

Juniper Networks NetScreen-Secure Access

IVE Platform version 5.3 R3 Build #10687

Secure Virtual Workstation and Support Meeting Release Notes



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

5 May 2006

Contents

Recommended Operation.....	1
New Features in this Release	3
Upgrading to this Release.....	3
Known Issues/Limitations Fixed in this Release	Error! Bookmark not defined.
All Secure Access Platforms.....	Error! Bookmark not defined.
SA 1000 through SA 6000 Items	Error! Bookmark not defined.
Known Issues and Limitations	4
All Secure Access Platforms.....	4
SA 1000 through SA 6000 Items	Error! Bookmark not defined.
Supported Platforms	5

Recommended Operation

- The Debug Log troubleshooting functionality should only be enabled after consultation with Juniper Networks Support.
- The IVE has an Automatic Version Monitoring feature which notifies Juniper Networks of the software version the IVE is running and the hardware ID of the appliance via an HTTPS request from the Administrator's Web browser upon login to the Admin UI. Juniper Networks collects this data to be able to inform customers about critical security patches they may need. Administrators can enable/disable this functionality by logging into the Admin UI and going to the **Maintenance > System > Options** menu. We strongly recommend that Administrators keep this setting enabled.
- When using W-SAM, Network Connect, or Secure Meeting, we recommend that the admin allow the client to automatically select between the optimized and non-optimized NCP options. This will allow clients to use optimized NCP where possible, and to fall back to non-optimized NCP where necessary. (28405)
- Graphical Identification and Network Authentication (GINA) functionality within Network Connect currently is not integrated with Cache Cleaner. We have now released support for Host Checker in Release 5.3. We recommend that you disable Cache Cleaner for the roles in which NC GINA is enabled.
- Multiple simultaneous sessions from a single client to the same IVE might cause unpredictable behavior and are not supported. This is primarily due to the pre-authentication mechanisms which might conflict between sessions. This caution also applies to situations where an end-user and admin session to a single host occur simultaneously.
- When using an external load balancer and accessing J-SAM, W-SAM, Network Connect, or the Online Meeting functionality, persistence must be employed on the load balancer. This persistence should be based on Source IP or Destination Source, depending on the load balancer being used.
- In order to access IVE resources as links from a non-IVE Web page, a selective rewriting rule for the IVE resources is required. For example, if you would like to include a link to the IVE logout page such as `http://<IVE server>/access/auth/logout.cgi` then you need to create a selective rewriting rule for `http://< IVE server >/*`. (26472)
- If two separate Web browser instances attempt to access different versions of the IVE, then the browser may prompt the user to reboot the PC after the NeoterisSetup.cab has been downloaded. Upon closing all browsers and logging in again, the prompt will no longer be displayed. No reboot is required.
- **Optimal Performance:** To optimize system performance, customers should ensure that the "Network Connect Packet Logging" feature is not used, as it will have a significant impact on system performance when under load. Additionally, cluster log synchronization is known to consume a lot of system resources (CPU + Memory), thus it is not recommended to activate this feature on systems that are widely used. (34276)
- When using the command-line W-SAM ("SAMLancher"), the URL entered must contain the prefix `https://`.
- W-SAM supports client-initiated UDP and TCP traffic by process name, by destination hostname, or by destination address range:port range. Except for Passive FTP, W-SAM only supports protocols that do not embed IP addresses in the header or payload. W-SAM also supports unicast client-initiated UDP.
- Users must launch drive maps through W-SAM in one of the following ways:

- **NetUse**--At the Command prompt, type: net use * \server\share /user:username
- Right-click on **My Computer > Map Network Drive**, or Explorer-enabled drive mapping. In Windows Explorer, go to **Tools > Map Network Drive**, then select "Connect using a different username".
- When using the W-SAM Access Control List (ACL), administrators should take extra precaution when granting access to hosts. We recommend that administrators use the IP address instead of the hostname. If the hostname is required, for security purposes, administrators should try to include additional ACLs with the corresponding IP address or IP addresses for that hostname. Reverse DNS lookups are not supported.
- To run Citrix NFuse through W-SAM, you must define a Caching rule to cache launch .asp files. For example, configure the resource policy to "<server name>:80,443/*.launch.asp" and the Caching Option to "Cache (do not add/modify caching headers)".
- When scripting the use of SAMLauncher.exe, users should provide the -reboot command-line flag, so that if the launcher requires a reboot, it happens automatically and does not exit, prompting the user to manually reboot. Note that during a fresh install (with NetBIOS enabled), W-SAM requires a reboot.
- When using Microsoft NetMeeting with W-SAM, hosting a meeting is not supported. There are no problems joining a meeting using Windows 2000. When using Windows XP, however, application sharing does not work as expected. In order for Windows XP users to work around this sharing issue, they must first turn on the **Only you can accept incoming calls** option.
- 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. 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: TCP-based and client-initiated.
- W-SAM support on Pocket PC-based Win CE 4.2 devices is now fully-qualified for several key handheld applications, and is now considered GA quality for the following applications (31708, 30252):
 - Pocket WTS
 - Pocket Outlook with IMAP/POP
 - Pocket Telnet
 - Pocket Outlook with ActiveSync
 - In order to get this working, Administrators of the SSL-VPN will need to add the "IP Address(es)" of the Exchange Server(s) to the "W-SAM Destination Hosts List" located in **Roles > WSAM > Applications**.
 - The following process names need to be defined under the **Roles > W-SAM > Applications** page:
 - Pocket Outlook: "tmail.exe"
 - Pocket Windows Terminal Services: "mstsc40.exe"
 - Pocket Telnet: "telnet.exe"
- Do not delete the main cluster licensing node. Doing so will delete the whole cluster. (27972)

New Features in this Release

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

Upgrading to this Release

- Please refer to the *Supported Platforms* document for important information pertaining to Microsoft Windows XP SP2 support.
- Automatic upgrades to this release from the following releases are supported (including from the Legacy Authentication mode):
 - 5.2 R2 Build 9895
 - 5.2 R1 Build 9469
 - 5.1 R7 Build 10081
 - 5.1 R6 Build 9837
 - 5.1 R5 Build 9627
 - 5.1 R4 Build 9403
 - 5.1 R3 Build 9311
 - 5.1 R2 Build 9092
 - 5.0 R6 Build 9343
 - 5.0 R4 Build 9085
 - 5.0 R2 Build 8721
 - 5.0 R1 Build 8553
 - 4.2 R5 Build 8559
 - 4.2 R4 Build 8375
 - 4.2 R3 Build 8175
 - 4.2 R2 Build 7891
 - 4.2 R1 Build 7803
 - 4.2 GA Build 7631
 - 4.1.1 R2 Build 7557
 - 4.1.1 R1 Build 7387
 - 4.1.1 S1 Build 7335
 - 4.1 R3 S1 Build 7345
 - 4.1 R2 S1 Build 7373
 - 4.1 R1 S1 Build 7347
 - 4.1 S1 Build 7337
 - 4.0 P2 S1 Build 7363

- 4.0 R1 S1 Build 7369
- 4.0 P1 S1 Build 7365
- 4.0 S2 Build 7367
- **Note:** If upgrading from a 3.x releases, you must upgrade to Release 5.0 prior to upgrading to Release 5.3.
- **Note:** If upgrading from a release which is not listed here, please upgrade to one of the listed releases first, and then upgrade to 5.3 R1.
- If using Beta software, please be sure to roll back to a prior production build and then upgrade to the 5.3 R1 software. (This process enables you to roll back to a production build if ever needed.)

Known Issues and Limitations

All Secure Access Platforms

Secure Virtual Workspace (SVW)

- While in the Secure Virtual Workspace, Microsoft Word is DISABLED as a default editor for Microsoft Outlook. The default editor is going to be Wordmail instead of Microsoft Word. (37144)
- Juniper Infranet clients will not be supported within the SVW context when using Java Delivery using Sun JVM. (36983)
- JSAM support for Microsoft Outlook/Exchange will not be supported within an SVW session because there are technical limitations in exceptionally allowing JSAM to modify the required registry modifications to the RPC binding order. (37355)
- SVW is configured using Host Checker's policy UI on the SSL-VPN Admin UI. SVW will not work in HC post-authentication mode. As part of Host Checker launch, SVW gets evaluated, and any evaluation of SVW will launch the SVW shell. (37438)
- When downloading *.exe executables within the SVW shell, upon successful downloading, the user gets a dialog box with 3 options: "Run", "Save", and "Cancel". This dialog will appear only when using Microsoft's Internet Explorer browser. The "Run" option is NOT supported within SVW for technical reasons. The user must "Save" the file within the SVW shell (e.g. desktop), and then launch it from the desktop. (34541)
- Uninstallation of Juniper SSL-VPN client components will not be supported while in the Secure Virtual Workspace. The workaround is to uninstall the applications from within the Real Desktop prior to launching SVW. (34430)
- Multiple users using the same password to encrypt their SVW workspace on the same host could gain access to the persistent data storage protected by that static password. It is recommended that strong passwords be used when securing their SVW persistent data store on multi-user systems. (37311)

Support Meeting

- On Windows platforms, the "Edit" menu used for chat functionality does not apply to Support Meeting. (36872)
- Support Meeting does not have chat functionality. On Windows platforms, the "Chat" tab under the Meeting > Preferences menu should be ignored. (36919)

- Support Meeting does not support Annotation. On Windows platforms, the option “Disable request for Annotation” under the Meeting > Preferences menu should be ignored. (36920)

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 IVE.

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