



Ivanti Policy Secure Release Notes

9.1R18.4

Ivanti Policy Secure 9.1R18.4 Build 10077

Ivanti Secure Access Client 22.3R1 Build 24467

Pulse Profiler Version (FPDB Version 51)

Default ESAP Version: ESAP 4.0.5

Copyright Notice

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.ivanti.com.

Copyright © 2024, Ivanti, Inc. All rights reserved.

Protected by patents, see <https://www.ivanti.com/patents>.

Contents

Introduction	4
Product Compatibility	4
New Features	6
Noteworthy Changes	17
Fixed Issues	20
Known Issues	32
Upgrade Instructions	54
Documentation	55

Introduction

This document contains information about what is included in this software release, new features, known issues, fixed issues, product compatibility, and upgrade instructions.

Security Advisory and Patch Update

Ivanti has released security advisories and mitigations for critical vulnerabilities in the Ivanti Pulse Secure gateways. The following CVE's have been fixed:

- CVE-2023-46805
- CVE-2024-21887
- CVE-2024-21888
- CVE-2024-21893
- CVE-2024-22024

For more details, see [forum link](#).

Product Compatibility

Hardware Platforms

You can install and use this software version on the following hardware platforms:

PSA300, PSA3000, PSA5000, PSA7000F, PSA7000C

To download software for these hardware platforms, go to:

<https://forums.ivanti.com/s/contactsupport>

Virtual Appliance Editions

This software version is available for the Virtual Pulse Secure Appliance (PSA-V) editions.

The following table lists the virtual appliance systems qualified with this release.

Platform	Qualified System
VMware	HP ProLiant DL380 G5 with Intel(R) Xeon(R) CPU ESXi 7.0
KVM	Contoller: OpenStack Wallaby on CentOS 7.6 Compute: OpenStack Wallaby Ubuntu 20.04LTS 24GB memory in host Allocation for virtual appliance: 4vCPU, 4GB memory and 40GB disk space
Hyper-V	Microsoft Hyper-V Server 2016 and 2019
Azure-V	Standard DS2 V2 (2 Core, 2 NICs) Standard DS3 V2 (4 Core, 3 NICs) Standard DS4 V2 (8 Core, 3 NICs)
Amazon Web Services (AWS)-V	T2.Medium (2 Core, 2 NICs) T2.Large (4 Core, 3 NICs and 2 NICs) T2.Xlarge (8 Core, 3 NICs and 2 NICs)

To download the virtual appliance software, go to: <https://forums.ivanti.com/s/contactsupport>



- From 9.1R1, VA-DTE is not supported.
- From 9.0R1 release, Ivanti has begun the End-of-Life (EOL) process for the VA-SPE virtual appliance. In its place, Ivanti is launching the new PSA-V series of virtual appliances designed for use in the data center

New Features

The following table describes the major features that are introduced in the corresponding release.

Features	Description
Release 9.1R18.2	
No new features introduced in this release.	
Release 9.1R18.1	
No new features introduced in this release.	
Release 9.1R18	
No new features introduced in this release.	
Release 9.1R17	
Allow Host checker policy on certificate expiry	This feature allows the administrators to pass host checker policies on endpoints after the machine certificate expires. The Administrator can assign endpoints to have remediation roles so that users can renew certificate.
Log Enhancements	This feature allows the admin to enter a custom message to display on the client highlight the host checker compliance errors.
Report scheduling enhancements	This feature supports scheduling multiple reports of the same type. Allows scheduling report notification on a customized time of a day/month/week.
Compliance report enhancements	The dashboard displays the chart for the compliant and non-compliant devices. The compliance report is enhanced to display the compliant devices.
Release 9.1R16	
Profiler IPv6 Support	Profiler now supports and discovers IPv6 devices. DDR report and other reports show IPV6 information.
Release 9.1R15	

Features	Description
Profiler IPv6 Support	Profiler now supports and discovers IPv6 devices. DDR report and other reports show IPV6 information.
Release 9.1R14	
DHCP Server Address Assignment in IPS	This feature allows to configure DHCP servers in Address Pool tab and assign IP addresses dynamically to the endpoints from the configured DHCP server. Note: One server can be configured with only one IP address.
Active/Active Cluster Support for IP pool feature for Framed IP Address	This feature allows to assign IP addresses dynamically for the users or nodes from IP address pools over radius protocol in Active/Active cluster mode.
Kerberos e-type extension	This feature allows Kerberos to use AES128 as the highest encryption type.
Release 9.1R13	
Framed-IP Address Pool	Ivanti Policy Secure allows the admins to assign IP addresses dynamically for the users or nodes from IP address pools. This feature is applicable only to RADIUS.
Delegated Admin Control	This feature enables super admin to configure different access levels to RADIUS, SNMP clients and policy configurations listed in the Network Access menu.
Release 9.1R12	
MS SQL Server support for Accounting	Ivanti Policy Secure supports storing the RADIUS accounting information to an external SQL database. Ivanti Policy Secure offers SQL Accounting feature under Auth Servers. MSSQL accounting supported only for 802.1x use cases and only one SQL server can be configured.
Enhancement to prevent MAC Spoofing	Profiler can now detect a device, which was already scanned and profiled but cannot be scanned anymore. Admin can configure e-mail notification to be sent based on configured interval for devices, which are assigned a group based on the number of failed scan attempts.

Features	Description
Cascading Authentication Server support	Cascading multiple external authentication servers provides a continuous, reliable process for authenticating and authorizing external users. If authentication fails on the first authentication server, then Ivanti Policy Secure attempts to authenticate the user by using the subsequent external authentication server configured in the realm under the sign-in policy page.
Ivanti Connect Secure Admission Control using Ivanti Policy Secure	The Firewall/SIEM detects compromised remote devices, Firewall/SIEM can send threat alert to Ivanti Policy Secure and Ivanti Policy Secure can instruct Ivanti Connect Secure to take action based on threat severity.
Release 9.1R11	
Ivanti Policy Secure and Profiler reporting enhancements	Ivanti Policy Secure supports report generation and sending it as a PDF attachment in a scheduled email based on filters and time settings.
Release 9.1R10	
No new features introduced in this release. See, Noteworthy Changes .	
Release 9.1R9	
Firewall Provisioning based on Profile Group	Ivanti Policy Secure allows Administrator to provision Auth Table Mapping policy, Resource Access policy and IoT Access policy configured using profile groups for the devices.
SBR migration service attribute field	Ivanti Policy Secure supports Service Type configuration in TACACS+ shell policy in SBR to Ivanti Policy Secure migration.
SBR Shared Secret Password Decryption	Ivanti Policy Secure supports decryption of shared secret and native user password (encrypted passwords only) in SBR to Ivanti Policy Secure migration.
Release 9.1R8	
McAfee ePO integration for endpoint protection	Ivanti Policy Secure integration with McAfee ePO supports assessing device security posture through querying of device attribute details and then assigning of roles based on the attribute values.

Features	Description
Nozomi networks Ivanti Policy Secure integration and policy provisioning	Ivanti Policy Secure integration with Nozomi Networks supports assessing device security posture through querying of device attribute details and then assigning of roles based on the attribute values.
SBR to Ivanti Policy Secure migration for TACACS+ usecase	SBR TACACS+ configurations can be migrated to Ivanti Policy Secure using configuration file import.
Support for pool of NTP servers and NTP status check	Ivanti Policy Secure now supports pool of NTP servers up to 4 NTP servers to sync date and time.
Assign RADIUS Return Attributes for Local and MAC Auth Users	Ivanti Policy Secure supports configuration of specific/custom attributes and assignment to a user or group of users. Administrator can use RADIUS Return Attribute Policy and User Return Attribute together to enforce on the client for 802.1x and MAC authentication mechanism.
MSSP Licensing	Ivanti Policy Secure now supports MSSP licensing model.
UEBA package for fresh installation of Ivanti Policy Secure	In case you have a fresh installation of Ivanti Policy Secure, you may download latest UEBA package from Pulse Secure Support Site (https://forums.ivanti.com/) and add the package at Behavior Analysis page before using Adaptive Authentication.
Profiler	
Profiler integration with Nozomi Networks	Profiler integration with Nozomi Networks supports classifying and categorizing OT devices using device attributes.
Agentless classification through RSPAN traffic	Enable passive listening of traffic through RSPAN using TCP and SMB protocols in profiler. This feature helps to detect devices and their attributes for endpoints which are configured with/without static IP addresses
Device time-bound approval	This feature allows the administrator to approve devices for a specific time period.
Profiler UI changes	The Ivanti Policy Secure User Interface has new tab for Profiler configuration and maintenance.

Features	Description
Profiler customized reports	This feature allows to download custom reports based on the filters applied.
Release 9.1R6	
Show Serial Number under Licensing Tab	The Ivanti Policy Secure Licensing tab (System > Configuration > Licensing) now displays the Serial Number.
Hardware ID is available on System Maintenance Tab	The Hardware ID is now included in System Maintenance > Platform tab.
Host Checker policies hyperlinked to policies page	Host Checker policies is now clickable (hyperlink) in User Realms page.
Release 9.1R5	
Ivanti Policy Secure on Amazon Web Services (AWS)	Provides NAC services (802.1x, MAC Auth, L3 Firewall Enforcement) to multiple on-premise networks using Ivanti Policy Secure deployed on Amazon Web Services (AWS) cloud.
SNMP policy enforcement (Alcatel-Lucent, Huawei, Arista)	SNMP policy enforcement is now supported on Alcatel-Lucent, Huawei and Arista switches.
McAfee ePolicy Orchestrator (ePO) integration	Ivanti Policy Secure (Ivanti Policy Secure) integration with the McAfee ePolicy Orchestrator (ePO) provides complete visibility of network endpoints and provide end to end network security. The Ivanti Policy Secure integration with McAfee ePO allows Admin to perform user access control based on alerts received from the McAfee ePO.
Splunk syslog add-on and Dashboard app	Splunk application for Ivanti Policy Secure uses the indexed data to render various charts and to show useful information on dashboard. The Pulse Secure App for Splunk allows you to view Ivanti Policy Secure data in a dedicated, customizable Splunk dashboard. This bidirectional interaction with Splunk allows security managers to quickly monitor the current operational/security posture.
IPv6 Support for Syslog, NTP and Log Archive	Ivanti Policy Secure now supports sending syslog messages to a syslog server using IPv6 address.

Features	Description
	Time synchronization using NTP server is now supported with IPv6 address. Ivanti Policy Secure also supports transferring archived Ivanti Policy Secure logs using FTP and SCP over IPv6 network.
SBR to Ivanti Policy Secure migration	SBR configurations (802.1x and Mac Address Authentication) can be migrated to Ivanti Policy Secure using XML import.
ECC certificate support for Juniper SRX firewall connection	Ivanti Policy Secure now supports Elliptic Curve Cryptography (ECC) certificate for SRX firewall connections.
Host Checker policy to detect hard disk Encryption in progress	Host Checker policy to allow detection of hard drive encryption in progress.
MSSQL support on Ivanti Policy Secure with external DB	Ivanti Policy Secure supports MSSQL as external Auth server for 802.1x and Layer 3 authentication.
PDF report capability	This feature in Ivanti Policy Secure allows the user to download the reports (User Summary Report, Single User Activities, Device Summary, Device Discovery, Single Device Activities, Authentication, Compliance, Infected Devices) in PDF format. Apart from the CSV, Tab Limited option, there is an option called PDF provided in Ivanti Policy Secure Reports.
Profiler	
Backup and Recovery, and Disaster management	Profiler deployments provides backup mechanism for enhanced disaster management (Profiler Forwarder, Remote Profiler, Centralized Standalone Profiler).
Viptela Switch Support	Viptela Switch support is added for SNMP Visibility.
Release 9.1R4	
Ivanti Policy Secure on Azure platform	Provides NAC services (802.1x, MAC Auth, L3 Firewall Enforcement) to multiple on-premise networks using Ivanti Policy Secure deployed on Microsoft Azure cloud.
Huawei - Guest Access	Supports guest access use cases with Huawei WLC.
Mist Juniper WLC	Supports 802.1x and guest access with Juniper Mist WLC.

Features	Description
TACACS+ support for Arista Switch	Support Administrator access control for Arista.
Common Access Card (CAC) support with TACACS+	Supports TACACS+ authorization using Ivanti Policy Secure. Authentication is performed by the third-party authentication server.
Provisioning only User-ID information to PAN firewall	Provides an option to admin in Auth table mapping policy to push only IP-User mapping to Palo Alto Networks firewall.
System Local user attribute support (Framed-IP-Address)	Allows to define user Attributes for system local server and associate those attributes to user names, including Framed-IP address. Values of those attributes to be defined for each user name.
Strong Hash	Supports protecting passwords stored in local authentication server using strong hash.
Release 9.1R3	
VSYS Support in PAN	Ivanti Policy Secure supports provisioning user identity and resource access/IoT policies to multiple VSYS or specific VSYS (other than vsys1) on PAN firewall.
IBM QRadar Integration	Ivanti Policy Secure along with IBM QRadar provides user access control based on threats/events received from IBM QRadar.
Splunk Integration	Splunk alert based integration supports sending alert information from Splunk to Ivanti Policy Secure. Ivanti Policy Secure uses its existing functionality of admission control, L2/L3 enforcement and provides role based access control to secure the network.
Fortinet Identity management using RADIUS accounting messages	Ivanti Policy Secure supports integration with FortiGate firewall using RADIUS accounting messages.
Mysql support	Ivanti Policy Secure supports MYSQL as external Authentication server.

Features	Description
Local user account import through CSV in System local DB	Allows importing user accounts via CSV file in System local auth server. The local authentication server is an authentication database that is built in to Ivanti Policy Secure.
SNMP Enforcement using ACL for 3Com, DELL	SNMP ACL enforcement support is now expanded for 3Com and Dell switches.
SNMP Enforcement using VLAN for 3Com, Juniper and DELL	SNMP VLAN enforcement support is now expanded for 3Com, Juniper and Dell switches.
One-to-One NAT support	Ivanti Policy Secure allows auth table provisioning for the endpoints behind NAT (One-to One NAT mapping).
vTM and Ivanti Policy Secure Integration for Load Balancing	The Platform Limit, Maximum Licensed User Count and Cluster Name attribute values are available for optimal load balancing.
Release 9.1R2	
Alert based integration with Nozomi Networks	Ivanti Policy Secure along with Nozomi Networks provides threat detection and threat response in ICS/OT environment.
Backup configs and archived logs on AWS S3/Azure Storage	Two new methods of archiving the configurations and archived logs are available apart from SCP and FTP methods: Ivanti Policy Secure/Ivanti Connect Secure supports pushing configurations and archived logs to the S3 bucket in the Amazon AWS deployment and to the Azure storage in the Microsoft Azure deployment.
EasiSMS Gateway Support	Ivanti Policy Secure supports EasiSMS gateway through the SMTP server. EasiSMS uses an email format to send SMS to end user mobile phones.
Flag Duplicate Machine ID in access logs	<p>Pulse client expects the machine ID is unique on each machine. If multiple endpoints have the same machine ID, for security reasons, the existing sessions with the same machine id are closed.</p> <p>A new access log message is added to flag the detection of a duplicate Machine ID in the following format: Message: Duplicate machine ID "<Machine_ID>" detected. Ending user session from IP address <IP_address>. Refer document KB25581 for details.</p>

Features	Description
Migration of Cisco ACS RADIUS/TACACS+ client configuration to Ivanti Policy Secure	Migrating RADIUS/TACACS+ client configuration configured on the Cisco ACS device.
Report Max Used Licenses to HLS VLS	The licensing client reports maximum used sessions count instead of the maximum leased licenses count. For MSP customers, this change helps in billing the tenants based on maximum sessions used.
V3 to V4 Opswat SDK mi-gration	Ivanti Policy Secure supports the migration of servers and clients to Opswat v4 to take advantage of latest updates.
VA Partition	Ivanti Connect Secure/Ivanti Policy Secure supports upgrading from Ivanti Connect Secure 8.2Rx/ Ivanti Policy Secure 5.3Rx to 9.1R2 for the following supported platforms: VMWare ESXi KVM Hyper-V When upgrading a VA-SPE running Ivanti Connect Secure 8.2R5.1/Ivanti Policy Secure 5.3Rx or below that was deployed with an OVF template to a higher version, the upgrade was failing. This feature solves the upgrade problem for VMWare, KVM and Hyper-V. Refer KB41049 for more details.
Profiler	
Profiler dashboard update	Profiler dashboard supports chart for Profile Groups. This chart is also part of downloaded PDF report.
Windows defender and Microsoft Security Essentials support	Agentless Host Checker with Profiler supports Windows defender and Microsoft Security Essentials.
Release 9.1R1	
DNS traffic on any physical interface	Prior to 9.1R1 release, DNS traffic was sent over the Internal interface. Starting with 9.1R1 release, an administrator can modify the DNS setting to any physical interface namely Internal Port, External Port or Management Port.

Features	Description
Google Auth Multi Factor Authentication	TOTP server can be added as a secondary auth server in Ivanti Policy Secure.
Machine certificate check on MacOS	Machine certificate check on Mac OS is now supported for Ivanti Policy Secure.
Meraki 802.1x and Guest Access support	802.1X and Guest Access support is qualified with Cisco Meraki WLC.
RADIUS server capability on External port	802.1X authentication is now supported on external port.
SAML Auth Server support	Ivanti Policy Secure can be configured as SAML service provider (SP) for all industry standard SAML IdP's.
Session bridging for Linux Platform	Ivanti Policy Secure supports bridging the Layer 2 Native Supplicant 802.1X session with Layer3 Agentless (Browser based) Session on Linux platform.
Session Migration using Cert authentication	Session migration in an IF-MAP federated network supports Cert Auth and SAML auth
SNMP Enforcement using ACL (Cisco, HP, Juniper)	SNMP enforcement using ACL is supported for Cisco, Juniper and HP switches.
TACACS+ Enhancements - DB sync, pass back attributes to devices such as F5 and Juniper	TACACS+ authorization support for Administrators using custom attributes for Juniper and F5 devices.
TACACS+ configuration synchronization across WAN cluster	
Profiler	
Distributed Profiler Enhancements	The Administrators can sync the profiled data from one Profiler to another from the profiler auth server configuration page. Multiple branch offices can sync their profiled data to central office. Ad-min can view the Device Discovery Report to view and control the multiple offices.


Features	Description
Profiler Device Age Out	Profiler device age-out interval configuration allows admin to automatically delete the devices from the database. Admin can define the age-out interval for a group of devices also using Profile Groups
Profile Windows devices using SNMP (HOST)	SNMP-HOST Collector is a collection method that receives endpoint information where the end-points are monitored through SNMP. Admin can configure subnets to scan and community strings in profiler auth server configuration page.
Approval for Profile Groups	Administrator can select "needs approval" for selected Profiler group.
Key-value based search in DDR	Administrator can search in DDR with key value-based query. Query syntax is similar to that of pro-file groups.
Publishing IP address from Profiler to Active User Session	Admin can add IP address from Profiler to active session for L3 enforcement when RADIUS account-ing is not enabled. This is supported only for MAC auth and dot1X.
Huawei switches added in supported list for Network Infrastructure Device	Admin can select Huawei switch from supported list in network infrastructure device page.

Noteworthy Changes

The following table describes the major feature changes that are introduced in the corresponding release.

Feature	Description
Release 9.1R18.2	
Unavailability of images	Hyper-V and Azure images are unavailable during fresh deployment.
Size availability	The file system is reorganized to free up data partition.
Release 9.1R18.1	
Hyper-V and Azure images are unavailable during fresh deployment.	
Release 9.1R18	
No Noteworthy Changes in this release.	
Release 9.1R17	
For PAN, Check-point, and Fortinet firewall when security policies are changed on firewall, ensure to restart the services on IPS for the reconciliation of the resource access policies.	
Supported ISAC Version	This release supports 22.2R1. For more info refer to https://forums.ivanti.com/s/article/KB45603
Release 9.1R16	
Anonymous Auth server	Re-introduced Anonymous authentication server.
Session IDs in logs	Host Checker logs enhanced to include session IDs.
Release 9.1R15	
Feature Deprecation	<p>From 9.1R15 onwards, some features are deprecated. Ensure you remove all related configurations before upgrading to 9.1R15. Upgrade may fail if all configurations are not removed. For more information refer KB45044.</p> <p>If upgrade is performed through Admin UI, the upgrade failure message displays the list of deprecated feature configuration that needs to be removed to proceed with upgrade.</p>

Feature	Description
	If the upgrade is performed using REST APIs or management servers like Pulse One, check serial console for the list of deprecated feature configurations.
Release 9.1R14	
Features targeted for deprecation	From release 9.1R14, few features are targeted for deprecation. For these features, 9.1R14 update does not support new configurations, however it supports modification to existing configuration. On upgrade, there are no changes to the existing configurations. These features will be permanently deprecated in next releases. For detailed list of deprecated features refer KB44747.
Rebranding Pulse Secure to Ivanti	Rebranding of Pulse Secure logo, copyright, and some references to reflect Ivanti branding is in progress. The rebranding activity to Ivanti will be continued through next release. Pulse Connect Secure (PCS) is referred to as Ivanti Connect Secure (ICS) and Pulse Policy Secure (PPS) is referred to as Ivanti Policy Secure (IPS).
Default periodic host checking interval increased	The default periodic host checking interval is set to 60 minutes. Setting aggressive intervals may result in performance issues.
Release 9.1R13	
Delegation to Network Infrastructure Device configuration moved	From 9.1R13, Delegation to Network Infrastructure Device related configuration is moved under Network Access configuration. Prior to 9.1R13, the settings were available in Log/Monitoring page under Admin Role.
Release 9.1R11	
Email Notifications modified to Email Scheduler	<p>“Email Notifications” under Configuration > Notification is now modified as “Email Scheduler”.</p> <p>“Email Notification” page was earlier accessible only if Profiler license is configured and Profiler server is created. Beginning with Release 9.1R11, Email Scheduler page will be available irrespective of Profiler license or server creation. If Profiler is not created, then “Device Discovery” will not be present in the list of report types in email scheduler page.</p>

Feature	Description
Release 9.1R10	
Host Header Enforcement	Host Header enforcement is introduced in 9.1R10. When this option is enabled on the server under System > Configuration > Security > Miscellaneous, the Pulse Client upgrade through IPS may fail. For more information, refer to KB44646.
Release 9.1R3	
OAC Client Removal	OAC client is deprecated beginning with Release 9.1R3.
Profiler <hr/>  For release 9.1R3, the minimum version of the fingerprints package supported is 41.	
NMAP Upgrade	Upgraded NMAP database and Binary for improving the detection and classification of new devices.
SNMP Performance improvements	Improved endpoint devices detection using SNMP.

Fixed Issues

The following table lists issues that have been fixed and are resolved by upgrading to this release.

Problem Report Number	Summary
Release 9.1R18.2	
PRS-415819	Forward and Sync Endpoint Data is not working.
PRS-415185	Unable to choose the date in the Guest Admin page after upgrade to 9.1R17
PRS-414870	RADIUS dictionary/vendor files are not in order on upgrading to 9.1R17
Release 9.1R18.1	
PRS-396726	Agentless connection from Big Sur machine displays wrong "Agent Type" version under Active user page.
PRS-415034	After upgrading to 9.1 R17 version, Profiler DDR shows 5 filters were applied by default.
PRS-415336	SBR auth process not recovering on its own after being overloaded
PRS-415656	Compliance is failing on McAfee 16 with ESAP 4.1.4
PRS-415686	ISAC shows password expiration warning even when the number of days configured in realm for warning is less than password expiration day. This only happens when you use DUO sign in page.
PRS-416052	Inconsistencies in Japanese Language while using Host Checker.
Release 9.1R18	
PRS-411280	Host Checker hangs during patch management check.
Release 9.1R17	
PRS-413663	uwsgi process fails
PRS-412793	PSA7000c unresponsive in Active-Passive cluster with warm restart on 9.1R16.
PRS-411539	Bi-Directional forward and sync endpoint data is not working.
PRS-411228	Host Checker: Virus Definition Check fails for Norton Security Ultra

Problem Report Number	Summary
PRS-410933	IPS is unable to classify Cisco AP.
PRS-410586	Host Checker reports Virus Definition are not up to date for AV VirIT eXplorer PRO.
PRS-410474	Host Checker: ICS do not recognize few vendors while configuring Antivirus and Spyware.
PRS-410138	On upgrading to 9.1R14.1, sporadically users are redirected with error https://auth/welcome.cgi.
PRS-409245	Post re-authentication, IPS sends Disconnect-Request within 2-3 minutes due "Max session timeout".
PRS-405730	Framed-IP address sent in disconnectmessage is incorrect.
Release 9.1R16	
PRS-411375	DDR entries are not showing on the reports page.
PRS-411257	Post Upgrade to 9.1R15, we can no longer change the precedence/ordering of the Sign-In URLs (Save changes take no effect).
PRS-410989	Device search is failing in DDR after upgrading to 9.1R15.
PRS-410887	Apex One (Mac) Security Agent 3.5.5709' failing in the policy re-evaluation
PRS-409984	"Pulse Collaboration" feature is still accessible in 9.1 R15 version
PRS-409543	Save All Logs button missing in 9.1R15 in IPS and ICS.
PRS-409492	Custom Sign-in pages display jumbled content post C9.1R15 upgrade.
PRS-409238	User IP address allocation logs intermittently not getting populated in User Access logs.
PRS-408829	Program TNCS failed.
PRS-408820	XML import shows failed when SQL Auth based being used as authorization along with CERT Auth being as authentication.
PRS-408552	Unable to Profile Thin client (Wyse)
PRS-408516	Agentless HC crashes with 3rd party NHC rule (heap corruption).

Problem Report Number	Summary
PRS-407539	Users are getting "authentication rejected by the server" when they click connect on pulse client.
PRS-404126	Users were unable to connect, existing users got disconnected due to aggressive "Periodic Check" timers.
PRS-403391	MAC spoofing not blocked.
PRS-403095	HC Logs in User Access shows Local Username instead of VPN Username while using Embedded Browser.
Release 9.1R15	
PRS-403905	TACACS+ Authorization is getting rejected with error "Authorization not enabled without authentication". When authentication and authorization requests use different port.
PRS-405579	MSSQL Accounting not working with PPS.
PRS-405730	Disconnect Message fails. Framed-IP sent in DM message is incorrect.
PRS-405982	WMI Scan fails for all the devices.
PRS-406663	After upgrading PCS to 9.1R13, users using embedded browser no longer receiving password expiry message when DUO is secondary auth server.
PRS-406807	Federate wide sessions are not getting synced between IF-MAP Replicas when persistent queue change log file is corrupted.
PRS-407143	Ignore Internet Check Flag needs to be updated in PDC/PCS/PPS 9.1R15.
PRS-407143	Internet Check during HC for EDR products is removed to prevent false-positive scenarios - https://forums.ivanti.com/s/article/KB45142?language=en_US .
PRS-407796	Continuous Radius process snapshots generated after upgrading PPS to C9.1R14
Release 9.1R14	
PRS-404150	Email Scheduler not working for DDR post 9.1R12 Upgrade.

Problem Report Number	Summary
PRS-403253	Event log shows "Closing connection with profiler 10.0.4.6 due to Server Error: (psycopg2.OperationalError) FATAL: sorry, too many clients already".
PRS-403391	Unable to detect the MAC spoofing because Nmap is not able to change the classification immediately after the device is spoofed.
PRS-402950	Admission Control action does not take place in case of session bridging scenario (When L2 session with native supplicant is bridging with Pulse L3 session) even after IPS receives alert.
PRS-399095	Profiler is not able to classify Device using DHCP collector.
Release 9.1R13.1	
PRS-404129	Misalignment of tables in Ivanti Policy Secure PDF reports.
Release 9.1R13	
PRS-402642	First time connection from MAC Big Sur with host checker enabled at realm level shows host checker looping and SecStaticCodeCheckValidity failure.
PRS-401418	Virus definition check fails for Cisco Advanced Malware Protection for Endpoints (7.x).
PRS-400993	Guest Sponsor not receiving emails on Ivanti Policy Secure for Pulse Guest access.
Release 9.1R12	
PRS-390315	Fed-Wide session sync delay between Replicas and User session getting removed from Imported sessions within few minutes.
PRS-396075	A warning message is added to notify users that the services will be restarted and the connections will be disconnected when the admin sets the network time manually (System -> Status -> Overview -> Date and Time).
PRS-400212	TACACS+ Authorization gets rejected despite successful authentication.
PRS-394901	"Program RADIUS recently failed" issue has been fixed.
PRS-395269	Ivanti Policy Secure default port 11122 (ScreenOS) and 11123 (SRX) , which supports TLS1.0 is now closed by default and is used only upon adding SRX/ScreenOS connections.

Problem Report Number	Summary
PRS-399186	User password displayed in clear-text in admin access logs during XML import failure in Ivanti Policy Secure.
PRS-399585	TACACS+ Accounting issue is resolved.
PRS-401053	Profiler forwarder forwarding profiling data of disconnected devices to standalone profiler results in unwanted consumption of profiler licenses.
PRS-398632	SAML Auth for Admin users fails generating an authentication error.
Release 9.1R11	
PRS-396507	Cisco L3 switch is displayed as Cisco WLC when the Cisco switch does not have CAM entries. Hence a proper log message has been added to cover this scenario.
PRS-397403	XML configuration export settings for roles such as guest role and user role are not retained and not matching with the GUI.
PRS-396313	DDR entries are deleted after power failure. This is now resolved.
PRS-397271	Issue with "Agentless mode with Profiler" HC policy for role and realm mapping.
PRS-393135	<p>TNCS process crashes when admin configures Host Checker NetBios rule with more than 1228 characters.</p> <p>Ivanti Policy Secure supports a maximum of 1,000 regex patterns in a single NetBIOS rule. In case, if there are more than 1,000 regex patterns in a single rule, split the rule into multiple rules.</p>
PRS-397072	Apple changed the OS version format in BigSur, which was not identified correctly. The OS Version check logic is updated to identify the new OS version format used in BigSur.
PRS-397433	Authentication fails for native users, post migration from SBR to Ivanti Policy Secure.
PRS-390086	ESAP package download was failing due to slow network speed on Mac platform. End-Points connected through slow Internet now will not hit the incomplete ESAP package download scenario.

Problem Report Number	Summary
Release 9.1R10	
PRS-394168	Multi Factor Authentication with Okta RADIUS for Networking devices like Cisco/Juniper Switches using SSH Access with Push notification is supported now.
PRS-380696	Predefined Host Checker policy can now be configured with a ignore category based on the vendor.
PRS-394560	Endpoints discovered having only IP Addresses (No associated MAC Addresses) by CDP/LLDP collectors from SNMP clients will now get updated in DDR.
PRS-394829	NMAP Package upgraded to version 7.91 and NMAP profile update algorithm modified to avoid frequent NMAP profile changes.
PRS-388935	The Authentication report now specifies the exact reason for the authentication failure.
PRS-394744	Error updating data for chart hc_failure_reason/auth_mechanism" log on Ivanti Policy Secure will no longer be seen. The Exception that was causing this error has been fixed.
PRS-390086	Endpoints connected via slow internet will not hit the incomplete ESAP package download scenario.
PRS-392973	SNMP Polling freezes when sys-name is not present in CDP table for an endpoint.
PRS-396427	Removed search box in TACACS+ Shell policy page due to conflict with policy reordering option.
Release 9.1R9	
PRS-393361	SNMPv3 clients can now be edited from New Profiler UI page.
PRS-394098	SNMP Discovery Issue with SNMP v3.
PRS-394069	Pulse Desktop Client disconnects when flipping VIP or rebooting appliance.

Problem Report Number	Summary
PRS-394759	DHCP set option is added for AWS (If no DNS server configured in DHCP option set, it will take the second IP address as primary DNS server from the internal port subnet).
PRS-394604	Agent Type in active users page on Ivanti Policy Secure is failing to show Windows OS version with 9.1R8 PDC builds.
Release 9.1R8.2	
PRS-388342	HC policy based on "Windows patch management" is not re-triggering post L2 connection.
PRS-391859	HC policy based on LANGUARD Patch Management is not working as expected in 802.1x environment.
PRS-391566	SMTP services not working post upgrade to C9.1R4.2.
PRS-393243	Host Checker policy evaluation fails if policy rules need to be evaluated based on Custom Rule expression.
Release 9.1R8.1	
PRS-393434	Time Drift is observed when NTP is configured on Virtual Appliances. This can affect Authentication, Cluster sync and cause licensing issues – KB44558 .
Release 9.1R8	
PRS-391864	Endpoints with NAT IP address were provisioned to SRX/ScreenOS firewall even if there is no matching policy for that user session. This issue is fixed.
PRS-388319	Ivanti Policy Secure used to display an error message if the SMTP credentials were not configured. The error message will not be displayed now since the configuration without credentials is allowed.
PRS-388790	profclustermoni process crash is observed when Hostchecker policies version is changed for more than 1000 times and WMI is not configured. This issue has been fixed.
PRS-389837	TACACS+ Authorization was failing for Cisco WLC with error message "Bad service type". The service configuration is now added under TACACS+ shell policy. The default arguments i.e timeout, idletime, privilege level must be configured under Custom Attributes in the TACACS+ shell policy.

Problem Report Number	Summary
PRS-380638	tncs process crash with HC caching enabled is now fixed.
PRS-388630	With current OPSWAT library code, the verification of update functionality was not working. OPSWAT has fixed the issue and provided new library code and issue is fixed.
PRS-378040	Host Checker file rule failed as Microsoft API 'GetVersion'/'GetFileVersionInfo' was returning a wrong version value in Windows 10. This issue has been fixed.
PRS-389865	Session termination action from admission control policy was not getting triggered post AP cluster failover for existing user sessions. This issue is fixed.
PRS-390274	For config elements with unicode characters and having length exceeding 4096 bytes, the config import on pulse one client was failing. The issue has been fixed now.
Release 9.1R7	
PRS-390665	The equal to (=) character is now supported in the Custom Attributes of TACACS+ Shell Policy.
PRS-388455	If epupdate_hist.xml is hosted internally with no authentication and if "Use Proxy Server" (With/without auth) is enabled with FQDN or IP Address, the first 3 characters are ignored thus causing it to fail. For example, proxy.domain.net is taken as xy.domain.net. This issue is now fixed for both Ivanti Connect Secure and Ivanti Policy Secure.
PRS-389209	With Ivanti Connect Secure 9.0R2-9.1R6 and Pulse 9.0R2-9.1R3, the client continues to send the CAV traffic to Ivanti Connect Secure every 300 seconds even when Cloud Secure license is not installed. From Ivanti Connect Secure 9.1R7 onwards, the PDC client (Pulse 9.0R2-9.1R3) will contact the Ivanti Connect Secure server only once per user session - KB44410 .
Release 9.1R6	
PRS-390130	Ivanti Policy Secure now sends the appropriate status code for authentication failure in Cisco Switch.
PRS-388996	CSV export of Profiler Device Discovery Report with large number of entries (>50,000) can now be performed without any failure.

Problem Report Number	Summary
PRS- 388645	After upgrading Ivanti Policy Secure to 9.1R3-9.1R5, slow Host Checker response is observed due to a very frequent re-evaluation of Cybereason Active Probe product.
PRS-389276	The corruption of blob during the epupdate results in Host Checker scan failure for users till next successful epupdate.
Release 9.1R5	
PRS- 387688	Inappropriate error displayed for 'Test Intune Connection is fixed. Appropriate error message is displayed.
PRS-381678	Cluster Enhancement: Improve VIP unreachable time during cluster upgrade. This works for cluster with version running release 9.1R5 and later.
PRS-380303	ECC device certificate support on Ivanti Policy Secure is now added for SRX connection. Juniper added ECC device certificate support from Junos Release 15.X.
PRS-382340	Dashboard was reporting incorrect Session based OS count in graphs. This issue has been fixed.
PRS-384845	Host Checker policy to detect Hard Disk encryption in progress is now added in this release.
PRS-385491	TLS handshake failed error messages observed after Ivanti Policy Secure upgrade is now fixed.
PRS-387624	When replica (IF-MAP) is not reachable, CombinedChangeLog files keep accumulating and consumes space on HDD partition till it reaches 95%. This issue is now fixed.
Profiler	
PRS-388101	Canon printer was misclassified on Ivanti Policy Secure Profiler. This issue is fixed in the latest fingerprint database.
PRS-387423	Ivanti Policy Secure Profiler was not detecting the next-gen Edge OS from IGEL devices. This issue is now fixed.
PRS-388953	Finger Print database was not loaded properly into the memory during initial loading of fingerprint file. This issue is now fixed.

Problem Report Number	Summary
PRS-387461	Ivanti Policy Secure Profiler full synchronization issue with Pulse One is now fixed.
PRS-387638	Ivanti Policy Secure Profiler Finger print database is now updated to detect ASUSTek COMPUTER INC" as Manufacturer.
PRS-388117	Full Sync start time used to be a default time, i.e., 01 Jan 1970 rather Current Time.
PRS-387717	The "View all 'Unapproved Devices'" link in E-mail received by admin for Device Approval was not getting redirected to Device Discovery Report. This issue is now fixed.
Release 9.1R4.2	
PRS-387461	While forwarder full-sync is in progress and new devices are getting discovered full-sync was aborted and restarted.
Release 9.1R4.1	
PRS-385491	TLS handshake failed error message observed due to state variable in RADIUS access request is fixed.
Release 9.1R4	
PRS-382021	Dismiss until next upgrade option is not working for banner related to perpetual licensing.
PRS-380327	Devices in Network Infrastructure Device are in Undiscovered state after importing Devices
PRS-380855	Profiler is polling deleted switches once after deletion.
Release 9.1R3.1	
PRS-382319	Port Bounce issue for SNMP VLAN enforcement with Cisco switch is now fixed.
PRS-382287	TNCS process fails randomly on the server while evaluating the Host Checker policies.
PRS-385089	Duplicate machine ID feature is reverted as part of this PR.
Profiler	

Problem Report Number	Summary
PRS-384666	Ivanti Policy Secure web interface is running extremely slow.
PRS- 384736	trap-collector process restarting due to high memory usage.
PRS-385372	"trap-collector" consuming high CPU during startup.
Release 9.1R3	
PRS- 376979	Clear config on Ivanti Policy Secure set the default 'Account Lockout' values to zero for 'Guest Authentica-tion' server and this value cannot be modified or saved.
PRS 379003	End user always gets the remediation role even after endpoint meets all the End Point Security Policies.
PRS-377371	New device anomaly is not detected when connecting to Pulse via embedded browser
PRS-377957	Ivanti Policy Secure not sending auth table entry to correct vsys in PAN firewall
Profiler	
PRS-378960	In dashboard, Profiler name not retained when revisiting the same page after moving to another page.
Release 9.1R2	
PRS- 376312	Factory reset from VMware VA console does not load the factory reset version and loads the current version.
PRS-376265	Invalid character error seen while adding Radius Return attribute value which contains "<" and ">" characters.
PRS-376465	Host Checker service in Pulse is crashing while performing policy monitoring when pulse client is retrying.
PRS-372699	NMAP scan profiling is inaccurate
PRS-372499	Session from Exported session list get purged on cluster if the passive node is disabled, re-booted and rejoined.
PRS-372440	Post Failover, Delayed session resumption with Pulse Client.

Problem Report Number	Summary
Release 9.1R1	
PRS-374583	Behavior of "re-authentication" and "termination" options in radius Return Attribute policy page is interchanged.
PRS-371733	Assigned VLAN is not updated if fetched on the next poll and always shows default config-ured. VLAN.
PRS-370902	Behavioral Analytics dashboard is not displaying charts for potential malware and anomalous traffic from IoT devices for more than 4 device categories intermittently.
PRS-370903	MAC address is not updated in the user session details.
PRS-374582	Behavior of "re-authentication" and "termination" options in radius Return Attribute policy page is interchanged.
PRS-374368	PSAL launch failed when proxy browser is configured.
PRS-374477	Fortinet admission control feature will not work with domain users (AD).
PRS-371536	Host Checker: Virus Definition Check for updates fails for K7 Virus Security ZERO (14.x),
PRS-373619	Host Checker: Virus Definition Check for updates fails for AVG Free Antivirus (19.2.x).

Known Issues

The following table lists the Known issues in the current release.

Problem Report Number	Description
Release 9.1R18.2	
There are no known issues in this release.	
Release 9.1R18.1	
There are no known issues in this release.	
Release 9.1R18	
PRS-403958	<p>Symptom:Swap memory consumption and high CPU usage.</p> <p>Condition: Performing SNMP polling on 200+ switches and monitoring 10,000 dot1x user sessions has the potential to significantly increase swap memory and CPU utilization by both, the SNMP collector and PostgresServer. The SNMP polling process requires the retrieval of ARP/CAM tables from all switches, which is a computationally intensive task that can consume significant CPU resources. Similarly, 10,000 dot1x user sessions results in frequent updates to the Postgres database with session details, leading to increased memory and CPU utilization. CPU utilization and Swap memory Usage will come down to normal levels once the polling is complete , the time of polling depends on number of switches being scanned..</p> <p>Workaround: None.</p>
Release 9.1R17	
PPS-414173	<p>Symptom:Host Checker on Unbantu OS is not supported on Firefox</p> <p>Condition: On Linux, Host checker on the Unbantu OS is not supported on Firefox.</p> <p>Workaround: None.</p>
PPS-10292	<p>Symptom: In Chinese language, machine certificate rule failed message showing in English.</p>

Problem Report Number	Description
	<p>Condition: When using Chinese language on Firefox ESR browser.</p> <p>Workaround: None.</p>
PPS-39791	<p>Symptom: Citrix Storefront with CTS client will not launch.</p> <p>Condition: When PSAL extension is enabled.</p> <p>Workaround: Disable PSAL extension, CSF-CTS client will launch.</p>
Release 9.1R16	
PPS-10117	<p>Symptom: Server is not allowing to connect a client, displays error "CreateRadiusRequest Faliure" or "Authentication Rejected by Server : 1308"</p> <p>Condition: When server is configured with "Advanced Host Checking" policy and client access the URL to evaluate this policy on Windows System .</p> <p>Workaround: Remove "Advanced Host Checking" policy from the Role/Realm on the server.</p>
PPS-10117	<p>Symptom: Server is not allowing to connect a client, displays error "CreateRadiusRequest Faliure" or "Authentication Rejected by Server : 1308"</p> <p>Condition: When server is configured with "Advanced Host Checking" policy and client access the URL to evaluate this policy on Windows System .</p> <p>Workaround: Remove "Advanced Host Checking" policy from the Role/Realm on the server.</p>
PPS-10086	<p>Symptom: After upgrade IPS/ICS server to 9.1R16 shows scroll bar instead of list during OS Hostcheck Policy configuration.</p> <p>Condition: Changes observed after upgrade Server to 9.1R16</p> <p>Workaround: There is no functionality impact to perform OS check on the client.</p>
PRS-411449	<p>Symptom: Some random radius logs getting generated on UI event logs.</p>

Problem Report Number	Description
	<p>Condition: On upgrading IPS 2-node cluster to 9.1R16.</p> <p>Workaround: None.</p>
Release 9.1R15	
No known issues in this release.	
Release 9.1R14	
No known issues in this release.	
Release 9.1R13.1	
PRS-404815	<p>Symptom: Remediation rule is not working.</p> <p>Condition: When the client is configured with the HKEY-CURRENT-USER.</p> <p>Workaround: None</p>
PRS-404756	<p>Symptom: Active user session from Windows 11 shows log-in from Windows 10 System.</p> <p>Condition: User logs in from Windows 11 systems using Browsers or PDC.</p> <p>Workaround: None</p>
Release 9.1R13	
PRS-404205	<p>Symptom: "DeleteAllSessions" not releasing the IP addresses assigned to the user sessions.</p> <p>Condition: Sessions with assigned IP address from IP address pools.</p> <p>Workaround: Select all sessions. Uncheck only "admin" session and click "delete selected sessions".</p>
PRS-403958	<p>Symptom: Swap memory consumption and high CPU usage.</p> <p>Condition: Increase in swap memory consumption and high CPU usage is observed in heavily loaded Profiler system.</p> <p>Workaround: None</p>

Problem Report Number	Description
PRS-403875	<p>Symptom: Guest Sponsor received e-mails do not contain some details entered during register process.</p> <p>Condition: When registered as guest with details of Company Name and Host or Sponsor.</p> <p>Workaround: None</p>
PRS-403525	<p>Symptom: ESAP diagnose tool collects only OPSWAT related logs and does not collect any Pulse logs.</p> <p>Condition: When an endpoint connected to latest 9.1R13 server and required components are installed.</p> <p>Workaround: From the endpoint manually collect Pulse logs or using PDC save required logs.</p>
PRS-403476	<p>Symptom: Active user session from Windows 11 shows log in from Windows 10 System.</p> <p>Condition: User login from Windows 11 systems using Browsers or PDC.</p> <p>Workaround: None</p>
Release 9.1R12	
PRS-402625	<p>Symptom: Juniper SRX firewall and Ivanti Policy Secure connection doesn't break after changing TLS version 1.2 with higher encryption setting for non-supported TLS1.2 version Juniper SRX firewall.</p> <p>Condition: Juniper SRX firewall is running lower version, which do not support TLS1.2 and Ivanti Policy Secure security setting (Configuration > Security > SSL Options) Accept only TLS 1.2 (maximize security) with Maximize Security (High Ciphers).</p> <p>Workaround: Need to restart uac-service in Juniper SRX firewall using the command (restart uac-service). Ivanti Policy Secure and SRX connection breaks and is reestablished with higher TLS and encryption settings.</p>
Release 9.1R10	

Problem Report Number	Description
PRS-396726	<p>Symptom: Active user page "Agent Type" shows "Mac OS 10.15" in place of "Mac OS 11.0.1".</p> <p>Condition: When using Safari on macOS version BigSur 11.0.1.</p> <p>Workaround: None</p>
Release 9.1R9	
PRS-394472	<p>Symptom: NTP will not synchronize time when default VLAN ID is configured on the interface.</p> <p>Condition: If default VLAN ID is configured on the interface.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Remove VLAN ID from the interface. 2. On PSA hardware, use "Set Time Manually" option. 3. On Ivanti Policy Secure virtual machines (VM's), disable NTP on Ivanti Policy Secure and Enable Sync with ESXi Host Option on VMware ESXi.
PRS-393851	<p>Symptom: Invalid Admin log shows as "Unable to synchronize time, either NTP server(s) are unreachable or provided symmetric key(s) are incorrect" even though NTP servers are reachable and clock is syncing.</p> <p>Condition: When upgrading to 9.1R8.1 or later builds.</p> <p>Workaround: None</p>
PRS- 394868	<p>Symptom: Sending Guest mail notification fails while using SMTP Server Config with SMTP Login/Password.</p> <p>Conditions: While SMTP configuration with SMTP Login and SMTP Password with or without SSL under System > Configuration > Guest Access > SMTP Settings</p> <p>Workaround: Configure SMTP Server without SMTP Login and SMTP Password and made SSL disable, perform NTLM authentication.</p>

Problem Report Number	Description
PRS-395918	<p>Symptom: Internal Error occurred while performing SNMPv3 Discovery from Profiler UI.</p> <p>Condition: Perform SNMPv3 Discovery from Profiler UI.</p> <p>Workaround: Retry from Profiler UI page or Navigate & Discover from Endpoint Policy > Network Access > Network Infrastructure page</p>
PRS-395705	<p>Symptom: While adding Palo Alto Network devices as SNMP Client in Profiler new UI (from Ivanti Policy Secure version 9.1R8 onwards) SSH options are not shown.</p> <p>Condition: Adding new Palo Alto Networks as SNMP client in new profiler UI.</p> <p>Workaround: Add SNMP client from Network Access > New network Infrastructure Devices.</p>
Release 9.1R8.2	
PRS-22360	<p>Symptom: SAML SLO is not initiated from Ivanti Policy Secure to its IDP when the user's browser-based session is ended.</p> <p>Condition: When user is authenticated using any browser to Ivanti Policy Secure with SAML authentication method where Ivanti Policy Secure is SAML SP, user session is ended in browser because of idle timeout or max session timeout or if admin ends the user session from Ivanti Policy Secure Admin console. Currently only manual sign out from browser session is supported to send SLO request to IDP from Ivanti Policy Secure side.</p> <p>Workaround: Close the browser window and launch a new browser window, so that user is prompted for authentication again for security reasons</p>
Release 9.1R8	
PRS-392283	<p>Symptom: SBR TACACS+ shell policies defined at the user level is not supported.</p> <p>Condition: If shell policy is defined at user level, only the user will be migrated to Ivanti Policy Secure but will not be mapped to shell policy.</p>

Problem Report Number	Description
	<p>Workaround: In this case, Admin has to manually configure role, shell policy and role mapping rule in the realm.</p>
PRS-392236	<p>Symptom: Hyper-V 9.1R8 upgrade from earlier versions is not supported.</p> <p>Condition: When upgrading from the earlier versions. For example, 9.1R5.</p> <p>Workaround: Install a fresh instance of 9.1R8 and import the configurations from the earlier version.</p>
PRS-392832	<p>Symptom: After upgrading to 9.1R8, admission control alert is not processed post VIP failover.</p> <p>Condition: Users connected to Active Node in A/P cluster will move to Passive Node on Cluster failover. If any Admission control event/alert is received for these users, action set in the Admission control policy will not be triggered.</p> <p>Workaround: Disabling and enabling any one of the admission control clients post VIP fail will address the issue.</p>
PRS-392571	<p>Symptom: Cisco WLC is not supporting default arguments with some roles.</p> <p>Condition: When Ivanti Policy Secure assigns any roles apart from ALL/MONITOR WLC throws error saying "bad authorization".</p> <p>Workaround: To handle this specific scenario if service type is configured as "ciscowlc" in Ivanti Policy Secure then no default attributes (session timeout, idle timeout and privilege level) are sent but if admin wants these attributes to be sent (in case of admin roles like ALL and MONITOR) admin must configure the attributes as custom attributes.</p>
PRS-384976	<p>Symptom: Host Checker (HC) installation error found Intermittently while installing HC or Pulse Client (HC enabled) through browser (Chromium Edge/Chrome/Firefox)</p> <p>Condition: Fresh Installation of HC or Pulse Client (HC enabled) through browser (Chromium Edge/Chrome/Firefox) after uninstalling old HC components</p>

Problem Report Number	Description
	<p>Workaround: Uninstall the HC/Pulse Client components manually and reboot the system or Manually kill the HC process before installing Pulse Client/HC Component.</p>
PRS-391305	<p>Symptom: Upgrading Azure images from 9.1R5 to any later releases returns with error message for Ivanti Policy Secure if the factory reset version is 9.1R5</p> <p>Conditions: When factory reset version is 9.1R5.</p> <p>Workaround: Admin has to take the backup of the existing configurations. Deploy the new image with latest version and import the backup configurations.</p>
Profiler	
PRS-391014	<p>Symptom: Calender pop-up in Advanced Filter on DDR Page does not work intermittently</p> <p>Condition: Navigate to System > Reports > Device Discovery Tab, enter the from/to dates in Advanced Filters</p> <p>Workaround: Refresh the page and retry.</p>
PRS-393086	<p>Symptom: If device sponsoring and time bound is configured for an endpoint in the selected sponsored category then during classification device sponsoring is given priority over time-bound. Due to which endpoint status is set to unapproved.</p> <p>Condition: With Device sponsoring configured and Time Bound option enabled for the selected categories in the Profile Group.</p> <p>Workaround: Don't configure device sponsoring, if time-bound configurations has to be used.</p>
PRS-393099	<p>Symptom: Roles are not getting updated based on updated status.</p> <p>Condition: Export DB (csv/binary) and then import DB for the same endpoint during active session.</p>

Problem Report Number	Description
	<p>Workaround: Roles will be updating after doing logout from the session and re-initiate session from the endpoint.</p>
PRS-393005	<p>Symptom: Configuring Agentles Hsostcheck policy Navigate to Auth Servers link wrongly redirects to Authentication Servers Page instead of Profiler page.</p> <p>Condition: User navigates to Endpoint Security > Host Checker and click "Profiler" collector under option or Endpoint Security > Host Checker > New Host Checker Policy and clicks "Auth Servers" settings.</p> <p>Workaround: Navigate to Profiler Configuration > Settings > Basic Configuration for configuration.</p>
Release 9.1R5	
PRS-389553	<p>Symptom: uacHostChecker process application exits unexpectedly</p> <p>Condition: Pulse Client with latest component tries to connect to lower server version, for example: 5.4R7.1 through Internet Explorer/Chrome/Firefox.</p> <p>Workaround: This issue is seen only on Windows 10 (1909) version whereas Windows RS5 (1809) and Windows7 Enterprise there is no issue.</p>
PRS-389409	<p>Symptoms: User sessions will not be synced for the session logged in at the time of second node upgrade in Active Passive cluster.</p> <p>Condition: During Active Passive cluster upgrade, when the first node comes up after upgrading newer version, it informs the other node to upgrade. During this time if any new user logs in then all those sessions will not be synced after second node upgrade.</p> <p>Workaround: Users needs to re-login</p>
PRS-389234	<p>Symptom: ECC device certificate is not supported with SRX firewall below Junos version 15.x.</p> <p>Condition: If the server uses ECC device certificate then the connection to SRX is established only with releases later than Junos 15.x version.</p>

Problem Report Number	Description
	<p>Workaround:</p> <p>ECC certificate support is introduced in releases later than 15.x Junos version.</p> <p>If the server uses ECC device certificate, then the connection to SRX is established only with releases later than Junos 15.x version.</p> <p>If the server has both the ECC and RSA device certificate installed, then Restart Services (System Maintenance > Platform > Restart Services) is required to switch from ECC to RSA or vice versa).</p>
PRS-389642	<p>Symptom: XML import is failing if configuration file has syslog IPv6 settings.</p> <p>Condition: If IPv6 syslog server on log settings is configured then the XML import fails.</p> <p>Workaround: Export the binary system configuration and import on another device.</p>
PRS-389078	<p>Symptom: When the end-user changes his password, login with the changed password fails.</p> <p>Condition: User won't be able to login with the changed password.</p> <p>Workaround: Admin can change the password for the end-user and that password can be used to login.</p>
PRS-389763	<p>Symptom: When SNMP Device is discovered using SNMP (v2/v3 version), Location Group and Default VLAN configured for the discovered device is not applied after clicking "Add Device".</p> <p>Condition: Discover a Switch using SNMP (v2/v3 version). Configure Location Group and Default VLAN, and then click on "Add Device". Added device will not have the Location Group and Default VLAN configuration.</p> <p>Workaround: Configuration has to be manually changed under Endpoint Policy > Network Access > Network Infrastructure Device.</p>

Problem Report Number	Description
PRS-385553	<p>Symptom: Connection error displayed while installing Host Check component. The issue is seen while performing agentless connection (Host Check enabled) after cleaning all the previously installed Host Check components.</p> <p>Conditions: "UAC Host Checker" process running in the background.</p> <p>Workaround: Kill the process or reboot the system and perform agentless connection.</p>
PRS-390106	<p>Symptom: Inconsistent upgrade issues seen while upgrading Hyper-V images in clustering and single node.</p> <p>Condition: Upgrading a Hyper-V image to 9.1R5.</p> <p>Workaround: If cluster upgrade fails, reboot the node which is not upgraded. If the issue persists, try upgrading the nodes individually and then form cluster.</p>
PRS-390303	<p>Symptom: The event Agent_session_bridge is not included in Login Type Dashboard chart formation in splunk App.</p> <p>Condition: It gets impacted only when a user forming L2 followed by L3 session from the PDC client. The reason is, this event is not been added in parsing regexp in backend , hence bridged session will not be appeared in Login_Type Dashboard chart in Ivanti Policy Secure App.</p> <p>Workaround: The event 'Agent_session_bridge' should be added in backend with applying regexp for the field to be extracted for further use.</p>
PRS-390300	<p>Symptom: The current splunk session displayed on Dashboard will not be retained when clicking on Ivanti Policy Secure App.</p> <p>Condition: Splunk limitation</p> <p>Workaround: Not Available</p>
Profiler	
PRS-389626	<p>Symptom: Full sync happens more than once in Forwarder A/P Cluster.</p>

Problem Report Number	Description
	<p>Condition: This issue is observed only after upgrading Forwarder A/P Cluster.</p> <p>Workaround: None</p>
PRS-389305	<p>Symptom: During "edit all similar devices" in DDR, the response message is displayed successful. However, devices are still getting classified in the background. Admin does not know when the re-classification is done for all the devices.</p> <p>Condition: This occurs when there is large number(~50K) of devices classified.</p> <p>Workaround: Refresh the DDR page after few minutes.</p>
PRS- 389161	<p>Symptom: If endpoints entries are deleted from DC, these endpoints are not deleted from DR and vice versa.</p> <p>Condition: This issue is only seen when full sync is in progress. If endpoints entries are deleted after full sync done, sync happens properly.</p> <p>Workaround: Delete the endpoints from DC/DR separately.</p>
PRS-388961	<p>Symptom: In the Switch View Bridge Interfaces are not showing up, all other interfaces are coming.</p> <p>Condition: Fetching the IFMIB doesn't gives the bridge interfaces.</p> <p>Workaround: None.</p>
Release 9.1R4	
PRS-386989	<p>Symptom: Mist is not sending class attribute and hence Ivanti Policy Secure unable to map session for incoming accounting request due to which the accounting stop will not remove the session from the Ivanti Policy Secure after Guest disconnects from SSID</p> <p>Condition: When SSID is disconnected from the endpoint by the Guest without logging out from the active session</p>

Problem Report Number	Description
	<p>Workaround: Manually remove the active session from Mist controller Or Provide lower session timeout value for Guest users in Ivanti Policy Secure.</p>
PRS- 387494	<p>Symptom: Mist is not sending class attribute and hence Ivanti Policy Secure unable to map session for incoming accounting request and hence IP is not getting updated in the Active Users page in Ivanti Policy Secure</p> <p>Condition: When active Guest session is formed</p> <p>Workaround: NA</p>
Release 9.1R3	
PRS-381239	<p>Symptom: CSV import to System local database will fail with error message as "Invalid User Name. Only ASCII characters are allowed on Ivanti Policy Secure UI.</p> <p>Condition: When username in the CSV file to be imported to System local database involves characters apart from ASCII</p> <p>Workaround: None</p>
PRS-381394	<p>Symptom: Microsoft Excel is changing the format of CSV file while saving.</p> <p>Condition: User tries to edit the CSV file using MS Excel.</p> <p>Workaround: User should make sure that CSV file fulfil all condition of CSV file format. Open file in simple editor like: notepad++, vim.</p>
PRS-381554	<p>Symptom: Policy evaluation failed on macOS 10.14x or any higher versions for a file rule configured to validate a file location with System default Directories <%HOME%></p> <p>Condition: Hostcheck policy with File Rule for macOS 10.14.x or higher versions for a file located at System Directories <%HOME%></p> <p>Workaround: Need to add permissions for "Pulse Client" under "Accessibility" and "Full Disk Access" and which can be accessed from System Preferences > Security & Privacy > Privacy Or without providing permission /tmp location can be used for File validation.</p>

Problem Report Number	Description
PRS-380471	<p>Symptom: Ivanti Policy Secure upgrade to 9.1R3 will not update the connection set and component set of the user role configured with Odyssey Access client settings.</p> <p>Condition: Fresh installation of Pulse client or migrating from OAC to Pulse client</p> <p>Workaround: OAC migration guide will help the administrators to configure the connection set and component set and map the same to appropriate roles.</p>
PRS-382021	<p>Symptom: Dismiss until next upgrade option is not working for banner related to perpetual licensing.</p> <p>Condition: Admin clicks on Dismiss until next upgrade.</p> <p>Workaround: For every new Admin login use the close button as a workaround.</p>
Release 9.1R2	
PRS-378002	<p>Symptom: Cache server is continuously crashing in Longevity setup. Unable to open admin UI, crash messages display.</p> <p>Condition: When cache memory is hitting more than 512mb this crash has been observed.</p> <p>Workaround: NA, rollback and upgrade to latest version to start the test again.</p>
PRS-378052	<p>Symptom: SMTP Port 465 is not working for Ivanti Policy Secure guest user.</p> <p>Condition: Under SMTP settings, port 465 should also supported for Guest user.</p> <p>Workaround: SMTP port 587 with selecting SSL works in case of guest.</p>

Problem Report Number	Description
PRS-379012	<p>Symptom: Radius Disconnect message (DM) is not working after importing user.cfg configuration from the previous release.</p> <p>Condition: When previous configuration (from 9.0R1) is loaded onto the box, overwrites the de-fault radius.dct. "Funk-Dest-IPv6-Address" attribute is missing in the old dictionary.</p> <p>Workaround: After restoring the dictionary to factory default, DM is sent to the switch and session is disconnected.</p>
PRS-379063	<p>Symptom: While performing L3 followed by L2 and frequently enable/disable migration option some time SDKs are replacing next periodic host check</p> <p>Conditions: On Windows Platform using Pulse performing L2 authentication with Host Check enabled on Role/Realm with Migration feature enabled.</p> <p>Workaround: For replacing expected SDKs wait for next periodic Handshake or Disconnect and again connect to server using Pulse.</p>
PRS-377549	<p>Symptom: PSIS is not upgrading to the 9.1R2 version.</p> <p>Condition: When CTS, WTS and VDI gets upgraded to 9.1R2 in Win10RS5+.</p> <p>Workaround: NA</p>
Profiler	
PRS-378956	<p>Symptom: Linkdown Trap is not updating device link status in Device Discovery Report when profiler processes for the first time.</p> <p>Condition: Profiler not processing Linkdown Trap without Linkup trap update in Device Discovery page for the device.</p> <p>Workaround: NA</p>
Release 9.1R1	

Problem Report Number	Description
PRS-372687	<p>Symptom: RADIUS CoA disconnect for Splash sign on page in Meraki WLC does not acknowledge the session disconnect message sent by Ivanti Policy Secure.</p> <p>Conditions: Guest session will be deleted from Ivanti Policy Secure, but the session will be active on WLC for the default timeout period of the guest session on Meraki WLC.</p> <p>Workaround: Admin can login to Meraki dashboard and de-authorize the guest manually from Wire-less > Splash logins page. In addition to that, we have raised an enhancement request to Meraki to support COA disconnect on splash sign on page with radius authentication.</p>
PRS-372794	<p>Symptom: RADIUS Accounting stop message is not sent by Meraki when guest logs out or gets disconnected from Guest SSID</p> <p>Conditions: The Guest session will remain active on Ivanti Policy Secure for the duration of Maximum Session Length (default=725 mins).</p> <p>Workaround: Admin can login to Meraki dashboard and de-authorize the guest manually from Wire-less > Splash logins page which will immediately send the Accounting stop message from Meraki to Ivanti Policy Secure.</p>
PRS-373861	<p>Symptom: TACACS+ Accounting start and stop messages are not sent by BIG IP F5 device</p> <p>Condition: Ivanti Policy Secure may have stale sessions as it does not receive stop accounting packets. However, these sessions are deleted from Ivanti Policy Secure when Maximum Session Timeout expires.</p> <p>Workaround: NA. If there is any stale TACACS+ session on Ivanti Policy Secure, it does not cause any security risk as any TACACS+ login is controlled by the BIG IP F5 device.</p>

Problem Report Number	Description
PRS-372849	<p>Symptom: Session migration fails for secondary auth server. User is prompted with secondary auth server password.</p> <p>Condition: If secondary auth server is configured for session migration.</p> <p>Workaround: NA</p>
PRS-372250	<p>Symptom: Session migration fails for 802.1X authentication.</p> <p>Condition: When the user tries to migrate the 802.1X sessions from Ivanti Policy Secure to Ivanti Connect Secure.</p> <p>Workaround: NA</p>
PRS-374476	<p>Symptom: Firewall SOH policy evaluation fails for domain user when Private and Public Net-works profiles in Windows Firewall are not turned ON.</p> <p>Condition: When Private and Public network profile for domain user is not turned ON for Windows firewall.</p> <p>Workaround: NA</p>
PRS-374663	<p>Symptom: L3 session is established with Internal IP while performing L3 followed by L2 using Pulse with Ivanti Policy Secure External VIP address.</p> <p>Conditions: When Ivanti Policy Secure nodes are in cluster and external port is used for RADIUS authentication.</p> <p>Workaround: NA</p>
PRS-360616	<p>Symptom: SAML authentication failed with error "Missing/Invalid sign-in URL" despite correct credentials while using PDC embedded browser version 9.0.1.</p> <p>Condition: Using PDC browser version 9.0.1 with Ivanti Policy Secure version 9.1R1.</p> <p>Workaround: Use latest PDC version with Release 9.1R1.</p>

Problem Report Number	Description
PRS-366966	<p>Symptom: Juniper Connector UI provides option to select TCP ports for communicating with Ivanti Policy Secure. However, Ivanti Policy Secure connector always use port 443, making the selected TCP port ineffective.</p> <p>Conditions: Configuring Ivanti Policy Secure as connector in Juniper PE.</p> <p>Workaround: Ensure that the Port number is always set to 443.</p>
PRS-367195	<p>Symptom: While configuring the Ivanti Policy Secure connector in Juniper PE, administrator need to enter the system-local administrator credentials as Ivanti Policy Secure admin and AD user account cannot be used for generating REST API key for Ivanti Policy Secure-Juniper PE communication.</p> <p>Conditions: Configuring Ivanti Policy Secure as Connector in Juniper PE.</p> <p>Workaround: Juniper SDSN integration with Ivanti Policy Secure requires creating a local Admin user on Ivanti Policy Secure.</p>
PRS-367291	<p>Symptom: Certificate Authentication fails due to configuration of "Skip Revocation when OCSP/CDP server is not available" for HC policy enforced at realm level.</p> <p>Condition: When admin enables Skip Revocation check and OSCP server is not reachable.</p> <p>Workaround: Set the OSCP timeout to less than 5 seconds.</p>
PRS-368055	<p>Symptom: Admin is allowed to create anomaly role mapping rules based on custom expressions when UEBA license is not installed.</p> <p>Condition: Configuring anomaly role mapping rules based on custom expressions when Behavioral Analytics license is not installed.</p> <p>Workaround: Install Behavioral Analytics License.</p>

Problem Report Number	Description
<p>PRS-366296</p> <p>PRS-369738</p>	<p>Symptom: Authentication to Ivanti Policy Secure fails as Duo custom sign-in pages are not displayed.</p> <p>Condition: User authenticates to Ivanti Policy Secure and assigned realm is configured with Duo as secondary authentication server.</p> <p>Workaround: Use passcode-based Duo authentication.</p>
<p>PRS-367024</p>	<p>Symptom: Authentication fails for browser-based login for Duo and LDAP combination with predefined user as <USER> in secondary authentication server.</p> <p>Condition: User authenticates to Ivanti Policy Secure and assigned realm is configured with Duo as primary and LDAP as secondary auth server</p> <p>Workaround: Use passcode based Duo authentication.</p>
<p>PRS-368136</p>	<p>Symptom: VIP failover fails in A/P cluster when the Active node becomes unreachable with SPAN configured on external port.</p> <p>Condition: Active node becomes unreachable in A/P Cluster with Local SPAN enabled on cluster nodes' external port.</p> <p>Workaround: Configure Remote SPAN.</p>
<p>PRS-368689</p>	<p>Symptom: OS Check rule is not supported when trying to connect from 9.0R3 Pulse client to old Ivanti Policy Secure (9.0R2\9.0R1) server on MAC OS platform.</p> <p>Condition: When OS check Host checker rule is evaluated with new Pulse client connecting to pre-9.0R3 Ivanti Policy Secure server.</p> <p>Workaround: Pulse client on MAC platform and Ivanti Policy Secure server need to be 9.0R3 for OS Check host checker policy to work as expected.</p>

Problem Report Number	Description
PRS-368967	<p>Symptom: Host checker fails on Mac OS 10.14 Mojave endpoint when Activate Older OPSWAT SDK in ESAP is enabled.</p> <p>Condition: When ESAP with V3 SDK is activated on the server.</p> <p>Workaround: Administrator should activate ESAP with V4 SDK on Ivanti Policy Secure for Host check to work as expected.</p>
Profiler	
PRS-369079	<p>Symptom: For Agentless Host Checker with Profiler, Antivirus Rule with "virus definition age" check may fail.</p> <p>Conditions: Windows registry does not maintain the timestamp, when last virus definition was in-stalled. Time is taken as midnight time (00:00:00) of the date, when the last definition was installed.</p> <p>Workaround: Create the rule with (expected number of definition age + 1) days.</p>
PRS-367687	<p>Symptom: Remote profiler is unable to communicate with Profiler; hence the remote endpoints are not profiled.</p> <p>Conditions: If self-signed certificate is used on Profiler Authentication server.</p> <p>Workaround: Using a CA signed certificate on Profiler server.</p>
PRS-361246	<p>Symptom: Endpoint session status is not updated in DDR table if the same endpoint is imported through Binary configuration.</p> <p>Conditions: Importing profiler data using Binary configuration.</p> <p>Workaround: Reconnect the existing user session.</p>
Cloud Application Visibility	

Problem Report Number	Description
PRS-370268	<p>Symptom: CAV fails to configure proxy on endpoint, when Juniper SRX is configured as an Infranet Enforcer for a resource.</p> <p>Condition: Juniper SRX is configured as Infranet Enforcer.</p> <p>Workaround: N/A</p>
PRS-370249	<p>Symptom: CAV policies are not applied when endpoints establish dot1x connection with a switch/access point.</p> <p>Condition: Authenticator is a third-party device and is configured to use Ivanti Policy Secure as authenticating server.</p> <p>Workaround: N/A</p>
PRS-370237	<p>Symptom: CAV policy updates are not sent to Ivanti Policy Secure if CAV Database is updated with Ivanti Connect Secure IP address.</p> <p>Condition: If CAV database at client side is updated with Ivanti Connect Secure IP address and the user establishes L2/L3 connection.</p> <p>Workaround: N/A</p>
PRS-370123	<p>Symptom: DNS resolution fails after CAV is re-enabled at user role level.</p> <p>Conditions: If already added user role is deleted from the CAV policies.</p> <p>Work Around: - N/A</p>
PRS-369277	<p>Symptom: CAV feature does not work when Pulse SAM is enabled on client.</p> <p>Conditions: Pulse SAM and CAV enabled for the same role.</p> <p>Work Around: - N/A</p>
PRS-369891	<p>Symptom: Authentication token fetching is failing under NATed environment on Pulse client for CAV policies update.</p> <p>Conditions: Ivanti Connect Secure configured behind a NAT device.</p> <p>Work Around: N/A</p>

Problem Report Number	Description
PRS-369279	<p>Symptom: Lockdown is not working properly if CAV policies are configured.</p> <p>Conditions: Enabling CAV with lock down.</p> <p>Work Around: N/A</p>

Upgrade Instructions

Upgrade Paths

The following table describes the tested upgrade paths.

Please note that here x and y refer to the following.

- x: Latest maintenance release version.
- y: Any previous release older than latest release.

Upgrade From	Qualified	Compatible
9.1Rx	Yes	-
9.1Ry		Yes



If your system is running beta software, roll back to the previously installed official software release before upgrading. This practice ensures the rollback version is a release suitable for production.

Upgrade Scenario Specific to Virtual Appliances

PSA-V cannot be upgraded to current release without core license.

Follow these steps to upgrade to the current release:

1. If PSA-V is running 5.4Rx:
 - Upgrade to 9.0Rx.
 - Install Core license through Authcode.
 - Upgrade to 9.1Rx.
2. If PSA-V is running 9.0Rx or later:
 - Install Core license through Authcode.
 - Upgrade to 9.1R11.

Documentation

When you need additional information or assistance, you can contact the Ivanti Global Support Center:

| <https://support.pulsesecure.net/>

| support@pulsesecure.net

Call us at 1- 844-751-7629 (toll-free USA)

For more technical support resources, browse the support website <https://support.pulsesecure.net/>