Pulse Connect Secure Release Notes

8.0 R13 Build 38659
September 2015

Revision 5.0

Introduction

These release notes contain information about new features, software issues that have been resolved and new software issues. If the information in the release notes differs from the information found in the documentation set, follow the release notes.

This is an incremental release notes describing the changes made from 8.0R1 release to 8.0R13. The 8.0R1 release notes still apply except for the changes mentioned in this document. Please refer to 8.0R1 release notes for the complete version.

Interoperability and Supported Platforms

Please refer to the *Junos Pulse 8.0R3 Supported Platforms Guide* for supported versions of browsers and operating systems in this release.

Pulse Connect Secure New Features in this release

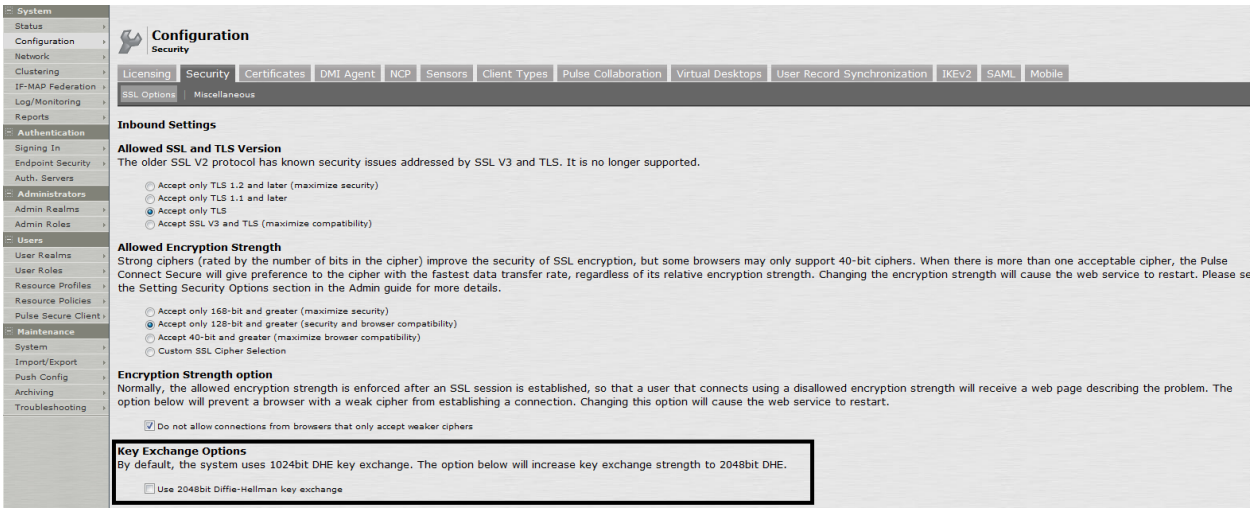
NDPP DHE-2048 Key Exchange Enhancement

To address the security vulnerability CVE-2015-4000 (Logjam issue), a new option has been added under 'System -> Configuration -> Security -> SSL Options' that ensures that all Diffie-Helman key exchanges use a 2048 bit key.

The TLS protocol uses Key Exchange algorithms to transfer the pre-master secret between TLS client and TLS server. The major key exchange algorithms supported in TLS are RSA, ECDHE and DHE. Security of the TLS transfer depends heavily on the use of stronger keys for key exchange algorithms.

The current Diffie-Hellman Key Exchange (DHE) uses 512 or 1024 bits keys which are considered cryptographically weak.

If this new option is enabled, the Diffie-Hellman Key Exchange will use 2048-bit keys.



Problems Resolved in this release

Table 1 Problems Resolved in This Release

Problem Report Number	Description
PRS-330432	Pulse connections may fail to establish tunnels when both L3 and L7 connections are used
PRS-330393	URL for subscription licensing now uses Pulse Secure URL
PRS-330094	Host Checker validation with Shavlik (patch management policies) may not complete and access will be denied
PRS-329556	Embedded file browsing links fail to rewrite correctly
PRS-327459	JuniperSetupClient.ocx may be prevented from running and marked as being from an untrusted CA due to invalid SKID validation
PRS-327393	Rewriting may fail if the HTML page is sent in single characters
PRS-326870	An application using VBScript may cause rewrite-server to fail

PRS-325965	SAML authentication in a cluster may cause swap memory utilization to increase
PRS-325564	Executing SNMP GET IfOperStatus command on PCS returns an incorrect interface status.
PRS-324850	ACL count in user access logs is incorrect after removing the duplicate IP table entries.
PRS-324480	Authorization only access URL may cause high CPU utilization if the client closes the connection prematurely
PRS-324164	Enabling multicast for VPN tunneling may cause 100% CPU utilization
PRS-323316	RADIUS authentication may trigger swap memory utilization and slow performance due to excessive invalid authentication attempts
PRS-318426	VPN Tunneling ACL limits are marked as reached prematurely when a user maps to multiple roles with overlapping ACLs

Known Issues in this release

Table 2 describes the open issues in this release

Table 2 Known Issues in this release

Problem Report Number	Description
PRS-331939	If you currently use the 'Authorization only or ActiveSync access' feature (i.e. PCS gateway acting as a proxy for ActiveSync traffic) or the IKEv2 based VPN functionality feature and these features are configured for Client Certificate authentication with client certificate having the EKU extension then we recommend not to upgrade to this version due to a memory leak issue which may eventually cause the process to crash. This issue exists in 8.0R9 and higher releases and will be resolved in an upcoming maintenance release (PRS-331939)
PRS-329563	invalid URL via core access. object%20Object% getting added instead of index.em7

Security Issues Resolved in this release

Table 3 describes issues that are resolved when you upgrade.

Table 3 Security Issues Resolved in This Release

Problem Report Number	Description
PRS-328850	PKCS7 crash with missing EnvelopedContent (CVE-2015-1790)
PRS-328848	CMS verify infinite loop with unknown hash function (CVE-2015-1792)
PRS-328777	Malformed ECParameters causes infinite loop (CVE-2015-1788)
PRS-328776	Exploitable out-of-bounds read in X509_cmp_time (CVE-2015-1789)
PRS-327414	Mac NC - Segmentation fault in ASN1_TYPE_cmp fix (CVE-2015-0286)
PRS-327410	Mac NC - Base64 decode (CVE-2015-0292) CVSS: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

Pulse Connect Secure New Features in 8.0R12.1

Pulse Secure Rebranding

Pulse Connect Secure 8.0R12.1 have been re-branded with the new Pulse Secure logo. The Pulse Secure logo has replaced Juniper logo. You will see certain changes on the admin console that indicate this re-brand.

Pulse client on desktop has been re-branded with the new corporate logo.

When you upgrade to 8.0R12.1/5.0R12.1, please be aware of these user-visible changes. There are no specific changes to the upgrade experience or to the overall behavior tied to re-branding. Several internal aspects such as filenames, location of install directories, registry keys and so on will remain the same in this release

NOTE: For Pulse Secure 5.0R12.1, the names of the Pulse Secure gateways (formerly collectively referred to as the IVE, or “Instant Virtual Extranet”) have changed.
The SSL-VPN headend (formerly called the Secure Access or SA device) is now called Pulse Connect Secure. The access-control headend (formerly called the Unified Access Control or UAC device, and also sometimes called the Infranet Controller or IC) is now called Pulse Policy Secure.

Problems Resolved in 8.0R12.1 release

A few of the fixes that were included in 8.0R11 were (inadvertently) not included in 8.0R12, this release fixes the issue. For details please refer TSB40051

Table 5 Problems Resolved in This Release

Problem Report Number	Description
PRS-324526	JIRA may not be rewritten correctly using IE 9
PRS-327629	Access of webmail via Office 365 through the rewriter fails.
PRS-329943	Office365-based OWA may fail to load correctly with IE
PRS-325789	When deleting an allowed server from a WSAM profile, the confirmation message shows the wrong server name
PRS-326867	For large file transfers through NC tunnel, User Access Logs show incorrect file transfer size
PRS-324055	Host Checker custom rule using environmental variable %LOCALAPPDATA% fails with Pulse
PRS-322044	Host Checker remediation messages may be displayed twice when using RADIUS authentication
PRS-327235	FIPS-based Network Connect may not connect successfully from a VM client
PRS-328367	Pulse App VPN does not require license.

PRS-327099	Signature verification for Host Checker binaries are taking more than 30 secs in some instances, which is causing the timeout in Setup client.
PRS-324747	Custom application Javascript rewriting failed to parse a 'match' sequence correctly.
PRS-324480	High CPU usage observed with ActiveSync enabled.
PRS-326609	When using dual authentication and the Pulse Secure client it may be possible for an erroneous source IP to be recorded for a user.
PRS-326964	Host checker fails to launch when there is a mismatch in the MMFName
PRS-320740	Automatic replies cannot be managed through Firefox when the session timer is enabled

Known Issues in 8.0R12.1 release

Table 6 describes the open issues in this release

Table 6 Known Issues in this release

Problem Report Number	Description
PRS-329301	Incorrect transferred bytes shown in NC client stats after it goes beyond ~5GB

Security Issues Resolved in 8.0R12.1 release

Table 7 describes issues that are resolved when you upgrade.

Table 7 Security Issues Resolved in This Release

Problem Report Number	Description

PRS-327488	XSS via UserAgent string
PRS-327388	Is SA/MAG vulnerable to CVE-2014-3572?
PRS-327354	Security vulnerability "APP-H-002: Reflected Cross-Site Scripting allows control of victim's browser"

Problems Resolved in 8.0R11

Table 8 Problems Resolved in This Release

Problem Report Number	Description
PRS-326748	If a user is assigned multiple roles and there is ACL duplication, the expected top-down processing may fail
PRS-326276	When roaming sessions are enabled, the cache may grow excessively large and cause a crash.
PRS-325285	Pulse WSAM's idle timer does not reset if it encounters NetBIOS traffic. From 8.0R11 onwards, an option is available to not consider NetBIOS traffic as user-initiated activity.
PRS-325004	Pulse fails to prompt for an updated secondary password if the second password is changed after being saved.
PRS-324749	With Pulse, Host Checker fails to delete the files from the path specified with <USERHOME> as environmental variable.
PRS-324164	Under certain conditions while multicast traffic is running, web process can cause 100% CPU
PRS-324033	Rewriting relative URI is failing because IVE does not handle certain special characters such as backward slash.

PRS-323933	When running Pulse on a Mac, if the internal DNS cannot resolve the IVE hostname then the user cannot directly access the IVE.
PRS-323861	In a clustered environment all the nodes in the cluster send logs to the syslog server even though synchronize log messages option is enabled.
PRS-323598	Pulse attempts to continuously connect to a second VPN connection continuously even though an existing VPN connection is connected.
PRS-323298	The policy trace logs on an IVS do not clear after clicking on “Clear Log”.
PRS-323178	Compliance reports may be missing data or include invalid data.
PRS-322973	Web server may crash when malformed IP packet is received at IVE.
PRS-322856	When an incorrect DNS failure response is received by the Pulse Connect Secure gateway, the dsagentd process may crash.
PRS-322710	If backend web application has a cookie name that ends with “DSID”, NCP connections authentication will fail.
PRS-322687	ICMP error messages are sent with the primary address of the exiting interface.
PRS-322071	Network Connect fails to restore actual proxy pac settings on abrupt restart of the client.
PRS-320296	WSAM resource profile destination using LDAP attributes is not parsing the host and the port properly from the value returned
PRS-318772	When bookmark name is a custom variable that uses an attribute-based expression with REGMATCH, if expression evaluates to empty, bookmark name is shown as zero.
PRS-315604	Pulse Cache Cleaner fails to delete the contents of "Recycle Bin" when "Empty Recycle Bin and Recent Documents list at the end of user session" is enabled.

Security Issues Resolved in 8.0R11

Table 9 describes issues that are resolved when you upgrade.

Table 9 Security Issues Resolved in This Release

Problem Report Number	Description
PRS-324926	Base64 decode (CVE-2015-0292)
PRS-324904	ASN.1 structure reuse memory corruption fix (CVE-2015-0287)
PRS-324902	Segmentation fault in ASN1_TYPE_cmp fix (CVE-2015-0286)
PRS-324910	Use After Free following d2i_ECPrivatekey error fix (CVE-2015-0209)

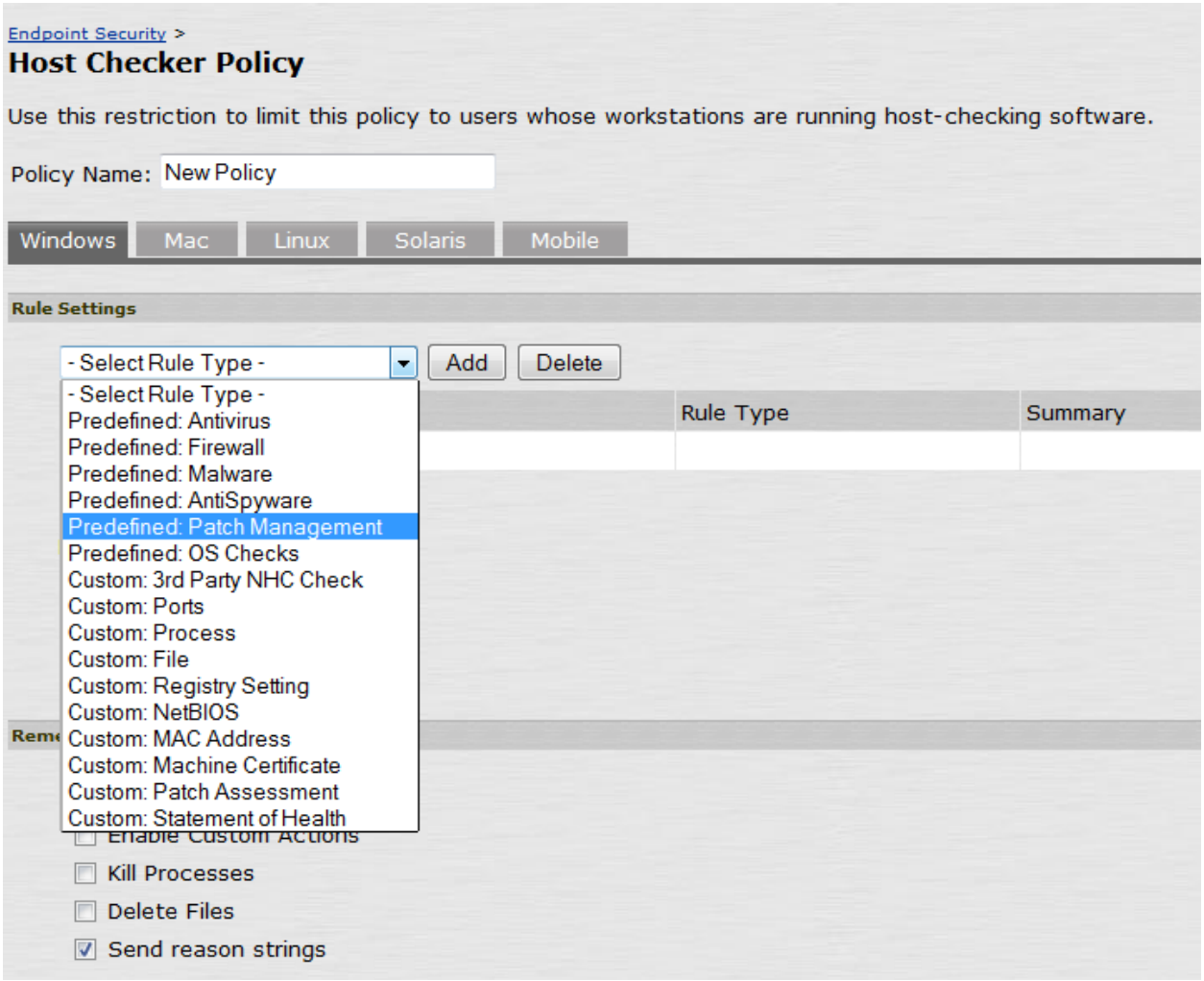
Noteworthy Changes in 8.0R10 Release

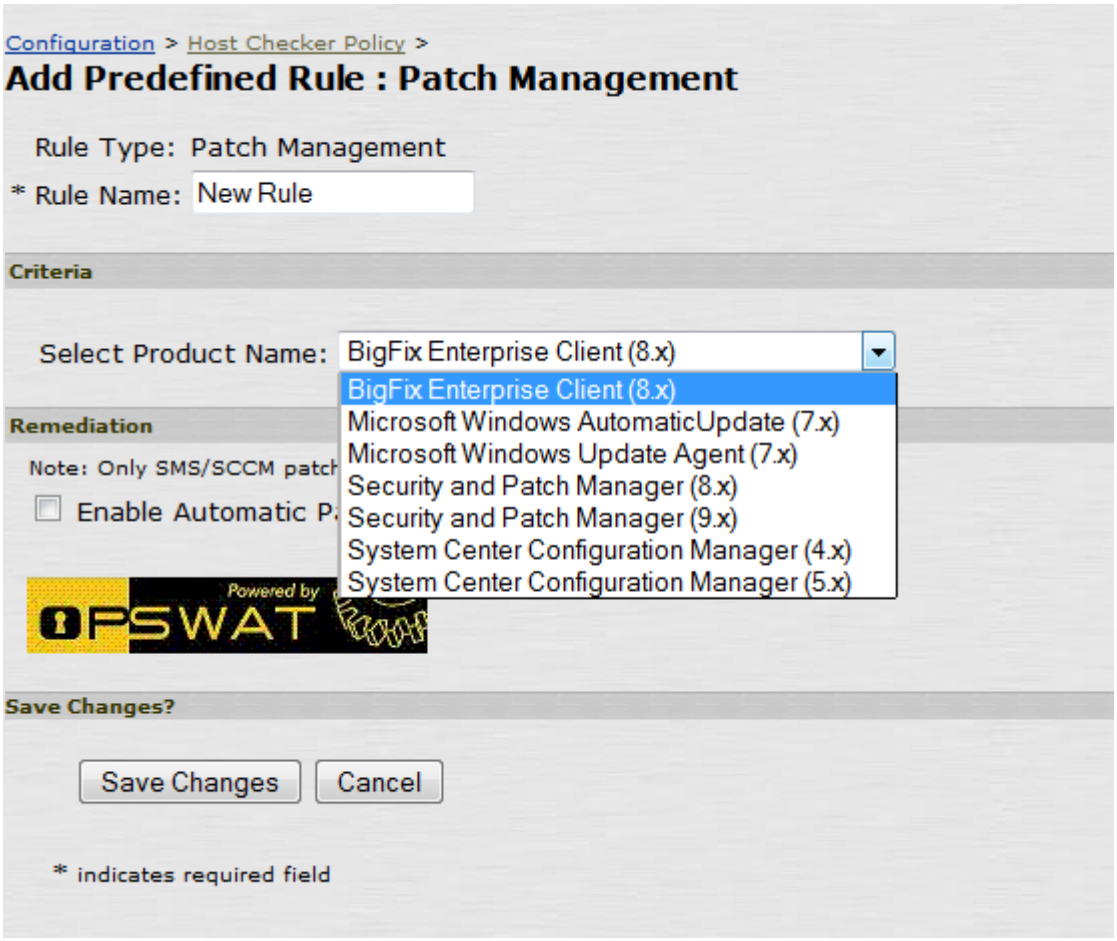
OPSWAT based patch management policies

In 8.1R1 release, patch assessment and remediation functionality offered by Shavlik is deprecated and replaced with OPSWAT patch management solution. Shavlik solution will be deprecated in future 8.0Rx release as well.

For an interim period, we are providing both Shavlik and OPSWAT patch solutions in 8.0R10 release. This will give administrators the opportunity to test and familiarize themselves with the OPSWAT-based policies for an easier transition when the Shavlik-based policies are deprecated.

OPSWAT based patch management policies can be configured by navigating to Authentication-> Endpoint Security -> Host Checker -> Policies **->** New:





SAM Idle Timer Option:

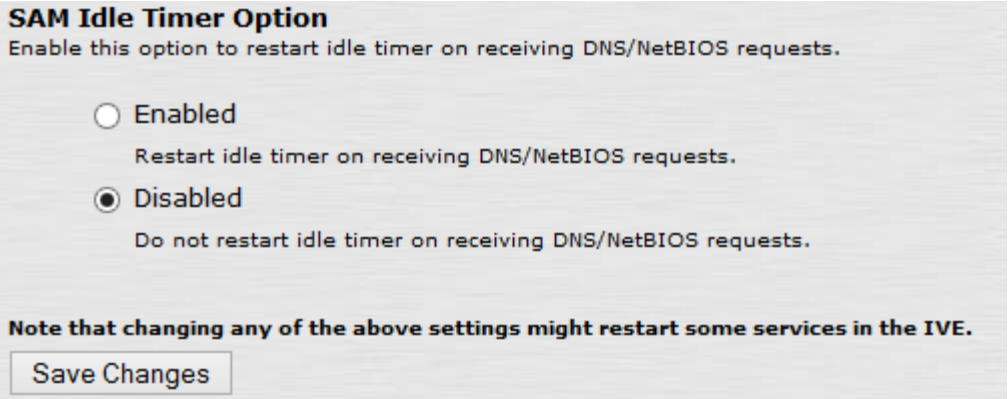
A new **SAM Idle Timer Option** has been added in the admin UI under XXXX to allow control of whether DNS/NetBIOS traffic is considered user-initiated activity or not. If enabled, the DNS/NetBIOS traffic is considered user-initiated activity and idle timer resets. Therefore, if there is a constant stream of NetBIOS packets, the user session will not hit the idle timer. When this option is disabled, this traffic does not count as user initiated activity and therefore if the only traffic encountered by the IVE is NetBIOS traffic, the idle timer will fire. This option applies only to the WSAM client and not to the Pulse SAM client.

Enabled

Restart idle timer on receiving DNS/NetBIOS requests.

Disabled

Do not restart idle timer on receiving DNS/NetBIOS requests.



Problems Resolved in 8.0R10 Release

Table 10 describes issues that are resolved when you upgrade.

Table 10 Resolved in This Release

Problem Report Number	Description
PRS-322740	Pulse may not connect if pre-signin notifications are configured.
PRS-322649	If the CRL CDP CRL is longer than 60 characters, certificate authentication will fail.
PRS-322365	HTTP 500 Internal error occurs while uploading a file in an environment which has delay or low bandwidth via Authorization Only access.
PRS-322303	SNMP MIB values are reported incorrectly.
PRS-322154	Rewriting large XML files may trigger a rewrite-server process crash.
PRS-322112	Rewrite engine may fail to rewrite application functions correctly and cause the page to not load.
PRS-322073	Updates to the DNS server values at System > Network > Overview may not be immediately loaded and honored.

PRS-321885	NetBIOS and DNS queries count toward the WSAM idle timeout value and prevent a session from timing out as an idle session.
PRS-321800	Changes to the SSL options are not recorded successfully in the events and admin access logs.
PRS-321651	iveSSLConnections reported erroneously for snmpwalk.
PRS-321629	AD authentication may not correctly fallback to secondary DNS server if the primary is unreachable.
PRS-321317	IVS log files may see log messages from other IVS instances.
PRS-320448	If a VPN tunnel client, Pulse or Network Connect, disconnects immediately the IP may be recorded as leased to that user erroneously and cause unexpected IP exhaustion.
PRS-319877	Clicking on a button in the CRL options page may not trigger the desired action.
PRS-319192	If the URL contains “%2B” it will be rewritten to ‘+’ and may trigger failure on the backend application.
PRS-318576	Content located inside <iframe> may not be rewritten correctly.
PRS-317704	The rewrite-server may crash if an application has a long string value on an HTML tag.
PRS-298999	License server may not display license client names correctly if the license clients are clustered.
PRS-324043	Shavlik-based patch management is being deprecated; OPSWAT-based patch management needs to be introduced.

Junos Pulse Secure Access New Features in 8.0R9 release

Disable TLS 1.0

The “Disable TLS 1.0” feature will provide a mechanism to allow administrators more fine-tuned control of the TLS version used for connections to the Pulse Secure Access Gateway.

The current SSL protocol selection mechanism is as below.

- Accept only TLS
- Accept only SSL V3 and TLS
- Accept SSL V2 and TLS V3 TLS

This granularity is required by multiple agencies; NIST standards note TLS 1.0 should not be used and will transition to stating only TLS 1.2 and higher should be allowed.

This feature will allow more fine-grained control of SSL and TLS versions to be used, for example:

- Accept only TLS 1.2 and later
- Accept only TLS 1.1 and later
- Accept only TLS
- Accept SSL V3 and TLS

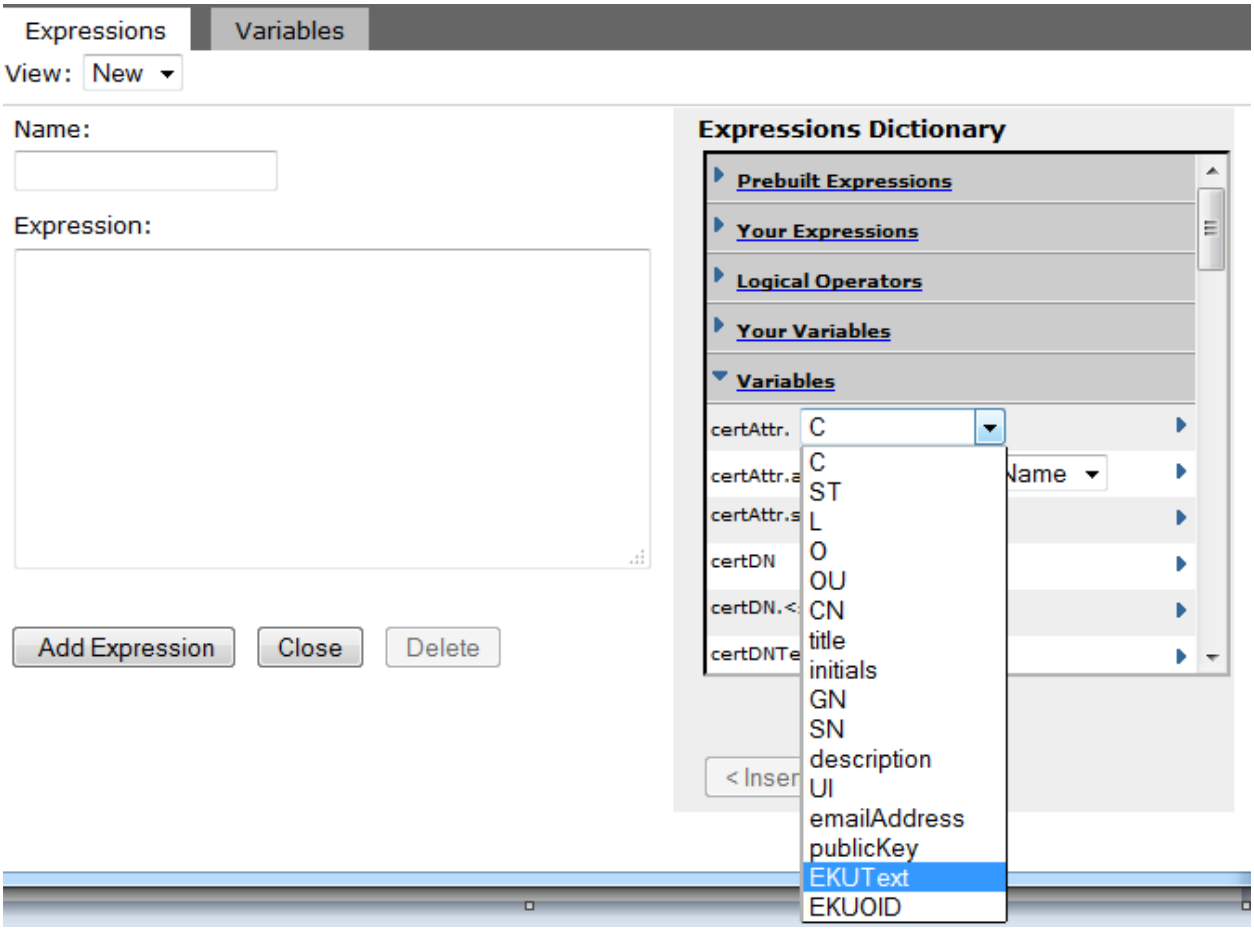
NOTE: This setting controls only connections into the device (Inbound Settings) and does not dictate settings for SSL connections that are initiated by the IVE.

NOTE: If TLSv1.1 or greater is enabled on the SA, Android devices 5.0 and greater will be able to connect whereas pre-Android 5.0 devices will not be able to connect since TLSv1.1 is disabled by default.

New Functionality to create role mapping rules based on EKU field of certificate:

8.0R9 for the Pulse Secure Access Gateway introduces the ability to create custom expressions based on OID and/or text-based extended key usage (EKU) fields of client certificates. The screenshot below shows where the option can be found in the certAttr field

Below screenshot shows the custom expressions:



Problems Resolved in 8.0R9 Release

Table 11 describes issues that are resolved when you upgrade.

Table 11 Resolved in This Release

Problem Report Number	Description
PRS-322152	New logging filter based on date does not allow selection for the year 2015.
PRS-322017	If the VPN Tunneling Connection Profile is set to search device DNS only AND the role is set to use split tunneling users may not be able to reconnect after a network connectivity disruption.
PRS-321666	SA/MAG acting as IDP: Error in SAML processing: 'Bad base64 format of SAMLRequest'.

PRS-321356	If the PAC URL in IE does not have a trailing slash, e.g. https://proxy.company.com, Network Connect reports the proxy as having an erroneous format and does not connect.
PRS-320630	Log data is not exported to defined syslog servers over UDP.
PRS-320249	After configuring a resource to optimize as a long-lived resource, the hprewrite daemon responsible may crash when using SSO.
PRS-320167	License clients may erroneously display iveMaxConcurrentUsers warning if licenses are still available to be leased from the license server.
PRS-320072	Session start script to map network drives may fail to launch through Junos Pulse.
PRS-319977	ActiveSync with certificate validation may prevent VPN tunnels from establishing.
PRS-319409	VMware View 6.0 fails to display correctly through rewriter.
PRS-318842	Delegated admin users can make changes to the device management setting.
PRS-318549	Applications utilizing GWT on script download framework fail to display properly.
PRS-318426	VPN Tunneling ACL limit is reached prematurely, if multiple roles use the same ACL and a user maps to multiple roles.
PRS-318124	Improper location object identification on German language browser/OS causes web application to fail to rewrite properly.
PRS-317832	Update the informational text at Maintenance>System>Options to confirm that both nodes in the cluster will reboot when toggling the SSL/Hardware acceleration setting.
PRS-317437	System>Status>Devices is visible to IVS administrators.
PRS-304724	VPN tunneling data transport halts when “TCP NO BUFFER” socket response is received.

Known Issues in 8.0R9 release

Table 12 describes the open issues in this release

Table 12 Known Issues in this release

Problem Report Number	Description
323238	Push Config from one IVE to another fails, if the target is configured to accept TLS 1.1 or higher and source is configured to use SSLv3.

Noteworthy Changes in 8.0R8.1

This release addresses the POODLE fix when hardware acceleration is enabled.

Problems Resolved in 8.0R8.1

Table 13 describes issues that are resolved when you upgrade.

Table 13 Resolved in This Release

Problem Report Number	Description
PRS-321986	Authentication failure when certificate authentication is enabled against a hardware acceleration IVE.

Noteworthy Changes in 8.0R8

To effectively support proxies on Windows clients, Network Connect and Pulse will generate URL-based proxy PAC files instead of file-based proxy PAC files due to access restrictions on Windows machines. (PRS-303538, PRS-319611)

Problems Resolved in 8.0R8

Table 14 describes issues that are resolved when you upgrade.

Table 14 Resolved in This Release

Problem Report Number	Description
PRS-319611	Microsoft applications will not connect if the IE proxy is configured as a file:// link.
PRS-319253	The CRL is downloaded for each authentication when using certificate authentication with CRL checking enabled.
PRS-319020	Rewritten web URL is not displayed when "Manage Your Preferences" link is clicked.
PRS-318833	Pulse may not resume the VPN session correctly after an active/cluster node failover.
PRS-318739	Patchupdate.dat may not update/display correctly if special characters are included in the patch detail.
PRS-318582	An IF-MAP federation client will record a major event every 3 minutes if it cannot connect to an IF-MAP server.
PRS-318544	A custom passthrough proxy application may fail when accessed using Safari on iOS 8.
PRS-318312	JSAM cannot open connection to hostname when proxy server is configured on the browser.
PRS-318090	Federated session on fed server has stale device attribute if the user logins in and logs out of fed client several times and if the session export policy is configured with "Set IF-MAP Device Attribute".
PRS-317867	Role and local domain suffix attributes are single-valued and not multi-valued.
PRS-317779	Improper type checking in certain functions is creating JavaScript errors.
PRS-317741	If the Network Connect installer file is located in a directory that the path is > 128 characters, installation fails.
PRS-317725	Custom file check with multiple checksum fails on Mac OS.
PRS-317644	Host Checker may not refresh past “loading components” on XP.
PRS-317599	EAP-GTC may cause the radius daemon to crash when using new PIN mode.
PRS-317585	Pulse erroneously requested secondary authentication credentials if the first entry failed.

PRS-317382	A high number of terminal service resource resource profiles (1000+) may cause high CPU utilization.
PRS-317116	SNMP traps may not honor 60 second firing frequency.
PRS-317062	Existing Tunnel-Private-Group-ID attribute syntax does not work with Aruba equipment.
PRS-316305	While allocating the license to a client (IC-6500, IC-6000, IC-4000 and SA-6500, SA-6000, SA-4000) the license allocation table is visible.
PRS-315976	An error message doesn't localize in Japanese when client from Network Connect mini browser.
PRS-315756	Pulse UI on Mac OS doesn't publish more than six connections.
PRS-315426	When Pulse is connected to a server with a VPN policy of "Search device DNS only", hard powering off a laptop and restarting it causes the login screen to take more than a minute to come up.
PRS-309845	Dashboard crashes during Host Checker policy evaluation.
PRS-309684	When SSL Acceleration is enabled, Pulse goes into reconnect mode when user signs out using the browser.
PRS-307945	Under certain scenarios when last login options are enabled, session cleanup is not being handled properly.
PRS-299313	A change to the way negative DNS responses are cached in Windows 8.1 can cause certain IPv4 destinations to be unreachable via Secure Application Manager tunnels on dual-stacked IPv4/IPv6 Windows 8.1 endpoints.

Noteworthy Changes in 8.0R7

This release addresses the issue described in the following Juniper Security Advisory: *http://kb.juniper.net/JSA10648*

Problems Resolved in 8.0R7

Table 15 describes issues that are resolved when you upgrade.

Table 15 Resolved in This Release

Problem Report Number	Description
PRS-318013, PRS-317942	JIS: Self upgrade results in UAC prompt for admin credentials
PRS-317503	Process check with Host Checker is validating only the first 15 characters.

PRS-317384	TNCS process crashes in some unknown scenarios under load.
PRS-317304	VMware View 6.0: HTML5 resource disconnect/freeze on IE10 and IE11 using re-write
PRS-317288	Syslog data not sent from license server
PRS-316791	Network Connect mini-browser support for IE6
PRS-316759	After a JIS upgrade both old and new versions are showing up in installed programs list. It should only show the new version as it performed an upgrade.
PRS-316669	IVE doesn't send Syslog over TCP after TCP connection broken
PRS-316517	Page gets stuck at "Generating Request" with IE browser when generating windows user certificate
PRS-316458	Read-Only Administrators have access to modify the URL in rewrite filters
PRS-316254	A request with disallowed characters is generated while accessing customer application
PRS-315774	Web becomes inaccessible and CPU touches 100% when ActiveSync is configured with Certificate authentication and CRL check for client certificates is enabled.
PRS-315708	img/src and script/src tags do not get rewritten
PRS-315688	Rewritten response from routing engine to browser includes HTTPonly cookies as well
PRS-315324	Pulse Collaboration is unable to connect when root level proxy exceptions are used.
PRS-315183	SA active node throws multiple web assertion during user logout during load.
PRS-314764	"Juniper: " is appended to syslog messages
PRS-314611	Memory utilization of dsSAMproxy.exe increases gradually when number of SAM connections via WSAM is more than 64.
PRS-313967	Users unable to establish IKEv2 session in some scenarios
PRS-313937	<localdomainsuffix> variable doesn't work for Web ACL policy.
PRS-313844	When user loses VPN tunneling due to Host Checker timeout, fatal errors are looping.
PRS-313614	LDAP is not completely recovering from transient connectivity issues until the processes are restarted
PRS-312383	Web process snapshot generated "Program web recently failed"; all users disconnected
PRS-311363	"CRL check started" access log sometimes is being logged on context of admin user.
PRS-310802	Active sync users cannot intermittently connect due to error failed in CRL checking; Status '3'; Detail: 'No valid CRL for revocation check'

PRS-310606	Rewrite server crash is observed when accessing a particular URL using SAML authentication
PRS-307622	24 hrs. timeframe does not show 24 hrs. data points on upgrade
PRS-305522	If the TCP connection to the syslog server is broken (for example when the syslog server is restarted), the TCP connection only gets re-established if there is no traffic for 15 minutes.
PRS-304546	ActiveSync traffic using client-certificate check with CRL enabled can result in web UI freeze when CRL size it big.
PRS-303798	Rewritten web URL is not displayed properly when "/" is encoded with "&frasl".
PRS-302621	Customer internal portal fails to open via PTP access because it contains more than one URL inside quote for a param's value.
PRS-297638	On the SA overview page the graphs for VPN Tunnel Users and Hits per sec might show extremely large incorrect values.
PRS-290518	On Mac OS, Network connect is not getting reconnected automatically after wake up from sleep mode.

Noteworthy changes in 8.0R6

Removal of AppAccel (WX) from this and subsequent releases on Junos Pulse

Support for AppAccel (WX) has been removed from this and subsequent releases of Pulse and the Pulse configuration.With the removal of WX this feature will no longer be installed with the Pulse client. Upgrading existing Pulse clients that have the AppAccel feature installed will result in this feature being removed. The Pulse UI will also reflect this by not showing the AppAccel portion since it will no longer be installed on the machine. If you have servers that have a Pulse connection set with WX connections then during server upgrade these connections are removed. This will result in version change for the connection set. When a Pulse client configured with a connection set containing the WX connection connects to the upgraded server that client will receive the upgraded connection set with no WX connection regardless if the client still supports WX or not. (999653)

Deprecating Steelhead optimization.

We are deprecating the Steelhead optimization in this release. Please refer to TSB16474 for additional information.

Problems Resolved in 8.0R6

Table 16 describes issues that are resolved when you upgrade.

Table 16 Resolved in This Release

Problem Report Number	Description

984996	Role variable <role> not working in personalized greeting.
1000605	When custom radius rules are configured IVE doesn't log Radius Reject messages.
996952	SAML: Redirect from SP not being honored.
1005071	SP (WebEx) returns an error message " SAML ASSERTION is unsigned (20) "
1002520	Automatic Version Monitoring sends wrong product type in case of IC devices.
1003683	Add MAC address to HC policy log messages in user access logs
926262	Bookmarks page fails to load after EES check completes.
927575	Fed Client is purging and re-exporting sessions during Fed Server cluster failover (A/P) and whenever fedclient connects to fedserver
982235	Presenter Viewer screen is blank on attendees meeting client UI.
985666	Pulse Collaboration Meeting UI re-launch not happening in certain scenarios
987707	Pulse Collaboration client intermittently crashes during Desktop sharing.
997395	Sharing desktop/application on company laptops gives blank grey screen.
947793	Pulse Collaboration through Auth proxy credentials are no longer passes seamlessly for the connection.
946513	During credential provider and smart card login with Junos Pulse when wrong smart card PIN was entered Junos Pulse keeps on connecting in the windows logon and does not return Wrong PIN message
1000766	When enable or disable the "Server certificate trust enforcement" at the system level for mobile there is not "Saved changes successfully." Message displays.
1000769	There is no way to include or exclude mobile related configuration during XML Import / Export operation under Maintenance-->Import/Export-->XML Import/Export page.
1000771	There is no Mobile tab is exported to XML file for a User role.
1001125	Import a previous release user configuration file will over write the current mobile setting to disable on the role level.

984831	When Junos Pulse is installed after hard powering off a laptop and starting it up again the time delay between pressing CTRL+ALT+DEL and login screen appearing is more than a minute.
988093	Logo does not appear on login page on Junos Pulse client on iPad
973534	Access log shows duration=0 and 'Closed connection to [IP ADDRESS] after 0 seconds' for tunnels that have been connected for a longer duration
979289	There are no DMI RPCs to view or configure ports that use a specific device certificate
936325	The netconf reply is missing the message-id causing RFC-compliant netconf clients to fail to work successfully.
992111	SRX firewalls are unable to remain connected to UAC A/P cluster in certain scenarios.
990204	Auto-reboot IVE if Cavium hangs and file system goes into read-only mode.
934402	Web server crashing when trying to parse a message from a client whose connection has been deleted
751346	VMWare View 5.0: "Disconnect and logoff" option in the vmimage is greyed out.
995198	Post-upgrade to 8.0R3.2 it has been reported that IE may not connect successfully using JICA
918534	Unable to access the backend server as applet URL was not getting correctly rewritten.
931576	Relative URLs with encoded characters are rewritten incorrectly; this may yield a page not found error.
960637	The rewriter is incorrectly modifying a resource, which uses the string "https://".
995712	Unable to open a DWF file through rewriter. DWF is a Design Web Format file developed by Autodesk.
998884	Unable to open OWA 2010 public folders upon upgrading to 7.4R9.3
1005511	Customer Internal resource shows error when accessed via Rewriter
989169	Missing frame content in JIRA application through SA rewriter on latest IE and Firefox browsers
990583	Custom application (mail module) is unable to load when accessing via Safari browser.
993129	In Internet Explorer 11 JavaScript errors observed, as "function.caller" is not accessible when strict parameter is used in JavaScript.

998065	Custom application does not load properly via rewriter.

Junos Pulse Secure Access 8.0R5 New Features

File Integrity Check during Boot up

The file integrity check is added to satisfy Common Criteria certification. File integrity check is performed at every system reboot to verify Juniper-built binary files. If the verification fails, a critical message is logged in the events log and message is also logged in the debug log with details of what failed.

New Junos Pulse Connect and Policy secure license SKU's

With the 8.0r5 release of the MAG Series gateway software, role specific licenses are being introduced in conjunction with the common access licenses. The Connect Secure licenses (CONSEC*) must be used on Junos Pulse Secure Access (SSL VPN) devices/personality only and Policy Secure (POLSEC*) licenses must be used on Junos Pulse Access Control (UAC) devices/personality only. Please refer to the Junos Pulse Ordering Guide and/or Admin Guide for further details

License JSA rollback and PAC license server side enforcement

Juniper had temporarily removed software-based license enforcement in its Pulse mobility products in SA/UAC versions 8.0/5.0 as part of evaluating a new licensing initiative. Please be advised that this release (8.0R5) will re-instate software-based license enforcement. The software-based license enforcement will be the same as in pre 8.0 releases.

Better logging for rewrite-server

978254: If the number of rewrite-server processes exceeds 1000 it is logged in the events log and sent as an SNMP message.

Problems Resolved in 8.0R6

Table 17 describes issues that are resolved when you upgrade.

Table 17 Resolved in This Release

Problem Report Number	Description
977889	Role mapping rules based on group membership may match incorrectly when using an AD/NT server instance with LDAP group search enabled if multiple rules share initial group name patterns (e.g. VPN-Group and VPN-Group-RDP)
973412	If the system local server instance is used with password management enabled AND the password change is at 8712-9999 days in the future, the password change constantly fails and user is unable to login

984983	Importing SAML metadata from the IDP without HTTP-Direct binding enabled may fail
954867	Custom sign-in pages for Meeting/Pulse Collaboration may show garbled UTF-8 characters
985519	Credential entry is not possible from mobile devices if the username and/or password label is long
965570	When launching JSAM with Java 7 update 51 user sees "Block & Don't Block " popup message.
949997	Proxy settings fail to be used when connecting from an IE 11 endpoint for VPN Tunneling
964979	Incorrect Windows Platform version reported in user agent string with Network Connect mini-browser for Windows 8.1
934779	If VPN Tunneling IP addresses are assigned via DHCP and there is high latency between the SA and DHCP server, the dhcpProxy daemon may crash
974820	When custom NOT rule is configured in Host Checker policy evaluation is failed with error message "Server has not received any information for this policy"
954701	Host Checker fails to detect XP SP2+ Windows firewall.
972354	If "Send Reason Strings" is disabled in policy and "Send Custom Instructions" is enabled, it is displaying "Server has not received any information for this policy" on Pulse UI under "Reason Strings" section.
963992	SA SPE running with VMware tools seen as out-of-date.
976039	'Decline' button does not appear with Junos Pulse (desktop) when using custom sign-in page
812263	Default gatekeeper settings require manual opening of the mpkg package for DMG-based install on Mac OS 10.8+
988668	When launching Pulse from the user bookmark page, an additional login prompt may be presented inside the Pulse client
970827	Pulse may fail to complete session resumption on Mac & Windows endpoints if roaming sessions are enabled for a select subnet and the user IP has changed inside that allowed range
998495	Windows Phone 8.1 clients may fail to pass Host Checker re-evaluation policies due to incorrect processing
990560	Excessive entries regarding process utilization may be recorded; if required, the frequency will be a minimum of 3 minutes with the number of suppressed messages recorded
952728	DMI-based XML import/export fails
846221	User limit set on a realm prevents license client from obtaining lease from license server.
999470	System snapshot may fail to complete and erroneously report another snapshot is in progress if taken during heavy load
940700	ACE authentication may trigger 100% CPU utilization

989521	Unable to establish L3 session with IC using Pulse after dot1x authentication.
935791	Virtual Desktop client fails to launch through Italian IE browser.
982665	Unable to open rewritten applets when using Siteminder authentication.
995407	Citrix Web interface resource profile configured for JICA fails from IE.
980997	Web: Ajax controls fail to auto-load when accessed via Safari.
938133	Client rewriting is not working as expected for custom JavaScript function 'showmodalDialog' with first argument as object where the native showmodalDialog JavaScript expects the first argument to be string.
951953	There is an attachment upload error with Lotus Notes 8.5.3 with ActiveX installed.
961895	Custom application fails to rewrite successfully in Chrome
972124	Color settings may be rewritten incorrectly on Firefox 20+
978712	Unable to edit, check in, or check out Office documents in SharePoint 2010 via rewriter.
986966	Authorization-only URLs (ActiveSync) access may fail.
984589	XLSM extension erroneously modified to .xls through rewriter
978259	If OWA 2010+ is configured as a long-lived resource AND the option to ignore periodic application activity is enabled, the session will not expire as expected. **NOTE**: Notifications are considered active/viable traffic and will be counted as session traffic
950590	Windows Terminal Service bookmarks fail to launch from IE when Italian language settings are applied
945102	License page does not display the installed license details correctly for other node in a cluster

Known Issues in this 8.0R6

Table 18 describes the open issues in 8.0R6

Table 18 Known Issues in this release

Problem Report Number	Description
999688	Junos Pulse (and OAC) UAC IPSec enforcement on Windows is performed in a Network (NDIS) Filter Driver. Other products such as IPSec based VPN clients may also perform IPSec processing in a Network Filter Driver. The order of processing of Network Filtering Drivers may affect interoperability between Junos Pulse UAC IPSec enforcement and third-party VPN clients. To minimize interoperability issues with Network Filter order UAC support forcing UDP encapsulation of IPSec traffic. When UDP encapsulation is enabled Junos Pulse IPSec packets will be correctly sent and received from the third-party VPN IPSec interface irrespective of Network Filter ordering.

Problems Resolved in 8.0R4

Table 19 describes issues that are resolved when you upgrade.

Table 19 Resolved in 8.0R4

Problem Report Number	Description
960853	JSAM upload log feature is not working with Java 7 update 51.
962767	Network Connect Client Check option on the client may be initialized erroneously
973499	Network Connect Auto Uninstall is not working when JIS is installed on a Windows workstation.
977550	Server side process for IKE (dsagentd) crashes when IKEv2 client connects over a network with packet loss and delays.
951935	Windows Mobile 6.1 users fail to connect to resources over WSAM when AES-128 and SSL Acceleration are enabled on the SA.

979567	Web process may not disconnect correctly and cause client connections to fail.
959061	When Administrator creates a new patch assessment policy the following warning is displayed on Admin UI "Patch Assessment functionality will be deprecated and a similar feature called Patch Management will be introduced in an upcoming release. Please refer to PSN at http://kb.juniper.net/TSB16374 for more details."
913784	If Host Checker is enforced on the role and the user failed policy evaluation for a policy with custom instructions enabled, but left blank, Pulse will report “Server has not received any information for this policy”
958117	Users are unable to create Junos Pulse Collaboration meeting.
965888	Pulse is unable to run session start/stop scripts from a network share accessible through the tunnel.
955023	If a client has IPv6 enabled, a machine on the same network may be able to reach the local IP despite the tunnel policy being set to enable traffic enforcement and disable split tunneling
949672	New PIN mode against an ACE server may cause the Radius process to crash
979853	Console login may fail for admin users with console access enabled.
927473	If license communication is configured for the external or management port, the license client may use excessive amounts of swap.
954485	ActiveSync/Authorization only access with client certificate check enabled and CRL checking is enabled may trigger the web interface to freeze (admin and user) for large CRLs.
927169	On an SA and UAC if the time zone for the system time is set to Jerusalem then the time change following DST policies of Israel will not occur.

945437	Citrix Desktop viewer Toolbar is not working in Citrix Xendesktop VDI profile
947823	Unable to upload a scanned file saved to a Web resource accessed via Web-Rewrite.
970920	Some button images for customer applications are not being rewritten.
929942	Rewriter process crashes sometimes in case of Kerberos SSO.
951953	Lotus Notes 8.5.3 with ActiveX may fail to upload attachments.
952779	The rewrite daemon may fail if the response has an empty HTTP status response.
963521	Web page redirection fails if "Un-rewritten pages open in new window" and "Optimize as long lived resource (no rewrite)" options are enabled.
971354	For iOS devices browser screen gets stuck on "Please wait..." if Network Connect/Pulse auto launch is enabled.
981147	Custom web application comment section fails to load.
977630	When the Citrix client is hosted on the IVE a user that does not have the Citrix client installed will now see the following message "The Citrix Client is not installed on your computer. Please click the button below to download and install the Citrix client".
971692	Terminal Resource profile with hostname/custom port not working when accessed from Windows 8.1 workstations.
954924	Users are unable to launch Secure Virtual Workspace on a Windows 64-bit workstation.

Problems Resolved 8.0R3.2 release

Table 20 describes issues that are resolved when you upgrade.

Table 20 Resolved in This Release

Problem Report Number	Description
981148	Includes fix for NC-FIPS client. Refer to JSA10623. For more detailed info please refer KB29004.

Problems Resolved in 8.0R3.1

Table 21 describes issues that are resolved when you upgrade.

Table 21 Resolved in This Release

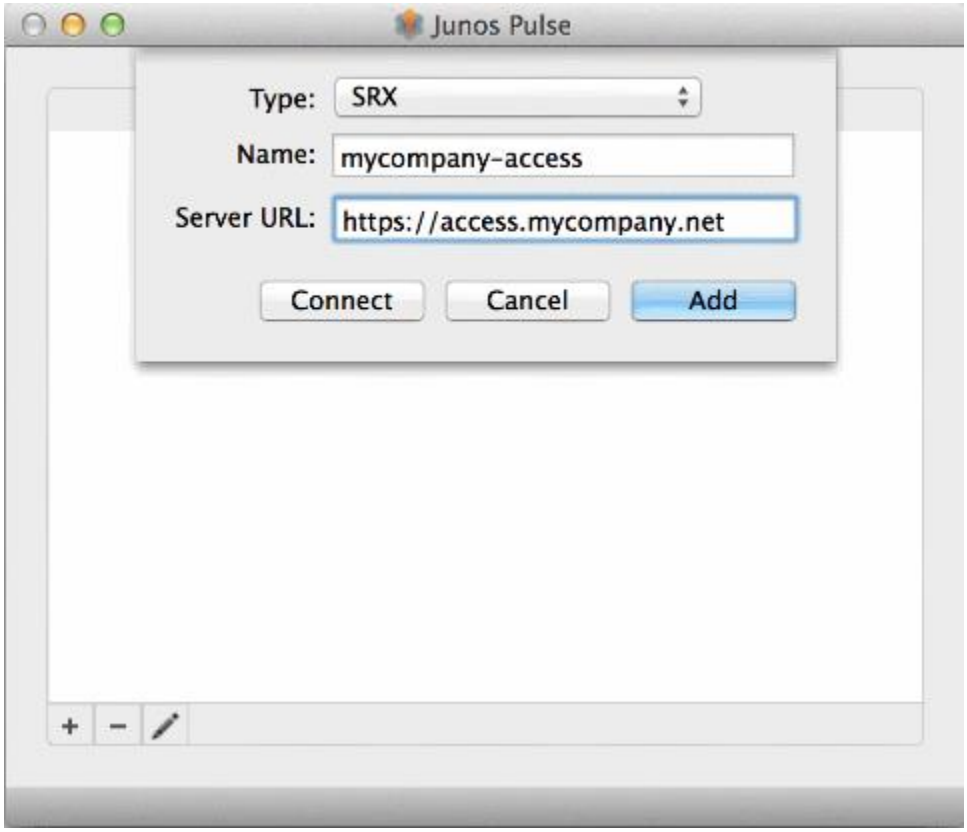
Problem Report Number	Description
981148	This release fixes the issue described in JSA10623. For more detailed info please refer KB29004.

Junos Pulse Secure Access 8.0R3 New Features

SRX Dynamic VPN Connections for Junos Pulse for Mac

Junos Pulse for Mac OS X adds support for Dynamic VPN tunnels to a Juniper Networks SRX gateway. Mac OS X endpoints can now use Junos Pulse client software to connect to SRX Branch series SRX100-SRX650 gateways that are running Junos OS Release 10.x or later, and that have dynamic VPN access enabled and configured. SRX gateways do not support deployment of the Mac version of the Junos Pulse Client. For deployment options for the Mac version of the Junos Pulse client, please read the Junos Pulse Admin guide.

Figure 1. Pulse for Mac



NOTE: The Junos Pulse Dynamic VPN functionality is compatible with SRX-Branch (SRX100-SRX650) devices only. SRX Data Center (SRX1400-SRX5800 – also called SRX HE or High End) devices do not support Junos Pulse Dynamic VPN from either Windows or Mac clients. For more details, please see KB 17436http://kb.juniper.net/InfoCenter/index?page=content&id=KB17436&smlogin=true..

Configuring a Junos Pulse Credential Provider Connection for Password or Smart Card Login

If you allow users to log in with smart cards or with a username/password, then you can have the Pulse credential provider automatically authenticate the user based on the login method. The Pulse user sees two different credential provider tiles for the Pulse connection, one for smart card authentication and one for username/password authentication. Credential provider tiles that launch a Pulse connection include a Pulse logo. See Figure 2. The Pulse connection determines which realm to use through preferred realm settings that you specify as part of the Pulse connection preferences. If the connection succeeds, the login type is saved so that, if re-authentication is needed, (for example, the connection times out), the same login type is used.

Figure 2. Pulse Credential Provider Tiles

Before you begin:

- Before you deploy a connection that uses this feature, make sure that you have created all the authentication realms that are required. You need one realm for smart card authentication and a different one for user name/password authentication. Both realms can be mapped to the same role or you can use different roles, and include a remediation role for endpoints that do not pass Host Checker evaluation. If you use machine authentication for a connection (machine-then-user-at-credprov), you need an authentication realm for the machine.
- Make sure that all of the realms that are used in the Pulse connection are included in the sign-in policy.
- The authentication realms on the Pulse server must be configured so that the Preferred Pre-login Smartcard Realm uses certificate authentication and the Preferred Pre-login Password Realm uses username/password authentication.

The following procedure summarizes the steps to create a Junos Pulse connection that uses credential provider authentication, and allows the user to choose either smart card login or username/password login. 0 describes the configuration options:

1. Click **Users > Junos Pulse > Connections** and create or select a connection set.
2. Create or edit a connection. For connection type, you can select either **UAC (802.1X)** for a Layer 2 connection or **SSL VPN or UAC (L3)** for a Layer 3 connection. The **SRX** and **App Acceleration** connection types do not support credential provider authentication.
3. For the Connection is established option, choose one of the credential provider options:
   - **Automatically at user login**—Enables Pulse client interaction with the credential provider software on the endpoint. The user credentials are used to establish the authenticated Pulse connection to the network, login to the endpoint, and login to the domain server.
   - **Automatically when the machine starts.** Connection is authenticated again at user login—Enables Pulse client interaction with the credential provider software on the endpoint. Machine credentials are used to establish the authenticated Pulse connection to the network using the specified Machine Connection

Preferences or Pre-login Connection Preferences. When the user provides user credentials, the connection is authenticated again.

4. For **SSL VPN or UAC (L3)** connections that are set to have the connection established automatically, you can define location awareness rules that enable an endpoint to connect conditionally.
5. For a Layer 2 connection that uses machine certificate authentication, make sure that the connection has an entry in the Trusted Server List. To allow any server certificate, type **ANY** as the Server certificate DN. To allow only one server certificate, specify the server certificate's full DN for example, `C=US; ST=NH; L=Kingston; O=My Company; OU=Engineering; CN=c4k1.stnh.mycompany.net; E=ausername@mycompany.com.`
6. For the desired connection behavior, set the connection preferences as described in Table 7.

Table 22 Configuration Options for Credential Provider Login

Pulse Client Credential Provider Login Behavior	Connection is established option	User Connection Preferences options	Pre-login Connection Preferences	Machine Connection Preferences
At user login, the user can choose from two credential provider tiles: smart card login or username/password login. The credentials are then used to connect to the network, login to the endpoint, and login to the domain server.	Automatically at user login	Preferred User Realm and Preferred User Role Set are not available if you specify values for Preferred Pre-login Password Realm Preferred Pre-login Smartcard Realm.	Enables Pulse credential provider tiles. The realm name appears on each tile. You must specify values for both of the following options: • Preferred Pre-login Password Realm—The authentication realm that provides username/password authentication. • Preferred Pre-login Smartcard Realm—The authentication realm that provides smartcard authentication.	Not available.
At machine login and at user login, the user can choose from two credential provider tiles: smart card login or username/password login.	Automatically when machine starts. Connection is authenticated again at user login.		Enables Pulse credential provider tiles. The realm name appears on each tile. • Preferred Pre-login Password Realm—The authentication realm that provides username/password authentication. • Preferred Pre-login Smartcard Realm—The authentication realm that provides smartcard authentication.	Preferred Machine Realm and Preferred Machine Role Set are not available if you specify values for Preferred Pre-login Password Realm Preferred Pre-login Smartcard Realm.

Updated NDIS Support

Junos Pulse for Windows includes a set of drivers that interface with the Windows Network Driver Interface Specification (NDIS) driver for communications with the endpoint's network interface. For Pulse 5.0R3, the NDIS5 compliant Juniper Network Agent (JNPRNA) has been replaced with the NDIS6 compliant Juniper Network Service (JNPRNS) to support enhanced functionality that is available in Windows Vista and later Windows versions. JNPRNA will continue to be available on Windows XP endpoints. Pulse on all other Windows versions will use JNPRNS. The Pulse for Windows file set changes are included in the *Junos Pulse Client Changes Guide 5.0R3.*

NOTE: JNPRNS does not support wired 802.1x for Odyssey Access Client (OAC). If OAC is already installed on the endpoint when you install Pulse 5.0R3, the new JNPRNS components will be installed to support Pulse, and the required legacy JNPRNA components will remain on the endpoint to support OAC functionality.

For more information about NDIS and upgrading to Pulse 5.0R3, see KB 28892.

Problems Resolved in 8.0R3

Table 23 describes issues that are resolved when you upgrade.

Table 23 Resolved in This Release

Problem Report Number	Description
971258	Windows non-admin users fail to install Network Connect, WSAM even when Juniper Installer Service in installed.
968526	Resource with basic authentication enabled does not open when accessed via Authorization-only sign-in policy.
962314	Network Connect client fails to translate based on end-user browser language preferences.
961761	If the web server fails to send chunk-size line, the rewrite engine may fail.
959763	On machines running Pulse 5.0r1 or 5.0r2, Pulse may freeze under certain conditions, including: * When the endpoint displays the splash screen after the device resumes from sleep * During the 'Remediating' state
956917	After upgrading the SA, IE9 may not download the new JavaScript files if a version is already cached.

Problem Report Number	Description
958557	Juniper client components (Host Checker, WSAM, Network Connect, Terminal Services, etc.) fail to download proxy .pac files if the server is configured with a non-standard (80, 443) port.
951953	Uploading an attachment results in error with Lotus Notes 8.5.3 with ActiveX installed.
952322	Carriage return are added to every line in Pulse Collaboration email invitation, this may cause user to fail login when clicking on the links to join Collaboration session.
939666	OpenSSL library may cause a rare crash.
952208	Hob applet (Premier Java RDP Applet) is upgraded to 3.3.0.785.

Known Issues in 8.0R3

Table 24 describes the open issues.

Table 24 Known Issues

Problem Report Number	Description
881922	Network Connect auto-uninstall does not work for the client users having admin privilege when Pulse or JIS is installed on the machine.
949997	Junos Pulse and Network Connect fails to connect when using client-side or server-side proxy with IE 11.

Problems Resolved in 8.0R2

Table 25 describes the problems resolved.

Table 25 Resolved in 8.0R2

Problem Report Number	Description
929171	When External User Records Management is enabled, if the number of active sessions exceeds the configured value for "Persistent user records limit" then the subsequent user login might fail.
925198	Password authentication policy page is missing from 7.2R1 if primary authentication server is Certificate and secondary authentication is enabled.

Problem Report Number	Description
951754	An end user with revoked certificate, having critical crlExtensions, is able to login, when certificate authentication is enabled
944239	Password feature under authentication policy for user realm is broken.
881922	Network Connect auto uninstall does not work for the client users having admin privilege.
935862	IKEv2 sessions get disconnected abruptly.
937176	WSAM UI uses Traditional Chinese instead of Simplified Chinese for Windows 7(Simplified Chinese)
952733	Host checker policy is not getting removed from the HC policy page though it is deleted. But refreshing the page again results in removing the policy from HC page.
952683	Clicking on ESAP link on Host Checker main page is always displaying list of products supported by active ESAP.
953541	Admin user is not warned when activating a sub-default ESAP package.
944660	The Antivirus product Super Security Zero 16.x fails to pass the number of updates check.
952926	Users fail to pass ESAP-based Host Checker policies with a client date later than Dec 13 2013 with ESAP older than 2.5.1
928964	Moving between logs page is displaying a log message "Unknown event SystemStatus" in debug log.
921871	Client fails to logon to a server, from a previously used ip address, due to presence of remnants of the older session.
900370	If the installation of Pulse is corrupted on an endpoint, users will be prompted to upgrade their Pulse client even though "Enable web installation and automatic upgrade of Junos Pulse Clients" is disabled."
897986	Pulse SSL tunnels provides less upload bandwidth than NC with SSL VPN tunnels. Pulse could take as much as two and a half times longer than NC. Exact performance variance depends on a number of factors, including underlying network substrate speed, server loading, etc. This performance discrepancy between Pulse and NC does not occur with VPN tunnels that use the UDP/ESP protocol, which is the default VPN protocol. Only users needing to use SSL due to the need to have FIPS compliance would experience this performance discrepancy.

Problem Report Number	Description
959240	Pulse fails to connect to SA with 'network error 1115' due to overloaded SBR process.
915552	After upgrading to JRE 7 Update 25,end users are receiving "An unsigned application from the location below is requesting permission to run “from java for SSH
947091	Post upgrade to 8.0, lab license does not contain IVS functionality any more.
911776	If an active/passive cluster is removed, the VIP cannot then be accessed when assigned to another port on the system.
915956	Unable to capture a filter for 64 bytes packets to a specific network
939534	Log query results with filters set do not show up correct data.
859959	Upgrading to a newer release in MAG is causing the process dsnetd to fail under specific conditions.
946820	Client side JavaScript rewriter fails to parse certain Hex Codes properly, resulting in HTTP 403 error for a particular option in SAP portal.
942158	The Microsoft ActiveX control, RSPrintClient, when used in Custom Applications fails to print document.
936312	SAP site using HTML5 and Kendo Controls fails to load completely via rewriter.
946720	Web pages are not loading via rewriter in rare cases when '#' is present in URL path.
955065	With JAVA 7 update 51, HOB and SSH applets fail to load with "Application blocked by Security Setting" warning.
960528	Pass through policy is not working, When selective rewriting policy for long-lived resource (no rewrite) and Pass through policy is configured for the same resource.
955427	Support for New Selective rewriting policy for long-lived resource (no rewrite) is added, Can be used for long-lived connections like OWA 2010 pending Request notification.
961761	Rewriter and hpproxy-server crashes when a backend server responds without chunk size and Transfer-encoding: chunked header set.

Known Issues in 8.0R2

Table 26 describes the open issues in 8.0R2.

Table 26 Known Issues in 8.0R2

Problem Report Number	Description
971258	Windows non-admin users fail to install Network Connect, WSAM even when Juniper Installer Service in installed.

Documentation

Pulse Connect Secure documentation is available at https://www.pulsesecure.net/support.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@pulsesecure.net

Technical Support

When you need additional information or assistance, you can contact Pulse Secure Global Support Center (PSGSC):

- http://www.pulsesecure.net/support
- 1-844-751-7629 within the United States
- 1-408-300-9668 from outside the United States

Revision History

Table 27 lists the revision history for this document.

Table 27 Revision History

Revision	Description
August 11, 2014	Initial publication.
March 24, 2015	8.0R10 draft
May 22, 2015	8.0R11 draft
August 7, 2015	8.0R12 draft
September 24, 2015	8.0R13 draft