

Overview

This guide describes how to configure the AirWave failover server to monitor your network. This guide also describes using AirWave to manage the failover process.

Contacting Support

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	hpe.com/networking/support
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team (SIRT)	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

Before setting up your failover server, you must have completed the AirWave installation. For instructions on how to install AirWave, refer to the *AirWave 8.2.6 Installation Guide*.

The setup workflow includes:

- "Adding the Failover License" on page 2
- "Upgrading the Software Version" on page 2

Adding the Failover License

Follow these steps to add a failover license:

1. Open a Web browser, then enter your AirWave server's IP address in the address bar to connect to the AirWave WebUI.
2. In the AirWave WebUI, navigate to **Home > License**, then click **Add**.
3. Enter your license key in the pop up window, and click **Add**.
4. Review the End User License Agreement, then click **I Accept**. The license you entered displays in the Licenses table, as shown in [Figure 1](#).

Figure 1: Failover License

Summary	
Type	Failover
Days Remaining	89
Approved Devices	0
Max. Device Count	2500

Licenses									
	ORGANIZATION	PRODUCT	PACKAGE	TYPE	DEVICE COUNT	IP ADDRESS	DAYS REMAINING	EXPIRATION DATE	VALID
<input type="checkbox"/>	Aruba Lab	AMP Failover	AW-FR-EVAL	Failover	2500	-	89	6/4/17, 12:09 PM	Yes

Upgrading the Software Version

Here's what you need to know before you begin the upgrade:

- If your failover requirement is 1 or 2 missed polls, disable failover monitoring before performing the upgrade. For information about disabling failover monitoring, see "[Best Practice: Maximizing Availability During the Setup](#)" on page 3.
- If you upgrade from AirWave 8.2.3.1 or earlier, you will no longer have root user access to the Linux shell after the upgrade. Your system will be converted to use the new AMP CLI. For information about using the AMP CLI, see the *AirWave 8.2.6 User Guide*. For information about upgrading the software, see "[Upgrade from AirWave 8.2.3.1 or Earlier](#)" on page 3.
- If you upgrade from AirWave 8.2.4 or later, you will use the new AMP CLI to install the upgrade package on your system. For information about upgrading the software, see "[Upgrading from AirWave 8.2.4 or Later](#)" on page 3.
- If your network doesn't allow AirWave to connect to the Internet, you must [manually download the software](#) and upload the software before performing the upgrade. For information about obtaining the software, see "[Manually Download the Software](#)" on page 5.

Best Practice: Maximizing Availability During the Setup

The failover server and all watched AMP servers must have the same AirWave software version. If needed, you can have the failover server take over for a watched AMP while you upgrade the software on the server to ensure high availability. Or, you can disable the failover server before you begin the upgrades.

To upgrade the software on the servers, follow these steps:

1. Disable failover polling on each managed node. Navigate to **Home > Overview > Managed AMP** page, then select "No" to disable the **Polling Enabled** option.
2. Upgrade AirWave on all watched AMPs and Master Console; then upgrade AirWave on the failover AMP (see ["Upgrading the Software Version" on page 2](#)).
3. Enable failover polling on each managed node. Navigate to **Home > Overview > Managed AMP** page, then select "Yes" to enable the **Polling Enabled** option.

Upgrade from AirWave 8.2.3.1 or Earlier

Follow these steps to upgrade from AirWave 8.2.3.1 or earlier:

1. Log in to the AirWave server as the root user.

2. Run the upgrade utility:

```
#start_amp_upgrade -v 8.2.6
```

The upgrade utility looks for the local upgrade package.

After the download completes, the following message appears while the software compiles:

```
Validating the upgrade package...
Upgrade package is OK.
Using upgrade script extracted from local package.
Upgrade package found in local cache.
```

If the software is not available, [manually download the software](#) and then perform this step again.

3. After the AMP services restart, you will see the following message:

```
Setting up secure accounts...
Setting admin user name...
Admin Username (default 'ampadmin'):
Admin user is admpadmin
Done
Setting admin password...
Admin Password:
Verify Password:
Done
Done
Removing alias for less...
Done
AMPCLI Setup completed
```

Enter the new ampadmin password. If you don't enter a user name, AirWave uses the default "ampadmin".

4. After setting the password, you will see the following message:

```
Your system has been converted to use AMPCLI. You may now
log in as ampadmin. If you lose the password for ampadmin you
may log in as amprecovery (password recovery) on the console to reset
the ampadmin password
```

5. Finally, remove any OS user accounts to prevent unauthorized access.

Upgrading from AirWave 8.2.4 or Later

Follow these steps to upgrade from AirWave 8.2.4 or later:

1. Log in to the AirWave server with the "ampadmin" user name and password. If you subsequently changed the ampadmin user name and password, enter the current admin name and password. The AMP CLI displays the following menu options.

```
AirWave Management Platform 3.2.4 on example.host.com
1 Upload File
2 Download File
3 Delete File
4 Backup
5 Restore
6 Support
7 Upgrade
8 Advanced
9 Security
10 Custom Commands
q >> Quit
Your choice: █
```

2. Enter **7** to select Upgrade.

```
AirWave Management Platform 3.2.4 on example.host.com
1 Upload File
2 Download File
3 Delete File
4 Backup
5 Restore
6 Support
7 Upgrade
8 Advanced
9 Security
10 Custom Commands
q >> Quit
Your choice: █
```

- a. At the next prompt, enter **1** to select Upgrade AirWave Management Platform.
- b. Enter **8.2.6**.

```
Upgrade
1 Upgrade AirWave Management Platform
2 Upgrade OS Kernel
b >> Back
Your choice: 1

Running Upgrade AirWave Management Platform
Enter desired version: 8.2.6 █
```

- c. Enter **y** to enable AirWave to connect to a proxy server. Or, you can enter **N** to bypass this step and go to [step d on page 5](#) to download the software. At the next prompt:
 - (1) Enter the server address and port number (for example, *test.proxy.com* and port 22).
 - (2) Enter **y** to enter the proxy user name and password (for example, *testuser* and *password*).

```
Upgrade package will be downloaded from the internet...
Do you use proxy server? (y/N): y
Enter the proxy server address (proxy.myprovider.net): test.proxy.com
Enter the proxy port: 22
Setting the proxy server to test.proxy.com:22.
Do you use a proxy username/password? (yes/no): y
Enter the proxy username: testuser
Enter the proxy password:
```

d. Enter **1** or **2** to log in to your customer portal with your support user name and password.

```
Download upgrade package from:
  1. Aruba Support Portal
  2. HPE My Networking Portal
Enter your choice (1 or 2): █
```

e. Follow the onscreen instructions to download the software.

Manually Download the Software

You can manually download the software if your AirWave server can't access the Internet.

1. Go to the [Aruba Support Portal](#) or the [HPE My Networking Portal](#) to download the upgrade image.
2. Click the upgrade package, then click **Save** and install the file later.
3. Upload the file:
 - If you are upgrading from AirWave 8.2.3.1 or earlier, copy the file to the AirWave server's **/root** directory using an SCP file transfer application.
 - If you are upgrading from AirWave 8.2.4 or later, upload the software:
 - (1) Log in to the AirWave server with the "ampadmin" user name and password. If you subsequently changed the ampadmin user name and password, enter the current admin name and password. The AMP CLI displays the following menu options.

```
AirWave Management Platform 8.2.4 on example.host.com
 1 Upload File
 2 Download File
 3 Delete File
 4 Backup
 5 Restore
 6 Support
 7 Upgrade
 8 Advanced
 9 Security
10 Custom Commands
q >> Quit
Your choice: █
```

- (2) Enter **1** to upload the file from the AMP server to a source location using SCP to transfer the file.
- (3) At the prompt, enter the location of the source file (for example, *user@host:path*. User is the name of the account on the host computer, host is the hostname of the computer on which the source file exists, and path is the location of the directory that contains the upgrade package).

```
AirWave Management Platform 8.2.4 on example.host.com air
1 Upload File
2 Download File
3 Delete File
4 Backup
5 Restore
6 Support
7 Upgrade
8 Advanced
9 Security
10 Custom Commands
q >> Quit
Your choice: 1

Running Upload File

SCP Source (user@host:path): █
```

(4) At the prompt, enter the password on the source location.

Minimum Requirements

Ensure that you have sufficient disk storage, memory, and hardware or software versions. As additional features are added to AirWave, increased hardware resources become necessary and hardware requirements vary by version. For the most recent hardware requirements, refer to the *AirWave 8.2.4 Server Sizing Guide* on the **Home > Documentation** page.

Supported Upgrades to AirWave 8.2.6

You can upgrade directly to AirWave 8.2.6 from the following software versions: 8.2.2, 8.2.2.1, 8.2.3, 8.2.3.1, 8.2.4, 8.2.4.1, 8.2.5, and 8.2.5.1. If you are running earlier versions of AirWave, upgrade to AirWave 8.2.2 before upgrading to 8.2.5.1.

You can set up a failover server to monitor watched AirWave servers after you install the AirWave Failover license. For information about installing licenses, see "Before You Begin" on page 1.



NOTE

Master Console and Failover services require an access account to the managed AMPs. You typically add this account into the Master Console and Failover local databases, and don't tie it to anyone's personal access account. As such, local database users don't respond to certificate authentication and fail when certificate authentication is required. For more information, see "[Disabling the Certificate Authentication Requirement](#)" on page 14.

The following sections will help you get started using AirWave server:

- "[About the Failover Server](#)" on page 7
- "[Test the Failover Configuration](#)" on page 8
- "[Failover Monitoring](#)" on page 11

About the Failover Server

The failover server:

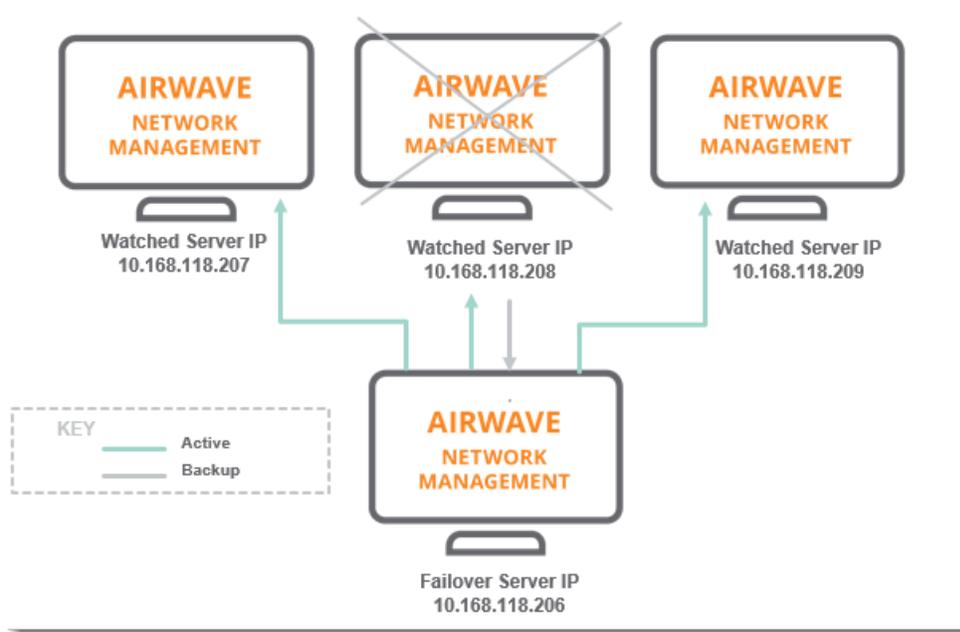
communicates with the watched AirWave servers using SSH, SNMP, and AMON over port 443.

When you use AirWave for failover monitoring, the failover server:

1. Polls the watched AirWave servers.
2. Copies the nightly backup from each server to itself.
3. Restores the watched server from the most recent nightly backup during a failover event. The watched server reboots and begins polling devices. There will be a gap in time between the last nightly backup of the watched AirWave server, and the time of the restoration event.
4. Fails back to its failover role (after a manual back up).

[Figure 2](#) shows the failover server taking over for AW-2 when AW-2 is offline. During this process, the failover server keeps its IP address.

Figure 2: Failover Process



Test the Failover Configuration

You should validate your failover server to ensure that it is capable of taking over for a watched AirWave server.

Failover testing includes:

- "Adding a Watched AirWave Server" on page 8
- "Testing the Failover" on page 9
- "Testing the Failback" on page 9

Adding a Watched AirWave Server

When you add an AirWave server to the watched list, the failover server begins polling the watched AirWave server and downloads the nightly backup. It is this backup that gets restored on the failover server when it takes over for the watched AirWave server.

When fail over occurs, there will be a gap in time between the last nightly back up of the watched AirWave server and fail over. During a planned fail over, such as an upgrade, you can shorten this loss period by running a manual backup from the CLI and copying it to the `/watched_amps` directory.

Follow these steps to add a watched AirWave server:

1. Navigate to **Home > Overview > Watched AMPs**, then click **Add**.
2. Enter the AirWave server's hostname or IP address.
3. Enter the name used for logging in to the AirWave server.
4. Enter the password (alphanumeric without spaces) for the user being created, then confirm the password.
5. Enter how many polls are missed before the failover AMP triggers a failover event. By entering 3, as shown in [Figure 3](#), the failover server will trigger a failover event after 3 missed polls during 5-minute polling intervals.

Figure 3: Adding a Watched AirWave Server

Watched AMP	
Hostname/IP Address:	<input type="text"/>
Username:	<input type="text" value="admin"/>
Password:	<input type="password" value="*****"/>
Confirm Password:	<input type="password" value="*****"/>
HTTP Timeout (5-1000 sec):	<input type="text" value="60"/>
Polling Enabled:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Polling Period:	<input type="text" value="5 minutes"/>
Missed Poll Threshold (1-100):	<input type="text" value="3"/>

6. Click **Add**. The AirWave server you added displays in the Watched AMPs table, as shown in [Figure 4](#).

Figure 4: Watched AMPs

Watched AMP	
Hostname/IP Address:	<input type="text"/>
Username:	<input type="text" value="admin"/>
Password:	<input type="password" value="*****"/>
Confirm Password:	<input type="password" value="*****"/>
HTTP Timeout (5-1000 sec):	<input type="text" value="60"/>
Polling Enabled:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Polling Period:	<input type="text" value="5 minutes"/>
Missed Poll Threshold (1-100):	<input type="text" value="60"/>

Testing the Failover

Perform a test to validate that your watched AirWave server can fail over to the failover server. To test the failover of a server, shut down the server for the minimum poll duration.

AirWave retries polling the AirWave server a number of times before it considers the AirWave server unavailable. Several configuration options affect how long it takes to complete the SNMP polling, including the HTTP timeout, SNMP polling interval, and missed poll threshold.

Testing the Failback

After the failover server fails over and becomes the primary, test the failback functionality.



These procedures will completely erase your existing AirWave installation and operating system and data from your server. Any custom scripts, files, and backups **MUST** be saved to another server.

- ["Restoring from a Backup"](#) on page 10
- ["Reinstating the Failover Server"](#) on page 11

Restoring from a Backup

If the data on the watched AirWave server is important and you want to restore the watched AirWave server from a backup before failing back, follow these steps:

1. Restart the watched AirWave server online.
2. Log in to the CLI on the failover server as the admin user. The following CLI menu appears:

Figure 5: CLI Menu

```
AirWave Management Platform 8.2.4.2 on example.host.com
 1 Upload File
 2 Download File
 3 Delete File
 4 Backup
 5 Restore
 6 Support
 7 Upgrade
 8 Advanced
 9 Security
10 Custom Commands
q >> Quit
Your choice: █
```

3. Run the on-demand backup:
 - a. Select **4** to open the Backup menu and press **Enter**.
 - b. Select **1** to start the backup and press **Enter**.

Figure 6: Running the Backup

```
Backup
 1 Backup Now
 2 Configure Automatic Transfer
 3 Local Backup Retention
b >> Back
Your choice: 1 █
```

4. Configure the backup file transfer from the AirWave server to an external location:
 - a. Select **2** to configure the automatic transfer and press **Enter**.
 - b. Select **1** to set the backup destination and press **Enter**.

Figure 7: Opening the Backup Destination Menu

```
Current Backup Destination: None
 1 Set Destination
 2 Clear Destination
c >> Cancel
Your choice: 1 █
```

- c. At the prompt, type the path of backup destination and press **Enter**.

Figure 8: Entering the Backup Destination

```
Current Backup Destination: None
 1 Set Destination
 2 Clear Destination
 c >> Cancel
Your choice: 1
Backup Destination (user@host:path): backupaccount@example.host.com:backup
```

d. At the prompt, type the password for the user account and **Enter**.

Figure 9: Entering the User Password

```
Current Backup Destination: None
 1 Set Destination
 2 Clear Destination
 c >> Cancel
Your choice: 1
Backup Destination (user@host:path): backupaccount@example.host.com:backup
Password:
```

Reinstating the Failover Server

If you want to make the backup AirWave server the failover server, restore the nightly backup on the failover server.

Failover Monitoring

AirWave Failover is a pared down version of AirWave. The starting point where you can monitor your network is the **Home > Overview** page. The header statistics at the top of the page display the status of your network, while the navigation pane on the left provides access to several pages.

Here are some of the tasks you can do from the WebUI:

- Add watched AirWave servers. On the **Home > Watched AMPs** page, click **Edit** to add an AirWave server to the watched list. For more information, see "[Adding a Watched AirWave Server](#)" on page 8.
- Configure SNMP polling. On the **Home > Watched AMPs** page, click  to change the HTTP timeout, polling interval, and missed poll threshold. For more information, see "[Setting the SNMP Polling Period](#)" on page 12.
- Manage your AirWave licenses. For more information, see "[Adding the Failover License](#)" on page 2.
- Update your user information. For information about changing the settings on the **Home > User Info** page, refer to the *AirWave 8.2.6 User Guide*.
- Manage triggers. On the **System > Triggers** page, click **Add** to create the Watched AMP Down trigger. For help creating a failover trigger, see "[Watched AMP Down Trigger](#)" on page 12.
- Acknowledge alerts. For information about viewing and acknowledging alerts on the **System > Alerts** page, refer to the *AirWave 8.2.6 User Guide*.
- Select a backup. For information, see "[Backup Files and Rotations](#)" on page 11.

Backup Files and Rotations

When selecting a backup file, be sure to select the most relevant backup:

- Nightly backups. The failover server keeps these backups in **/var/airwave-backup** and the backups of watched AirWaves in **/var/airwave-backup/watched_amps**. Backups are aged out by standard rotation.
- Failover backup. During a failover event, the failover server makes an on-demand backup and puts the file in the **/var/airwave-backup/watcher** directory.

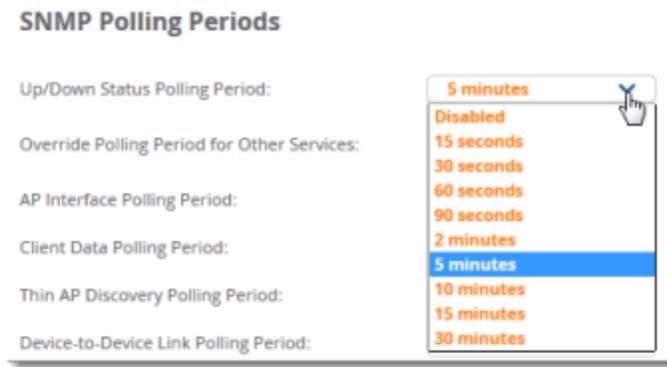
SNMP Polling Period

AirWave polls devices according to the SNMP polling period. The default time between Up/Down SNMP polling periods for each device in a group is 5 minutes.

To configure the polling period:

1. Log in to the watched AirWave server, navigate to **Groups > Basic**, then select the time period from the drop down menu (see [Figure 10](#)).

Figure 10: *Setting the SNMP Polling Period*



2. Click **Save and Apply**.
3. Confirm the changes, then click **Apply Changes Now**. Or, you can click **Schedule** to apply the change later.

Watched AMP Down Trigger

You can create a **Watched AMP Down** trigger to generate an alert when the failover server loses communication with the watched AirWave server. You can send an alert to an email address, or, if you use an NMS tool, to an NMS server.

To add the trigger:

1. Log in to the watched AirWave server, navigate to **System > Triggers**, then click **Add**.
2. Set the severity of the event from normal to critical.
3. Enter a note to be included with the alert.
4. Select the delivery method. The information required depends on the delivery method you choose:
 - Email requires email addresses for the sender and recipient.
 - NMS requires at least one trap destination, which has been preconfigured on the **AMP Setup > NMS** page.
5. Select whether to suppress alerts if an alert is acknowledged. If you select No, an alert is sent everytime an event is triggered.
6. Click **Add** to save the trigger.

Figure 11: Adding a Watched AMP Down Trigger

The Watched AMP Down trigger displays in the Triggers table, as shown in Figure 12.

Figure 12: Watched AMP Down Trigger

TYPE	TRIGGER	ADDITIONAL NOTIFICATION OPTIONS	NMS TRAP DESTINATIONS	SEVERITY	FOLDER	GROUP	INCLUDE SUBFOLDERS
<input type="checkbox"/>	Device Event - SNMP Trap Category is Hardware or SNMP Trap Category is S...	-	-	Normal	Top	-	Yes
<input type="checkbox"/>	Device Event - Event Type is Syslog and Syslog Severity >= Critical	-	-	Normal	Top	-	Yes
<input type="checkbox"/>	Device Event - Event Type is Syslog and Syslog Category is Hardware Monitor	-	-	Normal	Top	-	Yes
<input type="checkbox"/>	Disk Usage - Partition Percent Used >= 80%	-	-	Warning	-	-	-

Figure 13: Setting the SNMP Polling Period

SNMP Polling Periods

Up/Down Status Polling Period:

Override Polling Period for Other Services:

AP Interface Polling Period:

Client Data Polling Period:

Thin AP Discovery Polling Period:

Device-to-Device Link Polling Period:

- 5 minutes
- Disabled
- 15 seconds
- 30 seconds
- 60 seconds
- 90 seconds
- 2 minutes
- 5 minutes**
- 10 minutes
- 15 minutes
- 30 minutes

7. Click **Save and Apply**.
8. Confirm the changes, then click **Apply Changes Now**. Or, you can click **Schedule** to apply the change later.

Watched AMP Down Trigger

You can create a **Watched AMP Down** trigger to generate an alert when the failover server loses communication with the watched AirWave server. You can send an alert to an email address, or, if you use an NMS tool, to an NMS server.

To add the trigger:

1. Log in to the watched AirWave server, navigate to **System > Triggers**, then click **Add**.
2. Set the severity of the event from normal to critical.
3. Enter a note to be included with the alert.
4. Select the delivery method. The information required depends on the delivery method you choose:
 - Email requires email addresses for the sender and recipient.
 - NMS requires at least one trap destination, which has been preconfigured on the **AMP Setup > NMS** page.
5. Select whether to suppress alerts if an alert is acknowledged. If you select No, an alert is sent everytime an event is triggered.
6. Click **Add** to save the trigger.

Figure 14: Adding a Watched AMP Down Trigger

The Watched AMP Down trigger displays in the Triggers table, as shown in Figure 12.

Figure 15: Watched AMP Down Trigger

Triggers							
TYPE ▲	TRIGGER	ADDITIONAL NOTIFICATION OPTIONS	NMS TRAP DESTINATIONS	SEVERITY	LOGGED ALERT VISIBILITY	SUPPRESS UNTIL ACKNOWLEDGED	
<input type="checkbox"/>	Device Event	SNMP Trap Category is Hardware or SNMP Trap Ca...	-	Normal	By Triggering Agent	Yes	
<input type="checkbox"/>	Device Event	Event Type is Syslog and Syslog Severity >= Critical	-	Normal	By Triggering Agent	Yes	
<input type="checkbox"/>	Disk Usage	Partition Percent Used >= 80%	-	Warning	-	Yes	
<input type="checkbox"/>	Watched AMP Down	-	-	Normal	-	Yes	

4 Triggers
[Select All](#) - [Unselect All](#)

Disabling the Certificate Authentication Requirement

You might want to configure local database authentication, and in order to do so you should turn off the certificate authentication requirement and add your PEM bundle. Although certificate authentication is not required when disabled, certificate authentication, or OSCP validation, will occur for users with certificates.

To disable certificate authentication:

1. From the WebUI, go to **AMP Setup > Authentication**, select **Yes** to enable certificate authentication.
2. For the "Require Certificate Authentication" option, select **No**.

About the Command Line Interface

AirWave provides a modular command line interface (CLI) that allows you to run a finite set of management tools and configuration tasks. Some of these tasks include transferring files, enabling support connections, enabling FIPS security, upgrading software, and configuring network interfaces.

CLI Access

A change introduced in AirWave 8.2.4 prevents the root user from being able to connect to the CLI. You can access the CLI through an SSH connection by logging in to the AirWave server with the admin user created when you install or upgrade your software to AirWave 8.2.4. or later. For information about the admin user, see the *AirWave 8.2.6 Installation Guide*.

When the database is down and you access the CLI through an SSH connection, AirWave will skip the click through agreement and advance to the AMP CLI menu.

How to Reset Your Password

If you forgot your CLI password, you can generate a recovery key and contact Technical Support to decode the key and provide recovery password to you.

To reset your password:

1. From a local terminal, or the VM host console, log in using the amprecovery credentials:

```
<AMP server> login: amprecovery  
Password: recovery
```

AirWave displays the following menu options.

Figure 16: Password Recovery Menu

```
AirWave Management Platform 8.2.6 on example.host.com  
1 Generate Recovery Key  
2 SCP Recovery Key  
3 Activate Recovery Password  
q >> Quit  
Your choice:
```

2. Select **1** to generate the recovery key.

Figure 17: Generating the Recovery Key

```
AirWave Management Platform 8.2.6 on example.host.com
 1 Generate Recovery Credentials
 2 SCP Recovery Credentials
 3 Activate Recovery Credentials
 q >> Quit
Your choice: 1

Running Generate Recovery Credentials

Present the following info to customer support to obtain the new password.
You may also SCP this data to another server in order to send it to support
using the "SCP Recovery Credentials" menu option.
Chose the meun option "Activate Recovery Credentials" once you have the
password from customer support.

-----
Hit enter to continue, 's' to show output, 'r' to show return code.
```

3. Select **2** to upload the recovery key to another server using an SCP file transfer application.

```
AirWave Management Platform 8.2.6 on example.host.com
 1 Generate Recovery Key
 2 SCP Recovery Key
 3 Activate Recovery Password
 q >> Quit
Your choice: 2

Running SCP Recovery Key

SCP Destination (user@host:path): root@example.airwave.com:/root/path/
```

4. At the prompt, enter the destination location for the file (for example, user@host:path. User is the name of the account on the destination computer, host is the hostname or IP address of the computer on which the file will be transferred, and path is the path of the destination folder).

5. At the prompt, enter the password on the destination computer.

Figure 18: Authenticating the Destination Computer

```
AirWave Management Platform 8.2.6 on example.host.com
 1 Generate Recovery Key
 2 SCP Recovery Key
 3 Activate Recovery Password
 q >> Quit
Your choice: 2

Running SCP Recovery Key

SCP Destination (user@host:path): root@example.host.com:/root/csr/
Password:
Copying to root@example.host.com:/root/csr/
recovery.gpg                               100% 978      1.0KB/s   00:00

Hit enter to continue, 's' to show output, 'r' to show return code.
```

6. Send the **recovery.gpg** file to Technical Support for key translation.

7. Select **3** to activate the recovery password, then press **y** to continue.
8. Enter the password you received from Technical Support. If you enter the password incorrectly, the password remains unchanged.

Figure 19: Activating the Recovery Password

```
AirWave Management Platform 8.2.6 on example.host.com
 1 Generate Recovery Key
 2 SCP Recovery Key
 3 Activate Recovery Password
 q >> Quit
Your choice: 3

Running Activate Recovery Password

WARNING! Continuing will reset the password for the ampadmin user account.
Are you sure you want to continue (y/n)? y

Enter the password you received from customer support.
Password:
```

9. Log out from the recovery user.
10. Log back in to the CLI as ampadmin using the recovery password:

```
<AMP server> login: <ampadmin>
Password: recovery password
```

Figure 20: Changing the Password

```
Changing password for user ampadmin.
passwd: all authentication tokens updated successfully.

Hit enter to continue, 's' to show output, 'r' to show return code.
```

11. Select **9** to open the Security menu, then select **2** to reset the ampadmin password.
12. At the prompt, type a new password and press **Enter**.

CLI Options

Table 1 lists the CLI commands that are available in AirWave 8.2.6. If there are other important tasks that you can't do from the CLI, contact [technical support](#) for help.

Table 1: CLI Options

Option	Description
1 Upload File	Uploads a file to the AMP server you're currently logged in to using SCP for Unix.
2 Download File	Downloads a file from the local AMP to another server using SCP for Unix.
3 Delete File	Deletes a file from the AMP server. Files shown for deletion might include downloaded files, temporary files, and backup files.
4 Backup	Displays AMP Backup options.
4-1 Backup Now	Runs the back up now.

Option	Description
4-2 Configure Automatic Transfer	Sets the destination for the nightly backup files.
4-3 Local Backup Retention	Changes how many backups AirWave retains (maximum of 4).
5 Restore	Displays restore options.
5-1 AMP Restore	Restores the AMP server from an on-demand, nightly, or imported backup that you select.
5-2 VisualRF Restore	Restores the VisualRF database from the VisualRF backup that you select.
6 Support	Displays support options.
6-1 Show Tech Support	Displays information about the AMP server to show technical support.
6-2 Generate Diagnostic Tarball	Displays the compressed log collection for sending to customer support.
6-3 Initialize Support Connection	Loads the support_connection.tar file provided by customer support and creates the support user (by default, awsupport) and password.
6-4 Start Support Connection	Toggles on and off the support connection.
6-5 Delete Support User	Deletes the awsupport.gpg file.
6-6 Show contents of awsupport.gpg	Displays the encrypted support credentials.
7 Upgrade	Displays upgrade options.
7-1 Upgrade AirWave Management Platform	Runs the AirWave software upgrade.
7-2 Upgrade OS Kernel	Runs the kernel upgrade (requires rebooting the AMP server).
8 Advanced	Displays system options.
8-1 Restart Application	Restarts the AMP services.
8-2 Reboot System	Reboots the AMP server.
8-3 Configure Network Settings	Configures network settings.
8-4 Set Hostname	Sets the hostname of the AMP server.
8-5 Shutdown System (halt)	Shuts down the AMP server gracefully.
9 Security	Displays security options.

Option	Description
9-1 Reset Web admin Password	Resets the Web UI log in password for admin.
9-2 Change OS User Password	Changes the CLI log in password.
9-3 Add SSL Certificate	Installs the SSL certificate, used to establish secure web sessions, on your AMP server.
9-4 Add DTLS Certificates	Installs the DTLS certificates, used to encrypt secure AMON traffic, on your AMP server.
9-5 Enable FIPS	Toggles on or off FIPS 140-2 Approved Mode (reboot required action).
9-6 Show EngineID	Displays the SNMPv3 engine ID.
9-7 Module Key	Displays module key options.
9-7-1 Show	Displays the PGP key used to create a custom module.
9-7-2 Save	Saves the PGP key.
10 Custom Commands	Displays custom command option.
10-1 Add New Menu Module	Adds a new CLI menu module that you select (requires requesting module encrypted with a module key from customer support).
b >> Back (or Ctrl+c)	Returns to the previous menu.
c >> Cancel	Cancel the key request.
11 VisualRF Restore	Restores the visualrf_backup.pl file. Files shown for backup might include downloaded files, temporary files, and backup files. NOTE: If the STIG module is enabled on your system, this command option is unavailable.
12 Enter Commands	Some read-only commands are available from this menu. To see a list of commands, type a question mark (?) at the prompt. For more information, see Table 2 . NOTE: If the STIG module is enabled on your system, this command option is unavailable.
q	Exits the CLI session.

[Table 2](#) lists the running enter commands that are available when you select **12** from the CLI.

Table 2: *Running Enter Commands*

Command	Description
?	Displays the list of commands.
q	Returns to CLI menu.
h	Displays the history of commands you have typed.
h <pattern>	Displays history of all commands, matching the specified <pattern> input.

Table 2: Running Enter Commands (Continued)

Command	Description
ch	Clears the history of commands displayed on the screen.
r	Repeats the previous command.
r <number>	Repeats the command, specified by the <number> from the history list.
r /x/y	Repeats the previous command, replacing x with y.
clear	Clears the terminal screen.
date	Displays the current date and time.
date MMDDhhmm	Changes the date and time on the AMP server.
top	Displays the status of running processes.
daemons	Displays the running daemons.
wd	Displays the monitoring of running daemons, refreshing after 1-second intervals.
wd <n>	Displays the monitoring of running daemons, refreshing after the <n> interval.
ls	Lists the files in the AMP CLI directory. NOTE: You can use shell patterns with *, ?, and [].
rm	Removes files from the AMP CLI directory. NOTE: You can use shell patterns with *, ?, and [].
rd	Restarts the daemons.
psg <pattern>	Displays the running processes, matching the <pattern> you typed.
pss <pattern>	Displays the running processes like grep but shows more detailed information, matching the <pattern> you typed.
show_tech_support	Displays information about the AMP server to show technical support.
dbsize	Displays the 30 largest database tables.
crr	Displays the Red Hat version on your AMP server.
amp_version	Displays the AirWave version on your AMP server.
df -h	Shows disk space usage.
git diff	Checks for patches.
hostname	Displays the DNS name of the AMP server.
amp_backup	Runs a backup and puts the file in the AMP CLI directory.

Table 2: Running Enter Commands (Continued)

Command	Description
amp_restore <filename>	Restores the AMP server from the backup.
remove_visualrf_cache	Clears the visualrf_bootstrap file.
iptables -L	Displays the IP tables.
dmidecode	Displays the serial number of the AMP server. The serial number will display along with BIOS information.
network	Runs the network setup wizard.
service	Lists all services and allows you to manage them.
service iptables status	Displays the full status for IP tables.
service <service> status start stop restart	Manages the <service> you typed.
qlog	Lists the status of available qlog topics.
qlog enable <topic>	Enables debugging. As files are created, they appear in the AMP CLI directory. NOTE: If there is more than 1 qlog topic matching the substring, a numbered picklist will be displayed. Enter the desired qlog topic number or multiple numbers separate by spaces. You can give a unique prefix or a unique substring.
qlog disable <topic>	Disables debugging for an individual topic. NOTE: You can give a unique prefix or a unique substring.
qlog disable all	Disables debugging for all qlog topics. NOTE: If there is more than 1 qlog topic matching the substring, a numbered picklist will be displayed. Enter the desired qlog topic number or multiple numbers separate by spaces. You can give a unique prefix or a unique substring.
snoop	Displays the list of work queue snoop debug topics. NOTE: If there is more than 1 qlog topic matching the substring, a numbered picklist will be displayed. Enter the desired qlog topic number or multiple numbers separate by spaces. You can give a unique prefix or a unique substring.
snoop <topic>	Enables work queue snoop debug for the desired topics. NOTE: You can give a unique prefix or a unique substring.
snoop active	Displays the active work queue snoop topics.
snoop stop <topic>	Stops work queue snoop on the selected topic. NOTE: You can give a unique prefix or a unique substring.
snoop stop all	Stops all active work queue snoop debugging.