

Release Notes

Juniper Networks NetScreen-Secure Access

IVE Platform version 4.2 Build #7631



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

13 December 2004

Contents

New Features in IVE 4.2	1
Upgrading to IVE 4.2.....	1
Known Issues/Limitations Fixed in this Release	3
Known Issues and Limitations	4
Authentication	4
Password Management	5
Client-Side Digital Certificates/Cert-Based Authentication/PKI	5
Terminal Services	6
SNMP	6
Rewriter/Web Applications	8
Central Manager.....	8
Host Checker and Cache Cleaner.....	9
Secure Meeting	10
Windows based Secure Application Manager (W-SAM)	12
Java Secure Application Manager (J-SAM).....	14
MacOS Java Secure Application Manager (J-SAM)	14
Network Connect (NC)	15
Clustering Issues	16
Sun JVM/Code-Signing Certificates.....	18
Customizable Sign-In Pages	19
FIPS	19
Pass-Through Proxy Issues	19
Internationalization Issues	20
File Browsing Issues.....	20
Netegrity.....	21
Miscellaneous issues:	21
Supported Platforms	24

New Features in IVE 4.2

- Please refer to the **What's New** document for details about new features available in this release.

Upgrading to IVE 4.2

- Please refer to the **Supported Platforms** document about important information pertaining to **Microsoft Windows XP SP2 support**.
- In this release, automatic upgrades from the following releases, including from the Legacy Authentication mode, are supported:
 - 4.1.1 R2 Build 7557
 - 4.1.1 R1 Build 7387
 - 4.1.1 S1 Build 7335
 - 4.1 R3 S1 Build 7345
 - 4.1 R2 S1 Build 7373
 - 4.1 R1 S1 Build 7347
 - 4.1 S1 Build 7337
 - 4.0 P2 S1 Build 7363
 - 4.0 R1 S1 Build 7369
 - 4.0 P1 S1 Build 7365
 - 4.0 S2 Build 7367
 - 3.3.1 P2 Build 6355
 - 3.3.1 P1 Build 5847
 - 3.3.1 S2 Build 5811
 - Note: 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 4.2.
 - If using Beta software, please be sure to roll back to a prior production build and then upgrade to the 4.2 GA software so that you have a production build to roll back to if ever needed.
- As part of the AD authentication improvements in this release, all AD usernames are normalized into <domain\user> format even if the user logs into the IVE with just the username. Hence, the system variable <USER> always contains the normalized value "domain\user". If you want to use just the username without the domain component, please use one of the new system variables, e.g. <USERNAME> or <NTUser>.

This particular change in the AD authentication behavior might affect the following features in the IVE, so please make sure to review these configurations to make sure the appropriate variable is used after the upgrade.

1. LDAP Server Configuration User Filter - This applies to you if you configured a Realm with AD as the authentication server and use LDAP as the Directory/Attribute server.

If the LDAP user filter is set to "samAccountName = <USER>", then you might need to change this to "samAccountName = <USERNAME>".

2. RemoteSSO configuration: If you are passing AD username to a backend website and if the website is expecting only the username, then change the SSO variable from <USER> to <USERNAME>.

3. Bookmarks and applications: If you are passing the username in a bookmarked resource, then you may want to consider changing the variable from <USER> to <USERNAME>.

- In this release, the Integration with Netegrity has been changed so that it is more tightly coupled. One change which will occur during the upgrade is that if the IVE is configured to use Netegrity Auto-Login, and it assigns a Realm which is not configured to use the configured Policy Server as it's method of authentication, then a new Realm will be created, which is an exact replica of the existing auto-login Realm; however, it's Authentication server will be set to point to the configured Policy Server.

Additionally, when creating a new Policy Server, Administrators will not be able to configure Auto-Login until a Realm has also been created, which points to the newly created Policy Server. The drop-down list for the Auto-Login Realms will now only display Realms which are configured to use the Policy Server as its authentication server. The process for doing so would be:

1. Create the new Netegrity SiteMinder Policy Server authentication server instance on the IVE.
2. Create or modify an existing Realm to use the newly created Policy Server as its authentication server.
3. Go back to the Policy Server authentication server config on the IVE and enable Auto-Login and select the appropriate Realm. (22308)

- With the new backend SSL server certificate verification feature, upon upgrade to 4.2, Administrators may see several "Added CA Cert xyz" logs in the system event log. These logs can safely be ignored as they are merely documenting which CA certs are being established in the system for use by the new feature. (21514)
Additionally, sites which contain embedded objects which are linked from untrusted sites, will not display if the Administrator has configured the "Warn users about Certificate problems" for the user's role. (23379)
- If upgrading from pre-4.0, upon upgrade the IVE will retain any old 3.X licenses and continue to function as expected. If still using a 3.X license, in order to gain access to the new 4.X features, such as those in the Advanced model, or Central Manager, a new 4.X 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.X 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.
- In previous releases, RADIUS and LDAP attributes used underscores ("_") in place of dashes ("-"). Dashes are supported in this release. Any underscores stored in existing Role Mapping rules, will be automatically converted back to dashes; however, RADIUS attribute references used in any Custom Expressions and Policy Conditions are NOT converted, and must be converted manually. For example, the 4.0 custom expression "userAttr.Filter_Id = 'value'" could be converted for 4.1.X by changing it to "userAttr.Filter{-}ID = 'value'". The {} around the dash are required to use a dash in a variable name.
- By default, upon upgrade to 4.1.X, NC and W-SAM clients will not enable client-side logging. To enable this, visit the System → Configuration → Security → Client Side Logs configuration page.
- If using PKI Certificate Attributes in custom expressions and role mapping, be advised of changes in this release. Data will be migrated to the new variable names (17569):
 - Email certAttr.Email/certDn.Email/certIssuerDn.Email → certAttr.emailAddress/certDn.emailAddress/certIssuerDn.emailAddress
 - Given name certAttr.G/certDn.G/certIssuerDn.G → certAttr.GN/certDn.GN/certIssuerDn.GN
 - Initials certAttr.I/certDn.I/certIssuerDn.I → certAttr.initials/certDn.initials/certIssuerDn.initials
 - Title certAttr.T/certDn.T/certIssuerDn.T → certAttr.title/certDn.title/certIssuerDn.title
 - Description certAttr.D/certDn.D/certIssuerDn.D → certAttr.description/certDn.description/certIssuerDn.description

- Serial certAttr.SN/certDn.SN/certIssuerDn.SN →
 certAttr.serialNumber/certDn.serialNumber/certIssuerDn.serialNumber
 - Surname certAttr.S/certDn.S/certIssuerDn.S → certAttr.SN/certDn.SN/certIssuerDn.SN
- If upgrading an unlicensed appliance, please note that with this release, the links in the Help frame (which displays upon initial boot in the Admin UI) are not working properly. This includes the Help and Key Concepts links. After applying a license to the appliance, these links will be working once again.
 - Please review the following upgrade procedures:
 - Save a backup of the system/user configuration, log files before performing the upgrade.
 - To speed up the upgrade process and minimize downtime, we recommend you clear logs and other trace files which you have archived and then perform the upgrade. Afterwards, those archives can be re-imported. This is especially important for IVEs which have very large log files (based on the configured size limits), such as 200MB or larger, as these log files may be processed during upgrade, increasing the upgrade time significantly.
 - For upgrading clusters:
 - With Central Manager – Central Manager will detect the upgrade of a single node in the cluster, and upon its reboot/re-synch, it will instruct the other nodes to upgrade themselves automatically by sending them the service package.
 - Without Central Manager – To upgrade nodes in a cluster, the Admin should disable the clustered nodes, upgrade each node individually, and after the nodes reboot, re-enabled them in the cluster.

Known Issues/Limitations Fixed in this Release

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

1. Realm names with a “ “ (space) at the end of the name, no longer cause login failures. (19576)
2. The MSN and Google Toolbars no longer cause sign-in requests to hang. (19949)
3. Improvements have been made to clients using MacOS Safari during a meeting re-join. (19741)
4. Multiple Secure Terminal Access sessions now work correctly even if the login fails on one of the sessions. (12253)
5. Several improvements have been made when launching J-SAM on MacOS. (10766)
6. Network Connect Access Control Policies now accept multiple ports with the comma-separated notation (e.g. 20, 23). (18523)
7. Split-tunneling now works with Network Connect if the client has one or more pre-existing static routes. (19022)
8. Network Connect now properly removes the local subnet route when split-tunneling is disabled. (12221)
9. The Session Timeout Warning for Chinese now displays as expected. (19335)
10. The IP based matching for hostnames resource policy option now applies to auto-allow Windows file sharing bookmarks. (18794)
11. The IVE now honors the Netegrity Policy Server Idle and Max Session Timeout values; however, only if they are both configured. If they are not both configured or only one of them is configured, the IVE will use its configured timeouts (per Role). (18759)
12. Users with valid SMSESSION cookies that are automatically logged in to the IVE will always now be prompted to choose a role, if the Admin configures as such. In previous releases, these users had their

- roles merged automatically and were not prompted. (13651)
13. Users with expired SMSESSION cookies, will now be redirected to the configured Netegrity redirect URL, rather than seeing the IVE login page. (15247)
 14. User attributes (e.g. LDAP or RADIUS attributes) may now be used in Resource Policy rules even if they were not previously accessed during Role Mapping evaluation.
 15. The IVE now supports the import of Intermediate Server certificates. (5855 and 9410)
 16. The link on the System → Network → External → Settings tab for “Static Routes” now points to the correct configuration page. (20203)

Known Issues and Limitations

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

Authentication

1. To successfully authenticate as an administrator that belongs to the built-in Administrators authentication server or as an end-user that belongs to the IVE Authentication server, the username must always be entered in lowercase. Even if the username was created in upper case, login will fail unless the username is entered in lowercase. (24184)
2. For NT/AD Authentication, the Admin username and Kerberos realm name fields are now required.
3. The ACE Next-Pin and New-Token modes do not work properly when using ACE as the secondary login server. (21870)
4. If the Admin creates a new Authentication server, but doesn't fill out all of the required fields, and attempts to save the configuration, the configuration will fail, as expected. However, if the Admin then fills out the required fields, and saves changes, which will be successful, the new Authentication server will not work properly. This will be addressed in a future release. (23186)
5. The Realm-level option “Enable Password Management” needs to be enabled in order to allow the end-user or administrator to change their password via the “change password at next logon” (IVE Authentication – user accounts). (22969)
6. When configuring an NT/AD server for Authentication, if the Administrator username and password are set initially, then later removed (say for example if the Administrator account now has a null password), on the IVE Admin UI, even if the Admin removes the password (a series of ‘*’ characters), when the page is refreshed after the changes were saved, the password field will still show as a series of ‘*’ characters for security purposes; however, the password (in this case null) will have been saved properly. (20949)
7. The Multiple Sign-In Credentials feature is not supported for iMode devices. Administrators must create a separate sign-in URL which maps to a Realm requiring single authentication credential for Imode clients. This issue will be fixed in a future release. (22805)
8. During the AD authentication, the IVE joins the AD domain controller as a member and this allows the IVE to obtain group information for all the authenticated users. If the "IVE machine" name is manually deleted under "Active Directory Users/Computers", then the IVE takes up to 6hrs to re-join the domain controller and during this period all group lookups will fail. Hence, we do not recommend manually deleting the IVE machine name from AD console. If it was accidentally deleted, the Admin can forcibly restart all services on the IVE or reboot the IVE to allow the IVE to re-join the domain immediately. (22639)
9. When using the “Match Equivalent IP” Resource Policy option, if the hostname contains a wildcard character, such as ‘*’, this option will not work correctly and the policy rule will not be matched. (16450)
10. When using HTTP Basic Auth (in SSO), if a Realm Names (not IVE Realm but HTTP Auth Realm) is

encoded in Shift_JIS, and not UTF_8, the IVE will not properly display it. (15881)

11. When using special characters for user account names, such as “ ‘ , > , < , \$, % , etc... a JavaScript error may be displayed when accessing the server’s user listing. Administrators should avoid using characters of this type for user account names. (22452)
12. Accounts which are used for both administrator and end-user access to the IVE may conflict if they use the same username and authentication server. This may cause one another to get forced out of their IVE session when the other logs in. One simple solution is to duplicate the Authentication server on the IVE so that admin users log into one Authentication server and end users log into the duplicate and both Authentication servers (original and duplicate) point to the same backend system.
13. 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 un-check the “Sent Node Verification” setting on the ACE/Server for the IVE.
14. The IVE only supports Crypt/MD5 password hashes for NIS authentication.

Password Management

1. Password Management must be enabled at the Realm level if the Admin wishes to enable password expirations or require users to change their password at next logon.
2. When a user’s password is expired, and Password Management is NOT enabled for that user’s Realm, the error message displayed to the end-user shows “account disabled”, although this account may not truly be disabled. This will be addressed in a future release. (21654)
3. Password Management for AD (native) is not supported on the secondary login server, if it is type AD/NT. (21869)
4. When using Sun One/iPlanet as an Authentication server and enforcing both “password expiration in X days” and “allow password change after Y days”, if the user’s password is reset (or changed) then the user’s profile will have a new password expiration date. However, if the password expiration timeframe is changed (for example from 10 days to 20 days), then the user’s profile will still show the old password expiration time. This is what we adhere to. This is a limitation of Sun One/iPlanet.
5. 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.
6. 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.
7. 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 Juniper Networks Support site (<http://www.juniper.net/support/>).

Client-Side Digital Certificates/Cert-Based Authentication/PKI

1. When CRL checking is enabled, the CRL and the corresponding CA certificate need to use the same string type for Subject and Issuer fields. Otherwise, the CRL issuer DN and CA Subject DN will not match, causing the CRL download to fail.

2. Client Side Digital Certificates which contain foreign language strings should conform to certain guidelines in order to successfully work with the IVE. We support the following string types for subject and issuer DN fields: PrintableString, IA5String, BMPString, and UTF8String. The IVE has only partial support for T61Strings containing only European characters. Asian languages should use BMPString or UTF8String for DN values. (18305)
3. The IVE CRL checking mechanism will ignore the IssuingDistributionPoint CRL critical extension if included in the CRL object.
4. CRL download via HTTP Proxy is not supported.
5. Partitioned CRLs are not supported in this release. (16992)
6. 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.

7. Certificate users may get an HTTP 500 error if the end-user gives a wrong password for their private key file when challenged for a client certificate. (13489)
8. When using LDAP for a CDP, port numbers should not be specified in the CDP Server field. The default port number for LDAP is 389. To use a non-standard port, Manual CDP configuration should be used. (18578)
9. 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)

Terminal Services

1. The Terminal Services feature does support local drive mapping, however there is a Microsoft limitation Win2K that drive mapping is not allowed via RDP clients so this feature works only on Win2K3 until Microsoft establishes a fix.
2. For Citrix Terminal Services when using "Download from Citrix web site" or "Download from the URL..." options, the Admin needs to create a Caching policy for these Web client URLs. For "Download from Citrix web site", the Admin needs to create a Caching Policy for <http://download2.citrix.com/files/en/products/client/ica/current/wficat.cab>. For "Download from the URL", the Admin needs to create a Caching Policy for the URL entered on the Admin console. The Caching policy for these URLs should be set to "Cache (do not add/modify caching headers) and can be found at Resource Policies > Web > Caching. For ore information on the Caching Resource Policies, refer to the administrator's guide. (23064)

SNMP

1. When using the log alert SNMP functionality in a cluster, if a log alert is disabled for one node, it may cause other nodes to no longer send that alert. (22647)
2. 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.

3. There may be some inconsistencies between the IVE Enterprises SNMP CPU/Memory utilization objects and those used in the UC Davis MIB.
4. 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.

Rewriter/Web Applications

1. If using Safari on MacOS to access a web page through the IVE Rewriter, some pages may show up blank if the IVE Toolbar is enabled. Workarounds include refreshing the web page, or switching to the IVE Framed Toolbar.
2. The Documentum web application is not supported by the IVE Web Rewrite function.
3. Lotus iNotes in offline mode is not supported. (9889)
4. The correct caching resource policies must be configured to enable end-users to open and save email attachments in OWA. The “Smart Caching” option works for all document types other than text and html. To save attachments of type text and html, the cache control policy for these file types must be set to “Cache Control No Store”.
5. To enable iNotes users to open and save documents of type zip, Excel, pdf etc, the Web -> Caching resource policies must be configured to “Cache Control No Store”. For Word documents, a caching policy of “Smart Caching” is supported. The reason for this distinction is that the Domino server correctly identifies just the Microsoft Word documents and not any of the other document types.
6. 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)
7. 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)
8. 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)
9. Lotus Sametime Connect Chat functionality is supported only when using Web rewriting and J-SAM. Full Sametime connect functionality is supported using W-SAM and NC. 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.
10. When using iNotes with Cache-Control: No-Store, the browser may appear to hang for a few seconds under Windows XP and pages may appear to load slowly under Windows 2000.
11. To use OWA or Lotus iNotes with Internet Explorer with Compression enabled on an SA5000, Smart-Caching must be enabled. More information can be found at the following locations (15383):
 - <http://support.microsoft.com/default.aspx?scid=kb:en-us:825057>
 - <http://support.microsoft.com/default.aspx?scid=kb:en-us:312496>
 - <http://support.microsoft.com/default.aspx?scid=kb:en-us:325212>
 - <http://support.microsoft.com/default.aspx?scid=kb:en-us:327716>

Central Manager

1. The Dashboard graphs may not display properly if the IVE system time has been adjusted back too many hours or days in time before the data was recorded. (16920)
2. If the IVE system time is changed, the graphs displayed on the Dashboard may be shown incorrectly.
3. Push Config only pushes Web Proxy policies, but not the proxy server configuration. (14949)
4. Push Config is only supported among IVE Platforms running the same version/build.
5. Push Config supports up to 9,999 users when pushing Authentication Server config. (22165)

Host Checker and Cache Cleaner

1. A Value of ZERO in the Host Checker or Cache Cleaner “Client Idle Process Timeout” field will cause Host Checker or Cache Cleaner to go into a loop. This will be resolved in a future release by enforcing input validation for this field. (23134)
2. If using detailed policy rules, the expressions *CacheCleanerStatus = 0* is not evaluated correctly in this release. (23097)
3. If a “Restricted” user runs Host Checker, any checks to privileged locations or privileged directories in the registry are prohibited as a result of lack of privileges.
4. If a “Restricted” user runs Cache Cleaner, they will not be able to clean directories that are in privileged root directories, for example, *c:\program files\...*
5. If the 3rd Party Package for Sygate On-Demand Virtual Desktop is used, Administrators should be sure that the Virtual Desktop Policy is set to "Evaluate and Enforce". A sub policy for Virtual Desktop, VSDCheck, should not be enabled for Evaluation or Enforcement. Users will be taken into a Virtual Desktop and, within the VD they will be able to log into the IVE using a web browser. If VSDCheck is enabled for Evaluation and Enforcement, the user would NOT be able to log in. Juniper is working closely with Sygate to resolve this issue. (22995)
6. There are known clean-up problems in Cache Cleaner deleting any Admin-specified directories on Win98 clients. Any folder that is not in the user profile directory will not be deleted by Cache Cleaner. (22989)
7. 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.
8. 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.
9. In this release, Host checker and cache cleaner policies configured at the authentication Realm are evaluated and enforced at every host checker and cache cleaner update interval. Please note that in the previous release, only Role based HC/CC restrictions and resource policies are evaluated dynamically on every status update.
10. In some situations, such as if the connection between the end user machine and the IVE is not reliable, the cache cleaner and host checker status updates may not be received by the IVE within the configured time interval and therefore a user’s session might terminated. This happens when host checker or cache cleaner based policy enforcement is configured at the Realm or role level.
11. When Cache Cleaner is configured to remove content from specific hosts/domains, some associated web browser history may not get entirely removed. The user may manually delete the entire browser history if they so choose. (17124)
12. If two or more admin or end-user sessions to a specific IVE are initiated from a client, and at least one of them deploys Host Checker and/or Cache Cleaner, the sessions will be affected in unpredictable ways. Symptoms can range from HC & CC being shutdown to loss of role privileges and forced log outs.
13. 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 to fail.
14. After un-installing Host Checker, the Program Group may still exist in the user’s Start menu. This Program Group can be safely removed. (9057)
15. For certain Windows system services (e.g. *smss.exe* and *naPrdMgr.exe*), Host Checker will fail if the MD5 checksum is used to validate the executable. In such cases, Host Checker is unable to find the path, due to the manner in which Windows loads the process table. This should not be an issue for end-user client applications, such as a personal firewall or virus scanner. (10819)

16. When the security posture of an endpoint changes (e.g. a Personal Firewall starts/stops) there is latency between the time of this event and the corresponding policy changes on the server. For example, a user who is denied access due to the absence of a firewall process will not immediately be allowed access upon starting the firewall. The end user will need to wait until the policy is refreshed, which is governed by the Host Checker frequency. One way to overcome this is to delete the cookies from the IVE prior to restoring the security posture. (13947)
17. The McAfee Desktop Firewall 8.0 Host Checking method requires that the client be running build 485 or higher.

Secure Meeting

1. Extremely high values for the idle timeout and maximum session timeout will block a user from launching the meeting client. A value that is less than 600 minutes is recommended for idle or maximum session timeouts. (22982)
2. When using the Java client to launch a Secure Meeting if the user clicks "No" on the certificate warning presented by the JVM, the meeting client will not launch but it will appear to the user as if the applet is still loading (22712).
3. Full screen and Remote Control modes are not supported on the java client. (23148)
4. When using the annotation capability of the Secure Meeting white boarding feature, after the user has been granted access to draw, the button to disable drawing access is not working properly in this release. (22893)
5. If using a MacOS or Linux Secure Meeting client, if the IVE restarts or the clients somehow lose connectivity to the IVE, they will not automatically reconnect. (23002)
6. If an attendee joins a meeting after sharing and remote control has been enabled for some other meeting attendee, the new attendee's meeting client may show the wrong remote controller designation. (22908)
7. On the appointment tab in the Microsoft Outlook Calendar is a check box called, "This is an online meeting using..." This checkbox is not related to the Meeting Server or the Secure Meeting for Outlook Plug-in. This field cannot be used by a third party plug-in.
8. When installing the Secure Meeting plug-in on Microsoft Outlook 2000, a message appears warning that "the form you are installing may contain macros". Users may safely click either "Disable Macros" or "Enable Macros" since the Secure Meeting form does not contain macros. (21408)
9. The end-user must use the same Outlook profile to un-install the Secure Meeting Plug-In for Outlook as the one used to install the Plug-In. Switching profiles between the installation and un-installation of the Plug-In is not supported. (22655)
10. The locale for a meeting presenter running on a Mac OS X is based on the setting on the Macintosh rather than the setting in the IVE administrator console. (19573)
11. On the Macintosh and Linux platforms, even if the viewers are set to full screen mode, the toolbar will still be visible. (19506)
12. It is recommended that the Meeting IVE not be upgraded while Secure Meetings are running on Macintosh or Linux machines. If an upgrade is run during a Secure Meeting, Macintosh and Linux users may not be able to launch the client for a new meeting. This is due to bugs in the Safari and Mozilla browsers related to caching of Java applets. The user must quit and restart the browser to fix the problem. (22273)
13. When scheduling a meeting from Microsoft Outlook 2000 using the Secure Meeting Plug-in, the user must click "Delete Meeting from Server" on the Secure Meeting form to delete the meeting. The Delete button on the Outlook form will not delete the meeting from the meeting server. This is due to a bug in Microsoft Outlook. (21336)

14. When the presenter selects "Enable drawing for all attendees", the permission is granted to those attendees that are currently in the meeting. For all future attendees, the presenter has to individually grant permissions. When granting permission, the presenter may see an error message "Failed to change roles". (22777)
15. When the user launches Secure Meeting, he will see a Security Warning due to the SSL negotiation between the client and the IVE. The user must respond to the warning within 15 seconds for the meeting client to launch successfully. (22711)
16. Annotations on viewers' screens may be positioned incorrectly if the annotator's window has scroll bars. It is recommended that annotation be done with the viewing/annotating window in full screen mode. (22769)
17. Safari 1.0 has a bug wherein it does not fully support proxy configurations. As a result, the meeting client cannot be launched from this browser, if there is a proxy configured. We are working with Apple on this issue.
18. When using two IVEs in a Secure Meeting Cluster, users should always connect to the VIP address to join the Secure Meeting; not the IP address of the physical machine.
19. Red Hat Linux 9 with Mozilla 1.6 and SunJVM 1.4 has a problem with NTLM authentication when using ISA proxy server to download the Secure Meeting .jar file. This will cause the Secure Meeting client to not download properly.
20. When using MacOS 10.3.3 and Safari 1.0, if the user clicks "NO" on the certificate pop-up, the Secure Meeting client will not install. If the user wishes to try again and this time click "YES", they must first restart their Safari browser.
21. 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.
22. 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.
23. 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.
24. When creating a Secure Meeting using the MacOS Safari Web Browser, the organizer may be unable to add more than 250 attendees.
25. 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)
26. Secure Meeting attendee will not see the presenter's shared applications if the presenter locks his desktop.
27. Secure Meetings in progress will be stopped if a cluster is created during the meeting.
28. On a Windows platform, the meeting client picks up the proxy information from the IE browser settings. Hence, meeting will work on other browsers only if the proxy setting, if any, is also configured in IE. (17442)

Windows based Secure Application Manager (W-SAM)

1. Restricted Users can't install W-SAM using the Standalone Installer even with the presence of Installer Service. Installer Service is designed to provide application installation capability for users who are doing a standard Web-based install against the IVE. (22454)
2. If an XP client has Fast User Switching enabled, and a user is logged in as two separate users actively, and switching between them, W-SAM upgrade notifications could get crossed between these active user sessions. (23090)
3. Restricted Users who force W-SAM to "suppress the LSP conflict Dialog Box" will do so for good. Any future re-installations of W-SAM will not reset this setting. (22863)
4. Customers should be aware that Venturi Wireless Client is not written to interoperate with other well-designed LSP providers. When Venturi Wireless is installed on a system that has the Juniper Windows Secure Application Manager (W-SAM), the system could become unstable. Please be aware that Juniper does NOT claim compatibility with the Venturi Wireless client. (19690)
5. If using W-SAM in Host Mode with a host of '*:*', the PC may use existing cached name/DNS lookups if they exist, rather than performing a new name/DNS lookup (which W-SAM will intercept). This may cause the DNS resolution to be incorrect. (19519)
6. When downloading a file via FTP through Internet Explorer over a W-SAM tunnel, large files (>15MB) may cause IE to timeout unexpectedly. (18635)
7. When using SamLauncher with Persistent Cookies are enabled, launching SamLauncher again immediately after stopping W-SAM from a valid and authenticated session will cause the session to be authenticated using the Persistent Cookie even if an invalid username and/or password was entered from the command line. (19521)
8. If an end user attempts to un-install W-SAM through the Preferences form, and selects 'No' when asked to reboot, W-SAM will be partially un-installed from the client, and subsequent attempts to un-install W-SAM will fail. To complete the W-SAM un-installation, the user has two options. (1) From the Start Menu, run "Programs > NetScreen > Windows Secure Application Manager > Un-install W-SAM". (2) Run the application "c:\Program Files\Neoteris\Secure Application Manager\sameclean.exe".
9. W-SAM will not launch on Chinese (simplified & traditional) Win2K if msvcp60.dll, the Microsoft C++ Runtime Library, is missing.
10. When using the Command-Line W-SAM ("SamLauncher"), the URL entered must contain the prefix https://.
11. If you have the NCP Auto-select disabled, and click 'No' to the security warning during load time, then W-SAM will not initially launch; however, there is no additional impact to the user session." (18681)
12. 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)
13. 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, Juniper Networks recommends using Network Connect (SSL-VPN access).
14. To access a windows file share using W-SAM by hostname, the administrator must explicitly configure the server's NetBIOS name (alphanumeric string up to 15 characters) in the W-SAM Destination Host configuration page.

15. 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 for security purposes.
16. 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 un-installed.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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 via Cache Cleaner or manually after exiting W-SAM.
24. When end-users choose to un-install W-SAM through the System → Advanced Preferences page, the file NeoterisSetup.cab is deleted from the user's system. The effect is that the 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.
25. Currently there is no automatic discovery for file shares in W-SAM.
26. 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.
27. To run Citrix NFuse through W-SAM, you must define a Caching rule to cache launch.asp files. For example, configure resource policy to "<server name>:80,443/*launch.asp" and the Caching Option to "Cache (do not add/modify caching headers)".
28. 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:

- A. At the Command prompt, type: `net use * \\server\share /user:username`
 - B. In Windows Explorer, go to Tools → Map Network Drive, then select “Connect using a different username”.
29. When scripting the use of SamLauncher.exe, users should provide the `-reboot` command-line flag, so that if the launcher requires a reboot, it will happen automatically and not exit, prompting the user to manually reboot. Please also note that during a fresh install (with NetBIOS enabled), W-SAM will require a reboot.
 30. When a W-SAM user connects to an IVE with an earlier build version, W-SAM does not downgrade completely. The user will need to run the Samclean executable (with admin privileges) and install W-SAM fresh.

Java Secure Application Manager (J-SAM)

1. Outlook 2003 is not supported with J-SAM. (8251)
2. When using a static loop back address for a J-SAM application server configured on multiple ports, modifying that loop back address will require the admin to delete all applications referring to this application server and re-enter these applications with the new static loop back address. (22911)
3. When using Mac OS 10.2.8 and Safari 1.0.3, adding/removing a J-SAM application as an end-user may result in a blank page. However, the application list does get updated. (22672)
4. When running J-SAM on a MacOS X client, if the user clicks "No" on the SSL certificate warning, if there is one, the user must quit and restart the browser in order to launch J-SAM successfully.
5. 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:

```
grant { permission java.security.AllPermission; };
```
6. 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.
7. 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.
8. 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)

MacOS Java Secure Application Manager (J-SAM)

1. The Client/Server Session Recording functionality for use with Java Applet Rewriting and J-SAM is unavailable for J-SAM for MacOS.
2. When auto-launching J-SAM using Safari (versions prior to 1.2), J-SAM will open a new browser window to display the home page instead of updating the original window that launched J-SAM. This results in two open browser windows. This is due to a limitation in these versions of Safari. (21747)
3. On a Mac OS X, the first time J-SAM is launched after a reboot of the machine, the launch may fail. This is due to a bug in Apple's JVM code. (Apple Bug #3860749). (21746)
4. Citrix NFuse integration is not available on MacOS using Safari browser. (10780)

Network Connect (NC)

1. Network Connect Proxy Support Chart:

	<i>Explicit Proxy to get to IVE</i>	<i>Pac file to get to IVE</i>	<i>Explicit Proxy to get to Internal Applications</i>	<i>Pac file to get to internal applications</i>	<i>Hybrid: Proxy to get to IVE and Proxy to get to Internal applications</i>
<i>Split Tunneling Enabled</i>	<i>Supported</i>	<i>Not Supported</i>	<i>Supported</i>	<i>Supported</i>	<i>Not supported</i>
<i>Split Tunneling Disabled</i>	<i>Supported</i>	<i>Supported</i>	<i>Supported</i>	<i>Supported</i>	<i>Not supported</i>

2. The supported scenarios for NC are only when single client PC NICs are used throughout the NC connection. Any scenario involving switching NICs might work, but is not guaranteed. The recommended behavior for the customer for switching NICs would be to end their session, switch the NIC and then restart NC again. This is especially important when not using software such as IBM access connection manager that has a clean solution for switching which NIC is enabled. (22806)
3. If the client PC's web browser proxy is set to use a PAC script with a hostname:port, and not just a hostname, NC will not behave as expected. Using just the hostname, or an IP:port, works. (23184)
4. When split-tunneling is enabled, and the client PC is "suspended", after a resume, the NC client may still be running for a few moments even though it has been disconnected due to the PC being suspended. With split-tunneling disabled, NC will exit immediately. (23141)
5. If a Restricted user has Network Connect installed on their system, Network Connect can only be un-installed if a user with Admin privileges attempts to run the un-installer, or the Installer Service is installed. (22200)
6. After the IVE is upgraded, some remote users may encounter an "indefinite disconnect" of Network Connect of prior releases. If a user sees their Network Connect client (NCUI.exe) in a "Grayed out" mode within the system tray for any longer than 2-3 minutes, the user should uninstall Network Connect and then install the new version of Network Connect again. (23043)
7. There are known issues with Network Connect and Nortel Contivity VPN client v. 4.65 specifically in environments where client machines have to connect to the IVE using a client-side web proxy. In these situations, the presence of Nortel Contivity forces a state where the user won't be able to access the Corporate Intranet applications through NC. Un-installing the Contivity VPN Client fixes the problem. (21125)
8. If Palm Desktop or Hot-Sync software is being used, please make sure to force the software to bind to USB ports rather than Serial interfaces. If the user's machine does not support USB, the user should select a physical COM port instead of the virtual COM port NC installs. (20598)
9. When accessing a resource on the remote network (behind the IVE) which is on a different subnet from the IVE internal interface, the remote machine/server may not know how to route back to the client IP network which the IVE issued from its configured IP pool. To work-around this, a static route should be added to the router between the IVE's internal interface's network and the remote network to route packets destined for the IVE's NC IP Pool to the IVE's internal interface.
10. Network Connect will not work if the physical connection is a modem dial-up, and there is a connection entry which accepts incoming modem connections.

11. 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)
12. 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.
13. 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.
14. Users with only “Guest User” privileges will not be able to run Network Connect. Furthermore, Guest Users cannot un-install Network Connect. Any attempt in doing so may only partially un-install Network Connect and could leave some files behind, resulting in a corrupted Network Connect installation.
15. Network Connect cannot be run with “Limited User” privileges. (13493)
16. 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.
17. 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.
18. In some rare instances, Network Connect install/upgrade could result in a “RAS Error” message. If this message appears, then re-initiating the Network Connect install again should resolve the issue. If it is an upgrade, un-installing previous version of Network Connect (from the IVE UI or from Control Panel) and re-installing newer NC should resolve the issue. Deleting the Network Connect Dial-up adapter and re-connecting to NC should also resolve the issue.
19. TV Media spy ware (tvm.exe) is known to cause conflicts with Network Connect. Please ensure that this application isn't in play with the current configuration.
20. Downgrading from 4.1.X or 4.2.X ActiveX to 4.0 standalone NC installer gives 1078 error.

Clustering Issues

1. If a network problem causes a node in a cluster to not be able to communicate with other nodes, but other nodes can reach (“see”) that node, then cluster synchronization will fail. Network administrators should confirm connectivity using ping and traceroute tools available from the IVE troubleshooting menu. (18112)
2. In an Active/Passive scenario, using the default cluster/network configuration, under heavy load, Administrators may see the VIP switch back and forth among the two nodes every 6 to 8 hours. If this occurs, the Administrator may increase the ARP timeout value from the default 5 seconds to 10 seconds.
3. When using Virtual Ports in a non-cluster configuration or when using an Active/Passive cluster configuration, and then creating an Active/Active cluster, the joined nodes will lose their Virtual Port IP address information and they will need to be manually reconfigured using unique IP addresses.
4. When an Active/Active cluster is converted to an Active/Passive cluster, Virtual Port configuration will be copied to the backup cluster node from the node which the Admin is making the change. This copy

will cause Virtual Port configuration on the backup node to be overwritten with the master's Virtual Port configuration.

5. 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).
6. 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.
7. If deploying large clusters in a multi-site environment, if the connectivity between nodes is unstable, when a node joins the cluster it may get stuck in a synchronization loop until it gets fully synchronized with the other nodes. During this time, the node will show as "transitioning" in the Cluster Admin UI; however, when this occurs the IVE will be unable to service end-user requests. If the node remains in this state, the Admin may consider rebooting the node, and then during its boot, use the clustering options to remove it from the cluster. The node can then rejoin the cluster after the network connectivity between nodes has stabilized. (21479)
8. 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.
9. 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.
10. 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.
11. Changing the network 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 network settings, and then re-enable the cluster member in this scenario.
12. 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.
13. When creating an Active/Passive cluster, the administrator must enter values for both the *internal* and *external* interfaces. This is not a mandatory field, but is required for Active/Passive clustering.
14. 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.

15. In a Multi-Unit Cluster consisting of three nodes or more, there are three configurable options for setting the synchronization type:
 - **Unicast** – The IVE sends the same message to each node in the cluster
 - **Multicast** – The IVE sends one message to all cluster nodes on the network
 - **Broadcast** – The IVE sends one message to all machines on the network but non-clustered nodes would drop this message, as it was not intended for them

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

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

16. Clustering is not supported when an IVE is configured to have the same subnet for both the *internal* and *external* interfaces.
17. 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.
18. In an Active/Passive cluster with both internal and external interfaces enabled on each node, if the external gateway is unreachable, the external VIP will not fail over. Administrators should ensure gateways are reachable – either by using the ping tool in the IVE, or monitoring the logs to look for "external gateway unreachable" entries.

Sun JVM/Code-Signing Certificates

1. 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.
2. 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.
3. If users delay in responding to the web server security warnings then Java applets may not load. This includes J-SAM 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)
4. Due to a bug in Sun JVM, when users close their web browser window, it may seem to timeout. 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.
5. With Sun JVM 1.4.2, if caching is enabled, WRQ 6.0 will not load properly. (14008)

6. The policy tracing logs for when code signing certificates are used to re-sign Java applets is not accurate. Use the Simulation tool instead for troubleshooting purposes. (17411)

Customizable Sign-In Pages

1. To make sure that the New Pin and Next Token pages are customized for SoftID authentication, the administrator should copy the file NewPin.shtml to GeneratePin.shtml in the softid.zip and upload the modified zip to the IVE for the custom sign-in page.
2. The total combined size of all uploaded customizable UI zip files cannot exceed 12MB.
3. The new 4.X sign-in pages now offer additional customization for labels and informative text. By default, the text strings are in English. Administrators supporting non-English users may need to configure the sign-in pages to provide localized text labels. This can only be done on a per-sign-in page basis. For multi-language support, Administrators must configure different sign-in pages for different locales. For further customization, Administrators may upload their own customized sign-in pages using the Template Toolkit. Please contact Juniper Networks Support for details (<http://www.juniper.net/support>).
4. When creating customizable sign-in pages, Administrators should remember to save them as UTF-8.

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.
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.
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).

Pass-Through Proxy Issues

1. Cookies are not saved for hostnames which contain a “_” (underscore) due to a bug in Internet Explorer. For more details, see: <http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q275033>. (22614)
2. The Lotus iNotes welcome page is not rewritten if the IVE is intermediating the content through Pass-Through Proxy. (9236)
3. Pass-Through Proxy URLs must be hostnames. Paths off hostnames are not supported.
4. Juniper Networks strongly recommends Administrators not mix Pass-Through Proxy Port and Host modes.
5. Siebel7 is not supported through Pass-Through Proxy.
6. Using Mozilla with Pass-Through Proxy (with the IVE port configuration), the IVE may invalidate the user session causing the user to have to login again.
7. Pass-Through Proxy is not supported on Netscape 7.0, but is supported on 7.1. (7290)
8. 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'.

9. When using OWA through Pass-Through Proxy, if a user replies to or creates a new email, the recipient may receive a JavaScript error if they view the email through their Outlook client. (9233)

Internationalization Issues

1. When launching W-SAM on a Chinese OS with the language setting [ZH-CN] (Chinese (China)), the W-SAM GUI will launch with Traditional Chinese instead of Simplified. (22876)
2. With localized Pocket PCs, such as Japanese Pocket PC, the locale is not sent in the HTTP header, and thus the IVE is unable to detect which language to return, so English is returned by default. (22041)
3. Internet Explorer may truncate the Japanese filenames if they are too long. Additionally, some Excel files cannot be saved. More details can be found about this non-IVE issue at: <http://support.microsoft.com/?kbid=816868>.
4. 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*.
5. 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".
6. 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.
7. Special characters such as ①, I, ¥, and ~ are not supported for filenames for UNIX Servers.
8. Japanese characters are not supported in naming Authentication Servers.
9. Filenames using 5c characters such as 表 and 工 will be corrupted and cannot be deleted from UNIX servers.

File Browsing Issues

1. When opening a file in the Japanese locale the URL displayed in the Internet Explorer title bar and the URL bar is garbled. The file when viewed is displayed correctly. This is due to a bug in Internet Explorer. (19612)
2. Depending on the web browser, download files through the IVE with filenames of length 18 to 25 characters may not work. Files with longer or shorter filenames are OK.
3. 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.
4. 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)
5. NFS file browsing requires an NIS server to first be configured on the IVE in order to work properly. (14594)

Netegrity

1. 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.

Miscellaneous issues:

1. On the Preferences > Applications page for end-users, there are links to uninstall applications even if those applications are not installed or available on the client PC (such as if they are not using a Windows PC). (22978)
2. When using FTP Archive, if the Admin selects “clear log after archive”, the logging system may behave unexpectedly and new log entries will not be displayed. To resolve, the Admin may clear the log manually. This will be fixed in a future release. (23093)
3. For the Customizable Help Link, the Administrator must specify a pre-rewritten URL (a URL which was rewritten through the IVE already) if he wishes to link to an internal (rewritten) server which contains the help information. The alternative is to link to an external URL, which must be accessible by end-users without going through the IVE. (22552)
4. With FireFox 1.0, the Collapsing/Expanding of the Admin Hierarchical menus works; however, the icon ”-“ does not change to a ‘+’ as the Admin would expect. (22665)
5. If you use a multi-valued attribute in the bookmark name, only the first value is displayed for all the expanded bookmarks. (21629)
6. If the Admin submits some change and then closes the Task Guide or presses Back in their browser window, he may receive a prompt to repost form data. If this happens, the Admin may click cancel, and then Back. This is because closing the Task Guide, or pressing Back after some other page submit will go and try to reload the previous page, which was a submitted form. (22039)
7. Importing the system config does not import SSL Intermediate CA Certs (chains). (21040)
8. The format of the logs for system-generated events may show () and [], both of which can be ignored, as system events do not have an associated Realm or role name. (22321)
9. When "High browser security is enabled", a user might see a pop-up warning that is displayed confirming whether the Java Applet should be downloaded or not. There is nothing that Juniper Networks can do to suppress this warning message as it is a function of the browser. (21865)
10. Juniper Networks recommends that all un-installs of client applications (e.g. NC, W-SAM) happen against the Un-install link of the Un-installers UI under Preferences > Applications. (20415)
11. The OpenWave Simulator only supports making an SSL connection if the server, or in this case the IVE, signed by one of the following RootCAs: CyberTrust, Certicom, Diversinet, Entrust, GlobalSign, and VeriSign.
12. With log filtering, when using the *role* variable, the value must be contains within quotation marks, for example: role = “Users”.
13. When using the serial console troubleshooting tools, such as ping, if the tool becomes unresponsive CTRL+C should be used to terminate the tool and go back to the menu.
14. Web Server SSL Certificates issued by the IPSAC root are not supported by the IVE. SSL Certificates of the Netscape format must include the SSL Server Bit set in the “Netscape Cert Type” extension. Key Usage, Extended Key Usage, and Netscape Cert Type are all required for these certificates to work properly.

15. When upgrading to 4.1.X+ and using a temporary license generated for IVE 3.3, after the upgrade, the license time remaining may show incorrectly. To resolve this, please contact the Support department. (17918)
16. NFS Auto-mount is not supported with Linux NIS/NFS servers, only Sun servers. (2005)
17. In some locations throughout the Admin UI, drop-down select boxes may disappear during navigation through the left-hand hierarchical menu system. To make these select boxes reappear, simply move your mouse off of the left-hand menu. (17934)
18. By default, all access policies are closed, unless explicitly opened by a defined policy (e.g. 'allow' for '*').
19. The acceptable range of Session Time Warning values has changed in IVE 4.X. 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)
20. Due to lack of support in Microsoft Windows for certain SSL libraries, the best practice recommendation for the IVE is to configure any user roles to use non-optimized NCP for Windows NT, Windows 98 SE, and Windows ME clients when using W-SAM, Network Connect, or Secure Meeting.
21. 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)
22. 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.
23. The ARP Ping Timeout value in the Network Settings should always be greater than 0, else network connectivity may behave unexpectedly.
24. 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.
25. 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)
26. Resource Policy evaluation for J-SAM, W-SAM, Secure Terminal Access, Web, and File resources are not evaluated for already-established "in-flight" connections – they are only evaluated at the beginning of a transaction. A transaction is defined in the following way: Web – HTTP Request, Files – Upload/Download of a file or listing of shares/files, SAM – Beginning of a new connection to a backend resource. Support for this will be added in a future release. (14476)
27. 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.
28. 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.
29. 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.
30. 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)

31. 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; };**
32. 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.
33. The Stop button in the Secure Terminal Access window does not work when using Netscape 7.1 on MacOS X. (23063)
34. 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.
35. 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>
36. The IVE web browsing function does not support URLs more than 159 characters in length, including extensions, such as ".html".
37. The IVE toolbar should be disabled to view OWA pages with Safari browser. If the 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.
38. Even though you enter the password to archive users and system config files, this password is disregarded on the import.
39. 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.
40. 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.
41. 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)
42. 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.
43. When using OWA 2003, the Administrator should ensure that the OWA server has only NTLM or Basic Auth enabled, not both. However, Juniper recommends enabling at a minimum NTLMv2 or Kerberos-based authentication.
44. 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.
45. 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".
46. 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.
47. 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.
48. The Session Timeout Warning is only supported if the user is viewing web pages through the IVE (i.e. rewritten web pages) or the IVE homepages themselves. It is also supported if the user is running J-SAM. The warning will not be supported with W-SAM or Network Connect. We recommend that the Session Timeout Warning feature be disabled to minimize confusion for users of W-SAM and NC.
 49. 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.
 50. 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.
 51. 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.
 52. There are known issues with Microsoft's Popup blocker being enabled and certain OWA 2003 scripts not being able to run when being accessed through the IVE. Users could see "Script" errors in this case. Juniper Networks recommends that Popup blockers be disabled and that the user refreshes their OWA session after disabling the Popup blocker. Additionally, Popup blockers may cause problems with other IVE functionality which uses a pop-up, for example File Uploads, online Help, or on the Admin Console, the IVE Upgrade progress window, Dashboard configuration page, and Server Catalog configuration pages. (23092)
 53. The Debug Log troubleshooting functionality should only be enabled after consultation with Juniper Networks Support.
 54. The IVE has an Automatic Version Monitoring feature which notifies Juniper Networks what version of software the IVE is running and the Licensed Company via an HTTPS request from the Administrator's web browser upon login to the Admin UI. Juniper Networks collects this data to be able to inform customers about critical security patches they may need. Administrators can enable/disable this functionality by logging into the Admin UI and going to the Maintenance → System → Options menu. Juniper Networks strongly recommends that Administrators keep this setting enabled.

Supported Platforms

Please see the "Supported Platforms" document posted on the Juniper Networks Support Site (<http://www.juniper.net/support/>) under "IVE OS" 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 open a case or to obtain support information, please create an online on the Juniper Networks Support Site: <http://www.juniper.net/support>.