Cisco AnyConnect Secure Mobility Client VPN User Messages, Release 2.5

April 28, 2011

The following user messages appear on the AnyConnect client GUI. A description follows each message, along with recommended user and administrator responses if applicable. The recommended administrator responses apply to IT representatives with monitoring and configuration access to the secure gateway configured to provide VPN access.

Note Restarting the endpoint OS and AnyConnect might help to recover from some errors.

The messages in this document are in alphabetical order, except for the following one:

Message not present in this document

Description Message originated from the Cisco Adaptive Security Appliance 5500 series (ASA) in the role of the secure gateway. This error message can contain any error string.

The remaining messages originate from AnyConnect, unless the descriptions indicate otherwise.

A new PIN has been generated for you: *PIN*.

Description The server generated a new personal identification number (PIN) for use with the SDI authentication token.

Recommended User Response None.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

`A security threat has been detected in the received server certificate. A VPN connection will not be established.`

Description A security threat was detected in the received server certificate. The threat is likely the result of a null character prefix attack.

Recommended User Response Report the issue to your organization's technical support.

Recommended Administrator Response Provide instructions to obtain the certificate required for VPN access.

`A user other than the one who started the VPN connection has logged into the computer locally. The VPN connection has been disconnected. Close all sensitive networked applications.`

Description AnyConnect disconnected from the VPN because another user logged into the local console, the AnyConnect client profile Retain VPN on Logoff parameter is enabled, and the associated User Enforcement parameter is set to "Same user only." Thus, the client is configured to retain the VPN connection following the logoff of the local console user, and to disconnect from the VPN if a different user logs into the local console. The different user was not authenticated by the secure gateway for access to the private network, so the VPN connection has been disconnected to ensure the protection of the private network.

Recommended User Response Ask the unauthenticated user to log off, then try a new VPN connection.

`Account expired.`

Description Message originated from the Cisco ASA. The ASA rejected the VPN access request because your account is locked or expired.

Recommended User Response Report the issue to your organization's technical support.

`An internal error occurred while creating the DART bundle. Please try again later.`

Description Creation of the DART bundle failed due to an internal processing error.

Recommended User Response Restart the computer. Install the latest release of DART and run it to attempt the collection of another DART bundle. (See Using DART to Gather Troubleshooting Information.) If the problem persists, report the error to your organization's technical support.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC).

`An unknown error has occurred in the VPN client service while trying to reconnect.`

Description The VPN connection was terminated without a reconnect reason code because of a flaw in the client software.

Recommended User Response Try starting a new VPN connection. Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`An unknown error occurred while creating the DART bundle, possibly due to restricted file permissions. Please try again later.`

Description Creation of the DART bundle failed. Common causes may include a failure to write to, read from, or move a file, possibly due to restricted user access to it.

Recommended User Response Try recreating the DART bundle.

`An unknown reconnect error has occurred in the VPN client service.`

Description The client was attempting to establish a VPN connection, but the connection was terminated without a reason code because of a flaw in the client software. Typically, a reason code is generated, exposing a more detailed message.

Recommended User Response Restart the computer and device, then try starting a new VPN connection. If the error reoccurs, run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle if you cannot resolve the issue.

`An unknown termination error has occurred in the client service.`

Description The VPN connection or AnyConnect client service was terminated without a termination reason code, due to a flaw in the client software. Typically, a reason code is generated, exposing a more detailed message.

Recommended User Response Restart the computer and device, then try starting a new VPN connection. If the error reoccurs, run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle if you cannot resolve the issue.

Another user has logged into your computer locally, and only one local user is allowed. The VPN connection has been disconnected. Close all sensitive networked applications.

Description AnyConnect disconnected from the VPN because another user logged into the local console, the AnyConnect client profile Retain VPN on Logoff parameter is enabled, and the associated User Enforcement parameter is set to "Same user only." Thus, the client is configured to retain the VPN connection following the logoff of the local console user, and to disconnect from the VPN if a different user logs into the local console. The different user was not authenticated by the secure gateway for access to the private network, so the VPN connection has been disconnected to ensure the protection of the private network.

Recommended User Response Ask the unauthenticated user to log off, then try a new VPN connection.

Another user has logged into your computer, and only one user is allowed. The VPN connection has been disconnected. Close all sensitive networked applications.

Description AnyConnect disconnected from the VPN because another user logged into the local console, the AnyConnect client profile Retain VPN on Logoff parameter is enabled, and the associated User Enforcement parameter is set to "Same user only." Thus, the client is configured to retain the VPN connection following the logoff of the local console user, and to disconnect from the VPN if a different user logs into the local console. The different user was not authenticated by the secure gateway for access to the private network, so the VPN connection has been disconnected to ensure the protection of the private network.

Recommended User Response Ask the unauthenticated user to log off, then try a new VPN connection.

AnyConnect cannot confirm it is connected to your secure gateway. The local network may not be trustworthy. Please try another network.

Description AnyConnect cannot validate the secure gateway server certificate. The local network may not be trustworthy or the secure gateway certificate may not be trusted.

- A device between the endpoint and the secure gateway is attempting to intercept the VPN connection data (man-in-the-middle attack).
- The secure gateway was not properly provisioned with a valid server certificate. If strict mode is configured on the secure gateway, all remote access users experience the error.

Recommended User Response Try moving to a different network, then try a new VPN connection. If the problem persists, report the error to your organization's technical support.

Recommended Administrator Response Ensure the secure gateway is provisioned with a valid server certificate from a proper certificate authority (CA).

`AnyConnect is not enabled on the VPN server.`

Description Message originated from the Cisco ASA. Access to the secure gateway through AnyConnect is not allowed.

Recommended User Response Try connecting to another secure gateway.

Recommended Administrator Response Make sure that AnyConnect is enabled on the secure gateway and the user is authorized to use AnyConnect.

`AnyConnect profile settings mandate a single local user, but multiple local users are currently logged into your computer. A VPN connection will not be established.`

Description AnyConnect is configured to permit access only to the local console user whom the secure gateway authenticated. AnyConnect disconnected from the VPN to protect it from unauthorized use by another user who logged into the local console.

Recommended User Response Ask the remote users to log off, then retry the VPN connection.

`AnyConnect was not able to establish a connection to the specified secure gateway. Please try connecting again.`

Description A network connectivity problem caused a VPN connection attempt to fail after a successful authentication.

Recommended User Response Retry the VPN connection.

`Authentication failed.`

Description Message originated from the Cisco ASA. The VPN connection could not be established, most likely because of invalid credentials.

Recommended User Response Confirm your credentials and retry the VPN connection.

`Automatic profile updates are disabled and the local VPN profile does not match the secure gateway VPN profile.`

Description The secure gateway is configured to upload an AnyConnect XML profile. AnyConnect is configured to skip profile updates, but cannot update to this version of the profile. Because the profile can specify a security policy, AnyConnect cannot establish a connection. The most common cause of this condition is connecting to a secure gateway with a version of AnyConnect, such as the Palm Pre, that does not support profile updates, or connecting with the BypassDownloader setting configured in the local policy file.

Recommended Administrator Response Configure a group policy that does not require an AnyConnect profile.

`Cannot verify required local security policy. This device is not supported. Please contact your network administrator.`

Description The AnyConnect profile requires the endpoint to be protected by a mobile device policy, but the endpoint OS could not be identified.

Recommended Administrator Response To ensure maximum device compatibility, ensure that the endpoint is running the latest version of the AnyConnect client, and the ASA is running the latest software release.

`Certificate Enrollment - Certificate import has failed.`

Description AnyConnect failed to import the just-enrolled certificate. This failure can occur if the user declined a certificate store provider prompt, such as one for a password or a permission request.

`Certificate Validation Failure`

Description Message originated from the Cisco ASA. The ASA declined to accept the certificate provided by AnyConnect because it could not be validated. Please verify that the correct certificate is available in the certificate store.

Recommended User Response Report the error to your organization's technical support and ask for the proper certificate.

Recommended Administrator Response Provide instructions to obtain the certificate required for VPN access.

`Certificate enrollment succeeded. Your session will be disconnected. Please login again.`

Description Certificate enrollment through SCEP succeeded.

Recommended User Response To use the new certificate, start a new VPN connection.

`Clientless (browser) SSL VPN access is not allowed.`

Description Message originated from the Cisco ASA. The ASA requires the user of a full tunnel client such as AnyConnect for network access.

Recommended User Response Report the problem to your organization's technical support.

Recommended Administrator Response Refer to Configuring the Security Appliance to Deploy AnyConnect in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5*.

`Connect not available. Another AnyConnect application is running or the functionality was not requested by this application.`

Description AnyConnect is connected in a diminished mode. This can be the result of a specific request by a custom application or because of another AnyConnect client already running.

Recommended User Response Try restarting the computer or device, then try a new VPN connection.

`Connecting via a proxy is not supported with Always On.`

Description AnyConnect is configured for Always-on VPN, which does not support connecting through a proxy.

Recommended User Response Remove the local proxy and try a new VPN connection. To access the proxy settings on Windows, choose the **Control Panel > Internet Options > Connections** tab, and go to LAN Settings.

`Connection attempt failed. Please try again.`

Description An initialization error caused the VPN connection to fail.

Recommended User Response Try establishing a new VPN connection.

`Connection attempt has failed (error in response data).`

Description Communication with the secure gateway failed because it detected an error in the HTTP response body it received.

Recommended User Response Try starting a new VPN connection. Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`Connection attempt has failed (error in response header).`

Description Communication with the secure gateway failed because it detected an error in the HTTP response header it received.

Recommended User Response Try starting a new VPN connection. Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`Connection attempt has failed due to invalid host entry.`

Description A profile URL or user-entered address does not resolve to a valid secure gateway.

Recommended User Response Choose another gateway from the VPN list or request the URL from your organization's technical support.

`Connection attempt has failed due to network or PC issue.`

Description An unexpected error in the HTTP protocol was detected. This error is unlikely and indicates an error state on the endpoint, such as loss of either connectivity to the secure gateway or network connectivity in general.

Recommended User Response Ensure your computer or device has network access. Restart it if necessary. Then try a new VPN connection.

`Connection attempt has failed due to server communication errors. Please retry the connection.`

Description Thee connection attempt was terminated for one of a number of reasons. These can include too many redirects at the secure gateway, a host changed from one connection to the next, etc.

Recommended Administrator Response Look for additional errors in the log.

`Connection attempt has failed.`

Description The VPN connection could not be established.

Recommended User Response Look for additional error message that identifies the cause.

`Connection attempt has failed: Gateway/proxy received an invalid response from the host or was unable to contact the host. Verify the host is valid.`

Description The failed connection attempt was done through a proxy. Possible causes of this failure are that the proxy could not resolve the selected host, the selected host does not exist, or the host is unavailable and therefore the proxy did not get a response.

`Connection attempt has timed out. Please verify Internet connectivity.`

Description AnyConnect canceled the connection attempt because the wait for a response exceeded an internal time-out value.

Recommended User Response Try a new VPN connection.

`Connections to this secure gateway are not permitted.`

Description The VPN connection to the selected secure gateway is not allowed because the Always On feature is enabled, which restricts VPN connections to only secure gateways found in the profiles.

Recommended User Response Choose another gateway from the VPN list or request the URL from your organization's technical support.

`Cookies must be enabled to log in.`

Description Message originated from the Cisco ASA. In order to log into the secure gateway, cookies must be enabled. The secure gateway detects that it is unable to correctly set a cookie.

Recommended User Response Add the domain to the browser list of trusted sites.

`Could not connect to server. Please verify Internet connectivity and server address.`

Description AnyConnect could not contact the secure gateway. This error indicates a failure to establish a network connection. Possible causes of this failure include:

- Lack of network connectivity to the secure gateway.
- Connection to the wrong server host name or IP address
- Problems with the secure gateway.

Recommended User Response Verify network connectivity. Check whether other applications, such as a web browser or a ping tool, can contact the secure gateway.

Recommended Administrator Response Check whether other applications, such as a web browser or a ping tool, can contact the secure gateway.

`Error retrieving username from CSD data.`

Description The username from the certificate feature is configured to use the Cisco Secure Desktop Host Scan data when a certificate is unavailable. The secure gateway failed to get the username from the host scan data in the absence of a certificate.

Recommended User Response Try starting a new VPN connection. Report the error to your organization's technical support.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC).

`Error saving preferences. Please retry, or restart AnyConnect.`

Description An unexpected error occurred while saving the user or global preferences file.

Recommended User Response Restart AnyConnect.

Recommended Administrator Response Reattempting to store preferences might solve the issue.

```
Exiting. Bypassing start before logon.
```

Description The start before logon GUI is exiting because of one of the following reasons:

- AnyConnect disconnected from the VPN because it detected a trusted network.
- The user may be located at a coffee shop, airport or hotel, where an Internet service provider is restricting access to the Internet.

Recommended User Response None necessary if you are in the corporate network. Otherwise, start a web browser and satisfy the conditions of the local Internet service provider, then try to connect to the VPN.

```
FIPS compliant algorithms for encryption, hashing, and signing have not been
enabled on this system.
```

Description As part of the AnyConnect FIPS verification process, the Windows operating system FIPS registry key is checked to ensure that the system is in a FIPS compliant mode. The registry key value is not set to enable FIPS.

```
FIPS mode requires TLS to be enabled to establish a VPN connection
```

Description FIPS mode requires that the TLS protocol be enabled. AnyConnect failed to enable the TLS protocol through the registry key setting.

Recommended User Response Choose the **Control Panel > Internet Options > Advanced** tab, and check **Use TLS 1.0** under "Security."

```
Failed accessing AnyConnect package. This may be due to IE security settings that
are set too high.
```

Description An error occurred while trying to download contents from the AnyConnect package located on the secure gateway. An Internet Explorer security setting could be blocking HTTP file downloads.

Recommended User Response Change the Internet Explorer security settings to permit downloads.

```
Failed to load preferences.
```

Description An unexpected error occurred while reading the profiles or preferences files. The files might be corrupt or an initialization failure may have occurred.

Recommended User Response Restart AnyConnect and try a new VPN connection.

`Failed to verify FIPS mode.`

Description An unexpected error occurred during the AnyConnect FIPS verification process. The most likely cause is an AnyConnect flaw.

Recommended User Response Try starting a new VPN connection. If the problem reoccurs, run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`Failed to verify required local security policy. Please contact your network administrator.`

Description The following table shows the explanations of this message and the recommended actions.

Explanation	Recommended Administrator Response
A generic error occurred when attempting to verify the mobile device security policy specified by the AnyConnect profile. This error occurs when AnyConnect attempts to monitor the Windows Mobile device registry to ensure it conforms with settings in the AnyConnect profile.	NA
The AnyConnect profile requires the mobile device to be protected by a device lock such as a personal identification number (PIN), but the device does not conform to the specified policy.	Make sure the value of the DeviceLockRequired element under MobilePolicy in the AnyConnect profile is correct.
The AnyConnect profile requires the mobile device to be protected by a device lock with a minimum password length, but the device is either not configured with a password, or has a password that is too short.	Make sure the value of the MinimumPasswordLength attribute of the DeviceLockRequired element under MobilePolicy in the AnyConnect profile is correct.
The AnyConnect profile requires the mobile device to be protected by a device lock with a minimum device lock time-out, and the device is configured with a time-out that is too short.	Make sure the value of the MaximumTimeoutMinutes attribute of the DeviceLockRequired element under MobilePolicy in the AnyConnect profile is correct.
The policy for the device lock password is usually set only after the device synchronizes with an enterprise exchange server. One of the following is true: • The AnyConnect profile fails to specify the complexity required of the device lock password. • The password does not meet the password strength required by the AnyConnect profile.	Make sure the value of the PasswordComplexity attribute of the DeviceLockRequired element under MobilePolicy in the AnyConnect profile is correct.
AnyConnect detected that the device is not synchronized with an Exchange server configured with a security policy. The AnyConnect profile requires the mobile device to be protected by a mobile device policy set when the device synchronizes with an enterprise exchange server.	Make sure the MobilePolicy settings in the AnyConnect profile are correct.

Recommended User Response Report the issue to your organization's technical support.

Recommended Administrator Response See the previous table.

`Firefox certificate libraries could not be loaded. VPN connection cannot be established.`

Description AnyConnect could not access the Firefox certificate store and there was no alternative store located. A failure to verify server certificates results in the inability to verify the identity of the secure gateway. Also, AnyConnect cannot respond to certificate requests.

`Hostscan Configuration error.`

Description The Host Scan module could not be configured properly. Possible causes include errors loading the DLL or errors setting up the command line parameters to launch the stub executable for Host Scan.

`Hostscan Initialize error.`

Description Host Scan could not launch. Possible causes include the Host Scan executable stub as well as the Host Scan initialization routines.

Recommended User Response Report the issue to your organization's technical support.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC).

`Hostscan Installation error.`

Description Host Scan could not be loaded to perform the system scan. Possible errors occurred when loading the DLL and errors finding the stub executable for Host Scan.

Recommended User Response Report the issue to your organization's technical support.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC).

`Hostscan Prelogin error.`

Description During the pre-login check, Host Scan detected the local violation of a rule configured on the secure gateway. Examples of pre-login checks include:

- Host Scan detected a keylogger.
- A dynamic access policy matched an endpoint criterion disqualifies AnyConnect for VPN access.

Recommended User Response Restart the computer or device and try a new VPN connection.

`Hostscan Run error.`

Description Host Scan experienced an error while scanning the endpoint.

Recommended User Response Try a new VPN connection.

`Invalid authentication handle.`

Description Message originated from the Cisco ASA. The authentication ticket was removed before the user responded.

Recommended User Action Try logging on again.

`Invalid host entry. Please re-enter.`

Description The URL requested was not found.

Recommended User Action Verify that the URL is correct and try again.

Recommended User Action Verify the URL in the secure gateway configuration.

`Invalid session/bad session parameters while processing Config Request`

Description Message originated from the Cisco ASA. The session cookie is invalid and cannot be used to request parameters needed to establish a VPN tunnel.

Recommended User Action Try a new VPN connection.

`It may be necessary to connect via a proxy, which is not supported with Always On.`

Description AnyConnect is configured for Always-on VPN, which does not support connecting through a proxy.

Recommended User Response Remove the local proxy and try a new VPN connection. To access the proxy settings on Windows, choose the **Control Panel > Internet Options > Connections** tab, and go to LAN Settings.

`Leave both boxes blank to continue using current password`

Description Message originated from the Cisco ASA. The user password will expire soon. The user has the opportunity to change the password immediately.

Recommended User Action Enter a new password into the text boxes or leave them blank if you want to defer the password change for later.

`Login denied, unauthorized connection mechanism, contact your administrator.`

Description The secure gateway is not permitting AnyConnect or clientless access by the user.

Recommended User Response Report the issue to your organization's technical support.

`Login denied. `*`Message`*

Description Message originated from the Cisco ASA. The secure gateway enforced a dynamic access policy that rejects the login credentials.

Recommended User Response Report the issue to your organization's technical support.

`Login error.`

Description Message originated from the Cisco ASA. The secure gateway detected an error during login.

Recommended User Response Try a new VPN connection.

`Login failed.`

Description Message originated from the Cisco ASA. The VPN connection could not be established. The most likely cause of this error is invalid credentials.

Recommended User Response Verify your login credentials and try a new VPN connection.

`Login failed: `*`Message`*

Description Message originated from the Cisco ASA. The VPN connection could not be established. The message following “Login failed:” indicates the reason.

Recommended User Response Try using the reason in the message to resolve the issue and try a new VPN connection.

`Network access is restricted due to an administrator configured timer expiration. The connection must be retried manually.`

Description AnyConnect is configured with a connect failure policy of “closed” and a captive portal remediation time-out setting expired. You may be located at a coffee shop, airport or hotel, where an Internet service provider is restricting access to the Internet. AnyConnect grants full network access for a limited period specified by the remediation time-out so you can attempt to satisfy the Internet service provider requirements. To protect the endpoint, AnyConnect restricts access after the timer expires.

Recommended User Response Start a web browser and satisfy the conditions of the service provider. The remediation timer restarts. Retry the connection.

`New PIN way too big.`

Description Message originated from the Cisco ASA. The length of the personal identification number (PIN) entered exceeds the maximum length allowed.

Recommended User Response Consult your corporate guidelines to change your PIN or report the issue to your organization's technical support.

`New Password Required but user not allowed to change`

Description Message originated from the Cisco ASA. A password change is required to log in. An expired password is most likely the cause. The user does not have permission to change his/her own password.

Recommended User Response Report the issue to your organization's technical support.

`New password way too big.`

Description Message originated from the Cisco ASA. The length of the password entered exceeds the maximum length allowed.

Recommended User Response Consult your corporate guidelines to change your password.

`No certificate store has been found. VPN connection cannot be established.`

Description AnyConnect could not access the certificate store, resulting in the inability to verify the identity of the secure gateway by performing verification of server certificates. Also, AnyConnect cannot respond to certificate requests.

Recommended User Response Make sure Firefox is installed or the file store is provisioned with certificates.

Recommended Administrator Response Make sure the Local Policy file does not exclude all potential certificate stores. Ensure the user has Firefox installed or the file store is provisioned with certificates.

`No valid certificates available for authentication.`

Description The secure gateway did not accept any of the certificates AnyConnect provided. No more certificates remain.

`Password change required.`

Description Message originated from the Cisco ASA. A password change is required to log in. An expired password is most likely the cause.

Recommended User Response Report the issue to your organization's technical support and request an account for VPN access.

`Please establish an Internet connection. If a browser or other application opened a connections dialog window, please respond so that AnyConnect can proceed.`

Description If Internet Explorer is configured to always dial, or dial if no other connection is present, when the browser is launched the user is prompted to select a connection. If the user does not connect, or cancels the dialog and opens AnyConnect, the connection becomes unresponsive while AnyConnect contacts the secure gateway.

Recommended User Response Dismiss the connection dialog box. AnyConnect displays a new dialog box and proceeds with the connection.

`Posture Assessment: Failed`

Description A Host Scan error occurred. Common causes include failures to download or launch the Host Scan components, and the system scan exceeded 10 minutes to complete.

Recommended User Response Try a new VPN connection.

`Posture assessment with authenticating proxy is not implemented.`

Description Host Scan could not perform posture assessment of the endpoint because AnyConnect is configured to use an authenticating proxy. Host Scan does not have access to the credentials for the authenticating proxy.

Recommended User Response Try to bypass or disable the proxy, then try a new VPN connection.

Recommended User Response Disable authentication completely, or selectively when accessing the ASA.

`Server reboot pending, new logins disabled. Try again later.`

Description The secure gateway is being restarted.

`Session terminated.`

Description Message originated from the Cisco ASA. The authentication ticket was removed before the user responded.

Recommended User Response Try logging on again.

`System configuration settings could not be applied. A VPN connection will not be established.`

Description AnyConnect attempted to apply system configuration settings received from the secure gateway. The error occurred in the System Network Abstraction Kit (SNAK) layer, which could indicate an error with vendor-supplied plug-ins external to AnyConnect.

Recommended User Response Restart the computer or device, then try starting a new VPN connection. If the problem persists, run DART (See Using DART to Gather Troubleshooting Information) and report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response If the problem persists, open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The AnyConnect package on the secure gateway could not be located. You may be experiencing network connectivity issues. Please try connecting again.`

Description The AnyConnect package file could not be located on the secure gateway.

Recommended User Response Make sure you have network connectivity, then try a new VPN connection.

Recommended Administrator Response Make sure an AnyConnect package file for the user’s operating system is present on the ASA configuration.

```
The AnyConnect protection settings must be lowered for you to log on with the
service provider. Your current enterprise security policy does not allow this.
```

Description You may be located at a coffee shop, airport or hotel, where an Internet service provider is restricting access to the Internet. Corporate policies do not permit VPN access in this setting.

Recommended User Response Retry after relocating.

Recommended Administrator Action Change the AnyConnect client profile Always-on VPN ConnectFailurePolicy setting if you want to permit captive portal access.

```
The Connect Failure Policy will not be applied because the Secure Gateway could
not be found in the profile.
```

Description AnyConnect could not apply the Always-on VPN connect failure policy specified by the ConnectFailurePolicy profile setting, despite the connection failure. The target secure gateway is not present in the profile. AnyConnect permits connections only to the hosts specified in the profile because the Always-on VPN policy restricts traffic to other destinations.

```
The FIPS verification of the OpenSSL libraries have failed. Reinstalling
AnyConnect might fix this issue.
```

Description AnyConnect failed to configure OpenSSL into FIPS mode. The OpenSSL shared libraries installed with AnyConnect could have been tampered with or might be corrupt.

Recommended User Response Reinstall AnyConnect and try a new VPN connection.

```
The MTU of the physical adapter is too small. An MTU of at least 1374 bytes is
required for an IPv6 connection. Please contact your network administrator.
```

Description The Maximum Transmission Unit (MTU) of the endpoint system physical network interface is too small to support IPv6 data through a VPN connection.

Recommended User Response Use the SetMTU utility that comes with the legacy Cisco VPN Client to set the MTU to 1374, the minimum MTU for IPv6 on the physical adapter, or set it to a greater value. You will likely need to consult with your organization's technical support to perform this task.

```
The VPN GUI and Agent Process are not both in FIPS Mode.
```

Description Both the VPN GUI and VPN Agent are not operating in FIPS mode when configured to do so.

Recommended User Response Restart the computer or device and AnyConnect to synchronize the operating modes of both processes.

`The VPN client agent SSL engine encountered an error. Please retry, or restart AnyConnect.`

Description AnyConnect encountered an unexpected and unrecoverable error in the SSL protocol stack. One possible cause is an AnyConnect flaw.

Recommended User Response Restart the computer or device, then try starting a new VPN connection. If the problem persists, run DART (See Using DART to Gather Troubleshooting Information) and report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response If the problem persists, open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent attempt to signal readiness to the plugin thread failed.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while initializing the main thread of the AnyConnect for Apple iOS VPN plug-in.

Recommended User Response Try restarting the device and starting a new VPN connection. Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent decryption engine encountered an error.`

Description AnyConnect service encountered an unexpected and unrecoverable error in the protocol decryption engine.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent encountered a secure gateway protocol failure.`

Description The AnyConnect service encountered an unexpected and unrecoverable protocol error in an exchange with the secure gateway.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent encryption engine encountered an error.`

Description The AnyConnect service encountered an unexpected and unrecoverable error in the protocol encryption engine.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent experienced a failure initializing a required timer.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while initializing a required internal timer object.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent experienced a failure initializing trusted network detection.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while initializing the trusted network detection subsystem.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent experienced an internal failure with the interprocess communication depot.`

Description The AnyConnect service experienced an unexpected and unrecoverable error with its inter-process communication subsystem.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent experienced an unexpected internal error. The VPN connection has been disconnected. Please restart your computer or device, then try again.`

Description The client has experienced an unexpected and unrecoverable error. The error is possibly due to one of the following:

- Unable to access an internal data structure that is expected to always be available.
- Unable to retrieve a profile setting for which a value, at the very least a default, should always be available.
- A Windows Terminal Services operation failed.

Recommended User Response Please restart your computer or device, then try a new VPN connection. If the problem persists, run DART (See Using DART to Gather Troubleshooting Information) and report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response If the problem persists, open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent failed in receiving a message from an IPC peer requesting the creation of a VPN connection.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while processing a request from another client process to initiate a VPN connection.

Recommended User Response Try restarting the VPN connection. Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent failed in receiving a message from an IPC peer requesting the launch of an application.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while processing a request from another client process to launch a client application.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent failed to create a necessary processing component and cannot continue.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while attempting to create its main execution thread.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent failed to create an event necessary for agent service notification processing.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while attempting to create a required internal event object for internal notification processing.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent failed to create an event necessary for agent termination processing.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while attempting to create a required internal event object for internal termination processing.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent failed to create an event necessary for network adapter change processing.`

Description AnyConnect experienced an unexpected and unrecoverable error while attempting to create a required event object for local network adapter change notifications.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent failed to create an event necessary for system suspend processing.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while attempting to create a required internal event objects for local suspend processing.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent failed to launch the client user interface application.`

Description The VPN connection was started via a web browser, requiring the start of the AnyConnect UI, but it failed to start.

Recommended User Response Restart the computer or device and try again. If the problem reoccurs, report the error to your organization's technical support.

Recommended Administrator Response Try using the same OS to initiate a WebLaunch of AnyConnect. If it fails, open a case with the Cisco Technical Assistance Center (TAC).

`The VPN client agent failed to load the SNAK system plugin required by this version of AnyConnect.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while attempting to initialize its System/Network Abstraction Kit (SNAK) subsystem.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent was unable create the plugin loader.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while attempting to create its plug-in loader subsystem.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent was unable to create a necessary timer.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while attempting to create a required internal timer object.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent was unable to create the client VPN configuration manager.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while attempting to create its VPN connection configuration management subsystem.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent was unable to create the client host configuration manager.`

Description AnyConnect experienced an unexpected and unrecoverable error while attempting to create its local configuration management subsystem.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent was unable to create the client preferences manager.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while attempting to create its preferences management subsystem.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent was unable to create the interprocess communication depot.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while attempting to create a required internal interprocess communication object.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent was unable to create the network environment component.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while attempting to create its network environment monitoring subsystem.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent was unable to create the trusted network detection component.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while attempting to create its trusted network detection subsystem.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent was unable to enable FIPS Mode.`

Description The AnyConnect service experienced an unexpected and unrecoverable error while attempting to initialize its Federal Information Processing Standards (FIPS) operation mode.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent was unable to initialize the system network socket support.`

Description AnyConnect experienced an unexpected and unrecoverable error while attempting to initialize its local network socket subsystem.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent was unable to send a failure response to an IPC peer requesting the creation of a VPN connection.`

Description The AnyConnect service received a request from another client process to initiate a VPN connection. The service encountered an unexpected and unrecoverable failure while attempting to send an error notification back to the requesting client process.

Recommended User Response Try restarting the VPN connection. Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent was unable to send a failure response to an IPC peer requesting the launch of an application.`

Description The AnyConnect service received a request from another client process to launch a client application. The service encountered an unexpected and unrecoverable failure while attempting to send an error notification back to the requesting client process.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent was unable to send a success response to an IPC peer requesting the creation of a VPN connection.`

Description The AnyConnect service received a request from another client process to initiate a VPN connection. The service encountered an unexpected and unrecoverable failure while attempting to send a success notification back to the requesting client process.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client agent was unable to send a success response to an IPC peer requesting the launch of an application.`

Description The AnyConnect service received a request from another client process to launch a client application. The service encountered an unexpected and unrecoverable failure while attempting to send a success notification back to the requesting client process.

Recommended User Response Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client driver has encountered an error. Please restart your computer or device, then try again.`

Description The AnyConnect service could not configure or start the virtual adapter driver needed to perform a VPN connection. A likely cause is a problem with the virtual adapter installation or registry settings.

Recommended User Response Restart your computer or device, then try a new VPN connection. If the problem persists, run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response See "Microsoft Windows Updates" in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5*.

`The VPN client driver has encountered an error. Close all sensitive networked applications. Please restart your computer or device, then try again.`

Description AnyConnect received a notification from its virtual adapter indicating it is terminating communication. The likely cause of the error is a virtual adapter driver failure.

Recommended User Response Restart your computer or device, then try a new VPN connection. If the problem persists, run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client failed to establish a connection.`

Description The AnyConnect service failed to establish a secured connection to the secure gateway. Possible causes include the following:

- Proxy authentication failure
- Protocol handshake failure
- Bad client or server certificate
- Layer 2 communication failures

Recommended User Response Retry the VPN connection. Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client service has been stopped. The VPN connection has been disconnected. Close all sensitive networked applications.`

Description AnyConnect disconnected from the VPN because it received a stop notification from the endpoint.

Recommended User Response Restart AnyConnect and retry the VPN connection. If the problem persists, run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response If the problem persists, open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client was unable to modify the IP forwarding table. A VPN connection will not be established. Please restart your computer or device, then try again.`

Description AnyConnect failed to apply all the VPN configuration settings to the endpoint IP forwarding table. A VPN connection is not permitted because this failure could compromise both its security and operation. This error is unrecoverable.

Recommended User Response Restart your computer or device, then try a new VPN connection. If the problem persists, run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client was unable to setup IP filtering. A VPN connection will not be established.`

Description AnyConnect failed to apply the VPN configuration settings to its IP filtering subsystem. A VPN connection is not permitted because this failure could compromise both its security and data integrity. This error is unrecoverable.

Recommended User Response Restart the computer or device. Restart the VPN connection. Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`The VPN client was unable to successfully verify the IP forwarding table modifications. A VPN connection will not be established.`

Description AnyConnect could not verify the successful application of all the VPN configuration settings to the local IP forwarding table. A VPN connection is not permitted because settings that are not applied could compromise both its security and operation. Other software running on the endpoint might also be actively altering the IP forwarding table, interfering with the AnyConnect configuration.

Recommended User Response Restart the computer or device. Exit all applications. Restart the VPN connection. If necessary, report the error to your organization's technical support.

`The VPN configuration received from the secure gateway has an invalid format. Please contact your network administrator.`

Description AnyConnect received a VPN connection configuration from the secure gateway containing an invalid format. The secure gateway could be malfunctioning.

Recommended User Response Report the error to your organization's technical support.

Recommended Administrator Response Make sure the AnyConnect profile is an .xml file.

`The VPN configuration received from the secure gateway is invalid. Please contact your network administrator.`

Description AnyConnect received a VPN connection configuration from the secure gateway containing invalid or conflicting information.

Recommended User Response Report the error to your organization's technical support.

Recommended Administrator Response Examine and correct the VPN configuration settings on the secure gateway. Try using the AnyConnect profile editor to open and validate the AnyConnect profile.

`The VPN connection could not be automatically re-established following a mobile device wakeup. A new connection is necessary, which requires re-authentication.`

Description Automatic VPN reconnection attempts failed after a local OS sleep-and-wake-up cycle.

Recommended User Response Verify the device network connectivity. Try a new VPN connection.

`The VPN connection could not be automatically re-established following a system resume from standby or hibernate. A new connection is necessary, which requires re-authentication.`

Description Automatic VPN reconnection attempts failed after a local OS suspend-and-resume cycle.

Recommended User Response Verify the computer or device network connectivity. Then try a new VPN connection.

`The VPN connection could not be re-established when attempting to resume from the paused connection state.`

Description Automatic VPN reconnection attempts failed after a local pause-and-continue cycle.

Recommended User Response Try a new VPN connection.

`The VPN connection has been disconnected due to the mobile device sleeping. The reconnect capability is disabled. A new connection is necessary, which requires re-authentication.`

Description In accordance with the AnyConnect configuration, AnyConnect disconnected because the endpoint went to sleep.

Recommended User Response Try a new VPN connection.

Recommended Administrator Response Because mobile devices sleep more frequently than portable computers, consider configuring a different profile and group for mobile devices with the DisconnectOnSuspend preference set to “Reconnect on resume” if mobile device end-users encounter this message frequently.

`The VPN connection has been disconnected due to the system suspending. The reconnect capability is disabled. A new connection is necessary, which requires re-authentication.`

Description In accordance with the AnyConnect configuration, AnyConnect disconnected because an endpoint system suspend occurred.

Recommended User Response Try a new VPN connection.

Recommended Administrator Response None. Change the AnyConnect client profile Auto Reconnect Behavior value to another value if you want to change the reconnect policy.

The VPN connection is not allowed via a local proxy. This can be changed through AnyConnect profile settings.

Description In accordance with the AnyConnect configuration, AnyConnect prevented the use of a local proxy to establish a VPN connection.

Recommended User Response Remove the local proxy and try a new VPN connection.

Recommended Administrator Response None. Check Allow Local Proxy Connections on the AnyConnect client profile if you want to permit the use of a local proxy.

The VPN connection to the secure gateway was disrupted and could not be automatically re-established. A new connection is necessary, which requires re-authentication.

Description Automatic VPN reconnection attempts failed. The VPN connection required an automatic reconnection because of a connection failure or disruption. Possible causes include a local network failure, internet device failure, or secure gateway failure.

Recommended User Response Verify network connectivity, then try a new VPN connection.

The VPN connection was re-established but the secure gateway assigned a new configuration that could not be successfully applied. A new connection is necessary, which requires re-authentication.

Description Automatic VPN reconnection attempts failed. A modified VPN connection configuration from the secure gateway requires another automatic reconnection.

Recommended User Response Verify network connectivity, then try a new VPN connection.

The VPN connection was started by a remote desktop user whose remote console has been disconnected. It is presumed the VPN routing configuration is responsible for the remote console disconnect. The VPN connection has been disconnected to allow the remote console to connect again. A remote desktop user must wait 90 seconds after VPN establishment before disconnecting the remote console to avoid this condition.

Description AnyConnect detected a remote console disconnect within 90 seconds of the establishment of a VPN session. AnyConnect terminated the session because it detected an interruption of the remote console session, indicating the necessity of restoring the local IP forwarding table to permit the re-establishment of the remote console session.

Recommended User Response Remote console users should wait more than 90 seconds following VPN connection establishment before disconnecting the remote console session to avoid this condition.

`The VPN connection was terminated by the secure gateway and could not be automatically re-established. A new connection is necessary, which requires re-authentication.`

Description Automatic VPN reconnection attempts failed. The VPN connection required an automatic reconnection because the secure gateway closed the connection.

Recommended User Response Remote console users should wait more than 90 seconds following VPN connection establishment before disconnecting the remote console session to avoid this condition.

`The VPN connection was terminated due to a Windows connection manager failure. A new connection is necessary, which requires re-authentication.`

Description Automatic VPN reconnection attempts failed because of a Windows connection manager failure. The VPN connection requires an automatic reconnection.

Recommended User Response Repair the network connection or restart the device. Verify network connectivity, then establish a new VPN connection.

`The VPN connection was terminated due to a different client IP address assignment by the secure gateway and could not be automatically re-established. A new connection is necessary, which requires re-authentication.`

Description Automatic VPN reconnection attempts failed. The VPN connection required an automatic reconnection because the secure gateway returned a different private network IP address in response to an IP address renewal request.

Recommended User Response Try to start a new VPN connection.

`The VPN connection was terminated due to a rekey failure and could not be automatically re-established. A new connection is necessary, which requires re-authentication.`

Description Automatic VPN reconnection attempts failed because of a failure to rekey the encryption protocol.

Recommended User Response Try to start a new VPN connection.

`The VPN connection was terminated due to a system routing table modification and could not be automatically re-established. A new connection is necessary, which requires re-authentication.`

Description The local host configuration management subsystem could not correct a change in the local IP forwarding table. Automatic VPN reconnection attempts failed.

Recommended User Response Try to start a new VPN connection.

`The VPN connection was terminated due to an IP address renewal failure and could not be automatically re-established. A new connection is necessary, which requires re-authentication.`

Description A failure to perform a DHCP renewal of the private network IP address used by AnyConnect requires a new VPN connection. Automatic VPN reconnection attempts failed.

Recommended User Response Try to start a new VPN connection.

`The VPN connection was terminated due to incorrect tunnel MTU and could not be automatically re-established. A new connection is necessary, which requires re-authentication.`

Description AnyConnect detected that the tunnel MTU is incorrect. The VPN connection was torn down, but a new connection to enforce the correct tunnel MTU could not be established.

Recommended User Response Try a new VPN connection. If the problem persists, report the error to your organization's technical support.

Recommended Administrator Response Change the secure gateway group-policy svc-mtu setting. To do so using ASDM, go to the MTU parameter on the Configuration > Group Policies > Add or Edit > Advanced > AnyConnect Client panel.

`The VPN connection was terminated due to the loss of the network interface used for the VPN connection.`

Description The endpoint network interface used for the VPN connection lost its network connectivity. The interface either disconnected or no longer has a usable IP address. As a result, the VPN connection attempt failed, or the VPN session or idle time-out expired, halting VPN reconnect attempts.

Recommended User Response Repair the network connection or restart the device. Verify network connectivity, then establish a new VPN connection.

`The VPN connection was terminated due to the loss of the network interface. A new connection is necessary, which requires re-authentication.`

Description The VPN connection lost its physical network interface, requiring a new VPN connection.

Recommended User Response Repair the network connection or restart the device. Verify network connectivity, then establish a new VPN connection.

`The Windows Routing and Remote Access service is not compatible with the VPN client. The VPN client cannot operate correctly when this service is running. You must disable this service in order to use the VPN client.`

Description The Windows Routing and Remote Access service lets Microsoft Windows Server 2000, 2003 and 2008 function as a router, and as such it actively monitors and modifies the system IP forwarding table. AnyConnect cannot coexist with a running Routing and Remote Access service because it interferes with the AnyConnect configuration of the endpoint IP forwarding table for VPN connections and, if configured, the security of Always-on VPN.

Recommended User Response Disable Routing and Remote Access. To do so, choose **Start > Administrative Tools > Routing and Remote Access**, right-click the server icon, choose **Disable Routing and Remote Access**, and click **Yes** in the confirmation dialog box. Then establish a VPN connection.

`The certificate on the secure gateway is invalid. A VPN connection will not be established.`

Description A rare problem was encountered with the server certificate.

Recommended User Response Report the error to your organization's technical support.

Recommended Administrator Response Check the validity of the secure gateway server certificate.

`The client agent has encountered an error.`

Description AnyConnect encountered an unexpected and unrecoverable initialization failure.

Recommended User Response Try restarting the computer or device, then start a new VPN connection. Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Report the problem to Cisco TAC and include the DART bundle.

`The client could not connect because of a secure gateway address resolution failure. Please verify Internet connectivity and server address.`

Description The client was unable to connect due to a DNS resolution error. Common causes can include a hostname that does not properly resolve to an IP address, incorrect DNS settings on the client, or unreachable or non-responsive DNS servers on the client.

Recommended User Response Report the error to your organization's technical support.

Recommended Administrator Response Work with the user to verify local access to a DNS server.

`The client service has encountered an error and is stopping. Close all sensitive networked applications.`

Description AnyConnect encountered an unexpected and unrecoverable failure while interfacing with the local control subsystem.

Recommended User Response Try restarting the computer or device, then start a new VPN connection. Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Report the problem to Cisco TAC and include the DART bundle.

`The configuration of the VPN Server has changed. Please try again.`

Description The secure gateway configuration changed after AnyConnect first contacted the secure gateway.

Recommended User Response Start a new VPN connection.

Recommended Administrator Response Try starting a new VPN connection from another location.

`The required license for this type of VPN client is not available on the secure gateway. Please contact your network administrator.`

Description AnyConnect attempted to establish a VPN session with a secure gateway that is not activated with an AnyConnect license.

Recommended User Response Report the error to your organization's technical support.

Recommended Administrator Response Obtain an AnyConnect Essentials or Premium license from your Cisco Sales Engineer and activate it on the ASA.

`The secure gateway failed to reply to a connection initiation message and may be malfunctioning. Please try connecting again. If this problem persists, please contact your network administrator.`

Description An extended timer expired while AnyConnect was establishing a VPN connection with the secure gateway. The secure gateway probably failed to respond to a protocol handshake request. A flaw in the secure gateway software could be the cause.

Recommended User Response Try starting a new VPN connection. Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Report the problem to Cisco TAC and include the DART bundle.

`The secure gateway has rejected the connection attempt. A new connection attempt to the same or another secure gateway is needed, which requires re-authentication.`

Description AnyConnect received an error response (that is, an HTTP error code) from the secure gateway during the negotiation for a VPN session. AnyConnect logged the error code and any error description text provided in the secure gateway error response.

Recommended User Response Try starting a new VPN connection. If the problem persists, run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Examine the log. If you cannot resolve the problem, report it to Cisco TAC and include the DART bundle.

`The secure gateway has terminated the VPN connection.`

Description The secure gateway terminated the VPN connection. In the case of SSL, the message displayed to the user from the secure gateway indicates the reason for the termination.

Recommended User Response Try starting a new VPN connection. If the problem persists, run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Examine the log. If you cannot resolve the problem, report it to Cisco TAC and include the DART bundle.

`The secure gateway is responding, but AnyConnect could not establish a VPN session. Please retry.`

Description The Always-on VPN connect failure policy specified via the ConnectFailurePolicy profile setting will not be applied, despite the connection failure. While the UI failed to connect, AnyConnect could not contact the target secure gateway. Thus, the connection failure could not be confirmed and any existing network restrictions are maintained.

Recommended User Response Try starting a new VPN connection.

`The server certificate received or its chain does not comply with FIPS. A VPN connection will not be established.`

Description In accordance with the AnyConnect configuration, AnyConnect disconnected from the VPN because the server certificate received from the secure gateway or the certificate in the server certificate chain is not compliant with Federal Information Processing Standards (FIPS).

Recommended User Response Report the error to your organization's technical support.

Recommended Administrator Response Verify the secure gateway server certificate uses both the FIPS-required minimum RSA public key length and a FIPS compliant signature algorithm.

`The service provider in your current location is restricting access to the Internet.`

Description The user may be located at a coffee shop, airport or hotel, where an Internet service provider is restricting access to the Internet. A VPN connection cannot be established.

Recommended User Response Look for a second message for actions to correct the situation. Open a web browser and satisfy the conditions of the service provider. Then retry the connection.

`The service provider in your current location is restricting access to the secure gateway.`

Description The user may be located at a coffee shop, airport or hotel, where an Internet service provider is restricting access to the Internet. A VPN connection cannot be established.

Recommended User Response Look for a second message for actions to correct the problem. Open a web browser and satisfy the conditions of the local Internet service provider. Then retry the connection.

`Unable to complete connection: Cisco Secure Desktop not installed on the client`

Description A login was attempted but no CSD data was sent for the connection. There may have been an error installing or running CSD.

Recommended User Response Report the error to your organization's technical support.

Recommended Administrator Response Install CSD or verify that it is installed.

`Unable to contact` *`SecureGateway`*`.`

Description The secure gateway could not be contacted because of a DNS resolution error or an unreachable or non-responsive secure gateway.

Recommended User Response Check for an additional error message for more detail about the cause.

`Unable to establish connection with newly imported Certificate.`

Description AnyConnect could not locate a certificate recently obtained via enrollment. Common causes include the following:

- Misconfiguration of the secure gateway, such as missing trust points.
- Invalid certificate date.

Recommended User Response Report the error to your organization's technical support.

Recommended Administrator Response Verify the secure gateway configuration and certificate date.

```
Unable to proceed.
Cannot contact the VPN service.
```

Description A user attempted to perform an action such as connect and AnyConnect is not able to communicate with the AnyConnect agent. An alert message informing the user of this condition precedes this one.

Recommended User Response Restart the computer or device, then start a new VPN connection. If the problem persists, run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Examine the log. If you cannot resolve the problem, report it to Cisco TAC and include the DART bundle.

```
Unable to process remote proxy request. Please try again.
```

Description An unexpected error occurred while processing the user response to proxy authentication.

Recommended User Response Remove the local proxy and try a new VPN connection.

```
Unable to re-register for IP forwarding table change notifications. The VPN
connection has been disconnected.
```

Description AnyConnect encountered an unrecoverable error when it attempted to re-register for local IP forwarding table change notifications. The VPN was disconnected because the error prevents AnyConnect from ensuring both its security and correct operation.

Recommended User Response Restart the computer or device, then start a new VPN connection. If the problem persists, run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Report the error to Cisco TAC and include the DART bundle.

```
Unable to retrieve logon information to verify compliance with AnyConnect logon
enforcement and VPN establishment profile settings. A VPN connection will not be
established.
```

Description AnyConnect cannot enforce the user logon limit settings configured in the client profile because it cannot retrieve the local user login information. To ensure the protection of the private network, the VPN connection is not permitted.

Recommended User Response Report the error to your organization's technical support.

Recommended Administrator Response Verify secure gateway access to the AAA server.

`Unable to send authentication message.`

Description There was an error communicating with the authentication server.

Recommended User Response Report the error to your organization's technical support.

Recommended Administrator Response Verify secure gateway access to the AAA server.

`Unable to send authorization message.`

Description There was an error communicating with the authorization server.

Recommended User Response Report the error to your organization's technical support.

Recommended Administrator Response Verify secure gateway access to the AAA server.

`Unable to update the session management database`

Description The secure gateway encountered an error when attempting to add the VPN connection to the session database.

Recommended User Response Try a new VPN connection. If the problem persists, report it to your organization's technical support.

Recommended Administrator Response Try a new VPN connection.

`Unable to verify the necessary registry keys for FIPS`

Description The AnyConnect client could not access the local registry keys needed to verify FIPS compliance.

Recommended User Response Report the problem to your organization's technical support.

Recommended Administrator Response Try a new VPN connection.

`Unknown challenge.`

Description The authentication server returned an unrecognized challenge code.

Recommended User Response Report the problem to your organization's technical support.

Recommended Administrator Response Verify secure gateway access to the AAA server.

`Unknown error.`

Description The secure gateway experienced an unknown error.

Recommended User Response Try restarting the VPN connection. Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`Unknown login status.`

Description The secure gateway did not perform one of the expected actions (accept, reject, or challenge the login, or return an error).

Recommended User Response Retry the VPN connection. Report the problem to your organization's technical support.

Recommended Administrator Response Verify secure gateway access to the AAA server.

`Unwilling to perform password change.`

Description Message originated from the Cisco ASA. A password change is required to log in. An expired password is the likely cause. The server cannot modify the password.

Recommended User Response Report the problem to your organization's technical support.

`VPN Server could not parse request.`

Description The secure gateway could not parse the request sent by the VPN client.

Recommended User Response Try restarting the VPN connection. Run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) and include the DART bundle.

`VPN Server internal error.`

Description The secure gateway encountered an internal error such as low memory.

Recommended User Response Try restarting the VPN connection. Report the error to your organization's technical support.

Recommended Administrator Response Open a case with the Cisco Technical Assistance Center (TAC) if you cannot resolve the memory issue.

`VPN Service not available.`

Description The AnyConnect agent is not communicating. Likely causes include one of the following:

- The AnyConnect agent did not start.
- AnyConnect is not installed.

Recommended User Response Ask your organization's technical support for instructions on how to reinstall AnyConnect, then start a new VPN connection. If the problem persists, run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Report the problem to Cisco TAC and include the DART bundle.

`VPN Service not available. Exiting.`

Description The AnyConnect agent is not communicating. Likely causes include one of the following:

- The AnyConnect agent did not start. Because AnyConnect is configured to run in Start Before Logon mode, it exited to keep from blocking the user.
- AnyConnect is not installed.

Recommended User Response Try a new VPN connection. If the problem persists, ask your organization's technical support for instructions on how to reinstall AnyConnect, then start a new VPN connection. If the problem continues to persist, run DART. (See Using DART to Gather Troubleshooting Information.) Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Report the problem to Cisco TAC and include the DART bundle.

`VPN connection terminated, Smartcard removed from reader.`

Description The smartcard used to authenticate the VPN connection was removed from the Smartcard reader. The VPN was disconnected to ensure the protection of the private network.

Recommended User Response Re-insert the smartcard and try a new VPN connection.

`VPN established. Continuing with login.`

Description The start before logon components established a VPN connection. The GUI exits to let the user log in to the OS.

Recommended User Response Log in.

`VPN establishment capability from a remote desktop is disabled. A VPN connection will not be established.`

Description AnyConnect is not configured to permit the establishment of a VPN connection from within a remote desktop session on the endpoint.

Recommended User Response Log in directly, then connect to the VPN.

Recommended Administrator Response Refer to "Allowing a Windows RDP Session to Launch a VPN Session" in the *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5* if you want to enable VPN access from an RDP session.

`Warning: The following Certificate received from the Server could not be verified:`

Description The certificate presented by the secure gateway could not be verified. Possible causes include:

- Certificates could not be verified to a trusted Root Certificate.
- Misconfigured certificate names.
- Invalid host names entered by user causing name check failure.
- Expired or revoked certificates.

Recommended User Response Report the error to your organization's technical support and include the DART bundle.

Recommended Administrator Response Validate or replace the certificate.

`When in the Secure Vault, use the "Launch Login Page" button on the desktop to relaunch the client.`

Description Cisco Secure Desktop was detected as running on the endpoint.

Recommended User Response Click **Launch Login Page** inside the Secure Desktop to launch the client inside the Secure Desktop to continue using the VPN connection.

`You have no dial-in permission.`

Description The user's account does not have permission to access the network remotely.

Recommended User Response Report the error to your organization's technical support.

`You need to log on with the service provider before you can establish a VPN session. You can try this by visiting any website with your browser.`

Description The user may be located at a coffee shop, airport, or hotel, where an internet service provider is restricting access to the Internet. A VPN connection cannot be established.

Recommended User Response Look for a second message for actions to correct the situation. Open a web browser to see if you can satisfy the conditions for Internet access. Then retry the VPN connection.

`Your VPN connection has exceeded the session time limit. A new connection is necessary, which requires re-authentication.`

Description The VPN session was terminated because it exceeded the time permitted by the secure gateway for a VPN session. This feature helps protect the private network by requiring the user to re-authenticate with the secure gateway.

Recommended User Response Start a new VPN session.

`Your account is disabled.`

Description The user's account is disabled and cannot be used to access the VPN.

Recommended User Response Report the error to your organization's technical support.

`Your certificate is invalid for the selected group`

Description The secure gateway validated the certificate provided by AnyConnect, however, the applied connection policy (tunnel group) does not permit the certificate. The certificate might be valid for another connection policy configured on the secure gateway.

Recommended User Response Report the error to your organization's technical support and ask for the proper certificate.

Recommended Administrator Response Provide instructions to obtain the certificate required for VPN access.

`Your client certificate will be used for authentication`

Description Certificate-only authentication is in use. Instead of providing a username and password as credentials, the user's certificate will be used for authentication.

Recommended User Response None.

`Your connection to the secure gateway has been suspended longer than the allotted time limit. A new connection is necessary, which requires re-authentication.`

Description The VPN session was terminated because it exceeded the VPN session idle timer limit configured on the secure gateway. This feature helps protect the private network by requiring the user to re-authenticate with the secure gateway.

Recommended User Response Start a new VPN session.

Recommended Administrator Response None.