

Release Notes (Rev. 4)

Juniper Networks NetScreen-Secure Access

IVE Platform version 5.0 R1 Build #8555



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

31 May 2005

Contents

Admin Guide Correction	1
New Features in IVE 5.0 R1	1
Upgrading to IVE 5.0 R1	1
Known Issues/Limitations Fixed in this Release.....	3
Known Issues and Limitations	6
Authentication.....	6
Password Management.....	8
Client-Side Digital Certificates/Cert-Based Authentication/PKI.....	8
Terminal Services.....	9
SNMP	9
Rewriter/Web Applications.....	9
Central Manager	11
Host Checker and Cache Cleaner	11
Secure Meeting.....	13
Windows based Secure Application Manager (W-SAM).....	15
Java Secure Application Manager (J-SAM)	19
MacOS Java Secure Application Manager (J-SAM).....	20
Network Connect (NC).....	20
Administration.....	24
Clustering Issues.....	24
Sun JVM/Code-Signing Certificates	26
Customizable Sign-In Pages	27
FIPS.....	27
Pass-Through Proxy Issues.....	28
Internationalization Issues.....	28
File Browsing Issues	29
SiteMinder	29
XML Export	29
Miscellaneous issues:.....	30
Supported Platforms.....	34

Admin Guide Correction

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

- Push Configuration
- XML Import

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

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

New Features in IVE 5.0 R1

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

Upgrading to IVE 5.0 R1

- Please refer to the **Supported Platforms** document for important information pertaining to Microsoft Windows XP SP2 support.
- Automatic upgrades from this release from the following releases are supported in this release (including from the Legacy Authentication mode):
 - 4.2 R5 Build 8539
 - 4.2 R4 Build 8375
 - 4.2 R3 Build 8175
 - 4.2 R2 Build 8047
 - 4.2 R1 Build 7803
 - 4.2 GA Build 7631
 - 4.1.1 R2 Build 7557
 - 4.1.1 R1 Build 7387
 - 4.1.1 S1 Build 7335
 - 4.1 R3 S1 Build 7345
 - 4.1 R2 S1 Build 7373
 - 4.1 R1 S1 Build 7347
 - 4.1 S1 Build 7337
 - 4.0 P2 S1 Build 7363
 - 4.0 R1 S1 Build 7369
 - 4.0 P1 S1 Build 7365
 - 4.0 S2 Build 7367
 - 3.3.1 P2 Build 6355

- 3.3.1 P1 Build 5847
- 3.3.1 S2 Build 5811
- Note: If upgrading from a release which is not listed here, please upgrade to one of the listed releases first, and then upgrade to 5.0 R1.
- If using Beta software, please be sure to roll back to a prior production build and then upgrade to the 5.0 R1 software. (This process enables you to roll back to a production build if ever needed.)
- With the backend SSL server certificate verification feature introduced in 4.2, Administrators may see several “Added CA Cert xyz” logs in the system event log. You can safely ignore these logs as they are merely documenting which CA certs are being established in the system for use by the new feature. (21514) Additionally, sites that contain embedded objects that are linked from untrusted sites will not display if the Administrator has configured the “Warn users about Certificate problems” for the user’s role. (23379)
- If upgrading from pre-4.0, upon upgrade, the IVE retains any old 3.X licenses and continues to function as expected. In order to gain access to the new 4.X features, however, such as those in the Advanced model or Central Manager, you must apply a new 4.X base model license to the IVE. This is now called either the “Baseline” or “Advanced” model license. During this process, the IVE removes the old license and replaces it with the new IVE 4.X base model license. Any previously licensed feature upgrades will now require a separate feature license in order to continue working properly. The stored configuration for these features will be maintained during this process and re-activated upon license application.
- In previous releases, RADIUS and LDAP attributes used underscores (“_”) in place of dashes (“-”). Dashes are supported in this release. Any underscores stored in existing Role Mapping rules will be automatically converted back to dashes; however, RADIUS attribute references used in any Custom Expressions and Policy Conditions are NOT converted, and must be converted manually. For example, the 4.0 custom expression “userAttr.Filter_Id = ‘value’” could be converted for 4.1.X by changing it to “userAttr.Filter{-}ID = ‘value’”. The {} around the dash are required to use a dash in a variable name.
- By default, upon upgrade to 4.1.X, NC and W-SAM clients will not enable client-side logging. To enable logging, use settings in the System → Configuration → Security → Client Side Logs configuration page.
- If using PKI Certificate Attributes in custom expressions and role mapping, be advised of changes in this release. Data will be migrated to the new variable names (17569):
 - Email certAttr.Email/certDn.Email/certIssuerDn.Email → certAttr.emailAddress/certDn.emailAddress/certIssuerDn.emailAddress
 - Given name certAttr.G/certDn.G/certIssuerDn.G → certAttr.GN/certDn.GN/certIssuerDn.GN
 - Initials certAttr.I/certDn.I/certIssuerDn.I → certAttr.initials/certDn.initials/certIssuerDn.initials
 - Title certAttr.T/certDn.T/certIssuerDn.T → certAttr.title/certDn.title/certIssuerDn.title
 - Description certAttr.D/certDn.D/certIssuerDn.D → certAttr.description/certDn.description/certIssuerDn.description
 - Serial certAttr.SN/certDn.SN/certIssuerDn.SN → certAttr.serialNumber/certDn.serialNumber/certIssuerDn.serialNumber
 - Surname certAttr.S/certDn.S/certIssuerDn.S → certAttr.SN/certDn.SN/certIssuerDn.SN
- If upgrading an unlicensed appliance, please note that with this release, the links in the Help frame (which displays upon initial boot in the Admin UI) are not working properly. This includes the Help and Key Concepts links. After applying a license to the appliance, these links will work.
- Please review the following upgrade procedures:
 - Save a backup of the system/user configuration and log files before performing the upgrade.
 - To speed up the upgrade process and minimize downtime, we recommend you clear logs and other

trace files which you have archived and then perform the upgrade. Afterwards, you can re-import those archives. This process is especially important for IVEs which have very large log files such as 200MB or larger (based on the configured size limits), since the IVE may process these log files during upgrade and increase the upgrade time significantly.

- For upgrading clusters:
 - With Central Manager – Central Manager will detect the upgrade of a single node in the cluster, and upon its reboot/re-synch, it will instruct the other nodes to upgrade themselves automatically by sending them the service package.
 - Without Central Manager – To upgrade nodes in a cluster, the Admin should disable the clustered nodes, upgrade each node individually, and after the nodes reboot, re-enabled them in the cluster.

Known Issues/Limitations Fixed in this Release

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

1. To successfully authenticate as an administrator that belongs to the built-in Administrators authentication server or as an end-user that belongs to the IVE Authentication server, the username must always be entered in lowercase. Even if the username was created in upper case, login will fail unless the username is entered in lowercase. (24184)
2. If the Admin creates a new Authentication server and attempts to save the configuration without filling out all of the required fields, the configuration fails as expected. However, if the Admin then fills out the required fields and successfully saves changes, the new Authentication server will not work properly. (23186)
3. For AD/NT Authentication, the Admin username and Kerberos realm name fields are now required. You can use a regular user account in the Admin username. Here are the steps to create a regular account to be used in AD/NT authentication server:
 - a. Create a normal user. Create a new group and point this user to that group as Primary Group. (Just to eliminate that it is not using DomainUsers group)
 - b. Give permissions for this user for controlling computers. Grant the "Create Computer Objects" and "Delete Computer Objects" Access Control Entries (ACEs) to the User
 - From the Active Directory Users and Computers snap-in, click Advanced Features on the View menu so that the Security tab is exposed when you click Properties.
 - Right-click the Computers container, and then click Properties.
 - On the Security tab, click Advanced.
 - On the Permissions tab, click Add and add created user to the list of permission entries.
 - Make sure the "This object and all child objects" option is displayed in the Apply onto box.
 - From the Permissions box, click to select the Allow check box next to the Create Computer Objects and Delete Computer Objects ACEs, and then click OK.
 - c. Add the above user in the AD/NT configuration admin credentials section.
 - d. Restart the IVE services to confirm that it is not using the previous add before logging with a valid user.
 - e. Login with a valid user and verify in policy trace/snapshot and see whether "Join to Domain" is successful.
4. Password Management for AD (native) is not supported on AD/NT secondary login servers. (21869)
5. When launching W-SAM on a Chinese OS with the language setting [ZH-CN] (Chinese (China)), the W-SAM GUI will launch with Traditional Chinese instead of Simplified. (22876)
6. Extremely high values for the idle timeout and maximum session timeout will block a user from launching the meeting client. A value that is less than 600 minutes is recommended for idle or maximum session timeouts. (22982)
7. When using the annotation capability of the Secure Meeting white-boarding feature, the button to disable

- drawing access is not working properly after the user has been granted access to draw. (22893)
8. If using a MacOS or Linux Secure Meeting client, if the IVE restarts or the clients somehow loses connectivity to the IVE, the clients will not automatically reconnect. (23002)
 9. If an attendee joins a meeting after sharing and remote control has been enabled for some other meeting attendee, the new attendee's meeting client may show the wrong remote controller designation. (22908)
 10. The locale for a meeting presenter running on a Mac OS X is based on the Macintosh setting rather than the IVE administrator console setting. (19573)
 11. When the presenter selects "Enable drawing for all attendees", Secure Meeting grants the permission to those attendees that are currently in the meeting. For all future attendees, the presenter has to individually grant permissions. When granting permission, the presenter may see an error message "Failed to change roles". (22777)
 12. Annotations on viewers' screens may be positioned incorrectly if the annotator's window has scroll bars. We recommend enabling the viewing/annotating window in full screen mode when annotating. (22769)
 13. For Citrix Terminal Services, when using the "Download from Citrix web site" or "Download from the URL..." options, the Admin needs to create a Caching policy for these Web client URLs. For the "Download from Citrix web site" option, the Admin needs to create a Caching Policy for <http://download2.citrix.com/files/en/products/client/ica/current/wficat.cab>. For the "Download from the URL" option, the Admin needs to create a Caching Policy for the URL entered on the Admin console. The Caching policy for these URLs should be set to "Cache (do not add/modify caching headers)" and can be found in the Resource Policies > Web > Caching page. For more information on the Caching Resource Policies, refer to the administrator's guide. (23064)
 14. Cookies are not saved for hostnames which contain a "_" (underscore) due to a bug in Internet Explorer. For more details, see: <http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q275033>. (22614)
 15. For NFS file browsing to work properly, you must configure an NIS server on the IVE before enabling NFS file browsing. (14594)
 16. A Value of ZERO in the Host Checker or Cache Cleaner "Client Idle Process Timeout" field will cause Host Checker or Cache Cleaner to go into a loop. (23134)
 17. If using detailed policy rules, the expressions *CacheCleanerStatus = 0* is not evaluated correctly. (23097)
 18. There are known clean-up problems in Cache Cleaner deleting any Admin-specified directories on Win98 clients. Any folder that is not in the user profile directory will not be deleted by Cache Cleaner. (22989)
 19. Integrated telnet client security vulnerability identified by NIS. (26294)
 20. Welcome message now is capable of handling double quote and & characters. (24562)
 21. Welcome message now is capable of using html tags (24370)
 22. The IVE will notify the administrator when a particular IP address is used by another network device on the same LAN segment.
 23. Support for Citrix Metaframe Presentation Server 3.0, Web Interface 3.0, Program Neighborhood 8.x, and Web client 8.x were added in this release. If Citrix is selected as a standard application in J-SAM then J-SAM will now listen on ports 2598 and 1494 in order to support the session reliability feature in the 8.x Citrix clients. J-SAM will listen on both these ports even if the client being used is a 7.x client or if Session Reliability is disabled.
 24. Citrix client version 7.x works through J-SAM on Mac OS X.
 25. The Ctrl-C character combination for Secure Terminal Access on Mac OS 1 0.2.8 now works (8371).
 26. Web proxies that require NTLM or Basic authentication are now supported.

27. PDF file formats are now supported through the IVE rewriting engine with Acrobat 5.1 and greater. However, for the user to view inline PDF content in Acrobat 6.x, the user will have to click "Open" on the file download dialog. This issue is due to a bug related to IE and Acrobat 6.x over SSL (22680).
28. VIP Sourcing does not work for Windows File Share traffic. (25143)
29. If a failure occurs during XML Import, system services restart even though the system ignores the imported (failed) configuration. (25931)
30. During XML Import, an "Internal Error" label appears on the top line of the status page, and a successful import is reported as a "success" under Internal Error. (25926)
31. Error and status message changes are required in the administrator user interface for XML Import/Export to make them consistent across different components. (25890)
32. Exported XML instances contain empty nodes in some cases. These empty nodes will cause a problem on Full Import, since the empty nodes will be interpreted as a "delete" operation, causing corresponding elements to get deleted from the IVE system cache.(25886)
33. Ordering of resource policies as defined by the administrator is not preserved in the exported XML instance. If the same instance is imported, the resulting policy evaluation order could be different, resulting in incorrect system behavior. (26177)
34. XML Import/Export can now be used in a clustered deployment. Workaround for clustering provided for GA: The administrator can export configuration from one node of a live cluster, and then has to manually set the state of all other nodes to "disabled" in the XML file to be imported, perform the XML Import operation, and then disable and re-enable all the other nodes in the cluster to force them to synchronize their configuration to the newly imported configuration.
35. The IVE responds to SNMP requests regardless of the community name specified. (25961)
36. There is an error during creation of a snapshot on the serial console indicating that SCP failed. (25068)
37. Regular WSAM (No Netbios File Sharing): Moving from 4.2 GA to 5.0 R1 will still require WSAM to reboot because the infrastructure to prevent any further reboots is not in the existing 4.2 codebase installed on the machine. Once 5.0 R1 has been installed, and the user upgrades to 5.2, 5.3, etc, WSAM will NOT be rebooted as the infrastructure for parallel installations of the TDI Driver is in the 5.0 R1 code base installed on the machine.
38. WSAM with NetBIOS⁷ File Sharing: You will always require a reboot when File Sharing is enabled, because WSAM TDI Driver has to be layered between TCP/IP and NetBT⁷, which requires a reboot to take effect (Windows requirement).
39. The Passthrough Application List/Bypass Application List function in the Juniper W-SAM configuration no longer applies to Windows 2000 and Windows XP computers. This function is only applicable to LSP-based W-SAM, which now is only on Windows 98/ME. Windows 2000 and Windows XP both are now both built on a TDI framework, which features far fewer application conflicts. (25321)
40. W-SAM on Win2000 (all languages) does not launch if msvcp60.dll, the Microsoft C++ Runtime Library, is missing. (17166)
41. Network Connect re-architecture resolves this: After the IVE is upgraded, some remote users may encounter an "indefinite disconnect" of Network Connect of prior releases. If a user sees their Network Connect client (NCUI.exe) in a "Grayed out" mode within the system tray for any longer than 2-3 minutes, the user should uninstall Network Connect and then install the new version of Network Connect again. (23043)
42. When split-tunneling is enabled, and the client PC is "suspended", after a resume, the Network Connect client may still be running for a few moments even though it has been disconnected due to the PC being suspended. With split-tunneling disabled, Network Connect will exit immediately. (23141)
43. There are known issues with Network Connect and Nortel Contivity VPN client v. 4.65 specifically in

environments where client machines have to connect to the IVE using a client-side web proxy. In these situations, the presence of Nortel Contivity forces a state where the user won't be able to access the Corporate Intranet applications through NC. Un-installing the Contivity VPN Client fixes the problem. (21125)

44. If Palm Desktop or Hot-Sync software is being used, please make sure to force the software to bind to USB ports rather than Serial interfaces. If the user's machine does not support USB, the user should select a physical COM port instead of the virtual COM port NC installs. (20598)
45. Network Connect will not work if the physical connection is a modem dial-up, and there is a connection entry which accepts incoming modem connections.
46. In some rare instances, Network Connect install/upgrade could result in a "RAS Error" message. If this message appears, then re-initiating the Network Connect install again should resolve the issue. If it is an upgrade, un-installing the previous version of Network Connect (from the IVE UI or from the Control Panel) and re-installing a newer Network Connect should resolve the issue. Deleting the Network Connect Dial-up adapter and re-connecting to Network Connect should also resolve the issue.
47. Network Connect cannot be run with "Limited User" privileges. (13493). Please use the Installer Service.
48. Network Connect access control lists (ACLs) are only evaluated at the time when the Network Connect session is launched. If the ACLs are changed after a session is launched, or if an ACL has dynamic conditions (e.g., time of day, Host Checker variable) which change during the session, then these rules will not be taken into effect. If Administrators want to apply the new Network Connect ACLs, they need to force the user to log out, log back in, and launch Network Connect again.
49. TV Media spy ware (tvm.exe) is known to cause conflicts with Network Connect. Please ensure that this application isn't in play with the current configuration.
50. Downgrading from 4.1.X or 4.2.X ActiveX to 4.0 standalone Network Connect installer gives a 1078 error.
51. Resource Policy evaluation for J-SAM, W-SAM, Secure Terminal Access, Web, and File resources are not evaluated for already-established "in-flight" connections – they are only evaluated at the beginning of a transaction. A transaction is defined in the following way for Web – HTTP Request, Files – Upload/Download of a file or listing of shares/files, SAM:Beginning of a new connection to a backend resource. Support for this will be added in a future release. (14476)
52. Network Connect Proxy Support Chart:

	<i>Explicit Proxy to get to IVE</i>	<i>Pac file to get to IVE</i>	<i>Explicit Proxy to get to Internal Applications</i>	<i>Pac file to get to internal applications</i>	<i>Hybrid: Proxy to get to IVE and Proxy to get to Internal applications</i>
<i>Split Tunneling Enabled</i>	<i>Supported</i>	<i>Supported</i>	<i>Supported</i>	<i>Supported</i>	<i>Supported</i>
<i>Split Tunneling Disabled</i>	<i>Supported</i>	<i>Supported</i>	<i>Supported</i>	<i>Supported</i>	<i>Supported</i>

Known Issues and Limitations

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

Authentication

1. The username sent for single sign on to Basic Auth and NTLM-protected web and file servers has changed between the previous and current release. In 4.2, the IVE would always prepend the domain

name to the username. Therefore the username would always have the format domain\user. However, in 5.0 R1, the IVE will now send the exact text entered in the IVE login page. For example, if the user enters “john” on the IVE login page then the IVE will send “john” as the username. Or if the user enters SALES\john then the IVE will send SALES\john as the username.

2. For SSO to file servers protected by NTLM Auth, a new configuration option has been added under Resource Policies -> Files -> Windows Server Credentials. The Admin can now configure any IVE variable name as the SSO credentials to an NTLM-protected file server.
3. In order to retrieve all the groups from all the AD domains in the AD/NT Server Catalog, NTLMv1 setting is required. After the group is assigned in role mapping rules, administrator can set it back to NTLMv2. (27230)
4. The ACE Next-Pin and New-Token modes do not work properly when using ACE as the secondary login server. (21870)
5. The Realm-level option “Enable Password Management” needs to be enabled in order to allow the end-user or administrator to change their password via the “change password at next logon” (IVE Authentication – user accounts). (22969)
6. If you set an initial username and password for an administrator when configuring an NT/AD authentication server, and then remove the password later, the password field in the IVE admin UI still shows a series of ‘*’ characters for security purposes. (For instance, you may remove the password if the administrator account now has a null password.) Even though the IVE still shows asterisks in the password field after you have saved changes, it still removed the password as specified and saved your changes properly. (20949)
7. The Multiple Sign-In Credentials feature is not supported for iMode devices. Administrators must create a separate sign-in URL which maps to a Realm requiring single authentication credential for Imode clients. This issue will be fixed in a future release. (22805)
8. During the AD authentication, the IVE joins the AD domain controller as a member, enabling the IVE to obtain group information for all the authenticated users. If the "IVE machine" name is manually deleted under "Active Directory Users/Computers", then the IVE takes up to 6 hours to re-join the domain controller and during this period all group lookups will fail. Hence, we do not recommend manually deleting the IVE machine name from AD console. If you accidentally delete the IVE machine name, you can forcibly restart all services on the IVE or reboot the IVE to allow the IVE to re-join the domain immediately. (22639)
9. When using the “Match Equivalent IP” Resource Policy option, if the hostname contains a wildcard character, such as ‘*’, this option will not work correctly and the policy rule will not be matched. (16450)
10. When using HTTP Basic Auth (in SSO), if a Realm Names (not IVE Realm but HTTP Auth Realm) is encoded in Shift_JIS, and not UTF_8, the IVE will not properly display it. (15881)
11. When using special characters for user account names, such as “ ‘ , > , < , \$, % , etc... a JavaScript error may be displayed when accessing the server’s user listing. Administrators should avoid using characters of this type for user account names. (22452)
12. Accounts which are used for both administrator and end-user access to the IVE may conflict if they use the same username and authentication server. This practice may cause one account to force the other account out of an IVE session when the other logs in. One simple solution is to duplicate the Authentication server on the IVE so that Admin users log into one Authentication server and end users log into a duplicate server that points to the same backend system.
13. If you use RSA ACE/Server authentication and change the IVE IP address, you must delete the node verification file on the IVE for ACE/Server authentication to work. Also, make sure to un-check the “Sent Node Verification” setting on the ACE/Server for the IVE.
14. The IVE only supports Crypt/MD5 password hashes for NIS authentication.

15. The Backup Domain Controller configured in AD/NT authentication server is not used when doing group search in server catalog or during runtime group mapping. (26500)

Password Management

1. The Password Management for an expired password during authentication on Sun ONE Directory Server version 5.2 is not working. If the user's password has not expired, then changing the password through the Preferences page still works. (26142)
2. Password Management must be enabled at the Realm level if the Admin wishes to enable password expirations or require users to change their password at next logon.
3. When a user's password is expired, and Password Management is NOT enabled for that user's Realm, the error message displayed to the end-user shows "account disabled", although this account may not truly be disabled. This will be addressed in a future release. (21654)
4. When using Sun One/iPlanet as an Authentication server and enforcing both "password expiration in X days" and "allow password change after Y days", if the user's password is reset (or changed) then the user's profile will have a new password expiration date. However, if the password expiration timeframe is changed (for example from 10 days to 20 days), then the user's profile will still show the old password expiration time. This is a limitation of Sun One/iPlanet to which we adhere.
5. AD Domain Controllers synchronize security policy settings every 5 minutes. If a change is made to the security policy, for example "minimum password length", it could take up to 5 minutes before that change propagates to all Domain Controllers. This also applies to the Domain Controller on which the change was originally performed. For more information, please refer to:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/lpe_overview.asp.
6. Changing passwords in AD requires LDAPS support on the AD server. This can be enabled by importing a valid certificate/key into the "Personal Certificate Store" using the MMC and selecting the "Certificates" snap-in. In some situations, an external key and certificate may need to be imported. In this case, the key and certificate should be combined into one file, using PKCS #12 or PFX format. The imported certificate must be signed by a trusted CA.
7. For a list of what Password Management functions are supported, for the various platforms, and for a list of attributes, please see the administration guide.

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

1. When CRL checking is enabled, the CRL and the corresponding CA certificate need to use the same string type for Subject and Issuer fields. Otherwise, the CRL issuer DN and CA Subject DN will not match, causing the CRL download to fail.
2. Client Side Digital Certificates which contain foreign language strings should conform to certain guidelines in order to successfully work with the IVE. We support the following string types for subject and issuer DN fields: PrintableString, IA5String, BMPString, and UTF8String. The IVE has only partial support for T61Strings containing only European characters. Asian languages should use BMPString or UTF8String for DN values. (18305)
3. The IVE CRL checking mechanism will ignore the IssuingDistributionPoint CRL critical extension if included in the CRL object.
4. CRL download via HTTP Proxy is not supported.
5. Partitioned CRLs are not supported in this release. (16992)
6. After a Client-Side Digital Certificate has been loaded and used, Internet Explorer and Netscape both cache the credentials and certificate/private key as long as the web browser window remains open and in

some cases until the PC is rebooted. More details can be found at:

<http://support.microsoft.com/?kbid=290345>. This caching overrides password-protected certificates (you will not be prompted for the password again) and even USB tokens (you will not need to keep the token in the PC). For this reason, it is very important that Administrators train their end-users to always close their web browser after logout.

One helpful mechanism to achieve this is to add some text to the custom logout message asking users to close their web browser to properly end their session. This can be done under the Signing In menu by modifying the default sign-in page.

7. Certificate users may get an HTTP 500 error if the end-user gives a wrong password for their private key file when challenged for a client certificate. (13489)
8. When using LDAP for a CDP, port numbers should not be specified in the CDP Server field. The default port number for LDAP is 389. To use a non-standard port, Manual CDP configuration should be used. (18578)
9. When a client-side digital certificate authentication policy is configured for the Realm, if the client's certificate is expired, then the user will not be able to log into the Realm until he is given a valid client certificate. (14922)

Terminal Services

1. The Terminal Services feature 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 only works on Win2K3.

SNMP

1. On an IVE with a meeting license for 'n' simultaneous meetings, the meetingLimit SNMP trap is being sent at the time of launching the 'n+1'th meeting instead of after launching the 'n'th meeting. (27444)
2. Critical error message is also not being sent, even though Critical and major log alerts are enabled on the SNMP page. (27444)
3. The iveDiskFull SNMP trap is not being sent, even when the disk is completely full. Instead, the IVE keeps sending the iveDiskNearlyFull trap with value set to 100. (27408)
4. SNMP works with any community name, even with NO settings (name, location, community) specified on Admin console. Using Snpwalk/HP OpenView with ANY community name fetches SNMP values. However, clicking on the save settings button on SNMP page changes the Agent status to "Off". Snpwalk/OpenView produces a "no response" error and doesn't get SNMP values after this, which is the correct behavior. (25961)
5. The logNearlyFull SNMP trap cannot be disabled. (25061)
6. Snpwalk on the system displays the OS and kernel information. (14440)

Rewriter/Web Applications

1. In Siebel 7.5, the Help menu does not work through the content intermediation engine. (22871)
2. This release contains support for Flash version 5 and above. However, Flash applications that use the XMLSocket object or Flash Remoting are not supported.
3. The end-user may not be able to modify the User Preferences tab on the Citrix Web Interface 3.0 login page when accessing this application through the rewriter and J-SAM (25640).
4. Non-HTML content such as images, js, and css files that are served from a different SSL server than the HTML page may not load correctly. To work around this problem, upload a valid production SSL

- certificate on the servers that serve the non-HTML content or unselect the setting “Warn users about the certificate problems” under Roles -> Web -> Options -> “Allow browsing untrusted SSL web servers” (27281).
5. If using Safari on Mac OS, the browsing toolbar may not show up on web pages that contain Flash objects and Java applets (25896).
 6. The “Display Favorites” functionality on the IVE toolbar may not work on web sites that use iframes or frames (27361,24621).
 7. The following advanced features of the IVE framed toolbar are not available in PTP: (26091)
 - Bookmark current page
 - Displaying the original URL(always a blank display)
 - Displaying favorite bookmarks
 8. The IVE always intermediates a Web proxy using basic authentication, even if the administrator has disabled the “Intermediate Basic Authentication” option. (24675)
 9. The Documentum Web application is not supported by the IVE Web Rewrite function.
 10. The IVE does not support Lotus iNotes in offline mode. (9889)
 11. The correct caching resource policies must be configured to enable end-users to open and save email attachments in Microsoft OWA. The “Smart Caching” option works for all document types other than text and HTML. To save attachments of type text and HTML, the cache control policy for these file types must be set to “Cache Control No Store.”
 12. To enable iNotes users to open and save .zip, Excel, and .pdf documents, the Web -> Caching resource policies must feature the “Cache Control No Store” option. For Word documents, a “Smart Caching” caching policy is supported. The reason for this distinction is that the Domino server only identifies Microsoft Word documents correctly.
 13. When using Siebel 7.5 through the IVE, the user may see ActiveX warning pop-ups. To stop these pop-ups, the user must change their browser security settings. For IE, this can be done by going to Tools > Internet Settings > Security > Custom Level > and enabling each of the ActiveX items listed there. (8247)
 14. Some menus of Siebel 7 are not working. This is only a problem for menu-dependent applications. With Siebel 7.5, the menus work as expected. (9442)
 15. To use Web applications such as Microsoft OWA, Lotus iNotes, or Siebel via Internet Explorer with compression enabled on an SA5000, the caching policy must be set to “Cache” (15383, 27213). This is due to the following limitations with Internet Explorer and gzip compression:
 - <http://support.microsoft.com/default.aspx?scid=kb;en-us:825057>
 - <http://support.microsoft.com/default.aspx?scid=kb;en-us:312496>
 - <http://support.microsoft.com/default.aspx?scid=kb;en-us:325212>
 - <http://support.microsoft.com/default.aspx?scid=kb;en-us:327716>
 16. When accessing a Flash Web site through the IVE that requires the installation of Macromedia, the user is not prompted to install the Macromedia application. Therefore, Flash Web site does not render properly. (26391)
 17. The Java applet upload feature does not work with applets that require additional text files or configuration files to be uploaded. The only file types that can be uploaded are .jar, .cab, and .zip files. (26632)
 18. When using the Java Applet upload feature, if you include the <PASSWORD> token within the generated HTML it appears correctly if you view the source of the browser window launching the applet. This

behavior cannot be changed because the IVE does not control how the Java applet processes the password. (27033)

19. The Java applets upload feature may not work on Mozilla 1.6 unless the default cookie settings for the browser are modified. This is because of Mozilla 1.6 behavior where cookies are not passed from the browser to the Java applet. To work around this limitation, change the settings to "Enable all cookies" under Edit->Preferences->Privacy & security->Cookies. (27353)
20. Citrix Java applets will not work on Mac OS X unless a production Web server certificate has been uploaded to the IVE (25264).
21. Lotus Sametime Connect Chat functionality is supported only when using Web rewriting and J-SAM. Full Sametime connect functionality is supported using W-SAM and Network Connect. Users who access Lotus Sametime Connect directly and need to access it through the IVE should first remove the ActiveX control from their Internet browser's cache.
22. The native browser on a Symbian handheld device is not supported (22743).
23. The functionality to bookmark a page while browsing is not available on handheld devices (27371).
24. On a Symbian device, the toolbar logos may be aligned vertically instead of horizontally. In addition, the icons may appear as text links instead of GIFs. (27381, 27377)
25. The Browse field at the top of the home page or the framed toolbar supports different formats. Formats such as outlook:inbox (or any x:y format), however, are supported on Internet Explorer, but not Firefox. (27754)

Central Manager

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

Host Checker and Cache Cleaner

1. Please follow the steps below to uninstall Host Checker correctly after upgrading to 5.0R3 (29522):
 1. From the IVE Admin UI, remove/uncheck all the "Host Checker Connection Control" policy under Roles/Realms Host Checker Restrictions;
 2. Then uncheck "Create Host Checker Connection Control Policy" under System > Configuration > Security > Host Checker and click save changes;
 3. Now check "Create Host Checker Connection Control Policy" as in step 2;
 4. Add "Host Checker Connection Control" policy to Roles/Realms Host Checker Restrictions;
2. If a realm has the following three conditions, then users will not be able to log in (28246):
 - No Host Checker policy evaluated or enforced at the realm level;
 - Role mapping rules to map users to more than one role;
 - At least one of the mapped roles has Host Checker policy restrictions enabled;

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

3. On Macintosh and Linux OS, during the sign-in process, if a user waits too long to sign in, Host Checker is not restarted. The workaround is to close the browser, open a new browser, and try to access the sign in URL again. (27907)
4. Host Checker Connection Control does not work on Windows 98. (27646)
5. On Windows 98, the Host Checker remediation page is not loaded correctly when the user clicks on the Host Checker icon in the system tray. (26893)
6. For Host Checker to work correctly on Internet Explorer 5.5/SP2, you need to have Internet Explorer patch Q832894 installed. (25905)
7. If a user closes their browser and launches a new browser, the Host Checker may not start correctly. The workaround is to remove the browser cookies and try to sign in again. (26722)
8. If the "Default Web Browser" option in the Safari browser on a Macintosh is set to Internet Explorer, then Internet Explorer displays the remediation page after the user logs in. Otherwise, the Safari browser displays the remediation page. (24743)
9. In a Host Checker policy, when you create a rule to check file, you cannot specify the file path using wildcards and give a MD5 checksum. (27648)
10. In order for Host Checker to work, the browser has to be configured to return a cookie. (25612)
11. Host Checker will not work with proxy on Macintosh OS 10.3.3 or earlier. (25259)
12. On Macintosh OS, if the user receives a "Host Checker is already running" error when signing in, the user must locate the Java process, kill it, and try to sign in again. (27671)
13. Minimum version of file check is not working. The workaround is to use the file last modification time instead. (27642)
14. If a "Restricted" user runs Host Checker, any checks to privileged locations or privileged directories in the registry are prohibited.
15. If a "Restricted" user runs Cache Cleaner, they will not be able to clean directories that are in privileged root directories like c:\program files\..., for example.
16. If the 3rd Party Package for Sygate On-Demand Virtual Desktop is used, administrators should set the Host Checker login inactivity time-out to a value large enough to prevent Host Checker from prematurely uninstalling Virtual Desktop. (25324)
17. Cache Cleaner attempts to verify the session during its cleaning phase. During this time, a connection may be opened from the process back to the IVE.
18. If Cache Cleaner is configured for a Realm, users may be unable to log into the IVE if they cannot install the Cache Cleaner application on their PC. Administrators should take this into consideration when configuring Realm authentication policies, role restrictions, and resource policies.
19. In this release, Host Checker and Cache Cleaner policies configured at the authentication Realm are evaluated and enforced at every Host Checker and Cache Cleaner update interval. Please note that in the previous release, only Role based Host Checker/Cache Cleaner restrictions and resource policies are evaluated dynamically on every status update.
20. When Cache Cleaner is configured to remove content from specific hosts/domains, some associated Web browser history may not get entirely removed. The user can manually delete the entire browser history if they choose to do so. (17124)
21. If two or more administrator or end-user sessions to a specific IVE are initiated from a client, and at least one of them deploys Host Checker and/or Cache Cleaner, the sessions are affected in unpredictable ways. Symptoms can range from Host Checker and Cache Cleaner being shut down to losing role privileges and

forced disconnections.

22. After un-installing Host Checker, the Program Group may still exist in the user's Start menu. This Program Group can be safely removed. (9057)
23. For certain Windows system services (e.g. smss.exe and naPrdMgr.exe), Host Checker fails if the MD5 checksum is used to validate the executable. In such cases, Host Checker is unable to find the path, due to the manner in which Windows loads the process table. This should not be an issue for end-user client applications, such as a personal firewall or virus scanner. (10819)
24. When the security posture of an endpoint changes (e.g. a Personal Firewall starts/stops) there is latency between the time of this event and the corresponding policy changes on the server. For example, a user who is denied access due to the absence of a firewall process is not immediately allowed access upon starting the firewall. The end user needs to wait until the policy is refreshed, which is governed by the Host Checker verification frequency. One way to overcome this situation is to delete the cookies from the IVE prior to restoring the security posture. (13947)
25. The McAfee Desktop Firewall 8.0 Host Checking method requires that the client be running build 485 or higher.

Secure Meeting

1. When using the Java client to launch a Secure Meeting, if the user clicks "No" on the certificate warning presented by the JVM, the meeting client does not launch, but it appears to the user as though the applet is still loading. (22712)
2. Full screen and Remote Control modes are not supported on the Java client. (23148)
3. On the Appointment tab in the Microsoft Outlook Calendar is a check box called, "This is an online meeting using..." This checkbox is not related to the Meeting Server or the Secure Meeting for Outlook Plug-in. This field cannot be used by a third party plug-in.
4. When installing the Secure Meeting plug-in on Microsoft Outlook 2000, a message appears warning that "the form you are installing may contain macros." Users may safely click either "Disable Macros" or "Enable Macros" since the Secure Meeting form does not contain macros. (21408)
5. The end-user must use the same Outlook profile to un-install the Secure Meeting Plug-In for Outlook as the one used to install the Plug-In. Switching profiles between the installation and un-installation of the Plug-In is not supported. (22655)
6. On the Macintosh and Linux platforms, even if the viewers are set to full screen mode, the toolbar will still be visible. (19506)
7. We recommend that you not upgrade the Meeting while Secure Meetings are running on Macintosh or Linux machines. If an upgrade is run during a Secure Meeting, Macintosh and Linux users may not be able to launch the client for a new meeting. This is due to Safari and Mozilla browser behavior related to caching Java applets. The user must close and restart the browser to fix the problem. (22273)
8. When scheduling a meeting from Microsoft Outlook 2000 using the Secure Meeting Plug-in, the user must click "Delete Meeting from Server" on the Secure Meeting form to delete the meeting. The Delete button on the Outlook form will not delete the meeting from the meeting server. This is due to Microsoft Outlook behavior. (21336)
9. When the user launches Secure Meeting, a Security Warning is displayed regarding the SSL negotiation between the client and the IVE. The user must respond to the warning within 15 seconds for the meeting client to launch successfully. (22711)
10. Safari 1.0 has a bug wherein it does not fully support proxy configurations. As a result, if there is a proxy configured, the meeting client cannot be launched from this browser. We are working with Apple on this issue.

11. When using two IVEs in a Secure Meeting cluster, users should always connect to the VIP address to join the Secure Meeting--not the IP address of the physical machine.
12. Red Hat Linux 9 with Mozilla 1.6 and SunJVM 1.4 has a problem with NTLM authentication when using ISA proxy server to download the Secure Meeting .jar file. This causes the Secure Meeting client to download incorrectly.
13. When using MacOS 10.3.3 and Safari 1.0, if the user clicks "NO" on the certificate pop-up, the Secure Meeting client does not install. If the user wishes to try again, they must open a new Safari browser window.
14. The Secure Meeting Chat functionality only supports users using the same language encoding (based on Web browser) in a single meeting. Using a different encoding than what the person typing is using, will result in mangled text. Meeting invitations are sent based on the language setting in the creator's Web browser when meetings are created or saved.
15. If the user forming a Meeting is using Email invitations and accesses the IVE using a URL that is not the fully-qualified domain name for the IVE (e.g. <https://ive>, not <https://ive.company.com>), the Email invitation may display just <https://ive> in the invitation information and not the true hostname. As a result, email recipients may not be able to access the link from the email. We recommend that administrators configure the "Network Identity" under the Network section in the UI. If configured, Secure Meeting invitations will use that hostname, instead.
16. Secure Meeting may function erratically if the time clocks on IVEs in a cluster are not synchronized. We recommend that administrators use the same NTP server for each node within a cluster to keep the IVE times synchronized.
17. When creating a Secure Meeting using the MacOS Safari Web browser, the organizer may be unable to add more than 250 attendees.
18. When presenting, the presenter should consider what access methods are being used by attendees. Dial-up attendees may have bandwidth issues for presentations that redraw the screen or update the screen too frequently. If the presentation saturates the dial-up attendee's bandwidth, remote control and chat functions may not work, as they require sending data back to the IVE over the same, saturated, dial-up link over which they are receiving data. (15203)
19. Secure Meeting attendees do not see the presenter's shared applications if the presenter locks their desktop.
20. Secure Meetings in progress are stopped if a cluster is created during the meeting.
21. On a Windows platform, the meeting client picks up the proxy information from the Internet Explorer browser settings. Therefore, Secure Meeting works on other browsers only if the proxy setting is also configured in Internet Explorer. (17442)
22. Viewers on Linux and Macintosh clients may take a while to load the presentation if the presenter's desktop screen area is larger than 1856 x 1392. (23291)
23. The teleconference number in Secure Meeting Outlook plug-in is not included in the meeting invite. (24077)
24. If the Hide Attendees option is enabled, a "Failed to change roles" message appears when granting annotation permissions to another attendee. (24417)
25. In Fit To Window mode, attendees may sometimes see small blocks of mangled images in their Viewer window. (24427)
26. A presenter using a Linux client is not supported over slow DSL. (24480)
27. In a remote control session, annotation should not be started. (24902)
28. A presenter using a Linux client is not supported in a WAN environment. (24985)

29. In a WAN environment with Linux presenting, there are attendee viewing issues. (24986)
30. There is a limitation on the areas where a Linux and Mac presenter can annotate. If the Linux or Mac presenter annotates over the application toolbar at the top or bottom of the screen, then the annotated objects in those areas are not displayed on the viewers. (25555)
31. Part of the bottom of the presenter screen is truncated when viewed on Linux or Mac viewer in Fit to Window mode. (26468)
32. If the presenter is the only person in a meeting and has started annotation, annotation is not enabled. At least one other attendee must join the meeting for annotation to be enabled. (26717)
33. If the presenter is annotating his own desktop on a Linux or Macintosh system, the annotation viewer may appear to be frozen. To unfreeze the desktop, enter Alt+Tab. (26737)
34. The Secure Meeting Toolbar does not work on Linux KDE window manager if the attendee runs the Viewer in full screen mode. (26851)
35. When the last attendee leaves an annotation session hosted by a Linux or Macintosh presenter, any further annotation operations done by the presenter do not work. (27274)
36. On Linux systems with the application toolbar located at the top of the screen, if the height of the application toolbar is resized while Secure Meeting toolbar is also being displayed, then Secure Meeting toolbar may not respond well to the mouse event to activate and hide it. (27276)
37. The "Enable all drawings for all attendees" and "Disable all drawings for all attendees" options do not work on Linux and Macintosh presenters. (27402)
38. If there are no attendees, when a Linux or Macintosh presenter clicks on the Draw icon to enable annotation, the annotation session is not started. The presenter needs to click the Draw icon again after an attendee has joined the meeting. (27403)
39. When you change the password from the Launch Meeting page, an updated email is sent and the Conductor name is empty. (27487)
40. On Linux and Mac, if the icons on the Secure Meeting toolbar become unresponsive after the presenter enables annotation, look for "Secure Meeting" on the Linux menu bar and click on the entry corresponding to annotation. This will bring forward the Secure Meeting toolbar again with working icons. (27613)
41. On Linux and Macintosh clients, if the Secure Meeting toolbar is hidden, it cannot be displayed again by moving the mouse to the upper left corner on the desktop. The workaround is to ensure that you do not hide the Secure Meeting toolbar. (27616)
42. On a Linux or Macintosh client, if the presenter is in annotation mode and the last attendee leaves the meeting, the annotation icon on the Secure Meeting toolbar is inactive and the presenter will be left in annotation mode. The user should enter Ctrl-Q or click on the exit/end meeting icon on the Secure Meeting toolbar to exit annotation mode. If an attendee rejoins the meeting after the presenter exited from annotation mode, the presenter should stop and start sharing again to enable a new annotation session. (27755)
43. On a Windows client, if the presenter is in annotation mode and the last attendee leaves the meeting, the annotation session is disabled. For annotation to work again when an attendee rejoins the meeting, the presenter should stop and start sharing again and enable a new annotation session. (27762)

Windows based Secure Application Manager (W-SAM)

1. Netlimiter 1.3 software has an LSP which conflicts with our Win98/ME version of W-SAM. W-SAM has moved away from LSP for all Win2K and WinXP platforms, and has moved over to a new packet interception layer called TDI. However, since Win98/ME is still running on LSP, this application conflict

- is applicable here. (22875)
2. No Session Timeout warning message is displayed for W-SAM clients on Win98/ME platforms only. Windows 2000 and Windows XP clients will have full support for Session Timeout notification. (27111)
 3. When “WSAM uninstall at exit” is checked on the server, launching W-SAM twice within an authenticated session is not supported. Users must sign in to the IVE two separate times; the first one resulting in an uninstallation, and the second initiating a reinstallation. (26698)
 4. The W-SAM Error Codes displayed in all Informational and Error messages output through W-SAM are not verbose in the 5.0 R1 release. They act as identifiers so that users can cross reference them within the W-SAM error message documentation for detailed “Cause” and “Action” information. (26695)
 5. 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)
 6. Now that W-SAM has moved to a TDI architecture in the 5.0 R1 release, only one application (BitGuard Personal Firewall) is known to conflict with W-SAM.
 7. 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 these applications have with other well-written TDI drivers, like the one used by Windows Secure Application Manager (WSAM). Live update should be run before installing WSAM. (24285)
 8. Some W-SAM users on Windows 98/ME may experience a General Protection Fault after ending a session. Just opening W-SAM, troubleshooting, and switching among the individual tabs may result in this situation. If you see this situation in your environment, contact Juniper Support. (22797)
 9. When using Firefox on Windows 98/ME and launching W-SAM through an authenticated proxy, Firefox may crash due to Firefox’s LiveConnect feature behavior. It is commonly accepted that Firefox’s LiveConnect is not very stable on Windows 98/ME. (25701)
 10. 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)
 11. On Windows 98/ME, we recommend using the “Add/Remove Programs” link to manually uninstall W-SAM. There are known issues with using the Uninstall W-SAM link on the Juniper SSL-VPN Preferences page, where after uninstall, the “dsSamProxy.exe” process is not terminated. In the even that the uninstall is initiated from the Preferences page, manually terminate the “dsSamProxy.exe” process using Task Manager. (26937)
 12. The Passthrough Application List/Bypass Application List functionality is only applicable to LSP based WSAM, which now is only on Windows 98/ME.
 13. When ActiveX is disabled on the browser, the Adaptive Java Delivery method is used to install and run W-SAM, and Sun JRE is being used, W-SAM returns a query for “Reconnection” on the client during the auto-uninstall process. (25046)
 14. W-SAM launched using Scriptable Samlauncher does not generate a Session Timeout warning message. (26802)
 15. Restricted Users can't install W-SAM using the Standalone Installer, even in the presence of the Installer Service. The Installer Service is designed to provide application installation capability for users who are performing a standard Web-based installation from the IVE. (22454)
 16. 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)

17. Customers should be aware that the Venturi Wireless Client is not written to interoperate with other LSP providers. When Venturi Wireless is installed on a system that has Juniper W-SAM, the system may become unstable. Juniper does not claim compatibility with the Venturi Wireless client. (19690)
18. If using W-SAM in Host Mode with a host defined as “*:.*,” the client may look up cached name/DNS entries rather than looking up new name/DNS entries (which W-SAM will intercept). This may result in incorrect DNS resolution. (19519)
19. When downloading files via FTP through Internet Explorer over a W-SAM tunnel, large files (>15MB) may cause Internet Explorer to time-out unexpectedly. (18635)
20. When using SamLauncher with Persistent Cookies enabled, starting SamLauncher immediately after stopping an authenticated W-SAM session causes the session to be authenticated using the Persistent Cookie, even if an invalid username and/or password was entered from the command line. (19521)
21. If a user attempts to uninstall W-SAM through the Preferences page, and selects “No” when asked to reboot their machine, W-SAM is only partially uninstalled from the client, and subsequent attempts to uninstall W-SAM fail. To uninstall W-SAM, the user has two options. (1) From the Start Menu, run "Programs > NetScreen > Windows Secure Application Manager > Uninstall WSAM". (2) Run the "c:\Program Files\Neoteris\Secure Application Manager\samclean.exe" application.
22. When using the command-line W-SAM (“SamLauncher”), the URL entered must contain the prefix https://.
23. 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; however, there is no additional impact to the user session. (18681)
24. If an administrator configures W-SAM with NetBIOS support, once a user installs W-SAM, they are prompted to reboot their PC before continuing. If they do not reboot, W-SAM does not function correctly. (9158)
25. 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.
26. To access a windows file share by hostname using W-SAM, the administrator must explicitly configure the server’s NetBIOS name (alphanumeric string up to 15 characters) in the W-SAM Destination Host configuration page.
27. Users must launch drive maps through WSAM in one of the following ways:
28. NetUse--At the Command prompt, type: net use * \\server\share /user:username
29. Right Click on My computer -> Map network Drive, or Explorer-enabled drive mapping. In Windows Explorer, go to Tools → Map Network Drive, then select “Connect using a different username”.
30. 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.
31. When W-SAM is enabled with NetBIOS support, the presence of an installed VPN client can cause unexpected behavior. A common symptom is that NetBIOS connections work using IP addresses but not using hostnames. This issue is generally resolved by releasing and renewing the IP bindings (e.g. using ipconfig). Some extreme cases might require the VPN client to be uninstalled.
32. When using W-SAM on an IVE, we recommend installing a trusted SSL server certificate, otherwise users may receive pop-ups telling them it is not a trusted certificate while attempting to launch W-SAM.

33. When using SAM (both 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.
34. 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.
35. If W-SAM (with NetBIOS) filters traffic by IP address (as opposed to hostname), the entries in the W-SAM Host list must be specified with IP subnets (IP address/net mask) or single IP addresses. Using "*" in the W-SAM Host list does not work.
36. If W-SAM is configured in Host Mode, and the Web browser is configured to go through a proxy, W-SAM will not be able to tunnel traffic to the specified hosts. To work around this, users can add the specified hostname to the Web browser proxy exception list. Another approach is to secure all Web browser traffic using Application Mode.
37. On Windows 98/ME only, IBM Client Access cannot be secured through W-SAM because it is not a Winsock application. Instead, J-SAM may be used to secure this application.
38. On Windows 98/ME clients, W-SAM creates a log file on the Desktop named samlog.txt. This file does not interfere with the client machine in any way and can safely be removed via Cache Cleaner or manually after exiting W-SAM.
39. When end-users choose to un-install W-SAM through the System → Advanced Preferences page, the file NeoterisSetup.cab is deleted from the user's system. The effect is that the Active-X Installer control gets downloaded again when clientless functionality (e.g. Host Checker, Cache Cleaner, W-SAM, Network Connect, etc.) is invoked. No user intervention is required.
40. Currently, there is no automatic discovery for file shares in W-SAM.
41. On Windows 98/ME only, when W-SAM detects the presence of certain Layered Service Providers (LSPs) on the client PC, it does not launch or install. This behavior is currently limited to the new.net and Webhancer LSPs, installed by certain SpyWare applications.
42. 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)".
43. On Windows 2000 and Windows XP systems, drive mapping through W-SAM is not supported if the users log into a domain (when logging into their PC). If this occurs, the user should see one of the following error messages: "No Windows NT or Windows 2000 Domain Controller is available for..." or "There are currently no logon servers available to service the logon request." This is caused by Windows 2000 behavior which causes domain credentials to be cached. To work around this issue, please have the users log into their PC as a local or workgroup user.
44. When scripting the use of SamLauncher.exe, users should provide the -reboot command-line flag, so that if the launcher requires a reboot, it happens automatically and does not exit, prompting the user to manually reboot. Note that during a fresh install (with NetBIOS enabled), W-SAM requires a reboot.
45. When a W-SAM user connects to an IVE with an earlier build version, W-SAM does not downgrade completely. The user will need to run the Samclean executable (with admin privileges) and install W-SAM again.
46. There is a known issue on Korean version of the Windows Operating System, where if Windows Secure Application Manager is launched, the WSAM icon does not appear in the system tray, but rather it appears as a blank square. This is a known issue and will be resolved in a maintenance release. Customers will still be able to get access to the User Interface by clicking on the blank square, and all WSAM functionality is working correctly. It is just the cosmetic item that the System Tray icon doesn't appear. (28120)

47. For **W-SAM on Pocket PC**, W-SAM is supported on Windows CE 4.2 devices that have the ARM processor only. This includes DELL and HP handhelds. WSAM on Pocket PC is officially only **BETA quality**. Application Mode is only supported for WSAM on Pocket PC. Supported platforms are: Dell Axim: Windows Mobile 2003: Pocket IE 2003 and HP IPAQ: Windows Mobile 2003: Pocket IE 2003. Compatible platforms are: Windows Mobile 2003-based Pocket PCs– Compatible applications are ones that are TCP-based and client-initiated
48. When using WSAM on Pocket PC devices, if a user clicks on the “Logout” function of the Web User Interface of the IVE, there could be situations where WSAM application will not terminate. This is a known issue. We will be resolving this in an upcoming maintenance release. When the user were to re-login to the IVE the next time, and upon launching WSAM, the user would get a prompt saying that their WSAM is already running. They would need to “Exit WSAM” by bringing up their running WSAM Application User Interface. (26738)
49. There is a known issue when using Windows Secure Application Manager (WSAM) on Pocket PC where if a user clicks on “Exit WSAM” while a client application is being secured through it, WSAM might improperly terminate and force a reset. (26822)
50. Configuration Guide for WSAM on Pocket PC: When defining Client/Server applications to secure through Windows Secure Application Manager on Pocket PC devices, the IVE administrator should define the “Process Name” in the Role-> SAM -> Applications -> Add New Application UI. The process name for Pocket Outlook is “tmail.exe” and the process name for Windows Terminal Services is “mstsc40.exe”. Pocket Internet Explorer is “iexplore.exe.”
51. When using an existing WSAM role configuration originally setup for Windows PC users to provide secure access to defined applications for Pocket PC users also, please ensure that the list of Destination Hosts defined within the role is within 1500 bytes in length. Very large list of destination hosts will likely freeze WSAM launch on Pocket PC devices due to memory buffer constraints. (28457)

Java Secure Application Manager (J-SAM)

1. Outlook 2003 is not supported with J-SAM. The workaround is to use W-SAM or Network Connect. (8251)
2. When using a static loopback address for a J-SAM application server configured on multiple ports, modifying that loopback address requires the admin to delete all applications referring to this application server and re-enter these applications with the new static loopback address. (22911)
3. If the Network Protocol setting in the Citrix Program Neighborhood client is set to “TCP/IP,” then the application is not supported through J-SAM. This is because the “TCP/IP” setting produces UDP traffic. (23997)
4. When running J-SAM on a MacOS 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.
5. 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; };
```
6. J-SAM does not automatically launch when Embedded Applications are set to “Auto” in the Citrix NFuse Classic Administrator console. In these cases, we recommend you configure J-SAM to launch automatically after signing in. Otherwise, users must manually launch J-SAM before using Citrix NFuse.
7. When using SAM (both 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.
8. Due to a buffer overflow issue in Windows 98, J-SAM cannot support more than 10 simultaneous

applications when launched from a Windows 98 client.

9. With Citrix Program Neighborhood, application discovery (with a specified server), is supported; however, if a user attempts to use the server discovery feature, which does not work through the IVE, and then attempts to use the application discovery again, the application discovery will fail. The workaround is to restart Citrix Program Neighborhood. (8665)

MacOS Java Secure Application Manager (J-SAM)

1. If the custom company logo image uploaded to the IVE is a .bmp file then the image will not display correctly on the JSAM window on a Mac OS X. (25831)
2. J-SAM doesn't automatically exit on a Mac OS X when a user signs out of the IVE. (24905)
3. 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)
4. 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)
5. Citrix NFuse integration is not available on MacOS using the Safari browser. (10780)

Network Connect (NC)

1. Admin tries to modify a connection profile, and the connection profile in question was (or is a duplicated version of) one that was automatically created during upgrade to version 4.2 of the IVE, and has since not been modified. The workaround is to create a new connection profile, instead of modifying an existing profile. This issue will be fixed in a maintenance release that will be available shortly. (28250)
2. Graphical Identification and Network Authentication (GINA) functionality within Network Connect 5.0.0 is not currently integrated with Host Checker and Cache Cleaner. If either is enabled, GINA-based Network Connect launch does not work.
3. There is a known issue with the Network Connect standalone client and a login URL that has a custom start page enabled--Network Connect does not automatically launch on the client despite the auto-launch setting on the server being enabled. (25151)
4. Macintosh OS support issues (27126):
 - i. On Mac OS X 10.2, Safari doesn't support authenticated proxies or PAC files at all. Network Connect will not modify proxies on Mac OS X 10.2, so the client will always use whatever client-side static proxy is configured.
 - ii. On Mac OS X 10.3, Safari doesn't support authenticated proxies returned from a PAC file. This limitation affects users of Network Connect because Network Connect's proxy selection function depends on rewriting PAC files. To solve this problem, we developed a browser plugin for Safari which adds support for this proxy configuration to Safari. While Network Connect tries to install this proxy support automatically, Safari can sometimes get out of sync with the plugin. If you experience problems using Safari when connecting with Network Connect and an authenticated proxy, quit Safari, restart Safari, and click the Home button on Network Connect's status window once connected with Network Connect to manually install the plugin.
 - iii. Mac OS X 10.4 supports all the proxy settings Network Connect requires, so no special user action is needed.
5. Safari may not respect the new proxy settings introduced by Network Connect immediately after Network Connect is started. Restarting Safari will cause Safari to begin using the new proxy settings. (27090)
6. 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)
7. 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)
 8. Either the Checkpoint VPN client or the Checkpoint SSL VPN Extender client blocks the Network Connect 5.0.0 Virtual Adapter. Network Connect only installs and launches properly after both of these applications are uninstalled. (26282)
 9. When a Linux DHCP daemon is used as a DHCP server behind the IVE, a user might get different IP addresses assigned to them from one session to another.
 10. Juniper's Network Connect adapter does not appear as an adapter in the Local Area Connection properties as long as no Juniper Network Connect session and connected. (27561)
 11. When a server-side PAC file is defined, and Network Connect Split-tunneling is enabled, the IP address for the PAC source or the internal proxy should be part of the network or IP addresses defined within the Split-tunneling configuration. (26981)
 12. When Juniper's GINA is enabled, GINA does not install if it detects the presence of any other GINA on the client system. This is a design decision for the first version of GINA integration. (26399)
 13. When upgrading the client from prior versions of Network Connect to version 5.0.0, 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. The user should uninstall Network Connect from within Control Panel -> Add/Remove Programs. (25958)
 14. Network Connect GINA is installed on both Domain and Non-Domain machines. Juniper currently does not verify whether a computer is a Domain computer or not, prior to installing GINA. (25509)
 15. In some cases, upgrading the Network Connect client may require the user to manually delete NeoterisSetupControl from the Internet Explorer browser cache. (26971)
 16. When upgrading Network Connect to version 5.0.0, occasionally a client generates a "Driver Installation Fails" error. When this occurs, it is most likely due to the following: (27410)
 - a. "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce" is missing or has been renamed.
 - b. Manually re-creating the RunOnce registry key will fix the problems. In version 5.1, we are performing an automatic check on the client.
 17. There are known issues with occasional Network Connect "disconnections" and "failed reconnections" when a VIP fail-over occurs in an Active/Passive or Active/Active cluster. (27388)
 18. When Network Connect Resource Policy ACLs are configured on the gateway, pay particular attention to what the Resource Policy allows. Any sort of DNS calls that need to be made for name resolution should be a subset of this ACL. In past releases, Juniper employed an implicit ACL for DNS servers, and didn't have to be explicitly defined in the Resource Policies, but in 5.0.0, this has changed due to the AAA architecture being redesigned. (26385)
 19. There could be some isolated instances where if "Detailed Logging Policy Rules" are employed for a particular user, that user's actions might not get logged. This has only happened with a single user account within Juniper Quality Assurance, and we haven't been able to reproduce this beyond this one user. This is being investigated. (25194)
 20. When Network Connect is launched using Firefox 1.0.2, a "restricted" user might have problems starting Network Connect using Sun JRE versions 1.4.1_02, 1.4.2_08, and 1.5_02. The workaround is to utilize Internet Explorer on these restricted machines. (26728)

21. When using Network Connect on Mac OS X 10.2.8 with Safari 1.0.3, Network Connect launches successfully. In some cases, however, the web page does not redirect back to the user's SSL-VPN home page. Users must manually click on the redirection link on the application launcher intermediate page. (27538)
22. If the administrator has specified the Realm selection as "User types in Realm Name" on the login page, this functionality does not work with the Juniper Network Connect GINA-based launch. (27515)
23. Once a tunnel has been established to the Juniper SSL-VPN via the interactive GINA-based launch, if the user does not log into their local machine using the correct Windows credentials, the tunnel could stay up until the session timeout is reached. (27413)
24. When Network Connect is used on Redhat Linux 9.0, or other Linux flavors, clicking on the "Uninstall" link for Network Connect within the User -> Preferences page actually starts Network Connect. The workaround is to uninstall Network Connect using the command-line uninstaller. (27360)
25. In a particular isolated scenario, a user's web session with the IVE could continue even though the user has logged in from other locations. For example, the user signs in from Linux client 1 and establishes a successful Network Connect session. Then, the user logs in from client 2 with the same credentials. The user then refreshes the first Linux client session. The user's Bookmarks page stays open while the Network Connect application closes (due to second login). This is an issue only on Linux machines, and will be resolved in the next release. (27359)
26. No Standalone version of the Linux installer is available in the 5.0.0 version. All installation should be done over the Web. (26566)
27. Network Connect does not currently launch using a Firefox Browser if a Web proxy or a PAC is configured within Firefox. Internet Explorer should be used as a workaround. (24876)
28. Proxy exceptions and protocol-specific proxy settings within the Firefox browser are not evaluated when used with Network Connect 5.0.0. If proxy exceptions and protocol-specific proxies are required, Internet Explorer should be used instead of Firefox. All Windows components except Host Checker will not be able to support IVE in the Proxy Exception list in the 5.0 timeframe. This will be resolved in Release 5.2. (26489)
29. Juniper Network Connect 5.0.0 does not support the use case where a customer has both a PAC file pointer and a manual proxy enabled on the same Internet Explorer or Firefox browser. Only one proxy configuration should be set up on the browser at any one time. (26267)
30. Users could occasionally see an error message "Insufficient Privileges" or "user does not have Admin privileges" when upgrading or installing their Network Connect client. If this occurs here is a workaround for the issue: (26476)
 - a. Clear "C:\Documents and Settings\\Local Settings\Temp"
 - b. Clear "C:\Documents and Settings\\Local Settings\Temporary Internet Files"
 - c. Run the Uninstall command from the Start->All Programs->Juniper Networks->Network Connect 5.0.0
31. Due to the source IP address being the Network Connect assigned IP, the Roaming Session option should be enabled for the user's role (on the Juniper SSL VPN Admin Console) when the hostname of the IVE resolves to the internal IP when on the LAN and to the external IP when on the Internet. In this case, Host Checker and Cache Cleaner attempt to speak to the internal interface as they resolve against the internal DNS through the Network Connect tunnel. (Split-tunneling should be disabled.) (26845)
32. When an existing Network Connect session is established, adding a PCMCIA enabled Wireless card to a laptop will break the NC connection. (27522)
33. When Network Connect has already been installed on the client, and the user tries to install the standalone installer, a cryptic error is output: "Error opening file for writing: c:\windows\downloaded program

- files\Neoteris_Setup.ocx". Please make sure not to uninstall Network Connect prior to running the Standalone installer for Network Connect. (27519)
34. When a user "Exits" from Network Connect using the "Right-click->Exit" functionality on the System tray icon, the user should wait at least 10 seconds before re-initiating the Network Connect session (26479)
 35. The supported scenarios for NC are valid only when single client PC NICs are used throughout the NC connection. Any scenario involving switching NICs might work, but is not guaranteed. The recommended behavior for the customer for switching NICs would be to end their session, switch the NIC and then restart NC again. This is especially important when not using software such as the IBM Access Connection Manager that has a clean solution for switching to an enabled NIC. (22806)
 36. If the client PC's web browser proxy is set to use a PAC script with a hostname:port, and not just a hostname, NC will not behave as expected. Using just the hostname, or an IP:port, works. (23184)
 37. If a Restricted user has Network Connect installed on their system, Network Connect can only be un-installed if a user with Admin privileges attempts to run the un-installer, or the Installer Service is installed. (22200)
 38. When accessing a resource on the remote network (behind the IVE) that is on a different subnet from the IVE internal interface, the remote machine/server may not know how to route back to the client IP network that the IVE issued from its configured IP pool. To work around this, add a static route to the router between the internal interface's network and the remote network. This static route will route packets destined for the IVE's NC IP Pool to the IVE's internal interface.
 39. The NC Client IP pool UI 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 NC IP Pools with a more standard syntax (for example, IP/Net mask). (6378)
 40. Client IP pool configuration is synchronized among all nodes in a cluster; however, administrators may configure each IVE to use a certain subset of the global IP pool. Configure the client IP pool in the Network Settings > Network Connect tab, using an IP filter match.
 41. Network Connect may not install properly if users are running pop-up blocker software. In some instances, the symptoms may include unusually high CPU usage, and will require that all browser sessions be terminated.
 42. Users with only "Guest User" privileges will not be able to run Network Connect. Furthermore, Guest Users cannot un-install Network Connect. Any attempt to do so may only partially un-install Network Connect and could leave some files behind, resulting in a corrupted Network Connect installation.
 43. Network Connect is available to the IVE Admin as a stand-alone executable (NCInst.exe). This executable can be installed on the client and started by logging into the IVE and invoking Network Connect. If the user attempts to install NCInst.exe on a client that already has the same version previously installed, multiple error pop-ups occur, with the text "Error opening file for writing..." The user can safely click on Ignore on these pop-ups and NC should work after the installation has completed.
 44. When launching NC with non-Admin access on a Mac, the user will see an error saying that "Safari cannot find the Internet plug-in". This error can be ignored and will have no side effect unless Safari is configured to use an authenticated proxy. In the latter case, Safari may not work once NC is launched successfully, due to a Safari bug with authenticated proxies. (27781)
 45. The server-side setting under "Configuration -> NCP" for "Read Connection Timeout" goes blank after an IVE upgrade. This is a known issue. Please make sure that you set the default value of "120" or an alternate value if you feel it is necessary. The default value should suffice in most cases.
 46. The server-side setting under "Configuration -> NCP" for "NCP Auto-Select" occasionally goes into a Disabled state after IVE upgrade. NC does NOT work when NCP Auto-Select is set to Disabled. Please

re-enable it before allowing users to connect.

Administration

1. If no bookmark name is provided when creating the bookmark, it may cause the bookmark sorting to insert erroneous characters. (27938)
2. HTML tags may cause the collapse/expand function of the notification message to be inoperable. If this situation occurs, remove the HTML tags. (22264)
3. Logs (Events Log, Users Access Log, Admin Access Log, and Network Connect Packet Log) are not automatically moved to the new version when upgrading. The logs are, however, still available when rolling back to the original version.
4. Log filtering requires a wildcard character to be surrounded by double quote marks (“*”).
5. When user fail to authenticate, the log message may not have the correct IP address that is associated with the source request. (26652)
6. In serial console access mode, the `-b` feature for pinging a broadcast address in network troubleshooting is not available. (21903)
7. In number of active user statistics, the exact count is computed every hour. However, within the sampled period, the system does not subtract the users who drop off and will show a discrepancy in the actual active user vs. the recorded active user. (24775)
8. Depending on the switches, when the network interfaces are configured to be 100 mbps, the network throughput may suffer. Please maintain “auto” as the best configuration for the NIC. (24724)
9. When the disk storage space on the IVE becomes limited, upgrading to the new version may result in a failure to verify the new package. Please remove system snapshots, debug information, and other unnecessary information, and retry the operation. (22455)
10. There may be conditions where FIN packets that are destined for one interface (external or internal) can be found on the opposite interface. However, there are no security issues, because these are FIN packets only. (25095)
11. Roll back for clustering does not validate that the rolled back version of all cluster nodes are the same. Therefore, manually verify that all nodes have the same roll back version before commencing the operation.
12. In Firefox/Mozilla, Log Setting in-line editing does not work. To work around, delete the entry and re-add the information.
13. The log setting in-line editing will not function unless a Central Manager License is installed.
14. In case the system is unresponsive, there are additional debugging tools available through the serial console:
 - BREAK-8 to turn the log level to 8
 - BREAK-T to create a process dump
 - BREAK-B to reboot the machine

Clustering Issues

1. If a network problem causes a node in a cluster to lose communication with other nodes, but other nodes can reach (“see”) that node, then cluster synchronization will fail. Network administrators should confirm connectivity using ping and traceroute tools, available from the IVE troubleshooting menu. (18112)
2. In an Active/Passive scenario, using the default cluster/network configuration, under heavy load, Administrators may see the VIP switch back and forth among the two nodes every 6 to 8 hours. If this

- occurs, the Administrator may increase the ARP timeout value from the default 5 seconds to 10 seconds.
3. When using Virtual Ports in a non-cluster configuration, or when creating an Active/Active cluster while using an Active/Passive cluster configuration the joined nodes will lose their Virtual Port IP address information and will need to be manually reconfigured using unique IP addresses.
 4. When an Active/Active cluster is converted to an Active/Passive cluster, Virtual Port configuration will be copied to the backup cluster node from the node to which the Admin is making the change. This copy will cause Virtual Port configuration on the backup node to be overwritten with the master's Virtual Port configuration.
 5. In the case of a failover (both in Active/Passive and Active/Active configurations), all transactions currently in progress (such as telnet or SSH sessions or large file downloads/uploads) need to be restarted after the failover; there will not be a seamless failover for ongoing transactions using sockets (except for HTTP requests or non-stateful connections).
 6. When an IVE in an Active/Passive cluster loses network connectivity, it automatically moves into a temporarily "Disconnected" mode. In this mode, the IVE will relinquish a cluster VIP (if applicable), and stops servicing end-user requests for a few minutes. The IVE determines the status of a network connection based on both the carrier signal, and on connectivity to the Gateway by sending an ARP request. Therefore, we strongly recommend that you configure a highly available network gateway on the IVE, preferably using VRRP-based Primary/Backup Gateway configuration. When the network connectivity is restored, the IVE automatically joins the cluster.
 7. When deploying large clusters in a multi-site environment and the connectivity between nodes is unstable, a node joining the cluster may get stuck in a synchronization loop until it gets fully synchronized with the other nodes. During this time, the node will show as "transitioning" in the Cluster Admin UI. When this occurs the IVE will be unable to service end-user requests. If the node remains in this state, the Admin may consider rebooting the node, and then during its initialization, use the clustering options to remove it from the cluster. The node can then rejoin the cluster after the network connectivity between nodes has stabilized. (21479)
 8. In an Active/Passive Cluster Pair failover situation, the active IVE sends a gratuitous ARP request in the network indicating the new owner for the cluster virtual IP address (VIP). Some switches and firewalls may not respond to Gratuitous ARP requests and therefore still might try to contact the offline IVE. The workaround is to manually clear (disable) the ARP caches on these external devices or configure an Active/Active IVE cluster configuration using an external load-balancer.
 9. If you are deploying an Active/Passive cluster in the DMZ mode, please make sure to configure/enable the external interfaces on both machines before assigning an external VIP to the cluster.
 10. IVE system log messages are not synchronized during a Join Cluster operation even when the "synchronize log messages in a cluster" option is enabled. The log messages are synchronized across the IVEs in a cluster when all the machines are in "Enabled" and Status "OK" mode.
 11. Changing the network settings of an enabled cluster member (in particular, network routes and DNS settings) does not work in some rare cases. We recommend that you disable the cluster member, change the network settings, and then re-enable the cluster member in this scenario.
 12. You should avoid using the "multicast" synchronization method for Multi-Unit Clustering when the IVE is under heavy load (either from heavy traffic or a load test). During these periods, unicast is the preferred method of cluster synchronization.
 13. When creating an Active/Passive cluster, the administrator must enter values for both the *internal* and *external* interfaces. This is not a mandatory field, but is required for Active/Passive clustering.
 14. The minimal downtime cluster upgrade functionality is only supported AFTER the cluster has been migrated to version 4.0. Subsequent upgrades will then be able to take advantage of this functionality.
Note: The minimal downtime cluster upgrade functionality is only available with Central Manager and in

clusters of two nodes or more.

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

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

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

16. Clustering is not supported when an IVE is configured to have the same subnet for both the *internal* and *external* interfaces.
17. In an Active/Passive cluster, if the nodes lose communications with each other but not to their respective gateways, then it is possible for each IVE to activate the VIP. This can cause a problem since the upstream switch/router/firewall will potentially receive two gratuitous ARP requests. The second ARP request will override the first. If the two nodes regain communications afterwards, one node will deactivate its VIP. If this node is the one which sent the second gratuitous ARP and is therefore in the switch/router/firewall's ARP cache, end-user connectivity to the VIP could be lost as the ARP cache will be redirecting requests to the wrong MAC address (wrong IVE). To resolve this situation, the IVE Administrator may click on the "Failover VIP" button in the Clustering UI. This will automatically fail the VIP over from the active node to the backup node and thus send a new (and only one) gratuitous ARP request. To prevent this from happening, IVE Administrators are encouraged to ensure all IVE nodes have constant communication with each other and that the network segment(s) between them are never severed.
18. In an Active/Passive cluster with both internal and external interfaces enabled on each node, if the external gateway is unreachable, the external VIP will not fail over. Administrators should ensure gateways are reachable – either by using the ping tool in the IVE, or monitoring the logs to look for "external gateway unreachable" entries.

Sun JVM/Code-Signing Certificates

1. In WRQ versions 6 and 7, the WRQ administrator console is not supported through the Java rewriting functionality. (27881)
2. The TN 3270 WRQ 7.0 applet is not supported through the IVE. (26690)
3. A security setting of "Accept only TLS V1" option is not supported for Java applet rewriting over Sun JVM. This is due to a bug in Sun JVM. (25146)
4. IBM Host on Demand is not supported through the IVE rewriter because the Java applet performs an MD5 checksum upon execution. Alternate methods to secure this application are J-SAM or W-SAM.
5. When importing a new production certificate for Sun JVM, the end-user needs to disable caching in the Java Plug-In in order for the newly imported code-signing certificate to appear. Please refer to the Administration Guide for instructions on disabling the Java Plug-In cache.
6. If users delay in responding to the web server security warnings then Java applets may not load. This includes J-SAM and the Secure Terminal Access applets. As a workaround when the end-user encounters the web server certificate dialog, the end-user should select the "Always Trust" button. Once the user selects "Always Trust", the dialog will not appear and the applets will load without a problem. Note: Due

to a built-in timeout in the Java Plug-In, if the user waits too long to select the “Always Trust” option, the applet may not load properly. (8396)

7. Due to a bug in Sun JVM, when users close their web browser window, it may seem to timeout. To prevent this problem, users can make the following changes to their Java plug-in: Open the Java plug-in console (Control Panel → Java Plug-in) then under the Advanced tab, type: **-server -Xint -Xfuture** in the Java Runtime Parameters box and press Apply. Close the Java Console and Restart the web browser.
8. With Sun JVM 1.4.2, if caching is enabled, WRQ 6.0 will not load properly. (14008)
9. The policy tracing logs that result when code signing certificates are used to re-sign Java applets are not accurate. Use the Simulation tool instead, for troubleshooting purposes. (17411)

Customizable Sign-In Pages

1. If a pre-5.0 Softid or Kiosk zip file is used, please follow the steps to customize it for 5.0 R1 release (28075):
 - Unzip the old zip file
 - Delete the LoginPage-ppc.html
 - Edit the LoginPage.html to add the following text as the very FIRST line:
<%# NetScreen Page Version 1001 %>
 - Edit the LoginPage.html to add the following snippet anywhere in the page, except in a comment:
<% IF 0 %>
<% prompts %>
<% END %>
 - Zip up all the pages and associated objects
 - Upload this zip file
2. To make sure that the New Pin and Next Token pages are customized for SoftID authentication, the administrator should copy the file NewPin.html to GeneratePin.html in the softid.zip and upload the modified zip to the IVE for the custom sign-in page.
3. The total combined size of all uploaded customizable UI zip files cannot exceed 12MB.
4. The new 4.X sign-in pages now offer additional customization for labels and informative text. By default, the text strings are in English. Administrators supporting non-English users may need to configure the sign-in pages to provide localized text labels. This can only be done on a per-sign-in page basis. For multi-language support, Administrators must configure different sign-in pages for different locales. For further customization, Administrators may upload their own customized sign-in pages using the Template Toolkit. Please contact Juniper Networks Support for details (<http://www.juniper.net/support>).
5. When creating customizable sign-in pages, Administrators should remember to save them as UTF-8. (17211)

FIPS

1. If you replace an administrator card using option 10 in the serial console after upgrading an Access Series FIPS appliance, the Security World is modified to use the new administrator card. If you then try to perform a “rollback,” the new administrator card will not work. This is because the “rollback” reverts to the original Security World, which is not yet configured to use the new administrator card. To use the new card, you must use option 10 on the serial console once again.
2. Access Series FIPS does not support automatic time synchronization across cluster nodes. We suggest that you configure your cluster nodes to use the same NTP server - so they are synchronized. If the cluster nodes are not synchronized, time-based features such as Secure Meeting, will not function properly.

3. If the HSM module switch is set to I on a FIPS-enabled Access platform, the machine is in "initialize" mode. A reboot during this time will reinitialize the server key and invalidate the server certificate that is currently loaded. Administrators should be sure to leave the switch at O during normal operations (as per the instructions on the serial console and documentation).

Pass-Through Proxy Issues

1. The Lotus iNotes welcome page is not rewritten if the IVE is intermediating the content through Pass-Through Proxy. (9236)
2. Pass-Through Proxy URLs must be hostnames. Paths of hostnames are not supported.
3. Juniper Networks strongly recommends that Administrators not mix Pass-Through Proxy Port and Host modes.
4. Siebel7 is not supported through Pass-Through Proxy.
5. Using Mozilla with Pass-Through Proxy (with the IVE port configuration), the IVE may invalidate the user session causing the user to have to login again.
6. Pass-Through Proxy is not supported on Netscape 7.0, but is supported on 7.1. (7290)
7. When using Lotus iNotes through Pass-Through Proxy, if an XML rewrite is needed, administrators are encouraged to either enable XML rewriting in the Pass-Through Proxy configuration, change the default cache rule from 'No-Store' to 'Unchanged', or add a new cache rule with the IP/hostname of the Lotus Server and a path of * and value 'No-Store'.
8. When using OWA through Pass-Through Proxy, if a user replies to or creates a new email, the recipient may receive a JavaScript error if they view the email through their Outlook client. (9233)

Internationalization Issues

1. With localized Pocket PCs, such as the Japanese Pocket PC, the locale is not sent in the HTTP header, and thus the IVE is unable to detect which language to return, so English is returned by default. (22041)
2. Internet Explorer may truncate the Japanese filenames if they are too long. Additionally, some Excel files cannot be saved. More details can be found about this non-IVE issue at: <http://support.microsoft.com/?kbid=816868>. (14496)
3. The timestamp function of the IVE may not be in the same format as what is expected when working with the Japanese user UI. The formatting for the IVE is as follows: *hh:mm:ss (am/pm)* and *month/day/year*.
4. When using Netscape 4.7 and the Japanese language setting, the default font may incorrectly display characters and words on the End-user UI page. If this happens, you can change the font setting in Fonts section of the Netscape Preferences, where you can select the option "Netscape should override the fonts specified in the document".
5. With Secure Meeting, when using a Japanese language setting on the IVE, Meeting Invitations will be sent out using the Japanese template. If these invitations are sent to Yahoo or Hotmail or other web-based email accounts, some characters or possibly the entire email may not display correctly.
6. Special characters such as ①, I , ¥, and ~ are not supported in filenames for UNIX Servers.
7. Japanese characters are not supported in naming Authentication Servers.
8. Filenames using 5c characters such as 表 and 工 will be corrupted and cannot be deleted from UNIX servers.
9. Some of the Diagnostics content in W-SAM are not localized and will always be displayed in English. (22068)
10. Network Connect is supported on Linux English OS only. (24584)

11. In a Host Checker Policy, the Admin should enter Registry Settings rule settings in English. (25097)
12. W-SAM is supported on English Pocket PC only. (27221)
13. On Mac OS X Simplified Chinese system, Secure Meeting client comes up in Traditional Chinese. (27675)
14. On Mac OS X Simplified Chinese system, J-SAM client comes up in Traditional Chinese. (27675)
15. On a Simplified Chinese system, help pages from the Secure Meeting client will be in English. (27848)

File Browsing Issues

1. Session termination does not affect file transfers through Windows file share. (26897)
2. When opening a file in the Japanese locale the URL displayed in the Internet Explorer title bar and the URL bar is garbled. The file when viewed is displayed correctly. This is due to a bug in Internet Explorer. (19612)
3. Depending on the web browser, downloading files with filenames of length 18 to 25 characters may not work, through the IVE. Files with longer or shorter filenames are OK.
4. If administrators deny access to a file server by specifying the IP address, users can still browse to that server if they specify the server and the file share by name and are able to provide valid credentials. To avoid this, administrators should configure both the IP address and hostname in their file browsing ACLs.
5. The IVE attempts to connect to Windows file shares on port 445 first. If port 445 is blocked, the IVE may seem to hang for ~20 seconds, after which it will reconnect to the file share using ports 138 and 139. Administrators with a firewall between the IVE and a file server are encouraged to open port 445 up from the IVE to the file share servers to avoid this “hang”. (13394)

SiteMinder

1. When using SiteMinder as an Authentication server for the IVE, users must access the IVE using a fully-qualified domain name (for example, ive.company.com). This is required because the SiteMinder SMSESSION cookie will only be sent for the domain it was configured for. If users access the IVE using an IP address, they may get an authentication failure and will be prompted to authenticate again.

XML Export

1. **XML Export is a Beta quality feature in Release 5.0 R1. XML Import and Push Configuration are not available in Release 5.0 R1.**
2. On certain browsers, following XML Export, if the admin clicks “OPEN” instead of “SAVE” in the dialog box that appears, the operation fails with error message “THE PAGE CANNOT BE DISPLAYED”. The workaround for this problem is to save the exported file and then open it. (27329)
3. In performing XML export of realms, if “Administrator Realms” are selected for export but User Realms are not selected for export, the expected behavior is that only Administrator Realms will be exported. However, currently, User Realms also get exported. (26569)
4. XML Export of Custom Sign-In pages is not supported (26658)
5. The following options are present in the administrator user interface but not supported by XML Export: (27555)
 1. Roles -> General -> Overview -> Source IP
 2. Roles -> General -> Overview -> UI options -> Start Page -> “Allow access to directories below this URL”
 3. Roles -> General -> Overview -> UI options -> User Toolbar -> Session Counter
 4. Roles -> General -> Overview -> UI options -> User Toolbar -> Client Application sessions

5. Roles -> General -> Overview -> UI options -> Help page -> "Allow access to directories below this URL"
 6. Roles -> General -> Overview -> UI options -> Browsing Toolbar. All options except "Toolbar Type" and "Logo", are missing
 7. Roles -> Web bookmarks -> Auto-allow. "Only this url" and "Everything under this url" are missing
 8. Roles -> Network Connect -> Auto Uninstall and all GINA options are missing
-
6. XML Export of Network Connect filters in the Network Settings is not supported. (27694)
 7. XML Export of WINS Enable Network Discovery option is not supported. (27696)

Miscellaneous issues:

1. There is a casing error in the parameter name for Terminal Services Launcher. The bookmark name parameter should be *bmname* instead of *bmName* as documented. (27720)
2. In a customer network where you can simultaneously access two separate Juniper SSL VPN devices, one with a client application such as WSAM, Windows Terminal Services, or Network Connect, and the other with access to a web application, you can inadvertently terminate a session on one system when you logout from an application on the other system. Currently, we do not pass the host information from one application to another when a user logs out from one of two simultaneously connected client applications on two separate VPNs. (27697)
3. All Error and Informational messages within Windows Secure Application Manager and Network Connect contain an "Error Code" string. This "Error Code" string acts as an identifier for either the error message or the informational message and can be cross-referenced with the end-user online help to get "cause" and "action" information for the message displayed.
4. On the Preferences > Applications page for end-users, there are links to uninstall applications even if those applications are not installed or available on the client PC (such as if they are not using a Windows PC). (22978)
5. When using FTP Archive, if the Admin selects "clear log after archive", the logging system may behave unexpectedly and new log entries will not be displayed. To resolve, the Admin may clear the log manually. This will be fixed in a future release. (23093)
6. For the Customizable Help Link, the Administrator must specify a pre-rewritten URL (a URL which was rewritten through the IVE already) if he wishes to link to an internal (rewritten) server which contains the help information. The alternative is to link to an external URL, which must be accessible by end-users without going through the IVE. (22552)
7. With FireFox 1.0, the Collapsing/Expanding of the Admin Hierarchical menus works; however, the icon "-" does not change to a "+" as the Admin would expect. (22665)
8. If you use a multi-valued attribute in the bookmark name, only the first value is displayed for all the expanded bookmarks. (21629)
9. If the Admin submits some change and then closes the Task Guide or presses Back in the browser window, he may receive a prompt to repost form data. If this happens, the Admin may click cancel, and then Back. This is because closing the Task Guide, or pressing Back after some other submitting another page is equivalent to reloading the previous page, which was a submitted form. (22039)
10. Importing the system config does not import SSL Intermediate CA Certs (chains). (21040)
11. 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)
12. 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)

13. Juniper Networks recommends that to uninstall client applications (for example, NC, W-SAM) you use the Un-install link of the Un-installers UI under Preferences > Applications. (20415)
14. The OpenWave Simulator only supports making an SSL connection if the server, or in this case the IVE, is signed by one of the following RootCAs: CyberTrust, Certicom, Diversinet, Entrust, GlobalSign, or VeriSign. (18041)
15. With log filtering, when using the *role* variable, the value must be contained within double quotation marks, for example: `role = "Users"`.
16. When using the serial console troubleshooting tools, such as ping, if the tool becomes unresponsive, press CTRL+C to terminate the tool and go back to the menu.
17. Web Server SSL Certificates issued by the IPSAC root are not supported by the IVE. SSL Certificates of the Netscape format must include the SSL Server Bit set in the "Netscape Cert Type" extension. Key Usage, Extended Key Usage, and Netscape Cert Type are all required for these certificates to work properly.
18. When upgrading to 4.1.X+ and using a temporary license generated for IVE 3.3, after the upgrade, the license time remaining may show incorrectly. To resolve this, please contact the Support department. (17918)
19. NFS Auto-mount is not supported on Linux NIS/NFS servers, only on Sun servers. (2005)
20. In some locations throughout the Admin UI, drop-down select boxes may disappear during navigation through the left-hand hierarchical menu system. To make these select boxes reappear, simply move your mouse off of the left-hand menu. (17934)
21. By default, all access policies are closed, unless explicitly opened by a defined policy (for example, 'allow' for '*').
22. Due to lack of support in Microsoft Windows for certain SSL libraries, the best practice recommendation for the IVE is to configure any user roles to use non-optimized NCP for Windows NT, Windows 98 SE, and Windows ME clients when using W-SAM, Network Connect, or Secure Meeting.
23. When defining access policies, the Administrator must explicitly list each hostname and/or IP address. The policy checking system will not append or use the default domain or search domains in the IVE network settings. (13685)
24. PowerPoint files may not display properly with Office 2002 in Internet Explorer on Win2K. To work around this, administrators should have their end-users install Office 2002 SP1 and SP2.
25. The ARP Ping Timeout value in the Network Settings should always be greater than 0, else network connectivity may behave unexpectedly.
26. Multiple sessions from a single client to the same IVE might cause unpredictable behavior and are not supported. This is primarily due to the pre-authentication mechanisms which might conflict between sessions. This caution also applies to situations where an end-user and admin session to a single host occur simultaneously.
27. The following URL contains a list of characters which not supported for filenames or folders for Samba Servers: <http://support.biglobe.ne.jp/help/faq/character/izonmoji.html> (14529 and 14348)
28. When using 168-bit encryption on the IVE, some web browsers may still show 128-bit encryption (the gold lock on the browser status bar) even though the connection is 168-bit. This may be a limitation of the browser's capability.
29. The IVE supports web proxies that do NTLM authentication. However, the IVE does not support the case in which there is a proxy between the IVE and the backend server, and the backend server performs the NTLM authentication. (26144)
30. On some Administrator console pages, changing one or more parameters causes multiple log messages to

appear in the IVE system log that indicate that all the parameters are changed. However, this occurrence does not result in any incorrect behavior.

31. When upgrading from a 2.x release, the Web Proxy function may be disabled even if it had been enabled prior to the upgrade. Administrators who want this function to be enabled must manually re-enable it after upgrading. (7965)
32. Netscape can freeze when users close Secure Terminal Access (STA). To work around this problem, users can add the following line to their java.policy file: **grant { permission java.security.AllPermission; };**
33. 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.
34. 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.
35. When using Internet Explorer 5.5 or 6.0 and compression, HTTP objects will be cached, regardless of the object's cache settings. This is not a limitation of the IVE, rather an issue specific to Microsoft Internet Explorer and HTTP compression. For more details, please visit: <http://support.microsoft.com/default.aspx?scid=kb;en-us;321722>
36. The IVE web browsing function does not support URLs of more than 159 characters in length, including extensions, such as ".html".
37. On a Mac, the IVE toolbar should be disabled to view OWA pages with the Safari browser. If the toolbar is enabled, the Inbox may be blank until the page is refreshed once. To work around this, the toolbar can be disabled in the Roles → UI Options tab.
38. Even though you enter the password to archive users and system config files, the IVE disregards this password on the import.
39. If you enter a server for selective rewriting, and expect it to be accessed with and without the domain suffix, please enter both entries. If you have entry foo.company.com and try accessing foo, the response will not be served via pass through proxy. Similarly, if you have an entry for foo and try accessing foo.company.com, the response will not be served via selective rewrite.
40. When switching from Optimized NCP (NetScreen Communication Protocol) to Standard NCP, or vice versa, all NCP- Based communications must be restarted. This includes W-SAM, Network Connect, and Secure Meeting.
41. On Win98 clients, when Auto-Select is enabled for the NetScreen Control Protocol (NCP), the Optimized NCP will not be used. This should not cause any visible changes to the user experience. (10881)
42. When using OWA 2003, if the IVE has Forms-based Authentication enabled, the OWA 2003 login credentials are cleared upon logout; however, if this is disabled, the login credentials will not be cleared.
43. When using OWA 2003, the Administrator should ensure that the OWA server has only NTLM or Basic Auth enabled, not both. However, Juniper recommends enabling at a minimum NTLMv2 or Kerberos-based authentication.
44. When importing a custom HTML help file for end-users, if the file is encoded in a different language, for example Shift_JIS it must be converted to UTF-8 before it is imported by the IVE administrator. (10839)
45. When using Microsoft NetMeeting with W-SAM, hosting a meeting is not supported. To join a meeting using Win2K, there are now problems; however, when using Windows XP, application sharing does not work as expected. In order for Windows XP users to work around this sharing issue, they must first check the configuration box "Only you can accept incoming calls".
46. Upgrading the IVE clears all statistics; however, if the log system is configured to log statistics every hour, they will still be available in the log file, even after the upgrade.

47. When an Admin IVE session is timed out (due to inactivity or by reaching the hard limit), the “sign in again” link may take the Admin to the end-user sign in page instead of the Admin sign-in page. The Admin can simply type the Admin sign in URL (for example, /admin) to sign back into the IVE Admin Console again.
48. The Session Timeout Warning is only supported if the user is viewing web pages through the IVE (rewritten web pages) or the IVE homepages themselves. It is also supported if the user is running J-SAM. The warning is not supported with W-SAM or Network Connect. We recommend that the Session Timeout Warning feature be disabled to minimize confusion for users of W-SAM and NC.
49. After upgrading to 4.0 from 3.X, the Admin UI may be using a cached style sheet. Pressing CTRL+F5 on the web page should resolve this caching issue.
50. When the Administrator reduces the maximum size of a log file on the IVE, if the log is already larger than the new maximum size, the log size will show a larger % value on the Status page under “Logging Disk % full”. As soon as another log message is generated for that log file, the current log file will be archived and a new log file will be created. The display is momentarily incorrect due to this change.
51. If two separate web browser instances are accessing different versions of the IVE, then the browser may prompt the user to reboot their PC after the NeoterisSetup.cab has been downloaded. Upon closing all browsers and logging in again, the prompt will no longer be displayed.
52. There are known issues with Microsoft's Popup blocker being enabled and certain OWA 2003 scripts not being able to run when being accessed through the IVE. Users could see "Script" errors in this case. Juniper Networks recommends that Popup blockers be disabled and that the user refreshes their OWA session after disabling the Popup blocker. Additionally, Popup blockers may cause problems with other IVE functionality which uses a pop-up, for example File Uploads, online Help, or on the Admin Console, the IVE Upgrade progress window, Dashboard configuration page, and Server Catalog configuration pages. (23092)
53. The Debug Log troubleshooting functionality should only be enabled after consultation with Juniper Networks Support.
54. The IVE has an Automatic Version Monitoring feature which notifies Juniper Networks what version of software the IVE is running and the name of the Licensed Company via an HTTPS request from the Administrator's web browser upon login to the Admin UI. Juniper Networks collects this data to be able to inform customers about critical security patches they may need. Administrators can enable/disable this functionality by logging into the Admin UI and going to the Maintenance → System → Options menu. Juniper Networks strongly recommends that Administrators keep this setting enabled.
55. In order to access IVE resources as links from a non-IVE web page, a selective rewriting rule for the IVE resources is required. For example, if you would like to include a link to the IVE logout page such as `http://<IVE server>/dana-na/auth/logout.cgi` then you need to create a selective rewriting rule for `http://<IVE server>/*`.(26472)
56. Binary Import/Export on a FIPS box fails with the error message “store key failed for key certificate”.(27140)
57. The Source IP checkbox on the Roles page is not set properly, even after saving changes (27565)
58. Archiving option for NC Packet logs is not available under Maintenance->Archiving->FTP Server->Archive Schedule. (27105)
59. User will 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)

Supported Platforms

Please see the "Supported Platforms" document posted on the Juniper Networks Support Site (<http://www.juniper.net/support/>) under "IVE OS" for a current list of supported platforms (operating system/browser combinations). Note that some platforms do not completely conform to HTTP standards, so we have tested IVE functionality with the most common operating system/browser configurations used for the specific functionality. The "Supported Platforms" document summarizes the functionality tested, our testing model, and the supported platforms for the Neoteris IVE.

To open a case or to obtain support information, please create an online on the Juniper Networks Support Site: <http://www.juniper.net/support>.