



CHAPTER 3

Authenticating MARS Accounts with External AAA Servers

Revised: April 5, 2007

External Authentication, Authorization, and Auditing (AAA) servers can act as the authentication mechanism for MARS Appliance GUI logins (username and password). This permits authentication and centralized password management for all MARS Appliances.

Feature History for MARS Appliance AAA Authentication Method

Release	Modification
4.3.1 and 5.3.1	This feature was introduced.

Contents

This chapter describes the Authentication, Authorization and Accounting (AAA) feature for the MARS Appliances and includes the following sections:

- [Information About Authenticating MARS User Accounts with External AAA Servers](#)
- [Procedure for First-time Configuration of MARS AAA Feature](#)

Information About Authenticating MARS User Accounts with External AAA Servers

The administrator can configure MARS to authenticate GUI login attempts with an external AAA server, or with the default method of authenticating to the appliance's local database, as described in the following sections:

- [Supported AAA Protocols and Servers](#)
- [Configuration Overview](#)
- [Global Controller Considerations with External AAA Servers](#)
- [Failed Authentication Lockout \(Login Failure\)](#)
- [System Reports and Rules related to Authentication Method](#)

Supported AAA Protocols and Servers

The AAA protocol used by MARS is a basic Remote Authentication Dial In User Service (RADIUS) protocol. The supported external RADIUS servers are as follows:

- [Cisco Secure Access Control Server \(ACS\) for UNIX](#)
- [Cisco Secure Access Control Server \(ACS\) for Windows](#)
- [Microsoft Internet Authentication Service \(IAS\) Server](#)
- [Juniper Steel belted RADIUS](#)

Configuration Overview

The following overview describes the Local Controller. Global Controller differences are discussed in the later section, “[Global Controller Considerations with External AAA Servers.](#)”

Summary of MARS Appliance AAA Configuration Tasks

1. Create user accounts on the MARS Appliances.

On each MARS Appliance to which a user must have access, the MARS administrator must create a user account for that user (contact information, group permissions and role). The account can be created on the Local Controller or on a Global Controller and pushed to the Local Controller.

2. Configure all MARS Appliances to use AAA authentication method.

Each MARS Appliance must be individually configured to run the AAA authentication method. From the **AAA Configuration** page (**Admin > System Setup > Authentication Configuration**), manually add external AAA servers in a procedure similar to that of adding a software security application on a new host.

Up to three AAA servers can be selected for AAA server authentication. They are named the primary, secondary, and tertiary servers which signifies their rank in the AAA server failover sequence.



Note

When the administrator changes the MARS authentication method from Local to AAA, all passwords from accounts other than administrator, are deleted from the local user profiles. When changing from AAA to Local, the MARS administrator must recreate passwords for each local account.

When the MARS Appliance operates with the AAA authentication method, every login except the administrator accounts are authenticated by the external AAA server.

All authentication method changes, successful logins, and failed logins are captured as event messages.

Summary of AAA Server Configuration Tasks

1. Configure the MARS Appliance as an AAA client of the AAA server.
2. The AAA server administrator must create the MARS user accounts in the external AAA servers to provide only login name/password authentication for each MARS user.

See the user guide of your AAA server for details.

Global Controller Considerations with External AAA Servers

The following constraints and recommendations pertain to using the AAA authentication method with a Global Controller:

- **Global and Local Accounts for the Same User**

Using the Local authentication method, a user can have two accounts with the same login name and different passwords on a single appliance, for example, `global:person1` created on the Global Controller and pushed to the Local Controller and `local:person1` created on the Local Controller. Because the AAA server has only one password per login name, do the following to maintain the Local method functionality with the AAA method:

- Use the same password for both the global and local accounts
- Use different AAA servers to authenticate the global and local login names

- **Changing Global Controller to AAA Authentication Method**

Configuring AAA Authentication Method on a Global Controller is similar to configuring AAA on a Local Controller, except that AAA servers cannot be added, edited or deleted on a Global Controller. The list of available AAA server names in the GUI is populated from the Local Controllers reporting to the Global Controller. The hostname of the reporting Local Controller is prepended to the AAA server name. The Global Controller should use an AAA server from the closest Local Controller on the network.

- **Use the same Authentication Method for all Global and Local Controllers**

To avoid login problems, the optimal scenario is to have all Local Controller and Global Controllers use the same authentication method, either all Local or all AAA. For example, when a Global Controller uses AAA method, and a Local Controller uses Local method, any global user accounts pushed to the Local Controller will not have passwords. Any login attempt by the global user to that Local Controller fails until the administrator configures a password for the global account.

- **Setup accounts for Global Controller Users in all AAA servers used by Local Controllers**

When a Global Controller and a Local Controller use different AAA servers for authentication the Global Controller login name and password must be configured in one of the Local Controller's AAA servers or the Global Controller user will not be able to login to the Local Controller.

- **Deleting AAA servers on Local Controllers**

If a Local Controller deletes the AAA server in use by a Global Controller, the Global Controller is automatically switched to Local authentication. To reestablish AAA authentication for the Global Controller, the administrator must reconfigure the Global Controller to AAA authentication method and select another AAA server.

Just prior to a Local Controller being deleted from a Global Controller, a warning message appears if it is the Local Controller with the AAA server to which the Global Controller authenticates.

- **Unlocking Accounts**

Unlocking is not replicated through Global Controller–Local Controller communications, it applies only to the local appliance. An account locked on a Global Controller does not replicate the locked status to global accounts on Local Controllers. A global account locked on two different appliances must be unlocked manually on each appliance.

Failed Authentication Lockout (Login Failure)

For both Local or AAA authentication methods, GUI access is prevented (locked) for an account upon login failure, which occurs when a specified number of incorrect password entries are made for a single login name.

The maximum number of password attempts before locking is set by the Maximum Login Failures parameter in the Account Lockout Policy box of the AAA configuration page (**Admin > System Setup > Authentication Configuration**). The default setting is 5 attempts. By setting the Account Lockout Policy to **Never Lock**, the administrator can disable GUI locking for all accounts, but not specific accounts.

The count of incorrect attempts before login failure clears only when a successful login occurs, it does not age out. For example, if a user performs two incorrect password attempts then quits for the day, they must succeed on the first attempt the next morning or the account will be locked. A running session does not terminate if a login failure occurs for the same user account attempting to open another session, but the account will be locked to all future login attempts.

Once locked, an account must be unlocked by the MARS administrator.

The **Admin > User Management** page of the GUI displays locked accounts. The Status column indicates if the account is **active**, **locked** or **password expired**. An administrator can unlock accounts from the User Management page by selecting the accounts and clicking **Unlock**.

**Note**

An account password expires when the authentication method is changed from Local to AAA then back to Local, because the initial change from Local to AAA erased all the passwords of the non-administrative local accounts. The passwords must be reset by editing each account from the User Management page.

The CLI access through the console or through SSH is never locked. The **unlock** CLI command can unlock GUI access for some or all accounts. This is the recourse when the administrator is locked out from the GUI. For information on the **unlock** command, see the Command Reference chapter in the *Install and Setup Guide for Cisco Security MARS*, at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/5.3/installation/guide/apclir ef.html#wp1277272.

System Events related to Authentication and Login Attempts

Table 3-1 lists events triggered by Local and AAA authentication method actions.

Table 3-1 MARS AAA-related Events

Event	Raw Messages
CS-MARS admin user login success	<p>GUI Raw message: % MARS-3-400001 CS-MARS GUI login successful for admin user 'username(CS_MARS_LC)@LC42' from: <src-ip> using local authentication</p> <p>GUI Raw message: % MARS-3-400001 CS-MARS GUI login successful for admin user 'username(CS_MARS_GC)@GC41' from: <src-ip> using AAA authentication at server: <aaa-ip></p>
CS-MARS admin user login failure	<p>GUI Raw message: %MARS-2-400002 CS-MARS GUI login failure for admin user 'username(CS_MARS_LC)@LC42' from: <src-ip> using local authentication</p> <p>GUI Raw message: %MARS-2-400002 CS-MARS GUI login failure for admin user 'username(CS_MARS_LC)@LC42' from: <src-ip> using AAA, reason: user information is not verified in local DB</p> <p>GUI Raw message: %MARS-2-400002 CS-MARS GUI login failure for admin user 'username(CS_MARS_GC)@GC41' from: <src-ip> using AAA authentication at server: <aaa-ip>, reason: invalid user or password</p>
CS-MARS non-admin user login success	<p>GUI Raw message: %MARS-3-400003 CS-MARS GUI login successful for non-admin user 'username(CS_MARS_LC)@LC42' from: <src-ip> using local authentication"</p> <p>GUI Raw message: %MARS-3-400003 CS-MARS GUI login successful for non-admin user 'username(CS_MARS_GC)@GC41' from: <src-ip> using AAA authentication at server: <aaa-ip></p>
CS-MARS non-admin user login failure	<p>GUI Raw message: %MARS-2-400004 CS-MARS GUI login failure for non-admin user 'username(CS_MARS_LC)@LC42' from: <src-ip> using local authentication</p> <p>GUI Raw message: %MARS-2-400004 CS-MARS GUI login failure for non-admin user 'username(CS_MARS_LC)@LC42' from: <src-ip> using AAA authentication, reason: user information is not verified in local DB</p> <p>GUI Raw message: %MARS-2-400004 CS-MARS GUI login failure for non-admin user 'username(CS_MARS_GC)@GC41' from: <src-ip> using AAA authentication at server: <aaa-ip>, reason: invalid user or password</p>
CS-MARS failed to connect to AAA server	<p>GUI Raw message: %MARS-2-400005 CS-MARS GUI failed to connect to AAA server at: <aaa-ip> for authenticating admin user 'username(CS_MARS_LC)@LC42', reason: <reason-string></p> <p>GUI Raw message: %MARS-2-400005 CS-MARS GUI failed to connect to AAA server at: <aaa-ip> for authenticating non-admin user 'username(CS_MARS_LC)@LC42', reason: <reason-string></p>

Table 3-1 MARS AAA-related Events

Event	Raw Messages (continued)
CS-MARS padmin user password changed	<p>GUI raw message: %MARS-2-401001 CS-MARS 'padmin(CS_MARS_LC)@LC42' user password has changed from GUI at <src-ip></p> <p>CLI raw message: %MARS-2-401001 CS-MARS 'padmin(CS_MARS_LC)@LC42' user password has changed from CLI at <src-ip></p>
CS-MARS padmin user password remains default	raw message: %MARS-2-401002 CS-MARS 'padmin(CS_MARS_LC)@LC42' user password remains default for the past 24 hours
CS-MARS admin user account locked	<p>Raw message: %MARS-2-402001 CS-MARS locked admin user account 'username(CS_MARS_LC)@LC42' after <number> login failures. The current login attempt originated from: <src-ip> with local authentication</p> <p>Raw message: %MARS-2-402001 CS-MARS locked admin user account 'username(CS_MARS_LC)@LC42' after <number> login failures. The current login attempt originated from: <src-ip> with AAA authentication at server: <aaa-ip></p> <p>Raw message: %MARS-2-402001 CS-MARS locked admin user account 'username(CS_MARS_LC)@LC42' after <number> login failures. The current login attempt originated from: <src-ip> with AAA authentication but failed in local user verification</p>
CS-MARS admin user account unlocked	<p>GUI Raw message: %MARS-3-402003 CS-MARS unlocked admin user account 'username(CS_MARS_LC)@LC42' from GUI by admin user 'adminuser(CS_MARS_LC)@LC42' while logged in from: <src-ip></p> <p>CLI Raw message: %MARS-3-402003 CS-MARS unlocked admin user account 'username(CS_MARS_LC)@LC42' from CLI by admin user 'padmin(CS_MARS_LC)@LC42' while logged in from: <src-ip></p>
CS-MARS non-admin user account unlocked	<p>Raw message: %MARS-2-402002 CS-MARS locked non-admin user account 'username(CS_MARS_LC)@LC42' after <number> login failures. The current login attempt originated from: <src-ip> with local authentication</p> <p>Raw message: %MARS-2-402002 CS-MARS locked non-admin user account 'username(CS_MARS_LC)@LC42' after <number> login failures. The current login attempt originated from: <src-ip> with AAA authentication at server: <aaa-ip></p> <p>Raw message: %MARS-2-402002 CS-MARS locked non-admin user account 'username(CS_MARS_LC)@LC42' after <number> login failures. The current login attempt originated from: <src-ip> with AAA authentication but failed in local user verification</p>
CS-MARS unlocked all accounts	CLI raw message: %MARS-3-402005 CS-MARS unlocked all accounts while logged in from: <src-ip>

Table 3-1 MARS AAA-related Events

Event	Raw Messages (continued)
CS-MARS Authentication method changed from Local to AAA	GUI raw message: %MARS-2-403001 CS-MARS Authentication method was changed from Local to AAA by admin user 'username(CS_MARS_LC)@LC42' while logged in from: <src-ip>
CS-MARS Authentication method changed from AAA to Local	GUI raw message: %MARS-2-403002 CS-MARS Authentication method was changed from AAA to Local by admin user 'username(CS_MARS_LC)@LC42' while logged in from: <src-ip>'

System Reports and Rules related to Authentication Method

For descriptions of MARS reports and rules, please see the “Systems Rule and Reports Reference” at following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/5.3/user/guide/local_controller/appmars.html

System Reports

The following six reports disclose authentication events. All the reports are custom column, run on-demand only, with a time range of 1 day.

- Activity: CS-MARS Login Failures
- Activity: CS-MARS Successful Logins
- Activity: CS-MARS Accounts Locked
- Activity: CS-MARS Accounts Unlocked
- Activity: CS-MARS Authentication Method Modifications
- Activity: CS-MARS padmin User Password Status

System Rules

The following three rules capture authentication method configuration actions:

- System Rule: CS-MARS Authentication Method Modified - AAA to Local
- System Rule: CS-MARS Login Failures - Admin User
- System Rule: CS-MARS Login Failures - Non-Admin User

The following system rule is triggered depending on how events are grouped:

- System Rule: Vulnerable Host Found (Event: CS-MARS padmin user password remains default)

Because MARS login successes and failures are grouped into event groups the following rules could fire if a MARS Local Controller is also the target of attacks described in each of the following rules:

- System Rule: Local Attack - Attempt
- System Rule: Local Attack - Success Likely
- System Rule: Password Attack: System - Attempt
- System Rule: Password Attack: System - Success Likely

- System Rule: Password Attack: System - Success Likely

Login events groups—Info/SuccessfulLogin/System/Root, Info/SuccessfulLogin/System/Non-root, Penetrate/GuessPassword/System/Root and Penetrate/GuessPassword/System/Non-root

Procedure for First-time Configuration of MARS AAA Feature

This procedure demonstrates a first-time configuration of AAA Authentication method for a MARS Appliance.

Summary of steps:

1. Add a new external AAA Server
2. Select AAA Authentication
3. Configure Account Lockout Policy (optional)

Prerequisites

The following prerequisites are required to configure the AAA authentication method:

- User profiles created in each MARS Appliance (role and contact involve each intended user)
- MARS configured as an AAA client on the external AAA server.



Tip

For the Cisco Secure ACS, MARS must be configured as an AAA client. You may choose any vendor-specific attribute (VSA) configuration that uses port 1812 as an authentication port and port 1813 as an accounting port. We recommend the Cisco VPN3000/ASA/PIX 7.x+ VSA. For further information see the *User Guide for Cisco Secure Access Control Server 4.1* at the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/WebIntr.html#wp417167

- MARS user accounts created in the external AAA server to provide only login name/password authentication



Note

The MARS Appliance login name is case-sensitive, the Cisco Secure ACS User Setup username is not. For example, the MARS login names Victor, victor, and VICTOR will match the Cisco Secure ACS username “victor.” Thus, three MARS users could share the same password. We recommend that there be a one-to-one correspondance of MARS login names to Cisco Secure ACS usernames.

- (Local Controller only) AAA server configuration information required by MARS as follows:
 - Access and Reporting IP addresses
 - Interface addresses
 - Shared secret string
 - Authentication port (default is 1812)
 - Accounting port (default is 1813)

Step 1 Click the **Admin** tab to navigate to System Setup page, as shown in [Figure 3-1](#).

Figure 3-1 Admin > System Setup Page

The screenshot displays the Cisco MARS Admin interface. At the top, there is a navigation bar with tabs for 'SUMMARY', 'INCIDENTS', 'QUERY / REPORTS', 'RULES', 'MANAGEMENT', 'ADMIN', and 'HELP'. Below this, a secondary navigation bar includes 'System Setup', 'System Maintenance', 'User Management', 'System Parameters', and 'Custom Setup'. The 'System Setup' tab is selected. The page header shows the Cisco logo, a user profile for 'ADMIN', and system details: 'CS-MARS Standalone: nazereth v4.3'. A 'Select Case' dropdown menu is set to 'No Case Selected...'. The main content area is divided into three sections: 'CS-MARS Setup' (containing 'Configuration Information' and 'Authentication Configuration'), 'Device Configuration and Discovery Information' (containing 'Security and Monitor Devices', 'NetFlow Config Info (optional)', and 'IPS Signature Dynamic Update Settings'), and 'Topology Discovery Information (optional)' (containing 'Community String and Networks', 'Valid Networks', and 'Topology/Monitored Device Update Scheduler'). The footer contains copyright information and a breadcrumb trail: 'Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help'.

Step 2 Click **Authentication Configuration** to display the AAA configuration page, as shown in [Figure 3-2](#). If you are configuring a Global Controller, please skip to [Step 9](#).

Figure 3-2 AAA Configuration Page

The screenshot displays the AAA Configuration page. At the top, there is a navigation bar with tabs: SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. Below this is a secondary navigation bar with tabs: System Setup, System Maintenance, User Management, System Parameters, and Custom Setup. The user is logged in as ADMIN, and the system is identified as CS-MARS Standalone: nazareth v4.3. The date and time are Aug 2, 2007 11:09:15 AM PDT. There are buttons for Logout and Activate. A 'Select Case' dropdown menu is set to 'No Case Selected...'. Below this are buttons for View Cases and New Case.

The main configuration area is divided into three sections:

- Authentication Method:**
 - Local
 - AAA Server
 - Primary:
 - Secondary:
 - Tertiary:
- AAA Server Configuration:**
 -
 -
 -
 -
- Account Lockout Policy:**
 - Maximum Login Failures
 - Never Lock

At the bottom of the configuration area, there are buttons for Back and Submit.

Copyright © 2003–2007 Cisco Systems, Inc.
All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

250321

Add an external AAA Server

Step 3 Click **Add** in the AAA Server Configuration box. The Add Reporting Device page appears, as shown in [Figure 3-3](#).

Figure 3-3 Add Reporting Device Page

Note:

1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: Add AAA server on new host

↓

General	Reporting Applications						
→ *Device Name: <input type="text"/> → *Access IP: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> → Reporting IP: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> → Operating System: Generic <input type="button" value="Logging Info"/> → NetBIOS Name: <input type="text"/> → Monitor Resource Usage: NO <input type="button"/>							
Enter interface information: <table border="1"> <tr> <td><input type="button" value="Add Interface"/></td> <td><input type="button" value="Remove Interface/IP"/></td> </tr> <tr> <td>Name: <input type="text"/></td> <td>IP Address: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> Network Mask: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/></td> </tr> <tr> <td><input type="checkbox"/> ether0</td> <td><input type="button" value="Add IP/Network Mask"/></td> </tr> </table>		<input type="button" value="Add Interface"/>	<input type="button" value="Remove Interface/IP"/>	Name: <input type="text"/>	IP Address: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> Network Mask: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	<input type="checkbox"/> ether0	<input type="button" value="Add IP/Network Mask"/>
<input type="button" value="Add Interface"/>	<input type="button" value="Remove Interface/IP"/>						
Name: <input type="text"/>	IP Address: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> Network Mask: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>						
<input type="checkbox"/> ether0	<input type="button" value="Add IP/Network Mask"/>						

250322

Step 4 Type in the configuration information and click **Next**. The reporting application dialog appears as shown in [Figure 3-4](#).

The usage guidelines for the configuration fields are equivalent to those for adding a monitoring device.



Note The **Done** and **Apply** buttons are used when editing a configuration, not in a first-time configuration. Clicking **Done** returns you to the AAA Configuration page.

Figure 3-4 Reporting Application Dialog

Note:

1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: Edit host with security applications

↓

General	Reporting Applications				
Enter reporting application: <table border="1"> <tr> <td>→ Device Name: ACS Server</td> </tr> <tr> <td>→ Select application: Generic AAA Server <input type="button" value="Add"/></td> </tr> <tr> <td><input type="button" value="Edit"/> <input type="button" value="Remove"/></td> </tr> <tr> <td><input type="button" value="Device Type"/></td> </tr> </table>		→ Device Name: ACS Server	→ Select application: Generic AAA Server <input type="button" value="Add"/>	<input type="button" value="Edit"/> <input type="button" value="Remove"/>	<input type="button" value="Device Type"/>
→ Device Name: ACS Server					
→ Select application: Generic AAA Server <input type="button" value="Add"/>					
<input type="button" value="Edit"/> <input type="button" value="Remove"/>					
<input type="button" value="Device Type"/>					

250323

Select **Generic AAA Server** and then click **Add**.

The AAA Server Configuration pop-up window appears, as shown in [Figure 3-5](#).

Figure 3-5 AAA Server Configuration Pop-up Window

Aug 2, 2007 1:36:58 PM PDT
Standalone: nazareth v4.3 Login: Administrator (padmin) :: Close

AAA Server Configuration:

Name:

Shared Secret:

Authentication Port:

Accounting Port:

Test Connectivity Cancel Submit

Copyright © 2003–2007 Cisco Systems, Inc.
All rights reserved.

250324

Step 5 Enter AAA Server configuration information.

The default authentication and authorization port is 1812.

The default accounting port is 1813.

Step 6 Click **Test Connectivity**.

A pop-up window appears for success or failure, as shown in [Figure 3-6](#) and [Figure 3-7](#).



Note The AAA Server Configuration field values are provided by the AAA server administrator.

Figure 3-6 Connectivity Succeeds Pop-up Window

Feb 8, 2007 4:45:31 PM PST
Standalone: erebus v0.0 Login: Administrator (padmin) :: Close

Connection to AAA server succeeded!

Input user name and password to check authentication:

User Name:

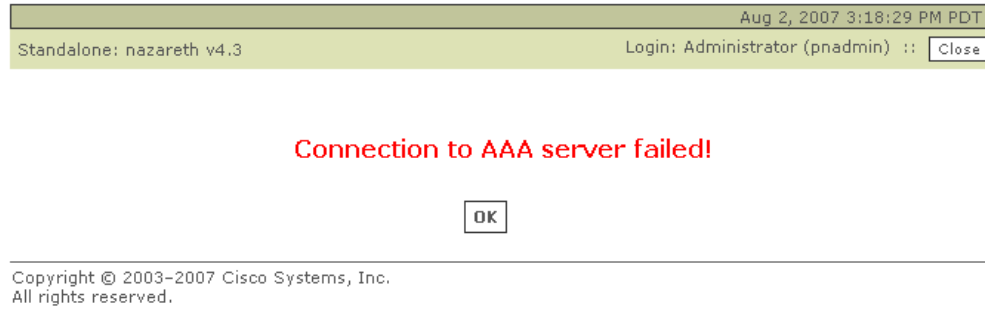
Password:

Cancel Submit

Copyright © 2003–2007 Cisco Systems, Inc.
All rights reserved.

Feedback

250325

Figure 3-7 Connectivity Fails Pop-up Window

- Step 7** If the connectivity test succeeds, enter any User Name and Password configured for MARS on the AAA server and click **Submit** to verify that the added external AAA server correctly authenticates you to the MARS account.

You are returned to the AAA Configuration Page, as shown in [Figure 3-2](#).

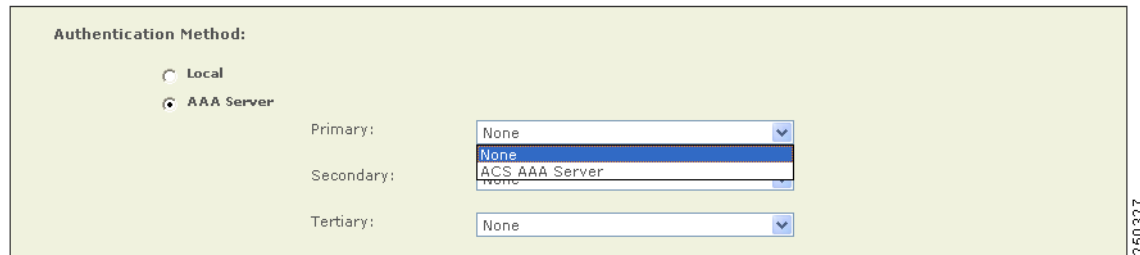
If the connectivity fails, you are returned to the AAA Server Configuration Pop-up Window, as shown in [Figure 3-5](#). Troubleshoot the AAA server connection until connectivity succeeds.

- Step 8** Add Secondary or Tertiary AAA servers per your administrative requirements.

Select AAA Authentication

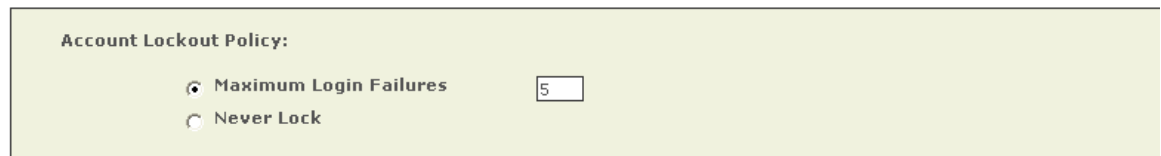
- Step 9** In the **Authentication Method** box of the AAA Configuration Page, click the AAA Server radio button, and select your primary AAA server from the drop-down list. Select secondary and tertiary servers as appropriate to your network.

If you are configuring a Global Controller, select the AAA server closest to the Global Controller.

Figure 3-8 Select Newly-added AAA Server From Drop-down List

Configure Account Lockout Policy (optional)

In the Account Lockout Policy box, configure the maximum login failures threshold, or click the Never Lock radio button.

Figure 3-9 Maximum Login Failure Parameter

- Step 10** Click **Submit**.

When the authentication method is changed from Local to AAA Server, all user passwords are removed from the MARS local database (except administrators). If you change the authentication method back to Local from AAA Server, you must reconfigure all the user passwords with the MARS GUI (Management > User Management).

When the MARS authentication is set to AAA server mode, user passwords can not be added or edited on the MARS User Management page.

End of [Procedure for First-time Configuration of MARS AAA Feature](#).

Procedure to Edit an External AAA Server

- Step 1** Click the **Admin** tab to navigate to System Setup page, as shown in [Figure 3-1](#).
- Step 2** Click **Authentication Configuration** to display the AAA configuration page, as shown in [Figure 3-2](#).
- Step 3** In the AAA Server Configuration box, select the external AAA Server to edit.
- Step 4** Click **Edit**. The Edit Server page appears, as shown in [Figure 3-10](#).

Figure 3-10 *Edit Server Page*

Note:

1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: Edit host with security applications

General
Reporting Applications

Enter reporting application:

→ Device Name: ACS

→ Select application: Generic AAA Server

Device Type

Generic AAA Server

250329

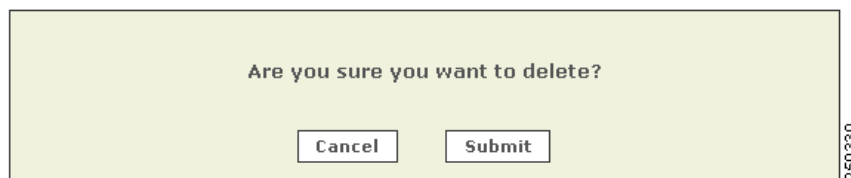
- Step 5** Click the checkbox of the Device Type to change then click **Edit**. The Server Configuration pop-up window appears, as shown in [Figure 3-5](#).
- Step 6** Make changes, click **Test Connectivity**.
- Step 7** If the connectivity test succeeds, enter your User Name and Password and click **Submit** to verify that the added external AAA server correctly authenticates you to your MARS account.
You are returned to the AAA Configuration Page, as shown in [Figure 3-2](#).
If the connectivity fails, you are returned to the AAA Server Configuration Pop-up Window, as shown in [Figure 3-5](#). Troubleshoot the AAA server connection until connectivity succeeds.
- Step 8** Click **Submit**. You are returned to AAA configuration page.
End of [Procedure to Edit an External AAA Server](#).

Procedure to Delete an External AAA Server

- Step 1** Click the **Admin** tab to navigate to System Setup page, as shown in [Figure 3-1](#).
- Step 2** Click **Authentication Configuration** to display the AAA configuration page, as shown in [Figure 3-2](#).
- Step 3** In the AAA Server Configuration box, select the external AAA Server to delete.
- Step 4** Click **Delete**. A delete confirmation pop-up window appears, as shown in [Figure 3-11](#).

Figure 3-11 Server Delete Confirmation

Application: Generic AAA Server



- Step 5** Click **Submit**. You are returned to AAA configuration page.
If the AAA server deleted is a primary server used by a Global Controller, The Global Controller automatically switches to the Local authentication method and the administrator must reconfigure the Global Controller to AAA method and select another AAA server as required.
End of [Procedure to Delete an External AAA Server](#).

Procedure to Unlock an Account after Login Failure

The following procedure details the steps required to unlock a non-administrative Local Controller or Global Controller account. To unlock an administrative account, use the **unlock** CLI command, as described at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/5.3/installation/guide/apclieref.html#wp1277272

A login failure to the MARS GUI is signaled by the Login Failure message, as shown in [Figure 3-12](#).

Figure 3-12 Login Failure Message



Login Failure
(less info)

Potential Login Failure Reasons:

1. Incorrect Login or Password
2. Connection to AAA server failed
3. Account Locked due to too many failed login attempts
4. Account Locked due to switching authentication methods

Please try again or contact system administrator

Login Name:

Password:

Type: ▾

250331


Step 1 Login to an administrator account.

Step 2 Navigate to the User Management subtab (Management > User Management), as shown in Figure 3-2.

The status column indicates which accounts are locked.

Click the checkbox of the user accounts to unlock.

Figure 3-13 Unlocking a Locked User Account



SUMMARY INCIDENTS QUERY / REPORTS RULES **MANAGEMENT** ADMIN HELP

Event Management IP Management Service Management **User Management** Aug 2, 2007 5:32:50 PM PDT

MANAGEMENT | CS-MARS Standalone: nazareth v4.3 Login: Administrator (pnadmin) :: ::

Select Case:

Select Group:

<input type="checkbox"/>	User Name	Status	Login	Email	Role	Organization	Groups
<input type="checkbox"/>	Administrator (pnadmin)	Active	pnadmin	admin@cisco.com	Admin	Cisco Systems, Inc.	Admin
<input type="checkbox"/>	Analyst, Test (bink)	Active	bink		Security Analyst		Security Analyst
<input checked="" type="checkbox"/>	Blauer, Fortz (fbauer)	Locked	fbauer	fbauer@capu.com	Operator	none	Operator,UserGroup Test
<input type="checkbox"/>	Documentation, Guest (pndocs)	Active	pndocs		Admin		Admin
<input type="checkbox"/>	Quick, Deletus	Active		bamm@gone.com		None	Notification
<input type="checkbox"/>	wu, xiaoli	Active		howl@rantor.com			Notification

1 to 6 of 6 25 per page ▾

250332

Step 3 Click **Unlock**. The status of the user account changes from Locked to Active.

End of [Procedure to Unlock an Account after Login Failure](#).
