

Neoteris IVE 3.3.1 Patch 1 Release Notes

Build #5847

1. New Features in 3.3.1 Patch 1	1
2. Known Issues and Limitations Fixed in 3.3.1 Patch 1 Release.....	1
3. IVE 3.3.1 Patch 1 Release Upgrade Considerations	2
4. General Notes	3
5. Known Issues and Limitations	3
6. Supported Platforms	20

1. New Features in 3.3.1 Patch 1

- **Framed Toolbar**

As an alternative to the standard toolbar a framed toolbar option is available. This option can be enabled at the group level. The framed toolbar appears as a fixed frame above the user's browser window and, like the standard IVE toolbar it provides one-click access for logging out and accessing the IVE home page and end-user help. The framed toolbar works with well-behaved applications such as OWA and iNotes but may not work with all web applications.

- **Stand-alone Network Connect Executable**

To provide added flexibility and control with the deployment of Network Connect, this application is now available as a Windows executable (NCInst.exe) in the release package and is available to IVE administrators for download from the Network Settings → Network Connect page. This executable can be packaged and distributed to client machines using standard software distribution tools.

2. Known Issues and Limitations Fixed in 3.3.1 Patch 1 Release

The following issues have been resolved in 3.3.1 Patch 1 Release:

1. Improvements to the Citrix ICA rewriter to check for extra “/” characters. (15437)
2. Improvements to W-SAM to better handle the uploading of large files. (1571)

The following issues have been resolved in 3.3.1 Release:

3. When using OWA, filenames for attachments (stored in the HTTP Content-Disposition header) longer than 155 characters (36 for Japanese, due to escape characters) are now supported. (10789)
4. On MacOS, the J-SAM log file `CurrentSessionManager.log` has now has a file size limit of 10MB. Additionally, the previous J-SAM session will be archived to `PreviousSessionManager.log`, which also has a file size limit of 10MB. If, during the session, the `CurrentSessionManager.log` reaches 10MB, it will be archived immediately rather than waiting until the next session. (10631)

5. The presence of a carriage return in the description field of a J-SAM application no longer causes J-SAM to not load properly when launched on the end-user's PC. (10701)
6. During cluster synchronization nodes which have existing host mapping configuration will no longer be overwritten, but instead the new mappings will be added to all nodes within the cluster. (12475)
7. J-SAM using Sun JVM is now supported on Japanese Windows; however, the registry changes made for Outlook are not reverted back when J-SAM exits, as they are when running J-SAM on English Windows. (10621)
8. Network Connect on French Windows now installs properly. (12503)
9. Password Management now functions as expected when using an external group lookup server. (12442)
10. Enabling Alarms in iNotes 5.0.10 no longer prompts the user with the warning "A script on this page is causing Internet Explorer to run slowly. If it continues to run, your computer may become unresponsive." (8308)
11. OWA 2003 is now supported using Pass-Through Proxy when configured either using DNS (hostname-based) mode or port mode. (10873)
12. In some cases, specifically with Windows 98 and Windows ME, the W-SAM LSP module may be loaded in a different order than anticipated. If this happens, W-SAM may not function properly. To adjust the ordering of LSP modules within the system, `sporder.exe` may be used. Known issues of this type have been fixed in this release. (12456)
13. Cache Cleaner now removes downloaded PowerPoint files (.ppt) from the IE content cache. (13182)

3. IVE 3.3.1 Patch 1 Release Upgrade Considerations

- The legacy authentication mode (pre 3.0) will be supported through IVE release 3.3.1 Patch 1. For those customers currently running in legacy mode, Neoteris will provide an upgrade path from 3.3.1 Patch 1 to a later version of the IVE – this version will be available early next year. Customers currently running in legacy mode should be planning on migrating to the new mode in the near future.
- You can upgrade to 3.3.1 Patch 1 Release from any IVE running version 2.2.x or higher. To upgrade from a 1.4 version (pre 2.2.x), upgrade first to IVE 2.2.x, and then upgrade to 3.3.1 Patch 1 Release.
- If you are currently running a PreRelease or Beta version, the recommendation is that you roll back the system to the release you were running before, and then upgrade to 3.3.1 Patch 1 Release. This option provides the flexibility of running your previous software version. If you upgrade directly to this release, the only option of running an earlier software version is to perform a factory reset.
- Starting from 3.0.1 Release, the IVE handles usernames in a case-insensitive manner. For example, when a user signs in to the IVE as "jsmith" or "JSMITH", the user would see the same settings on the IVE in both cases. The IVE still sends user credentials to the external authentication server in the case entered by the user, allowing the IVE to work correctly for case-sensitive authentication servers.

- During the upgrade from a Pre-3.x Release, if there are two users with the same username but different cases (such as “jsmith” and “JSMITH” in the previous example), the IVE picks the first username and upgrades only that user’s settings. An IVE system log message is reported in such cases.
- When upgrading from an Active/Passive Cluster Pair to a Multi-Site Cluster, administrators will need to import a new license for Multi-Site. Administrators should also be reminded to remove the Active/Passive Virtual IP address (VIP). This VIP is not needed with Multi-Site Clustering, since it is Active/Active not Active/Passive. (8471)
- Make sure to archive the previous IVE system and user configurations before performing an upgrade.
- When upgrading, Optimized NCP will be disabled unless the release previously running had Optimized NCP support, in which case, the setting for Optimized NCP will be carried over through the upgrade. For new IVEs, Optimized NCP is enabled by default.
- In this release the “Network Identity” feature is enabled. This feature (available in the Network Settings section) is part of the core IVE configuration and should be configured. It requires a hostname by which the IVE is normally referenced.

4. General Notes

Initial Configuration

To connect to the IVE serial console for initial setup, use the female-to-female null-modem cable included with the packaging.

External Group Lookup

The 3.x standard authentication mode has no “Map NFS IDs” feature. To enable users to access NFS shares, you must configure an NIS authentication server on the IVE so that NFS IDs are returned for users. You may disable the NIS server for authentication if you do not want users to sign in to the IVE using NIS credentials.

5. Known Issues and Limitations

The following list enumerates known issues and limitations in the IVE 3.3.1 Patch 1 Release.

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. 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 Functional Matrix available in the Product Documentation of the Neoteris Support site (<http://support.neoteris.com/>).

3. 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.
4. Password Management is not available when using Legacy Mode Authentication.

FIPS

1. If you choose to replace an administrator card using option 11 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 11 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)

Secure Meeting

1. 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)
2. Secure Meeting Upgrade is not supported in legacy mode. To use this feature, please make sure that your IVE is in the "User Selects Auth server (USA)" mode. For more details, please refer to the "Release Upgrade Considerations" section of the Release Notes.
3. If the IVE has a self-signed SSL certificate then the Secure Meeting functionality may have intermittent problems. Specifically, users may see a "Cannot Connect to the Secure Meeting server..." error message. To workaround this issue, when meeting attendees access the meeting and see a certificate warning, they should click "View Certificate" and then "Install Certificate" to install the certificate. An alternative, to avoid this issue and certificate warnings altogether, would be to install a production level, CA-issued, SSL certificate (that the browser can verify and trust) onto the IVE. (8603)
4. Users using a Proxy Server for their Internet browser configuration may run into problems downloading the Secure Meeting Client. (9388)
5. 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)

6. 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)
7. Users should be reminded that the Secure Meeting Sharing functionality transfers the live screen display to all attendees. This can cause a reduction in performance, especially if the network links between presenter and the IVE is slow. Attendees on slower connections, such as dial-up, may experience “lag” due to buffering. Once the buffer fills up, the attendee’s client may crash unexpectedly. Dial-up connections are not supported. (8999 and 9255)
8. The Secure Meeting Sharing functionality may be confusing, as it does not clearly display which applications are being shared now versus which ones were already shared. (8930)
9. 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)
10. Windows 98 and Netscape without ActiveX are not currently supported for the Secure Meeting functionality. Windows 2000 and Windows XP with Internet Explorer 6.0 are fully supported. (8844 and 9297)
11. 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)
12. 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)
13. When using the Chat function, attendees which are currently also using remote control may have problems using their own Chat window. (9832)
14. 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)
15. When canceling a meeting which has already been configured to send out email invitations, attendees may not receive the cancelled meeting email. (9759)
16. If Remote Control is disabled, the icon still shows as enabled during meetings. If the presenter attempts to delegate remote control to a user, they will receive a “Failed to change roles” error message. If the presenter then attempts to change remote control to themselves, the presenter’s Secure Meeting client may hang unexpectedly. (9854)
17. Users who do not receive the Secure Meeting email invitation as expected, may need to check their Spam Filter settings, since the invitation currently uses a blank “To” field. (10686)

Host Checker

1. 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)
2. Host Checker is only supported on Web browsers which have ActiveX. If using a non-ActiveX enabled Web browser, the user may get “stuck” during the Host Check. Since this may be confusing to the user, administrators are encouraged to configure Browser Restrictions for IE for any group configured to use Host Checker. This way, users will get redirected back to the login page and will see a warning about their web browser not being supported for that group. (9064)
3. 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)
4. When using custom Registry settings for Host Checker, the Subkey should not be preceded with a ‘\’. (10787)
5. If Host Checker is configured for a group, users with an unsupported Web browser may get stuck at the “Starting Host Checker, please wait…” page. (10690)
6. For certain Windows system services (e.g. winlogon.exe, smss.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)

Windows based Secure Application Manager (W-SAM)

1. W-SAM supports only client-initiated TCP traffic. Furthermore, W-SAM only supports those protocols which do not embed IP addresses within the header or payload. The one exception being Passive FTP.
2. 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)
3. 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)
4. In order to access a share using W-SAM by hostname, the IVE administrator must explicitly configure the server’s NetBIOS name (alphanumeric string up to 15 characters) into the W-SAM Destination Host configuration page. There is no support for wildcard hostnames in this release. (8967)
5. 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.
6. For WSAM to connect to a remote server for file-sharing, the server name should be listed with the DNS. Having only a WINS entry is not sufficient.

7. 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):
 1. At the Command prompt, type: `net use * \\server\share /user:username`
 2. In Windows Explorer, go to Tools → Map Network Drive, then select "Connect using a different username".
8. 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.
9. When using the "destination host" mode of W-SAM, administrators should remember to create an ACL to allow access to that server. (7246)
10. 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)
11. Since the W-SAM functionality of the IVE binds to a localhost (127.0.0.x) address on the user's PC, users with virus programs and other network intrusion detection programs may get a warning or alert when SAM initially loads and starts up. Users can ignore this warning, as it is part of the SAM functionality for secure application connections to the IVE. (7329)
12. 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.
13. 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)
14. 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.
15. The Secure Drive Mapping function of W-SAM (with NetBIOS Support) may behave unexpectedly if Norton Anti-virus Professional Edition 2003 client is installed. (9384)
16. 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)
17. 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.

18. When upgrading to W-SAM 2.0 (IVE Release 3.2.X) from an older release, it is recommended that previous versions of WSAM be removed. If you are upgrading from WSAM 1.0 (3.1.X Release), please delete the folder `Program Files\Neoteris\Application Proxy`. Additionally, users may need to un-register the `gapsp.dll` object (`regsvr32 -u gapsp.dll` from the working directory) in order to delete it. Then reboot your system. Users upgrading from an older version should run the uninstall application under `Program Files\Neoteris\Secure Application Manager`. This will leave a few objects behind, but rebooting your system will get rid of these objects. (9330)
19. For users with Netscape web browsers, in order to use W-SAM, they must first download and install an ActiveX plug-in for Netscape.
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 can not be secured through W-SAM because it is not a Winsock 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. W-SAM will cease to function if the New.Net software is installed. This is due to the fact that New.Net installs a proprietary namespace provider which blocks traffic to the W-SAM client. (13107)
24. 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 Neoteris 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)
25. 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)
26. Under certain conditions, W-SAM does not terminate completely. A process named `gapsvc.exe` may be left running and could prevent W-SAM from being re-launched. To resolve this, the end-user may end the `gapsvc.exe` process by using the Windows Task Manager. (13899)
27. W-SAM ceases to function on clients where McAfee Virus Scan v7.0 is installed after W-SAM is installed. Uninstalling the McAfee software corrupts the IP stack, which must then be recovered with appropriate repair tools, or by reinstalling the TCP/IP protocol. (15981)

Java Secure Application Manager (J-SAM)

1. The "Restore System Settings" button under the end-user's Advanced Preferences page may not work properly if the user is currently running J-SAM. (9836)
2. J-SAM must be enabled to use the Citrix NFuse, Lotus Notes, or Exchange functionalities of the IVE. These options will appear once J-SAM has been enabled.

3. Outlook 2003 is not supported with J-SAM. (8251)
4. When a user clicks on "No" when the session mgr applet downloads but later tries to start the session manager manually, sometimes the session manager applet download does not appear. The work around is to kill the browser and start over.
5. Client/Server support is available for SunJVM; however, the functionality available on Linux and Macintosh does not meet the functionality available on Windows. These functionality levels are as follows:
 - a. On Linux, J-SAM support is available on Red Hat Linux, with the following exceptions:
 - i. J-SAM will not automatically modify the /etc/hosts file since root permissions are needed to modify the file. To automate the /etc/hosts file change, the user, as root, may relax the permissions on the /etc/hosts file or run the web browser as root. Another option is that the user may access the secured host with the mapped localhost IP address. For example, the telnet command may be run as `telnet 127.0.1.10 <port>`. The Details pane on the J-SAM window will display the IP address to which the server is mapped. A third option is that the external DNS may be modified to map the server that needs to be secured with the appropriate localhost address.
 - ii. The session manager will not be able to bind on the privileged ports (less than 1024) unless the user runs the Web browser as root. A potential workaround is to configure the client application and the J-SAM application's client port to run at a higher port number (greater than 1024). Please refer to the Administrator's Guide for more details.
6. Support for multiple client/server applications does not work if you use IP addresses for the servers. In other words, this feature only works if the server name is a DNS hostname (fully qualified or unqualified). When an IP address is used in the client/server definition, the session manager ONLY listens on the 127.0.0.1 IP address for the configured port.
7. 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)
8. End-users must specify all of the servers listening on a port in a single client/server application definition on the IVE. Defining the servers as separate client/server application definitions will get an error in the UI. The UI validation check will be removed in a future release. (9071)
9. 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; };
```
10. If the number of entries in the web browser "Proxy Exception List" is greater than 18, Outlook 2000 does not work with J-SAM. Other clients, such as VNC and Terminal Services, are not affected. Additionally, if entries in the exception list are not delimited with a semicolon (;), Outlook 2000 will not work J-SAM when using SunJVM. (9766)
11. The string "Lotus Notes – HTTP Proxy" in the application field is a reserved string for applications configured on port 1352. The presence of this string assumes that users will be running Lotus Notes in the HTTP Tunnel mode. (8912)

12. On Windows XP machines using JSAM, if drive mapping (using ports 137, 138, or 139) is configured, JSAM may leave behind a file called `neoteris_read_xxxx`, where `xxxx` is a number. This file can safely be ignored after the PC has been rebooted for drive mapping support. (9974)
13. 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 advisable that J-SAM be configured to automatically launch after login.
14. Multiple Secure Terminal Access sessions may not work correctly if the login fails on one of the sessions. (12253)
15. Registry changes made for J-SAM applications, such as for Drive Mapping, can be undone by going to Advanced Preferences and clicking on the "Restore System Settings" button for J-SAM; however, this function does not work properly on Japanese Windows and thus changes to the registry will not be restored. This should not cause any problems with the OS or other applications. (10621)
16. Due to a buffer overflow issue in Windows 98, J-SAM cannot support more than approximately 10 simultaneous applications. (12515)
17. On Windows 2000 clients, the registry change made by J-SAM for Outlook and Drive Mapping, cannot be performed if the client has the Microsoft Pocket PC Connection Wizard installed. (12379)
18. J-SAM will create two log files the end-user's PC named `netscreen.log0` and `netscreen.log1` in the `c:\windows\java` or `c:\winnt\java` directory. 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 JSAM for the Mac, once a user has launched JSAM, 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 again to be able to run J-SAM again. (10766)
2. When using J-SAM for the Mac, 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 Mac, users that do not enter the administrator password during the J-SAM install process will not have access to J-SAM applications that have been configured with hostnames. They will only have access to applications that have been defined with IP addresses. (10854)
5. When using J-SAM for the Mac, if the user's session is terminated, their J-SAM window may still display the status of "OK". (10767)
6. When using JSAM for the Mac, three files may be left behind in the `~/Library/Application Support/Neoteris` directory. These files are `libAuthKit.jnilib`, `NeoterisSun.jar`, and `SessionManager.log`. These files may safely be removed after exiting J-SAM. (10638)

Sun JVM/Code-Signing Certificates

1. 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.
2. 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)
3. 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.
4. To sign applets for the MS JVM environment, the admin must import VeriSign Microsoft Authenticode certificates. Applets running in MS JVM, signed with Thawte Microsoft Multi-Purpose Authenticode certificates will not show up as trusted applets, therefore the user will not be able to click the "Always Trust" button for these applets. (8269)

Network Connect (NC)

1. Since NC modifies the user's routing table, if an NC user has a proxy configured for their Web browser, they may be unable to directly access Web sites and other IP-based resources, unless they can access them through the IVE using the NC tunnel. (10626)
2. The IVE Admin may only specify 254 IP addresses for the Network Connect Client IP Pool. This is a limitation of the input mechanism in the UI and will be addressed in a future release. (6378)
3. If a group that is initially configured to use custom NC ACLs is reconfigured to inherit settings from the Users group, existing sessions will need to be re-started for the ACL changes to take effect (This is not required for other ACL changes, which are dynamically applied). (9046)
4. Client IP Pool configuration is initially synchronized across IVEs in a cluster. When using NC with a clustered node, administrators are reminded to verify/reconfigure the client IP pool after the node joins a cluster. This will be addressed in a future release.
5. 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.
6. On Windows XP, when the IVE is configured to "Disable Split-Tunneling" for NC, the local subnet route will remain in the end-user's routing table allowing them local access. (12221)
7. 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)

8. On Windows XP Home Edition, Network Connect cannot be run with "Limited User" privileges. (13493)
9. If a user without Administrative privileges clicks on "Uninstall Network Connect", only some of the files will be removed and Network Connect will remain on the client in a partial and potentially inoperative state. (13325)

Citrix Integration Issues

1. IVE 3.1.x was not qualified for use with Project Columbia running on NFuse.
2. If Citrix option is disabled in the Admin UI, then clicking on the NFuse settings will not take you to the Citrix advanced configuration page. To see the Citrix advanced configuration page you need first to enable Citrix for the group of users.
3. 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)

General Authentication/Authorization Issues

1. In Legacy mode, IVE admin can enable/disable authentication servers, but this does not prevent users from logging into the IVE.
2. If client side certificate are required to log into the IVE and a user installs a bad client side certificate in the browser, then they may see a "Page Not Found" error message.

Pass-Through Proxy Issues

1. When using OWA with Pass-Through Proxy, users may need to access the OWA server by including **/exchange/** at the end of the URL for the OWA server. (10651)
2. Siebel7 is not supported through Pass-Through Proxy. (7487)
3. When using OWA through Pass-Through Proxy, the Distribution List functionality (for Contacts) does not display. (9375)
4. On Netscape and Mozilla, using Pass-Through Proxy (with the IVE port configuration) invalidates the user session causing the user to have to login again. (7290)
5. When using Pass-Through Proxy in Host mode and configuring multiple applications to use the same hostname alias, web ACLs will be matched to the first application in the list. This means that if the first application listed is not explicitly allowed in the web ACL, users will be denied access to all other Pass-Through Proxy applications for that hostname alias. (9194)
6. When using Netegrity, Pass-Through Proxy requests will not be authorized against the Netegrity SiteMinder policy server. (7932)
7. When using a Netegrity authentication server and the IVE is configured for auto-login and configured to use the HTTP Form Post method, users may be unable to login to OWA and Lotus iNotes configured as Pass-Through Proxy applications. This is only for Netegrity authentication, local users are not affected. (8972)

8. When using Lotus iNotes through Pass-Through Proxy, links on the welcome page may not be rewritten. The Inbox and other functionalities are working. (9236)
9. When using Lotus iNotes through Pass-Through Proxy, if XML rewrite is needed, administrators are encouraged to enable XML rewriting in the Pass-Through Proxy configuration or 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)
10. If a server is configured via Pass-Through Proxy via DNS resolution, the server must be accessed from the IVE browse bar or via an IVE bookmark using the servers real IP or hostname. This will automatically be redirected to the alias hostname. Accessing the alias hostname directly does not set the cookie properly and redirects the user to the IVE login page. (9235)
11. 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)

Clustering Issues

1. Because of changes in clustering from 3.0 to 3.1+, an upgrade of a node in stand-alone mode will erase all clustering information/configuration. Administrators will manually need to re-enter this information after the upgrade is complete and the IVE has rebooted. To maintain proper configuration during an upgrade like this, administrators are encouraged to upgrade the node(s) while they are still part of the cluster.
2. IVE statistics information is not synchronized in the cluster. You need to manually collect and aggregate the statistics from the individual members. This issue will be fixed in a future release.
3. 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).
4. 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. In the previous release, the network connectivity status is determined by the 'existence of carrier signal on the physical interface. In this release, 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 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. This is a change from the previous release based on the feedback from many customers.

5. 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.

6. If the cluster is changed from active-passive to active-active, the cluster VIP (corresponding to the active-passive cluster) will still be active until manually removed.
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 cases. We recommend that you disable the cluster member, change 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. 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 standard LAN-based 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. The configured transport setting on the clustering properties page is used only within members of the same site (same subnet).

12. When using an IVE from the serial console and joining an existing cluster, if the join fails, the IVE boots into stand-alone mode without any notification or message on the console. An error messages will be added in a future release. When joining a node to a cluster using the administrative UI, an error message is properly displayed.
13. Changing the IP address on an active node in the cluster is not supported and may yield erratic results. The workaround is to disable the clustering service, change the network settings and then enable the clustering service on this node.
14. When using clustering, the administrator should remember that each node must be assigned a node name.
15. Clearing the log entries on a node in a cluster will clear all log entries on all nodes in that cluster. This issue will be addressed in a future release. (9032)
16. 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.

17. Clustering is not supported when an IVE is configured to have the same subnet for both the *internal* and *external* interfaces.

Internationalization Issues

1. The Japanese character ~ (double-byte tilde) is not displayed properly through the IVE. This will be addressed in a future release. (7611)
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. Japanese characters are not supported in naming Authentication Servers. (7924)

External Group Lookup Issues

1. If you have more than one authentication server of the same type (such as two RADIUS servers), then disabling the first authentication server (first in alphabetical order) results in none of the authentication servers (of this type) to show up on the sign-in page. The workaround is to make sure that the first authentication server (of the same type) is always enabled. This issue will be fixed in a following release.
2. The IVE LDAP group mapping functionality does not support authorization based on containers. The group lookup functionality is only supported for standard LDAP user attributes and static group objects.
3. In the IVE group mapping scheme, if a user belongs to multiple groups in the external authentication server, then the user will be presented, upon login, with a list of possible groups to log into. Once the user is logged into a group, they cannot go back and log into a different group – they must sign out and re-authenticate again, then choose a different group to log into.
4. If you switch between the legacy authentication mode (pre-3.0) and the new authentication mode, local user records are not automatically carried forward. In other words, the old/new authentication modes do not interoperate. The legacy mode is intended only for backwards-compatibility purposes.
5. Advanced functionality, such as LDAP Dynamic Groups or referrals with complex LDAP queries, is not supported in this release. This is currently planned as a future enhancement.
6. The IVE is unable to look up groups in an RSA/ACE Server with or without a fronting RSA/ACE Server. The workaround when fronting an RSA/ACE Server with a RADIUS server is to manually assign ACE users to Radius groups (profiles).

Windows File Browsing Issues

1. If you deny access to a file server by specifying the IP Address, the 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.

2. If you deny access to a file server by specifying the IP Address and users try to browse to the server by specifying the IP of the file share, they will be challenged for credentials and after they provide them they will get the message stating that there are no file shares available on this server.

Group Power Editing Issues

1. Web Browsing Open/Closed policy vs. Windows Open/Closed Policy. Please note that the Grant Tag (Allowed resource) contains the exception list for the Closed Policy while the Deny Resource List contains the exception list for the Open Policy. This is different from Web ACLs in which the Open tag encloses the exception list for the Open policy.
2. The IVE doesn't perform any verification checking on the ACL/Bookmark values, just the syntax. Administrators are encouraged to test ACL/Bookmark settings in a testing environment before uploading to their production IVEs.

Cache Cleaner

1. Cache Cleaner does not remove the following:
 - o Browser history
 - o Files which have been explicitly saved by the end-user
 - o IE plug-ins and Active-X controls
 - o Data from the IVE Welcome Page, e.g. Neoteris logo and Auth cookie
 - o Entries in index.dat (a private hash table of URLs maintained by IE)
2. Cache Cleaner will attempt to verify the session during its cleaning phase. During this time, a connection may be opened from the process to the IVE which the users are connected to. (10456)
3. If Cache Cleaner is configured for a group, users may be unable to log into the IVE if they cannot install the Cache Cleaner application on their PC. (10822)
4. If Cache Cleaner is configured for a group, users who are not using the Internet Explorer Web browser, i.e. Netscape users, may still log in. To work around this limitation, IVE administrators may configure browser-based restrictions for a group. (10697)

Other Issues

1. The IVE only supports sending SNMPv2 traps. If the SNMP trap manager client does not support SNMPv2, the traps may not be received and displayed properly. Results may vary based on client software.
2. 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.
3. The Web Proxy feature may only be configured for HTTP requests. HTTPS requests are sent directly to the origin. When the Web Proxy feature is enabled, 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.
4. URLs embedded in Macromedia Flash content are not currently supported by the IVE. This feature is scheduled for a future release.

5. There are some known issues with OWA functionality when the Web Proxy feature is enabled on the IVE. These issues will be fixed a future release.
6. 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.
7. Access Control Lists—For Web and file browsing access control lists (ACLs), we currently do not perform reverse DNS lookups. For example, if you have an ACL to deny access to <http://www.mycompany.com>, a user can still get to the "mycompany" site by entering its IP address, such as in <http://a.b.c.d> where a.b.c.d is the "mycompany" site IP address. The workaround is to list both the IP address and the hostname in the ACL rules.
8. The *Administration Guide* PDF may not be accessible through the Netscape browser running on UNIX. You can find a PDF plug-in for Netscape running on UNIX at the Adobe Web site (<http://www.adobe.com>).
9. 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.
10. Occasionally you may see broken links or incomplete content when browsing Web pages. Please email a detailed description to the Neoteris Support Department and include a complete trace of the user transaction using the built-in debugger application.
11. When using the auto-login function of that IVE, i.e. logging in from another cgi elsewhere on a web server, any user-agent checks will be bypassed. This is because the login took place in a different way than the traditional login of the IVE. (7933)
12. 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)
13. 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; };
```
14. 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.
15. 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)
16. URLs embedded in ActiveX controls are partially handled in this release and additional support will be provided in a future release.
17. 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)

18. 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)
19. The IVE web browsing function does not support URLs more than 159 characters in length, including extensions, such as ".html". (7248)
20. 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>
21. The legacy mode support for NIS authentication does not work.
22. 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)
23. When configuring a Netegrity Policy Server, In the *Resource for insufficient protection level* field, administrators should enter a resource on the Web agent to which the IVE redirects users when they do not have the appropriate permission. This resource is static so administrators are encouraged to write a generic message on the page to which they are redirected to. For example, administrators may want to redirect users to a sign-in page. Note that the entire URL does not need to be entered for the resource (e.g. just /index.html).

Note: With version 5.5 or higher of the Web agent with V5QMR3, users with insufficient permissions can be redirected back to their original resource by leaving the *Resource for insufficient protection level* field blank in the Administrator UI and disabling the Web agent's form credential collector compatibility mode (FCCCCompatMode=no) on the Netegrity Agent Conf Object.
24. The Netegrity Policy Poll Interval only supports values of -1 and positive integers, not 0.
25. Only SSL certificates which have single values for each field (for example only one value for OU) are supported. This is only a concern when importing a certificate which was generated elsewhere, not if it was generated on the IVE. (8543)
26. When using the Import Users function, the Administrator should verify no fields have a comma (,) character within them. For example, a FullName field of *Smith, John* is not acceptable due to the comma. (8801)
27. Due to a bug in Netscape 6.1, administrators will encounter some issues when using Netscape 6.1. This is because Netscape 6.1 has some problems when referrers are checked. To work around this, administrators are encouraged to upgrade to Netscape 6.2 or later. (8169)
28. 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)
29. 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)

30. The IVE does not support the import of Intermediate CA certificates; however, Verisign and Comodo are supported internally. (5855 and 9410)
31. When using OWA with Mac Safari, the left-hand navigation bar will show up, but the main window pane may not. Clicking on the Inbox icon in the left-hand navigation bar, will bring up the Inbox properly. (9778)
32. Lotus iNotes in offline mode is not currently supported. (9889)
33. Even though you enter the password to archive users and system config files, this password is disregarded on the import.
34. The Session Timeout Warning alert message will display in the English language regardless of your browser's language setting. This issue will be addressed in a future release. (10577)
35. The Session Timeout Warning settings only apply to user sessions, not Administrator sessions. Administrator sessions will not receive any timeout warnings. (13407)
36. 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.
37. When Remote SSO is configured and later unlicensed, the "Configure Remote SSO" option will still be displayed on the end-user menu.
38. The Remote SSO functionality will not work for login pages which have been configured for Pass-Through Proxy. (10115)
39. When switching from Optimized NCP (Neoteris Communication Protocol) to Standard NCP, or vice versa, all NCP- Based communications must be restarted. This includes W-SAM, Network Connect, and Secure Meeting.
40. On Win98 clients, when Auto-Select is enabled for the Neoteris Control Protocol (NCP), the Optimized NCP will not be used. This should not cause any visible changes to the user experience. (10881)
41. 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)
42. 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)
43. 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.
44. The Alarm feature in Lotus iNotes 5.0.X versions is not supported through the IVE rewriter, but is supported using Pass-Through Proxy.
45. 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)

46. 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".

6. Supported Platforms

Please see the "Supported Platforms" document posted on the Neoteris Support Site (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