



CHAPTER 14

Configuring AAA Servers and the Local Database

This chapter describes support for AAA (pronounced “triple A”) and how to configure AAA servers and the local database.

This chapter includes the following sections:

- [Information About AAA, page 14-1](#)
- [Configuring AAA Server Groups, page 14-7](#)
- [Testing Server Authentication and Authorization, page 14-14](#)
- [Adding a User Account, page 14-14](#)
- [Configuring LDAP Attribute Maps, page 14-15](#)
- [Adding an Authentication Prompt, page 14-16](#)

Information About AAA

AAA enables the FWSM to determine who the user is (authentication), what the user can do (authorization), and what the user did (accounting).

AAA provides an extra level of protection and control for user access than using access lists alone. For example, you can create an access list allowing all outside users to access Telnet on a server on an inside interface. If you want only some users to access the server and you might not always know IP addresses of these users, you can enable AAA to allow only authenticated and/or authorized users to make it through the FWSM. (The Telnet server enforces authentication, too; the FWSM prevents unauthorized users from attempting to access the server.)

You can use authentication alone or with authorization and accounting. Authorization always requires a user to be authenticated first. You can use accounting alone, or with authentication and authorization.

If you use multiple security contexts, AAA settings are discrete per context, not shared between contexts. This provides you the opportunity to control access, authorize resources and commands, and perform accounting differently among contexts.

This section includes the following topics:

- [About Authentication, page 14-2](#)
- [About Authorization, page 14-2](#)
- [About Accounting, page 14-2](#)
- [AAA Server and Local Database Support, page 14-3](#)

About Authentication

Authentication controls access by requiring valid user credentials, which are typically a username and password. You can configure the FWSM to authenticate the following items:

- All administrative connections to the FWSM including the following sessions:
 - Telnet
 - SSH
 - Serial console
 - ASDM (using HTTPS)
 - VPN management access
- The **enable** command
- Network access

About Authorization

Authorization controls access *per user* after users authenticate. You can configure the FWSM to authorize the following items:

- Management commands
- Network access
- VPN access for management connections

Authorization controls the services and commands available to each authenticated user. Were you not to enable authorization, authentication alone would provide the same access to services for all authenticated users.

If you need the control that authorization provides, you can configure a broad authentication rule, and then have a detailed authorization configuration. For example, you authenticate inside users who attempt to access any server on the outside network and then limit the outside servers that a particular user can access using authorization.

The FWSM caches the first 16 authorization requests per user, so if the user accesses the same services during the current authentication session, the FWSM does not resend the request to the authorization server.

About Accounting

Accounting tracks traffic that passes through the FWSM, enabling you to have a record of user activity. If you enable authentication for that traffic, you can account for traffic per user. If you do not authenticate the traffic, you can account for traffic per IP address. Accounting information includes when sessions start and stop, username, the number of bytes that pass through the FWSM for the session, the service used, and the duration of each session.

AAA Server and Local Database Support

The FWSM supports a variety of AAA server types and a local database that is stored on the FWSM. This section describes support for each AAA server type and the local database.

This section contains the following topics:

- [Summary of Support, page 14-3](#)
- [RADIUS Server Support, page 14-4](#)
- [TACACS+ Server Support, page 14-4](#)
- [Local Database Support, page 14-6](#)
- [NT Server Support, page 14-5](#)
- [Kerberos Server Support, page 14-6](#)
- [LDAP Server Support, page 14-6](#)
- [Local Database Support, page 14-6](#)

Summary of Support

[Table 14-1](#) summarizes the support for each AAA service by each AAA server type, including the local database. For more information about support for a specific AAA server type, see the topics following the table.

Table 14-1 Summary of AAA Support

AAA Service	Database Type						
	Local	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP
Authentication of . . .							
VPN users ¹	Yes	Yes	Yes	Yes	Yes	Yes	No
Firewall sessions	Yes	Yes	Yes	No	No	No	No
Administrators	Yes	Yes	Yes	No	No	No	No
Authorization of . . .							
VPN users ¹	Yes	Yes	No	No	No	No	Yes
Firewall sessions	No	Yes ²	Yes	No	No	No	No
Administrators	Yes ³	No	Yes	No	No	No	No
Accounting of . . .							
VPN connections ¹	No	Yes	Yes	No	No	No	No
Firewall sessions	No	Yes	Yes	No	No	No	No
Administrators	No	No	Yes	No	No	No	No

1. VPN is available for management connections only.
2. For firewall sessions, RADIUS authorization is supported with user-specific access lists only, which are received or specified in a RADIUS authentication response.
3. Local command authorization is supported by privilege level only.

RADIUS Server Support

The FWSM supports RADIUS servers.

This section contains the following topics:

- [Authentication Methods, page 14-4](#)
- [Attribute Support, page 14-4](#)
- [TACACS+ Server Support, page 14-4](#)

Authentication Methods

The FWSM supports the following authentication methods with RADIUS:

- PAP
- CHAP
- MS-CHAPv1
- MS-CHAPv2

MS-CHAPv2 supports password management when the RADIUS server communicates with a Windows Active Directory server. When your password expires, you are prompted to change your password (see the **auth-prompt** command).

Attribute Support

The FWSM supports the following sets of RADIUS attributes:

- Authentication attributes defined in RFC 2138.
- Accounting attributes defined in RFC 2139.
- RADIUS attributes for tunneled protocol support, defined in RFC 2868.
- Cisco IOS VSAs, identified by RADIUS vendor ID 9.
- Cisco VPN-related VSAs, identified by RADIUS vendor ID 3076.
- Microsoft VSAs, defined in RFC 2548.

RADIUS Authorization Functions

The FWSM can use RADIUS servers for user authorization for network access using dynamic access lists or access list names per user. To implement dynamic access lists, you must configure the RADIUS server to support it. When the user authenticates, the RADIUS server sends a downloadable access list or access list name to the security appliance. Access to a given service is either permitted or denied by the access list. The security appliance deletes the access list when the authentication session expires.

TACACS+ Server Support

The security appliance supports TACACS+ authentication with ASCII, PAP, CHAP, and MS-CHAPv1.

SDI Server Support

The FWSM can use RSA SecureID servers for VPN authentication. These servers are also known as SDI servers. When a user attempts to establish VPN access and the applicable tunnel-group record specifies a SDI authentication server group, the FWSM sends to the SDI server the username and one-time password and grants or denies user access based on the response from the server.

This section contains the following topics:

- [SDI Version Support, page 14-5](#)
- [Two-step Authentication Process, page 14-5](#)
- [SDI Primary and Replica Servers, page 14-5](#)

SDI Version Support

The FWSM offers the following SDI version support:

- **Versions prior to Version 5.0**—SDI versions prior to 5.0 use the concept of an SDI master and an SDI slave server which share a single node secret file (SECURID).
- **Versions 5.0**—SDI Version 5.0 uses the concepts of an SDI primary and SDI replica servers. Each primary and its replicas share a single node secret file. The node secret file has its name based on the hexadecimal value of the ACE/Server IP address with .sdi appended.

A Version 5.0 SDI server that you configure on the FWSM can be either the primary or any one of the replicas. See the “[SDI Primary and Replica Servers](#)” section on page 14-5 for information about how the SDI agent selects servers to authenticate users.

Two-step Authentication Process

SDI Version 5.0 uses a two-step process to prevent an intruder from capturing information from an RSA SecurID authentication request and using it to authenticate to another server. The SDI agent first sends a lock request to the SecurID server before sending the user authentication request. The server locks the username, preventing another (replica) server from accepting it. This means that the same user cannot authenticate to two FWSMs using the same authentication servers simultaneously. After a successful username lock, the FWSM sends the passcode.

SDI Primary and Replica Servers

The FWSM obtains the server list when the first user authenticates to the configured server, which can be either a primary or a replica. The FWSM then assigns priorities to each of the servers on the list, and subsequent server selection derives at random from those assigned priorities. The highest priority servers have a higher likelihood of being selected.

NT Server Support

The FWSM supports authentication of VPN-based management connections with Microsoft Windows server operating systems that support NTLM Version 1, which we collectively refer to as NT servers. When a user attempts to establish VPN access and the applicable tunnel-group record specifies an NT authentication server group, the FWSM uses NTLM Version 1 to for user authentication with the Microsoft Windows domain server. The FWSM grants or denies user access based on the response from the domain server.

**Note**

NT servers have a maximum length of 14 characters for user passwords. Longer passwords are truncated. This is a limitation of NTLM Version 1.

Kerberos Server Support

The FWSM can use Kerberos servers for VPN-based management connections. When a user attempts to establish VPN access, and the traffic matches an authentication statement, the FWSM consults the Kerberos server for user authentication and grants or denies user access based on the response from the server.

The FWSM supports 3DES, DES, and RC4 encryption types.

**Note**

The FWSM does not support changing user passwords during tunnel negotiation. To avoid this situation happening inadvertently, disable password expiration on the Kerberos/Active Directory server for users connecting to the FWSM.

LDAP Server Support

The FWSM can use LDAP servers for authorization of VPN-based management connections. When user authentication for VPN access has succeeded and the applicable tunnel-group record specifies an LDAP authorization server group, the FWSM queries the LDAP server and applies to the VPN session the authorizations it receives.

Local Database Support

The FWSM maintains a local database that you can populate with user profiles.

This section contains the following topics:

- [User Profiles, page 14-6](#)
- [Fallback Support, page 14-6](#)

User Profiles

User profiles contain, at a minimum, a username. Typically, a password is assigned to each username, although passwords are optional. You can add other information to a specific user profile. The information you can add includes VPN-related attributes, such as a VPN session timeout value.

Fallback Support

The local database can act as a fallback method for several functions. This behavior is designed to help you prevent accidental lockout from the FWSM.

For users who need fallback support, we recommend that their usernames and passwords in the local database match their usernames and passwords in the AAA servers. This provides transparent fallback support. Because the user cannot determine whether a AAA server or the local database is providing the

service, using usernames and passwords on AAA servers that are different than the usernames and passwords in the local database means that the user cannot be certain which username and password should be given.

The local database supports the following fallback functions:

- Console and enable password authentication—If the servers in the group all are unavailable, the FWSM uses the local database to authenticate administrative access. This can include enable password authentication, too.
- Command authorization—If the TACACS+ servers in the group all are unavailable, the local database is used to authorize commands based on privilege levels.
- VPN authentication and authorization—VPN authentication and authorization are supported to enable remote access to the FWSM if AAA servers that normally support these VPN services are unavailable. When VPN client of an administrator specifies a tunnel group configured to fallback to the local database, the VPN tunnel can be established even if the AAA server group is unavailable, provided that the local database is configured with the necessary attributes.

Configuring AAA Server Groups

If you want to use an external AAA server for authentication, authorization, or accounting, you must first create at least one AAA server group per AAA protocol and add one or more servers to each group. You identify AAA server groups by name. Each server group is specific to one type of server: Kerberos, LDAP, NT, RADIUS, SDI, or TACACS+.

The FWSM contacts the first server in the group. If that server is unavailable, the FWSM contacts the next server in the group, if configured. If all servers in the group are unavailable, the FWSM tries the local database if you configured it as a fallback method (management authentication and authorization only). If you do not have a fallback method, the FWSM continues to try the AAA servers.

This section includes the following procedures:

- [Adding a Server Group, page 14-7](#)
- [Adding a Server to a Group, page 14-8](#)
- [AAA Server Parameters, page 14-9](#)
- [Testing Server Authentication and Authorization, page 14-14](#)
- [Configuring LDAP Attribute Maps, page 14-15](#)

Adding a Server Group

To add a server group, perform the following steps:

-
- Step 1** From the Configuration > Device Management > Users/AAA > AAA Server Groups > AAA Server Groups area, click **Add**.
- The Add AAA Server Group dialog box appears.
- Step 2** In the Server Group field, add a name for the group.
- Step 3** From the Protocol drop-down list, choose the server type:
- **RADIUS**
 - **TACACS+**

- **SDI**
- **NT Domain**
- **Kerberos**
- **LDAP**

- Step 4** In the Accounting Mode field click the radio button for the mode you want to use (**Simultaneous** or **Single**).
- In Single mode, the FWSM sends accounting data to only one server.
- In Simultaneous mode, the FWSM sends accounting data to all servers in the group.
- Step 5** In the Reactivation Mode field, click the radio button for the mode you want to use (**Depletion** or **Timed**).
- In Depletion mode, failed servers are reactivated only after all of the servers in the group are inactive.
- In Timed mode, failed servers are reactivated after 30 seconds of down time.
- Step 6** If you chose Depletion reactivation mode, add a time interval in the Dead Time field.
- The Dead Time is the duration of time, in minutes, to elapse between the disabling of the last server in a group and the subsequent reenabling of all servers.
- Step 7** In the Max Failed Attempts field, add the number of failed attempts permitted.
- This option sets the number of failed connection attempts allowed before declaring a nonresponsive server to be inactive.
- Step 8** Click **OK**.
- The dialog box closes and the server group is added to the AAA server groups table.
- Step 9** In the AAA Server Groups dialog box, click **Apply** to save the changes.
- The changes are saved.
-

Adding a Server to a Group

To add a AAA server to a group, perform the following steps:

- Step 1** From the Configuration > Device Management > Users/AAA > AAA Server Groups > AAA Server Groups area, click the server group to which you want to add a server.
- The row is highlighted in the table.
- Step 2** In the Servers in the Selected Group area (lower pane), click **Add**.
- The Add AAA Server Group dialog box appears for the server group.
- Step 3** From the Interface Name drop-down menu, choose the interface name where the authentication server resides.
- Step 4** In the Server Name or IP Address field, add either a server name or IP address for the server you are adding to the group.
- Step 5** In the Timeout field, either add a timeout value or keep the default. The timeout is the duration of time, in seconds, that the FWSM waits for a response from the primary server before sending the request to the backup server.

- Step 6** The other parameters available depend on the server type. See the following sections for parameters unique to each server type:
- [RADIUS Server Fields, page 14-9](#)
 - [TACACS+ Server Fields, page 14-11](#)
 - [SDI Server Fields, page 14-11](#)
 - [Windows NT Domain Server Fields, page 14-11](#)
 - [Kerberos Server Fields, page 14-12](#)
 - [LDAP Server Fields, page 14-12](#)
- Step 7** Click **OK**.
- The dialog box closes and the AAA server is added to the AAA server group.
- Step 8** In the AAA Server Groups pane, click **Apply** to save the changes.
- The changes are saved.
-

AAA Server Parameters


The following sections list the unique fields for each server type when adding a server to a server group (see the “Adding a Server to a Group” section on page 14-8):

- [RADIUS Server Fields, page 14-9](#)
- [TACACS+ Server Fields, page 14-11](#)
- [SDI Server Fields, page 14-11](#)
- [Windows NT Domain Server Fields, page 14-11](#)
- [Kerberos Server Fields, page 14-12](#)
- [LDAP Server Fields, page 14-12](#)

RADIUS Server Fields

The following table describes the unique fields for configuring RADIUS servers, for use with the “Adding a Server to a Group” section on page 14-8.

Field	Description
Server Authentication Port	The server port to be used for authentication of users. The default port is 1645.
Server Accounting Port	The server port to be used for accounting of users. The default port is 1646.
Retry Interval	The duration of time, 1 to 10 seconds, that the FWSM waits between attempts to contact the server.

Field	Description
Server Secret Key	The shared secret key used to authenticate the RADIUS server to the FWSM. The server secret you configure here should match the one configured on the RADIUS server. If you do not know the server secret, ask the RADIUS server administrator. The maximum field length is 64 characters.
Common Password	<p>A case-sensitive password that is common among users who access this RADIUS authorization server through this security appliance. Be sure to provide this information to your RADIUS server administrator.</p> <p>Note For an authentication RADIUS server (rather than authorization) do not configure a common password.</p> <p>If you leave this field blank, the users username is the password for accessing this RADIUS authorization server.</p> <p>Never use a RADIUS authorization server for authentication. Common passwords or usernames as passwords are less secure than assigning unique user passwords.</p> <p>Note Although the password is required by the RADIUS protocol and the RADIUS server, users do not need to know it.</p>
ACL Netmask Convert	<p>How you want the security appliance to handle netmasks received in downloadable access lists.</p> <ul style="list-style-type: none"> • Detect automatically: The security appliance attempts to determine the type of netmask expression used. If it detects a wildcard netmask expression, it converts it to a standard netmask expression; <p> Note Because some wildcard expressions are difficult to detect clearly, this setting may misinterpret a wildcard netmask expression as a standard netmask expression.</p> <ul style="list-style-type: none"> • Standard: The security appliance assumes downloadable access lists received from the RADIUS server contain only standard netmask expressions. No translation from wildcard netmask expressions is performed. • Wildcard: The security appliance assumes downloadable access lists received from the RADIUS server contain only wildcard netmask expressions and it converts them all to standard netmask expressions when the access lists are downloaded.

TACACS+ Server Fields

The following table describes the unique fields for configuring TACACS+ servers, for use with the [“Adding a Server to a Group”](#) section on page 14-8.

Field	Description
Server Port	The port to be used for this server.
Server Secret Key	The shared secret key used to authenticate the TACACS+ server to the FWSM. The server secret you configure here should match the one configured on the TACACS+ server. If you do not know the server secret, ask the RADIUS server administrator. The maximum field length is 64 characters.

SDI Server Fields

The following table describes the unique fields for configuring SDI servers, for use with the [“Adding a Server to a Group”](#) section on page 14-8.

Field	Description
Server Port	The TCP port number by which this server is accessed.
Retry Interval	The duration of time, 1 to 10 seconds, that the FWSM waits between attempts to contact the server.

Windows NT Domain Server Fields

The following table describes the unique fields for configuring Windows NT Domain servers, for use with the [“Adding a Server to a Group”](#) section on page 14-8.

Field	Description
Server Port	Port number 139, or the TCP port number used by the FWSM to communicate with the Windows NT server.
Domain Controller	The host name (no more than 15 characters) of the NT Primary Domain Controller for this server. For example, PDC01. You must enter a name, and it must be the correct host name for the server whose IP Address you added in the field, Authentication Server Address. If the name is incorrect, authentication fails.

Kerberos Server Fields

The following table describes the unique fields for configuring Kerberos servers, for use with the [“Adding a Server to a Group”](#) section on page 14-8.

Field	Description
Server Port	Server port number 88, or the UDP port number over which the FWSM communicates with the Kerberos server.
Retry Interval	The duration of time, 1 to 10 seconds, that the FWSM waits between attempts to contact the server.
Realm	<p>The name of the Kerberos realm, for example:</p> <ul style="list-style-type: none"> example.com example.net example.org <p>The maximum length is 64 characters. The following types of servers require that you enter the realm name in all uppercase letters:</p> <ul style="list-style-type: none"> Windows 2000 Windows XP Windows.NET <p>You must enter this name, and it must be the correct realm name for the server whose IP address you entered in the Server IP Address field.</p>

LDAP Server Fields

The following table describes the unique fields for configuring LDAP servers, for use with the [“Adding a Server to a Group”](#) section on page 14-8.

Field	Description
Enable LDAP over SSL check box	<p>When checked, SSL secures communications between the security appliance and the LDAP server. Also called secure LDAP.</p> <p>Note If you do not configure SASL protocol, we strongly recommend that you secure LDAP communications with SSL.</p>
Server Port	TCP port number 389, the port which the FWSM uses to access the LDAP server.
Server type	<p>A drop-down list for choosing one of the following LDAP server types:</p> <ul style="list-style-type: none"> Detect Automatically/Use Generic Type Microsoft Novell OpenLDAP Sun

Field	Description
Base DN	The Base Distinguished Name (DN), or location in the LDAP hierarchy where the server should begin searching when it receives an authorization request. For example, OU=people, dc=cisco, dc=com.
Scope	The extent of the search the server should make in the LDAP hierarchy when it receives an authorization request. The available options are: <ul style="list-style-type: none"> • One Level: Searches only one level beneath the Base DN. This option is quicker. • All Levels: Searches all levels beneath the Base DN; in other words, search the entire subtree hierarchy. This option takes more time.
Naming Attribute(s)	The Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server. Common naming attributes are Common Name (cn) and User ID (uid).
Login DN	The login Distinguished Name (DN), or the name of the directory object for FWSM authenticated binding. Examples are: <ul style="list-style-type: none"> • cn=Administrator • cn=users • ou=people • dc=Example Corporation • dc=com For anonymous access, leave this field blank. Some LDAP servers (including the Microsoft Active Directory server) require the FWSM to establish a handshake via authenticated binding before accepting requests for other LDAP operations. The security appliance identifies itself for authenticated binding by attaching a Login DN field to the user authentication request. The Login DN field defines the FWSM's authentication characteristics; these characteristics should correspond to those of a user with administration privileges.
Login Password	The login password. The characters you type are replaced with asterisks.
LDAP Attribute Map	The LDAP attribute maps that you can apply to LDAP server. Used to map Cisco attribute names to user-defined attribute names and values. See the “Configuring LDAP Attribute Maps” section on page 14-15 .
SASL MD5 authentication check box	When checked, the MD5 mechanism of the Simple Authentication and Security Layer (SASL) authenticates communications between the FWSM and the LDAP server.
SASL Kerberos authentication	When checked, the Kerberos mechanism of the SASL secures authentication communications between the FWSM and the LDAP server.
Kerberos Server Group	The Kerberos server or server group used for authentication. The Kerberos Server group option is disabled by default and is enabled only when SASL Kerberos authentication is chosen.

Testing Server Authentication and Authorization

To determine whether the FWSM can contact an AAA server and authenticate or authorize a user, perform the following steps:

-
- Step 1** From the Configuration > Device Management > Users/AAA > AAA Server Groups > AAA Server Groups table, click the server group where the server resides.
The row is highlighted in the table.
- Step 2** From the Servers in the Selected Group table, click the server you want to test.
The row is highlighted in the table.
- Step 3** Click **Test**.
The Test AAA Server dialog box appears for that server.
- Step 4** Click the type of test you want to perform, **Authentication** or **Authorization**.
- Step 5** In the Username field, add a username.
- Step 6** If you are testing authentication, in the Password field, add the password for the username.
- Step 7** Click **OK**.
The FWSM sends an authentication or authorization test message to the server. If the test fails, ASDM displays an error message.
-

Adding a User Account

The local database is used for the following features:

- ASDM per-user access

By default, you can log into ASDM with a blank username and the enable password (see the [“Device Name/Password” section on page 7-7](#)). However, if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.



Note Although you can configure HTTP authentication using the local database, that functionality is always enabled by default. You should only configure HTTP authentication if you want to use a RADIUS or TACACS+ server for authentication.

- Console authentication
- Telnet and SSH authentication
- enable command authentication

This setting is for CLI-access only and does not affect the ASDM login.

- Command authorization

If you turn on command authorization using the local database, then the FWSM refers to the user privilege level to determine what commands are available. Otherwise, the privilege level is not generally used. By default, all commands are either privilege level 0 or level 15. ASDM allows you

to enable three predefined privilege levels, with commands assigned to level 15 (Admin), level 5 (Read Only), and level 3 (Monitor Only). If you use the predefined levels, then assign users to one of these three privilege levels.

- Network access authentication
- VPN client authentication (management only)

You cannot use the local database for network access authorization.

For multiple context mode, you can configure usernames in the system execution space to provide individual logins at the CLI using the **login** command; however, you cannot configure any AAA rules that use the local database in the system execution space.

To add a user account to the FWSM local database, perform the following steps:

-
- Step 1** From the Configuration > Device Management > Users/AAA > User Accounts pane, click **Add**.
The Add User Account dialog box appears.
- Step 2** In the Username field, add a username between 4 to 64 characters long.
- Step 3** In the Password field add a password between 3 and 32 characters. Entries are case-sensitive. The field displays only asterisks. To protect security, we recommend a password length of at least 8 characters.
- Step 4** In the Confirm Password field, add the password again.
For security purposes, only asterisks appear in the password fields.
- Step 5** From the Privilege Level drop-down menu, choose a value from 0 (lowest) to 15 (highest). The privilege level is used with local command authorization.
- Step 6** Click **Apply**.
The user is added to the local FWSM database and changes are saved to the running configuration.
-

**Note**

To configure the enable password from the User Accounts pane (instead of in the “[Device Name/Password](#)” section on page 7-7), change the password for the enable_15 user. The enable_15 user is always present in this pane, and represents the default username. This method of configuring the enable password is the only method available in ASDM for the system configuration. If you configured other enable level passwords at the CLI (**enable password 10**, for example), then those users are listed as enable_10, etc.

Configuring LDAP Attribute Maps

If you are introducing a FWSM to an existing LDAP directory, your existing LDAP attribute names and values are probably different from the existing ones. You must create LDAP attribute maps that map your existing user-defined attribute names and values to Cisco attribute names and values that are compatible with the FWSM. You can then bind these attribute maps to LDAP servers or remove them as needed. You can also show or clear attribute maps.

**Note**

To use the attribute mapping features correctly, you need to understand the Cisco LDAP attribute names and values as well as the user-defined attribute names and values.

The names of frequently mapped Cisco LDAP attributes and the type of user-defined attributes they would commonly be mapped to include:

IETF-Radius-Class – Department or user group
IETF-Radius-Filter-Id – Access control list
IETF-Radius-Framed-IP-Address – A static IP address
IPSec-Banner1 – A organization title
Tunneling-Protocols – Allow or deny dial-in

To map the LDAP attribute names used in your organization to their Cisco counterparts on the FWSM, perform the following steps:

-
- Step 1** From the Configuration > Remote Access VPN > AAA Local Users > LDAP Attribute Map pane, click **Add**.
- The Add LDAP Attribute Map dialog box appears with the Map Name tab active.
- Step 2** In the Name field, add a name for the map.
- Step 3** In the Customer Name field, add the name of your organization's corresponding attribute.
- Step 4** From the Cisco Name drop-down list, choose an attribute.
- Step 5** Click **Add**.
- Step 6** To add more names, repeat steps 1 through 5.
- Step 7** To map the customer names, click the **Map Value** tab.
- Step 8** Click **Add**.
- The Add LDAP Attributes Map Value dialog box appears.
- Step 9** Choose the attribute from the Customer Name drop-down list.
- Step 10** In the Customer Value field, add the value for this attribute.
- Step 11** In the Cisco Value field, add the Cisco value that the value in step 10 maps to.
- Step 12** Click **Add**.
- The values are mapped.
- Step 13** To map more names, repeat steps 8 through 12.
- Step 14** Click **OK** to return to the Map Value tab, and then click **OK** again to close the dialog box.
- Step 15** In the LDAP Attribute Map pane, click **Apply**.
- The value mappings are saved in the running configuration.
-

Adding an Authentication Prompt

You can specify text to display to the user during the AAA authentication challenge process. You can specify the AAA challenge text for HTTP, FTP, and Telnet access through the FWSM when requiring user authentication from TACACS+ or RADIUS servers. This text is primarily for cosmetic purposes and displays above the username and password prompts that users view when logging in.

If you do not specify an authentication prompt, users will see the following when authenticating with a RADIUS or TACACS+ server:

Connection type	Default prompt
FTP	FTP authentication
HTTP	HTTP Authentication
Telnet	None

To add an authentication prompt, perform the following steps:

- Step 1** From the Configuration > Device Management > Users/AAA > Authentication Prompt pane, add a message to appear above the username and password prompts that users see when logging in by entering text in the Prompt field.

The following are maximum characters allowed for authentication prompts:

Application	Character limit for Authentication prompt
Microsoft Internet Explorer	37
Telnet	235
FTP	235

- Step 2** In the Messages area, add messages in the User accepted message and User rejected message fields.
- If the user authentication occurs from Telnet, you can use the User accepted message and User rejected message options to display different status prompts to indicate that the authentication attempt is accepted or rejected by the AAA server.
- If the AAA server authenticates the user, the FWSM displays the User accepted message text, if specified, to the user; otherwise it displays the User rejected message text, if specified. Authentication of HTTP and FTP sessions displays only the challenge text at the prompt. The User accepted message and User rejected message text are not displayed.
- Step 3** Click **Apply**.
- The changes are saved to the running configuration.

