



CHAPTER 33

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.

The chapter includes the following sections:

- [AAA Overview, page 33-1](#)
- [AAA Server and Local Database Support, page 33-3](#)
- [Configuring the Local Database, page 33-8](#)
- [Identifying AAA Server Groups and Servers, page 33-11](#)
- [Configuring an LDAP Server, page 33-15](#)
- [Using Certificates and User Login Credentials, page 33-20](#)
- [Differentiating User Roles Using AAA, page 33-21](#)
- [AAA Servers Monitoring Commands, page 33-23](#)
- [Additional References, page 33-24](#)
- [Feature History for AAA Servers, page 33-25](#)

AAA Overview

AAA enables the adaptive security appliance 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 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 connect through the adaptive security appliance. (The Telnet server enforces authentication, too; the adaptive security appliance 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.

This section includes the following topics:

- [About Authentication, page 33-2](#)
- [About Authorization, page 33-2](#)
- [About Accounting, page 33-3](#)

About Authentication

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

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

About Authorization

Authorization controls access *per user* after users are authenticated. You can configure the adaptive security appliance to authorize the following items:

- Management commands
- Network access
- VPN access

Authorization controls the services and commands that are available to each authenticated user. If you did not 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 can 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 adaptive security appliance caches the first 16 authorization requests per user, so if the user accesses the same services during the current authentication session, the adaptive security appliance does not resend the request to the authorization server.

About Accounting

Accounting tracks traffic that passes through the adaptive 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 session start and stop times, username, the number of bytes that pass through the adaptive security appliance for the session, the service used, and the duration of each session.

AAA Server and Local Database Support

The adaptive security appliance supports a variety of AAA server types and a local database that is stored on the adaptive security appliance. This section describes support for each AAA server type and the local database, and includes the following topics:

- [Summary of Support, page 33-3](#)
- [RADIUS Server Support, page 33-4](#)
- [TACACS+ Server Support, page 33-5](#)
- [RSA/SDI Server Support, page 33-5](#)
- [NT Server Support, page 33-6](#)
- [Kerberos Server Support, page 33-6](#)
- [LDAP Server Support, page 33-7](#)
- [HTTP Forms Authentication for Clientless SSL VPN, page 33-7](#)
- [Local Database Support, page 33-7](#)

Summary of Support

[Table 33-1](#) 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 33-1 Summary of AAA Support

AAA Service	Database Type							
	Local	RADIUS	TACACS+	SDI (RSA)	NT	Kerberos	LDAP	HTTP Form
Authentication of...								
VPN users ¹	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes ²
Firewall sessions	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Administrators	Yes	Yes	Yes	Yes ³	Yes	Yes	Yes	No
Authorization of...								
VPN users	Yes	Yes	No	No	No	No	Yes	No
Firewall sessions	No	Yes ⁴	Yes	No	No	No	No	No
Administrators	Yes ⁵	No	Yes	No	No	No	No	No
Accounting of...								

Table 33-1 Summary of AAA Support (continued)

AAA Service	Database Type							
	Local	RADIUS	TACACS+	SDI (RSA)	NT	Kerberos	LDAP	HTTP Form
VPN connections	No	Yes	Yes	No	No	No	No	No
Firewall sessions	No	Yes	Yes	No	No	No	No	No
Administrators	No	Yes ⁶	Yes	No	No	No	No	No

1. For SSL VPN connections, either PAP or MS-CHAPv2 can be used.
2. HTTP Form protocol supports both authentication and single sign-on operations for clientless SSL VPN users sessions only.
3. RSA/SDI is supported for ASDM HTTP administrative access with ASA5500 software version 8.2(1) or later.
4. For firewall sessions, RADIUS authorization is supported with user-specific access lists only, which are received or specified in a RADIUS authentication response.
5. Local command authorization is supported by privilege level only.
6. Command accounting is available for TACACS+ only.

**Note**

In addition to the native protocol authentication listed in table Table 1-1, the adaptive security appliance supports proxying authentication. For example, the adaptive security appliance can proxy to an RSA/SDI and/or LDAP server via a RADIUS server. Authentication via digital certificates and/or digital certificates with the AAA combinations listed in the table are also supported.

RADIUS Server Support

The adaptive security appliance supports the following RADIUS servers for AAA, in addition to the one available on the adaptive security appliance itself:

- Cisco Secure ACS 3.2, 4.0, 4.1
- RSA RADIUS in RSA Authentication Manager 5.2 and 6.1

Authentication Methods

The adaptive security appliance supports the following authentication methods with RADIUS:

- PAP—For all connection types.
- CHAP and MS-CHAPv1—For L2TP-over-IPsec connections.
- MS-CHAPv2—For L2TP-over-IPsec connections, and for regular IPsec remote access connections when the password management feature is enabled. You can also use MS-CHAPv2 with clientless connections.
- Authentication Proxy modes—Including RADIUS to Active Directory, RADIUS to RSA/SDI, RADIUS to Token-server, and RSA/SI to RADIUS connections,

**Note**

To enable MS-CHAPv2 as the protocol used between the adaptive security appliance and the RADIUS server for a VPN connection, password management must be enabled in the tunnel group general attributes. Enabling password management generates an MS-CHAPv2 authentication request from the adaptive security appliance to the RADIUS server. See the description of the **password-management** command for details.

If you use double authentication and enable password management in the tunnel group, then the primary and secondary authentication requests include MS-CHAPv2 request attributes. If a RADIUS server does not support MS-CHAPv2, then you can configure that server to send a non-MS-CHAPv2 authentication request by using the **no mschapv2-capable** command.

Attribute Support

The adaptive security appliance 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.
- Cisco VSA (Cisco-Priv-Level), which provides a standard 0-15 numeric ranking of privileges, with 1 being the lowest level and 15 being the highest level. A zero level indicates no privileges. The first level (login) allows privileged EXEC access for the commands available at this level. The second level (enable) allows CLI configuration privileges.

RADIUS Authorization Functions

The adaptive security appliance 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 adaptive security appliance. Access to a given service is either permitted or denied by the access list. The adaptive security appliance deletes the access list when the authentication session expires.

TACACS+ Server Support

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

RSA/SDI Server Support

The RSA SecureID servers are also known as SDI servers.

This section includes the following topics:

- [RSA/SDI Version Support, page 33-6](#)
- [Two-step Authentication Process, page 33-6](#)
- [RSA/SDI Primary and Replica Servers, page 33-6](#)

RSA/SDI Version Support

The adaptive security appliance supports SDI Versions 5.0, 6.0, and 7.0. SDI 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, 6.0, or 7.0 SDI server that you configure on the adaptive security appliance can be either the primary or any one of the replicas. See the [“RSA/SDI Primary and Replica Servers” section on page 33-6](#) for information about how the SDI agent selects servers to authenticate users.

Two-step Authentication Process

SDI Versions 5.0, 6.0, and 7.0 use 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 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 action means that the same user cannot authenticate to two adaptive security appliances using the same authentication servers simultaneously. After a successful username lock, the adaptive security appliance sends the passcode.

RSA/SDI Primary and Replica Servers

The adaptive security appliance obtains the server list when the first user authenticates to the configured server, which can be either a primary or a replica. The adaptive security appliance 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 adaptive security appliance supports Microsoft Windows server operating systems that support NTLM Version 1, collectively referred to as NT servers.

**Note**

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

Kerberos Server Support

The adaptive security appliance supports 3DES, DES, and RC4 encryption types.

**Note**

The adaptive security appliance 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 adaptive security appliance.

For a simple Kerberos server configuration example, see [Example 33-2 on page 33-15](#).

LDAP Server Support

The adaptive security appliance supports LDAP. For detailed information, see the [“Configuring an LDAP Server” section on page 33-15](#).

HTTP Forms Authentication for Clientless SSL VPN

The adaptive security appliance can use the HTTP Form protocol for both authentication and single sign-on (SSO) operations of Clientless SSL VPN user sessions only.

Local Database Support

The adaptive security appliance maintains a local database that you can populate with user profiles. This section includes the following topics:

- [User Profiles, page 33-7](#)
- [Fallback Support, page 33-7](#)

User Profiles

User profiles include, at a minimum, a username. Typically, a password is assigned to each username, although passwords are optional.

To add other information to a specific user profile, enter the following command:

Command	Purpose
username {name} attributes	Enters username attributes mode, which lets you configure attributes for specific users. The information that you can add includes VPN-related attributes, such as a VPN session timeout value.
Example: hostname(config)# username anyuser attributes hostname(config-username)#	

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 adaptive 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 practice 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**—When you use the **aaa authentication console** command, you can add the **LOCAL** keyword after the AAA server group tag. If the servers in the group are all unavailable, the adaptive security appliance uses the local database to authenticate administrative access, which can also include enable password authentication.


- Command authorization—When you use the **aaa authorization** command, you can add the **LOCAL** keyword after the AAA server group tag. If the TACACS+ servers in the group are all 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 adaptive security appliance if AAA servers that normally support these VPN services are unavailable. The **authentication-server-group** command, available in tunnel-group general attributes mode, lets you specify the **LOCAL** keyword when you are configuring attributes of a tunnel group. When a 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 the Local Database

This section describes how to manage users in the local database. You can use the local database for CLI access authentication, privileged mode authentication, command authorization, network access authentication, and VPN authentication and authorization. You cannot use the local database for network access authorization. The local database does not support accounting.

For multiple context mode, you can configure usernames in the system execution space to provide individual logins using the **login** command; however, you cannot configure any **aaa** commands in the system execution space.

To define a user account in the local database, perform the following steps:

	Command	Purpose
Step 1	<p>username <i>username</i> [nopassword password <i>password</i> [mschap]] [privilege <i>priv_level</i>]</p> <p>Example: hostname(config)# username exampleuser1 privilege 1</p>	<p>Creates the user account. The <i>username</i> keyword is a string from 4 to 64 characters long. The password <i>password</i> argument is a string from 3 to 16 characters long. The mschap keyword specifies that the password is converted to Unicode and hashed using MD4 after you enter it. Use this keyword if users are authenticated using MSCHAPv1 or MSCHAPv2. The privilege level argument sets the privilege level, which ranges from 0 to 15. The default is 2. This privilege level is used with command authorization.</p> <div>  <p>Caution If you do not use command authorization (the aaa authorization console LOCAL command), then the default level 2 allows management access to privileged EXEC mode. If you want to limit access to privileged EXEC mode, either set the privilege level to 0 or 1, or use the service-type command (see Step 4).</p> </div> <p>The nopassword keyword creates a user account with no password.</p> <p>The encrypted and nt-encrypted keywords are typically for display only. When you define a password in the username command, the adaptive security appliance encrypts it when it saves it to the configuration for security purposes. When you enter the show running-config command, the username command does not show the actual password; it shows the encrypted password followed by the encrypted or nt-encrypted keyword (when you specify mschap). For example, if you enter the password “test,” the show running-config output would appear as something similar to the following:</p> <pre>username user1 password DLaUiAX3l78qgoB5c7iVNw== nt-encrypted</pre> <p>The only time you would actually enter the encrypted or nt-encrypted keyword at the CLI is if you are cutting and pasting a configuration file for use in another adaptive security appliance, and you are using the same password.</p>

	Command	Purpose
Step 2	aaa authorization exec authentication-server Example: <pre>hostname(config)# aaa authorization exec authentication-server</pre>	<p>(Optional) Enforces user-specific access levels for users who authenticate for management access (see the aaa authentication console LOCAL command). This command enables management authorization for local users and for any users authenticated by RADIUS, LDAP, and TACACS+. See the “Limiting User CLI and ASDM Access with Management Authorization” section on page 34-13 for information about configuring a user on a AAA server to accommodate management authorization.</p> <p>For a local user, configure the level of access using the service-type command.</p>
Step 3	username username attributes Example: <pre>hostname(config)# username exampleuser1 attributes</pre>	<p>(Optional) Configures username attributes. The <i>username</i> argument is the username that you created in Step 1.</p>
Step 4	service-type {admin nas-prompt remote-access} Example: <pre>hostname(config-username)# service-type admin</pre>	<p>(Optional) Configures the user level if you configured management authorization in Step 2. The admin keyword allows full access to any services specified by the aaa authentication console LOCAL commands. The admin keyword is the default.</p> <p>The nas-prompt keyword allows access to the CLI when you configure the aaa authentication {telnet ssh serial} console LOCAL command, but denies ASDM configuration access if you configure the aaa authentication http console LOCAL command. ASDM monitoring access is allowed. If you enable authentication with the aaa authentication enable console LOCAL command, the user cannot access privileged EXEC mode using the enable command (or the login command).</p> <p>The remote-access keyword denies management access. The user cannot use any services specified by the aaa authentication console LOCAL commands (excluding the serial keyword; serial access is allowed).</p> <p>(Optional) If you are using this username for VPN authentication, you can configure many VPN attributes for the user. For more information, see the “Configuring Attributes for Specific Users” section on page 63-82.</p>

Examples

The following command assigns a privilege level of 15 to the admin user account:

```
hostname(config)# username admin password passw0rd privilege 15
```

The following command creates a user account with no password:

```
hostname(config)# username user34 nopassword
```

The following commands enable management authorization, create a user account with a password, enter username attributes configuration mode, and specify the service-type attribute:

```
hostname(config)# aaa authorization exec authentication-server  
hostname(config)# username user1 password g0ge0us  
hostname(config)# username user1 attributes  
hostname(config-username)# service-type nas-prompt
```

Identifying AAA Server Groups and Servers

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+.

You can have up to 100 server groups in single mode or 4 server groups per context in multiple mode. Each group can have up to 16 servers in single mode or 4 servers in multiple mode. When a user logs in, the servers are accessed one at a time starting with the first server you specify in the configuration, until a server responds. If all servers in the group are unavailable, the adaptive security appliance 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 adaptive security appliance continues to try the AAA servers.

How Fallback Works with Multiple Servers in a Group

If you configure multiple servers in a server group and you enable fallback to the local database for the server group, fallback occurs when no server in the group responds to the authentication request from the adaptive security appliance. To illustrate, consider this scenario:

You configure an LDAP server group with two Active Directory servers, server 1 and server 2, in that order. When the remote user logs in, the adaptive security appliance attempts to authenticate to server 1.

If server 1 responds with an authentication failure (such as *user not found*), the adaptive security appliance does not attempt to authenticate to server 2.

If server 1 does not respond within the timeout period (or the number of authentication attempts exceeds the configured maximum), the adaptive security appliance tries server 2.

If both servers in the group do not respond, and the adaptive security appliance is configured to fallback to the local database, the adaptive security appliance attempts to authenticate to the local database.

To create a server group and add AAA servers to it, perform the following steps:

	Command	Purpose
Step 1	aaa-server <i>server_group</i> protocol { kerberos ldap nt radius sdi tacacs+ } Example: <pre>hostname(config)# aaa-server servergroup1 protocol ldap hostname(config-aaa-server-group)#</pre>	<p>Identifies the server group name and the protocol. For example, to use RADIUS to authenticate network access and TACACS+ to authenticate CLI access, you need to create at least two server groups, one for RADIUS servers and one for TACACS+ servers.</p> <p>You can have up to 15 single-mode server groups or 4 multi-mode server groups. Each server group can have up to 16 servers in single mode or up to 4 servers in multi-mode.</p> <p>When you enter the aaa-server protocol command, you enter aaa-server group mode.</p>
Step 2	max-failed-attempts <i>number</i> Example: <pre>hostname(config-aaa-server-group)# max-failed-attempts 2</pre>	<p>Specifies the maximum number of requests sent to a AAA server in the group before trying the next server. The <i>number</i> argument can range from 1 and 5. The default is 3.</p> <p>If you configured a fallback method using the local database (for management access only; see the “Configuring Local Command Authorization” section on page 34-16 and the “Configuring TACACS+ Command Authorization” section on page 34-21 to configure the fallback mechanism), and all the servers in the group fail to respond, then the group is considered to be unresponsive, and the fallback method is tried. The server group remains marked as unresponsive for a period of 10 minutes (by default) so that additional AAA requests within that period do not attempt to contact the server group, and the fallback method is used immediately. To change the unresponsive period from the default, see the reactivation-mode command in the next step.</p> <p>If you do not have a fallback method, the adaptive security appliance continues to retry the servers in the group.</p>
Step 3	reactivation-mode { depletion [deadtime <i>minutes</i>] timed } Example: <pre>hostname(config-aaa-server-group)# reactivation-mode deadtime 20</pre>	<p>Specifies the method (reactivation policy) by which failed servers in a group are reactivated.</p> <p>The depletion keyword reactivates failed servers only after all of the servers in the group are inactive.</p> <p>The deadtime <i>minutes</i> argument specifies the amount of time in minutes, between 0 and 1440, that elapses between the disabling of the last server in the group and the subsequent reenabling of all servers. The default is 10 minutes.</p> <p>The timed keyword reactivates failed servers after 30 seconds of down time.</p>

	Command	Purpose
Step 4	accounting-mode simultaneous Example: <pre>hostname(config-aaa-server-group)# accounting-mode simultaneous</pre>	<p>Sends accounting messages to all servers in the group (RADIUS or TACACS+ only).</p> <p>To restore the default of sending messages only to the active server, enter the accounting-mode single command.</p>
Step 5	aaa-server server_group (interface_name) host server_ip Example: <pre>hostname(config)# aaa-server servergroup1 outside host 10.10.1.1 hostname(config-aaa-server-host)</pre>	<p>Identifies the server and the AAA server group to which it belongs.</p> <p>When you enter the aaa-server host command, you enter aaa-server host mode. As needed, use host mode commands to further configure the AAA server.</p> <p>The commands in host mode do not apply to all AAA server types. Table 33-2 lists the available commands, the server types to which they apply, and whether a new AAA server definition has a default value for that command. Where a command is applicable to the specified server type and no default value is provided (indicated by “—”), use the command to specify the value.</p>

Table 33-2 Host Mode Commands, Server Types, and Defaults

Command	Applicable AAA Server Types	Default Value
accounting-port	RADIUS	1646
acl-netmask-convert	RADIUS	standard
authentication-port	RADIUS	1645
kerberos-realm	Kerberos	—
key	RADIUS	—
	TACACS+	—
ldap-attribute-map	LDAP	—
ldap-base-dn	LDAP	—
ldap-login-dn	LDAP	—
ldap-login-password	LDAP	—
ldap-naming-attribute	LDAP	—
ldap-over-ssl	LDAP	—
ldap-scope	LDAP	—
maschapv2-capable	RADIUS	enabled
nt-auth-domain-controller	NT	—
radius-common-pw	RADIUS	—
retry-interval	Kerberos	10 seconds
	RADIUS	10 seconds
	SDI	10 seconds

Table 33-2 Host Mode Commands, Server Types, and Defaults (continued)

Command	Applicable AAA Server Types	Default Value
sasl-mechanism	LDAP	—
server-port	Kerberos	88
	LDAP	389
	NT	139
	SDI	5500
	TACACS+	49
server-type	LDAP	auto-discovery
timeout	All	10 seconds

Examples

[Example 33-1](#) shows commands that add one TACACS+ group with one primary and one backup server, one RADIUS group with a single server, and an NT domain server.

Example 33-1 Multiple AAA Server Groups and Servers

```
hostname(config)# aaa-server AuthInbound protocol tacacs+
hostname(config-aaa-server-group)# max-failed-attempts 2
hostname(config-aaa-server-group)# reactivation-mode depletion deadtime 20
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthInbound (inside) host 10.1.1.1
hostname(config-aaa-server-host)# key TACPlusUauthKey
hostname(config-aaa-server-host)# exit
hostname(config)# aaa-server AuthInbound (inside) host 10.1.1.2
hostname(config-aaa-server-host)# key TACPlusUauthKey2
hostname(config-aaa-server-host)# exit
hostname(config)# aaa-server AuthOutbound protocol radius
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key RadUauthKey
hostname(config-aaa-server-host)# exit
hostname(config)# aaa-server NTAAuth protocol nt
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server NTAAuth (inside) host 10.1.1.4
hostname(config-aaa-server-host)# nt-auth-domain-controller primary1
hostname(config-aaa-server-host)# exit
```

[Example 33-2](#) shows commands that configure a Kerberos AAA server group named watchdogs, add a AAA server to the group, and define the Kerberos realm for the server. Because [Example 33-2](#) does not define a retry interval or the port that the Kerberos server listens to, the adaptive security appliance uses the default values for these two server-specific parameters. [Table 33-2](#) lists the default values for all AAA server host mode commands.



Note

Kerberos realm names use numbers and upper-case letters only. Although the adaptive security appliance accepts lower-case letters for a realm name, it does not translate lower-case letters to upper-case letters. Be sure to use upper-case letters only.

Example 33-2 Kerberos Server Group and Server

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Configuring an LDAP Server

This section describes how to configure an LDAP directory with the adaptive security appliance for user authentication and VPN authorization and includes the following topics:

- [Authentication with LDAP, page 33-15](#)
- [Authorization with LDAP for VPN, page 33-17](#)
- [LDAP Attribute Mapping for Authorization, page 33-18](#)

Authentication with LDAP

During authentication, the adaptive security appliance acts as a client proxy to the LDAP server for the user, and authenticates to the LDAP server in either plain text or by using the SASL protocol. By default, the adaptive security appliance passes authentication parameters, usually a username and password, to the LDAP server in plain text. Whether using SASL or plain text, you can secure communications between the adaptive security appliance and the LDAP server with SSL using the **ldap-over-ssl** command.

**Note**

If you do not configure SASL, we strongly recommend that you secure LDAP communications with SSL using the **ldap-over-ssl** command.

When user LDAP authentication has succeeded, the LDAP server returns the attributes for the authenticated user. For VPN authentication, these attributes generally include authorization data that is applied to the VPN session. Thus, using LDAP accomplishes authentication and authorization in a single step.

Securing LDAP Authentication with SASL

The adaptive security appliance supports the following SASL mechanisms, listed in order of increasing strength:

- Digest-MD5—The adaptive security appliance responds to the LDAP server with an MD5 value computed from the username and password.
- Kerberos—The adaptive security appliance responds to the LDAP server by sending the username and realm using the GSSAPI Kerberos mechanism.

You can configure the adaptive security appliance and LDAP server to support any combination of these SASL mechanisms. If you configure multiple mechanisms, the adaptive security appliance retrieves the list of SASL mechanisms that are configured on the server and sets the authentication mechanism to the strongest mechanism configured on both the adaptive security appliance and the server. For example, if both the LDAP server and the adaptive security appliance support both mechanisms, the adaptive security appliance selects Kerberos, the stronger of the mechanisms.

Examples

The following example configures the adaptive security appliance for authentication to an LDAP directory server named `ldap_dir_1` using the digest-MD5 SASL mechanism, and communicating over an SSL-secured connection:

```
hostname(config)# aaa-server ldap_dir_1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
hostname(config-aaa-server-host)# sasl-mechanism digest-md5
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)#
```

Setting the LDAP Server Type

The adaptive security appliance supports LDAP version 3 and is compatible with the Sun Microsystems JAVA System Directory Server (formerly named the Sun ONE Directory Server), the Microsoft Active Directory, Novell, OpenLDAP, and other LDAPv3 directory servers.

By default, the adaptive security appliance auto-detects whether it is connected to Microsoft Active Directory, Sun LDAP, Novell, OpenLDAP, or a generic LDAPv3 directory server. However, if auto-detection fails to determine the LDAP server type, and you know the server is either a Microsoft, Sun or generic LDAP server, you can manually configure the server type using the keywords **sun**, **microsoft**, **novell**, **openldap**, or **generic**.

Examples

The following example sets the LDAP directory server “`ldap_dir_1`” to the Sun Microsystems type:

```
hostname(config)# aaa-server ldap_dir_1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
hostname(config-aaa-server-host)# server-type sun
hostname(config-aaa-server-host)#
```



Note

- The DN configured on the adaptive security appliance to access a Sun directory server must be able to access the default password policy on that server. We recommend using the directory administrator, or a user with directory administrator privileges, as the DN. Alternatively, you can place an ACI on the default password policy.
- You must configure LDAP over SSL to enable password management with Microsoft Active Directory and Sun servers.
- The adaptive security appliance does not support password management with Novell, OpenLDAP, and other LDAPv3 directory servers.
- The adaptive security appliance uses the Login Distinguished Name (DN) and Login Password to establish trust (bind) with an LDAP server. The Login DN represents a user record in the LDAP server that the administrator uses for binding. When binding, the adaptive security appliance authenticates to the server using the Login DN and the Login password. For example, when performing a Microsoft Active Directory read-only operation (such as authentication, authorization, or group-search), the adaptive security appliance can bind with a Login DN with fewer privileges. For example, the Login DN can be a user whose AD “Member Of” designation is part of Domain Users. For VPN password management operations, the Login DN needs elevated privileges and must be part of the Account Operators AD group. The following is an example of a Login DN:
`cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com`
- The adaptive security appliance supports the following authentication methods:

- Simple LDAP authentication with an unencrypted password on port 389
- Secure LDAP (LDAP-S) on port 636
- Simple Authentication and Security Layer (SASL) MD5
- SASL Kerberos



Note The adaptive security appliance does not support anonymous authentication.

Authorization with LDAP for VPN

When user LDAP authentication for VPN access has succeeded, the adaptive security appliance queries the LDAP server which returns LDAP attributes. These attributes generally include authorization data that applies to the VPN session. Thus, using LDAP accomplishes authentication and authorization in a single step.

There may be cases, however, where you require authorization from an LDAP directory server that is separate and distinct from the authentication mechanism. For example, if you use an SDI or certificate server for authentication, no authorization information is passed back. For user authorizations in this case, you can query an LDAP directory after successful authentication, accomplishing authentication and authorization in two steps.

To set up VPN user authorization using LDAP, perform the following steps:

	Command	Purpose
Step 1	aaa-server <i>server_group</i> protocol { kerberos ldap nt radius sdi tacacs+ } Example: hostname(config)# aaa-server servergroup1 protocol ldap hostname(config-aaa-server-group)	Creates a AAA server group.
Step 2	tunnel-group <i>groupname</i> Example: hostname(config)# tunnel-group remotegrp	Creates an IPSec remote access tunnel group named “remotegrp.”
Step 3	tunnel-group <i>groupname</i> general-attributes Example: hostname(config)# tunnel-group remotegrp general-attributes	Associates the server group and the tunnel group.
Step 4	authorization-server-group <i>group-tag</i> Example: hostname(config-general)# authorization-server-group ldap_dir_1	Assigns a new tunnel group to a previously created AAA server group for authorization.

Examples

While there are other authorization-related commands and options available for specific requirements, the following example shows fundamental commands for enabling user authorization with LDAP. The example then creates an IPsec remote access tunnel group named “remote-1,” and assigns that new tunnel group to the previously created “ldap_dir_1” AAA server group for authorization:

```
hostname(config)# tunnel-group remote-1 type ipsec-ra
hostname(config)# tunnel-group remote-1 general-attributes
hostname(config-general)# authorization-server-group ldap_dir_1
hostname(config-general)#
```

After you complete this fundamental configuration work, you can then configure additional LDAP authorization parameters such as a directory password, a starting point for searching a directory, and the scope of a directory search by entering the following commands:

```
hostname(config)# aaa-server ldap_dir_1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
hostname(config-aaa-server-host)# ldap-login-dn obscurepassword
hostname(config-aaa-server-host)# ldap-base-dn starthere
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)#
```

LDAP Attribute Mapping for Authorization

If you are introducing an adaptive security appliance to an existing LDAP directory, your existing LDAP attribute names and values are probably different from the current 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 adaptive security appliance. You can then bind these attribute maps to LDAP servers or remove them, as needed. You can also show or clear attribute maps.



Note

For more information about LDAP attribute maps, see [Active Directory/LDAP VPN Remote Access Authorization Use Cases](#), page C-16.

To create an unpopulated LDAP attribute map table, enter the following command:

Command	Purpose
<code>ldap attribute-map map-name</code>	Creates an unpopulated LDAP attribute map table named “att_map_1.”
Example: <code>hostname(config)# ldap attribute-map att_map_1</code> <code>hostname(config-ldap-attribute-map)</code>	

To map a user-defined attribute name to the Cisco attribute name, enter the following command:

Command	Purpose
<code>map-name user-attribute-name Cisco-attribute-name</code>	Maps the user-defined attribute name “department” to the Cisco attribute name “IETF-Radius-Class.”
Example: <code>hostname(config-ldap-attribute-map)# map-name</code> <code>department IETF-Radius-Class</code>	

To map a user-defined map value to the user-defined attribute value and the Cisco-defined attribute value, enter the following command:

Command	Purpose
map-value <i>user-attribute-name</i> <i>Cisco-attribute-name</i>	Maps the user-defined map value “department” to the user defined attribute value “Engineering” and the Cisco attribute value “group1.”
Example: <pre>hostname(config-ldap-attribute-map)# map-value department Engineering group1 hostname(config-ldap-attribute-map)</pre>	

To bind the attribute map to the LDAP server, enter the following commands:

	Command	Purpose
Step 1	aaa-server <i>server_group</i> (<i>interface_name</i>) host <i>server_ip</i> Example: <pre>hostname(config)# aaa-server ldap_dir_1 host 10.1.1.4</pre>	Identifies the server and the AAA server group to which it belongs. Creates the LDAP server group “ldap_dir_1” and identifies the host IP address “10.1.1.4” to which it is assigned.
Step 2	ldap-attribute-map <i>map-name</i> Example: <pre>hostname(config-aaa-server-host)# ldap-attribute-map att_map_1 hostname(config-aaa-server-host)</pre>	Binds the attribute map “att_map_1” to the LDAP server “ldap_dir_1.”


Note

The command to create an attribute map (**ldap attribute-map**) and the command to bind it to an LDAP server (**ldap-attribute-map**) differ only by a hyphen and the mode.

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

- IETF-Radius-Class—A department or user group
- IETF-Radius-Filter-Id—An access control list enforced on IPsec and SSL VPN clients
- IETF-Radius-Framed-IP-Address—A static IP address
- Banner1—A message displayed to VPN users at login
- Tunneling-Protocols—Allows or denies dial-in

Examples

The following example shows how to limit management sessions to the adaptive security appliance based on an LDAP attribute called accessType. The accessType attribute has three possible values:

- VPN
- admin
- helpdesk

Each value is mapped to one of the valid IETF RADIUS Service-Types that the adaptive security appliance supports: remote-access (Service-Type 5) Outbound, admin (Service-Type 6) Administrative, and nas-prompt (Service-Type 7) NAS Prompt:

```
hostname(config)# ldap attribute-map MGMT
hostname(config-ldap-attribute-map)# map-name accessType IETF-Radius-Service-Type
hostname(config-ldap-attribute-map)# map-value accessType VPN 5
hostname(config-ldap-attribute-map)# map-value accessType admin 6
hostname(config-ldap-attribute-map)# map-value accessType helpdesk 7

hostname(config-ldap-attribute-map)# aaa-server LDAP protocol ldap
hostname(config-aaa-server-group)# aaa-server LDAP (inside) host 10.1.254.91
hostname(config-aaa-server-host)# ldap-base-dn CN=Users,DC=cisco,DC=local
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-login-password test
hostname(config-aaa-server-host)# ldap-login-dn
CN=Administrator,CN=Users,DC=cisco,DC=local
hostname(config-aaa-server-host)# server-type auto-detect
hostname(config-aaa-server-host)# ldap-attribute-map MGMT
```

The following example shows how to display the complete list of Cisco LDAP attribute names:

```
hostname(config)# ldap attribute-map att_map_1
hostname(config-ldap-attribute-map)# map-name att_map_1?

ldap mode commands/options:
cisco-attribute-names:
  Access-Hours
  Allow-Network-Extension-Mode
  Auth-Service-Type
  Authenticated-User-Idle-Timeout
  Authorization-Required
  Authorization-Type
  :
  :
  X509-Cert-Data
hostname(config-ldap-attribute-map)#
```

Using Certificates and User Login Credentials

The following section describes the different methods of using certificates and user login credentials (username and password) for authentication and authorization. These methods apply to both IPsec and Clientless SSL VPN.

In all cases, LDAP authorization does not use the password as a credential. RADIUS authorization uses either a common password for all users or the username as a password.

This section includes the following topics:

- [Using User Login Credentials, page 33-20](#)
- [Using Certificates, page 33-21](#)

Using User Login Credentials

The default method for authentication and authorization uses the user login credentials.

- Authentication
 - Enabled by authentication server group setting

- Uses the username and password as credentials
- Authorization
 - Enabled by authorization server group setting
 - Uses the username as a credential

Using Certificates

If user digital certificates are configured, the adaptive security appliance first validates the certificate. It does not, however, use any of the DNs from certificates as a username for the authentication.

If both authentication and authorization are enabled, the adaptive security appliance uses the user login credentials for both user authentication and authorization.

- Authentication
 - Enabled by authentication server group setting
 - Uses the username and password as credentials
- Authorization
 - Enabled by authorization server group setting
 - Uses the username as a credential

If authentication is disabled and authorization is enabled, the adaptive security appliance uses the primary DN field for authorization.

- Authentication
 - DISABLED (set to None) by the authentication server group setting
 - No credentials used
- Authorization
 - Enabled by authorization server group setting
 - Uses the username value of the certificate primary DN field as a credential



Note

If the primary DN field is not present in the certificate, the adaptive security appliance uses the secondary DN field value as the username for the authorization request.

For example, consider a user certificate that includes the following Subject DN fields and values:

Cn=anyuser, OU=sales, O=XYZCorporation, L=boston, S=mass, C=us, ea=anyuser@example.com

If the Primary DN = EA (E-mail Address) and the Secondary DN = CN (Common Name), then the username used in the authorization request would be anyuser@example.com.

Differentiating User Roles Using AAA

This section includes the following topics:

- [Using Local Authentication, page 33-22](#)
- [Using RADIUS Authentication, page 33-22](#)
- [Using LDAP Authentication, page 33-23](#)

- [Using TACACS+ Authentication, page 33-23](#)

The adaptive security appliance enables you to distinguish between administrative and remote-access users when they authenticate using RADIUS, LDAP, TACACS+, or the local user database. User role differentiation can prevent remote access VPN and network access users from establishing an administrative connection to the adaptive security appliance.

To differentiate user roles, use the **service-type** attribute in username configuration mode. For RADIUS and LDAP (with the **ldap-attribute-map** command), you can use a Cisco Vendor-Specific Attribute (VSA), Cisco-Priv-Level, to assign a privilege level to an authenticated user.

Using Local Authentication

Before you configure the **service-type** attribute and privilege level when using local authentication, you must create a user, assign a password, and assign a privilege level. To do so, enter the following command:

```
hostname(config)# username admin password mysecret123 privilege 15
```

Where **myscret123** is the stored password and 15 is the assigned privilege level, which indicates an admin user.

The available configuration options for the **service-type** attribute include the following:

- **admin**, in which users are allowed access to the configuration mode. This option also allows a user to connect via remote access.
- **nas-prompt**, in which users are allowed access to the EXEC mode.
- **remote-access**, in which users are allowed access to the network.

The following example designates a **service-type** of **admin** for a user named admin:

```
hostname(config)# username admin attributes
hostname(config-username)# service-type admin
```

The following example designates a **service-type** of **remote-access** for a user named ra-user:

```
hostname(config)# username ra-user attributes
hostname(config-username)# service-type remote-access
```

Using RADIUS Authentication

The RADIUS IETF **service-type** attribute, when sent in an access-accept message as the result of a RADIUS authentication and authorization request, is used to designate which type of service is granted to the authenticated user. The supported attribute values are the following: administrative(6), nas-prompt(7), Framed(2), and Login(1).

For more information about using RADIUS authentication, see the [“Configuring an External RADIUS Server” section on page C-30](#). For more information about configuring RADIUS authentication for Cisco Secure ACS, see the Cisco Secure ACS documentation on Cisco.com.

The RADIUS Cisco VSA **privilege-level** attribute (Vendor ID 3076, sub-ID 220), when sent in an access-accept message, is used to designate the level of privilege for the user. For a list of supported RADIUS VSAs used for authorization, see the [“Configuring an External RADIUS Server” section on page C-30](#).

Using LDAP Authentication

When users are authenticated through LDAP, the native LDAP attributes and their values can be mapped to Cisco adaptive security appliance attributes to provide specific authorization features. For the supported list of LDAP VSAs used for authorization, see the [“Configuring an External LDAP Server” section on page C-3](#).

You can use the LDAP attribute mapping feature for LDAP authorization. For examples of this feature, see the [“Understanding Policy Enforcement of Permissions and Attributes” section on page C-2](#).

The following example shows how to define an LDAP attribute map. In this example, the security policy specifies that users being authenticated through LDAP map the user record fields or parameters title and company to the IETF-RADIUS service-type and privilege-level, respectively.

To define an LDAP attribute map, enter the following commands:

```
hostname(config)# ldap attribute-map admin-control
hostname(config-ldap-attribute-map)# map-name title IETF-RADIUS-Service-Type
hostname(config-ldap-attribute-map)# map-name company Privilege-Level
```

The following is sample output from the **ldap-attribute-map** command:

```
ldap attribute-map admin-control
  map-name company Privilege-Level
  map-name title IETF-Radius-Service-Type
```

To apply the LDAP attribute map to the LDAP AAA server, enter the following commands:

```
hostname(config)# aaa-server ldap-server (dmz1) host 10.20.30.1
hostname(config-aaa-server-host)# ldap-attribute-map admin-control
```



Note

When an authenticated user tries administrative access to the adaptive security appliance through ASDM, SSH, or Telnet, but does not have the appropriate privilege level to do so, the adaptive security appliance generates syslog message 113021. This message informs the user that the attempted login failed because of inappropriate administrative privileges.

Using TACACS+ Authentication

For information about how to configure TACACS+ authentication, see the [Configuring an External Server for Authorization and Authentication, page C-1](#).

AAA Servers Monitoring Commands

To monitor AAA Servers, enter one of the following commands:

Command	Purpose
<code>show aaa-server</code>	Shows the configured AAA server statistics.
	To clear the aaa server configuration, enter the clear aaa-server statistics command.

<code>show running-config aaa-server</code>	Shows the AAA server running configuration. To clear aaa server statistics, enter the clear configure aaa-server command.
<code>show running-config all ldap attribute-map</code>	Shows all LDAP attribute maps in the running configuration. To clear all LDAP attribute maps in the running configuration, use the clear configuration ldap attribute-map command.
<code>show running-config zonelabs-integrity</code>	Shows the Zone Labs Integrity server configuration. To clear the Zone Labs Integrity server configuration, use the clear configure zonelabs-integrity command.
<code>show ad-groups name [filter string]</code>	Applies only to AD servers using LDAP, and shows groups that are listed on an AD server.

Additional References

For additional information related to implementing LDAP mapping, see the following sections:

- [Related Documents, page 33-25](#)
- [RFCs, page 33-25](#)

Related Documents

Related Topic	Document Title
LDAP commands and AAA server host mode commands	<i>Cisco ASA 5500 Series Command Reference</i>
Example configuration procedures used to set up LDAP authentication or authorization	Configuring an External Server for Authorization and Authentication, page C-1
List of Cisco LDAP attribute names and values	
Extracting data from the HTTP GET and POST exchanges when using HTTP Form (if logging into the authenticating web server directly, instead of through the adaptive security appliance)	<i>Cisco ASA 5500 Series Configuration Guide using the CLI</i>

RFCs

RFC	Title
2138	Remote Authentication Dial In User Service (RADIUS)
2139	RADIUS Accounting
2548	Microsoft Vendor-specific RADIUS Attributes
2868	RADIUS Attributes for Tunnel Protocol Support

Feature History for AAA Servers

[Table 3](#) lists each feature change and the platform release in which it was implemented.

Table 3 Feature History for AAA Servers

Feature Name	Platform Releases	Feature Information
AAA Servers	7.0(1)	AAA Servers describes support for AAA and how to configure AAA servers and the local database.

