AirWave 8.2.11.1

Failover Guide

About This Guide

This guide describes how to configure the AirWave failover server to monitor your network and to AirWave to manage the failover process. This document includes the following sections:

What's New

The following sections of the AirWave Failover Guide have been updated for this release. For a full list of new features and updates in AirWave 8.2.11.1, including updates to other documents, refer to the *AirWave 8.2.11.1 Release Notes*.

Table 1: *What's New in This Version of the Failover Guide*

Update	Description
Enable certificate authentication to a watched server	Starting with AirWave 8.2.11.1, you can specify if you want to enable certificate authentication to authenticate to the watched AirWave server. This option is disabled by default. If you select **Yes**, additional fields appear on this page that prompt you to browse to and select the certificate (.pfx) file, and to enter and confirm the certificate password.

Contacting Support

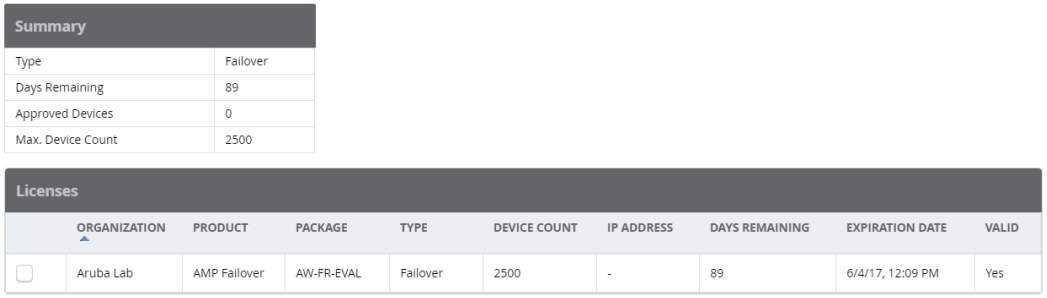
Main Site	arubanetworks.com
Support Site	asp.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	lms.arubanetworks.com
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 8.2.11.1 Installation Guide*.

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
☐	Aruba Lab	AMP Failover	AW-FR-EVAL	Failover	2500	-	89	6/4/17, 12:09 PM	Yes

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 {Page_Link}“Before You Begin” (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 10.

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

About the Failover Server

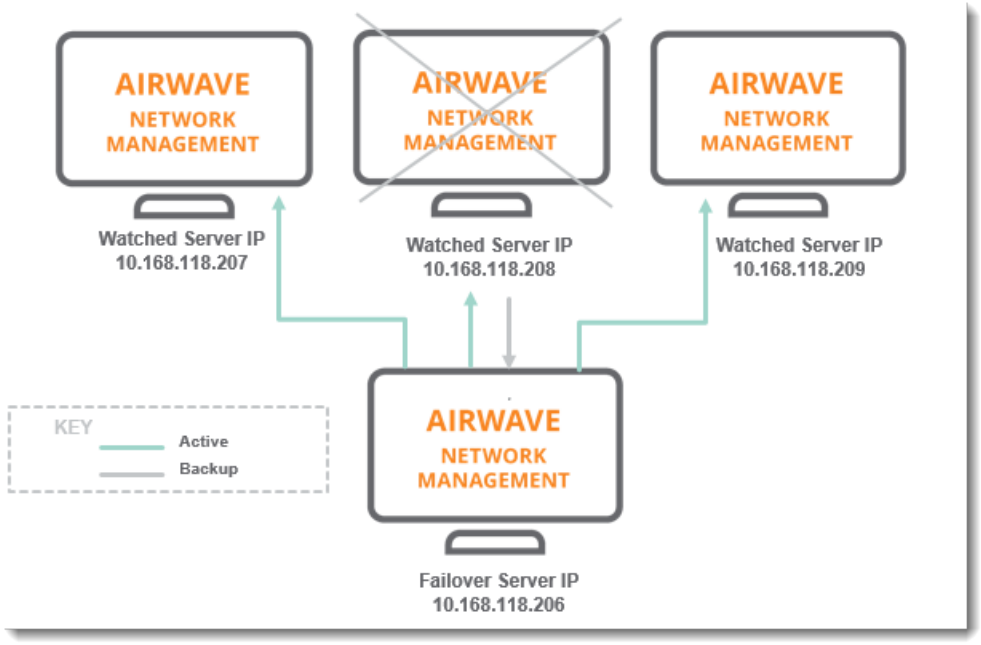
The failover server communicates with the watched AirWave servers using SSH, SNMP, and AMON over port 443.

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 4
- "Testing the Failover" on page 5
- "Testing the Failback" on page 5

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.

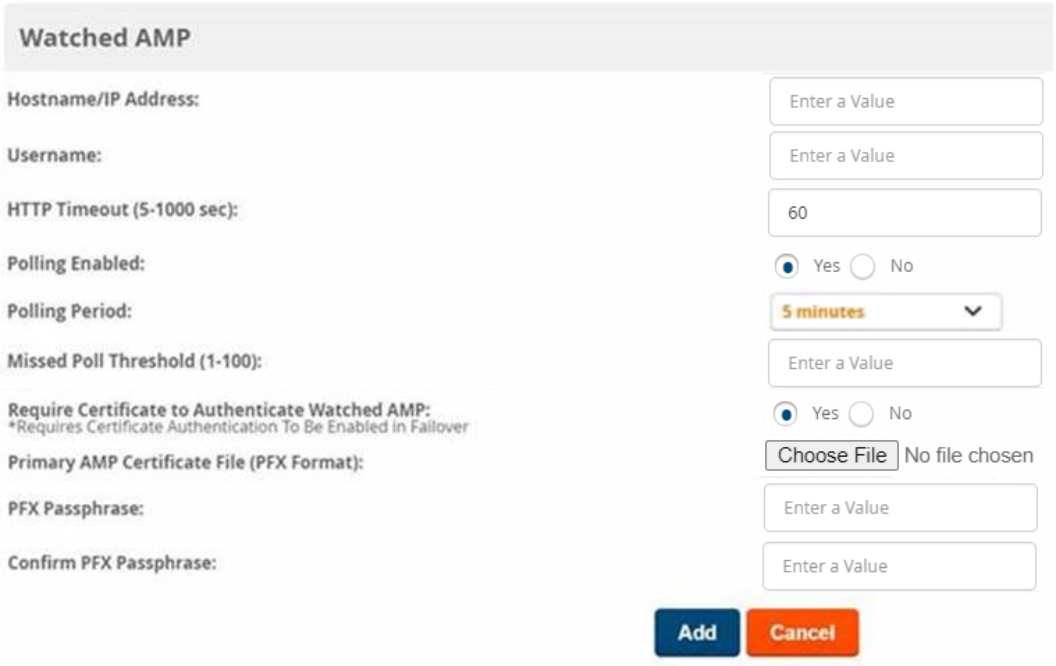
When fail over occurs, there will be a gap in time between the last nightly back up of the watched AirWave server and fail over. During a planned fail over, such as an upgrade, you can shorten this loss period by running a manual backup from the CLI and copying it to the **/watched_amps** directory.

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. If you plan on enabling certificate authentication in Step 6, enter the certificate's common name (CN)
4. Enter the password (alphanumeric without spaces) for the user being created, then confirm the password. This field does not appear if certificate authentication is enabled.
5. Enter how many polls should be missed during the specified polling period before the failover AirWave server triggers a failover event. For example, by entering **3** the failover server will trigger a failover event after three missed polls during 5-minute polling intervals.

6. Starting with AirWave 8.2.11.1, you can specify if you want to enable certificate authentication to authenticate to the watched AirWave server. This option is disabled by default. If you select **Yes**, additional fields appear on this page that prompt you to browse to and select the certificate (.pfx) file, and to enter and confirm the certificate password.

Figure 3: *Adding a Watched AirWave Server (certificate authentication enabled)*



7. Click **Add**.
8. If you enabled certificate authentication in Step 6, you must also configure the failover AirWave server with the login certificate.
   a. Navigate to **AMP Setup > Authentication**, and select **Yes** to enable certificate authentication.
   b. For the **Require Certificate Authentication** option, select No.
   c. Enter your certificate bundle in the text field.
   d. Scroll down, then click **Save**.

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.

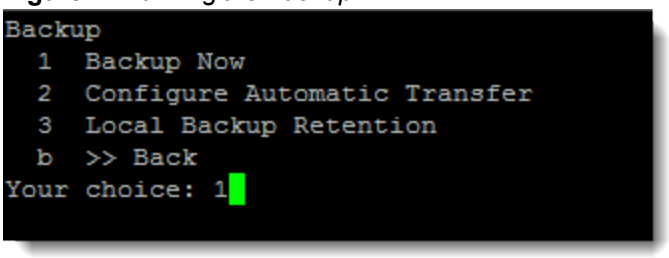
- "Restoring from a Backup" on page 6
- "Reinstating the Failover Server" on page 7

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:

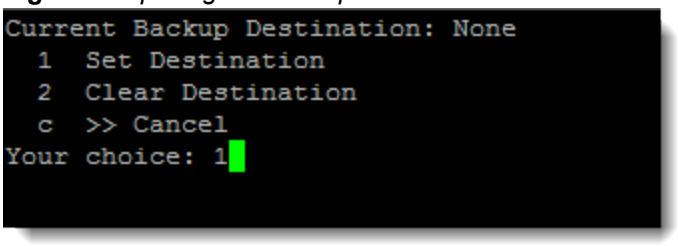
1. Restart the watched AirWave server online.
2. Log in to the CLI on the failover server as the admin user.
3. Run the on-demand backup:
   a. Select **2** to open the Backup menu and press **Enter**.
   b. Select **1-1** to start the on-demand backup and press **Enter**.

Figure 4: *Running the Backup*



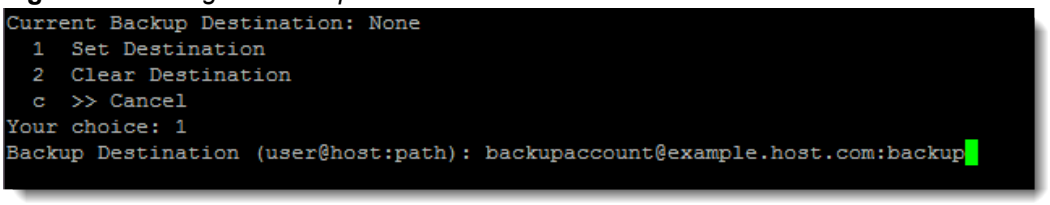
4. Configure the backup file transfer from the AirWave server to an external location:
   a. Select **2** to open the Backup menu and press **Enter**.
   b. Select **2-1** to configure c automatic transfer and set the backup destination. Press **Enter**.

Figure 5: *Opening the Backup Destination Menu*



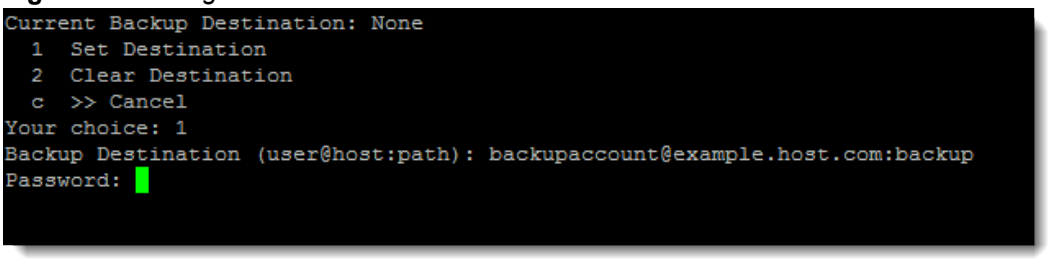
   c. At the prompt, type the path of backup destination and press **Enter**.

Figure 6: *Entering the Backup Destination*



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

Figure 7: *Entering the User 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 4.
- 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 8.
- Manage your AirWave licenses. For more information, see "Initial Setup" on page 2.
- Update your user information. For information about changing the settings on the **Home > User Info** page, refer to the *AirWave 8.2.11.1 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 8.
- Acknowledge alerts. For information about viewing and acknowledging alerts on the **System > Alerts** page, refer to the *AirWave8.2.11.0 User Guide*.
- Select a backup. For information, see "Backup Files and Rotations" on page 7.

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 AirWaveservers 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 8).

Figure 8: *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.

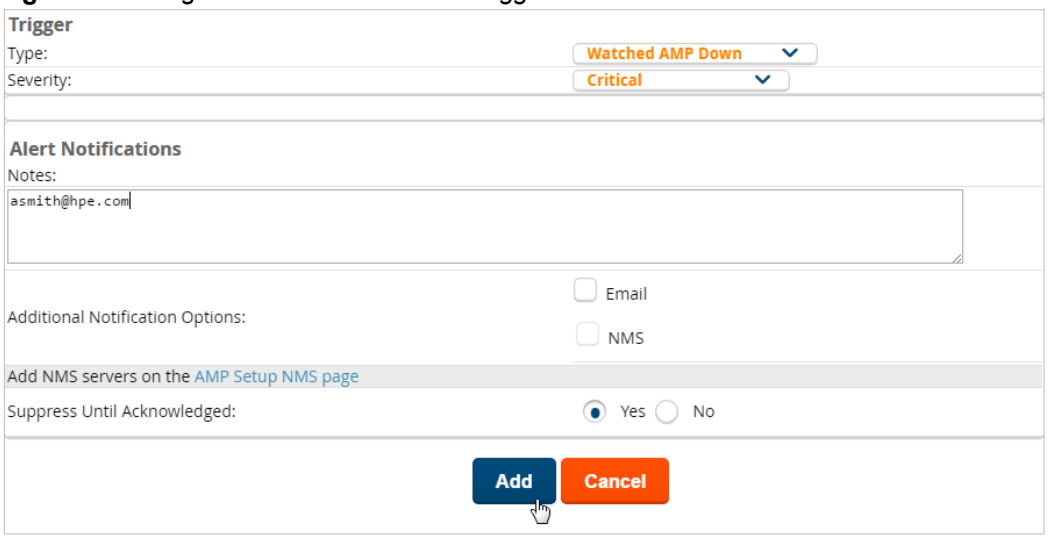
Watched AMP Down Trigger

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 9: *Adding a Watched AMP Down Trigger*



The Watched AMP Down trigger displays in the Triggers table, as shown in Figure 10.

Figure 10: *Watched AMP Down Trigger*

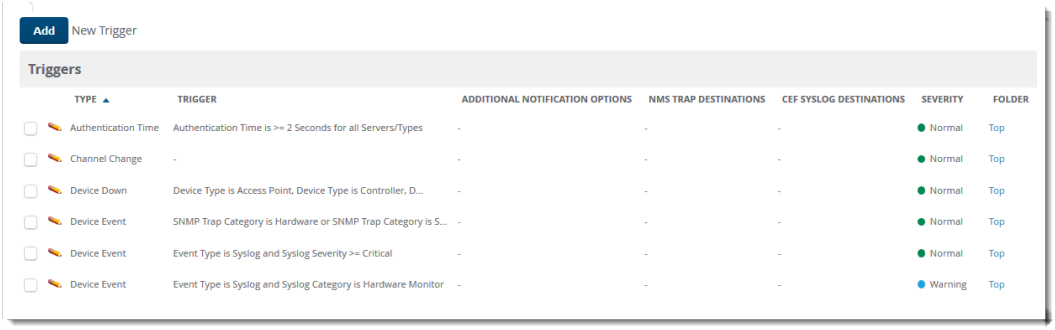


Figure 11: *Setting the SNMP Polling Period*

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

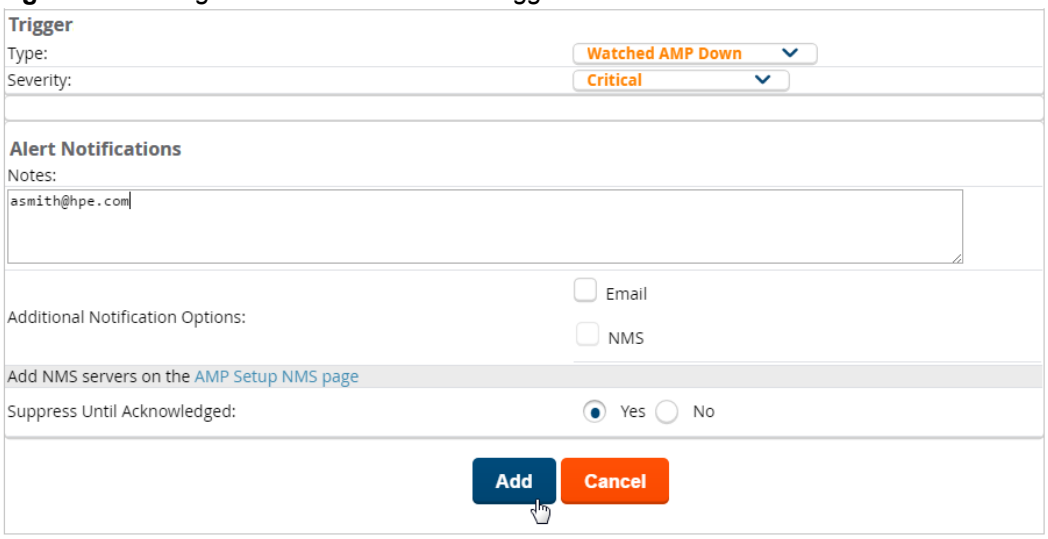
Watched AMP Down Trigger

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:

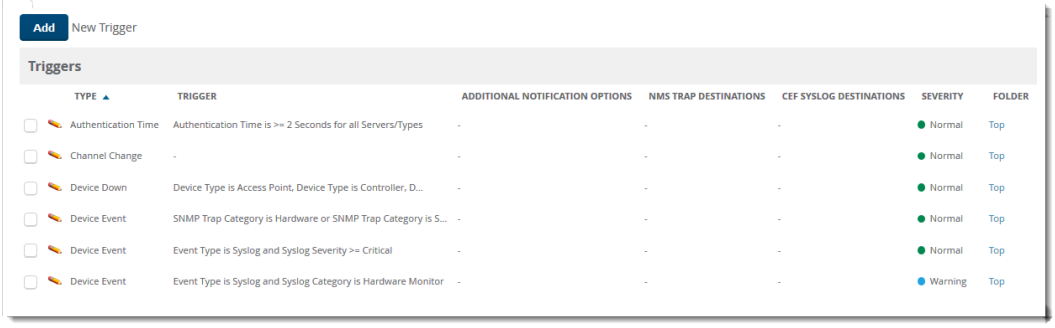
1. Log in to the watched AirWave server, navigate to **System > Triggers**, then click **Add**.
2. Set the severity of the event from normal to critical.
3. Enter a note to be included with the alert.
4. Select the delivery method. The information required depends on the delivery method you choose:
   - 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 12: *Adding a Watched AMP Down Trigger*



The Watched AMP Down trigger displays in the Triggers table, as shown in Figure 10.

Figure 13: *Watched AMP Down Trigger*

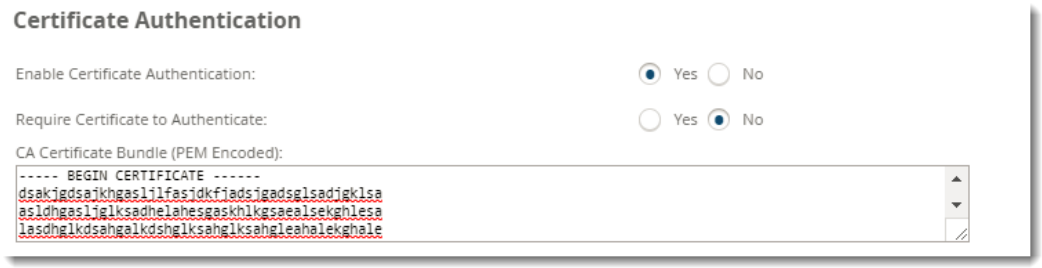


Disabling the Certificate Authentication Requirement

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, certifcate authentication, or OCSP 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**.
3. Enter your PEM certificate bundle in the text field.



4. Scroll down, then click **Save**.

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

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 8.2.11.1. For information about the admin user, see the *AirWave 8.2.11.1 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.

CLI Options

Table 3 lists the CLI commands that are available in AirWave 8.2.11.1. If there are other important tasks that you can't do from the CLI, contact technical support for help.

Table 2: *CLI Options*

Option	Description
1 Files	Displays AMP file options
1-1 Upload File	Uploads a file to the AMP server you're currently logged in to using SCP for Unix.
1-2 Download File	Downloads a file from the local AMP to another server using SCP for Unix.
1-3 Delete File	Deletes a file from the AMP server. Files shown for deletion might include downloaded files, temporary files, and backup files.
2 Backup	Displays AMP backup and restore options.
2-1 Backup >	Displays AMP backup options.
2-1-1 Backup Now	Runs the back up now.
2-1-2 Configure Automatic Transfer	Sets the destination for nightly backup files. When you configure the automatic backup transfer, you won't see the backup file on the external server until the next nightly maintenance window passes.
2-1-3 Local Backup Retention	Changes how many backups AirWave retains (maximum of 4).

Option	Description
2-2 Restore >	Displays restore options.
2-2-1 AMP Restore	Restores the AMP server from an on-demand, nightly, or imported backup that you select.
2-2-2 VisualRF Restore	Restores the VisualRF database from the **visualrf_backup.pl** file that you select. Files shown for backup might include downloaded files, temporary files, and backup files.
3 Configuration	Displays AMP configuration options
3-1 Configure Network Settings	Configures network settings. You will be prompted to select an interface. Once an interface is selected, you can modify any of the following settings: 1) IPv4 Address 2) IPv4 Netmask 3) IPv4 Gateway 4) IPv6 Address (optional) 5) IPv6 Gateway (optional) 6) Primary DNS Server 7) Secondary DNS Server
3-2 Set Hostname	Sets the hostname of the AMP server.
3-3 Set Timezone	Sets the timezone of the AMP server. You will be prompted to select a continent/ocean, country and region, or specify the time zone using the Posix TZ format.
3-4 Certificates >	Displays certificate options.
3-4-1 Add SSL Certificate	Installs the SSL certificate, used to establish secure web sessions, on your AMP server.
3-4-2 Generate Certificate Signing Request	Creates a CSR that identifies which server will use the certificate.
3-4-3 Install Signed Certificate	Installs a signed certificate. AirWave supports signed certificates in PEM format with *.crt file extensions.
3-4-4 Install Self-Signed Certificate	Regenerates the self-signed certificate created when you installed AirWave.
3-4-5 Add DTLS Certificates	Installs the DTLS certificates, used to encrypt secure AMON traffic, on your AMP server.

Option	Description
3-4-6 OCSP >	Displays options for OCSP responders.
3-4-6-1 Make OCSP Optional/Required	Toggles on or off OCSP certificate validation when certificate authentication is required from the UI. **NOTE:** When configuring OCSP and CRL, one type of validation must be made mandatory if the other is optional. The optional validation type will be used if the initial validation type fails. When OCSP is optional, AirWave will first check for CRL certificate validation, and only check OCSP validation if CRL validation fails.
3-4-6-1 Manage OCSP URIs	This setting allows you to ad OCSP URIs. Click the a option to add a new URI.
3-4-7 CRL >	Manage AMP Certificate Revocation List (CRL) options for certificate path discovery and validation.
3-4-7-1 Make CRL Optional/Required	Toggles on or of CRL validation. **NOTE:** When configuring OCSP and CRL, one type of validation must be made mandatory if the other is optional. The optional validation type will be used if the initital validation type fails. When CRL is optional, AirWave will first check for OCSP certificate validation, and only check CRL validation if OCSP validation fails.
3-4-7-2 Manage CRL distribution URLs	Select this option to delete an existing URL, or click the **a** option to add a new URL
3-4-7-3 Manage CRL files	Select this option to delete an CRL file, or click the **a** option to add a new file.
3-5 SSHD >	Displays options for the SSH daemon (SSHD).
3-5-1 Set MaxAuthTries	Sets a limit on how many authentication attempts are allowed per user session.
3-5-2 Use Compatible Ciphers	Use this command to enable weak ciphers *aes128-cbc*, a*es192-cbc*, and *aes256-cbc* if the config file has ciphers set and these algorithms are not part of the existing AirWave ciphers.
4 System	Displays AirWave system options.
4-1 Upgrade	Runs the AirWave software upgrade.
4-1-1 Aruba Support Portal (asp.arubanetworks.com)	Download the upgrade package from the Aruba Support Portal at asp.arubanetworks.com

Option	Description
4-1-2 HPE My Networking Portal	Download the upgrade package from the HPE My Networking Portal
4-2 Disable AMP	Toggles on and off the stopping and starting of all AMP services.
4-3 Restart AMP	Restarts the AMP services.
4-4 Reboot System	Reboots the AMP server.
4-5 Shutdown System (halt)	Shuts down the AMP server gracefully.
4-6 Show EngineID	Displays the SNMPv3 engine ID.
4-7 Module Key >	Displays module key options.
4-7-1 Show	Displays module key options.
4-7-2 Save	Saves a copy of the module key to the file <host>.module.key (e.g., AirWave.example.com.module.key).
5 **Users**	Displays User options.
5-1 Reset Web admin Password >	Resets the WebUI login password for the admin user.
5-1-1 admin	Changes the password for the WebUI admin user.
5-2 Change CLI User Password >	Changes the CLI log in password.
5-2-1 ampadmin	Changes the password for the CLI ampadmin user.
5-2-2 amprecovery	Changes the amprecovery password.
5-3 Add File Transfer User	Creates a new file transfer user account that works to transfer files between the AMP server and an SSHD client.
5-4 Remove amprecovery Account	Remove an AMP recovery user account.
5-5 Advanced >	Remove an AMP recovery user account.
5-5-1 Enable/Disable Complex Password Rules	Toggles on or off the configuration of password rules. This option only appears if STIGs are not applied to the AirWave server.
5-5-2 Set Lockout Threshold	Sets the number of failed log in attempts before the CLI user account is locked.
5-5-3 Set Lockout Timer	Sets the waiting period before the CLI user account is unlocked.

Option	Description
5-5-4 Set Password Length	Sets the length of the password.
5-5-5 Set Inactivity Threshold for CLI Users	Sets the period of inactivity before logging out the CLI user.
5-5-6 Unlock Web Users	Unlocks the Web user account. You will be prompted to select a user.
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.
6-7 Paste Encoded Text	Provides the option to paste the encoded format of the support_connection.tar file instead of upload the package.
7 Security	Displays AirWave security options.
7-1 Apply STIGs	Applies and enforces the Security Technical Implementation Guide (STIG) modules according to the Defense Information Systems Agency (DISA) for STIG compliance. If you enable this setting, it can't be changed.
7-2 Enable FIPs (requires reboot)	Toggles on or off FIPS 140-2 Approved Mode (requires a reboot).
7-3 Configure SELinux >	Toggles on or off Security-Enhanced Linux (SELinux), which provides users more access control of security policies.
7-3-1 Leave Disabled	Leave SELinux disabled.
7-3-2 Permissive (requires reboot)	in **Permissive** mode, SELinux displays warnings only but does not enforce the security policy. This mode is useful for debugging permissions issues.
7-3-3 Enforcing (requires reboot)	In **Enforcing** mode, the SELinux security policy is enforced.

Option	Description
7-4 Enable Firmware Integrity Check	Toggles on or off a validation check of the firmware code.
8 Advanced	Displays advanced system options.
8-1 Custom Commands >	Displays the custom command option.
8-1-1 Add New Menu Module	If you have already requested a new CLI module encrypted with a module key from customer support, you can use this command to select and add that module.
8-2 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 4.
8-3 Configure Network Settings	Configures network settings.
8-4 Enable DB transaction logging	Use this option to enable or disable additional logging of postgres database transactions. This option only appears when STIGs are applied to the AirWave server. **NOTE:** Enabling this option will increase disk usage and impact performance.
b >> Back (or Ctrl+c)	Returns to the previous menu.
c >> Cancel	Cancels the key request.
q	Exits the CLI session.

Table 3: *CLI Options*

Table 4 lists the running enter commands that are available when you select **11** from the CLI.

Table 4: *Running Enter Commands*

Command	Description
?	Displays the list of commands.
help <topic>	Displays the help for the <topic>.
man <topic>	Invokes the linux `man` command for the <topic>.
quit	Returns to CLI menu.
q	Returns to CLI menu.
exit	Returns to CLI menu.
history	Displays the history of commands you have typed.

Table 4: *Running Enter Commands (Continued)*

Command	Description
h	Displays the history of commands you have typed.
h <pattern>	Displays history of all commands, matching the specified <pattern> input.
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 [ ].
cleanup	Deletes files that are no longer needed, including log files, old source files, and pre-upgrade backups.
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.
dbsize <n>	Displays the <n> largest database tables.
dbsize -l	Displays details of disk space consumed, tuple spaces, and the actual size of the 30 largest tables.

Table 4: *Running Enter Commands (Continued)*

Command	Description
dbsize -l <n>	Displays details of disk space consumed, tuple spaces, and the actual size of the <n> largest tables.
osrel	Displays the release version of the operating system.
license	Displays the license for the 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.
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 along with BIOS information.
network	Runs the network setup wizard.
dci	Displays the device communication interface, which configures the ethernet interface used for communication with devices.
ifconfig <interface>	Displays the status of the network interfaces.
ip route	Displays the IP routing tables.
disable_whitelist	Resets the AMP whitelist to allow access (and restarts the AMP web server).
sw <ap id> args	Uses SNMP v1GETBULK to send a request to the database and walks back a list of all items up to a specified limit.
sw2 <ap id> args	Uses SNMP v2c GETBULK to send a request to the database and walks back a list of all items up to a specified limit.
sw3 <ap id> args	Uses SNMP v3 GETBULK to send a request to the database and walks back a list of all items up to a specified limit.
tcpdump args	Sends TCP packet data to an output file that you can use for later troubleshooting.
ping args	Sends ICMP echo request to confirm whether your network is reachable.
nslookup args	Queries the Internet name server, or the host name of the name server.

Table 4: *Running Enter Commands (Continued)*

Command	Description
traceroute args	Tracks the route packets from an IP network to a host, using the IP protocol's time to live (TTL) value and getting an ICMP time exceeded response from each gateway along the path to the host.
free args	Displays the amount of free and used memory in the system.
service iptables	Displays the full status for IP tables.
service	Lists all services and allows you to manage them.
service <service> status|start|stop|restart	Manages the <service> you typed.
service <service>	Displays the status of the service.
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.
ethernet_bonding <ip><netmask><gateway>	Enables ethernet bonding of two network interfaces. **NOTE:** If you enter ethernet_bonding without variables, you will be prompted for 3 input variables.
docker <bridge_ip_ address/cidr_bits>	Configures the AirWave Glass feeder service. **NOTE:** If you enter docker without variables, you will be prompted for 2 input variables.