CHAPTER 10

Cisco Trust Agent 802.1x Wired Client Logging

In the event of operational problems, with local hardware, with a network access device or authentication server, or internally, these features are available to aid a user or support technician debug an unexpected event in the client:

- Technical Log
- System Report

Tip When using any antivirus software with the client, it is best to configure the antivirus software, if possible, to ignore scanning/processing current "active" log files in order to avoid consuming processing resources during an authentication.

This chapter contains the following sections:

Technical Log

The technical log file is a time-stamped, Unicode text file that is the destination for log messages capable of being viewed with Notepad (or equivalent) on Windows 2000 and Windows XP. These are the characteristics of the Technical Log:

- The “file” is actually a series of files. The client stops using the current log file and creates a new log file whenever the client starts up or the maximum file size is reached (1MB).
- The set of files have a maximum amount of allocated non-volatile (disk) space of approximately 5 MB. When the maximum storage level is reached, the oldest log file is deleted.
- The current log file has the format: log_current.txt.
- Each archived file has the following naming format: log_<date>_<time>.txt, where <date> has the format YYYY-MM-DD, where YYYY is the year, MM is the month and DD is the day and <time> has the format: hh.mm.ss, where hh is the hour, mm is the minute and ss is the second.

  The date/time indicates when the file was archived. Archived files therefore contain events prior to this time.
- The set of files are located in a folder named ‘log’, below the main install folder. This would be **Program Files\Cisco Systems\Cisco Trust Agent 802_1x Wired Client\log** for the default install folder.
- Each log file contains a list of single line entries, where each entry defines a single log event.

The technical log level is intended for those users who have training in 802.1x, 802.11i, EAP, EAP methods, PKI and understand the profiles and policies of the client.

See “Understanding the Technical Log Status and Error Messages” section on page 10-3 for a description of all the error codes.

Understanding the Technical Log Status and Error Messages

This section describes the format and contents of the Technical Log status and error messages.

Technical Log Message Format

Every log entry has the format:

```
<date & time> [process] <log message id> <log message class> <context IDs> <grammatical log message>
```

These are the descriptions of each part of a log entry:

Table 10-1 Log Entry Field Descriptions

Log Entry Field	Description
<date & time>	Provided in the format MM/DD/YYYY HH:mm:SS.sss, where: • MM - numeric month (01-12) • DD - numeric day (01-31) • YYYY - numeric year (e.g. 2005) • HH - numeric hour on a 24 hour clock (00-23) • mm - numeric minutes past the hour (00-59) • SS.sss - numeric seconds with SS being seconds, and sss being fractions of a second.
[process]	An internal process identifier developers use in troubleshooting problems.
<log message id>	The unique number for the log message.

Table 10-1 Log Entry Field Descriptions (continued)

Log Entry Field	Description
<log message class>	Determines the type of log message and is one of the following: • I – informational log message - used to indicate a client state that is part of normal processing. • W – warning log message - used to indicate a client state that is insecure or unexpected but which still allows processing. • E – error log message - used to indicate an exception that prevents normal processing.
<context IDs>	Conveys zero or more identifiers to define the context of this log event. Each has the following format: • <code><unique string/number> where: • n < code> is a two letter code that indicates the class of the term. • n < unique string/number> is string or number that is guaranteed to be unique. • Adapter Identifier - AD<MAC address in hexadecimal for the adapter> • Access Identifier - AC<MAC/BSSID for the access device> • Media Type Identifier - MT<Ethernet | WiFi> (Note: MT may or may not be explicitly indicated) • Connection Identifier - CN<an incrementing integer> • Profile Identifier - PR<profile name truncated to 16 characters>
<grammatical log message>	A sentence that describes the event. It may also contain a variable <value>.
<value>	The <value> in the <grammatical log message> is a placeholder for a variable value to be placed in the message.

Example 10-1 Technical log content:

```
04/20/2006 15:28:47.859 [ 432. 728]  103 I CN<3> Cisco Trust Agent 802.1X wired client
AD<000cf1aeddfc> AC<000cf1aeddfc> Connection Requested automatically from user context.
04/20/2006 15:28:47.875 [ 432.1716]  109 I CN<3> AD<000cf1aeddfc> Connection
Authentication Started in user context.
```

```
04/20/2006 15:28:47.875 [ 432.1136]   29 I CN<3> AD<000cf1aeddfc> Port State Machine
transition to AC_PORT_STATE_CONNECTING(AC_PORT_STATUS_STARTED)
04/20/2006 15:28:48.812 [ 432.1136]   29 I CN<3> AD<000cf1aeddfc> Port State Machine
transition to AC_PORT_STATE_UNAUTHENTICATED(AC_PORT_STATUS_EAP_FAILURE)
04/20/2006 15:28:48.812 [ 432.1136]   77 E CN<3> AD<000cf1aeddfc> Connection
Authentication Failed.
04/20/2006 15:28:49.828 [ 432.1136]   29 I CN<3> AD<000cf1aeddfc> Port State Machine
transition to AC_PORT_STATE_AUTHENTICATING(AC_PORT_STATUS_8021x_ACQUIRED)
04/20/2006 15:28:49.843 [ 432.1716]   24 I CN<3> AD<000cf1aeddfc> Identity requested.
04/20/2006 15:28:58.968 [ 432.1136]   25 I CN<3> AD<000cf1aeddfc> Identity sent.
04/20/2006 15:28:58.984 [ 432.1532]   28 I CN<3> AD<000cf1aeddfc> Authentication method
started: EAP-FAST, level 0
04/20/2006 15:28:59.000 [ 432.1136]   26 I CN<3> AD<000cf1aeddfc> EAP method suggested by
server: EAP-FAST
04/20/2006 15:28:59.000 [ 432.1136]   27 I CN<3> AD<000cf1aeddfc> EAP methods requested by
client:  EAP-FAST
04/20/2006 15:28:59.015 [ 432. 728]   73 I CN<3> Client is validating the server.
04/20/2006 15:28:59.015 [ 432. 728]  140 I CN<3> Server AID validated:
57dda0ae0004a74f8c7c959d687c4ed2
04/20/2006 15:28:59.062 [ 432.1532]   28 I CN<3> AD<000cf1aeddfc> Authentication method
started: EAP-GTC, level 1
04/20/2006 15:28:59.062 [ 432.1136]   26 I CN<3> AD<000cf1aeddfc> EAP method suggested by
server: EAP-GTC
04/20/2006 15:28:59.062 [ 432.1136]   27 I CN<3> AD<000cf1aeddfc> EAP methods requested by
client:  EAP-GTC
04/20/2006 15:28:59.062 [ 432.1532]   24 I CN<3> AD<000cf1aeddfc> Identity requested.
04/20/2006 15:28:59.078 [ 432.1136]   25 I CN<3> AD<000cf1aeddfc> Identity sent.
04/20/2006 15:29:04.078 [ 432.1136]   29 I CN<3> AD<000cf1aeddfc> Port State Machine
transition to AC_PORT_STATE_AUTHENTICATED(AC_PORT_STATUS_8021x_ACQUIRED)
```

Technical Log Message Content

These are the messages that can be recorded in the technical log file.

Note See "Additional Message <value> Descriptions" section on page 10-11 for the descriptions of the message <value> fields.

Note See "Port Status Values" section on page 10-12 for the list of expanded descriptions of a <Port State> value.

Table 10-2 Technical Log Messages and Codes

Class	ID	Context IDs	Message
Client processing messages			
I	1		Client Service Auto Started. <Client's service name>, <version number>, <OS Name>
I	101		Client Service Manually Started. <Client's service name>, <version number>, <OS Name>
I	2		Client Service Normal Shutdown. <Client's service name>, <version number>, <OS Name>
E	133		Client Service Fatal Error Shutdown. <Client's service name>, <version number>, <OS Name> *Recovery Action*: Manually stop and start the service or in extreme cases, uninstall and reinstall the client (your configuration files will be maintained).
I	3		Boot processing initiated.
Client environment processing messages			
I	85		Entering power save mode. *Note*: Entering standby/hibernate mode.
I	86		Exiting power save mode (automatic) *Note*: Exiting standby mode - will be followed with Error Msg #87.
I	87		Exiting power save mode. *Note*: Exiting standby mode if preceded by Error Msg #86, otherwise exiting hibernate mode.
User Logon processing messages			
I	4		User logon processing initiated.
I	134		Manual user <logon type> logon processing initiated by user <user id>.
I	129		User single sign-on credentials obtained from Novell GINA
I	130		User single sign-on credentials obtained from Microsoft GINA

Table 10-2 Technical Log Messages and Codes (continued)

Class	ID	Context IDs	Message
I	5		User logoff processing initiated
Adapter processing messages			
I	6	AD< > MT< >	Adapter Detected.
I	8	AD< >	Adapter Controlled.
E	30	AD< >	Adapter startup failed because driver is in use. *Recovery Action*: Manually disable competing utility.
I	14	AD< >	Control has been released for this adapter.
I	135	AD< >	Wired Access device disappeared.
I	7	AD< >	Adapter Removed.
I	95	AD< >	User: User requested client to manage adapter
I	96	AD< >	User: User requested client to not manage adapter
Access device processing messages			
I	15	AC< >	Wired Access device detected.
Connection processing messages			
I	16	CN< > PR < > AD< > AC< >	Connection Requested automatically from machine context.
I	103	CN< > PR < > AD< > AC< >	Connection Requested automatically from user context.
I	104	CN< > PR < > AD< > AC< >	Connection Requested by user from user context.
I	94	PR < >	User: User requested disconnect for network.
I	17	CN< >	Connection Terminated by user request.
I	105	CN< >	Connection Terminated due to service shutdown.
I	106	CN< >	Connection Terminated because adapter was removed.
I	107	CN< >	Connection Terminated because access device disappeared.

Table 10-2 Technical Log Messages and Codes (continued)

Class	ID	Context IDs	Message
E	108	CN< >	Connection Terminated due to fatal error number <error number>: <error text>. *Recovery Action:* Manually restart the Cisco Trust Agent 802.1x Wired Client service.
Connection processing - IP specific messages			
I	82	CN< >	DHCP: Sending DHCP request.
E	84	CN< >	DHCP: Request failed because of time out. *Recovery Action*: Verify network readiness - failure outside of client.
E	110	CN< >	DHCP: Server responded with failure. *Recovery Action*: Verify network readiness - failure outside of client.
E	111	CN< >	DHCP: Unknown failure has occurred. *Recovery Action*: Verify network readiness - failure outside of client.
I	78	CN < >	Connection IP Address Received: Address: <IP Address>.
Authentication processing messages			
I	23	CN< > AD< >	Connection Authentication Started in machine context.
I	109	CN< > AD< >	Connection Authentication Started in user context.
I	24	CN< > AD< >	Identity requested.
I	25	CN< > AD< >	Identity sent.
I	26	CN< > AD< >	EAP method suggested by server: <Authentication Method name>.
I	27	CN< > AD< >	EAP methods requested by client: (<Authentication Method name>, …, <Authentication Method name>).
I	28	CN< > AD< >	Authentication method started: <tunnel depth>, <sequence number>, <Authentication Method name>.
I	29	CN< > AD< >	Port State Machine transition to <Port State>(<Port status>).
I	76	CN< > AD< >	Connection Authentication Success.

Table 10-2 Technical Log Messages and Codes (continued)

Class	ID	Context IDs	Message
E	77	CN< > AD< >	Connection Authentication Failed. *Recover Action*: Verify consistency of client, access point and server configuration.
EAP Notification messages			
I	143	CN< >	EAP Notification message received from: <ssid> <EAP Notification>
Authentication processing - FAST specific messages			
W	125	CN< > AD< >	FAST: unauthenticated provisioning supported.
Authentication processing - server validation specific messages			
W	72	CD< >	Trusted Server list empty, server can not be validated.
I	73	CN< >	Client is validating the server.
I	74	CD< >	Server certificate validated: <Authentication Server Id>.
W	142	CD< >	Profile does not require server validation.
E	75	CD< >	Server certificate invalid because unknown CA. *Recovery Action*: Verify that the correct CA certificate is in the Windows trusted root certificate store.
E	115	CD< >	Server certificate invalid because CN mismatch in Subject: <CN name from server cert>. *Recovery Action*: Verify the server validation rule configuration.
E	116	CD< >	Server certificate invalid because DC mismatch in Subject: <DC name from server cert>. *Recovery Action*: Verify the server validation rule configuration.
E	117	CD< >	Server certificate invalid because Subject Alternative Name mismatch: <Alternative name from server cert>. *Recovery Action*: Verify the server validation rule configuration.
I	140	CN< >	Server AID validated: <AID-info>
E	141	CN< >	Server not trusted because AID mismatch: <AID-info> *Recovery Action*: Verify the server validation rule configuration.

Table 10-2 Technical Log Messages and Codes (continued)

Class	ID	Context IDs	Message
User profile configuring - manage trusted servers messages			
I	97		User: User added certificate based trusted server <Rule name>: <certificate-based trusted server rule>
I	112		User: User added pac based trusted server <Rule name>: with AID: <AID-info>
I	98		User: User removed all trusted servers.
I	99		User: User modified trusted server list, <certificate-based trusted server rule>.
License processing messages			
I	89		Licensing: License file found.
E	90		Licensing: License file not found. *Recovery Action*: verify existence of the <install folder>\licenseTransport.txt file.
I	91		Licensing: License read: <License string>.
W	92		Licensing: License invalid because trial period expired <License string>, <trial period>.
W	118		Licensing: License invalid because termination date reached: <License string>, <termination date>.
W	119		Licensing: License invalid because operating system mismatch: <License string>, <licensed os>.
W	120		Licensing: License invalid because product id does not match: <License string>, <licensed product id>.
W	121		Licensing: License invalid because OEM id does not match: <License string>, <licensed OEM id>.
W	122		Licensing: License invalid because maintenance date reached: <License string>, <maintenance date>.
W	123		Licensing: License invalid due to unknown problem: <License string>, <termination date>.
W	131		Licensing: Ignoring trial license. Tampering detected: <License string>.

Table 10-2 Technical Log Messages and Codes (continued)

Class	ID	Context IDs	Message
I	93		Licensing: License is valid and accepted: <License string>.
Internal messages			
W	0		Technical log message ID[<msgId>] not found.

Additional Message <value> Descriptions

Table 10-3 Message <value> Variables and Descriptions

Variables in log messages	Description
<Client's service name>	The Windows service name for the client.
<version number>	The version number of the client.
<OS Name>	The operating system for which the client was built: Windows 2K/XP
<logon type>:	Novell, Windows
<user id>	User id for user logging on to endpoint.
<error number>	An internal error number.
<error text>	If the <error number> has a text equivalent.
<Authentication Method name>	EAP-PEAP, EAP-TTLS, EAP-TLS, EAP-LEAP, EAP-MD5, EAP-GTC, EAP-FAST, EAPSIM, EAP-MSCHAPv2, MSCHAPv2, MSCHAP, CHAP, PAP.
<tunnel depth>	A number indicating authentication tunnel depth starting at 0 for outer most and 1 for the inner nested method.
<sequence number>	A number indicating where in a chain of authentications this authentication is beginning.
<port state>	The adapter authentication AC_PORT_STATE values: _STOPPED, _CONNECTING, _AUTHENTICATING, _AUTHENTICATED, _REAUTHENTICATING, _UNAUTHENTICATED, _AUTH_NOT_REQD.

Table 10-3 Message <value> Variables and Descriptions (continued)

Variables in log messages	Description
<port status>	More detailed information on the success/failure of the authentication (and other associated state changes). It often acts as a sub-status of a particular AC_PORT_STATE. See "Port Status Values" section on page 10-12 for the description of these values.
<AID-info>	The AID (Authority/Server Identifier) in the PAC.
<Authentication Server Identifier>	The fully qualified domain name for the server or the PAC info field truncated to 16 characters.
<EAP Notification>	Unsolicited messages from the authentication server.
<IP Address>	IP address that the end station will use in the standard IP format xxx.xxx.xxx.xxx.
<rule name>	Trusted server rule name.
<certificate-based trusted server rule>	Defines the trusted server rule.
<License string>	The license string read from the license file.
<trial period>	The number of days in trial period.
<termination date>	Date in format yyyy-mm-dd that the license expired.
<licensed os>	The name of the operating systems that the license allows.
<licensed product id>	The product id that the license allows.
<licensed OEM id>	The OEM id that the license allows.

Port Status Values

Some messages describe a port's state and a port status, for example, "Port State Machine transition to <Port State>(<Port status>)." This section describes the possible port status values.

Status codes related to running state

AC_PORT_STATUS_UNKNOWN

AC_PORT_STATUS_STOPPED

AC_PORT_STATUS_STARTED

Status codes related to link state

AC_PORT_STATUS_LINK_DOWN

AC_PORT_STATUS_LINK_UP

AC_PORT_STATUS_LINK_RESET

Status codes related to 802.1x state machine

AC_PORT_STATUS_8021x_START

AC_PORT_STATUS_8021x_FAILED

AC_PORT_STATUS_8021x_ACQUIRED

AC_PORT_STATUS_8021x_LOGOFF

AC_PORT_STATUS_8021x_TIMEOUT

Error and status codes during 802.1x authentication

AC_PORT_STATUS_ERR_CLIENT_EAP_METHOD_REJECTED

AC_PORT_STATUS_ERR_CLIENT_GENERIC_REJECTED

AC_PORT_STATUS_ERR_CLIENT_IDENTITY_REJECTED

AC_PORT_STATUS_ERR_CLIENT_TLS_CERTIFICATE_REJECTED

AC_PORT_STATUS_ERR_CHALLENGE_TO_AP_FAILED

AC_PORT_STATUS_ERR_ROGUE_AUTH_TIMEOUT

AC_PORT_STATUS_ERR_SERVER_TLS_CERTIFICATE_REJECTED

AC_PORT_STATUS_ERR_UNKNOWN

AC_PORT_STATUS_ERR_RESTRICTED_LOGON_HOURS

AC_PORT_STATUS_ERR_ACCT_DISABLED

AC_PORT_STATUS_ERR_NO_DIALIN_PERMISSION

AC_PORT_STATUS_ERR_CHANGING_PASSWORD

AC_PORT_STATUS_ERR_INVALID_TLV

AC_PORT_STATUS_ERR_UNKNOWN_TLV

AC_PORT_STATUS_ERR_TLV_NAK_RECEIVED

AC_PORT_STATUS_ERR_INVALID_CMAC

AC_PORT_STATUS_ERR_NO_CRYPTO_BINDING

AC_PORT_STATUS_EAP_FAST_PROVISIONING

AC_PORT_STATUS_ERR_EAP_FAST_INVALID_PAC_OPAQUE

AC_PORT_STATUS_ERR_EAP_FAST_INVALID_PAC_KEY

Status codes related to EAP

AC_PORT_STATUS_EAP_FAILURE

AC_PORT_STATUS_EAP_SUCCESS

AC_PORT_STATUS_WRN_CLEARTEXT_EAP_FAILURE

AC_PORT_STATUS_WRN_CLEARTEXT_EAP_SUCCESS

Status codes related to credentials

AC_PORT_STATUS_ERR_WRONG_PIN

AC_PORT_STATUS_ERR_PIN_REQUIRED

AC_PORT_STATUS_ERR_NO_DEVICE

AC_PORT_STATUS_ERR_NO_CARD

AC_PORT_STATUS_ERR_SIM_FAILURE

Status codes related to CCX

AC_PORT_STATUS_POSSIBLE_ROGUE_AP_START

AC_PORT_STATUS_POSSIBLE_ROGUE_AP_STOP

AC_PORT_STATUS_CCX_CCKM_ROAM

System Report

The System Report utility provides end users a simple way to automatically gather data needed by support personnel to troubleshoot any problems. It captures the following information:

- Current end-user technical log contents.
- Current internal application activity log.
- Information on the machine's hardware and software environment.

The System Report utility is packaged with the CTA 802.1x Wired Client and automatically installed with the CTA 802.1x Wired Client, however, it is a separate utility and it operates whether the CTA 802.1x Wired Client is active or not.

The System Report utility creates a single compressed file, the System Report, that contains information about the end station's hardware and software environment, the CTA 802.1x Wired Client, as well as the gathered technical and developer logs. The compressed file has these features:

- A consolidated and compressed collection of files
- Uses a non-configurable file name: CiscoLiteSysRepLog<YYYYMMDD_hhmm>.zip, where YYYY is the year, MM is the month, DD is the day, hh is the hour and mm are the minutes. Hours are stated in 24-hour time.
- The System Report is saved to the Microsoft Windows Desktop. This location is not configurable.

The System Report utility also creates a companion “System Report log” text file which allows one to view the end station environment information that was collected. This file is part of the System Report. It will be overwritten each time the utility is run with the same date.

Note In the event of a failure during the creation of the System Report zip file, this file reports the failure.

The System Report log text file has these features:

- Uses a non-configurable file name: CiscoLiteSysRepLog<YYYYMMDD>.txt, where YYYY is the year, MM is the month, and DD is the day.
- The System Report log text file is saved to the Microsoft Windows Desktop. This location is not configurable.
- The System Report tool is accessible by navigating through the Windows start menu: Start > Programs > Cisco Systems, Inc. Cisco Trust Agent 802.1x Wired Client > Cisco Trust Agent 802.1x Wired Client System Report.

Creating a System Report

Once you create a System Report, it can be shared with customer support to troubleshoot problems that arise.

Step 1 Run the System Report utility by navigating from the Windows Start menu > Programs > Cisco Systems, Inc. Cisco Trust Agent 802.1x Wired Client > Cisco Trust Agent 802.1x Wired Client System Report.

Step 2 Check the **Protect sensitive data with following password** to encrypt some of the collected files, such as, your configuration files and license files during the zip consolidation and compression process.

Step 3 Enter your password in the text box

Note You will need to provide this password to the recipient of the System Report file.

Tip Not all “unzip” utilities support a null password (empty password textbox) - it's recommended that you supply one.

Step 4 Click the **Collect Data** button to initiate the information gathering - this will take approximately 1/2 a minute or so.

Step 5 Once the report is saved, the user will see the statement, “Report generation done ... Log file has been archived” and the following buttons are enabled:

- **Copy To Clipboard** - copies the contents of companion System Report Log file to the Windows clipboard.
- **Locate Report File** - opens Windows Explorer at the desktop