

Juniper Networks Secure Access Release Notes

IVE Platform Version 7.0R2 Build # 16499

This is an incremental release notes describing the changes made from 7.0R1 release to 7.0R2. The 7.0R1 GA release notes still apply except for the changes mentioned in this document. Please refer to 7.0R1 GA release notes for the complete version.

The NSM schema for this software version will not be published.

1. Since the schema for this software version is not published an attempt to manage a device running this version would result in adjust-os-version to fail on NSM. Device object needs to be deleted and recreated in NSM. After that, NSM will be able to manage the device using the published schema
2. SA Device upgrade to this OS version using NSM would not work as noted in the General NSM limitations Section

General NSM Limitations

1. If there is a mismatch between software catalog build version and release build version on the device, upgrading the device using NSM will not work

For example, 6.5R3 schema was published using build 15215 (software catalog version), but subsequently, 6.5R3.1 was released with build 15255. In this case, NSM will not recognize build 15255 as a valid upgradable release. However, if device is manually upgraded to build 15255, since there were no additional schema changes, the device should still be manageable via NSM.
(523868)

Best Practices for FIPS Devices

1. Do not import a previously exported system config since it might contain a corrupted FIPS keystore database. If you must import an older system config, the option “Import Device Certificate(s)” must be unchecked when importing.
2. After upgrading to 6.5R2 it is strongly recommended that the system config be exported to take a back up of FIPS keystore database. The newly created system config will contain a clean FIPS keystore database.
3. After upgrading to 6.5R2, in case the admin console reports a “FIPS disassociated” state, go into serial console and reload the FIPS keystore database (Option 9 -> Sub-option 1).

Known Issues/Limitations not Fixed in 7.0R2 Release

The following list enumerates known issues which were not fixed in this release:

1. asg-general-documentation - The 2048-bit CSR creation is not supported on the SA4000FIPS and SA6000FIPS machines, even though the option is presented on the Admin UI. (587240)

Known Issues/Limitations Fixed in 7.0R2 Release

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

1. aaa-active-directory - Group membership checks fail. (527878)
2. aaa-client-cert – The valid CRL was not passed to secondary auth server when primary LDAP authentication fails. (522141)

3. aaa-local - Entry of a user is present in xml export even after deletion of the user from WebUI if username is created in the xml and if it contains capital letters. (489917)
4. aaa-passwd-mgmt-nt-ad - The message logging is incorrect even when the password change is successful by an AD user. (518336)
5. aaa-realms - Unsuccessful attempts of Admin login from different Source IP being recorded in the User access Logs when source IP restriction is applied on admin role. (502346)
6. aaa-realms - The role mapping rule with 'is not' did not work with multiple usernames. (516822)
7. aaa-roles - NC was not auto-launching after session/idle timeout. (519829)
8. aaa-roles - The User Admin functionality did not work for AD authenticated users. (520350)
9. aaa-sign-in-pages – After changing of password, i-mode users get redirected to default sign-in URL. (525683)
10. aaa-sign-in-pages – After login to a Siteminder Agent, when an user logs into a non-siteminder sign-in page, the authentication happens through siteminder instead of the auth server specified for the sign-in page. (532174)
11. clustering-active-passive – If UDP traffic is blocked between the nodes of a cluster but TCP traffic is permitted then both the nodes will become the leader and the VIP won't failover.(489754)
12. clustering-other – When joining into a cluster is enabled through the console and wrong password is provided, then the join action fails and hangs the IVE. (518512)
13. cs-jsam-other – JSAM does not launch when UAC is enabled on Vista. (440039)
14. cs-jsam-other – If a user re-logs in before his session expires and re-launches his Citrix session through JSAM then a process on the IVE may crash and cause all JSAM sessions to drop. (544711)
15. cs-nc-enduser - The Windows 7 users are unable to login using the smart card credentials for authentication. (435417)
16. cs-nc-enduser - The DNS SearchList is not populated correctly with a backup, when the DHCPDomain key is missing. (500129)
17. cs-nc-enduser - The user receives less than 1/2 the configured bandwidth management policy. (503756)
18. cs-nc-enduser - The NC launch on Windows 7 is not happening properly when the DNS service is restarted. (505114)
19. cs-nc-enduser - The NC Launcher is unable to recognize resources in foreign language (French, German etc) resource files. (509647)
20. cs-nc-enduser - NC reconnect time is slow. (509996)
21. cs-nc-enduser - The route table with conflicting routes are not restored on the Linux client after the NC is disconnected. (520071)
22. cs-nc-enduser - The DNS binding for the Windows 7 client running NC on PPP interface is not handled properly. (528655)
23. cs-nc-i18n - NC session timeout warning message gets partially garbled when a user logs into the IVE using web browser with Japanese locale and launch NC. (511593)

24. cs-nc-other - A performance issue occurs when more users join a multicast stream with NC. (501918)
25. cs-nc-other – NC client would not get the configured IP address when the cache entries were not flushed. (513030)
26. cs-nc-other - NC IP address was not cleaned-up when the tunnel setup fails in a certain scenario. (517726)
27. cs-nc-other - The Network connect process may crash when using push config to update a large number of NC ACLs. (525561)
28. cs-wsam-i18n - WSAM version info is missing in Japanese Windows OS. (535139)
29. cs-wsam-other - Occasionally applications secured by WSAM may freeze/stall as the communication between WSAM client and SA is stalled. (521275)
30. cs-wsam-other – A process crashes and all WSAM users are disconnected when WSAM is launched and UDP traffic is sent from the client to the server when the service is unavailable. (524674)
31. cs-wsam-resource-profiles – Users are unable to connect to WSAM destination profile resources on a copied role until the role has been removed and added back to the profile. (528503)
32. endpointintegrity-custom-check - HC crashes in linux/suse machines when a process without a name is running. (520471)
33. endpointintegrity-ees - EES initializing page text reads malwares instead of malware. (513198)
34. endpointintegrity-ees - End users experienced delay in connection establishment because of EES scan taking long time. (522410)
35. endpointintegrity-install - In Windows 2000 HC installation fails if msvcp80.dll is not installed. (516762)
36. endpointintegrity-opswat - HC fails when a policy for SOPHOS 9.0.3 AV virus definition file version is configured. (511455)
37. endpointintegrity-others - MAC address check for wireless port fails on Windows Vista and 7 when the wired port is not connected. (511946)
38. msp-ivs – In IVS, DNS lookup to secondary DNS is sourced from root IVE's internal port instead of the IVS's. (535868)
39. sysmgmt-snmp - The UCD-SNMP MIB objects are not properly handled by the IVE. (517050)
40. system-network - Proper error messages are now displayed when a network services are restarted due to changes in VLAN configuration. (530840)
41. system-other - During the session timeout, with remainder, when the user tries to re-login, IVE sends Authentication requests over the VLAN IP instead of the internal IP. (502342)
42. system-other - Fallback to CRL fails when OCSP connection times out. (509698)
43. system-other - Unable to download 'virus signature and patch management data' as the intermediate CA is missing during certificate verification. (530600)
44. system-other - Certificate Attribute "publicKey" was not available to be used in Role Mapping Rules. (533914)
45. system-other - The entire client certificate was not getting logged in the User Access Logs, when it is enabled in the User Access Log setting. (533916)

46. virtual-desktop-other - C:\Windows is not displayed in My computer inside SVW while using IE8 (528292)
47. web-flash – Flash rewriter has memory usage issues. (515340)
48. web-flash - There was problem with rewriter not rewriting flash :`"embed />"` src link. (537940)
49. web-java-sun-jvm - Code signing certificate uploaded to IVE is not used for a particular uploaded JAVA applet. (472451)
50. web-javascript - Javascript link from within a web bookmark fails to open on Firefox if the IVE was opened initially using an external link with `target=_blank`. (512901)
51. web-other - When IVS is used and OWA rewrite filter is enabled on root, "Unable to read enabled flag from cache for filter" event logs are generated. (494995)
52. web-other - Code change has been done to handle BasicAuth SSO for requests to any extranet site, with large POST body. (498843)
53. web-other - Jar file download history is not being recorded in the user access logs. (509670)
54. web-other - Javascript Rewriter has an issue related to `window.open` calls. (510951)
55. web-other – Rewriting of a POST to target server was failing when "Don't Rewrite:Redirect to target server" policy is created. (513667)
56. web-other – Rewriting of a Class path is not done properly when a specific application is accessed. (517606)
57. web-other - Reposition toolbar does not move when user clicks the arrows button while user using IE 8 is accessing web resources which use JavaScript (517623)
58. web-other - Rewriter is unable to handle the expression `"https:/"`. (522566)
59. web-other - Critical error messages were getting logged in the events log when users try to access files/shares on a Sun Unified Storage device (7000 series). (525163)
60. web-other - Javascript rewriter issue where popup results in a blank page. (525901)
61. web-other – Rewriting throws an unknown error when custom headers are present. (527211)
62. web-other - In rewriter when the form action is set to `""` (empty), it is rewritten to `empty.html` (528864)
63. web-other - The anonymous requests, with virtual hostnames, are not handled properly by the rewriter. (529603)
64. web-other - The rewriter module stops parsing if it sees `"-->"` during dynamic js parsing. (530201)
65. web-other – Rewriting of the ORACLE webcenter, version 11.1.2, is not handled properly . (532185)
66. web-other – Rewriting of the ORACLE webcenter, version 11.1.2, containing transparent URLs is not handled properly. (533183)
67. web-other – There is an error in the Javascript rewriter related to the `getAttributeNode` method.(534609)
68. web-other - In the rewriter, IVE is dropping responses if backend web server responds with 401 header without a valid WWW-Authenticate header (535247)

69. web-supportedapps – Active sync is not working properly in a certain scenario. (505619)
70. web-supportedapps - Unable view SMIME encrypted mail using OWA 2003. (513916)
71. win-term-svcs-enduser - TS with seamless connection to a remote app on win2008 R2 where it launches two simultaneous instances of bookmark is not handled properly. (515975)
72. win-term-svcs-other – The customer specific application Rogers’s online protection is not able to handle a flag gracefully and was leading to a crash. (519936)
73. Browser request follow through and externally launched terminal services are not working. (541265)