AirWave 8.2.11.0

Security Deployment Guide

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett-Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Enterprise Company
Attn: General Counsel
6280 America Center Drive
San Jose, CA 95002
USA

Please specify the product and version for which you are requesting source code.

You may also request a copy of this source code free of charge at: http://hpe.com/software/opensource.

Contents

Introduction **5**
External Security Testing and Accreditation 5
FIPS 140-2 5
Common Criteria 5
Internal Security Testing 5
Vulnerability Management Process 6
Bug Bounty Program 6
Contacting Support 6
Security Configuration **7**
Before You Begin 7
Step 1: Harden the System 7
Step 2: Enable Security Enhanced Linux (SELinux) 8
Step 3: Configure External Logging 9
Step 4: Disable Configuration Auditing 9
Step 5: Create User Roles 11
Example: Read-Only Role 11
Example: Read-Write Role for a Device Manager 12
Example: Read-Write Role for an AMP Admin 12
Step 6: Configure Remote Authentication 13
Step 7: Configure Two-Factor Authentication 14
Step 8: Configure OCSP 15
Step 9: Configure a Certificate Revocation List (CRL) 15
Step 10: Delete the Default Admin User and Roles 16
Step 11: Configure the Click Through Agreement 17
Step 12: Configure the Idle Timeout 17
Step 13: Configure an Absolute Timeout 17
Step 14: Configure Session Limits 18
Step 15: Configure the Whitelist 18
Step 16: Create a Disk Usage Trigger 18
Step 17: Disable the Update Checker 19
Step 18: Configure Secure NTP and DNS with Redundancy 19
Step 19: Configure Automated Backup Transfer 20
Step 20: Generate a Certificate Signing Request (CSR) 21
Step 21: Installing the Signed Certificate 22
Step 22: Configure Transaction Logging 23
Backup and Recovery **24**
Back up Your Data 24
Download the Backup 24
Upload the Backup 24
Restore from a Backup 25
Failover Basics **26**
About the Failover Server 26
Test the Failover Configuration 27
Adding a Watched AirWave Server 27
Testing the Failover 28

Testing the Failback 28
Restoring from a Backup 29
Reinstating the Failover Server 30
Failover Monitoring 30
Backup Files and Rotations 30
SNMP Polling Period 31
Watched AMP Down Trigger 31
Watched AMP Down Trigger 32
Disabling the Certificate Authentication Requirement 33
Appendix A Reference Information 35
Other Authentication Options 35
RADIUS Authentication and Authorization 35
TACACS+ Authentication 35
ClearPass Policy Manager (CPPM) for AirWave 36
Appendix B Complete Security Technical Implementation Guide (STIG) List 39
Best Practices for STIG Application 39

This document is intended to assist customers and partners in configuring AirWave in a secure manner. You should complete additional hardening steps. Security recommendations often involve tradeoffs, and not every recommendation in this document will be appropriate for every situation. Recommendations given in this document represent security best practices and should be followed wherever network security is a priority.

External Security Testing and Accreditation

Aruba spends a significant amount of time and money conducting independent third-party security testing of its products. While the majority of this testing is relevant to and required by government agencies, it has value to all types of users. In some cases, organizations might want to rely on recognized security testing authorities rather than conducting their own product testing.

FIPS 140-2

The Federal Information Processing Standards is a system for testing and certifying cryptographic modules. As part of this testing, a laboratory accredited by the US and Canadian governments examines design documentation, source code, and development practices, in addition to conducting extensive testing of cryptographic functions. Products that implement FIPS 140-2 validated cryptography are assured to be using cryptography correctly. For more information about FIPS 140-2, see the NIST website.

Aruba Networks provides a FIPS-compliant version of AirWave. In order to maintain this compliance, AirWave includes a stripped-down CLI. With AirWave, the ability for root to ssh directly into the AMP CLI has been removed. For information about the CLI, see "Appendix B, AMP Command Line Interface" in the *AirWave 8.2.11.0 User Guide*.

The FIPS-compliant WebUI includes all the same functionality as the regular AirWave WebUI.

Common Criteria

The Common Criteria for Information Technology Security Evaluation (abbreviated as CC) is an international standard (ISO/IEC 15408) for computer security evaluation. It is recognized by the governments of approximately 47 nations, and products that have received CC certificates are generally accredited for use in unclassified government systems. Whereas FIPS 140-2 is focused on cryptography, Common Criteria focuses on “everything else” that is security relevant, including management protocols, authentication mechanisms, vulnerabilities, and selections of parameters such as cipher suites. In the United States, Common Criteria is administered and controlled by NIAP – the National Information Assurance Partnership. For more information about NIAP and Common Criteria, see the NIAP website.

Internal Security Testing

Each AirWave release goes through extensive quality assurance testing. As part of the testing process, we use Nessus.

Any findings returned by this scanner are examined to determine if they are genuine vulnerabilities or false positives. Actual vulnerabilities will cause a bug to be opened.

In addition to quality assurance testing, an internal group known as Aruba Threat Labs provides advanced vulnerability research against Aruba products. Aruba Threat Labs conducts penetration testing through both black-box and white-box testing, also including source code analysis. Aruba Threat Labs also contracts with external third-party penetration testing firms to conduct targeted testing.

Vulnerability Management Process

Aruba publishes a vulnerability response policy at Aruba Security Advisories. This location also hosts security advisories published by Aruba. An RSS feed is available from this page as well. Any customer with an active support contract will receive vulnerability advisories by email; if you want to receive advisories but do not have a support contract, go to http://community.arubanetworks.com/t5/AAA-NAC-Guest-Access-BYOD/Security-vulnerability-advisories/m-p/176738 to subscribe to the thread and be notified of updates.

Bug Bounty Program

Aruba operates a bug bounty program, through which security researchers are paid a reward for finding and reporting security vulnerabilities in Aruba products. The program is managed by Bugcrowd, a third-party company that manages the researcher pool, reward payout, and the tracking and reporting process on behalf of Aruba. For more information, see the Bugcrowd website.

Contacting Support

Contact Technical Support for help on your Aruba systems.

Main Site	arubanetworks.com
Aruba Support Site	support.arubanetworks.com
North American Telephone	1-800-633-3600 1-800-943-4526 (Aruba legacy) 1-408-754-1200 (Aruba legacy)
HPE Support Site	hpe.com/networking/support

This chapter provides step-by-step instructions for securing your system. We recommend performing these steps in the order presented to maximize the benefits of logging.

NOTE

If you are unable to log in to AirWave WebUI, contact Technical Support to change the AMP authentication configuration through the CLI. You will need your CLI user name and password to reset the ampadmin password.

Before You Begin

There are 3 types of licenses: AMP, Master Console, and Failover. Ensure that you have installed the AMP license before continuing with the security configuration.

NOTE

AirWave pages are protected via SSL. Some browsers will display a confirmation dialog for your self-signed certificate. Signing your certificate will prevent this dialog from displaying.

To install the AMP license:

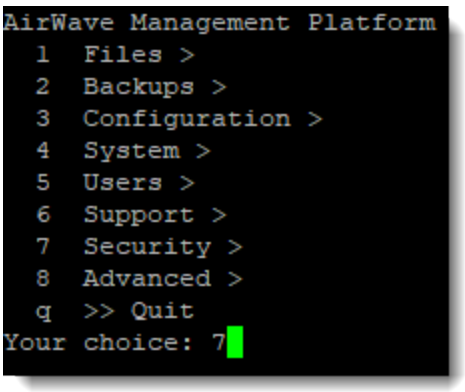
1. Open a Web browser, then enter your AirWave server's IP address in the address bar to connect to the AirWave WebUI.
2. Navigate to **Home > License**, then click **Add**.
3. Enter your license key in the pop up window, then click **Add**.
4. Review the End User License Agreement, then click **I Accept**.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

Step 1: Harden the System

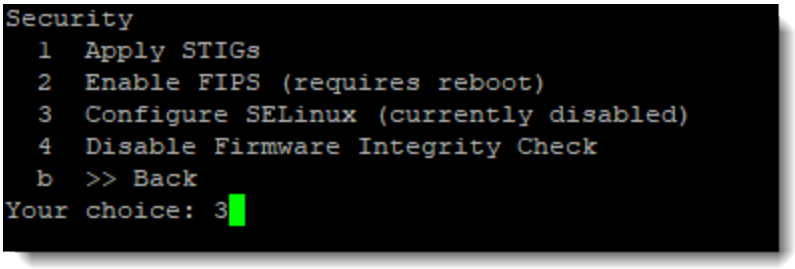
Hardening the system requires that you run the STIG module to enable Defense Information Systems Agency (DISA) STIG compliance and turn on FIPS 140-2 approved mode.

To harden the system:

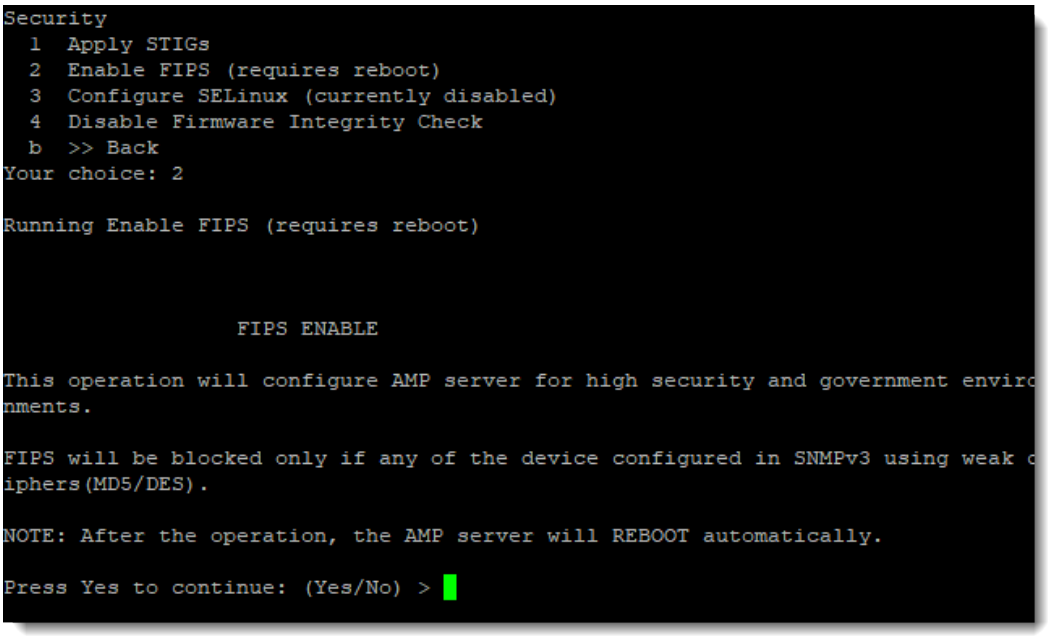
1. Use SSH to connect to the AirWave server and log with the user name (*ampadmin*) and password (*password for ampadmin*). If you changed the ampadmin user name and password, enter the current admin name and password.
2. At the CLI prompt, enter **7** to open the **Security** menu.



3. Enter **1** to run the STIG scripts.



4. Enter **2** to enable FIPS 140-2 approved mode.



The AirWave server reboots automatically after it turns on FIPS mode. After the reboot, the AirWave WebUI takes five to 10 minutes to update with the changes. The system will be ready for testing when it's back online.

Step 2: Enable Security Enhanced Linux (SELinux)

To enable SELinux for more access control of security policies:

1. Log in to the CLI as the admin user, then enter **7** to open the **Security** menu, then enter **3** to enable SELinux.

```
Security
  1  Apply STIGs
  2  Enable FIPS (requires reboot)
  3  Configure SELinux (currently disabled)
  4  Disable Firmware Integrity Check
  b  >> Back
Your choice: 3
```

2. Enter **3** to enforce.

Step 3: Configure External Logging

In order for AirWave to send audit and system events to external syslog servers, you must enable the "Include Event Log Messages" and "Include Audit Log Messages" options.

NOTE

In the event of a system failure, no particular information needs to be retained in order for AirWave to come back online.

To configure external logging:

1. Navigate to **AMP Setup > General**, then click **External Logging**.

Figure 1: *External Logging Settings*

2. In the **Include Event Log Messages** option, click **Yes**, then enter the IP address and port number for up to four syslog servers.
3. In the **Include Audit Log Messages** option, click **Yes**, then select the audit facility. By default, the event and audit log facility identifiers are set to **local1**.
4. Click **Save** at the bottom of the page.

Step 4: Disable Configuration Auditing

AirWave runs the `encrypt disable` command when auditing the configuration of an Aruba controller. Disable configuration auditing if you're not planning to do any config pushes, or use management mode. You can also disable configuration auditing to stop sending controller "encrypt disable" messages to existing groups with controllers, or all groups.

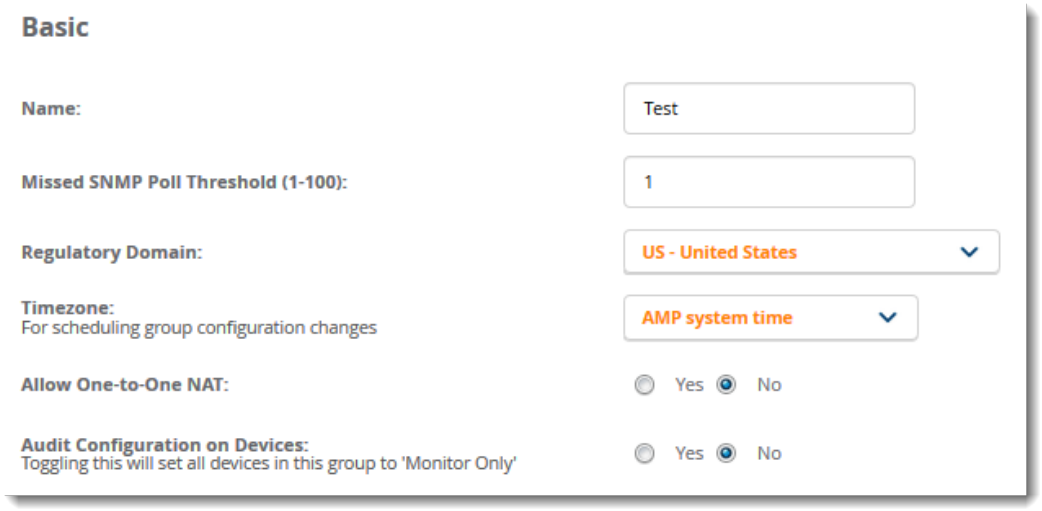
NOTE

For new groups, perform this step before you add controllers to the group.

To disable configuration auditing:

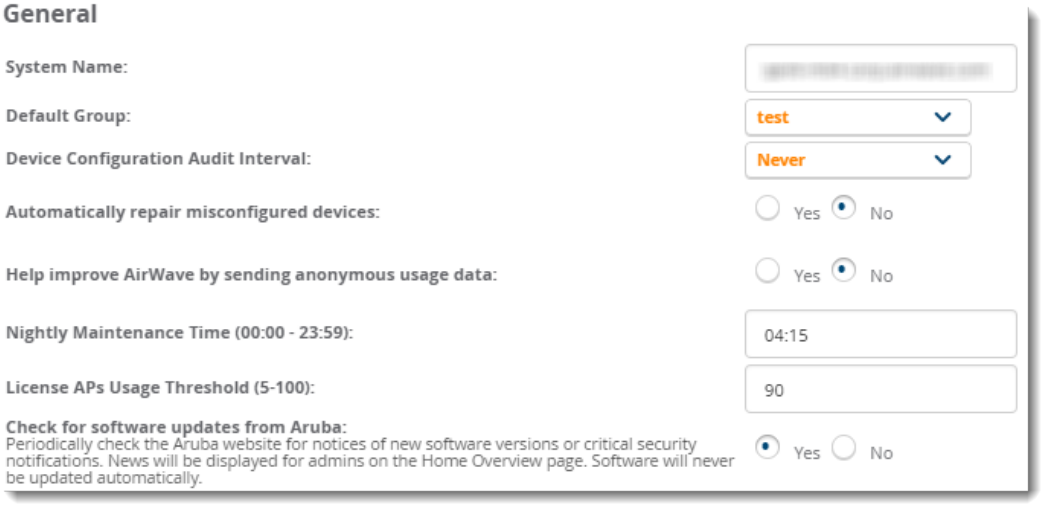
1. Navigate to **Groups**, then select a group of devices. Or, click **Add** to create a group.
2. Click **Basic** from the navigation sidebar.
3. Change the **Audit Configuration on Devices** option to **No**.

Figure 2: *Disabling Configuration Auditing*



4. Click **Save** and **Apply**. Confirm the changes, or you can apply this setting to other groups if you select multiple groups, then click **Apply Changes Now**.
5. Navigate to **AMP Setup > General**.
6. Change the **Device Configuration Audit Interval** option to **Never**.

Figure 3: *Setting the Device Configuration Audit Interval to Never*



7. Click **Save**.

Step 5: Create User Roles

Create a new role in order for an external authentication server to authenticate user logins. Roles define which folders, and devices grouped by folders, users can see and which operations they can perform. For example, users with the admin role can view logs.

NOTE

When you enable external authentication, the authentication server determines which role is assigned to the user.

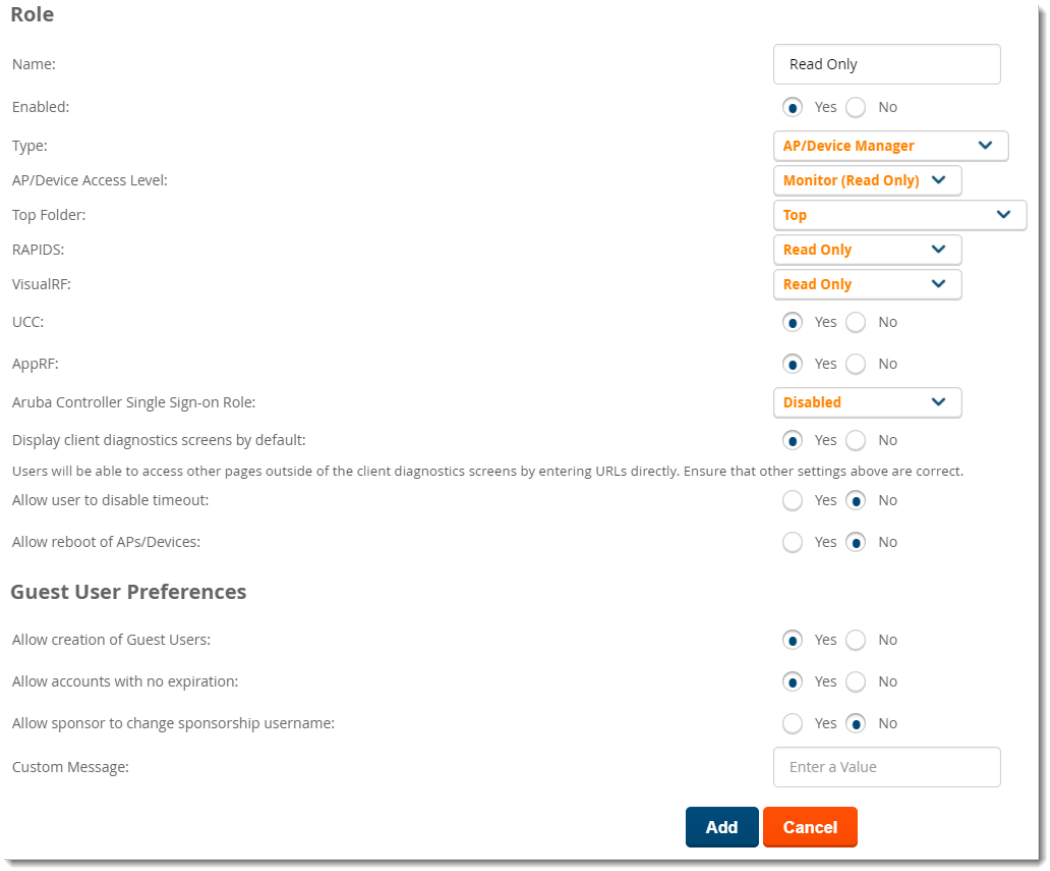
Example: Read-Only Role

To create a user role with read-only permissions:

1. Go to the **AMP Setup** > **Roles** and click **Add**.
2. Enter a name for the user role, then set the following options:
   - Type: AP/Device Manager
   - AP/Device Access Level: Monitor (Read Only)
   - Top Folder: Top
   - Aruba Controller Single Sign-on Role: Disabled

Figure 4 shows a role named Read Only being created.

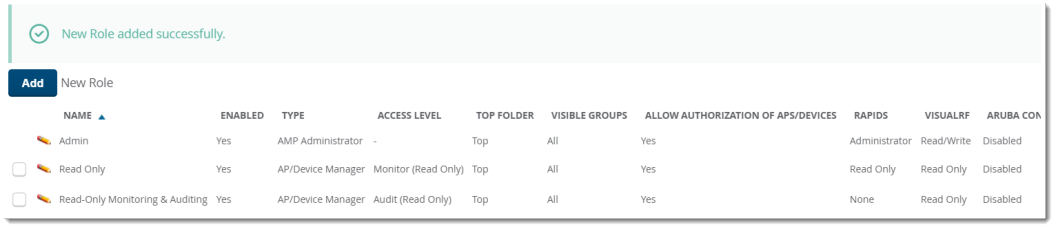
Figure 4: *Adding a Role called Read Only*



3. Click **Add**. You will be prompted to re-enter your password.
4. Enter the admin password.
5. Click **Add** again.

Figure 5 shows the newly created role named Read Only in the Roles table.

Figure 5: *Newly Created Read Only Role*



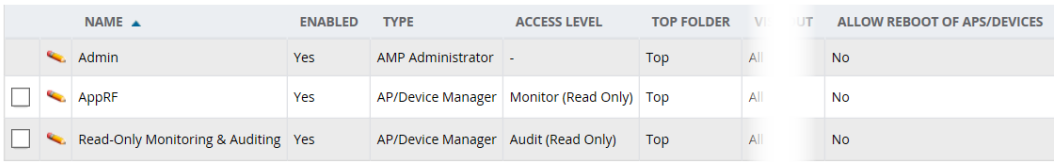
Example: Read-Write Role for a Device Manager

To create a user role with read or write permissions for a device manager:

1. Go to the **AMP Setup** > **Roles** and click **Add**. You will be prompted to re-enter your password.
2. Enter a name for the user role, then set the following options:
   - Type: **AP/Device Manager**
   - AP/Device Access Level: **Manage (Read/Write)**
   - Select permission levels for RAPIDS and VisualRF
   - (Optional) Enable roles for UCC and AppRF.
   - Top Folder: **Top**
   - Aruba Controller Single Sign-on Role: **read-only** or **root**.

Figure 6 shows the newly created role named AppRF in the Roles table. The user with this role will have read-write access in AppRF at the top folder.

Figure 6: *Newly Created Read-Write Role for an AP/Device Manager*



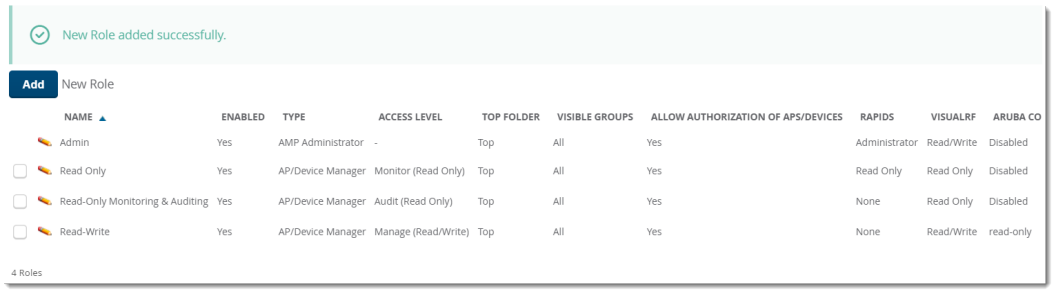
Example: Read-Write Role for an AMP Admin

To create a user role with read-write permissions for the AMP admin:

1. Go to the **AMP Setup** > **Roles** and click **Add**. You will be prompted to re-enter your password.
2. Enter a name for the user role, then set the following options:
   - Type: **AMP Administrator**
   - Aruba Controller Single Sign-on Role: **root**

Figure 7 shows the newly created role called Admin in the Roles table. The user with this role will have admin access and the ability define additional users, limit device access, and limit WebUI views.

Figure 7: *Newly Created Read-Write Role for an AMP Admin*



Step 6: Configure Remote Authentication

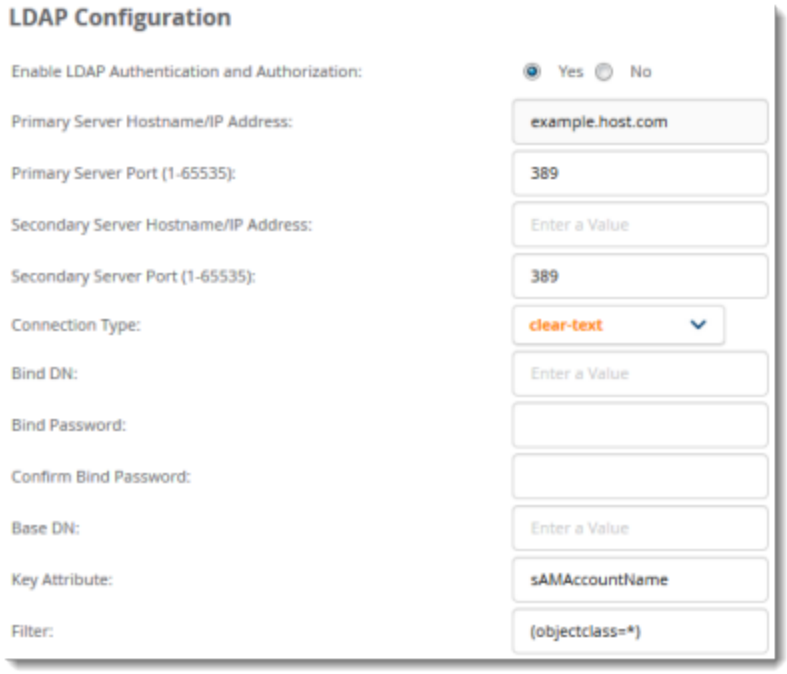
LDAP (Lightweight Directory Access Protocol) provides users with a way of accessing and maintaining distributed directory information services over a network. When LDAP is enabled, a client can begin a session by authenticating against an LDAP server which by default is on TCP port 389.

For additional authentication reference information, see Reference Information on page 35.

To configure LDAP authentication:

1. Navigate to **AMP Setup > Authentication**.
2. Click **Yes** to enable LDAP authentication and authorization, then enter the following information:
   - **Primary Server Hostname/IP Address**. The hostname or IP address of the Primary LDAP server.
   - **Primary Server Port (1-65535)**. The TCP port of the primary LDAP server.
   - **Connection Type**. Send LDAP authentication messages in clear text using the **cleartext** option, or send messages securely using the **ldap-s** or **start-tls** options.
   - **Verify Server Certificate**. When you select **ldap-s** or **start-tls** options, you can require that the server certificate be verified.
   - **Bind DN**. The full distinguished name (DN) of the node in your directory tree which is the starting point for record searches.
   - **Bind Password and Confirm Bind Password**. The Active Directory password for the account that can search for users.
   - **Base DN**. The common name (CN) of an LDAP user account. This user must have privileges to search for users and is usually the administrator.
   - **Key Attribute**. The attribute to use as a key when searching for the LDAP server. The default, for Active Directory, is **sAMAccountName**.
   - **Filter**. The filter applied when searching for a user in the LDAP database.

Figure 8: *Example LDAP Configuration*



3. Click **Save**.

Step 7: Configure Two-Factor Authentication

On the **AMP Setup > Authentication** page, you can specify whether to use two-factor authentication. With two-factor authentication, the AMP user name and password and a PEM-encoded certificate bundle is required. When using the Smart Card or token, AirWave will prompt you to enter the PIN.

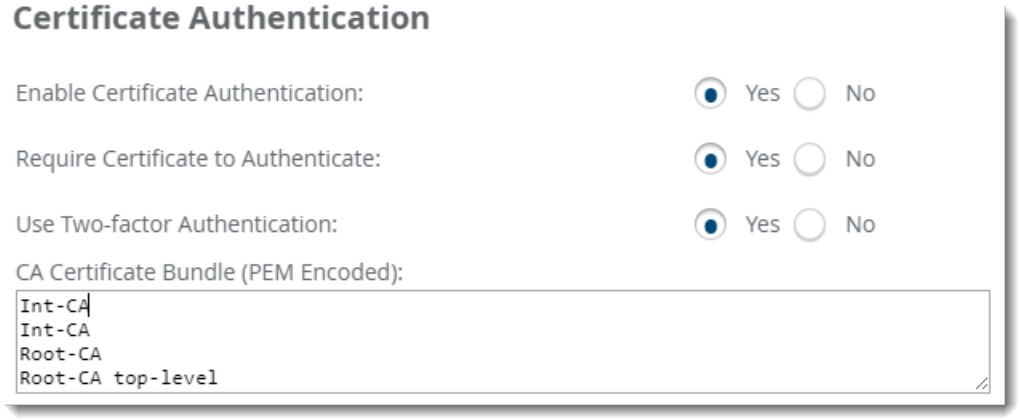
NOTE

When entering the PEM bundle, you must install every member in the certificate chain provided by the SSL vendor in order for smart card or token authentication to work.

To configure two-factor authentication:

1. Go to **AMP Setup > Authentication**.
2. Select **Yes** to enable certificate authentication. Once enabled, certificate authentication options will display.
3. Select **Yes** to turn on the **Use Two-factor Authentication** option.
4. Enter your PEM certificate bundle in the text field. For example, in Figure 9, two intermediate certificates are bundled with the two root certificates, one being at the top of the chain.

Figure 9: *Two-Factor Authentication Configuration Example*



5. Scroll to the bottom of the page, then click **Save**.

Step 8: Configure OCSP

AirWave supports Online Certificate Status Protocol (OCSP) validation of client certificates. OCSP maintains server security by replacing the need for intermediate certificate validation.

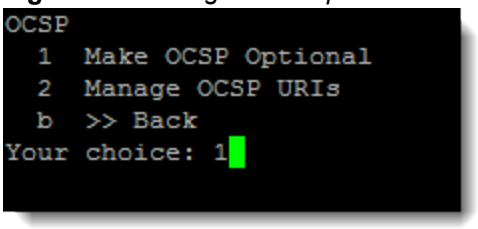
NOTE

AirWave obtains the OCSP server URL used for validation from the smart card or certificate.

To configure OCSP:

1. Upload OCSP certificates into AirWave by going to **Device Setup > Certificates** in the WebUI.
2. Click **Add**, then click **Save**. Ensure you use the correct OCSP label to distinguish the responder certificate from the signing certificate.
3. Enable certificate authentication under **AMP Setup > Authentication**, then select **Yes** for the **Enable Certificate Authentication** option.
4. Log in to the AMP CLI session, and enter **3-4-6** to open the **Configuration > Certificates > OCSP** menu.

Figure 10: *Making OCSP Optional*



5. Enter **2** to manage OCSP URIs, then enter **a** to add OCSP URIs.

Step 9: Configure a Certificate Revocation List (CRL)

When you configure a CRL, AirWave checks to see if the certificate sent by the requesting device is revoked. You could also use a CRL to skip the OCSP check when an OCSP server is not accessible to perform certificate validation.

To configure the CRL:

1. Log in to the CLI as the admin user, then enter **3-4-7** to open the **Configuration > Certificates > CRL** menus.

Figure 11: *Opening the CRL Menu*

```
Certificates
  1  Add SSL Certificate
  2  Generate Certificate Signing Request
  3  Install Signed Certificate
  4  Regenerate Self-Signed Certificate
  5  Add DTLS Certificates
  6  OCSP >
  7  CRL >
  b  >> Back
Your choice: 7
```

2. Enter **1** to make CRL required, then follow the prompts to run the function and return to the **CRL** menu.
3. Enter **2** to configure a CRL distribution URL, then follow the prompt to add the CRL distribution URL.
4. Enter **3** to add a CRL files and follow the prompt to add the file.
5. Enter the password for the AMP server.
6. Click **Update** to save the configuration.

Step 10: Delete the Default Admin User and Roles

After you have configured user authentication, delete the default admin user and roles that were installed with AirWave for initial authentication, login, and access privileges.

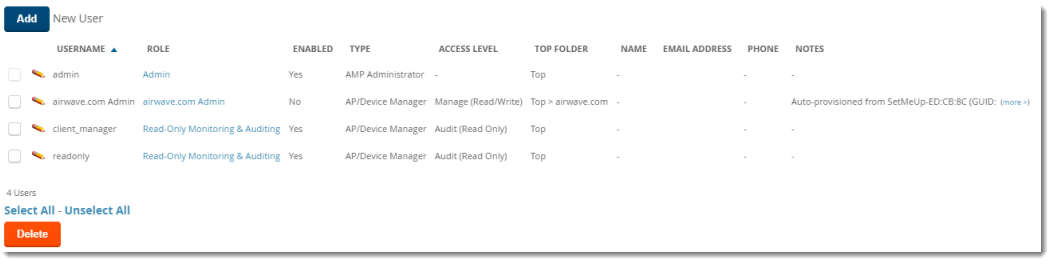
NOTE

For emergency access reasons, it's a good idea to create a new admin user and assign the AMP Admin role to this user. This user will have access with admin capability if the external authentication source fails. "Example: Read-Write Role for an AMP Admin" on page 12.

To delete the default admin user and roles:

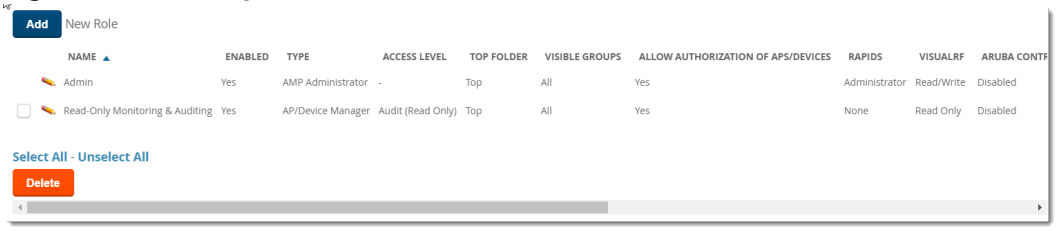
1. Log in as the RADIUS admin user, then go to **AMP Setup > Users**.
2. Select the user.

Figure 12: *Users Page*



3. Click **Delete**.
4. Navigate to **AMP Setup > Roles**.
5. Select the Admin role, then click **Delete**. Repeat this step for the Read Only role.

Figure 13: *Roles Page*



Step 11: Configure the Click Through Agreement

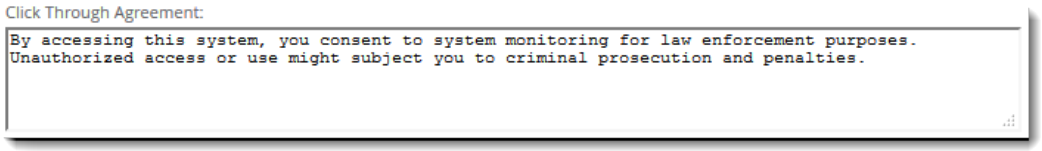
If you configure a click through agreement, the user sees this message before logging into AirWave.

To configure the click through agreement:

1. Navigate to **AMP Setup > Authentication > Login Configuration**.
2. In the Click Through Agreement field, type a message that the user must accept in order to access the system. In general, the click through agreement should explain terms of access, authorization, privacy, and consent.

   Figure 14 shows an example of a click-through agreement.

Figure 14: *Example Click Through Agreement*



3. Click **Save** at the bottom of the page.

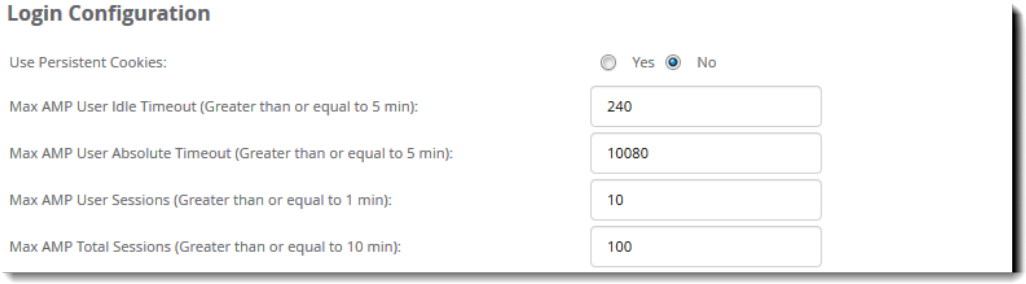
Step 12: Configure the Idle Timeout

When the user session times out, AirWave records session timeout events in the AirWave event log.

Follow these steps to configure the idle timeout:

1. Navigate to **AMP Setup > Authentication > Login Configuration**.
2. Enter 600 seconds (10 minutes) or less. The default is 240 seconds (4 minutes).

Figure 15: *Default Settings for the Login Configuration Page*



3. Click **Save** at the bottom of the page.

Step 13: Configure an Absolute Timeout

You can avoid a security risk created when a user leaves a session open by closing the session after an absolute period of time. In doing so, you force the user to re-authenticate in order to ensure the session is still active.

Follow these steps to configure an absolute timeout:

1. Navigate to **AMP Setup > Authentication > Login Configuration** (see Figure 15).
2. Enter 20 minutes or less. The default is 10080 minutes (7 days).
3. Click **Save** at the bottom of the page.

Step 14: Configure Session Limits

Limit the number of users and concurrent sessions per user to prevent risks associated with denial of service attacks by entering a non-zero value.

To configure session limits:

1. Navigate to **AMP Setup > Authentication > User Sessions** (see Figure 15).
2. Enter how many user sessions and total session settings are allowed. The default for both is 0.
3. Click **Save** at the bottom of the page.

Step 15: Configure the Whitelist

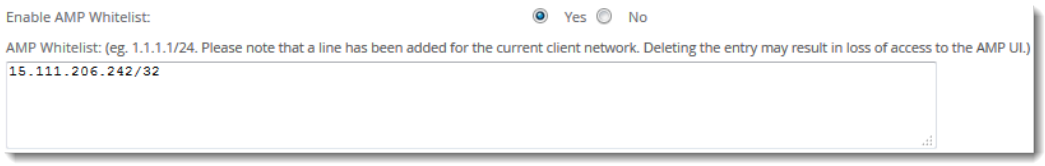
By adding subnets to a whitelist, you can limit AirWave access to users on a list of trusted subnets.

Do not delete the current client network from the AirWave whitelist, or you might lose access to the AirWave WebUI.

To configure the whitelist:

1. Navigate to AMP Setup > Authentication.
2. In the Login Configuration section, select **Yes** for the **Enable AMP Whitelist** option. When you enable this functionality, AirWave displays the whitelist with the current client network as the first entry.

Figure 16: *Enabling the AMP Whitelist*



3. To enter additional subnets, add the additional subnets on the same line, separated by commas. (For example, 192.168.0.13/32,172.16.0.0/24)
4. Click **Save** at the bottom of the page.

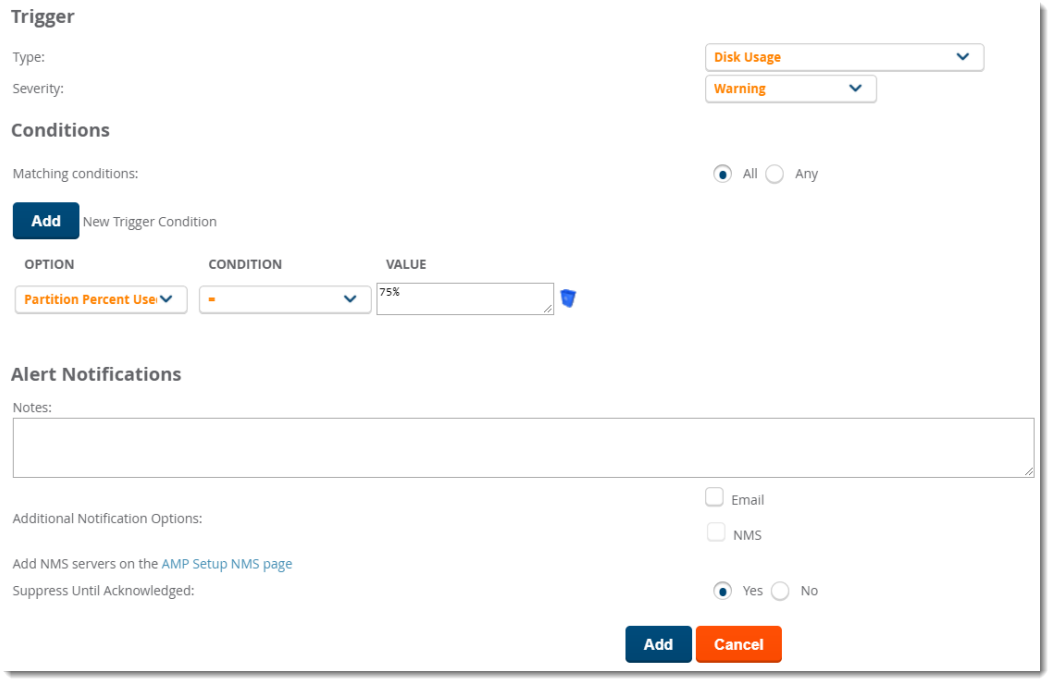
Step 16: Create a Disk Usage Trigger

You can create a disk usage trigger to generate an alert when the AMP server is running out of storage. You can send an alert to an email address, or, if you use an NMS tool, to an NMS server.

Follow these steps to add the trigger:

1. Navigate to **System > Triggers**, then click **Add**.
2. Select **Disk Usage** for the type of trigger.
3. Select **Warning** for the severity level.
4. Click **Add**, then add a match condition. In order to comply with several STIG requirements, create a trigger when the disk space used is greater than or equal to 75%, as shown in Figure 17.

Figure 17: *Adding a Condition for a Disk Usage Trigger*



5. If you want to configure alert notifications, including the note that will be included with the alert, select the notification options.
6. Click **Add** to save the trigger.

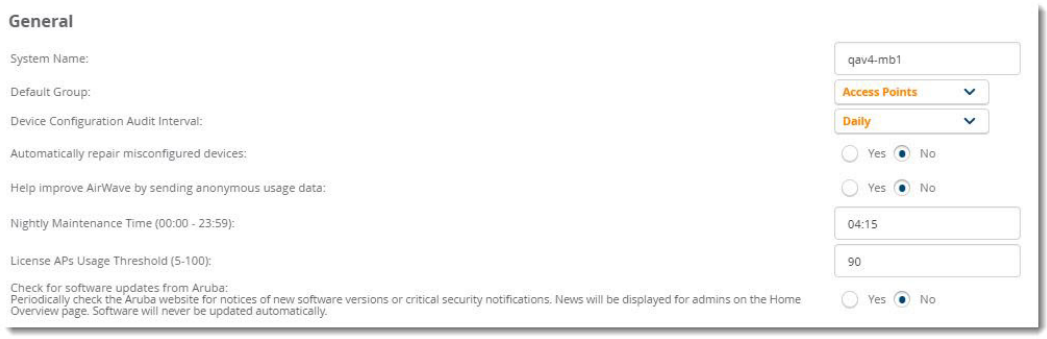
Step 17: Disable the Update Checker

By default, AirWave automatically checks for software updates, device template files, important security updates, and important news.

To disable the update checker:

1. Navigate to **AMP Setup > General**, then find the **Check for software updates from Aruba** option under the **General** section.
2. Click **No**.

Figure 18: *Disabling Software Updates*



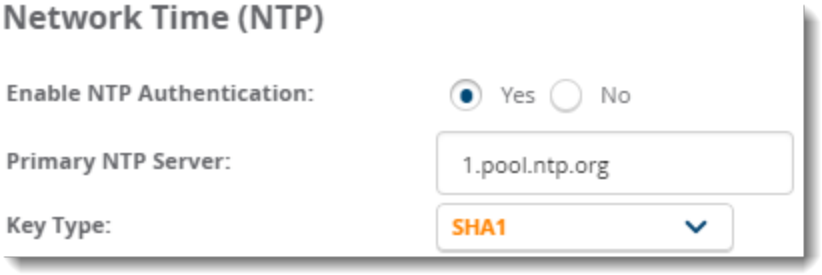
Step 18: Configure Secure NTP and DNS with Redundancy

NTP servers synchronize the time on the AirWave server. You can enable secure NTP authentication using SHA1 hashing from the WebUI.

Follow these instructions to configure the NTP servers:

1. Go to **AMP Setup > Network**, locate the Network Time (NTP) section.
2. To enable NTP authentication, select **Yes**.
3. Enter the primary NTP server host name.
4. Select the SHA1 key type from the drop-down menu.

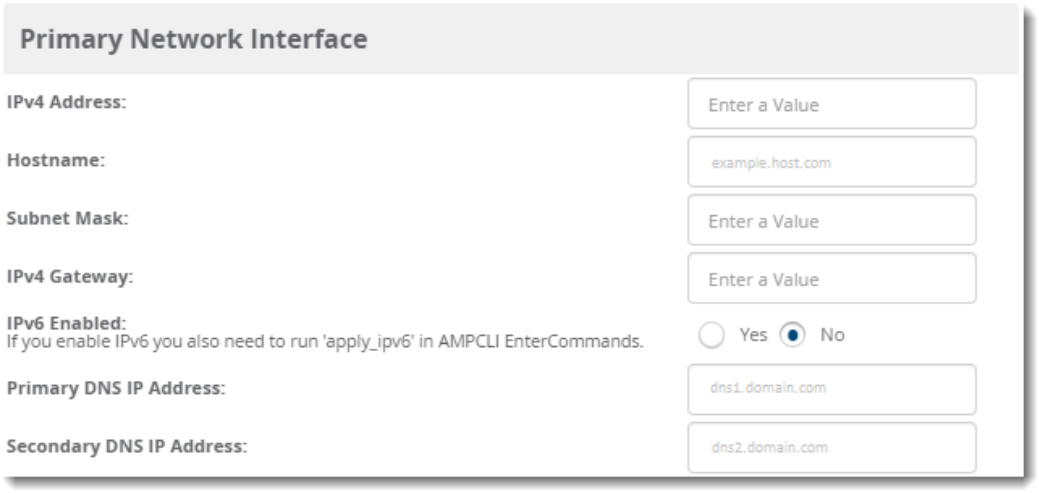
Figure 19: *Network NTP Server Settings*



5. Click **Save** at the bottom of the page.

For AMP servers running Red Hat Enterprise Linux (RHEL) using DNS resolution, you must configure at least two name servers when you install AirWave. You can configure this on the **AMP Setup > Network** page in the Primary Network Interface section (see the example in Figure 20), or from the AMP CLI by selecting **3-1** to access the **Configure Network Settings** menu.

Figure 20: *Configuring the DNS Name Server*



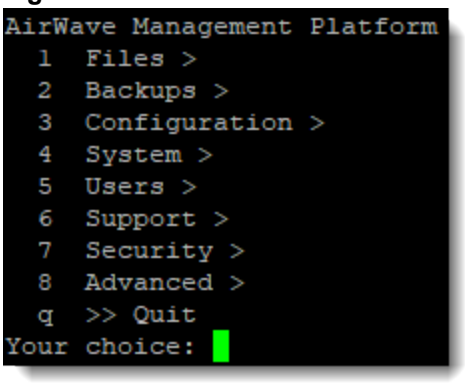
Step 19: Configure Automated Backup Transfer

AirWave creates nightly archives of all relational data, statistical data, and log files. You can configure the secure network file transfer through the AMP CLI to a backup destination that runs an SCP server service.

To configure automated backup transfer:

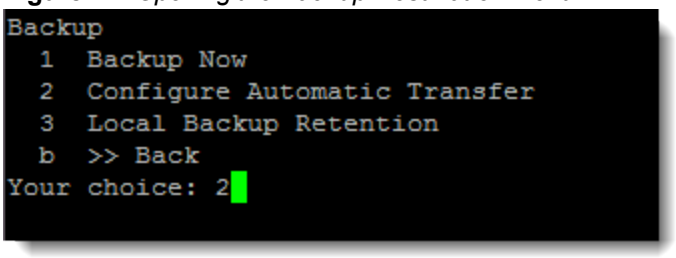
1. Log in to the AMP CLI as the ampadmin user. If you subsequently changed the ampadmin user name and password, enter the current admin name and password.
2. At the prompt, type **Y** to accept the terms of usage and press **Enter**. The CLI menu appears, as shown in Figure 21.

Figure 21: *CLI Menu*



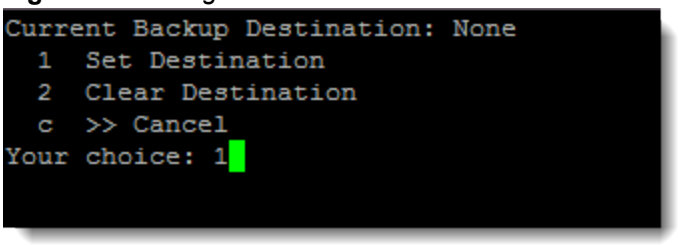
3. Enter **4** to open the **Backup** menu, then enter **2** to select **Configure Automatic Transfer**.

Figure 22: *Opening the Backup Destination Menu*



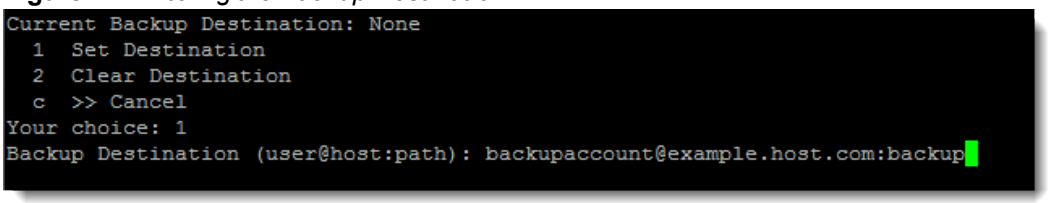
4. Enter **1** to select **Set Destination**.

Figure 23: *Setting the Destination*



5. Type a directory path where the file output will be saved (for example, user@servername:destination), then press **Enter**.

Figure 24: *Entering the Backup Destination*



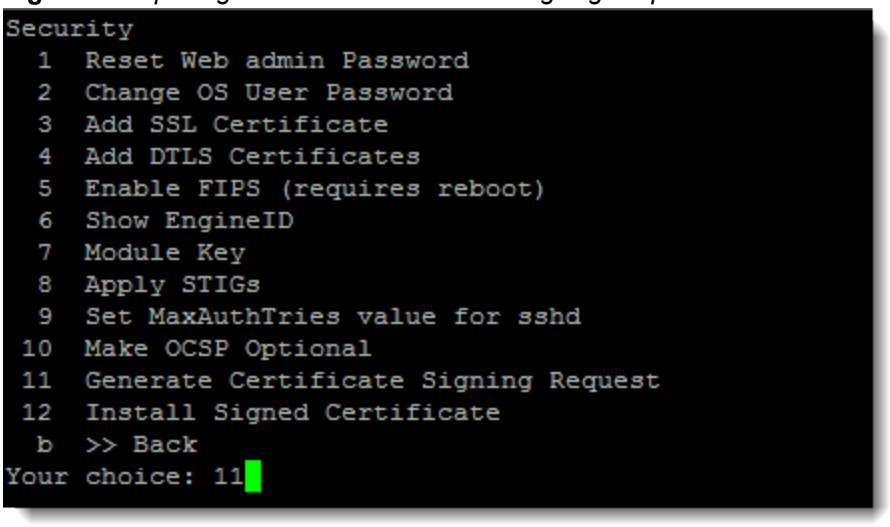
Step 20: Generate a Certificate Signing Request (CSR)

You can use the AMP CLI to request a certificate from AirWave.

To generate the CSR:

1. From the AMP CLI, enter **3-4-2** to open the **Configuration > Certificates > Generate Certificate Signing Request** menu.

Figure 25: *Opening the Generate Certificate Signing Request Menu*



2. Follow the prompt to enter the data associated with the organization:
   a. 2-letter country code
   b. State or province
   c. Locality or city
   d. Organization or company
   e. Organization unit or department
   f. Common name or server host name
   g. Email address
   h. Fully qualified DNS name
   i. IP addresses

Figure 26: *Entering the Certificate Data*

3. Enter **a** to accept the changes and save the data.

Step 21: Installing the Signed Certificate

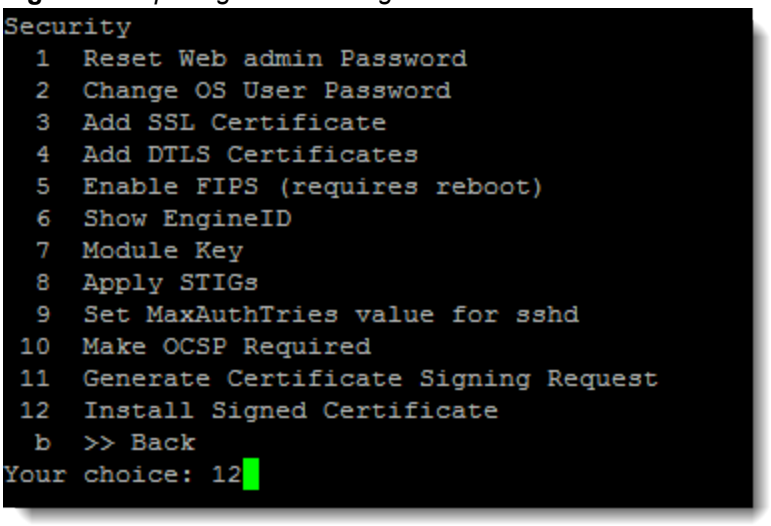
Before you install the signed certificate, you must export the CSR created in "Step 20: Generate a Certificate Signing Request (CSR)" on page 21 to a third-party certificate authority (CA) and then upload the returned

certificate to the AirWave server.

To install the signed certificate:

1. From the AMP CLI, enter **3-4-3** to open the **Configuration > Certificates > Install Signed Certificate** menu.

Figure 27: *Opening the Install Signed Certificate Menu*



2. Follow the prompt to select the certificate, then press **Enter**. The signed certificate should be PFX-encoded with a *.crt file extension.

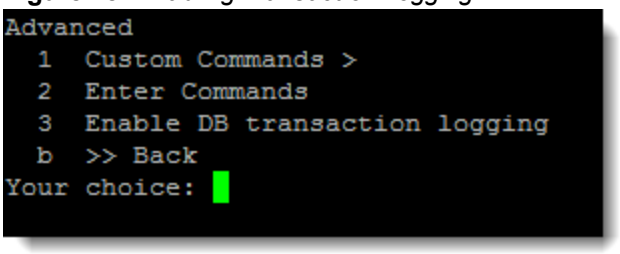
Step 22: Configure Transaction Logging

Transaction logs contain a sequential record of all changes to the database and can be helping in debugging and maintaining application availability. After you install AirWave 8.2.10, transaction logging is available, and must remain enabled.

This option is only available when you have applied STIGs (refer to "Step 1: Harden the System" on page 7).

To enable transaction logging, from the AMP CLI, enter **8** to open the Advanced menu, then enter **3** to **Enable DB transaction logging**.

Figure 28: *Enabling Transaction Logging*



Regular backups are essential to ensure continuous data operation after data loss or system failure.

Back up Your Data

AirWave automatically backs up log files, relational data, historical data, system files, statistical data, and AirWave settings at the nightly maintenance time. The default is 4:15 am.

Follow these steps to change the backup schedule, or do a manual backup:

- **Automatic**. Log in to the WebUI as the admin user, the navigate to **AMP Setup > General** and change the "Nightly Maintenance Time" option.
- **On-Demand**. Log in to the AMP CLI as the admin user, then select **2-1-1** to run the backup now. Follow the onscreen instructions to create the backup. AirWave doesn't automatically transfer on-demand backups.

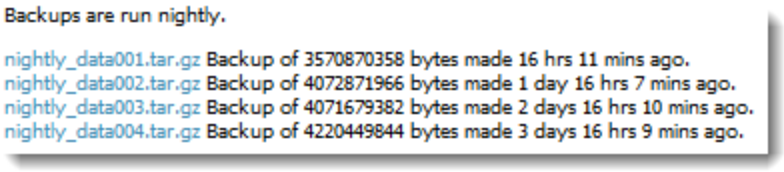
Download the Backup

You should regularly save the data backup file to another machine or media. AirWave saves the backup as **nightly_data00[1-4].tar.gz** and keeps the last four archives.

To download the backup file:

1. Find the backup files by navigating to **System > Backups**.

Figure 29: *Example of Nightly Backups*



2. Click the backup file, then click **Save File**.

Upload the Backup

You need a file transfer utility like SCP for Unix, or Bitvise for Windows, to perform this procedure.

To upload the backup file:

1. Log in to the AMP CLI as the admin user, then select **1-1** to upload the backup file to the AMP server you're currently logged in to using SCP for Unix.
2. Follow the onscreen instructions to enter the file path.

   For example:

   `username@<ipaddress>:nightly_data001.tar.gz`
3. Enter the password for the AMP server.

Restore from a Backup

In order to restore the AirWave data, you only need the most recent backup file that you uploaded on to the new AMP server.

Ensure that the new AirWave server has the same IP address, name, and software version as the AMP server that created the backup file,.

To restore a backup:

1. Log in to the CLI as the admin user, then select **2-2** to restore the AMP server from an on-demand, nightly, or imported backup file.
2. Follow the onscreen instructions to select the backup file you want to restore. This process will take several minutes to complete, and you can get started using the WebUI after a few more minutes.

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 7.

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 33.

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

- "About the Failover Server" on page 26
- "Test the Failover Configuration" on page 27
- "Failover Monitoring" on page 30

About the Failover Server

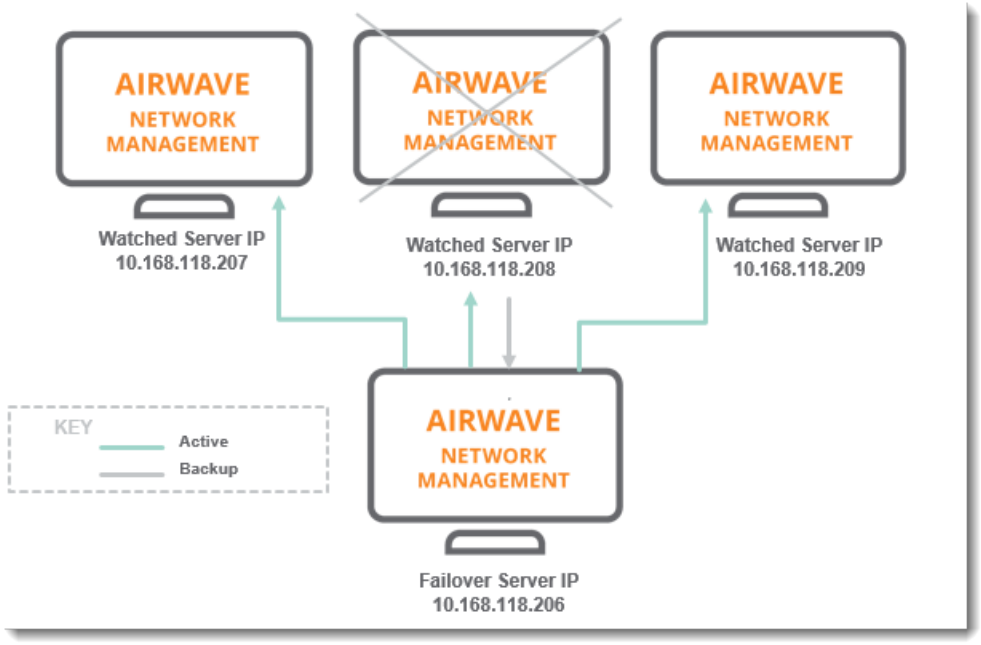
The failover server communicates with the watched AirWave servers using SSH, SNMP, and AMON over port 443.

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 30 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 30: *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 27
- "Testing the Failover" on page 28
- "Testing the Failback" on page 28

Adding a Watched AirWave Server

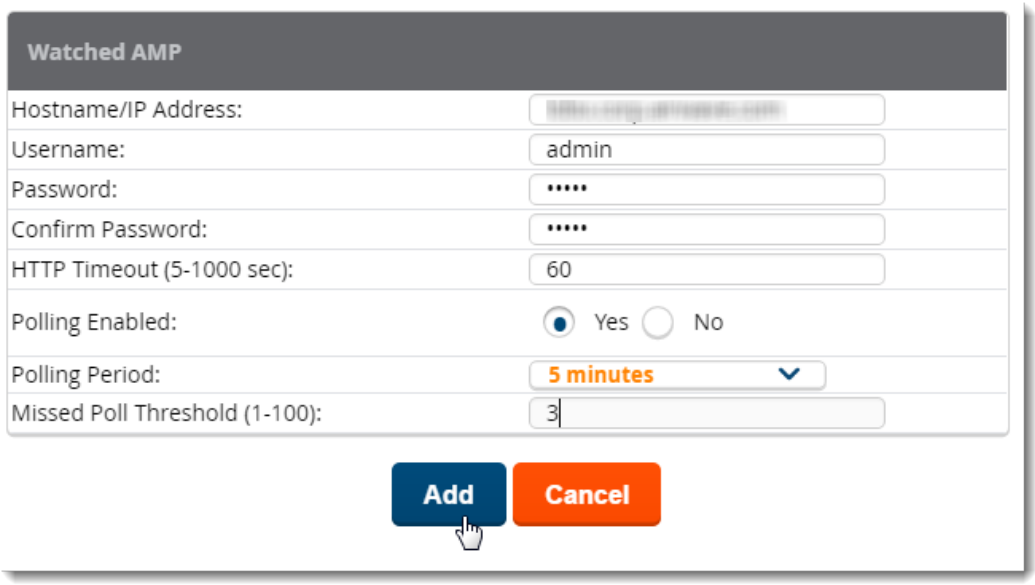
When you add an AirWave server to the watched list, the failover server begins polling the watched AirWave server and downloads the nightly backup. It is this backup that gets restored on the failover server when it takes over for the watched AirWave server.

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:

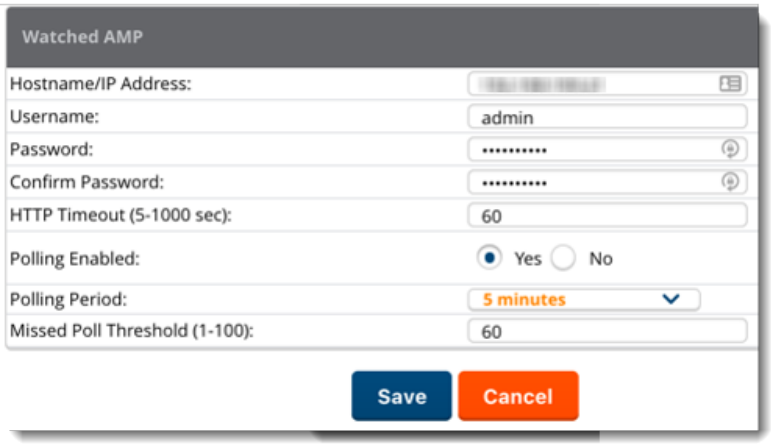
1. Navigate to **Home > Overview > Watched AMPs**, then click **Add**.
2. Enter the AirWave server's hostname or IP address.
3. Enter the name used for logging in to the AirWave server.
4. Enter the password (alphanumeric without spaces) for the user being created, then confirm the password.
5. Enter how many polls are missed before the failover AMP triggers a failover event. By entering 3, as shown in Figure 31, the failover server will trigger a failover event after 3 missed polls during 5-minute polling intervals.

Figure 31: *Adding a Watched AirWave Server*



6. Click **Add**. The AirWave server you added displays in the Watched AMPs table, as shown in Figure 32.

Figure 32: *Watched AMPs*



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.

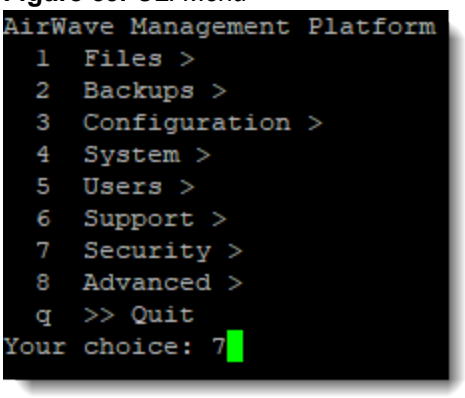
- "Restoring from a Backup" on page 29
- "Reinstating the Failover Server" on page 30

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:

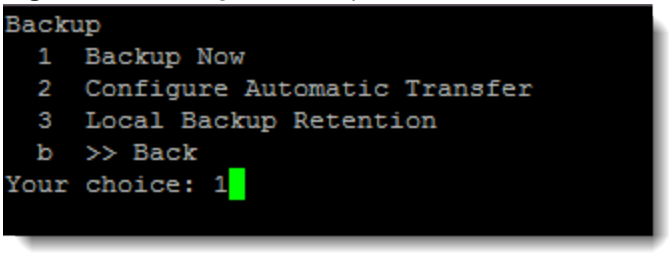
1. Restart the watched AirWave server online.
2. Log in to the CLI on the failover server as the admin user. The following CLI menu appears:

Figure 33: *CLI Menu*



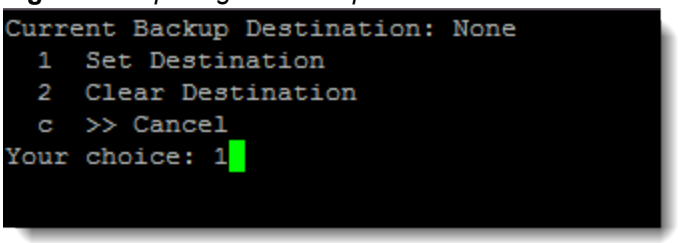
3. Run the on-demand backup:
   a. Select **2** to open the Backup menu and press **Enter**.
   b. Select **1-1** to start the on-demand backup and press **Enter**.

Figure 34: *Running the Backup*



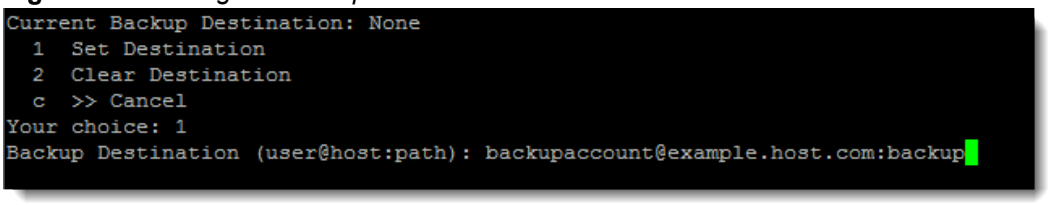
4. Configure the backup file transfer from the AirWave server to an external location:
   a. Select **2** to open the Backup menu and press **Enter**.
   b. Select **2-1** to configure the automatic transfer and set the backup destination. Press **Enter**.

Figure 35: *Opening the Backup Destination Menu*



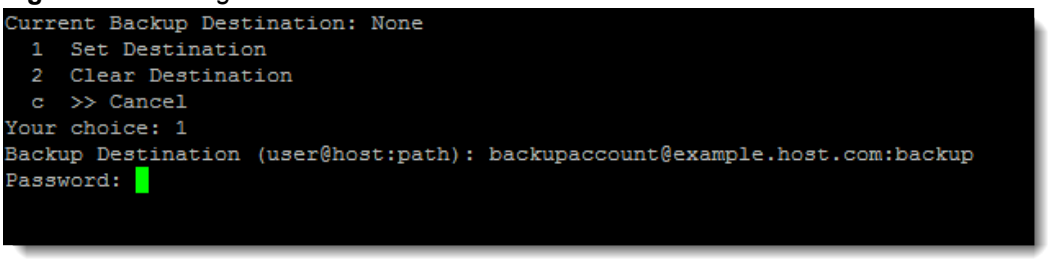
   c. At the prompt, type the path of backup destination and press **Enter**.

Figure 36: *Entering the Backup Destination*



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

Figure 37: *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 27.
- 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 31.
- Manage your AirWave licenses. For more information, see "Adding the Failover License" on page 1 For more information, see "Before You Begin" on page 1.
- Update your user information. For information about changing the settings on the **Home > User Info** page, refer to the *AirWave 8.2.11.0 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 31.
- 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 30.

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 38).

Figure 38: *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.

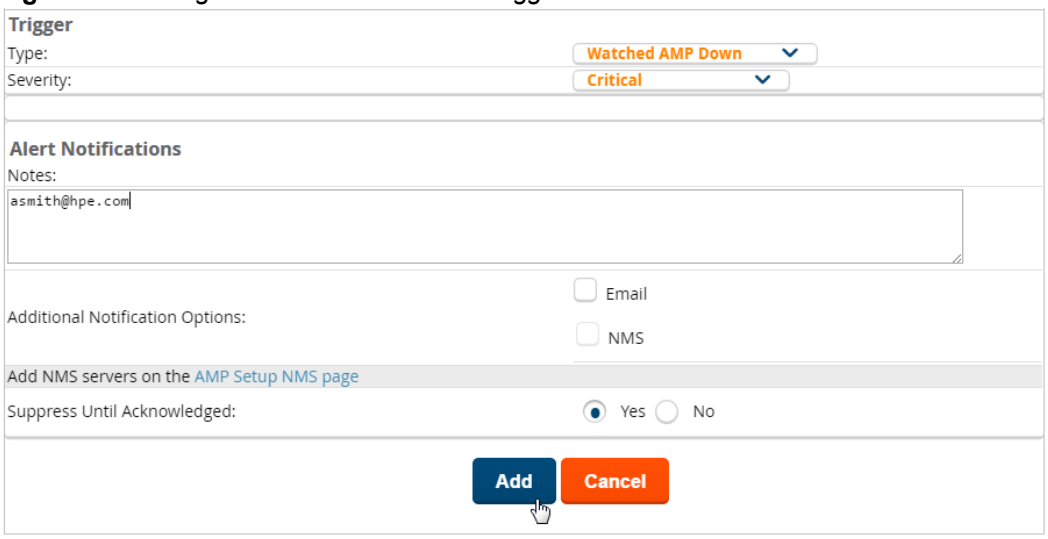
Watched AMP Down Trigger

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 39: *Adding a Watched AMP Down Trigger*



The Watched AMP Down trigger displays in the Triggers table, as shown in Figure 40.

Figure 40: *Watched AMP Down Trigger*

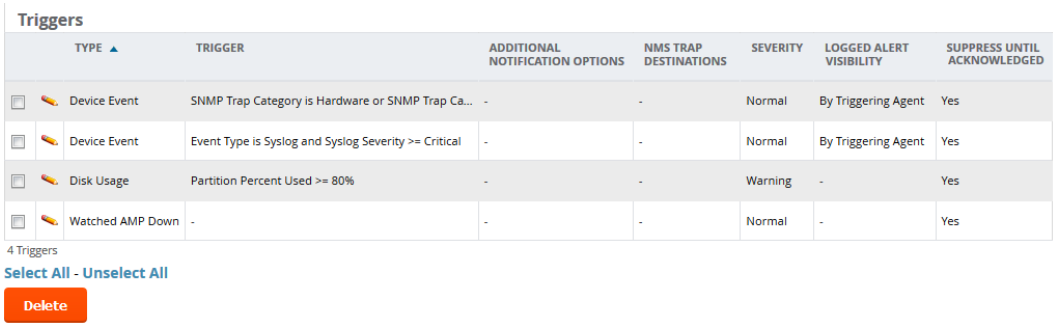


Figure 41: *Setting the SNMP Polling Period*

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

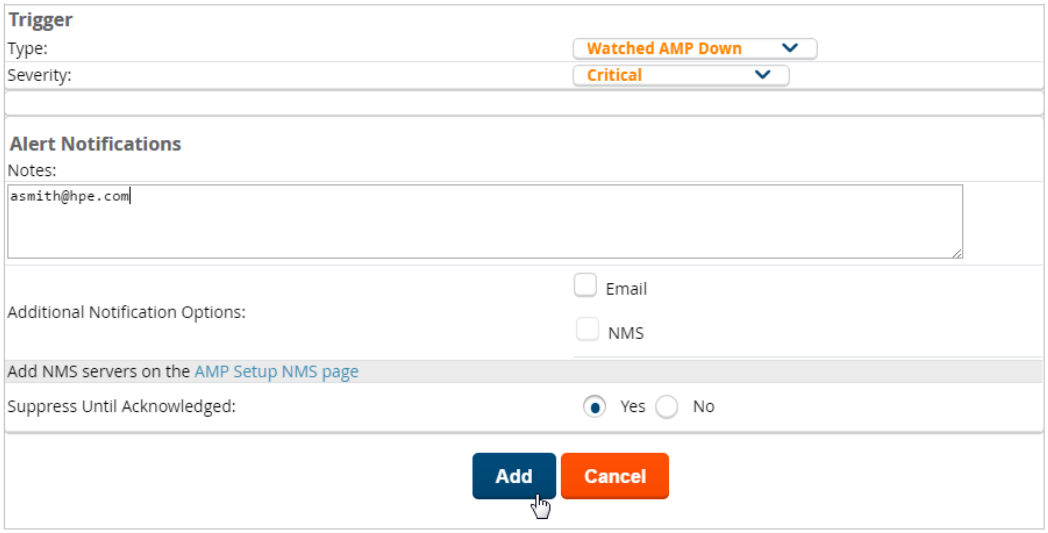
You can create a **Watched AMP Down** trigger to generate an alert when the failover server loses communication with the watched AirWave server. You can send an alert to an email address, or, if you use an NMS tool, to an NMS server.

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.

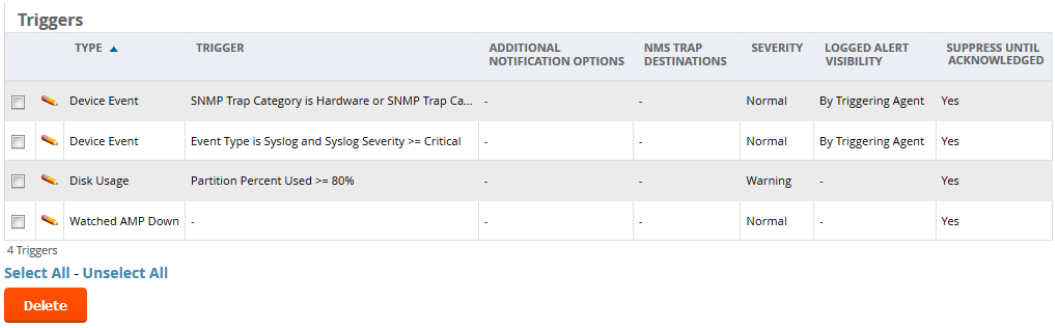
3. Enter a note to be included with the alert.
4. Select the delivery method. The information required depends on the delivery method you choose:
   - Email requires email addresses for the sender and recipient.
   - NMS requires at least one trap destination, which has been preconfigured on the **AMP 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 42: *Adding a Watched AMP Down Trigger*



The Watched AMP Down trigger displays in the Triggers table, as shown in Figure 40.

Figure 43: *Watched AMP Down Trigger*

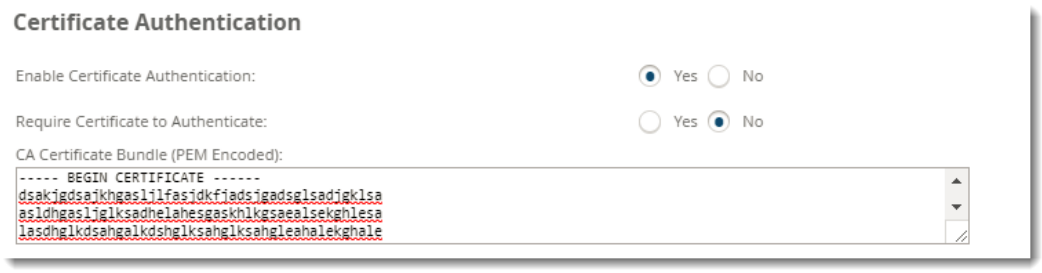


Disabling the Certificate Authentication Requirement

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**.

This appendix provides additional information that helps you to configure and use AirWave in the most secure manner, including:

- "Other Authentication Options" on page 35
- "ClearPass Policy Manager (CPPM) for AirWave" on page 36

Other Authentication Options

AirWave can use RADIUS, TACACS+ or LDAP servers to authenticate AirWave users. You can also configure RADIUS authentication using Clear Pass Policy Manager (CPPM) as the authentication server.

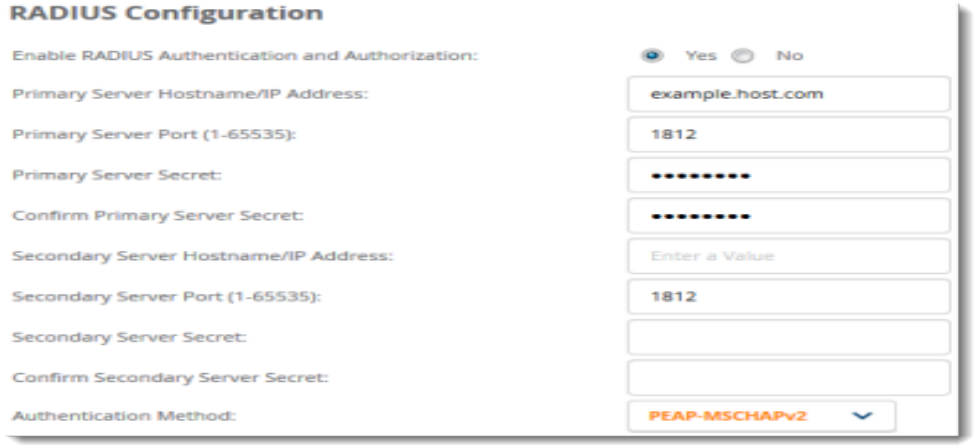
RADIUS Authentication and Authorization

Follow these steps to configure RADIUS authentication:

1. Navigate to **AMP Setup > Authentication**, then scroll down to the RADIUS Configuration section.
2. Click **Yes** to enable RADIUS authentication and authorization, and enter the following information for the primary RADIUS server:
   - Primary Server Hostname/IP Address. The hostname or IP address of the primary RADIUS server.
   - Primary Server Port (1-65535). The TCP port of the primary RADIUS server.
   - Primary Server Secret (and Confirm Primary Server Secret). The password used to access the primary RADIUS server.

   The secondary RADIUS server settings are optional.
3. Select either PAP or PEAP-MSCHAPv2 for the authentication method.

Figure 44: *Example RADIUS Configuration*



4. Click **Save**.

TACACS+ Authentication

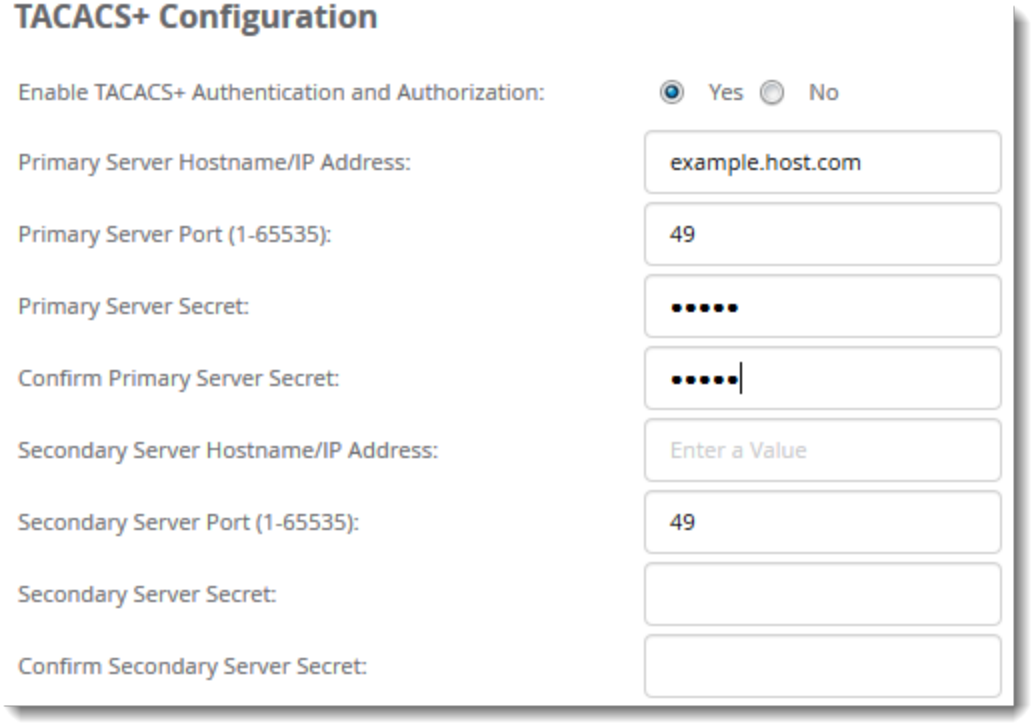
Follow these steps to configure TACACS+ authentication:

1. Navigate to **AMP Setup > Authentication**, then scroll down to the TACACS+ Configuration section.

2. Select **Yes** to enable TACACS+ authentication, and enter the following information for the primary TACACS+ server:
   - Primary Server Hostname/IP Address. The hostname or IP address of the primary TACACS+ server.
   - Primary Server Port (1-65535). The TCP port of the primary TACACS+ server.
   - Primary Server Secret (and Confirm Primary Server Secret). The password used to access the primary TACACS+ server.

   The secondary TACACS+ server settings are optional.

Figure 45: *Example TACACS+ Configuration*



3. Click **Save**.

ClearPass Policy Manager (CPPM) for AirWave

AirWave 8.2.8.2 provides improved security using two-factor authentication. You'll need a common access card (CAC) and a personal identity verification (PIV) card to log in to AirWave.

To use this feature, you must configure ClearPass Policy Manager (CPPM) for AirWave authorization as follows:

1. On the CPPM server, configure AirWave authentication on **Configuration > Services**.

Configuration » Services » Edit - Airwave Authorization

Services - Airwave Authorization

Summary | Service | Authorization | Roles | Enforcement

Service:

Name:	Airwave Authorization
Description:	AMP Authorization Service using RADIUS
Type:	RADIUS Authorization
Status:	Enabled
Monitor Mode:	Disabled
More Options:	Authorization

Service Rule

Match ANY of the following conditions:

	Type	Name	Operator	Value
1.	Connection	NAD-IP-Address	EQUALS	AMP Server IP Here

Authorization:

Strip Username Rules:	user:@
Authorization Details:	Active Directory -- LDAP over SSL [Active Directory]

Roles:

Role Mapping Policy:	Airwave Admin Role Mapping

Enforcement:

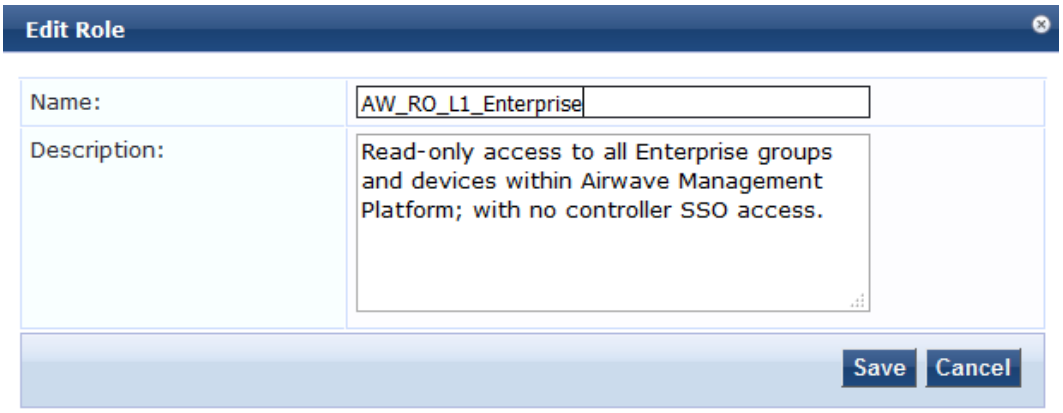
Use Cached Results:	Disabled
Enforcement Policy:	Airwave Login Enforcement Policy

Service Rule

Matches ◉ ANY or ○ ALL of the following conditions:

	Type	Name	Operator	Value
1.	Connection	NAD-IP-Address	BELONGS_TO_GROUP	Airwave Devices
2.	Click to add...			

2. Configure ClearPass User Roles



3. Configure ClearPass Role Mapping under **Configuration > Identity > Role Mappings** in ClearPass.

Configuration » Identity » Role Mappings » Edit - Airwave Admin Role Mapping

Role Mappings - Airwave Admin Role Mapping

Summary | Policy | Mapping Rules

Policy:

Policy Name:	Airwave Admin Role Mapping
Description:	Role Mapping for Airwave Users
Default Role:	No Access

Mapping Rules:

Rules Evaluation Algorithm: First applicable

	Conditions	Role Name
1.	(Authentication:Username EQUALS L2-Site-Username1) OR (Authentication:Username EQUALS L2-Site-Username2) OR (Authentication:Username EQUALS L2-Site-Username3)	AW_RW_L2_WASHINGTON
2.	(Authentication:Username EQUALS L1-Username1) OR (Authentication:Username EQUALS L1-Username2) OR (Authentication:Username EQUALS L1-Username3)	AW_RO_L1_Enterprise
3.	(Authentication:Username EQUALS L2-Username1) OR (Authentication:Username EQUALS L2-Username2) OR (Authentication:Username EQUALS L2-Username3)	AW_RW_L2_Enterprise
4.	(Authentication:Username EQUALS L3-Username1) OR (Authentication:Username EQUALS L3-Username2) OR (Authentication:Username EQUALS L3-Username3)	AW_RW_L3_Enterprise
5.	(Authentication:Username EQUALS L4-UserName1) OR (Authentication:Username EQUALS L4-UserName2) OR (Authentication:Username EQUALS L4-UserName3)	AW_RW_L4_Enterprise

4. Configure ClearPass Enforcement Policy under **Configuration > Enforcement > Policies**.

Configuration » Enforcement » Policies » Edit - Airwave Login Enforcement Policy

Enforcement Policies - Airwave Login Enforcement Policy

Summary | Enforcement | Rules

Enforcement:

Name:	Airwave Login Enforcement Policy
Description:	Airwave User Enforcement Policy
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Tips:Role *EQUALS* AW_RW_L2_WASHINGTON) *AND* (Authorization: **Active Directory** LDAP over SSL:memberOf *CONTAINS* AMP-RW-L2 WASHINGTON SITE)	AW_RW_L2_WASHINGTON
2.	(Tips:Role *EQUALS* AW_RO_L1_Enterprise) *AND* (Authorization: **Active Directory** LDAP over SSL:memberOf *CONTAINS* AMP-RO-L1 All Sites)	AW_RO_L1_Enterprise
3.	(Tips:Role *EQUALS* AW_RW_L2_Enterprise) *AND* (Authorization: **Active Directory** LDAP over SSL:memberOf *CONTAINS* AMP-RW-L2 All Sites)	AW_RW_L2_Enterprise
4.	(Tips:Role *EQUALS* AW_RW_L3_Enterprise) *AND* (Authorization: **Active Directory** LDAP over SSL:memberOf *CONTAINS* AMP-RW-L3 All Sites)	AW_RW_L3_Enterprise
5.	(Tips:Role *EQUALS* AW_RW_L4_Enterprise) *AND* (Authorization: **Active Directory** LDAP over SSL:memberOf *CONTAINS* AMP-RW-L4 All Sites)	AW_RW_L4_Enterprise

Appendix B
Complete Security Technical Implementation Guide (STIG) List

This appendix provides a reference list for the security features that AirWave applies when you run the STIGs.

Best Practices for STIG Application

When you apply STIGs from the CLI by selecting **7-1-2**, AirWave enforces and applies the following STIGs:

- Only three consecutive invalid logon attempts by a user during a 15 minute time period (APSCDV000530)
- When a password is changed, the characters are changed in at least eight of the positions within the password (APSCDV001730)
- Remove unneeded suid programs, and disable shells of application accounts (AW00001)
- Do not use persistent cookies (AW00002)
- Remove amprecovery user (AW00003)
- Disabling tftpd service (AW00004)
- Remove nullok from /etc/pam.d/system-auth (AW00005)
- Configure audit system to audit all attempts to alter system time through adjtimex (AW00008)
- Preventing a DOS by removing mod_proxy_ajp (CVE20100408)
- Setting FAIL_DELAY to 4 in /etc/login.defs (GEN000480)
- Password changes no more than once a day (GEN000540)
- Password strength and length requirements (GEN000580, GEN000600, GEN000620, GEN000640)
- Accounts will be disabled after 35 days of inactivity (GEN000760)
- Passwords reuse within five changes (GEN000800)
- 60-day password limit (GEN000820)
- Root account home directory permissions (GEN000920)
- Fix missing home directories (GEN001460)
- Fixing permissions on home directories (GEN001480)
- Fixing group permissions on home directories (GEN001520)
- Setting permissions on local init files (GEN001880)
- Remove .rhost support from PAM (GEN002100)
- Changing default umasks (GEN002560)
- Populate /etc/cron.allow and /etc/cron.deny (GEN002960)
- Setting crontab permissions (GEN003080)
- Set permissions on /etc/cron.allow and /etc/cron.deny (GEN003200)
- Adding system users to at.deny (GEN003320)
- Disabling core dumps (GEN003500)
- xinetd permissions (GEN003740)
- Removing tcpdump (GEN003865)
- traceroute permissions (GEN004000)
- Disable sendmail decode command (GEN004640)
- Setting MIB file permissions (GEN005340)
- syslog.conf permissions (GEN005400)

- Remove unnecessary users shutdown/halt/sync (LNX00320)
- Disable unnecessary accounts (operator news games gopher nfsnobody) (LNX00340)
- /etc/security/access.conf permissions (LNX00440)
- sysctl.conf permissions (LNX00520)
- Disable ctrl-alt-del handling (LNX00580)
- Securing Apache's PID file (WA00530)
- Disable TRACE and TRACK for Apache (WA00550)
- Remove symlinks in the DocRoot (WG360)
- Set seas_config column stigged_timestamp to current time (ZZ00001)