



APPENDIX **B**

Cisco Secure Client Services Release 5.0 Log Messages

This appendix lists the log messages produced by Cisco Secure Client Services Release 5.0.

- **Starting Cisco_SSCservice.exe: *version number***—indicates the SSC service is starting.

Cisco Trust Agent successfully loaded

Failed to load Cisco Trust Agent

Password sent

Certificate sent

Manual user *logon type* logon processing initiated by user *user id*

Normal Shutdown —indicates a normal shutdown.

Fatal Shutdown —indicates a fatal shutdown.

—indicates the client is beginning its boot time processing.

—indicates the client detected a user logon.

SSO credentials (Microsoft)—indicates when the client collects credentials from the Microsoft GINA (whether they are used or not during a network authentication)

—indicates the client detects a user logoff

Adapter Id

Adapter Id

refers to the adapter's globally unique identifier (GUID).

error code

error code

{WPA | WPA2} unsupported.

adapter does or does not support WPA or WPA2.

Wireless Zero Config deactivated

— indicates when control was taken of an adapter that

Wireless Zero Config was detected and automatically deactivated for that adapter.

—indicates control was released for a particular adapter.

- *WiFi Association /Encryption Mode*
 requested on a WiFi adapter an association must occur. This log message indicates the SSC client is attempting to associate to an ssid. *WiFi Association/Encryption mode* could be one of these values:
 - Open
 - Shared 40 bit key
 - Shared 128 bit key
 - Static WEP 40 bit key
 - Static WEP 128 bit key
 - Dynamic WEP 40 bit key
 - Dynamic WEP 128 bit key
 - WPA-Personal TKIP encryption
 - WPA-Personal AES encryption
 - WPA-Enterprise TKIP encryption
 - WPA-Enterprise AES encryption
 - WPA2-Personal TKIP encryption
 - WPA2-Personal AES encryption
 - WPA2-Enterprise TKIP encryption
 - WPA2-Enterprise AES encryption

Starting wired connection, skipping association

Connection Association Success (link up)

Connection Association Failed. (Failure:

Connection Authentication Started

Identity requested – when an identity request comes in from the AP.

Identity sent - whenever an identity is sent.

EAP suggested by server: *Authentication Method name*
Authentication Method name

EAP-TTLS
 EAP-TLS
 EAP-LEAP
 EAP-MD5
 EAP-GTC
 EAP-FAST
 EAP-MSCHAPv2
 MSCHAPv2
 MSCHAP

- CHAP
- PAP

)—indicates an EAP authentication method was requested by the client.
is one of these values:

EAP-PEAP
EAP-TTLS
EAP-TLS
EAP-LEAP
EAP-MD5
EAP-GTC
EAP-FAST
EAP-MSCHAPv2
MSCHAPv2
MSCHAP
CHAP
PAP

Port State *Port status*

Port State

AC_PORT_STATE_STOPPED – indicates port is stopped
AC_PORT_STATE_CONNECTING – when it is waiting to start authentication
AC_PORT_STATE_AUTHENTICATING – is actively performing the initial 802.1x authentication
AC_PORT_STATE_AUTHENTICATED – successfully completed authentication
AC_PORT_STATE_REAUTHENTICATING – is actively performing 802.1x reauthentication
AC_PORT_STATE_UNAUTHENTICATED – when port wants to authenticate, but can't because of other conditions such as link is down or incorrect credentials
AC_PORT_STATE_AUTH_NOT_REQUIRED – when 802.1x authentication is not required. This state only exists for wired adapters or wireless adapters in WEP mode.

depends on the Port State value. This indicates a sub-state of the port state.

—indicates FAST unauthenticated

provisioning is supported by the adapter.

FAST: phase 1 tunnel for unauthenticated provisioning

Allowing session resumption—indicates when the SSC client begins a TLS-based authentication (PEAP, TTLS, FAST or TLS) and attempts session resumption with a previous session id.

Authentication Success—indicates an authentication completed successfully.

Authentication Failed—indicates an authentication completed unsuccessfully.

IP Address Received:

DHCP: Sending DHCP request.
DHCP: Request failed
Wireless Zero Config reactivated for adapter
WiFi access device has invalid channel number: SSID channel
Adapter Id **Couldn't find pre-shared key in profile**
: EAP-TTLS method requested by client:
Starting wifi connection, trying ssid
Licensing: No license found
Licensing: License read: License string.
License string
License string trial period
License string ermination date
termination date
License string licensed product
id
License string licensed OEM id
License string maintenance date
maintenance date the d
License string
License string
License string
License string
error string
Validating the server: Authentication Server Id
Server certificate validated: Authentication Server Id
Authentication Session Id Server certificate invalid (unknown CA)
Server certificate invalid (name mismatch: CN/DC/Alt name from server cert
Outer method: invalid/unsupported inner authentication method: inner method
Invalid outer EAP method: method name
Outer method: No inner authentication methods configured
Disallowed element in configuration: wireless adapters unlicensed
Disallowed element in configuration: wired adapters unlicensed
Disallowed element in configuration: EAP method: method name
Disallowed element in configuration: Association mode: association mode
Symbolic name: GUID of adapter AC address of adapter MTU size
percentage encryption modes auth modes

The wildcard (*key length, should be %d or %d* **) in the pattern is unknown and will be removed**
Internal error **, contact software manufacturer**

