



CHAPTER 15

Configuring AAA Devices

Revised: February 23, 2007

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, page 2-53](#) and [Enable NAC-specific Messages, page 4-4](#)). 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 logs in 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.

The following sections detail supporting a Cisco Secure ACS server:

- [Bootstrap Cisco Secure ACS, page 15-3](#)
- [Install and Configure the PN Log Agent, page 15-7](#)
- [Add and Configure the Cisco ACS Device in MARS, page 15-12](#)

Supporting Cisco Secure ACS Solution Engine

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 15-3](#).
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 15-7](#).

4. Add the remote logging host to MARS as a Cisco ACS 3.x reporting device. To perform this task see [Add and Configure the Cisco ACS Device in MARS, page 15-12](#), and substitute the ACS server references with the remote logging host.

Bootstrap Cisco Secure ACS

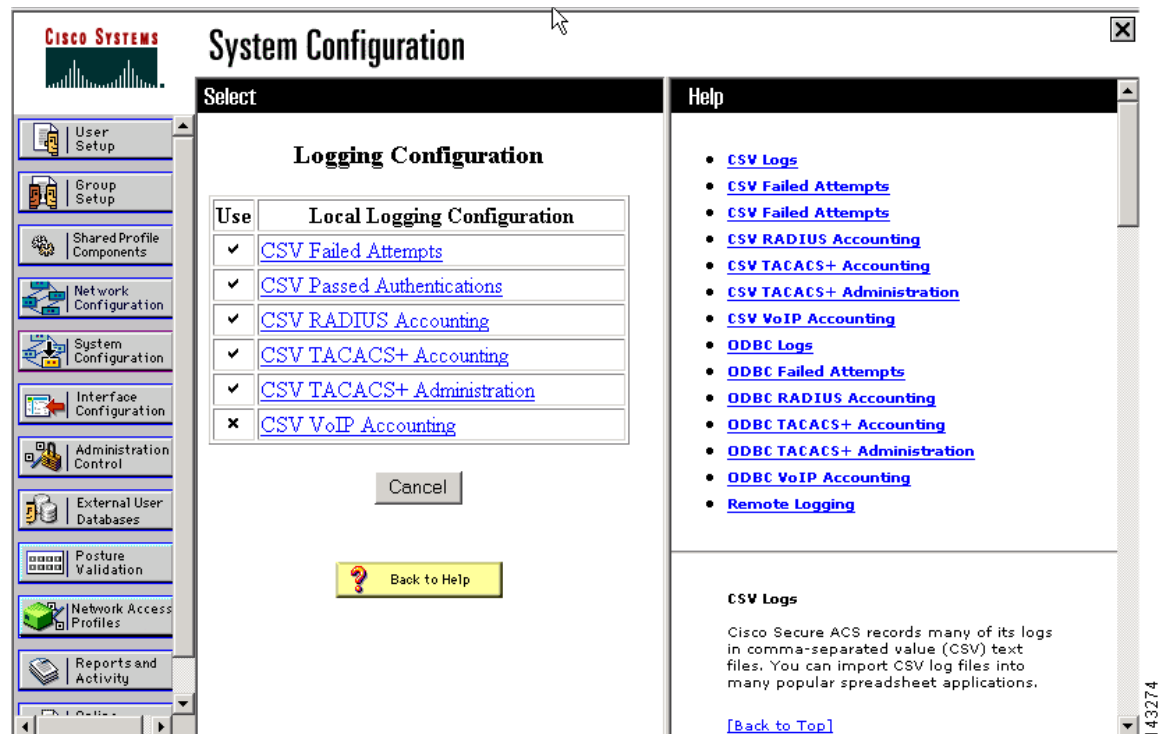
Bootstrapping the Cisco Secure ACS includes the following task:

- [Configure Cisco Secure ACS to Generate Logs, page 15-3](#)
- [Define AAA Clients, page 15-5](#)
- (Optional) [Configure TACACS+ Command Authorization for Cisco Routers and Switches, page 15-7](#)

Configure Cisco Secure ACS to Generate Logs

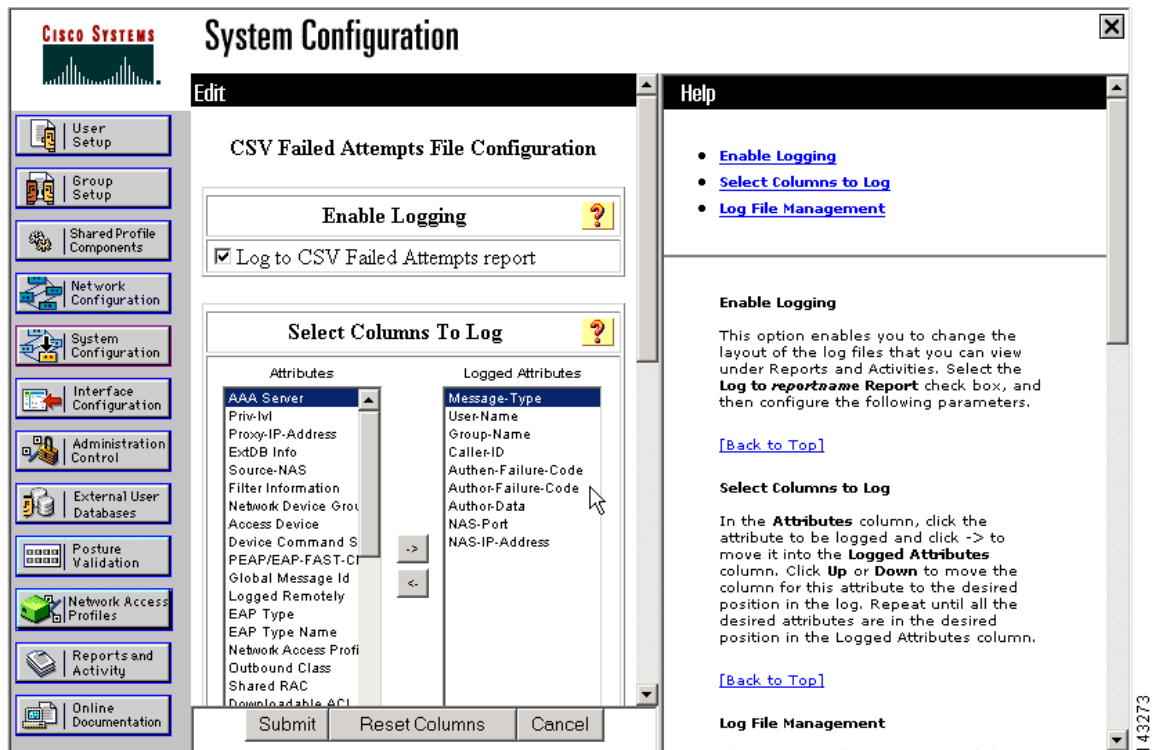
To configure Cisco Secure ACS to generate the audit logs required by MARS, follow these steps:

- Step 1** Log in to the Cisco Secure ACS server or Solution Engine.
- Step 2** Select **System Configuration > Logging**.



- Step 3** Verify that CSV Failed Attempts, CSV Passed Authentications and CSV 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

CSV RADIUS Accounting File Configuration

The screenshot displays two configuration windows. The first window, titled 'Enable Logging', has a yellow question mark icon and contains a checked checkbox labeled 'Log to CSV RADIUS Accounting report'. The second window, titled 'Select Columns To Log', also has a yellow question mark icon and is divided into two panes. The left pane, 'Attributes', lists various RADIUS attributes such as Service-Type, Framed-Protocol, Login-IP-Host, Login-Service, Class, Termination-Action, Called-Station-Id, NAS-Identifier, Proxy-State, Login-LAT-Service, Login-LAT-Node, Login-LAT-Group, Acct-Delay-Time, Acct-Input-Octets, Acct-Output-Octets, Acct-Session-Id, Acct-Authentic, Acct-Session-Time, Acct-Input-Packets, and Acct-Output-Packets. The right pane, 'Logged Attributes', lists the selected attributes: User-Name, Calling-Station-Id, Acct-Status-Type, Framed-IP-Address, NAS-Port, NAS-IP-Address, and cisco-av-pair. Between the panes are arrows for moving items, and 'Up' and 'Down' buttons are at the bottom right. A small number '143275' is visible on the right side of the window.

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 15-1 displays example settings for such a client.

Figure 15-1 Configure a AAA Client to Support 802.1x

The screenshot shows the Cisco Secure ACS Network Configuration interface. The main window is titled "AAA Client Setup For 802.1xrouter". The configuration fields are as follows:

- AAA Client IP Address: 20.1.1.1
- Key: protego
- Authenticate Using: RADIUS (IETF)
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure):
- Log Update/Watchdog Packets from this AAA Client:
- Log RADIUS Tunneling Packets from this AAA Client:
- Replace RADIUS Port info with Username from this AAA Client:

Buttons at the bottom include: Submit, Submit + Apply, Delete, Delete + Apply, Cancel, and Back to Help.

The Help sidebar on the right contains the following links:

- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Deleting a AAA Client](#)
- [Renaming a AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)
- [Replace RADIUS Port info with Username from this AAA Client](#)

The AAA Client IP Address help text states: "Type the IP address information for this AAA client. If you want to designate more than one AAA client with a single AAA client entry in Cisco Secure ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**. You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address"

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 15-10](#).

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 15-10](#).

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.



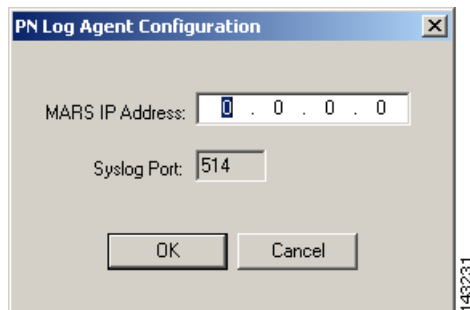
Note If installing on a remote logging host, you must have configured the Cisco Secure ACS Remote Agent for Windows on the target remote logging host.

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**.

Result: The PN Log Agent Configuration dialog box appears.

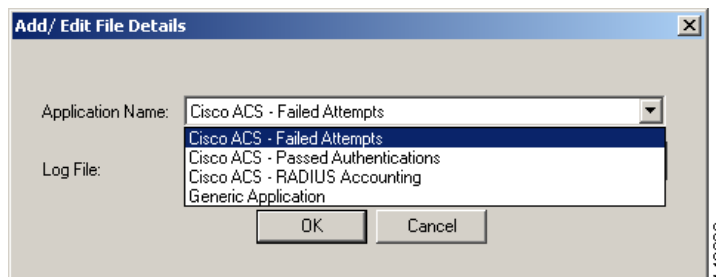


- Step 4** In the MARS IP Address field, enter the address of the MARS Appliance, and click **OK**.

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

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

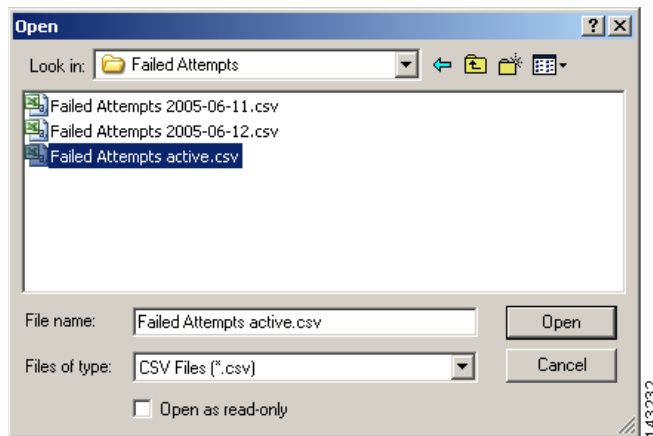
Result: The Add/Edit File Details dialog box appears.



- 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.

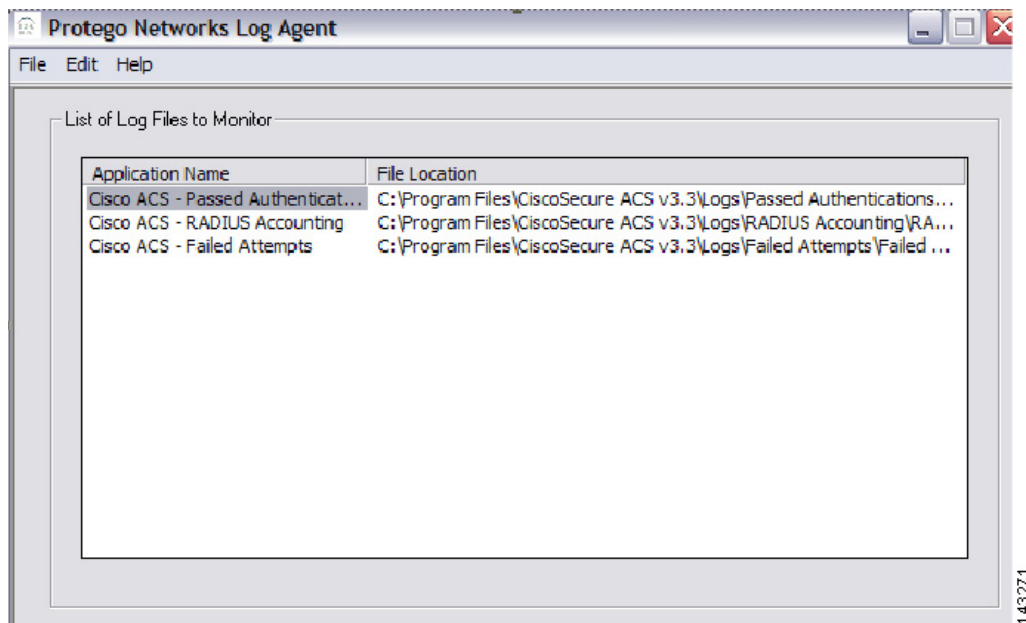
Result: The Open dialog box appears.



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

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

Result: 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.
- To uninstall the old agent, click **Start > Control Panel > Add/Remove Programs**.
 - Select **PnLogAgent** in the list of currently installed programs, and click **Remove**.
 - 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 15-7](#).
-

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 15-1](#) categories the types of messages that can occur and explains their affects on the PnLog Agent service.

Table 15-1 Possible Application Log Messages for PN Log Agent

Type/Message	Effect on Service/Cause of Error
Fatal Errors	

Table 15-1 Possible Application Log Messages for PN Log Agent (continued)

Type/Message	Effect on Service/Cause of Error
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>	
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	
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	

Table 15-1 Possible Application Log Messages for PN Log Agent (continued)

Type/Message	Effect on Service/Cause of Error
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 the Cisco ACS Device 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** 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 6** Click **Apply**.
 - Step 7** Click **Next** to move the Reporting Applications tab.

↓

General	Reporting Applications	
---------	------------------------	--

Enter reporting application:

→ Device Name: Softie II

→ Select application: Select one Add

Edit
Remove

Device Type

Select one

CheckPoint Opsec NG AI

CheckPoint Opsec NG FP3

Cisco ACS 3.x

Cisco CSA 4.x

Cisco ICS 1.x

Enterasys Dragon 6.x

Entercept Entercept 2.5

Entercept Entercept 4.0

Foundstone FoundScan 3.0

Generic Web Server Generic

ISS RealSecure 6.5

ISS RealSecure 7.0

IntruVert IntruShield 1.5

McAfee ePO 3.5

143255

Step 8 In the Select Application box, select **Cisco ACS 3.x**, and then click **Add**.

Result: The Cisco ACS 3.x Windows Requirements page appears, explaining that you must have installed an agent on the server as described in [Install and Configure the PN Log Agent, page 15-7](#).



Note

The Cisco ACS 3.x option supports both Cisco Secure ACS 3.x and Cisco Secure ACS 4.0. No explicit 4.0 option exists for Cisco Secure ACS.

Step 9 Click **Submit** to add this application to the host.

Result: Cisco ACS 3.x appears in the Device Type list.

Step 10 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 11-12](#).

Step 11 Click **Done** to save the changes.

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

Step 12 To activate the device, click **Activate**.

