

Release Notes

Juniper Networks NetScreen Secure Access

IVE Platform version 4.1 R1 Build #6873



Juniper Networks, Inc.
1194 North Matilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

05 August 2004

Contents

Known Issues/Limitations Fixed in this Release	1
Known Issues and Limitations	1
Client-Side Digital Certificates/Cert-Based Authentication	1
Central Manager.....	2
Host Checker and Cache Cleaner.....	2
Secure Meeting	3
Windows based Secure Application Manager (W-SAM).....	5
Java Secure Application Manager (J-SAM).....	7
MacOS Java Secure Application Manager (J-SAM)	8
Network Connect (NC)	9
Clustering Issues	10
Sun JVM/Code-Signing Certificates.....	12
I-Mode Support	12
Customizable Sign-In Pages	12
Password Management	13
FIPS	13
Pass-Through Proxy Issues	14
Internationalization Issues	14
File Browsing Issues.....	15
Cache Cleaner	15
Netegrity.....	15
Miscellaneous issues:	15
Supported Platforms	20

Known Issues/Limitations Fixed in this Release

The following list enumerates known issues which fixed in this release:

1. When Network Connect is configured with to auto-launch and there is a custom start page, the re-direct problem to that start page is resolved in this release. (19212)
2. An issue with installation of Network Connect on Win XP Professional has been resolved in this release. (19681)
3. Network Connect supports static proxies with an exception list in the format of *.domain.com. (19278)
4. An issue with the stand alone Network Connect installer generating an error condition has been resolved in this release. (19181)
5. A problem accessing Windows file shares in a different domain is addressed in this release. (19360)
6. Problems accessing NetApp and EMC Celerra file shares have been addressed in the release. (19155, 18407)
7. Connecting to a Novell eDirectory LDAP server using encrypted port 636 is now handled. (19294)
8. An issue with Host Checker not updating properly when the user's IP address changes after the pre-authentication check has been resolved in this release. (19240)
9. FTP archiving failures for a specific UNIX FTP server have been resolved in this release. (19053)
10. Various rewrite issues have been resolved in this release. (19127)

Known Issues and Limitations

The following list enumerates known issues which are still outstanding in this release:

Client-Side Digital Certificates/Cert-Based Authentication

1. The IVE CRL checking mechanism will ignore the IssuingDistributionPoint CRL critical extension if included in the CRL object. (18211)
2. CRL download via HTTP Proxy is not supported.
3. Partitioned CRLs are not supported in this release. (16992)
4. After a Client-Side Digital Certificate has been loaded and used, Internet Explorer and Netscape both cache the credentials and certificate/private key as long as the web browser window remains open and in some cases until the PC is rebooted. More details can be found at: <http://support.microsoft.com/?kbid=290345>. This caching overrides password-protected certificates (you will not be prompted for the password again) and even USB tokens (you will not need to keep the token in the PC). For this reason, it is very important that Administrators train their end-users to always close their web browser after logout.

One helpful mechanism to achieve this is to add some text to the custom logout message asking users to close their web browser to properly end their session. This can be done under the Signing In menu by modifying the default sign-in page. (14637)

5. Certificate users may get an HTTP 500 error if the end-user gives a wrong password for their private key file when challenged for a client certificate.
6. When using LDAP for a CDP, port numbers should not be specified in the CDP Server field. The default port number for LDAP is 389. To use a non-standard port, Manual CDP configuration should be used. (18578)
7. When a client-side digital certificate authentication policy is configured for the Realm, if the client's certificate is expired, then the user will not be able to log into the Realm until he is given a valid client certificate. (14922)
8. If no Root CA is uploaded to the IVE for client certificate authentication/authorization, the end-user may be prompted to choose from a list of all of their client certificates, rather than just the certificate specific to the IVE. No matter which certificate they select, the IVE will always show the "Invalid Certificate" error page, because no Root CA has been uploaded to verify the client certificate with. This also occurs if the end-user clicks "Cancel" on the Client-Certificate Selection pop-up window. Closing the browser window will reset this behavior.

Central Manager

1. If the IVE system time is changed, the graphs displayed on the Dashboard may be shown incorrectly.
2. Push Config only pushes Web Proxy policies, but not the proxy server configuration. (14949)
3. Push Config is only supported among IVE Platforms running the same version/build. (18236)

Host Checker and Cache Cleaner

1. In this release, Host checker and cache cleaner policies configured at the in an authentication realm are evaluated and enforced at every host checker and cache cleaner update interval. Please note that in the previous release, only Role based HC/CC restrictions and resource policies are evaluated dynamically on every status update.

In some situations, such as connection between the end user machine and the IVE is not reliable, the cache cleaner and host checker status updates may not be received by the IVE within the configured time interval and therefore a user's session might be forced. This happens when host checker or cache cleaner based policy enforcement is configured at the realm or role level.

2. When Cache Cleaner is configured to remove content from specific hosts/domains, the associated web browser history will not be removed. The user may manually delete the entire browser history if they so choose. (17124)
3. If two or more admin or end-user sessions to a specific IVE are initiated from a client, and at least one of them deploys Host Checker and/or Cache Cleaner, the sessions will be affected in unpredictable ways. Symptoms can range from HC & CC being shutdown to loss of role privileges and forced log outs. (15404)
4. If Cache Cleaner or Host Checker is configured to be installed or run for a Realm during pre-authentication, and the user accesses the login page but does not log in, the Cache Cleaner and Host Checker processes (dsCacheCleaner.exe and dsHostChecker.exe) will continue to run on the client. This does not have any adverse effect, and the user may kill the process if they so desire. (13748, 14538, and 14306)
5. The Zone Labs option for Host checker is only supported for Zone Alarm Pro and Integrity products from Zone Labs. Using this option with a different Zone Labs product, may cause the client host check verification to fail. (9075)

6. After uninstalling Host Checker, the Neoteris Program Group may still exist in the user's Start menu. This Program Group can be safely removed. (9057)
7. For certain Windows system services (e.g. `smss.exe` and `naPrdMgr.exe`), Host Checker will fail if the MD5 checksum is used to validate the executable. In such cases, Host Checker is unable to find the path, due to the manner in which Windows loads the process table. This should not be an issue for end-user client applications, such as a personal firewall or virus scanner. (10819)
8. When the security posture of an endpoint changes (e.g. a Personal Firewall starts/stops) there is latency between the time of this event and the corresponding policy changes on the server. For example, a user who is denied access due to the absence of a firewall process will not immediately be allowed access upon starting the firewall. He will need to wait until the policy is refreshed, which is governed by the Host Checker frequency. One way to overcome this is to delete the cookies from the IVE prior to restoring the security posture. (13947)
9. The McAfee Desktop Firewall 8.0 Host Checking method requires that the client be running build 485 or higher. (13444)
10. A Pocket PC user will see compilation errors and will not be able to log in when accessing a Sign-In URL that has Host Checker enabled. (14978)
11. Host Checker configuration will be lost during an upgrade from 3.2 to 4.X. After upgrading to 4.0, the IVE Administrator will need to re-configure Host Checker policies. Upgrades from 3.3+ are supported. (16130)

Secure Meeting

1. If in a meeting on IVE 3.3.1 and the IVE is upgraded during the meeting, if end-users try to reconnect to the meeting after the upgrade, they will be unable to. They will need to start a new meeting. (19048)
2. During failover of a Secure Meeting active/passive cluster, the viewer window may update slower than before. (18969)
3. When disabling the port on a switch in order to simulate a fail-over for a Secure Meeting cluster, clients already connected to an in-progress meeting may not properly reconnect. (18971)
4. During failover of a Secure Meeting active/passive cluster, if the presenter is using a Mac, they will not receive the "disconnected" pop-up. If the viewer is using a Mac, the viewer window may come back up after the "disconnected" pop-up; however, the screen may be black in some cases. (18771)
5. When using two IVEs in a Secure Meeting Cluster, users should always connect to the VIP address to join the Secure Meeting; not the IP address of the physical machine. (17294)
6. Red Hat Linux 9 with Mozilla 1.6 and SunJVM 1.4, has a problem with NTLM authentication when using ISA proxy server to download the Secure Meeting.jar file. This will cause the Secure Meeting client to not download properly. (17445)
7. When sharing individual applications, the "Shared" icon may not appear in the Title bar, depending on the application, whether or not it has a title bar, and whether or not it is sized properly to accommodate the icon. (15070)
8. When using MacOS 10.3.3 and Safari 1.0, if the user clicks "NO" on the certificate pop-up, the Secure Meeting client will not install. If the user wishes to try again and this time click "YES", they must first restart their Safari browser. (17331)

9. Using MacOS 10.2 and Safari 1.0 may yield a Java Null pointer Exception error. Using MacOS 10.3.3+ or using Safari 1.2.1+ should remedy this. (18064)
10. If a MacOS user is presenting, and a Windows user is using remote control, both users will have control of the mouse. When the MacOS user moves his or her mouse, it should pop-up a window to take back over control, but may not. (18672)
11. The Secure Meeting Chat functionality only supports users using the same language encoding (based on web browser) in a single meeting. Using a different encoding than what the person typing is using, will result in mangled text. Meeting invitations are sent based on the language setting in the creator's web browser when meetings are created or saved. (9630 and 9688)
12. When using the Secure Meeting Sharing functionality, some attendees' screens may not update immediately. This is because the screen sharing tool updates pixel by pixel as the applications and/or mouse cursors come into focus. It is recommended, when this happens, that presenters minimize all windows and then restore them in order to update the viewers' screens. (9229)
13. Upon changing a license on the IVE, the Secure Meeting service will be restarted. This will cause any active meetings to be halted forcing all attendees to need to re-join the meeting. (9124)
14. If the user forming a Meeting is using Email invitations and accesses the IVE using a URL which is not the fully-qualified domain name for the IVE (e.g. <https://ive>, not <https://ive.company.com>), the Email invitation may display just <https://ive> in the invitation information and not the true hostname. This may cause Email recipients to be unable to access the link from the email. It is recommended that Administrators configure the "Network Identity" under the Network section in the UI. If configured, Secure Meeting invitations will use that hostname instead. (9381)
15. Windows 98 using Netscape without ActiveX is not currently supported for the Secure Meeting functionality. Windows 2000 and Windows XP with Netscape (ActiveX enabled or disabled) and Internet Explorer 6.0 are fully supported. (8844 and 9297)
16. When searching for invitees for the Secure Meeting, if the search function is set to search an external authentication server (e.g. Active Directory), it will only search those username entries which have been cached. If a user has not yet signed into the IVE, user entry information will not be cached, potentially causing unexpected results during the search. (9038)
17. The Secure Meeting functionality may have erratic behavior if the time clocks on IVEs in a cluster are not synchronized. It is recommended that administrators use the same NTP server for each node within a cluster to keep the IVE times in sync. (9407)
18. When creating a Secure Meeting using the MacOS Safari Web Browser, the organizer may be unable to add more than 250 attendees. (14533)
19. If an attendee begins to log into a meeting as a non-IVE user (that is, goes to the /meeting/<mid> URL), then attempts to log into the IVE with their normal user account, they are unable to. They must first close the browser and then log into their IVE account. Additionally, if the attendee exits a meeting, they must close their web browser in order to join a different meeting. (9829 and 9941)
20. Changing the meeting password on the "Launch" page, will not send an email invitation update. Changing the meeting password from the Meeting Configuration "Details" page, will send an email update. (14404)
21. In some cases the attendee's meeting viewer may not display information or screen updates properly. If this happens, the attendee can safely close their viewer window and re-open it again. (15338)
22. The Secure Meeting Java Client may not run longer than 3 hours for a single meeting. (14530)

23. When presenting, the presenter should consider what access methods are being used by attendees. Dial-up attendees may have bandwidth issues for presentations which redraw the screen or update the screen too frequently. If the presentation saturates the dial-up attendee's bandwidth, remote control and chat functions may not work, as they require sending data back to the IVE over the same, saturated, dial-up link in which they are receiving data. (15203)
24. Signing out of the IVE using the "Sign Out" link will exit the end-user from any meetings which they are currently attending. (14742)
25. On Windows XP, if ActiveX is disabled, an attempt will be made to launch the Secure Meeting client using a Java-based installer, even if a JVM is not installed on the client's PC. (14700)
26. The Secure Meeting functionality must explicitly be enabled at the Role level in order for authenticated users to have access to the Secure Meeting functionality.
27. An attendee using the Secure Meeting Java Client cannot initialize two successive meetings within the same web browser session. The attendee must exit and restart the browser in between meeting sessions. (15228)
28. Secure Meeting attendee will not see the presenter's shared applications if the presenter locks his desktop. (13961)
29. During a Secure Meeting Cluster fail-over, the Chat History will be lost. (15364 and 15364)
30. During a Secure Meeting Cluster fail-over, the Client may take several moments before reconnecting. During this time, the Client may behave as if there is a network outage. (15364 and 15365)
31. If using MacOS, and Remote Control toggling gets out of synch, the Secure Meeting Presenter client will stop presentation updates.
32. Secure Meetings in progress will be stopped if a cluster is created during the meeting.

Windows based Secure Application Manager (W-SAM)

1. WSAM is not qualified on Windows 2000 or 20003 Server platforms.
2. WSAM will not launch on Chinese (simplified & traditional) Win2K if msvcp60.dll, the Microsoft C++ Runtime Library, is missing. (17166)
3. When using the Command-Line W-SAM ("SamLauncher"), the URL entered must contain the prefix https://. (17420)
4. If you have the NCP Auto-select disabled, and click 'No' to the security warning when WSAM is launched, the gapsvc.exe process may crash. WSAM will not launch, and there is no additional impact to the user session." (18681)
5. If an administrator configures W-SAM with NetBIOS support, once a user installs W-SAM, they will be prompted to reboot their PC before continuing. If they do not reboot, W-SAM will not function correctly. (9158)
6. W-SAM supports client-initiated TCP traffic by process name, by destination hostname, or by destination address range: port range. W-SAM only supports those protocols which do not embed IP addresses within the header or payload. The one exception being Passive FTP. W-SAM supports unicast client-initiated UDP as well; however, for full UDP (and ICMP) protocol support, NetScreen recommends using Network Connect (SSL-VPN access).

7. To access a share using W-SAM by hostname, the administrator must explicitly configure the server's NetBIOS name (alphanumeric string up to 15 characters) in the W-SAM Destination Host configuration page. There is no support for wildcard hostnames in this release. (8967)
8. When using W-SAM, users should be reminded that W-SAM will only secure applications which are launched after W-SAM has been downloaded and initialized on the client PC. If an application is running prior to the complete initialization of W-SAM, the application (i.e. the executable) must be restarted in order for it to be secured via W-SAM.
9. Drive mapping through W-SAM is not supported if the users are logging into a domain (when logging into their PC). If this occurs, the user should see one of the following error messages: "No Windows NT or Windows 2000 Domain Controller is available for..." or "There are currently no logon servers available to service the logon request." This is caused by a bug in Windows 2000 which causes domain credentials to be cached. To work around this issue, please have the users log into their PC as a local user or workgroup user. If that is not feasible, the user may do the one of the following (8954):
 - A. At the Command prompt, type: `net use * \\server\share /user:username`
 - B. In Windows Explorer, go to Tools → Map Network Drive, then select "Connect using a different username".
10. When using the Access Control List (ACL) function of W-SAM, administrators should take extra precaution when specifying hosts to allow access to. It is recommended that administrators use the IP address instead of the hostname. If the hostname is required, administrators should try to include additional ACLs with the corresponding IP address or IP addresses for that hostname.
11. When W-SAM is enabled with NetBIOS support, the presence of an installed VPN client may sometimes cause unexpected W-SAM behavior. In many such cases, a common symptom is that NetBIOS connections work using IP addresses but not using hostnames. This issue is generally resolved by releasing and renewing the IP bindings (e.g. using `ipconfig`), but in some extreme cases, might require that the VPN client be uninstalled. (9899)
12. When using W-SAM with 'outlook.exe' configured as a SAM application, users may be unable to modify the outlook settings while running SAM. Users must first end the SAM session, and then may configure their outlook client. An additional workaround is to list the Exchange/Domain controller (AD) servers in the destination host mode. (7770)
13. When using W-SAM on an IVE we recommend installing a trusted SSL server certificate, otherwise users may receive pop-ups telling them it is not a trusted certificate while attempting to launch SAM.
14. When using SAM (both W-SAM and J-SAM), if a user has a program which blocks or hides pop-up windows, that user may exhibit problems waiting for SAM to fully load. A pop-up window alerting the customer to accept the SAM plug-in may be waiting in the background behind the Internet browser. (7054)
15. The application descriptions of the W-SAM window do not wrap properly, so administrators are encouraged to use short descriptions for the applications they have configured for W-SAM.
16. The Secure Drive Mapping function of W-SAM (with NetBIOS Support) may not function if Norton Anti-virus Professional Edition 2003 client is installed. (9384)
17. If W-SAM (with NetBIOS) has to filter traffic by IP address (as opposed to hostname), the entries in the W-SAM Host list must be specified with IP subnets (IP address/net mask) or single IP addresses. Using '*' in the W-SAM Host list will not work. (10728)
18. For users with Netscape web browsers, in order to use W-SAM, they must first download and install an ActiveX plug-in for Netscape.

19. Please note that UDP support in W-SAM is limited to handling only client-initiated unicast connections. Server-initiated UDP connections and support for UDP protocols which embed IP addresses inside the header is not available in this release.
20. If W-SAM is configured in Host Mode, and the Web browser is configured to go through a proxy, W-SAM will not be able to tunnel traffic to the specified hosts. To work around this, users can add the specified hostname to the Web browser proxy exception list. Another approach is to secure all Web browser traffic using Application Mode.
21. IBM Client Access cannot be secured through W-SAM because it is not a Winsock application. Instead, J-SAM may be used to secure this application. (10860)
22. On Win98 clients, W-SAM will create a log file on the Desktop named `samlog.txt`. This file will not interfere with the client machine in any way and can safely be removed after exiting W-SAM.
23. When end-users choose to uninstall W-SAM through the System → Advanced Preferences page, the file `NeoterisSetup.cab` is deleted from the user's system. The effect is that the NetScreen Active-X Installer control will get downloaded again when clientless functionality (e.g. Host Checker, Cache Cleaner, W-SAM, NC, etc.) is invoked. No user intervention is required. (13318)
24. The Browser Request Follow-Through feature does not work as expected when using W-SAM with auto-launch. This feature would typically prompt the user to login after an expired session, and then follow-through to the originally requested URL. This does not work with W-SAM, since W-SAM closes and re-opens the browser during the instantiation process. (10668)
25. In some cases, if W-SAM is uninstalled by an Admin or Power user, a standard user may not be able to access the Internet using their web browser. If this happens, the user can try installing the following component on the PC in an effort to work-around this issue:
http://download.microsoft.com/download/vc60pro/Update/1/W9XNT4/EN-US/VC6RedistSetup_enu.exe (12820)
26. Currently there is no automatic discovery for file shares in W-SAM.
27. If the W-SAM "Auto-Upgrade" option is disabled for a Role, users of that Role who do not yet have the W-SAM client installed will not be able to install the client. (15447)
28. When W-SAM detects the presence of certain LSPs (Layered Service Providers) on the client PC, it will not launch or install. This behavior is currently limited to the new.net and Webhancer LSPs, installed by certain SpyWare applications.
29. To run Citrix NFuse through WSAM, you must define a Caching rule to cache `launch.asp` files. For example, configure resource policy to "`<server name>:80,443/*launch.asp`" and the Caching Option to "Cache (do not add/modify caching headers)".

Java Secure Application Manager (J-SAM)

1. Outlook 2003 is not supported with J-SAM. (8251)
2. In order to use J-SAM with HOBLink on Mozilla 1.6, users must make sure that the cookie settings in their browser are set to "Enable all cookies". (18963)
3. With the Framed Toolbar, J-SAM Auto-Launch by URL does not work in this release. (18916)
4. When a user clicks on "No" when the session mgr applet downloads but later tries to start the session manger manually, sometimes the session manager applet download does not appear. The work around is to kill the browser and start over.

5. When J-SAM downloads onto a client, if it encounters problems, no error may be reported. This silent failure may cause problems with the J-SAM functionality for that client. (3471 and 9100)
6. When using Netscape, users who close J-SAM may experience Netscape freezing on them. To work around this problem, users can add the following line to their java.policy file (9326):

```
grant { permission java.security.AllPermission; };
```
7. J-SAM does not automatically launch when Embedded Applications are set to "Auto" in the Citrix NFuse Classic Administrator console. In these cases, it is recommended that J-SAM be configured to automatically launch after login or else end-users must manually launch J-SAM before using Citrix NFuse.
8. Multiple Secure Terminal Access sessions may not work correctly if the login fails on one of the sessions. (12253)
9. Due to a buffer overflow issue in Windows 98, J-SAM cannot support more than 10 simultaneous applications when launched from a Windows 98 client. (12515)
10. On Windows XP, an attempt will be made to launch J-SAM even though a JVM is not present on the client's PC. (13158 and 14700)
11. With Citrix Program Neighborhood, application discovery (with a specified server), is supported; however, if one attempts to use the server discovery feature, which does not work through the IVE, and then attempts to use the application discovery again, then the application discovery will fail. The workaround is to restart Citrix Program Neighborhood. (8665)
12. J-SAM will create two log files the end-user's PC named `netscreen.log0` and `netscreen.log1` in `c:\windows\java\` or `c:\winnt\java\` (for MS JVM) or `c:\documents and settings\\` (for SunJVM). Each log may grow up to be 10MB and contain Java runtime messages which may be important during troubleshooting. They do not contain any application or other sensitive user data. (15808)

MacOS Java Secure Application Manager (J-SAM)

1. When using J-SAM for the MacOS with Safari web browser, once a user has launched J-SAM, and then is no longer authenticated through the IVE either due to a session timeout, idle timeout, or by signing out, the user must quit Safari and re-launch it to be able to run J-SAM again. (10766)
2. When using J-SAM for the MacOS, if the IVE gets disconnected while running an application, the J-SAM status field may not immediately indicate that the session is inactive. The status indicator updates every few minutes. (10865)
3. First-Class Citrix NFuse integration is not available on MacOS. (10780)
4. When using J-SAM for the MacOS, three files may be left behind in the `~/Library/Application Support/Neoteris` directory. These files are `libAuthKit.jnilib`, `Neoterisun.jar`, and `SessionManager.log`. These files may safely be removed after exiting J-SAM. (10638)
5. The "New Window" button on the Mac J-SAM client does not work correctly and may inadvertently close the J-SAM client window. This will be fixed in a future release. (15446)

Network Connect (NC)

1. Access Control Policies do not accept multiple ports with the comma-separated notation (e.g. 20, 23). (18523)
2. When Network Connect is employed in a clustered configuration, there may be an issue in how IP Address Pools and multiple filters are handled. If users are not able to connect after the upgrade, the admin should split the pools in such a way that the pools actually reflect the split IP range that would yield the result of applying the filter.

As an example, if the IP pool is specified as x.y.z.1-254 and the filters are x.y.z.0/25 on one machine and x.y.z.128/25 on a second machine. Splitting the IP Address Pools as x.y.z.1-127 and x.y.z.128-254 and not modifying the filters will remedy the problem. This issue will be addressed in a future release. (19958)
3. Split-tunneling will not function through Network Connect if the client has one or more pre-existing static routes. (19022)
4. If using NCInst.exe (Stand-Alone NC Installer), existing pre-4.1 Network Connect must be uninstalled first before using the 4.1 installer. (18837)
5. Network Connect will not work if the physical connection is a modem dial-up, and there is a connection entry which accepts incoming modem connections. (16908)
6. NC through a proxy is supported in this release; however, the proxy configuration must use an IP address and not a hostname. (18709)
7. The UI for specifying the NC Client IP pool requires IP addresses to be entered as ranges with a maximum of 254 addresses per range. Each range is specified on a single line. To specify a larger pool for a specific role, the IVE Admin must enter multiple IP address ranges. In the future, we will mitigate this by allowing NC IP Pools to be entered with a more standard syntax (e.g. IP/Net mask). (6378)
8. Client IP pool configuration is synchronized among all nodes in a cluster; however, administrators may configure each IVE to use a certain subset of the global IP pool. This is configured in the Network Settings → Network Connect tab, using an IP filter match.
9. Network Connect may not install properly if users are running pop-up blocker software. In some instances, the symptoms may include unusually high CPU usage, and will require that all browser sessions be terminated.
10. On Windows XP, regardless of NC Split-Tunneling configuration, the local subnet route will remain in the end-user's routing table allowing them local access. (12221)
11. Users with only "Guest User" privileges will not be able to run Network Connect. Furthermore, Guest Users cannot uninstall Network Connect. Any attempt in doing so may only partially uninstall Network Connect and could leave some files behind, resulting in a corrupted Network Connect installation. (13772)
12. Network Connect cannot be run with "Limited User" privileges. (13493)
13. Network Connect is available to the IVE Admin as a stand-alone executable (NCInst.exe). This executable can be installed on the client and started by logging into the IVE and invoking Network Connect. If the user attempts to install NCInst.exe on a client that already has the same version previously installed, multiple error pop-ups with the text "Error opening file for writing..." will occur. The user can safely click on Ignore on these pop-ups and NC should work after the installation has completed. (13922)

14. Network Connect ACLs are only evaluated at the time when the NC session is launched. If the ACLs are changed after a session is launched, or if an ACL has dynamic conditions (e.g., time of day, Host Checker variable) which change during the session, then these rules will not be taken into effect. If Administrators want to apply the new NC ACLs, they will need to force the user to log out and have the user re-login and launch NC again. (9046)
15. When system locale defaults are modified on non-English installations of Win2K or WinXP, NC will not be able to set the proper modem initialization string and will fail to connect. (14044)
16. Network Connect has successfully been tested with VoIP applications; however, network latency and other network performance issues caused by various external factors independent of the IVE can impact how well VoIP works over Network Connect.

Clustering Issues

1. In an Active/Passive scenario, using the default cluster/network configuration, under heavy load, Administrators may see the VIP switch back and forth among the two nodes every 6 to 8 hours. If this occurs, the Administrator may increase the ARP timeout value from the default 5 seconds to 10 seconds.
2. When using Virtual Ports in a non-cluster configuration or when using an Active/Passive cluster configuration, and then creating an Active/Active cluster, the joined nodes will lose their Virtual Port IP address information and they will need to be manually reconfigured using unique IP addresses.
3. When an Active/Active cluster is converted to an Active/Passive cluster, Virtual Port configuration will be copied to the backup cluster node from the node which the Admin is making the change. This copy will cause Virtual Port configuration on the backup node to be overwritten with the master's Virtual Port configuration.
4. In the case of a fail-over (both in active-passive and active-active configurations), all transactions currently in progress (such as telnet or SSH sessions or large file downloads/uploads) need to be restarted after the fail-over; there will not be a seamless fail-over for on-going transactions using sockets (except for HTTP requests or non-stateful connections).
5. When an IVE in an active/passive cluster loses network connectivity, it automatically moves in to a temporarily "Disconnected" mode. In this mode, the IVE will relinquish a cluster VIP (if applicable), and stops servicing end user requests for a few minutes. The IVE determines the status of a network connection based on both a) the carrier signal and b) connectivity to the Gateway by sending an ARP request. In other words, if the IVE cannot reach the internal/external gateway, then it temporarily moves itself into a "Disconnected" mode. Therefore, we strongly recommend that you configure a highly available network gateway on the IVE, preferably using VRRP based Primary/Backup Gateway configuration. When the network connectivity is restored, the IVE would automatically join the cluster.
6. In an active-passive Cluster Pair fail-over situation, the active IVE sends a Gratuitous ARP request in the network reflecting the new owner for the cluster virtual IP address (VIP). Some switches and firewalls may not respond to Gratuitous ARP requests and therefore still might try to contact the offline IVE. The workaround is to manually clear (disable) the ARP caches on these external devices or configure an active-active IVE cluster configuration using an external load-balancer.
7. If you are deploying an active-passive cluster in the DMZ mode, please make sure to configure/enable the external interfaces on both machines before assigning an external VIP to

the cluster.

8. IVE system log messages are not synchronized during a Join Cluster operation even when the “synchronize log messages in a cluster” is enabled. The log messages are synchronized across the IVEs in a cluster when all the machines are in “Enabled” and Status “OK” mode.
9. Changing the networking settings of an enabled cluster member (in particular, network routes and DNS settings) does not work in some rare cases. We recommend that you disable the cluster member, change the networking settings, and then re-enable the cluster member in this scenario.
10. The “multicast” synchronization method for Multi-Unit Clustering should be avoided when the IVE is under heavy load, either from heavy traffic or a load test. During these periods, unicast is the preferred method of cluster synchronization.
11. When creating an Active/Passive cluster, the administrator must enter values for the *internal* and *external* interfaces. This is not a mandatory field, but is required for Active/Passive clustering.
12. The minimal downtime cluster upgrade functionality is only supported AFTER the cluster has been migrated to version 4.0. Subsequent upgrades will then be able to take advantage of this functionality. Note: The minimal downtime cluster upgrade functionality is only available with Central Manager and in clusters of two nodes or more.
13. In a Multi-Unit Cluster consisting of three nodes or more, there are three configurable options for setting the synchronization type:
 - **Unicast** – The IVE sends the same message to each node in the cluster
 - **Multicast** – The IVE sends one message to all cluster nodes on the network
 - **Broadcast** – The IVE sends one message to all machines on the network but non-clustered nodes would drop this message, as it was not intended for them

In the case of a 2-unit cluster, the IVE uses **Unicast** as the synchronization type. This option is not configurable.

In the case of a multi-site cluster, the IVE uses **Unicast** as the synchronization type for inter-site (different subnets) synchronization. The configured transport setting on the clustering properties page is then used intra-site (same subnet) synchronization.

14. Clustering is not supported when an IVE is configured to have the same subnet for both the *internal* and *external* interfaces.
15. In an Active/Passive cluster, if the nodes lose communications with each other but not to their respective gateways, then it is possible for each IVE to activate the VIP. This can cause a problem since the upstream switch/router/firewall will potentially receive two gratuitous ARP requests. The second ARP request will override the first. If the two nodes regain communications afterwards, one node will deactivate its VIP. If this node is the one which send the second gratuitous ARP and is therefore in the switch/router/firewall’s ARP cache, end-user connectivity to the VIP could be lost as the ARP cache will be redirecting requests to the wrong MAC address (wrong IVE). To resolve this situation, the IVE Administrator may click on the “Failover VIP” button in the Clustering UI. This will automatically fail the VIP over from the active node to the backup node and thus send a new (and only one) gratuitous ARP request out. To prevent this from happening, IVE Administrators are encouraged to ensure each IVE node has constant communication with each other and the network segment(s) between them are never severed.

Sun JVM/Code-Signing Certificates

1. When using Microsoft XP, the IVE will skip the JVM check and will always assume a JVM is installed. Therefore, the IVE will attempt to intermedate the Java applet. (17737)
2. IBM Host on Demand is not supported through the IVE rewriter because the Java applet performs an MD5 checksum upon execution. Alternate methods to secure this application are J-SAM or W-SAM.
3. When importing a new production certificate for Sun JVM, the end-user needs to disable caching in the Java Plug-In in order for the newly imported code-signing certificate to show up. Please refer to the Administration Guide for instructions on disabling the Java Plug-In cache.
4. If users delay in responding to the web server security warnings then Java applets may not load. This includes the Session Manager and the Secure Terminal Access applets. As a workaround when the end-user encounters the web server certificate dialog, the end-user should select the "Always Trust" button. Once the user selects "Always Trust", the dialog will not appear and the applets will load without a problem. Note: Due to a built-in timeout in the Java Plug-In, if the user waits too long to select the "Always Trust" option, the applet may not load properly. (8396)
5. Due to a bug in Sun JVM, when users close their web browser window, it may seem to hang or crash. To prevent this problem, users can make the following changes to their Java plug-in: Open the Java plug-in console (Control Panel → Java Plug-in) then under the Advanced tab, type: `-server -xint -xfuture` in the Java Runtime Parameters box and press Apply. Close the Java Console and Restart the web browser.
6. With Sun JVM 1.4.2, if caching is enabled, WRQ 6.0 will not load properly. (14008)
7. The policy tracing logs for when code signing certificates are used to re-sign Java applets is not accurate. Use the Simulation tool instead for troubleshooting purposes. (17411)

I-Mode Support

1. The following phones/browsers are not supported for I-Mode client access:
 - N211iS
 - N502it
 - N252i
 - N504iS
 - N251iS
 - D505i
2. The OpenWave Simulator only supports making an SSL connection if the server, or in this case the IVE, signed by one of the following RootCAs: CyberTrust, Certicom, Diversinet, Entrust, GlobalSign, and VeriSign. (18041)

Customizable Sign-In Pages

1. To make sure that the New Pin and Next Token pages are customized for SoftID authentication, the administrator should copy the file `NewPin.shtml` to `GeneratePin.shtml` in the `softid.zip` and upload the modified zip to the IVE for use by the custom sign-in page. (18398)
2. When uploading the `kiosk.zip` file for a customized sign-in page, the administrator may receive some validation errors. Administrators should check the "skip validation" option to bypass these errors. (18562)

3. The total combined size of all uploaded customizable UI zip files cannot exceed 7.5 MB. (13906)
4. The new 4.X sign-in pages now offer additional customization for labels and informative text. By default, the text strings are in English. Administrators supporting non-English users may need to configure the sign-in pages to provide localized text labels. This can only be done on a per-sign-in page basis. For multi-language support, Administrators must configure different sign-in pages for different locales. For further customization, Administrators may upload their own customized sign-in pages using the Template Toolkit. Please contact NetScreen Support for details (<http://support.netscreen.com>). (13605)
5. When creating customizable sign-in pages, Administrators should remember to save them as UTF-8. (17211)

Password Management

1. AD Domain Controllers synchronize security policy settings every 5 minutes. If a change is made to the security policy, for example "minimum password length", it could take up to 5 minutes before that change has propagated to all Domain Controllers. This also applies to the Domain Controller which the change was originally performed on. For more information, please refer to:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/lpe_overview.asp. (9861)
2. Changing passwords in AD requires LDAPS support on the AD server. This can be enabled by importing a valid certificate/key into the "Personal Certificate Store" using the MMC and selecting the "Certificates" snap-in. In some situations, an external key and certificate may need to be imported. In this case, the key and certificate should be combined into one file, using PKCS #12 or PFX format. The imported certificate must be signed by a trusted CA.
3. For a list of what Password Management functions are supported, for the various platforms, and for a list of attributes, please see the Password Management Technology Integration Guide ("TIG") available in the Product Documentation of the NetScreen Support site (<http://support.neoteris.com/>).

FIPS

1. If you choose to replace an administrator card using option 10 in the serial console after upgrading an Access Series FIPS appliance, the Security World is modified to use the new administrator card. If you then choose to perform a "rollback," the new administrator card will not work. This is because the "rollback" reverts to the original Security World, which is not yet configured to use the new administrator card. To use the new card, you must use option 10 on the serial console once again. (9841)
2. Access Series FIPS does not support automatic time synchronization across cluster nodes. We suggest that you configure your cluster nodes to use the same NTP server - so they are synchronized. If the cluster nodes are not synchronized, time based features such as Secure Meeting, will not function properly. (9407 and 9577)
3. If the HSM module switch is set to I on a FIPS enabled Access platform, the machine is in "initialize" mode. A reboot during this time will reinitialize the server key and invalidate the server certificate that is currently loaded. Administrators should be sure to leave the switch at O during normal operations (as per the instructions on the serial console and documentation). (12476)

Pass-Through Proxy Issues

1. The Lotus iNotes welcome page is not rewritten if the IVE is intermediating the content through Pass-Through Proxy. (9236)
2. Pass-Through Proxy URLs must be hostnames. Paths off hostnames are not supported. (18754)
3. NetScreen strongly recommends Administrators not mix Pass-Through Proxy Port and Host modes.
4. Siebel7 is not supported through Pass-Through Proxy. (7487)
5. Using Mozilla with Pass-Through Proxy (with the IVE port configuration), the IVE may invalidate the user session causing the user to have to login again.
6. Pass-Through Proxy is not supported on Netscape 7.0, but is supported on 7.1. (7290)
7. When using Lotus iNotes through Pass-Through Proxy, if XML rewrite is needed, administrators are encouraged to either enable XML rewriting in the Pass-Through Proxy configuration, change the default cache rule from 'No-Store' to 'Unchanged', or add a new cache rule with the IP/hostname of the Lotus Server and a path of * and value 'No-Store'. (9164)
8. When using OWA through Pass-Through Proxy, if a user replies to or creates a new email, the recipient may receive a JavaScript error if they view the email through their Outlook client. (9233)

Internationalization Issues

1. Internet Explorer may truncate the Japanese filenames if they are too long. Additionally, some Excel files cannot be saved. More details can be found about this non-IVE issue at: <http://support.microsoft.com/?kbid=816868> (14496)
2. The timestamp function of the IVE may not be in the same format as what is expected when working with the Japanese user UI. The formatting for the IVE is as follows: *hh:mm:ss (am | pm)* and *month/day/year*. (7626)
3. When using Netscape 4.7 and the Japanese language setting, the default font may incorrectly display characters and words on the End-user UI page. If this happens, the font setting may be changed by going into the Netscape Preferences, and going into the Fonts section. In there the user can select "Netscape should override the fonts specified in the document". (7945)
4. With Secure Meeting, when using a Japanese language setting on the IVE, Meeting Invitations will be sent out using the Japanese template. If these invitations are sent to Yahoo or Hotmail or other web-based email accounts, some characters or possibly the entire email may not display correctly. (15615)
5. Special characters such as ①、 I、 ¥、 and ~ are not supported for filenames for UNIX Servers. (14529)
6. Japanese characters are not supported in naming Authentication Servers. (7924)
7. Filenames using 5c characters such as 表 and 工 will be corrupted and cannot be deleted from UNIX servers. (14348)
8. When using the Japanese language with OWA, the UI will be corrupted when the "Reply", "Reply All", and "Forward" buttons are clicked. (15323)
9. Downloading files through the IVE with filenames of length 18 to 25 characters may not work. Files with longer or shorter filenames are OK. (14496).

File Browsing Issues

1. If administrators deny access to a file server by specifying the IP address, users can still browse to that server if they specify the server and the file share by name and are able to provide the valid credentials. To avoid this, administrators should configure both the IP address and hostname in their file browsing ACLs.
2. The IVE attempts to connect to Windows file shares on port 445 first. If port 445 is blocked, the IVE may seem to hang for ~20 seconds, after which it will reconnect to the file share using ports 138 and 139. Administrators with a firewall between the IVE and a file server are encouraged to open port 445 up from the IVE to the file share servers to avoid this "hang". (13394)
3. NFS file browsing requires an NIS server to first be configured on the IVE in order to work properly. (14594)

Cache Cleaner

1. Cache Cleaner will attempt to verify the session during its cleaning phase. During this time, a connection may be opened from the process back to the IVE. (10456)
2. If Cache Cleaner is configured for a realm, users may be unable to log into the IVE if they cannot install the Cache Cleaner application on their PC. Administrators should take this into consideration when configuring realm authentication policies, role restrictions, and resource policies. (10822)
3. If Cache Cleaner is configured to "load" for a realm, users who are not using an ActiveX enabled web browser may still log in. To work around this limitation, IVE administrators may configure a client pre-authentication assessment policy for the realm. (10697)

Netegrity

1. Netegrity Authentication will fail if either Max Session Timeout or Idle Timeout options are not set on the Policy Server realm. (18759)
2. When using Netegrity as an Authentication server for the IVE, users must access the IVE using a fully-qualified domain name (e.g. ive.company.com). This is required because the Netegrity SMSESSION cookie will only be sent for the domain it was configured for. If users access the IVE using an IP address, they may get an authentication failure and prompted to authenticate again. (8374)
3. Users with valid SMSESSION cookies that are automatically logged in to the IVE will always have their roles merged if they are mapped to multiple roles. These users will not be prompted to select their desired role from a list of roles which they have been mapped to. (13651)
4. Netegrity SSO users with expired SMSESSION cookies who access the IVE homepage using the sign-in URL (e.g. /) will be prompted with an IVE login page, rather than get redirected to the configured Netegrity redirect URL. (15247)

Miscellaneous issues:

1. LDAP group mapping will fail if using the <USER> parameter and users are signing-in using the DOMAIN\USERNAME syntax. (17706)
2. When upgrading to 4.1, and using a temporary license generated for IVE 3.3, after the upgrade, the license time remaining may show incorrectly. To resolve this, please contact the Support department. (17918)

3. In some locations throughout the Admin UI, drop-down select boxes may disappear during navigation through the left-hand hierarchical menu system. To make these select boxes reappear, simply move your mouse off of the left-hand menu. (17934)
4. Importing a configuration will not import the license keys in this release, unless you have no license keys applied already. If license keys exist already on the appliance, the configuration will be imported, but the license keys will not. (18653)
5. By default, all access policies are closed, unless explicitly opened by a defined policy (e.g. 'allow' for '*').
6. Due to comprehensive changes in the Access Management model, the IVE 3.X "Import Users" functionality is not available in this release. (14940)
7. The acceptable range of Session Time Warning values has changed in IVE 4.0. If previous values are no longer applicable, the administrator must reset them after the upgrade. The best way to check this is to bring up the Default Roles Options page, make any modifications as necessary, and Save Changes. (14028)
8. The IVE only supports Crypt/MD5 password hashes for NIS authentication. (14228)
9. Steel-Belted Radius is not supported with the IVE when using RSA SecurID 5.0.1. (13754)
10. Due to lack of support in Microsoft Windows for certain SSL libraries, the IVE should be configured to use non-optimized NCP for Windows NT, Windows 98 SE, and Windows ME clients when using W-SAM, Network Connect, or Secure Meeting. (14519)
11. When defining access policies, the Administrator must explicitly list each hostname and/or IP address. The policy checking system will not append or use the default domain or search domains in the IVE network settings. (13685)
12. PowerPoint files may not display properly with Office 2002 in Internet Explorer on Win2K. To work around this, administrators should have their end-users to install Office 2002 SP1 and SP2. (14101)
13. The ARP Ping Timeout value in the Network Settings should always be greater than 0. (13599)
14. Port numbers are ignored if you specify a generic rule for all protocols. They are only used if you specify a rule specifically for "TCP" or "UDP", since port numbers do not have any meaning for other protocols. (14567)
15. Multiple sessions from a single client to the same IVE might cause unpredictable behavior and is not supported. This is primarily due to the pre-authentication mechanisms which might conflict between sessions. This caution also applies to situations where an end-user and admin session to a single host are occurring simultaneously. (14341)
16. The following URL contains a list of characters which not supported for filenames or folders for Samba Servers: <http://support.biglobe.ne.jp/help/faq/charactor/izonmoji.html> (14529 and 14348)
17. Resource Policy evaluation for J-SAM, W-SAM, Secure Terminal Access, Web, and File resources are not evaluated for already-established "in-flight" connections - they are only evaluated at the beginning of a transaction. A transaction is defined in the following way: Web - HTTP Request, Files - Upload/Download of a file or listing of shares/files, SAM - Beginning of a new connection to a backend resource. Support for this will be added in a future release. (14476)
18. Accounts which are used for both administrator and end-user access to the IVE may conflict if they using the same username and authentication server. This may cause one another to get forced out of their IVE session when the other logs in. (13981)

19. Only attributes which are referenced by Role Mapping rules may be used for Resource Policy evaluation. (14524)
20. The IVE only supports sending SNMP v2c traps. If the SNMP trap manager client does not support SNMP v2c, the traps may not be received and displayed properly. Results may vary based on client software.
21. There may be some inconsistencies between the IVE Enterprises SNMP CPU/Memory utilization objects and those used in the UC Davis MIB. (14612)
22. Some SNMP MIB Browsers, such as Getif, may not properly display some MIB-II objects. Other MIB Browsers, such as MG-Soft or SNMPWalk (with the -v 2c option) can be used instead. (15209)
23. When using 168-bit encryption on the IVE, some web browsers may still show 128-bit encryption (the gold lock on the browser status bar) even though the connection is 168-bit. This may be a limitation of the browser's capability.
24. The Web Proxy feature may only be configured for HTTP and HTTPS requests. When the Web Proxy feature is enabled, administrators should make sure to turn off HTTP proxy authentication (407 based) on the Web proxy. The IVE does not respond to 407 based authentication challenges from the Web proxy.
25. If you use RSA ACE/Server authentication and change the IVE IP address, you must delete the node verification file on the IVE for ACE/Server authentication to work. Also, make sure to uncheck the "Sent Node Verification" setting on the ACE/Server for the IVE.
26. Lotus iNotes in offline mode is not currently supported. (9889)
27. On some Administrator Console pages, changing one or more parameters causes multiple log messages to appear in the IVE system log that indicate that all the parameters are changed. However, this occurrence does not result in any incorrect behavior.
28. When upgrading from a 2.x release, the Web Proxy function may be disabled even if it had been enabled prior to the upgrade. Administrators who want this function to be enabled must manually re-enable it after upgrading. (7965)
29. When using Netscape, users who close Secure Terminal Access (STA) may experience Netscape freezing on them. To work around this problem, users can add the following line to their java.policy file: `grant { permission java.security.AllPermission; };`
30. OWA and Lotus iNotes both have various problems with opening and saving email attachments. Many of these issues are not specific to the IVE, but a problem with OWA and Lotus iNotes themselves. Please refer to Appendix B in the Admin Guide for additional details as well as IVE caching rules which can be configured to help overcome these issues.
31. When using Secure Terminal Access (STA), the user must first click in the Java Applet window to set the focus. Then, the user may begin typing and using the Telnet/SSH functionality. (6604)
32. When using an external load balancer and accessing J-SAM, W-SAM, Network Connect, or the Online Meeting functionalities, persistence must be employed on the load balancer. This persistence should be based on Source IP or Destination Source, depending on the load balancer being used. (9004)
33. When using Internet Explorer 5.5 or 6.0 and compression, HTTP objects will be cached, regardless of the object's cache settings. This is not a limitation of the IVE, rather an issue specific to Microsoft Internet Explorer and HTTP compression. For more details, please visit: <http://support.microsoft.com/default.aspx?scid=kb;en-us;321722>

34. When using Siebel 7.5 through the IVE, the user may see ActiveX warning pop-ups. To stop these pop-ups, the user must change their browser security settings. For IE, this can be done by going to Tools -> Internet Settings -> Security -> Custom Level -> and enabling each of the ActiveX items listed there. (8247)
35. The IVE web browsing function does not support URLs more than 159 characters in length, including extensions, such as “.html”. (7248)
36. Some menus of Siebel7 are not working. This only is a problem for users using applications which are menu dependent. With Siebel7.5, the menus work as expected. (9442)
37. WRQadmin uses ‘.’ notation in some of their URLs. This is disallowed by the IVE, due to security reasons and may cause erratic behavior within WRQadmin. (9623)
38. The IVE does not support the import of Intermediate Server certificates; however, VeriSign and Comodo are supported internally. (5855 and 9410)
39. The NetScreen toolbar should be disabled to view OWA pages with Safari browser. If the NetScreen toolbar is enabled, the Inbox may show up blank until the page is refreshed once. To work around this, the toolbar can be disabled in the Roles → UI Options tab. (9778 and 13739)
40. Even though you enter the password to archive users and system config files, this password is disregarded on the import.
41. If you enter a server for selective rewriting, and expect it to be accessed with and without the domain suffix, please enter both entries. If you have entry foo.company.com and try accessing foo, the response will not be served via pass through proxy. Similarly, if you have an entry for foo and try accessing foo.company.com, the response will not be served via through selective rewrite.
42. When switching from Optimized NCP (NetScreen Communication Protocol) to Standard NCP, or vice versa, all NCP- Based communications must be restarted. This includes W-SAM, Network Connect, and Secure Meeting.
43. On Win98 clients, when Auto-Select is enabled for the NetScreen Control Protocol (NCP), the Optimized NCP will not be used. This should not cause any visible changes to the user experience. (10881)
44. When using OWA 2003, if the IVE has Forms-based Authentication enabled, the OWA 2003 login credentials are cleared upon logout; however, if this is disabled, the login credentials will not be cleared. (10821)
45. When using OWA 2003, the Administrator should ensure that the OWA server has only NTLM or Basic Auth enabled, not both. (15098)
46. When importing a custom HTML help file for end-users, if the file is encoded in a different language, for example Shift_JIS it must be converted to UTF-8 before it is imported by the IVE administrator. (10839)
47. When using Microsoft NetMeeting with W-SAM, hosting a meeting is not supported. To join a meeting using Win2K, there are now problems; however, when using Windows XP, application sharing does not work as expected. In order for Windows XP users to work around this sharing issue, they must first check the configuration box “Only you can accept incoming calls”.
48. Upgrading the IVE clears all statistics; however, if the log system is configured to log statistics every hour, they will still be available in the log file, even after the upgrade. (2901)

49. When an Admin IVE session is timed out (due to inactivity or by reaching the hard limit), the “sign in again” link may take the Admin to the end-user sign in page instead of the Admin sign-in page. The Admin can simply type the Admin sign in URL (e.g. /admin) to sign back into the IVE Admin Console again. (15268)
50. The Session Timeout Warning is only supported on web pages which are viewed through the IVE (i.e. rewritten web pages) and on the IVE homepages themselves. The warning will not apply to pages viewed through Pass-Through Proxy, W-SAM, J-SAM, or Network Connect. If not needed, we recommend that the Session Timeout Warning feature be disabled to minimize confusion for users of W-SAM, J-SAM, NC, and Pass-Through Proxy. (14834 & 14831)
51. After upgrading to 4.0 from 3.X, the Admin UI may be using a cached style sheet. Pressing CTRL+F5 on the web page should resolve this caching issue. (14934)
52. When the Administrator reduces the maximum size of a log file on the IVE, if the log is already larger than the new maximum size, the log size will show a larger % value on the Status page under “Logging Disk % full”. As soon as another log message is generated for that log file, the current log file will be archived and a new log file will be created. The display will just be momentarily incorrect due to this change. (15054)
53. If two separate web browser instances are accessing different versions of the IVE, then the browser may prompt the user to reboot their PC after the NeoterisSetup.cab has been downloaded. Upon closing all browsers and logging in again, the prompt will no longer be displayed. (14919)
54. Pop-Up Blockers may cause problems with any IVE functionality which uses a pop-up, for example J-SAM, File Uploads, Help, or if using the Admin Console, the IVE Upgrade progress window, Dashboard configuration page, and Server Catalog. (14873)
55. The Debug Log troubleshooting functionality should only be enabled after consultation with NetScreen Support. (15494)
56. The IVE has an Automatic Version Monitoring feature which notifies NetScreen what version of software the IVE is running and the Licensed Company via an HTTPS request from the Administrator’s web browser upon login to the Admin UI. NetScreen collects this data to be able to inform customers about critical security patches they may need. Administrators can enable/disable this functionality by logging into the Admin UI and going to the Maintenance → System → Options menu. NetScreen strongly recommends that Administrators keep this setting enabled.
57. User and Admin session timeout log messages may show the user’s Realm Type (User or Admin) rather than the actual Realm name. (15049)
58. Users who access Lotus Sametime Connect directly and need to access it through the IVE should first remove the ActiveX control from their Internet browser’s cache. (14770)
59. To use OWA or Lotus iNotes with Internet Explorer with Compression enabled on an A5000, Smart-Caching must be enabled. More information can be found at the following locations (15383):
 - <http://support.microsoft.com/default.aspx?scid=kb:en-us;825057&Product=ie>
 - <http://support.microsoft.com/default.aspx?scid=kb:en-us;312496&Product=ie>
 - <http://support.microsoft.com/default.aspx?scid=kb:en-us;327716&Product=ie>
60. When using iNotes with Cache-Control: No-Store, the browser may appear to hang for a few seconds under Windows XP and pages may appear to load slowly under Windows 2000. (15489)

Supported Platforms

Please see the “Supported Platforms” document posted on the NetScreen Support Site (<http://support.neoteris.com/>) under “Production Releases” for a current list of supported platforms (operating system/browser combinations). Note that some platforms do not completely conform to HTTP standards, so we have tested IVE functionality with the most common operating system/browser configurations used for the specific functionality. The “Supported Platforms” document summarizes the functionality tested, our testing model, and the supported platforms for the Neoteris IVE.

To report a bug or for support information, please email us at:

help@support.neoteris.com