Technical Guide

Secure Shell (SSH)

Feature Overview and Configuration Guide

Introduction

This guide describes how the Secure Shell protocol (SSH) is implemented in the AlliedWare Plus™ Operating System (OS).

It covers:

- support for Secure Shell.
- configuring your device as a Secure Shell server and client.
- using Secure Shell to manage your device.
- a SSH server configuration example.

AlliedWare Plus supports the SSH protocol version 2.

Caution: SSH was upgraded in 5.5.1-1.1, to increase security. Since that upgrade, some older SSH clients may no longer connect to your AlliedWare Plus device. To resolve this, see "From 5.5.1-1.1 onwards, older SSH clients can't connect to AlliedWare Plus devices" on page 5.

Secure management is important in modern networks, as the ability to easily and effectively manage switches and routers, and the necessity for security, are two almost universal requirements.

Protocols such as Telnet and commands like UNIX's rlogin allow you to manage devices remotely, but can have serious security problems, such as relying on reusable clear text passwords that are vulnerable to wiretapping or password guessing. The Secure Shell protocol is superior to these access methods by providing encrypted and strongly authenticated remote login sessions.

SSH provides sessions between a host running a SSH server and a machine with a SSH client. AlliedWare Plus includes both a

SSH server and a SSH client to enable you to securely—with the benefit of cryptographic authentication and encryption—manage your devices over an insecure network.

In summary, SSH:

- replaces Telnet for remote terminal sessions; SSH is strongly authenticated and encrypted.
- remote command execution allows you to send commands to a device securely and conveniently, without requiring a terminal session on the device.
- allows you to connect to another host from your switch or AR-Series device.

AlliedWare Plus supports Secure Copy (SCP) and SSH File Transfer Protocol (SFTP). Both these protocols allow you to securely copy files between your device and remote machines. SFTP provides additional features from SCP, such as allowing you to manipulate the remote files, and halt or resume file transfers without closing the session.

Products and software version that apply to this guide

This guide applies to all AlliedWare Plus products, running software version **5.4.4** or later.

From software version **5.4.7-0.1** onwards, if the SSH service is enabled on a device and that device detects that the host key is missing, the device generates a new host key automatically instead of terminating SSH.

In software version **5.4.9-2.1**, 3DES was removed from the supported cypher set for SSH. Modern clients and servers can continue to interoperate using AES-based cyphers transparently.

In software version **5.5.1-1.1**, support was removed for the ssh-rsa algorithm in OpenSSH and for SSH protocol v1.

For more information, see the following documents:

- The product's Datasheet
- The product's Command Reference

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

Content

Secure Shell on AlliedWare Plus

Secure Shell supports the following features:

- Inbound SSH connections (server mode) and outbound SSH connections (client mode).
- File loading to and from remote machines using Secure Copy, using either the SSH client or SSH server mode.
- Public keys:
  - RSA keys with lengths of 768–32768 bits, and
  - ECDSA keys with key size of 256 or 384 bits (default is 256).
  - Keys are stored in a format compatible with other SSH implementations, and mechanisms are provided to copy keys to and from your device.
- Secure encryption, such as AES.
- Remote non-interactive shell that allows arbitrary commands to be sent securely to your device, possibly automatically.
- Compression of Secure Shell traffic.
- Tunneling of TCP/IP traffic.
- File loading from remote machines using SSH File Transfer Protocol (SFTP).
- A login banner on the SSH server, that displays when SSHv2 clients connect to the server.

Feature support in Secure Mode

Secure Mode enhances security by disabling any algorithms that are not supported under FIPS (Federal Information Processing Standards). This includes MD5, RSA-1 and DSA. Secure Mode is available on a number of Allied Telesis switches.

For step-by-step instructions on enabling Secure Mode, see “How to Enable Secure Mode” in the Getting Started with AlliedWare Plus Feature Overview and Configuration Guide.

From 5.5.1-1.1 onwards, older SSH clients can't connect to AlliedWare Plus devices

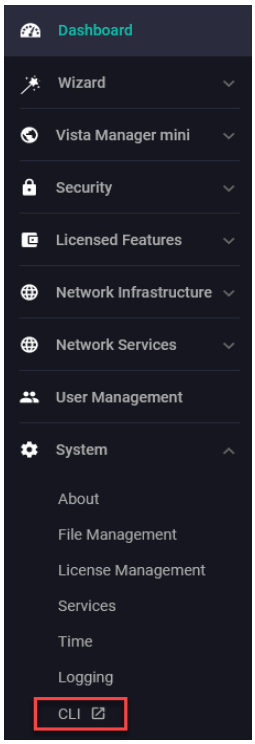
In AlliedWare Plus version 5.5.1-1.1, OpenSSH was upgraded. This means 5.5.1-1.1 and later versions no longer support the following insecure options:

- the ssh-rsa algorithm in OpenSSH, which is based on SHA1
- SSH protocol version 1

Unfortunately, some older SSH clients and older libraries still expect to use ssh-rsa. Therefore, before you upgrade to 5.5.1-1.1 or later, we recommend you:

- ensure your SSH client is up to date, and
- create an ECDSA key for the server to use, in case the client does not support secure SSH RSA algorithms

To create the ECDSA key, use the following steps:



1. Access the CLI of the AlliedWare Plus device. If you have already upgraded to 5.5.1-1.x or later and can no longer use your SSH client, you can access the device through its console port or its GUI as shown in this screenshot.

2. Create an ECDSA key using the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate hostkey ecdsa 384
```

3. Either reboot the device, or turn the SSH service off and on again, using the commands:

```
awplus(config)# no service ssh
awplus(config)# service ssh
```

Note that you only need to do this procedure on existing AlliedWare Plus devices. From 5.5.1-1.1 onwards, AlliedWare Plus automatically creates an ECDSA key on factory-new devices and devices that have been returned to a factory state.

Configuring the SSH Server

This section provides instructions on:

Creating a host key

The SSH server uses either an RSA or ECDSA host key to authenticate itself with SSH clients. Once created, the host key is stored securely on the device.

When you enable the SSH server, if no host keys exist, the server automatically generates SSHv2 host key pairs using ECDSA with a curve length of 384, and RSA with a 1024-bit key (unless in secure mode, when it only generates the ECDSA key).

If you need different keys, you can create them as follows.

- To generate an **RSA** host key for the SSH server, use the command:

```
awplus(config)#crypto key generate hostkey rsa [<768-32768>]
```

- To generate an **ECDSA** host key for the SSH server, use the command:

```
awplus(config)#crypto key generate hostkey ecdsa [256|384]
```

The default key length is 256, but you can set it to 384 instead.

- To **destroy** a host key, use the command:

```
awplus(config)#crypto key destroy hostkey {rsa|ecdsa}
```

- To **display** a host key stored on your device, use the command:

```
awplus#show crypto key hostkey [rsa|ecdsa]
```

Enabling the server

You must enable the SSH server before connections from SSH, SCP, and SFTP clients are accepted. When the SSH server is disabled it rejects connections from SSH clients. The SSH server is disabled by default on your device.

- To enable the SSH server, use the command:

```
awplus(config)#service ssh [ip|ipv6]
```

- To disable the SSH server, use the command:

```
awplus(config)#no service ssh [ip|ipv6]
```

When enabled, the SSH server allows SCP and SFTP sessions by default.

- To disable these services, use the commands:

```
awplus(config)#no ssh server scp
awplus(config)#no ssh server sftp
```

This allows you to reject SCP or SFTP file transfer requests, while still allowing Secure Shell connections.

- To re-enable SCP and SFTP services, use the commands:

```
awplus(config)#ssh server scp
awplus(config)#ssh server sftp
```

Modifying the server

- To modify the SSH protocol version that the server supports, use the command:

```
awplus(config)#ssh server {v1v2|v2only}
```

From version 5.5.1-1.1 onwards, SSH protocol version 1 is not supported.

- To modify the TCP port that the server listens to for incoming sessions, use the command:

```
awplus(config)#ssh server <1-65535>
```

By default, the server listens on port 22 for incoming sessions.

- To modify the number of unauthenticated connections the server allows, use the command:

```
awplus(config)#ssh server max-startups <1-128>
```

The SSH server only allows only 10 unauthenticated SSH sessions at any point in time, by default.

- To modify session and login timeouts on the SSH server, use the command:

```
awplus(config)#ssh server [session-timeout <0-3600>]
[login-timeout <1-600>]
```

By default, the SSH server waits 60 seconds for a client to authenticate itself. You can alter this waiting time by using the **login-timeout** parameter. If the client is still not authenticated after the timeout, then the SSH server disconnects the session.

Once a client has authenticated, the SSH session does not time out, by default. Use the **session-timeout** parameter to set a maximum time period the server waits before deciding that a session is inactive and terminating it.

For example:

- To set the session timeout to 600 seconds, the login timeout to 30 seconds, and the maximum number of concurrent unauthenticated sessions to 5, use the command:

```
awplus(config)#ssh server session-timeout 600 login-timeout 30
max-startups 5
```

- To remove the configured timeouts and maximum startups, use the command:

```
awplus(config)#no ssh server session-timeout login-timeout max-startups
```

Validating the server configuration

- To validate the SSH server configuration, use the commands:

```
awplus#show running-config ssh
```

or

```
awplus#show ssh server
```

```
awplus#show ssh server
Secure Shell Server Configuration
------------------------------------------------------------------------------
SSH Server                          : Enabled
Protocol                            : IPv4,IPv6
Port                                : 22
Version                             : 2,1
Services                            : scp, sftp
User Authentication                 : publickey, password
Resolve Hosts                       : Disabled
Session Timeout                     : 0 (Off)
Login Timeout                       : 60 seconds
Maximum Authentication Tries        : 6
Maximum Startups                    : 10
Debug                               : NONE
Ciphers                             : aes128-cbc,aes128-ctr,aes192-ctr,aes256-ctr
KEX                                 : curve25519-sha256@libssh.org,
                                      ecdh-sha2-nistp256,ecdh-sha2-nistp384,
                                      ecdh-sha2-nistp521,
                                      diffie-hellman-group-exchange-sha256,
                                      diffie-hellman-group-exchange-sha1,
                                      diffie-hellman-group14-sha1
```

Adding SSH users

The SSH server requires you to register SSH users. Users that are not registered cannot access the SSH server. Ensure first that you have defined the user in the Authorized User Database of your device.

- To add a new user, use the command:

```
awplus(config)#username <username> privilege <1-15> password <password>
```

- To register a user with the SSH server, use the command:

```
awplus(config)#ssh server allow-users <username-pattern> [<hostname-pattern>]
```

Registered entries can contain just the username, or the username with some host details, such as an IP address range. Additionally you can specify a range of users or hostname details by using an asterisk to match any string of characters.

For example:

- To allow any user from the IP range 192.168.1.1 to 192.168.1.255, use the command:

```
awplus(config)#ssh server allow-users * 192.168.1.*
```

- To display the list of allowed users, use the command:

```
awplus#show ssh server allow-users
```

- To delete an entry from the list of allowed users, use the command:

```
awplus(config)#no ssh server allow-users <username-pattern> [<hostname-pattern>]
```

The SSH server also contains a list of **denied** users. The server checks all incoming sessions against this list and denies any matching session, regardless of whether the session matches an entry in the allowed users list.

- To add an entry to the list of denied users, use the command:

```
awplus(config)#ssh server deny-users <username-pattern> [<hostname-pattern>]
```

This allows you to deny specific users from a range of allowed users.

For example:

- To deny a user with the IP address 192.168.1.12, use the command:

```
awplus(config)#ssh server deny-users * 192.168.1.12
```

- To display the database of denied users, use the command:

```
awplus#show ssh server deny-users
```

- To delete a client from the database of denied users, use the command:

```
awplus(config)#no ssh server deny-users <username-pattern> [<hostname-pattern>]
```

Authenticating SSH users

SSH users can use either their password or public key authentication to authenticate themselves with the SSH server. To use public key authentication, copy the user's public key file from their client device to the SSH server. To associate the key with a user, use the command:

```
awplus(config)#crypto key pubkey-chain userkey <username> [<filename>]
```

For example:

- To associate the file key.pub with the user "langley", use the command:

```
awplus(config)#crypto key pubkey-chain userkey langley key.pub
```

- To add a key as text into the terminal for user "geoff", first enter the command:

```
awplus(config)#crypto key pubkey-chain userkey geoff
```

then paste or type the key in as text. You can add multiple keys for the same user.

- To display the list of public keys associated with a user, use the command:

```
awplus#show crypto key pubkey-chain userkey <username> [<1-65535>]
```

The `<1-65535>` parameter allows you to display an individual key.

- To delete a key associated with a user from your device, use the command:

```
awplus(config)#no crypto key pubkey-chain userkey <username> <1-65535>
```

Adding a login banner

You can add a login banner to the SSH server for sessions.

The server displays the banner to clients before the login prompt.

- To set the login banner's message, use the command:

```
awplus(config)#banner login
```

then enter your message and use Ctrl+D to finish.

- To view the configured login banner, use the command:

```
awplus#show banner login
```

- To remove the configured message for the login banner, use the command:

```
awplus(config)#no banner login
```

Monitoring the server and managing sessions

- To display the current status of the SSH server, use the command:

```
awplus#show ssh server
```

- To display the current status of SSH sessions on your device, use the command:

```
awplus#show ssh
```

Note that this displays both SSH server and SSH client sessions that your Allied Telesis device is running. Use this command to view the unique identification number assigned to each incoming or outgoing SSH session. You need the ID number when terminating a specific session from your device.

- To terminate a session, or all sessions, use the command:

```
awplus#clear ssh {<1-65535>|all}
```

Creating host keys automatically when replacing devices

You can replace a failed device and copy the old device's configuration onto the replacement device, making it easier to remotely access the replacement device. This is possible because when you enable the SSH server, if no host keys exist, the server automatically generates keys.

So, if you need to replace a device and copy its existing configuration file, use the following steps:

1. Make sure that the new device is in a factory-clean state. If necessary, use the **erase factory-default** command to achieve this
2. Copy the firmware and configuration file from the old device to the Flash file system of the new device
3. Set the copied files as the boot firmware and configuration files
4. Reboot the new device.

Because the host keys are new on the device, if a remote user tries to connect to the new device with existing SSH credentials, the SSH client will notice that the host keys for the device are different and may give a warning. The warning will include a selection option to replace the old host key, or instructions on how to do this. Follow the client's selection option or instructions.

For example, a Linux client displays the following warning:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle
attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
55:7d:82:00:7e:6f:ac:ac:de:1c:f1:53:08:51:1c:68.
Please contact your system administrator.
Add correct host key in /Users/fergus/.ssh/known_hosts to get rid of
this message.
Offending RSA key in /Users/fergus/.ssh/known_hosts:12
RSA host key for 192.168.1.1 has changed and you have requested
strict checking.
Host key verification failed.
```

Debugging the server

Information which may be useful for troubleshooting the SSH server is available using the SSH debugging function. You can enable server debugging while the SSH server is functioning.

To enable server debugging, use the command:

```
awplus#debug ssh server [brief|full]
```

To disable SSH server debugging, use the command:

```
awplus#no debug ssh server
```

Configuring the SSH Client

This section provides instructions on:

Modifying the client

You can configure a selection of variables when using the SSH client. Note that the following configuration commands apply only to client sessions initiated after the command. The configured settings are not saved; after you have logged out from the SSH client, the client returns to using the default settings.

Use the command:

```
awplus#ssh client {port <1-65535>|session-timeout <0-3600>|connect-timeout
<1-600>}
```

The SSH client uses TCP port 22, by default. You can change the TCP port for the remote SSH server by using the **port** parameter.

The client terminates sessions that are not established after 30 seconds, by default. You can change this time period by using the **session-timeout** parameter.

Once the client has authenticated with a server, the client does not time out the SSH session, by default. Use the **connect-timeout** parameter to set a maximum time period the client waits before deciding that a session is inactive and terminating the session.

- To modify the SSH client so that it uses port 2000 for sessions, use the command:

```
awplus#ssh client port 2000
```

- To modify the SSH client so that unestablished sessions time out after 60 seconds, and inactive connection time out after 100 seconds, use the command:

```
awplus#ssh client session-timeout 60 connect-timeout 100
```

- To remove the configured port, session timeout, and connection timeout settings, use the command:

```
awplus#no ssh client port session-timeout connect-timeout
```

Adding SSH servers

SSH servers identify themselves using a host key (see "Creating a host key" on page 6). Before the SSH client establishes a session with a SSH server, it confirms that the host key sent by the server matches its database entry for the server. If the database does not contains a host key for the server, then the SSH client requires you to confirm that the host key sent from the server is correct.

- To add an SSH server to the client's database, use the commands:

```
awplus(config)#crypto key pubkey-chain knownhosts [ip|ipv6] <hostname>
[rsa|ecdsa]
```

```
awplus(config)#crypto key pubkey-chain knownhosts [vrf <vrf-name>] [ip|
ipv6] <hostname> [rsa|ecdsa]
```

- To display the SSH servers in the client's database, use the commands:

```
awplus(config)#show crypto key pubkey-chain knownhosts [<1-65535>]
```

```
awplus(config)#show crypto key pubkey-chain knownhosts [vrf <vrf-name>|
global] [<1-65535>]
```

- To remove an entry in the database, use the commands:

```
awplus(config)#no crypto key pubkey-chain knownhosts <1-65535>
```

```
awplus(config)#no crypto key pubkey-chain knownhosts [vrf <vrf-name>] <1-
65535>
```

Authenticating with a server

You can authenticate your session with a server by either using a password, or using RSA, DSA or ECDSA public key authentication. To use public key authentication, you must generate a pair of keys, one private and one public, and copy the public key onto the SSH server.

- To generate an **RSA** set of private and public keys for an SSH user, use the command:

```
awplus(config)#crypto key generate userkey <username> rsa [<768-32768>]
```

- To generate an **ECDSA** set of private and public keys for an SSH user, use the command:

```
awplus(config)#crypto key generate userkey <username> ecdsa [256|384]
```

The default key length is 256, but you can set it to 384 instead.

You can generate one key of each encryption type per user on your client.

- To copy the public key onto the SSH server, you must display the key onscreen. To display the public key associated with a user, use the command:

```
awplus#show crypto key userkey <username> [rsa|ecdsa]
```

To display the public keys set for other users, you must specify their username. Only users with the highest privilege setting can use this command to view the keys of other users.

- To delete a public and private pair of keys associated with a user, use the command:

```
awplus(config)#crypto key destroy userkey <username> {rsa|ecdsa}
```

Connecting using SSH

- To connect to a remote device that is acting as an SSH server, use the command:

```
awplus#ssh <hostname>
```

The <***hostname***> parameter specifies the server and can be either an IP address or a host name.

You can also optionally specify other parameters when connecting, including the VRF instance, to use IPv6, the port number to connect on, and a command to execute on the server.

The command is:

```
awplus#ssh [vrf <vrf-name>] [ip|ipv6] [user <username>]|[port <1-65535>]
<hostname> [<command>]
```

Note that you can only specify one of user or port. To change the default port, use the command **ssh client**.

For example:

- to connect to the SSH server at 192.168.1.2 as user “john”, and execute the command **show sys**, use the command:

```
awplus(config)#ssh user john 192.168.1.2 “show sys”
```

Copying files to and from the server

You can use either the SCP or SFTP client to transfer files from a remote SSH server.

Use the command:

```
awplus#copy <source-url> <destination-url>
```

For example:

- to use SFTP to load a file from the SSH server 192.168.1.2, onto the Flash memory of your device, use the command:

```
awplus#copy sftp://192.168.1.2/key.pub flash
```

Using SSH in Secure Mode

Secure Mode enhances security by disabling any algorithms that are not supported under FIPS (Federal Information Processing Standards). This includes MD5, RSA-1 and DSA. Secure Mode is available on a number of Allied Telesis switches.

For step-by-step instructions on enabling Secure Mode, see “How to Enable Secure Mode” in the Getting Started with AlliedWare Plus Feature Overview and Configuration Guide.

Secure Mode lets you optionally force an SSH connection to use specific FIPS-compliant algorithms. To do this, specify the desired cipher, HMAC, public key and/or key exchange, using the command:

```
ssh [cipher {aes128-cbc|aes256-cbc|aes128-ctr|aes192-ctr|aes256-ctr}]
[hmac hmac-sha2-256]
[public-key {ecdsa-sha2-nistp256|ecdsa-sha2-nistp384}]
[key-exchange {ecdh-sha2-nistp256|ecdh-sha2-nistp384}]
[ip|ipv6] [user <username>|port <1-65535>|version 2] <remote-device>
[<command>]
```

Debugging the client

Information which may be useful for troubleshooting the SSH client is available using the SSH debugging function. You can enable client debugging while the SSH client is functioning, using the command:

```
awplus#debug ssh client [brief|full]
```

- To disable SSH client debugging, use the command:

```
awplus#no debug ssh client
```

SSH Server Configuration Example

This section provides a Secure Shell server configuration example, where:

- the SSH server uses ECDSA encryption
- three SSH users are configured: Manager, John, and Asuka. “manager” can connect from only a defined range of hosts, while “john” and “asuka” can SSH from all hosts
- the SSH users use ECDSA private and public key authentication, using keys generated by the client device.

This example shows how to create RSA encryption keys, configure the Secure Shell server, and register users to make Secure Shell connections to your device.

Step 1: **Login as a highest Privileged User**

To create the keys and add users, you must login as a privileged user.

Step 2: **Create encryption keys**

On new devices, keys will be created automatically when you start the SSH service. Or you can create one, using the commands:

```
awplus#configure terminal
awplus(config)#crypto key generate hostkey ecdsa 384
awplus(config)#exit
```

This creates a key with a size of 384. To verify the key creation, use the command:

```
awplus#show crypto key hostkey
```

Step 3: **Enable the Secure Shell server**

Enable Secure Shell on the device using the commands:

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

Modify the SSH server settings as desired.

For example, to set the login-timeout to 60, and the session-timeout to 3600, use the commands:

```
awplus(config)#ssh server session-timeout 3600 login-timeout 60
```

To verify the server configuration, use the command:

```
awplus#show ssh
```

Step 4: **Create SSH users**

In order to connect and execute commands, you must register users in the SSH user database, and in the User Authentication Database of the device.

To create the users **john** and **asuka** in the User Authentication Database, use the commands:

```
awplus#configure terminal
awplus(config)#username john privilege 15 password secret
awplus(config)#username asuka privilege 15 password very-secret
```

To register **john** and **asuka** as SSH clients, use the commands:

```
awplus(config)#ssh server allow-users john
awplus(config)#ssh server allow-users asuka
```

To register **manager** as an SSH client so that can only connect from the IP address 192.168.1.1, use the command:

```
awplus(config)#ssh server allow-users manager 192.168.1.1
```

Step 5: **Set up authentication**

SSH users cannot connect unless the server can authenticate them. There are two ways to authenticate an SSH session:

- password authentication, and
- private/public key authentication.

When using password authentication, the user must supply their User Authentication Database password.

To use private/public key authentication, copy the public keys for each user onto the device. To copy the files onto Flash from the key directory of an attached TFTP server, use the commands:

```
awplus#copy tftp://key/john.pub flash:/john.pub
awplus#copy tftp://key/asuka.pub flash:/asuka.pub
```

To associate the key file with each user, use the commands:

```
awplus#configure terminal
awplus(config)#crypto key pubkey-chain userkey john john.pub
awplus(config)#crypto key pubkey-chain userkey asuka asuka.pub
awplus(config)#crypto key pubkey-chain userkey manager manager.pub
```


Allied Telesis NETWORK SMARTER

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com