnel remote selector

tunnel remote selector

Overview Use this command to specify a destination address as the traffic selector. A traffic selector is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote addresses.

Use the **no** variant of this command to remove the destination address and traffic selector.

Syntax

```
tunnel remote selector {<ipv4-address>|<ipv6-address>}
no tunnel remote selector
```

Parameter	Description
<ipv4-address>	IPv4 address in the format of A.B.C.D/M
<ipv6-address>	IPv6 address in the format of X:X::X:X/M

Default No traffic selector is specified.

Mode Interface Configuration

Usage The Security Policy Database (SPD) stores the static IPsec configuration on how to process different types of traffic entering and leaving the device. The SPD is a list of selectors that define the matching criteria for packets that must be protected. For GRE based tunnels these selectors specify the source and destination addresses of the tunnels and IP protocol type 47 (GRE). If outgoing packets match these selectors, then the packet is marked for IPsec processing using the SA or SA's linked to from the policy entry.

Examples To specify a destination address as the traffic selector for the traffic to match for `tunnel0`, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel source eth1
awplus(config-if)# tunnel destination 10.0.0.2
awplus(config-if)# tunnel local name office
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel local selector 192.168.1.0/24
awplus(config-if)# tunnel remote selector 192.168.2.0/24
```

To remove the destination address from tunnel0, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel remote selector
```

Related Commands tunnel local selector

show ipsec profile

Overview Use this command to show IPsec default and custom profiles.

An IPsec profile consists of a set of parameters that are used by IPsec when establishing IPsec SAs with a remote peer. AlliedWare Plus provides default ISAKMP and IPsec profiles that contain a priority ordered set of transforms that are considered secure by the security community.

Syntax `show [crypto] ipsec pofile [<profile_name>]`

Parameter	Description
`crypto`	Security specific.
`ipsec`	Internet Protocol Security defines the protection of IP packets using encryption and authentication.
`profile`	An IPsec profile consists of a set of parameters that are used by IPsec SAs with a remote peer.
<profile_name>	Custom profile name.

Mode Privileged Exec

Examples To show all IPsec profiles, including the default profile, use the following command:

```
awplus# show ipsec profile
```

Output Figure 5-1: Example output from the **show ipsec profile** command

```
awplus#show ipsec profile
IPsec Profile: default
  Replay-window:  32
  Expiry:         8h
  PFS group:      disabled
  Transforms:
      Protocol  Integrity   Encryption
    1    ESP       SHA256      AES256
    2    ESP       SHA1        AES256
    3    ESP       SHA256      AES128
    4    ESP       SHA1        AES128
    5    ESP       SHA256      3DES
    6    ESP       SHA1        3DES
IPsec Profile: my_profile
  Replay-window:  32
  Expiry:         8h
  PFS group:      disabled
  Transforms:
       Protocol  Integrity   Encryption
    2    ESP       SHA1        3DES
```

Examples To show IPsec profile “my_profile”, use the command:

```
awplus# show ipsec profile my_profile
```

Output Figure 5-2: Example output from the **show ipsec profile** command

```
awplus#show ipsec profile my_profile
IPsec Profile: my_profile
  Replay-window:  32
  Expiry:         8h
  PFS group:      disabled
  Transforms:
       Protocol  Integrity   Encryption
    2    ESP       SHA1        3DES
```

Related Commands crypto ipsec profile

show isakmp peer

Overview Use this command to show ISAKMP profile and key status for ISAKMP peers.

Syntax `show isakmp peer [<host-name>|<ipv4-addr>|<ipv6-addr>]`

Parameter	Description
<host-name>	Destination hostname.
<ipv4-addr>	Destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<ipv6-addr>	Destination IPv6 address. The IPv6 address uses the format X:X::X:X.

Mode Privileged Exec

Examples To show ISAKMP profile and key status for ISAKMP peers, use the following command:

```
awplus# show isakmp peer
```

Output Figure 5-3: Example output from the **show isakmp peer** command

```
awplus#show isakmp peer
Peer                      Profile (* incomplete)                    Key
------------------------------------------------------------------------------
example.com               LEGACY                                    Not Found
2.2.2.2                   default                                   PSK
1.1.1.1                   SECURE                                    PSK
```

Related Commands crypto isakmp peer

show isakmp profile

Overview Use this command to show ISAKMP default and custom profiles.

Syntax `show [crypto] isakmp profile [<profile_name>]`

Parameter	Description
<profile_name>	Custom profile name.

Mode Privileged Exec

Examples To show ISAKMP profiles, including the default profile, use the command:

```
awplus# show isakmp profile
```

Output Figure 5-4: Example output from the **show isakmp profile** command

```
awplus#show isakmp profile
ISAKMP Profile: default
  Version:        IKEv2
  Authentication: PSK
  Expiry:         24h
  DPD Interval:   30s
  Transforms:
       Integrity   Encryption  DH Group
    1    SHA256      AES256      14
    2    SHA256      AES256      16
    3    SHA1        AES256      14
    4    SHA1        AES256      16
    5    SHA256      AES128      14
    6    SHA256      AES128      16
    7    SHA1        AES128      14
    8    SHA1        AES128      16
    9    SHA256      3DES        14
   10    SHA256      3DES        16
   11    SHA1        3DES        14
   12    SHA1        3DES        16

ISAKMP Profile: my_profile
  Version:        IKEv2
  Authentication: PSK
  Expiry:         24h
  DPD Interval:   30s
  Transforms:
       Integrity   Encryption  DH Group
    2    SHA1        3DES        5
```

Examples To show ISAKMP profile “my_profile”, use the command:

```
awplus# show isakmp profile my_profile
```

Output Figure 5-5: Example output from the **show isakmp profile** command

```
awplus#show isakmp profile my_profile
ISAKMP Profile: my_profile
  Version:        IKEv2
  Authentication: PSK
  Expiry:         24h
  DPD Interval:   30s
  Transforms:
       Integrity   Encryption  DH Group
    2    SHA1         3DES         5
```

Related Commands crypto isakmp profile

6 DNS Domain Name Matching Commands

description (Domain List)

Overview Use this command to give a description to a domain-list.

Use the **no** variant of this command to delete the description.

Syntax

```
description <LINE>
no description
```

Parameter	Description
<LINE>	Description string, 128 characters maximum.

Mode Domain List Mode

Usage When creating a domain-list, it is helpful to write a short description of what the list is to be used for.

Examples To add a description to a domain list:, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list mydomains
awplus(config-domain-list)# description This is a useful
description of my domain list
```

To delete the description, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list mydomains
awplus(config-domain-list)# no description
```

Related Commands ip dns forwarding domain-list

domain (Domain List)

Overview Use this command to add a domain to a domain list.

Use the **no** variant of this command to delete the domain.

Syntax

```
domain <domain-string>
no domain <domain-string>
```

Parameter	Description
<domain-string>	• A domain name must only contain a-z, A-Z, 0-9, '-' (en-dash) and '.'(period) characters. • Each sub-section of the domain must not start or end with the '-' character. • Each sub-section must have no more than 64 characters including the '.'. • The last section must not have a '.' at the end. • The whole domain must be less than 254 characters long.

Mode Domain List Mode

Usage Domain lists are objects that contain unsorted lists of domain names. After a domain list has been created, you can use this command to add domains to the domain list. There is no limit on the number of domains that can be added to a domain list.

Examples To add the domain "compu-global-hyper-mega.net" to a domain list, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list
homer-simpsons-company
awplus(config-domain-list)# domain compu-global-hyper-mega.net
```

To delete the domain, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list
homer-simpsons-company
awplus(config-domain-list)# no domain
compu-global-hyper-mega.net
```

Related Commands ip dns forwarding domain-list

ip dns forwarding domain-list

Overview Use this command to create a domain-list that can be used as a suffix-list for DNS lookups.

Use the **no** variant of this command to delete the domain-list.

Syntax

```
ip dns forwarding domain-list <domain-list-name>
no ip dns forwarding domain-list <domain-list-name>
```

Parameter	Description
<domain-list-name>	Name of the list.

Mode Global Configuration

Usage The domain list can be used by features that need to match against domains. A domain list by itself does nothing; it must be attached to another feature to have functionality (like a prefix-list).

The first use is to specify a domain list to be used as a suffix list on an DNS name-server. The DNS server can be either statically configured, or learned over a PPP connection.

This command puts the device into a new mode where subsequent commands can be entered. The new mode is "Domain List Configuration" mode.

Note that this command is separate from the existing **ip domain-list** command, which is used by DNS client to append a domain on to the end of a partial hostname to form a fully-qualified domain.

Examples To create a domain list to include domains that are internal to the company such as "engineering.acme" or "intranet.acme", use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list corporatedomains
awplus(config)# description internal network domain
awplus(config)# domain engineering.acme
awplus(config)# domain intranet.acme
```

To delete the domain list, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding domain-list
corporatedomains
```

Related Commands

description (Domain List)

domain (Domain List)

ip dns forwarding

ppp ipcp dns suffix-list

ppp ipcp dns suffix-list

Overview Use this command to configure a suffix-list to be associated with DNS name-servers learned over the PPP connection.

Use the **no** variant of this command to delete the suffix-list.

Syntax

```
ppp ipcp dns suffix-list <domain-list-name>
no ppp ipcp dns suffix-list
```

Parameter	Description
<domain-list-name>	The name of the DNS domain-list

Mode Interface Configuration

Usage A PPP connection can be configured to learn DNS servers from the remote peer by using the command ppp ipcp dns.

This command allows a user to associate a domain-list to be used to match against the suffixes of incoming DNS requests. For example, a customer branch office may have a router that is used to give remote-access to their head office, over which they learn the IP address of the head office's DNS server. A domain list can be created that contains a suffix used for services internal to that company, for example, "example.lc". This domain-list is associated as a suffix-list to the PPP connection. So when the PPP connection is completed with the head office, users at the branch office that browse to "intranet.atlnz.lc" will have the DNS request forwarded to the DNS server learned over the PPP connection. Without having the suffix-list configured, the DNS request for "intranet.atlnz.lc" would instead be sent to the primary DNS server, which is likely to be the branch office's ISP, and they will simply respond with a negative reply, because .atlnz.lc is not a globally routable domain.

Examples At a branch office, to direct DNS lookups for domains with suffixes of "engineering.acme" or "intranet.acme" to an internal corporate name-server run at head-office that was learned over a PPP connection, use the commands::

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list corporatedomains
host(config-domain-list)# description Our internal network
domains; do not send DNS requests to internet
host(config-domain-list)# domain engineering.acme
host(config-domain-list)# domain intranet.acme
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns required
awplus(config-if)# ppp ipcp dns suffix-list corporatedomains
```

Related Commands

ip dns forwarding domain-list

ppp ipcp dns

7 Authentication Commands

Introduction

Overview This chapter provides an alphabetical reference for authentication commands.

auth critical

Overview This command enables the critical port feature on the interface. When the critical port feature is enabled on an interface, and all the RADIUS servers are unavailable, then the interface becomes authorized.

The **no** variant of this command disables critical port feature on the interface.

Syntax

```
auth critical
no auth critical
```

Default The critical port of port authentication is disabled.

Mode Interface Configuration for an Ethernet port

Examples To enable the critical port feature on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth critical
```

To disable the critical port feature on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth critical
```

Validation Commands

show auth-web-server

show dot1x

show running-config

auth host-mode

Overview This command selects host mode on the interface. Multi-host is an extension to IEEE802.1X.

Use the **no** variant of this command to set host mode to the default setting (single host).

Syntax

```
auth host-mode {single-host|multi-host|multi-supplicant}
no auth host-mode
```

Parameter	Description
`single-host`	Single host mode. In this mode, only one host may be authorized with the port. If other hosts out the interface attempt to authenticate, the authenticator blocks the attempt.
`multi-host`	Multi host mode. In this mode, multiple hosts may be authorized with the port; however only one host must be successfully authenticated at the Authentication Server for all hosts to be authorized with the port. Upon one host being successfully authenticated (state Authenticated), the other hosts will be automatically authorized at the port (state ForceAuthorized). If no host is successfully authenticated, then all hosts are not authorized with the port.
`multi-supplicant`	Multi supplicant (client device) mode. In this mode, multiple hosts may be authorized with the port, but each host must be individually authenticated with the Authentication Server to be authorized with the port. Supplicants which are not authenticated are not authorized with the port, while supplicants which are successfully authenticated are authorized with the port.

Default The default host mode for port authentication is for a single host.

Mode Interface Configuration for an Ethernet port.

Usage Ports residing in the unauthorized state for host(s) or supplicant(s), change to an authorized state when the host or supplicant has successfully authenticated with the Authentication Server.

When multi-host mode is used or auth critical feature is used, all hosts do not need to be authenticated.

Examples To set the host mode to multi-supplicant on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth host-mode multi-supplicant
```

To set the host mode to default (single host) on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth host-mode
```

Validation Commands

show dot1x interface

show running-config

auth log

Overview Use this command to configure the types of authentication feature log messages that are output to the log file.

Use the **no** variant of this command to remove either specified types or all types of authentication feature log messages that are output to the log file.

Syntax

```
auth log auth-web {success|failure|logoff|all}
no auth log auth-web {success|failure|logoff|all}
```

Parameter	Description
`auth-web`	Specify only Web-Authentication log messages are output to the log file.
`success`	Specify only successful authentication log messages are output to the log file.
`failure`	Specify only authentication failure log messages are output to the log file.
`logoff`	Specify only authentication log-off messages are output to the log file. Note that link down, age out and expired ping polling messages will be included.
`all`	Specify all types of authentication log messages are output to the log file Note that this is the default behavior for the authentication logging feature.

Default All types of authentication log messages are output to the log file by default.

Mode Interface Configuration for an Ethernet port.

Examples To configure the logging of Web-Authentication failures to the log file for supplicants (client devices) connected to interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth log auth-web failure
```

To configure the logging of all types of authentication log messages to the log file for supplicants (client devices) connected to interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth log all
```

Validation Commands show running-config

auth max-supplicant

Overview This command sets the maximum number of supplicants (client devices) on the interface that can be authenticated. After this value is exceeded supplicants are not authenticated.

The **no** variant of this command resets the maximum supplicant number to the default (1024).

Syntax

```
auth max-supplicant <2-1024>
no auth max-supplicant
```

Parameter	Description
<2-256>	Limit number.

Default The max supplicant of port authentication is 1024.

Mode Interface Configuration for an Ethernet port.

Examples To set the maximum number of supplicants to `10` on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth max-supplicant 10
```

To reset the maximum number of supplicant to default on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth max-supplicant
```

Validation Commands show dot1x interface

show running-config

auth reauthentication

Overview This command enables re-authentication on the interface specified in the Interface mode.

Use the **no** variant of this command to disables reauthentication on the interface.

Syntax
```
auth reauthentication
no auth reauthentication
```

Default Reauthentication of port authentication is disabled by default.

Mode Interface Configuration for an Ethernet port.

Examples To enable reauthentication on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth reauthentication
```

Validation Commands
show dot1x interface

show running-config

auth supplicant-ip

Overview This command adds a supplicant (client device) IP address on a given interface.

Use the **no** variant of this command to delete the supplicant IP address added by the **auth supplicant-ip** command, and resets to the default for the supplicant parameter. The IP address can be determined before authentication for only auth-web client.

Syntax

```
auth supplicant-ip <ip-addr> [max-reauth-req <1-10>]
[port-control {auto|force-authorized|force-unauthorized}]
[quiet-period <1-65535>] [reauth-period <1-4294967295>]
[supp-timeout <1-65535>] [server-timeout <1-65535>]
[reauthentication]
```

```
no auth supplicant-ip <ip-addr> [reauthentication]
```

Parameter	Description
<ip-addr>	IP address of the supplicant entry in A.B.C.D/M format.
`max-reauth-req`	No of reauthentication attempts before becoming unauthorized (default 2).
<1-10>	Count of reauthentication attempts.
`port-control`	Port control commands.
`auto`	Allow port client to negotiate authentication.
`force-authorized`	Force port state to authorized.
`force-unauthorized`	Force port state to unauthorized.
`quiet-period`	Quiet period in the HELD state (default 60 seconds).
<1-65535>	Seconds for quiet period.
`reauth-period`	Seconds between reauthorization attempts (default 3600 seconds).
<1-4294967295>	Seconds for reauthorization attempts (reauth-period).
`supp-timeout`	Supplicant response timeout (default 30 seconds).
<1-65535>	Seconds for supplicant response timeout.
`server-timeout`	Authentication server response timeout (default 30 seconds).
<1-65535>	Seconds for authentication server response timeout.
`reauthentication`	Enable reauthentication on a port.

Default No supplicant IP address for port authentication exists by default until first created with the **auth supplicant-ip** command. The defaults for parameters applied are as shown in the command syntax parameter table.

Mode Interface Configuration for an Ethernet port, or Auth Profile.

Exam

To add the supplicant IP address 192.168.10.0/24 to force authorized port control for interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth supplicant-ip 192.168.10.0/24
port-control force-authorized
```

To delete the supplicant IP address 192.168.10.0/24 for interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth supplicant-ip 192.168.10.0/24
```

To reset reauthentication to disable for the supplicant(s) IP address 192.168.10.0/24, for interface eth1 use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth supplicant-ip 192.168.10.0/24
reauthentication
```

To add the supplicant IP address 192.168.10.0/224 to force authorized port control for auth profile 'student', use the following commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth supplicant-ip
192.168.10.0/24 port-control force-authorized
```

To delete the supplicant IP address 192.168.10.0/24 for auth profile 'student', use the following commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth supplicant-ip
192.168.10.0/24
```

To reset reauthentication to disable for the supplicant IP address 192.168.10.0/24, for auth profile 'student', use the following commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-if)# no auth supplicant-ip 192.168.10.0/24
reauthentication
```

Validation Commands

auth supplicant-mac

show dot1x interface

show running-config

auth supplicant-mac

Overview This command adds a supplicant (client device) MAC address or MAC mask on a given interface with the parameters as specified in the table below.

Use the **no** variant of this command to delete the supplicant MAC address added by the **auth supplicant-mac** command, and resets to the default for the supplicant parameter.

Syntax

```
auth supplicant <mac-addr> [mask <mac-addr>] [max-reauth-req
<1-10>] [port-control
{auto|force-authorized|force-unauthorized}] [quiet-period
<1-65535>] [reauth-period <1-4294967295>] [supp-timeout
<1-65535>] [server-timeout <1-65535>] [reauthentication]
```

```
auth supplicant <mac-addr> [mask <mac-addr>] [max-reauth-req
<1-10>] [port-control
{auto|force-authorized|force-unauthorized}] [quiet-period
<1-65535>] [reauth-period <1-4294967295>] [supp-timeout
<1-65535>] [server-timeout <1-65535>] [reauthentication]
```

```
no auth supplicant-mac <macadd> [reauthentication]
```

Parameter	Description
<mac-addr>	MAC (hardware) address of the Supplicant entry in HHHH.HHHH.HHHH MAC address hexadecimal format.
`mask`	MAC mask
`port-control`	Port control commands.
`auto`	Allow port client to negotiate authentication.
`force-authorized`	Force port state to authorized.
`force-unauthorized`	Force port state to unauthorized.
`quiet-period`	Quiet period in the HELD state (default 60 seconds).
<1-65535>	Seconds for quiet period.
`reauth-period`	Seconds between reauthorization attempts (default 3600 seconds).
<1-4294967295>	Seconds for reauthorization attempts (reauth-period).
`supp-timeout`	Supplicant response timeout (default 30 seconds).
<1-65535>	Seconds for supplicant response timeout.
`server-timeout`	Authentication server response timeout (default 30 seconds).
<1-65535>	Seconds for authentication server response timeout.
`reauthentication`	Enable reauthentication on a port.

Parameter	Description
`max-reauth-req`	No of reauthentication attempts before becoming unauthorized (default 2).
<1-10>	Count of reauthentication attempts.

Default No supplicant MAC address for port authentication exists by default until first created with the **auth supplicant-mac** command. The defaults for parameters applied are as shown in the parameter table.

Mode Interface Configuration for an Ethernet port.

Examples To add the supplicant MAC address `0009.41A4.5943` to force authorized port control for interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth supplicant-mac 0009.41A4.5943
port-control force-authorized
```

To add the supplicant MAC address 0009.41A4.0000 with mask ffff.ffff.0000 to force authorized port control for interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth supplicant-mac 0009.41A4.5943 mask
ffff.ffff.0000 port-control force-authorized
```

To delete the supplicant MAC address `0009.41A4.5943` for interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth supplicant-mac 0009.41A4.5943
```

To reset reauthentication to disable for the supplicant MAC address `0009.41A4.5943`, for interface `eth1` use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth supplicant-mac 0009.41A4.5943
reauthentication
```

To reset reauthentication to disable for the supplicant MAC address `0009.41A4.5943`, for interface `port1.1.2` use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.1.2
awplus(config-if)# no auth supplicant-mac 0009.41A4.5943
reauthentication
```

Validation Commands

show dot1x interface

show running-config

auth timeout connect-timeout

Overview This command sets the connect-timeout period for the interface.

Use the **no** variant of this command to reset the connect-timeout period to the default (30 seconds).

Syntax

```
auth timeout connect-timeout <1-65535>
no auth timeout connect-timeout
```

Parameter	Description
<1-65535>	Seconds.

Default The connect-timeout default is 30 seconds.

Mode Interface Configuration for an Ethernet port.

Usage This command is used for Web-Authentication. If the connect-timeout has lapsed and the supplicant has the state **connecting**, then the supplicant is deleted. When auth-web-server session-keep or auth two-step enableis enabled, we recommend you configure a longer connect-timeout period.

Examples To set the connect-timeout period to `3600` for interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth timeout connect-timeout 3600
```

To reset the connect-timeout period to the default (30 seconds) for interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth timeout connect-timeout
```

Validation Commands show dot1x interface

auth timeout quiet-period

Overview This command sets the time period for which the authentication request is not accepted on a given interface, after the authentication request has failed an authentication.

Use the **no** variant of this command to reset quiet period to the default (60 seconds).

Syntax

```
auth timeout quiet-period <1-65535>
no auth timeout quiet-period
```

Parameter	Description
<1-65535>	Seconds.

Default The quiet period of port authentication is 60 seconds.

Mode Interface Configuration for an Ethernet port.

Examples To set the quiet period to `10` for interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth timeout quiet-period 10
```

To reset the quiet period to the default (60 seconds) for interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth timeout quiet-period
```

auth timeout reauth-period

Overview This command sets the timer for reauthentication on a given interface. The re-authentication for the supplicant (client device) is executed at this timeout. The timeout is only applied if the **auth reauthentication** command is applied.

Use the **no** variant of this command to reset the **reauth-period** parameter to the default (3600 seconds).

Syntax

```
auth timeout reauth-period <1-4294967295>
no auth timeout reauth-period
```

Parameter	Description
<1-4294967295>	Seconds.

Default The default reauthentication period for port authentication is 3600 seconds, when reauthentication is enabled on the port.

Mode Interface Configuration for an Ethernet port.

Examples To set the reauthentication period to 1 day for interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth timeout reauth-period 86400
```

To reset the reauthentication period to the default (3600 seconds) for interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth timeout reauth-period
```

Validation Commands show running-config

auth timeout server-timeout

Overview This command sets the timeout for the waiting response from the RADIUS server on a given interface.

The **no** variant of this command resets the server-timeout to the default (30 seconds).

Syntax

```
auth timeout server-timeout <1-65535>
no auth timeout server-timeout
```

Parameter	Description
<1-65535>	Seconds.

Default The server timeout for port authentication is 30 seconds.

Mode Interface Configuration for an Ethernet port.

Examples To set the server timeout to 120 seconds for interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth timeout server-timeout 120
```

To set the server timeout to the default (30 seconds) for interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth timeout server-timeout
```

auth-web enable

Overview This command enables Web-based authentication in Interface mode on the interface specified.

Use the **no** variant of this command to disable Web-based authentication on an interface.

Syntax

```
auth-web enable
no auth-web enable
```

Default Web-Authentication is disabled by default.

Mode Interface Configuration for an Ethernet port.

Usage You need to configure an IPv4 address for the Ethernet interface on which Web Authentication is running.

Examples To enable Web-Authentication on eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth-web enable
```

To disable Web-Authentication on eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth-web enable
```

Validation Commands show auth

show running-config

Related Commands aaa accounting auth-web default

aaa authentication auth-web

auth-web forward

Overview This command enables the Web-Authentication packet forwarding feature on the interface specified. This command also enables ARP forwarding, and adds forwarded packets to the **tcp** or **udp** port number specified.

The **no** variant of this command resets to the default setting of the packet forwarding feature on the interface.

Syntax `auth-web forward [<ip-address>] {arp|dhcp|dns|tcp <1-65535>|udp <1-65535>}`

`no auth-web forward [<ip-address>] {arp|dhcp|dns|tcp <1-65535>|udp <1-65535>}`

Parameter	Description
<ip-address>	Enable forwarding to the destination IPv4 address.
`arp`	Enable forwarding of ARP.
`dhcp`	Enable forwarding of DHCP (67/udp).
`dns`	Enable forwarding of DNS (53/udp).
`tcp`	Enable forwarding of TCP specified port number.
<1-65535>	TCP Port number.
`udp`	Enable forwarding of UDP specified port number.
<1-65535>	UDP Port number.

Default Packet forwarding for port authentication is enabled by default for “arp”, “dhcp” and “dns”.

Mode Interface Configuration for an Ethernet port.

Usage For more information about the *<ip-address>* parameter, and an example, see the “auth- web forward” section in the Alliedware Plus Technical Tips and Tricks.

Examples To enable the ARP forwarding feature on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth-web forward arp
```

To add the TCP forwarding port 137 on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth-web forward tcp 137
```

To add the DNS Server IP address 192.168.1.10 on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# switchport mode access
awplus(config-if)# auth-web enable
awplus(config-if)# auth-web forward 192.168.1.10 dns
```

To disable the ARP forwarding feature on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth-web forward arp
```

To delete the TCP forwarding port 137 on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth-web forward tcp 137
```

To delete the all of TCP forwarding on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth-web forward tcp
```

Validation Commands

show auth

show auth interface

show running-config

auth-web idle-timeout enable

Overview Use this command to enable the idle-timeout for client of web authentication on the interface.

The **no** variant of this command to disable the idle-timeout for client of web authentication on the interface.

Syntax

```
auth-web idle-timeout enable
no auth-web idle-timeout enable
```

Default The idle-timeout is disabled by default.

Mode Interface Mode and Auth Profile

Example To enable the idle-timeout on an interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config)# auth-web enable
awplus(config-if)# auth-web idle-timeout enable
```

To disable the idle-timeout on an interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth-web idle-timeout enable
```

Related Commands auth-web enable

auth-web idle-timeout timeout

auth-web idle-timeout timeout

Overview Use this command to set the timeout value for web authentication client in seconds. The client will be unauthorized when the elapsed time of no packet coming exceeds the timeout value.

The **no** variant of this command sets the timeout value to the default setting, 3600 seconds.

Syntax

```
auth-web idle-timeout timeout <300-86400>
no auth-web idle-timeout timeout
```

Parameter	Description
<300-86400>	Time in seconds.

Default The timeout is 3600 seconds by default.

Mode Interface Mode and Auth Profile

Example To set 30 minutes to the idle-timeout, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth-web idle-timeout timeout 1800
```

To set the idle-timeout to default, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth-web idle-timeout timeout
```

Related Commands auth-web enable

auth-web idle-timeout enable

auth-web max-auth-fail

Overview This command sets the number of authentication failures allowed before rejecting further authentication requests. When the supplicant (client device) fails more than has been set to the maximum number of authentication failures then login requests are refused during the quiet period.

The **no** variant of this command resets the maximum number of authentication failures to the default (three authentication failures).

Syntax

```
auth-web max-auth-fail <0-10>
no auth-web max-auth-fail
```

Parameter	Description
<0-10>	Lock count specified.

Default The **max-auth-fail** lock counter is set to three authentication failures by default.

Mode Interface Configuration for an Ethernet port.

Examples To set the lock count to 5 on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth-web max-auth-fail 5
```

To set the lock count to the default on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth-web max-auth-fail
```

Validation Commands show auth all

show auth interface

show running-config

Related Commands auth timeout quiet-period

auth-web method

Overview This command sets the authentication method of Web-Authentication that is used with RADIUS on the interface specified.

The **no** variant of this command sets the authentication method to PAP for the interface specified when Web-Authentication is also used with the RADIUS authentication method.

Syntax

```
auth-web method {eap-md5|pap}
no auth-web method
```

Parameter	Description
`eap-md5`	Enable EAP-MD5 as the authentication method.
`pap`	Enable PAP as the authentication method.

Default The Web-Authentication method is set to PAP by default.

Mode Interface Configuration for an Ethernet interface.

Example To set the Web-Authentication method to eap-md5 on interface `eth1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth-web method eap-md5
```

Validation Commands

show auth all

show auth interface

show running-config

auth-web-server dhcp ipaddress

Overview Use this command to assign an IP address and enable the DHCP service on the Web-Authentication server for supplicants (client devices).

Use the **no** variant of this command to remove an IP address and disable the DHCP service on the Web-Authentication server for supplicants.

Syntax

```
auth-web-server dhcp ipaddress <ip-address/prefix-length>
no auth-web-server dhcp ipaddress
```

Parameter	Description
<ip-addr/prefix-length>	The IPv4 address and prefix length assigned for the DHCP service on the Web-Authentication server for supplicants.

Default No IP address for the Web-Authentication server is set by default.

Mode Global Configuration

Usage See the Authentication Feature Overview and Configuration Guide for information about:

- using DHCP with web authentication, and
- restrictions regarding combinations of authentication enhancements working together

Note that DHCP Snooping and Web Authentication virtual DHCP server cannot be enabled at same time.

Examples To assign the IP address `10.0.0.1` to the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp ipaddress 10.0.0.1/8
```

To remove an IP address on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server dhcp ipaddress
```

Validation Commands show running-config

Related Commands show auth-web-server

auth-web-server dhcp lease

auth-web-server dhcp lease

Overview Use this command to set the DHCP lease time for supplicants (client devices) using the DHCP service on the Web-Authentication server.

Use the **no** variant of this command to reset to the default DHCP lease time for supplicants using the DHCP service on the Web-Authentication server.

Syntax

```
auth-web-server dhcp lease <20-60>
no auth-web-server dhcp lease
```

Parameter	Description
<20-60>	DHCP lease time for supplicants using the DHCP service on the Web-Authentication server in seconds.

Default The default DHCP lease time for supplicants using the DHCP service on the Web-Authentication server is set to 30 seconds.

Mode Global Configuration

Usage See the Authentication Feature Overview and Configuration Guide for information about:

- using DHCP with web authentication, and
- restrictions regarding combinations of authentication enhancements working together

Examples To set the DHCP lease time to 1 minute for supplicants using the DHCP service on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp lease 60
```

To reset the DHCP lease time to the default setting (30 seconds) for supplicants using the DHCP service on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server dhcp lease
```

Validation Commands show running-config

Related Commands show auth-web-server

auth-web-server dhcp ipaddress

auth-web-server dhcp-wpad-option

Overview This command sets the DHCP WPAD (Web Proxy Auto-Discovery) option for the Web-Authentication temporary DHCP service.

For more information and examples, see the "Web Auth Proxy" section in the Alliedware Plus Technical Tips and Tricks.

Use the **no** variant of this command to disable the DHCP WPAD function.

Syntax

```
auth-web-server dhcp wpad-option <url>
no auth-web-server dhcp wpad-option
```

Parameter	Description
<url>	URL to the server which gets a .pac file.

Default The Web-Authentication server DHCP WPAD option is not set.

Mode Global Configuration

Usage If the supplicant is configured to use WPAD, the supplicant's web browser will use TCP port 80 as usual. Therefore, the packet can be intercepted by Web-Authentication as normal, and the Web-Authentication Login page can be sent. However, after authentication, the browser does not know where to get the WPAD file and so cannot access external web pages. The WPAD file is usually named proxy.pac file and tells the browser what web proxy to use.

Use this command to tell the supplicant where it can get this file from. The switch itself can be specified as the source for this file, and it can deliver it to the supplicant on request.

Example To specify that the proxy.pac file is found on the server at 192.168.1.100, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp wpad-option
http://192.168.1.100/proxy/proxy.pac
```

Related Commands show auth-web-server

auth-web-server host-name

Overview This command assigns a hostname to the web authentication server.

Use the **no** variant of this command to remove the hostname from the web authentication server.

Syntax

```
auth-web-server host-name <hostname>
no auth-web-server host-name
```

Parameter	Description
<hostname>	URL string of the hostname

Default The web authentication server has no hostname.

Mode Global Configuration

Usage When the web authentication server uses HTTPS protocol, the web browser will validate the certificate. If the certificate is invalid, the web page gives a warning message before displaying server content. However, the web page will not give warning message if the server has a hostname same as the one stored in the installed certificate.

Examples To set the auth.example.com as the hostname of the web authentication server, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server host-name auth.example.com
```

To remove hostname auth.example.com from the web authentication server, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server host-name
```

Related Commands aaa authentication auth-web

auth-web enable

auth-web-server intercept-port

Overview This command specifies any additional TCP port numbers that the Web-Authentication server is to intercept.

Use the **no** variant of this command to stop intercepting the TCP port numbers.

Syntax

```
auth-web-server intercept-port {<1-65535>|any}
no auth-web-server intercept-port {<1-65535>|any}
```

Parameter	Description
<1-65535>	TCP port number.
any	Intercept all TCP packets

Default No additional TCP port numbers are intercepted by default.

Mode Global Configuration

Usage If this command is not specified, AlliedWare Plus Web-Authentication intercepts the supplicant's initial TCP port 80 connection to a web page and sends it the Web-Authentication Login page. However, if the supplicant is configured to use a web proxy, then it will usually be using TCP port 8080 (or another user configured port number). In this case Web-Authentication cannot intercept the connection.

To overcome this limitation you can use this command to tell the switch which additional port it should intercept, and then send the Web-Authentication Login page to the supplicant.

When the web authentication switch is in a guest network, the switch does not know the proxy server's port number in the supplicant's proxy setting. To overcome this limitation, you can use the **any** option in this command to intercept all TCP packets.

When you use this command in conjunction with a proxy server configured in the web browser, you must add the proxy server's network as a 'No Proxy' network. You can specify 'No Proxy' networks in the proxy settings in your web browser. For more information, see the "Web Auth Proxy" section in the Alliedware Plus Technical Tips and Tricks.

Example To additionally intercept port number 3128, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server intercept-port 3128
```

Related Commands show auth-web-server

auth-web-server ipaddress

Overview This command sets the IP address for the Web-Authentication server.

Use the **no** variant of this command to delete the IP address for the Web-Authentication server.

Syntax

```
auth-web-server ipaddress <ip-address>
no auth-web-server ipaddress
```

Parameter	Description
<ip-address>	Web-Authentication server dotted decimal IP address in A.B.C.D format.

Default The Web-Authentication server address on the system is not set by default.

Mode Global Configuration

Examples To set the IP address `10.0.0.1` to the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ipaddress 10.0.0.1
```

To delete the IP address from the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ipaddress
```

Validation Commands

show auth all

show auth-web-server

show running-config

auth-web-server login-url

Overview This command sets the web-authentication login page URL.

Use the **no** variant of this command to delete the set URL.

Syntax

```
auth-web-server login-url <URL>
no auth-web-server login-url
```

Parameter	Description
<URL>	Set login page URL

Default The built-in login page is set by default.

Mode Global Configuration

Examples To set http://example.com/login.html as the login page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server login-url
http://example.com/login.html
```

To unset the login page URL, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server login-url
```

Related Commands show running-config

auth-web-server page logo

Overview This command sets the type of logo that will be displayed on the web authentication page.

Use the **no** variant of this command to set the logo type to **auto**.

Syntax

```
auth-web-server page logo {auto|default|hidden}
no auth-web-server page logo
```

Parameter	Description
`auto`	Display the custom logo if installed; otherwise display the default logo
`default`	Display the default logo
`hidden`	Hide the logo

Default Logo type is **auto** by default.

Mode Global Configuration

Examples To display the default logo with ignoring installed custom logo, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page logo default
```

To set back to the default logo type **auto**, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page logo
```

Validation Commands show auth-web-server page

auth-web-server page sub-title

Overview This command sets the custom sub-title on the web authentication page.

Use the **no** variant of this command to reset the sub-title to its default.

Syntax

```
auth-web-server page sub-title {hidden|text <sub-title>}
no auth-web-server page sub-title
```

Parameter	Description
`hidden`	Hide the sub-title
<sub-title>	Text string of the sub-title

Default "Allied-Telesis" is displayed by default.

Mode Global Configuration

Examples To set the custom sub-title, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page sub-title text Web
Authentication
```

To hide the sub-title, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page sub-title hidden
```

To change back to the default title, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page sub-title
```

Validation Commands show auth-web-server page

auth-web-server page success-message

Overview This command sets the success message on the web-authentication page.

Use the **no** variant of this command to remove the success message.

Syntax

```
auth-web-server page success-message text <success-message>
no auth-web-server page success-message
```

Parameter	Description
<success-message>	Text string of the success message

Default No success message is set by default.

Mode Global Configuration

Examples To set the success message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page success-message text Your success message
```

To unset the success message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page success-message
```

Validation Commands show auth-web-server page

auth-web-server page title

Overview This command sets the custom title on the web authentication page.

Use the **no** variant of this command to remove the custom title.

Syntax

```
auth-web-server page title {hidden|text <title>}
no auth-web-server page title
```

Parameter	Description
`hidden`	Hide the title
<title>	Text string of the title

Default "Web Access Authentication Gateway" is displayed by default.

Mode Global Configuration

Examples To set the custom title on the web authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page title text Login
```

To hide the title on the web authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page title hidden
```

To unset the custom title on the web authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page title
```

Validation Commands show auth-web-server page

auth-web-server page welcome-message

Overview This command sets the welcome message on the web-authentication page.

Use the **no** variant of this command to remove the welcome message.

Syntax

```
auth-web-server page welcome-message text <welcome-message>
no auth-web-server page welcome-message
```

Parameter	Description
<welcome-message>	Text string of the welcome message

Default No welcome message is set by default.

Mode Global Configuration

Examples To set the welcome message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page welcome-message text Your welcome message
```

To remove the welcome message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page welcome-message
```

Validation Commands show auth-web-server page

auth-web-server ping-poll enable

Overview This command enables the ping polling to the supplicant (client device) that is authenticated by Web-Authentication.

The **no** variant of this command disables the ping polling to the supplicant that is authenticated by Web-Authentication.

Syntax

```
auth-web-server ping-poll enable
no auth-web-server ping-poll enable
```

Default The ping polling feature for Web-Authentication is disabled by default.

Mode Global Configuration

Examples To enable the ping polling feature for Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll enable
```

To disable the ping polling feature for Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll enable
```

Validation Commands show auth-web-server

show running-config

auth-web-server ping-poll failcount

Overview This command sets a fail count for the ping polling feature when used with Web-Authentication. The **failcount** parameter specifies the number of unanswered pings. A supplicant (client device) is logged off when the number of unanswered pings are greater than the failcount set with this command.

Use the **no** variant of this command to resets the fail count for the ping polling feature to the default (5 pings).

Syntax

```
auth-web-server ping-poll failcount <1-100>
no auth-web-server ping-poll failcount
```

Parameter	Description
<1-100>	Count.

Default The default failcount for ping polling is 5 pings.

Mode Global Configuration

Examples To set the failcount of ping polling to 10 pings, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll failcount 10
```

To set the failcount of ping polling to default, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll failcount
```

Validation Commands show auth-web-server

show running-config

auth-web-server ping-poll interval

Overview This command is used to change the ping poll interval. The interval specifies the time period between pings when the supplicant (client device) is reachable.

Use the **no** variant of this command to reset to the default period for ping polling (30 seconds).

Syntax

```
auth-web-server ping-poll interval <1-65535>
no auth-web-server ping-poll interval
```

Parameter	Description
<1-65535>	Seconds.

Default The interval for ping polling is 30 seconds by default.

Mode Global Configuration

Examples To set the interval of ping polling to 60 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll interval 60
```

To set the interval of ping polling to the default (30 seconds), use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll interval
```

Validation Commands show auth-web-server

show running-config

auth-web-server ping-poll reauth-timer-refresh

Overview This command modifies the **reauth-timer-refresh** parameter for the Web-Authentication feature. The **reauth-timer-refresh** parameter specifies whether a re-authentication timer is reset and when the response from a supplicant (a client device) is received.

Use the **no** variant of this command to reset the **reauth-timer-refresh** parameter to the default setting (disabled).

Syntax

```
auth-web-server ping-poll reauth-timer-refresh
no auth-web-server ping-poll reauth-timer-refresh
```

Default The `reauth-timer-refresh` parameter is disabled by default.

Mode Global Configuration

Examples To enable the `reauth-timer-refresh` timer, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll reauth-timer-refresh
```

To disable the `reauth-timer-refresh` timer, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll
reauth-timer-refresh
```

Validation Commands show auth-web-server

show running-config

auth-web-server ping-poll timeout

Overview This command modifies the ping poll **timeout** parameter for the Web-Authentication feature. The **timeout** parameter specifies the time in seconds to wait for a response to a ping packet.

Use the **no** variant of this command to reset the timeout of ping polling to the default (1 second).

Syntax

```
auth-web-server ping-poll timeout <1-30>
no auth-web-server ping-poll timeout
```

Parameter	Description
<1-30>	Seconds.

Default The default timeout for ping polling is 1 second.

Mode Global Configuration

Examples To set the timeout of ping polling to 2 seconds, use the command:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll timeout 2
```

To set the timeout of ping polling to the default (1 second), use the command:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll timeout
```

Validation Commands show auth-web-server

show running-config

auth-web-server port

Overview This command sets the HTTP port number for the Web-Authentication server.

Use the **no** variant of this command to reset the HTTP port number to the default (80).

Syntax

```
auth-web-server port <port-number>
no auth-web-server port
```

Parameter	Description
<port-number>	Set the local Web-Authentication server port within the TCP port number range 1 to 65535.

Default The Web-Authentication server HTTP port number is set to 80 by default.

Mode Global Configuration

Examples To set the HTTP port number 8080 for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server port 8080
```

To reset to the default HTTP port number 80 for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server port
```

Validation Commands show auth-web-server

show running-config

auth-web-server redirect-delay-time

Overview Use this command to set the delay time in seconds before redirecting the supplicant to a specified URL when the supplicant is authorized.

Use the variant **no** to reset the delay time set previously.

Syntax

```
auth-web-server redirect-delay-time <5-60>
no auth-web-server redirect-delay-time
```

Parameter	Description
`redirect-delay-time`	Set the delay time before jumping to a specified URL after the supplicant is authorized.
<5-60>	The time in seconds.

Default The default redirect delay time is 5 seconds.

Mode Global Configuration

Examples To set the delay time to 60 seconds for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server redirect-delay-time 60
```

To reset the delay time, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server redirect-delay-time
```

Validation Command show auth-web-servershow running-config

Related Commands auth-web-server redirect-url

show auth-web-server

auth-web-server blocking-mode

auth-web-server redirect-url

Overview This command sets a URL for supplicant (client device) authentication. When a supplicant is authorized it will be automatically redirected to the specified URL. Note that if the http redirect feature is used then this command is ignored.

Use the **no** variant of this command to delete the URL string set previously.

Syntax

```
auth-web-server redirect-url <url>
no auth-web-server redirect-url
```

Parameter	Description
<url>	URL (hostname or dotted IP notation).

Default The redirect URL for the Web-Authentication server feature is not set by default (null).

Mode Global Configuration

Examples To enable and set redirect a URL string `www.alliedtelesis.com` for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server redirect-url
http://www.alliedtelesis.com
```

To delete a redirect URL string, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server redirect-url
```

Validation Commands show auth-web-server

show running-config

Related Commands auth-web-server http-redirect (deleted)

auth-web-server redirect-delay-time

auth-web-server session-keep

Overview This command enables the session-keep feature to jump to the original URL after being authorized by Web-Authentication.

Use the **no** variant of this command to disable the session keep feature.

Syntax
```
auth-web-server session-keep
no auth-web-server session-keep
```

Default The session-keep feature is disabled by default.

Mode Global Configuration

Usage This function doesn't ensure to keep session information in all cases. Authenticated supplicant may be redirected to unexpected page when session-keep is enabled. This issue occurred by supplicant sending HTTP packets automatically after authentication page is displayed and the URL is written.

Examples To enable the session-keep feature, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server session-keep
```

To disable the session-keep feature, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server session-keep
```

Validation Commands show auth-web-server

show running-config

auth-web-server ssl

Overview This command enables HTTPS functionality for the Web-Authentication server feature.

Use the **no** variant of this command to disable HTTPS functionality for the Web-Authentication server.

Syntax
```
auth-web-server ssl
no auth-web-server ssl
```

Default HTTPS functionality for the Web-Authentication server feature is disabled by default.

Mode Global Configuration

Examples To enable HTTPS functionality for the Web-Authentication server feature, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ssl
```

To disable HTTPS functionality for the Web-Authentication server feature, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ssl
```

Validation Commands show auth-web-server

show running-config

auth-web-server ssl intercept-port

Overview Use this command to register HTTPS intercept port numbers when the HTTPS server uses custom port number (not TCP port number 443).

Note that you need to use the **auth-web-server intercept-port** command to register HTTP intercept port numbers.

Use the **no** variant of this command to delete registered port number.

Syntax

```
auth-web-server ssl intercept-port <1-65535>
no auth-web-server ssl intercept-port <1-65535>
```

Parameter	Description
<1-65535>	TCP port number in the range from 1 through 65535

Default 443/TCP is registered by default.

Mode Global Configuration

Examples To register HTTPS port number 3128, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ssl intercept-port 3128
```

To delete HTTPS port number 3128, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ssl intercept-port 3128
```

Validation Commands show auth-web-server

Related Commands auth-web-server intercept-port

copy proxy-autoconfig-file

Overview Use this command to download the proxy auto configuration (PAC) file to your switch. The Web-Authentication supplicant can get the downloaded file from the system web server.

Syntax

```
copy <filename> proxy-autoconfig-file
```

Parameter	Description
<filename>	The URL of the PAC file.

Mode Privileged Exec

Example To download the PAC file to this device, use the command:

```
awplus# copy tftp://server/proxy.pac proxy-autoconfig-file
```

Related Commands

show proxy-autoconfig-file

erase proxy-autoconfig-file

copy web-auth-https-file

Overview Use this command to download the SSL server certificate for web-based authentication. The file must be in PEM (Privacy Enhanced Mail) format, and contain the private key and the server certificate.

Syntax

```
copy <filename> web-auth-https-file
```

Parameter	Description
<filename>	The URL of the server certificate file.

Mode Privileged Exec

Example To download the server certificate file `veriSign_cert.pem` from the TFTP server directory `server`, use the command:

```
awplus# copy tftp://server/veriSign_cert.pem
web-auth-https-file
```

Related Commands

auth-web-server ssl

erase web-auth-https-file

show auth-web-server

erase proxy-autoconfig-file

Overview Use this command to remove the proxy auto configuration file.

Syntax
```
erase proxy-autoconfig-file
```

Mode Privileged Exec

Example To remove the proxy auto configuration file, use the command:
```
awplus# erase proxy-autoconfig-file
```

Related Commands
show proxy-autoconfig-file

copy proxy-autoconfig-file

erase web-auth-https-file

Overview Use this command to remove the SSL server certificate for web-based authentication.

Syntax
```
erase web-auth-https-file
```

Mode Privileged Exec

Example To remove the SSL server certificate file for web-based authentication use the command:

```
awplus# erase web-auth-https-file
```

Related Commands
auth-web-server ssl

copy web-auth-https-file

show auth-web-server

show auth

Overview This command shows authentication information for Web-based authentication.

Syntax

```
show auth [all]
```

Parameter	Description
`all`	Display all authentication information for each authenticated interface. This can be a static channel (or static aggregator), or a dynamic (or LACP) channel group, or a switch port.

Mode User Exec andPrivileged Exec

Example To display all Web-Authentication information, enter the command:

```
awplus# show auth all
```

Output Figure 7-1: Example output from the **show auth** command

```
awplus# show auth all
802.1X Port-Based Authentication Enabled
MAC-based Port Authentication Disabled
WEB-based Port Authentication Enabled
 RADIUS server address (auth): 150.87.17.192:1812
   Last radius message id: 4
Authentication Info for interface eth1
 portEnabled: true - portControl: Auto
 portStatus: Authorized
 reAuthenticate: disabled
 reAuthPeriod: 3600
 PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
 BE: suppTimeout: 30 - serverTimeout: 30
 CD: adminControlledDirections: in
 KT: keyTxEnabled: false
 critical: disabled
 guestVlan: disabled
 authFailVlan: disabled
 dynamicVlanCreation: disabled
 hostMode: single-host
 dot1x: enabled
   protocolVersion: 1
 authMac: disabled
 authWeb: enabled
   method: PAP
   maxAuthFail: 3
   packetForwarding:
     10.0.0.1 80/tcp
     dns
     dhcp
```

```
twoStepAuthentication:
   configured: enabled
   actual: enabled
supplicantMac: none
Supplicant name: oha
Supplicant address: 000d.6013.5398
   authenticationMethod: WEB-based Authentication
   Two-Step Authentication:
     firstAuthentication: Pass - Method: dot1x
     secondAuthentication: Pass - Method: web
   portStatus: Authorized - currentId: 3
   abort:F fail:F start:F timeout:F success:T
   PAE: state: Authenticated - portMode: Auto
   PAE: reAuthCount: 0 - rxRespId: 0
   PAE: quietPeriod: 60 - maxReauthReq: 2
   BE: state: Idle - reqCount: 0 - idFromServer: 2
   CD: adminControlledDirections: in - operControlledDirections: in
   CD: bridgeDetected: false
   KR: rxKey: false
   KT: keyAvailable: false - keyTxEnabled: false
```

show auth diagnostics

Overview This command shows Port-Authentication diagnostics, optionally for the specified interface, which may be an Ethernet port.

If no interface is specified then authentication diagnostics are shown for all interfaces.

Syntax `show auth diagnostics [interface <interface-list>]`

Parameter	Description
`interface`	Specify ports to show.
`<interface-list>`	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `eth1`) • a continuous range of interfaces, e.g. `eth1-2` • a comma-separated list of the above; e.g. `eth1, eth2`. The specified interfaces must exist.

Mode User Exec andPrivileged Exec

Output Figure 7-2: Example output from the **show auth diagnostics** command

```
Authentication Diagnostics for interface eth1
     Supplicant address: 00d0.59ab.7037
         authEnterConnecting: 2
         authEaplogoffWhileConnecting: 1
         authEnterAuthenticating: 2
         authSuccessWhileAuthenticating: 1
         authTimeoutWhileAuthenticating: 1
         authFailWhileAuthenticating: 0
         authEapstartWhileAuthenticating: 0
         authEaplogoggWhileAuthenticating: 0
         authReauthsWhileAuthenticated: 0
         authEapstartWhileAuthenticated: 0
         authEaplogoffWhileAuthenticated: 0
         BackendResponses: 2
         BackendAccessChallenges: 1
         BackendOtherrequestToSupplicant: 3
         BackendAuthSuccess: 1
```

Related Commands show dot1x interface

show auth interface

Overview This command shows the status for Port based authentication on the specified interface.

Use the optional **diagnostics** parameter to show authentication diagnostics for the specified interface. Use the optional **sessionstatistics** parameter to show authentication session statistics for the specified interface. Use the optional **statistics** parameter to show authentication diagnostics for the specified interface. Use the optional **supplicant** (client device) parameter to show the supplicant state for the specified interface.

Syntax
```
show auth interface <interface-list>
[diagnostics|sessionstatistics|statistics|supplicant [brief]]
```

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. eth1) • a continuous range of interfaces, e.g. `eth1-2` • a comma-separated list of the above; e.g. `eth1, eth2` The specified interfaces must exist.
`diagnostics`	Diagnostics.
`sessionstatistics`	Session statistics.
`statistics`	Statistics.
`supplicant`	Supplicant (client device).
`brief`	Brief summary of supplicant state.

Mode User Exec and Privileged Exec

Example To display the Port based authentication status for `eth1`, enter the command:

```
awplus# show auth interface eth1
```

If port-based authentication is not configured, the output will be

```
% Port-Control not configured on eth1
```

To display the Port based authentication status for `eth1`, enter the command:

```
awplus# show auth interface eth1
```

```
awplus# show auth interface eth1
Authentication Info for interface eth1
 portEnabled: true - portControl: Auto
 portStatus: Authorized
 reAuthenticate: disabled
 reAuthPeriod: 3600
 PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
 BE: suppTimeout: 30 - serverTimeout: 30
 CD: adminControlledDirections: in
 KT: keyTxEnabled: false
 critical: disabled
 guestVlan: disabled
 authFailVlan: disabled
 dynamicVlanCreation: disabled
 hostMode: single-host
 dot1x: enabled
   protocolVersion: 1
 authMac: disabled
 authWeb: enabled
   method: PAP
   maxAuthFail: 3
   packetForwarding:
     10.0.0.1 80/tcp
     dns
     dhcp
 twoStepAuthentication:
   configured: enabled
   actual: enabled
 supplicantMac: none
```

To display Port-Authentication diagnostics for `eth1`, enter the command:

```
awplus# show auth interface eth1 diagnostics
```

```
Authentication Diagnostics for interface eth1

Supplicant address: 00d0.59ab.7037
authEnterConnecting: 2
authEaplogoffWhileConnecting: 1
         authEnterAuthenticating: 2
         authSuccessWhileAuthenticating: 1
         authTimeoutWhileAuthenticating: 1
         authFailWhileAuthenticating: 0
         authEapstartWhileAuthenticating: 0
         authEaplogoggWhileAuthenticating: 0
         authReauthsWhileAuthenticated: 0
         authEapstartWhileAuthenticated: 0
         authEaplogoffWhileAuthenticated: 0
         BackendResponses: 2
         BackendAccessChallenges: 1
         BackendOtherrequestToSupplicant: 3
         BackendAuthSuccess: 1
```

To display Port-Authentication session statistics for `eth1`, enter the command:

```
awplus# show auth interface eth1 sessionstatistics
```

```
Authentication
session statistics for interface eth1
Authentication
session
statistics for interface eth1
     session user name: manager
         session authentication method: Remote server
         session time: 19440 secs
         session terminat cause: Not terminated yet
```

To display Port-Authentication statistics for `eth1`, enter the command:

```
awplus# show auth statistics interface eth1
```

To display the Port-Authenticated supplicant on interface `eth1`, enter the command:

```
awplus# show auth interface eth1 supplicant
```

show auth sessionstatistics

Overview This command shows authentication session statistics for the specified interface.

Syntax `show auth sessionstatistics [interface <interface-list>]`

Parameter	Description
`interface`	Specify ports to show.
<interface-list>	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `eth1`) • a continuous range of interfaces, e.g. `eth1-2` • a comma-separated list of the above; e.g. `eth1,eth2` The specified interfaces must exist.

Mode User Exec and Privileged Exec

Example To display authentication statistics for `eth1`, enter the command:

```
awplus# show auth sessionstatistics interface eth1
```

Output Figure 7-3: Example output from the **show auth sessionstatistics** command

```
Authentication
session statistics for interface eth1
Authentication
session
statistics for interface eth1
     session user name: manager
         session authentication method: Remote server
         session time: 19440 secs
         session terminat cause: Not terminated yet
```

show auth statistics interface

Overview This command shows the authentication statistics for the specified interface.

Syntax `show auth statistics interface <interface-list>`

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `eth1`) • a continuous range of interfaces, e.g. `eth1-2` • a comma-separated list of the above; e.g. `eth1,eth2` The specified interfaces must exist.

Mode User Exec and Privileged Exec

Example To display Port-Authentication statistics for `eth1`, enter the command:

```
awplus# show auth statistics interface eth1
```

show auth supplicant

Overview This command shows the supplicant (client device) state when Web-Authentication is configured for the switch. This command shows a summary when the optional **brief** parameter is used.

Syntax `show auth supplicant [<macadd>] [brief]`

Parameter	Description
<macadd>	Mac (hardware) address of the supplicant. Entry format is HHHH.HHHH.HHHH (hexadecimal).
`brief`	Brief summary of the supplicant state.

Mode Privileged Exec

Examples To display Web authenticated supplicant information on the device, enter the command:

```
awplus# show auth supplicant
```

show auth supplicant interface

Overview This command shows the supplicant (client device) state for the Web authenticated interface. This command shows a summary when the optional **brief** parameter is used.

Syntax

```
show auth-web supplicant interface <interface-list> [brief]
```

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `eth1`) • a continuous range of interfaces, e.g. `eth1-2` • a comma-separated list of the above; e.g. `eth1,eth2` The specified interfaces must exist.
`brief`	Brief summary of the supplicant state.

Mode User Exec and Privileged Exec

Examples To display the Port authenticated supplicant on the interface `eth1`, enter the command:

```
awplus# show auth supplicant interface eth1
```

To display brief summary output for the Port authenticated supplicant, enter the command:

```
awplus# show auth supplicant brief
```

show auth-web-server

Overview This command shows the Web-Authentication server configuration and status on the switch.

Syntax

```
show auth-web-server
```

Mode User Exec and Privileged Exec

Example To display Web-Authentication server configuration and status, enter the command:

```
awplus# show auth-web-server
```

Output Figure 7-4: Example output from the **show auth-web-server** command

```
Web authentication server
     Server status: enabled
     Server mode: none
     Server address: 192.168.1.1/24
       DHCP server enabled
       DHCP lease time: 20
       DHCP WPAD Option URL: http://192.168.1.1/proxy.pac
     HTTP Port No: 80
     Security: disabled
     Certification: default
     SSL Port No: 443
     Redirect URL: --
     Redirect Delay Time: 5
     HTTP Redirect: enabled
     Session keep: disabled
     PingPolling: disabled
     PingInterval: 30
     Timeout: 1
     FailCount: 5
     ReauthTimerReFresh: disabled
```

Related Commands

auth-web-server gateway (deleted)

auth-web-server http-redirect (deleted)

auth-web-server ipaddress

auth-web-server port

auth-web-server redirect-delay-time

auth-web-server redirect-url

auth-web-server session-keep

auth-web-server ssl

auth-web-server sslport (deleted)

show auth-web-server page

Overview This command displays the web-authentication page configuration and status.

Syntax

```
show auth-web-server page
```

Mode Privileged Exec

Examples To show the web-authentication page information, use the command:

```
awplus# show auth-web-server page
```

Table 7-1: Example output from the **show auth-web-server page** command on the console.

```
awplus#show auth-web-server page
Web authentication page
  Logo: auto
  Title: default
  Sub-Title: Web Authentication
  Welcome message: Your welcome message
  Success message: Your success message
```

Related Commands

auth-web forward

auth-web-server page logo

auth-web-server page sub-title

auth-web-server page success-message

auth-web-server page title

auth-web-server page welcome-message

show proxy-autoconfig-file

Overview This command displays the contents of the proxy auto configuration (PAC) file.

Syntax

```
show proxy-autoconfig-file
```

Mode Privileged Exec

Example To display the contents of the proxy auto configuration (PAC) file, enter the command:

```
awplus# show auth proxy-autoconfig-file
```

Output Figure 7-5: Example output from the **show proxy-autoconfig**-file

```
function FindProxyForURL(url,host)
{
 if (isPlainHostName(host) ||
     isInNet(host, “192.168.1.0”,”255.255.255.0”)) {
   return “DIRECT”;
}
 else {
   return “PROXY 192.168.110.1:8080”;
 }
}
```

Related Commands

copy proxy-autoconfig-file

erase proxy-autoconfig-file

8 AAA Commands

Introduction

Overview This chapter provides an alphabetical reference for AAA commands for Authentication, Authorization and Accounting. For more information, see the AAA Feature Overview and Configuration Guide.

aaa accounting auth-web default

Overview This command configures a default accounting method list for Web-based Port Authentication. The default accounting method list specifies what type of accounting messages are sent and specifies which RADIUS Servers the accounting messages are sent to. The default accounting method list is automatically applied to interfaces with Web-based Authentication enabled.

Use the **no** variant of this command to disable AAA accounting for Web-based Port Authentication globally.

Syntax

```
aaa accounting auth-web default {start-stop|stop-only|none}
group {<group-name>|radius}
```

```
no aaa accounting auth-web default
```

Parameter	Description
`start-stop`	Start and stop records to be sent.
`stop-only`	Stop records to be sent.
`none`	No accounting record to be sent.
`<group-name>`	Server group name.
`radius`	Use all RADIUS servers.

Default RADIUS accounting for Web-based Port Authentication is disabled by default.

Mode Global Configuration

Usage There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius** : use all RADIUS servers configured by radius-server host command
- **group** *<group-name>* : use the specified RADIUS server group configured with the aaa group server command

Configure the accounting event to be sent to the RADIUS server with the following options:

- **start-stop**: sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only**: sends a **stop** accounting message at the end of a session.
- **none**: disables accounting.

Examples To enable RADIUS accounting for Web-based Authentication, and use all available RADIUS Servers, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# aaa accounting auth-web default start-stop
group radius
```

To disable RADIUS accounting for Web-based Authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting auth-web default
```

Related Commands aaa authentication auth-web

aaa accounting update

Overview This command enables periodic accounting reporting to either the RADIUS or TACACS+ accounting server(s) wherever login accounting has been configured.

Note that unlimited RADIUS servers and up to four TACACS+ servers can be configured and consulted for accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, i.e. is unreachable.

Use the **no** variant of this command to disable periodic accounting reporting to the accounting server(s).

Syntax

```
aaa accounting update [periodic <1-65535>]
no aaa accounting update
```

Parameter	Description
`periodic`	Send accounting records periodically.
<1-65535>	The interval to send accounting updates (in minutes). The default is 30 minutes.

Default Periodic accounting update is disabled by default.

Mode Global Configuration

Usage Use this command to enable the device to send periodic AAA login accounting reports to the accounting server. When periodic accounting report is enabled, interim accounting records are sent according to the interval specified by the **periodic** parameter. The accounting updates are start messages.

If the **no** variant of this command is used to disable periodic accounting reporting, any interval specified by the **periodic** parameter is reset to the default of 30 minutes when accounting reporting is reenabled, unless this interval is specified.

Examples To configure the switch to send period accounting updates every 30 minutes, the default period, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting update
```

To configure the switch to send period accounting updates every 10 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting update periodic 10
```

To disable periodic accounting update wherever accounting has been configured, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting update
```

Related Commands

aaa accounting auth-web default

aaa accounting login

aaa authentication auth-web

Overview This command enables Web-based Port Authentication globally and allows you to enable an authentication method list (in this case, a list of RADIUS Servers). It is automatically applied to every interface running Web-based Port Authentication.

Use the **no** variant of this command to globally disable Web-based Port Authentication.

Syntax

```
aaa authentication auth-web default group {<group-name>|radius}
no aaa authentication auth-web default
```

Parameter	Description
<group-name>	Server group name.
`radius`	Use all RADIUS servers.

Default Web-based Port Authentication is disabled by default.

Mode Global Configuration

Usage There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius**: use all RADIUS servers configured by radius-server host command
- **group** *<group-name>*: use the specified RADIUS server group configured with the aaa group server command

Note that you need to configure an IPv4 address for the VLAN interface on which We Authentication is running.

Examples To enable Web-based Port Authentication globally for all RADIUS servers, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication auth-web default group radius
```

To disable Web-based Port Authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication auth-web default
```

Related Commands aaa accounting auth-web default

aaa login fail-delay

Overview Use this command to configure a gap between failed login attempts. This setting applies to login attempts via the console, SSH and Telnet.

Use the **no** variant of this command to reset the gap to the default (1 second).

Syntax

```
aaa login fail-delay [<1-10>]
no aaa login fail-delay [<1-10>]
```

Parameter	Description
<1-10>	The number of seconds required between login attempts

Default 1 second

Mode Global configuration

Example To make users wait 5 seconds before they can try to log in again after a failed login attempt, use the commands:

```
awplus# configure terminal
awplus(config)# aaa login fail-delay 5
```

Related Commands aaa authentication login

AlliedWare Plus Version 5.4.5-1.x

for SwitchBlade x8100 Series, SwitchBlade x908, x930 Series, x610 Series, x510 Series, IX5-28GPX, x310 Series, x230 Series, and x210 Series Switches, and for AR3050S and AR4050S Next-Generation Firewalls

Contents

Introduction

This release note describes the new features and enhancements in AlliedWare Plus software version 5.4.5-1.x. For more information, see the Command Reference for your switch or next-generation firewall (NGFW). Software file details for this version are listed in Table 1 below.

Caution: Software version 5.4.5 requires a release license for the SBx908 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.5 license certificate before you upgrade.

If an SBx908 or SBx8100 switch already has a version 5.4.5 license installed, that license also covers 5.4.5-1.x versions. Such switches do not need a new license before upgrading to version 5.4.5-1.x.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 206 and
- "Licensing this Software Version on a Control Card for an SBx8100 Series Switch" on page 208.

The first 5.4.5-1.x software version is numbered 5.4.5-1.1. The following table lists model names and software files for this version.

Table 1: Models and software file names

Models	Family	Software File	Date	GUI File
x210-9GT x210-16GT x210-24GT	x210 Series	x210-5.4.5-1.1.rel	07/2015	x210-gui_545_10.jar
x230-10GP x230-18GP x230-28GP	x230 Series	x230-5.4.5-1.1.rel	07/2015	x230-gui_545_09.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310 Series	x310-5.4.5-1.1.rel	07/2015	x310-gui_545_10.jar
IX5-28GPX	IX5	IX5-5.4.5-1.1.rel	07/2015	IX5-gui_545_06.jar
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 Series	x510-5.4.5-1.1.rel	07/2015	x510-gui_545_10.jar
x610-24Ts x610-24Ts-PoE+ x610-24Ts/X x610-24Ts/X-PoE+ x610-24SPs/X x610-48Ts x610-48Ts-PoE+ x610-48Ts/X x610-48Ts/X-PoE+	x610 Series	x610-5.4.5-1.1.rel	07/2015	x610-gui_545_10.jar

Table 1: Models and software file names

Models	Family	Software File	Date	GUI File
SwitchBlade x908 (see Table 2)	SBx908	SBx908-5.4.5-1.1.rel	07/2015	SBx908-gui_545_09.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930 Series	x930-5.4.5-1.1.rel	07/2015	x930-gui_545_11.jar
SBx81CFC400 SBx81CFC960	SBx8100 Series	SBx81CFC400-5.4.5-1.1.rel SBx81CFC960-5.4.5-1.1.rel	07/2015	SBx81CFC400-gui_545_09.jar SBx81CFC960-gui_545_09.jar
AR3050S AR4050S	NGFW Series	AR3050S-5.4.5-1.1.rel AR4050S-5.4.5-1.1.rel	07/2015	n/a

Under version 5.4.5, not all models of XEM are supported in the SwitchBlade x908. The following table lists which XEMs are and are not supported under version 5.4.5.

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.5-x.x

Product	Supported in version 5.4.5-x.x
XEM-1XP	No
XEM-2XP	Yes
XEM-2XS	Yes
XEM-2XT	Yes
XEM-12S	No
XEM-12T	No
XEM-12Sv2	Yes
XEM-12Tv2	Yes
XEM-24T	Yes

Caution: Using a software version file for the wrong switch or NGFW model may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

New Products

AlliedWare Plus version 5.4.5-1.x supports the following recently-released products.

x230-28GP

The Allied Telesis x230-28GP features 24 10/100/1000T PoE+ ports with 4 SFP Gigabit uplink ports. Its full feature-set and Power over Ethernet Plus (PoE+) are ideal for applications at the network edge.

The AT-x230-28GP supports today's converged networks with Gigabit Ethernet to the desktop, while powering VoIP phones, wireless access points, and IP security cameras.

For more information on the x230-28GP, see the *x230 Series Data Sheet, Installation Guide* and *Command Reference*. These documents are available from our website at **alliedtelesis.com/switches/x230**.

AT-x930-28GSTX

The Allied Telesis x930-28GSTX features 24 Gigabit combo ports with 4 10 Gigabit uplinks, providing the ability to mix copper and fiber connectivity for fully flexible deployment.

Long-distance stacking of up to 8 units supports distributed environments, and Allied Telesis Management Framework (AMF) and Wireless Manager provide unified network management for your entire wired and wireless infrastructure.

An optional module offers either 40 Gigabit stacking or network links, increasing the switch's versatility.

For more information on the AT-x930-28GSTX, see the *x930 Series Data Sheet, Installation Guide* and *Command Reference*. These documents are available from our website at **alliedtelesis.com/switches/x930**.

New Features and Enhancements

This section describes the new features in 5.4.5-1.x.

For a list of all new and modified commands, see "Command Changes in this Version" on page 204. For more information about all features on the switch or NGFW, see the Command Reference for your switch or NGFW.

Unless otherwise stated, all new features and enhancements are available on all switch and NGFW models running this version of AlliedWare Plus.

AMF Enhancements

Allied Telesis Management Framework (AMF) is a sophisticated suite of management tools that provides a simplified approach to network management. Common tasks are automated or made so simple that the day-to-day running of a network can be achieved without the need for highly trained, and expensive, network engineers. Powerful features like centralized management, auto-backup, auto-upgrade, auto-provisioning and auto-recovery enable plug-and-play networking and zero-touch management.

This software version includes the following enhancements to AMF:

AMF: 20-Node Master License for the AR4050S NGFW

A 20-node AMF Master feature license is now available for the AR4050S NGFW. The license model name is AT-FL-AR4-AM20.

AMF: 40-Node Master Licence for x930 Series Switches

A 40-node AMF Master feature license is now available for x930 Series switches. The license model name is AT-FL-x930-AM40.

The new license is in addition to the existing 20-node AMF license already available for the x930 Series.

AMF: Support for LACP Aggregations as AMF Links

AMF is now supported on dynamic channel-groups (LACP links) and AMF auto-recovery (reincarnation) is now supported via LACP links. The following sections describe this support.

- "LACP Global Passive Mode" on page 192
- "AMF auto-recovery via LACP" on page 194
- "AMF auto-recovery on NGFWs" on page 194

The following new command is supported:

- "lacp global-passive-mode enable" on page 193

The following existing commands can now also be used on dynamic LACP channel groups:

- switchport atmf-arealink remote-area
- switchport atmf-crosslink
- switchport atmf-link
- atmf provision

Using LACP aggregations as AMF links requires specific default behavior on the part of AMF nodes.

AMF requires that a completely unconfigured node, when attached to an AMF network, will successfully form an AMF connection, and become integrated into the network.

So, if the unconfigured node is attached to the network by an LACP aggregation, it must be possible for the unconfigured node to form an LACP aggregation.

Therefore AMF nodes need to be able, by default, to recognize when the connected ports on a neighbor device are a dynamic (LACP) aggregation, and then to negotiate an aggregated link with that neighbor's ports.

Specific functionality is now available in Alliedware Plus to support this default behavior. It is called LACP Global Passive Mode.

LACP Global Passive Mode

AlliedWare Plus devices can self-configure LACP channel-groups dynamically when they are connected to another device that has LACP channel-groups configured with Active Mode.

When a device starts from factory default configuration (or the start-up configuration file is missing), LACP global passive mode is turned on automatically. This is useful if you want to attach a new device to an existing LACP configured network. The newly added device will then automatically form LACP channel-groups.

This feature can be turned on or off by the following CLI commands in Global Configuration mode:

- **lacp global-passive-mode enable**
- **no lacp global-passive-mode enable**

The current configuration setting is displayed by using the command **show running-config**.

Dynamically learned LACP channel-groups

Dynamically learned LACP channel-groups behave the same as manually configured ones (which are configured by the **channel-group** command). The only exception is dynamically learned LACP channel-groups are not displayed in the running configuration. Currently known (both dynamically created and manually configured) LACP channel-groups are displayed in the following commands:

- **show etherchannel**
- **show etherchannel detail**

A dynamically learned LACP channel-group will be removed from the port, if:

- LACP global passive mode is turned off
- the port is removed (hot-swapped out)
- the port is down
- the **no channel-group** command is executed on that port.

A dynamically learned LACP channel-group will become a normal, manually configured, LACP channel-group and appear in the running configuration, if:

- you add any configuration in Interface Configuration mode of the aggregation or any member of the aggregation
- the **channel-group** command is executed in any member of the aggregation, or
- a new port is added to the aggregation.

Do not mix LACP configurations (manual & dynamic)

When LACP global passive mode is turned on (by using the **lacp global-passive-mode enable** command), we do not recommend using a mixed configuration in a LACP channel-group; i.e. some links are manually configured and others are dynamically learned in the same channel-group.

The details of the new **lacp global-passive-mode enable** command are:

lacp global-passive-mode enable

Overview

Use this command to enable LACP channel-groups to dynamically self-configure when they are connected to another device that has LACP channel-groups configured with Active Mode.

Syntax

```
lacp global-passive-mode enable
no lacp global-passive-mode enable
```

Default

Enabled

Mode

Global Configuration

Example

To enable global passive mode for LACP channel groups, use the command:

```
awplus(config)# lacp global-passive-mode enable
```

To disable global passive mode for LACP channel groups, use the command:

```
awplus(config)# no lacp global-passive-mode enable
```

AMF auto-recovery via LACP

Note that to support auto-recovery via LACP, the neighboring AMF node must configure LACP in active mode.

AMF auto-recovery on NGFWs

When an NGFW is configured as an AMF node over a WAN link, it cannot auto-recover from the AMF master directly, because if the NGFW fails, then the WAN link will fail as well. An NGFW first retrieves its configuration from the neighbour node by the existing "neighbour recovery" feature. With the restored configuration, the NGFW then starts auto-recovery from the AMF master.

AMF: Backup Redundancy

AMF Masters now support redundant backup to USB removable media on switches with USB slots. On the AR3050S and AR4050S, redundant backup is now only supported on SD removable media.

A new command enables or disables redundant backup to removable media:

- "atmf backup redundancy enable" on page 195

These commands are modified:

- "show atmf backup" on page 195
- "show atmf backup area" on page 195

If a Master or Controller has been configured with one or two remote file servers for backups, then the default behavior is no longer to send backups to removable media.

But, if removable media is present in the unit, and you wish to send backups to that media as well as to the remote file server(s), then this functionality can be enabled by the command **atmf backup redundancy enable**.

When this has been enabled, the rules are:

- If remote file servers are configured and accessible, then the Primary backup destination will always be one of the remote file servers.
- When a backup to the primary remote server is complete, the backup is first synchronized to the other remote file server (if a second remote server has been configured, and is accessible) and then to the removable media.
- The remote file server(s) will always be the preferred location for retrieving backups for a recovery, if available. The removable media will only be used for delivering files for a recovery if no remote file servers are accessible.
- The command **atmf backup synchronize** will synchronize the backed up files between all backup destinations - the remote file server(s) and the removable media.
- If the removable media has been absent for a while, and a new piece of removable media is installed into the Controller/Master node, the backed up files on the Remote File Server(s) will not be automatically synchronized over to the removable media. The synchronization must be initiated manually, using the command **atmf backup synchronize**.

atmf backup redundancy enable

Overview This command is used to enable/disable AMF backup redundancy.

Syntax
```
atmf backup redundancy enable
no atmf backup redundancy enable
```

Default Disabled

Mode Global Configuration

Usage If the AMF Master or Controller supports any removable media (SD card/USB), it uses the removable media as the redundant backup for the AMF data backup.

This feature is valid only if remote file servers are configured on the AMF Master or Controller.

Example To enable AMF backup redundancy

```
awplus# configure terminal
awplus(config)# atmf backup redundancy enable
```

To disable AMF backup redundancy

```
awplus# configure terminal
awplus(config)# no atmf backup redundancy enable
```

show atmf backup

The output of this command now displays whether AMF backup redundancy is enabled or disabled.

show atmf backup area

The output of this command now displays whether AMF backup redundancy is enabled or disabled.

AMF: Virtual Links for NGFWs

AMF virtual links are now supported on the AR3050S and AR4050S NGFWs (through the **atmf virtual-link** command). This allows for AMF to extend between sites that communicate with each other via the Internet, or to be able to hop over a section of non-AMF-capable equipment within a site. Virtual links are achieved by encapsulating AMF protocol packets within IP wrappers (L2TPv3 encapsulation), so that they can be transported across any arbitrary path that consists of IP forwarding devices.

For details about how to configure AMF virtual links, see the AMF Feature Overview and Configuration Guide.

The following new command has been added for all products:

- "atmf mtu" on page 196

The following commands have been modified:

- "tunnel local id" on page 196
- "tunnel remote id" on page 196
- "mtu (PPP)" on page 197
- "show atmf detail" on page 197

atmf mtu

Overview This command configures the AMF network Maximum Transmission Unit (MTU), which sets the maximum size of all ATMF packets generated from the device. The MTU value will be applied to the AMF Management VLAN, the AMF Domain VLAN and AMF Area links.

Syntax

```
atmf mtu <1300-1442>
no atmf mtu
```

Parameter	Description
<1300-1442>	The value of the maximum transmission unit for the AMF network, which sets the maximum size of all ATMF packets generated from the device.

Default 1300

Mode Global Configuration

Usage The default value of 1300 will work for all AMF networks (including those that involve virtual links over IPSec tunnels). If there are virtual links over IPsec tunnels anywhere in the AMF network, we recommend not changing this default. If there are no virtual links over IPsec tunnels, then this AMF MTU value may be increased for network efficiency.

Example To change the AMF network MTU to 1442, use the command:

```
awplus(config)# atmf network mtu 1442
```

tunnel local id

The valid values for the tunnel local id parameter have changed to <1-2147483647> (previously <1-4294967295>):

Syntax

```
tunnel local id <1-2147483647>
```

tunnel remote id

The valid values for the tunnel remote id parameter have changed to <1-2147483647> (previously <1-4294967295>):

Syntax

```
tunnel remote id <1-2147483647>
```

mtu (PPP)

The maximum size of the MTU that can now be specified for a PPP interface has been reduced to 1492 (previously 1582).

Syntax `mtu <68-1492>`

show atmf detail

The AMF network MTU is now displayed in the output from the show atmf detail command.

New parameter in the **show atmf detail** command:

Parameter	Description
`Network Mtu`	The network MTU for AMF, as configured on this device by the **atmf mtu** command.

AMF: Information about Discarded Packets

The command **show atmf link statistic** now displays a description of each type of discarded packet, to help with troubleshooting. The following example output shows the new descriptions.

```
ATMF Packet Discards:
Type0   0            : Gateway hello msg received from unexpected neighbor
Type1   0            : Stack hello msg received from unexpected neighbor
Type2   0            : Discard TX update bitmap packet - bad checksum
Type3   0            : Discard TX update packet - neighbor not in correct state
Type4   0            : Discard update packet - bad checksum or type
Type5   0            : Discard update packet - neighbor not in correct state
Type6   0            : Discard update bitmap packet - bad checksum or type
Type7   0            : Incarnation is not possible with the data received
Type8   2            : Discard crosslink hello received - not correct state
Type9   0            : Discard crosslink domain hello received on non crosslink
Type10  0            : Discard crosslink domain hello - not in correct state
Type11  0            : Crosslink uplink hello received on non crosslink port
Type12  0            : Discard crosslink uplink hello - not in correct state
Type13  0            : Wrong network-name for this ATMF
Type14  0            : Packet received on port is too long
Type15  0            : Bad protocol version, received on port
Type16  0            : Bad packet checksum calculation
Type17  0            : Bad authentication type
Type18  0            : Bad simple password
Type19  0            : Unsupported authentication type
Type20  0            : Discard packet - unknown neighbor
Type21  3            : Discard packet - port is shutdown
Type22  0            : Non broadcast hello msg received from unexpected neighbor
Type23  0            : Arealink hello msg received on non arealink port
Type24  20           : Discard arealink hello packet - not in correct state
Type25  0            : Discard arealink hello packet - failed basic processing
```

x930 Series: 40Gbps Network Switch Port Support

For x930 Series switches only.

The ports on the AT-StackQS card can now be configured as 40Gbps network switch ports, when AT-QSFPSR modules are installed. The ports are numbered port1.1.1 and port1.1.5.

To configure the AT-StackQS ports as network switch ports, you need to disable VCStack on the ports. There are two options for doing this:

- make the switch into a standalone switch, by running the command **no stack <*stack-id*> enable**, or
- use the 10Gbps front-panel SFP+ ports for stacking, by running the command **stack enable builtin-ports**

Then, run the **reboot** command to restart the switch. This reboots the switch with the ports configured as 40Gbps switch ports.

By default, the switch autonegotiates the port speed. You can instead use the **speed** command to manually set the port speed.

To fix the port speed at 40Gbps, use the following commands:

```
awplus(config)# interface port1.1.1,port1.1.5
awplus(config-if)# speed 40000
```

To set the ports to autonegiate their speed at only 40Gbps, use the following commands:

```
awplus(config)# interface port1.1.1,port1.1.5
awplus(config-if)# speed auto 40000
```

x930 Series: PoE Boost Mode Default Changed

For x930 Series switches only.

With this software update, the default state for PoE RPS Boost Mode has been changed from Enabled to **Disabled**. To enable it, use the command **power-inline rps boost**.

MSS Clamping

For the AR3050S and AR4050S NGFWs only.

Previously, TCP MSS clamping in AlliedWare Plus routers allowed you to set a feasible MSS value on PPP interfaces only. Now, TCP MSS clamping in AlliedWare Plus NGFWs allows you to set a feasible MSS value on the following interfaces:

- PPPoE
- Ethernet
- VTI Tunnels (IPSeC, GRE, IPv6, L2TP, OpenVPN)
- VLANs

You can also adjust TCP MSS automatically with respect to the MTU on the interface by using the **pmtu** option in the **ip tcp adjust-mss** command.

Previously, you could not set the IPv6 TCP MSS. Now you can set the IPv6 TCP MSS on an interface by using the **ipv6 tcp adjust-mss** command.

The commands for this enhancement are:

- **ip tcp adjust-mss**: This command sets the IPv4 TCP Maximum Segment Size (MSS) on an interface
- **ipv6 tcp adjust-mss**: This command sets the IPv6 TCP Maximum Segment Size (MSS) on an interface.

Optical Digital Diagnostic Monitoring MIB

For all AlliedWare Plus switches that support SFP and SFP+ pluggables.

The Digital Diagnostic Monitoring (DDM) MIB is an additional MIB that has been created so you can view optical pluggables such as SFPs and SFP+. You can query real-time properties of these pluggables such as temperature, transceiver supply voltage, transmit bias current, output and input power, and received loss of signal. All of these parameters are useful in monitoring the health of your pluggables installed in your device.

You can query these parameters from the MIB, or by using the **show system pluggable diagnostics** command.

The parameters that are provided by this MIB are specifically DDM parameters, as defined by the SFF committee's SFF-8472 standard.

The MIB will not provide information for those Optical Modules that do not support DDM.

Management ACLs

For x230, x310, IX5, x510, x610, x930, SBx908, and SBx8100 Series switches.

The Management ACLs feature restricts who is allowed remote access to your device using Telnet or SSH. This Management ACL is a simple security feature that binds an ACL (Access Control List) to the VTY's (Virtual Terminal Lines). This will allow or deny IP addresses included in the ACL to create a connection to your device. The commands are:

- **vty ipv6 access-class** and
- **vty access-class**.

Both commands have a **no** variant.

To check the ACLs' setting run the **show running-config** command.

GUI Timeout

For all AlliedWare Plus switches that can be accessed via a GUI.

The GUI Timeout feature is a security option that enables you to control the length of time a GUI session can remain open but inactive. It allows you to set a time in minutes and/or seconds to activate the timeout feature. After the GUI has been idle for the time set, you will see a dialogue box informing you that the session has been ended due to inactivity and you will have to login again. The GUI timeout feature is initially disabled.

Running the **gui-timeout** command configures the idle timeout period for a GUI session. An optional **minutes** parameter specifies the idle time in minutes from 0 through 35791 and an optional **seconds** parameter specifies the idle time in seconds from 0 through 2147483.

To check the status of the GUI timeout feature run the **show running-config** command.

Enhancements to Support for Microsoft NLB Clustering

Multicast MAC addresses

For SBx908, and SBx8100 with CFC400 or CFC960 only.

Previously, the **arp** command accepted only a single port to be entered and saved in the configuration file. With this update, the user can now specify multiple ports (for a multicast MAC address) for the packets to be forwarded out.

The **arp** command has been changed to accept a port list for static ARPs with multicast MAC addresses:

```
arp <ip-addr> <multicast-mac-address> [<port-list>]
```

The entire port list is now stored in the configuration file when a multicast address is entered with the ARP command. (For a non-multicast MAC address, only a single egress port can be configured, as before.)

The **show arp** command has been updated to show all of the ports, rather than a single port, associated with the ARP entry with a multicast address. The **show mac address-table** command output has also been updated to handle multicast entries differently and reflect that these multicast entries are actually attached to a multi-egress-port structure, and not the CPU interface.

Flooding in unicast mode

For SBx8100 with CFC960 only.

A new **unicast** parameter has been added to the **arp-mac-disparity** command.

When configured, if a disparate unicast ARP reply is received, the switch will install a "**flood to vlan**" entry for the target MAC address.

This option was added to support flooding of traffic to NLB clusters operating in unicast mode.

LACP Hashing on x510 Series Switches

For x510 Series switches only.

With this software update, the hashing algorithm used to decide which port of an aggregation a packet should be sent to, has been reverted to the algorithm that was used in previous releases, unless the **platform load-balance** command is used.

Legacy ifAdminStatus

With this software update, a new command **snmp-server legacy-adminstatus** has been added. This command sets the ifAdminStatus to reflect the operational state of the interface, rather than the administrative state. This was the behaviour in early AlliedWare Plus releases.

Important Considerations Before Upgrading to this Version

Licensing

From software version 5.4.4-0.4 onwards, AlliedWare Plus software releases need to be licensed for SBx908 and SBx8100 switches.

If you are upgrading to 5.4.5-1.x on your SBx908 or SBx8100 switch, please ensure you have a 5.4.5 license on your switch. To obtain a license, contact your authorized Allied Telesis support center. You will need to provide the MAC addresses of the switches you want to license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 206 and
- "Licensing this Software Version on a Control Card for an SBx8100 Series Switch" on page 208.

Upgrading a VCStack

This version supports VCStack "reboot rolling" upgrades. With the **reboot rolling** command, you can reduce downtime when upgrading a VCStack.

You can use the **reboot rolling** command to upgrade to any 5.4.5-1.x version from 5.4.5-0.x or from any 5.4.4-x.x version.

You cannot use rolling reboot to upgrade directly to 5.4.5-1.x from 5.4.3-x.x releases. If you wish to use rolling reboot, you must first use it to upgrade from 5.4.3-0.0 to 5.4.4-0.x, then from 5.4.4-0.x to 5.4.5-1.x.

Forming or extending a VCStack

If you create a VCStack from switches that are running different software versions, auto-synchronization ensures that all members will run the same software version when they boot up.

Auto-synchronization is supported between all versions of 5.4.5-1.x, 5.4.5-0.x and 5.4.4-2.x or later. It is not supported between 5.4.5-x.x and earlier versions of 5.4.4 (5.4.4-1.x or 5.4.4-0.x).

Before you add a new switch to a stack, make sure the new switch's software version is compatible with the stack's version. If the new switch is running an incompatible version, it cannot join the stack until you have manually upgraded it.

AMF software version compatibility

We strongly recommend that all switches in an AMF network run the same software release.

If this is not possible, switches running version 5.4.5-0.x or 5.4.5-1.x are compatible with switches running version 5.4.3-2.6 and later, or any 5.4.4 version.

Upgrading all switches in an AMF network

This version supports upgrades across AMF networks. There are two methods for upgrading firmware on an AMF network:

- Reboot-rolling, which upgrades and reboots each switch in turn
- Distribute firmware, which upgrades each switch, but does not reboot them. This lets you reboot the switches at a minimally-disruptive time.

You can use either of these methods to upgrade to this software version.

You can use these methods to upgrade to this version from 5.4.3-2.6 and later.

In summary, the process for upgrading firmware on an AMF network is:

1. Copy the release .rel files for each switch family to the media location you intend to upgrade from (Flash memory, SD card, USB stick etc).
2. Decide which AMF upgrade method is most suitable.
3. Initiate the AMF network upgrade using the selected method. To do this:
    a. create a working-set of the switches you want to upgrade
    b. enter the command **atmf reboot-rolling <*location*>** or **atmf distribute-firmware <*location*>** where **<*location*>** is the location of the .rel files.
    c. Check the console messages to make sure that all switches are “release ready”. If they are, follow the prompts to perform the upgrade.

ISSU (In-Service Software Upgrade) on SBx8100 with CFC960

ISSU is available on standalone SBx8100 Series switches with dual CFC960 control cards, and on switches using VCStack Plus™ to create a single virtual unit out of two chassis (where each chassis has a pair of CFC960 control cards). ISSU allows you to upgrade the software release running on the CFCs with no disruption to network traffic passing through the chassis.

This minor release cannot be upgraded from any previous release using ISSU.

For each software change on these platforms, the change will take effect as indicated when:

- CFCs upgraded: The change will apply once all CFCs have rebooted and are running the same SW version.
- ISSU Complete: The change will apply once all cards in the system are running the same SW version.

Please refer to the ISSU compatibility matrix below to determine ISSU release compatibility. In the matrix:

- "C" (compatible) indicates that you **can** use ISSU to upgrade from the "FROM" release to the "TO" release.
- "I" (incompatible) indicates that you **cannot** use ISSU to upgrade from the "FROM" release to the "TO" release.

		TO			
	RELEASE	**5.4.5-0.2**	**5.4.5-0.3**	**5.4.5-0.4**	**5.4.5-1.1**
FROM	**5.4.5-0.1**	**C**	**C**	**I**	**I**
	5.4.5-0.2		**C**	**I**	**I**
	5.4.5-0.3			**I**	**I**
	5.4.5-0.4				**I**
	5.4.5-1.1				

Command Changes in this Version

The following table lists new and modified commands for the features that have been modified in this version.

Table 3: New and modified commands in 5.4.5-1.x. This table also indicates which devices the change applies to

Command	Status	x210	x230	x310	IX5	x510	x610	x908	x930	SBx8100 CFC400	SBx8100 CFC960	AR3050S	AR4050S	Description
atmf backup redundancy enable	New	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	This command is used to enable/disable AMF backup redundancy.
atmf mtu	New	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	This command configures the AMF network Maximum Transmission Unit (MTU). The MTU value will be applied to the AMF Management VLAN, the AMF Domain VLAN and AMF Area links.
lacp global-passive-mode enable	New	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	This command enables LACP channel-groups to dynamically self-configure when they are connected to another device that has LACP channel-groups configured with Active Mode.
mtu (PPP)	Modified	N	N	N	N	N	N	N	N	N	N	Y	Y	The maximum value of MTU size that can now be specified for a PPP interface has been reduced to 1492 (previously 1582).
show atmf backup	Modified	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	The output of this command now displays whether AMF backup redundancy is enabled or disabled.
show atmf backup area	Modified	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	The output of this command now displays whether AMF backup redundancy is enabled or disabled.
show atmf detail	Modified	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	The AMF network MTU is now displayed in the output from this command.
tunnel local id	Modified	N	N	N	N	N	N	N	N	N	N	Y	Y	The valid values for the tunnel local id parameter have changed to <1-2147483647> (previously <1-4294967295>)
tunnel remote id	Modified	N	N	N	N	N	N	N	N	N	N	Y	Y	The valid values for the tunnel remote id parameter have changed to <1-2147483647> (previously <1-4294967295>)
show atmf link statistic	Modified	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	The output of this command now displays a description of each type of discarded packet, to help with troubleshooting.
ip tcp adjust-mss	Modified	N	N	N	N	N	N	N	N	N	N	Y	Y	This command sets the IPv4 TCP Maximum Segment Size (MSS) on an interface. TCP MSS clamping in AlliedWare Plus NGFWs now allows you to set a feasible MSS value on the following interfaces: PPPoE, Ethernet, VLAN, and VTI Tunnels (IPSec, GRE, IPv6, L2TP, OpenVPN).
ipv6 tcp adjust-mss	New	N	N	N	N	N	N	N	N	N	N	Y	Y	This command sets the IPv6 TCP Maximum Segment Size (MSS) on an interface.
vty access-class	New	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	This command configures the Management ACLs feature, which controls security for remote access by Telnet or SSH to your device using standard access control lists.

Table 3: New and modified commands in 5.4.5-1.x. This table also indicates which devices the change applies to(cont.)

Command	Status	x210	x230	x310	IX5	x510	x610	x908	x930	SBx8100 CFC400	SBx8100 CFC960	AR3050S	AR4050S	Description
vty ipv6 access-class	New	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	This command configures the Management ACLs feature, which controls security for remote access by Telnet or SSH to your device using standard access control lists.
gui-timeout	New	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N	N	This command configures the GUI Timeout feature, which is a security option that allows you to control the length of time a GUI session can remain open but inactive. It allows you to set a time in minutes and/or seconds to activate the timeout feature. After the GUI has been idle for the time set, you will have to login again.
arp	Modified	N	N	N	N	N	N	Y	N	Y	Y	N	N	In this command, you can now specify multiple ports (for a multicast MAC address) for the packets to be forwarded out.
show arp	Modified	N	N	N	N	N	N	Y	N	Y	Y	N	N	The output of this command has been updated to show all of the ports associated with an ARP entry, when multiple ports have been associated with the ARP entry that has a multicast address.
show mac address-table	Modified	N	N	N	N	N	N	Y	N	Y	Y	N	N	The output of this command has been modified for multicast MAC address entries. It now reflects that these multicast entries are actually attached to a multi-egress-port structure, and not the CPU interface.
arp-mac-disparity	Modified	N	N	N	N	N	N	N	N	N	Y	N	N	A new **unicast** parameter has been added to this command. When configured, if a disparate unicast ARP reply is received, the switch will install a "**flood to vlan**" entry for the target MAC address. This option was added to support flooding of traffic to NLB clusters operating in unicast mode.
snmp-server legacy-adminstatus	New	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	This command sets the ifAdminStatus to reflect the operational state of the interface, rather than administrative state. This was the behaviour in early AlliedWare Plus releases.
power-inline rps boost	Modified	N	N	N	N	N	N	N	Y	N	N	N	N	The default state for PoE RPS Boost Mode has been changed from Enabled to Disabled on x930 Series switches.

Licensing this Software Version on an SBx908 Switch

Release licenses are applied with the **license certificate** command, then validated with the **show license** or **show license brief** commands. Follow these steps:

- Obtain the MAC address for a switch
- Obtain a release license for a switch
- Apply a release license on a switch
- Confirm release license application

Step 1: Obtain the MAC address for a switch

A release license is tied to the MAC address of the switch.

Switches may have several MAC addresses. Use the **show system mac license** command to show the switch MAC address for release licensing:

```
awplus# show system mac license
MAC address for licensing:
eccd.6d9d.4eed
```

Step 2: Obtain a release license for a switch

Contact your authorized Allied Telesis support center to obtain a release license.

Step 3: Apply a release license on a switch

Use the **license certificate** command to apply a release license to your switch.

Note the license certificate file can be stored on internal flash memory, or an external SD card, or on a server accessible by the TFTP, SCP or HTTP protocols.

Entering a valid release license changes the console message displayed about licensing:

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus#license certificate demo1.csv
A restart of affected modules may be required.
Would you like to continue? (y/n): y
11:58:14 awplus IMI[1696]: SFL: The current software is licensed. Exiting
unlicensed mode.

Stack member 1 installed 1 license

1 license installed.
```

Step 4: Confirm release license application

On a stand-alone switch, use the commands **show license** or **show license brief** to confirm release license application.

On a stacked switch, use the command **show license member** or **show license brief member** to confirm release license application.

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus switches:

```
awplus# show license
OEM Territory : ATI USA
Software Licenses
------------------------------------------------------------------------
Index                          : 1
License name                   : Base License
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Mar-2015
License expiry date            : N/A
Features included              : EPSR-MASTER, IPv6Basic, MLDSnoop, OSPF-64,
                                 RADIUS-100, RIP, VRRP

Index                          : 2
License name                   : 5.4.5-rl
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Mar-2015
License expiry date            : N/A
Release                        : 5.4.5
```

Licensing this Software Version on a Control Card for an SBx8100 Series Switch

Release licenses are applied with the **license certificate** command, then validated with the **show license** or **show license brief** commands. Follow these steps:

- Obtain the MAC address for a control card
- Obtain a release license for a control card
- Apply a release license on a control card
- Confirm release license application

If your control card is in a stacked chassis, you do not need to perform these steps on each chassis in the stack, only on the stack master.

If your license certificate contains release licenses for each control card present in a stacked chassis, entering the **license certificate** command on the stack master will automatically apply the release licenses to all the control cards within the stack.

Step 1: Obtain the MAC address for a control card

A release license is tied to the control card MAC address in a chassis.

Chassis may have several MAC addresses. Use the **show system mac license** command to show the control card MAC address for release licensing. Note the MAC addresses for each control card in the chassis. The chassis MAC address is not used for release licensing. Use the card MAC address for release licensing.

```
awplus#show system mac license

MAC address for licensing:


Card                MAC Address
-----------------------------------
1.5                 eccd.6d9e.3312
1.6                 eccd.6db3.58e7

Chassis MAC Address eccd.6d7b.3bc2
```

Step 2: Obtain a release license for a control card

Contact your authorized Allied Telesis support center to obtain a release license.

Step 3: Apply a release license on a control card

Use the **license certificate** command to apply a release license to each control card installed in your chassis or stack.

Note the license certificate file can be stored on internal flash memory, a USB drive, or on a server accessible by the TFTP, SCP or HTTP protocols.

Entering a valid release license changes the console message displayed about licensing:

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus# license certificate demo1.csv
A restart of affected modules may be required.
Would you like to continue? (y/n): y
11:58:14 awplus IMI[1696]: SFL: The current software is licensed. Exiting
unlicensed mode.

Stack member 1 installed 1 license

1 license installed.
```

Step 4: Confirm release license application

On a stand-alone chassis, use the commands **show license** or **show license brief** to confirm release license application.

On a stacked chassis, use the command **show license member** or **show license brief member** to confirm release license application.

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus chassis:

```
awplus# show license
OEM Territory : ATI USA
Software Licenses
------------------------------------------------------------------------
Index                          : 1
License name                   : Base License
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Mar-2015
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                                 Virtual-MAC, VRRP

Index                          : 2
License name                   : 5.4.5-rl
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Mar-2015
License expiry date            : N/A
Release                        : 5.4.5
```

Installing this Software Version

Caution: Software versions 5.4.5-x.x require a release license for the SBx908 and SBx8100 switches. Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 206 and
- "Licensing this Software Version on a Control Card for an SBx8100 Series Switch" on page 208.

To install and enable this software version, use the following steps:

1. Copy the software version file (.rel) onto your TFTP server.

2. If necessary, delete or move files to create space in the switch's Flash memory for the new file. To see the memory usage, use the command:

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

   ```
   awplus# del <filename>
   ```

   You cannot delete the current boot file.

3. Copy the new release from your TFTP server onto the switch.

   ```
   awplus# copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.

4. Move from Privileged Exec mode to Global Configuration mode, using:

   ```
   awplus# configure terminal
   ```

   Then set the switch to reboot with the new software version. For example, for 5.4.5-1.1, use one of the following commands:

Switch	Command
x210 series	`awplus(config)# boot system x210-5.4.5-1.1.rel`
x230 series	`awplus(config)# boot system x230-5.4.5-1.1.rel`
x310 series	`awplus(config)# boot system x310-5.4.5-1.1.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.4.5-1.1.rel`
x510 series	`awplus(config)# boot system x510-5.4.5-1.1.rel`
x610 series	`awplus(config)# boot system x610-5.4.5-1.1.rel`
SBx908	`awplus(config)# boot system SBx908-5.4.5-1.1.rel`
x930 series	`awplus(config)# boot system SBx930-5.4.5-1.1.rel`
SBx8100 with CFC400	`awplus(config)# boot system SBx81CFC400-5.4.5-1.1.rel`
SBx8100 with CFC960	`awplus(config)# boot system SBx81CFC960-5.4.5-1.1.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.4.5-1.1.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.4.5-1.1.rel`

5. Return to Privileged Exec mode and check the boot settings, using:

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

6. Reboot using the new software version.

```
awplus# reload
```

Installing the GUI

This section describes how to install and set up the AlliedWare Plus GUI using an SD card, a USB storage device, or a TFTP server. The version number in the GUI Java applet filename (**.jar)** gives the earliest version of the software file (**.rel**) that the GUI can operate with.

To install and run the AlliedWare Plus GUI requires the following system products and setup:

- PC Platform:
  Windows XP SP2 and up / Windows Vista SP1 and up
- Browser: (must support Java Runtime Environment (JRE) version 6)
  Microsoft Internet Explorer 7.0 and up / Mozilla Firefox 2.0 and up

To install the GUI on your switch, use the following steps:

1. Copy to the GUI Java applet file (**.jar** extension) onto your TFTP server, SD card or USB storage device.

2. Connect to the switch's management port, then log into the switch.

3. If necessary, delete or move files to create space in the switch's Flash memory for the new file.

   To see the memory usage, use the command:

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

   ```
   awplus# del <filename>
   ```

   You cannot delete the current boot file.

4. Assign an IP address for connecting to the GUI. Use the commands:

   ```
   awplus# configure terminal
   awplus(config)# interface vlan1
   awplus(config-if)#ip address <address>/<prefix-length>
   ```

   Where <*address*> is the IP address that you will subsequently browse to when you connect to the GUI Java applet. For example, to give the switch an IP address of 192.168.2.6, with a subnet mask of 255.255.255.0, use the command:

   ```
   awplus(config-if)# ip address 192.168.2.6/24
   ```

5. If required, configure a default gateway for the switch.

   ```
   awplus(config-if)# exit
   awplus(config)# ip route 0.0.0.0/0 <gateway-address>
   ```

   Where <*gateway-address*> is the IP address for your gateway device. You do not need to define a default gateway if you browse to the switch from within its own subnet.

6. Copy the GUI file onto your switch from the TFTP server, SD card, or USB storage device.

   TFTP server: Use the command:

   ```
   awplus# copy tftp://<server-address>/<filename.jar> flash:/
   ```

   SD card: use the command:

   ```
   awplus# copy card:/<filename.jar> flash:/
   ```

   USB storage device: use the command:

   ```
   awplus# copy usb:/<filename.jar> flash:/
   ```

   where <*server-address*> is the IP address of the TFTP server, and where <*filename.jar*> is the filename of the GUI Java applet.

7. Ensure the HTTP service is enabled on your switch. Use the commands:

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

   The HTTP service needs to be enabled on the switch before it accepts connections from a web browser. The HTTP service is enabled by default. However, if the HTTP has been disabled then you must enable the HTTP service again.

8. Create a user account for logging into the GUI.

   ```
   awplus(config)# username <username> privilege 15 password
                   <password>
   ```

   You can create multiple users to log into the GUI. For information about the **username** command, see the AlliedWare Plus Command Reference.

9. Start the Java Control Panel, to enable Java within a browser

   On your PC, start the Java Control Panel by opening the Windows Control Panel from the Windows Start menu. Then enter Java Control Panel in the search field to display and open the Java Control Panel.

   Next, click on the 'Security' tab. Ensure the 'Enable Java content in the browser' checkbox is selected on this tab.

10. Enter the URL in the Java Control Panel Exception Site List

    Click on the 'Edit Site List' button in the Java Control Panel dialog Security tab to enter a URL in the Exception Site List dialog. In the 'Exception Site List' dialog, enter the IP address you configured in Step 4, with a http:// prefix.

    After entering the URL click the Add button then click OK.

11. Log into the GUI.

    Start a browser and enter the switch's IP address. The GUI starts up and displays a login screen. Log in with the username and password specified in the previous step.

AlliedWare Plus Version 5.4.5-0.x

for SwitchBlade x8100 Series, SwitchBlade x908, x930 Series, x610 Series, x510 Series, IX5-28GPX, x310 Series, x230 Series, and x210 Series Switches, and for AR3050S and AR4050S Next-Generation Firewalls

Contents

Introduction

This release note describes the new features and enhancements in AlliedWare Plus software version 5.4.5-0.x. For more information, see the Command Reference for your switch or next-generation firewall (NGFW). Software file details for this version are listed in Table 1 below.

Caution: Software version 5.4.5 requires a release license for the SBx908 and SBx8100 switches. If you are using either of these switches, ensure that you load your license certificate onto each switch before you upgrade. Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 231 and
- "Licensing this Software Version on a Control Card for an SBx8100 Series Switch" on page 233.

The first 5.4.5-0.x software version is numbered 5.4.5-0.1. The following table lists model names and software files for this version.

Table 1: Models and software file names

Models	Family	Software File	GUI File	Date
x210-9GT x210-16GT x210-24GT	x210 Series	x210-5.4.5-0.1.rel	x210-gui_545_08.jar	03/2015
x230-10GP x230-18GP	x230 Series	x230-5.4.5-0.1.rel	x230-gui_545_07.jar	03/2015
x310-26FT x310-50FT x310-26FP x310-50FP	x310 Series	x310-5.4.5-0.1.rel	x310-gui_545_08.jar	03/2015
IX5-28GPX	IX5	IX5-5.4.5-0.1.rel	IX5-gui_545_04.jar	03/2015
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 Series	x510-5.4.5-0.1.rel	x510-gui_545_08.jar	03/2015
x610-24Ts x610-24Ts-PoE+ x610-24Ts/X x610-24Ts/X-PoE+ x610-24SPs/X x610-48Ts x610-48Ts-PoE+ x610-48Ts/X x610-48Ts/X-PoE+	x610 Series	x610-5.4.5-0.1.rel	x610-gui_545_08.jar	03/2015

Table 1: Models and software file names

Models	Family	Software File	GUI File	Date
SwitchBlade x908*	SBx908	SBx908-5.4.5-0.1.rel	SBx908-gui_545_07.jar	03/2015
x930-28GTX x930-28GPX x930-52GTX x930-52GPX	x930 Series	x930-5.4.5-01.rel	n/a	03/2015
SBx81CFC400 SBx81CFC960	SBx8100	SBx81CFC400-5.4.5-0.1.rel SBx81CFC960-5.4.5-0.1.rel	SBx81CFC400-gui_545_07.jar SBx81CFC960-gui_545_07.jar	03/2015
AR3050S AR4050S	NGFW	AR3050S-5.4.5-0.1.rel AR4050S-5.4.5-0.1.rel	n/a	03/2015

*Expansion Modules for the SwitchBlade x908 in version 5.4.5

Product	Supported in version 5.4.5
XEM-1XP	No
XEM-2XP	Yes
XEM-2XS	Yes
XEM-2XT	Yes
XEM-12S	No
XEM-12T	No
XEM-12Sv2	Yes
XEM-12Tv2	Yes
XEM-24T	Yes

Caution: Using a software version file for the wrong switch or NGFW model may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

New Products

AlliedWare Plus version 5.4.5 supports the following recently-released products.

x510L Series

The x510L Series switches make the ideal choice at the network edge where security, resiliency and flexibility are required. The x510L comes with a choice of 24- and 48-port models with 1G/10G uplink ports, plus the power of Virtual Chassis Stacking (VCStack™).

The x510L features stacking capability of up to four devices and can mix with any x510 Series model, and supports long distance stacking. Any Allied Telesis 10G SFP+ module can be used for stacking.

The x510L is differentiated from other x510 models by having a single internal PSU.

A feature license is required on the x510L Series switches to upgrade uplink ports from 1G to 10G. The premium license for the x510L is the same as for the x510 Series models.

The x510L Series is supported since version 5.4.4-2.3.

Table 2: x510L Series models and port specifications

Product	10/100/1000T (RJ-45) Copper Ports	10 Gigabit Stacking Ports	1G/10G SFP+ Ports
x510L-28GT	24	2*	4 (2 if stacked)*
x510L-28GP	24	2*	4 (2 if stacked)*
x510L-52GT	48	2*	4 (2 if stacked)*
x510L-52GP	48	2*	4 (2 if stacked)*

*Stacking ports can be configured as additional 1G/10G Ethernet ports when the switch is not stacked.

For more information on the x510L Series switches, see the *x510 Series Data Sheet, Installation Guide* and *Command Reference*. These documents are available from our website at **alliedtelesis.com/switches/x510**.

AT-x510DP-28GTX

The Allied Telesis AT-x510DP-28GTX stackable Gigabit edge switch is the idel Data Center Top-of-Rack (ToR) switch, featuring 24 x 10/100/1000T ports and 4 x 10G SFP+ uplink ports for high speed server and storage connectivity.

Dual hot-swappable load-sharing AC or DC power supplies with reverse airflow guarantee maximum uptime. Allied Telesis VCTack allows multiple units to be connected as a single virtual chassis, creating a highly resilient solution with no single point of failure that can even be distributed over long distances. The AT-x510DP-28GTX is the perfect choice for ciritical Data Center applications requiring uninterrupted service.

The ATx510-28GTX is supported since version 5.4.4-2.3.

For more information on the AT-x510-28GTX switches, see the *x510 Series Data Sheet, Installation Guide* and *Command Reference*. These documents are available from our website at **alliedtelesis.com/switches/x510**.

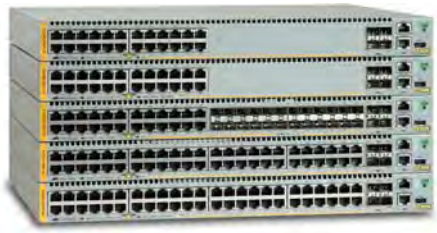
AT-x510-28GSX-80

The new x510-28GSX-80 uses DC power and provides 24 SFP ports, supporting industrial and provider network environments.

The AT-x510-28GSX-80 is supported since version 5.4.4-1.1.

For more information on the AT-x510-28GSX-80 switches, see the *x510 Series Data Sheet, Installation Guide* and *Command Reference*. These documents are available from our website at **alliedtelesis.com/switches/x510**.

x930 Series



The x930 Series of stackable Gigabit Layer 3 switches provide resiliency, reliability and high performance, making them ideal for distribution and network core solutions.

The x930 Series switches are a high-performing and feature-rich choice for today's networks. With a choice of 24- and 48-port models with 10 Gigabit uplink ports, plus the power of Virtual Chassis Stacking (VCStack™) with up to 160 Gbps of stacking bandwidth per switch, the x930 Series have the flexibility and performance for key network connectivity.

The x930 Series has the capability to manage large-scale wired and wireless networks on a single platform to reduce complexity and increase administrative consistency.

The x930 Series can form a VCStack of up to eight devices for enhanced resiliency and simplified device management. Stacks can be created over long distance, making it the perfect choice for distributed environments or disaster recovery.

Table 3: x930 models and port specifications

Product	10/100/1000T (RJ-45) Copper Ports	100/1000X SFP Ports	1/10Gigabit SFP+ Ports	10 Gigabit Stacking Ports
x930-28GTX	24	-	4 (2 if stacked)*	2*
x930-28GPX	24	-	4 (2 if stacked)*	2*
x930-52GTX	48	-	4 (2 if stacked)*	2*
x930-52GPX	48	-	4 (2 if stacked)*	2*

*Stacking ports can be configured as additional 1G/10G Ethernet ports when the switch is not stacked, or if the StackQS module is used.

For more information on the x930 Series switches, see the *x930 Series Data Sheet, Installation Guide* and *Command Reference*. These documents are available from our website at **alliedtelesis.com/switches/x930**.

Next-Generation Firewall Products

The new range of Next-Generation Firewalls (NGFWs) have an integrated architecture built on AlliedWare Plus, bringing its verified and superior operation to the security needs of today's networks. As well as Allied Telesis' industry leading key features, our NGFW integrated security platforms utilize best of breed security providers, for up-to-the-minute protection from all known threats.

Traditional routers and firewalls are no longer capable of protecting Enterprise networks from the host of external and internal threats that endanger corporate security.

A new breed of products have consolidated threat management capabilities into a single device to increase the security of business communications. Allied Telesis NGFW products are an evolution of these devices. Multiple threat detection and protection capabilities are now integrated within a purpose-built solution that provides single-pass low-latency inspection and protection for all network traffic.

The AR3050S and AR4050S combine next generation firewall and threat protection with routing and switching in a single, high-performance integrated security platform. An ideal choice for high-speed internet gateway applications, the Allied Telesis integrated security platforms meet the needs of modern Enterprise networks.

AR3050S

The AR3050S combines NGFW and threat protection with routing and switching, in a single high-performance integrated security platform.

The AR3050S is the ideal choice for high speed Internet gateway applications. The AR3050S features an integrated security platform to provide up-to-the-minute threat protection and advanced networking capabilities, meeting the needs of modern networks.

Table 4: AR3050S port specifications

	WAN Ports					
Product	10/100/1000T (RJ-45) Copper Ports	100/1000 combo SFP Ports	10/100/1000T combo (RJ-45)	High-Availability Bypass	External Ports	External Memory
AR3050S	8	2	2	2	1 x RJ-45, 1 x USB	1 x SDHC slot

For more information on the AR3050S NGFW, see the *AR3050S Data Sheet, Installation Guide* and *Command Reference*. These documents are available from our website at **alliedtelesis.com/switches/securityapps**.

Key new features for AR3050S

- Next-Generation DPI Firewall
- Application and web control
- Intrusion Detection/Prevention System (IDS/IPS)
- IP Reputation services
- Malware Protection
- Secure remote VPN access
- Site-to-site VPN connectivity
- Advanced routing capabilities
- Traffic shaping and prioritization
- Strong authentication
- Flexible licensing options
- AMF-compatible for easy installation and management
- Multi-core processor for high performance

AR4050S

The AR4050S combines NGFW and threat protection with routing and switching, in a single high-performance integrated security platform.

The AR4050S is the ideal integrated security platform for medium size Enterprises. NGFW and threat protection is combined with routing and switching, to provide an innovative high performance solution.

The AR4050S is the ideal choice for high speed Enterprise gateway applications. The AR4050S features an integrated security platform to provide up-to-the-minute threat protection and advanced networking capabilities, meeting the needs of medium size Enterprise networks.

Table 5: AR4050S port specifications

		WAN Ports				
Product	10/100/1000T (RJ-45) Copper Ports	100/1000 combo SFP Ports	10/100/1000T combo (RJ-45)	High-Availability Bypass	External Ports	External Memory
AR4050S	8	2	2	2	1 x RJ-45, 1 x USB	1 x SDHC slot

For more information on the AR4050S NGFW, see the *AR4050S Data Sheet, Installation Guide* and *Command Reference*. These documents are available from our website at **alliedtelesis.com/switches/securityapps**.

Key new features for AR4050S

- Next-Generation DPI Firewall
- Application and web control
- Intrusion Detection/Prevention System (IDS/IPS)
- IP Reputation services
- Malware Protection
- Antivirus
- Secure remote VPN access
- Site-to-site VPN connectivity
- Advanced routing capabilities
- Traffic shaping and prioritization
- Strong authentication
- Flexible licensing options
- AMF-compatible for easy installation and management
- Multi-core processor for high performance

Key New Features and Enhancements

This section summarizes the key new features. For a list of all new and enhanced features and commands, see "Changes in this Version" on page 227. For more information about all features on the switch or NGFW, see the Command Reference for your switch or NGFW. Unless otherwise stated, all new features and enhancements are available on all switch and NGFW models running this version of AlliedWare Plus.

Allied Telesis Management Framework

Allied Telesis Management Framework (AMF) is a sophisticated suite of management tools that provides a simplified approach to network management. Common tasks are automated or made so simple that the day-to-day running of a network can be achieved without the need for highly trained, and expensive, network engineers. Powerful features like centralized management, auto-backup, auto-upgrade, auto-provisioning and auto-recovery enable plug-and-play networking and zero-touch management.

AMF Controller

An AMF master can manage networks of up to 120 nodes, which can be located locally or across WAN links. This can be dramatically increased by installing the AMF Controller, which enables multiple AMF Masters to be managed from a single point. With the AMF Controller, a network of over 7000 devices can be managed, allowing all the time saving, cost reducing benefits of AMF to be multiplied and efficiencies to be increased.

AMF Controller is now available on the Switchblade x8100 (CFC960).

The Wireless Manager

The Allied Telesis Wireless Manager has been designed specifically to meet the requirements of enterprise organizations and addresses key concerns about mobility, security, and TCO. The Wireless Manager is embedded within the operating system of the switch so no separate server is required. It is able to control a number of Allied Telesis TQ Series wireless access points and can centralize the provisioning, operation, administration, and maintenance for the entire enterprise wireless infrastructure.

The Wireless Manager runs on x930 Series, SwitchBlade x8100 (CFC960 only) and SwitchBlade x908 switches.

The Wireless Manager supports APs running version 3.x or later firmware.

The Wireless Manager TQ-series AP support status is:

- TQ4600 - Supported.
- TQ-3200/TQ-3400/TQ-4400 series - Supported - available in Japan only
- TQ2450 - Not supported
- TQ3600 - Not supported - legacy product

This information is accurate as at November 2015. For the latest support information, see your Allied Telesis authorized reseller or distributor.

OpenFlow Capabilities

OpenFlow is a protocol used to manage switches from a remote controller. An openFlow switch can be configured to operate with similar results to a traditional switch, without having to manually re-configure the switch if the network changes.

Support for OpenFlow v1.3 is now available on the x510, x930 Series switches.

Cable Fault Locator

The Cable Fault Locator (CFL) is a cable diagnostic tool for copper (but not fiber) cables. You can select a port and the CFL will display, for that port, connection status or faults that exist in either the connected cable or in its terminations. The CFL operates using a technology known as Time Domain Reflectometry (TDR) to test all four pairs of wires inside the cable.

CFL is now supported on all AlliedWare Plus switches that support version 5.4.5.

Premium License for the x310

The Premium License is now available for the x310. This enables the following features on the x310 platform:

- OSPFv2 and OSPFv3
- RIP and RIPng
- PIM-SM, PIM-DM, PIM-SSM, for IPv4
- PIM-SM, PIM-SSM for IPv6
- EPSR master
- VRRP, VRRPv3

Dual-rate Pluggable Support

If you want to upgrade your equipment in stages and need to run SFP and SFP+ modules, dual rate support is now available on certain models, see your product datasheet for details. The pluggables will accept any link speed without further configuration.

Stacking Modules

Any Allied Telesis 10G SFP+ module can now be used for long distance stacking.

Management Stacking on the x230

Management stacking is the ability for multiple network devices to be managed from a single console. Other similar implementation are known by names such as Enhanced Stacking, Virtual Stacking and Clustering.

In essence, management stacking enables CLI commands to be issued from a single command switch to another switch in the stack. Therefore the user only needs to remember one management IP address to be able to reach any device in the stack. On edge switches, this feature reduces the burden of managing many individual devices.

Management stacking supports up to 24 devices in the stack, and is only available on the x230 switches. Only one device can be controlled at a time via the command node.

PIM-SSM for IPv6

Protocol Independent Multicast - Source Specific Multicast (PIM-SSM) is derived from Protocol Independent Multicast - Sparse Mode (PIM-SM) and is a simplified version of PIM-SM.

The key difference is that with PIM-SSM the hosts requesting streams need to know the source address of the stream they are requesting, and must specify the source in their request.

PIM-SSM for IPv6 is now supported on all switches that support Layer 3 multicasting.

Important Considerations Before Upgrading to this Version

Licensing

From software version 5.4.4-0.4 onwards, AlliedWare Plus software releases need to be licensed for SBx908 and SBx8100 switches.

If you are upgrading to 5.4.5-0.x on your SBx908 or SBx8100 switch, please ensure you have a 5.4.5 license on your switch. To obtain a license, contact your authorized Allied Telesis support center. You will need to provide the MAC addresses of the switches you want to license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 231 and
- "Licensing this Software Version on a Control Card for an SBx8100 Series Switch" on page 233.

Upgrading a VCStack

This version supports VCStack "reboot rolling" upgrades. With the **reboot rolling** command, you can reduce downtime when upgrading a VCStack.

You can use the **reboot rolling** command to upgrade to any 5.4.5-0.x version from any 5.4.4-x.x version.

You cannot use rolling reboot to upgrade directly to 5.4.5-0.x from 5.4.3-x.x releases. If you wish to use rolling reboot, you must first use it to upgrade from 5.4.3-0.0 to 5.4.4-0.x, then from 5.4.4-0.x to 5.4.5-0.x.

Forming or extending a VCStack

If you create a VCStack from switches that are running different software versions, auto-synchronization ensures that all members will run the same software version when they boot up.

Auto-synchronization is supported between all versions of 5.4.5-0.x and 5.4.4-2.x or later. It is not supported between 5.4.5-0.x and earlier versions of 5.4.4 (5.4.4-1.x or 5.4.4-0.x).

Before you add a new switch to a stack, make sure the new switch's software version is compatible with the stack's version. If the new switch is running an incompatible version, it cannot join the stack until you have manually upgraded it.

AMF software version compatibility

We strongly recommend that all switches in an AMF network run the same software release.

If this is not possible, switches running version 5.4.5-0.x are compatible with switches running version 5.4.3-2.6 and later, or any 5.4.4 version.

Upgrading all switches in an AMF network

This version supports upgrades across AMF networks. There are two methods for upgrading firmware on an AMF network:

- Reboot-rolling, which upgrades and reboots each switch in turn
- Distribute firmware, which upgrades each switch, but does not reboot them. This lets you reboot the switches at a minimally-disruptive time.

You can use either of these methods to upgrade to this software version.

You can use these methods to upgrade to this version from 5.4.3-2.6 and later.

In summary, the process for upgrading firmware on an AMF network is:

1. Copy the release .rel files for each switch family to the media location you intend to upgrade from (Flash memory, SD card, USB stick etc).
2. Decide which AMF upgrade method is most suitable.
3. Initiate the AMF network upgrade using the selected method. To do this:
    a. create a working-set of the switches you want to upgrade
    b. enter the command **atmf reboot-rolling <*location*>** or **atmf distribute-firmware <*location*>** where **<*location*>** is the location of the .rel files.
    c. Check the console messages to make sure that all switches are “release ready”. If they are, follow the prompts to perform the upgrade.

Changes in this Version

Table 6 on page 228 below lists new and modified commands for the features that have been modified in this version. It shows which chapter of the Command References has details of each command.

These tables do not show commands for new features. See the Command Reference for your switch or NGFW.

Table 6: New commands in 5.4.5

Command	Status	x210	x230	x310	IX5	x510	x610	x908	x930	SBx8100 CFC400	SBx8100 CFC960	AR3050S	AR4050S	Software Reference Chapter	Description
linkflap action	New	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	**Switching Commands**	This command enables port flapping detection. Port flapping detection will disable any ports that flap more than 15 times in less than 15 seconds. This limits the impact of an unreliable link.
ipv6 pim ssm	New	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	**PIM-SMv6 Commands**	This command defines the Source Specific Multicast (SSM) range of IPv6 multicast addresses.
atmf area name	New	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command creates an AMF area and gives it a name and ID number. It is only valid on AMF controllers and master nodes.
atmf area password	New	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command sets a password on an AMF area, so that an AMF controller can communicate with it.
atmf backup area-masters delete	New	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command deletes a backup of a specified node in a specified area. It is only valid on AMF controllers.
atmf backup area-masters enable	New	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command enables backup of remote area-masters from the AMF controller.
atmf backup area-masters now	New	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command runs a backup of one or more remote area-masters from the AMF controller immediately.
atmf controller	New	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command configures the switch as an AMF controller. This enables you to split a large AMF network into multiple areas.
atmf select-area	New	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command enables you to access devices in an area outside the core area on the controller network, or to return to the local controller network.
show atmf area	New	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command displays information about an AMF controller, and the AMF area-masters and area gateway nodes that the controller is connected to.
show atmf area summary	New	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command displays a summary of IPv6 addresses used by AMF, for one or all of the areas controlled by an AMF controller.
show atmf area nodes	New	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command displays summarized information about an AMF controller's remote nodes.
show atmf area nodes-detail	New	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command displays detailed information about an AMF controller's remote nodes.

Table 6: New commands in 5.4.5(cont.)

Command	Status	x210	x230	x310	IX5	x510	x610	x908	x930	SBx8100 CFC400	SBx8100 CFC960	AR3050S	AR4050S	Software Reference Chapter	Description
show atmf backup area	New	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command displays backup status information for the master nodes in one or more areas. It is only valid on AMF controllers.
switchport atmf-arealink remote-area	New	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command configures a port or aggregator as an AMF arealink. AMF arealinks operate between two nodes in different areas in an AMF network.

Table 7: Modified commands in 5.4.5. This table also indicates which devices the change applies to

Command	Status	x210	x230	x310	IX5	x510	x610	x908	x930	SBx8100 CFC400	SBx8100 CFC960	AR3050S	AR4050S	Software Reference Chapter	Description
atmf recover	Modified	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command manually initiates the recovery (or replication) of an AMF node. With 5.4.5, nodes can now be recovered from information held by an AMF controller.
atmf virtual-link id ip remote-id remote-ip	Modified	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command enables AMF nodes to transparently communicate across a wide area network. A **remote-area** parameter has been added, to allow communication between areas that are connected via WAN links.
debug atmf	Modified	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command turns on debugging for a variety of AMF events. It now includes arealink debugging.
debug atmf packet	Modified	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command turns on AMF packet debugging for all or a subset of packets. That subset can now include Area Hello Packets and Gateway Hello Packets (type 12 and 13).
show atmf	Modified	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command now indicates if the device is an AMF controller.
show atmf backup	Modified	N	N	N	N	N	Y	Y	Y	Y	Y	N	N	**AMF Commands**	This command has been modified to include two new parameters. The **synchronize** parameter displays whether the backup file servers are synchronized. The **logs** parameter displays the logs for the last synchronization for each backup file server.

Table 7: Modified commands in 5.4.5. This table also indicates which devices the change applies to(cont.)

Command	Status	x210	x230	x310	IX5	x510	x610	x908	x930	SBx8100 CFC400	SBx8100 CFC960	AR3050S	AR4050S	Software Reference Chapter	Description
show atmf detail	Modified	N	N	N	N	N	N	N	Y	Y	Y	N	N	**AMF Commands**	This command now includes the management IPv6 address for the device.
show atmf debug	Modified	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command now includes the status of arealink debugging.
show atmf links	Modified	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command now includes information about arealinks.
show atmf links statistics	Modified	N	N	N	N	N	N	N	N	N	Y	N	N	**AMF Commands**	This command now includes statistics about AMF controllers

Table 8: Deleted and deprecated commands in 5.4.5

Command	Status	x210	x230	x310	IX5	x510	x610	x908	x930	SBx8100 CFC400	SBx8100 CFC960	AR3050S	AR4050S	Software Reference Chapter	Description
service terminal-length (deleted)	Deleted	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	**User Access Commands**	This command has been deleted.
system territory (deprecated)	Deprecated	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	**System Configuration and Monitoring Commands**	This command has been deprecated since version 5.4.4-0.1, and now has no effect.

Licensing this Software Version on an SBx908 Switch

Release licenses are applied with the **license certificate** command, then validated with the **show license** or **show license brief** commands. Follow these steps:

- Obtain the MAC address for a switch
- Obtain a release license for a switch
- Apply a release license on a switch
- Confirm release license application

Step 1: Obtain the MAC address for a switch

A release license is tied to the MAC address of the switch.

Switches may have several MAC addresses. Use the **show system mac license** command to show the switch MAC address for release licensing:

```
awplus# show system mac license
MAC address for licensing:
eccd.6d9d.4eed
```

Step 2: Obtain a release license for a switch

Contact your authorized Allied Telesis support center to obtain a release license.

Step 3: Apply a release license on a switch

Use the **license certificate** command to apply a release license to your switch.

Note the license certificate file can be stored on internal flash memory, or an external SD card, or on a server accessible by the TFTP, SCP or HTTP protocols.

Entering a valid release license changes the console message displayed about licensing:

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus#license certificate demo1.csv
A restart of affected modules may be required.
Would you like to continue? (y/n): y
11:58:14 awplus IMI[1696]: SFL: The current software is licensed. Exiting
unlicensed mode.

Stack member 1 installed 1 license

1 license installed.
```

Step 4: Confirm release license application

On a stand-alone switch, use the commands **show license** or **show license brief** to confirm release license application.

On a stacked switch, use the command **show license member** or **show license brief member** to confirm release license application.

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus switches:

```
awplus# show license
OEM Territory : ATI USA
Software Licenses
------------------------------------------------------------------------
Index                          : 1
License name                   : Base License
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Mar-2015
License expiry date            : N/A
Features included              : EPSR-MASTER, IPv6Basic, MLDSnoop, OSPF-64,
                                 RADIUS-100, RIP, VRRP

Index                          : 2
License name                   : 5.4.5-rl
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Mar-2015
License expiry date            : N/A
Release                        : 5.4.5
```

Licensing this Software Version on a Control Card for an SBx8100 Series Switch

Release licenses are applied with the **license certificate** command, then validated with the **show license** or **show license brief** commands. Follow these steps:

- Obtain the MAC address for a control card
- Obtain a release license for a control card
- Apply a release license on a control card
- Confirm release license application

If your control card is in a stacked chassis, you do not need to perform these steps on each chassis in the stack, only on the stack master.

If your license certificate contains release licenses for each control card present in a stacked chassis, entering the **license certificate** command on the stack master will automatically apply the release licenses to all the control cards within the stack.

Step 1: Obtain the MAC address for a control card

A release license is tied to the control card MAC address in a chassis.

Chassis may have several MAC addresses. Use the **show system mac license** command to show the control card MAC address for release licensing. Note the MAC addresses for each control card in the chassis. The chassis MAC address is not used for release licensing. Use the card MAC address for release licensing.

```
awplus#show system mac license

MAC address for licensing:


Card                MAC Address
-----------------------------------
1.5                 eccd.6d9e.3312
1.6                 eccd.6db3.58e7

Chassis MAC Address eccd.6d7b.3bc2
```

Step 2: Obtain a release license for a control card

Contact your authorized Allied Telesis support center to obtain a release license.

Step 3: Apply a release license on a control card

Use the **license certificate** command to apply a release license to each control card installed in your chassis or stack.

Note the license certificate file can be stored on internal flash memory, a USB drive, or on a server accessible by the TFTP, SCP or HTTP protocols.

Entering a valid release license changes the console message displayed about licensing:

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus# license certificate demo1.csv
A restart of affected modules may be required.
Would you like to continue? (y/n): y
11:58:14 awplus IMI[1696]: SFL: The current software is licensed. Exiting
unlicensed mode.

Stack member 1 installed 1 license

1 license installed.
```

Step 4: Confirm release license application

On a stand-alone chassis, use the commands **show license** or **show license brief** to confirm release license application.

On a stacked chassis, use the command **show license member** or **show license brief member** to confirm release license application.

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus chassis:

```
awplus# show license
OEM Territory : ATI USA
Software Licenses
------------------------------------------------------------------------
Index                          : 1
License name                   : Base License
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Mar-2015
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                                 Virtual-MAC, VRRP

Index                          : 2
License name                   : 5.4.5-rl
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Mar-2015
License expiry date            : N/A
Release                        : 5.4.5
```

Installing this Software Version

Caution: Software version 5.4.5 requires a release license for the SBx908 and SBx8100 switches. Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 231 and
- "Licensing this Software Version on a Control Card for an SBx8100 Series Switch" on page 233.

To install and enable this software version, use the following steps:

1. Copy the software version file (.rel) onto your TFTP server.

2. If necessary, delete or move files to create space in the switch's Flash memory for the new file. To see the memory usage, use the command:

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

   ```
   awplus# del <filename>
   ```

   You cannot delete the current boot file.

3. Copy the new release from your TFTP server onto the switch.

   ```
   awplus# copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.

4. Move from Privileged Exec mode to Global Configuration mode, using:

   ```
   awplus# configure terminal
   ```

   Then set the switch to reboot with the new software version. For example, for 5.4.5-0.1, use one of the following commands:

Switch	Command
x210 series	`awplus(config)# boot system x210-5.4.5-0.1.rel`
x230 series	`awplus(config)# boot system x230-5.4.5-0.1.rel`
x310 series	`awplus(config)# boot system x310-5.4.5-0.1.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.4.5-0.1.rel`
x510 series	`awplus(config)# boot system x510-5.4.5-0.1.rel`
x610 series	`awplus(config)# boot system x610-5.4.5-0.1.rel`
SBx908	`awplus(config)# boot system SBx908-5.4.5-0.1.rel`
x930 series	`awplus(config)# boot system SBx930-5.4.5-0.1.rel`
SBx8100 with CFC400	`awplus(config)# boot system SBx81CFC400-5.4.5-0.1.rel`
SBx8100 with CFC960	`awplus(config)# boot system SBx81CFC960-5.4.5-0.1.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.4.5-0.1.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.4.5-0.1.rel`

5. Return to Privileged Exec mode and check the boot settings, using:

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

6. Reboot using the new software version.

```
awplus# reload
```

Installing the GUI

This section describes how to install and set up the AlliedWare Plus GUI using an SD card, a USB storage device, or a TFTP server. The version number in the GUI Java applet filename (**.jar)** gives the earliest version of the software file (**.rel**) that the GUI can operate with.

To install and run the AlliedWare Plus GUI requires the following system products and setup:

- PC Platform:
  Windows XP SP2 and up / Windows Vista SP1 and up
- Browser: (must support Java Runtime Environment (JRE) version 6)
  Microsoft Internet Explorer 7.0 and up / Mozilla Firefox 2.0 and up

To install the GUI on your switch, use the following steps:

1. Copy to the GUI Java applet file (**.jar** extension) onto your TFTP server, SD card or USB storage device.

2. Connect to the switch's management port, then log into the switch.

3. If necessary, delete or move files to create space in the switch's Flash memory for the new file.

   To see the memory usage, use the command:

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

   ```
   awplus# del <filename>
   ```

   You cannot delete the current boot file.

4. Assign an IP address for connecting to the GUI. Use the commands:

   ```
   awplus# configure terminal
   awplus(config)# interface vlan1
   awplus(config-if)#ip address <address>/<prefix-length>
   ```

   Where <*address*> is the IP address that you will subsequently browse to when you connect to the GUI Java applet. For example, to give the switch an IP address of 192.168.2.6, with a subnet mask of 255.255.255.0, use the command:

   ```
   awplus(config-if)# ip address 192.168.2.6/24
   ```

5. If required, configure a default gateway for the switch.

   ```
   awplus(config-if)# exit
   awplus(config)# ip route 0.0.0.0/0 <gateway-address>
   ```

   Where <*gateway-address*> is the IP address for your gateway device. You do not need to define a default gateway if you browse to the switch from within its own subnet.

6. Copy the GUI file onto your switch from the TFTP server, SD card, or USB storage device.

   TFTP server: Use the command:

   ```
   awplus# copy tftp://<server-address>/<filename.jar> flash:/
   ```

   SD card: use the command:

   ```
   awplus# copy card:/<filename.jar> flash:/
   ```

   USB storage device: use the command:

   ```
   awplus# copy usb:/<filename.jar> flash:/
   ```

   where <*server-address*> is the IP address of the TFTP server, and where <*filename.jar*> is the filename of the GUI Java applet.

7. Ensure the HTTP service is enabled on your switch. Use the commands:

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

   The HTTP service needs to be enabled on the switch before it accepts connections from a web browser. The HTTP service is enabled by default. However, if the HTTP has been disabled then you must enable the HTTP service again.

8. Create a user account for logging into the GUI.

   ```
   awplus(config)# username <username> privilege 15 password
                   <password>
   ```

   You can create multiple users to log into the GUI. For information about the **username** command, see the AlliedWare Plus Command Reference.

9. Start the Java Control Panel, to enable Java within a browser

   On your PC, start the Java Control Panel by opening the Windows Control Panel from the Windows Start menu. Then enter Java Control Panel in the search field to display and open the Java Control Panel.

   Next, click on the 'Security' tab. Ensure the 'Enable Java content in the browser' checkbox is selected on this tab.

10. Enter the URL in the Java Control Panel Exception Site List

    Click on the 'Edit Site List' button in the Java Control Panel dialog Security tab to enter a URL in the Exception Site List dialog. In the 'Exception Site List' dialog, enter the IP address you configured in Step 4, with a http:// prefix.

    After entering the URL click the Add button then click OK.

11. Log into the GUI.

    Start a browser and enter the switch's IP address. The GUI starts up and displays a login screen. Log in with the username and password specified in the previous step.