



CHAPTER 14

Configuring AAA Servers and the Local Database

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

This chapter includes the following sections:

- [AAA Overview, page 14-1](#)
- [AAA Server and Local Database Support, page 14-3](#)
- [Configuring AAA Server Groups, page 14-9](#)
- [Testing Server Authentication and Authorization, page 14-18](#)
- [Adding a User Account, page 14-18](#)
- [Configuring LDAP Attribute Maps, page 14-22](#)
- [Adding an Authentication Prompt, page 14-23](#)

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).

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.)

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 14-2](#)
- [About Authorization, page 14-2](#)
- [About Accounting, page 14-2](#)

About Authentication

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

- All administrative connections to the 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 authenticate. You can configure the security appliance to authorize the following items:

- Management commands
- Network access
- VPN access

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.

AAA Server and Local Database Support

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

This section contains the following topics:

- [Summary of Support, page 14-3](#)
- [RADIUS Server Support, page 14-4](#)
- [TACACS+ Server Support, page 14-4](#)
- [SDI Server Support, page 14-5](#)
- [NT Server Support, page 14-5](#)
- [Kerberos Server Support, page 14-5](#)
- [LDAP Server Support, page 14-6](#)
- [SSO Support for WebVPN with HTTP Forms, page 14-7](#)
- [Local Database Support, page 14-8](#)

Summary of Support

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

Table 14-1 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
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.

RADIUS Server Support

The security appliance supports RADIUS servers.

This section contains the following topics:

- [Authentication Methods, page 14-4](#)
- [Attribute Support, page 14-4](#)
- [RADIUS Authorization Functions, page 14-4](#)

Authentication Methods

The security appliance supports the following authentication methods with RADIUS:

- PAP—For all connection types.
- CHAP—For L2TP-over-IPSec.
- MS-CHAPv1—For L2TP-over-IPSec.
- MS-CHAPv2—For L2TP-over-IPSec, and for regular IPSec remote access connections when the password management feature is enabled.

Attribute Support

The 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.

RADIUS Authorization Functions

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

TACACS+ Server Support

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

SDI Server Support

The RSA SecurID servers are also known as SDI servers.

This section contains the following topics:

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

SDI Version Support

The security appliance supports SDI Version 5.0 and 6.0. 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 or 6.0 SDI server that you configure on the security appliance can be either the primary or any one of the replicas. See the “[SDI Primary and Replica Servers](#)” section on page 14-5 for information about how the SDI agent selects servers to authenticate users.

Two-step Authentication Process

SDI version 5.0 and 6.0 uses a two-step process to prevent an intruder from capturing information from an RSA SecurID authentication request and using it to authenticate to another server. The Agent first sends a lock request to the SecurID server before sending the user authentication request. The server locks the username, preventing another (replica) server from accepting it. This means that the same user cannot authenticate to two security appliances using the same authentication servers simultaneously. After a successful username lock, the security appliance sends the passcode.

SDI Primary and Replica Servers

The 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 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 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. This is a limitation of NTLM version 1.

Kerberos Server Support

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

**Note**

The 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 security appliance.

LDAP Server Support

This section describes LDAP server support, and includes the following topics:

- [Authentication with LDAP, page 14-6](#)
- [Securing LDAP Authentication with SASL, page 14-6](#)
- [LDAP Server Types, page 14-7](#)
- [Authorization with LDAP for VPN, page 14-7](#)

Authentication with LDAP

During authentication, the 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 using the Simple Authentication and Security Layer (SASL) protocol. By default, the 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 the communications between the security appliance and the LDAP server with SSL.

**Note**

If you do not configure SASL, we strongly recommend that you secure LDAP communications with SSL.

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 which is applied to the VPN session. Thus, using LDAP accomplishes authentication and authorization in a single step.

Securing LDAP Authentication with SASL

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

- Digest-MD5 — The security appliance responds to the LDAP server with an MD5 value computed from the username and password.
- Kerberos — The security appliance responds to the LDAP server by sending the username and realm using the GSSAPI (Generic Security Services Application Programming Interface) Kerberos mechanism.

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

LDAP Server Types

The 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, and other LDAPv3 directory servers.

By default, the security appliance auto-detects whether it is connected to a Microsoft Active Directory, a Sun LDAP directory server, 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.



Note

- Sun—The DN configured on the 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.
- Microsoft—You must configure LDAP over SSL to enable password management with Microsoft Active Directory.
- Generic—The security appliance does not support password management with a generic LDAPv3 directory server.

Authorization with LDAP for VPN

When user LDAP authentication for VPN access has succeeded, the 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.

SSO Support for WebVPN with HTTP Forms

The security appliance can use the HTTP Form protocol for single sign-on (SSO) authentication of WebVPN users only. Single sign-on support lets WebVPN users enter a username and password only once to access multiple protected services and Web servers. The WebVPN server running on the security appliance acts as a proxy for the user to the authenticating server. When a user logs in, the WebVPN server sends an SSO authentication request, including username and password, to the authenticating server using HTTPS. If the server approves the authentication request, it returns an SSO authentication cookie to the WebVPN server. The security appliance keeps this cookie on behalf of the user and uses it to authenticate the user to secure websites within the domain protected by the SSO server.

In addition to the HTTP Form protocol, WebVPN administrators can choose to configure SSO with the HTTP Basic and NTLM authentication protocols (the **auto-signon** command), or with Computer Associates eTrust SiteMinder SSO server (formerly Netegrity SiteMinder) as well. For an in-depth discussion of configuring SSO with either HTTP Forms, **auto-signon** or SiteMinder, see the [Clientless SSL VPN](#) chapter.

Local Database Support

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

This section contains the following topics:

- [User Profiles, page 14-8](#)
- [Fallback Support, page 14-8](#)

User Profiles

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

The **username attributes** command lets you enter the username mode. In this mode, you can add other information to a specific user profile. The information you can add includes VPN-related attributes, such as a VPN session timeout value.

Fallback Support

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

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 all are unavailable, the security appliance uses the local database to authenticate administrative access. This can include enable password authentication, too.
- **Command authorization**—When you use the **aaa authorization command** command, you can add the **LOCAL** keyword after the AAA server group tag. If the TACACS+ servers in the group all are unavailable, the local database is used to authorize commands based on privilege levels.
- **VPN authentication and authorization**—VPN authentication and authorization are supported to enable remote access to the 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 VPN client of an administrator specifies a tunnel group configured to fallback to the local database, the VPN tunnel can be established even if the AAA server group is unavailable, provided that the local database is configured with the necessary attributes.

Configuring AAA Server Groups

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

The security appliance contacts the first server in the group. If that server is unavailable, the security appliance contacts the next server in the group, if configured. If all servers in the group are unavailable, the 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 security appliance continues to try the AAA servers.

This section includes the following procedures:

- [Adding a Server Group, page 14-9](#)
- [Adding a Server to a Group, page 14-10](#)
- [AAA Server Parameters, page 14-11](#)

Adding a Server Group

To add a server group, perform the following steps:

Step 1 From the Configuration > Device Management > Users/AAA > AAA Server Groups > AAA Server Groups area, click **Add**.

The Add AAA Server Group dialog box appears.

Step 2 In the Server Group field, add a name for the group.

Step 3 From the Protocol drop-down list, choose the server type:

- **RADIUS**
- **TACACS+**
- **SDI**
- **NT Domain**
- **Kerberos**
- **LDAP**
- **HTTP Form**

Step 4 In the Accounting Mode field click the radio button for the mode you want to use (**Simultaneous** or **Single**).

In Single mode, the security appliance sends accounting data to only one server.

In Simultaneous mode, the security appliance sends accounting data to all servers in the group.



Note This option is not available for the HTTP Form protocol.

Step 5 In the Reactivation Mode field, click the radio button for the mode you want to use (**Depletion** or **Timed**).

In Depletion mode, failed servers are reactivated only after all of the servers in the group are inactive.

In Timed mode, failed servers are reactivated after 30 seconds of down time.



Note This option is not available for the HTTP Form protocol.

Step 6 If you chose Depletion reactivation mode, add a time interval in the Dead Time field.
The Dead Time is the duration of time, in minutes, to elapse between the disabling of the last server in a group and the subsequent reenabling of all servers.

Step 7 In the Max Failed Attempts field, add the number of failed attempts permitted.
This option sets the number of failed connection attempts allowed before declaring a nonresponsive server to be inactive.



Note This option is not available for the HTTP Form protocol.

Step 8 Click **OK**.
The dialog box closes and the server group is added to the AAA server groups table.

Step 9 In the AAA Server Groups dialog box, click **Apply** to save the changes.
The changes are saved.

Adding a Server to a Group

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

-
- Step 1** From the Configuration > Device Management > Users/AAA > AAA Server Groups > AAA Server Groups area, click the server group to which you want to add a server.
The row is highlighted in the table.
- Step 2** In the Servers in the Selected Group area (lower pane), click **Add**.
The Add AAA Server Group dialog box appears for the server group.
- Step 3** From the Interface Name drop-down menu, choose the interface name where the authentication server resides.
- Step 4** In the Server Name or IP Address field, add either a server name or IP address for the server you are adding to the group.
- Step 5** In the Timeout field, either add a timeout value or keep the default. The timeout is the duration of time, in seconds, that the security appliance waits for a response from the primary server before sending the request to the backup server.
- Step 6** The other parameters available depend on the server type. See the following sections for parameters unique to each server type:
- [RADIUS Server Fields, page 14-11](#)
 - [TACACS+ Server Fields, page 14-13](#)
 - [SDI Server Fields, page 14-13](#)
 - [Windows NT Domain Server Fields, page 14-13](#)

- [Kerberos Server Fields, page 14-14](#)
- [LDAP Server Fields, page 14-15](#)
- [HTTP Form Server Fields, page 14-17](#)

Step 7 Click **OK**.

The dialog box closes and the AAA server is added to the AAA server group.

Step 8 In the AAA Server Groups pane, click **Apply** to save the changes.

The changes are saved.

AAA Server Parameters


The following sections list the unique fields for each server type when adding a server to a server group (see the [“Adding a Server to a Group”](#) section on page 14-10):

- [RADIUS Server Fields, page 14-11](#)
- [TACACS+ Server Fields, page 14-13](#)
- [SDI Server Fields, page 14-13](#)
- [Windows NT Domain Server Fields, page 14-13](#)
- [Kerberos Server Fields, page 14-14](#)
- [LDAP Server Fields, page 14-15](#)
- [HTTP Form Server Fields, page 14-17](#)

RADIUS Server Fields

The following table describes the unique fields for configuring RADIUS servers, for use with the [“Adding a Server to a Group”](#) section on page 14-10.

Field	Description
Server Authentication Port	The server port to be used for authentication of users. The default port is 1645.
Server Accounting Port	The server port to be used for accounting of users. The default port is 1646.
Retry Interval	The duration of time, 1 to 10 seconds, that the security appliance waits between attempts to contact the server.
Server Secret Key	The shared secret key used to authenticate the RADIUS server to the security appliance. The server secret you configure here should match the one configured on the RADIUS server. If you do not know the server secret, ask the RADIUS server administrator. The maximum field length is 64 characters.

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

TACACS+ Server Fields

The following table describes the unique fields for configuring TACACS+ servers, for use with the [“Adding a Server to a Group”](#) section on page 14-10.

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

SDI Server Fields

The following table describes the unique fields for configuring SDI servers, for use with the [“Adding a Server to a Group”](#) section on page 14-10.

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

Windows NT Domain Server Fields

The following table describes the unique fields for configuring Windows NT Domain servers, for use with the [“Adding a Server to a Group”](#) section on page 14-10.

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

Kerberos Server Fields

The following table describes the unique fields for configuring Kerberos servers, for use with the [“Adding a Server to a Group”](#) section on page 14-10.

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

LDAP Server Fields

The following table describes the unique fields for configuring LDAP servers, for use with the [“Adding a Server to a Group”](#) section on page 14-10.

Field	Description
Enable LDAP over SSL check box	When checked, SSL secures communications between the security appliance and the LDAP server. Also called secure LDAP (LDAP-S). Note If you do not configure SASL protocol, we strongly recommend that you secure LDAP communications with SSL.
Server Port	TCP port number 389, the port which the security appliance uses to access the LDAP server for simple (non-secure) authentication or TCP port 636 for secure authentication (LDAP-S). All LDAP servers support authentication and authorization. Only Microsoft AD and Sun LDAP servers additionally provide VPN remote access password management capability, which requires LDAP-S.
Server type	A drop-down list for choosing one of the following LDAP server types: <ul style="list-style-type: none"> • Detect Automatically/Use Generic Type • Microsoft • Novell • OpenLDAP • Sun
Base DN	The Base Distinguished Name (DN), or location in the LDAP hierarchy where the server should begin searching when it receives an LDAP request. For example, OU=people, dc=cisco, dc=com.
Scope	The extent of the search the server should make in the LDAP hierarchy when it receives an authorization request. The available options are: <ul style="list-style-type: none"> • One Level: Searches only one level beneath the Base DN. This option is quicker. • All Levels: Searches all levels beneath the Base DN; in other words, search the entire subtree hierarchy. This option takes more time.
Naming Attribute(s)	The Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server. Common naming attributes are Common Name (CN), sAMAccountName, userPrincipalName, and User ID (uid).

Field	Description
Login DN	<p>The 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.</p> <p>When binding, the security appliance authenticates to the server using the Login DN and the Login Password. When performing a Microsoft Active Directory read-only operation (such as for authentication, authorization, or group-search), the security appliance can bind with a Login DN with less 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.</p> <p>An example of a Login DN include:</p> <pre>cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com</pre> <p>The security appliance supports:</p> <ul style="list-style-type: none"> • 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. <p>The security appliance does not support anonymous authentication.</p>
Login Password	The password for the Login DN user account. The characters you type are replaced with asterisks.
LDAP Attribute Map	The LDAP attribute maps that you can apply to LDAP server. Used to map Cisco attribute names to user-defined attribute names and values. See the “Configuring LDAP Attribute Maps” section on page 14-22 .
SASL MD5 authentication check box	When checked, the MD5 mechanism of the Simple Authentication and Security Layer (SASL) authenticates communications between the security appliance and the LDAP server.
SASL Kerberos authentication	When checked, the Kerberos mechanism of the SASL secures authentication communications between the security appliance and the LDAP server.
Kerberos Server Group	The Kerberos server or server group used for authentication. The Kerberos Server group option is disabled by default and is enabled only when SASL Kerberos authentication is chosen.

Field	Description
Group Base DN	Used only for Active Directory servers using LDAP protocol. This DN specifies the location in the LDAP hierarchy to begin searching for the AD groups. That is, the list of memberOf enumerations. If this field is not configured, the security appliance uses the Base DN for AD group retrieval. ASDM uses the list of retrieved AD groups to define AAA selection criterion for dynamic access policies. For more information, see the show ad-groups command in CLI Command Reference Guide.
Group Search Timeout	Specifies the maximum time to wait for a response from an Active Directory server queried for available groups.

HTTP Form Server Fields

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.

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 *Cisco Security Appliance Command Line Configuration Guide*, for more detail on extracting these parameters from the HTTP exchanges.

The following table describes the unique fields for configuring HTTP Form servers, for use with the [“Adding a Server to a Group” section on page 14-10](#).

Field	Description
Start URL	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	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	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	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.

Field	Description
Hidden Values	The 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) 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.

Testing Server Authentication and Authorization

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

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

Adding a User Account

The local database is used for the following features:

- ASDM per-user access

By default, you can log into ASDM with a blank username and the enable password (see [Device Name/Password, page 6-12](#)). However, if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.



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

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

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

- Command authorization

If you turn on command authorization using the local database, then the security appliance refers to the user privilege level to determine what commands are available. Otherwise, the privilege level is not generally used. By default, all commands are either privilege level 0 or level 15. ASDM allows you to enable three predefined privilege levels, with commands assigned to level 15 (Admin), level 5 (Read Only), and level 3 (Monitor Only). If you use the predefined levels, then assign users to one of these three privilege levels.

- Network access authentication
- VPN client authentication

You cannot use the local database for network access authorization.

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

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

-
- Step 1** From the Configuration > Device Management > Users/AAA > User Accounts pane, click **Add**.
The Add User Account—Identity dialog box appears.
- Step 2** In the Username field, add a username between 4 to 64 characters long.
- Step 3** In the Password field add a password between 3 and 32 characters. Entries are case-sensitive. The field displays only asterisks. To protect security, we recommend a password length of at least 8 characters.
- Step 4** In the Confirm Password field, add the password again.
For security purposes, only asterisks appear in the password fields.
- Step 5** To enable MSCHAP authentication, check **User authenticated using MSCHAP**.
This option specifies that the password is converted to unicode and hashed using MD4 after you enter it. Use this feature if users are authenticated using MSCHAPv1 or MSCHAPv2.
- Step 6** To specify the VPN groups that the user belongs to, enter a group name in the Member of field, and click **Add**.
To delete a VPN group, choose the group in the window, and click **Delete**.
- Step 7** In the Access Restriction area, set the management access level for a user. You must first enable management authorization using the **Perform authorization for exec shell access** option on the Configuration > Device Management > Users/AAA > AAA Access > Authorization tab.
Choose one of the following options:

- **Full Access (ASDM, Telnet, SSH and console)**—If you configure authentication for management access using the local database, then this option lets the user use ASDM, SSH, Telnet, and the console port. If you also configure enable authentication, then the user can access global configuration mode.
 - **Privilege Level**—Selects the privilege level for this user to use with local command authorization. The range is 0 (lowest) to 15 (highest).
- **CLI login prompt for SSH, Telnet and console (no ASDM access)**—If you configure authentication for management access using the local database, then this option lets the user use SSH, Telnet, and the console port. The user cannot use ASDM for configuration (if you configure HTTP authentication). ASDM monitoring is allowed. If you also configure enable authentication, then the user cannot access global configuration mode.
- **No ASDM, SSH, Telnet, or console access**—If you configure authentication for management access using the local database, then this option disallows the user from accessing any management access method for which you configured authentication (excluding the Serial option; serial access is allowed).

Step 8 If you want to configure VPN policy attributes for this user, see the “[Configuring VPN Policy Attributes for a User](#)” section on page 14-20.

Step 9 Click **Apply**.

The user is added to the local security appliance database and changes are saved to the running configuration.



Note

To configure the enable password from the User Accounts pane (instead of in [Device Name/Password, page 6-12](#)), change the password for the enable_15 user. The enable_15 user is always present in this pane, and represents the default username. This method of configuring the enable password is the only method available in ASDM for the system configuration. If you configured other enable level passwords at the CLI (**enable password 10**, for example), then those users are listed as enable_10, etc.

Configuring VPN Policy Attributes for a User

By default, each user inherits the settings set in the VPN policy. To override the settings, you can customize VPN attributes by performing the following steps:

Step 1 If you have not already added a user according to the “[Adding a User Account](#)” section on page 14-18, from the Configuration > Device Management > Users/AAA > User Accounts pane, click **Add**.

The Add User Account—Identity dialog box appears.

Step 2 In the left-hand pane, click **VPN Policy**.

By default, the Inherit check box is checked for each option, which means the user account inherits the settings from the VPN policy. To override each setting, uncheck **Inherit**, and fill in a new value:

- **Group Policy**—Choose a group policy from the list.
- **Tunneling Protocols**—Specifies what tunneling protocols that this user can use, or whether to inherit the value from the group policy. Check the desired Tunneling Protocols check boxes to select the VPN tunneling protocols that this user can use. Users can use only the selected protocols. The choices are as follows:

- IPsec—IP Security Protocol. IPsec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. Both LAN-to-LAN (peer-to-peer) connections and client-to-LAN connections can use IPsec.
- Clientless SSL VPN—VPN via SSL/TLS. Uses a web browser to establish a secure remote-access tunnel to a VPN Concentrator; requires neither a software nor hardware client. Clientless SSL VPN can provide easy access to a broad range of enterprise resources, including corporate websites, web-enabled applications, NT/AD file share (web-enabled), e-mail, and other TCP-based applications from almost any computer that can reach HTTPS Internet sites.
- SSL VPN Client—Lets users connect after downloading the Cisco AnyConnect Client application. Users use a clientless SSL VPN connection to download this application the first time. Client updates then occur automatically as needed whenever the user connects.
- L2TP over IPsec—Allows remote users with VPN clients provided with several common PC and mobile PC operating systems to establish secure connections over the public IP network to the security appliance and private corporate networks.



Note If no protocol is selected, an error message appears.

- Filter—Specifies what filter to use, or whether to inherit the value from the group policy. Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the security appliance, based on criteria such as source address, destination address, and protocol. To configure filters and rules, see the Configuration > VPN > VPN General > Group Policy pane.
- Manage—Displays the ACL Manager pane, on which you can add, edit, and delete Access Control Lists (ACLs) and Extended Access Control Lists (ACEs).
- Tunnel Group Lock—Specifies whether to inherit the tunnel group lock or to use the selected tunnel group lock, if any. Selecting a specific lock restricts users to remote access through this group only. Tunnel Group Lock restricts users by checking if the group configured in the VPN client is the same as the user's assigned group. If it is not, the security appliance prevents the user from connecting. If the Inherit check box is not selected, the default value is --None--.
- Store Password on Client System—Specifies whether to inherit this setting from the group. Deselecting the Inherit check box activates the Yes and No radio buttons. Selecting Yes stores the login password on the client system (potentially a less-secure option). Selecting No (the default) requires the user to enter the password with each connection. For maximum security, we recommend that you *not do allow* password storage. This parameter has no bearing on interactive hardware client authentication or individual user authentication for a VPN 3002.

Step 3 To change Connection Settings, uncheck **Inherit**, and fill in a new value:

- Access Hours—If the Inherit check box is not selected, you can select the name of an existing access hours policy, if any, applied to this user or create a new access hours policy. The default value is Inherit, or, if the Inherit check box is not selected, the default value is --Unrestricted--.
- New—Opens the Add Time Range dialog box, on which you can specify a new set of access hours.
- Simultaneous Logins—If the Inherit check box is not selected, this parameter specifies the maximum number of simultaneous logins allowed for this user. The default value is 3. The minimum value is 0, which disables login and prevents user access.



Note While there is no maximum limit, allowing several simultaneous connections could compromise security and affect performance.

- **Maximum Connect Time**—If the **Inherit** check box is not selected, this parameter specifies the maximum user connection time in minutes. At the end of this time, the system terminates the connection. The minimum is 1 minute, and the maximum is 2147483647 minutes (over 4000 years). To allow unlimited connection time, select the **Unlimited** check box (the default).
 - **Idle Timeout**—If the **Inherit** check box is not selected, this parameter specifies this user's idle timeout period in minutes. If there is no communication activity on the user's connection in this period, the system terminates the connection. The minimum time is 1 minute, and the maximum time is 10080 minutes. This value does not apply to users of clientless SSL VPN connections.
- Step 4** To set a dedicated IP address for this user, enter an IP address and subnet mask in the **Dedicated IP Address (Optional)** area.
- Step 5** To configure clientless SSL settings, in the left-hand pane, click **Clientless SSL VPN**.
To override each setting, uncheck **Inherit**, and fill in a new value. See the “[Group Policies](#)” section on page 35-4.
- Step 6** To configure SSL VPN settings, in the left-hand pane, click **SSL VPN Client**.
To override each setting, uncheck **Inherit**, and fill in a new value. See the “[Configuring SSL VPN Connections](#)” section on page 35-34.
- Step 7** Click **Apply**.
-

Configuring LDAP Attribute Maps

If you are introducing a security appliance to an existing LDAP directory, your existing LDAP attribute names and values are probably different from the existing ones. You must create LDAP attribute maps that map your existing user-defined attribute names and values to Cisco attribute names and values that are compatible with the 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

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

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

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

For a list of Cisco LDAP attribute names and values, see [Appendix C, “Configuring an External LDAP Server”](#).

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

- Step 1** From the Configuration > Remote Access VPN > AAA Local Users > LDAP Attribute Map pane, click **Add**.

The Add LDAP Attribute Map dialog box appears with the Map Name tab active.

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

Adding an Authentication Prompt

You can specify text to display to the user during the AAA authentication challenge process. You can specify the AAA challenge text for HTTP, FTP, and Telnet access through the 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 you do not specify an authentication prompt, users will see the following when authenticating with a RADIUS or TACACS+ server:

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

To add an authentication prompt, perform the following steps:

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

The following are maximum characters allowed for authentication prompts:

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

Step 2 In the Messages area, add messages in the User accepted message and User rejected message fields. If the user authentication occurs from Telnet, you can use the User accepted message and User rejected message options to display different status prompts to indicate that the authentication attempt is accepted or rejected by the AAA server.

If the AAA server authenticates the user, the 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.

Step 3 Click **Apply**.

The changes are saved to the running configuration.
