Pulse Connect Secure Release Notes

8.1 R3.2 Build 36361:
May 2015
Revision 00

Contents

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 8.1R1.1 release to 8.1R3.2. The 8.1R1 release notes still apply except for the changes mentioned in this document. Please refer to 8.1R1 release notes for the complete version.

NOTE: This Pulse Connect Secure maintenance release introduces new features. These new features are documented in this document.

Interoperability and Supported Platforms

Please refer to the *Pulse Connect Secure 8.1R1 Supported Platforms Guide* for supported versions of browsers and operating systems in this release.

Problems Resolved in 8.1R3.2 Release

Table 1 describes issues that are resolved when you upgrade.

Table 1 Resolved in This Release

Problem Report Number	Description
PRS-325984	Under high load of VPN tunnels, a process crash might be seen.
PRS-326751	On a Windows platform, when upgrading Pulse desktop from an older release to Pulse5.1r3 or Pulse5.1r3.1, the openssl libraries will not get upgraded.

Known Issues in 8.1R3.2 release

Table 2 describes the open issues in 8.1R3.2 release

Table 2 Known Issues in 8.1R3.2 release

Problem Report Number	Description
PRS-327235	On a Windows 7 Virtual Machine, NC FIPS fails to connect to SA after upgrading to 8.1R3.2

PRS-295093	The Pulse Mobile Onboarding functionality does not work in this release.

Problems Resolved in 8.1R3.1 Release

Table 2 describes issues that are resolved when you upgrade.

Table 2 Resolved in This Release

Problem Report Number	Description
PRS-325765	PKCS7 NULL pointer dereferences fix (CVE-2015-0289)
PRS-325766	ASN.1 structure reuse memory corruption fix (CVE-2015-0287)
PRS-325868	Segmentation fault in ASN1_TYPE_cmp fix (CVE-2015-0286)
PRS-325767	Base64 decode (CVE-2015-0292)
PRS-325768	Use After Free following d2i_ECPrivatekey error fix (CVE-2015-0209)

For more details, please read the public advisory at
https://kb.juniper.net/InfoCenter/index?page=content&id=TSB16661

Pulse Connect Secure New Features in 8.1R3

Captive Portal Detection

This feature is to have Pulse detect when it is at a hotspot, and delay its connections until internet access is granted. Additionally Pulse will display enough status so that the user can understand what is happening, and can be directed to take appropriate action. An Admin UI option has been added so this feature can be enabled or disabled by the administrator.

Currently depending on the specifics of the hotspot, Pulse currently exhibit one of the behaviors below, all of which are not very helpful to the end user.

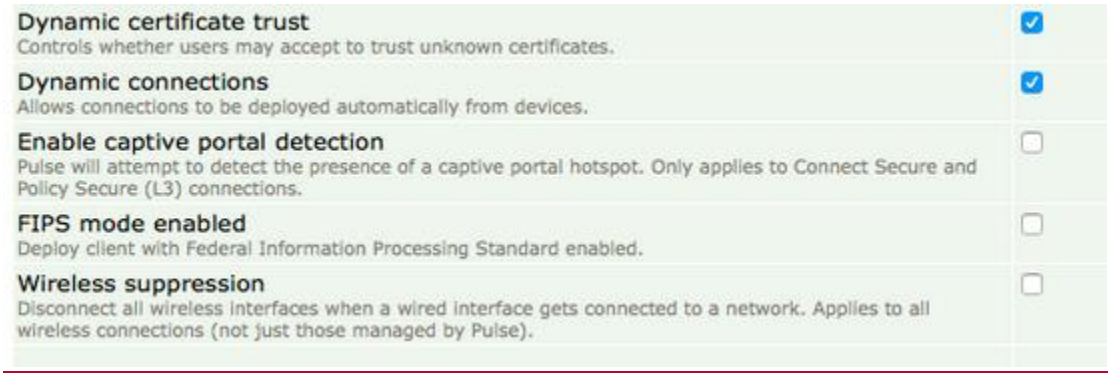
- Display an error
- Display a trust prompt with the certificate of the portal
- Remain in the “connecting” stat with no error message

With this new feature, whenever Pulse Desktop attempts a connection to an SA or IC, it will first detect if it is in a captive portal and if so, notify the user of this condition. The notifications include:

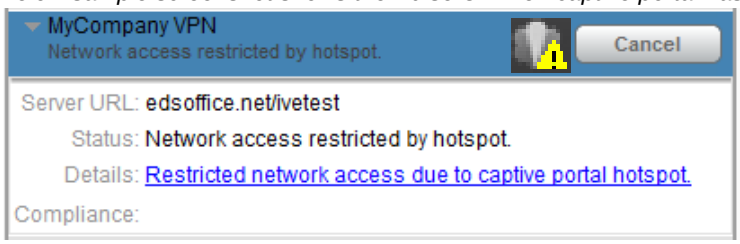
- Displaying a new message on the tray rollover
- Displaying a new tray icon
- Displaying a new status for the connection on the main UI
- Displaying a new icon for the connection on the main UI

Pulse then periodically reattempts the connection, and continues to display the notifications as long as Pulse is in the captive portal. Once the user has authenticated to the captive portal (e.g. using a browser), Pulse will detect that it is no longer in a captive portal, and will attempt to connect to the IVE as usual, and display the normal icons and status messages.

Below sample screenshot shows the Admin UI option Administrator can enable:



Below sample screenshot shows the Pulse UI when captive portal has been detected:



Noteworthy changes in this Release

The goal of this feature is to have Pulse detect when it is at a hotspot, and delay its connections until internet access is granted. Additionally Pulse will display enough status so that the user can understand what is happening, and can be directed to take appropriate action. An Admin UI option has been added so this feature can be enabled or disabled by the administrator.

Problems Resolved in 8.1R3 Release

Table 3 describes issues that are resolved when you upgrade.

Table 3 Resolved in This Release

Problem Report Number	Description
PRS-325285	L2/802.1x connection does not timeout even if the L3 TCP connection to the Pulse Policy Secure (PPS/IC) is lost
PRS-324164	Multicast traffic may cause the web daemon to use 100% of the available CPU
PRS-324108	Captive Portal Detection can now be enabled/disabled through the admin UI
PRS-324033	Relative URL rewriting fails when backslashes are used in conjunction with query strings
PRS-323933	Hosts file entries fail to populate on Mac OS clients
PRS-323861	All nodes in a cluster send syslog data even though log data is synchronized. The fixed behavior is that only the node marked as 'LEADER' will forward the log data to the syslog server
PRS-323699	In the event of user session deletion or time out, the Pulse Secure client reconnects to the last used IP rather than issuing a new DNS lookup
PRS-323615	Captive Portal detection prevents successful connections if there is no rejection of the HTTP probe
PRS-323598	If a VPN session is active and a user attempts to login to a second system, the client continually authenticates to the second node
PRS-323447	No process dump was created for a specific daemon
PRS-323435	URL redirection may trigger an erroneous captive portal message on the Pulse Secure client
PRS-323028	Extraneous log message recorded on the console during upgrade
PRS-322973	Web server may crash when malformed IP packet is received at IVE.
PRS-322710	Web applications that include *DSID* in the name may cause connection failure for Pulse Secure helper software
PRS-322112	Rewrite engine may fail to rewrite application functions correctly and cause the page not to load
PRS-321885	DNS and NetBIOS lookups prevent WSAM from hitting idle session timeout

PRS-321800	SSL cipher settings changes are not recorded in the admin and event logs
PRS-321629	AD authentication may not correctly fallback to secondary DNS server if the primary is unreachable
PRS-320605	TLS syslog authentication is not initiated immediately in the event of disconnect
PRS-320571	HTML5-based VDI sessions may trigger 100% system resource utilization
PRS-320296	Port values for bookmarks are not parsed correctly when the bookmark is defined as <userAttr.url>

Known Issues in this release

Table 4 describes the open issues in this release

Table 4 Known Issues in this release

Problem Report Number	Description
PRS-326413	IVS syslog messages are sent over the management port

Pulse Connect Secure Access New Features in 8.1R2 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

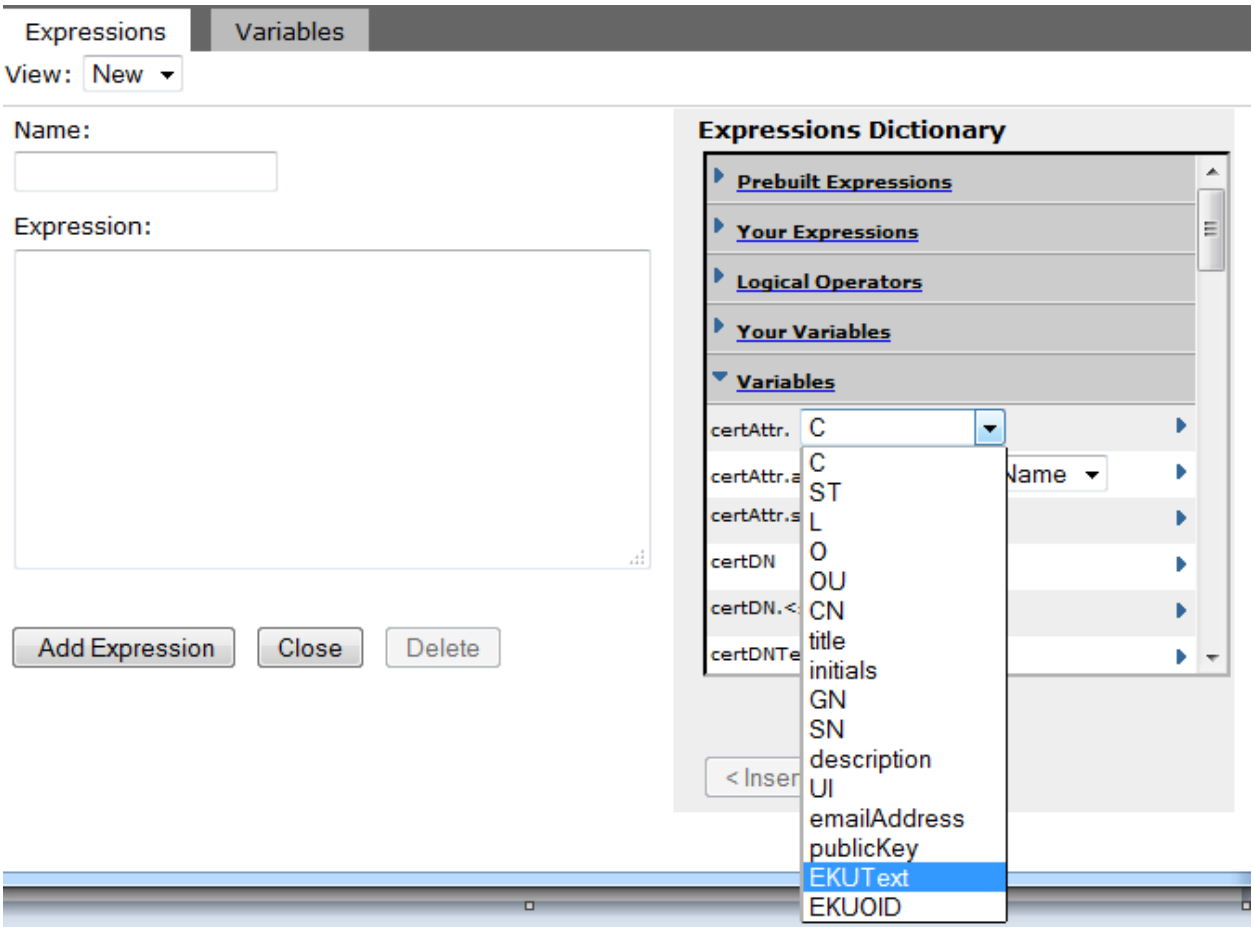
NOTE: This setting controls only connections into the device (Inbound Settings) and does not dictate settings for SSL connections that are initiated by the IVE.

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:

8.1R2 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 8.1R2 Release

Table 5 describes issues that are resolved when you upgrade.

Table 5 Resolved in This Release

Problem Report Number	Description
PRS-322649	certificate auth fails due to memory corruption when CRL CDP URL is more than 60 characters
PRS-322543	When the role is configured with "Allow VPN through firewall" option, a process memory leak can occur.
PRS-322486	Slow import/export on fed client after upgrading to UAC 5.1R1 on Fed Server and Fed Clients.
PRS-322365	HTTP 500 Internal error occurs while uploading a file in a environment which has delay or low bandwidth via Authorization Only access.
PRS-322303	SNMP MIB values being reported incorrectly in Pulse Secure Access 8.0.
PRS-322154	Rewriting large XML data may trigger rewrite-server process crashes.
PRS-322073	Updated DNS server values at System>Network>Overview may not be immediately loaded.
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-321843	As long as no change in cipher switching between FIPS ON or FIPS OFF should not prompt for saving the setting.
PRS-321783	TLS 1.1 cipher negotiation fails
PRS-321692	UI option under System -> Configuration -> Security -> SSL Options have been changed to allow selection of TLS versions.
PRS-321666	Base64 data containing carriage returns or line feeds fail for SAMLRequest processing.
PRS-321659	On-boarding VPN profile creation fails for VPN on Demand when using wildcard certificates

PRS-321657	Profile installation fails on iOS 8.1 devices if vpn-ondemand is enabled for a vpn profile.
PRS-321651	iveSSLConnections reported erroneously for snmpwalk
PRS-321590	VA-DTE: Onboarding feature is NOT visible
PRS-321533	Certificate fields are enhanced to use EKU in custom expressions.

Known Issues in 8.1R2 release

Table 6 describes the open issues in this release

Table 6 Known Issues in this release

Problem Report Number	Description
PRS-324077	User isn't automatically connected to the server after a browser based upgrade from a Pulse 5.0-based client to a Pulse 5.1-based client.

Documentation

Junos Pulse documentation is available at http://www.juniper.net/techpubs.

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@juniper.net.

Technical Support

When you need additional information or assistance, you can contact Juniper Networks Technical Assistance Center (JTAC):

- http://www.juniper.net/support/requesting-support.html
- support@juniper.net
- 1-888-314-JTAC within the United States
  1-408-745-9500 from outside the United States

For more technical support resources, browse the support website (http://www.juniper.net/customers/support/#task).

Revision History

Table 7 for Revision History

Revision	Description
27 May 2015	Initial publication.