CHAPTER 26

Configuring AAA Devices

Revised: Jan 4, 2008

Authentication, authorization, and accounting (AAA) devices provide accountability throughout your network, ensuring that valid users are authorized to use the network services they request and providing detailed event logs regarding failures and successes in such requests.

The AAA server is a key component in the Network Access Control (NAC)initiative (see Configuring Network Admission Control Features and Enable NAC-specific Messages, page 17-4). Cisco Secure Access Control Server (ACS), which is the AAA server for NAC, returns access control decisions to the network access device on the basis of the antivirus credentials of the hosts that are requesting network services.

MARS supports the Cisco Secure ACS software and the Cisco Secure ACS Solution Engine, version 3.3 and later. In the case of Cisco Secure ACS software, support is provided by an agent that resides on the Cisco Secure ACS server. For the Cisco Secure ACS Solution Engine, this agent must reside on a remote logging host. This agent provides MARS with three event logsin syslog format. The logs are as follows:

- Passed authentication log (requires Cisco Secure ACS, 3.3 or later)
- Failed attempts log
- RADIUS accounting log

To support NAC and the 802.1x features, Cisco Secure ACS uses the RADIUS authentication protocol and the cisco-av-pair attributes. For more information on configuring Cisco Secure ACS as a posture validation server for NAC, see the following URLs:

- "Network Admission Control" chapter in *User Guide for Cisco Secure ACS for Windows Server, Version 3.3*

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/3.3/user/guide/nac.html

- "Posture Validation" chapter in *User Guide for Cisco Secure ACS for Windows, Version 4.0*

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/user/guide/nac.html

- "Using Profile Templates" section in the "Network Access Profiles" chapter in *User Guide for Cisco Secure ACS for Windows, Version 4.0*

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/user/guide/sp.html#wp1075429

For more information on the cisco-av-pair attributes, see the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/user/guide/ac.html

This chapter explains how to prepare the Cisco Secure ACS server or the Cisco Secure ACS Solution Engine to allow MARS to collect the event logs. It also describes how to configure MARS to receive and process these logs correctly. Using the web interface, you must define a host to represent the Cisco Secure ACS server (or the remote logging agent collecting logs for the Cisco Secure ACS Solution Engine) and then add the software application to that host.

Supporting Cisco Secure ACS Server

To configure a Cisco Secure ACS server to act as a reporting device, you must perform three tasks:

1. Configure Cisco Secure ACS server to generate the correct log files and details and define the AAA clients.
2. Install the PN Log Agent on the Cisco Secure ACS server and configure it to forward the correct log files.
3. Add the Cisco Secure ACS server to the MARS web interface

You can also configure Cisco Secure ACS to provide command authorization for the MARS Appliance. In this role, Cisco Secure ACS verifies that the MARS Appliance is authorized to execute specific commands on reporting devices and mitigation devices.

Supporting Cisco Secure ACS Solution Engine 4.x

MARS supports the Cisco Secure ACS Solution Engine via a remote logging host. Cisco Secure ACS Remote Agent for Windows is a Windows-based application that supports Cisco Secure ACS Solution Engine for remote logging.

Even though the Cisco Secure ACS Solution Engine supports up to five appliance via a remote logging host, MARS currently supports only one Cisco Secure ACS Solution Engines per remote logging host. Otherwise, MARS cannot identify the IP address of the originating Cisco Secure ACS Solution Engine.

To enable this support, follow these steps:

1. Configure the Cisco Secure ACS Solution Engine to publish logs to the MARS appliance. To perform this task, see Configure Cisco Secure ACS 4.x to Generate Logs, page 26-3
2. Add the Cisco Secure ACS Solution Engine to MARS as a Cisco ACS 4.x reporting device. To perform this task see Add and Configure a Cisco Secure ACS Solutions Engine in MARS, page 26-15, and substitute the ACS server references with the remote logging host.

Supporting Cisco Secure ACS Solution Engine 3.x

MARS supports the Cisco Secure ACS Solution Engine via a remote logging host. Cisco Secure ACS Remote Agent for Windows is a Windows-based application that supports Cisco Secure ACS Solution Engine for remote logging.

Even though the Cisco Secure ACS Solution Engine supports up to five appliance via a remote logging host, MARS currently supports only one Cisco Secure ACS Solution Engines per remote logging host. Otherwise, MARS cannot identify the IP address of the originating Cisco Secure ACS Solution Engine.

To enable this support, follow these steps:

1. Configure the Cisco Secure ACS Solution Engine to publish logs to the remote logging host. See Bootstrap Cisco Secure ACS, page 26-3.
2. Install and configure the Cisco Secure ACS Remote Agent for Windows on the target remote logging host. This host must be running a supported version of Microsoft Windows.

   For instructions on installing and configuring the remote agent, see Installation and Configuration Guide for Cisco Secure ACS Remote Agents.
3. Install the pnLog Agent on the remote logging host.

   For information on installing and configuring the pnLog Agent, see Install and Configure the PN Log Agent, page 26-8.
4. Add the remote logging host to MARS as a Cisco ACS 3.x reporting device. To perform this task see Add and Configure an Cisco Secure ACS Server in MARS, page 26-13, and substitute the ACS server references with the remote logging host.

Bootstrap Cisco Secure ACS

Bootstrapping the Cisco Secure ACS includes the following tasks:

- Configuring the ACS device to generate the desired logs.
  - Configure Cisco Secure ACS 4.x to Generate Logs, page 26-3
  - Configure Cisco Secure ACS 3.x to Generate Logs, page 26-4
- Define AAA Clients, page 26-6
- (Optional) Configure TACACS+ Command Authorization for Cisco Routers and Switches, page 26-8

Configure Cisco Secure ACS 4.x to Generate Logs

MARS support the Cisco Secure ACS sever and the ACS Solutions Engine (SE). This procedure details how to configure the 4.x version of either of these devices so as to generate the syslog messages required parsed by MARS. It also explains how to configure ACS to publish those syslogs to the MARS appliance.

To configure Cisco Secure ACS 4.x to generate the syslogs required by MARS and to publish to MARS, follow these steps:

Step 1 Refer to the "Syslog Logging Configuration Scenario" in the *Configuration Guide for Cisco Secure ACS* for details.

Step 2 Enable the following syslog events:

- **CisACS_01_PassedAuth**—Cisco ACS passed authentications.
- **CisACS_02_FailedAuth**—Cisco ACS failed attempts.
- **CisACS_03_RADIUSAcc**—Cisco ACS RADIUS accounting.
- **CisACS_04_TACACSAcc**—Cisco ACS TACACS+ accounting.
- **CisACS_05_TACACSAdmin**—Cisco ACS TACACS+ administration.
- **CisACS_06_VoIPAcc**—Cisco ACS VoIP accounting.

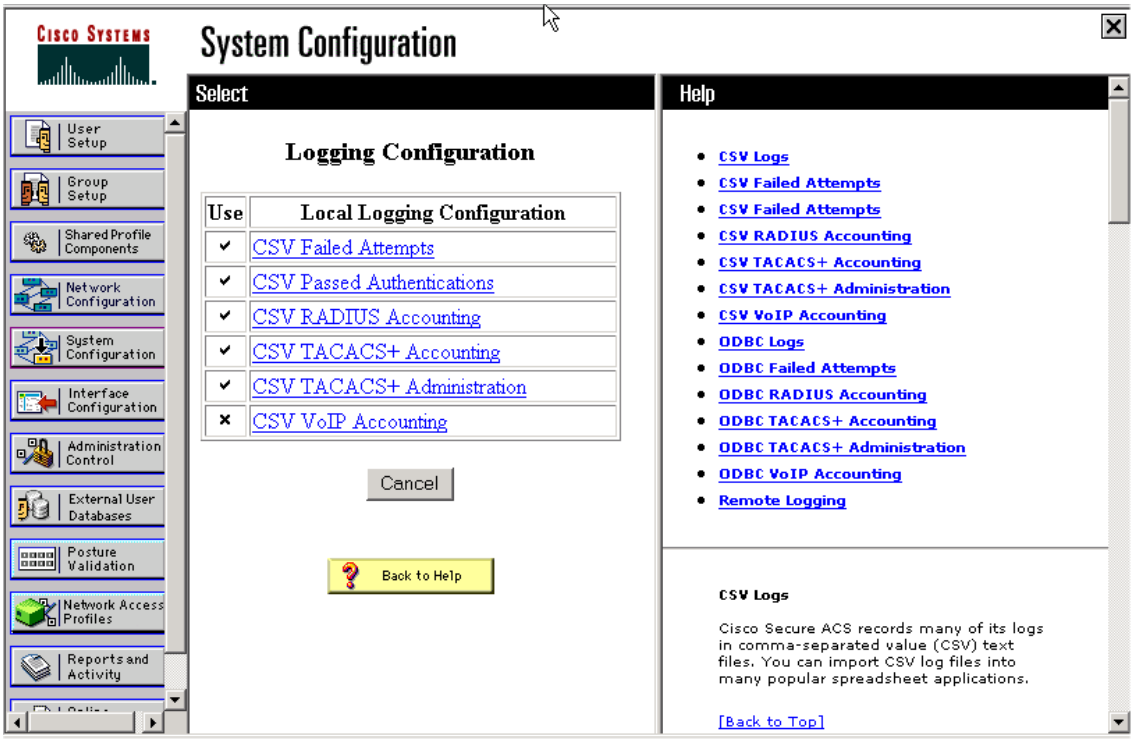
- **CisACS_11_BackRestore**—ACS backup and restore log messages. These events are not used for monitoring. If enabled, they are stored as Generic ACS events.
- **CisACS_12_Replication**—ACS database replication log messages. These events are not used for monitoring. If enabled, they are stored as Generic ACS events.
- **CisACS_13_AdminAudit**—ACS administration audit log messages. These events are not used for monitoring. If enabled, they are stored as Generic ACS events.
- **CisACS_14_PassChanges**—ACS user password changes log messages.
- **CisACS_15_ServiceMon**—ACS service monitoring log messages.
- **CisACS_16_ApplAdmin**—ACS appliance administration audit log messages. These events are not used for monitoring. If enabled, they are stored as Generic ACS events.

Configure Cisco Secure ACS 3.x to Generate Logs

To configure Cisco Secure ACS to generate the audit logs required by MARS, follow these steps:

Step 1 Log in to the Cisco Secure ACS server or Solution Engine.

Step 2 Select **System Configuration > Logging**.

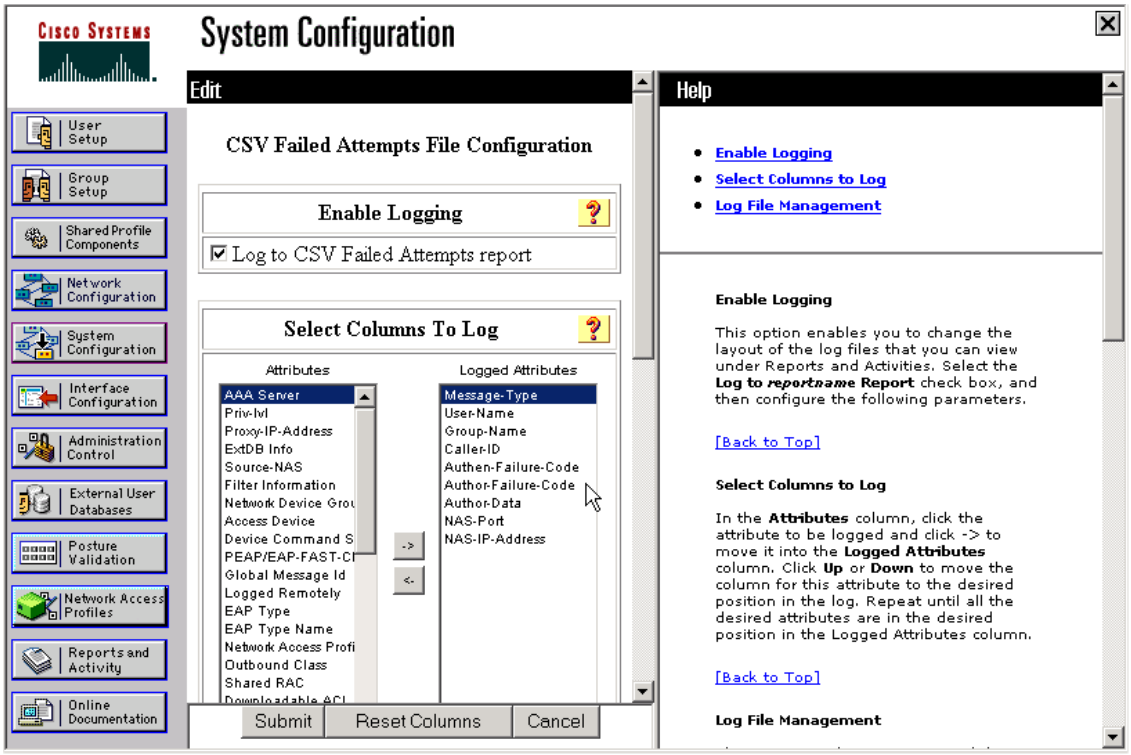


Step 3 Verify that CVS Failed Attempts, CVS Passed Authentications and CVS RADIUS Accounting Logging are enabled.

Step 4 Click **CSV Failed Attempts**, and verify that the following attributes appear in the Logged Attributes list:

- User-Name

- Caller-ID
- NAS-Port
- NAS-IP-Address
- AAA-Server
- Authen-Failure-Code
- Message-Type



Step 5 Click **Submit**.

Step 6 Click **CVS Passed Authentications**, and verify that the following attributes appear in the Logged Attributes list:

- AAA Server'
- User-Name
- Caller-ID
- NAS-Port
- NAS-IP-Address
- System-Posture-Token
- EAP Type Name

Step 7 Click **Submit**.

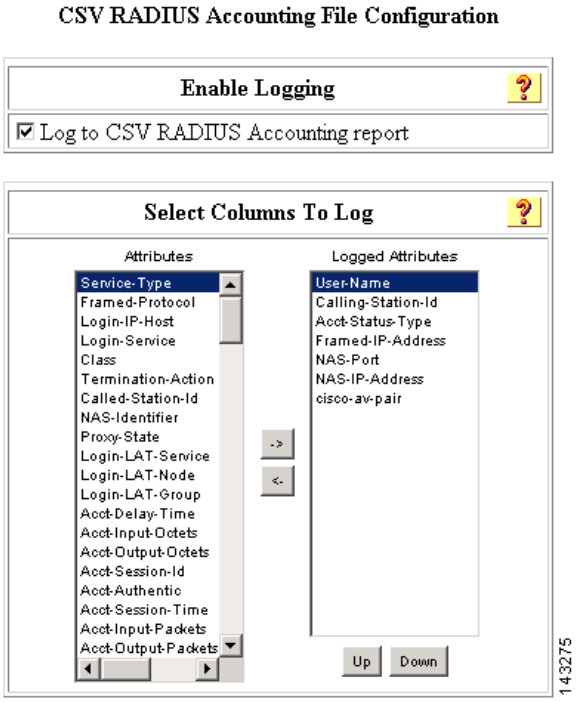
Step 8 Click **CVS RADIUS Accounting**, and verify that the following attributes appear in the Logged Attributes list:

- User-Name

- Calling-Station-Id
- Acct-Status-Type
- NAS-Port
- NAS-IP-Address
- AAA Server
- Framed-IP-Address

Step 9 To support the 802.1x features of NAC, select the following RADIUS accounting attributes:

- Framed-IP address
- cisco-av-pair



Step 10 Click **Submit**.

For additional details on the RADIUS attributes supported by Cisco Secure ACS, see to the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/user/guide/ad.html

Define AAA Clients

To support the 802.1x features of NAC, you must also define the Cisco switches as AAA clients within Cisco Secure ACS. When defining a AAA client, verify the following settings:

- Enable the authentication method that best supports the 802.1x functionality that you want to enable. This option is selected in the Using Authentication box.

- Enable logging of watchdog packets, interim updates. Select the Log Update/Watchdog Packets from this AAA Client check box. This option ensures that interim updates are sent from the Cisco Secure ACS to MARS.

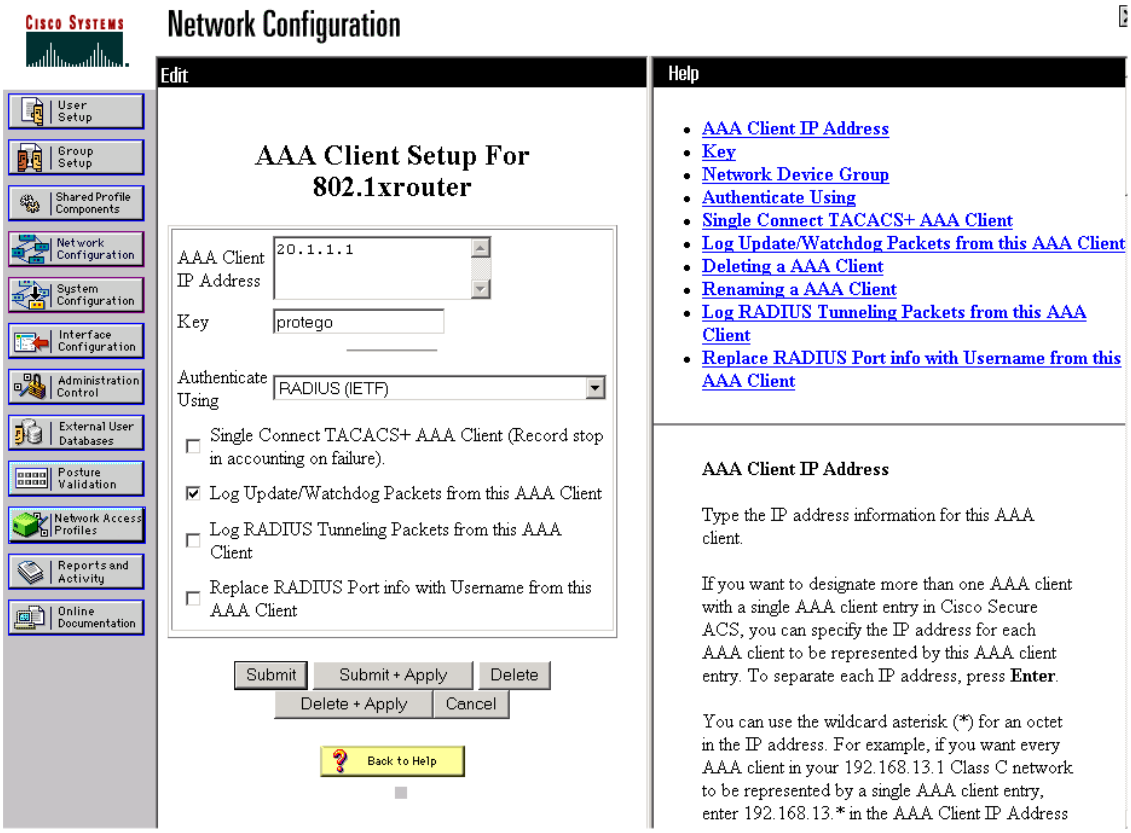
To enable 802.1x logging support, the following configuration must also be completed.

- Ensure DHCP snooping is enabled on each network access device that you plan to define as an 802.1x client in MARS

Note The attack path can not be calculated for a NAC 802.1x security incident when the events triggering the incident are reported to the MARS Appliance by Cisco Secure ACS. However, the MARS Appliance knows the switch port to block so you can mitigate without the attack path.

Figure 26-1 displays example settings for such a client.

Figure 26-1 Configure a AAA Client to Support 802.1x



For more information on defining AAA clients, see the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/user/guide/n.html#wp342084

Configure TACACS+ Command Authorization for Cisco Routers and Switches

You can use the TACACS+ feature of Cisco Secure ACS to authorize the command sets that MARS is allowed to execute on a reporting device. The use of this feature is not required by MARS. However, if you are using this feature on your routers and switches, you must ensure that MARS is allowed to execute specific commands. Required commands are grouped under two operations: configuration retrieval and mitigation.

The following commands support configuration retrieval:

- all **show** commands
- **changeto system**
- **changeto context <*context_name* >**
- **enable**
- **page**
- **no page**
- **terminal length 0**
- **terminal pager lines 0**
- **write terminal**

The following commands support mitigation:

- **conf terminal**
- **interface <*interface_name* >**
- **shutdown**
- **set port disable <*port_name* >**

For more information on configuring command authorization sets in Cisco Secure ACS, see the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/user/guide/c.html#wp697557

Install and Configure the PN Log Agent

MARS includes the PN Log Agent to monitor Cisco Secure ACS active log files (failed attempts, passed authentications, and RADIUS accounting). This agent pushes these log files via syslog to MARS. You can download the PN Log Agent from the software download center at the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars-misc

Note If you are upgrading to a new version of the PN Log Agent, see Upgrade PN Log Agent to a Newer Version, page 26-11.

As part of its operation, the PNLog Agent service writes error and informational message to the Application Log, which can be viewed using the Event Viewer. To learn more about these messages, see Application Log Messages for the PN Log Agent, page 26-11.

To install and configure the PNLog Agent, follow these steps:

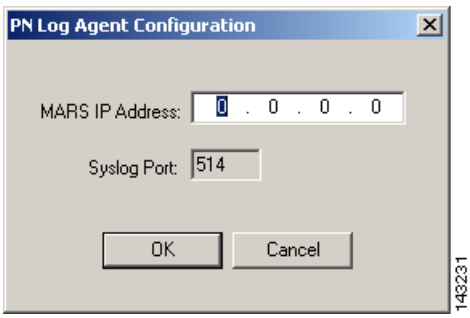
Step 1 Download the PN Log Agent and install it on the server running Cisco Secure ACS or on the remote logging host to which the Cisco Secure ACS Solution Engine is publishing its logs.

Note If installing on a remote logging host, you must have configured the Cisco Secure ACS Remote Agent for Windows on the target remote logging host. For instructions on installing and configuring the remote agent, see Installation and Configuration Guide for Cisco Secure ACS Remote Agents.

Step 2 Select **Start > All Programs > Protego Networks > PNLogAgent > Pn Log Agent**

Step 3 Click **Edit > PN-MARS Config**.

The PN Log Agent Configuration dialog box appears.

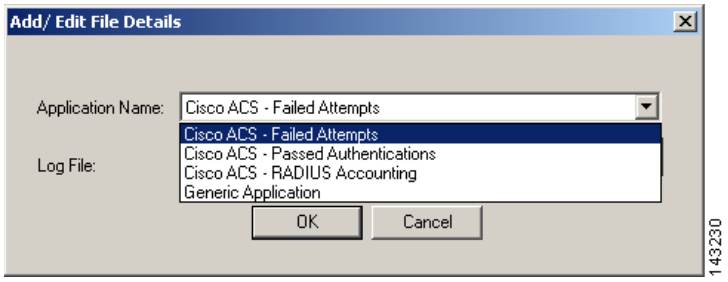


Step 4 In the MARS IP Address field, enter the address of the MARS Appliance, and click **OK**.

Step 5 Select **Edit > Log File Config > Add**.

Step 6 From the Edit pull down menu select **Add**.

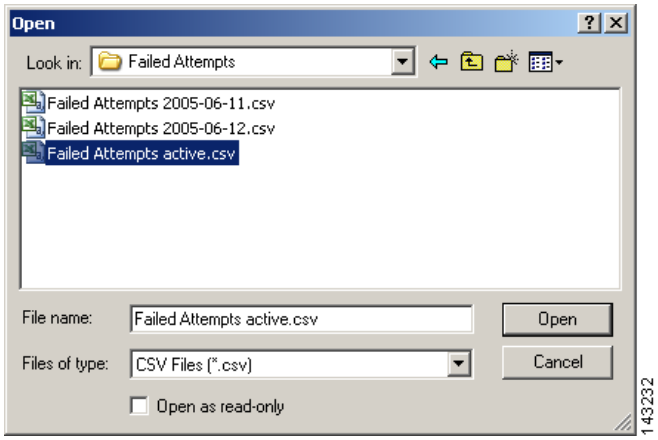
The Add/Edit File Details dialog box appears.



Step 7 From the Application Name list, select the **Cisco ACS-Failed Attempts**.

Step 8 Click on the **...** button to select the appropriate log where all Cisco Secure ACS logs are stored. In this example after selecting **Failed Attempts** application, be sure to select the matching log file, **Failed Attempts** active log.

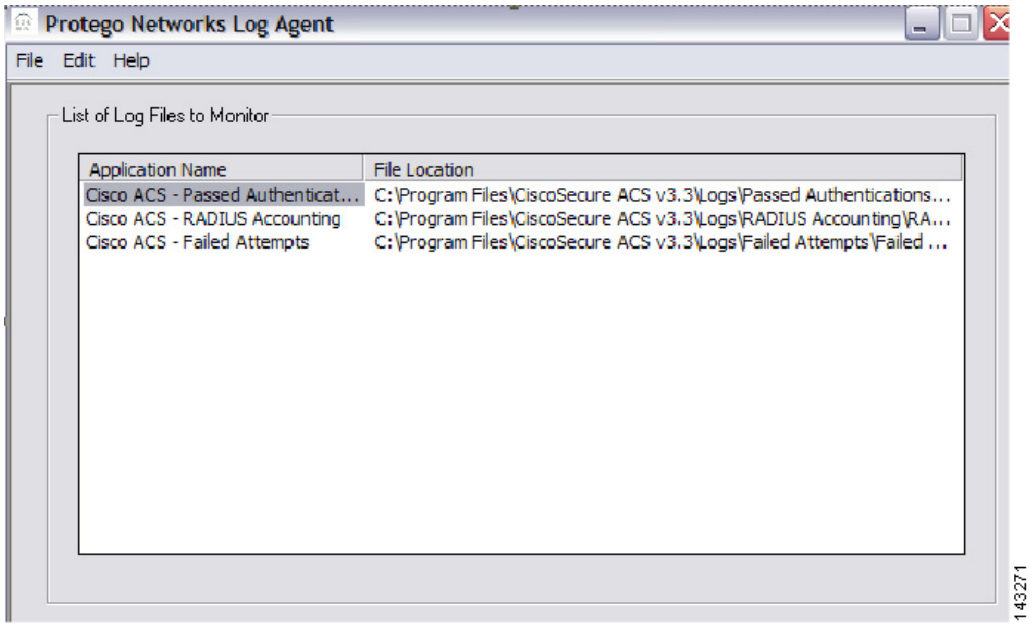
The Open dialog box appears.



Step 9 Add all 3 applications and their active log files:

- Failed Attempts active
- Passed Authentications active
- RADIUS Accounting active

The configured files appear in the List of Log Files to Monitor list.



Step 10 Select **File > Activate**.

Upgrade PN Log Agent to a Newer Version

You can determine which version of the PN Log Agent is running on your server by selecting Help > About in the PN Log Agent Configuration dialog box. This program is updated independently of the MARS Appliance software updates. Therefore, the version number does not correspond to any release of the MARS Appliance software.

Note Beginning with the 4.1.3 release of the pnLog agent, the agent requires a minimum of Cisco Security Monitoring, Analysis, and Response System, release 4.1.3 running on the appliances to which it is reporting in order to operate correctly.

To upgrade to the new PN Log Agent from an existing installation, you must perform the following steps:

Step 1 On the Cisco Secure ACS or syslog server where PN Log Agent is running, uninstall the old agent.

a. To uninstall the old agent, click **Start > Control Panel > Add/Remove Programs** .

b. Select **PnLogAgent** in the list of currently installed programs, and click **Remove** .

c. Select **Yes** to confirm the removal.

Step 2 Reboot the server.

Step 3 Install the new agent. You can download this tool from the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars-misc

Step 4 Re-configure the new agent, specifying the list of files and IP address of the MARS Appliance, etc.

For information on configuring the pnLog Agent, see Install and Configure the PN Log Agent, page 26-8.

Application Log Messages for the PN Log Agent

The PN Log Agent service writes events to the Application Log of Event Viewer on the Cisco Secure ACS server. The agent, identified in the log messages as PNLogAgentService, writes status messages, such as successful service start and stop. It also writes error messages for incomplete configuration and error conditions, such as when the service is out of memory.

Table 26-1 categories the types of messages that can occur and explains their affects on the PNLog Agent service.

Table 26-1 Possible Application Log Messages for PN Log Agent

Type/Message	Effect on Service/Cause of Error
Fatal Errors	
Failed to start thread to monitor file.	Windows errors or configuration errors that will stop the service
The service failed to monitor the configured file. Please check service privileges.	
The service failed to obtain path from log file name and shall exit the thread now!	
The service failed to get the CS-MARS device IP Address. Please use the PnLogAgent to configure it.	
The service has detected an invalid IP address. Please use the PnLogAgent to configure the correct IP Address for CS-MARS.	
Error	
Network detected to be down while attempting to send syslog message	Network connectivity errors that will cause the service to not send syslog messages, but will keep the service running
Destination network unreachable while attempting to send syslog message	
Network dropped connection on reset condition while attempting to send syslog message	
Connection reset by peer while attempting to send syslog message	
Connection refused by target while attempting to send syslog message	
No route exists to host. Please check the network connectivity	
Attempt to send syslog returned error code: <error_code>	
The log file doesn't have all required attributes. Attribute missing: <missing_attribute>	Error in configuration
The number of attributes in the file header don't match the number of attributes in the value. Hence this log entry shall not be sent to CS-MARS.	
The service detected that the configured file is missing some mandatory header attributes. A list of mandatory attributes is available in the CS-MARS user documentation.	
The service failed to read the file pnWinEvent.dat and will now wait for an update to the configuration.	
Failure in reading from pnWiinEvent.dat. Service will wait for an update	

Table 26-1 Possible Application Log Messages for PN Log Agent (Continued)

Warning	
The attribute <attribute_name> has a value that exceeds the CS-MARS limit for an individual attribute value and shall be split.	Warning in case some attribute data in the file exceeds MARS raw message length... MARS will store the data after splitting it into multiple events
Informational	
PnLogAgentService started	Informational messages describing expected operations for the service.
PnLogAgentService Exiting	
The service read the configuration and will attempt to process files.	
As the service has no logs configured, it shall wait for an update	
Exiting thread processing file as service stop received!	

Add and Configure an Cisco Secure ACS Server in MARS

To add the host and Cisco Secure ACS software application to MARS, follow these steps:

Step 1 Click **Admin > Security and Monitor Devices > Add**.

Step 2 From the Device Type list, select **Add SW Security apps on a new host**.

You can also select **Add SW Security apps on an existing host** if you have already defined the host within MARS, perhaps as part of the Management > IP Management settings or if you are running another application on the host, such as Microsoft Internet Information Services.

Step 3 In the Device Name field, enter the hostname of the server or the remote logging host.

Step 4 In the Reporting IP field, enter the IP address of the interface in Cisco Secure ACS server or the remote logging host from which the syslog messages will originate.

Step 5 In the Operating System field, select **Windows**.

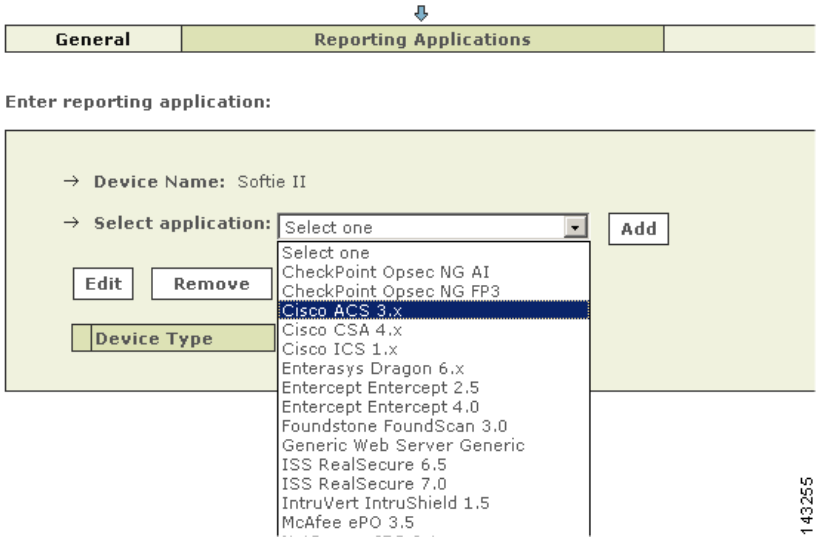
Cisco Secure ACS SW runs only on a Windows host. Windows 2000 and Windows 2003 are the supported platforms for Cisco Secure ACS.

Step 6 Under Enter interface information, enter the interface name, IP address, and netmask value of the interface in Cisco Secure ACS server or remote logging host from which the syslog messages will originate.

This address is the same value as the Reporting IP address.

Step 7 Click **Apply**.

Step 8 Click **Next** to move the Reporting Applications tab.



Step 9 In the Select Application box, select **Cisco ACS 3.x** or **Cisco ACS 4.x**, and then click **Add**.

The Cisco ACS Windows Requirements page appears.

- (3.x) This page explains that you must have installed an agent on the server as described in Install and Configure the PN Log Agent, page 26-8.
- (4.x) This page explains that you must either have enabled the ACS device to publish syslogs to MARS as described in Configure Cisco Secure ACS 4.x to Generate Logs, page 26-3. The PNLog agent *cannot* be used to support the 4.x devices.

Step 10 Click **Submit** to add this application to the host.

`Cisco ACS 3.x` appears in the Device Type list.

Step 11 Click the **Vulnerability Assessment Info** link to define the host information that MARS uses to determine false positive attacks against this host. Continue with Define Vulnerability Assessment Information, page 36-12.

Step 12 Click **Done** to save the changes.

The new host appears in the Security and Monitoring Information list.

Step 13 To enable MARS to start sessionizing events from this device, click **Activate**.

MARS begins to sessionize events generated by this module and evaluate those events using the defined inspection and drop rules. Any events published by the device to MARS before activation can be queried using the reporting IP address of the device as a match criterion. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 1-15.

Add and Configure a Cisco Secure ACS Solutions Engine in MARS

MARS supports the native syslog format for the Cisco Secure ACS Solutions Engine (SE), version 4.x and later. This topic explains how to configure MARS so that it can parse the syslogs it receives from the Cisco Secure ACS SE device.

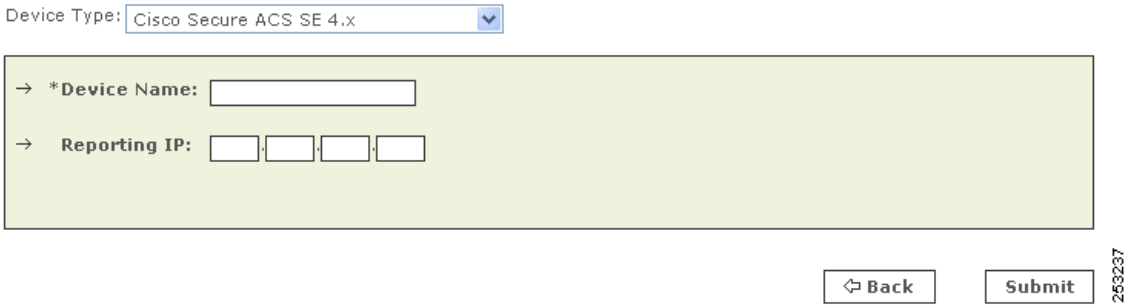
Before You Begin

You must either have enabled the ACS SE device to publish syslogs to MARS as described in Configure Cisco Secure ACS 4.x to Generate Logs, page 26-3. The PNLog agent *cannot* be used to support the 4.x devices.

To add the host and Cisco Secure ACS SE appliance to MARS, follow these steps:

Step 1 Click **Admin > Security and Monitor Devices > Add**.

Step 2 From the Device Type list, select **Cisco Secure ACS SE 4.x**.



Step 3 In the Device Name field, enter the hostname of the appliance.

Step 4 In the Reporting IP field, enter the IP address of the interface in Cisco Secure ACS appliance from which the syslog messages will originate.

Step 5 Click **Submit** to add this application to the host.

`Cisco ACS SE 4.x` appears in the Security and Monitoring Information list.

Step 6 To enable MARS to start sessionizing events from this device, click **Activate**.

MARS begins to sessionize events generated by this module and evaluate those events using the defined inspection and drop rules. Any events published by the device to MARS before activation can be queried using the reporting IP address of the device as a match criterion. For more information on the activate action, see Activate the Reporting and Mitigation Devices, page 1-15.

Troubleshooting Cisco Secure ACS Integration

To verify that MARS is receiving event data from a Cisco Secure ACS, use one of the following options:

- When you configure PN Log Agent, verify that the logs show up in the list of configured files and that you were able to click Activate without errors. If errors occur, verify that you have configured the options as defined in Configure Cisco Secure ACS 3.x to Generate Logs, page 26-4.
- Use TCPDUMP at the MARS CLI to verify that MARS is receiving syslog traffic on port 514 from the PN Log Agent running on the Cisco Secure ACS or remote logging host.
- Use the web interface to submit an inline query to determine whether events are being received from the Cisco Secure ACS. The query definition should include the 'All matching events' option as the Result Format value and Real Time as the Filter By Time value.
- When upgrading to Cisco Secure ACS 4.1, the location of the log files changes. To address this issue, you must reconfigure the PN Log Agent to point to the new folders.

Error Messages

The service detected that the configured file is missing some mandatory header attributes.

Issue: It is possible receive an error in the Application Log accessed using the Event Viewer that states the following:

```
Event Type: Error
Event Source: pnLogAgentService
Event Category: None
Event ID: 1
Date:  9/7/2006
Time:  12:00:53 AM
User:  N/A
Computer: ACS1
Description:
LogEventService: The service detected that the configured file is missing some mandatory header attributes. A
list of mandatory attributes is available in the CS-MARS user documentation.
```

This error is not accompanied with any advice about how to resolve the error and PN Log Agent indicates no errors during configuration. The cause of this error messages is that when the log file changes at midnight, the file header is not written out until an event is generated. Thus, when the PN Log Agent service detects that the logs are missing headers, it generates the error.

Resolution: You can safely ignore such errors that re-occur daily around the same time (around midnight) as long as the MARS Appliance still receives events from the he Cisco Secure ACS or remote logging host. If you are otherwise receiving this message, it indicates that you have not properly configured the Cisco Secure ACS to generate events required by the PN Log Agent. Verify that you have configured the options as defined in Configure Cisco Secure ACS 3.x to Generate Logs, page 26-4.