Pulse Secure

Pulse Connect Secure

Release Notes

Release, Build	**8.1R6 39491**
Published	**October 2015**
Document Version	**1.0**

Contents

INTRODUCTION **4**

INTEROPERABILITY AND SUPPORTED PLATFORMS **4**

NEW FEATURES IN PULSE CONNECT SECURE 8.1R6 ..... **4**

PROBLEMS RESOLVED IN 8.1R6 RELEASE **5**

Table 1: Resolved in This Release *5*

KNOWN ISSUES IN 8.1R6 RELEASE **6**

Table 2: Known Issues in This Release *6*

NEW FEATURES IN PULSE CONNECT SECURE 8.1R5.1 ..... **7**

PROBLEMS RESOLVED IN 8.1R5.1 RELEASE **7**

Table 3: Resolved in This Release *7*

KNOWN ISSUES IN 8.1R5.1 RELEASE **7**

Table 4: Known Issues in This Release *7*

NEW FEATURES IN PULSE CONNECT SECURE 8.1R5 ..... **7**

LDAP Group Sync Integration for Pulse Workspace Auto-provisioning 7

Enhanced Logging for OCSP Enhancement 8

NOTEWORTHY CHANGES IN 8.1R5 RELEASE **8**

SECURITY ISSUES RESOLVED IN 8.1R5 RELEASE **8**

PROBLEMS RESOLVED IN 8.1R5 RELEASE **8**

Table 5: Resolved in This Release *8*

KNOWN ISSUES IN 8.1R5 RELEASE **10**

Table 6: Known Issues in This Release *10*

NOTEWORTHY CHANGES IN 8.1R4.1 RELEASE **11**

PROBLEMSRESOLVEDIN8.1R4.1 RELEASE **11**

Table 7: ResolvedinThisRelease *11*

KNOWN ISSUES IN 8.1R4.1 RELEASE **11**

Table 8: Known Issues in This Release *11*

NOTEWORTHY CHANGES IN 8.1R4 RELEASE **12**

Table 9: Resolved in This Release *12*

PROBLEMSRESOLVEDIN8.1R4 RELEASE **12**

Table 10: Resolved in This Release *12*

KNOWN ISSUES IN 8.1R3.2 RELEASE **14**

Table 11: Known Issues in This release *14*

PROBLEMSRESOLVEDIN8.1R3.1 RELEASE **14**

Table 12: Resolved in This Release *14*

PULSE CONNECT SECURE NEW FEATURES IN 8.1R3 ..... **14**

Captive Portal Detection 14

NOTEWORTHY CHANGES IN 8.1R3 RELEASE **15**

PROBLEMS RESOLVED IN 8.1R3 RELEASE **16**

Table 13: Resolved in This Release *16*

KNOWN ISSUES IN 8.1R3 RELEASE **17**

Table 14: Known Issues in This Release *17*

NEW FEATURES IN PULSE CONNECT SECURE 8.1R2 RELEASE **17**

DISABLE TLS 1.0 17

CREATE ROLE MAPPING RULES BASED ON EKU FIELD OF CERTIFICATE 18

PROBLEMS RESOLVED IN 8.1R2 RELEASE **18**

Table 15: Resolved in This Release *18*

KNOWN ISSUES IN 8.1R2 RELEASE **19**

Table 16: Known Issues in This Release *19*

DOCUMENTATION **20**

DOCUMENTATION FEEDBACK **20**

TECHNICAL SUPPORT **20**

REVISION HISTORY **20**

Table 17: Revision History *20*

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 8.1R6. 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 maintenance release introduces new features. These new features are documented in this document.

Interoperability and Supported Platforms

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

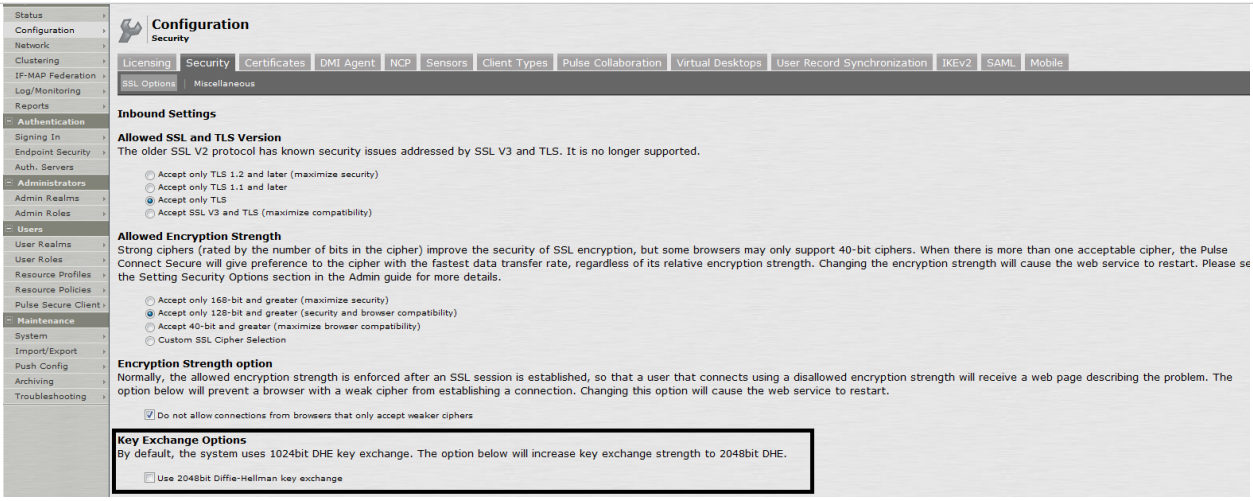
New Features in Pulse Connect Secure 8.1R6

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 an SSL client and an SSL 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 8.1R6 Release

Table 1 describes issues that are resolved when you upgrade.

Table 1: Resolved in This Release

Problem Report Number	Description
PRS-327644	Log archiving may fail intermittently.
PRS-330765	When using the rewriter, "Add Expense report" functionality in PeopleSoft ERP 9.2 fails.
PRS-330678	When the policy, “Don't rewrite content: Redirect to target web server” is configured for a large FORM POST then this might result in a rewrite process crash.
PRS-330432	Some Pulse users might having trouble setting up a connection when the Pulse Connect Secure device is under load.
PRS-330047	When using certificate authentication with IKEv2 tunnels and Activesync connections, the memory usage on the device can grow.
PRS-333033	When using IKEv2 functionality, there is a per connection memory leak.
PRS-329556	Access to shared drive within a web resource through web rewrite fails.
PRS-329334	When both primary and secondary authentication are used, Pulse user is unable to change secondary password when it expires.
PRS-328952	Users are unable to connect to PCS through WSAM/NC when Microsoft provided registry entries to disable DHE Cipher suites are set in the client machine.
PRS-328902	Syslog messages do not contain 'PulseSecure' string in them. Syslog messages will now contain the “PulseSecure” string
PRS-328239	The agent type for Pulse users on Windows 10 show up as "Windows Vista Pulse Secure" on the Active

	Users page. This has now been fixed to display "Windows 10 Pulse Secure."
PRS-328234	When Pulse Secure client on devices running Chrome OS is used, Pulse Connect Secure will display wrong agent type, "Pulse Secure Inbox Plugin", on "Active Users" page after SSL VPN connection is established. This has now been corrected to display, "Chrome OS Pulse Secure App".
PRS-327913	Network Connect does not lease an IP correctly on Windows 10.
PRS-326870	When rewriting a web page that contains VBScript, the rewrite server process might crash.
PRS-326846	Pulse and Network Connect tunnels are unable to connect if Bandwidth management is enabled.
PRS-325965	Sometimes long lived SAML server processes can lead to higher swap memory utilization.
PRS-325502	Automatic DNS registration fails for Network Connect.
PRS-324850	ACL count in user access logs is incorrect after removing duplicate IP table entries.
RS-323482	Windows 'Onboard' button is missing on end user home page on Windows 10 OS.
PRS-323316	RADIUS process may use excessive memory due to high volume of incomplete authentications.
PRS-320571	HTML5 resource access causes 100% CPU and the PCS becomes unreachable.
PRS-319166	Troubleshooting page options greyed out on clicking the Guidance link.
PRS-318593	When accessing desktop sessions over HTML5, the webserver may crash in an environment with network delays.
PRS-318426	If a VPN tunneling is used by multiple roles and a user maps to multiple roles that use the same ACL, the ACL limit is reached prematurely.
PRS-312175	Pulse fails to upgrade if the initial connection is through machine authentication.
PRS-331187	Client applications in 8.1R1 and earlier fail to launch when Pulse Setup Client 8.1R2+ is installed.

Known Issues in 8.1R6 Release

Table 2 describes the open issues in 8.1R6 release

Table 2: Known Issues in This Release

Problem Report Number	Description
PRS-333494	On Mac OS X endpoints, Pulse Collaboration and JSAM launch fails to launch unless the user installs Java

PRS-333645	On Windows 10, there are intermittent connection failures with Network Connect after Network Connect has been uninstalled and then relaunched.

New Features in Pulse Connect Secure 8.1R5.1

No new features have been added to 8.1R5.1 Release. It just has defects fixes related to Pulse One as mentioned in the Problems Resolved section below.

Problems Resolved in 8.1R5.1 Release

Table 3 describes issues that are resolved when you upgrade.

Table 3: Resolved in This Release

Problem Report Number	Description
PCS-2577	REST send/receive update fails due to REST thread in SA went into deadlock state
PCS-2511	Wrong Auth Failure count displayed on the PulseOne console
PCS-2385	Config upload fails to retry after two failed attempts
PCS-2367	Configuration Upload to Pulse One server fails following a DNS address change
PCS-2317	If registration fails because Pulse One unreachable, appliance displays bad message

Known Issues in 8.1R5.1 Release

Table 4 describes the open issues in 8.1R5.1 release

Table 4: Known Issues in This Release

Problem Report Number	Description
NA	NA

New Features in Pulse Connect Secure 8.1R5

LDAP Group Sync Integration for Pulse Workspace Auto-provisioning

PCS appliance can be integrated with the Pulse Workspace console server (PWS) to auto-provision

Workspace for mobile devices based on user's LDAP group membership.

Enhanced Logging for OCSP Enhancement

This feature is an enhancement in our user access logs to show detailed logging information during the process of Certification Revocation Check using OCSP Protocol. There are no UI enhancements as part of this feature.

With this enhanced logging, when user has multiple OCSP Responder Server for the Client Certificate Revocation Check and Need to know at any given point in time the following information is provided in the User Access Logs:

I. Which user name whose certificate is checked for Revocation against which OCSP URL of the responder Server holding what IP Address.

II. OCSP Revocation Checking Start Message, IVE Send Request to OCSP Responder Server Message, OCSP Responder Response Message (both OCSP Error Response and OCSP Valid Response Info), and OCSP Revocation Checking Succeeded Message.

Noteworthy Changes in 8.1R5 Release

The "Pulse One" menu option has moved from the main menu. This option is now available under "Settings" -> "Configuration" -> "Pulse One".

This release of 8.1R5 (or 5.2R3 as applicable) comes with Pulse One option enabled.
However, this option is not available for use until Pulse One SaaS application is officially released. For additional details on Pulse One, please click on **https://www.pulsesecure.net/products/pulse-one**

Security Issues Resolved in 8.1R5 release

Table 5 describes issues that are resolved when you upgrade.

Table 1 Security Issues Resolved in This Release

Problem Report Number	Description
PRS-327861	TLS issue with SA server (Finished message) (CVE-2015-5369)

Problems Resolved in 8.1R5 Release

Table 5 describes issues that are resolved when you upgrade.

Table 5: Resolved in This Release

Problem Report Number	Description
329943	Accessing certain Office 365 OWA features through rewriter gives an error.
329631	If JIS is installed, after upgrade, user sees popup error while downloading setup client.
328574	After upgrading during the first reboot(post-install) prints error messages like VM- integer expression expected
328558	Contents in Iframe are not rendered properly through SA after upgrade.
328518	Proxy-server is crashing when PTP policy is available for the URL inlocation header.
328277	Secure Meeting does not launch on Windows 10 when using a browser with Java delivery.
327662	Logoff on connect feature is causing Network connect to remain in connecting state during login into windows after initial logoff.
327629	Access of webmail via Office 365 through the rewriter fails.
327478	Not able to change RESOURCE and POST URL in SSO for Citrix Storefront.
327437	When using DHCP to assign VPN tunneling IP address DNS suffix within the DHCP offer is incorrectly parsed.
327393	In certain cases when backend server sends data character by character the rewriter fails to inject the preclude.
326609	wrong source IP gets displayed in the user access logs as the secondary auth is successful before the primary auth when a user tries to authenticate to PCS configured with dual auth.
325564	Executing SNMP GET IfOperStatus command on PCS returns an incorrect interface status.
320740	Automatic replies cannot be managed through Firefox when the session timer is enabled
319363	When PCS acts as an SP and received an SAML AuthnRequest which contains unsupported authn context refs than it rejects it.
317413	Modifying inner HTML property which is readonly in certain cases is causing runtime exception in Internet Explorer
325487	There is no mechanism available for Pulse connect secure admin to delete the stale Activesync device records when the appliance is not an activesync provider anymore on the Pulse workspace console.
325527	When a Pulse workspace admin selects a different appliance as the activesync provider, the activesync records from the previous appliance are not deleted.
325330	The notification with respect to configuration options applicable for Pulse workspace onboarded devices should be placed correctly.
325505	Admin delete action should be denied for the role which is currently enabled for Pulse workspace onboarded devices under Pulse One Active Sync Handler Configuration.

3255497	Roles which are not enabled with secure email feature should not get listed in the Activesync Handler configuration options.
330819	Host Checker on Windows 10 is stuck on Loading Components screen.

Known Issues in 8.1R5 Release

Table 6 describes the open issues in 8.1R5 release

Table 6: Known Issues in This Release

Problem Report Number	Description
PRS-319166	During AD configuration, troubleshooting page options are greyed out on clicking the Guidance link
PRS-330371	Web: Session timer prevents the out of office/automatic reply page from completely loading on Firefox
PRS-329828	NC_GINA: NC GINA is reporting failed authentication
PCS-2047	User Group membership would fail for Pulse Workspace if the users are from the sub domain of the configured LDAP domain.
PCS-2149	Pulse Workspace group validation might fail if the Group has members or memberOf Groups from sub domains.
PCS-2033	Pulse Workspace user membership search and group validation results in invalid data if the configured LDAP servers are not reachable.
PCS-2364	Pulse Workspace User membership search can result in invalid data if the users are from different domains.
PCS-2253	Importing XML configuration of Pulse One ActiveSync role settings throws a warning message: 'Invalid path-reference', but saves the configuration successfully.

Noteworthy Changes in 8.1R4.1 Release

PSA300, PSA3000, PSA5000, PSA7000c, and PSA7000f new hardware models are supported from this release onwards. Please refer to PSA New Hardware Guide (will update with correct link) for more information.

PSA7000c and PSA7000f models have LCD in the front panel that shows basic information of the system.

PSA7000c and PSA7000f models have software RAID1 support. Handling of disk failure in software RAID is different compare to hardware RAID in the older hardware MAG. Admin needs to remove a disk from the RAID and add a disk to the RAID through admin console. Please look at the admin guide for more details.

Problems Resolved in 8.1R4.1 Release

Table 7 describes issues that are resolved when you upgrade.

Table 7: Resolved in This Release

Problem Report Number	Description
PRS-329943	Accessing certain Office 365 OWA features through rewriter gives an error.
PRS-329631	If JIS is installed, after upgrade, user sees popup error while downloading setup client.

Known Issues in 8.1R4.1 Release

Table 8 describes the open issues in 8.1R4.1 release

Table 8: Known Issues in This Release

Problem Report Number	Description
PRS-327629	Unable to access webmail via Office 365 through the rewriter. The workaround is to create a selective rewrite policy for URL https://r1.res.office365.com/owa/prem/16.0.751.21/scripts/boot.worldwide.0.mouse.js with action as "Don't rewrite content: Do not redirect to target web server"
PRS-329814	PSA7000c and PSA7000f don’t send SNMP trap for power supply.
PRS-328992	On PSA7000c and PSA7000f LCD, internal IP shows blank before internal IP is configured.
PRS-328986	When license server is not responding, HTML error is shown on licensing configuration page instead of a user-friendly error.

PCS-1092	Fiber ports negotiates highest link speed by default thus Configure Link Speed doesn't work for fiber ports on PSA7000f models.
PRS-329376	After doing clear config on the system, it takes a couple of minutes before fan and RAID status is shown in SA admin page.
PRS-328442	PSA300 and PSA3000 models do not show CPU temperature.
PRS-328991	New hardware - LCD testing - Internal IP is not displaying as disabled when it gets disabled
PRS-328993	Occasionally after factory reset, on PSA new hardware, MTU is showing as zero by default in external port settings

Noteworthy Changes in 8.1R4 Release

Table 9 describes issues that are resolved when you upgrade.

Table 9: Resolved in This Release

Problem Report Number	Description
PRS-323214	An option has been added in the admin console so that Pulse client doesn't automatically reconnect after the session ends.
PRS-325752	In the welcome message of the sign in page, the admin can now include hyperlinks with VMWare-View custom protocol (vmware-view://). The set of allowed hyperlinks are now vmware-view, http, https, mailto, ftp.

Problems Resolved in 8.1R4 Release

Table 10 describes issues that are resolved when you upgrade.

Table 10: Resolved in This Release

Problem Report Number	Description
PRS-327235	Network Connect using FIPS mode may not connect successfully using Windows 7.
PRS-325984	dsagentd or cache-server may crash (create process snapshots) under high VPN Tunnel load
PRS-327099	Signature verification for Host Checker binaries are taking more than 30 secs in some instances, which is causing the timeout in SetupClient.
PRS-326964	Host Checker fails to launch when the MMF name does not match between the installed version (Juniper) and updated version (Pulse Secure).
PRS-326748	If there are duplicate VPN tunneling ACLs assigned to a user then the order of evaluation of the policies might be reversed from the chronological order.

PRS-326276	In cases where session roaming is enabled for users, the cache may grow excessively large and could lead to a crash.
PRS-325375	Captive Portal detection error may be triggered if there is HTTP 302 response code received while connecting to IVE.
PRS-324825	Using a 3rd party Host Checker policy for OPSWAT Gears may cause corrupt/garbled characters to display when the policy fails.
PRS-324749	With Pulse, Host Checker fails to delete the files from the path specified with <USERHOME> as environmental variable.
PRS-324544	The get-active-users DMI RPC doesn't work.
PRS-324526	JIRA may not rewrite properly using IE 9 (404 messages or display rendering errors).
PRS-324480	High CPU usage may be observed when using ActiveSync enforcement on authorization only access URL configuration.
PRS-324055	Host Checker custom rule using environmental variable %LOCALAPPDATA% fails with Pulse.
PRS-323298	Logging: Policy trace fails to be cleared on IVS.
PRS-322856	An invalid DNS failure response from an external DNS server that is received by the Pulse Secure server may cause dsagentd to crash.
PRS-322740	The Pulse Secure client may be unable to connect if a pre-signin notification is configured with Host Checker
PRS-322687	ICMP error messages are sent with the physical port address rather than the VLAN address
PRS-322071	Network Connect fails to restore PAC settings if the client machine is forcefully/abruptly rebooted
PRS-322044	Host Checker remediation messages are presented twice when using Defender RADIUS
PRS-320448	If VPN tunneling is configured for DHCP-based IP address assignment AND a Pulse or Network Connect user connects and disconnects in rapid succession, the IP may be leased successfully on connection and not released upon disconnect
PRS-324747	There was an error parsing the "match" method in the clientside javascript parser.
PRS-323067	When a PCS/PPS client successfully pulls a feature license from the license server, invalid license count numbers may be recorded

Known Issues in 8.1R3.2 Release

Table 11 describes the open issues in 8.1R3.2 release

Table 11: Known Issues in This 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 12 describes issues that are resolved when you upgrade.

Table 12: 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**)
PRS-320183	In IVS, Syslog messages sent to syslog server are sent from management port.

For more details, please read the public advisory at
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/SA40001

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.

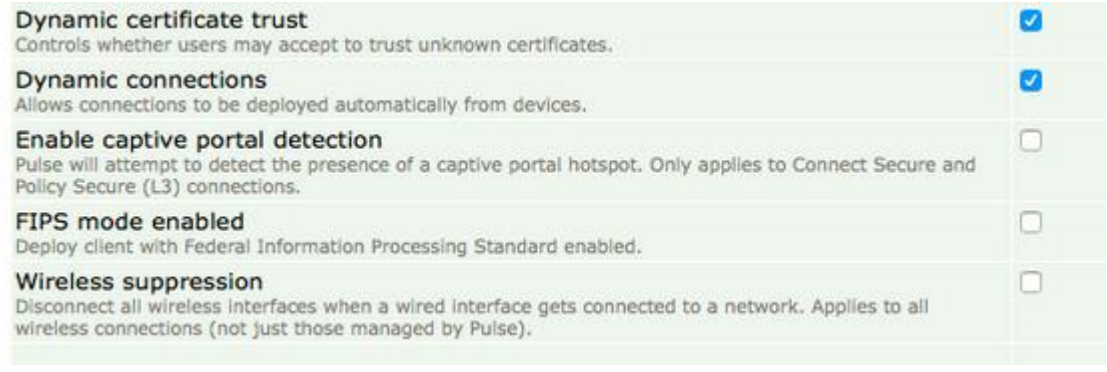
- Display an error
- Display a trust prompt with the certificate of the portal
- Remain in the “connecting” stat with no error message

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:

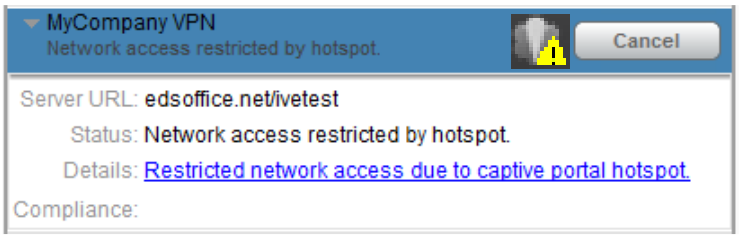
- Displaying a new message on the tray rollover
- Displaying a new tray icon
- Displaying a new status for the connection on the main UI
- Displaying a new icon for the connection on the main UI

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.

The sample screenshot below shows the Admin UI option Administrator can enable:



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



Noteworthy Changes in 8.1R3 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 13 describes issues that are resolved when you upgrade.

Table 13: 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-320296	Port values for bookmarks are not parsed correctly when the bookmark is defined as <userAttr.url>

Known Issues in 8.1R3 Release

Table 14 describes the open issues in this release

Table 14: Known Issues in This Release

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

New Features in Pulse Connect Secure 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

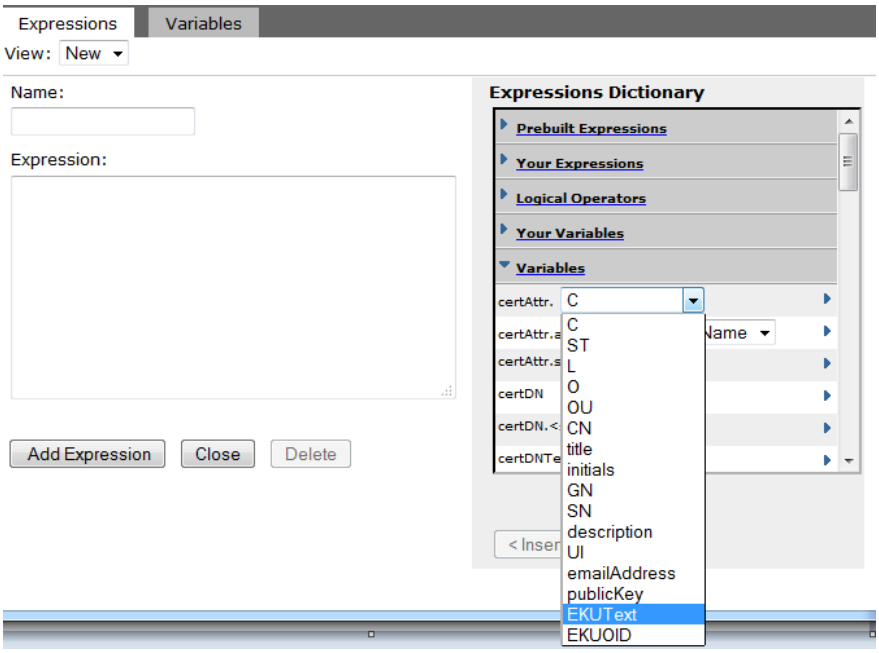
Note: This setting controls only connections into the device (Inbound Settings) and does not dictate settings for SSL connections that are initiated by the IVE.

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.

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.

The screenshot below shows the custom expressions:



Problems Resolved in 8.1R2 Release

Table 15 describes issues that are resolved when you upgrade.

Table 15: 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 16 describes the open issues in this release

Table 16: 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

Pulse documentation is available at **https://www.pulsesecure.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@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**
- **support@pulsesecure.net**
- Call us at 844 751 7629 (Toll Free, US)

For more technical support resources, browse the support (**website http://www.pulsesecure.net/support**).

Revision History

Table 17 lists the revision history for this document.

Table 17: Revision History

Problem Report Number	Description
27 May 2015	Initial publication.
27 August 2015	Update for 8.1R5
29 September 2015	Update for 8.1R5.1
19 October 2015	Update for 8.1R6