Release Notes (Rev. 1.1)

Juniper Networks – Junos Pulse Secure Access Service

Secure Access Service version 7.1R1 Build 17675

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

April 12, 2012

Contents

Recommended Operation

- The Debug Log troubleshooting functionality should only be enabled after consulting with Juniper Networks Support.
- SA (Secure Access Service) has an Automatic Version Monitoring feature which notifies Juniper Networks of the software version the SA appliance 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.
- More than one simultaneous session from a single client to the same SA appliance may cause unpredictable behavior and is not supported. This is primarily due to the pre-authentication mechanisms which might conflict between sessions. This caution also applies to situations where an end-user and administrator 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 SA resources as links from a non-SA Web page, a selective rewriting rule for the SA resources is required. For example, if you would like to include a link to the SA logout page such as http://<SA server>/access/auth/logout.cgi then you need to create a selective rewriting rule for http://< SA server >/*. (26472)
- If two separate Web browser instances attempt to access different versions of SA appliances, the browser may prompt the user to reboot the PC after the NeoterisSetup.cab file has been downloaded. Upon closing all browsers and logging in again, the prompt will no longer be displayed. No reboot is required.
- 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 **My Computer > Map Network Drive**, or in Windows Explorer, go to **Tools > Map Network Drive** and 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)".
- Hosting a meeting is not supported when using Microsoft NetMeeting with W-SAM. 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.

- When using WSAM on Pocket PC, roaming for SA sessions should be enabled when being used over GPRS because the IP address of the phone may change.
- When using WSAM on Pocket PC, if you have multiple roles defined, select the "Merge settings for all assigned roles" option under Administrators > Admin Realms > [Realm] > Role Mapping.
- During device upgrade, while package download is in progress, administrator must not navigate away from the web page. (536543)
- In cluster configuration, under Synchronization Settings, the protocol must be set to Unicast. A setting of Multicast does not function in all situations. Multicast setting will be deprecated in a future release. (482611)
- It is required the administrator explicitly associate the device certificate to the external and management ports after they are enabled. Without performing the explicit association through the admin UI, the device will randomly pick a certificate and use it. (511856)
- Do not delete the main cluster licensing node. Doing so will lose all cluster licenses.

New Features in this Release

- Please refer to the *What's New* document for details about new features of SA (Secure Access Service) available in this release.

Upgrading to this Release

- Please refer to the *Supported Platforms* document for important information pertaining platforms supported. Windows 98 SE and Windows NT are not supported on the 5.5 and later releases. The SA1000, SA3000 and SA5000 series platforms are not supported on the 6.1 and later releases.
- The supported upgrade paths to this release are when you upgrade from any one of the below mentioned releases. In order to ensure configuration and user data integrity after the upgrade, we strongly recommend that you follow a supported upgrade path.
  - 7.0R*x*
  - 6.5R*x*
  - 6.4R*x*
  - 6.3R*x*
  - 6.2R*x*
  - 6.1R*x*
  - **Note:** If upgrading from a release not listed here, please upgrade to one of the listed releases first, and then upgrade to 7.1 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 7.1 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

AAA

- A role mapping rule based on Username or Certificate involving the “is not” operator will now work if the values box in the admin user interface has more than one value. (516822)
- Under heavy load, the source IP of the Event log message “CRT30663” is logged as “127.0.0.1” instead of the actual client source IP. (551217, 567282)

File Browsing

- File SSO policy will work for resource paths of maximum two levels only, even though entering more than two levels is allowed. More than two levels of file resource path should not be configured in the SA Admin UI. (463227)

Terminal Services

- In case of user getting mapped to multiple roles, only one role’s settings for the user experience options of Terminal services configured at the role level, will be effective. (499990)
- For Citrix WI 5.1, the cookie value does not get saved when creating new profiles unless “Send the following data as request headers” checkbox is enabled. (532110)

VDI

- For Windows platforms, with no Java and JIS installed, and the 'Download Signed ActiveX’ option in the browser is disabled, the user is not redirected to an intermediate page to install setup client. (528976)

Integrated Web SSO (CD/Kerberos/NTLM/Basic)

- NTLMV2 authentication through SA will fail if the username contains non-ascii characters. Kerberos authentication through SA will fail if the password contains non-ascii characters. (483077)

System

- The incremental lease is not working correctly for EES licenses. The workaround is for the administrator to allocate the entire anticipated usage by a client device as the reserved capacity for the client. (529691)
- Once a license client seeks incremental leases (beyond the reserved capacity) from a license server, it will not be able to return the incremental leases even if the load on the client goes down and the client has already satisfied the minimum lease duration criteria. Administrators can force a client to return part of now unnecessary leases by changing the client’s license allocation configuration at the license server. (528877)
- With the kernel change in 6.0 and later, the reporting of the load average in an idle system is different from previous releases; the minimum value at idle will be 1 as the kernel accounts for system related processes. (385631)
- When the external port is disabled, SA must be rebooted to for the action to take place, and until rebooted, SA may continue to pass traffic on the external port. (509892)
- On the "Hits Per Second" graph in the System Status page, the Y-axis label may not appear when the number of hits per second is low (less than about 100 hits/second) (476734)

- After an A/P cluster is deleted, the device certificate association to the cluster VIPs will still be visible in the admin UI. However, the cluster VIPs will be shutdown and not accessible. (485538)
- On SA4500-FIPS or SA6500-FIPS platforms, TCP dump packet capture capability with SSL dump is not supported. (482552)
- When importing system configuration, if there is a SSL acceleration setting mismatch between the current SA settings and settings from imported configuration, the SA appliance will reboot, however there will be no prior notification regarding a required reboot on the admin UI. (421576)
- When syslog is enabled, large configuration changes done will now be reported via syslog. The message, if longer than 2048 bytes, will be truncated to 2048 bytes. (565630)

JSAM

- When Vista's UAC (User Access Control) is enabled, JSAM reports "You do not have permission to change hosts file. JSAM works as expected when UAC is disabled.(440039)
- MS Windows Vista crashes for a specific JSAM scenario (Windows Vista Enterprise, SP1 and Windows 7) If a user logs in and launches JSAM, and then closes JSAM by clicking X in JSAM window, the following warning message appears: "Are you sure you want to navigate away from this page"? If the user clicks OK, a MS Windows crash message appears. (507231)

Secure Meeting

- This following issue is fixed in this release: If no multi-user session is configured and if the user is already logged in, schedule a meeting using the Outlook plug-in logs user out of the existing user session. If multi-user session is configured and the user has as many concurrent logged in user sessions as the maximum allowed per configuration, schedule a meeting using the Outlook plug-in logs user out of one of the existing user sessions. (530044)

Network Connect

- Network Connect Credential Provider is not enabled on a non-domain client machine. (513652)

Noteworthy Changes Applicable In This Release

AAA

- A yellow information bar may appear momentarily at the top of IVE's login page and then disappear. This is a side-effect of enhanced security checks performed on the browser. The momentary flashing of the message is not a reason to be alarmed, but if the information bar persists, a message on the browser's security status also will be displayed.

Adaptive Delivery – AX and Java Installers

- For restricted users on Windows XP when launching a client component, if 'Download Signed Active-X' is disabled and 'Java' is not installed, user will be redirected to an intermediate page to install Setup client. In prior release, only users on Windows Vista or Windows 7 would be redirected to this intermediate page to download and install Setup client. (461889)

File Browsing

- For File resources, ACL check behavior has been restored to pre-6.5 state in which ACL check is done for the DFS shares initial path only. No further ACL checks are done on the chased referrals, if any. (510847)
- For file resources with a path of more than two level, "/*" is not added by default to the newly created ACL policies, to handle the scenarios where ldap attributes may be used containing a slash at the end. Manual addition of "/*" at the end of resource string is required in this case. (519215)

MSP

- This release supports importing and exporting of IVS configurations by IVS administrators. IVSes can be created by root IVS administrators by importing IVS profile configurations. However, note that an IVS must already exist on the target device for import of its configuration to succeed.

Rewriter/Web Applications

- For HTML rewriting, the maximum size of JavaScripts allowed in a page has been increased to 5MB.
- For Win Mobile, the bookmarks will be displayed in the following manner. If the bookmark contains a "/ ", "– " or a space within the first 28 characters it will be auto-wrapped but a maximum of two lines of 28 characters each will get displayed, or else a single line of maximum 28 characters will be displayed.
- Sharepoint 2010 is supported via the rewriter in this release, with some caveats. Please refer to the KB article http://kb.juniper.net/InfoCenter/index?page=content&id=KB11501 for the limitations in Sharepoint support.

Terminal Services

- For Citrix Listed Application profile, even if screen size is set to "Full Screen" in the bookmark page, if 'Desktop' application gets launched, it is launched with a resizable window but with the connection bar, due to the behavior of Citrix clients. This behavior is same as what happens when connecting directly. (564592)
- The Hob applet that is shipped with SA is shared across all IVS. Any modifications in code sign certs in root context will affect the Hob applet and the changes are reflected across all IVS. (477783)
- An admin option has been added to enable or disable the RDP launcher toolbar. Upon upgrading

from 6.5R1 to 7.x, this option has been disabled by default unless the admin has modified the Java support for the RDP launcher. To re-enable the launcher, go to System User Roles>Terminal Services>Options. (471512)

VDI

- For Vmware / Citrix client uploading, the maximum size of the package has been increased to 25MB.
- When a new SA is installed/ IVS instance created, the defaults for system-level VDI download URLs (System > Configuration > Virtual Desktops > VMware and System > Configuration > Virtual Desktops > Citrix) and role-level Terminal Service download URL (Users > User Roles > User Role > Terminal Services > Options will be set to blank. The administrator needs to set it to an appropriate URL (491211)

Known Issues and Limitations in this Release

All Secure Access Platforms

AAA

- Active Directory users effecting a password change may see failure message though the operation actually succeeds. This happens when connection to an AD server on ports 139 and 445 fails while changing password using SAMR protocol but the password change succeeds using LANMAN protocol (518336)
- On a FIPS SA device, testing connection to an LDAP server using LDAPS shows an error message saying that the server is not reachable. This message maybe a false negative. Check if user authentication is succeeding, and if it is, there is no connectivity issue (531320)
- SA does not sign artifact resolution requests (552620).
- SAML Request Signing and Encryption is not supported on FIPS boxes (552893)
- SA does not generate signed SAML Metadata.
- SAML Access Control List (ACL) Policies are not supported.
- This applies to the management of SAML auth servers via NSM.
    - In the NSM UI, the title for the attribute "inter-site-transfer-url" in SAML 1.1 is displayed incorrectly using the SAML 2.0 term "Identify Provider SSO Service URL".
    - There was supposed to be help text explaining: "If SAML version is 1.1, this field is called Source Site Inter-Site Transfer Service URL. In case of SAML 2.0 it is called Identity Provider SSO Service URL. User is redirected to this URL in destination first scenario.", but the help is not displayed.
    - This issue also impacts existing pre 7.1 devices. If a pre-7.1 SA device is managed by NSM, and a Juniper update is performed on the NSM server after the schema for 7.1 is published, the SAML 2.0 term "Identity Provider SSO Service URL" will be incorrectly displayed for the inter-site transfer service URL.
    - However, these issues are cosmetic in nature and do not affect NSM management of the SAML objects in question, either for SA 7.0 or for SA 7.1. (PR 566859)
- On MAG2600 and MAG4610 platforms a 'Chassis Auth' Server, a 'Chassis SSO' sign-in URL policy and a 'Chassis SSO' administrator realm is created by default. These configuration items should not be auto-created on these fixed chassis based platforms and this issue will be fixed in 7.1R2. These configuration items will not cause any issues or side effects (569233)

Adaptive Delivery – AX and Java Installers

- Using IE8 and JAVA, after a user signs-out from the Secure Gateway, they may see an application error with a null pointer exception when closing the browser. (394181)
- When a user clicks "No" on the "Setup Control - Warning" dialog, a JAVA script error may appear. (455887)
- If a user did not select "always" on the "Setup Control - Warning" dialog, when the user tries to change "Host checker Remediation" option under Advanced > Preferences, the "Setup Control - Warning" dialog appears again. (458370)

Rewriter/Web Applications

- An additional notification alert icon appears on the task bar in the Firefox browser when accessing OWA 2010 SP1 through the IVE rewriter. Clicking on the alert icon results in an error message being displayed : "Notifications cannot be retrieved". The alert appears because the backend server delivers realtime notifications to the client, but the IVE does not deliver these notifications to the client in real time. This specific issue does not impact overall OWA 2010 SP1 functionality via the IVE rewriter. (556302)
- The Rweb R3 VT ssh applet does not work through the IVE rewriter. However, the telnet version of the applet, and the ssh applet in previous versions of Rweb (prior to R3) work correctly through the IVE rewriter. (559517)
- OWA 2010 will not work with the framed toolbar. The workaround is to use the standard floating toolbar, or no toolbar. (560004)
- When accessing iNotes 8.5 through the IVE pass-through proxy from the Firefox 3.6 browser, tab names do not get displayed in the browser window. The workaround is to disable the Google Update plugin from the browser. (564191)
- The rewriter does not support iNotes 8.5.2 via the Firefox browser. The possible workarounds are to use iNotes in lite-mode, which is supported through the rewriter, or to use a different SA access method such as PTP, JSAM or NC. (555737)
- 2048 bit JavaSoft code signing certificates cannot be imported into the IVE's certificate store. If 2048-bit code signing is a requirement in a customer deployment, the alternatives are to use Microsoft authenticode certificates or PKCS12 keystores. (576130)
- Sharepoint 2010 is supported via the rewriter, with some caveats. Please contact Juniper JTAC for the full set of caveats.
- SMS support on OWA 2010 is not supported via the rewriter.
- IM support on OWA 2010 is not supported via the rewriter.
- For OWA 2010 SP1, if Form Post Login is configured as the OWA server properties authentication method, PTP mode access does not work (578899)
- The "client certificate for virtual ports" feature which applies to ActiveSync and other applications that are intermediated via the authorization-only proxy only works on the root system. It is not available within IVS context.
- For Win Mobile, a few of the warning display pages may not fit within the IE browser. (526284)
- The floating toolbar does not work as expected in certain PTP (pass-through proxy) scenarios. For example, the floating toolbar does not operate correctly for OWA 2007/OWA 2010 access over PTP from an IE8 or Firefox browser. It is recommended that the floating toolbar be disabled for such scenarios (499218).
- When a client type is selected for editing in the SA admin UI (System->Configuration>Client types), the admin UI page shows that all client type entries are selected(highlighted). All rows on that page get highlighted and check boxes are checked automatically. (579792)
- Changes made to user agents or client types in the SA admin UI (System->configuration->Client types page)do not get recorded in the Admin Access logs. However, the configuration changes get properly applied to the system.(579793)
- Configuration management of the new client types introduced in 7.1 for the Android and Symbian platforms is only supported via the admin UI. XML Import/Export, Push Configuration

and management via NSM are not supported for these objects. If the administrator seeks to propagate configuration across SA devices via these mechanisms, they will need to manually update the client type settings on the target device after the fact. (580188)

JSAM

- TCP connections created by Java applets using hostnames fail to match Java ACL resource policies with matching hostname resources. To work around this problem, please use IP based resource in your Java ACL resource policies, or enable the "IP based matching for Hostname based policy resources" option on the Resource Policies > Web > Options page. (461542)

Integrated Web SSO (CD/Kerberos/NTLM/Basic)

- If there are two separate CD accounts configured for the same Kerberos realm with different service lists that apply to the same SA user role, a user logging into the SA appliance will be able to access only one of the service lists but not the other. (416372)
- Cross-realm Kerberos SSO is not supported in this release.(450001)
- Cross-realm Kerberos Constrained Delegation is not supported in this release.(422736)
- If NTLM entry is defined under Resource Policies > Web > General with Variable credential type with domain using <REALM> and there is no policy for this resource (using the SSO under the General tab), user login to an AD realm which is different from the server realm, the SSO failed with NTLM intermediation page with the server domain. Hardcoded realm name works.(460386)
- For Kerberos SSO to work from the IVE to a backend proxy server, the proxy server's hostname (and not its IP address) must be configured on the IVE. (463414)
- Discrepancy between NSM UI and IVE admin UI : On the NSM UI, if the admin performs the following steps:
  - Edit configuration, Go to Users->Resource Policies->Web->General->Kerberos->Kerberos Intermediation and enable 'Fallback to NTLM V2' option.
  - Go to Users->Resource Policies->Web->Basic Auth/NTLM SSO.
  - Create a new policy with Authentication type as Kerberos.
  - Then:

    'Default' value is not present for the Label option.

    However, a similar workflow when performed on the IVE admin UI results in the 'Default' value being present in the dropdown. To work around this issue, the NSM administrator needs to manually enter the value for the Label field. (464103)
- The Kerberos debug tools do not support special characters in the username or password. (482003)
- If a Kerberos SSO policy is set up with System or Variable Credential Type and an end-user logs in to the IVE by authenticating to an AD server, the user access displays the credential type of that user as "Fixed Credential" instead of the System or Variable Credential. (PR 542282)
- When a user accesses a backend server via the IVE rewriter using Basic Auth without an SSO policy, the user access log displays the realm incorrectly as ": !PRIMARY!" instead of the correct realm. This is a cosmetic issue and does not impact backend access.(575364)

User Access

- If a user logs in to the SA appliance from two different client machines, they will see a warning page in the second machine indicating that the session is active along with an option to continue. If the user chooses to continue, the session on the first machine is terminated. However, if the user logs in again to the first machine, they will simply see a login screen with no warning message. (447903)

JSAM

- When Citrix is enabled as an application for JSAM, a null pointer exception is seen on the Java console by the end user during launch of JSAM. The exception does not prevent Citrix from working through JSAM. (423257)
- If JSAM client side logs are enabled on SA, Java exceptions are thrown in the Java console when a telnet session is launched. (419917)

Terminal Services

- For CTS sessions, ”Allow clipboard sharing option” is not supported. Even if this flag is enabled/disabled in the role options, it will not have any effect. (458619)
- When using WTS or VDI with RDP clients, for a single RDP session, two tabs are shown in the windows taskbar due to a Microsoft RDP client issue. (434705)
- When Citrix 5.0/5.1/5.2 Web Interface profile is created using NSM, caching auto-policy does not get created and has to be added manually. (537016)
- When launching the HOB applet, errors are noted in the user access log regarding missing files. This is due to Secure Access Service stripping off the help files from HOB applet. These errors can be ignored. (748875)

System

- In release 7.1R1, four time zones were added: GMT Casablanca, GMT Coordinated Universal Time, GMT Monrovia/Reykjavik and GMT+5:30 Kolkata. XML export and import of configuration that use any of these time zones is not supported. Workaround is to use binary export and import. (575918)
- When a CSR is generated on an SA4500 or SA6500 appliance, there is a possibility of a webserver core being seen, but it is harmless, and it can be ignored. (505834)
- In MAG-series appliances and service modules, during initial system bring up, or during service personality selection via the console: Unless the user is connected via a serial console to the device, the user may miss seeing the following prompt:

  ```
  Please select a factory-reset personality:
  [1] Junos Pulse Secure Access Service 7.1 R1:daily (Build 17454)
  [2] Junos Pulse Access Control Service 4.1 R1:daily (Build 16918)
  Choice:
  ```

  and will only see the text

  ```
  Choice:
  ```

  when pressing carriage return. (577679)
- On MAG-SM360 service module, in the user interface under Maintenance and then System, the hard disk locations are reported opposite of actual placement in the chassis. Care should be taken when identifying the disk that has failed and requires removal. A failed disk in a RAID volume is properly identified by a red LED next to the failed drive in the rear of the chassis. Further

information is available on this KB: http://kb.juniper.net/KB20117. This issue will be resolved in 7.1R2. (585496)

XML Import/Export

- It is expected that XML Import of a large configuration will increase CPU utilization. It is recommended that such operations be performed during maintenance windows. (56761)
- On doing XML import of SAML metadata, it becomes non-expiring metadata (PR 574537)
- Import of a local auth server with the options "Password stored as clear text" AND "New passwords must be different from previous password" set will not be successful. (562243)

Host Checker

- HC process checks with MD5 checksum fails on win7 and vista if user does not have SeDebugPrivilege (552502).

IF-MAP

- When enabling IF-MAP client on a SA device, existing sessions matching the configured session export policy will not be exported to the IF-MAP Server. All sessions created after IF-MAP client is enabled will be exported per the configured export policy. (427843)
- When configuring an IF-MAP client and IF-MAP server to use certificate authentication, a device certificate signed by a Certificate Authority (CA) is required to be installed on the IF-MAP client. Please note that the default self-signed device certificate created at installation time cannot be used for this purpose. (413383)
- Enabling the IF-MAP client feature on an IC or SA device, may cause memory and device resources to be consumed if there are issues establishing a connection to the IF-MAP Server. Be sure to disable the IF-MAP functionality when not in use and ensure connectivity problems are resolved when IF-MAP is enabled. (430487)

NSM Integration Issues

NSM usage notes:

This section describes some differences in user experience between the NSM UI and the SA administrative user interface.

- In the NSM UI, the group selector panels titled “Members/Non-Members” map to the panels titled “Available/Selected” or “Available List/Selected List” in the SA or Infranet Controller admin UI. (55674)
- Identifier names (names of key fields) in the SA and Infranet Controller configuration, such as the names or realms, roles, sign-in URLS, sign-in pages and so forth, cannot be changed through the NSM UI. This is correct NSM behavior. However, identifier names can be changed through the SSL VPN SA and Infranet Controller Web UI. (57104)
- Selection of multiple objects is not available through the NSM UI, even though this capability is available on the SA and Infranet Controller admin UI in multiple places. (57190)
- The SA and Infranet Controller admin UI allows duplication of objects such as roles or resource profiles. This capability does not exist in the NSM UI. (55527)

NSM Support Issues:

Please refer to the NSM release notes for 2009.1r1, 2010.1, 2010.2 and later releases.

Secure Virtual Workspace:

- If session start and end scripts are configured for NC client, the scripts can't be run when NC is launched inside SVW. (549154)

Resource Policies:

- If an SA 7.0R1 device is added to NSM 2009.1r1 or 2010.1, after first import, they will see a configuration validation error at Resource policies > General > Kerberos Intermediation. The workaround is to create a dummy realm under Kerberos realm definition and attach it to Kerberos intermediation, but this workaround can only be applied if Kerberos SSO is not employed in the customer's deployment. (485829)

Clustering:

- If a software upgrade operation is performed on one of the nodes of an Active/Passive cluster from NSM, the upgrade completes successfully, but assertions are seen in the event logs in the second node. The assertions occur in the DMI agent software executing on the second node prior to the completion of the upgrade operation, and are not seen when the SA appliance restarts with the new (upgraded) software image. (465766)

SA 2000 through SA 6500 Items

All Client Applications

Network Connect

- The node-specific NC connection profile will be visible and configurable on both device object and template but will not take effect when standalone device object is pushed to the device. (384263)
- The compression and encryption options in the NC connection profile only apply to ESP mode. These values are ignored when oNCP/NCP is selected. In oNCP/NCP mode, compression is controlled by the global IVE "Enable GNIP compression" option on the system options page. (440012)
- SA doesn't support IKEv2 client that is configured to use multi authentication. (548849)
- In order to successfully connect a Windows 7 IKEv2 client to SA that uses a Windows 2008 AD R1 server, the following configuration is required: (549267)
  - Disable "Domain controller is a Windows 2008 server" on the Active Directory/Windows NT auth server configuration page on SA admin UI.
  - Configure the 2008 AD server to allow MSCHAPv2 auth protocol
    - Log on to a Windows server 2008 domain controller
    - Click start, click run, type gpmc.msc, click OK

        - In the Group Policy Management console, expand Forest: DomainName, expand DomainName, expand Domain Controllers Policy, and then click Edit.
        - In the Group Policy Management Editor console, expand Computer Configuration, expand Policies, expand Administrative Templates, expand System, click Net Logon, and then double-click Allow cryptography algorithms compatible with Windows NT 4.0
        - In the Properties dialog box, click the Enabled option, and then click OK.
    - Windows 2008 AD R2 server is not supported.
- When DPE is enabled, and NC access changes triggered by and HC compliance change causes the NC tunnel to switch from ESP transport mode to SSL transport mode. (542767)
- If split tunneling is disabled and roaming session enabled and if the route changes during an NC session then the NC client might exit silently. (547166)

MAC Client

-
- Standalone MAC launcher displays blank page when connect to a role which NC is not enabled. (532152)
- When NC is upgraded, NC system tray icon may not show properly. (560157)

Windows Client

-
- Using Network Connect Credential Provider, it is possible for someone to login to Windows using a different Windows login user from IVE login name as long as the Windows login occurs within 5 minutes after NC tunnel is established. Mix-matched login is also allowed, ie. Someone can login to IVE using smart card while login to Windows using user name and password. (442685)
- On a Windows 2003 server with AD installed, Network Connect adapter unable to release IP address when NC is disconnected. (443501)

Windows Secure Application Manager

- CIFS over WSAM is not supported if Trend Micro TDI driver is installed on the endpoint (528025)
- Certificate based authentication may fail from a Windows mobile device if expired and valid certificates with the same CN name are present on the device (516387)
- If Pulse 2.0 is installed on the mobile device, browser based login from a Windows Mobile device into a pre 7.1 SA and WSAM/Pulse 1.0 launch is not supported. (569919)

MSP (IVS)

- Sensor logs are not supported in IVS instances (539037)

Secure Meeting

- Launching Secure Meeting inside Symantec SODA or Juniper Secure Virtual Workspace is not supported. (462294/462329)

- Through NSM, if user selects “Sequential room number with prefix” option, and leaving a blank value, an error is thrown “Meeting room number prefix cannot by empty”. In spite of this error, if the configuration is pushed to the SA through update device, then the following results may happen depends on the configuration of the IVE: (384371)
  - In the Admin UI, if the “Meeting Name” is set to “User”, then update device will fail with the error “Please specify a Room for the Meeting Name”. This is the expected behaviour, as described in the bug description.
  - In the Admin UI, if the “Meeting Name” is set to “Expression”, then the update device will succeed. But the result is wrong, as described in the comment 5. The “Meeting Name” will be set to “Sequential Room with prefix”, but the value of the prefix will be incorrect.
- With multi user session option enabled, if the same user signed into a meeting from different locations a (#) is appended to the user’s login name. However, on JAVA client, there may be two issues: 1) if the user exit the meeting at a later time, the user is not removed from the attendee’s list; 2) a (#) may be also mistakenly appended to an unrelated login name. (566606)
- When using Secure Meeting on Vista/Windows 7 (x64 and x32) and IE 8 (32-bit), a warning may be seen that the "application must be started through a browser" as the application launches successfully. (535507)
- During Secure Meeting Outlook plug-in uninstallation, user receives 'Please Start Outlook...' alert window even if Outlook plug-in is running. (581598)

Archived Known Issues and Limitations

All Secure Access Platforms

System Status and Logs

- On some administrator console pages, changing one or more parameters causes multiple log messages to appear in the SA 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 SA 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 250 Mbytes as it may cause the system to run out of disk space. (36153)
- The legend may still be displayed on the Central Manager display even though it is disabled in the display setting. (39573)
- "Saving all Logs" is 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 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)
- The default filter setting under System > Log/Monitoring > *log type* > Filters > *filter* > Make default is not supported through XML Import/Export. (57568)
- Upgrading to 6.2R1 may fail with "Unable to import data" error message if the user configuration is very large. The recommendation is to keep the number of user records within 160K. (56657)

System

- If the administrator configures virtual ports for the external interface when the external interface is disabled, NSM accepts the configuration without any validation errors. However, when the configuration is pushed to the device, device-side validation fails and the device throws an error, resulting in a failed config update from NSM. (58625)
- When configuring IP address for virtual ports, no validation check is performed on the NSM side. When the configuration is updated to the SA device, an error will be generated if the IP address is invalid. (58627)
- In NSM, administrators are allowed to edit virtual ports settings from the Passive node, provided the Cluster license is installed on that node. (59215)
- The ARP cache entries cannot be deleted through the serial console. (59834)
- Through XML Import/Export or NSM, an invalid MAC address configured in an ARP cache entry is accepted. However, during runtime, this ARP entry is be used. (59608)
- In NSM, when configuring cluster nodes in a template, the Add and Delete buttons for VLAN and virtual ports are disabled. This is due to the missing of license info in a template. (59290)
- License upgrade may not work if the original licenses are installed in 3.x releases. (46110)
- When Custom Cipher Selection is used, the selected ciphers are enforced to the SSL connections from clients. SA will always present "High" ciphers to backend servers when making SSL connections. (47718)
- The "RC4-64-MD5" cipher is no longer supported in "LOW" setting. (48967)
- The current SSL-VPN configuration import functionality does not track any platform specific functionality like SSL Acceleration cards etc. Therefore, if an administrator were to import the configuration from an SA appliance (SA3000) into an SA6000, SSL crypto acceleration would be disabled as the SA3000 does not have the crypto functionality (38433)
- The option "Enable cluster network troubleshooting server" under Maintenance > Troubleshooting > Monitoring > Cluster in the admin UI is not exposed on the NSM. (412021)
- The User Record Synchronization feature will not start automatically after importing a system

configuration that has this feature enabled. The workaround is to disable User Record Synchronization and then enable User Record Synchronization from the user interface after the configuration import. (460913)

Maintenance

- The System Snapshot options, under Maintenance > Troubleshooting > System Snapshot, may not be pushed correctly to target device through Push Config. (57576)

Push Config

- Push Config does not currently support deletion of objects. Through Push Config, the administrator can only change settings for existing objects, or create new objects on the target system. (57332)
- On a source and target SA device, configure the same web ACLs or push them individually from source to target through the Selective Push operation. Then, if the order of the ACLs is changed on the source SA and a second Selective Push operation is performed from the source, the resulting order of the ACLs on the target will differ from that on the source. To work around this issue, the ACLs need to be manually re-ordered on the target following the second Selective Push operation. (57162)
- The following settings are excluded from the Selective Push Config operation: internal port, external port, management port (for SA 6000, SA 6000-SP and SA 6500) and VLAN ports. (54323)
- If Security > Lockout options "rate" and "attempts" are configured to be "4294967295" on one SA device and then pushed to another SA device via Selective Push Config, the resulting value on the target SA device is "2147483647". (57548)
- Push Config (Full Push) incorrectly clears the DMI Agent settings on the target device. The workaround is for the administrator to re-enter the DMI Agent settings manually on the target after the Push operation has completed. (60373).

XML Import/Export

- A combination of the "insert" operation and "create" operation of the same XML element in the XML document won't work in XML import operation if "insert" operation was executed before "create" operation. (55655)

To work around this problem, there are two options:

Option 1 : Use the ″insert″ operation with all the required attributes since the ″insert″ operation will create the object if it does not exist, or

Option 2 : Separate the ″create″operation and ″insert″operations to two different XML documents, and import XML document with ″create″operations first, then import XML document with ″insert″operations.

Binary Import/Export

- When an binary configuration import is performed with the option "Import everything except network settings and licenses", apart from the network settings & licenses, several other settings are excluded from the import, such as: 'cluster configurations', 'certificates', 'defined SNMP settings' and 'syslog configurations' (56329)

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.
- The iveRebootTrap is not sent if the SA appliance 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)
- SNMP MIB walk or the entire SA MIB is expected to be CPU intensive. The recommendation is to configure the external SNMP monitoring application to bypass the tcpTable in the TCP MIB when walking the SA MIB.(44894)
- When the SNMP agent is disabled from the admin UI, an admin log is generated stating that the query status has been changed to "off". However, there is no corresponding event log stating that the operational state of the agent has been changed to "off". (47205)
- Standard traps as specified in MIB-2 such as linkUp, linkDown, etc are not supported. The administrator is advised to monitor traps specified in the SA MIB such as netExternalInterfaceUp or netExternalInterfaceDown. (41339)
- System healthcheck reporting via SNMP traps, and system parameters reported via the admin UI dashboard graphs under System > Status > Overview are not synchronized. As a result, SNMP memUtilNotify and cpuUtilNotify traps can be generated even though the dashboard graphs do not show a spike in memory or CPU utilization. (56817)

Archiving

- The admin UI will show the following checkboxes unchecked, though they are configured, when the administrator logs in with Read-Only right: Archive events log, Archive user access log, Archive admin access log, Archive NC packet log, Archive Sensors log, and Archive client-side log uploads. This is just a UI presentation issue and not affecting actual archiving functionality. (42548)

AAA

- The upload of custom sign-in pages may some times fail. This occurs rarely. The workaround is to try again, preferably with debug log enabled. (372708).

- Windows Server 2008-based authentication on networks consisting solely of Windows Server 2008 domain controllers is guaranteed work, as is authentication on networks consisting solely of legacy domain controllers. However, authentication on networks with a mix of new and legacy servers MAY work. In the latter case, administrators must choose “Domain Controller is a Windows 2008 Server” option on the SA Active Directory configuration page
- 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. (364625)
- Importing the system config does not import SSL Intermediate CA Certificates (chains). (21040)
- Web Server SSL Certificates issued by the IPSAC root are not supported by SA. 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 using HTTP Basic Auth (in SSO), if a Realm name (not an SA Realm but an HTTP Auth Realm) is encoded in Shift_JIS, and not UTF_8, SA will not properly display it. (15881)
- Accounts that are used for both administrator and end-user access to the SA appliance 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 SA session when the other logs in. One solution is to duplicate the Authentication server on the SA appliance so that administrator users log in to one Authentication server and end-users login to a duplicate server that point to the same backend system.
- "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)
- The variable NTDOMAIN[2] does not work. (375689)
- XML Import containing changes to User Roles with insufficient data will succeed leading to inconsistent configuration state (383573).
- XML Import/Export of device certificates and code-signing certificates is not supported.
- Novell eDir: Starting with this release, a password policy that allows all grace logins to be consumed by the user is not enforced. The user will always have two grace logins left. This change is made so that users are not confronted with a situation where they login only to discover that they cannot change their password.
- On upgrading from 5.X releases to this release, the name of the Siteminder Auth Server becomes uneditable (377086).
- On the SA device web admin UI, under Configuration > user realms > <REALM NAME> > Role mapping rules, there are three options: 1. Merge settings of all assigned roles, 2. User must select among the assigned roles, and 3. User must select sets of merged roles assigned by each rule. Of these options, the first one is never exported or imported via XML Export/Import. Instead, the system assumes that the first option applies (i.e. that it needs to Merge Settings for all Roles) if the second and third options are set to <false> in the imported XML document (382974).
- In a newly-created delegated admin role, the default delegation settings for user roles or realms in the General > Overview page show "Deny All". Then, if the administrator navigates to the Users > Roles or realms tabs, and clicks Save Changes without making any changes and then navigates back to the General > Overview page, the "Deny All" is replaced by "Custom Settings"

(383960)

- Administrator is required to manually configure the OCSP options and OCSP responders should it be necessary, for the certificate to sign the OCSP request and the certificate to validate the OCSP response, after the intermediate CA is imported and the OCSP responder is created for that CA (405805)

Password Management

- 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. (347422)

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

- 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 "Use SSL 3.0" option in the browser as well. (42901)
- Client certificate authentication will fail when the client machine has Windows 2003 SP1 installed. The solution is to install the Microsoft hotfix KB931494.
- SA does not perform revocation checking on Root CA certificates. If a user tries to log in to the SA using a valid certificate issued by a revoked Root CA, the SA allows the user to sign in. (28892)
- 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

- Some keys under HKEY_LOCAL_MACHINE\SOFTWARE are shared by both 32-bit and 64-bit applications on 64-bit Windows. These shared 64-bit registry keys cannot be checked using Host Checker (421235)
- Host Checker remains at the "Loading Components..." page when a user clicks Cancel from the proxy credential dialog box. (503726)
- Occasionally the Firefox browser may go into an indefinite "try again" loop if manual intervention is needed to correct a detected anomaly, such as deleting a file. If this occurs, terminate the browser session and restart again.
- Cache Cleaner policy is not supported on Windows Mobile Devices. Any realm and role restrictions that require Cache Cleaner will fail.
- Host Checker Connection Control is not supported on the Vista Platform (44515).
- When using Host Checker functionality on Linux OS platform, "firefox" needs to be available in the system PATH in order for remediation instructions to be displayed (47414)

- Auto remediation for Microsoft Windows Firewall on Vista fails if UAC is ON. (51824)
- On Windows Mobile, if a user selects “do not show remediation for this session” option on the remediation page then there is no way to undo it for the session as “Advanced preferences” page is not available on Win Mobile. (56003)
- On Linux/Unix MD5 check for Process works only if process is launched using absolute path. (52885)
- Shavlik patch rule admin UI: Sometimes the browser hangs if you add or remove a lot of “specific products”. The browser operates normally some time after the java script completes processing.
- During XML import the credentials used to download the files from staging server for “Virus signature version monitoring” and “Patch Management Info monitoring” under Endpoint Security are not verified. (53497)
- Host Checker options "Create Host Checker Connection Control" and "Enable: Advanced Endpoint Defense" are not exported during XML export. They are policies exposed as options as in the UI. To achieve equivalent export the policies which are created by enabling these options in the admin UI (57573)
- On the realm restrictions page, during XML import/export, for all or some policies only the "Require and Enforce" option should not be enabled. The "Evaluate Policies" option should also be enabled for correct Host Checker behavior. (57993)
- XML import fails when a Host Checker policy has custom expression defined.
- If you have a NetBIOS rule with a required option and a MAC address rule with deny option configured under one policy and both rules fails, only the NetBIOS reason strings are displayed (407661)
- When configuring Host Checker registry check rule types via NSM or XML Import, the input type validation is not completed for DWORD and binary registry values. (384845)
- Disabling Auto completion of web addresses is not working on Internet Explorer 8(385861).
- If a large number of patches are missing on the endpoint in some cases remediation message to the end user states "Remediation data truncated" (446977)
- EES is not supported with NC CLI launcher, WSAM CLI launcher and NC-GINA login mode (459274,459672)
- Symantec SODA doesn’t work with Java on XP (451599)
- In Private browsing in IE8 does not allow creation of persistent cookies and hence host checker is not supported with it.
- Trial package of 25 AED users has now been replaced by the trial pack of 2 EES users.

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 SA 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 SA 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-SA issue at:

  http://support.microsoft.com/?kbid=816868. (14496)

- The timestamp function of the SA may not be in the same format as what is expected when working with the Japanese user interface. The formatting for SA 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 occurs, 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 SA, 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 administrator should enter Registry Settings rule settings in English. (25097)
- 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, when installing the Setup Client application or any other Juniper client application, UAC prompts and Setup dialogs may 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)
- If ActiveX control was installed and a user cancels a UAC prompt, Java delivery is invoked and redirects user to setup client download page. (48351)
- Some UAC prompt may not come in foreground during the SA clients' installation. (44753)
- When Juniper Installer Service is installed on a Vista client machine, Juniper setup ActiveX control is installed, however, when a restricted user attempts to download an SA client for the first time, a "Run Prompt" is shown. (47877)

- When Vodafone Mobile Connect application version 9.1.0.4345 is installed on a Vista machine, it modifies the current user's APPDATA directory from "c:\Users\<user>\AppData\Roaming" to "C:\Documents and Settings\ReleaseEngineer.MACROVISION\Application Data". This is a problem with Vodafone Mobile Connect application. It should not modify user's APPDATA directory. This error behavior of Vodafone Mobile Connect application causes Juniper setup client fails to install correctly. If you see issues with Juniper setup client installation, please check if you have Vodafone Mobile Connect application installed. (49755)

Existing Windows XP/Windows 2K platforms

- Users may see the following warning message when signing in using the Firefox browser:

  > A script from "Juniper Networks, Inc." is requesting enhanced abilities that are UNSAFE and could be used to compromise your machine or data.

  Firefox will not execute JavaScript that is signed by a certificate whose CA is not already trusted by Firefox. Therefore, this is a safe script. To avoid seeing this message every time the user signs in, the user should check the box "Remember this decision".

  The purpose of the script is to allow components such as W-SAM, Network Connect, and Secure Meeting, to be launched from Firefox. (23824)

- 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 reverts 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)
- 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 running under Windows Vista, the Network Connect standalone launcher causes the Java installer to load, successfully, in spite of the fact that the ActiveX installer is enabled (56157)
- Java delivery fails in 64-bit XP with a "Failed to download the application" error (57681)

All Client Applications

Windows Vista additions

- On Windows Vista, *ONLY* Version 5.5 and later Juniper client applications are supported. Windows Vista will display 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 the Juniper client package "installerservicesetup.exe" on a Windows Vista platform, the user will incorrectly see a Microsoft UAC prompt as mentioned above. (46180)
- All UAC prompts that display "known incompatibility" warnings incorrectly display application name to be: Juniper Citrix Services Client.

Network Connect

- 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)

- When using RedHat DHCP server, the IP address assigned to a Network Connect user is not released when the user sign out from the Secure Gateway. (26994)
- 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)
- If Network Connect has been launched from a computer that has an older JVM, the browser hangs. (38269)
- Standalone Network Connect login doesn't support client certificate on a USB smart card. (41272)
- When AES 256 is specified to be the only allowed encryption algorithm on the SA admin console, only Network Connect on Vista supports this configuration. This is not supported by Network Connect running on Windows 2000 and Windows XP. (46060)
- NCP Idle Connection Timeout should be configured to be greater than ESP key lifetime. Otherwise, Network Connect may experience random session disconnect. (46723)
- If NC ACL is created as *.*:*, Network Connect client fails to connect. (56476)
- Network Connect client send/receive byte count wrap back to zero after it reaches 4GB. This is same for Windows client, MAC client and Linux client. (56829)
- When configuring Network Connect bandwidth of roles, value is validate to ensure that total configured bandwidth of all roles do not exceed the bandwidth configured for the SA appliance. However, the administrator may go back and lower the SA total Network Connect bandwidth to be less than total of bandwidth configured for all roles. (56413)
- Network Connect access policies applied to a user are not captured in the Policy Tracing logs. (56169)
- SA does not send GARP for an assigned Network Connect client IP if the IP address is not in the same subnet as the SA appliance's internal port. (54054)
- When using Network Connect and the user signs out from the web page, the error message "Failure to download the Application" appears when attempting to reconnect via Network Connect. Users that sign out via the Network Connect menu are not affected (57381).
- After a Network Connect Bandwidth Management policy is created, if the Maximum Network Connect Bandwidth of the SA was modified to be smaller than the Maximum Bandwidth configured in the policy, the value saved in the policy is not changed. However, the actual maximum bandwidth of the policy will be limited to the Maximum Network Connect Bandwidth of the SA. (58052)
- If an NC user signs out through NC within a very short duration (less than 5 minutes), Radius accounting byte count shows 0. (459924)
- If a server certificate is changed on the Secure Access Gateway, all current connected Network Connect client will disconnect. (442395)
- When an IKEv2 client connects to the SA, if the IKEv2 client gets a different local IP address and then reestablishes the IKEv2 connection, a new connection is added to the SA because the SA doesn't have means to understand both of these two connections are from the same IKEv2 client. (487926)
- If a client machine supports VIP and separate IKEv2 requests were sent from this client machine to an SA with different a VIP, the SA treats each IKEv2 request as from different client. Thus there may be multiple IKEv2 connections established from this client machine to SA. (489438)

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)
- 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)
- When clicking Sign Out from a browser user may see a message “session terminated due to duration restrictions”. (47829)
- Client side proxy is not supported MAC OS X 10.2 (47885, 47960)
- Authenticated proxy is not supported on MAC OS earlier than 10.3.9 (49009)
- Microsoft Live communication doesn’t work over Network Connect tunnel. (51928)
- Because the Macintosh Network Connect client checks log file size every second to decide if log file roll over is required, the Network Connect log may go above 10MB before the log is rolled over. (59507)
- On MAC, MS Messenger needs to use TLS when connecting through Network Connect. (385479, 449911)
- With Safari 4.0, if authenticated proxy is configured, NC unable to connect to the Secure Gateway. This is a bug in Safari. We’ve opened a case with Apple. (459653)

Linux Client

- Users should not remove the /etc/resolv.conf file while Network Connect is running as it causes 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 SA to be unreachable. (34481, 33938)
- Shortcut keys for localized menu items are not correct. (35672)
- Sometimes a Network Connect tunnel fails to setup when launched from a command line. (38735)
- Auto-uninstall on sign-out is not working. (41010)
- Network Connect client doesn’t have reconnect functionality in Linux. (47211)
- To install Network Connect on Ubuntu using the standalone installation package, the user must install RPM on the Ubuntu machine using “alien” first. (55679)
- Linux command line launcher ncsvc provides a –k option, when this is option is used, Network Connect client is killed, but the user is not signed out from SA. This is by design. (497520)

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 SA homepage. (22200)
- 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)
- When an existing Network Connect session is established, adding a PCMCIA-enabled Wireless card to a laptop will cause the Network Connect to reconnect. (27522)
- While still installing the Network Connect client, if a user tries to launch Network Connect (for example, from a previously installed version), Network Connect displays an error message "Error opening file for writing". (28143)
- In certain situations, users may get a "Cannot connect to IVE" error 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)
- When ActiveX is Disabled and the Sun JRE 1.4.1 or higher is enabled, signing out of the SA 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 or 6.0 is installed on the same PC. (33123, 46903)
- 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)
- Local proxy exception list is not supported when NC is configured with split tunneling disabled option. (45439)
- 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 SA. 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 and later. (36137, 35292)
- If you install the Odyssey client when a Network Connect client is running, the Network Connect client is disconnected. (40159)
- The Network Connect client doesn't support the proxy auto detection configuration. (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)
- On Vista, the Virtual Adapter of Network Connect shows the default gateway as 0.0.0.0. This is because of a Microsoft issue: http://support.microsoft.com/?id=935269 "The IP address of the

default gateway for a dial-up connection in Windows Vista is 0.0.0.0 ". (45131)

- The New Secure Gateway Window menu button is not supported on Vista. (45157, 47978)
- In Vista, the Network Connect virtual adapter doesn't show user friendly name. (46345)
- Because the Network Connect 64-bit driver is not signed by Microsoft, when Network Connect is installed on a 64-bit Vista machine, users will see a pop up message requesting permission to install the Juniper signed Network Connect driver. (46654)
- Because the Network Connect driver dsNcAdpt.sys is signed by Microsoft release and there has been no changes since release 5.5, until Network Connect driver is signed by Microsoft again on 32-bit machines, dsNcAdpt.sys always shows 5.5 as its file version. (47034)
- "Copy to Log" button on Performance tab doesn't show a copy successful confirmation message. (47959)
- If a client machine is shutdown when Network Connect is connected, the client side proxy setting may not be restored properly. (48328)
- If Cisco VPN Client 4.8 is installed on the same client machine, accessing shared folder when Network Connect is running, user may see a blue screen. (48590)
- Network Connect doesn't support Firefox 2.0 on 64-bit Windows 2003. (48598)
- On Firefix 1.0, if client side auth proxy is configured, the security alert displays in the same Firefox window so user has to click on back button to get back to the home page. (48170)
- In 64-bit windows 2003, if you launch Network Connect using nclauncher Sign Out from browser may show an error message saying that the Network Connect session has timed out. (48602)
- Network Connect is a 32-bit application that has supported to be run in a 64-bit machine. Network Connect client is not a true 64-bit application. (48687)
- Auto-Uninstall of Network Connect client when Network Connect is used by a restricted user is not supported on Windows XP. (48978)
- Enabling Microsoft TCP Chimney causes performance degradation when accessing Onyx server through Network Connect. (49421)
- When Juniper Installer Service is running, a standard user still can not install Network Connect on a 64-bit Vista because the user is not able to see the Network Connect driver installation pop-up message displayed by Vista. See release notes for bug 46654 for reference. (50097)
- Because Nclauncher and NC standalone application are based on Internet Explorer, Nclauncher and NC standalone application are not aware of proxy that is configured in Firefox. (50205)
- Occasionally, after Network Connect client is installed using the standalone Network Connect package, dsNcAdpt.inf file is left on the install directory. (56149)
- On Vista, if the Windows network address is changed or if the network adapter is disabled then enabled after Network Connect client launched once, the Network Connect client can't be launched anymore. This problem doesn't occur on Vista SP1. (56628)
- Due to a Windows issue, user will get Network Connect session timeout error when Network Connect is connected to SA through proxy with enabled "bypass proxy server for local address." Refer to http://support.microsoft.com/kb/262981 for details. (57065)
- On a Vista 64-bit machine, nclauncher.exe may fail to launch Network Connect. (57435)
- Network Connect clients may fail to connect if Adobe bonjour software is installed and running. (50808)
- If DisableDHCPMediaSense is disabled, Network Connect displays an nc.windows.app.23712

error “The Network Connect session terminated. Do you want to reconnect?” Enable DisableDHCPMediaSense resolves this problem. (54001)

- After launching Network Connect from IE7, if the user signs out from the browser, and then signs in to the SA again and attempts to download an SA client from the same IE7 browser, the user will receive a “Failed to download the application” message. (57381)
- In Advanced View, Logs tab, when View All Logs are selected in the drop down box, the Log Content viewer window is empty. When a specific log such as dsNetworkConnect is selected, Log Content viewer will show the proper log entries. (59792)
- When a Network Connect client is not connected and you click Start Diagnostics on the Diagnostics tab, the Network Connect Tunnel shows “Established” even when Network Connect is not connected. (59634)
- With “split tunneling disabled”, Network Connect disconnects and reconnects when DHCP renew happens on the physical adapter. (428690)
- It has been observed that ESET NOD32 mistakenly deletes dsNetworkConnect.exe when NC was initially installed. This causes NC fail to connect to the Secure Gateway. (446259)
- Nclauncher may fail to establish NC tunnel successfully if NC upgrade is required, especially if the connection is through a slow link. (433954)
- On Windows 7, if the Network Connect adapter is the default by Windows in public profile, and if the firewall is configured to be off in public profile, then Windows 7 firewall is set to off on the Network Connect adapter. Please note that Windows 7 firewall is on for all profiles by default. This issue doesn’t occur on Vista because there is no Private firewall and Public firewall segregation. (502405)

Windows Interactive User Logon

- 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 log in to the SA using NC GINA, the user has to use the same SA IP address / hostname as used by the browser. For example, if the SA has external IP and internal IP addresses, and the client is able to reach the SA via either of the two IP addresses. If the user uses the SA appliance’s external IP address to login using browser, when using NC GINA the user must use the SA appliance’s external IP address. If the user uses the SA appliance’s internal IP address, the NC tunnel can not be established. (34534)
- GINA/HC: Advanced Endpoint Defense: Integrated Malware Protection detection works only in user context mode and in certain situations as described in the documentation. (34806)
- GINA doesn’t support certificate authentication. (36093, 34534)
- If the SA appliance 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 is 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)

- GINA logon screen doesn't support domain\user login. (56348)
- Proxy configured for the dial-up connection is not supported with Credential Provider. This issue will be fixed in 6.2R2(57763)
- Smartcard with user name and password is not supported through NC Credential Provider. (391624)
- If the client machine is configured to use DHCP, NC GINA may complain that there is no network connection when user login soon after the client machine is powered up. This is due to a race condition where the user is attempting to use NC GINA before the client machine obtained an IP address. (438615)
- If HC is configured to be used in conjunction with NC Credential Provider and the HC policy check fails, NC Credential Provider shows an incorrect error message nc.windows.gina.23816 "Secure Gateway authentication failed." (460277)
- If a 3rd party GINA is installed after NC GINA, the behavior of NC GINA is dependent on the 3rd party GINA thus undefined. (518109)

Network Connect 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 the IE 6.0 SP1 problem: http://support.microsoft.com/?kbid=329802 (38869)
- The Network Connect launcher doesn't support Cache Cleaner in this release. (38876)
- nclauncher –signout doesn't support auto-uninstall Network Connect client option. (55859)
- nclauncher –exit doesn't restore proxy settings. (53009)
- Nclauncher.exe – stop doesn't restore proxy settings. (59915)

Installer Service

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

Rewriter/Web Applications

- Accessing PDF files larger than 32MB will cause high CPU utilization. (438100)
- The use of iframe in the toolbar causes interop issues with JavaScript rewriting and does not work with FireFox browser. A new option called "Use Iframe in Toolbar" was added to solve both these issues. iframe will be used only if this option is explicitly enabled. (426334)
- If an SA session times out when accessing iNotes 7.0/8.0 the browser may hang or give an error. On iNotes 8, there is an XMLHTTP request on clicking the mail after session timeout which returns a re-direction, but iNotes 8 does not honor the redirect. This causes the error. If alarms are enabled it may also help to close all fired alarms before attempting to close the browser window. (422887)
- While accessing OWA 2007 through the rewriter and saving a html file from an email has the extension of the type ",DanaInfo=10.11.11.11+attachment.ashx" and the file cannot be opened. Workarounds: Rename the saved file to a .html extension and open the file. OR create a caching policy *:*/owa/* as unchanged for OWA 2007 to get the correct filename while saving. (412231)
- For OWA 2003 Web resource profiles, if the Autopolicy-SSO option is enabled, the auto-created resource policy is incorrectly. For example, if the OWA server in the resource profile

is http:/ / 10.11.11.11/ exchange, the resource policy is incorrectly generated as http:/ / 10.11.11.11/ exchange/ *. Instead, it should be generated as http:/ / 10.11.11.11:80/ *. The administrator can manually change the resource policy to reflect the correct URL. (416918)

- Mixed authentication modes of NTLM and Basic Auth are not supported. (387708)
- If a web page is sending a POST request to an SSL-enabled webserver that does not have a valid SSL certificate and SA is configured to display a warning for invalid server certs then the POST request will not succeed. To workaround this issue, purchase a valid SSL certificate for the webserver or disabled the invalid server certificate warning for end-users. (46806)
- Microsoft Office 2007 XML documents that include references to external files are not rewritten. (Bug 41422)
- The PDF rewriter does not support PDF files that contain 2 objects for the same link. (41572, 44040)
- The PDF rewriter does not support Adobe forms, i.e. submitting a FORM from within a PDF file is not supported. (37684)
- 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 SA appliance.
    2. The Oracle application must be set to the “Forms Listener Servlet” mode.
    3. If using a self-signed certificate on SA then you must follow the steps outlined in http://www.oratransplant.nl/2005/07/11/using-self-signed-ssl-certificates-with-jinitiator/ or you must upload a production Web server certificate to the SA appliance (38806).
- SA does not work with Whole Security Confidence Online version 4.3. It works with Confidence Online version 5.0. (35634)
- Some Java applets (including Citrix Java applets) on Mac OS 10.4 running JVM 1.5 might fail through the SA rewriter if a production SSL certificate is not installed on the SA appliance. (29303)
- 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 SA, 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)
- The “Display Favorites” functionality on the SA toolbar may not work on Web sites that use iFrames or frames. (27361,24621)
- Checking in of documents in the Documentum Web application is not supported through the Java rewriter.
- Lotus iNotes in offline mode is not supported through the rewriter. (9889)
- When using Siebel 7.5 through SA, 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 selecting **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 SA, 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)
- 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 SA, 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.
- 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 SA. Users may 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 SA functions using pop-ups (for example, file uploads, online Help, or the SA 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)
- 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 > Do 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 SA toolbar does not appear in the iNotes application in Safari 1.3. (29926)
- To preserve filenames that contain non-English characters when doing a multiple file download in Windows File Browsing, go to Users > Resource Policies > Files > Options and select the appropriate encoding option. (38304)
- Sending email with attachments fails when accessing Domino version 8 through the rewriter. (57468)
- URL obfuscation does not happen when accessing Domino version 8 via the rewriter. (57537)

- Composing a new email in Domino version 8 via rewriter will be present a secure/insecure warning. (57469)
- When SSO is disabled and the IIS server is setup with Basic or NTML authentication for WebDav Virtual directory only, accessing Webdav through the rewriter results in the user unable login to the Webdav server with write access. (57083)
- When any PDF file accessed through rewriter is saved, "Danainfo" gets appended to the name of the file. (55946)
- XML import allows creating a Web Resource Profile > OWA 2007 resource profile > Form post SSO, even when user does not specify any POST parameters. (58139)
- Importing XML for Web SSO settings may result in the following error message: "Modification of this attribute is not allowed". (58256)

  This error will occur in the following scenarios:
  1. The <auth-type> attribute is not set to "basic-predefined" or "ntlm-predefined", and the <pre-defined-username>, <pre-defined-password-type>, <variable-password>, <explicit-password>, or <domain> attributes are being modified by the XML import.
  2. The <auth-type> attribute is set to "basic-predefined" or "ntlm-predefined" and <pre-defined-password-type> is set to "variable", and the <explicit-password> attribute is being modified by the XML import.
  3. The <auth-type> attribute is set to "basic-predefined" or "ntlm-predefined" and <pre-defined-password-type> is set to "explicit", and the <variable-password> attribute is being modified by XML import.
  Note: This problem and related scenarios apply to Web SSO settings in resource policies and web resource profiles.
- When accessing a file via the rewriter and trying to save it through the right click menu will append string similar to "DanaInfo=10.10.10.10+Design.doc" to the filename. This happens because the right click menu picks up the name from the URL. Saving via the download pop-up will retain the filename without appending any string. (53642)

Pass-Through Proxy Issues

- To use OWA 2007 with Pass Through Proxy, the administrator must configure a Selective Rewriting policy for resource "*:*/owa/ev.owa?*" and action set to "Don't rewrite content: Do not redirect to target web server". (46344)
- If the user is using Mozilla Firefox with Pass-Through Proxy (with the SA port configuration), SA 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 Lotus iNotes through Pass-through Proxy clicking on the logout button in Lotus iNotes will logout the user from SA. (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).

Hosted Java Applet Issues

- 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 SA admin console. (27353)

File Browsing

- When a user attempts to upload more than 500MB file, the "Internet explorer cannot display webpage" error page appears. (479288)
- The shortcut files created within shared folders on Longhorn server do not get listed. (385575,59800)
- Multiple file download is not supported on Windows Mobile devices, due to the unavailability of Zip tool by default. (47026)
- 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).
- Due to a bug in Microsoft Network discovery API NetServerEnum2 SA will not be able to extract the workgroup information if the master browse server is in a different subnet (43172).
- To preserve filenames that contain non-English characters when doing a multiple file download in Windows File Browsing, go to Users > Resource Policies > Files > Options and select the appropriate encoding option. (38304)

Integrated Web SSO (CD/Kerberos/NTLM/Basic)

- SA does not support cross realm constrained delegation. Constrained delegation will not work when a constrained delegation account and the associated services are on a different realm from the user realm. It will also not work if the both user and CD account are on the same realm but the associated services are in a different realm. (422736)
- When using web SSO, having a proxy between the SA and the backend server is not supported.
- Only Kerberos intermediation/SSO is supported for a Negotiate challenge. NTLM and Basic intermediation/SSO is not supported for Negotiate challenge.

Pass Through Proxy

- Accessing OWA 2007 through PTP gives an error while creating a new mail unless a selective rewriting policy for *:*/owa/ev.owa?* with "Don't rewrite content: Do not redirect to target web server" option enabled is added. (417953, 385883)
- Accessing One-line summary of the PRINotes 8.0.1 on IE 7 through PTP host mode gives script error.(415049)

JSAM

- If JSAM client side logs are enabled on the SA appliance, Java exceptions are thrown in the Java console when a telnet session is launched. (419917)

SA 2000 through SA 6500 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.
- 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 listed above. 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.
- 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 SA appliance two separate times—the first one resulting in a de-installation, 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 SA. (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 SA, 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)
- If the administrator doesn't enter any value in "Allowed Server Ports" field, it is interpreted as "*:*" by WSAM. (42119)
- Enabling client log for WSAM impacts throughput. (44585)
- If WSAM is configured by destination with multiple hostnames corresponding to the same physical IP address, only traffic for the first hostname would be secured. The workaround is to specify IP address in WSAM configuration. (46830)
- WSAM does not provide an option to reconnect in the message box displayed on idle timeout with the SA appliance. (47417)
- When a user signs out of SA on a Firefox or an Internet Explorer browser, if WSAM is still transferring traffic the user may see a "Session Timeout" message because the timeout message may reach WSAM before a sign out event. (45033, 438099)
- In Application mode, WSAM will forward all DNS requests to the Secure Gateway, which in turn forward all packets to internal LAN. (45792)
- Windows Secure Application Manager (WSAM) does not support NetBIOS file browsing on Vista SP1 if the file server supports NetBIOS traffic only on port 139. (56414)
- If standalone WSAM Installer is installed on Vista, then launching of WSAM using IE will not work if JRE is not installed on the PC (54513).
- When using WSAM or Terminal Services to remotely connect to the enterprise network, if you want to access UAC (Juniper Networks' Unified Access Control) protected resources, you need to create a policy in UAC to treat traffic coming from the SA appliance as an unmanaged device. (52840)
- On XP, WSAM needs Microsoft KB 951748 to be installed on the system to control the behavior of DNS cache to open and close sockets for DNS requests. (395237)
- The domain controller has to be added to the WSAM ACL list to enable password change thru WSAM
- WSAM is not supported on multiple Terminal Service/Citrix sessions running on the same Windows server (419891)
- On Vista, WSAM uninstall from user preferences> applications> wsam uninstall doesn't work if Juniper Installer Service is installed (385930)
- If Kaspersky antivirus is present on the machine, WSAM will stay in disconnected mode till we reboot the machine after installing WSAM (419868).
- WSAM/JSAM/Terminal Service users will get disconnected if any application secured with WSAM sends UDP traffic to a host denied access using an ACL in the SA resource policy (427700).
- Scriptable WSAM (Samlauncher.exe) is no longer available as a standalone exe. It is now packaged as part of WSAM package. (437185).

- If the Windows XP based client machine has other TDI driver based software like Symantec's Norton 360 or Norton Internet Security it may cause Windows Blue Screen errors (465562)
- If the Windows Vista based client machine has other TDI driver based software like Symantec's Norton 360 or Norton Internet Security it may cause the machine to freeze and will require a reboot to recover. (480529)
- If only SMB (port 445) is enabled and NetBios (port 139) is disabled on the destination file server, two users cannot simultaneously access the same file (471200)
- If Juniper Installer Service is not installed for a standard user usage on an endpoint with Kaspersky Anti Virus installed, WSAM will exit gracefully and log following message into log file : "couldn't delete RebootRequired key, Installer service is not running, exiting" (506854)
- Changing log levels thru WSAM is not persistent for a standard user .(506783)
- When accessing resources thru Internet Explorer 8 thru WSAM, if the destination policies are hostname based and more than one tabs are open on the explorer, access to WSAM protected pages will not be available if the user signs out and signs in again within 2-3 minutes. The workaround is to close all browser pages or wait more than 3 minutes before accessing the protected resource. (508061)
-

Pocket PC

- Windows SAM options under Users > User Roles > Select Role > SAM > Options are not supported on Pocket PC. (45956)
- WSAM doesn't support client auth proxy settings in PAC files thru Firefox. (47769)
- By design, SAM UI sign-in does not support role selection. (44832)
- When using WSAM on the Treo, please disable the manual proxy on the device (46081)
- On a Cingular 8125 device when using WSAM on an ActiveSync connection, samizing access to public internet sites is not working. (48524)
- WSAM does not support two-tier Windows Mobile Smartphone devices. (56737)
- WSAM does not support Windows Live Messenger on Windows Mobile devices. (53871)
- To create application specific WSAM log file for an application already launched before WSAM is installed e.g. repllog.exe, please add the application name to the WSAM debug list and reboot the device. (52924).
- If the SA admin has enabled persistent cookies, on HTC devices, once you install Pulse on Windows Mobile device successfully, reboot and login to SA, an erroneous message saying, "Pulse is not installed on your device" is displayed which has to be ignored. (512186)
- For accessing an SA appliance from a Windows Mobile 6.1.4 browser in desktop mode, the SA needs to be configured to recognize User-Agent : 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)' as client type PocketPC. (514764)
- **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 th**en tr**y 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)

- If a binary system configuration is imported with "include network settings" selected to a SA appliance with IVSs and VLANs, then existing VLANs are replaced. This may leave an IVS with no Selected VLANs in its profile. To work around this issue, the IVS root administrator 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. (366857)
- When an IVS license is added to a SA appliance that already has the VLAN license installed, the expected behavior is that all existing roles should get unbound from VLANs and access to backend resources via VLANs should fail after addition of the SA license. The actual behavior is that the admin UI presents the roles as being disassociated from their former VLANs, but user access to backend resources continues to work over VLAN interfaces. It takes an SA reboot for backend access to fail as expected. (374012)

MSP administrator advisories:

- 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 SA. The syslog server could be a central server across multiple IVS systems, or a dedicated syslog server for a single IVS.
- When a binary system configuration (system.cfg) is imported into an SA on which IVS’s have been configured, the recommended binary import option is “Import everything except network settings and licenses.” This option preserves VLAN interfaces configured on the SA appliance. The option “Import everything except IP” should be avoided since it will result in overwriting the VLAN interfaces on the SA with the VLAN interfaces in the imported file, resulting in a mismatch between the VLANs in the IVS profile settings and the newly imported VLANs in the Network settings. (366857)

Java Secure Application Manager (JSAM)

- On Vista, NetBIOS File browsing does not work through JSAM. (44952)
- For JSAM on Vista, to support applications that require registry modifications, etc/hosts and etc/lmhosts modification, a UAC prompt labeled Juniper JSAM Tool will be displayed to enter administrator credentials.

- JSAM fails to exit successfully (JSAM window does not close and hosts file is not restored) when two users use JSAM in the following manner: user A launches JSAM on a timed out session while user B logs into the login window and launches JSAM. (46033)

- The JSAM Autolaunch Policy has been enhanced so that JSAM will auto-launch if the configured URL matches a URL that is requested through the rewriter. Previously, JSAM would auto-launch only if the URL was accessed from the SA bookmarks page. The exact URL for which the JSAM is expected to launch should be entered as the resource. Including wildcards in the resource could result in the web page displaying incorrectly. (48851)

- The configuration where the JSAM autolaunch resource policy is the same as a PTP hostname is not supported. (48614)

- The restore system settings operation will not restore the hosts file successfully if you log in as a different user from the one that originally launched JSAM. (25828)

- If WINS server is being used for name server resolution 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 SA. This only affects configurations where the published application is accessed throug JSAM. To workaround this issue,
  - Add the SA as a trusted site or
  - Go to Tools > Internet options > Security > Custom level button > Downloads. 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. (43061)

  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 in to SA.
  - 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 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.

- 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 and Outlook 2007 are 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 Web Interface. To workaround this issue, configure J-SAM to launch automatically when user accesses the Citrix Web Interface login page.
- 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 SA, and then attempts to use the application discovery again, the application discovery fails. The workaround is to restart Citrix Program Neighborhood. (8665)
- When Auto launch JSAM is configured for a PTP port mode web policy JSAM goes into infinite loop on Mac OS. (57144)
- Mac JSAM fails to upload logs when the user is authenticated to the SA using Siteminder authentication with the following message: "Uploading failed: It appears that you are not logged-in". (57742)
- Auto-Launch JSAM for a PTP URL will cause infinite loop on the client. Workaround is to Auto-Launch JSAM at start of user session.(57144)
- When JSAM is launched in Firefox 2.0.0.12 on Vista, and if UAC mode is on, user would see a message “You do not have permission to change hosts files. Please talk to your system administrator.” This is expected behavior because UAC prohibits JAVA applet from changing host files. (55079)

Mac OS Specific J-SAM Items

- On Mac OS X 10.2.X, if the framed toolbar is configured then the JSAM autolaunch policy feature is not supported. (46594)
- 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 SA appliance is a .bmp file then the image will not display correctly on the J-SAM window on a Mac OS X using JVM 1.4. (25831*)*

Hardware

- On the SA6000, avoid hot-plugging RAID drive connect-disconnect-connect sequences that are faster than 5 minutes. Doing so causes the system to accept the drive as healthy even if the drive has missed updates. (31583)
- 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. 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

- We recommend that you do not upgrade the meeting while Secure Meeting is running on Macintosh or Linux machines. If an upgrade is performed during a Secure Meeting, Macintosh and Linux users may not be able to launch the client for a new meeting. This is due to Safari and Mozilla browser behavior related to caching Java applets. The user must close and restart the browser to fix the problem. (22273)
- 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. (17550)

- 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. (17445)
- 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. (17331)
- 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)
- 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)
- You should not start annotation in a remote control session. (24902)
- A presenter using a Linux client is not supported in a WAN environment. (24985)
- There are attendee viewing issues in a WAN environment with Linux presenting. (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)
- 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 the Hide Attendees option is enabled, the role information is not displayed next to the attendee name in the Chat window. (30633)
- 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 Macintosh, Linux, and Windows platforms. (31603, 31604)

- 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)
- In Hide Attendees mode, annotation may not work well for conductor and presenter on Windows. (40869)
- 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 some Intel iMac systems, the toolbar continuously displays and hides once the toolbar is set to auto-hide. (41469)
- On the Macintosh 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 the 6.0 release, the format of the notification email has been updated. In addition, if “Authentication Requirements” is not set to “Require secure gateway authentication”, conductor will receive two URLs in the notification email: conductor should sign in to SA using the “Conductor URL” and send the “Attendee URL” for attendees to join the meeting. (43346)
- During a remote control session involving non-English Windows OS, the characters typed by remote controller on presenter’s desktop will not appear correctly. The workaround is for remote controller to select the IME to be language X on the presenter desktop and to select remote controller’s own IME to English, then remote controller can type language X’s characters into presenter desktop. (44684)
- On Windows platform, there is a delay in remote control in Fit To Window mode. (44708)
- "Select All" does not work in Customize Drawing Permissions window. (45612)
- In 6.0, Secure Meeting under Resource Policies has been moved to the Configuration page. (46969)
- If the remote controller changes the screen resolution on Mac or Linux presenter desktop, the presenter gets an error message "Could not share desktop. Contact your system administrator" and the remote controller gets disconnected. (47724, 21404)
- After the presenter enables "Hide Drawing" during annotation and an attendee on Mac/Linux joins the meeting, he is able to draw even though hide drawing mode is enabled. (47891)
- On Mac with JVM 1.4 or below, users have to point their mouse over the menu item to actually see the update state of the menu item. The workaround is to use JVM 1.5.x. (47924)
- On Vista platform, if the Viewer images are mangled, you can minimize/maximize or close/reopen the Viewer window to refresh the images. (48072)
- On Windows, chat messages are duplicated if the Secure Meeting disconnects and reconnects. (48210)

- On Windows platform, the presenter's "Take Control" button is not enabled if the presenter grants remote control to an attendee via "Controller" button. To take control back, the presenter should select his name and click on "Controller" button. (48212)
- After upgrading to 6.0, using the same browser window, the administrator will see a javascript error when he clicks on the Meetings tab under Roles. The workaround is to sign in to SA again or close and open a new browser. (48777)
- 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)
- If the services are restarted on an Active/Passive cluster, the active meeting clients may have to be re-launched. (50060)
- Attendees invited through the Secure Meeting Outlook Plugin are not listed in the meeting archived file. (53408)
- After presenter on Windows machine enables "Hide Drawing" during annotation, if an attendee joins the meeting, he will see the drawings on his Viewer window even though Hide Drawing mode is enabled. (55518)
- If Symantec's Confidence Online blocks the Secure Meeting client process on the presenter's machine, then attendees will see black screen appearing on their viewers. The presenter must unblock "dsCboxUI.exe" in the "Blocked List" tab in Confidence Online Application. (57020)
- On Macintosh or Linux platforms, "Pause" sharing does not work. (57186)
- On Vista, the Secure Meeting application is run at medium integrity level. It will not be able to access other applications/processes running at higher integrity level. Therefore, remote controlling those applications/processes running at higher integrity level on a Vista machine will not work. (57667)
- Under Configuration > Secure Meeting, if "Sequential room number with prefix" has an empty room value in the XML document, when the XML document is imported back into SA device, the room value will default to "room". (58571)
- Meetings that are scheduled on the DST start day and the DST end day are placed on a row that is one hour off from the actual meeting starting time. This is only a display problem. Meetings will start on correct scheduled time. (59607)
- When Outlook plug-in is installed through Firefox, the "User ID" and "Realm" fields are empty in the "Provide server details" page. These fields should be auto populated. (59778)
- Through NSM, User is able to update Secure Meeting configuration on SA service successfully even if "SMTP Login" and "SMTP Password" are invalid. (59632)
- Secure Meeting doesn't support application sharing of Mokafive. Use sharing desktop as a workaround. (392575)
- After installing Outlook Secure Meeting plug-in, if authentication proxy is configured, user are prompted to enter proxy authentication twice when creating Secure Meeting from Microsoft Outlook. (418839)
- On a hardware video acceleration capable computer, Secure Meeting is not able to display the Video screen. The workaround is to disable hardware acceleration in the Video play. (423034)
- Meeting viewers are able to see Outlook Desktop alert notifications even if unrelated applications are shared on the Windows desktop. (423336)
- If Auth proxy is required to connect to Secure Gateway and if Firefox is used to launch Secure Meeting from https://<SecureGatewayURL>/meeting/<MeetingID>, the Secure Meeting client

can't be downloaded and installed. (426017)

- If a user is presenting from a Windows XP machine, pauses and then started Yahoo slide show in the presentation, viewers using XP and Vista clients see a green wait cursor. The slides are changing continuously. This issue may happen for Power Point presentation too. Viewers using Linux or MAC don't see this problem. (426340)
- Sometimes the cursor may continuously blink when the meeting presenter is using Windows XP. (427181)
- When remote controlling screens of a Vista presenter, if the controller moves the mouse too fast, the remote control may stop working. To recover from this, the Vista presenter has to restart the Secure Meeting client. (450256)
- On Windows 7, when a desktop is shared, the right click context menu of Internet Explorer browser is not visible to viewers. This is because the context menu is not a child of the Internet Explorer window, thus Secure Meeting presenter can't capture it. (492899)
- Secure Meeting currently doesn't support with local proxy PAC file. This includes the local proxy PAC file that is created by NC. (503744)
- On Mac, under certain usage scenarios, the viewer screen is not displayed as Fit to Window mode even if it is configured so. (493746)

Secure Virtual Workspace (SVW)

- The Secure Virtual Desktop does not support real time Anti-Virus scan. (34385, 48587)
- 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 SA 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 SA 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)
- SVW is configured using Host Checker's policy UI on the SSL-VPN admin UI. SVW does 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)
- Microsoft Outlook will work in SVW only when connecting to a Microsoft Exchange server through the MAPI protocol (40877).
- 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)
- Applications can not modify Local Machine registry keys inside SVW. Thus, all applications require modification in Local Machine during installation can't be installed inside SVW. If they are previously installed on the client machine, they can be launched inside SVW. (45899)

- When persistent data is configured for SVW, if the machine lost power or crashed (not graceful shutdown), the default desktop background is set to same as SVW desktop background. (51131).
- Attendee does not get a request for control denied message when the presenter denies the request for control. This happens when the presenter is running on Linux or Macintosh. (57161)
- In a Japanese OS, sometimes MS office 2007 can't be launched inside SVW. (56316)
- User may get an error message when viewing property of a file inside SVW. (56310)
- When Microsoft Exchange Outlook application is launched inside SVW, user may see a few error pop up messages. (56558)
- After Host Checker launches SVW, the browser page on real desktop shows "You do not have permission to login. Please contact your administrator." (37021)
- When Yahoo toolbar is installed, once SVW launches, user is switched back to real desktop. This is due to compatibility issue with Yahoo toolbar. User can manually switch back to SVW desktop. (53703)
- When the Google Toolbar is installed, and SVW is launched by a restricted user, IE in SVW launches very slowly. (53706)
- JSAM configured with Netbios file browsing does not work inside SVW. (60265)
- With persistent data is enabled, if user modifies proxy setting on the real desktop after SVW been launched once, SVW will not recognize the new proxy settings. (403398)
- If user launch Windows personal Firewall from inside SVW, the Windows personal firewall screen will be shown on the real desktop. (410805)
- While user is inside SVW, if a Windows personal Firewall alert is shown, the alert will be shown on the real desktop. (412241)
- Installing a .msi package inside SVW is not supported. (425653)
- When accessing help from the SA home browser inside SVW, JAVA script error may be shown. (466003)
- When user clicks on IE7 help inside SVW, the IE help window is shown on main desktop. (468625)
- SVW doesn't support printers that do not use Windows print spooler. (433090)
- When opening a file with Windows Photo Viewer inside SVW, the file is shown on the real desktop rather than inside SVW. (447409)
- Writing files back to SharePoint Server 2007 is not supported within SVW. (523060, 485540)
- A blue screen may occur when launching SVW on a Windows 7 with Kaspersky Internet Security 2010 running. The crash seems to be caused by Kaspersky. (510355)

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 SA appliance, 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 administrator SA session times out (due to inactivity or by reaching the hard limit), the

"sign in again" link may take the adminiswtrator to the end-user sign in page instead of the administrator sign-in page. The administrator can simply type the administrator sign-in URL (for example, /admin) to sign back into the SA admin console.

- 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 may not display properly if the SA 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. SA does not respond to 407-based authentication challenges from the Web proxy.
- SA 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 maximum log size of the sensor logs cannot be set when SA is upgraded from 5.2 or an earlier release (42185)
- The time to generate a system snapshot will increase dramatically if there are a lot of client connections and the DNS server is unreachable. (46642)
- Periodic snapshots will not be taken if the system configuration is imported without network settings from another SA. The workaround is to disable and then enable the periodic snapshot on the new SA again. (49585)

End-User Interface

- Welcome messages and portal name are displayed even if the greeting is disabled. (22728)
- If HTML tags are used in the notification message then the collapse/expand feature is not available. (22264)

Clustering

- SA does not support a common IP address pool for NC for an Active/Active cluster. In active/active Network Connect 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 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)
- Changing the IP address of a cluster node can sometimes cause the cluster to not converge. (40046)
- When upgrading A/P cluster to 6.1, the administrator may need to manually associate the device certificates to cluster internal and external VIPs in order for the device certificate to be presented to the right port. (48608)
- The admin UI will show just one IP address in virtual port configuration page, even though there

may be more than one IP address configured for each cluster node. (48643)

- An active/passive cluster loses the VIP if one of the nodes is removed from the cluster. (48857)
- Changing VLAN IP to different network could leave the VLAN virtual ports configuration in different network than the underlying VLAN. (48904)
- To migrate system and user configuration from an SA cluster C1 to a replacement cluster C2 with different type of SA machines, follow the steps listed below: (54213)

  1. Export the system user and IVS configuration from C1's primary node (PN1).

     Note down the following information
     - Cluster name – C_Name
     - cluster password - C_Password
     - Name of the node where export was done - PN_Name
     - Internal IP address of PN1 – PN_InternalIP
     - Internal network mask of PN1 - PN_InternalNetmask
     - Internal network gateway of PN1 - PN_InternalGateway
     - Names of all other nodes in the C1 cluster and their internal network IP address, network masks and gateways
  2. Shut down the machines in the existing cluster C1.
  3. Bring up one of the new machine (which should already be running a software release 6.1R1 or newer) that will be part of the cluster C2 on the same network to which PN1 was attached. Let's call this machine PN2.
  4. When prompted configure the internal network settings of PN2 to exactly match the internal network settings of PN1 as noted down in Step 2.
  5. Install the new primary licenses on PN2.
  6. Navigate to the admin UI Clustering tab and click on Create Cluster. Create the cluster C2 using the exact same cluster name and cluster password that were in use at cluster C1. This first cluster node PN2 must also be assigned the name PN_Name as noted down in Step 2.
  7. Navigate to the cluster status page and add the remaining nodes to the cluster configuration. Nodes being added must be assigned exactly the same names that existed in original cluster C1. The internal network settings of the newly added nodes must also exactly match the corresponding settings in the original cluster C. **Do not join the newly added nodes to the cluster C2 yet.**
  8. Import the data exported in step 1 into the new cluster Node PN2.
     - Import the system configuration – pick the option "Import everything (except Device Certificate(s))"
     - Import the device certificates
     - Import user accounts
     - Import any ivs settings
  9. Bring up the remaining new machines; configure the bare minimal internal network settings needed to bring up the machine – the network settings must match what has already been configured in the cluster C2 on node PN2. Do not do make any other configuration changes on these machines as they will be lost when these machines join the cluster. Do not add licenses on these machines yet.

10. Join the machines brought up in step 9 to the cluster, wait for the cluster status to stabilize.

11. Install the CL licenses on the newly joined nodes.

- Network settings that are part of the system configuration exported from a cluster can not be imported into another cluster with a different cluster configuration. To import system configuration including network settings previously exported from a cluster back into the same cluster, the administrator must ensure that the import operation is initiated at the same node from which the system configuration was exported. Note that during the import operation nodes in the cluster will be disabled and enabled internally. In general it is preferable to exclude network settings when importing system configuration in a running cluster. (55054)
- A cluster may split into two different cluster configurations when adding/joining/deleting a node in a WAN cluster under heavy load. (48743)
- An administrator will not be able to install any new license on a cluster primary node if all the licenses are deleted first. (56077)

Virtual Desktops

- For XenDesktop, if only the COM port option is enabled on bookmarks page without Printer or Drive options, it will not work as Citrix does not support it. (458914)

Terminal Services

- For Citrix plugin 12.0 onwards, a Citrix helper yellow bar is shown even if the Citrix client is installed. The user needs to allow the Citrix helper to be installed for the client-detection to work correctly. (518681)
- For the pre-packaged hob applet that is shipped with SA, clicking the Help button in the applet window does not display any help (478644)
- When using custom ICA file, a maximized window may have a size more than specified percent in the ICA file, due to the behavior of Citrix native client (505593)
- Citrix client can not be downloaded using Citrix Download Manager. Instead the user should download the package using the "click here" link. If the user has already installed the Download Manager, it should be un-installed by going to the browser add-ons list and deleting the Download Manager add-on and then downloading the client through 'click here' link. (426307)
- When using Citrix Web Interface 5.0 on Windows-XP and IE6, with Embedded Citrix client and JSAM access method, clicking on the Applications will cause a looping pop-up window. (417481)
- Citrix HDX functionality for accelerating flash content can be supported only when the site hosting the flash content is directly reachable from the end users' machine. (473758)
- In releases prior to 6.0, the "Connect local XXX resources" options defined under Roles > Terminal Services > Options had two functions: first it determined if this option was visible in an end-user bookmark; second it determined whether the local resource would be available for all users of this role. Therefore this role-level option overrode a similar option in the admin bookmark. This behavior has been changed to clarify the use of these options. In 6.0 the role level options determine if this option will be visible in an end-user bookmark. To support this new behavior, the following changes will be made during an upgrade: if a terminal services resource profile is associated with multiple roles and their individual role level settings conflict then these corresponding options in all the bookmarks defined under these roles will be disabled. Therefore it is possible that user in a pre-6.0 release had access to local resources and does not have access after the upgrade to 6.0. If the end-user behavior could vary after an upgrade then the change is logged in the admin access logs. (47028)
- If the user is mapped to two roles, one configured to use CTS to run applications on the Citrix

Web Interface (through Citrix WI web resource profile) and the other configured to use JSAM or WSAM to run applications, then SA will use the CTS client to run the applications on the Citrix Web Interface (45629)

- 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 SA. (25264)
- 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)
- The Citrix client version 10.2 and 10.0 are 7.8MB and 4.8Mb respectively in size. The user session might hit idle time out for those coming from slow connections while downloading the Citrix client. Customers are advised to use a sufficiently large timeout to avoid this problem (46104)
- Starting with SA version 5.5 and later, 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)
- Netscape may 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; };
  ```
- 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)
- When using Windows Terminal Services with ThinPrint client on Vista, you need to use ThinPrint client's Vista compatible version. (45748)
- When using Web Citrix resource profile with “launch using CTS” option, the “connect all disconnected sessions” feature may not work at times. (54816)

Telnet/SSH

- 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 using the [Tab] + [Enter] key in IE 7 in a telnet/ssh window, the main telnet/ssh window loses focus. To workaround this issue, configure IE to allow the telnet/ssh window to open without an address bar.
  - Choose Tools>Internet Options>Security.
  - Click "Custom level...".
  - Scroll down to the "Miscellaneous" section.
  - Click "Enable" under "Allow websites to open windows without address or status bars". (46143)
- Telnet/SSH windows configured with screen size 132*60 and font size 36 pixels does not work well. The stop button is missing and scrolling does not work.(49440)
- Telnet/SSH bookmarks can not have duplicate names. So if older versions have bookmarks with duplicate names created the upgrade process will modify the names to make them unique. Ex:

BookmarkA, BookmarkA would become 1-BoomarkA, 2-BookmarkA. (51949)

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 SA 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.juniper.net/support.

Supported NSM releases

NSM manageability of SA 7.1 has been qualified with NSM releases 2010.1, 2010.2, 2010.3 and 2010.4.