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 32-1
- AAA Server and Local Database Support, page 32-3
- Configuring AAA Server Groups, page 32-8
- Testing Server Authentication and Authorization, page 32-18
- Adding a User Account, page 32-18
- Configuring LDAP Attribute Maps, page 32-22
- Adding an Authentication Prompt, page 32-23
- AAA Servers Monitoring, page 32-24
- Additional References, page 32-25
- Feature History for AAA Servers, page 32-26

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 32-2
- About Authorization, page 32-2
- About Accounting, page 32-3
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 32-3
- RADIUS Server Support, page 32-4
- TACACS+ Server Support, page 32-5
- RSA/SDI Server Support, page 32-5
- NT Server Support, page 32-6
- Kerberos Server Support, page 32-6
- LDAP Server Support, page 32-7
- HTTP Forms Authentication for Clientless SSL VPN, page 32-7
- Local Database Support, page 32-7

Summary of Support

Table 32-1 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>
<thead>
<tr>
<th>AAA Service</th>
<th>Database Type</th>
<th>Database Type</th>
<th>Database Type</th>
<th>Database Type</th>
<th>Database Type</th>
<th>Database Type</th>
<th>Database Type</th>
<th>Database Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Local</td>
<td>RADIUS</td>
<td>TACACS+</td>
<td>SDI (RSA)</td>
<td>NT</td>
<td>Kerberos</td>
<td>LDAP</td>
<td>HTTP Form</td>
</tr>
<tr>
<td>Authentication of...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN users</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Firewall sessions</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Administrators</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Authorization of...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN users</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Firewall sessions</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administrators</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Accounting of...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 32-1 Summary of AAA Support
AAA Server and Local Database Support

Chapter 32 Configuring AAA Servers and the Local Database

Table 32-1 Summary of AAA Support (continued)

<table>
<thead>
<tr>
<th>AAA Service</th>
<th>Database Type</th>
<th>Local</th>
<th>RADIUS</th>
<th>TACACS+</th>
<th>SDI (RSA)</th>
<th>NT</th>
<th>Kerberos</th>
<th>LDAP</th>
<th>HTTP Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN connections</td>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Firewall sessions</td>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administrators</td>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

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.

In addition to the native protocol authentication listed in 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/SDI to RADIUS connections,

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 32-6
- Two-step Authentication Process, page 32-6
- RSA/SDI Primary and Replica Servers, page 32-6
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 32-6 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 actions 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.
LDAP Server Support

The adaptive security appliance supports LDAP. For detailed information, see the “Configuring LDAP Attribute Maps” section on page 32-22.

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 32-7
- Fallback Support, page 32-7

User Profiles

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

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 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+.

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 that 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 this further, 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.

This section includes the following topics:
- Adding a Server Group, page 32-8
- Adding a Server to a Group, page 32-10
- AAA Server Parameters, page 32-10

### Adding a Server Group

To add a server group, perform the following steps:

**Step 1** Choose Configuration > Device Management > Users/AAA > AAA Server Groups.

**Step 2** In the AAA Server Groups area, click Add.
The Add AAA Server Group dialog box appears.

**Step 3** In the Server Group field, add a name for the group.

**Step 4** From the Protocol drop-down list, choose the server type:
- RADIUS
- TACACS+
- SDI
- NT Domain
- Kerberos
- LDAP
- HTTP Form

**Step 5** In the Accounting Mode field, click the radio button for the mode you want to use (**Simultaneous** or **Single**).

In Single mode, the adaptive security appliance sends accounting data to only one server.
In Simultaneous mode, the adaptive security appliance sends accounting data to all servers in the group.

**Note** This option is not available for the following protocols: HTTP Form, SDI, NT, Kerberos, and LDAP.

**Step 6** In the Reactivation Mode field, click the radio button for the mode you want to use (**Depletion** or **Timed**).

In Depletion mode, failed servers are reactivated only after all of the servers in the group are inactive.
In Timed mode, failed servers are reactivated after 30 seconds of down time.

**Step 7** If you chose the Depletion reactivation mode, add a time interval in the Dead Time field.

The Dead Time is the duration of time, in minutes, that elapses between the disabling of the last server in a group and the subsequent reenabling of all servers.

**Step 8** In the Max Failed Attempts field, add the number of failed attempts permitted.

This option sets the number of failed connection attempts allowed before declaring a nonresponsive server to be inactive.

**Step 9** (Optional) If you are adding a RADIUS server type, perform the following steps:

a. Check the **Enable interim accounting update** check box if you want to enable multi-session accounting for clientless SSL and AnyConnect sessions.

b. Click the **VPN3K Compatibility Option** to expand the list, and click one of the following radio buttons to specify whether or not a downloadable ACL received from RADIUS should be merged with a Cisco AV-pair ACL:
   - Do not merge
   - Place the downloadable ACL after Cisco AV-pair ACL
   - Place the downloadable ACL before Cisco AV-pair ACL

**Step 10** Click **OK**.

The dialog box closes, and the server group is added to the AAA Server Groups table.

**Step 11** In the AAA Server Groups dialog box, click **Apply** to save the changes.
The changes are saved to the running configuration.

## Adding a Server to a Group

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

**Step 1** Choose Configuration > Device Management > Users/AAA > AAA Server Groups, and in the 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 list, choose the interface name on which 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 that 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 adaptive 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 that are unique to each server type:

- RADIUS Server Fields, page 32-11
- TACACS+ Server Fields, page 32-12
- SDI Server Fields, page 32-13
- Windows NT Domain Server Fields, page 32-13
- Kerberos Server Fields, page 32-13
- LDAP Server Fields, page 32-15
- HTTP Form Server Fields, page 32-17

**Step 7** Click OK. The Add AAA Server Group 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 to the running configuration.

## AAA Server Parameters

The following sections list the unique fields for each server type when you add a server to a server group:

- RADIUS Server Fields, page 32-11
- TACACS+ Server Fields, page 32-12
- SDI Server Fields, page 32-13
For more information, see the “Adding a Server to a Group” section on page 32-10.

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 32-10.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Authentication Port</td>
<td>The server port to be used for authentication of users. The default port is 1645.</td>
</tr>
<tr>
<td>Server Accounting Port</td>
<td>The server port to be used for accounting of users. The default port is 1646.</td>
</tr>
<tr>
<td>Retry Interval</td>
<td>The duration of time, 1 to 10 seconds, that the adaptive security appliance waits between attempts to contact the server.</td>
</tr>
<tr>
<td>Server Secret Key</td>
<td>The shared secret key used to authenticate the RADIUS server to the adaptive 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.</td>
</tr>
<tr>
<td>Common Password</td>
<td>A case-sensitive password that is common among users who access this RADIUS authorization server through this adaptive security appliance. Be sure to provide this information to your RADIUS server administrator.</td>
</tr>
</tbody>
</table>

Note For an authentication RADIUS server (rather than authorization) do not configure a common password.

If you leave this field blank, the users username is the password for accessing this RADIUS authorization server.

Never use a RADIUS authorization server for authentication. Common passwords or usernames as passwords are less secure than assigning unique user passwords.

Note Although the password is required by the RADIUS protocol and the RADIUS server, users do not need to know it.
Chapter 32      Configuring AAA Servers and the Local Database

Configuring AAA Server Groups

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 32-10.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Port</td>
<td>The port to be used for this server.</td>
</tr>
<tr>
<td>Server Secret Key</td>
<td>The shared secret key used to authenticate the TACACS+ server to the adaptive security appliance. The server secret that you configure here should match the one that is 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.</td>
</tr>
</tbody>
</table>
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 32-10.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Port</td>
<td>The TCP port number by which this server is accessed.</td>
</tr>
<tr>
<td>Retry Interval</td>
<td>The duration of time, 1 to 10 seconds, that the adaptive security appliance waits between attempts to contact the server.</td>
</tr>
</tbody>
</table>

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 32-10.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Port</td>
<td>Port number 139, or the TCP port number used by the adaptive security appliance to communicate with the Windows NT server.</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 32-10.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Port</td>
<td>Server port number 88, or the UDP port number over which the adaptive security appliance communicates with the Kerberos server.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Retry Interval | The duration of time, 1 to 10 seconds, that the adaptive security appliance waits between attempts to contact the server.
Realm | The name of the Kerberos realm. For example:
- EXAMPLE.COM
- EXAMPLE.NET
- EXAMPLE.ORG

**Note** | Most Kerberos servers require the realm to be all uppercase for authentication to succeed.

The maximum length is 64 characters. The following types of servers require that you enter the realm name in all uppercase letters:
- Windows 2000
- Windows XP
- Windows.NET

You must enter the correct realm name for the server whose IP address you entered in the Server IP Address field.
## 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 32-10.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable LDAP over SSL check box</td>
<td>When checked, SSL secures communications between the adaptive security appliance and the LDAP server. Also called secure LDAP (LDAP-S).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you do not configure the SASL protocol, we strongly recommend that you secure LDAP communications with SSL.</td>
</tr>
<tr>
<td>Server Port</td>
<td>TCP port number 389, the port which the adaptive 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 a VPN remote access password management capability, which requires LDAP-S.</td>
</tr>
<tr>
<td>Server type</td>
<td>A drop-down list for choosing one of the following LDAP server types:</td>
</tr>
<tr>
<td></td>
<td>• Detect Automatically/Use Generic Type</td>
</tr>
<tr>
<td></td>
<td>• Microsoft</td>
</tr>
<tr>
<td></td>
<td>• Novell</td>
</tr>
<tr>
<td></td>
<td>• OpenLDAP</td>
</tr>
<tr>
<td></td>
<td>• Sun</td>
</tr>
<tr>
<td>Base DN</td>
<td>The Base Distinguished Name, 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).</td>
</tr>
<tr>
<td>Scope</td>
<td>The extent of the search the server should make in the LDAP hierarchy when it receives an authorization request. The available options are:</td>
</tr>
<tr>
<td></td>
<td>• One Level: Searches only one level beneath the Base DN. This option is quicker.</td>
</tr>
<tr>
<td></td>
<td>• All Levels: Searches all levels beneath the Base DN; in other words, searches the entire subtree hierarchy. This option takes more time.</td>
</tr>
<tr>
<td>Naming Attribute(s)</td>
<td>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).</td>
</tr>
</tbody>
</table>
## Chapter 32 Configuring AAA Servers and the Local Database

### Configuring AAA Server Groups

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. 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:

- 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

The adaptive security appliance does not support anonymous authentication.

### Login DN

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. 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:

- 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

The adaptive security appliance does not support anonymous authentication.

### 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 32-22.

### SASL MD5 authentication check box

When checked, the MD5 mechanism of the SASL authenticates communications between the adaptive security appliance and the LDAP server.

### SASL Kerberos authentication

When checked, the Kerberos mechanism of the SASL secures authentication communications between the adaptive 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login DN</td>
<td>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. 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</td>
</tr>
<tr>
<td>Login Password</td>
<td>The password for the Login DN user account. The characters you type are replaced with asterisks.</td>
</tr>
<tr>
<td>LDAP Attribute Map</td>
<td>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 32-22.</td>
</tr>
<tr>
<td>SASL MD5 authentication check box</td>
<td>When checked, the MD5 mechanism of the SASL authenticates communications between the adaptive security appliance and the LDAP server.</td>
</tr>
<tr>
<td>SASL Kerberos authentication</td>
<td>When checked, the Kerberos mechanism of the SASL secures authentication communications between the adaptive security appliance and the LDAP server.</td>
</tr>
<tr>
<td>Kerberos Server Group</td>
<td>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.</td>
</tr>
</tbody>
</table>
Chapter 32 Configuring AAA Servers and the Local Database

Configuring AAA Server 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 adaptive security appliance.

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 32-10.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Base DN</td>
<td>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 adaptive security appliance uses the Base DN for AD group retrieval. ASDM uses the list of retrieved AD groups to define AAA selection criteria for dynamic access policies. For more information, see the show ad-groups command.</td>
</tr>
<tr>
<td>Group Search Timeout</td>
<td>Specifies the maximum time to wait for a response from an AD server that was queried for available groups.</td>
</tr>
<tr>
<td>Start URL</td>
<td>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.</td>
</tr>
<tr>
<td>Action URI</td>
<td>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.</td>
</tr>
<tr>
<td>Username</td>
<td>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.</td>
</tr>
<tr>
<td>Password</td>
<td>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.</td>
</tr>
</tbody>
</table>
Chapter 32      Configuring AAA Servers and the Local Database

Testing Server Authentication and Authorization

To determine whether the adaptive 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 in which the server resides. The row is highlighted in the table.

Step 2  From the Servers in the Selected Group table, click the server that you want to test. The row is highlighted in the table.

Step 3  Click Test. The Test AAA Server dialog box appears for the selected 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 adaptive 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 the “Configuring the Hostname, Domain Name, and Passwords” section on page 9-1). 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.
Adding a User Account

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 adaptive security appliance refers to the user privilege level to determine which 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 adaptive security appliance local database, perform the following steps:

**Step 1** Choose **Configuration > Device Management > Users/AAA > User Accounts**, and then click **Add**.

The Add User Account-Identity dialog box appears.

**Step 2** In the Username field, add a username from 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 (see the “Configuring Authentication for CLI, ASDM, and enable command Access” section on page 33-11), then this option lets the user use ASDM, SSH, Telnet, and the console port. If you also 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) See the “Configuring Command Authorization” section on page 33-13 for more information.

• **CLI login prompt for SSH, Telnet and console (no ASDM access)**—If you configure authentication for management access using the local database (see the “Configuring Authentication for CLI, ASDM, and enable command Access” section on page 33-11), 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 (see the “Configuring Authentication for CLI, ASDM, and enable command Access” section on page 33-11), 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 32-20.

**Step 9** Click **Apply**.

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

---

**Note**

To configure the enable password from the User Accounts pane (see the “Configuring the Hostname, Domain Name, and Passwords” section on page 9-1), 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, and so on.

---

### 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 32-18, 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**.
Chapter 32 Configuring AAA Servers and the Local Database

Adding a User Account

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 the Inherit check box, and enter a new value:

a. Choose a group policy from the list.

b. Specify which tunneling protocols are available for use, or whether the value is inherited from the group policy. Check the desired Tunneling Protocols check boxes to choose the VPN tunneling protocols that are available for use. Only the selected protocols are available for use. The choices are as follows:
   - 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.
   - VPN via SSL/TLS (Clientless SSL VPN) 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 shares (web-enabled), e-mail, and other TCP-based applications from almost any computer that can reach HTTPS Internet sites.
   - The 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 adaptive security appliance and private corporate networks.

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

c. Specify which filter (IPv4 or IPv6) 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 adaptive 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.

d. Click Manage to display the ACL Manager pane, on which you can add, edit, and delete ACLs and ACEs.

e. Specify 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 adaptive security appliance prevents the user from connecting. If the Inherit check box is not checked, the default value is None.

f. Specify whether to inherit the Store Password on Client System setting from the group. Uncheck the Inherit check box to activate the Yes and No radio buttons. Click Yes to store the login password on the client system (potentially a less-secure option). Click No (the default) to require 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 effect on interactive hardware client authentication or individual user authentication for a VPN 3002.

Step 3 To change Connection Settings, uncheck the Inherit check box, and enter a new value:

a. If the Inherit check box is not checked, you can select the name of an existing access hours policy, if any, to apply to this user or create a new access hours policy. The default value is Inherit, or, if the Inherit check box is not checked, the default value is Unrestricted.
Configuring LDAP Attribute Maps

If you are introducing an adaptive security appliance to an existing LDAP directory, your security policy will likely involve setting permissions or authorization entitlements for the VPN remote access policy user from that LDAP directory. You must create LDAP attribute maps that map your existing user-defined attribute names and values to Cisco attribute names and values that are used for permission settings on 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 To use the attribute mapping features correctly, you need to understand 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 that they would commonly be mapped to include the following:

- **Group_Policy**—Sets the group policy based on the directory’s department or user group (for example, Microsoft Active Directory memberOf) attribute value. The Group-Policy attribute replaced the IETF-Radius-Class attribute with ASDM version 6.2/ASA version 8.2 or later.
- **IETF-Radius-Filter-Id**—An access control list or ACL applied to VPN clients, IPsec, and SSL.
- **IETF-Radius-Framed-IP-Address**—Assigns a static IP address to a VPN remote access client, IPsec, and SSL.
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 adaptive security appliance when requiring user authentication from TACACS+ or RADIUS servers. This text is primarily for cosmetic purposes and appears above the username and password prompts that users see when they log in.

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

- Banner1—Displays a text banner when the VPN remote access user logs in.
- Tunneling-Protocols—Allows or denies the VPN remote access session based on the access type.

Note

A single ldapattribute map may contain one or many attributes. You can only assign one ldap attribute map to a specific LDAP server.

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

**Step 1** Choose Configuration > Remote Access VPN > AAA Local Users > LDAP Attribute Map, and then 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 to which the value in Step 10 maps.

**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 to the running configuration.
AAA Servers Monitoring

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 they log in by entering text in the Prompt field.

The following are the allowed character limits for authentication prompts:

<table>
<thead>
<tr>
<th>Application</th>
<th>Character Limit for Authentication Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Internet Explorer</td>
<td>37</td>
</tr>
<tr>
<td>Telnet</td>
<td>235</td>
</tr>
<tr>
<td>FTP</td>
<td>235</td>
</tr>
</tbody>
</table>

**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 adaptive security appliance displays the User accepted message text, if specified, to the user; otherwise, the adaptive security appliance 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.

---

**AAA Servers Monitoring**

To monitor AAA Servers, see the following panes:

<table>
<thead>
<tr>
<th>Path</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring &gt; Properties &gt; AAA Servers</td>
<td>Shows the configured AAA server statistics.</td>
</tr>
<tr>
<td>Monitoring &gt; Properties &gt; AAA Servers</td>
<td>Shows the AAA server running configuration.</td>
</tr>
</tbody>
</table>
For additional information related to implementing LDAP mapping, see the following sections:

- Related Documents, page 32-26
- RFCs, page 32-26
Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP commands and AAA server host mode commands</td>
<td>Cisco ASA 5500 Series Command Reference</td>
</tr>
<tr>
<td>Example configuration procedures used to set up LDAP authentication or authorization</td>
<td>Configuring an External Server for Authorization and Authentication, page B-1</td>
</tr>
<tr>
<td>List of Cisco LDAP attribute names and values</td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td>Cisco ASA 5500 Series Configuration Guide using the CLI</td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2138</td>
<td>Remote Authentication Dial In User Service (RADIUS)</td>
</tr>
<tr>
<td>2139</td>
<td>RADIUS Accounting</td>
</tr>
<tr>
<td>2548</td>
<td>Microsoft Vendor-specific RADIUS Attributes</td>
</tr>
<tr>
<td>2868</td>
<td>RADIUS Attributes for Tunnel Protocol Support</td>
</tr>
</tbody>
</table>

Feature History for AAA Servers

Table 2 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Servers</td>
<td>7.0(1)</td>
<td>AAA Servers describes support for AAA and how to configure AAA servers and the local database. The following screens were introduced: Configuration &gt; Device Management &gt; Users/AAA &gt; AAA Server Groups Configuration &gt; Remote Access VPN &gt; AAA Local Users &gt; LDAP Attribute Map Configuration &gt; Device Management &gt; Users/AAA &gt; User Accounts</td>
</tr>
</tbody>
</table>