

Release Notes (Rev. 4)

Juniper Networks NetScreen-Secure Meeting

IVE Platform version 5.0 R1 Build #8555



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

31 May 2005

Contents

Admin Guide Correction	1
New Features in IVE 5.0 R1	1
Upgrading to IVE 5.0 R1	1
Known Issues/Limitations Fixed in this Release.....	3
Known Issues and Limitations	4
Authentication.....	4
Local Authentication - Password Management.....	5
Client-Side Digital Certificates/Cert-Based Authentication/PKI.....	6
SNMP	6
Rewriter/Web Applications.....	7
Central Manager	8
Host Checker and Cache Cleaner	9
Secure Meeting.....	10
Administration.....	13
Clustering Issues.....	13
Sun JVM/Code-Signing Certificates	15
Pass-Through Proxy Issues.....	16
Internationalization Issues.....	17
File Browsing Issues	17
XML Export	17
Miscellaneous issues:.....	18
Supported Platforms.....	22

Admin Guide Correction

The following features documented in the admin guide will not be available in IVE release 5.0 R1

- Push Configuration
- XML Import

Administrators are recommended to use the binary import/export feature to import or export IVE configuration.

(Binary Import/Export is available through
Maintenance > Import/Export > Configuration and
Maintenance > Import/Export > User Accounts)

New Features in IVE 5.0 R1

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

Upgrading to IVE 5.0 R1

- Please refer to the **Supported Platforms** document for important information pertaining to Microsoft Windows XP SP2 support.
- Automatic upgrades from this release from the following releases are supported in this release (including from the Legacy Authentication mode):
 - 4.2 R5 Build 8539
 - 4.2 R4 Build 8375
 - 4.2 R3 Build 8175
 - 4.2 R2 Build 8047
 - 4.2 R1 Build 7803
 - 4.2 GA Build 7631
 - 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 listed here, please upgrade to one of the listed releases first, and then upgrade to 5.0 R1.
- If using Beta software, please be sure to roll back to a prior production build and then upgrade to the 5.0 R1 software. (This process enables you to roll back to a production build if ever needed.)
- With the backend SSL server certificate verification feature introduced in 4.2, Administrators may see several “Added CA Cert xyz” logs in the system event log. You can safely ignore these logs as they are merely documenting which CA certs are being established in the system for use by the new feature. (21514) Additionally, sites that contain embedded objects that 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 retains any old 3.X licenses and continues to function as expected. In order to gain access to the new 4.X features, however, such as those in the Advanced model or Central Manager, you must apply a new 4.X base model license to the IVE. This is now called either the “Baseline” or “Advanced” model license. During this process, the IVE removes the old license and replaces 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.
- 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 work.
- Please review the following upgrade procedures:
 - Save a backup of the system/user configuration and 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, you can re-import those archives. This process is especially important for IVEs which have very large log files such as 200MB

or larger (based on the configured size limits), since the IVE may process these log files during upgrade and increase 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. 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. If the Admin creates a new Authentication server and attempts to save the configuration without filling out all of the required fields, the configuration fails as expected. However, if the Admin then fills out the required fields and successfully saves changes, the new Authentication server will not work properly. (23186)
3. For AD/NT Authentication, the Admin username and Kerberos realm name fields are now required. You can use a regular user account in the Admin username. Here are the steps to create a regular account to be used in AD/NT authentication server:
 - a. Create a normal user. Create a new group and point this user to that group as Primary Group. (Just to eliminate that it is not using DomainUsers group)
 - b. Give permissions for this user for controlling computers. Grant the "Create Computer Objects" and "Delete Computer Objects" Access Control Entries (ACEs) to the User
 - From the Active Directory Users and Computers snap-in, click Advanced Features on the View menu so that the Security tab is exposed when you click Properties.
 - Right-click the Computers container, and then click Properties.
 - On the Security tab, click Advanced.
 - On the Permissions tab, click Add and add created user to the list of permission entries.
 - Make sure the "This object and all child objects" option is displayed in the Apply onto box.
 - From the Permissions box, click to select the Allow check box next to the Create Computer Objects and Delete Computer Objects ACEs, and then click OK.
 - c. Add the above user in the AD/NT configuration admin credentials section.
 - d. Restart the IVE services to confirm that it is not using the previous add before logging with a valid user.
Login with a valid user and verify in policy trace/snapshot and see whether "Join to Domain" is successful.
4. 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)
5. If using detailed policy rules, the expressions *CacheCleanerStatus = 0* is not evaluated correctly in this release. (23097)
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. Realm names with a " " (space) at the end of the name, no longer cause login failures. (19576)

8. The MSN and Google Toolbars no longer cause sign-in requests to hang. (19949)
9. Improvements have been made to clients using MacOS Safari during a meeting re-join. (19741)
10. The Session Timeout Warning for Chinese now displays as expected. (19335)
11. The IP based matching for hostnames resource policy option now applies to auto-allow Windows file sharing bookmarks. (18794)
12. 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.
13. The IVE now supports the import of Intermediate Server certificates. (5855 and 9410)
14. The link on the System → Network → External → Settings tab for “Static Routes” now points to the correct configuration page. (20203)
15. 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)
16. When using the annotation capability of the Secure Meeting white-boarding feature, the button to disable drawing access is not working properly after the user has been granted access to draw. (22893)
17. If using a MacOS or Linux Secure Meeting client, if the IVE restarts or the clients somehow loses connectivity to the IVE, the clients will not automatically reconnect. (23002)
18. 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)
19. The locale for a meeting presenter running on a Mac OS X is based on the Macintosh setting rather than the IVE administrator console setting. (19573)
20. When the presenter selects "Enable drawing for all attendees", Secure Meeting grants the permission 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)
21. Annotations on viewers' screens may be positioned incorrectly if the annotator's window has scroll bars. We recommend enabling the viewing/annotating window in full screen mode when annotating. (22769)
22. The IVE will notify the administrator when a particular IP address is used by another network device on the same LAN segment.
23. 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)
24. For NFS file browsing to work properly, you must configure an NIS server on the IVE before enabling NFS file browsing. (14594)

Known Issues and Limitations

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

Authentication

1. The username sent for single sign on to Basic Auth and NTLM-protected web and file servers has changed between the previous and current release. In 4.2, the IVE would always prepend the domain name to the username. Therefore the username would always have the format domain\user. However, in 5.0 R1, the IVE will now send the exact text entered in the IVE login page. For example, if the user enters “john” on the IVE login page then the IVE will send “john” as the username. Or if the user enters

SALES\john then the IVE will send SALES\john as the username.

2. For SSO to file servers protected by NTLM Auth, a new configuration option has been added under Resource Policies -> Files -> Windows Server Credentials. The Admin can now configure any IVE variable name as the SSO credentials to an NTLM-protected file server.
3. In order to retrieve all the groups from all the AD domains in the AD/NT Server Catalog, NTLMv1 setting is required. After the group is assigned in role mapping rules, administrator can set it back to NTLMv2. (27230)
4. The ACE Next-Pin and New-Token modes do not work properly when using ACE as the secondary login server. (21870)
5. If you set an initial username and password for an administrator when configuring an NT/AD authentication server, and then remove the password later, the password field in the IVE admin UI still shows a series of '*' characters for security purposes. (For instance, you may remove the password if the administrator account now has a null password.) Even though the IVE still shows asterisks in the password field after you have saved changes, it still removed the password as specified and saved your changes properly. (20949)
6. During the AD authentication, the IVE joins the AD domain controller as a member, enabling 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 6 hours 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 you accidentally delete the IVE machine name, you can forcibly restart all services on the IVE or reboot the IVE to allow the IVE to re-join the domain immediately. (22639)
7. 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)
8. 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)
9. 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)
10. 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 practice may cause one account to force the other account out of an 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 a duplicate server that points to the same backend system.
11. 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.
12. The IVE only supports Crypt/MD5 password hashes for NIS authentication.
13. The Backup Domain Controller configured in AD/NT authentication server is not used when doing group search in server catalog or during runtime group mapping. (26500)

Local Authentication - Password Management

1. The Password Management for an expired password during authentication on Sun ONE Directory Server version 5.2 is not working. If the user's password has not expired, then changing the password through the Preferences page still works. (26142)
2. 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. (22969)

3. 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)

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)

SNMP

1. On an IVE with a meeting license for 'n' simultaneous meetings, the meetingLimit SNMP trap is being sent at the time of launching the 'n+1'th meeting instead of after launching the 'n'th meeting. (27444)
2. Critical error message is also not being sent, even though Critical and major log alerts are enabled on the SNMP page. (27444)
3. The iveDiskFull SNMP trap is not being sent, even when the disk is completely full. Instead, the IVE keeps sending the iveDiskNearlyFull trap with value set to 100. (27408)
4. SNMP works with any community name, even with NO settings (name, location, community) specified

on Admin console. Using Snmpwalk/HP OpenView with ANY community name fetches SNMP values. However, clicking on the save settings button on SNMP page changes the Agent status to "Off". Snmpwalk/OpenView produces a "no response" error and doesn't get SNMP values after this, which is the correct behavior. (25961)

5. The logNearlyFull SNMP trap cannot be disabled. (25061)
6. Snmpwalk on the system displays the OS and kernel information. (14440)

Rewriter/Web Applications

1. In Siebel 7.5, the Help menu does not work through the content intermediation engine. (22871)
2. This release contains support for Flash version 5 and above. However, Flash applications that use the XMLSocket object or Flash Remoting are not supported.
3. The end-user may not be able to modify the User Preferences tab on the Citrix Web Interface 3.0 login page when accessing this application through the rewriter (25640).
4. Non-HTML content such as images, js, and css files that are served from a different SSL server than the HTML page may not load correctly. To work around this problem, upload a valid production SSL certificate on the servers that serve the non-HTML content or unselect the setting "Warn users about the certificate problems" under Roles -> Web -> Options -> "Allow browsing untrusted SSL web servers" (27281).
5. If using Safari on Mac OS, the browsing toolbar may not show up on web pages that contain Flash objects and Java applets (25896).
6. The "Display Favorites" functionality on the IVE toolbar may not work on web sites that use iframes or frames (27361,24621).
7. The following advanced features of the IVE framed toolbar are not available in PTP: (26091)
 - Bookmark current page
 - Displaying the original URL(always a blank display)
 - Displaying favorite bookmarks
8. The IVE always intermediates a Web proxy using basic authentication, even if the administrator has disabled the "Intermediate Basic Authentication" option. (24675)
9. The Documentum Web application is not supported by the IVE Web Rewrite function.
10. The IVE does not support Lotus iNotes in offline mode. (9889)
11. The correct caching resource policies must be configured to enable end-users to open and save email attachments in Microsoft 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."
12. To enable iNotes users to open and save .zip, Excel, and .pdf documents, the Web -> Caching resource policies must feature the "Cache Control No Store" option. For Word documents, a "Smart Caching" caching policy is supported. The reason for this distinction is that the Domino server only identifies Microsoft Word documents correctly.
13. 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)
14. Some menus of Siebel 7 are not working. This is only a problem for menu-dependent applications. With Siebel 7.5, the menus work as expected. (9442)

15. To use Web applications such as Microsoft OWA, Lotus iNotes, or Siebel via Internet Explorer with compression enabled on an SA5000, the caching policy must be set to "Cache" (15383, 27213). This is due to the following limitations with Internet Explorer and gzip compression:
 - <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>
16. When accessing a Flash Web site through the IVE that requires the installation of Macromedia, the user is not prompted to install the Macromedia application. Therefore, Flash Web site does not render properly. (26391)
17. The Java applet upload feature does not work with applets that require additional text files or configuration files to be uploaded. The only file types that can be uploaded are .jar, .cab, and .zip files. (26632)
18. When using the Java Applet upload feature, if you include the <PASSWORD> token within the generated HTML it appears correctly if you view the source of the browser window launching the applet. This behavior cannot be changed because the IVE does not control how the Java applet processes the password. (27033)
19. The Java applets upload feature may not work on Mozilla 1.6 unless the default cookie settings for the browser are modified. This is because of Mozilla 1.6 behavior where cookies are not passed from the browser to the Java applet. To workaround this limitation, change the settings to "Enable all cookies" under Edit->Preferences->Privacy & security->Cookies. (27353)
20. Citrix Java applets will not work on Mac OS X unless a production Web server certificate has been uploaded to the IVE (25264).
21. The native browser on a Symbian handheld device is not supported (22743).
22. The functionality to bookmark a page while browsing is not available on handheld devices (27371).
23. On a Symbian device, the toolbar logos may be aligned vertically instead of horizontally. In addition, the icons may appear as text links instead of GIFs. (27381, 27377)
24. The Browse field at the top of the home page or the framed toolbar supports different formats. Formats such as outlook:inbox (or any x:y format), however, are supported on Internet Explorer, but not Firefox. (27754)
25. Lotus Sametime Connect Chat functionality is supported only when using Web rewriting. 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.

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 on the Dashboard may display incorrectly.
3. The Push Config command only pushes Web Proxy policies, not the proxy server configuration. (14949)
4. The Push Config command is only supported among multiple IVEs running the same software version/build.
5. The Push Config command supports up to 9,999 users when pushing the authentication server configuration. (22165)

Host Checker and Cache Cleaner

1. Please follow the steps below to uninstall Host Checker correctly after upgrading to 5.0R3 (29522):
 1. From the IVE Admin UI, remove/uncheck all the "Host Checker Connection Control" policy under Roles/Realms Host Checker Restrictions;
 2. Then uncheck "Create Host Checker Connection Control Policy" under System > Configuration > Security > Host Checker and click save changes;
 3. Now check "Create Host Checker Connection Control Policy" as in step 2;
 4. Add "Host Checker Connection Control" policy to Roles/Realms Host Checker Restrictions;

2. If a realm has the following three conditions, then users will not be able to log in (28246):

- No Host Checker policy evaluated or enforced at the realm level;
- Role mapping rules to map users to more than one role;
- At least one of the mapped roles has Host Checker policy restrictions enabled;

The workaround is to evaluate at least one Host Checker policy at the realm level.

1. On Macintosh and Linux OS, during the sign-in process, if a user waits too long to sign in, Host Checker is not restarted. The workaround is to close the browser, open a new browser, and try to access the sign in URL again. (27907)
2. Host Checker Connection Control does not work on Windows 98. (27646)
3. On Windows 98, the Host Checker remediation page is not loaded correctly when the user clicks on the Host Checker icon in the system tray. (26893)
4. For Host Checker to work correctly on Internet Explorer 5.5/SP2, you need to have Internet Explorer patch Q832894 installed. (25905)
5. If a user closes their browser and launches a new browser, the Host Checker may not start correctly. The workaround is to remove the browser cookies and try to sign in again. (26722)
6. If the "Default Web Browser" option in the Safari browser on a Macintosh is set to Internet Explorer, then Internet Explorer displays the remediation page after the user logs in. Otherwise, the Safari browser displays the remediation page. (24743)
7. In a Host Checker policy, when you create a rule to check file, you cannot specify the file path using wildcards and give a MD5 checksum. (27648)
8. In order for Host Checker to work, the browser has to be configured to return a cookie. (25612)
9. Host Checker will not work with proxy on Macintosh OS 10.3.3 or earlier. (25259)
10. On Macintosh OS, if the user receives a "Host Checker is already running" error when signing in, the user must locate the Java process, kill it, and try to sign in again. (27671)
11. Minimum version of file check is not working. The workaround is to use the file last modification time instead. (27642)
12. If a "Restricted" user runs Host Checker, any checks to privileged locations or privileged directories in the registry are prohibited.
13. If a "Restricted" user runs Cache Cleaner, they will not be able to clean directories that are in privileged root directories like c:\program files\..., for example.
14. If the 3rd Party Package for Sygate On-Demand Virtual Desktop is used, administrators should set the Host Checker login inactivity time-out to a value large enough to prevent Host Checker from prematurely uninstalling Virtual Desktop. (25324)

15. Cache Cleaner attempts to verify the session during its cleaning phase. During this time, a connection may be opened from the process back to the IVE.
16. 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.
17. 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 Host Checker/Cache Cleaner restrictions and resource policies are evaluated dynamically on every status update.
18. When Cache Cleaner is configured to remove content from specific hosts/domains, some associated Web browser history may not get entirely removed. The user can manually delete the entire browser history if they choose to do so. (17124)
19. If two or more administrator 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 are affected in unpredictable ways. Symptoms can range from Host Checker and Cache Cleaner being shut down to losing role privileges and forced disconnections.
20. 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)
21. For certain Windows system services (e.g. smss.exe and naPrdMgr.exe), Host Checker fails 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)
22. 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 is not immediately allowed access upon starting the firewall. The end user needs to wait until the policy is refreshed, which is governed by the Host Checker verification frequency. One way to overcome this situation is to delete the cookies from the IVE prior to restoring the security posture. (13947)
23. The McAfee Desktop Firewall 8.0 Host Checking method requires that the client be running build 485 or higher.

Secure Meeting

1. 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 does not launch, but it appears to the user as though the applet is still loading. (22712)
2. Full screen and Remote Control modes are not supported on the Java client. (23148)
3. 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.
4. 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)
5. 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)
6. On the Macintosh and Linux platforms, even if the viewers are set to full screen mode, the toolbar will

still be visible. (19506)

7. We recommend that you not upgrade the Meeting 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 Safari and Mozilla browser behavior related to caching Java applets. The user must close and restart the browser to fix the problem. (22273)
8. 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 Microsoft Outlook behavior. (21336)
9. When the user launches Secure Meeting, a Security Warning is displayed regarding 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)
10. Safari 1.0 has a bug wherein it does not fully support proxy configurations. As a result, if there is a proxy configured, the meeting client cannot be launched from this browser. We are working with Apple on this issue.
11. 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.
12. 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 causes the Secure Meeting client to download incorrectly.
13. When using MacOS 10.3.3 and Safari 1.0, if the user clicks "NO" on the certificate pop-up, the Secure Meeting client does not install. If the user wishes to try again, they must open a new Safari browser window.
14. 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.
15. If the user forming a Meeting is using Email invitations and accesses the IVE using a URL that 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. As a result, email recipients may not be able to access the link from the email. We recommend that administrators configure the "Network Identity" under the Network section in the UI. If configured, Secure Meeting invitations will use that hostname, instead.
16. Secure Meeting may function erratically if the time clocks on IVEs in a cluster are not synchronized. We recommend that administrators use the same NTP server for each node within a cluster to keep the IVE times synchronized.
17. When creating a Secure Meeting using the MacOS Safari Web browser, the organizer may be unable to add more than 250 attendees.
18. When presenting, the presenter should consider what access methods are being used by attendees. Dial-up attendees may have bandwidth issues for presentations that 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 over which they are receiving data. (15203)
19. Secure Meeting attendees do not see the presenter's shared applications if the presenter locks their desktop.
20. Secure Meetings in progress are stopped if a cluster is created during the meeting.

21. On a Windows platform, the meeting client picks up the proxy information from the Internet Explorer browser settings. Therefore, Secure Meeting works on other browsers only if the proxy setting is also configured in Internet Explorer. (17442)
22. Viewers on Linux and Macintosh clients may take a while to load the presentation if the presenter's desktop screen area is larger than 1856 x 1392. (23291)
23. The teleconference number in Secure Meeting Outlook plug-in is not included in the meeting invite. (24077)
24. If the Hide Attendees option is enabled, a "Failed to change roles" message appears when granting annotation permissions to another attendee. (24417)
25. In Fit To Window mode, attendees may sometimes see small blocks of mangled images in their Viewer window. (24427)
26. A presenter using a Linux client is not supported over slow DSL. (24480)
27. In a remote control session, annotation should not be started. (24902)
28. A presenter using a Linux client is not supported in a WAN environment. (24985)
29. In a WAN environment with Linux presenting, there are attendee viewing issues. (24986)
30. There is a limitation on the areas where a Linux and Mac presenter can annotate. If the Linux or Mac presenter annotates over the application toolbar at the top or bottom of the screen, then the annotated objects in those areas are not displayed on the viewers. (25555)
31. Part of the bottom of the presenter screen is truncated when viewed on Linux or Mac viewer in Fit to Window mode. (26468)
32. If the presenter is the only person in a meeting and has started annotation, annotation is not enabled. At least one other attendee must join the meeting for annotation to be enabled. (26717)
33. If the presenter is annotating his own desktop on a Linux or Macintosh system, the annotation viewer may appear to be frozen. To unfreeze the desktop, enter Alt+Tab. (26737)
34. The Secure Meeting Toolbar does not work on Linux KDE window manager if the attendee runs the Viewer in full screen mode. (26851)
35. When the last attendee leaves an annotation session hosted by a Linux or Macintosh presenter, any further annotation operations done by the presenter do not work. (27274)
36. On Linux systems with the application toolbar located at the top of the screen, if the height of the application toolbar is resized while Secure Meeting toolbar is also being displayed, then Secure Meeting toolbar may not respond well to the mouse event to activate and hide it. (27276)
37. The "Enable all drawings for all attendees" and "Disable all drawings for all attendees" options do not work on Linux and Macintosh presenters. (27402)
38. If there are no attendees, when a Linux or Macintosh presenter clicks on the Draw icon to enable annotation, the annotation session is not started. The presenter needs to click the Draw icon again after an attendee has joined the meeting. (27403)
39. When you change the password from the Launch Meeting page, an updated email is sent and the Conductor name is empty. (27487)
40. On Linux and Mac, if the icons on the Secure Meeting toolbar become unresponsive after the presenter enables annotation, look for "Secure Meeting" on the Linux menu bar and click on the entry corresponding to annotation. This will bring forward the Secure Meeting toolbar again with working icons. (27613)
41. On Linux and Macintosh clients, if the Secure Meeting toolbar is hidden, it cannot be displayed again by

moving the mouse to the upper left corner on the desktop. The workaround is to ensure that you do not hide the Secure Meeting toolbar. (27616)

42. On a Linux or Macintosh client, if the presenter is in annotation mode and the last attendee leaves the meeting, the annotation icon on the Secure Meeting toolbar is inactive and the presenter will be left in annotation mode. The user should enter Ctrl-Q or click on the exit/end meeting icon on the Secure Meeting toolbar to exit annotation mode. If an attendee rejoins the meeting after the presenter exited from annotation mode, the presenter should stop and start sharing again to enable a new annotation session. (27755)
43. On a Windows client, if the presenter is in annotation mode and the last attendee leaves the meeting, the annotation session is disabled. For annotation to work again when an attendee rejoins the meeting, the presenter should stop and start sharing again and enable a new annotation session. (27762)

Administration

1. Logs (Events Log, Users Access Log, Admin Access Log, and Network Connect Packet Log) are not automatically moved to the new version when upgrading. The logs are, however, still available when rolling back to the original version.
2. Log filtering requires a wildcard character to be surrounded by double quote marks (“*”).
3. When user fail to authenticate, the log message may not have the correct IP address that is associated with the source request. (26652)
4. In serial console access mode, the -b feature for pinging a broadcast address in network troubleshooting is not available. (21903)
5. In number of active user statistics, the exact count is computed every hour. However, within the sampled period, the system does not subtract the users who drop off and will show a discrepancy in the actual active user vs. the recorded active user. (24775)
6. Depending on the switches, when the network interfaces are configured to be 100 mbps, the network throughput may suffer. Please maintain “auto” as the best configuration for the NIC. (24724)
7. When the disk storage space on the IVE becomes limited, upgrading to the new version may result in a failure to verify the new package. Please remove system snapshots, debug information, and other unnecessary information, and retry the operation. (22455)
8. There may be conditions where FIN packets that are destined for one interface (external or internal) can be found on the opposite interface. However, there are no security issues, because these are FIN packets only. (25095)
9. Roll back for clustering does not validate that the rolled back version of all cluster nodes are the same. Therefore, manually verify that all nodes have the same roll back version before commencing the operation.
10. In Firefox/Mozilla, Log Setting in-line editing does not work. To work around, delete the entry and re-add the information.
11. The log setting in-line editing will not function unless a Central Manager License is installed.

Clustering Issues

1. If a network problem causes a node in a cluster to lose communication 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 creating an Active/Active cluster while using an Active/Passive cluster configuration the joined nodes will lose their Virtual Port IP address information and 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 to 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. When an IVE in an Active/Passive cluster loses network connectivity, it automatically moves into 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 the carrier signal, and on connectivity to the Gateway by sending an ARP request. 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 automatically joins the cluster.
 6. When deploying large clusters in a multi-site environment and the connectivity between nodes is unstable, a node joining the cluster 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. 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 initialization, 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)
 7. In an Active/Passive Cluster Pair failover situation, the active IVE sends a gratuitous ARP request in the network indicating 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.
 8. 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.
 9. IVE system log messages are not synchronized during a Join Cluster operation even when the "synchronize log messages in a cluster" option is enabled. The log messages are synchronized across the IVEs in a cluster when all the machines are in "Enabled" and Status "OK" mode.
 10. 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.
 11. You should avoid using the "multicast" synchronization method for Multi-Unit Clustering 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.
 12. 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.
 13. 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.
 14. 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.

15. Clustering is not supported when an IVE is configured to have the same subnet for both the *internal* and *external* interfaces.
16. 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 sent 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. To prevent this from happening, IVE Administrators are encouraged to ensure all IVE nodes have constant communication with each other and that the network segment(s) between them are never severed.
17. 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. In WRQ versions 6 and 7, the WRQ administrator console is not supported through the Java rewriting functionality. (27881)
2. The TN 3270 WRQ 7.0 applet is not supported through the IVE. (26690)
3. A security setting of "Accept only TLS V1" option is not supported for Java applet rewriting over Sun JVM. This is due to a bug in Sun JVM. (25146)
4. 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.
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 appear. Please refer to the Administration Guide for instructions on disabling the Java Plug-In cache.
6. 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)
7. 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.

8. With Sun JVM 1.4.2, if caching is enabled, WRQ 6.0 will not load properly. (14008)
9. The policy tracing logs that result when code signing certificates are used to re-sign Java applets are not accurate. Use the Simulation tool instead, for troubleshooting purposes. (17411)

Pass-Through Proxy Issues

1. The Lotus iNotes welcome page is not rewritten if the IVE is intermediating the content through Pass-Through Proxy. (9236)
2. Pass-Through Proxy URLs must be hostnames. Paths of hostnames are not supported.
3. Juniper Networks strongly recommends that Administrators not mix Pass-Through Proxy Port and Host modes.
4. Siebel7 is not supported through Pass-Through Proxy.
5. Using Mozilla with Pass-Through Proxy (with the IVE port configuration), the IVE may invalidate the user session causing the user to have to login again.
6. Pass-Through Proxy is not supported on Netscape 7.0, but is supported on 7.1. (7290)
7. When using Lotus iNotes through Pass-Through Proxy, if an 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'.
8. When using OWA through Pass-Through Proxy, if a user replies to or creates a new email, the recipient may receive a JavaScript error if they view the email through their Outlook client. (9233)

Internationalization Issues

1. With localized Pocket PCs, such as the 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)
2. 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>.
3. 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*.
4. 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, you can change the font setting in Fonts section of the Netscape Preferences, where you can select the option “Netscape should override the fonts specified in the document”.
5. 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.
6. Special characters such as ①, I, ¥, and ~ are not supported in filenames for UNIX Servers.
7. Japanese characters are not supported in naming Authentication Servers.
8. Filenames using 5c characters such as 表 and 工 will be corrupted and cannot be deleted from UNIX servers.
9. In a Host Checker Policy, the Admin should enter Registry Settings rule settings in English. (25097)
10. On Mac OS X Simplified Chinese system, Secure Meeting client comes up in Traditional Chinese. (27675)
11. On a Simplified Chinese system, help pages from the Secure Meeting client will be in English. (27848)

File Browsing Issues

1. Session termination does not affect file transfers through Windows file share. (26897)
2. 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)
3. Depending on the web browser, downloading files with filenames of length 18 to 25 characters may not work, through the IVE. Files with longer or shorter filenames are OK.
4. 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 valid credentials. To avoid this, administrators should configure both the IP address and hostname in their file browsing ACLs.
5. 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)

XML Export

1. **XML Export is a Beta quality feature in Release 5.0 R1. XML Import and Push Configuration are not available in Release 5.0 R1.**
2. On certain browsers, following XML Export, if the admin clicks “OPEN” instead of “SAVE” in the

- dialog box that appears, the operation fails with error message “THE PAGE CANNOT BE DISPLAYED”. The workaround for this problem is to save the exported file and then open it. (27329)
3. In performing XML export of realms, if “Administrator Realms” are selected for export but User Realms are not selected for export, the expected behavior is that only Administrator Realms will be exported. However, currently, User Realms also get exported. (26569)
 4. XML Export of Custom Sign-In pages is not supported (26658)
 5. The following options are present in the administrator user interface but not supported by XML Export: (27555)
 1. Roles -> General -> Overview -> Source IP
 2. Roles -> General -> Overview -> UI options -> Start Page -> “Allow access to directories below this URL”
 3. Roles -> General -> Overview -> UI options -> User Toolbar -> Session Counter
 4. Roles -> General -> Overview -> UI options -> User Toolbar -> Client Application sessions
 5. Roles -> General -> Overview -> UI options -> Help page -> “Allow access to directories below this URL”
 6. Roles -> General -> Overview -> UI options -> Browsing Toolbar. All options except "Toolbar Type" and "Logo", are missing
 7. Roles -> Web bookmarks -> Auto-allow. "Only this url" and "Everything under this url" are missing
 8. Roles -> Network Connect -> Auto Uninstall and all GINA options are missing
 6. XML Export of Network Connect filters in the Network Settings is not supported. (27694)
 7. XML Export of WINS Enable Network Discovery option is not supported. (27696)

Miscellaneous issues:

1. In a customer network where you can simultaneously access two separate Juniper SSL VPN devices, one with a client application such as WSAM, Windows Terminal Services, or Network Connect, and the other with access to a web application, you can inadvertently terminate a session on one system when you logout from an application on the other system. Currently, we do not pass the host information from one application to another when a user logs out from one of two simultaneously connected client applications on two separate VPNs. (27697)
2. All Error and Informational messages within Windows Secure Application Manager and Network Connect contain an “Error Code” string. This “Error Code” string acts as an identifier for either the error message or the informational message and can be cross-referenced with the end-user online help to get “cause” and “action” information for the message displayed.
3. 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)
4. 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)
5. 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)
6. 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)
7. If you use a multi-valued attribute in the bookmark name, only the first value is displayed for all the expanded bookmarks. (21629)

8. If the Admin submits some change and then closes the Task Guide or presses Back in the 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 submitting another page is equivalent to reloading the previous page, which was a submitted form. (22039)
9. Importing the system config does not import SSL Intermediate CA Certs (chains). (21040)
10. 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)
11. When "High browser security is enabled", a user might see a pop-up warning confirming whether or not the Java Applet should be downloaded. There is nothing that Juniper Networks can do to suppress this warning message as it is a function of the browser. (21865)
12. Juniper Networks recommends that to uninstall client applications (for example, NC, W-SAM) you use the Un-install link of the Un-installers UI under Preferences > Applications. (20415)
13. NFS Auto-mount is not supported on Linux NIS/NFS servers, only on Sun servers. (2005)
14. When using the serial console troubleshooting tools, such as ping, if the tool becomes unresponsive, press CTRL+C to terminate the tool and go back to the menu.
15. 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.
16. 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)
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 (for example, '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 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 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 are 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 occur 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/character/izonmoji.html> (14529 and 14348)
26. 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.
27. 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.
28. 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.
29. 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)
30. When using an external load balancer and accessing Secure Meeting, 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.
31. 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>
32. The IVE web browsing function does not support URLs of more than 159 characters in length, including extensions, such as ".html".
33. On a Mac, the IVE toolbar should be disabled to view OWA pages with the Safari browser. If the toolbar is enabled, the Inbox may be blank until the page is refreshed once. To work around this, the toolbar can be disabled in the Roles → UI Options tab.
34. Even though you enter the password to archive users and system config files, the IVE disregards this password on the import.
35. 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 selective rewrite.
36. When switching from Optimized NCP (NetScreen Communication Protocol) to Standard NCP, or vice versa, all NCP- Based communications must be restarted. This includes Secure Meeting.
37. 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)
38. 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.
39. 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.
40. 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.
41. 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.

42. 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 (for example, /admin) to sign back into the IVE Admin Console again.
43. The Session Timeout Warning is only supported if the user is viewing web pages through the IVE (rewritten web pages) or the IVE homepages themselves. It is also supported if the user is running J-SAM. The warning is not 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.
44. 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.
45. 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 is momentarily incorrect due to this change.
46. 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.
47. 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)
48. The Debug Log troubleshooting functionality should only be enabled after consultation with Juniper Networks Support.
49. The IVE has an Automatic Version Monitoring feature which notifies Juniper Networks what version of software the IVE is running and the name of 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.
50. In order to access IVE resources as links from a non-IVE web page, a selective rewriting rule for the IVE resources is required. For example, if you would like to include a link to the IVE logout page such as `http://<IVE server>/dana-na/auth/logout.cgi` then you need to create a selective rewriting rule for `http://<IVE server>/*`.(26472)

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>.