PRODUCT BULLETIN

PULSE CONNECT SECURE, PULSE POLICY SECURE AND PULSE CLIENT UPDATES FOR 9.0R3

Bulletin Date

December 2018

Applicable to All Regions

Effective Change Date

December 2018

Introduction

Today's digital era is challenging workforce productivity, from the 9-to-5 workdays to means of accessing and digesting data. More importantly, access to data and applications across different mediums, mobile to cloud, are redefining traditional IT processes and policies. Pulse Secure has made it easier to secure your data center, provide mobile access and enable new cloud services with our integrated Secure Access Solution. This Product Bulletin describes new features and functions available in the 9.0R3 release of Pulse Connect Secure, Pulse Policy Secure, and the Pulse Secure Desktop Client.

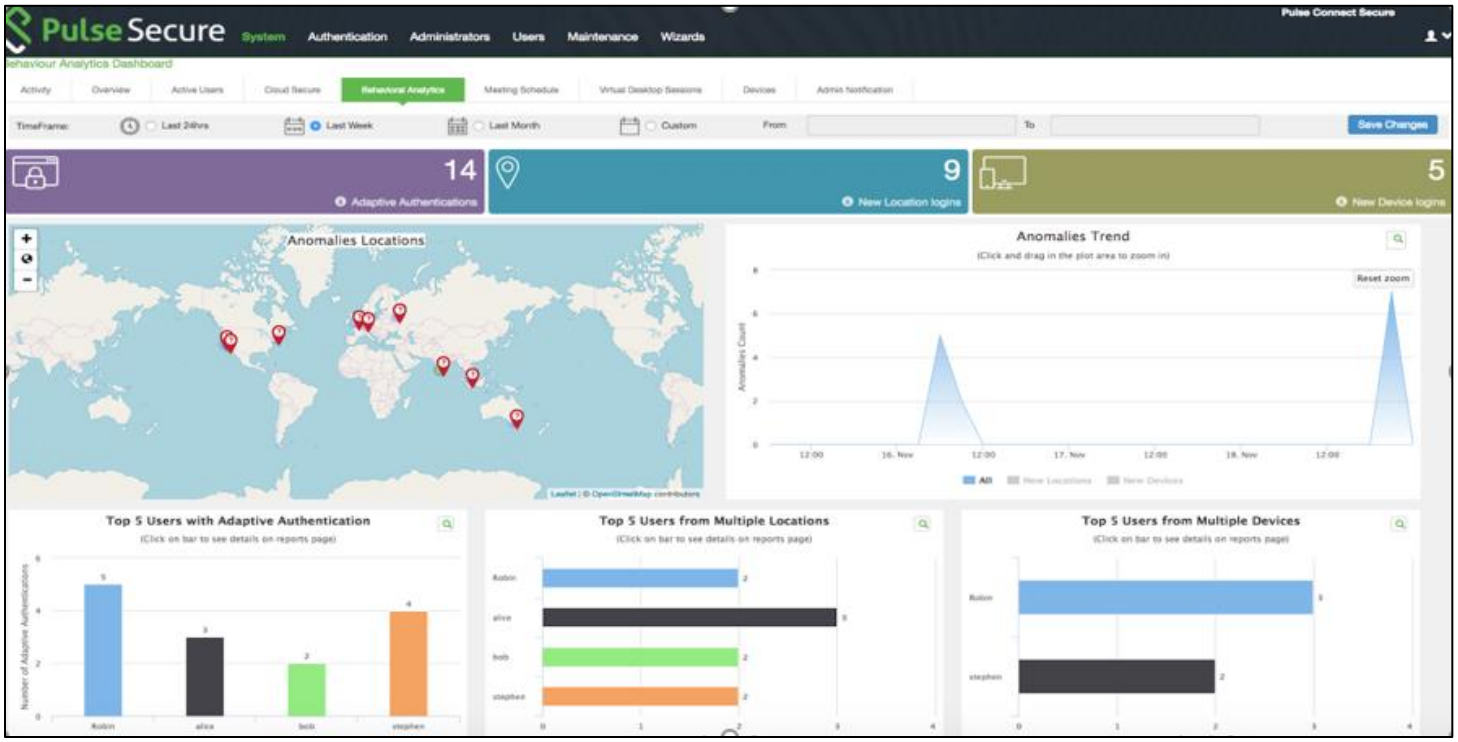
These new releases from Pulse Secure enable security and network administrators to expand their secure access solution support for network performance and security.

This release focuses on enhancements to user authentication, authorization and behavior analytics, secure IoT/IIoT solution, enhanced REST API interfaces, security and compliance-related enhancements, deeper integration with firewall and switch partners, profiling enhancements to reporting, classification, agentless host checking amongst others. New licensing schemes add support for named user licensing and licensing for MSP partners.

What's New

Common Features for Pulse Connect Secure and Pulse Policy Secure

Key Feature	Benefit
• AAA traffic via MGMT and EXT	• Allows reaching out to external and internal authentication servers through the management and external interfaces. Earlier, the AAA traffic could only be sent over the Internal interface.
• Adaptive Authentication	• On successful primary authentication, Adaptive Authentication creates an overall risk profile using user, device and location behavior that determines whether the secondary authentication challenge should be issued or bypassed before proceeding to session creation.
• Support TLSv1/2 with LDAPS	• TLS v1 and v2 are now supported with LDAPS communication to LDAP servers.
• Custom HTTP response headers	• Allows administrators to inject custom HTTP response headers in the management UI for compliance and security requirements, available via *System* > *Configuration* > *Security* > *Advanced* page.
• Embedded Browser - Custom sign-in page support	• Customization of sign-in pages is now supported with the Pulse Embedded Browser that is used for authentication with Pulse Client.
• Option to skip certification revocation checks	• Provides an option to skip CRL, OCSP revocation checks when the revocation service is slow or not available.
• Support default VLAN tagging in virtual appliance clusters	• Virtual appliances in cluster allow VLAN tagging of outgoing packets. Earlier this was available for standalone virtual appliance nodes only. • Tags untagged packets on the appliance interfaces, before packets are sent out.
• Support forest-level trust with standard AD mode	• Forest-level trust is now supported with Standard AD mode configuration.
• 64-bit support for SNMP	• The SNMP module has been updated to support 64-bit values.
• Centralized Named User Licensing	• Provides for licensing using unique user identity, rather than concurrent sessions. Consult sales representative for additional information.
• MSP Licensing	• Introduces new licensing options for managed service provider partners. Consult sales representative for additional information.
• Host Checker – MAC address and Domain check for MacOS	• Domain/NetBIOS and MAC address rule for macOS platform is added for policy evaluation with the Host Checker.
• New Pulse Secure SHA2 code signing certificate	• New code-signing certificates have been added that are valid till 2021.


Pulse Secure
System
Authentication
Administrators
Users
Maintenance
Wizards
Pulse Connect Secure
Behaviour Analytics Dashboard
Activity
Overview
Active Users
Cloud Secure
Behavioral Analytics
Meeting Schedule
Virtual Desktop Sessions
Devices
Admin Notification
TimeFrame:
Last 24Hrs
Last Week
Last Month
Custom
From
To
Save Changes
14
Adaptive Authentications
9
New Location logins
5
New Device logins
Anomalies Locations
Anomalies Trend
(Click and drag in the plot area to zoom in)
Reset zoom
Anomalies Count
12:00
16. Nov
17. Nov
18. Nov
All
Top 5 Users with Adaptive Authentication
(Click on bar to see details on reports page)
Number of Adaptive Authentications
Robin
alice
bob
stephen
Top 5 Users from Multiple Locations
(Click on bar to see details on reports page)
Top 5 Users from Multiple Devices
(Click on bar to see details on reports page)

Pulse Connect Secure 9.0R3

Highlighted Features in this Release

Key Feature	Benefit
• Enhanced REST API	Enhancements include: • Export, import full configuration via REST • API to pull license state from server • API to fetch all groups available in a configured LDAP or AD authentication server • APIs to get active sessions, system information, leased client counts, configure device certificates • APIs to configure certificates based on CSR workflow • APIs to perform cluster operations • Realm-based admin login for REST APIs
• TOTP Auth Server Enhancements	Enhancements include: • Support for centralized TOTP server across cluster boundaries, remote PCS units can query this centralized server for validating user secrets through any of the network interface or VLANs • TOTP can now be configured as an independent secondary authentication server, allowing the use of a single OTP from the authenticator app across realms using different primary auth servers • Option to export and import TOTP users (from TOTP Auth server page) through Admin UI and REST API • Option to suppress QR and backup codes, if required by the administrator
• HTML5 Access Enhancements	Enhancements include: • Support HMAC-SHA-256 with SSH • Specifying HTML5 session values using URL query-parameters • Support for custom pages • Opening the book mark in new window • New page for prompting user credentials • Keyboard is set to "Text Input" by default for mobile devices • TLSv1.1 and TLSv1.2 support for backend communication
• Enhanced Pulse Application Launcher support for Mac	• JSAM, Premier Java RDP Applet and other client modules are now launched using Pulse Application Launcher (PSAL), rather than the NPAPI (Netscape Plugin API); as the later has been removed in MacOS Mojave.
• Resource Throttling for System Stability	• Enhances system stability by employing cgroups to limit and isolate the resource usage (CPU, memory, etc.) of different modules.
• INITIAL_CONTACT support for IKEv2	• Preforms initial contact processing, if the initial contact notification is received in the IKE_AUTH exchange. Stale sessions are identified as those which have the same user, realm and source IP as the new one being requested.
• WTS support for NLA with smart cards	• Allows enabling NLA for cross-domain smart card authentication. This is disabled by default and must be enabled explicitly.
• High latency (WAN) clustering for additional appliances	• The PSA5000, PSA3000 and PSA Virtual appliances have been qualified for high-latency clustering (config only).
• PSAL 64-bit Support	• Pulse Application Launcher now supports 64-bit platforms.
• Azure Gov Marketplace	• PCS is now available in the Microsoft Azure Government Marketplace.

Key Feature	Benefit
• Third Party Applications	Following third party applications are qualified with 9.0R3: • VMware Horizon 7.4, 7.5 (Server and Client) • Safari 12 (MacOS 10.13, 10.14) • Firefox ESR 60 (Windows only) • IBM iNotes 9.0

Cloud Secure Specific Features in Pulse Connect Secure 9.0R3

Key Feature	Benefit
• Dashboard Drill-Down support	• Added Cloud Secure Reports which provides details on Application Access, Device Compliance details, Device details and Role assignments. The Cloud Secure dashboard have option to drill down to the report page.
• Multiple SP support with ADFS Federation & Bookmark with re-writer	• Allows users to access multiple cloud services using bookmarks in ADFS deployments with re-writer functionality enabled.

Figure 2: Cloud Secure Dashboard Drill down option

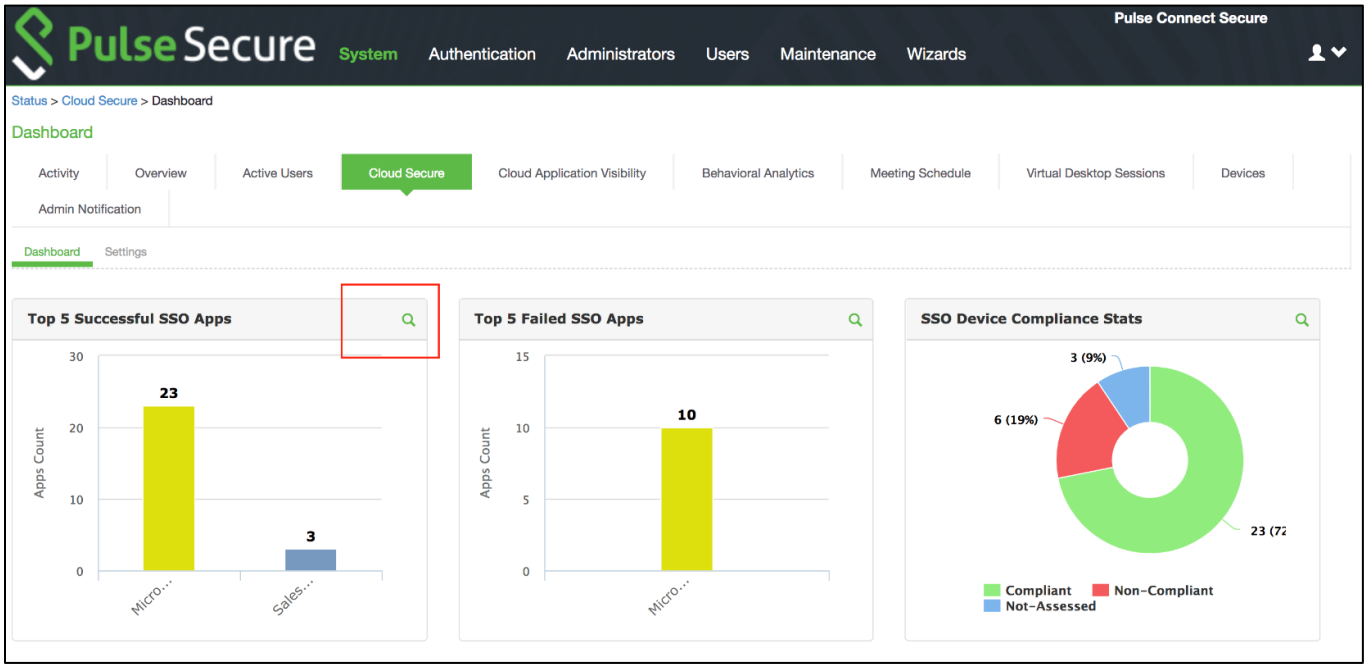
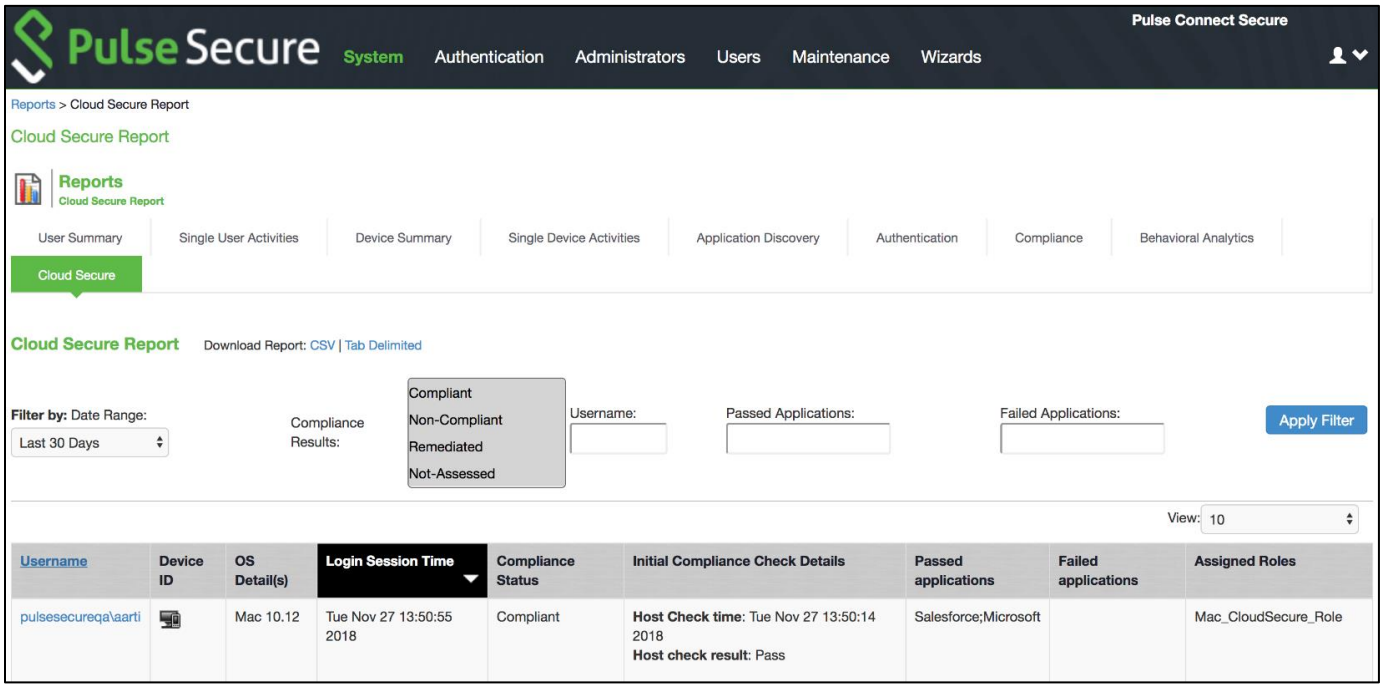


Figure 3: Cloud Secure Reports



Pulse Policy Secure 9.0R3

Highlighted Features in this Release

Key Feature	Benefit
• Behavioral Analytics	• Behavioral Analytics has two components 1) Adaptive Authentication 2) User and Entity Behavioral Analytics (UEBA). UEBA is a "Technology Preview" feature that leverages machine learning to identify suspicious network activity or anomalous behavior, providing faster detection and mitigation against zero-day and advanced persistent threats, as compared to traditional rule-based security. In addition, it provides automated analysis and detection of Domain Generation Algorithms (DGA)-based malware. **Note**: • UEBA (Anomaly Detection, Potential Malware Detection) is a "Technology Preview" feature for evaluation purposes for this release, and may require additional licensing at the time of general availability • Adaptive authentication is part of CONSEC/POLSEC license (described in common section above)
• IoT/IIoT Auto Provisioning using PAN firewall	• PPS enables secure access to IoT/IIoT devices through PPS/Profiler and PAN firewall integration. It allows the Admin to configure an IoT Access policy so that only authorized users can access the IoT/IIoT devices. It also enables automatic access control for the newly discovered devices.
• RADIUS dictionary updates	• 802.1x port-based security is enhanced with updated RADIUS dictionary attributes.
• Juniper SDSN Integration (Alert-based Integration)	• PPS enhances the security by isolating or taking action at the endpoint level based on threat alerts receives from Juniper SDSN.
• Host Checker – NETBIOS and Mac address check for MacOS	• Improve security on macOS platform.
• L2 Simplification	• Simplification of L2 configuration using RADIUS return attribute policy (ACL name and ACL rule).
• Secondary Authentication Server	• PPS supports authentication using a Secondary Authentication Server.
• 802.1X support for Huawei Switch	• PPS supports integration with Huawei Switch/WLC for 802.1X support.
• RSA support in TACACS+	• PPS supports RSA server authentication in TACACS+.
Profiler	
• Agentless Mode with Profiler	• Agentless Host Checker with Profiler allows user authorization based on the user device attributes without the need to install agents on their machines.
• Profile Groups	• The devices can be grouped based on device attributes and rules for easy access and identification. Group names can be used in role mapping rules, resource policies, filtering etc.
• Profiler Report Scheduling	• The Profiler reports (PDF) can be scheduled, and the reports can be delivered in the e-mail notifications to the specified addresses.
• On-Demand subnet scan	• On demand subnet scan allows administrator to manually trigger active collector (NMAP, WMI and SSH) scan and discover devices in a network. The discovered devices are added to the Profiler database.

Key Feature	Benefit
• DDR enhancements	• Device Discovery Reports table is enhanced with switch port view and sort with Profiler authentication server options.

Figure 4: Behavioral Analytics Dashboard

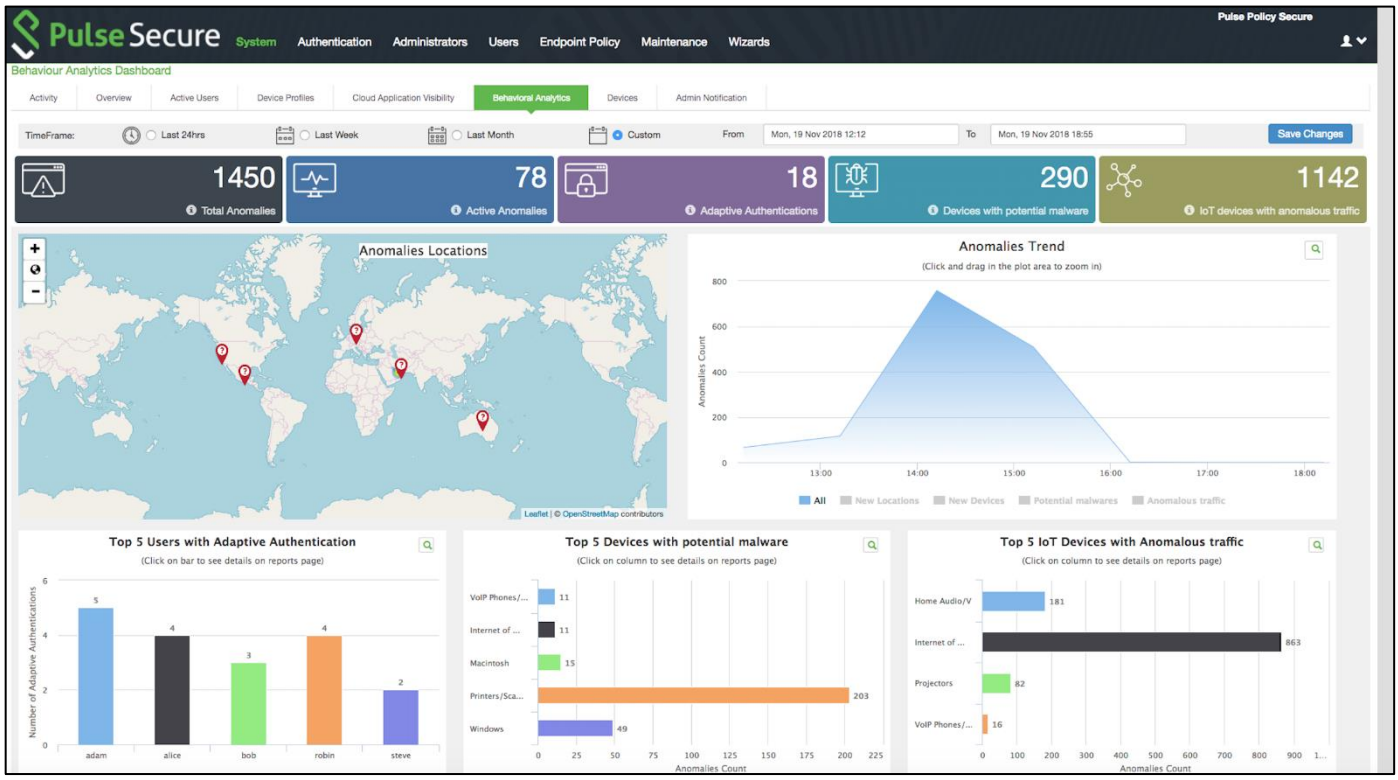
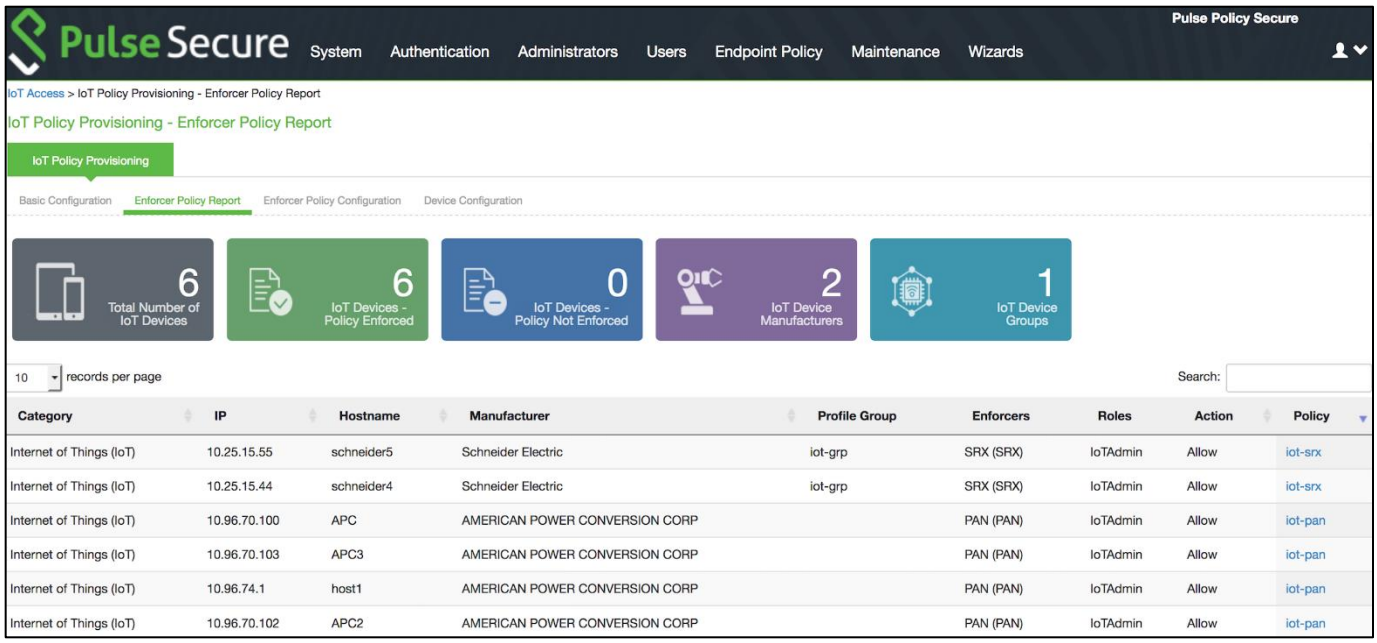


Figure 5: IoT/IIoT Auto Provisioning using Juniper and Palo Alto Networks Firewall



Pulse Secure Desktop Client 9.0R3

Highlighted Features in this Release

Key Feature	Benefit
• PSAM + L3 Tunnel Co-existence	• Pulse Desktop Client on Windows now supports simultaneous PSAM (L4) and SSL VPN (L3) tunnels to different PCS Gateways. For customers who have resources spread across multiple locations or who have highly protected zones within one location, Pulse Desktop Client can establish one SSL VPN (L3) tunnel to one PCS Gateway, and one PSAM (L4) tunnel to another PCS Gateway simultaneously. It helps the user to access all the resources at the same time without switching the Gateways.
• Stealth mode (background) tunnels with step-up and step-down auth	• Pulse Desktop Client on Windows now supports Stealth mode tunnels with step-up / step-down auth mechanism. For customers using Machine Certificate based authentication for pre-login to PCS, and second level of authentication for user tunnels, Pulse Desktop Client now provides the capability to manually control the switching between machine tunnel to user tunnel. The machine tunnel remains in the same state till user manually selects to Connect to PCS, at which point user will be prompted for additional authentication and then switch to user tunnel mode. When user logs off from user tunnel, the session falls back to machine tunnel mode. Admin can configure in such a way that machine tunnel presence is oblivious to the user. This capability is useful for customers who need different policies in machine tunnel mode and user tunnel mode.
• Embedded Browser – Custom sign-in page support	• Pulse Desktop Client on Windows and Mac now supports Embedded Browser with Custom sign-in pages. For customers who have customized the sign-in pages for branding and localization requirements, they can now enable Pulse Desktop Client to use Embedded Browser for displaying the sign-in page and complete the authentication and host checking steps. This provides better user experience as there is no dependency on local browser and no switching between browser and client.
• Support for Mojave 10.14	• Pulse Desktop Client on Mac now supports the latest macOS 10.14 (Mojave) OS.
• Support for Redstone 5	• Pulse Desktop Client on Windows now supports the Redstone 5.
• MTU calculation Enhancement through PMTU	• By default, Pulse Desktop Client uses MTU 576 in case of missing TCP MSS value, this is as per the RFC guidelines. For customers who don't want the default behaviour and would like to use 1400 MTU, Pulse Desktop Client provides an option to configure the same on Gateway. When this option is set, Client uses 1400 MTU when TCP MSS is missing.
• HVCI Compatibility	• The new Pulse Desktop Client on Windows is now compatible with Microsoft Windows 10 HVCI settings. Windows 10 HVCI settings are part of Windows Device Guard security features for mitigating cybersecurity threats. When HVCI is enabled, Windows OS performs code integrity checks and allows only secured applications. Pulse Desktop Client on Windows is compatible with these settings which would help customers adopt the latest security features of Windows.

Learn More

Resources

- Pulse Connect Secure resources
- Pulse Policy Secure resources
- Pulse Cloud Secure resources

https://www.pulsesecure.net/

About Pulse Secure, LLC

Pulse Secure, LLC is a leading provider of access and mobile security solutions to both enterprises and service providers. Enterprises from every vertical and of all sizes utilize Pulse Secure's Virtual Private Network (VPN), Network Access Control (NAC) and mobile security products to enable secure end-user mobility in their organizations. Pulse Secure's mission is to provide integrated enterprise system solutions that empower business productivity through seamless mobility.

Corporate and Sales Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
www.pulsesecure.net