

NetScreen Secure Access Series

IVE 4.0 Release Notes

Build #5531

1. NEW FEATURES IN IVE 4.0.....	2
<i>New Access Management (AM) System.....</i>	<i>2</i>
<i>Central Manager.....</i>	<i>3</i>
<i>Support for Windows DFS File shares.....</i>	<i>3</i>
<i>AD/NT Password Management.....</i>	<i>3</i>
<i>New Licensing system.....</i>	<i>3</i>
<i>Realm-based Concurrent User Limits.....</i>	<i>3</i>
<i>Secure Meeting Improvements.....</i>	<i>4</i>
<i>Anonymous Authentication Server.....</i>	<i>4</i>
2. UPGRADING TO IVE 4.0.....	4
3. KNOWN ISSUES AND LIMITATIONS FIXED IN THIS RELEASE.....	5
4. KNOWN ISSUES AND LIMITATIONS.....	6
<i>Client-Side Digital Certificates/Cert-Based Authentication.....</i>	<i>6</i>
<i>Central Manager.....</i>	<i>7</i>
<i>Host Checker and Cache Cleaner.....</i>	<i>7</i>
<i>Customizable Login Pages.....</i>	<i>8</i>
<i>Password Management.....</i>	<i>8</i>
<i>FIPS.....</i>	<i>9</i>
<i>Secure Meeting.....</i>	<i>9</i>
<i>Windows based Secure Application Manager (W-SAM).....</i>	<i>11</i>
<i>Java Secure Application Manager (J-SAM).....</i>	<i>13</i>
<i>MacOS Java Secure Application Manager (J-SAM).....</i>	<i>15</i>
<i>Sun JVM/Code-Signing Certificates.....</i>	<i>15</i>
<i>Network Connect (NC).....</i>	<i>16</i>
<i>Pass-Through Proxy Issues.....</i>	<i>17</i>
<i>Clustering Issues.....</i>	<i>18</i>
<i>Internationalization Issues.....</i>	<i>19</i>
<i>External Group Lookup Issues.....</i>	<i>20</i>
<i>File Browsing Issues.....</i>	<i>20</i>
<i>Group Power Editing Issues.....</i>	<i>21</i>
<i>Cache Cleaner.....</i>	<i>21</i>
<i>Netegrity.....</i>	<i>21</i>
<i>Miscellaneous issues:.....</i>	<i>22</i>
5. SUPPORTED PLATFORMS.....	28

1. New Features in IVE 4.0

IVE 4.0 introduces the next-generation Secure Remote Access appliance with the following major features. Please refer to the Admin Guide for additional details and configuration instructions :

- New Access Management (AM) System – Supports flexible and dynamic authentication and authorization policies, including the ability to support multiple login hostnames with an option to customize the login pages.

Some of the main features of the new AM system are as follows:

- LDAP Authentication Enhancements such as support for LDAP referrals, static and dynamic groups and multiple user attributes.
- Dynamic Authorization Resource Policies – Ability to define granular resource-based policies (e.g., ACLs) using a combination of user profile (username, authentication method used, certificate attributes etc) and session profile conditions (SourceIP, TimeOfDay etc).
- Improved Host checker and Cache Cleaner policy enforcements with ability to enforce end-point security policies before user could attempt to login to the IVE. As part of these Access Management enhancements, the IVE now has a separate “Sign out” page, which will be displayed upon logout, instead of redirecting the user back to their login page – this is an improved security measure.
- Role based delegation – Ability to define multiple administrative roles with different administrative privileges on the system.
- Support for multiple sign-in hosts – Ability to host multiple sign-in pages for different login URLs.
- Customizable Login pages – Ability to customize the user login pages by uploading fully customizable web pages using set of defined templates. The customized pages along with corresponding images and style sheets must be combined into a zip file and uploaded to the IVE. The uploaded zip file can be associated with a Sign-In URL. Users accessing that sign-in URL will then see the uploaded customized pages instead.

Pages which are customizable include:

- Login and Logout pages
- ACE pages (New Pin, Next Token, and Generate Pin)
- Host Checker and Cache Cleaner “Please Wait” pages
- Multiple role select page
- Netegrity ACE pages
- Miscellaneous warning pages (Concurrent user limit exceeded, SSL cipher limit warning pages)
- Certificate based authentication and authorization – Users can login to the IVE using certificate as the credential, and then the certificate users can be mapped to an LDAP directory so that users attributes, groups can be retrieved for authorization.

- Central Manager – A new product in the management series with several features such as System Dashboard, Logging and monitoring enhancements, minimal downtime cluster upgrades etc. Note: Central Manager requires a separate feature license.

The primary features of Central Manager are:

- System Dashboard – Capacity Utilization Graphs
- Minimal downtime cluster upgrade – Ability to do a cluster-wide upgrade without breaking the cluster while keeping at least one node in service all the time.
- Deterministic Cluster recovery – Ability to assign ranks to various nodes in a cluster such that when a cluster recovers from a “Split-brain” situation the node with the highest rank propagates the correct cluster state.
- Enhanced Log/Monitoring – Rich filtering and formatting of the system logs that are componentized into Event Log, User Access Log and Admin Access Logs based on the types of information they store.

The SNMP MIB has been enhanced to provide capacity utilization metrics. The new MIB is available as a download from the admin console.

- Ability to save up to 10 Local Backups of System/User configuration, stored directly on the IVE.
- Push Configuration from one IVE to any other IVE in the enterprise – Push is supported for User Roles, Resource Policies and Delegated Administration Roles.
- Support for Windows DFS File shares – Also includes the support for authentication against Windows 2003 servers.
- AD/NT Password Management – IVE can now intermediate AD/NT (as well as LDAP-Based) password messages at the time of user login, including Password Expiry, Account Lockout etc. Please refer to the Password Management Technology Integration Guide (“TIG”) for additional details and server-specific notes.
- New Licensing system - The IVE licensing system has been modified in the following ways:
 - The IVE now uses a base license and optionally one or more feature licenses. The base license provides information about the core system, including clustering capabilities. The base license may be either the existing 3.X license, a new 4.0 Baseline license, or the new 4.0 Advanced license.
 - Upgrades, features, and packages have been separated into individual feature licenses.
- Realm-based Concurrent User Limits – Authentication Realms can be configured to restrict a certain number of concurrent users. This is configured on a per-realm basis.

- Secure Meeting Improvements – The Secure Meeting functionality has been improved to increase usability:
 - Cross-Platform Support – The Secure Meeting client now includes support for a larger spectrum of OS/Browser combinations. Please refer to the Supported Platforms Guide for additional details.
 - Java-Based Secure Meeting Client – The Secure Meeting client has been ported to Java in order to run on Mac OS X and RedHat Linux 7.3. The Java client is only offered as Beta at this time.
 - Java Installer – The Secure Meeting client may now be installed via Java, if ActiveX is not supported, or to install the Secure Meeting client on Windows platforms where the end-user does not have permission to install applications.
 - Support for Dial-Up clients – The Secure Meeting client now supports dial-up users with the following caveat:
 - Viewing a high-bandwidth presentation will cause the Chat to not work and the viewer may lose transmitted data during the presentation.
 - Seamless Recovery from Network Outages – The Secure Meeting client is now more resilient in these cases.
 - Improved Protocol – The Secure Meeting client now supports the Optimized NCP (NetScreen Communications Protocol) to improve performance for meetings.
 - Instant Meeting – Secure Meeting users now have access to a one-click meeting functionality, useful for scheduling on-the-fly meetings.
 - Test Link – A tool is now available for end-users to test their client PC to ensure it meets the requirements to install the Secure Meeting client.
 - Troubleshooting Guide – Available from the NetScreen support site is a troubleshooting guide for Administrators.
 - Better Error Messages and Improved Logging – The Secure Meeting functionality has better error-reporting capabilities in this release.
- Anonymous Authentication Server – Anonymous Authentication provides access to the Secure Access gateway without requiring authentication credentials to be provided. This can only be used for end-user realms, and only sign-in URLs which have only this kind of Auth server configured. This auth server may not be mixed with other auth server types.

2. Upgrading to IVE 4.0

- 2.1. In this release, automatic upgrades from the following releases, including from the Legacy Authentication mode, are supported:
- 3.3.1 GA Build 5147
 - 3.3 Patch 1 Build 4797
 - 3.3 GA Build 4683
 - 3.2.1 Patch 1 Security Fix 1 Build 4495
 - 3.2 Security Fix 1 Build 4391
 - 3.1.1 GA Build 1971

If upgrading from a release which is not in the above list, please upgrade to one of the above listed releases first, and then to 4.0.

- 2.2. **Important Note:** If you are already using IVE 4.0 Beta, you should first rollback to the previous 3.x configuration and then upgrade to IVE 4.0.
- 2.3. **New Source Ports:** IVE 3.X and earlier used TCP ports 6,000 to 32,000 as the source port when making a TCP socket connection to a backend resource. With version 4.0 and later, the IVE now uses ports 32,768 to 61,000 to make these socket connections. Administrators who have a firewall between the IVE and backend resources should be sure to update their firewall rules to reflect this change.
- 2.4. Please make sure to use the following steps in preparing to migrate to IVE 4.0:
 1. Save a backup of the system/user configuration, log files before performing the upgrade.
 2. To speed up the upgrade process, it is strongly recommended that the Administrator archive the log files and then clear them. Log files which are not cleared will be automatically converted to the new 4.0 standard Log message format. Depending on size and quantity, this will slow down the upgrade process.
 3. Read the NetScreen IVE 4.0 Migration Guide for 3.x to 4.x Admin User interface mapping and a high-level overview on the new access management system and information on how to configure user access and delegated admin policies.
 4. Upgrade the IVE to IVE 4.0. The IVE will reboot as part of the upgrade process.
 5. Upon upgrade to 4.0, the IVE will retain the old 3.x license and continue to function as expected. In order to gain access to the new 4.0 features, such as those in the Advanced model, or Central Manager, a new 4.0 base model license must be applied to the IVE. This is now called either the "Baseline" or "Advanced" model license. During this process, the IVE will remove the old license and replace it with the new IVE 4.0 base model license. Any previously licensed feature upgrades will now require a separate feature license in order to continue working properly. The stored configuration for these features will be maintained during this process and re-activated upon license application.

Please apply all of your supplied IVE 4.0 license keys under System → Configuration → License. Note: If you would like to apply the base model license and the feature upgrade licenses all at the same time, the base model license should be on the first line of the input textbox. Also Note: When entering multiple license keys, Administrators must include the prefixed comment and the ':' delimiter into the license key input textbox. This should have been sent along with the license keys.

3. Known Issues and Limitations Fixed in this Release

The following list enumerates known issues which have been resolved in this release:

1. Secure Meeting is now supported for users configured to use a Proxy server. (9388)
2. Secure Meeting is now supported even when using a Self-Signed SSL Certificate. (8603)
3. Dial-up Clients using Secure Meeting are now supported. (8999 and 9255)

4. Secure Meeting email invitations are now sent out for meeting cancellations. (9759)
5. J-SAM Registry changes can now be undone for Japanese Windows by going to the Advanced Preferences and clicking on "Restore System Settings". (10621)
6. When using J-SAM for the Mac, users that do not enter the administrator password during the J-SAM install process now have access to J-SAM applications that have been configured with hostnames as well as those configured with IP addresses. (10854)
7. When using Lotus iNotes through Pass-Through Proxy, links on the welcome page are now properly rewritten. (9236)
8. The Japanese character ~ (double-byte tilde) is now displayed properly through the IVE. (7611)
9. IVE user and admin sessions are now maintained across upgrades.

4. 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. 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)
2. The IVE does not support uploading of Root CA chains or Intermediate CA certificates; however, if the client certificate has a chain inside, we will honor the chain. The top chain in the client certificate must be signed by the uploaded Root CA to validate the client certificate. Support for multiple Root CA's (including chains) and Intermediate CA certificates are planned for a future release.
3. Certificate users may get an HTTP 500 error in the end-user gives a wrong password for their private key file when challenged for a client certificate.
4. 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)
5. 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. The Push Configuration function only pushes Web Proxy policies, but not the proxy server configuration. (14949)
2. Restoring the system configuration from a Local Backup on the IVE without selecting the Network Settings still restores the Virtual Hostname configuration parameter, found under Network Settings. This issue will be addressed in a future release. (15149)
3. With the Enhanced Logging, if a custom filter is deleted but is already in use by a component, such as SYSLOG, or Log Archiving, the component will revert back to using the NetScreen "Standard" default filter. When deleting a filter used by one of the other log viewers, no filter will be set up access, and the Admin may need to choose one from the list and click "Update" in order to display the logs. This issue will be resolved in the next release. (13674)

Host Checker and Cache Cleaner

1. Cache Cleaner and Host Checker will launch automatically if they are configured for any of the realms for the sign-in page being accessed, even if they are not configured for the realm which will be used for that user session. This is by design and is a behavior change from 3.X (14115)
2. 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)
3. 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)
4. Cache Cleaner and Host Checker are end-point security controls launched via ActiveX. Since launching these client-side security tools require ActiveX, Administrators are encouraged to add "Browser" authentication policies in conjunction with Host Checker or Cache Cleaner for ActiveX enabled web browsers such as IE (e.g. Mozilla/4.0 (compatible; MSIE 5*, Mozilla/4.0 (compatible; MSIE 6*). This will help to reduce unexpected behavior of non-ActiveX enabled browsers during the Pre-Authentication assessment. (9064)
5. 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)
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)
7. The Host Checker and Cache Cleaner "Repeat Check" interval feature sometimes may show different access rights at the time of sign-in or in the middle of a user/admin session if the user's PC's security policies change, such as if a Personal Firewall stops/starts. This information is available in IVE logs. Administrators should be sure to specify an interval which meets their security/usability requirements. (13947)
8. The Overview page for Realms does not display the Host Checker and Cache Cleaner settings. (15154)

9. Setting the “Repeat Check” interval to 0 minutes for Host Checker or Cache Cleaner, will leave the client application running even after signing out of the IVE. The system default value is set to 10 minutes. Administrators should be sure to specify a non-zero value for this interval. This will be fixed in a future release. (13947)
10. The McAfee Desktop Firewall 8.0 Host Checking method requires that the client be running build 485 or higher. (13444)
11. 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)
12. Persistent Cookies should be disabled when using Host Checker or Cache Cleaner, due to an issue in this release. This issue will be addressed in the next release.

Customizable Login Pages

1. The total combined size of all uploaded customizable UI zip files cannot exceed 7.5 MB. (13906)
2. The Password Management pages and Defender Radius pages cannot be customized in this release. Support for customization of these pages is planned for a future release.
3. The new 4.0 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://www.netscreen.com>). (13605)

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)

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. 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)
3. 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)
4. 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)
5. 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)
6. 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)
7. 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)

8. Secure Meeting attendees using the Java Client cannot present or “share” files. (14319)
9. When creating a Secure Meeting using the MacOS Safari Web Browser, the organizer may be unable to add more than 250 attendees. (14533)
10. 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)
11. 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)
12. 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)
13. 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)
14. Signing out of the IVE using the “Sign Out” link will exit the end-user from any meetings which they are currently attending. (14742)
15. 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)
16. The Secure Meeting Java Client may not run longer than 3 hours for a single meeting. (14530)
17. 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.
18. The Meeting Schedule times displayed in the Administrator console are shown in GMT. This issue will be resolved in the next release. (15389)
19. 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)
20. If the Secure Meeting Client is installed using the Java Installation service, the language setting will default to English and not be locale-specific. This will be resolved in a future release. (15492)
21. A Secure Meeting attendee will not see the presenter’s shared applications if the presenter locks his desktop. (13961)
22. During a Secure Meeting Cluster fail-over, the Chat History will be lost. (15364 and 15364)

23. 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)

Windows based Secure Application Manager (W-SAM)

1. 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).
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. 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):
 - i. At the Command prompt, type: `net use * \\server\share /user:username`
 - ii. In Windows Explorer, go to Tools → Map Network Drive, then select "Connect using a different username".
7. Currently there is no automatic discovery for file shares in W-SAM. This may be planned for a future release.
8. Netegrity does not work through W-SAM. (13551)
9. 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.

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. 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.
12. 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.
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. For users with Netscape web browsers, in order to use W-SAM, they must first download and install an ActiveX plug-in for Netscape.
18. 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.
19. 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.
20. 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)
21. 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.
22. 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)
23. 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)

24. The W-SAM client window may display incorrect port numbers for configured hosts. The client; however, will still use the ports configured on the IVE. (15455)
25. 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)
26. 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)
27. 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.

Java Secure Application Manager (J-SAM)

1. NetScreen recommends users only use the J-SAM "Restore System Settings" (under Advanced Preferences) when J-SAM is not currently running. Doing otherwise, may cause J-SAM applications to fail or disconnect abruptly. This will be fixed in the next release. (9836)
2. Outlook 2003 is not supported with J-SAM. (8251)
3. 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.
4. 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 caveats:
 - 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.
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. 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. (9776)
8. The string "Lotus Notes - HTTP Proxy" in the application name is a reserved string for applications configured on port 1352 and cannot be used for custom J-SAM applications. (8912)
9. On Windows XP machines using J-SAM, if drive mapping (using ports 137, 138, or 139) is configured, J-SAM may leave behind a file in the user's home directory called **neoteris_read_xxxx.reg**. This file can be safely removed after the PC has been rebooted for drive mapping support. (9974)
10. 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.
11. Multiple Secure Terminal Access sessions may not work correctly if the login fails on one of the sessions. (12253)
12. 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)
13. On Windows 2000 and XP clients, the registry change made by J-SAM for Outlook cannot be performed if the client has the Microsoft Pocket PC Connection Wizard installed. (12379)
14. 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)
15. J-SAM is not supported on Windows 98 with Sun JVM. This issue will be resolved in the next release. (14800)
16. Formerly in J-SAM, if an IP address was specified in the destination server field, then the assigned loopback IP address would be 127.0.0.1. With this release, a unique loopback address (127.0.1.X) will be used, allowing support for multiple servers that are specified with IP addresses on the same port. (10235)
17. The J-SAM "Restore System Settings" window is not localized. This will be fixed in the next release. (10722)
18. Project Columbia running on NFuse is not supported.
19. During an upgrade from 3.X to 4.0, the Name field of the standard J-SAM applications Exchange, Citrix, and Lotus Notes may appear blank in the Admin UI and End-User UI. To populate these names (fix this issue), the Admin must go to Roles → <RoleName> → SAM, click on the standard application to bring up the application details page, and then click "Save Changes". This will auto-populate the Name field. This must be done for each standard application which is not showing the Name properly. (15445)

20. 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)
21. During an upgrade from 3.X to 4.0, the Name field of the Citrix application may appear blank in the Admin UI and End-User UI. This may also cause JSAM to not properly bind to the loopback addresses provisioned for Citrix NFuse, resulting in Citrix traffic not being tunneled through J-SAM. To fix this issue, the Admin must go to Roles → <RoleName> → SAM, click on the standard application to bring up the application details page, and then click "Save Changes". This will auto-populate the Name field. (15445)
22. In the 3.X release, a J-SAM user would see a warning if a web proxy had been configured on their browser. The warning would ask the user to add the J-SAM loopback addresses to the browser's exception list. In 4.0, this warning will not be displayed unless Exchange is one of the configured applications and the "Skip web-proxy registry check" is not checked. This will be fixed in the next release. (15607)
23. J-SAM and Java Rewriting are not supported when using the Mozilla 1.6 web browser.

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)

Sun JVM/Code-Signing Certificates

1. 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)
2. 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.

3. 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)
4. With Sun JVM 1.4.2, if caching is enabled, WRQ 6.0 will not load properly. (14008)
5. 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.

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 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)
3. 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.
4. 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.
5. 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)
6. 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)
7. On Windows XP Home Edition, Network Connect cannot be run with "Limited User" privileges. (13493)
8. 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)
9. 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)

10. 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)
11. 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)
12. If persistent session cookies are enabled and Network Connect is launched, the user may not be able to access any links on the IVE homepage. Doing so, may result in a login prompt instead of the desired resource. (15609)
13. Detailed rules for Network Connect ACLs are supported in this release
14. 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.

Pass-Through Proxy Issues

1. NetScreen strongly recommends Administrators not mix Pass-Through Proxy Port and Host modes.
2. Pass-Through Proxy supports using ports 11,000 to 11,099 (inclusive).
3. Siebel7 is not supported through Pass-Through Proxy. (7487)
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.
5. Pass-Through Proxy is not supported on Netscape 7.0, but is supported on 7.1. (7290)
6. 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)
7. When using Netegrity, Pass-Through Proxy requests will not be authorized against the Netegrity SiteMinder policy server. (7932)
8. When using a Netegrity authentication server and the IVE is configured for auto-login and to use the HTTP Form Post method, users may be unable to login to OWA and Lotus iNotes, if configured as Pass-Through Proxy applications. This is only for Netegrity authentication; local users are not affected. (8972)
9. 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)

10. The Alarm feature in Lotus iNotes 5.0.X versions is not supported through the IVE rewriter, but is supported using Pass-Through Proxy.
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)
12. If OWA 2003 is configured to be run through Pass-Through Proxy, then the end-user may see a JavaScript error when viewing the attendee list for an appointment/meeting. (14999)

Clustering Issues

1. IVE statistics are not synchronized in the cluster. Administrators will need to manually collect and aggregate the statistics from the individual members. This issue will be fixed in a future release.
2. 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).
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.

10. 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 cluster pair (2 nodes), the ME 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).

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

Internationalization Issues

1. 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)
2. 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)
3. Japanese characters are not supported in naming Authentication Servers. (7924)
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 ? ? | ? ? ? and ~ are not supported for filenames for UNIX Servers. (14529)
6. Filenames using 5c characters such as ? and ? will be corrupted and cannot be deleted from UNIX servers. (14348)
7. When using the Japanese language with OWA, the UI will be corrupted when the “Reply”, “Reply All”, and “Forward” buttons are clicked. (15323)
8. 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).

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 Radius Server. The workaround when fronting an RSA/ACE Server with a RADIUS server is to manually assign ACE users to Radius groups (profiles).

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

3. 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)
4. NFS file browsing requires an NIS server to first be configured on the IVE in order to work properly. (14594)

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 on their syntax. Administrators are encouraged to test ACL/Bookmark settings in a test 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. NetScreen logo and last Auth realm 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 back to the IVE. (10456)
3. 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)
4. 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. When using the auto-login function of the 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)
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. The Netegrity Policy Poll Interval only supports values of -1 and positive integers, not 0.
4. 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)
5. 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. By default, all access policies are closed, unless explicitly opened by a defined policy (e.g. 'allow' for '*').
2. Due to comprehensive changes in the Access Management model, the IVE 3.X "Import Users" functionality is not available in this release. (14940)
3. 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)
4. The "-" and " " (space) characters are not supported in the LDAP Server Catalog. This will be fixed in a future release. (14579)
5. The IVE only supports Crypt/MD5 password hashes for NIS authentication. (14228)
6. Steel-Belted Radius is not supported with the IVE when using RSA SecurID 5.0.1. (13754)
7. The ARP Ping Timeout value in the Network Settings should always be greater than 0. (13599)
8. 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)
9. 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)
10. 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)
11. 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)
12. Trying to access a Secure Terminal Bookmark which connects to a downed resource may cause the browser to appear to hang until the connection times out (~ 60 seconds). (14559)

13. 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)
14. 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)
15. When creating access policies for web resources, the Administrator should ensure that they do not include a trailing '/', as it may cause problems for end-users accessing resources without the trailing '/'. (14609)
16. Resource Policy evaluation for JSAM, 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)
17. 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)
18. Only attributes which are evaluated for a user during Role Mapping may be used for Resource Policy evaluation. (14524)
19. 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.
20. There may be some inconsistencies between the IVE Enterprises SNMP CPU/Memory utilization objects and those used in the UC Davis MIB. (14612)
21. 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. Additional MIB Browsers will be supported in a future release. (15209)
22. The SNMP **meetingUserLimit** trap is not functioning properly in this release. (15614)
23. URLs embedded in Macromedia Flash content are not currently supported by the IVE. This feature is scheduled for a future release.
24. 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.
25. 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.
26. 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.

27. For Web and file browsing access control lists (ACLs), the IVE does not currently perform reverse DNS lookups. For example, if there is 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`. The workaround is to list both the IP address and the hostname in the ACL rules.
28. 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.
29. 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>).
30. 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.
31. Occasionally you may see broken links or incomplete content when browsing Web pages. Please email a detailed description to NetScreen Support and include a complete trace of the user transaction using the built-in debugger application.
32. 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)
33. 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; };`
34. 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.
35. URLs embedded in ActiveX controls are partially handled in this release and additional support will be provided in a future release.
36. 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)
37. 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)
38. The IVE web browsing function does not support URLs more than 159 characters in length, including extensions, such as ".html". (7248)
39. 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>

40. 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)
41. 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)
42. 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)
43. The IVE does not support the import of Intermediate CA certificates; however, VeriSign and Comodo are supported internally. (5855 and 9410)
44. 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)
45. Lotus iNotes in offline mode is not currently supported. (9889)
46. Even though you enter the password to archive users and system config files, this password is disregarded on the import.
47. 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.
48. When Remote SSO is configured and later unlicensed, the "Configure Remote SSO" option will still be displayed on the end-user menu.
49. The Remote SSO functionality will not work for form pages which have been configured for Pass-Through Proxy. (10115)
50. 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.
51. 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)
52. 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)
53. When using OWA 2003, the Administrator should ensure that the OWA server has only NTLM or Basic Auth enabled, not both. (15098)
54. 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)

55. 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.
56. 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".
57. 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)
58. 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)
59. In some instances the username for various "Connection Succeeded", "Connection Denied", and "Connection Closed" log messages may be incorrect. These log messages are used by Secure Meeting, Secure Terminal Access, and applications which are accessed through the IVE Java Rewrite engine. (15267)
60. The "Enable Session Timeout Warning" option in the Delegated Administrators Roles does not work. This is by design. The settings only apply to end-user roles. This setting will be removed in a future release. (14938)
61. The Session Timeout Warning is only supported on web pages which are viewed through the IVE or the IVE homepage itself. (14834)
62. 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)
63. The Session Timeout Warning settings only apply to user sessions, not Administrator sessions. Administrator sessions will not receive any timeout warnings. (13407)
64. 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, or for W-SAM and Network Connect users. If not needed, NetScreen recommends that the Session Timeout Warning feature be disabled to minimize confusion for users of W-SAM, NC, and Pass-Through Proxy. (14831)
65. 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)
66. XML import/export for Roles and Policies does not work with Java Code Signing and Windows File Browsing Credentials resource policies. (14995)
67. Some log messages generated as a result of some end-user or Admin activity may incorrectly show up in the User and Admin access logs rather than the Event log. Such messages will display "System" in the user field of the log. This issue will be resolved in the next release. (15212, 15174, and 15064)

68. The Hostname Encoding feature does not work if the "Framed Toolbar" is enabled. This issue will be addressed in the next release. (15141)
69. 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)
70. 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)
71. Pop-Up Blockers may cause problems with any IVE functionality which uses a pop-up, for example File Uploads, Help, or if using the Admin Console, the IVE Upgrade progress window. (14873)
72. Auth servers names with more than one contiguous ' ' (space) character are not supported. (15467)
73. LDAP over TLS does not work correctly in this release. This will be fixed in the next release. (14132)
74. The Debug Log troubleshooting functionality should only be enabled after consultation with NetScreen Support. (15494)
75. The IVE has an Automatic Version Monitoring feature which notifies NetScreen what version of software the IVE is running and the Licensed Company Name via a HTTPS request from the Administrator's web browser when they log into the Admin UI. NetScreen collects this data so we are able to inform our 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.
76. User and Admin session timeout log messages may show the user's Realm Type (User or Admin) rather than the actual Realm name. (15049)
77. The Lotus Sametime Connect Audio/Video functionality is not supported using the Java Rewriter; however, the Chat functionality is supported. Both functions are fully supported through W-SAM and Network Connect. (14770)
78. 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)
79. To use OWA with Compression enabled on an A5000, Smart-Caching must be enabled.
80. To use Lotus iNotes, Smart-Caching must be enabled. Using Cache-Control: No-Store may cause the browser to appear to hang for a few seconds under Windows XP and pages may appear to load slowly under Windows 2000. (15489)

5. Supported Platforms

Please see the “Supported Platforms” document posted on the NetScreen 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