CHAPTER 6

Cisco Trust Agent Event Logging

CTA logging is disabled by default because CTA is intended to be a transparent application to end users. If you enable logging, CTA logs events generated by CTA components and the posture plugins for the NAC-compliant applications that reside on the system.

This chapter contains the following sections:

How Logging Works

Event logging is implemented as a service on the network client. When the CTA Event Logger service starts, it reads the logging configuration file, ctalogd.ini and uses any logging levels and settings that are specified. If no logging levels or settings are specified in the ctalogd.ini file, the logging service uses its default values.

If logging is enabled, the events are evaluated against the default logging levels or those defined in the ctalogd.ini file. Events that meet the logging level are formatted and written to the log file.

Note CTA logging is disabled by default and can be enabled by using the clogcli utility, see "The clogcli Logging Utility" section on page 6-4 for more information.

CTA Log Files

CTA log files are text files created by the Cisco Trust Agent Event Logging service. They are ASCII text files that you can view using any text editor. Log file names are automatically generated by the event logger whenever a log file is created. A new log file is created when one of the following events occur:

- Logging is changed from disabled to enabled.
- The log file is cleared while logging is enabled.
- The current log file reaches the maximum file size.

Note The creation of the log file does not occur until the first event is received while logging is enabled.

On **Windows** operating systems, this is the default location of log files:

```
\Program Files\Cisco Systems\CiscoTrustAgent\Logging\Logs
```

On **Linux** and **Mac OS X** operating systems, this is the default location of log files:

```
/var/log/CiscoTrustAgent
```

These log file directory locations can be changed using the clogcli utility. See, "The clogcli Logging Utility" section on page 6-4 for this procedure.

The logfile names use the date and time the event logger was started to create unique file names. The log file names contain the following format:

CTALOG-YYYY-MM-DDTHH-MM-SS_N.txt.

- **CTALOG**—A fixed prefix indicating that CTA created the log.
- **YYYY**—A four-digit value for the year.
- **MM**—A two-digit value for the month.
- **DD**—A two-digit value for the day.
- **T**—A fixed separator between the date and time.
- **HH**—A two-digit value for the hours, specified in 24-hour time.
- **MM**—A two-digit value for the minutes.
- **SS**—A two-digit value for the seconds.
- **N**—The n^{th} log file created since the event logger was started. This occurs when the current log file reaches the maximum size or when logging is disabled and then enabled.

For example, if the event logger was started on September 20, 2007 at 5:12:58 p.m. the generated log file name would be named `CTALOG-2007-09-20T17-12-58_1.txt`.

Log File Format

The log file contains the following fields:

- **Logging Instance**—An incremental number for the log entry.
- **Date/Time**—The date and time the entry was logged.
- **Severity**—The severity of the logged event. Valid severity values are:
  - Critical
  - Info
  - Warning
- **Error Code**—The error code associated with the event.
- **Message Body**—Text describing the event.

The following displays examples of log file entries:

Example 6-1 CTA Log File Sample Entries

```
Cisco Systems Trust Agent Version 2.0
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Trust Agent Type(s): Windows, WinNT Running on: 5.1.2600

1   15:29:57.748  07/13/05 Sev=Info/3  PADaemon/0x6300000C
Starting service:

2   15:30:40.719  07/13/05 Sev=Info/3  NetTrans/0x63100016
NAD proposed AssociationID 56789
```

Logging Considerations

Log files remain on the disk until a user deletes them, the allotted disc space for logs is used up, or the log file reaches a certain age.

If you enable a high-level of logging, you can potentially fill the disk over time. If you enable logging by default, ensure that a policy for regular log file removal or archival is in place.

The clogcli Logging Utility

CTA provides a utility, **clogcli**, which can be run locally on the end user system. clogcli provides a way for users to enable, disable, and configure logging. This utility is useful in situations where local system troubleshooting is required. The clogcli utility runs at the command line.

On Windows operating systems, clogcli is stored in this directory:

```
\Program Files\Cisco Systems\CiscoTrustAgent\
```

On Linux and Mac OS X operating systems, clogcli is stored in this directory:
`/opt/CiscoTrustAgent/sbin`

To run the clogcli utility, follow this procedure:

Step 1 Open a Command Prompt Window (Windows) or a Terminal Window (Linux and Mac OS X).

Step 2 Change the directory to the one in which clogcli is stored:

- For Windows operating systems, change the directory to: `\Program Files\Cisco Systems\CiscoTrustAgent\`
- For Linux and Mac OS X operating systems, change the directory to: `/opt/CiscoTrustAgent/sbin`

Step 3 At the prompt type **clogcli**, followed by the proper command, and press <Enter>. The command syntax is the same for Windows and Linux operating systems and slightly different for Mac OS X operating systems.

Table 6-1 describes all the commands and options for the clogcli utility.

Table 6-1 clogcli Utility Command Option

Option	Description and example
clear	Clears the current log file. A new log file is created if logging is enabled. Linux and Windows example: #> **clogcli clear** Mac OS X example: $ **./clogcli clear**
disable	Disables logging. Parameter name in ctalogd.ini: EnableLog=0 Linux and Windows example: #> **clogcli disable** Mac OS X example: $ **./clogcli disable**

Table 6-1 clogcli Utility Command Option (continued)

Option	Description and example
enable	Enables logging. Parameter name in ctalogd.ini: EnableLog=1 Linux and Windows example: #> **clogcli enable** Mac OS X example: $ **./clogcli enable**
enable -t	Enables logging until the machine is rebooted. Parameter name in ctalogd.ini: EnableLog=2 Linux and Windows example: #> **clogcli enable -t** Mac OS X example: $ **./clogcli enable -t**

Table 6-1 clogcli Utility Command Option (continued)

Option	Description and example
logdir	Sets the log file location for CTA logs. Parameter name in ctalogd.ini: LogDir Default Windows Location: \Program Files\Cisco Systems\CiscoTrustAgent\Logging\Logs Default Linux Location: `/var/log/CiscoTrustAgent` Range of Values: Any existing directory location. Windows example: > **`clogcli logdir c:\Temp\CTALogs`** Linux example: # **`clogcli logdir /tmp/CTALogs`** Mac OS X example: $ **`./clogcli logdir /tmp/CTALogs`** **Note** This note is for **Linux** systems only. For security reasons, ctalogd does not run with "administrator" or "root" permissions. Therefore, it is possible for you to specify a directory that ctalogd does not have permission to write to. If ctalogd is not able to create the log file in the directory you specify, then it will create the log file in the default logging directory. You should also see an error message in the syslog. After you begin logging, check both your chosen and the default directories to verify the location of your log file.

Table 6-1 clogcli Utility Command Option (continued)

Option	Description and example
loglevel	Sets the log level for all CTA components at once and to the same level. See, "Logging Levels" section on page 6-11 for descriptions of the logging levels. Default Value: 3 Range of values: 1-3, 15 Linux and Windows example: #> **clogcli loglevel 2** Mac OS X example: $ **./clogcli loglevel 2**
maxdisk	Sets the maximum number of megabytes of space that may be used for logging. Parameter name in ctalogd.ini: MaxDiskSize Default Value: 50 Range of Values: 50-100 Special Value: 0 - If maxdisk is set to zero then there is no disk space limit for log files. Linux and Windows example: #> **clogcli maxdisk 60** Mac OS X example: $ ./**clogcli maxdisk 60**

Table 6-1 clogcli Utility Command Option (continued)

Option	Description and example
maxfile	Sets the minimum log file size in megabytes. Parameter name in ctalogd.ini: MaxFileSize Default Value: 4 MB Range of Values: 0 - 50 MB. Special Value: 0 - If maxfile is set to zero, then there is no limit on the log size. Linux and Windows example: #> **clogcli maxfile 5** Mac OS X example: $ **./clogcli maxfile 5**

Table 6-1 clogcli Utility Command Option (continued)

Option	Description and example
zipit	This command retrieves log files and configuration files and inserts the files into a zip file which is stored on the Windows desktop and in the user's home directory on Linux or Mac OS X operating systems. Linux and Windows example: #> clogcli **zipit** Mac OS X example: $ **./clogcli zipit** The zip file is named: *NAC-TS-YYYY-MM-DDTHH-MM-SS*.zip Where "NAC-TS" stands for Network Admission Control - Technical Support. The log file follows the Year-Month-DayTHours-Minutes-Seconds convention of the ctalog file. These are the files collected by the **clogcli zipit** command: • CTA log files: \Program Files\Cisco Systems\CiscoTrustAgent\Logging\Logs**CTALOG*.txt** • If CTA 802.1x Wired Client is installed or was once installed and the old log files were not deleted, these files will also be collected: – \Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client \system\log**apiDebug*.txt** – \Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client \system\log**clientDebug*.txt** – \Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client**log*.txt** • Output from ctastat: **ctastat-output.txt** • **ctad.ini file** • **ctalogd.ini file** **Note** Log files generated by Cisco Secure Services Client are not collected by the clogcli zipit command.

Logging Levels

Setting the logging level determines which events are added to the log file. Each logging level provides an incremental addition to the logging information provided by the level below it.

- **1-LOW** — Low-level logging includes critical events. The intent of the low setting is to ensure that your log file does not grow too large while still logging the events that are likely most worth your attention.
- **2-MEDIUM** — Medium-level logging includes warnings and the critical events provided in the low setting.
- **3-HIGH** — High-level logging includes informational events, such as success messages, warnings, and critical events.
- **15-EVERYTHING** — This is the most verbose level of logging. It captures all messages.

HIGH is the default level used when logging is enabled. You can change the logging level for each CTA component using the clogcli utility.

As a general guideline, when troubleshooting problems on systems running CTA, keep the logging level set to **3** to receive the most information about the system operation. If you configure logging to be enabled and there are no issues, you should set the logging level to Medium or Low. Setting the logging level to medium or low prevents the log file from growing rapidly and consuming disk space, yet provides enough information to diagnose any possible problems with CTA, posture plugins, or system posture.

Configuring CTA Logging For Large Deployments

To deploy a specialized level of logging state, logging size, log file locations and log file size, you can create a ctalogd.ini file that can be distributed in a custom installation package.

The ctalogd.ini file contains the configuration parameters for CTA logging. The ctalogd.ini file is not delivered at the time of installation; it is created when you use the clogcli utility to enable logging and change logging attributes.

CTA logging is disabled by default. Once logging is enabled, the default logging attributes are used unless you specify different attributes in the ctalogd.ini file.

To configure CTA logging, follow this procedure:

Step 1 Use the simplest method to install CTA on a test machine. See, Chapter 2, "Installing the Cisco Trust Agent on Linux Operating Systems," Chapter 3, "Installing the Cisco Trust Agent on Macintosh Operating Systems,"or Chapter 4, "Installing the Cisco Trust Agent on Windows Operating Systems" for the appropriate installation method.

Step 2 Verify that CTA has been installed and is running by using the "Verifying Cisco Trust Agent Installation" procedure in the installation chapter.

Step 3 Enable logging by using the **clogcli enable** command as described in the "The clogcli Logging Utility" section on page 6-4.

Step 4 On the test machine, start the resident file management application and change the directory to the /etc/opt/CiscoTrustAgent directory on Linux and Mac OS X operating systems or the \Programs\Cisco Systems\CiscoTrustAgent\Logging directory on Windows operating systems. You should see the ctalogd.ini file in that directory.

Step 5 Read the ctalogd.ini file. You should see one section and one entry in the file:

```
[main]
EnableLog=1
```

Step 6 Close the ctalogd.ini file.

Step 7 Continuing to use the clogcli logging utility, specify the logging attributes and logging levels you desire.

Step 8 When you are done configuring the logging attributes, you can distribute the ctalogd.ini file to an individual machine, by storing it in the /etc/opt/CiscoTrustAgent directory on Linux and Mac OS X operating systems or the \Programs\Cisco Systems\CiscoTrustAgent\Logging directory on Windows operating systems. You can also distribute the ctalogd.ini file to many machines when you perform a CTA installation with a custom installation package. These machines will all use the logging attributes you specified in the file.

Sample ctalogd-temp.ini File

CTA logging is disabled by default. The clogcli utility is designed to create the ctalogd.ini file which defines logging parameters for a local installation. There is also a ctalogd-temp.ini file that is shipped with CTA as a template file. Advanced users can edit the file directly if they so choose.

The ctalogd-temp.ini file is delivered to this location on Windows operating systems: \Program Files\Cisco Systems\CiscoTrustAgent\Logging

The ctalogd-temp.ini file is delivered to this location on Linux and Mac OS X operating systems: /etc/opt/CiscoTrustAgent

See Example 6-2 for an example of the ctalogd-temp.ini file.

Example 6-2 Sample ctalogd-temp.ini File

```
; This file contains Cisco Trust Agent log settings.
; To use these settings, save a coy of this file as ctalogd.ini
; and edit that file.
; This file may be used for Linux, Mac OS X, and Windows operating
; systems.

[main]
; This section turns logging on or off and defines the size, age and
; location of CTA log files.
EnableLog=0
; 0 = disable logging
; 1 = enable logging
MaxFileSize=4
MaxDiskSize=50
FileDeleteAge=30
;LogDir=/var/log/CiscoTrustAgent
LogDir=D:\Program Files\Cisco Systems\CiscoTrustAgent\Logging\Logs

[LogLevel]
; This section allows you to set the logging levels
; for various components of the Cisco Trust Agent.
; 0 = disable
; 1 = log critical events only
; 2 = log critical and warning events
; 3 = log critical, warning, and informational events
; 15 = log all events and messages
```

```
PADaemon=3
NetTrans=3
PAPlugin=3
CTAMsg=3
CTAD=3
PEAP=3
EAPTLV=3
EAPSQ=3
PPMgr=3
PSDaemon=3
HostPP=3
CTASC=3
CTASTATE=3
```