Juniper Networks Secure Access

WSAM and Network Connect Error Messages

Release 6.5

Year 2000 Notice

Juniper Networks hardware and software products are Year 2000 compliant. The JUNOS software has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

Software License

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

End User License Agreement

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. The Parties. The parties to this Agreement are Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. The Software. In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller.

3. License Grant. Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use the Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller, unless the applicable Juniper documentation expressly permits installation on non-Juniper equipment.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. Use Prohibitions. Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use the Software on non-Juniper equipment where the Juniper documentation does not expressly permit installation on non-Juniper equipment; (j) use the Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; or (k) use the Software in any manner other than as expressly provided herein.

5. Audit. Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. Confidentiality. The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. Ownership. Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. Warranty, Limitation of Liability, Disclaimer of Warranty. The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. Termination. Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. Taxes. All license fees for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

11. Export. Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. Commercial Computer Software. The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. Interface Information. To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. Third Party Software. Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html.

15. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

Windows Secure Access Manager (WSAM) Error Messages

This section contains the following types of Windows Secure Application Manager error messages:

- "Windows Application Error Messages (sam.windows.app)" on page 1

- "Windows Setup Error Messages (sam.windows.setup)" on page 4

- "Windows UI Error Messages (sam.windows.ui)" on page 6

Windows Application Error Messages (sam.windows.app)

sam.windows.app.23798

System Log Message   The Windows Secure Application Manager is unable to resolve the secure gateway's host name and must close. You may have originally accessed the secure gateway using a Web proxy.

Cause   You may have originally accessed the secure gateway using a Web proxy or you may have an incorrect DNS server configured.

Action   Verify that the Web proxy is set correctly on your browser and is reachable and verify DNS connectivity and resolution.

sam.windows.app.23799

System Log Message   Although the Windows Secure Application Manager is not able to direct your web browser back to the secure gateway home page, you may continue to use the Windows Secure Application Manager normally.

Cause   You may have suffered a temporary loss of network connectivity or your browser contain a proxy configuration.

Action   Click the re-direct hyperlink on the Web "Launching application" page displayed in your browser. If you are not directed to the secure gateway home page, contact your system administrator to verify network connectivity.

sam.windows.app.23800

System Log Message   The Windows Secure Application Manager is already running on this computer. Click **OK** to end your previous session and start a new Windows Secure Application Manager session.

Cause   A Windows Secure Application Manager session is already active on this computer. You cannot operate more than one Windows Secure Application Manager at a time.

Action   Click **OK** to end your previous session and start a new Windows Secure Application Manager session.

sam.windows.app.23802

System Log Message Unable to terminate the previous Windows Secure Application Manager session.

Cause The previous Windows Secure Application Manager session could not be automatically terminated.

Action Terminate the existing Windows Secure Application Manager session manually before reconnecting to the secure gateway.

sam.windows.app.23803

System Log Message The Windows Secure Application Manager installation was successful. You need to reboot your computer to complete the installation process. Close all applications to avoid loss of data and click **OK** to reboot your computer.

Cause This is an informational message.

Action Close all applications to avoid loss of data and click **OK** to reboot your computer.

sam.windows.app.23804

System Log Message Windows Secure Application Manager file sharing has been configured on the secure gateway, which requires automatic driver configuration. You must reboot your computer to complete driver configuration. Close all applications to avoid loss of data and click **OK** to reboot your computer.

Cause When Windows Secure Application Manager file sharing is enabled on the secure gateway, the **neofltr.sys** driver is required between TCP/IP and NetBT. This automatic configuration requires you to reboot your computer.

Action Close all applications to avoid loss of data and click **OK** to reboot your computer.

sam.windows.app.23805 (Windows 98 operating system only)

System Log Message A Layered Service Provider (LSP) application changed the Winsock protocol catalog, altering the Windows Secure Application Manager application order. You need to reboot your computer to restore the original application order. Close all applications to avoid loss of data and click **OK** to reboot your computer.

Cause An application may have recently been installed on this client that overrides the Windows Secure Application Manager application order.

Action Reboot your computer to reset the Windows Secure Application Manager application order.

sam.windows.app.23822 (Windows 98 operating system only)

System Log Message The following Layered Service Provider (LSP) programs were installed on the client and may cause the Windows Secure Application Manager to function incorrectly: < *list of LSP programs* > Click **Continue** to launch the Windows Secure Application Manager.

Cause The Windows Secure Application Manager has detected that other applications have installed the specified Layered Service Provider program(s) on your system. These LSPs have not been confirmed to be incompatible with the Windows Secure Application Manager, but, conflicts between these LSP programs and the Windows Secure Application Manager may cause adverse effects.

Action Contact your system administrator for instructions on dealing with the LSP programs before launching the Windows Secure Application Manager.

sam.windows.app.23823 (Windows 98 operating system only)

System Log Message The following incompatible Layered Service Provider (LSP) programs were installed on the client and are causing the Windows Secure Application Manager to function incorrectly: *< list of LSP programs >*

Cause The Windows Secure Application Manager has detected that other applications have installed the specified Layered Service Provider program(s) on your system. The specified LSPs are known to be incompatible with the Windows Secure Application Manager, introducing instability to your system. These LSPs are often spyware applications that do not conform to any security standards.

Action The Windows Secure Application Manager will not install or run while these LSPs are present. Contact your system administrator for instructions on uninstalling the applications or otherwise dealing with the LSPs.

sam.windows.app.24068

System Log Message The system settings have been changed. You need to reboot your computer to use Windows Secure Application Manager. Close all applications to avoid loss of data and click OK to reboot your computer.

Cause Driver could not load because the Irp stack size and the McAfee driver is installed or the Kaspersky driver is installed.

Action Click OK to reboot your computer.

sam.windows.app.24069

System Log Message Windows Secure Application Manager was unable to reboot the system. Please close all applications and reboot the system from Start Menu before launching Windows Secure Application Manager again.

Cause Your computer did not automatically reboot.

Action Close all applications and reboot your computer.

sam.windows.app.24070

System Log Message The system settings have been changed for Windows Secure Application Manager to interoperate with other TDI drivers installed on this system. It's recommended you reboot your computer to reload the new driver configuration. Close all applications to avoid loss of data and click OK to reboot your computer.

Cause No blacklist driver is installed and the Irp stack size is not set correctly.

Action Close all applications and reboot your computer.

Windows Setup Error Messages (sam.windows.setup)

sam.windows.setup.23641

System Log Message You must have administrator privileges to install and run the Windows Secure Application Manager.

Cause The Windows Secure Application Manager performs tasks within the registry and the file system requiring administrator privileges unavailable to the current user.

Action Ensure that the current user on this computer has administrator privileges or the Juniper Networks Win32 Installer Service is loaded.

sam.windows.setup.23642

System Log Message Cannot launch the current version of the Windows Secure Application Manager because you are running a version that is older than on the secure gateway. You need to upgrade your version of the Windows Secure Application Manager, which requires you to reboot your computer. Close all applications to avoid loss of data and click **OK** to reboot your computer.

Cause You are running a version of the Windows Secure Application Manager that is older than the version on the secure gateway.

Action You need to upgrade your version of the Windows Secure Application Manager, which requires you to reboot your computer. Close all applications to avoid loss of data, reboot your computer, and sign in to the secure gateway again.

sam.windows.setup.23643

System Log Message You must add IP addresses for hosts or networks you want to secure via Windows Secure Application Manager to Internet Explorer's proxy exception list when you use a Web proxy server.

Cause The Windows Secure Application Manager needs to be able to trap HTTP(S) calls originating from Internet Explorer in order to process them.

Action You must add destination hosts to Internet Explorer's proxy exception list to enable access via the Windows Secure Application Manager.

sam.windows.setup.23644

System Log Message An error occurred during the Windows Secure Application Manager installation.

Cause The installation was preempted or there was an error during installation.

Action Forward relevant component logs to your system administrator. Then, try uninstalling and re-installing the Windows Secure Application Manager. (You may need to manually uninstall the Windows Secure Application Manager before you can re-install.)

sam.windows.setup.23645

System Log Message   Windows Secure Application Manager upgraded successfully. You need to reboot your computer to complete the upgrade process. Close all applications to avoid loss of data and click **OK** to reboot your computer.

Cause   This is an informational message.

Action   Close all applications to avoid loss of data and click **OK** to reboot your computer.

sam.windows.setup.23646

System Log Message   The Windows Secure Application Manager is not compatible with the operating system on your computer.

Cause   The operating system on your computer does not support installing or operating the Windows Secure Application Manager. The Windows Secure Application Manager is only supported on Windows 98, Windows 2000, Windows ME, and Windows XP.

Action   No action on your part is necessary.

sam.windows.setup.23647

System Log Message   Cannot launch the current version of the Windows Secure Application Manager because you are running a version that is incompatible with the secure gateway. You need to upgrade the Windows Secure Application Manager, which requires you to reboot your computer. Close all applications to avoid loss of data and click **OK** to reboot.

Cause   You are running a version of the Windows Secure Application Manager that is incompatible with the version on the secure gateway.

Action   You need to upgrade the Windows Secure Application Manager, which requires you to reboot your computer. Close all applications to avoid loss of data, reboot your computer, and sign in to the secure gateway again.

sam.windows.setup.23648

System Log Message   Uninstalling the Windows Secure Application Manager, which also requires you to reboot your computer, may cause some active applications to become unstable. Close all applications to avoid loss of data and then click **OK** to complete the Windows Secure Application Manager uninstallation and reboot your computer.

Cause   This is a warning message is designed to make you aware of a potential issue resulting from the Windows Secure Application Manager uninstallation process.

Action   Close all applications to avoid loss of data and click **OK** to reboot your computer.

sam.windows.setup.23649

System Log Message   This version of Windows Secure Application Manager already exists on your computer. No upgrade is required.

Cause   You are attempting to upgrade the Windows Secure Application Manager stand-alone installer, but the up-to-date version already exists on your computer.

Action   Use the existing stand-alone installer on your computer.

sam.windows.setup.23650

System Log Message   You must have administrator privileges to uninstall the Windows Secure Application Manager.

Cause   Administrator privileges are required to uninstall components of the Windows Secure Application Manager application.

Action   Ensure that the current user on this computer has administrator privileges or the Juniper Networks Win32 Installer Service loaded.

Windows UI Error Messages (sam.windows.ui)

sam.windows.ui.23793

System Log Message   Unable to open the Windows Secure Application Manager debug log file.

Cause   The Windows Secure Application Manager debug log file could not be opened. The file might have been deleted, become corrupted, or been moved. Your system administrator might also have disabled the log file setting on the secure gateway.

Action   Contact your system administrator.

sam.windows.ui.23794

System Log Message   Unable to open the Windows Secure Application Manager APPDATA folder.

Cause   The directory where the log files are located could not be opened because the current user does not have appropriate access permission.

Action   Ensure that the you have appropriate access permission for the APPDATA\Juniper Networks\Secure Application Manager folder.

sam.windows.ui.23795

System Log Message   You must restart the Windows Secure Application Manager for the new debug log setting to take effect.

Cause   The Windows Secure Application Manager debug log setting has been changed. You need to terminate the current session and launch the Windows Secure Application Manager again to enable the new setting.

Action   Terminate the existing session and launch a new Windows Secure Application Manager session.

sam.windows.ui.23796

System Log Message This Windows Secure Application Manager session will time out due to inactivity in $<x>$ minutes $<y>$ seconds. Click **Extend Session** to continue your Windows Secure Application Manager session.

Cause Your Windows Secure Application Manager session has been inactive for a period of time sufficient to trigger an automatic termination. The system administrator configures this value on the secure gateway.

Action Click **Extend Session** to continue your Windows Secure Application Manager session.

sam.windows.ui.23797

System Log Message The Windows Secure Application Manager session will time out in $<x>$ minutes $<y>$ seconds. Ensure that any work dependent on the secure gateway session is saved before the session times out.

Cause Your session duration is approaching the maximum session time-out value configured on the secure gateway.

Action Click **OK** and ensure that any work dependent on the secure gateway session is saved before the session times out. Then, start a new secure gateway session.

Network Connect Error Messages

This section contains the following types of Network Connect error messages:

- "Windows Application Messages (nc.windows.app)" on page 8
- "Windows GINA Error Messages (nc.windows.gina)" on page 17
- "Windows Command Line Launcher Messages (nc.windows.nclauncher)" on page 23
- "Windows Setup Messages (nc.windows.setup)" on page 26
- "Macintosh Messages (nc.mac.app)" on page 30

Windows Application Messages (nc.windows.app)

This section contains the Network Connect error messages for Windows.

nc.windows.app.23660

System Log Message Unable to load resource *< resource name >*. Loading English resource library, instead.

Cause The specified resource library could not be found.

Action Re-install the Network Connect client. If the resource you want to use is still inaccessible, contact your system administrator.

nc.windows.app.23661

System Log Message Cannot load resource *< resource name >*.

Cause The specified resource library could not be found.

Action Re-install the Network Connect client. If the specified resource library is still inaccessible, contact your system administrator.

nc.windows.app.23662

System Log Message Network Connect client cannot start due to missing components.

Cause The Network Connect stand-alone client credentials are valid, but a required component is missing. Network Connect must terminate the session.

Action Uninstall and then re-install the Network Connect stand-alone client before trying to start Network Connect again.

nc.windows.app.23663

System Log Message Network Connect is already running on the client. Please terminate your existing session before starting a new one.

Cause   Network Connect is already running on this computer.

Action   Click **OK** to close the new Network Connect application, manually terminate the existing Network Connect session, and start Network Connect again.

nc.windows.app.23664

System Log Message   The Network Connect virtual adapter driver is not installed properly. Please re-install Network Connect.

Cause   The Network Connect driver is not installed properly.

Action   Uninstall and re-install Network Connect and try to sign in to the secure gateway again. If Network Connect is still not properly installed, contact your system administrator.

nc.windows.app.23677

System Log Message   Would you like to enable the Graphical Identification and Authentication (GINA) automatic sign-in function to start Network Connect when Windows starts?

Cause   Your system administrator has enabled the GINA automatic sign-in function for your user role. You can choose to enable GINA at this time or postpone installing GINA. (GINA enables you to start Network Connect when Windows starts.)

Action   Click **Yes** to enable the GINA automatic sign-in function on your computer. Click **No** to sign in to Network Connect manually.

nc.windows.app.23678

System Log Message   The Graphical Identification and Authentication (GINA) automatic sign-in function has been enabled on your computer.

Cause   Your system administrator has enabled the GINA automatic sign-in function on the secure gateway, which automatically starts Network Connect when you sign in to Windows. This function will take effect the next time you boot your computer and start Windows.

Action   This is an informational message. Click **OK** to continue.

nc.windows.app.23679

System Log Message   Network Connect is configured to start when Windows starts, but this function cannot be enabled due to conflict with another Windows application.

Cause   Your system administrator enabled the Graphical Identification and Authentication (GINA) automatic sign-in feature for this user role on the secure gateway, but your computer has an existing GINA component installed from another application.

Action   Click **OK** to continue. After you have signed in to Windows, sign in to the secure gateway and launch Network Connect from the secure gateway Web console page.

nc.windows.app.23680

System Log Message The Network Connect system administrator disabled the Graphical Identification and Authentication (GINA) automatic sign-in feature. This change will take effect the next time you start Windows.

Cause The GINA automatic sign-in function was originally enabled for this user, but the system administrator has disabled the function on the secure gateway.

Action Click **OK** to continue your network connect session.

nc.windows.app.23681

System Log Message Network Connect could not initialize the Graphical Identification and Authentication (GINA) automatic sign-in feature.

Cause You either do not have appropriate administrative privileges, or you do not have the Juniper Installer Service installed on this computer.

Action Contact your system administrator to get the Juniper Installer Service, or the correct GINA-enabled Network Connect application, installed on your computer.

nc.windows.app.23682

System Log Message Network Connect could not disable the Graphical Identification and Authentication (GINA) automatic sign-in feature.

Cause Your system administrator disabled GINA for your user role, however, you either do not have appropriate administrative privileges, or you do not have the Juniper Installer Service installed on this computer.

Action Contact your system administrator to get the Juniper Installer Service, or the correct Network Connect application, installed on your computer.

nc.windows.app.23686

System Log Message You must reboot your computer to enable the auto-connect function. Auto-connect enables you to launch a Network Connect tunnel when Windows starts. Would you like to reboot now?

Cause The user has selected "Auto connect" in the Network Connects options dialog box. This setting is only enabled if the secure gateway administrator has allowed the user to select the option on the client.

Action Click **OK** to reboot your computer and enable the auto-connect option. Click **No** to reboot your computer later. Click **Cancel** to close the dialog box without activating the auto-connect option.

nc.windows.app.23687

System Log Message Network Connect is configured to start when Windows starts, but this function cannot be enabled due to conflict with another Windows application. Network Connect installation has terminated.

Cause Your system administrator enabled the Graphical Identification and Authentication (GINA) automatic sign-in feature for this user role on the secure gateway, but your computer has an existing GINA component installed from another application.

Action Click **OK** to exit installation. After you have signed in to Windows, sign in to the secure gateway and launch Network Connect from the secure gateway Web console page.

nc.windows.app.23689

System Log Message Unable to open the APPDATA folder.

Cause The folder is either requires privileged permissions, is not present, has been deleted or moved, or has become corrupt.

Action Try to verify the current user's access level and wether or not the user is able to open his/her own application data folder. (The location of the folder is APPDATA\Juniper Networks\Network Connect <*version*>\.) Then, sign out of Network Connect and sign in to Windows again. If you still cannot open the application data folder, contact your system administrator.

nc.windows.app.23703

System Log Message Successfully copied information to log file.

Cause This messages confirms that the log file has been successfully updated.

Action This is an informational message. No action on your part is required.

nc.windows.app.23704

System Log Message Connection attempt timed out.

Cause The Network Connect client timed out waiting for a response from the secure gateway.

Action Close the Network Connect client and try to sign in again. If you are still unable to sign in, contact your system administrator.

nc.windows.app.23705

System Log Message Unable to display connection information.

Cause Network Connect is unable to retrieve and display secure gateway connection information. (Connection information includes bytes sent/received, encryption protocol, compression information, and transport mode information.) Check your firewall or network configuration to ensure that the client has network connectivity to the secure gateway.

Action Sign out of the secure gateway and try to connect again. If you are still unable to view connection information, contact your system administrator.

nc.windows.app.23706

System Log Message Network Connect automatic connection error.

Cause Network Connect is unable to attach to the automatic secure gateway connection established during Windows sign-in.

Action Try to connect to the secure gateway again. If you are still unable to attach to the automatic secure gateway connection, contact your system administrator.

nc.windows.app.23707

System Log Message Cannot open a connection to the NCService component.

Cause Network Connect is unable to open a connection to the NCService component. The Network Connect service may have become disabled, or a problem may have occurred during Network Connect installation.

Action Restart the Network Connect client. If you are unable to connect, uninstall and re-install Network Connect and try signing in again. If you are still unable to open a connection to the NCService component, contact your system administrator.

nc.windows.app.23708

System Log Message Cannot connect to the secure gateway.

Cause Network Connect is unable to connect to the secure gateway. This is likely a network or firewall problem, or may be configuration issue on the secure gateway.

Action Verify your network connection, proxy settings (if applicable), and firewall/router ACL rules with your system administrator to ensure that the client is able to connect to the secure gateway. Then, try to connect to the secure gateway again. If you are still unable to open a connection to the secure gateway, contact your system administrator.

nc.windows.app.23709

System Log Message Cannot open a connection to the secure gateway.

Cause Network Connect is unable to open a connection to the secure gateway. This is likely a network or firewall problem, or may be configuration issue on the secure gateway.

Action Verify your network connection, proxy settings (if applicable), and firewall/router ACL rules with your system administrator to ensure that the client is able to connect to the secure gateway. Then, try to connect to the secure gateway again. If you are still unable to open a connection to the secure gateway, contact your system administrator.

nc.windows.app.23710

System Log Message Unable to retrieve connection information from the secure gateway.

Cause Network Connect is unable to get connection configuration information from secure gateway. The connection to the secure gateway may have been lost.

Action Sign out of the secure gateway and try to connect again. Then, verify your network connection, proxy settings (if applicable), and firewall/router ACL rules with your system administrator to ensure that the client is able to connect to the secure gateway. If you are still unable to open a connection to the secure gateway, contact your system administrator.

nc.windows.app.23711

System Log Message The Network Connect session terminated. Do you want to re-connect?

Cause The Network Connect client disconnected from the secure gateway because the client's routing table was altered.

Action Click **Yes** to sign in to the secure gateway and launch Network Connect again. Click **No** to close the Network Connect client.

nc.windows.app.23712

System Log Message The Network Connect session terminated. Do you want to re-connect?

Cause The Network Connect client was disconnected from the secure gateway because of a failure in the client's configuration. It is possible a network adapter or other piece of hardware failed.

Action Click **Yes** to re-establish your connection to the secure gateway. Click **No** to close the Network Connect client. If you are still having trouble, contact your system administrator and verify your computer's system configuration before signing in to the secure gateway and launching Network Connect again. You can also try uninstalling and reinstalling Network Connect.

nc.windows.app.23713

System Log Message Proxy authentication required to connect to the secure gateway.

Cause There is a proxy server configured between your client and the secure gateway. This proxy server requires valid authentication credentials to allow connection to the secure gateway

Action Input valid credentials into the proxy authentication dialog box.

nc.windows.app.23714

System Log Message Failed to connect to the secure gateway.

Cause The previous Network Connect session failed to disconnect from secure gateway.

Action Ensure that the previous session has terminated and try to connect to the secure gateway again. If you are still unable to connect to the secure gateway, contact your system administrator.

nc.windows.app.23715

System Log Message   Unable to retrieve connection information from the secure gateway.

Cause   Network Connect received an error while retrieving connection information from the secure gateway. The secure gateway may have become unreachable, or might not be operating correctly.

Action   Sign out of the secure gateway and try to connect again. (You might also try uninstalling and re-installing your Network Connect client.) If you are still unable to view connection information, contact your system administrator.

nc.windows.app.23786

System Log Message   The Network Connect NCService component is not running.

Cause   The Network Connect service is not running and the current user does not have adequate administrative privileges to start the service.

Action   Re-install Network Connect and try to sign in to the secure gateway again. If you still cannot launch Network Connect, contact your system administrator.

nc.windows.app.23787

System Log Message   Cannot start the Network Connect service. Please re-install Network Connect.

Cause   The Network Connect NCService component is not running and the client is unable to start it.

Action   Uninstall and re-install Network Connect and try to sign in to the secure gateway again. If you still cannot launch Network Connect, contact your system administrator.

nc.windows.app.23788

System Log Message   Unable to retrieve connection information from the secure gateway < *Secure Gateway name* > .

Cause   Network Connect is unable to get connection configuration information from the secure gateway. The connection to the secure gateway may have been lost.

Action   Sign out of the secure gateway and try to connect again. Then, verify your network connection, proxy settings (if applicable), and firewall/router ACL rules with your system administrator to ensure that the client is able to connect to the secure gateway. If you are still unable to open a connection to the secure gateway, contact your system administrator.

nc.windows.app.23789

System Log Message   Unable to retrieve connection information from the secure gateway < *Secure Gateway name* > .

Cause Network Connect received an error while retrieving connection information from the secure gateway. The secure gateway may have become unreachable, or might not be operating correctly.

Action Sign out of the secure gateway and try to connect again. (You might also try uninstalling and re-installing your Network Connect client.) If you are still unable to view connection information, contact your system administrator.

nc.windows.app.23790

System Log Message The Network Connect session timed out.

Cause The Network Connect client has been disconnected from secure gateway because the session timed out. Your session may have reached the idle session time-out or the maximum session length your administrator configured on the secure gateway.

Action Sign in to the secure gateway and launch Network Connect again.

nc.windows.app.23791

System Log Message The secure gateway denied the connection request from this client.

Cause The secure gateway denied your computer's connection request. Your system may be configured with an option to auto-detect proxy settings, which is not supported by Network Connect.

This error also occurs when there is an error on the server.

Action Try to connect to the secure gateway again. If you are still unable to connect to the secure gateway, contact your system administrator.

Also check the server error log for messages.

nc.windows.app.23792

System Log Message Failed to connect to the secure gateway. Do you want to reconnect?

Cause The secure gateway denied your computer's connection request.

Action Contact your system administrator. You may need to uninstall and reinstall your computer's Java Runtime Engine (JRE). If your \Documents and Settings folder is encrypted, you will need to right-click on the folder and select **Properties**. Then, you need to click the **Advanced** button, uncheck the option to **Encrypt contents to secure data**, and click **OK**.

nc.windows.app.24043

System Log Message A Network Connect tunnel is already configured on the client. Please terminate your existing session and wait for it to terminate completely before starting a new one.

Cause An existing Network Connect tunnel already exists. If Network Connect was recently disconnected, the resource is not released yet.

Action   Wait a few minutes and try connecting again.

nc.windows.app.24044

System Log Message   Network Connect could not initialize the Type of Service (TOS) feature.

Cause   Your system administrator has enabled the TOS feature for your user role, but the local Network Connect client application cannot enable it.

Action   Contact your system administrator.

nc.windows.app.24045

System Log Message   Network Connect could not disable the Type of Service (TOS) feature.

Cause   Your system administrator has disabled the TOS feature for your user role, but the local Network Connect client application cannot disable it.

Action   Contact your system administrator.

nc.windows.app.24052

System Log Message   The Network Connect session will time out due to inactivity in $<x>$ minute(s) $<y>$ second(s).

Cause   Your Network Connect session has been inactive for a period of time sufficient to trigger an automatic termination. The system administrator configures this value on the secure gateway.

Action   Click the **Extend Session** button to continue your Network Connect session.

Connect again.

nc.windows.app.24054

System Log Message   The Network Connect session will time out in $<x>$ minute(s) $<y>$ second(s).

Cause   Your Network Connect session is approaching the maximum session duration configured by your system administrator.

Action   After the session has terminated, sign in to the secure gateway and launch Network Connect again.

nc.windows.app.24058

System Log Message   You must reboot your computer to enable the Type of Service (TOS) feature. Would you like to reboot now?

Cause   Enabling the Type of Service (TOS) feature requires you to reboot your system.

Action   Click **Yes** to reboot now, **No** to reboot later.

nc.windows.app.24061

System Log Message Reconnect attempt to the secure gateway failed

Cause Network Connect failed to reconnect to the secure gateway.

Action Exit out of Network Connect and try to log in to the secure gateway again.

nc.windows.app.24062

System Log Message Launching Network Connect will automatically terminate your WSAM session, which may render some network resources unreachable. Do you want launch Network Connect?

Cause You have initiated a Network Connect session while a WSAM session is already active.

Action Click **Yes** to automatically terminate WSAM and launch Network Connect. Click **No** to return to the active WSAM session without launching Network Connect. (**Note:** If you click **No**, the Network Connect client application will be installed on your computer, but will not launch.)

nc.windows.app.24362

System Log Message Unable to start Network Connect. Try again.

Cause Network Connect cannot find the session parameters because of an internal error.

Action Launch Network Connect from the secure gateway home page. If the error message appears again, contact your system administrator.

Windows GINA Error Messages (nc.windows.gina)

nc.windows.gina.23806

System Log Message Network Connect sign-in using the Graphical Identification and Authentication (GINA) automatic sign-in feature is not configured on the secure gateway.

Cause The user's sign-in credentials are valid, but the system administrator has not enabled GINA for the use's role.

Action Contact your system administrator to ensure GINA is enabled for the user's role.

nc.windows.gina.23807

System Log Message Cannot launch the current version of Network Connect via the Graphical Identification and Authentication (GINA) automatic sign-in feature. You are running a version that is older than on the secure gateway. After Windows starts, sign in to the secure gateway and upgrade your version of Network Connect

Cause You are running a version of Network Connect that is older than the version on the secure gateway. Therefore, the GINA automatic sign-in feature cannot launch Network Connect when Windows starts.

Action   After Windows starts, sign in to the secure gateway and upgrade your version of Network Connect.

nc.windows.gina.23808

System Log Message   Could not establish a Network Connect tunnel. The Graphical Identification and Authentication (GINA) automatic sign-in feature is not enabled on the secure gateway.

Cause   The user's sign-in credentials are valid, but GINA is not enabled for the user's role. GINA may have been enabled on this role in a prior installation and then disabled by the system administrator.

Action   Contact your system administrator to ensure GINA is enabled for the user's role.

nc.windows.gina.23809

System Log Message   The Network Connect tunnel has disconnected because you are not signed into a NT domain.

Cause   You may have signed in to your Windows session using cached credentials that do not match the Windows NT or Windows Active Directory domain credentials.

Action   Ensure that your computer is a member of the correct Windows NT or Windows Active Directory domain and that your Windows sign-in credentials are valid.

nc.windows.gina.23810

System Log Message   You must enter a valid proxy server IP address or host name.

Cause   The proxy server option has been activated, but the proxy IP address or host name is invalid or no proxy server information has been specified.

Action   Ensure that the proxy server information is valid and try to sign in to the secure gateway again.

nc.windows.gina.23811

System Log Message   Enter a complete URL in the format https://www.server.yourcompany.com.

Cause   The URL specified is invalid or formatted incorrectly.

Action   Verify that the https:// prefix is included and that the secure gateway's host name is correct.

nc.windows.gina.23812

System Log Message   Enter the HTTP port required to communicate with the proxy server.

Cause   The port specified for the proxy server is incorrect or is not a TCP port.

Action   Contact your system administrator to verify the port number for the proxy server.

nc.windows.gina.23813

System Log Message Enter a user name recognized by the proxy server.

Cause The user name or password entered is not correct.

Action Enter the correct user name and password.

nc.windows.gina.23814

System Log Message Enter a user name recognized by the secure gateway.

Cause The user name field has been left empty.

Action Specify a valid user name and try to connect again.

nc.windows.gina.23815

System Log Message Could not establish a Network Connect tunnel. Host Checker or Cache Cleaner is configured on the secure gateway, which is not compatible with the Graphical Identification and Authentication (GINA) automatic sign-in feature.

Cause Incompatible Host Checker or Cache Cleaner policies are configured on the secure gateway causing GINA sign-in to fail.

Action Login to Windows without GINA sign-in and use your browser to sign in to the secure gateway.

nc.windows.gina.23816

System Log Message Secure gateway authentication failed.

Cause The authentication user name and/or password you entered are invalid and were rejected by the secure gateway.

Action Verify the user name and password and try signing in again. If you believe the user name and password you specified are correct, contact your system administrator.

nc.windows.gina.23817

System Log Message Could not establish a Network Connect tunnel.

Cause A Network Connect tunnel between the client and the secure gateway could not be established. Your network may have suffered a temporary loss of connectivity, there may be an issue with your proxy settings, or there may have been a communication error between the Graphical Identification and Authentication (GINA) automatic sign-in feature and the Network Connect service.

Action Contact your system administrator to verify network connectivity, proxy settings, and secure gateway settings.

nc.windows.gina.23818

System Log Message Your connection to the secure gateway has terminated.

Cause   The Network Connect service unexpectedly terminated during authentication.

Action   After you have signed in to Windows, uninstall Network Connect. Then sign in to the secure gateway and re-install Network Connect.

nc.windows.gina.23819

System Log Message   Could not establish a Network Connect tunnel. You are associated with multiple user roles on the secure gateway, which is not compatible with the Graphical Identification and Authentication (GINA) automatic sign-in feature.

Cause   The secure gateway is configured to prompt the user with a role-selection page, which is not supported when GINA is enabled for the user's role.

Action   The system administrator must ensure that GINA is disabled for the user, or the user is only associated with a single role.

nc.windows.gina.23820

System Log Message   The secure gateway was unable to authenticate your user credentials after two consecutive attempts. The Graphical Identification and Authentication (GINA) automatic sign-in feature will not attempt to sign in to the secure gateway again during the current windows sign in session.

Cause   The secure gateway was unable to authenticate the specified user credentials after two consecutive attempts.

Action   Verify your user credentials and connect to the secure gateway after Windows has started. If you believe the credentials used during Windows sign-in were correct, contact your system administrator.

nc.windows.gina.23937

System Log Message   Tunnel establishment aborted because Gina is Disabled in the Secure Access Gateway.

Cause   The user's sign-in credentials are valid, but GINA is not enabled for the user's role. GINA may have been enabled on this role in a prior installation and then disabled by the system administrator.

Action   Contact your system administrator to ensure GINA is enabled for the user's role.

nc.windows.gina.24039

System Log Message   Network Connection configuration file is not available on you local system, you cannot start Network Connection through Gina. You can repair it after you log in to your domain by launching Network Connection through the web browser.

Cause   The Network Connection configuration file may have been deleted by accident.

Action   Log in to your domain by launching Network Connection through the web browser and repair the Network Connection configuration file.

nc.windows.gina.24040

System Log Message The Program File is not available.

Cause A user accidentally deleted or renamed the C:\Program Files directory.

Action Reinstall the Windows operating system.

nc.windows.gina.24041

System Log Message GINA cannot reach the secure gateway server. Click OK to try connecting again. If GINA still fails to connect, check the host name or proxy setting or cancel the GINA sign-in process.

Cause Network Connect failed to connect to the secure gateway. Possible causes include a failed network connection, incorrect host name, or incorrect proxy setting.

Action Click OK to try connecting again. If GINA still fails to connect, check the host name or proxy setting or cancel the GINA sign-in process and try signing in again after your computer has had a chance to properly connect to the network. If you are still unable to connect to the secure gateway, contact your system administrator.

nc.windows.gina.24213

System Log Message HostChecker is not installed for current user. Please login without using Juniper GINA and install HostChecker through Web browser.

Cause Current user does not have HostChecker installed.

Action Log on to the local machine and install HostChecker through the Web browser.

nc.windows.gina.24214

System Log Message HostChecker installed version is not compatible with secure gateway. Please login without using Juniper Networks GINA and re-install HostChecker through Web browser.

Cause The version of the HostChecker installed on the local system is not compatible with the secure gateway.

Action Log on to the local machine and re-install HostChecker through the Web browser.

nc.windows.gina.24215

System Log Message HostChecker launching failed. Please logon without using Juniper Networks GINA.

Cause HostChecker could not start successfully.

Action Click **Cancel** to logon without using Juniper Networks GINA.

nc.windows.gina.24216

System Log Message Your local machine doesn't meet the security policy requirement, access to secure gateway is denied. Click OK to logon without using Juniper Networks GINA.

Cause	The local system failed to meet the security policy requirements.
Action	Quit logon using Juniper Networks GINA.

nc.windows.gina.24334

System Log Message	NetworkConnect is not enabled, please logon without using Juniper Networks GINA.
Cause	network Connect is disabled for this role.
Action	Logon without using Juniper Networks GINA.

nc.windows.gina.24381

System Log Message	Version file is not found or corrupted, Click OK to exit GINA logon
Cause	The secure gateway cannot find a version file for GINA or the version file is corrupted.
Action	Click **OK** to exit the GINA sign-in page and contact your system administrator.

nc.windows.gina.24382

System Log Message	The secure gateway and Network Connect client versions do not match. (The Network Connect GINA client automatically connects to the last secure gateway server that you accessed, which may not use the Network Connect version defined in the GINA client.) Click OK to upgrade to the install the correct Network Connect version. Or, click Cancel to sign into a different secure gateway.
Cause	The Network Connect GINA client automatically connects to the last secure gateway server that the user accessed, which may not use the Network Connect version defined in the GINA client.
Action	Click **OK** to upgrade to the correct Network Connect version. Or, click **Cancel** to sign into the secure gateway that uses the older version of Network Connect.

nc.windows.gina.24407

System Log Message	Currently loaded Network Connect GINA client version is different from selected Secure Gateway. Click OK to continue (the correct version will be automatically loaded) or click Cancel to choose another Secure Gateway.
Cause	When Network Connect GINA starts up, the latest installed version is always automatically loaded and used to connect to the last accessed Secure Gateway. The last accessed Secure Gateway may not be the latest released version (the Secure Gateway may have been downgraded or the user may have logged into a different Secure Gateway.) If the latest released Network Connect GINA version matches the latest installed version on the client, the user can choose to continue logging in to the current Secure Gateway (the Network Connect client automatically loads the correct version of Network Connect GINA) or select a different Secure Gateway.
Action	Click **OK** to continue or **Cancel** to select a different Secure Gateway.

nc.windows.gina.24442

System Log Message You are not allowed to sign into to the secure gateway.

Cause Your computer does not meet the requirements of the Host Checker policy configured by your system administrator.

Action Click **OK** to exit and contact your system administrator.

nc.windows.gina.24443

System Log Message You have entered an invalid username and/or password.

Cause You have entered an invalid username and/or password.

Action Click **OK** to return to previous sign-in page and try to enter your username/password again.

nc.windows.gina.24628

System Log Message The secure gateway and Network Connect client versions do not match. (The Network Connect client automatically connects to the last secure gateway server that you accessed, which may not use the version defined in the Network Connect client.) Click OK to continue to log into your desktop, and then login to your secure gateway to upgrade Network Connect. Or, click Cancel to sign into the secure gateway that uses different version of Network Connect.

Cause The Network Connect GINA client automatically connects to the last secure gateway server that the user accessed, which may not use the Network Connect version defined in the GINA client.

Action Click **OK** to continue to log into your desktop, and then login to your secure gateway to upgrade Network Connect. Or, click Cancel to sign into the secure gateway that uses different version of Network Connect.

Windows Command Line Launcher Messages (nc.windows.nclauncher)

This section contains the error messages for the Network Connect command line launcher.

nc.windows.nclauncher.23806

System Log Message Network Connect has started

Cause Network Connect has started.

Action No action required.#

nc.windows.nclauncher.24431

System Log Message Invalid program arguments have been specified

Cause You have not entered valid command line arguments for Network Connect

Action   Use the -help command to see a list of valid command line options.#

nc.windows.nclauncher.24432

System Log Message   Network Connect was unable to connect to [secure gateway].

Cause   General connection failure. The secure gateway is not reachable.

Action   Contact your system administrator.

nc.windows.nclauncher.24433

System Log Message   The specified credentials do not authenticate.

Cause   The credentials entered when launching Network Connect are invalid.

Action   Re-check your credentials and try again.

nc.windows.nclauncher.24434

System Log Message   The specified role is invalid or does not exist.

Cause   The role entered when launching Network Connect is invalid.

Action   Re-check your role and try again.

nc.windows.nclauncher.24435

System Log Message   Network Connect cannot start because Host Checker or Cache Cleaner could not be started

Cause   Host Checker or Cache Cleaner is enabled on the secure gateway.

Action   Your system administrator must disable Host Checker and Cache Cleaner in order for you to run the Network Connect launcher.

nc.windows.nclauncher.24436

System Log Message   Network Connect installation failed

Cause   Network Connect could not be installed.

Action   Try again. If the problem persists, contact your system administrator.

nc.windows.nclauncher.24437

System Log Message   Network Connect was unable to perform a required software upgrade

Cause   Network Connect was unable to perform a required software upgrade.

Action   Contact your system administrator.

nc.windows.nclauncher.24438

System Log Message Network Connect has exited

Cause Network Connect has exited.

Action No action is required.

nc.windows.nclauncher.24439

System Log Message Network Connect has exited and the user has signed out of secure gateway

Cause Network Connect has exited and signed the user out of the secure gateway.

Action No action is required.

nc.windows.nclauncher.24440

System Log Message Network Connect is not running. Unable to signout from Secure Gateway.

Cause User entered –signout option. Network Connect is not running, so it can't signout from secure gateway.

Action No action is required.

nc.windows.nclauncher.24441

System Log Message Network Connect is not running.

Cause User entered –stop option, but Network Connect is not running.

Action No action is required.

nc.windows.nclauncher.24557

System Log Message The server you are attempting a connection with does not currently support this feature.

Cause Network Connect nclauncher unable to sign-in because Network Connect is not enabled on the secure gateway.

Action Login to the secure gateway using a browser and check whether Network Connect is enabled. If Network Connect is already enabled, contact technical support.

nc.windows.nclauncher.24558

System Log Message Network Connect failed to authenticate the client certificate.

Cause Network Connect nclauncher is unable to sign-in because of a client certificate error.

Action Check whether you are using the correct client certificate.

nc.windows.nclauncher.24559

System Log Message	NCLauncher failed to authenticate the client certificate. The certificate is invalid.
Cause	NCLauncher is not able to sign-in because the client certificate is invalid.
Action	Check whether you are using the correct client certificate.

nc.windows.nclauncher.24560

System Log Message	NCLauncher failed to authenticate the client certificate. The certificate is expired.
Cause	NCLauncher is not able to sign-in because the client certificate is expired.
Action	Check whether you are using the correct client certificate.

nc.windows.nclauncher.24561

System Log Message	NCLauncher failed to authenticate the client certificate. The certificate is revoked.
Cause	NCLauncher is not able to sign-in because the client certificate is revoked.
Action	Check whether you are using the correct client certificate.

nc.windows.nclauncher.24653

System Log Message	Network Connect could not start. Host checker has failed to evaluate your computer's security requirements.
Cause	Host checker has failed to evaluate one or more security policy.
Action	Contact your system administrator.

Windows Setup Messages (nc.windows.setup)

nc.windows.setup.24046

System Log Message	You must have administrator privileges to install Network Connect on this computer. Network Connect installation has terminated.
Cause	The user currently signed in to this computer does not have administrative privileges, which are required to install and run the Network Connect client.
Action	Sign in to Windows as the system administrator and try to install Network Connect again.

nc.windows.setup.24047

System Log Message	Network Connect is not supported on this operating system. Network Connect installation has terminated.
Cause	Only Windows 2000 and Windows XP support installing this version of the Network Connect client.

Action   Click **OK** to exit Network Connect installation.

nc.windows.setup.24048

System Log Message   The Graphical identification and Authentication (GINA) automatic sign-in function has been enabled on your computer.

Cause   Your administrator has enabled the GINA function.

Action   No action is required. This is an information message only.

nc.windows.setup.24049

System Log Message   Network Connect is configured to start when Windows starts, but this function cannot be enabled due to conflict with another Windows application. Network Connect installation has terminated

Cause   Your administrator enabled the Graphical identification and Authentication (GINA) automatic sign-in function, but the GINA client installed on your computer and is not compatible with our GINA.

Action   Remove your current GINA installation. Contact your system administrator if you need assistance.

nc.windows.setup.24050

System Log Message   Network Connect upgrade failed. Please manually uninstall the Network Connect client and try installing again.

Cause   The Network Connect upgrade process experienced a problem. Network Connect may have been partially installed, causing the un-installation step in the upgrade process to fail.

Action   Click **OK** to close this message box, manually un-install Network Connect, and then install the upgraded version.

nc.windows.setup.24051

System Log Message   You must reboot your computer to complete Network Connect installation. Would you like to reboot your computer now?

Cause   The Network Connect Installation process encountered a problem. The prior version of the NCService component may not have stopped within the Service Control manager.

Action   Click **Yes** to complete the upgrade process and reboot your computer.

nc.windows.setup.24053

System Log Message   Please close any open Microsoft Internet Explorer windows. Aborting Network Connect Installation…

Cause   An open Internet Explorer window is suspending the Juniper ActiveX control, thus disabling Network Connect installation.

Action	Click **OK**, close all Internet Explorer windows, and then try to install Network

nc.windows.setup.24055

System Log Message	You must reboot your computer to finish setting up Network Connect.
Cause	The uninstallation portion of the Network Connect setup process encountered an error when stopping the NCService component. You must reboot your computer to correct the problem.
Action	Click **OK** to reboot your computer and complete Network Connect installation.

nc.windows.setup.24056

System Log Message	You must have administrator privileges to uninstall Network Connect on this computer. Network Connect setup has terminated.
Cause	You do not have administrator privileges.
Action	Contact your system administrator.

nc.windows.setup.24057

System Log Message	Network Connect has detected that Plug and Play has been disabled on your computer. Your system does not currently allow certain components of Network Connect to be installed on your computer. Please refer to the secure gateway online documentation for instructions on how to turn on plug and play.
Cause	This message appears when Plug and Play has been disabled by some other application on the computer. This prevents complete installation of the Network Connect driver.
Action	The following registry key should be created: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce on the client system. This will enable Plug and Play on the client system.

nc.windows.setup.24058

System Log Message	You must reboot your computer to complete the installation process. Save your work and then click OK to restart your computer.
Cause	You are installing Network Connect on a Windows 98 system, which requires you to reboot your computer to complete the installation process.
Action	Save your work, close all running applications, and click **OK** to reboot your computer.

nc.windows.setup.24059

System Log Message	You must reboot your computer to complete the uninstallation process. Save your work and then click OK to restart your computer.
Cause	You are removing Network Connect from a Windows 98 system, which requires you to reboot your computer to complete the uninstallation process.

Action   Save your work, close all running applications, and click **OK** to reboot your computer.

nc.windows.setup.24060

System Log Message   Usage: NCInst.exe [[en|es|ko|zh|zh_cn|ja|de|fr] [gina] | [help] | [version]]

Cause   This is a usage alert that appears when a flag is passed to NCInst.exe.

Action   Click **OK** to close the dialog box.

nc.windows.setup.24084

System Log Message   Network Connect application is still in use. Please stop NC application and then try uninstallation again.

Cause   User tries to uninstall Network Connect while it is still running.

Action   Stop Network Connect, then try uninstalling it again.

nc.windows.setup.24314

System Log Message   The GINA client that automatically starts Network Connect is chained to other GINA clients on your system. You cannot uninstall the Network Connect GINA, since it will invalidate the other GINA clients with it. Please uninstall the GINA clients that automatically start other Windows components on your system, then try again.

Cause   The GINA client that automatically starts Network Connect is chained (that is, configured to pass information) to other GINA clients on the user's system. The user tries to uninstall the Network Connect GINA client, which would invalidate the other GINA functions with it.

Action   Uninstall the GINA clients that automatically start other Windows components on your system, then try uninstalling the Network Connect GINA client again.

nc.windows.setup.24322

System Log Message   Network Connect installation failed. You must reboot your computer and try again. Save your work and click OK.

Cause   Network Connect installation failed.

Action   Save your work and click **OK** to reboot your computer. Then, try installing Network Connect again.

nc.windows.setup.24323

System Log Message   Network Connect uninstallation failed. You must reboot your computer and try again. Save your work and click OK.

Cause   Network Connect failed to uninstall successfully.

Action   Save your work and click **OK** to reboot your computer. Then, try uninstalling Network Connect again.

nc.windows.setup.24324

System Log Message Network Connect driver installation failed. Please exit and try again.

Cause Network Connect driver installation failed.

Action Exit Network Connect and try installing it again.

Macintosh Messages (nc.mac.app)

This section contains the Network Connect error messages for Macintosh.

nc.mac.app.1003

System Log Message Network Connect cannot connect to the secure gateway.

Cause The secure gateway was found using the stand-alone Network Connect client, but the connection was refused or timed out.

Action Ensure you have entered the host name or IP address correctly and try signing in to the secure gateway again.

nc.mac.app.1004

System Log Message Network Connect cannot find the secure gateway.

Cause The secure gateway can't be found using the stand-alone Network Connect client. You may have entered an incorrect host name, or there may be a DNS configuration problem.

Action Ensure that you entered the host name or IP address correctly and try signing in to the secure gateway again. If you still cannot establish a connection to the secure gateway, contact your system administrator.

nc.mac.app.1005

System Log Message Network Connect cannot connect to the secure gateway.

Cause The Network Connect stand-alone client could not retrieve required data from the secure gateway. The secure gateway may have returned a zero-byte resource for an "HTTPS GET" function on the front page. This can happen when using an HTTPS proxy that is not properly configured, resulting in Safari showing a blank page for any session information passing through the proxy.

Action Try signing in to the secure gateway again. If you still cannot establish a connection to the secure gateway, contact your system administrator.

nc.mac.app.1100

System Log Message Network Connect is already running.

Cause Another instantiation of Network Connect is running on your computer. You can only launch one Network Connect session on your computer at a time.

Action　Ensure that no other Network Connect sessions are running before launching Network Connect.

nc.mac.app.1104

System Log Message　Your session timed out.

Cause　The session was terminated because Network Connect did not receive a heartbeat/health check message from the secure gateway for at least 90 seconds. (See the Log Viewer for more information.)

Action　Sign in to the secure gateway again. If you cannot establish a connection to the secure gateway, contact your system administrator.

nc.mac.app.1106

System Log Message　Upgrade Network Connect?

Cause　The version of the stand-alone Network Connect client on your computer (*<version>*) is not the same as the version on the secure gateway (*<version>*).

Action　Click **Upgrade** to upgrade your version of Network Connect, or click **Cancel** to terminate the connection.

nc.mac.app.1108

System Log Message　Your computer's network interface has changed.

Cause　Your computer's network settings changed, independent of the Network Connect session. Due to the security policies configured on the secure gateway, your connection was terminated. Changes may have been made to your System Preferences, network interfaces may have come up or gone down (e.g., PPP, AirPort wireless), a DHCP lease may have been renewed, or a malicious agent may have been introduced.

Action　Click **Reconnect** to re-establish the Network Connect session, or click **Cancel**. If you are using a stand-alone client, you are re-directed to the Network Connect sign-in window. If you are using a Web-launched client, the program will exit.

nc.mac.app.1109

System Log Message　Your computer's network interface has changed.

Cause　Your computer's network settings changed, independent of the Network Connect session. Due to the security policies configured on the secure gateway, your connection was terminated. Changes may have been made to your System Preferences, network interfaces may have come up or gone down (e.g., PPP, AirPort wireless), a DHCP lease may have been renewed, or a malicious agent may have been introduced.

Action　Click **OK**. If you are using a stand-alone client, you are re-directed to the Network Connect sign-in window. If you are using a Web-launched client, the program will exit.

nc.mac.app.1200

System Log Message Network Connect cannot establish a secure session.

Cause Network Connect can't start the tunneling service. There may have been a problem during installation. (See the Log Viewer for more information.)

Action Reinstall Network Connect and try signing in to the secure gateway again. If you still cannot establish a connection to the secure gateway, contact your system administrator.

nc.mac.app.1202

System Log Message Network Connect cannot establish a secure session.

Cause Network Connect was able launch and initiate communication with the secure gateway, but, for an unknown reason, couldn't start the tunneling service. (See the Log Viewer for more information.)

Action Reinstall Network Connect and try signing in to the secure gateway again. If you still cannot establish a connection to the secure gateway, contact your system administrator.

nc.mac.app.1203

System Log Message Your session terminated unexpectedly.

Cause A software error caused the Network Connect tunneling service to terminate. This may have been the result of a non-zero exit code—usually indicative of a software crash. (See the Log Viewer for more information.)

Action Try signing in to the secure gateway again. If you still cannot establish a connection to the secure gateway, contact your system administrator.

nc.mac.app.1204

System Log Message Your computer's routing table changed.

Cause Changes were made to your computer's routing table, independent of Network Connect. Due to the security policies configured on the secure gateway, your connection was terminated.

Action Click **Reconnect** to re-establish the Network Connect session, or click **Cancel**. If you are using a stand-alone client, you are re-directed to the Network Connect sign-in window. If you are using a Web-launched client, the program will exit.

nc.mac.app.1205

System Log Message Your computer's routing table has changed.

Cause Changes were made to your computer's routing table, independent of Network Connect. Due to the security policies configured on the secure gateway, your connection was terminated.

Action   Click **OK**. If you are using a stand-alone client, you are re-directed to the Network Connect sign-in window. If you are using a Web-launched client, the program will exit.

nc.mac.app.1206

System Log Message   Network Connect cannot establish a secure session.

Cause   The Network Connect tunneling service cannot authenticate with your HTTPS proxy server. (See the Log Viewer for more information.)

Action   Try signing in to the secure gateway again. If you still cannot establish a connection to the secure gateway, contact your system administrator.

nc.mac.app.1207

System Log Message   Your session timed out.

Cause   Due to session duration restrictions configured on the secure gateway, your Network Connect session expired.

Action   Try signing in to the secure gateway again. If you still cannot establish a connection to the secure gateway, contact your system administrator.

nc.mac.app.1400

System Log Message   Network Connect could not use your HTTPS proxy.

Cause   The Automatic Proxy Configuration (PAC) script could not be loaded from the URL provided in the Network pane of System Preferences. You may have typed a non-URL string into the text field in System Preferences.

Action   Verify the PAC script URL in your System Preferences and try signing in to the secure gateway again. If you still cannot establish a connection to the secure gateway, contact your system administrator.

nc.mac.app.1401

System Log Message   Network Connect could not use your HTTPS proxy.

Cause   The Automatic Proxy Configuration (PAC) script could not be loaded from the URL provided in the Network pane of System Preferences. This may be due to either a Domain Name service (DNS) error or a network connectivity-related error.

Action   Verify the PAC script URL in your System Preferences and try signing in to the secure gateway again. If you still cannot establish a connection to the secure gateway, contact your system administrator.

nc.mac.app.1402

System Log Message   Network Connect could not use your HTTPS proxy.

Cause	There may be errors in the Automatic Proxy Configuration (PAC) script at the URL specified in the Network pane of System Preferences. Otherwise, the PAC file may not be a text file, or uses an encoding method that cannot be read as UTF-8.
Action	Check with your network administrator and try signing in to the secure gateway again.

nc.mac.app.1403

System Log Message	Network Connect couldn't use your HTTPS proxy.
Cause	There may be errors in the Automatic Proxy Configuration (PAC) script at the URL specified in the Network pane of System Preferences. The PAC script may contain syntax errors.
Action	Check with your network administrator and try signing in to the secure gateway again.

nc.mac.app.1700

System Log Message	The Network Connect uninstallation failed.
Cause	An error occurred while uninstalling Network Connect.
Action	Check with your network administrator before attempting to uninstall or sign in to the secure gateway again.

nc.mac.app.1701

System Log Message	The Network Connect upgrade failed.
Cause	The stand-alone Network Connect upgrade package failed to download due to a network error.
Action	Check with your network administrator before attempting to install Network Connect again.

nc.mac.app.1804

System Log Message	Your session will expire shortly.
Cause	Due to session length restrictions configured on the secure gateway, your session will expire when the timer counts down to zero.
Action	Click **OK**. After your session has terminated, launch Network Connect or sign in to the secure gateway again.

nc.mac.app.1805

System Log Message	Do you want to extend your session?
Cause	You are approaching the maximum session idle time-out value configured on the secure gateway. If you choose not to extend your Network Connect session, due to inactivity, your session will expire when the timer counts down to zero.

Action   Click **Extend Session** to extend your session, click **Sign Out** to terminate your
connection to the secure gateway, or click **Do Nothing** to allow the connection to
expire once the timer has counted down to zero.