

Release Notes (Rev. 1.2)

Juniper Networks NetScreen-Secure Access

IVE Platform version 5.5 R1 Build # 11711



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

April 11, 2007

Contents

Recommended Operation.....	1
New Features in this Release	3
Upgrading to this Release.....	3
Known Issues/Limitations Fixed in this Release	4
All Secure Access Platforms.....	4
SA 1000 through SA 6000 Items	6
Known Issues and Limitations	6
All Secure Access Platforms.....	6
SA 1000 through SA 6000 Items	31
Supported Platforms	46

Recommended Operation

- The Debug Log troubleshooting functionality should only be enabled after consultation with Juniper Networks Support.
- The IVE has an Automatic Version Monitoring feature which notifies Juniper Networks of the software version the IVE is running and the hardware ID of the appliance 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. We strongly recommend that Administrators keep this setting enabled.
- When using W-SAM, Network Connect, or Secure Meeting, we recommend that the admin allow the client to automatically select between the optimized and non-optimized NCP options. This will allow clients to use optimized NCP where possible, and to fall back to non-optimized NCP where necessary. (28405)
- Multiple simultaneous 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.
- When using an external load balancer and accessing J-SAM, W-SAM, Network Connect, or the Online Meeting functionality, 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.
- 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>/access/auth/logout.cgi` then you need to create a selective rewriting rule for `http://< IVE server >/*`. (26472)
- If two separate Web browser instances attempt to access different versions of the IVE, then the browser may prompt the user to reboot the PC after the NeoterisSetup.cab has been downloaded. Upon closing all browsers and logging in again, the prompt will no longer be displayed. No reboot is required.
- **Optimal Performance:** To optimize system performance, customers should ensure that the "Network Connect Packet Logging" feature is not used, as it will have a significant impact on system performance when under load. Additionally, cluster log synchronization is known to consume a lot of system resources (CPU + Memory), thus it is not recommended to activate this feature on systems that are widely used. (34276)
- When using the command-line W-SAM ("SAMLancher"), the URL entered must contain the prefix `https://`.
- W-SAM supports client-initiated UDP and TCP traffic by process name, by destination hostname, or by destination address range:port range. Except for Passive FTP, W-SAM only supports protocols that do not embed IP addresses in the header or payload. W-SAM also supports unicast client-initiated UDP.
- Users must launch drive maps through W-SAM in one of the following ways:
 - **NetUse**--At the Command prompt, type: `net use * \\server\share /user:username`
 - Right-click on **My Computer > Map Network Drive**, or Explorer-enabled drive mapping. In

Windows Explorer, go to **Tools > Map Network Drive**, then select “Connect using a different username”.

- When using the W-SAM Access Control List (ACL), administrators should take extra precaution when granting access to hosts. We recommend that administrators use the IP address instead of the hostname. If the hostname is required, for security purposes, administrators should try to include additional ACLs with the corresponding IP address or IP addresses for that hostname. Reverse DNS lookups are not supported.
- To run Citrix NFuse through W-SAM, you must define a Caching rule to cache launch.asp files. For example, configure the resource policy to “<server name>:80,443/*.launch.asp” and the Caching Option to “Cache (do not add/modify caching headers)”.
- When scripting the use of SAMLauncher.exe, users should provide the -reboot command-line flag, so that if the launcher requires a reboot, it happens automatically and does not exit, prompting the user to manually reboot. Note that during a fresh install (with NetBIOS enabled), W-SAM requires a reboot.
- When using Microsoft NetMeeting with W-SAM, hosting a meeting is not supported. There are no problems joining a meeting using Windows 2000. When using Windows XP, however, application sharing does not work as expected. In order for Windows XP users to work around this sharing issue, they must first turn on the **Only you can accept incoming calls** option.
- Do not delete the main cluster licensing node. Doing so will delete the whole cluster. (27972)

New Features in this Release

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

Upgrading to this Release

- In this release, Adaptive Java Delivery for IVE clients it is not supported or qualified with IE7 on Vista. It is supported on other platform and browser combinations. Hence, caution is recommended in rolling out this release to users who may be using IE7 and Vista and may have Active-X disabled or unavailable.
- In this release, only 32-bit Vista clients are supported and qualified.
- Please refer to the *Supported Platforms* document for important information pertaining platforms supported. From 5.5 release onwards, Windows 98 SE and Windows NT are not supported.
- Automatic upgrades to this release from the following releases are supported (including from the Legacy Authentication mode):
 - 5.4 R3 Build 11621
 - 5.4 R2.1 Build 11529
 - 5.4 R1 Build 11359
 - 5.3 R8 Build 11339
 - 5.3 R7 Build 11255
 - 5.3 R6.1 Build 11199
 - 5.3 R5.3 Build 11159
 - 5.3 R4 Build 10769
 - 5.3 R3.1 Build 10741
 - 5.3 R2.1 Build 10641
 - 5.3 R1 Build 10197
 - 5.2 R6.1 Build 11167
 - 5.2 R5.2 Build 11161
 - 5.2 R4.1 Build 10573
 - 5.2 R3 Build 10171
 - 5.2 R2 Build 9895
 - 5.2 R1 Build 9469
 - 5.1 R8.1 Build 11095
 - 5.1 R7 Build 10081
 - 5.1 R6 Build 9837
 - 5.1 R5 Build 9627
 - 5.1 R4 Build 9403

- 5.1 R3 Build 9311
- 5.1 R2 Build 9092
- 5.0 R6 Build 9343
- 5.0 R4 Build 9085
- 5.0 R2 Build 8721
- 5.0 R1 Build 8553
- 4.2 R5 Build 8559
- 4.2 R4 Build 8375
- 4.2 R3 Build 8175
- 4.2 R2 Build 7891
- 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
- **Note:** If upgrading from a 3.x releases, you must upgrade to Release 5.0 prior to upgrading to Release 5.5 R1.
- **Note:** If upgrading from a release which is not listed here, please upgrade to one of the listed releases first, and then upgrade to 5.5 R1.
- If using Beta or Early Access (EA) software, please be sure to roll back to a prior production build and then upgrade to the 5.5 R1 software. (This process enables you to roll back to a production build if ever needed.)

Known Issues/Limitations Fixed in this Release

All Secure Access Platforms

Internet Explorer 7 Support

- IVE pages are not compressed for IE 7 users when admin enables gzip compression under System Options page. (45079)

AAA

- For a delegated admin, the Read and Write permission to manage a user role's Telnet/SSH feature is tied to SAM permissions. The admin will not be able to manage Telnet/SSH sessions if permission to manage SAM is Read or Deny. The reverse is not true (SAM permissions are not dependent on those of Telnet/SSH). (43123)
- When importing AD auth server configuration to another SA with an XML file or through Push Config, the Computer Object name needs to be changed manually after the import. Unexpected problems might arise if two SA systems join an AD domain using the same computer object. (42761)
- When duplicating a role that has been assigned to a resource profile, the new duplicate role may lose its association with the resource profile. (42211)

Network Connect

Macintosh Client

- This following issue is no longer observed with our current release: DNS changes do not take effect after the Network Connect tunnel is established. (38689)

Windows Client

- The issue that NC log files grow beyond 10MB limit is fixed. (41544)
- This following is fixed in this release: Network Connect is not able to handle the following PAC file statement: `if(shExpMatch(url, "http://<host>/*"))`. The workaround is to modify the above statement to `if(shExpMatch(url, "http://<host>*"))`. (44150)
- Network Connect diagnostics no longer shows "failed" at "NC tunnel" while Network Connect is actually connected. (43058)
- This issue is resolved: on canceling the UAC prompt for the Network Connect installer while launching Network Connect for the first time, the IVE page will not get redirected to the IVE home page automatically (44648). Now IVE page is redirected properly.
- Restricted user is able to install Network Connect even using Installer Service in this release. (44687)
- This issue is no longer observed with this release build: sign out on IVE home page from a Firefox browser terminates WSAM session but leaves WSAM reconnect dialog popup open. (45033)
- Network Connect client 32 bit driver is currently signed by Microsoft, thus user will not see the pop up that request permission during Network Connect client installation anymore. (42825)

Rewriter/Web Applications

- If Microsoft KB918899 patch exists on a Windows XP then Oracle Expense report application will not work through the rewriter (35328).
- Microsoft Sharepoint 2003 through the rewriter:
 - If the hostname of the SA appliance and the Sharepoint server are identical then certain functionality in the Sharepoint server may not work. If the two server names need to be identical then use hostname-based PTP as a clientless mode of accessing Sharepoint. (40973)
 - Viewing a readonly Office document is not supported through the rewriter. To workaround this issue, save the document to disk so as to view the contents. (42249, 41950)

Hosted Java Applet Issues

- The use of document.write in the HTML used to launch the hosted java applet does not work on Safari. (42873)

SA 1000 through SA 6000 Items

Java Secure Application Manager (JSAM)

- When adding servers for JSAM using resource profiles, more than 12 servers cannot be added. As a workaround use Roles -> SAM -> Applications to add JSAM applications. (41353)

Windows Secure Application Manager

- This following issue is fixed in 5.5 GA: when user cancels UAC prompt for the WSAM installer while launching WSAM for the first time, the IVE page will not get redirected to the IVE home page automatically (44648). In 5.5 GA, when user cancels UAC prompt during WSAM first time installation, IVE is automatically redirected to the IVE home page.

Pocket PC

- When using an existing W-SAM role configuration originally set up for Windows PC users to provide secure access to defined applications for Pocket PC users, the list of Destination Hosts defined within the role can be greater than 1500 bytes in length. (28457)
- W-SAM can always be successfully launched through ActiveSync in the 5.5 release. (41113)

Secure Meeting

- When presenter moves his mouse cursor, the cursor movement is not seen on the attendee's Viewers. (44622)
- Eval, Lab and ICE licenses allow 1 Secure Meeting and 3 meeting attendees instead of the maximum number of meetings and attendees supported by the platform. The workaround is to install a Secure Meeting license.(44927)

Known Issues and Limitations

All Secure Access Platforms

Internet Explorer 7 Support

- IE7 prevents the removal of the URL/address bar when users are opening a bookmark in a new window where they have configured the "Do not display the Web browser's URL address bar" setting. This can be seen with JSAM or any pop-up displayed by the backend web application accessed through the IVE. There is no current workaround for this and we expect the impact to be minimal.
- Closing the IVE tab or window in IE 7 does not necessarily end the IVE user session. To make sure that the session with IVE ends, the user should click Sign out.
- If there are 3rd party browser toolbars or add-ons installed in Internet Explorer, they need to be upgraded to be compatible with IE 7. If the updates for the 3rd party software are not available they should be uninstalled. Otherwise, IVE client components such as Network Connect and WSAM may crash when they redirect the browser to the IVE home page.
- IVE will not be able to launch JSAM if pop-up blocker is enabled. The user will have to disable

the pop-up blocker for IVE host by selecting 'Always allow pop-ups from this site' on the yellow bar shown at the top of the browser by the pop-up blocker.

System Status and Logs

- With log filtering, when using the role variable, the value must be contained within double quotation marks. (For example, role = "Users".)
- 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.
- Default filter for logs may be incorrectly set after deleting a custom filter. (31694)
- 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 (if they are not using a Windows PC, for example). (22978)
- When switching from Optimized NetScreen Communication Protocol (oNCP) to standard NCP, or vice-versa, you must restart all NCP-based communications. This includes W-SAM, Network Connect, and Secure Meeting.
- An Internet Explorer cache problem exists when handling the HTTP No-Cache directive in the Microsoft Internet Explorer Web browser. Web content is sometimes served with the HTTP directives. No-Cache or No-Store browsers should not cache such content. When GZIP compressed content with the No-Cache or No-Store directive is served to Internet Explorer the browser saves a copy of the uncompressed content in its cache. If a user then uses the Back button in their browser, Internet Explorer displays the file from its cache, instead of sending a new request. Internet Explorer only exhibits this problem when the served No-Cache content is compressed. To work around this problem, you can configure the IVE not to compress specific files, directories, or types of content using the URL rules commands. (29133)
- The external port on the administrator Web console may show "Connected" status even though the network cable is not connected. (31987)
- When configuring the size of log file, please do not configure multiple log files to have larger than 250Mbytes as it may cause the system to run out of disk space. (36153)
- Archiving event logs may have erroneous login names. (37685)
- The legend may still be displayed on the Central Manager display even though it is disabled in the display setting. (39573)
- After a time zone change, please restart the services in order to align all process times. (33205)
- "Saving all Logs" only designed for Event, Access, and User logs. It does not include sensor logs and uploaded client logs. (35127)
- There are rare situations in which, after binary import, the log utilization is shown to be -1%. (42183)
- When multiple syslog servers are configured only one of them will receive the syslog entries. (43184)
- When a VLAN interface is deleted, two log messages are generated. The first log message is redundant, and is missing the VLAN interface name. The second log message is valid and contains the correct VLAN interface name. (34287)

Management Port (SA 6000 and SA 6000-SP only)

- When selecting the interface to view routing information, an entry for the management port may appear even though the management port is not supported on the particular hardware platform.

This will not cause any abnormal behavior to the system. (41858)

- Backend traffic originated from the IVE that is not tied to user sessions and is not specifically designated by the system as “management traffic” always has the Internal Port’s IP address as the Source IP. (IVE-IDP traffic and DNS traffic are examples of this category). Even if the route to the destination IP address uses a different outgoing interface (such as the Management Port on an SA 6000), the source IP address for all outgoing traffic in this category is the IP address of the Internal Port. This is as designed and is not a bug. This behavior is typically observed in customer networks where AAA servers, DNS servers or IDP servers are placed on the same network as the IVE Management Port, and a static route to these servers is configured in the Internal Port route table, with the Management Port as the outgoing interface. (40846)
- When archiving data through the Management port the user name “System” is missing from certain event logs, such as the event log generated when the archive server (SCP or FTP) is unreachable. The event log appears in the format

2007-01-13 07:15:11 - ive - [127.0.0.1] Root::()[] - Archiving could not connect to 'scp://10.209.138.86:22', Events log not archived,

Instead of

*2007-01-13 07:15:11 - ive - [127.0.0.1] Root::**[System]**()[] - Archiving could not connect to 'scp://10.209.138.86:22', Events log not archived, (44944)*

- If the “Management Port” option is selected on the Troubleshooting > Commands page in the administrator user interface, but the Management Port itself is disabled, the expected behavior is that the troubleshooting commands should fail. However, the actual system behavior differs in that the traffic generated by the troubleshooting commands egresses over the Internal Port instead. (44928)
- When archiving data through the Management Port, if the archiving server is unreachable and SNMP traps are enabled on the system, archiving retries will be sent out over the Internal Port. However, this is a transient issue that only affects the rounds of archiving that occur simultaneously with the archiving server being unreachable. Once the server becomes reachable, subsequent archiving traffic will be correctly sent over the Management Port. (Bug 44902)
- In certain cases, services for which traffic normally egresses via the Management Port (syslog, SCP/FTP archiving, SNMP etc.) lose their association to the Management Port and fall back to sending all traffic over the Internal Port instead. This problem could manifest itself in several scenarios : upgrading to 5.4R1, adding nodes to a cluster, importing system configuration from a non-SA 6000 etc. (Bug 43743)

System Services

- The current SSL-VPN config import functionality does not track any platform specific functionality like SSL Acceleration cards etc. Hence if an Admin were to import the configuration from an IVE platform (SA3000) into an SA6000, SSL crypto acceleration would be disabled as the SA3000 does not have the crypto functionality (38433)
- There are known problems where the data storage on the IVE subsystem could lose data updates if the system time on the IVE is rolled backwards. This is an unlikely situation. A fix for this problem has gone into Release 5.2, however if upgrading to Release 5.1 and older versions,

customers could experience data loss under mentioned conditions. As a symptom, customers have reported issues in missing IVS licensing information. (32598)

Administration Tools

- If a serial console troubleshooting tool (such as ping) becomes unresponsive, press CTRL+C to terminate the tool and return to the menu.
- VLAN tags do not show up in the TCPDUMP troubleshooting tool due to hardware acceleration. (28400)

Connectivity

- FIN packets may leak from internal port to external port. However, there are no security ramifications for this activity. (25095)

SNMP

- Snmpwalk does not report NC tunnel interfaces due to performance overhead related with retrieving the corresponding OIDs. This behavior is different from previous releases, where all network interfaces were reported by snmpwalk.
- The iveRebootTrap is not sent if the IVE is rebooted via the serial console. However, an event of severity "Major" is logged in the Event Log. Additionally, if the "Major Log Trap" checkbox is selected on the Log/Monitoring > SNMP page, a major log trap is generated for this event. (41829)
- The Internal and External ports on an A6K report incorrect values for the ifOperStatus MIB object when the underlying physical interfaces are disconnected. When both the physical interfaces in the bonded pair represented by the Internal port are disconnected, the ifOperStatus should be reported as DOWN. Instead, is it reported as UP. The same issue is observed for the External port as well. (41334).
- The proprietary traps iveNetInternalInterfaceDown and iveNetExternalInterfaceDown are not generated when these Internal Port or External Port are rendered inoperable by disconnecting the underlying physical interfaces. (41338).
- When the Interface MIB (if-mib) is queried on an A6K, an incorrect value is returned for the ifOperStatus of the physical interfaces eth0, eth1, eth2 and eth3. (41332).

Binary Import/Export

- Client Log settings for Host Checker and Cache Cleaner are not getting exported and imported correctly. If client log setting is enabled for Host Checker and Cache Cleaner, the setting is lost when system configuration is exported and imported later. (38449)
- In this release, binary import with the option "Import everything except IP" correctly preserves IP address, netmask and default gateway for the internal/external/management ports (ie does not result in these values being overwritten by values in the imported configuration). However, the following inconsistencies can arise :
 1. VIPs associated with the internal/external/management ports get overwritten by imported values. The administrator needs to manually reconfigure the VIPs following the binary import.
 2. Static routes in the route tables associated with the internal/external/management ports are overwritten by the imported values. The administrator needs to manually reconfigure the static routes within the internal/external/management route tables. (40618)

XML Import/Export and Push Config

- If a User Role has UI options enabled, and if any custom page URL under UI Options contains a variable (e.g., <USER>), then the XML export of that role fails.
- Quick XML import is not supported for Secure Meeting policies. (31214)
- XML Import/Export and Push Config are not supported for the Host Mapping Values configured under Outlook for J-SAM. (29264)
- XML Import/Export and Push Config of Resource Profiles data are not supported. Therefore, any resource policies or bookmarks created from within a resource profile will not be exported or imported in an XML Import/Export operation.
- XML Import/Export is not supported when uploading applets. The IVE generates an error message during import and the workaround is to remove the applet bookmarks from the XML file (32173):
 1. Export the System configuration under **Maintenance -> Import/Export -> Configuration** page.
 2. Import the exported file back into the IVE under the **Maintenance -> Import/Export -> Configuration** page. Select the "Import everything except network settings and licenses" option.
- XML Import/Export for Basic Auth and NTLM auth resource policies is not supported. (31383)
- XML Import/Export is not supported for the following Terminal Services options: "Users can add sessions", "Users can connect drives", "User can connect printers". (34685)
- When an XML Import or Binary Import operation is performed on a cluster node, it can take up to 15 minutes for the operation to complete, including the time to synchronize this configuration across all the nodes in the cluster. There is no progress bar or other UI indication of the progress during this interval. The same issue is seen when a Push Config operation is applied to a target cluster. (40621, 25888)
- If Push Config or XML Import is performed onto a node in a cluster, if any of the cluster nodes are disabled or unreachable for any reason, the Push Config or XML Import operations can take up to 15 minutes to complete on the remaining nodes. (40609)
- If an XML file containing Secure Meeting settings is to be imported into an IVE device via the XML Import operation, or if an IVE device is the target for a Selective Push Config operation where the incoming configuration contains Secure Meeting settings, then the target IVE device must have a Secure Meeting license installed. (43423)
- If the Secure Meeting license is removed, then XML Export will fail if "ALL sign-in URLs" is selected under "Sign-in Settings". The workaround is to use the "SELECTED sign-in URLs..." option and select the Sign-in URLs from the available list. (43754)
- XML Import/Export of 500 or more user records into/from the configuration does not work. The admin UI will appear to hang. (44715)

AAA

- The IVE currently does not support load balancing during ACE authentication. It has no option

to upload the sdopts.rec file which is internally used for load balancing by the ACE client. (37656)

- The maximum number of combined bookmarks a role can have is ~500. If a role has more than 500 bookmarks, some operations (e.g., delete role, duplicate role) may not work correctly. The workaround is to split a role with a large number of bookmarks into multiple roles. (41557)
- The following attributes are not supported in the RADIUS Auth Server, even though they can be selected from the Admin UI: (40856)
 - Vendor-Specific (26)
 - Event-Timestamp (55)
 - Message-Authenticator (80)
 - NAS-IPv6-Address (95)
 - Framed-Interface-Id (96)
 - Framed-IPv6-Prefix (97)
 - Login-IPv6-Host (98)
 - Digest-Attributes (207)
 - Expiration (1010)
 - Acct-Session-Start-Time (1050)
 - LM-Password (1057)
 - NT-Password (1058)
- Using the Treo 650, a user will not be able to sign in to the SA device if the Host Checker is enabled at the realm. The workaround is to sign in through another realm that has Host Checker disabled. (39164)
- When the user signs in and gets redirected to a custom start page, then the access to that page will be allowed in that session either through a bookmark or browsing toolbar, even though there is no explicit policy to allow access. (38853)
- The data statistics (bytes in and bytes out) for RADIUS Accounting may not be sent for a J-SAM/W-SAM/NC session if the session is less than five minutes long and the applications keep connections open all the time (e.g., Telnet, Citrix). (30493)
- When specifying a time condition in policy detail rules, the specified time range cannot cross midnight. The workaround is to break the time range into two conditions. (27811)
- By default, all access policies are closed, unless explicitly opened by a defined policy (for example, 'allow' for '*').
- Importing the system config does not import SSL Intermediate CA Certs (chains). (21040)
- The OpenWave Simulator only supports making an SSL connection if the server, or in this case the IVE, is signed by one of the following RootCAs: CyberTrust, Certicom, Diversinet, Entrust, GlobalSign, or VeriSign. (18041)
- 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.
- 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)

- 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.
- 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 now sends 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 sends SALES\john as the username.
- 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.
- The ACE Next-Pin and New-Token modes do not work properly when using ACE as the secondary login server. (21870)
- 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" option (IVE Authentication – user accounts). (22969)
- 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 did remove the password as specified and saved your changes properly. (20949)
- 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 a single authentication credential for iMode clients. This issue will be fixed in a future release. (22805)
- 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. During this period all group lookups will fail. Hence, we do not recommend manually deleting the IVE machine name from the 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)
- When using HTTP Basic Auth (in SSO), if a Realm name (not an IVE Realm but an HTTP Auth Realm) is encoded in Shift_JIS, and not UTF_8, the IVE will not properly display it. (15881)
- Avoid using special characters for user account names, such as ", ' , > , < , \$, % , and so on, otherwise, a JavaScript error may be displayed when accessing the server's user listing. (22452)
- Accounts that 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 login to one Authentication server and end-users login to a duplicate server that point to the same backend system.
- If you use RSA ACE/Server authentication and change the IVE IP address, you must delete the node verification file on the IVE for ACE/Server authentication to work. Also, make sure to uncheck the "Sent Node Verification" setting on the ACE/Server for the IVE.
- The IVE only supports Crypt/MD5 password hashes for NIS authentication.
- The Backup Domain Controller configured in an AD/NT authentication server is not used when

doing a group search in a server catalog or during runtime group mapping. (26500)

- When the Session Timeout Warning option is enabled and the user signs in from more than one browser window on the same machine, the Session Timeout Warning window is still displayed from the first browser window, even though the IVE session from the first browser window has already expired. (29160)
- 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)
- Under Session Options, the minimum value for Idle Timeout is 5 and the minimum value for Max. Session Length is 6. The documentation incorrectly lists the values for these two options. (41665)
- Session Timeout Warning is not supported on handheld devices.
- "Sign Juniper Web Controls" feature will not sign Juniper web controls that are windows executables. On Vista, User Access Control (UAC) prompts may appear for some of these windows executables, and user will see Juniper Networks company name in the UAC prompts. (46687)
- When using Siteminder-based authentication, the primary and backup policy servers must run the same version of Policy Server software. This means that a "mixed" deployment where the primary runs one version (say, 6.0) and the backup runs another (say, 5.5), is not supported.
- If multiple AD servers are configured on an IVE, then each of the servers must be associated with a different and unique machine account name. The same machine account name should NOT be used for all the servers. (46148)
- When "Test Configuration" button on AD server Admin UI is repeatedly pressed in quick succession, an error message maybe reported on the UI. This is because the IVE attempts to talk to the AD server to determine if it (i.e., IVE) has the necessary privileges to effect, among other things, a change of password. The backend AD server imposes a configurable limit on the number of times a password can be changed. Hence the error. There no work-around. The Admin must allow sufficient amount of time to elapse before testing the configuration again.

Password Management

- Password Management must be enabled at the realm level if the Admin wishes to enable password expirations or require a user to change a password at the next log-on.
- 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)
- 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 a limitation of Sun One/iPlanet to which we adhere.
- 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 propagates to all Domain Controllers. This also applies to the Domain Controller on which the change was originally performed. For more information, please refer to:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/lpe_overview.asp.

- 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.
- For a list of which Password Management functions are supported for the various platforms, and for a list of attributes, please see the Administration Guide or online Help.

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

- When using the Pocket PC (Win Mobile 5.0) to authenticate to an SA device using loginname and password, if there is a client certificate restriction set at the realm level, a "Page not found" error will be displayed after the certificate selection. If user tries to log in again, then the authentication will succeed. Currently there is no workaround. However, if a client certificate is used for authentication, then the authentication will go through the first time without the error. (43567)
- When the SA device is configured to "Accept SSL V2 and V3 and TLS V1 (maximize browser compatibility)" and the browser is set to "Use SSL 2.0" only, then the client authentication using the certificate will fail. The workaround is to check the option "Use SSL 3.0" in the browser as well. (42901)
- Client certificate authentication will fail when the client machine has Windows 2003 SP1 installed. (42869)
- Under Safari/Mac OS 10.4 and earlier, if there are multiple client certificates installed in the system, the user will not be prompted to select the appropriate certificate to connect to the SA device. The first client certificate is always passed by the system. This is a limitation in the Safari/Mac OS system and currently there is no workaround. (40217)
- The IVE does not perform revocation checking on Root CA certificates. If a user tries to login to the IVE using a valid certificate issued by a revoked Root CA, the IVE allows the user to sign in. (28892)
- When CRL checking is enabled, the CRL and the corresponding CA certificate must 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.
- Client Side Digital Certificates containing foreign language strings must conform to certain guidelines to work successfully 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)
- The IVE CRL checking mechanism ignores the IssuingDistributionPoint CRL critical extension if included in the CRL object.
- CRL download via HTTP Proxy is not supported.
- 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 are not prompted for the password again) and even USB tokens (you do 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 browsers after

logout.

One helpful mechanism to achieve this is to add 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.

- Certificate users may get an HTTP 500 error if an end-user provides an incorrect password for a private key file when challenged for a client certificate. (13489)
- When using LDAP for a CDP, do not specify port numbers in the CDP Server field. The default port number for LDAP is 389. To use a non-standard port, use Manual CDP configuration. (18578)

If you configure a client-side digital certificate authentication policy for the Realm, and the client's certificate is expired, the user cannot login to the Realm until he is given a valid client certificate. (14922)

Host Checker and Cache Cleaner

- When manually importing the virus signatures list file, Juniper recommends using the Firefox browser to download the virus signatures list file and save. Using Internet Explorer to download the file and save will cause the content to be altered such that the import will fail. (42585)
- If a client is accessing the IVE via a dial-up connection, the Host Checker installation process may time out, which prevents the user from logging in to IVE. Currently, there is no workaround available. (32627)
- If Cache Cleaner is enabled, then the last used realm will not be preserved when the user logs out and logs in again. (32418)
- If there is more than one valid IVE session (both user and admin) from a single machine and Host Checker and/or Cache Cleaner are used in those sessions, then when a user signs out from one of the sessions, all sessions will be terminated. The workaround is to turn off Host Checker/Cache Cleaner for those sessions that do not need Host Checker/Cache Cleaner. (29193)
- 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.
- 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 some previous releases, only role-based Host Checker/Cache Cleaner restrictions and resource policies were evaluated dynamically on every status update.
- 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 lost role privileges and forced disconnections.
- For installing Host Checker on the client machine while logging in with the Internet Explorer browser, either ActiveX or Java needs to be enabled. However, if the JVM on the client is the Microsoft JVM, the installation of Host Checker may fail the first time. If so, please click on the 'Try Again' button and the subsequent installation will succeed.
- Sometimes when using the Firefox browser, it may go into an indefinite "try again" loop if manual intervention is needed to correct a detected anomaly, such as deleting a file. If so, terminate the browser session and restart again.
- Host Checker and Cache Cleaner are not supported on Windows Mobile Devices and hence will not load on them. Any realm and role restrictions that require Host Checker or Cache Cleaner will fail (39116).

- Host Checker and Cache Cleaner do not work on Firefox when using Sun JVM 1.4.2_04 for the delivery of the Juniper Setup Applet. (40628)
- The Cache Cleaner option "Disable AutoComplete for Web addresses" does not work in IE7 on Windows Vista (45362).
- Whole Security Confidence Online is not supported on the Vista platforms.
- Sygate Virtual Desktop is not supported on the Vista platforms.
- Host Checker Connection Control is not supported on the Vista Platform (44515).
- When Hostchecker periodic update results in a loss of a subset of all roles associated with the session, the remediation page may not be displayed correctly. User should log out and log back in to resolve the issue (46914).

Internationalization Issues

- When importing a custom HTML Help file for end-users, if the file is encoded in a different language, for example, Shift_JIS, it must be converted to UTF-8 before it is imported by the IVE administrator. (10839)
- The following URL contains a list of characters which are not supported for filenames or folders on Samba Servers: <http://support.biglobe.ne.jp/help/faq/charactor/izonmoji.html>. (14529 and 14348)
- 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)
- Internet Explorer may truncate Japanese filenames if they are too long. Additionally, some Excel files cannot be saved. More details can be found about this non-IVE issue at:
<http://support.microsoft.com/?kbid=816868>. (14496)
- The timestamp function of the IVE may not be in the same format as what is expected when working with the Japanese user interface. The formatting for the IVE is as follows: hh:mm:ss (am|pm) and month/day/year.
- When using Netscape 4.7 and the Japanese language setting, the default font may incorrectly display characters and words on the user interface page. If this happens, you can change the font setting in the **Fonts** section of the Netscape Preferences, where you can select the option "Netscape should override the fonts specified in the document."
- 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.
- Special characters such as ①, I, ¥, and ~ are not supported in filenames for UNIX servers.
- Japanese characters are not supported in naming Authentication Servers.
- Filenames using 5c characters such as 表 and 工 will be corrupted and cannot be deleted from UNIX servers.
- Some of the diagnostics content in W-SAM is not localized and will always be displayed in English. (22068)
- In a Host Checker policy, the Admin should enter Registry Settings rule settings in English. (25097)
- W-SAM is only supported in English on the Pocket PC. (27221, 32183, 38166)

- Bolded characters in Korean, Chinese, and Japanese Help files may be difficult to read. To fix this problem change your browser's text size to a larger font. For instance, in Internet Explorer 6.0, choose **View > Text Size > Largest**. (29603)
- If you try to print Asian language Help from Firefox on Linux, square characters may appear in the printed Help. To fix the problem, use another browser such as Internet Explorer. (30017)
- Advanced Endpoint Defense: Integrated Malware Protection is only supported in English. (32550)
- End-user help will appear only in English in this release. A translated version of the end-user help will be available in the first maintenance release after the general availability release. (35712)

Adaptive Delivery – AX and Java Installers

Windows Vista additions

- On Windows Vista, with the introduction of the new “Setup Client” infrastructure that manages all downloads, configuration and launch of Juniper client applications, first time download of this component within the User Access Control (UAC) paradigm within Windows Vista will present some additional authorization dialogs in the background. This is by design due to the Windows security model. After first time installation, the time to login is very quick (46088)
- On Windows Vista, when installing the Setup Client application or any other Juniper client application, UAC prompts and Setup dialogs could be hidden in the background. However, when these dialogs appear in the background, they will blink within the user’s Start Menu “Dock”. Users should pay attention to this when working in a multi-window workspace (45441)

Existing Windows XP/Windows 2K platforms

- The Java Installer Security patch is present in Release 5.4. When a user updates their client to an SSL-VPN running version 5.4, and then they go back to an older version that doesn't have the security patch, client applications will not load using the Java Installer. Additionally, there will not be any notification to the user due to the non-persistent nature of the applet. (40923)
- Java Installer Security Patch: When "C:\Documents and Settings\<USER>\Local Settings\Temp\Juniper Networks\setup" directory is deleted, a user is able to install an "unpatched" Java installer control onto the client system. This is operating by design. It is very important that customers upgrade their SSL-VPN gateways to one of the security patches Juniper releases on 5.0, 5.1, 5.2, 5.3 or 5.4 release vehicles. (40921)
- Juniper’s Installer Service is NOT designed to update the version of ActiveX and Java Installer that is loaded on the client system. The user must go to a web browser and logon using an interactive Web Browser launch to ensure that the updated controls are installed on the client-side.
- “When using Sun Java Runtime Environment, in order to download and run the Adaptive Installer Java Applet, the user should select “Always Trust” within the Certificate warning that appears, close the browser, and restart the browser. This is a one-time operation.” (40931)

All OS platforms

- In the event that a “standalone installer” of Network Connect or WSAM is provisioned to the client, a machine that has the browser restricted such that no additional trusted publishers can be added, the ActiveX control or Java Applet required to launch the application will not be registered, and the application will not launch and will fail with **no** error. (46718)

All Client Applications

Windows Vista additions

- On Windows Vista, ONLY Version 5.5 of Juniper client applications will be supported. Windows Vista will output a warning: “This program has known incompatibility issues” when a Juniper client version 5.4 and older is attempted to install and/or launch on a Vista platform
- When installing Version 5.4 of Juniper client package: “installerservicesetup.exe” on a Windows Vista platform, the user will incorrectly see a Microsoft UAC prompt mentioned above. (46180)
- All UAC prompts that display “known incompatibility” warnings incorrectly display application name to be: Juniper Citrix Services Client.

Network Connect

- When accessing a resource on the remote network (behind the IVE) that 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 that the IVE issued from its configured IP pool. To work around this, add a static route to the router between the internal interface’s network and the remote network. This static route will route packets destined for the IVE’s Network Connect IP Pool to the IVE’s internal interface.
- The Network Connect Client IP address pool user interface requires you to enter IP addresses as ranges, with a maximum of 254 addresses per range. Specify each range on a single line. To specify a larger pool for a specific role, enter multiple IP address ranges. In the future, we will mitigate this by allowing you to enter Network Connect IP address pools with a more standard syntax (for example, IP/netmask). (6378)
- There could be some isolated instances in which, if “Detailed Logging Policy Rules” are employed for a particular user, that user’s actions might not get logged. This has only happened with a single user account within Juniper Quality Assurance, and we have not been able to reproduce this beyond this one user. This is being investigated. (25194)
- When a server-side PAC file is defined and Network Connect Split-tunneling is enabled, the IP address for the PAC source or the internal proxy should be part of the network or IP addresses defined within the Split-tunneling configuration. (26981)
- The Network Connect multicast is only compatible with switches that support IGMPv3. For IGMPv2 switches, static IGMP snooping group membership should be enabled on the port which connects to IVE. (35129)
- When signing out of Lotus iNotes 6.52, iNotes’ ActiveX deletes all cookies on the browser, including the IVE’s session cookie. If a user starts with the IVE bookmarks page and uses the same browser to access iNotes through Network Connect, J-SAM or W-SAM, then after user signs out, iNotes’ ActiveX deletes the IVE session cookie in that browser instance. As a result, when the user clicks on any links on the IVE bookmarks page, she will see an IVE login page again. Note that when the ActiveX deletes the IVE session cookie, it only affects that browser instance. The Network Connect, W-SAM or J-SAM session is not disconnected. To avoid this issue, open a new browser instance to access iNotes. (36064)
- A User-Agent string sent by a standalone Network Connect login is changed from “NcWin32” to “NcWin32<IEUserAgent>”. Any authentication policy based on a user-agent string needs to be reviewed to ensure its accuracy. For example, a previous authentication policy which checks the “NcWin32” user-agent needs to be modified to check “NcWin32*”. (37753)
- The Network Connect ACL definition requirement changed from 5.2 to 5.3 onwards. For example, xx.xx.xx.xx:80,430 is supported in 5.2, but not in 5.3 onwards. From 5.3 onwards, an ACL definition without protocol definition but with port number is not valid because ICMP doesn’t require port number.

The example ACL should be modified to: TCP://xx.xx.xx.xx:80,430 and UDP://xx.xx.xx.xx:80,430. (37997, 39905)

- If Network Connect has been launched from a computer that has an older JVM, the browser hangs. (38269)
- Network Connect supports a multicast server of the following multicast group: 224.0.0.0/8, 232.0.0.0/8, 233.0.0.0/8, and 239.0.0.0/8. (41175)
- Standalone Network Connect login has issues with client certificate on a USB smart card. (41272)
- The user is not able to select “Use Detailed Rules” when configuring Network Connect Logging policies. (41663)
- The user must have administrator privileges in order to run Network Connect diagnostics. (43096)
- NCP Idle Connection Timeout should be configured to be greater than ESP key lifetime. Otherwise, Network Connect may experience random session disconnect. (46723)

Macintosh Client

- When a Network Connect tunnel is established on a Mac OS X computer, Network Connect might encounter failures when PING packets with sizes greater than 8000 bytes are sent. This is a limitation of the underlying Mac OS X platform. (24809)
- Occasionally, Safari may not respect the new proxy settings introduced by Network Connect immediately after Network Connect is started. Restarting Safari will cause Safari to begin using the new proxy settings. (27090)
- Network Connect fails to reconnect when a VIP fail-over occurs in an Active/Passive cluster environment if the client is on the same subnet with both nodes of the cluster. (27388)

Linux Client

- Users should not remove the /etc/resolv.conf file while NC is running as it will cause the client to terminate. (31037)
- In some situations, when authenticated proxy is used with Network Connect, the proxy takes precedence over the Network Connect route, causing an HTTP resource behind the IVE to be unreachable. (34481, 33938)
- Due to a Firefox issue on Linux, CPU usage goes up significantly when the NC client is getting downloaded and installed. (34949)
- Shortcut keys for localized menu items are not correct. (35672)
- It had been observed that Network Connect client doesn't exit after Session Timeout happens. In addition, the Network Connect client remains in disconnected state after user login to IVE again. (46396, 46513)
- Sometimes a Network Connect tunnel fails to setup when launched from a command line. (38735)
- Auto-uninstall on sign-out is not working. (41010)
- Clicking the “SignOut” button on the Network Connect client or the “OK” button on the session timeout message box does not close the Network Connect client. The user must click the “Close” icon on the top right hand corner of the Network Connect client. (41012)

Windows Client

- If a Restricted user has Network Connect installed on their system, Network Connect can only be uninstalled if a user with Admin privileges attempts to run the uninstaller, or the Installer Service is installed and the restricted user uninstalls from the uninstall link under Preferences in the user's IVE homepage. (22200)
- The supported scenarios for Network Connect are valid only when the client PC does not switch NICs during the Network Connect session. Any scenario involving switching NICs might work, but is not guaranteed. The recommended behavior for the customer for switching NICs would be to end the session, switch the NIC, and then restart Network Connect. This is especially important when not using software such as the IBM Access Connection Manager that has a clean solution for switching to an enabled NIC. (22806)
- Microsoft has limited API support for parsing a proxy PAC file. If a PAC file located inside the client's PAC, i.e. Internet Explorer's "Use automatic configuration script" is "<file:///C:/myproxy.pac>," Network Connect is not able to extract the correct proxy information. (24933)
- There is a known issue with the Network Connect standalone client when a custom start page is enabled. Network Connect does not automatically launch on the client as is expected with the standalone client. (25151, 32269)
- When upgrading the client from prior versions of Network Connect to version 5.0.0 or later, it is important to note that attempting to "uninstall" Network Connect from the Juniper SSL-VPN Web UI will not uninstall older versions of Network Connect. Each version of Network Connect will need to be uninstalled separately. (25958)
- In rare situations, Windows is not able to renew the DHCP lease on the Network Connect driver, as the driver has reached its DHCP NACK limit. In this situation, the Network Connect adapter will lose its IP, consequently disconnecting the user. The client may still show a false "connected" state. The workaround is to exit and launch Network Connect again. (27425)
- When an existing Network Connect session is established, adding a PCMCIA-enabled Wireless card to a laptop will break the Network Connect connection. (27522)
- While still installing the Network Connect client, if a user tries to launch Network Connect (say from a previously installed version), Network Connect throws an error message "Error opening file for writing". (28143)
- In certain situations, users may get a "Cannot connect to IVE" the first time they launch Network Connect. Subsequent launches will connect without issues. This is due to conflicting software that does not allow Network Connect to bind to the TCP/IP stack properly. (28845)
- Some diagnostic tests in the Advanced View of the Network Connect client may fail on unsupported platforms due to lack of libraries that the tests depend on. (29082)
- If a 5.1R2 or later Network Connect client is installed in a PC that already has a 5.0R2 or earlier version of Network Connect installed, then uninstalling either client could render the remaining client inoperable. The workaround is to uninstall all clients and reinstall the older clients first and the newer client next. (29425)
- If both Network Connect and W-SAM are enabled for auto-launch for the same role, only W-SAM auto-launches. We recommend that users only use one access method at a time, as using both causes unnecessary performance overhead for the client. (30604)
- If the Network Connect client is running, and the user tries to launch another client, the user gets an appropriate error message. However, the user is not redirected back to the IVE homepage from the "Please Wait" page. (31103)

- When ActiveX is “Disabled,” and the Sun JRE 1.4.1 or higher is enabled, signing out of the IVE Web interface will prompt the user to accept the SSL certificate up to two times (32129). Accepting the certificate prompt will successfully log the user out. This affects ALL Windows applications, including W-SAM, Network Connect, Windows Terminal Services, Secure Meeting, Host Checker, and Cache Cleaner
- The Network Connect client fails to launch if Kaspersky 5.0 Pro is installed on the same PC. (33123)
- Network Connect fails to connect if early versions of Checkpoint Secure client are installed on the same computer. Network Connect supports Checkpoint Secure client R5.5. (33162)
- Network Connect fails to connect when using the VIP on the DX. (34905)
- When Network Connect is connected to the Secure Gateway externally, an entry is added to the hosts file to point to the external interface of the Secure Gateway. (35774)
- Uninstalling the Network Connect client driver manually causes the Network Connect client to be unable to connect to the IVE. The client driver displays a “Failed to Connect to the Secure Gateway. Reconnect?” message. (35993)
- When running on Windows XP SP1, the Network Connect client has compatibility issues with iPass/Telia if split tunneling is disabled. This is due to Windows XP SP1 system issue. This issue doesn’t exist on Windows XP SP2. (36137, 35292)
- If a split tunnel is enabled and the configured IVE server IP address is not in the split tunnel subnet, after NC tunnel connects, NC diagnostics shows an incorrect message stating that NC has failed to establish a connection to the NC server. This is because the configured IVE server IP is not routed through the split tunnel network, thus, NC diagnostics are not able to ping the server IP when the NC tunnel is established. (39228)
- If you install the Odyssey client when a Network Connect client is running, the Network Connect client will be disconnected. (40159)
- The Network Connect client doesn’t support the configuration where both PAC file proxy and manual proxy are selected. (40061)
- On rare occasions, if Windows is not able to sync with the timer server when the Network Connect client is running, Network Connect may repeatedly display a session timeout message box. (40718)
- The Virtual Adapter of Network Connect shows the default gateway as 0.0.0.0 (45131)
- New Secure Gateway Window menu button is not supported in this release. (45157)
- McAfee Enterprise version 8.5.0i is blocking Network Connect client from functioning properly. (45292)
- With Vista strong host model enabled, when Network Connect client connects to IVE, current local area network traffic doesn’t go through Network Connect tunnel even if split tunnel disabled is configured. (45695)
- (46182) Vista Advanced firewall by default blocks all inbound traffic and allow all outbound traffic. To have Network Connect working in conjunction with Vista Advanced firewall, please configure the following settings:
 - Change Vista Advance firewall default settings to block all inbound and outbound

traffic.

- Create the following outbound rules in the appropriate firewall profile:
 - Create a port rule to allow any to any IP and TCP any port to 443
 - Create a custom rule to allow 127.0.0.1 to 127.0.0.1 TCP any to any
- Allow iExplorer.exe

GINA

- The Network Connect client needs to be installed prior to Windows logon for the GINA launch to occur. We strongly recommend that you do not enable auto-uninstall of Network Connect on sign out for roles where GINA is enabled. (29937)
- To login to IVE using NC GINA, user has to use same IVE IP address / hostname as used using browser. For example, if IVE has external IP and internal IP addresses, and client is able to reach IVE via either of the two IP addresses. If user used IVE's external IP address to login using browser, when using NC GINA, user has to use the IVE's external IP address. If user uses IVE's internal IP address, NC tunnel can not be established. (34534)
- When connecting to the IVE using GINA/HC with authenticated proxy, the user is asked to enter credentials twice, once for Network Connect GINA and once for Host Checker. (34656)
- GINA/HC: Advanced Endpoint Defense: Integrated Malware Protection detection works only in user context mode and in certain situations described in the documentation. (34806)
- When GINA starts with Host Checker enabled, and Cache Cleaner is running, log entries appear in the User Access Logs. (35223)
- Network Connect GINA installs but does not launch on computers that are not within the domain one is trying to log into. (35566)
- GINA doesn't support certificate authentication. (36093, 34534)
- If the IVE is not responsive, the GINA login progress screen may freeze for up to 30 seconds. (37299)
- Occasionally, after the user successfully launches Network Connect using the GINA login, the Network Connect icon remains grayed out. (37615/43300)
- When Network Connect is upgraded, the GINA from the upgraded version does not take effect until the user reboots the machine. This works by design. A reboot warning message should be displayed. (38856)
- Network Connect GINA has a compatibility issue with the Odyssey client GINA. There are two workarounds: 1. Disable the Odyssey client GINA to enable the Network Connect GINA to function properly; 2. Enter Machine authentication credentials into the Odyssey Client so that it can authenticate against the Access Point prior to Windows login. (40091)
- If a 3rd party GINA is installed after Network Connect GINA, Network Connect can not be uninstalled until user uninstalls the 3rd party GINA. (44102)
- When user login via Juniper GINA to an IVE, if there is a matching version of Network Connect client present in user's PC, Juniper GINA establishes Network Connect connection

to IVE using the appropriate version of Network Connect client. If there is no matching version of Network Connect client present, Juniper GINA will not be able to setup a Network Connect connection to IVE. Prior to release 5.4, Juniper GINA displays a version mismatch warning message and allows user to login to Windows desktop using the cached credentials. Release 5.4 Juniper GINA has a added feature that after user is logged in to Windows desktop with the cached credentials, a standalone Network Connect client is automatically launched which user can use to login to IVE and the appropriate version of Network Connect client will be automatically downloaded and launched. (44327)

NC Command Launcher

- If a user is using Microsoft Internet Explorer 6.0 Service Pack 1 and a proxy is configured, the user is not able to launch a New Secure Gateway window from the Network Connect icon menu. This is due to IE 6.0 SP1 problem: <http://support.microsoft.com/?kbid=329802> (38869)
- The Network Connect launcher doesn't support Host Checker and Cache Cleaner in this release. (38876)
- If NC Command Launcher is executed when another NC session is running, this may freeze the first NC session. (42205)
- Possible return codes from the NC Command Launcher:

Return Code	Meaning
-1	(- Stop/ -Signout) Network Connect is not currently running. System error happened.
0	Network Connect has started.
1	Invalid program arguments have been specified
2	Network Connect was unable to connect to <the Secure Gateway>.
3	Network Connect was unable to authenticate with the server.
4	The specified role is invalid or does not exist.
5	Network Connect can not run because a required pre-authentication application could not be started.
6	Network Connect installation has failed.
8	Network Connect was unable to perform a required software upgrade.
10	The server you are attempting a connection with does not currently support this feature.
12	Network Connect failed to authenticate the client certificate.

Installer Service

- The Installer Service shows in the services manager as "neoterisSetupService". It will be changed

to "JuniperSetupService". (35134)

- If Encrypted File System is enabled on current user's temp directory, Install Service fails to install. (36569)

Client-side Log Upload

- On Windows, the Secure Meeting client should write to log files if log upload is enabled even if client side logging is disabled. However, the Secure Meeting client doesn't write to log files if client side logging is disabled. This will be fixed before the product release. (36212)
- Enabling Log Upload on IVE console will triggers client side logging. This may have a performance impact. (40171)

Rewriter/Web Applications

- In IVE versions 5.4 and greater, the rewriter behavior was modified for the "Unchanged" caching policy. In versions prior to 5.4, for the "Unchanged" caching policy, the IVE would strip out Cache-Control:no-cache and pragma:no-cache headers in the response header. In versions 5.4 and later, the caching headers are not modified and sent as is. One implication of this change is for the Citrix published application through Web Interface. In some cases the Web Interface server may send a Cache-Control:no-cache in the response header for an ICA file. In 5.4, with a caching policy of "Unchanged", this caching header will not be removed and therefore the ICA file will not be downloaded to the PC. To fix this issue, change the caching policy to Smart Caching. (48861)
- Creating contact with similar name as a previous contact will overwrites the previous contact in OWA 2000 and 2003. The workaround is to configure HTTP 1.1 policy under Resource Policies > Web > Protocol for "http(s)://<exchange server>/exchange/*" and "http(s)://<exchange>/exchweb/*" (44818)
- Form Post SSO is not supported on iMode appliances. (43648)
- The PDF rewriter does not support PDF files that contain 2 objects for the same link. (41572, 44040)
- If there is a difference between the time on the SA and the end user machine then the session timeout reminder popup will be off by a value equal to the time difference. This is true if the only access mechanism enabled on the SA is the rewriter or file browsing. (41260)
- Microsoft Office XML documents that reference or include external files are not supported through the rewriter. (Bug 41422)
- In the detailed rules for SSO Form POST and the SSO Cookie/Headers resource policies, if the configured POST values or header values are re-sorted then all the configured values are erased. (43896)
- When saving attachments of type .htm or .html, the Caching policy in the IVE must be configured to "Unchanged". If the caching policy is configured to "Smart Caching" then the IVE will prevent the attachment from being saved to disk. (43983)
- Opening an attachment in a new email that has not been sent does not work in OWA 2000. (40372)
- Web applications that contain either http://localhost or https://localhost are not supported through the rewriter. (40734)
- For security reasons, if the <password> token is configured in an IVE bookmark then it is not replaced with the user's password to the SA appliance. This behavior was changed in the 5.0 release. (39966)

- When accessing a hostname using a short name and this short name has been added to the SA hosts file then the resource matching for resource policy evaluation will be done against the short name. On the other hand, if a host entry does not exist for the short name on the SA and the hostname resolution is done by DNS by adding the domains entered on the Networks configuration page then the FQDN will be used for matching resource names when doing resource policy evaluation. (39987)
- To improve the response time to access the SA index page on a handheld device, the following images will not be displayed on the SA home page: the help logo, the sign out logo, the open bookmark in new page logo, and the WSAM logo. These logos will be replaced with text. (38844)
- For some versions of Internet Explorer (see <http://support.microsoft.com/?kbid=327286>), if gzip is enabled on the SA appliance then some pages in the iNotes or OWA web application may show up blank. To workaroud this issue, either disable gzip on the SA appliance or change the caching resource policy to “Unchanged” . For OWA 2003, by setting “Unchanged” for the resource `http[s]://*:/exchange/` should be sufficient (39589).
- Web content does not get cached on a Pocket PC over an SSL connection even if caching headers are sent by the SA appliance to Pocket IE. Therefore multiple requests to the server will be seen for pages accessed through the SA (39482).
- To support the Oracle Financials application in a clientless manner, the following steps must be taken:
 1. The Oracle application must be configured as a Pass Through Proxy application on the IVE.
 2. The Oracle application must be set to the “Forms Listener Servlet” mode.
 3. If using a self-signed certificate on the IVE then you must follow the steps outlined in <http://www.oratransplant.nl/2005/07/11/using-self-signed-ssl-certificates-with-iiinitiator/> or you must upload a production Web server certificate to the IVE (38806).
- NTLM, Basic Auth, and Form POST SSO will not work with application servers that expect the username and password characters in a non-UTF-8 encoding (38522).
- PDF files greater than 32 Mb are not supported through the rewriter (38375).
- IVE does not work with Whole Security Confidence Online version 4.3. It works with Confidence Online version 5.0. (35634)
- Unauthenticated POST content that is larger than 4K will fail when sending content to a server that is protected by Basic Authentication. (27707)
- Some Java applets (including Citrix Java applets) on Mac OS 10.4 running JVM 1.5 might fail through the IVE rewriter if a production SSL certificate is not installed on the IVE. (29303)
- 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 deselect the setting “Warn users about the certificate problems” under **Roles > Web > Options > Allow browsing untrusted SSL Web servers**. (27281)
- If using Safari on Mac OS, the browsing toolbar may not show up on Web pages that contain Flash objects and Java applets. (25896)
- When accessing, through the IVE, a Flash Web site that requires Macromedia, the user is not prompted to install the Macromedia application. Therefore, the Flash Web site does not render properly (26391).
- When accessing Flash content, if the Flash content is generating Actionscript from within

Actionscript and that Actionscript is generating links, then it may not work through the rewriter. (38638)

- Flash video files (.flv files) that are included in a SWF file using Actionscript commands and played back at runtime are not supported through the Flash rewriter. As a workaround, use PTP. (43108)
- The Macromedia Breeze application is not supported through the Flash Rewriting feature. (33275, 34489)
- The “Display Favorites” functionality on the IVE toolbar may not work on Web sites that use iFrames or frames. (27361,24621)
- The IVE always intermediates a Web proxy using basic authentication, even if the administrator has disabled the “Intermediate Basic Authentication” option. (24675)
- Checking in of documents in the Documentum Web application is not supported through the Java rewriter.
- Accessing documents in Documentum v5.3 is not supported through the rewriter due to the application's use of a variant of JNLP technology. JSAM or WSAM can be used to support this application. (43424)
- Lotus iNotes in offline mode is not supported through the rewriter. (9889)
- The correct caching resource policies must be configured to enable end-users to open and save email attachments of different document types in OWA and iNotes. To successfully open and save attachments of different document types, use the OWA and iNotes template under Resource Profiles -> Web.
- In Firefox 2.0, when trying to save attachments in OWA or iNotes, ",DanaInfo=<webserver name>" might show up in the filename. For Firefox releases prior to 2.0, a caching policy of "Unchanged" will allow you to save attachments without "DanaInfo.." appearing in the filename. (43660)
- 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)
- 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)
- 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 Network Connect. 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.
- The native browser on a Symbian handheld device is not supported. (22743)
- On a Symbian handheld 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)
- PowerPoint files may not display properly with Office 2002 in Internet Explorer on Windows 2000. To work around this limitation, administrators should advise end-users to install Microsoft Office 2002 Service Pack 1 and Service Pack 2.
- 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)
- The IVE supports Web proxies that do NTLM authentication. However, the IVE does not support

the case in which there is a proxy between the IVE and the backend server, and the backend server performs the NTLM authentication. (26144)

- When using Internet Explorer 5.5 or 6.0 with 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>
- The IVE Web browsing function does not support URLs of more than 159 characters in length, including extensions, such as ".html".
- On a Macintosh, 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. To work around this, the toolbar can be disabled in the **Roles > UI Options** tab.
- If you enter a server for selective rewriting, and want to be able to access it with and without the domain suffix, you must specify both types of entry. If you have specified "foo.company.com" and try accessing "foo," the response will not be served via pass through proxy. Similarly, if you specify an entry for "foo" and try accessing "foo.company.com," the response will not be served via selective rewrite.
- When using OWA 2003, if you have enabled the forms-based Authentication option on the IVE, the OWA 2003 log-in credentials are cleared when you log out. If this option is disabled, however, the log-in credentials are not cleared.
- When using OWA 2003, the Administrator should ensure that the OWA server has only NTLM or Basic Authentication enabled, not both.
- There are known issues with Microsoft's pop-up 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 pop-up blockers be disabled and that the user refresh their OWA session after disabling the pop-up blocker. Additionally, pop-up blockers may cause problems with other IVE functions using pop-ups (for example, file uploads, online Help, or the IVE Upgrade Progress window, Dashboard Configuration page, and Server Catalog Configuration pages in the Admin console. (23092)
- With Mozilla Firefox and Netscape, saving files containing Japanese characters may result in garbled file names. (30602)
- Microsoft Sharepoint 2003 through the rewriter:
 - A production certificate is required on the IVE to be able to download or edit Microsoft Office documents. If a production certificate is not installed in the IVE and the user attempts to download a Microsoft Office document then the Office application might hang (35593).
 - Microsoft Office 2003 SP1 or greater is required when editing/viewing documents through the document library or through Explorer view. (38916)
 - Microsoft Office 2003 SP1 or greater is required for the multiple picture upload functionality. (38917)
 - Downloading documents larger than 32 Mb through Sharepoint is not supported through the rewriter. (38375)
 - When using the Netegrity authentication server, in-line editing of Microsoft Office documents in Sharepoint is not supported. (36776)
 - When accessing the Explorer View in Sharepoint through the rewriter, the following items are not available on the left-hand nav bar: "File and Folder Tasks" , "Details" , "Publish this file to the Web" , "Email this file" , and "Print this file" . This is the

- same behavior if the Sharepoint server has SSL enabled and is accessed directly without the rewriter. (37710)
- Explorer view "move" copies the file and does not delete the file from the source folder. (35033)
 - When uploading a document through Explorer View in Sharepoint, the new document is not displayed unless you exit and then restart Explorer View. This is a limitation within Sharepoint. (38870)
 - Using the Frontpage editor from the Internet Explorer toolbar to edit a Sharepoint web page and then saving it back to the Sharepoint server is not supported through the rewriter (40611).
 - The Picture Manager functionality is not available if using the Siteminder authentication server.
 - The Sharepoint Forms feature is not supported.
 - In an Active/Passive cluster, if the user edits a document through the Shared Documents view during a failover, the document may open up as read-only. As a workaround, click the document again.
 - In an Active/Passive cluster, if the user launches the Picture Manager to upload multiple documents during a failover, the Picture Manager might fail to launch. As a workaround, click the "Upload Multiple Files..." link again.
 - The images in the pulldown menu for each listed document in the document library are missing if persistent session cookie is enabled. This is a limitation of Internet Explorer. To workaround this problem, check "Override automatic cookie handling" under Internet Tools-> Internet Options -> Privacy tab -> Advanced button. Select "Accept" under First-party Cookies. (42001)
 - Office 2002 through Sharepoint is not supported. (44318, 44213)
- Microsoft Sharepoint 2003 on Vista
 - To use Sharepoint 2003 through the rewriter on Vista, users must add the IVE to the Trusted Sites zone on IE7 where Protected Mode is disabled. (44588, 44937, 44719, 44716, 45466, 45464, 45423, 45420)
 - A production certificate is required on the IVE to use Explorer View on the Vista platform. (44588)
 - On Vista, admin must enable Persistent Session under **Roles -> Session Options** for Explorer View to work. (44588)
 - If Explorer View is opened within the IE7 browser instead of a separate window, it contains less functionality. For example, the list of folders and directory browsing are not displayed in the left panel. (44588)
 - Using IE7, if user encounters problems accessing Explorer View the second time after he sign out of IVE and sign back in, try deleting IE 7 file cache. (44588)
 - HDML used by Openwave browsers is not supported through the rewriter. (28627)
 - For OWA 2003 support, the following compression resource policy must be added, **Resource Policies > Web > Compression**, `http://<OWA server>:80/exchange/*/?cmd=treehierarchy > not compress.` (35937)

- The rewriter does not support load balancers that use version 3 session ID Secure Socket Layer (SSL) for client-server stickiness. (35619)
- The JavaScript call `window.createpopup` is not supported with persistent cookies. This call is used in Siebel 7.5. The workaround is to disable persistent cookie for Siebel 7.5. (32044)
- The standard and framed IVE toolbar does not appear in the iNotes application in Safari 1.3. (29926)
- You may see a secure/insecure warning from the browser when accessing the Citrix NFuse page with gzip compression enabled on the IVE. To turn off this warning, disable compression for the following resource: `http://<Nfuse server>:80/citrix/metaframe/default/html/timeoutrefresh.html`. (35281)
- To enable rewriting support on the Vodafone and KDDI phones, additional configuration information must be added under **System > Configuration > Client Types**. For Vodafone, add *Vodafone* for the user-agent string and "Compact HTML" for the Client Type. For support of the KDDI phone, add *KDDI* for the user-agent string and "Compact HTML" for the Client Type. (36180)

Pass-Through Proxy Issues

- If PTP is configured in hostmode and the virtual hostname is different from the IVE hostname and if a persistent cookie is enabled under **Roles -> Session Options** then the following option must be enabled in IE for the PTP rewriting to work successfully: 'Override automatic cookie handling' under **Tools->Internet Options->Privacy->Advanced Privacy Settings**. (38989)
- 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
- Pass-Through Proxy URLs must be hostnames. Paths of hostnames are not supported.
- Juniper Networks strongly recommends that Administrators not mix Pass-Through Proxy Port and Host modes.
- If the user is using Mozilla Firefox with Pass-Through Proxy (with the IVE port configuration), the IVE may invalidate the user session, thus requiring the user to sign in again.
- 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, path '*', and value 'No-Store'.
- When using OWA via 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 using Microsoft Outlook. (9233)
- Browser request follow-through does not work in Pass-Through Proxy if the virtual hostname is different from the IVE hostname. (37462)
- When using Lotus iNotes through Pass-through Proxy clicking on the logout button in Lotus iNotes will logout the user from the IVE (41825)
- If Pass-through proxy with "Rewrite external links" is configured for OWA or iNotes then links embedded in email messages are not clickable (44053).
- To use Sharepoint 2003 through Pass Through Proxy Hostmode on Vista, users must add the

virtual hostname to the Trusted Sites zone on IE7 where Protected Mode is disabled. (46059)

Hosted Java Applet Issues

- When using the Java applet upload feature, if you include the <PASSWORD> token within the generated HTML, it appears in cleartext 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. We strongly discourage the use of the <PASSWORD> token in the HTML code. (27033)
- The Java applet upload feature may not work on Mozilla Firefox 1.6 unless the default cookie settings for the browser are modified. This is because Mozilla Firefox 1.6 does not pass cookies from the browser to the Java applet. To work around this limitation, change the settings to "Enable all cookies" in Mozilla's **Edit > Preferences > Privacy & Security > Cookies** or enable "Include IVE session cookie in URL" in the IVE Admin console. (27353)
- The "useslibrarycabbase" does not work with hosted Java applets. We strongly recommend that "useslibrarycabbase" not be used as a PARAM to reference the cab file (34209).

File Browsing

- When a file with Japanese characters in the filename is opened right after the download, the filename looks corrupted. This is due to the IE browser not honoring the content-disposition header when the file is opened directly. (32266)
- NFS Auto-mount is not supported on Linux NIS/NFS servers, only on Sun servers. (2005)
- Session termination does not affect file transfers through Windows file share. (26897)
- Depending on the Web browser, downloading files with filenames 18 to 25 characters in length may not work through the IVE. Files with longer or shorter filenames are okay.
- If an administrator denies 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 situation, administrators should configure both the IP address and hostname in their file browsing ACLs.
- For NFS file browsing to work properly, you must configure an NIS server on the IVE before enabling NFS file browsing. (14594)
- 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 incorrectly. This is due to a bug in Internet Explorer. (19612)
- When using the multiple file download feature in Windows File Browsing, the downloaded zip file will not preserve the names of the files if the file name contains non-English characters (38304).
- In the Administration Guide, the following text is incorrect: "The encoding option in Users > Resource Policies > Files > Encoding allows you to tune the rewriter to support localized pages during rewrite and file browsing." The encoding option only applies to file browsing, not to the rewriter. (42136)
- If the File Policy option 'Allow NTLM V1' is enabled, the IVE will use only NTLM V1 for File Share authentication. If this option is disabled, IVE will use NTLM V2 for File Share authentication and will not fall back to NTLM V1 if the authentication using NTLM V2 fails. (39244)
- Windows network discovery is not disabled by default in a newly created IVS. It may be disabled if the file browsing feature is not used for the IVS. (43152)

- Due to a bug in Microsoft Network discovery API NetServerEnum2 IVE will not be able to extract the workgroup information if the master browse server is in a different subnet (43172).
- NFS file browsing does not work if user authenticates with Active Directory or System Local auth servers. (44157)
- For DFS file sharing on Windows 2003 Server and Windows 2003 R2 Server, if the domain root is a hidden share (name contains an ending \$) and has links to shared folders on same or different domains, file operations do not work. (42557)
- For DFS file sharing on Windows 2003 Server and Windows 2003 R2 Server, if the domain root is a hidden share and has links to hidden root shares on same or different domains, file operations do not work. (42557)
- For DFS file sharing, file operations do not work on a root share that refers to another root share in the same or different domain. (42557)
- For DFS file sharing on Windows 2003 Server and Windows 2003 R2 Server, if the domain root has links to hidden root shares on same or different domains, file operations do not work. (42557)

SA 1000 through SA 6000 Items

Windows Secure Application Manager

- When using Citrix Terminal Services over Windows Secure Application Manager (WSAM), the Citrix "Session Reliability" feature should be disabled on the Citrix Metaframe clients. There are some complex TCP sequence interactions that are causing the application to break when this feature is enabled (21421)
- When WSAM applications are defined in Application Mode, in some cases, clients might find duplicate entries of this application name being displayed in the **WSAM client > Detailed** tab. This is a cosmetic problem and will be resolved in future releases. (41400)
- In order to uninstall W-SAM, the end-user should use the Uninstall link in the UI under **Preferences > Applications**. (20415)
- If the Lotus Notes Background Replicator is used within the Lotus Notes Client with the other email and database functionality, and the remote user needs access to this functionality through the Secure Access Gateway, Network Connect is required. If Lotus Notes Background Replicator is not used, W-SAM and J-SAM will both work as access methods. There is a chance that this might work in Release 5.0 W-SAM and later versions, but it has not been verified yet. (23346)
- When using WSAM with Checkpoint Secure Remote R56 client, there are known interoperability issues introduced by the Checkpoint product. (34584)
 - If WSAM is installed prior to Checkpoint Secure Remote R56 install, then WSAM will work fine.
 - If WSAM is installed **after** installing Checkpoint Secure Remote R56, WSAM does not work.
 - We have also identified that Checkpoint R60 works fine with WSAM in either scenario (a) or scenario (b). This indicates that there were code changes in Checkpoint 6.0 that resolved this interoperability issue with WSAM and other TDI driver-based clients. We are pursuing this issue with Checkpoint R&D.
- In Release 5.2, Juniper investigated support for DFS File Sharing through W-SAM. However, we have identified that the system needs to trigger Domain Authentication via ICMP/Kerberos, and this functionality is currently not supported. Once Domain Authentication is fully supported through W-SAM, there is a high probability Juniper can make DFS File sharing work. There is no

ETA at the moment for supporting Domain Authentication. (30587)

- When the “W-SAM uninstall at exit” option is activated on the server, the user cannot launch W-SAM twice within an authenticated session. Users must sign in to the IVE two separate times—the first one resulting in an uninstallation, and the second initiating a reinstallation. (26698)
- When using W-SAM diagnostic tools and the built-in log viewer, we recommend that you make your log level selection first, and then launch/re-launch W-SAM so that the log file can be viewed from the diagnostic utility. (25038)
- Now that the W-SAM client for Windows 2000/XP is built on a TDI-based architecture, only one application (BitGuard Personal Firewall) is known to be incompatible with W-SAM.
- Customers who use Norton Antivirus Personal Edition 2003 and 2004 should be aware of a live update that Symantec has made available to resolve some TDI compatibility issues with other TDI drivers, like the one used by Windows Secure Application Manager (W-SAM). We recommend you run Symantec live update before installing W-SAM. (24285)
- If Auto-Upgrade is disabled on the gateway, and the user has the older version of W-SAM installed on their computer, an error message appears instructing them to uninstall their existing application prior to reinstalling W-SAM. The user must manually re-direct their browser by clicking on the available hyperlink. (27350)
- Restricted users can't install W-SAM using the Stand-alone Installer, even in the presence of the Installer Service. The Installer Service is designed to provide application installation capability for users who are performing a standard Web-based installation from the IVE. (22454)
- If a Windows XP client has the “Fast User Switching” option enabled and is switching between two active user sessions, W-SAM upgrade notifications may get crossed between these active user sessions. (23090)
- If you have the NCP Auto-select option disabled, and answer “No” to the security warning during the load process, W-SAM does not initially launch. There is no additional impact to the user session. (18681)
- 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.
- If W-SAM is configured in Host Mode, and the Web browser is configured to go through a proxy to access the IVE, W-SAM is not able to tunnel traffic to the specified hosts. To resolve this issue, 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.
- If Samlauncher.exe is launched from the root directory, such as *c:*, start test on diagnostics tab doesn't work. The workaround is to launch Samlauncher.exe from a subdirectory, such as *c:\Juniper Networks*. (43617)
- In Firefox 2.0, when launching WSAM, another tab will be opened on the browser. (43770)
- The New Window menu button doesn't redirect user to IVE home page (42546).
- Sign out on IVE home page from a Firefox browser terminates WSAM session but leaves WSAM reconnect dialog popup open. (45033)
- Outlook Express is not supported through WSAM. (45267)
- If admin doesn't input any value in “Allowed Server Ports” field, it is interpreted as “*:*” by WSAM. (42119)
- Enable client log for WSAM impacts throughput. (44585)

Pocket PC

- Please enable Roaming for IVE sessions when being used over GPRS because the IP address of the phone may change.
- WSAM UI strings are not localized. (38166)
- W-SAM menu strings are not visible if the Pocket PC device's tool bar has extremely dark color. This problem was observed on Orange M5000 device. (40544)
- On occasions, Direct Push Technology doesn't work well. (42805)
- W-SAM on PPC doesn't support persistent session. If persistent session is enabled, after W-SAM launches, it redirects browser to the initial log-in IVE page instead of IVE home page. (42870)
- On certain devices, such as Cingular 8125, user is asked to reboot the device when launching W-SAM on a different IVE even though this IVE has same release version as the installed W-SAM. (42870)

Customizable Sign-In Pages

- If custom sign-in pages are used, after upgrade to 5.4, please check the Admin Access log to see whether there are any validation errors in those pages. If there are any errors, please re-customize based on the error messages to make custom sign-in pages work properly on the 5.4 release. (32083)
- We do not recommended associating custom sign-in pages with the default sign-in URL (*). Doing so may cause the log-in process to go into a loop if there is problem in the custom sign-in pages. (30154)
- If a pre-5.0 .zip file is used, please follow the steps to customize it for the 5.0 R1 release (28075):
 1. Unzip the old .zip file.
 2. Delete the LoginPage-ppc.shtml file.
 3. Edit the LoginPage.shtml file to add the following text as the very FIRST line:

```
<%# NetScreen Page Version 1001 %>
```
 4. Edit the LoginPage.shtml file by adding the following snippet anywhere in the page (except in a comment):

```
<% IF 0 %>  
<% prompts %>  
<% END %>
```
 5. Zip up all the pages and associated objects.
 6. Upload this .zip file.
- To ensure that the New Pin and Next Token pages are customized for SoftID authentication, 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.
- The total combined size of all uploaded customizable UI .zip files cannot exceed 12MB.
- IVE sign-in pages 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, you can upload customized sign-in pages using the Template Toolkit. Please contact Juniper Networks Support for details (<http://www.juniper.net/support>).

- When creating customizable sign-in pages, save them as UTF-8. (17211)
- Four new required variables have been added to the LoginPage.shtml (46536). They are as follows:
 - hcInAcTimeout – Specifies the Host Checker login inactivity timeout in minutes.
 - hcRunning – Specifies whether Host Checker is running or not.
 - ccInAcTimeout – Specifies the Cache Cleaner login inactivity timeout in minutes.
 - ccRunning – Specifies whether Cache Cleaner is running or not.
- Please retry again if you receive an error message "Unable to save new Custom Sign-In pages" while uploading custom sign-in pages. (46936)

FIPS

- If you replace an administrator card using option 10 in the serial console after upgrading a Secure Access Series FIPS appliance, the Security World is modified to use the new administrator card. If you then try to perform a “rollback,” the new administrator card does 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 activate the new administrator card, you must use option 10 on the serial console once again.
- Secure 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 to ensure they are synchronized. If the cluster nodes are not synchronized, time-based features (such as Secure Meeting) do not function properly.
- If the HSM module switch is set to I on a FIPS-enabled Secure Access appliance, the machine is in “initialize” mode. Rebooting the appliance during this time reinitializes the server key and invalidates the current server certificate. Administrators must leave the switch at O during normal operation (as per the instructions on the serial console and in the documentation).
- To setup a WAN FIPS Cluster, it is recommended that the devices be configured at one site before sending the unit to the final location as the initial configuration requires the smart cards to be available.
- The FIPS Status LED on the front panel of the SA 4000 FIPS and SA 6000 FIPS product lines is reserved for future use. The device operates correctly under the FIPS specification regardless of the state of the LED.

MSP (IVS/VLAN)

- In an Active/Passive clustered MSP deployment with a large number of configured VLANs and VLAN virtual ports (200 VLANs, 2 virtual ports per VLAN), migration of the VLAN virtual ports from the formerly Active Node to the newly Active Node can take 2 to 4 minutes to complete. During this interval, the VLAN virtual ports will be unreachable. (32030)
- NC address assignment within an IVS via a centralized DHCP server (configured to serve multiple IVS's) does not work if the IVS name contains certain special characters. The following special characters -, _ (, . , < , > , [,] , { , } , @ and : are supported. The administrator is advised to avoid using any other special characters in the IVS name. (33793)
- While doing an upgrade on an SA700 (which does not have an IVS license), the text "Importing

ivs data" is displayed on the serial console. (35596)

- The `iveMaxConcurrentUsersVirtualSystem` trap is not sent when the maximum allowable number of users (per the IVS profile configuration) are signed in to the IVS. However, the major log trap is generated correctly for this event, so the workaround is to turn on the Major Log checkbox under Log/Monitoring in the root system. (40729)
- If a binary system config is import with "include network settings" selected, to an IVE with IVSs and VLANs, then existing VLANs will be replaced. This may leave an IVS with no Selected VLANs in its profile. To work around this issue, the IVS root admin must go into each individual IVS and reconfigure the "Selected VLANs" and mark the appropriate VLAN in each IVS as default. In addition, they need to go into each Role within each IVS and click on "Save changes" to ensure that the default VLAN configured for the IVS is correctly reflected in the Role's VLAN/Source IP settings. (41085)
- If IVS configuration import is performed on one node of a cluster, and any of the imported IVS's have JSAM configured, then JSAM for IVS's can only be activated on the node into which the IVS configuration was imported. Attempts to launch JSAM on IVS's on any other cluster node will fail. To work around this issue, the MSP root admin has to manually import the IVS configuration into each of the other nodes in the cluster. (44003)

MSP administrator advisories:

- For clients to be able to establish Network Connect sessions to an IVS, the IVS must have DNS settings for the IVS. Otherwise, the Network Connect session initiation fails and displays an error message.
- The Internal Port must be assigned to the root system and marked as the default VLAN. Additionally, VLAN interfaces can be assigned to the root system. All authentication servers configured for the root system, however, must have routes in the Internal Port's route table, even if the servers are reachable via VLAN interfaces. Routes to servers reachable via VLAN interfaces must have the next-hop gateway set to the configured gateway for the VLAN interface, and the output port defined as the VLAN port.
- Custom sign-in pages could potentially require a large amount of memory and disk space. In order to provide custom sign-in pages per IVS, we recommend you customize the sample custom sign-in pages provided on the IVE.
- For an Active/Passive clustered deployment, the root admin of an MSP network should configure all VLAN ports with at least one virtual port (**System > Network > VLANs > Virtual Ports**). The router admin must configure routes for the IVS Network Connect IP ranges that point to the VLAN virtual port's IP address as the next-hop gateway. This is required for Network Connect session failover from an IVS in the Active Node to the corresponding IVS in the Passive Node.
- The standalone client installers are not accessible directly from the Admin UI of an IVS. As a workaround, the root admin can make the following link available to IVS administrators if the IVS administrators need to download standalone installers:

<https://myive/dana-admin/sysinfo/installers.cgi>

where "myive" is the hostname of your IVE.

- End-users or administrators can sign into an IVS over VLAN interfaces or over virtual ports specifically defined to accommodate such sign-in activity. This is an extension of the IVS sign-in feature, not a limitation.
- For MSP subscribers with logging requirements that exceed 1MB, the recommendation is to redirect the corresponding IVS logs to a syslog server rather than rely on native logging on the

IVE. The syslog server could be a central server across multiple IVS systems, or a dedicated syslog server for a single IVS.

Java Secure Application Manager (JSAM)

- JSAM session manager window will update the status when traffic is passed through JSAM. Therefore, if there is no traffic, the status will not reflect session timeout, network outage, etc. (45124)
- If the SA denies access to the destination server due to ACL checks when using JSAM, WSAM, or Terminal Services, the end-user might not receive an error message indicating that the connection has been denied. (45007)
- On Vista, NetBIOS File browsing does not work through JSAM. (44952)
- On Vista, when “Skip web-proxy registry check” is disabled and user configures proxy on browser, the warning message “A web proxy has been configured” is masked by “You do not have permissions to modify the hosts file” message. (44626)
- On Vista, we don’t support applications that require JSAM to modify the registry, etc/hosts and etc/lmhosts.sam. The following are not supported: (44195)
 - Outlook
 - Deployment where external DNS setup is not used to map hostnames to loopback addresses
 - Applications where the loopback addresses cannot be configured as the destination server
- If the WINS server is responding to name server resolution requests on a PC then NetBIOS through JSAM is not supported. (43197)
- Internet Explorer 6.0 with the latest automatic updates does not support the auto-launching of the Citrix application when clicking on a published application through the IVE. This only affects configurations where the published application is accessed through JSAM. To work around this issue,
 - Add the IVE as a trusted site or
 - Go to Tools -> Internet options -> Security -> Custom level button -> Downloads section. Enable "Automatic Prompting for file downloads". (43061)
- Internet Explorer 7.0 will not automatically launch JSAM when a user clicks on a published application on the Citrix Web Interface page. In order to tunnel Citrix traffic, the user must pre-launch JSAM before clicking on the published application. JSAM can be pre-launched in one of the following ways:
 - Select "Auto-launch Secure Application Manager" under Roles -> <role Name> -> SAM -> Options. JSAM will automatically launch when the user logs into the IVE.
 - Create a Launch JSAM resource policy for IE 7 users. You can use detailed rules functionality to create this policy only for IE 7 users. To create a detailed rule, do the following:
 1. Set the resource to "*".
 2. Under Action, select "Detailed Rules" and click on the Detailed Rules link.
 3. Click "New Rule". Under Resources, add the URL for the Citrix Web Interface login page. For example, "http://<Citrix server>/Citrix/MetaFrame/site/login.aspx".

4. Under conditions, enter `userAgent = '*MSIE 7*'`. Click "Save Changes". (43061)

- Restricted users on a Windows machine that are using a Firefox browser may have trouble launching JSAM. To workaroud this issue, install a production SSL certificate on the IVE. (43820)
- When using JSAM within SODA 2.6 (SODA build prior to 2237), the `etc/hosts` file does not get restored to its original state when JSAM is exited. The `etc/hosts` file does get restored with SODA 2.5 and with SODA 2.6 builds 2237 and greater. (37486)
- Outlook 2003 is not supported with J-SAM. To work around this issue, use W-SAM or Network Connect. (8251)
- Netscape may lock up on users who close J-SAM. To work around this problem, users can add the following line to their "java.policy" file:

```
grant { permission java.security.AllPermission; };
```
- J-SAM does not automatically launch when Embedded Applications are set to "Auto" in the Citrix NFuse Classic Administrator console. In these cases, we recommend you configure J-SAM to launch automatically after signing in. Otherwise, users must manually launch J-SAM before using Citrix NFuse.
- When using W-SAM and J-SAM, if a user has a pop-up blocker, that user may experience 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.
- The application discovery functionality within Citrix Program Neighborhood is supported once port 80 is configured under J-SAM. However, if a user attempts to use the server discovery feature, which does not work through the IVE, and then attempts to use the application discovery again, the application discovery fails. The workaround is to restart Citrix Program Neighborhood. (8665)

Mac OS Specific J-SAM Items

- When auto-launching J-SAM using Safari (versions prior to 1.2), J-SAM opens 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)
- On a Mac OS X, the first time J-SAM is launched after rebooting the machine, the launch may fail. This is due to Apple's JVM code behavior. (Apple Bug #3860749) (21746)
- When running J-SAM on a Mac OS X client, if the user clicks "No" on the SSL certificate warning, the user must quit and restart the browser in order to launch J-SAM successfully.
- If the custom company logo image uploaded to the IVE is a .bmp file then the image will not display correctly on the J-SAM window on a Mac OS X client. (25831)

Hardware

- On the SA6000, avoid hot-plugging RAID drive connect-disconnect-connect sequences that are faster than 5 minutes. Doing so will cause the system to accept the drive as healthy even if the drive has missed updates. (31583)
- RAID status lights will not work as expected when the bay is empty after upgrading. Rebooting the device will resolve the issue. (37176)
- After an upgrade, occasionally an SA6000 system could see inconsistent LED behavior where the RAID Status LED blinks in RED and the Hard Disk LED is not lit. This incorrect LED behavior is

cosmetic and does not reflect the actual state of the system. It is caused by the fact that the system didn't initialize itself properly during soft reset. A cold restart will fix this problem. (35150)

- If an SA6000 goes from a two-drive configuration to a single-drive configuration (due to drive failure and/or removal) and is rebooted, the machine halts during boot and displays a serial console message similar to the following:

```
Adaptec Embedded SATA HostRAID BIOS V3.1-1 1255
(c) 1998-2004 Adaptec, Inc. All Rights Reserved.
<<< Press <Ctrl><A> for Adaptec RAID Configuration Utility! >>>
Controller #00: HostRAID-ICH5R at PCI Bus:00, Dev:1F, Func:02
Loading Configuration...Done.
Port#00 WDC WD800JD-00LSA0 06.01D06 74.53 GB Healthy
Following SATA device(s) are not present or responding:
Port#1
```

```
WARNING !!! Configuration Change(s) detected !!!
Press <Enter> to accept the current configuration or power off
the system and check the drive connections.
```

The user should hit Enter to continue using the machine with a degraded array until a replacement drive can be obtained.

- An SA6000 should NEVER be power-cycled or rebooted while rebuilding. If an SA6000 is rebooted while rebuilding the RAID array, the rebuild operation may never complete. This can be seen from the following BIOS screen on reboot:

```
Adaptec Embedded SATA HostRAID BIOS V3.1-1 1255
(c) 1998-2004 Adaptec, Inc. All Rights Reserved.

<<< Press <Ctrl><A> for Adaptec RAID Configuration Utility! >>>

Controller #00: HostRAID-ICH5R at PCI Bus:00, Dev:1F, Func:02
Loading Configuration...Done.
Port#00 WDC WD800JD-23JNA1 06.01C06 74.53 GB Healthy
Port#01 WDC WD800JD-23JNA1 06.01C06 74.53 GB Healthy

Array #0 - RAID-1 IVE 74.47 GB Building

1 Logical Device(s) Found
```

To recover from this condition, the machine should be fully booted into the IVE. Then the drive which had been previously replaced should be removed from the unit for 2 minutes and then re-inserted. After the drive is removed and re-inserted the raid rebuild should proceed normally.

Secure Meeting

- 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)
- On the Appointment tab in the Microsoft Outlook Calendar is a checkbox 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.

- 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)
- 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)
- On the Macintosh and Linux platforms, even if the viewers are set to full screen mode, the toolbar is still visible. (19506)
- We recommend that you do not upgrade the Meeting while Secure Meetings are running on Macintosh or Linux machines. If an upgrade is performed during a Secure Meeting, Macintosh and Linux users might 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)
- 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 does not delete the meeting from the meeting server. This is due to Microsoft Outlook behavior. (21336)
- 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)
- 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.
- 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.
- Red Hat Linux 9 with Mozilla Firefox 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.
- When using Mac OS X 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.
- The Secure Meeting Chat functionality only supports users using the same language encoding (based on the Web browser settings) in a single meeting. Using a different encoding than what the person typing is using, results in mangled text. Meeting invitations are sent based on the language setting in the creator’s Web browser when meetings are created or saved.
- 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 use that hostname, instead.
- 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.

- When creating a Secure Meeting using the Mac OS Safari Web browser, the organizer may be unable to add more than 250 attendees.
- When presenting, the presenter should consider which 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 attendees' 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)
- Secure Meeting attendees do not see the presenter's shared applications if the presenter locks his or her desktop.
- Secure Meetings in progress are stopped if a cluster is created during the meeting.
- 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)
- 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)
- If the Hide Attendees option is enabled, a "Failed to change roles" message appears when granting annotation permissions to another attendee. (24417)
- In Fit To Window mode, attendees may sometimes see small blocks of mangled images in their Viewer window. (24427)
- A presenter using a Linux client is not supported over slow DSL. (24480)
- On Macintosh and Linux platforms, Fit to Window does not work well when the presenter changes the resolution while presenting. (24543)
- In a remote control session, you should not start annotation. (24902)
- A presenter using a Linux client is not supported in a WAN environment. (24985)
- In a WAN environment with Linux presenting, there are attendee viewing issues. (24986)
- 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 to the viewers. (25555)
- Part of the bottom of the presenter screen is truncated when viewed on a Linux or Mac viewer in Fit to Window mode. (26468)
- The Secure Meeting Toolbar does not work on the Linux KDE window manager if the attendee runs the Viewer in Full Screen mode. (26851)
- 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)
- 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)
- When annotating on a Mac or Linux viewer window, if the attendee closes the viewer window and reopens it again, annotation does not work. (28938)
- When the Hide Attendees option is enabled, the role information is not displayed next to the attendee name in the Chat window. (30633)
- Even after a presenter has enabled or disabled drawings for all users, when an attendee requests drawing permissions, the presenter is still prompted to accept or deny permission. (31139)

- Auto-scrolling in the viewer window on Mac or Linux can be slow at times. (31353)
- If a presenter starts sharing while the Hide Attendees option has been enabled and the presenter has ongoing private chats with other attendees, then the private chat tabs are disabled on Mac and Linux. On Windows, the private chat tabs are enabled, the presenter can click on them, and those private chat messages will be seen by other attendees. (31456)
- On Windows, auto-scrolling in the viewer window is incorrectly controlled by the auto-scroll option under the presenter's preferences. Therefore, only when the presenter enables auto-scroll will the attendees on the Windows platform see auto-scrolling in their viewer window. (31602)
- During annotation, auto-scrolling in the viewer window is not working on Mac, Linux, and Windows platforms. (31603, 31604)
- On Windows platform, the Edit menu used for chat functionality does not apply to Support Meeting. (36872)
- Support Meeting does not have chat functionality. The Chat tab under Meeting > Preferences menu should be ignored. (36919)
- Support Meeting does not support Annotation. The option "Disable Request for Annotation" under Meeting > Preferences menu should be ignored. (36920)
- Secure Meeting Outlook Plugin installation fails on WinXP SP1 for Outlook 2003 SP1. (37865)
- On Windows, the chat messages do not reappear after the user un-hides the messages. (37868)
- Secure Meeting does not launch on Sygate Virtual Desktop if the Secure Meeting client is not already installed on the real desktop. (39413)
- There is an issue with Mozilla 1.6 such that if it is configured with an authenticated proxy, Secure Meeting will not launch. (39857)
- During annotation, the attendee lost the annotations when disconnected and reconnected. (40470)
- On Linux and Mac, the Support Meeting's "Exit" option will end the meeting instead of exiting the client. (40681)
- In Hide Attendees mode, annotation may not work well for conductor and presenter on Windows. (40869)
- Assume that you have two browser instances where one is signed into SA and the other is signed into the meeting login page. After closing the meeting's browser instance, when the session on the SA browser instance has timed out, if you click on the prompt to re-login, you'll be brought to the meeting login page instead of the SA login page. (40943)
- After a failover in Active/Passive cluster, the secure meeting clients do not reconnect. (41149)
- When a Linux or Mac user is presenting and a Windows attendee is the remote controller, if the Windows attendee clicks on the Draw icon, he'll get an incorrect message "Request for control failed". The correct message should be he cannot annotate while sharing control of the presentation. (41217)
- On a Windows client, deleting an annotation may not work well. (41388)
- On some Intel iMac systems, the toolbar continuously displays and hides once the toolbar is set to auto-hide. (41469)
- On some Intel iMac systems, the presentation feature may not work well. (41470)
- On Mac platform, when the attendee draws past the presenter's screen, vertical lines appear in his Viewer window. (41530)
- On Macintosh and Linux platforms, annotated objects are not scaled properly if attendee enables

Fit to Window mode. (41992)

- If two or more attendees select the same annotated object and move it, the object will be move to an unexpected location. (41995)
- In 5.1 and older releases, the notification email conductor receives contains a URL that points to the meeting page for a non-secure gateway user. Post 5.1 release, the URL has been changed to the sign-in URL. (43346)
- Outlook plugin authentication will not work if the realm enables Host Checker policies or requires users to select role. (43439)
- When Mac or Linux is presenting and in annotation mode, attendees who joined after the annotation has started will see a gray/black Viewer window. To workaround the issue, presenter should stop and re-start annotation, and attendees may need to close and re-open the Viewer window. (42940)
- On Windows platform, if attendee gets a disconnect message immediately after joining a meeting, attendee needs to rejoin the meeting again. (46810)
- On Windows platform, when attendee exits a meeting, they may see an intermittent crash of the Secure Meeting window. (46841)
- On Windows platform, when attendee enables Fit To Window mode on his Viewer, presenter's mouse cursor will be displayed with "wavy" or "fishbowl" effect as the presenter moves his mouse. (53025)

SiteMinder

- Implemented in release 5.3, the IVE Admin can configure the SiteMinder auth server to be compatible with the 5.5 or 6.0 SiteMinder Policy Server. The "compatible with 5.5 Policy Servers mode" works with either the 5.5 or the 6.0 Policy Server. However, the "compatible with 6.0 Policy Servers mode" only works with the 6.0 Policy Server. There is no difference in the SiteMinder auth server functionality based on whichever compatibility mode the IVE Admin configures. This option only controls which version of the Netegrity SDK to use when interacting with Policy Server. The recommendation is to match the compatibility mode with the version of PolicyServer.
- The IVE, from release 4.2 onwards, is compatible with 5.x and later SiteMinder agents. Older versions of SiteMinder agents are susceptible to a cookie validation failure problem. (29840)
- When using SiteMinder as an Authentication server for the IVE, users must access the IVE using a fully-qualified domain name (for example, iva.company.com). This is required because the SiteMinder SMSESSION cookie is only sent for the domain it was configured for. If users access the IVE using an IP address, they might get an authentication failure and will be prompted to authenticate again.

Secure Virtual Workspace (SVW)

- SVW is not supported on the Vista platforms.
- Uninstallation of Juniper SSL-VPN client components will not be supported while in the Secure Virtual Workspace. The workaround is to uninstall the applications from within the Real Desktop after closing SVW. (34430)
- When downloading *.exe executables within the SVW shell, upon successful downloading, the user gets a dialog box with 3 options: "Run", "Save", and "Cancel". This dialog will appear only when using Microsoft's Internet Explorer browser. The "Run" option is NOT supported within SVW for technical reasons. The user must "Save" the file within the SVW shell (e.g. desktop), and then launch it from the desktop. (34541)

- When Host Checker remediation is configured for a Secure Virtual Workspace policy, the Try Again button on the end user remediation page will not launch Secure Virtual Workspace again. The workaround is to restart the browser and connect to the IVE again (36682).
- When SVW is configured to start before user authentication the end user will see the message "You do not have permission to login. Please contact your administrator" in the browser on the real desktop. This could be confusing as the end user can login to the IVE from within SVW. To avoid any confusion this message can be altered using the custom sign-in pages by customizing the message for error code 1025 in SSL.thtml (37021).
- While in the Secure Virtual Workspace, Microsoft Word is DISABLED as a default editor for Microsoft Outlook. The default editor is going to be Wordmail instead of Microsoft Word. (37144)
- Multiple users using the same password to encrypt their SVW workspace on the same host could gain access to the persistent data storage protected by that static password. It is recommended that strong passwords be used when securing their SVW persistent data store on multi-user systems. (37311)
- JSAM support for Microsoft Outlook/Exchange will not be supported within an SVW session because there are technical limitations in exceptionally allowing JSAM to modify the required registry modifications to the RPC binding order. (37355)
- SVW is configured using Host Checker's policy UI on the SSL-VPN Admin UI. SVW will not work in HC post-authentication mode. As part of Host Checker launch, SVW gets evaluated, and any evaluation of SVW will launch the SVW shell. (37438)
- If a sign-in URL is configured to map to two realms both of which are configured to start Secure Virtual Workspace either pre-authentication or post-authentication, the resulting end user behaviour is undefined (37891).
- End user messages in Secure Virtual Workspace will appear only in English. The Secure Virtual Workspace functionality is tested only on English Windows XP and English Windows 2000 (38167).
- End users will not be able to save files in MS Word when using Japanese Office 2000 on a Japanese Windows XP machine (39297).
- Microsoft Outlook will work in SVW only when connecting to a Microsoft Exchange server through the MAPI protocol (40877).
- When JSAM is configured to modify hosts file, it will give a registry error popup when started in SVW. The JSAM functionality will work fine but the hosts file will not get restored to its original state in the event of a browser crash or system reboot (41993).
- Secure Virtual Workspace does not work when IBM Sametime 7.5 is running in the default desktop. This is because IBM Sametime 7.5 automatically switches user back to default desktop from the virtual workspace. (42018)
- Secure Virtual Workspace does not work in an IVS environment if the IVS is not configured using a dedicated IP address (42703)
- End users will not be able to print from within SVW even if SVW is configured to permit printing (43029).
- Some applications are single instance by design, such as Acrobat Reader. Because of this limitation, these applications can't be launched in the default desktop and inside SVW simultaneously. (43695)
- Secure Virtual Workspace is not supported in Vista. In this release, SVW installation silently fails in a Vista machine. (44512)

System Administration and User Interface

System Status and Logs

- 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)
- 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 is archived and a new log file is created. The display is momentarily incorrect due to this change.
- When an Admin IVE session times 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.
- The ivelognearlyfull trap for Network Connect logs ignores the configured values of the trap threshold. It sends the traps only if the logs are 90% full.
- Editing the syslog entry in-line does not work when using Mozilla Firefox. (27689)
- If the custom Help page is blocked by an Access Control policy, then the standard error page is displayed with a link to "Return to previous page." This link does not work. (26077)
- The Dashboard graphs might 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)
- 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.
- The IVE no longer automatically enables hardware acceleration when the license is installed that enables the acceleration feature. The administrator must manually activate it on the serial console or Web interface.
- The hardware port status may not be correctly updated when the network port is not connected. (31987)
- The serial console may display "Too many open files" messages under load. These message will not cause system abnormal behaviors as they are reporting info. (41110)
- The sensor logs will be cleared even if the 'Clear log after archiving' option is not set (39525).
- If a filter is applied on the sensor logs, it will not be effective on the archiving of the sensor logs (42285)
- The maximum log size of the sensor logs cannot be set when the IVE is upgraded from 5.2 or an earlier release (42185)

End-User Interface

- Welcome messages and portal name are displayed even if the greeting is disabled. (22728)
- HTML tags in a notification message cause the collapse/expand feature to fail, along with other format problems. (22264)
- In Netscape 8.0, when clicking on an IVE bookmark that is configured to open in a new window, the page opens in a new tab within the same window. (30905)

Clustering

- Cluster upgrades from IVE software version 4.0p1 to version 5.3 do not complete successfully. An intermediate step is required for the upgrade process to succeed. The recommended process for the administrator is: first perform an upgrade from 4.0p1 to 5.0, and then perform an upgrade from 5.0 to 5.3. (35695)
- The IVE does not support a common IP address pool for NC for an Active/Active cluster. In A/A NC deployments, the recommendation to the administrator is to split up the NC IP pool into node-specific sub-pools. Further, the administrator is advised to perform static route configuration on the backend router infrastructure in a coordinated fashion, with static routes to each sub-pool pointing to the internal IP address of the hosting cluster node as the next-hop gateway. (32829)
- When the cluster is reforming, cluster operations may yield unpredictable results. (18572)
- When the node cannot join the cluster, it will disable itself. The administrator must intervene and restart the reform process. (25694)
- When setting up the device, the serial console cluster add feature is not functioning. (39755)
- VIPs may still be responding to ARP after a cluster is deleted. Restarting services will resolve the issue. (38781)
- When log synchronization is not turned on, the nodes that do not have a log archiving server configured will not archive the logs. (26182)
- After a certificate is de-associated with an interface, it must be deleted before the new certificate will be present on the interface. (42351)
- If a customer experiences frequent “Cluster Splits and Rejoins”, a new feature, added in Release 5.4, called the Cluster Synchronization Timeout, should be increased to a larger value (10 is recommended). (42613)
- Changing the IP address of a cluster node can sometimes cause the cluster to not converge. (40046)

Terminal Services

- The Terminal Services feature supports local drive mapping, but cannot support it on Windows 2000 due to a Microsoft limitation. (Windows 2000 does not allow drive mapping via RDP clients.) Until Microsoft establishes a fix, local drive mapping will work only on Win2K3.
- Citrix Java applets will not work on Mac OS X unless a production Web server certificate has been uploaded to the IVE. (25264)
- Netscape can freeze when users close Secure Terminal Access (STA). To resolve this issue, users can add the following line to their java.policy file:

```
grant { permission java.security.AllPermission; };
```
- 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.
- When Citrix Terminal Services or Windows Terminal Services is configured for full screen, any dialog boxes that are popped up by the applications, such as certificate messages, could stay behind the terminal services full screen. The only solution to this issue is for the applications to ensure that the dialog boxes stay on top. (30908)

- Creating a Citrix Terminal Services session using a custom ICA file will not work if there is already a Citrix Terminal Services session in the role that is having the same name for the Custom ICA file. Use a different file name for the ICA file to work around the problem. (41475)
- The Installer Service has problems installing the Windows Terminal Services client on Windows XP if the Windows Terminal Services session has SSO defined. (40975)
- Duplicating a Citrix Terminal Services session in a role or a Citrix Terminal Services resource profile will not work if it has a custom ICA file defined. (40803)
- Launching a Windows Terminal Services session on user login will not work if WSAM or NC are also configured to automatically launch at user login. (39581)
- Launching a Windows Terminal Services session on user login will not work if multiple Windows Terminal Services sessions are configured to auto-launch. (30693)
- When creating a Windows or Citrix terminal services session on the SA device, a greater number of color depths are listed than what the RDP or ICA client supports. Please check the client documentation for supported color depths. (41027)
- Restricted users on a Windows machine that are using a Firefox browser may have trouble launching Juniper Windows Terminal Services. To workaroud this issue, install a production SSL certificate on the IVE. (43817)
- Windows Terminal Services session does not work without SSO parameters configured if the RDP client is upgraded to version 6.0 through Microsoft update KB925876 (44388).
- Citrix Terminal Services is supported on Windows Vista only with Citrix client versions 10.0 and above. If a pre-10.0 version of the Citrix Active-x control is uploaded to the IVE in the options under Terminal Services in a role, then it should be updated with a 10.0 version of the active-x control in order to use with IVE release 5.5 (45794)
- The Citrix client version 10.0 is 4.8Mb in size. The user session might hit idle time out for those coming from slow connections while downloading this version of Citrix client. Customers are advised to use a sufficiently large timeout to avoid this problem (46104)
- The title of the Windows Terminal Services window on Windows Vista in the full screen mode will show a loopback IP address instead of the host name or IP address of the target server. This issue will be resolved in IVE release 6.0 (44674).
- From IVE 5.5 onwards, Windows Terminal Services uses mstscax.dll on Windows Vista to launch the terminal services session in both the SSO and non-SSO cases. End users should not remove this DLL from their Windows Vista machines or otherwise Windows Terminal Services will not work (42450)

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 visit the Juniper Networks Support Site: <http://www.junipernet/support>.