



CHAPTER 10

Configuring AAA Servers

This section contains the following topics:

- [Understanding AAA](#)
- [AAA Implementation in ASDM](#)
- [AAA Setup](#)

Understanding AAA

This section contains the following topics:

- [AAA Overview](#)
- [Preparing for AAA](#)
- [LOCAL Database](#)

AAA Overview

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

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 the DMZ network. 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 security appliance. (The Telnet server enforces authentication, too; the security appliance prevents unauthorized users from attempting to access the server.)

- **About Authentication**—Authentication grants access based on user identity. Authentication establishes user identity by requiring valid user credentials, which are typically a username and password.
- **About Authorization**—Authorization controls access per user after users authenticate. 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 security appliance caches the first 16 authorization requests per user, so if the user accesses the same services during the current authentication session, the security appliance does not resend the request to the authorization server.

- About Accounting—Accounting tracks traffic that passes through the security appliance, 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 security appliance for the session, the service used, and the duration of each session.

Preparing for AAA

AAA services depend upon the use of the LOCAL database or at least one AAA server. You can also use the LOCAL database as a fallback for most services provided by a AAA server. Before you implement AAA, you should configure the LOCAL database and configure AAA server groups and servers.

How you configure the LOCAL database and AAA servers depends upon the AAA services you want the security appliance to support. Regardless of whether you use AAA servers, you should configure the LOCAL database with user accounts that support administrative access, to prevent accidental lockouts and, if so desired, to provide a fallback method when AAA servers are unreachable. For more information, see LOCAL Database.

Table 10-1 provides a summary of AAA service support by each AAA server type and by the LOCAL database. You manage the LOCAL database by configuring user profiles in the Configuration > Properties > Device Administration > User Accounts pane. You establish AAA server groups and add individual AAA servers to the server groups in the Configuration > Properties > AAA Setup > AAA Server Groups pane.

Table 10-1 Summary of AAA Support

AAA Service	Database Type							
	Local	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP	HTTP Form
Authentication of...								
VPN users	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes ¹
Firewall sessions	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Administrators	Yes	Yes	Yes	Yes ²	Yes	Yes	Yes	No
Authorization of...								
VPN users	Yes	Yes	No	No	No	No	Yes	No
Firewall sessions	No	Yes ³	Yes	No	No	No	No	No
Administrators	Yes ⁴	No	Yes	No	No	No	No	No
Accounting of...								
VPN connections	No	Yes	Yes	No	No	No	No	No

Table 10-1 Summary of AAA Support (continued)

AAA Service	Database Type							
	Local	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP	HTTP Form
Firewall sessions	No	Yes	Yes	No	No	No	No	No
Administrators	No	Yes ⁵	Yes	No	No	No	No	No

1. HTTP Form protocol supports single sign-on authentication for WebVPN users only.
2. SDI is not supported for HTTP administrative access.
3. For firewall sessions, RADIUS authorization is supported with user-specific access lists only, which are received or specified in a RADIUS authentication response.
4. Local command authorization is supported by privilege level only.
5. Command accounting is available for TACACS+ only.

LOCAL Database

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

- **User Profiles**—User profiles contain, at a minimum, a username. Typically, you assign a password to each username, although passwords are optional. User profiles can also specify VPN access policy per user. You can manage user profiles with the Configuration > Properties > Device Administration > User Accounts pane.
- **Fallback Support**—The local database can act as a fallback method for console and enable password authentication, for command authorization, and for VPN authentication and authorization. This behavior is designed to help you prevent accidental lockout from the security appliance. 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.

AAA Implementation in ASDM

You can use AAA for the following:

- [AAA for Device Administration](#)
- [AAA for Network Access](#)
- [AAA for VPN Access](#)

AAA for Device Administration

You can authenticate all administrative connections to the security appliance, including:

- Telnet
- SSH
- Serial console

- ASDM
- VPN management access

You can also authenticate administrators who attempt to enter enable mode. You can authorize administrative commands. You can have accounting data for administrative sessions and for commands issued during a session sent to an accounting server.

You can configure AAA for device administration with the Configuration > Properties > Device Access > AAA Access pane.

AAA for Network Access

You can configure rules for authenticating, authorizing, and accounting for traffic passing through the firewall by using the Configuration > Security Policy > AAA Rules tab. The rules you create are similar to access rules, except that they specify whether to authenticate, authorize, or perform accounting for the traffic defined; and which AAA server group the security appliance is to use to process the AAA service request.

AAA for VPN Access

AAA services for VPN access include the following:

- User account settings for assigning users to VPN groups, configured in the Configuration > Properties > Device Administration > User Accounts pane.
- VPN group policies that can be referenced by many user accounts or tunnel groups, configured in the Configuration > VPN > General > Group Policy pane.
- Tunnel group policies, configured in the Configuration > VPN > General > Tunnel Group pane.

AAA Setup

The **AAA Setup** panes let you configure AAA server groups, AAA servers, and the authentication prompt. This section includes the following topics:

- [AAA Server Groups](#)
- [Auth. Prompt](#)
- [LDAP Attribute Map](#)

AAA Server Groups

The **AAA Server Groups** pane lets you:

- Configure AAA server groups and the protocols the security appliance uses to communicate with the servers listed in each group.
- Configure and add individual servers to AAA server groups.

You can have up to 15 groups in single-mode or 4 groups in multi-mode. Each group can have up to 16 servers in single mode or 4 servers in multi-mode. When a user logs in, the servers are accessed one at a time, starting with the first server you specify, until a server responds.

If AAA accounting is in effect, the accounting information goes only to the active server, unless you have configured simultaneous accounting.

For an overview of AAA services, see [Understanding AAA](#).

Fields

The fields in the **AAA Server Groups** pane are grouped into two main areas: the AAA Server Groups area and the Servers In The Selected Group area. The **AAA Server Groups** area lets you configure AAA server groups and the protocols the security appliance uses to communicate with the servers listed in each group.



Note

Double-clicking any of the rows in the AAA Server Groups table opens the Edit AAA Server Group dialog box, in which you can modify the AAA Server Group parameters. These changes are immediately reflected in the table, but you must click **Apply** to save them to the configuration.

Clicking a column head sorts the table rows in alphanumeric order according to the contents of that column.

- **Server Group**—*Display only*. Shows the symbolic name of the selected server group.
- **Protocol**—*Display only*. Lists the AAA protocol that servers in the group support.
- **Accounting Mode**—*Display only*. Shows either simultaneous or single mode accounting. In single mode, the security appliance sends accounting data to only one server. In simultaneous mode, the security appliance sends accounting data to all servers in the group.
- **Reactivation Mode**—*Display only*. Shows the method by which failed servers are reactivated: Depletion or Timed reactivation mode. 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.
- **Dead Time**—*Display only*. Shows the number of minutes that will elapse between the disabling of the last server in the group and the subsequent reenabling of all servers. This parameter applies only in depletion mode.
- **Max Failed Attempts**—*Display only*. Shows the number of failed connection attempts allowed before declaring a nonresponsive server inactive.
- **Add**—Displays the Add AAA Server Group dialog box.
- **Edit**—Displays the Edit AAA Server Group dialog box, or, if you have selected LOCAL as the server group, displays the Edit AAA Local Server Group dialog box.
- **Delete**—Removes the currently selected server group entry from the server group table. There is no confirmation or undo.

The Servers In Selected Group area, the second area of the **AAA Server Groups** pane, lets you add and configure AAA servers for existing AAA server groups. The servers can be RADIUS, TACACS+, NT, SDI, Kerberos, LDAP, or HTTP-form servers.

- **Server Name or IP Address**—*Display only*. Shows the name or IP address of the AAA server.
- **Interface**—*Display only*. Shows the network interface where the authentication server resides.
- **Timeout**—*Display only*. Shows the timeout interval, in seconds. This is the time after which the security appliance gives up on the request to the primary AAA server. If there is a standby AAA server, the security appliance sends the request to the backup server.
- **Add/Edit**—Displays the Add/Edit AAA Server dialog box.

- Delete—Removes the selected AAA server from the list.
- Move up—Moves the selected AAA server up in the AAA sequence.
- Move down—Moves the selected AAA server back in the AAA sequence.
- Test—Displays the Test AAA Server dialog box.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	• ¹	•	•	—

1. HTTP Form and WebVPN are supported only in single routed mode.

Add/Edit AAA Server Group

The **Add/Edit AAA Server Group** dialog box lets you add or modify AAA server groups. The results appear in the AAA Server table.

Fields

- Server Group—*Display only*. Shows the name of the selected server group.
- Protocol drop-down list—Specifies the protocols supported by servers in the group. They include RADIUS, TACACS+, NT Domain, SDI, Kerberos, LDAP, and HTTP Form for single sign-on (WebVPN users only).



Note The following fields are not available after selecting the HTTP Form protocol.

- Accounting Mode—Specifies the accounting mode used with the server group.
 - Simultaneous—Configures the security appliance to send accounting data to all servers in the group.
 - Single—Configures the security appliance to send accounting data to only one server of the group.
- Reactivation Mode—Specifies the method by which failed servers are reactivated.
 - Depletion—Configures the security appliance to reactivate failed servers only after all of the servers in the group are inactive.
 - Timed—Configures the security appliance to reactive failed servers after 30 seconds of down time.
- Dead Time—Specifies the number of minutes that will elapse between the disabling of the last server in the group and the subsequent reenabling of all servers. This field is not available for timed mode.
- Max Failed Attempts—Specifies the number of failed connection attempts (1 through 5) allowed before declaring a nonresponsive server inactive.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	• ¹	•	•	—

1. HTTP Form and WebVPN are supported only in single routed mode.

Edit AAA Local Server Group

The **Edit AAA Local Server Group** dialog box lets you specify whether to enable local user lockout and the maximum number of failed login attempts to allow before locking out the user. If a user is locked out, and administrator must clear the lockout condition before the user can successfully log in.

Fields

- **Enable Local User Lockout**—Enables locking out and denying access to a user who has exceeded the configured maximum number of failed authentication attempts.
- **Maximum Attempts**—Specifies the maximum number of failed login attempts allowed before locking out and denying access to a user. This limit applies only when the LOCAL database is used for authentication.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	• ¹	•	•	—

1. HTTP Form and WebVPN are supported only in single routed mode.

Add/Edit AAA Server

The **Add/Edit AAA Server** dialog box lets you modify the parameters of an existing AAA server or add a new AAA server to an existing group selected in the AAA server groups table.

Fields**Note**

The first four fields are the same for all types of servers. The area contents area is specific to each server type.

- **Server Group**—*Display only*. Shows the name of the server group.
- **Interface Name**—Specifies the network interface where the server resides.
- **Server Name or IP Address**—Specifies the name or IP address of the AAA server.

- Timeout—Specifies the timeout interval, in seconds. This is the time after which the security appliance gives up on the request to the primary AAA server. If there is a standby AAA server, the security appliance sends the request to the backup server.
- RADIUS Parameters area—Specifies the parameters needed for using a RADIUS server. This area appears only when the selected server group uses RADIUS.
 - Retry Interval—Specifies the number of seconds to wait after sending a query to the server and receiving no response, before reattempting the connection. The minimum time is 1 second. The default time is 10 seconds. The maximum time is 10 seconds.
 - Server Authentication Port—Specifies the server port to use for user authentication. The default port is 1645.

**Note**

The latest RFC states that RADIUS should be on UDP port number 1812, so you might need to change this default value to 1812.

- Server Accounting Port—Specifies the server port to use for user accounting. The default port is 1646.
- Server Secret Key—Specifies the server secret key (also called the shared secret) to use for encryption; for example: C8z077f. The secret is case-sensitive. The field displays only asterisks. The security appliance uses the server secret to authenticate to the RADIUS server. The server secret you configure here should match the one configured on the RADIUS server. If you do not know the server secret for the RADIUS server, ask the administrator of the RADIUS server. The maximum field length is 64 characters.
- Confirm Server Secret Key—Requires that you reenter the server secret, to confirm its accuracy. The secret is case-sensitive. The field displays only asterisks.
- Common Password—Specifies the common password for the group. The password is case-sensitive. The field displays only asterisks. If you are defining a RADIUS server to be used for authentication rather than authorization, do not provide a common password.

A RADIUS authorization server requires a password and username for each connecting user. You enter the password here. The RADIUS authorization server administrator must configure the RADIUS server to associate this password with each user authorizing to the server via this security appliance. Be sure to provide this information to your RADIUS server administrator. Enter a common password for all users who are accessing this RADIUS authorization server through this security appliance.

If you leave this field blank, each user password will be his or her own username. For example, a user with the username “jsmith” would enter “jsmith”. As a security precaution never use a RADIUS authorization server for authentication. Use of a common password or usernames as passwords is much less secure than strong passwords per user.

**Note**

The password field is required by the RADIUS protocol and the RADIUS server requires it; however, users do not need to know it.

- Confirm Common Password—Requires that you reenter the common password, to confirm its accuracy. The password is case-sensitive. The field displays only asterisks.
- ACL Netmask Convert—Specifies how the security appliance handles netmasks received in downloadable access lists. The security appliance expects downloadable access lists to contain standard netmask expressions whereas Cisco Secure VPN 3000 series concentrators expect downloadable access lists to contain wildcard netmask expressions, which are the reverse of a

standard netmask expression. A wildcard mask has ones in bit positions to ignore, zeros in bit positions to match. The ACL Netmask Convert list helps minimize the effects of these differences upon how you configure downloadable access lists on your RADIUS servers.

If you choose 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; however, because some wildcard expressions are difficult to detect unambiguously, this setting may occasionally misinterpret a wildcard netmask expression as a standard netmask expression.

If you choose 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.

If you choose 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+ Parameters—Specifies the parameters needed for using a TACACS+ server. This area appears only when the selected server group uses TACACS+.
 - Server Port—Specifies the server port to use.
 - Server Secret Key—Specifies the server secret key to use for encryption. The secret is case-sensitive. The field displays only asterisks.
 - Confirm Server Secret Key—Requires that you reenter the server secret, to confirm its accuracy. The secret is case-sensitive. The field displays only asterisks.
- SDI Parameters—Specifies the parameters needed for using an SDI server. This area appears only when the selected server group uses SDI.
 - Server Port—Specifies the server port to use.
 - Retry Interval—Specifies the number of seconds to wait before reattempting the connection.
- Kerberos Parameters—Specifies the parameters needed for using a Kerberos server. This area appears only when the selected server group uses Kerberos.
 - Server Port—Specifies the server port that the Kerberos server listens to.
 - Retry Interval—Specifies the number of seconds to wait before reattempting the connection. Enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the security appliance declares this server inoperative and uses the next Kerberos/Active Directory server in the list. The minimum number of retries is 0. The default number of retries is 2. The maximum number of retries is 10.
 - Kerberos Realm—Specifies the name of the Kerberos realm to use, for example: USDOMAIN.ACME.COM. The maximum length is 64 characters. The following types of servers require that you enter the realm name in all uppercase letters: Windows 2000, Windows XP, and Windows.NET. 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.
- LDAP Parameters—Specifies the parameters needed for using an LDAP server. This area appears only when the selected server group uses LDAP.
 - Enable LDAP Over SSL—Specifies that SSL secures communications between the security appliance and the LDAP server. Also called secure LDAP.
 - Server Port—Specifies the server port to use. Enter the TCP port number by which you access the server.

- Server Type—Lets you manually set the LDAP server type as a Sun Microsystems JAVA System Directory Server (formerly the Sun ONE Directory Server) or a Microsoft Active Directory, or lets you specify auto-detection for server type determination.
- Base DN—Specifies the Base DN. Enter the 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—Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request—One Level (Search only one level beneath the Base DN. This option is quicker.) All Levels (Search all levels beneath the Base DN; in other words, search the entire subtree hierarchy. This option takes more time.)
- Naming Attribute(s)—Specifies 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—Specifies the login DN. Some LDAP servers (including the Microsoft Active Directory server) require the security appliance to establish a handshake via authenticated binding before they will accept requests for any 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 security appliance's authentication characteristics; these characteristics should correspond to those of a user with administration privileges. Enter the name of the directory object for security appliance authenticated binding, for example: `cn=Administrator, cn=users, ou=people, dc=Example Corporation, dc=com`. For anonymous access, leave this field blank.
- Login Password—Specifies the login password. The characters you type are replaced with asterisks.
- LDAP Attribute Map—Lists the LDAP attribute maps that you can apply to LDAP server. The LDAP attribute map translates Cisco attribute names into user-defined attribute names and values.
- SASL MD5 authentication—Specifies that the MD5 mechanism of the Simple Authentication and Security Layer secures authentication communications between the security appliance and the LDAP server.
- SASL Kerberos authentication—Specifies that Kerberos mechanism of the Simple Authentication and Security Layer secures authentication communications between the security appliance and the LDAP server.
- Kerberos Server Group—Specifies the Kerberos server or server group used for authentication.
- NT Domain Parameters—Specifies the parameters needed for using an NT server and includes the following fields:
 - Server Port—Specifies the TCP port number by which you access the server. The default port number is 139.
 - NT Domain Controller— Specifies the NT Primary Domain Controller host name for this server, for example: `PDC01`. The maximum host name length is 15 characters. You must enter this name, and it must be the correct host name for the server for which you entered the IP Address in Authentication Server Address; if the name is incorrect, authentication fails.
- HTTP Form Parameters—Specifies the parameters for the HTTP Form protocol for single sign-on authentication, available only to WebVPN users. This area appears only when the selected server group uses HTTP Form, and only the Server Group name and the protocol are visible. Other fields are not available when using HTTP Form.

**Note**

To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

If you do not know what the following parameters are, use an HTTP header analyzer to extract the data from the HTTP GET and POST exchanges when logging into the authenticating web server directly, not through the security appliance. See the *WebVPN* chapter in the *Cisco ASA 5500 Series Configuration Guide using the CLI* for more detail on extracting these parameters from the HTTP exchanges.

- Start URL—Specifies the complete URL of the authenticating web server location where a pre-login cookie can be retrieved. This parameter must be configured only when the authenticating web server loads a pre-login cookie with the login page. A drop-down list offers both HTTP and HTTPS. The maximum number of characters is 1024, and there is no minimum.
- Action URI—Specifies the complete Uniform Resource Identifier for the authentication program on the authorizing web server. The maximum number of characters for the complete URI is 2048 characters.
- Username—Specifies the name of a username parameter—not a specific username—that must be submitted as part of the HTTP form used for SSO authentication. The maximum number of characters is 128, and there is no minimum.
- Password—Specifies the name of a user password parameter—not a specific password value—that must be submitted as part of the HTTP form used for SSO authentication. The maximum number of characters is 128, and there is no minimum.
- Hidden Values—Specifies hidden parameters for the HTTP POST request submitted to the authenticating web server for SSO authentication. This parameter is necessary only when it is expected by the authenticating web server as indicated by its presence in the HTTP POST request. The maximum number of characters is 2048.
- Authentication Cookie Name—(Optional) Specifies the name of the cookie that is set by the server on successful login and that contains the authentication information. It is used to assign a meaningful name to the authentication cookie to help distinguish it from other cookies that the web server may pass back. The maximum number of characters is 128, and there is no minimum.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	• ¹	•	• 1.	—

1. HTTP Form and WebVPN are supported only in single routed mode.

Test AAA Server**Note**

Test AAA Server is not available for HTTP Form authentication servers.

Use the **Test** button to determine whether the security appliance can contact the selected AAA server. Failure to reach the AAA server may be due to incorrect configuration in ASDM or the AAA server may be unreachable for other reasons, such as restrictive network configurations or server downtime.

After you complete the fields in this dialog box and click OK, the security appliance sends the applicable test message to the selected server. If the test fails, ASDM displays an error message about the type of error encountered. If the error message suggests a configuration error in ASDM, correct the configuration and try the test again.

**Tip**

Checking for basic network connectivity to the AAA server may save you time in troubleshooting. To test basic connectivity, click **Tools > Ping**.

Fields

- AAA Server Group—*Display only*. Shows the AAA server group that the selected AAA server belongs to.
- Host —*Display only*. Shows the hostname of the AAA server you selected.
- Authorization—Specifies that ASDM tests authorizing a user with the selected AAA server. If the server type selected does not support authorization, this radio button is not available. For example, the security appliance cannot support authorization with Kerberos servers.
- Authentication—Specifies that ASDM tests authenticating a user with the selected AAA server. If the server type selected does not support authentication, this radio button is not available. For example, the security appliance cannot support authentication with LDAP servers.
- Username—Specifies the username you want to use to test the AAA server. Make sure the username exists on the AAA server; otherwise, the test will fail.
- Password—Specifies the password for the username you entered in the **Username** field. The **Password** field is available only for authentication tests. Make sure the password is correct for the username entered; otherwise, the authentication test will fail.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	• ¹	•	•	—

1. HTTP Form and WebVPN are supported only in single routed mode.

Auth. Prompt

The Auth. Prompt pane lets you 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 security appliance 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 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 security appliance 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.

**Note**

Microsoft Internet Explorer displays up to 37 characters in an authentication prompt. Netscape Navigator displays up to 120 characters, and Telnet and FTP display up to 235 characters in an authentication prompt.

Fields

- **Prompt**—(Optional) Enables the display of AAA challenge text, specified in the field below the check box, for through-the-security appliance user sessions.
- **Text**—(Optional) Specify a string of up to 235 alphanumeric characters or 31 words, limited by whichever maximum is first reached. Do not use special characters; however, spaces and punctuation characters are permitted. Entering a question mark or pressing the Enter key ends the string. (The question mark appears in the string.)
- **User accepted message**—(Optional) Enables the display of text, specified in the field below the check box, confirming that the user has been authenticated.
- **User rejected message**—(Optional) Enables the display of text, specified in the field below the check box, indicating that authentication failed.

**Note**

All of the fields in this pane are optional. If you do not specify an authentication prompt, FTP users see FTP authentication, HTTP users see HTTP Authentication Telnet users see no challenge text.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

LDAP Attribute Map

The LDAP Attribute Map pane lets you create and name an attribute map for mapping custom (user-defined) attribute names to Cisco LDAP attribute names. If you are introducing a security appliance to an existing LDAP directory, your existing custom LDAP attribute names and values are probably different from the Cisco attribute names and values. Rather than renaming your existing attributes, you can create LDAP attribute maps that map your custom attribute names and values to Cisco attribute names and values. By using simple string substitution, the security appliance then presents you with only your own custom names and values.

You can then bind these attribute maps to LDAP servers or remove them as needed. You can also delete entire attribute maps or remove individual name and value entries.

**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.

Fields

- Name—Displays the names of the LDAP attribute maps available for editing.
- Attribute Map Name—Displays the mappings of custom attribute names to Cisco attribute names within each attribute map.
- Add—Displays the Add LDAP Attribute Map dialog box.
- Edit—Displays the Edit LDAP Attribute Map dialog box.
- Delete—Deletes the selected LDAP Attribute Map.

Add/Edit LDAP Attribute Map

The **Add/Edit LDAP Attribute Map** dialog box lets you modify or delete an existing LDAP attribute map, add a new LDAP attribute map, and populate attribute maps with attribute name and value mappings.

Your typical steps to add a new attribute map using the LDAP Attribute Map dialog box would be as follows:

1. Create a new, unpopulated attribute map.
2. Populate the attribute map with name mappings that translate Cisco attribute names to custom, user-defined attribute names.
3. Populate the attribute map with value mappings that apply custom, user-defined attribute values to the custom attribute name and to the matching Cisco attribute name and value.

You would then bind the attribute map to an LDAP server when adding or editing the LDAP server using the [Add/Edit AAA Server](#) dialog box.

Fields

- Name—Specifies the name of the LDAP attribute map you are adding or editing. If you are adding a new map, you enter the name of the map in this field. If you are editing a map that was selected in the LDAP Attribute Map pane, the name of the selected map displays as read-only text in this field. To change the map, you must return to the LDAP Attribute Map pane and choose the desired map.
- Name Map—Displays the fields necessary for mapping custom attribute names to Cisco attribute names.
- Value Map—Displays the fields necessary for mapping custom attribute values to custom attribute names and to the matching Cisco attribute name and value.

Add/Edit LDAP Attribute Map > Map Name Tab

The **Add/Edit LDAP Attribute Map** dialog box lets you modify or delete an existing LDAP attribute map, add a new LDAP attribute map, and populate attribute maps with attribute name and value mappings. See also [Add/Edit LDAP Attribute Map](#).

Some fields vary depending upon whether you have selected the Map Name tab or the Map Value tab. When you click the Map Name tab, the following fields display.

Fields

- **Name**—Specifies the name of the LDAP attribute map you are adding or editing. If you are adding a new map, you enter the name of the map in this field. If you are editing a map that was selected in the LDAP Attribute Map pane, the name of the selected map displays as read-only text in this field. To change the map, you must return to the LDAP Attribute Map pane and choose the desired map.
- **Custom Name**—Specifies the custom, user-defined attribute name that maps to an attribute name selected from the Cisco Name drop-down list.
- **Cisco Name**—Specifies the Cisco attribute name you want to map to the user-defined name in the Custom Name field.
- **Add**—Inserts the name mapping into the attribute map.
- **Remove**—Removes the selected name mapping from the attribute map.
- **Custom Name**—Displays the custom attribute names of mappings in the attribute map.
- **Cisco Name**—Displays the Cisco attribute names of mappings in the attribute map.

Add/Edit LDAP Attribute Map > Map Value Tab

The **Add/Edit LDAP Attribute Map** dialog box lets you modify or delete an existing LDAP attribute map, add a new LDAP attribute map, and populate attribute maps with attribute name and value mappings. See also [Add/Edit LDAP Attribute Map](#).

Some fields vary depending upon whether you have selected the Map Name tab or the Map Value tab. When you click the Map Value tab, the following fields appear.

Fields

- **Name**—Specifies the name of the LDAP attribute map you are adding or editing. If you are adding a new map, you enter the name of the map in this field. If you are editing a map that was selected in the LDAP Attribute Map pane, the name of the selected map displays as read-only text in this field. To change the map, you must return to the LDAP Attribute Map pane and choose the desired map.
- **Custom Name**—Displays the custom attribute names of mappings in the attribute map.
- **Custom to Cisco Map Value**—Displays the mapping of a custom value to a Cisco value for a custom attribute.
- **Add**—Displays the Add LDAP Attributes Map Value dialog box.
- **Edit**—Displays the Edit LDAP Attributes Map Value dialog box.
- **Delete**—Deletes the selected attribute value mapping from the LDAP attribute map.

Add/Edit LDAP Attributes Value Map

The Add/Edit LDAP Attribute Map Value dialog box lets you map a custom attribute value for a custom attribute name to the Cisco value of the associated Cisco attribute name.

Fields

- Custom Name—If adding a new attribute value mapping, this is a drop-down list that lets you choose a custom attribute name from a list of attributes which do not yet have a custom value mapped to a Cisco attribute value. If editing an existing attribute value mapping, this is a read-only field which displays the name of the custom attribute selected on the Map Value tab of the Add/Edit LDAP Attribute Map dialog box.
- Custom Value—Specifies a custom value for the selected custom attribute.
- Cisco Value—Specifies the Cisco value for the selected custom attribute.
- Add—Adds the value mapping to the custom attribute value map.
- Remove—Removes the value mapping from the custom attribute value map.
- Custom Name—Displays the custom value for the custom attribute name.
- Cisco Name—Displays the Cisco value for the Cisco attribute name.