



CHAPTER 18

Using the Internal AAA Server (WLSE Express Only)

WLSE 2.15 includes an integrated authentication and authorization server that provides LEAP, Cisco-PEAP, MS-PEAP, EAP-FAST, and EAP-TLS authentication for access points.

The internal AAA server is available on the Wireless LAN Solution Engine Express (WLSE 1030) only.

The AAA server Web interface is accessible by selecting **Admin > AAA Administration**.

This chapter provides overview information and procedures for using the internal AAA server:

- [About the AAA Server, page 18-1](#)
- [Configuring the AAA Server—Overview, page 18-6](#)
- [Using AAA Server Screens, page 18-7](#)
- [Using AAA Server Log Files, page 18-28](#)
- [Monitoring the AAA Server, page 18-28](#)
- [Using AAA Server CLI Commands, page 18-30](#)
- [RADIUS Attributes for the AAA Server, page 18-46](#)

About the AAA Server

The AAA server is a RADIUS (Remote Authentication Dial-In User Service) server that allows multiple devices to use a common authentication and authorization database.

The server receives requests from users attempting to access clients and authenticates and/or authorizes users.

This section includes the following descriptions of AAA server features:

- [Basic Authentication and Authorization, page 18-2](#)
- [RADIUS Attributes of the AAA Server, page 18-2](#)
- [Supported Services, page 18-3](#)
- [Methods of Storing User Information, page 18-3](#)
- [Extensible Authentication Services, page 18-4](#)
- [Methods of Configuring the AAA Server, page 18-4](#)
- [Backup/Restore and Software Upgrades, page 18-5](#)

- [Ports Used by the AAA Server, page 18-5](#)
- [Fault Monitoring and Trend Reports, page 18-5](#)
- [Certificates and RSA Keys, page 18-5](#)

Basic Authentication and Authorization

The WLSE AAA server allows you to better manage access to your network, as it allows you to store all security information in centralized databases instead of distributing the information around the network.

The AAA server is based on a client/server model. The client passes information to the AAA server and acts on the response from the server. The server receives user access requests, authenticating the user and returning any available configuration information for the client to pass on to the user.

The AAA server handles the following tasks:

- Authentication—determines the identity of users and whether they may be allowed to access the network.
- Authorization—determines the level of network services available to authenticated users after they are connected.
- Session and resource management—tracks user sessions and allocates dynamic resources

The protocol is a simple packet exchange in which the client sends a request packet to the AAA server with a name and password. The AAA server looks up the name and password to verify that it is correct and returns an accept packet. The AAA server can also reject the request packet. To ensure network security, the client and server use a shared secret, which is known to both. Also, user passwords are encrypted between the client and the server.

Three participants (user, client, and AAA server) are involved in this interaction as follows:

1. The user contacts the client and supplies a name and password.
2. The client begins the session:
 - a. The client receives the name and password.
 - b. The client formats this information into an access-request packet.
 - c. The client forwards this packet to the AAA server.
3. The AAA server determines which client sent the request and parses the request. The server chooses a service to authenticate and/or authorize the user.
4. The AAA server's authentication service verifies that the name and password are in the database.
5. The AAA server's authorization service creates the response packet with the appropriate attribute's for the user's session.
6. The AAA server formats the response and sends the response to the client.
7. The client receives the response and communicates with the user.

RADIUS Attributes of the AAA Server

The AAA server comes with the standard RADIUS attributes (as defined by RFC 2865). For more information about AAA server attributes, see [RADIUS Attributes for the AAA Server, page 18-46](#).

Supported Services

The AAA server supports the following services:

- Windows active directory—see [Domain Authentication, page 18-3](#)
- Lightweight Directory Access Protocol (LDAP)—see [Lightweight Directory Access Protocol \(LDAP\), page 18-3](#)
- Extensible authentication services (EAP)—see [Extensible Authentication Services, page 18-4](#)

Methods of Storing User Information

When configuring an authentication service, you need to specify the user service; that is, where the user profile information is stored. This information can be stored locally on the AAA server or on an LDAP server. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user.

As an alternative to LDAP or the local service, you can use the Domain Authentication method and store user information in Windows Active Directory.

This section briefly describes these services:

- [Local User Database, page 18-3](#)
- [Lightweight Directory Access Protocol \(LDAP\), page 18-3](#)
- [Domain Authentication, page 18-3](#)

Local User Database

When using this service, you must enter each user and password on the AAA server. You can assign RADIUS attributes to each user. With the local service, you can have the AAA server perform authentication and/or authorization using a specific user list. For more information, see [Managing AAA Users, page 18-24](#).

Lightweight Directory Access Protocol (LDAP)

LDAP servers store directory information about users in order to authenticate them.

You can designate both a central LDAP server and local LDAP servers. The local LDAP server is primary, and the centralized server is secondary.

For more information about LDAP, see [Managing the LDAP Central Server, page 18-11](#) and [Managing the LDAP Local Server, page 18-12](#).

Domain Authentication

The AAA server can authenticate against the user database in Windows Active Directory on a Windows domain controller (WDC). Using this service requires that you download and configure a remote agent from Cisco.com and install the remote agent on the domain controller system.

To use domain authentication, you must install a remote agent on the WDC. You can download the remote agent from Cisco.com.

For information on downloading the remote agent and using domain authentication, see [Configuring Windows Domain Authentication, page 18-15](#).

Extensible Authentication Services

You can configure and use more than one of the following authentication services at the same time. If more than one service is configured, the WLSE negotiates which one to use.

The AAA server supports Extensible Authentication Protocol (EAP) to provide a common protocol for differing authentication mechanisms. EAP enables the dynamic selection of the authentication mechanism at authentication time based on information transmitted in the Access-Request. The AAA server supports the following EAP authentication methods.

The supported EAP methods are described in [Table 18-1 on page 18-4](#). You enable each EAP method by configuring it, using the WLSE UI or WLSE CLI commands.

Table 18-1 Supported EAP Methods

EAP Method	Description
LEAP	LEAP (Lightweight Extensible Authentication Protocol) is a Cisco-proprietary protocol that was defined and implemented for Cisco's Aironet product family.
PEAP	Protected EAP (PEAP) is an authentication method that was designed to mitigate several weaknesses of EAP. PEAP leverages TLS to achieve certificate-based authentication of the server (and optionally the client) and creation of a secure session that can then be used to authenticate the client. The AAA server supports the following versions of PEAP: <ul style="list-style-type: none"> • Cisco-PEAP (PEAP Version 1) • MS-PEAP (Microsoft PEAP, PEAP Version 0) PEAP can be used for authentication between wireless clients, such as inventory devices, and access points (either WDS access points or infrastructure access points).
EAP-FAST	EAP-FAST is a two-phase authentication protocol: <ul style="list-style-type: none"> • Phase 0, provisioning. Provision client with a credential called PAC (Protected Access Credential). • Phase 1, authentication. Use the PAC to establish a tunnel with the server and authenticate the username and password. The PAC is a security credential that is used to establish a shared secret between clients and the server. For EAP-FAST on the WLSE's AAA server, the PAC is created automatically.
EAP-TLS	EAP Transport Level Security (EAP-TLS) is an authentication method that was designed to mitigate several weaknesses of EAP. EAP-TLS leverages TLS, described in RFC 2246, to achieve certificate-based authentication of the server and (optionally) the client. EAP-TLS provides many of the same benefits as PEAP but differs from it in the lack of support for legacy authentication methods.

Methods of Configuring the AAA Server

For this release, the AAA server is pre-configured with appropriate parameters, so initial configuration is minimal. A WLSE user with system administration privileges can configure the AAA server. The configuration methods for the AAA server are WLSE CLI commands and the WLSE web interface. For information on the AAA Web interface, see [Using AAA Server Screens, page 18-7](#).

Most of the functions of the AAA server's Web interface can be performed by using command-line interface (CLI) commands. Additional functions that are not in the Web interface are provided through CLI commands: generating certificates, configuring logging method, reinitializing the database, and starting or stopping daemons. For details on CLI commands, see [Using AAA Server CLI Commands, page 18-30](#).

Backup/Restore and Software Upgrades

Backup and restore of the AAA server database is handled by the normal WLSE backup and restore functions—See [Backing Up and Restoring Data, page 16-21](#). Upgrade of the AAA server is performed during a normal WLSE software upgrade—See [Managing WLSE System Software, page 16-8](#).

Ports Used by the AAA Server

The AAA server requires sole use of the following ports on the WLSE:

- UDP ports 1812 and 1813—for RADIUS
- TCP ports 2785 and 2786—for internal process communication

Fault Monitoring and Trend Reports

The RADIUS, LEAP, and Cisco-PEAP protocols are monitored by the WLSE's fault mechanism. MS-PEAP and EAP-FAST are not monitored.

After configuring the AAA server and setting up AAA server monitoring, you can view faults, configure fault monitoring, and run reports for the authentication protocol that you select. A given WLSE can only monitor one protocol per AAA server. For information on configuring the WLSE to monitor the AAA server, see [Monitoring the AAA Server, page 18-28](#).

Related Topics

- [Using AAA Server Screens, page 18-7](#)
- [Configuring the AAA Server—Overview, page 18-6](#)
- [Fault Monitoring, page 3-1](#)
- [Using Reports, page 10-1](#)

Certificates and RSA Keys

A self-signed certificate is automatically generated by the WLSE during initial startup and is placed in a location where it can be used by the AAA server. A self-signed certificate is required; the AAA server will not operate without a self-signed certificate.

If you need to obtain a more secure certificate from a certificate authority, obtain an RSA key, or regenerate the self-signed certificate in order to make changes in it, you will need to enter the pathnames of the certificates and the key in the relevant AAA server screens.

When you request a certificate from the certificate authority you receive an RSA key and two certificates: your certificate for your site and a certificate that certifies the issuing authority.

The self-signed certificate is not as secure as a certificate issued by a certificate authority, but may be adequate if your network is not accessible from the outside. Also, you may wish to generate your own self-signed certificate that contains the name of your organization and other identifying information.

**Note**

For detailed information about how to generate certificates to be used with the WLSE, and how to configure AAA certificates to be used on the WLSE, see the *WLSE AAA Server Certificate Configuration Guide* on Cisco.com.

Configuring the AAA Server—Overview

This section contains the following topics:

- [Naming Guidelines, page 18-6](#)
- [Configuration Methods, page 18-6](#)
- [Configuration Tasks, page 18-6](#)
- [Reconfiguration Tasks, page 18-7](#)

Naming Guidelines

For AAA server usernames, group names, and client names, you can use up to 255 characters and any character except for the forward slash (/).

Configuration Methods

You can configure the AAA server by using the screens in the Web interface ([Using AAA Server Screens, page 18-7](#)) or the CLI commands ([Using AAA Server CLI Commands, page 18-30](#)).

Configuration Tasks

To configure the AAA server, perform the tasks in [Table 18-2 on page 18-6](#).

Table 18-2 Tasks for Configuring the AAA Server

Task Description	Reference
Configure the authentication services you are going to use.	Configuring LEAP Settings, page 18-18 Configuring Cisco-PEAP Settings, page 18-18 Configuring MS-PEAP Settings, page 18-19 Configuring EAP-TLS Settings, page 18-21 Configuring EAP-FAST Settings, page 18-21
If you are using the local user database, add users.	Managing AAA Users, page 18-24
If you are using LDAP as the user database, configure LDAP parameters on the WLSE. ^{1 2}	Managing the LDAP Central Server, page 18-11 Managing the LDAP Local Server, page 18-12

Table 18-2 Tasks for Configuring the AAA Server (continued)

Task Description	Reference
If you are using domain authentication (Windows Active Directory) for the user database, configure domain authentication parameters on the WLSE.	Configuring Windows Domain Authentication, page 18-15
If you are using domain authentication groups, you can create local groups and map them to groups on the WDC.	Managing Groups, page 18-26
Add clients. ³	Managing AAA Clients, page 18-23
(Optional) Configure the WLSE to monitor the internal AAA server.	Monitoring the AAA Server, page 18-28
(Optional) Configure logging (syslog or local)	aaa-server logging, page 18-40

1. You can use LDAP or domain authentication for one service and use the local database for another.
2. If you are using LDAP, you need to add a WLSE user on the LDAP server.
3. The WLSE appliance must be added as a client of the AAA server.

Reconfiguration Tasks

If you change any of the information listed in [Table 18-3 on page 18-7](#) after initial configuration, you will need to make corresponding changes on the WLSE.

Table 18-3 Reconfiguring the AAA Server

Change	Reference
LDAP server characteristics	Managing the LDAP Central Server, page 18-11 Managing the LDAP Local Server, page 18-12
IP address of a client device	Managing AAA Clients, page 18-23
RADIUS shared secret of a client device	Managing AAA Clients, page 18-23
Addition of devices or users	Managing AAA Clients, page 18-23 Managing AAA Users, page 18-24

Using AAA Server Screens



Note

If you are using the WLSE redundancy feature, AAA screens are not displayed on the standby WLSE.

This section contains procedures for configuring the AAA server and includes the following topics:

- [AAA Server Administration Subtab Functions, page 18-8](#)
- [Displaying AAA Server Status, page 18-9](#)
- [Setting AAA Server Trace Level and Viewing Trace Logs, page 18-10](#)
- [Managing the LDAP Central Server, page 18-11](#)
- [Managing the LDAP Local Server, page 18-12](#)

- [Configuring Windows Domain Authentication, page 18-15](#)
- [Configuring LEAP Settings, page 18-18](#)
- [Configuring Cisco-PEAP Settings, page 18-18](#)
- [Configuring MS-PEAP Settings, page 18-19](#)
- [Configuring EAP-TLS Settings, page 18-21](#)
- [Configuring EAP-FAST Settings, page 18-21](#)
- [Managing AAA Clients, page 18-23](#)
- [Managing AAA Users, page 18-24](#)
- [Managing Groups, page 18-26](#)
- [Viewing and Releasing Sessions, page 18-27](#)

AAA Server Administration Subtab Functions



Note

The AAA Administration subtab may not be visible to some users; whether you see the Admin tab or its subtabs depends on the user roles assigned to your login.

The options under the AAA Administration subtab are:

Table 18-4 AAA Server Subtab Functions

Option	Function
AAA Server Status	Display status of server processes— Displaying AAA Server Status, page 18-9
AAA Server Trace Level	Set level of trace logging— Setting AAA Server Trace Level and Viewing Trace Logs, page 18-10
LDAP Central Server	Configure LDAP if using LDAP for user database: Managing the LDAP Central Server, page 18-11 Managing the LDAP Local Server, page 18-12
LDAP Local Server	
Windows Domain Auth Server	Configure domain authentication— Configuring Windows Domain Authentication, page 18-15
LEAP Settings	Configure the AAA protocols you are using: Configuring LEAP Settings, page 18-18 Configuring Cisco-PEAP Settings, page 18-18 Configuring MS-PEAP Settings, page 18-19 Configuring EAP-TLS Settings, page 18-21 Configuring EAP-FAST Settings, page 18-21
Cisco-PEAP Settings	
MS-PEAP Settings	
EAP-TLS Settings	
EAP-FAST Settings	
Clients	Add, modify, and delete clients— Managing AAA Clients, page 18-23
Users	Add modify and delete users if you are using the local user database— Managing AAA Users, page 18-24

Table 18-4 AAA Server Subtab Functions (continued)

Option	Function
Groups	Manage groups for domain authentication— Managing Groups
Sessions	Display and release sessions— Viewing and Releasing Sessions, page 18-27

Displaying AAA Server Status

To display information on AAA server processes, select **Admin > AAA Admin > AAA Server Status**. The status of the following processes (running or not) and the PID of each process is displayed.

In addition, the health of the AAA server is displayed. The message *Server is Running, its health is 10 out of 10* means that the AAA server is running optimally. If this health indicator decreases, you should inspect the AAA server logs for any anomalous behavior. For example, if the percent of rejected requests grows significantly over time, the health indicator will decrease. For information on these logs, see [Using AAA Server Log Files, page 18-28](#).

For information on any outstanding AAA server faults, select **Faults > Display Faults**. Faults and reports on the AAA server are only displayed after the WLSE has been configured to monitor the AAA server. For more information, see [Monitoring the AAA Server, page 18-28](#).

Table 18-5 AAA Server Processes

Process	Function
AAA server	Processes AAA packets, listening for RADIUS requests, deciding what to do with them (may include making an LDAP query), and then sending RADIUS responses.
AAA daemon manager	Similar to the WLSE daemon manager. Restarts any of the other processes when necessary and coordinates orderly startup and shutdown of the other processes.
AAA database lock manager	Controls access to the database process by multiple clients. In particular, the server, CLI, and Web interface all need to access the database and must be coordinated.
AAA database	Maintains AAA configuration data, including any internal users that have been defined.

Related Topics

- [About the AAA Server, page 18-1](#)
- [Displaying Fault Information, page 3-1](#)
- [Monitoring the AAA Server, page 18-28](#)

Setting AAA Server Trace Level and Viewing Trace Logs

The AAA Server Trace Level page displays the current trace level for the AAA server. Trace information can be used for debugging or validating the behavior of the AAA server. The trace level governs how much information is logged about the contents of a packet. The higher the trace level, the more information is logged. Trace levels are inclusive, so if you set trace level to 3, you log all of the information for trace levels 1 and 2.

Tracing is meant to be temporary, and you should not leave tracing turned on for more than a brief period of time. If tracing is left on, it will quickly fill up available disk space. The rate of consumption of disk space depends on the trace level selected and the current traffic rate (that is, the number of access points authenticating per second).

For information on the trace levels and the information logged at each level, see [Trace Levels and Information Logged](#), page 18-10.



Note

If you have configured the WLSE to monitor the AAA server, you can display information on any outstanding AAA server faults in **Faults > Display Faults**.

The AAA-server-trace.log file contains the results of tracing; the file contains data only when tracing is turned on. To use this file, select **Admin > Appliance > Status > View Log File**.

Procedure

-
- Step 1** Select **Admin > AAA Administration > AAA Server Trace Level**.
 - Step 2** Select the desired trace level, from 0 (no tracing) to 5 (most verbose).
 - Step 3** Click **Submit**.
-

Related Topics

- [About the AAA Server](#), page 18-1
- [Displaying Fault Information](#), page 3-1
- [Monitoring the AAA Server](#), page 18-28

Trace Levels and Information Logged

lists the trace levels and the information logged at each level. This information is logged in the AAA-server-trace.log, accessible by **Admin > AAA Administration > View Log File**. Trace levels are inclusive; for example, if trace level is set at 3, the information from trace levels 2 and 3 are also logged.

Table 18-6 Trace Levels and Information Logged

Trace Level	Information Returned
0	No trace performed
1	Reports when packet is sent or received or when there is a change in the remote server's status.

Table 18-6 Trace Levels and Information Logged (continued)

Trace Level	Information Returned
2	Logs the following: <ul style="list-style-type: none"> • Services and session managers used to process a packet • Client and vendor objects used to process a packet • Remote server details for LDAP and RADIUS, such as sending packets and timing out • Details about poorly formed packets • Details included in trace level 1
3	Logs the following: <ul style="list-style-type: none"> • Error traces in TCL scripts when referencing invalid RADIUS attributes • Scripts that were executed • Details about local UserList processing • Details included in trace levels 1 and 2
4	Logs the following: <ul style="list-style-type: none"> • Information about advanced duplication detection processing • Details about creating, updating, and deleting sessions • Trace details about scripting APIs called • Details included in trace levels 1, 2, and 3
5	Logs the following: <ul style="list-style-type: none"> • Details about use of the policy engine: rules that were run, what the rules did, whether the rule passed or failed, which policies were called • Details included in trace levels 1, 2, 3, and 4

Managing the LDAP Central Server



Note

If you are using the default method of having LEAP query the internal database, you do not need to configure LDAP servers. For PEAP, the default is to use LDAP.

The Lightweight Directory Access Protocol (LDAP) screens allow you to enter information about local and central LDAP servers. LDAP servers store directory information about users in order to authenticate them.

The WLSE must also be added to the LDAP server.

Procedure

To modify the properties of the LDAP central server:

Step 1 Select **Admin > AAA Administration > LDAP Central Server**.

The Configure LDAP Central Server screen has two parts: the top part is for setting general parameters, and the bottom part is for creating LDAP-to-RADIUS attribute mappings.

- Step 2** Enter or modify the information in the screen. For details on the fields and how the parameters are used, see [About LDAP Parameters, page 18-13](#).
- Step 3** (Optional) LDAP-to-RADIUS attribute mapping. You can add or delete mappings as follows. For information on the RADIUS attributes that are native to the AAA server, see [RADIUS Attributes for the AAA Server, page 18-46](#).



Note Once entered, a mapping cannot be modified. To modify a mapping, you must first delete the mapping and then add it again.

To add a mapping:

- a. Select **Add**.
Result: The LDAP Attribute and Maps to RADIUS Attribute text boxes appear, along with an **Apply** button.
- b. Enter the desired mapping.
- c. Click **Apply**.

To delete a mapping:

- a. Select the mapping from the **LDAP Attributes to RADIUS Attributes** list.
- b. Click **Delete**.

Step 4 To save your changes, click **Submit**.

Step 5 To cancel your changes, click **Cancel**.

Related Topics

- [About the AAA Server, page 18-1](#)
- [About LDAP Parameters, page 18-13](#)
- [Managing the LDAP Local Server, page 18-12](#)
- [Configuring the AAA Server—Overview, page 18-6](#)

Managing the LDAP Local Server



Note If you are using the default method of having LEAP query the internal database, you do not need to configure LDAP servers. The default for PEAP is to use LDAP.

Use the Lightweight Directory Access Protocol (LDAP) screens to enter information about local and central LDAP servers. LDAP servers store authentication and authorization information.

The WLSE must also be added to the LDAP server.

Procedure

To modify the attributes of a LDAP local server:

Step 1 Select **Admin > AAA Administration > LDAP Local Server**.

The Configure LDAP Local Server screen has two parts: the top part is for setting general parameters, and the bottom part is for creating LDAP-to-RADIUS attribute mappings.

- Step 2** Enter or modify the general information in the top part of the screen. For details on the fields and how the parameters are used, see [About LDAP Parameters, page 18-13](#).
- Step 3** (Optional) LDAP-to-RADIUS attribute mapping. You can add or delete mappings as follows. For information on the RADIUS attributes that are native to the AAA server, see [RADIUS Attributes for the AAA Server, page 18-46](#).



Note Once a mapping has been added, you cannot modify it. You must first delete the mapping and then add it again.

To add a mapping:

- a. Select **Add**.
Result: The LDAP Attribute and RADIUS Attribute text boxes appear, along with an **Apply** button.
- b. Enter the desired mapping.
- c. Click **Apply**.

To delete a mapping:

- a. Select the mapping from the **LDAP Attributes to RADIUS Attributes** list.
- b. Click **Delete**.

Step 4 To save your changes, click **Submit**.

Step 5 To cancel your changes, click **Cancel**.

Related Topics

- [About the AAA Server, page 18-1](#)
- [About LDAP Parameters, page 18-13](#)
- [Managing the LDAP Central Server, page 18-11](#)
- [Configuring the AAA Server—Overview, page 18-6](#)

About LDAP Parameters

This section contains:

- Details on the LDAP parameters in the LDAP screens—See [LDAP Parameter Details, page 18-13](#).
- How the parameters are used—See [How LDAP Settings are Used, page 18-15](#).

LDAP Parameter Details

The LDAP parameters you can set in the AAA server LDAP server screens are described in [Table 18-7 on page 18-14](#). All parameters are required, except as indicated. The values you enter are used as described in [How LDAP Settings are Used, page 18-15](#).

Table 18-7 LDAP Parameters

Field	Description
Host Name	Host name or IP address of the LDAP server.
Port	Port on the LDAP server for the bind (usually, port 389). The port number must be an integer between 1 and 65536.
Bind Name (optional)	The distinguished name (DN) (administrator name) to use when establishing a connection between the LDAP and AAA servers.
Bind Password (optional)	Password associated with the Bind Name.
Search Path	Path that indicates where in the LDAP database to start the search for user information. The path is specified as a distinguished name (DN). LDAP references an LDAP object by its distinguished name. Specifying a DN (such as ou=Engineering, o=cisco.com) as the Search Path restricts user queries to objects that match those property values.
Search Filter	Search filter used by the AAA server when querying the LDAP server for user information. Use the notation %s to indicate where the user ID should be inserted. For example, a typical value for this property is (uid=%s), which means that when querying for information about user joe, use the filter uid=joe. <i>uid</i> is the name of the LDAP property that contains the same values as the RADIUS User Name attributes that are being authenticated.
User Password	LDAP property that contains the passwords to use for authentication. This property must be a property of all objects that match the Search Path.
Password Encryption	Select an encryption method for the user password: <ul style="list-style-type: none"> • None—no encryption (the default). • Dynamic—This setting instructs the AAA server to choose the encryption mechanism on a case-by-case basis after the server determines the presence of a known prefix, which the server prepends to the password attribute. • Crypt—AAA server encryption using the Unix crypt algorithm. • SHA-1 or SSHA-1— Secure Hash Algorithm; a hashing algorithm that produces a 160-bit digest based upon the input. The algorithm produces SHA passwords that are irreversible or prohibitively expensive to reverse. Enables the AAA server to authorize users whose passwords are stored in an LDAP server and hashed by using the SHA-1 encoding scheme. SSHA-1 is Netscape's (iPlanet) enhancement of the SHA-1 algorithm which includes salted password data.
Timeout	Timeout for bind attempts. How long (in seconds) the AAA server will wait for a response from the LDAP server. The default is 15 seconds.

Table 18-7 LDAP Parameters (continued)

Field	Description
LDAP to RADIUS mappings (optional)	<p>List of name/value pairs. The name is an LDAP attribute to retrieve from the user record, and the value is the RADIUS attribute to set to the value of the LDAP attribute.</p> <p>An error message is displayed:</p> <ul style="list-style-type: none"> • If you attempt to map the same attribute more than once, an error message will be displayed. • If you enter an incorrect RADIUS attribute. <p>See the relevant vendor documentation for information about which attributes you may need to enter. The AAA server will operate properly with no authorization attributes; however, the client device may not provide the appropriate service because of the lack of certain authorization attributes. For a list of the RADIUS attributes native to the AAA server, see RADIUS Attributes for the AAA Server, page 18-46.</p>

How LDAP Settings are Used

The LDAP settings that you configure in the LDAP screens are used as follows.

The AAA server connects as an LDAPv3 client to the LDAP server on the named Port. The AAA server uses the Bind Name and Bind Password to connect. If the LDAP server does not respond within the number of seconds specified as the Timeout, the server times out. This connection is made once at startup and again if the connection is dropped.

Each time an Access-Request is received, the AAA server queries the subtree rooted at the Search Path, using the Search Filter (substituting the RADIUS User-Name for %s) to specify an object in the subtree. If such an object is found, the User Password Attribute and specified LDAP Attribute values are returned.

On the AAA server, the RADIUS User-Password attribute value is encrypted, using the Password Encryption technique, and is then compared to the returned User Password Attribute value (which must be encrypted using the same technique). If these values match, the other LDAP Attribute values that are returned are mapped as specified to RADIUS attributes. These composed attribute-value pairs are added to the Access-Accept packet.

Related Topics

- [Managing the LDAP Central Server, page 18-11](#)
- [Managing the LDAP Local Server, page 18-12](#)

Configuring Windows Domain Authentication

Use this option to configure the AAA server to use Windows domain authentication service as the user database. This service uses a user database stored in Windows Active Directory on a Windows Domain Controller. Use of this service requires that you download and configure a remote agent and install it on the Windows Domain Controller.

**Note**

To use domain authentication service, you must first download a remote agent and install it on the Windows Domain Controller. The remote agent provides a secure tunnel between Active Directory and the WLSE. For information about downloading and installing the remote server, see [Installing the Remote Server for Domain Authentication, page 18-17](#).

A user can optionally specify the domain name along with a user ID while logging on. The domain name is used for authentication:

- If the domain is not specified, authentication is first performed with the WDC/AD default domain and then with all the other trusted domain controllers until the user is found.
- If the domain is specified, authentication is performed only on that domain, which could be the local WDC/AD or one of the trusted WDC/ADs.

If you want to map RADIUS attributes to values in Active Directory, you can create AAA server groups and map them to Active Directory groups.

Optionally, users can be authorized using WDC/AD. The list of groups to which the user belongs in the WDC/AD is used. You map this list of groups to an internal group in the AAA server by means of a group map. The group map is a map between a list of external groups in WDC/AD and an internal AAA user group. You can configure an optional default group, which is used when there is no mapping found or when there is no hit in the maps. When a hit is encountered, the corresponding group is used. For example, if the user is in groups A, B, C, and D and a map for ABC is found before the map for ABCD, the ABC map is used.

Procedure

Step 1 Select **Admin > AAA Administration > Windows Domain Auth Server**.

Step 2 Enter the following information.

Field	Description
Host Name	Set the hostname for the local WDC/AD. Default is localhost.
Port	Set the port number. Default is 2004.
Default Domain	(Optional) Sets the default domain name. The default domain is used to locate the user if the user does not specify a domain when logging in.
Group mapping:	
Default AAA Server Group	Select an AAA server group to be mapped to WDC/AD groups. A default AAA server group is provided (domain-auth-usergroup), or you can create your own default group to be mapped to all WDC/AD groups. If you are not mapping groups, select None. Note To configure RADIUS attributes in the default user group, create another default group, or create other groups to be mapped to WDC/AD groups, you use the Groups option. See Managing Groups, page 18-26 .

Field	Description
AAA User Group to Windows Group Mappings	<p>(Optional) If you are using group maps, map the AAA groups to WDC/AD groups as needed:</p> <ol style="list-style-type: none"> 1. Click Add. 2. Two fields appear at the bottom of the screen: AAA User Group and Maps to Windows Group. 3. Enter a group name and click Apply. Repeat this step to add more groups. After you click Apply, the group is added to the list under Default AAA Server Group. <p>Note The AAA server groups must first be defined under Admin > AAA Administration > Groups.</p>

Step 3 To save your changes, click **Submit**. To discard your changes, click **Cancel**.

Installing the Remote Server for Domain Authentication

Use the following instructions to download and install the mandatory remote server on a Windows Domain Controller (WDC). The remote server should be installed on a WDC that has access to your Active Directory server.

Procedure

- Step 1** Navigate to the following URL on Cisco.com and log in:
<http://www.cisco.com/cgi-bin/tablebuild.pl/acs-soleng-3des>
- Step 2** Download Remote-Agent-ACSse-win-v3.3.2.2-K9.zip.
- Step 3** Unzip the archive and run Setup.exe:
- At the prompt for an ACS appliance, enter the IP address or hostname of the WLSE.
 - At the prompt for the software to be installed, select windows authentication.
- Step 4** Finish the installation

Related Topics

- [Installing the Remote Server for Domain Authentication, page 18-17](#)
- [Configuring the AAA Server—Overview, page 18-6](#)
- [About the AAA Server, page 18-1](#)
- [Managing Groups, page 18-26](#)

Configuring LEAP Settings

The AAA server uses LEAP to authenticate repeater access points via a WDS access point. By default, user information is stored locally in the AAA server.

Procedure

-
- Step 1** Select **Admin > AAA Administration > LEAP Settings**
- Step 2** Select the service to use after LEAP negotiation. This specifies the location of user information for authentication and authorization. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user.
- Local—authenticates against user information stored locally.
 - [LDAP](#)—authenticates against user information on the LDAP server.
 - Windows Domain-Auth—authenticates against WDC/AD.
- Step 3** To save your changes, click **Submit**. To discard your changes, click **Cancel**.
-

Related Topics

- [About the AAA Server, page 18-1](#)
- [Configuring the AAA Server—Overview, page 18-6](#)
- [Configuring Windows Domain Authentication, page 18-15](#)
- [Managing AAA Users, page 18-24](#)
- [Managing the LDAP Central Server, page 18-11](#)
- [Managing the LDAP Local Server, page 18-12](#)

Configuring Cisco-PEAP Settings

The AAA server uses PEAPV1 tunneling EAP-GTC for authentication and authorization of wireless supplicants via access points. User profile information is stored in [LDAP](#) by default.

Procedure

-
- Step 1** Select **Admin > AAA Administration > Cisco-PEAP Settings**.
- Step 2** Enter the following information.

Field	Description
Private Key Password	The server's private key password for PEAPV1.
Confirm Private Key Password	

Field	Description
Certificate Upload	Enter the absolute pathname of the file that contains your enterprise's certificate or browse for the file.
RSA Key Upload	Enter or browse for the absolute pathname of the file that contains the RSA private key.
CA Certificate Upload	Enter or browse for the absolute pathname of the file that contains the certificate authority's certificate.
Inner Service	Select the source of user information for authentication and authorization. <ul style="list-style-type: none"> Local—authenticates against user information stored locally. All users must be entered on the AAA server. See Managing AAA Users, page 18-24. LDAP—authenticates against user information on the LDAP server. This is the default. See Managing the LDAP Central Server, page 18-11 and Managing the LDAP Local Server, page 18-12. Windows Domain-Auth—authenticates against user information in an Active Directory database on a Windows Domain Controller. See Configuring Windows Domain Authentication, page 18-15.

Step 3 To save your changes, click **Submit**. To discard your changes, click **Cancel**.

Related Topics

- [About the AAA Server, page 18-1](#)
- [Configuring the AAA Server—Overview, page 18-6](#)
- [Managing AAA Users, page 18-24](#)
- [Configuring Windows Domain Authentication, page 18-15](#)
- [Managing the LDAP Central Server, page 18-11](#)
- [Managing the LDAP Local Server, page 18-12](#)

Configuring MS-PEAP Settings

This option allows you to set PEAP V0 parameters for AAA. User profile information is stored in [LDAP](#) by default.



Note

The AAA server cannot monitor MS-PEAP; therefore, there is no fault monitoring and reports are not available for this protocol.

Procedure

Step 1 Select **Admin > AAA Administration > MS-PEAP Settings**.

Step 2 Enter the following information.

Field	Description
Private Key Password	The server's private key password for PEAPv0. The password must match the ServerRSAKeyFile certificate file.
Confirm Private Key Password	
Certificate Upload	Enter absolute pathname of file that contains your enterprise's certificate or browse for the file.
RSA Key Upload	Enter or browse for absolute pathname of file that contains the RSA private key.
CA Certificate Path	Enter or browse for absolute pathname of file that contains the certificate authority's certificate.
Inner Service	<p>Select the source of user information for authentication and authorization. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user.</p> <ul style="list-style-type: none"> • Local—authenticates against user information stored locally. All users must be entered on the AAA server. See Managing AAA Users, page 18-24. • LDAP—authenticates against user information on an LDAP server. This is the default. See Managing the LDAP Central Server, page 18-11 and Managing the LDAP Local Server, page 18-12. • Windows Domain-Auth—authenticates against user information in a Windows active directory database on a Windows domain authentication server. See Configuring Windows Domain Authentication, page 18-15.

Step 3 To save your changes, click **Submit**. To discard your changes, click **Cancel**.

Related Topics

- [Configuring the AAA Server—Overview, page 18-6](#)
- [About the AAA Server, page 18-1](#)
- [Managing AAA Users, page 18-24](#)
- [Managing the LDAP Central Server, page 18-11](#)
- [Managing the LDAP Local Server, page 18-12](#)
- [Configuring Windows Domain Authentication, page 18-15](#)

Configuring EAP-TLS Settings

This option allows you to set PEAP V0 parameters for AAA. User profile information is stored in [LDAP](#).

Procedure

- Step 1** Select **Admin > AAA Administration > EAP-TLS Settings**.
- Step 2** Enter the following information; all fields are required.

Field	Description
Private Key Password	The server's private key password.
Confirm Private Key Password	
Certificate Upload	If you obtain a certificate from a certificate authority, enter the absolute pathname of the certificate files or browse for them.
RSA Key Upload	If you obtain a certificate from a certificate authority, enter the absolute pathname of the file that contains the RSA key or browse for it.

- Step 3** To save your changes, click **Submit**. To discard your changes, click **Cancel**.

Configuring EAP-FAST Settings

Use this option to configure EAP-FAST settings for the AAA server.



Note

The AAA server cannot monitor EAP-FAST on the internal AAA server; therefore, there is no fault monitoring and reports are not available for this protocol.

Procedure

- Step 1** Select **Admin > AAA Administration > EAP-FAST Settings**.
- Step 2** Enter the following information.



Note

The fields that are grayed out are not currently supported.

Table 18-8 *EAP-FAST Parameters*

Field	Description
Always Authenticate	If selected, provisioning always rolls over into authentication without relying on a separate setting. Wireless performs better when this is selected.

Table 18-8 EAP-FAST Parameters (continued)

Field	Description
Authority Identifier	Set the authority identifier. Must be a single string that uniquely identifies this server; spaces and quotation marks are not allowed.
Authority Information	Enter the authority information, which provides human-readable descriptive text for the credential issuer; for example the enterprise and/or server name. The value might be displayed to the client for identification purposes. Uniquely identifies the PAC issuer. Can contain spaces.
Credential Lifetime	Set the lifetime of the credential: <ul style="list-style-type: none"> • Forever—Credential never expires. • Timespan—Click Timespan to activate the following fields. Click Forever to delete the values of the following fields and deactivate them (gray them out). <ul style="list-style-type: none"> – weeks – days – hours – minutes
Provisioning Mode	Set the provisioning mode. Only Anonymous is supported.
Inner Service	Select the service to use after LEAP negotiation. This specifies the location of user information for authentication and authorization. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user. <ul style="list-style-type: none"> • Local—authenticates against user information stored locally. All users must be entered on the AAA server; see Managing AAA Users, page 18-24. • LDAP—authenticates against user information on the LDAP server. • Windows Domain-Auth—authenticates against user information in an Active Directory database on a Windows Domain Controller. See Configuring Windows Domain Authentication, page 18-15.

Step 3 To save your changes, click **Submit**. To discard your changes, click **Cancel**.

Related Topics

- [About the AAA Server, page 18-1](#)
- [Configuring the AAA Server—Overview, page 18-6](#)
- [Managing AAA Users, page 18-24](#)
- [Configuring Windows Domain Authentication, page 18-15](#)
- [Managing the LDAP Central Server, page 18-11](#)
- [Managing the LDAP Local Server, page 18-12](#)

Managing AAA Clients

In the context of the AAA server, a client is a device that submits a request for authorization on behalf of infrastructure access points. Clients that should be added under this option are:

- Devices that provide Wireless Domain Services (WDS). These include WDS access points, Wireless LAN Services Modules (WLSMs), or routers running an image that includes WDS capabilities.
- If you are *not* using WDS, all of the [infrastructure access points](#) with users who should be authenticated should be added as clients.
- The WLSE itself (for monitoring the internal AAA server).

To set up the WLSE to monitor the internal AAA server, see [Monitoring the AAA Server, page 18-28](#).

- Any other device that communicates directly with the AAA server.

By using address ranges or wildcards (*), you can add multiple clients at the same time.

Procedure

Step 1 Select **Admin > AAA Administration > Clients**.

Step 2 Add the WLSE as a client. If you are using a redundant pair of WLSEs, add both WLSEs to the list of clients.

Writer question: For the redundant pair, do you use the VIPs?

- Click **Add Client**.
- Enter the IP address of the WLSE.
- Enter a shared secret.



Note You will need this shared secret when configuring the WLSE to monitor the AAA server—See [Monitoring the AAA Server, page 18-28](#).

Step 3 Add other clients:

- Click **Add Client**.
- Enter the following information.

Field	Description
Name	Name for the client.
IP Address	Client IP address. You can enter: <ul style="list-style-type: none"> • A single address; for example 191.168.168.5. • Ranges; for example, 192.168.168.3-5. • The * wildcard; for example, 192.168.*.*.
Shared Secret	RADIUS shared secret set on the client.

- Click **Submit**.
- Click **Cancel** to cancel submission of the new client.

- Step 4** To modify a client:
- Click the client name.
 - Edit the client as desired.
 - Click **Submit**.
 - Click **Cancel** to cancel your changes to the client.
- Step 5** To delete a client:
- Click the client name. The Edit Client screen appears.
 - Click **Delete**.
-

Related Topics

[About the AAA Server, page 18-1](#)

Managing AAA Users

In the context of the AAA server, a user is any entity that is being authenticated by a client; for example, a person, an infrastructure access point, or a MAC address.

Enter all users in this screen unless you are using LDAP or Windows domain authentication as the source of user information.

If you have chosen “local” as the Inner Service for a protocol, enter all users to be authenticated in this screen.

Possible users include:

- Users on any of the devices that are using the AAA server to authenticate or authorize those users.
- Administrators who are using authentication to access APs through Telnet.
- A WLSE user, if you are using the WLSE to monitor the performance of the internal AAA server. For more information about using the WLSE to monitoring the internal AAA server, see [Monitoring the AAA Server, page 18-28](#).

You can [Add a User](#), [Modify a User](#), and [Delete a User](#).

Add a User

- Step 1** Select **Admin > AAA Administration > Users**.
- Step 2** Click **Add User**. The Add User page appears.
- Step 3** Enter the user name and user password and confirm the password.
- These are the values that will be assigned to the RADIUS User-Name and User-Password attributes when the access point authenticates with WDS.
- A user name can have up to 255 characters. You can use any character except the forward slash (/).
- Step 4** (Optional) In the “RADIUS attributes to value mappings” section, add RADIUS attribute mappings as follows.



Note See the relevant vendor documentation for information about which attributes you may need to enter. The AAA server will operate properly with no authorization attributes; however, the client device may not provide the appropriate service because of the lack of certain authorization attributes. For a list of the RADIUS attributes native to the AAA server, see [RADIUS Attributes for the AAA Server, page 18-46](#).

- a. Select **Add**.
Result: The RADIUS Attribute and Attribute Value text boxes appear.
- b. Enter the desired mappings.
- c. Click **Apply**.



Note Mappings cannot be modified. To change a mapping, first delete it from the RADIUS Attributes to Values list, then create a new mapping.

Step 5 To add the user, click **Submit**. To cancel the creation of the user, click **Cancel**.



Note If you entered an incorrect RADIUS attribute in Step 4, or you attempt to map the same attribute more than once, an error message will be displayed after you click **Submit**. The user will not be added. Click **Back** to make corrections in the mappings.

Modify a User

- Step 1** Select **Admin > AAA Administration > Users**.
- Step 2** Click the user name. The User Edit screen appears.
- Step 3** To change the name, enter a new name in the Name field.
- Step 4** To change the password, click **Change Password**. Then, enter the new password and confirm it.
- Step 5** To add RADIUS attribute mappings, see [Modify a User, page 18-25](#) for details.
- Step 6** To delete a RADIUS attribute mapping, select the mapping from the RADIUS Attributes to Values list, then click **Delete**.



Note Mappings cannot be modified. To change a mapping, first delete it, then create a new mapping.

Step 7 Click **Submit**. To cancel your changes to the user, click **Cancel**.

Delete a User

- Step 1** Select **Admin > AAA Administration > Users**.
- Step 2** Click the user name. The Edit User page appears.

Step 3 Click **Delete**.

Related Topics

- [Configuring the AAA Server—Overview, page 18-6](#)
- [About the AAA Server, page 18-1](#)

Managing Groups

When you select **Admin > AAA Administration > Groups**, the Groups List screen displays.

In this screen, you define the user groups to be mapped to WDC/AD groups in the Windows Domain Auth screen. You can define a default group to be mapped to all WDC/AD groups.

You must define AAA server groups in this screen before you can map AAA server groups to WDC/AD groups (unless you are using the default AAA server group). The group mapping feature is used to assign RADIUS attributes to groups of users stored in an Active Directory database on a Windows Domain Controller. For more information on mapping groups, see [Configuring Windows Domain Authentication, page 18-15](#).

You can add groups, edit existing groups, or delete existing groups.

Procedure

Step 1 To add a group, click **Add Group** in the Groups List page.

Step 2 Enter the group name in the Name field.

A group name can have up to 255 characters. You can use any character except the forward slash (/).

Step 3 (Optional) Add RADIUS attribute values as follows.



Note See the relevant vendor documentation for information about which attributes you may need to enter. For a list of the RADIUS attributes native to the AAA server, see [RADIUS Attributes for the AAA Server, page 18-46](#)

- Select **Add**.
Result: The RADIUS Attribute and Value text boxes appear.
- Enter the desired mappings.
- Click **Apply**.
- Repeat steps a-c to add more mappings.

Step 4 After you have finished creating the group, click **Submit**.



Note If you entered an incorrect RADIUS attribute in Step 2d, or you attempt to map the same attribute more than once, an error message will be displayed after you click **Submit**. The user will not be added. Click **Back** to make corrections in the mappings.

Step 5 To modify a group:

- Click the group name. The Group Edit screen appears.

- b. To change the name, enter a new name in the Name field.
 - c. To add or delete RADIUS attribute mappings, see Step 3 for details.
 - d. To delete a RADIUS mapping, select the mapping, then click **Delete**.
 - e. Click **Submit**.
- Step 6** To delete a group:
- a. Click the group name. The Edit Group page appears.
 - b. Click **Delete**.
- Step 7** To cancel your changes, click **Cancel**.
-

Related Topics

[Configuring Windows Domain Authentication, page 18-15](#)

Viewing and Releasing Sessions

The Sessions screen allows you to:

- Display information about a user session by entering a username or session ID: Username, Time the session started and session ID.
- Release all sessions.

Procedure

- Step 1** Select **Admin > AAA Administration > Sessions**.
- Result: A list of all the currently active sessions is displayed.
- Step 2** To query for a session, enter a session ID or username.
- The Username, Time, and Session ID of the query or the message that no session was found is displayed. The Username is the RADIUS username. The Time is the time the session began.
 - To release the session, Click **Release**.
 - To return to the main Sessions page, click **Cancel**.
- Step 3** To release all sessions, select **Release All**.
-

Related Topics

- [About the AAA Server, page 18-1](#)
- [Configuring the AAA Server—Overview, page 18-6](#)

Using AAA Server Log Files

The AAA server log files, and log files for other WLSE functions can be accessed through **Admin > Appliance > Status > View Log File**. For detailed information on how to download, search, and email log files (and information about other WLSE log files), see [Using WLSE Log Files, page 16-4](#).

Table 18-9 Log Files for the Internal AAA Server

Log File	Content
AAA-accounting.log	Formatted accounting records received from the access points, generated for each accounting request. For example: Mon, 26 Jan 2004 12:12:56 User-Name = user1 NAS-IP-Address = 127.0.0.1 NAS-Port = 1 Framed-IP-Address = 1.1.1.1 Called-Station-Id = 14085271703 Calling-Station-Id = 14085271703 NAS-Identifier = localhost Acct-Status-Type = Stop Acct-Session-Id = 1
AAA-cli.log	Information on AAA server CLI commands that have been executed.
AAA-daemon-manager.log	Output from watchdog and AAA database daemon processes.
AAA-database.log	Information on AAA database activity.
AAA-server-trace.log	Output from AAA server tracing, when tracing is enabled.
AAA-server.log	Output from RADIUS daemon processes.
AAA-status.log	Startup and shutdown history of AAA processes. Also, AAA server installation and deinstallation history.

Monitoring the AAA Server

You can use the WLSE's fault-monitoring feature to monitor a single protocol on the AAA server (either RADIUS, Cisco-PEAP, or LEAP).

The WLSE does not monitor MS-PEAP or EAP-FAST on the WLSE's built-in AAA server.

A given WLSE can only monitor one protocol per AAA server.

The WLSE monitors the following for the selected protocol:

- Server availability
- Server state (for example, degraded, overloaded, or OK)
- Server authentication errors


After configuring the AAA server and the WLSE as described in the following procedure, you can monitor the performance of the internal AAA server by selecting **Faults > Display Faults** and view reports about the AAA server by selecting **Reports > Trends**. For more information on faults and reports, see [Chapter 3, "Fault Monitoring"](#) and [Chapter 10, "Using Reports."](#)



Note

The WLSE must also be added to the AAA server as a client.

Procedure

-
- Step 1** You will need the name and password of a WLSE user. If necessary, add a user—see [Managing GUI Users, page 16-51](#). You will need this data in Steps 3 and 4.
- Step 2** Select **Admin > AAA Administration > Clients**.
Add the WLSE as a client.
- Step 3** Add the WLSE user to the user database:
- If you are using the local database for users, add the WLSE user to the list of AAA server users under **Admin > AAA Administration > Users**.
 - If you are using LDAP, add the WLSE user to the LDAP database of users.
- Step 4** Select **Devices > Discover > AAA Server**:
- a. Select RADIUS from the Server Type list.
 - b. Enter the hostname or IP address of the WLSE in the Server Name field.
 - c. Enter 1812 in the Server Port field.
 - d. Enter the username and password of the WLSE user from Step 1 in the Username and Password fields.
 - e. Enter the shared secret of the WLSE in the Secret field.
This is the shared secret that you entered when adding the WLSE as a client of the AAA server.
 - f. Click **Save**.
- Step 5** If the WLSE is a member of a redundant pair, repeat Step 4 for the second WLSE.
- Step 6** Select **Faults > Manage Fault Settings**:
- a. Select the Default profile, then click **Edit**.
 - b. Select **AAA SERVER > RADIUS Response Time**.
 - c. Select **Enable**.
 - d. Set the Poll Interval to 1 minute.
 - e. Set consecutive polling cycles to 2 for the “Server is unavailable” Setting.
-  **Note** Leave the consecutive polling cycles at the default of 1 for the remaining settings in this window.
-
- f. Click **Apply**.
-

Related Topics

- [Configuring the AAA Server—Overview, page 18-6](#)
- [Monitoring AAA Servers, page 4-15](#)

Using AAA Server CLI Commands

This section provides details on the AAA server CLI commands. [Table 18-10 on page 18-30](#) lists all of the commands. Most of the features provided in the Web interface are also available via CLI commands. Some functions that are not provided in the Web interface are provided through CLI commands; such as generating self-signed certificates, configuring logging method, reinitializing the database, and starting or stopping daemons.

For general information about using WLSE CLI commands, see [Appendix A, “Command Line Interface \(CLI\) Commands.”](#)

When AAA server CLI are executed, these events are logged in the AAA-cli.log. You can access this log from **Admin > Appliance > Status > View Log File**.

Table 18-10 AAA Server CLI Commands

Command	Privilege Level	Description	Reference
aaa-server cisco-peap	15	Configures PEAP server on the AAA server.	aaa-server cisco-peap, page 18-32
aaa-server client	15	Manages AAA server clients.	aaa-server client, page 18-33
aaa-server domain-auth	15	Configures WDC domain authentication.	aaa-server domain-auth, page 18-34
aaa-server eap-fast	15	Configures EAP-FAST.	aaa-server eap-fast, page 18-35
aaa-server eap-tls	15	Configures EAP-TLS.	aaa-server eap-tls, page 18-37
aaa-server ldap	15	Configures LDAP server parameters on the AAA server.	aaa-server ldap, page 18-37
aaa-server leap	15	Specifies AAA service to use after LEAP negotiation.	aaa-server leap, page 18-39
aaa-server logging	15	Configures AAA server logging (local or syslog).	aaa-server logging, page 18-40
aaa-server ms-peap	15	Configures MS-PEAP.	aaa-server ms-peap, page 18-41
aaa-server reinit	15	Reinitializes AAA server database.	aaa-server reinit, page 18-42
aaa-server session	15	Deletes or displays current AAA server sessions.	aaa-server session, page 18-43
aaa-server start	15	Starts or stops AAA server daemons.	aaa-server start, page 18-43
aaa-server status	15	Displays status of AAA server.	aaa-server status, page 18-44

Table 18-10 AAA Server CLI Commands (continued)

aaa-server trace	15	Sets or displays the AAA server trace level.	aaa-server trace, page 18-44
aaa-server user	15	Manages AAA server users (access points).	aaa-server user, page 18-45
aaa-server usergroup	15	Manages user groups for Windows domain authentication.	aaa-server usergroup, page 18-45

aaa-server cisco-peap

This command displays and configures Cisco PEAP parameters: the server's password, certificates and RSA private key, and AAA service to use after PEAP negotiation.

Syntax Description

<pre>aaa-server cisco-peap private-key-password <i>password</i> aaa-server cisco-peap private-key-password</pre>	<p>Sets or displays server's private key password for PEAPv1.</p>
<pre>aaa-server cisco-peap inner-service aaa-server cisco-peap inner-service { ldap local domain-auth }</pre>	<p>Displays or specifies the service to use after LEAP negotiation. This command specifies the location of user information for authentication and authorization. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user.</p> <ul style="list-style-type: none"> • local—authenticates against user information stored locally. This is the default. Enter the users in the AAA server. • LDAP—authenticates against user information on the LDAP server. This is the default. • domain-auth—authenticates against user information stored in an Active Directory database on a Windows Domain Controller.
<pre>aaa-server cisco-peap mkcert</pre>	<p>Generates a self-signed certificate. A self-signed certificate is automatically generated by the WLSE, but you can use this command to generate another one if you need to make changes. This command is interactive, and requests the following optional information: country, organization and organizational unit, and server or installation name.</p>

Related Commands

[aaa-server user](#), page 18-45

[aaa-server domain-auth](#), page 18-34

[aaa-server ldap](#), page 18-37

aaa-server client

This command adds, deletes, and displays clients or resets a client's parameters. The clients of the AAA server might be infrastructure access points (if not using WDS) or WDS devices. The WLSE itself should be added as a client of the AAA server if you will use the WLSE to monitor the AAA server.

Syntax Description

aaa-server client	Displays all properties of all clients: name, IP address, shared secret, and authorization type.
aaa-server client <i>name</i>	Displays name, IP address, shared secret, and authorization type for a client.
aaa-server client <i>name</i> ip-address <i>ip-address</i> secret <i>secret</i>	<p>Adds a client or resets a client's IP address, shared secret, and authorization type.</p> <ul style="list-style-type: none"> <i>name</i> is chosen by the administrator to identify the client and must be a single string, without spaces or surrounding quotation marks. <i>secret</i> is a single string, without spaces or surrounding quotation marks. <i>ip-address</i> can be a single IP address, or can include ranges and the * wildcard. <p>All arguments are required. The properties are overwritten if a client exists with the same name.</p>
no aaa-server client <i>name</i>	Deletes a client.

Examples

This command adds a client. All arguments are required.

```
aaa-server client ap001 ip-address 10.10.10.1 secret boo
aaa-server client ap001 ip-address 10.10.10.1 secret boo
```

This command displays information about a client:

```
aaa-server client
aaa-server client ap001 ip-address 10.10.10.1 secret boo
```

aaa-server domain-auth

This command configures the domain authentication/authorization service. Configure this service if you are using Windows Domain Controller/Active Directory (WDC/AD) as your user database for the AAA server.

Syntax Description

aaa-server domain-auth host-name <i>ad-host-name</i>	Sets or displays the hostname of the WDC/AD server. <i>ad-host-name</i> must be a single string, without spaces or surrounding quotation marks.
aaa-server domain-auth port <i>portnumber</i>	Sets the port number. Must be a valid number between 1 and 65535.
aaa-server domain-auth port	Displays the port number.
aaa-server domain-auth defaultusergroup <i>group-name</i>	Sets the default user group name (must be the name of an existing group), displays the default user group name, or clears the default user group.
no aaa-server domain-auth defaultusergroup	To create a default AAA user group, use the aaa-server usergroup command.
aaa-server domain-auth groupmap <i>group-name=windows-group-names</i>	Maps a single AAA group to one or more WDC/AD groups. The group name must be an existing group. If you are listing more than one WDC/AD group, separate the group names by commas. The group mapping feature is used to assign RADIUS attributes to groups of users stored in an Active Directory database on a Windows Domain Controller. To create AAA groups, use the aaa-server usergroup command.
no aaa-server domain-auth groupmap <i>groupnum</i>	Removes a group mapping. <i>groupnum</i> must be valid group number. To obtain group numbers, use the following command to display all of the group mappings.
aaa-server domain-auth groupmap	Displays group mappings.

Usage Guidelines

Use the [aaa-server usergroup](#) command to define AAA user groups.

Examples

To display the hostname of the active directory server:

```
aaa-server domain-auth host-name
aaa-server domain-auth host-name adhost
```

To add group mappings:

```
aaa-server domain-auth groupmap aaagroup1=wingroup2,wingroup3
```

To display group mappings:

```
aaa-server domain-auth groupmap
  1. aaagroup1=wingroup2,wingroup3
  2. aaagroup2=wingroup3,wingroup4
```

To remove a group mapping:

```
no aaa-server domain-auth groupmap 1
```

Related Commands

[aaa-server usergroup](#), page 18-45

aaa-server eap-fast

This command configures EAP-FAST parameters.

Syntax Description

aaa-server eap-fast always-authenticate { true false } aaa-server eap-fast always-authenticate	Sets or displays the flag indicating whether provisioning should always roll over into authentication without relying on a separate session. Most environments (including wireless) perform better when this parameter is set to true.
aaa-server eap-fast authority-identifier <i>name</i> aaa-server eap-fast authority-identifier	Sets or displays the authority identifier. <i>name</i> must be a single string, without spaces or quotation marks.
aaa-server eap-fast authority information <i>description</i> aaa-server eap-fast authority information	Sets or displays the authority information. <i>description</i> is human-readable descriptive text for this credential issuer and may be displayed to the client for identification purposes. If the description contains spaces, it must be surrounded by double-quotes.
aaa-server eap-fast credential lifetime <i>lifetime</i> aaa-server eap-fast credential lifetime	Sets or displays the credential lifetime. <i>lifetime</i> is specified as a string consisting of pairs of numbers and units. Units may be one of the following: <ul style="list-style-type: none"> • M, minute, or minutes • H, hour, or hours • D, day, or days • W, week or week If the credential never expires, specify <i>lifetime</i> as forever. If lifetime contains spaces, it must be surrounded by double-quotes.

<pre>aaa-server eap-fast inner service [ldap local domain-auth] aaa-server eap-fast inner service</pre>	<p>Sets or displays the service to use after LEAP negotiation. This determines the location of user information for authentication and authorization. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user.</p> <ul style="list-style-type: none"> • local—authenticates against user information stored locally. Enter the users in the AAA server. • LDAP—authenticates against user information on the LDAP server. This is the default. • domain-auth—authenticates against user information stored in an Active Directory database on a Windows Domain Controller.
<pre>aaa-server eap-fast adhp-mode [anonymous signed]</pre>	<p>Sets or displays the ADHP (provisioning) mode. Only anonymous is supported.</p>

Examples

To set the authority information:

```
aaa-server eap-fast authority-information "some descriptive text"
aaa-server eap-fast authority-information "some descriptive text"
```

To set the credential lifetime:

```
aaa-server eap-fast credential-lifetime "8 days 4 hours"
aaa-server eap-fast credential-lifetime "8 days 4 hours"
```

```
aaa-server eap-fast credential-lifetime forever
aaa-server eap-fast credential-lifetime forever
```

Related Commands

[aaa-server domain-auth, page 18-34](#)

[aaa-server user, page 18-45](#)

[aaa-server ldap, page 18-37](#)

aaa-server eap-tls

This command sets EAP-TLS parameters.

Syntax Description

aaa-server eap-tls private-key-password <i>password</i>	Sets or displays the server's private key password. The password must be a single string, without spaces or surrounding quotation marks.
aaa-server eap-tls private-key-password	
aaa-server eap-tls mkcert	Generates a self-signed certificate. A self-signed certificate is automatically generated by the WLSE, but you can use this command to generate another certificate if you need to make changes. This command is interactive, and requests the following optional information: country, organization and organizational unit, and server or installation name.

aaa-server ldap

This command configures [LDAP](#) server parameters.

Syntax Description

In the following commands, specify **local** for the LDAP local server or **central** for the LDAP central server.

aaa-server ldap	Displays LDAP settings for both the central and local LDAP servers.
aaa-server ldap { local central }	Displays LDAP settings for either the local or central server.
aaa-server ldap { local central } timeout <i>timeout</i>	Sets or displays the timeout (in seconds) for bind attempts or displays current timeout setting, how long the AAA server waits for a response from the LDAP server.
aaa-server ldap { local central } timeout	
aaa-server ldap { local central } host-name [<i>ipaddr hostname</i>]	Sets or displays hostname or IP address of the LDAP server. The hostname must be all lower-case. The hostname is not checked to make sure it is a valid hostname.
aaa-server ldap { local central } host-name	
aaa-server ldap { local central } port <i>portnumber</i>	Sets or displays port of the LDAP server. The port number must be an integer between 1 and 65536. The validity of the number is not checked.
aaa-server ldap { local central } port	
aaa-server ldap { local central } bind-name <i>bindname</i>	Sets or displays administrator name with which to bind. The bindname must be a single string, without spaces or surrounding quotation marks.
aaa-server ldap { local central } bind-name	

<pre>aaa-server ldap { local central } bind-password <i>password</i> aaa-server ldap { local central } bind-password</pre>	<p>Sets or displays (in clear text) administrator password with which to bind. The password must be a single string, without spaces or surrounding quotation marks.</p>
<pre>aaa-server ldap { local central } search-path <i>path</i> aaa-server ldap { local central } search-path</pre>	<p>Sets or displays root of the search tree in LDAP. The path must be a single string, without spaces or surrounding quotation marks.</p>
<pre>aaa-server ldap { local central } search-filter [<i>filter</i>] aaa-server ldap { local central } search-filter</pre>	<p>Sets or displays the search filter (uid=%s), where uid is the name of the LDAP property that contains the same values as the RADIUS User Name attributes that are being authenticated.</p> <p>The search filter must be in the form “(somename=%s)”. The value must be surrounded by double quotes, and spaces are not allowed. The LHS (somename) is not validated.</p>
<pre>aaa-server ldap { local central } user-password [<i>property-name</i>] aaa-server ldap { local central } user-password</pre>	<p>Sets or displays LDAP property name that contains user passwords. The property name must be a single string, without spaces or surrounding quotation marks. Must be a property of all objects that match the search path.</p>
<pre>aaa-server ldap { local central } use-ssl [true false] aaa-server ldap { local central } use-ssl</pre>	<p><i>This option has not been implemented and will be removed in a future release.</i></p>
<pre>aaa-server ldap { local central } user-password-encryption { dynamic none crypt sha-1 ssha-1 } aaa-server ldap { local central } user-password-encryption</pre>	<p>Sets or displays the encryption style for the user password property:</p> <p>dynamic—instructs the AAA server to choose the encryption mechanism on a case-by-case basis after the server determines the presence of a known prefix, which the server prepends to the password attribute.</p> <p>none—no encryption (the default).</p> <p>crypt—AAA server encryption using the Unix crypt algorithm.</p> <p>sha-1 or ssha-1—Secure Hash Algorithm; a hashing algorithm that produces a 160-bit digest based upon the input. The algorithm produces SHA passwords that are irreversible or prohibitively expensive to reverse. Enables the AAA server to authorize users whose passwords are stored in an LDAP server and hashed by using the SHA-1 encoding scheme. SSHA-1 is Netscape's (iPlanet) enhancement of the SHA-1 algorithm which includes salted password data.</p>

<pre> aaa-server ldap { local central } attribute-mapping aaa-server ldap { local central } attribute-mapping <i>ldap-property</i> [<i>radius-attribute</i>] no aaa-server ldap { local central } attribute-mapping <i>ldap-property</i> </pre>	<p>Adds, resets, or displays mapping between an LDAP property and a RADIUS authorization attribute.</p> <p>The no form deletes the mapping.</p> <p>For information on AAA server attributes, see RADIUS Attributes for the AAA Server, page 18-46</p>
--	---

Examples

To display all of the properties of the local LDAP server:

```

aaa-server ldap local
host-name = 127.0.0.1
  port = 389
  bind-name =
  bind-password =
  search-path = o=cisco.com
  search-filter = (uid=%s)
  user-password = userpassword
  user-password-encryption = Dynamic
  timeout = 15
  use-ssl = FALSE
  attribute-mapping =

```

To set the timeout for bind attempts (in seconds) on the central LDAP server:

```

aaa-server ldap central timeout 15
aaa-server ldap central timeout 15

```

To display the root of the search tree in LDAP:

```

aaa-server ldap local search-path
aaa-server ldap local search-path o-cisco.com

```

To set the search filter:

```

aaa-server ldap local search-filter "(top=%s)"
aaa-server ldap local search-filter (top=%s)

```

aaa-server leap

To specify or display the AAA service to use after LEAP negotiation, use the following command:

```

aaa-server leap inner-service
aaa-server leap inner-service { ldap | local | domain-auth }

```

Syntax Description

Specify the service to use after LEAP negotiation. This specifies the location of user information for authentication and authorization. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user.

- **local**—authenticates against user information stored locally. This is the default. Enter the users in the AAA server.

- **LDAP**—authenticates against user information on an LDAP server.
- **domain-auth**—authenticates against user information in an Active Directory database on a Windows domain controller.

Example

To display information about the currently configured AAA service to use after LEAP negotiation, use the following command:

```
aaa-server leap inner-service
aaa-server leap inner-service local
```

Related Commands

[aaa-server domain-auth, page 18-34](#)

[aaa-server ldap, page 18-37](#)

[aaa-server user, page 18-45](#)

aaa-server logging

The following commands configure syslog and local logging for the AAA server. Syslog logging is disabled by default. Local logging is enabled by default.

Syslog logging requires a UNIX host running a syslog daemon as a receiver for the AAA messages.

Syntax Description

aaa-server logging	Displays current values for logging: <ul style="list-style-type: none"> • Whether syslog and local logging are enabled. • Syslog server IP address and facility local number, if configured.
aaa-server logging syslog no aaa-server logging syslog	Enables or disables syslog logging. Causes the AAA server to stop and restart.
aaa-server logging local no aaa-server logging local	Enables or disables local logging. Causes the AAA server to stop and restart.
aaa-server logging syslog ip-address <i>address</i> aaa-server logging syslog ip-address	Sets or displays the current IP address used by the syslog server.
aaa-server logging syslog facility-local-number <i>number</i> aaa-server logging syslog facility-local-number	Sets or displays the syslog facility local number. The number must be in the range 0-16. If the facility local number is changed and syslog is enabled, the AAA server will be restarted.

Usage Guidelines



Note

The AAA server stops before modifications to logging settings are made and restarts afterward.

Multiple settings cannot be combined into one command.

Syslog logging will not work unless you provide both the server IP address and facility local number.

Syslog logging and local logging are independent of each other.

Example

The following command shows that syslog logging is disabled and local logging is enabled:

```
aaa-server logging
no aaa-server logging syslog
aaa-server logging local
```

The following command stops local logging and restarts the AAA server:

```
no aaa-server logging local
no aaa-server logging local
restarting the AAA server...
```

The following command changes the syslog facility local number and restarts the AAA server:

```
aaa-server logging syslog facility-local-number 10
aaa-server logging syslog facility-local-number 10
restarting the AAA server...
```

aaa-server ms-peap

The following commands configure MS-PEAP.

Syntax Description

aaa-server ms-peap private-key-password <i>password</i>	Sets or displays the server's private key password for PEAPv0. The password must be a single string without spaces or quotation marks. The password must match the ServerRSAKeyFile certificate file.
aaa-server ms-peap private-key-password	

aaa-server ms-peap inner service [ldap local domain-auth]	<p>Specifies the service to use after LEAP negotiation. This determines the location of user information for authentication and authorization. When the AAA server receives a request, it directs the request to the specified service. Then the service looks up the user and authenticates or authorizes the user.</p> <ul style="list-style-type: none"> • local—authenticates against user information stored locally. Enter the users in the AAA server. • LDAP—authenticates against user information on the LDAP server. This is the default. • domain-auth—authenticates against user information stored in an Active Directory server on a Windows domain controller.
aaa-server ms-peap mkcert	<p>Generates a self-signed certificate. A self-signed certificate is automatically generated by the WLSE, but you can use this command to generate another certificate if you need to make changes. This command is interactive, and requests the following optional information: country, organization and organizational unit, and server or installation name.</p>

Related Commands

[aaa-server user, page 18-45](#)

[aaa-server ldap, page 18-37](#)

[aaa-server domain-auth, page 18-34](#)

aaa-server reinit

The following command reinitializes the AAA server database to its starting configuration:

```
aaa-server reinit
```

Example

To reinitialize the AAA server database:

```
aaa-server reinit
```

```
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" started Thu Dec 30 02:00:21
2004
```

```
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" finished Thu Dec 30 02:00:21
2004
```

```
Waiting for these processes to die (this may take some time):
```

```
AAA server running (pid: 1374)
```

```
AAA daemon manager running (pid: 1309)
```

```
AAA database lock running (pid: 1316)
```

```
AAA database running (pid: 1315)
```

```
4 processes left.....k2 processes left.0 processes left
```

```
AAA Daemon Manager shutdown complete.
```

```
# execute /opt/CSCOar/conf/add-on/pre-fixup-symlink
Starting AAA Daemon Manager..completed.
```

Usage Guidelines

This command causes AAA server processes to stop and then restart.

aaa-server session

The following commands delete or display current sessions. If no name or session ID is specified, all sessions are listed.

Syntax Description

no aaa-server session <i>name</i>	Deletes a session.
no aaa-server session	Deletes all sessions.
aaa-server session	Displays all sessions.
aaa-server session <i>name</i>	Displays the named session.
aaa-server session id <i>id</i>	Displays a session by session identifier.
no aaa-server session id <i>id</i>	Deletes a session by session identifier.

Example

To display all current sessions:

```
aaa-server session
aaa-server session ap008 id 1 start-time 02/14/1990 15:38.54
aaa-server session ap005 id 2 start-time 02/15/1990 05:10:40
aaa-server session ap005 id 3 start-time 02/15/1990 05:11:14
```

aaa-server start

The following command starts or stops the AAA server daemons:

```
aaa-server { start | stop }
```

Usage Guidelines

If the AAA server is already up and you attempt to start it, the following messages are displayed:

```
aaa-server start
WARNING: Some AAA Server components are already running.

AAA server running           (pid: 1374)
AAA daemon manager running  (pid: 1309)
AAA database lock running    (pid: 1316)
AAA database running         (pid: 1315)
```

Use "aaa-server stop" to terminate these processes.

Nothing started.

If you attempt to stop the AAA server and another user is active and running a CLI command, for example, the following is displayed:

```
aaa-server stop
WARNING: You can not shut down AAA server while the
CLI is being used. Current list of running CLI with process id is:
26342 aregcmd
Shutdown failed.
```

Related Commands

[aaa-server status, page 18-44](#)

aaa-server status

The following command displays the status of the AAA server:

```
aaa-server status
```

Example

Example output:

```
aaa-server status
AAA server running (pid: 1127)
AAA daemon manager running (pid: 1111)
AAA database running (pid: 1117)
AAA database lock running (pid: 1118)
```

Related Commands

[aaa-server start, page 18-43](#)

aaa-server trace

The following command sets or displays the trace level:

```
aaa-server trace [ 0 | 1 | 2 | 3 | 4 | 5 ]
```

There are 6 levels of tracing; 0 means no tracing; 5 is complete tracing (most verbose).

For more information about trace levels, see [Trace Levels and Information Logged, page 18-10](#).

Usage Guidelines

Trace output can only be viewed in the Web interface. Select **Administration > Appliance > View Log Files** and view AAA-server-trace.log.

aaa-server user

The following commands configure, delete, or modify AAA server users in the local user database. AAA server users are the infrastructure access points (the access points that register with the WDS access point).

Syntax Description

aaa-server user <i>name</i> password <i>password</i>	Adds user or resets name or password of user. The name and password must be a single string, without spaces or surrounding quotation marks. User names can be up to 255 characters in length and any character is allowed, except for the forward slash (/).
no aaa-server user <i>name</i>	Deletes a user.
aaa-server user	Displays all properties of all users.
aaa-server user <i>name</i>	Displays properties of named user.
aaa-server user <i>name</i> attribute <i>radius-attr</i> <i>value</i>	Adds or resets a RADIUS authorization attribute of the user. All arguments are required. <ul style="list-style-type: none"> <i>name</i> must be an existing user. <i>radius-attr</i> must be an existing attribute. For information on the native attributes, see RADIUS Attributes for the AAA Server, page 18-46. <i>value</i> must be a single string, with no spaces or surrounding quotation marks. If the attribute is already defined for this user, the previous value is overwritten.
no aaa-server user <i>name</i> attribute <i>radius-attr</i>	Deletes RADIUS attribute from an existing user.

Examples

The following command displays all users:

```
aaa-server user
aaa-server user ap008 password <encrypted>
aaa-server user ap005 password <encrypted>
  attributes =
    Framed-Ip-Address = 1.1.11.1
```

The following example command displays a single user:

```
aaa-server user ap008
aaa-server user ap008 password <encrypted>
```

aaa-server usergroup

The following commands display, add, modify or delete AAA server user groups. These groups are mapped to WDC/AD groups for authorizing users. To map AAA groups to WDC/AD groups, use the [aaa-server domain-auth](#) command.

aaa-server usergroup	Displays all properties of all user groups.
aaa-server usergroup <i>name</i>	Creates a user group. Group names can be up to 255 characters in length and any character is allowed, except for the forward slash (/).
no aaa-server usergroup <i>name</i>	Deletes a user group.
aaa-server usergroup <i>name</i> attribute <i>radius-attr value</i>	Adds a RADIUS authorization attribute to an existing user group. <ul style="list-style-type: none"> <i>name</i> must be an existing user group. <i>radius-attr</i> must be an attribute native to the AAA server. For information on RADIUS attributes, see RADIUS Attributes for the AAA Server, page 18-46. <i>value</i> must be a single string; spaces and quotation marks are not allowed.
no aaa-server usergroup <i>name</i> attribute <i>radius-attr value</i>	Deletes RADIUS authorization attribute from a user group.

Examples

To display user groups:

```
aaa-server usergroup
  aaa-server usergroup aaagroup1
    attributes =
      user-name = buster
      called-station-id = 77
  aaa-server usergroup aaagroup2
```

To add an attribute to an existing user group:

```
aaa-server usergroup aaagroup1 attribute called-station-id 77
```

Related Commands

[aaa-server domain-auth, page 18-34](#)

RADIUS Attributes for the AAA Server

This section lists the RADIUS attributes supported by the internal AAA server. RADIUS attributes carry the specific authentication and authorization information, and configuration details for requests and replies.

All RADIUS requests and responses consist of one or more attributes, such as the user's name, user's password, and type of service the client should provide to the user.

The attribute dictionary contains prefigured authentication, authorization, and accounting attributes that can be part of a client's or user's configuration. The dictionary entries translate an attribute into a value the AAA server uses to parse incoming requests and generate responses.

Each vendor has its own list of supported attributes. See the vendor's documentation for information about these attributes.

For more detailed information about specific attributes, refer to the appropriate RFC as listed in [Table 18-11](#). You can find RFCs on the world wide web at www.ietf.org.

This section contains the following information:

- List of all attributes of the internal AAA server—See [Table 18-12 on page 18-47](#).
- How to set tunnel attributes—See [Setting Tunnel Attributes, page 18-50](#).

Table 18-11 RFCs for RADIUS Attributes

RFC Subject	RFC Number
Standard RADIUS Attributes	2865
RADIUS Accounting Attributes	2866
Accounting Modifications for Tunnel Protocol Support	2867
Attributes for Tunnel Protocol Support	2868
RADIUS Extensions	2869
RADIUS for IPv6	3162

The standard, non vendor-specific RADIUS attributes supported by the AAA server are listed in [Table 18-12](#).

Table 18-12 RADIUS Attributes Supported by the AAA Server

Attribute Name	Attribute Number
Acct-Authentic	45
Acct-Delay-Time	41
Acct-Input-Gigawords	52
Acct-Input-Octets	42
Acct-Input-Packets	47
Acct-Interim-Interval	85
Acct-Link-Count	51
Acct-Multi-Session-Id	50
Acct-Output-Gigawords	53
Acct-Output-Octets	43
Acct-Output-Packets	48
Acct-Session-Id	44
Acct-Session-Time	46
Acct-Status-Type	40
Acct-Terminate-Cause	49
Acct-Tunnel-Connection	68
Acct-Tunnel-Packets-Lost	86
Acquire-group-session-limit	280
ARAP-Challenge-Response	84

Table 18-12 RADIUS Attributes Supported by the AAA Server (continued)

Attribute Name	Attribute Number
ARAP-Features	71
ARAP-Password	70
ARAP-Security	73
ARAP-Security-Data	74
ARAP-Zone-Access	72
Callback-Id	20
Callback-Number	19
Called-Station-Id	30
Calling-Station-Id	31
Change-Password	17
CHAP-Challenge	60
CHAP-Password	3
Class	25
Configuration-Token	78
Connect-Info	77
Digest-Attributes	207
Digest-Response	206
EAP-Message	79
Error-Cause	101
Event-Timestamp	55
Filter-Id	11
Framed-AppleTalk-Link	37
Framed-AppleTalk-Network	38
Framed-AppleTalk-Zone	39
Framed-Compression	13
Framed-Interface-Id	96
Framed-IP-Address	8
Framed-IP-Netmask	9
Framed-IPv6-Pool	100
Framed-IPv6-Prefix	97
Framed-IPv6-Route	99
Framed-IPX-Network	23
Framed-MTU	12
Framed-Pool	88
Framed-Protocol	7
Framed-Route	22

Table 18-12 RADIUS Attributes Supported by the AAA Server (continued)

Attribute Name	Attribute Number
Framed-Routing	10
Idle-Timeout	28
Login-IP-Host	14
Login-IPv6-Host	98
Login-LAT-Group	36
Login-LAT-Node	35
Login-LAT-Port	63
Login-LAT-Service	34
Login-Service	15
Login-TCP-Port	16
Message-Authenticator	80
NAS-Identifier	32
NAS-IP-Address	4
NAS-IPv6-Address	95
NAS-Port	5
NAS-Port-ID	87
NAS-Port-Type	61
Originating-Line-Info	94
Password-Expiration	21
Password-Retry	75
Port-Limit	62
Prompt	76
Proxy-State	33
Reply-Message	18
Service-Type	6
Session-Timeout	27
State	24
Termination-Action	29
Text-Ascend-Data-Filter	225

Table 18-12 RADIUS Attributes Supported by the AAA Server (continued)

Attribute Name	Attribute Number
For special instructions on setting the following tunnel attributes, see Setting Tunnel Attributes , page 18-50.	
Tunnel-Assignment-ID	82
Tunnel-Client-Auth-ID	90
Tunnel-Client-Endpoint	66
Tunnel-Medium-Type	65
Tunnel-Password	69
Tunnel-Preference	83
Tunnel-Private-Group-ID	81
Tunnel-Server-Auth-ID	91
Tunnel-Server-Endpoint	67
Tunnel-Type	64
User-Name	1
User-Password	2
Vendor-Specific Attributes	26

Setting Tunnel Attributes

When using the tunnel attributes listed in [Table 18-13 on page 18-50](#), attach a tag consisting of `_tag` followed by a value from 1 to 31. For example, Tunnel-Client-Endpoint_tag3.

Table 18-13 Tunneling Attributes Supported by the AAA Server

Attribute Number	Attribute
64	Tunnel-Type
65	Tunnel-Medium-Type
66	Tunnel-Client-Endpoint
67	Tunnel-Server-Endpoint
69	Tunnel-Password
81	Tunnel-Private-Group-ID
82	Tunnel-Assignment-ID
83	Tunnel-Preference
90	Tunnel-Client-Auth-ID
91	Tunnel-Server-Auth-ID