Ivanti Connect Secure Release Notes

9.1R18.7

Ivanti Connect Secure Build 25581

Ivanti Secure Access Client 22.7R1.1 Build 29163

Default ESAP Version: ESAP 4.3.8

Copyright Notice

Contents

Revision History

The following table lists the revision history for this document:

Document Revision	Date	Description
18.7	June 2024	Updated for release 9.1R18.7
18.6	May 2024	Updated for release 9.1R18.6
18.5	April 2024	Updated to indicate the security updates for release 9.1R18.5
18.4	February 2024	Updated to indicate the security updates for release 9.1R18.4
18.2.1	November 2023	Updated Noteworthy Information for 9.1R18.2.
18.2	September 2023	Updated for release 9.1R18.2
18.1	July 2023	Updated for release 9.1R18.1
18.0	April 2023	Updated for release 9.1R18
17.1	March 2023	Updated fixed issues for release 9.1R17.1
17.0	November 2022	Updated for release 9.1R17
16.1	September 2022	Updated default ESAP version and Fixed issues for 9.1R16.1
16.0	July 2022	Updated for release 9.1R16
15.0	April 2022	Version 9.1R15: • Added "Noteworthy Information in 9.1R15 Release" on page 13 • Added "Release 9.1R15 Features" on page 18 • Added to the Fixed Issues the "Release 9.1R15 PRs" on page 44 • Added to the Known Issues "Release 9.1R15 PRs" on page 91

Document Revision	Date	Description
14.0	January 2022	Version 9.1R14: • Re-branded the entire document text to make it Ivanti, Ivanti Connect Secure and Ivanti Ploicy Secure specific as applicable • Added "Noteworthy Information in 9.1R15 Release" on page 13 • Added "Release 9.1R15 Features" on page 18 • Added to the Fixed Issues the "Release 9.1R14 PRs" on page 46 • Added to the Known Issues "Release 9.1R14 PRs" on page 94
13.1	December 2021	Version 9.1R13.1: • Added "Noteworthy Information in 9.1R13.1 Release" on page 14 • Added to the Fixed Issues the "Release 9.1R13.1 PRs" on page 49 • Added to the Known Issues "Release 9.1R13.1 PRs" on page 95
13.0	October 2021	Version 9.1R13: • Added the "Noteworthy Information in 9.1R13 Release" on page 14 • Added "Release 9.1R13 Features" on page 20 • Added to the Fixed Issues the "Release 9.1R13 PRs" on page 49 • Added to the Known Issues "Release 9.1R13 PRs" on page 96

Document Revision	Date	Description
		Version: 9.1R11.5: Added one point to the "Noteworthy Information in 9.1R11.5 Release" on page 15
12.2	October 2021	Version 9.1R12.1: A new "Release 9.1R12.1 PRs" on page 51 section in Fixed Issues. Added two PRs.
12.1	September 2021	Version 9.1R12: Updated the Noteworthy Information in 9.1R12 Release section.
12	August 2021	Version 9.1R12: • Added the Noteworthy Information in 9.1R12 Release section. • Added the New Features > Release 9.1R12 Features section. • Updated the Fixed Issues section > 9.1R12 list. • Updated the Known Issues section > 9.1R12 list.
11.4	May 2021	Updated the Noteworthy Information in 9.1R11 Release section and updated the Fixed Issues.
11.4	April 2021	Updated the Fixed and Known Issues for 9.1R11.4.
11.3	April 2021	Updated Fixed Issues and Known for 9.1R11.3.
11.0	January 2021	Changed the company logo, initial publication for 9.1R11.
10.1	December 2020	Updated the Noteworthy Information in 9.1R10 Release section with the MSSP License reporting enhancements.
10.0	December 2020	Version 9.1R10: Initial Publication.
9.1	November 2020	• Updated the Fixed Issues > 9.1R9.1 list. • Updated the Known Issues > 9.1R9.1 list.
9.0.1	November 2020	

Document Revision	Date	Description
		• Updated the Fixed Issues > 9.1R8.2 list. • Updated the Known Issues > 9.1R9 list.
9.0	October 2020	Initial Publication: 9.1R9
8.4	September 2020	Initial Publication: 9.1R8.2
8.3	August 2020	Initial Publication: 9.1R8.1
8.2	August 2020	Updated the Known Issues section.
8.1	July 2020	Updated the Fixed Issues > 9.1R7 and 9.1R8 list.
8.0	July 2020	Initial Publication: 9.1R8
7.0	June 2020	Initial Publication 9.1R7 Updated the Fixed Issues > 9.1R1 Release with PRS-368927
6.0	May 2020	Initial Publication: 9.1R6
5.3	April 2020	Updated the Known Issues section for 9.1R5
5.2	April 2020	Cosmetic change for 9.1R5
5.1	April 2020	Updated the New Features section for 9.1R5
5.0	April 2020	Initial Publication: 9.1R5
4.3	April 2020	Initial Publication: 9.1R4.3
4.2	March 2020	Initial Publication: 9.1R4.2
4.1	February 2020	Initial Publication: 9.1R4.1
4.0	January 2020	Initial Publication: 9.1R4
3.1	October 2019	Updated the Known Issues section for 9.1R3
3.0	October 2019	Initial Publication: 9.1R3
2.0	July 2019	Initial Publication: 9.1R2
1.0	May 2019	Initial Publication: 9.1R1

Introduction

This document is the release notes for Ivanti Connect Secure Release 9.1R18.7. This document contains information about what is included in this software release: supported features, feature changes, unsupported features, and known issues. If the information in the release notes differs from the information found in the documentation set, follow the release notes.

Security Advisory and Patch Update

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

- CVE-2024-21894
- CVE-2024-22052
- CVE-2024-22053
- CVE-2024-22023
- CVE-2023-46805
- CVE-2024-21887
- CVE-2024-21888
- CVE-2024-21893
- CVE-2024-22024
- CVE-2023-41719

For more details, see Ivanti forums.

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 Product Downloads.

Virtual Appliance Editions

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

- 9.1R1 release onwards, VA-DTE is not supported.
- From 9.0R1 release, the End-of-Life (EOL) process has begun for the VA-SPE virtual appliance. In its place, Ivanti has launched the new PSA-V series of virtual appliances designed for use in the data center or with cloud services such as Microsoft Azure, Amazon AWS, OpenStack Fabric and Alibaba Cloud.

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

Platform	Qualified System
VMware	• HP ProLiant BL460c G10 with Intel(R) Xeon(R) CPU • ESXi 7.0 Update 2c
OpenStack KVM	• CentOS 7.7 • Linux Server Release 6.4 on an Intel Xeon CPU L5640 @ 2.27GHz • 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)
AWS-V	• T2.Medium (2 Core, 3 NICs and 2 NICs) • T2.Xlarge (4 Core, 3 NICs) • T2.2Xlarge (8 Core, 3 NICs)
Alibaba Cloud	• ecs.g6.2xlarge (8 vCPU, 32GB, 2 NICs)

To download the virtual appliance software, go to: Product Downloads.

VMware Applications

The following table lists the VMware applications qualified:

Platform	Qualified
VMware	
VMware Horizon View Connection Server version 8.6	Rewriter
VMware Horizon Agent version 8.6	VDI Profiles
VMware Horizon View HTML Access version 8.6	VDI Profiles
VMware Horizon View Client version 8.2	VDI Profiles

Upgrade Paths

The following table describes the tested upgrade paths. Please note that here x and y refer to the following:

x: Latest release version:

y: Versions less than x (essentially, x-1 or x-2)

Upgrade From	Qualified	Compatible
9.1Rx	Yes	-
9.1Ry	-	Yes

When upgrading to 9.1Rx releases, ensure to initially upgrade to 9.1R14.6 and then to latest 9.1Rx version.

If your system is running beta or hot-fix version of the software, roll back to your previously installed official software release before you upgrade to 9.1Rx. This practice ensures that the rollback version is a release suitable for production.

General notes

1. For policy reasons security issues are not normally mentioned in release notes. For more information on our security advisories, please see our security advisory page.

2. In 8.2R1.1 and above, all the PCS client access binaries (Network Connect, WSAM, Host Checker, JSAM, Windows Terminal Services, Citrix Terminal Services) are signed with a SHA2 code signing certificate to improve security and ensure compatibility with Microsoft OS's 2016 restrictions on SHA1 code signing. This certificate will expire on April 12, 2021. For details, refer to the KB articles KB14058 and KB43834.

3. Important note: Windows 7 machines must contain a March 10, 2015 Windows 7 Update to be able to accept and verify the SHA2-signed binaries properly. This Windows 7 update is described here and here. If this update is not installed, then Ivanti Connect Secure 8.2R1.1 and later will suffer from reduced functionality (see PRS-337311 underneath). (As a general rule, Ivanti recommends that client machines be kept current with the latest OS updates to maximize security and stability).

4. When custom ciphers are selected, there is a possibility that some of the ciphers are not supported by the web browser. If any ECDH/ECDSA ciphers are selected, they require an ECC certificate to be mapped to the internal/external interface. If a ECC certificate is not installed and mapped to the internal and external ports (if enabled), administrators may not be able to sign in to the appliance. The only way to recover from this situation is to connect to the system console and select option 8 to reset the SSL settings. Option 8 resets the SSL setting to factory default. Any customization is lost and will need to be reconfigured. This is applicable only to Inbound SSL settings.

5. Pre-5.0 Android and pre-9.1 iOS devices don't support Suite B ciphers. If Suite B is enabled, Pulse client on pre-5.0 Android and pre-9.1 iOS devices will not be able to connect to the Ivanti Connect Secure device.

6. The minimum ESAP version supported is 4.3.8 and later.

- 9.1R2 release onwards, Network Connect (NC) client and legacy Windows Secure Application Manager (WSAM) client are not supported.
- From 9.1R1 release onwards, Active Directory Legacy Mode configuration is not supported. If you have an existing Active Directory authentication server using Legacy Mode, first migrate to Standard Mode and then upgrade Ivanti Connect Secure. For the detailed migration procedure, refer KB40430.

Noteworthy Information in 9.1R18.7 Release

- Due to code signing certificate expiry for earlier releases, release 9.1R18.7 is updated with latest code signing certificate.

Noteworthy Information in 9.1R18.2 Release

- Under Troubleshooting–> Monitoring–> Node Monitor, Nodemon logsize displays 1 by default, must be updated as 30 manually.
- The re-organization of the file system on to free up data partition.
- Application Visibility logs are not displayed by default. You can delete the default `id` filters to view the logs. Application visibility logs are per connection based on the application access.

Noteworthy Information in 9.1R18.1 Release

- Resources may not be accessible through Ivanti Secure Access Client on Android when **Enable TOS Bits Copy** is configured for the role under VPN Tunneling Options on the ICS. Disable the option under **Users > User Roles > Role > VPN Tunneling** on ICS UI to access all resources.

Noteworthy Information in 9.1R17 Release

- 9.1R17 release supports latest Ivanti Secure Access Client version 22.2R1. For more info refer to KB45603.

Noteworthy Information in 9.1R16.1 Release

- From 9.1R16.1, default ESAP version is 4.0.5.

Noteworthy Information in 9.1R16 Release

- From 9.1R16, Pulse Secure Client is re-branded as Ivanti Secure Access Client. Complete UX rebranding and the UI upgrade is implemented. There is also an option to switch between the Classic UI and New-UI to maintain user experience. The Pulse Secure client icon is replaced by Ivanti Secure Access Client icon  . For more information refer KB45301.
- Number of Multicast groups an end-user can join is increased to 30 groups.
- Increase number of ports allowed on a resource from 15 to 32.
- Resource Profile filter supports IPv6 addresses.
- Increased number of Split tunneling networks from 512 to 1024.

- Host Checker logs enhanced to include session IDs.
- FQDN ACLs allows to include ports.

Noteworthy Information in 9.1R15 Release

- **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.**
  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.
  If the upgrade is performed using REST APIs or management servers like Pulse One, check serial console for the list of deprecated feature configurations.
- This release supports adding gateways with ISA hardware platforms as license clients and can lease licenses from 9.1R15 license server.

Noteworthy Information in 9.1R14 Release

- Re-branding of the Pulse Secure logo, copyright, and some references to reflect that the Ivanti branding is in progress. The re-branding activity to Ivanti will be continued through next release. Pulse Connect Secure (PCS) is referred to as Ivanti Connect Secure (Ivanti Connect Secure) and Pulse Policy Secure (PPS) is referred to as Ivanti Policy Secure (Ivanti Policy Secure).
- A few features are targeted for deprecation from release 9.1R14. 9.1R14 update does not support new configurations for these features, however it supports modification to the existing configuration. On upgrade, there are no changes to the existing configurations. These features will be permanently deprecated in the next releases. Refer to KB44747 and KB44913 for a detailed list of the deprecated features.
- The default periodic host checking interval is set to 60 minutes. Setting aggressive intervals may result in performance issues.
- A single user name / certificate used by a large number of users might overload the session database and lead to connection drops. New users may be unable to establish connections.
- Trusted server CA certificate names are changed due to expiry and renewal of the certificates. Following certificate names are changed:
  - Cybertrust Global Root is Baltimore CyberTrust Root
  - GlobalSign-2 is GlobalSign

- Refer KB44877 and follow the mandatory steps before staging or upgrading an appliance.
- Split tunneling entries increased from 255 to 512.

Noteworthy Information in 9.1R13.1 Release

From 9.1R13.1, ISA virtual platforms can be configured as license clients. For more information, refer to the *License Management Guide*.

Noteworthy Information in 9.1R13 Release

- At role level, based on the admin selection of solution type, end users can create HTML5 bookmarks.
- Logs are enhanced to include client certificate information.
- Refer to KB44408 for the recommendations / best practices to deploy Virtual Appliance and the logs needed for analysis/troubleshooting.
- An option to configure the PSAL time-out under System Maintenance à Options.
- A warning message regarding the session disconnection displays when the localization settings are changed.
- Logs are enhanced to provide more ICT related information.

Noteworthy Information in 9.1R12 Release

- SNMP monitoring enhancement to map index numbers of the interfaces across ifTable and ipAddrTable.
- The grace period for expired licenses is now reduced from 91 days to 31 days.
- Logs are refined and enhanced. They now include session information such as the Session ID, Session start data and end data.
- Enhancements to dsagentd done to address session resumption issues.
- Source IP restrictions can now be disabled for admin realms from the serial console menu through an option we have provided newly.

Noteworthy Information in 9.1R11.5 Release

- Added an option for the Admin to enable users to download the Pulse Client Components removal (Pulse Upgrade Helper) tool on Windows End User machines upon Browser access. This option helps to remediate the certificate expiry issue. For more information, refer KB44781 and KB44810.
- This release provides important security hardening. For more information refer to SA44800.
- Source IP restriction (RFC1918) is removed on Admin Realms for fresh deployments on OpenStack KVM platform. Default source IP restrictions are applicable for PSA appliances, VMWare, and Hyper-V platforms.
- An option is available on adminUI to force the users to re-authenticate on IDP inspite of the active user session.

Noteworthy Information in 9.1R11.4 Release

- This release provides important security hardening. For more information refer to SA44784.

Noteworthy Information in 9.1R11 Release

- The HTTP only DSDID session cookies were introduced from Release 9.0R3. From release 9.1R11 onwards, the DSDID cookies are enabled by default for all new roles created. On upgrade, if DSDID is not enabled for any of the roles, a warning message displays on the dashboard. A link displays on the UI, administrator can click to enable DSDID cookies option for all the roles.
- Major browsers disable TLS1.0 and TLS1.1 by default. Administrators are recommended to use TLS1.2 and later and also select Maximize Security option under **Configuration > Security> SSL options** for inbound and outbound connections. If not selected, a warning message displays. From 9.1R11 onwards, for new ESP VPN Tunneling Connection Profiles, AES256/SHA256 (maximize security) encryption is chosen by default.
- User logs and Administrator logs are refined and enhanced to display more information.
- A source IP restriction is added on Admin Realms so that admins can connect with only private addresses (RFC1918) on fresh deployments or when the configurations are cleared. This restriction is applicable to PSA appliances, VMWare, Hyper-V, and OpenStack KVM.
- From 9.1R11, SHA1 hashing algorithm is removed from the “Maximize Security (High Ciphers)” settings

Noteworthy Information in 9.1R10 Release

- Added stability improvements for L4 JSAM connections.
- Added following licensing reporting enhancements on MSSP deployments:
    - When the license client has concurrent users license installed locally, the client excludes the local installed count while sending lease usage to the license server.
    - When the license client has ICE license enabled or has an evaluation license installed which gives maximum platform limit for concurrent users, the license lease usage reported by client is zero.
    - The license client allows 10% extra usage over the licensed limit. This applies for maximum lease limit as well. In such case, the license client reports only the maximum lease limit usage. For example, if license client has leased 100 licenses and 110 users are logged in, license client reports only 100 as usage to the license server.
- Host header validation is introduced in 9.1R10. When this option is enabled on the server under **System** > **Configuratin** > **Security** > **Miscellaneous**, the Pulse Client upgrade through Ivanti Connect Secure may fail. For more information, refer to KB44646.
- Added graphs to display advanced HTML5 connections under System Status dashboard. Refer to "Displaying System Status" in *Ivanti Connect Secure Administration Guide*.

Noteworthy Information in 9.1R8 Release

For 9.1R8, Pulse Collaboration Client is packaged using Ivanti Connect Secure 9.1R7 build.

Noteworthy Information in 9.1R4.3 Release

- In 9.1Rx OVF a critical issue was observed. The 9.1R4.3 release addresses this issue.
- On some of the installations, it was observed that a few read-only files were being overwritten. Customers are experiencing HTTP 500 response for some of the admin requests. The 9.1R4.3 release addresses this issue.
- Upgrade works only if VA is deployed with 8.3 OVF onwards. If VA is deployed with pre 8.3 OVF, upgrade to this image will not work.
- Refer to KB44408 **for the recommendations / best practices to deploy Virtual Appliance and the logs needed for analysis/troubleshooting**.

New Features

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

Feature	Description
Release 9.1R18.7 Features	
No new features introduced in this release.	
Release 9.1R18.6 Features	
No new features introduced in this release.	
Release 9.1R18.5 Features	
No new features introduced in this release.	
Release 9.1R18.4 Features	
No new features introduced in this release.	
Release 9.1R18.2 Features	
No new features introduced in this release.	
Release 9.1R18.1 Features	
No new features introduced in this release.	
Release 9.1R18 Features	
No new features introduced in this release.	
Release 9.1R17.1 Features	
No new features introduced in this release.	
Release 9.1R17 Features	
AES 256 e-type encryption support	This feature allows the administrators to enable AES 256 encryption type. This feature is applicable only for Active Directory Authentication Server using Kerberos Authentication protocol.
FQDN IP entries in ACL	This feature allows to retain FQDN IP entries for lifetime of the FQDN IP in an ACL. **Note**: This feature works with Ivanti Secure Access Client 22.3R1 and later.

Feature	Description
Allow Host checker policy on certificate expiry	This feature allows the administrators to pass host checker policies on endpoints after the user certificate expiry. 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.
Release 9.1R16.1 Features	
No new features applicable to this release.	
Release 9.1R16 Features	
Microsoft 365 support through re-writer	Ivanti Connect Secure supports Microsoft Office 365 through re-writer.
PSAL browser extension	An option for administrator to enable browser extension for the end-users. For installation instructions refer to *Pulse Secure Application Launcher Deployment Guide* under Ivanti Secure Access Client Documents.
Ivanti Neurons for MDM (formerly MobileIron Cloud)	Ivanti Connect Secure now supports Ivanti Neurons for MDM (formerly MobileIron Cloud).
Release 9.1R15 Features	
End user bookmark creation	This feature allows the users to create SSH/Telnet/VNC HTML5 bookmarks to initiate which SSH/Telnet/VNC connections. This feature also allows admins to select the bookmark types that users can create.
Admin controlled session recording	This feature allows admins to control and store the session recordings, for end user and admin created bookmarks, to internal or external storage on Advanced HTML5 sessions.
Intune integration enhancement	This feature allows to check compliance of an end user and retrieval of Device attributes using the Device ID. Support Intune Government cloud is available in Preview only mode for this release.

Feature	Description
DHCP options enhancement	This feature allows ICS to act as a relay agent and communicate to the DHCP server the subnet/link to allocate an IP address. This feature allows Admins to configure any sub-option (1-255) for DHCP option including DHCP option 82, sub-option 5.
OAuth/OpenId Connect Enhancements	This feature enhancement includes: • using an URL to fetch OAuth metadata • force authentication • traffic segregation for OAuth server
Accessibility Conformance report	Accessibility conformance report helps to check the level of accessibility compliance of the product.
Release 9.1R14 Features	
oAuth/openID support for authentication	Ivanti Connect Secure supports OAuth as an Auth Server which can be added and configured for End User authentication. OAuth is an open-standard authorization protocol or framework that describes how unrelated servers and services can safely allow authenticated access to their assets without sharing the initial, related, single logon credential. OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. This feature allows users to authenticate with any standard OpenID Provider like Google, OKTA, Azure AD, to connect to Ivanti Connect Secure.
REST API enhancements	The new REST API methods allows the admin to configure and manage the Ivanti Connect Secure seamlessly. Supports new REST API functions for Upgrade, Reboot, Rollback, Read-Only Admin, Console password protection, Monitor NTP status, Map interfaces to certificates, Toggle Fault Tolerance and Telemetry Settings.
SAML enhancements	A new option introduced in SAML Auth Server config, where admin can override default FQDN and provide custom FQDN to talk to SAML providers and end user authentications.

Feature	Description
Advanced HTML5 enhancements	For RDP bookmarks, fetch domain feature supports automatic detection of domain for AD servers. This feature supports AD servers only. License count is changed from session basis to user login basis.
Admin Authentication fallback URL	Introduced an option to provide a fallback URL in case the Auth server is not reachable while admin tries to login.
Geo-Location to the realm restrictions	This feature provides an option to restrict or allow logins based on location. **Note**: Ensure UEBA package is uploaded on the ICS for this feature to work.
Kerberos e-type extension	This feature allows Kerberos to use AES128 as the highest encryption type.
Audio Support on Citrix desktops	Audio support for Citrix desktops that are hosted on a Citrix server using an admin created VDI bookmark.
Release 9.1R13.1 Features	
ISA virtual platforms as license clients	ISA virtual platforms can be configured as license clients from 9.1R13.1. For more information, refer to the *License Management Guide*.
Release 9.1R13 Features	
AWS marketplace publishing	AWS marketplace publishing with GP3 AMI image to reduce the Ivanti Connect Secure upgrade time on AWS.
Release 9.1R12.1 Features	
No new features applicable to this release.	
Release 9.1R12 Features	
Integrity Checker	The integrity tool allows an administrator to verify the Ivanti Connect Secure package installed on Virtual or Hardware Appliances This tool checks the integrity of the complete file system and finds any additional/modified files in the system.
Intune integration enhancements	This feature enhancement allows Windows users to fetch attributes from Intune by using MAC address option.

Feature	Description
Advanced HTML5 Enhancements	The feature enhancement allows users to create admin/end-user Advanced HTML5 bookmarks.
SeamlessMigration of Ivanti Connect Secure instance in AWS.	This feature allows to modify internal port and external port of Ivanti Connect Secure deployed in AWS.
Choice of interface for each configured syslog server	This feature enhancement allows to add Source interface selection for each syslog servers configured in the Ivanti Connect Secure. It enables the admin to select a source interface with which address packets are sent to the syslog server.
REST API Enhancements for Named Users	This feature enables the admin to access the named users and its information and delete them on both Ivanti Connect Secure and License Server in Named User Repository mode using REST APIs.
Release 9.1R11.5 Features	
No new features applicable for this release.	
Release 9.1R11.4 Features	
No new features applicable for this release.	
Release 9.1R11.3 Features	
No new features applicable for this release.	
Release 9.1R11 Features	
Advanced HTML5 solution (General Availability version)	Ivanti Connect Secure supports Advanced HTML5 Access solution. This Advanced HTML5 Access solution supports two Advanced HTML5 sessions by default and includes multiple monitors, session recording, audio recording, high sound quality, and camera support. From 9.1.R11, Advanced HTML5 access is available as General Availability version.
Release 9.1R10 Features	
No new features applicable for this release. Refer to Noteworthy Information in 9.1R10 Release for more details.	
Release 9.1R9.1 Features	

Feature	Description
No new features applicable for this release.	
Release 9.1R9 Features	
SNMP v3 multiple user support	Ivanti Connect Secure supports two users to be registered with an SNMP engine with different authentication and privilege settings.
ESP Tunnel for Mixed Mode	Ivanti Connect Secure provides option to use ESP tunnel for 6in4 and 4in6 traffic.
Advanced HTML5 solution (Trial version)	Ivanti Connect Secure supports Advanced HTML5 Access solution. This Advanced HTML5 Access solution supports two Advanced HTML5 sessions by default and includes multiple monitors, session recording, audio recording, high sound quality, and camera support.
Remote microphone support in WTS	Supports microphones connected to the client computer during the remote session.
Release 9.1R8.2 Features	
No new features added in this release.	
Release 9.1R8.1 Features	
No new features added in this release.	
Release 9.1R8 Features	
UEBA package for fresh installation of Ivanti Connect Secure/Ivanti Policy Secure	In case you have a fresh installation of Ivanti Connect Secure/Ivanti Policy Secure, you may download latest UEBA package from Support Site and add the package at Behavior Analysis page before using Adaptive Authentication or Geolocation based Conditional Access.
Show users by access type	Apart from showing the number of concurrent user sessions, Ivanti Connect Secure Dashboard now shows the L4 access type (PSAM) and Clientless access type (Browser) logins as non-tunnel users.
Ivanti Connect Secure Protection from Overload	This feature disallows user login, user login via Pulse Desktop, HTML5 connection or connection to a web resource when the CPU load is above a certain threshold. By default, this option is disabled for Ivanti Connect Secure upgrades and enabled for new installation.

Feature	Description
Reset/Unlock TOTP user through REST API	This release provides REST API to Reset/Unlock a user under a TOTP server.
New license SKUs for Ivanti Connect Secure/Ivanti Policy Secure	In this release, added around 120 new license SKUs for Ivanti Connect Secure/Ivanti Policy Secure.
Support for pool of NTP servers and NTP status check	Ivanti Connect Secure now supports pool of NTP servers up to 4 NTP servers to sync date and time.
Release 9.1R7 Features	
Automatic enable/disable ICE license	This release provides automatic management of ICE license. Ivanti Connect Secure enables ICE license when the logged in users count crosses the maximum licensed users count and disables ICE license when the logged in users count drops below the maximum licensed users count. As an example, If you installed 100 licensed user counts, when the 101th user logs in, ICE license gets automatically enabled.
Show current HTML5 RDP sessions in Dashboard	This release provides HTML5 sessions information in the dashboard and the trend graph that helps admin to view the CPU usage and take necessary action to provide better remote access experience for the users.
Support for srcset attribute in HTML	Ivanti Connect Secure provides support for the responsive images (in web applications) via rewriter by rewriting the srcset attribute value. The corresponding images would be fetched on client application based on screen size, resolutions and other features.
Enable/Disable FQDN ACL	FQDN ACL feature was enabled by default earlier even though there are no policies configured. A new admin configurable option to enable or disable FQDN ACL feature is added in 9.1R7 at System > Configuration > VPN tunneling.
Release 9.1R6 Features	

Feature	Description
Hyperlink to Host Checker Policies	In the User Realms > Authentication Policy > Host Checker page, the policy names now have hyperlinks. Click the link to view the policy configuration.
Hardware ID in the System Maintenance page	The System > Maintenance > Platform page displays Hardware ID along with the other platform details.
Serial number in the Licensing screen	The System > Configuration > Licensing page, displays Hardware Id and Serial number.
Enable/Disable option for ICE license	This release provides REST API to do the following on a Standalone/Cluster: • enable/disable ICE license • get the current status of ICE license.
Release 9.1R5 Features	
Terraform template support for AWS and Azure	Ivanti Connect Secure can be deployed using Terraform templates on supported hypervisors and cloud platforms.
Location based Conditional Access	Conditional Access feature for Cloud Secure now provides a mechanism to enforce access control policies based on location parameters by defining policies for applications.
Password management for Open LDAP	LDAP based password management works with generic LDAP servers such as OpenLDAP.
Microsoft Intune MDM integration	In this release, device access management framework supports integration with Microsoft Intune.
HTML5 Sessions report	Active number of HTML5 sessions on Ivanti Connect Secure can be obtained using a REST API call to api/v1/stats/active-html5-sessions.
MSSP Reporting enhancements	It is now possible to extract any particular license client/cluster report through REST API. Enhancements include: • Cluster-wise view in the license report.

Feature	Description
	• License report in JSON format through REST. • Options to get cluster/client/period sub-section of the granular report through REST.
SSLDump for VLAN	In this release, SSLDump utility supports VLAN. Admins can use this tool for debugging / data collection purpose.
Edit default gateway configuration	In Ivanti Connect Secure hosted on a cloud environment, it is now possible to edit default gateway configuration from UI.
Host Checker feature enhancement	Host Checker policy to detect and allow hard disk in which encryption is in progress.
License server with Active-Active cluster	Administrators can: • create license server with Active Active cluster on virtual/cloud and hardware platforms. • lease all different type of licenses to license clients from any node of active-active cluster. • surrender/recall licenses from any node of active-active cluster.
Release 9.1R4.3 Features	
No new features added for this release	
Release 9.1R4.2 Features	
No new features added for this release	
Release 9.1R4.1 Features	
No new features added for this release	
Release 9.1R4 Features	
Ivanti Connect Secure VA on Alibaba Cloud	Ivanti Connect Secure now supports VA deployment on Alibaba Cloud.

Feature	Description
Conditional Access	Conditional Access feature for Cloud Secure provides a mechanism to enforce access control policies based on user and device parameters by defining policies for applications. Conditional Access policies are evaluated during application access time while roles are mapped to the session during the session creation time.
REST API enhancements	Enhancements include: • Update to "Getting Active Sessions" • Update to "Getting System Information" • Added "Fetching the User Login Statistics" • Added "Health Check Status" • Added "VIP Failover" • Added "Applying License" • Added "Deleting License" • Added "Getting License Clients" • Added "Getting License Report from License Server" • Added Profiler REST APIs
vTM and Ivanti Connect Secure Integration for Load Balancing	The Platform Limit, Maximum Licensed User Count and Cluster Name attribute values are available for optimal load balancing.
Support for Windows Redstone 6	In 9.1R4 release, Windows Redstone 6 - version 1909 is qualified.
Support for SharePoint 2019	In 9.1R4 release, SharePoint 2019 is qualified.
Support for VMware VDI 7.9, and 7.10	In 9.1R4 release, VMware VDI versions 7.9 and 7.10 are qualified.

Feature	Description
Support for Citrix Virtual Apps and Desktops 7 1909	In 9.1R4 release, Citrix Virtual Apps and Desktops 7 1909 is qualified.
Protect passwords stored in local auth server using stronger hash	When a new local authentication server is created, now admin has a choice to store the password with strong hashing using pbkdf2.
Support license reporting per license client	Licensing report is enhanced with usage statistics for each Ivanti Connect Secure instance - maximum user count per month per Ivanti Connect Secure/per MSSP. MSSPs can now: • generate accurate usage reports of their customers. • make the structured report in XML format to enable for parsing and usage for dashboard.
Release 9.1R3 Features	
Consolidated system and troubleshooting logs	The various system logs and troubleshooting logs that help in investigating user access issues and system issues can be configured and accessed using the Log Selection page.
Connect to nearest available DC	The LDAP authentication configuration is enhanced in 9.1R3 to locate the nearest Microsoft domain controllers, which are spread across the globe, by resolving DNS SRV records.
Zero touch provisioning	From 9.1R3 release, Ivanti Connect Secure can detect and assign DHCP networking settings automatically at the Ivanti Connect Secure VM boot up. In the script included in the PSA-V package, the Ivanti Connect Secure parameters should be set to null in order to fetch the networking configuration automatically from the DHCP server. This feature is not supported on PSA hardware.
Ivanti Connect Secure hosted in OpenStack cloud	OpenStack is an open source cloud computing platform that allows deploying and managing a cloud infrastructure as an IaaS service. As part of this release, Ivanti Connect Secure supports deploying Ivanti Connect Secure KVM in OpenStack cloud.

Feature	Description
VMware tools support	From 9.1R3 release, VMware support is qualified for VMware 10.3.10, ESXi 6.7 Update 2c.
Debug Log storage expansion	From 9.1R3 release, the maximum debug log size is increased to 1024 MB on hardware platforms.
Periodic iostat data collection	From 9.1R3 release, the "iostat" information is gathered periodically and made available as part of node monitoring in system snapshot.
Control copy/paste option for a user from an HTML5 session	9.1R3 release provides option to the administrators as well as end-user to enable/disable copy/paste from HTML5 RDP sessions. This option will be available under User Roles as well as Admin Created Bookmarks".
Enhancements to Local Authentication Server default password	From 9.1R3 release, for a fresh installation, the valid password range defined is 0-999. Minimum length 10 and maximum length 128 are set as default values.
Restricting access to default resource policies	From 9.1R3 release, for a fresh installation, the following predefined resource policies are set to "Deny" state by default. • Web Access Resource Policy "Initial Policy for Local Resources" • Windows File Access Resource Policy "Initial File Browsing Policy" The predefined policy for VPN Tunneling is not provided.
IKEv2 Fragmentation	IKEv2 packets can be larger than the MTU especially the IKE_AUTH packets which include the certificate chain. These larger IKE packets get fragmented in the intermediate devices. This feature implements fragmentation at IKE level and avoids IP fragmentation.

Feature	Description
MSS value for TCP connections on Tun devices	Due to larger IPv6 header as compared to IPv4, if the MSS of the Ivanti Connect Secure external interface is not set appropriately, the packets would be dropped on the external interface. This feature enables to set MSS to a lower value so that TCP connections are not dropped for 6-in-4 cases or when there is NAT translation somewhere in the network before reaching Ivanti Connect Secure.
Release 9.1R2 Features	
SP-Initiated SAML SSO	Ivanti Connect Secure supports SP-initiated SAML SSO when Ivanti Connect Secure is configured as IdP in gateway mode. Ivanti Connect Secure uses the existing user session in generating SAML assertion for the user for SSO.
IDP initiated SAML Single Logout	This feature provides a single logout functionality wherein if a user gets logged out of a session from one application, Ivanti Connect Secure (configured as IdP) notifies all other connected applications of that user with Single Logout.
Flag Duplicate Machine ID in access logs	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. 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.*
Microsoft RDWeb HTML5 Access	The newly introduced Microsoft RDWeb resource profile controls access to the published desktops and applications based on HTML5. The Microsoft RDWeb templates significantly reduce the configuration time by consolidating configuration settings into one place and by pre-populating a variety of resource policy settings. In the 9.1R2 release, Microsoft RDWeb HTML5 access does not support Single Sign On. SSO will be made available in the future release.

Feature	Description
Backup configs and archived logs on AWS S3/Azure Storage	Two new methods of archiving the configurations and archived logs are available now apart from SCP and FTP methods: Ivanti Connect Secure now 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.
V3 to V4 OPSWAT SDK migration	Ivanti Connect Secure supports the migration of servers and clients to OPSWAT v4 to take advantage of latest updates.
Report Max Used Licenses to HLS|VLS	From 9.1R2 release, the licensing client (Ivanti Connect Secure) starts reporting 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.
VA Partition Expansion	Ivanti Connect Secure/Ivanti Policy Secure supports upgrading from 8.2Rx to 9.1R2 for the following supported platforms: • VMware ESXi • OpenStack KVM • Hyper-V When upgrading a VA-SPE running 8.2R5.1 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, OpenStack KVM and Hyper-V. Refer KB41049 for more details.
Release 9.1R1 Features	
Software Defined Perimeter	SDP uses ICS appliances which individually act as either an SDP controller or an SDP gateway. Mobile users of the Pulse Client perform authentication on an SDP controller which runs an Authentication, Authorization and Accounting (AAA) Service. The SDP controller then enables direct communication between the user and the SDP gateways that protect the user's authorized resources and enables requested encryption.

Feature	Description
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.
Authentication failure management	Account Lockout option is provided to manage user authentication failures for admin users of local authentication server. The admin user account will be locked after specified number of consecutive wrong password attempts. The account will be unlocked after the specified lockout period or by using the Unlock option.
Support for “client-name” parameter in HTML5 Access	User can pass "client-name" in HTML5 rdp using launcher method. The %clientname% variable is matched with a workstation ID and normally that variable is unique and dedicated remote desktop computer name.
Deploying PSA-V in OpenStack KVM	User can deploy PSA-V in OpenStack KVM using a template.
User access to internet resources on an Azure-based or AWS-based Ivanti Connect Secure	AWS VPC GW and Azure VNet GW drop packets if the source IP is the endpoint tunnel IP. This feature NATs endpoint tunnel IP to Internal interface IP. The NAT allows user to access internet resources when connected to a VPN tunnel on an Azure or AWS-based Ivanti Connect Secure.
REST API enhancements	Enhancements include: Getting Config without Pulse packages such as ESAP package and Pulse Client package Backing up and restoring binary configuration

Fixed Issues

The following table lists release numbers and the PRS numbers with the summary of the issue fixed during that release:

Problem Report Number	Summary
Release 9.1R18.7 PRs	
1353427	IPTable rules default policy set to "ACCEPT" allowing all ports.
1353913	100% CPU observed post upgrade to 9.1R18.6.
1302272	Session ID is not displayed in the "Closed connection" logs consistently.
1350553	staging user summary table entries are being appended
1355655	JSAM Certificate is expired in 9.1R18.6/22.7R2
1355856	OlderPCSLogs (event /admin/user access), before the upgrade to 9.1 R18/R18.1 shows question mark Character(?) in the incomplete logs entries after upgrade to these versions.
1356547	Two adminintartors accessing the ICS GUI at same time (not reccomended), will not be able to use user access logs filter's simultaneously.
1302246	User access logs provides 127.0.0.1 address for source IP when an attempt with wrong credentials fails.
Release 9.1R18.6 PRs	
PRS-419817	Geolocation based realm restriction fails for user login.
PRS-419357	Display of state storage warning message.
PRS-419344	Upgrade from 9.1R18.3 to 9.1R18.4 (Patch Upgrade for Security) fails with error message "The service package you uploaded is not valid".
PRS-419198	Automatic detection with "unknown Keyboard" as keyboard layout doesn't work in Advance HTML5 pre-Login.
PRS-419162	Wildcard Device certificate deletion with REST API is not working Properly.

Problem Report Number	Summary
PRS-418924	Vietnam users are failing realm restrictions when using “Allow or deny users from the following Location” in User Realms > Users > Authentication Policy.
PRS-418700	Sessions are dropped when device failed over occurs.
PRS-418576	User access logs shows wrong Username, when ending a Terminal Session.
PRS-418305	EXT port to Virtual port certificate mapping Issue is observed on 9.1R17.1.
PRS-418222	Login syntax change impacts syslog agents after device upgrade.
PRS-418219	MDM setup issues is observed on Microsoft Intune for authentication and authorization.
PRS-418161	SNMP Traps are not getting generated when one of the redundant power supplies is turned off in PSA-7000c.
PRS-418134	Display full SID information in user access log for end user login.
PRS-418027	iveMaxConcurrentUsersSignedIn SNMP alert observed for Leased licenses from License Server.
PRS-418021	UEBA option is missing in Pulse one admin UI and UEBA reports does not come to Pulse One.
PRS-417963	Multiple users not able to connect to the VPN due to IP allocation failure.
PRS-417819	CRL cert next update shows incorrect info.
PRS-417750	Port agility issues observed as iOS 17 has introduced a change in the IKE code, to make it stricter in compliance with RFC-7296.
PRS-417319	CPU usage at 100 % for 9.1R18 PCS version due to 64K size DNS response.
PRS-417302	Database percentage goes to 99, shard 3 operation above threshold is seen with IPS - 9.1R17.1.
PRS-417300	Ikev2 error messages seen in the User Access logs.

Problem Report Number	Summary
PRS-417152	Upgrade to 9.1 R18.1 fails due to SSH/Telnet deprecation check.
PRS-417140	Failing to GET Intune MDM Attribute Intermittently
PRS-416861	“Dropping the duplicate tunnel session from client” is seen in User Access Logs more frequently post upgrading to 9.1R18.
PRS-405381	White screen is seen for Telnet session even when the copy/paste option is disabled.
Release 9.1R18.5 PRs	
No New fixed issues in this release.	
Release 9.1R18.4 PRs	
No New fixed issues in this release.	
Release 9.1R18.2 PRs	
PRS-417325	Watchdog process displays critical error about exceeded number of file descriptors in event logs.
PRS-417128	Unable to fetch device username attribute from Airwatch.
PRS-416930	Unstable cluster on upgrade due to Watchdog process and Web process crash.
PRS-416920	Difference in configuration when same bookmark is exported and imported back to appliance.
PRS-416902	VPN session end accounting message contains incorrect data.
PRS-416890	Source IP restriction for "Korea, Republic of" is failing.
PRS-416805	Effective count shows 1100 licenses, when the reserved count/leased count from server to client is fetched as 1200 licenses.
PRS-416764	Forwarded IP displays in the primary authentication success log and does not display in the authentication failure log.
PRS-416742	"User Access log is full" log message displays on upgrading to 9.1R18.

Problem Report Number	Summary
PRS-416708	Within seconds of logging into the New UI as a delegated admin, the navigation options disappear.
PRS-416627	DHCP FQDN is getting truncated in ICS DNS query.
PRS-416573	Role mapping configured for Geo location-based customer filter expression fails and cause authentication failure.
PRS-416429	User Record Synchronization is not working correctly, displays duplicates or few HTML5 session details are not displayed.
PRS-416392	ICS device shows one Hour time ahead of the normal time when time zone (GMT+11) Magadan Solomon New Caledonia is selected.
PRS-416354	End user is not able to use custom port number when adding a terminal services bookmark.
PRS-416313	Advance HTML5 RDP Access: White Space and resolution issues observed.
PRS-416238	Additional blank character (space) is added in username when using SAML username template.
PRS-416118	HC with certificate check fails using CRL that is expired after upgrading the devices to 9.1R17.1.
PRS-416085	On upgrading to the 9.1R18, displays wrong time on Windows machine when connecting using Advanced HTML5 RDP bookmarks.
PRS-415982	Advanced HTML5 RDP resource is accessible by the same user under different role with RDP disabled.
PRS-415928	ICS can delete the Trusted Client CA which is mapped to the Hostchecker policy.
PRS-415784	LMDB is getting corrupted due to web crash and memory leak.
PRS-415731	Citrix Workspace application does not work after version 21.9.1.
PZT-41472	Config sync template status not progressing and shows as Pending.
PZT-41791	Frequent restarts of Fluent-Bit services.
Release 9.1R18.1 PRs	

Problem Report Number	Summary
PRS-414906	The VPN tunnel disconnects and shows the error as “Server busy”.
PRS-415013	Web profile access using the Launch JSAM option fails.
PRS-415043	The critical event logs as Program hprewrite-server fails.
PRS-415082	ICE license does not deactivate automatically when the number of users goes below licensed user count. Issue only occurs when there is no subscription/consec license installed.
PRS-415248	On Terminal Service, NLA checkbox is not enabled by default while duplicating resource profile.
PRS-415647	Update the note "Note: Please do not disable this option as it helps to debug system issues. This option does not affect system performance." Under Troubleshooting -> Monitoring -> Node Monitor.
PRS-415802	Change the Pulse Embedded KB links to equivalent Ivanti Links.
PRS-416052	Inconsistencies in Japanese Language while using Host Checker.
PRS-415885	Built-in Integrity check scanner tool does not accept 0 in hour field for scheduled scan on ICS.
PRS-416241	ICS crashes sometimes when using ipv6.
Release 9.1R18 PRs	
PRS-414659	RADIUS accounting User-Name is blank after upgrading to 9.1R17.
PRS-414456	Input validation check on the IP Destination Field in ACL check failing causing VPN disruption.
PRS-414418	Image uploaded in the default sign in page does not show up in the new GUI after upgrading the server to 9.1R17.
PRS-414409	REST API allows two certificates to be mapped with the same port.
PRS-414406	REST API Delete causes device to not respond in 9.1R17.
PRS-414310	Wong username and ip address are seen in the logs (unauthenticated requests and Invalid URL log) because auth context was not set correctly.

Problem Report Number	Summary
PRS-414292	Source IP based on Geo-Location Czechia is not working.
PRS-414283	Client users failing LDAP based authorization first attempt but works in next attempt.
PRS-414259	Unable to allocate IP address to the users from static pool due to failure in setting up ACLs for the tunnel.
PRS-414222	Upgrade fails while checking the AD legacy Authentication Check.
PRS-414063	Program fqdnacl fails on 9.1R15.
PRS-414054	User Records increments constantly after upgrading to 9.1R15
PRS-413998	Users are redirected to dana/meeting/meeting_weekly.cgi post logging in to the VPN.
PRS-413953	ICS is not showing the assigned IP addresses when using Infoblox as DHCP server in the active users tab and concurrent user session graph. UI issue only.
PRS-413953	ICS is not showing the assigned IP addresses when using Infoblox as DHCP server in the active users tab and concurrent user session graph. UI issue only
PRS-413919	dsagentd and rewrite-server processes crashes very often.
PRS-413891	The client does not display the custom messages for failures when using TOTP RADIUS server.
PRS-413842	SNMP polling is not working for Node 100 after upgrading to 9.1r15 version in Active/ Active cluster with Zabbix SNMP manager
PRS-413821	Duplicated and pushed configuration with lockdown exceptions assigned to a role does not update the exceptions
PRS-413793	On registering Ivanti Policy Secure devices to the Pulse One device, IPS displays a "Publish Failed" message and crashes.
PRS-413761	Mouse-related issues like scroll and click when using Advanced HTML5.
PRS-413696	Warning message found in Edge browser in IE mode with 9.1R16.

Problem Report Number	Summary
PRS-413678	Duplicating connection sets with lockdown exceptions enabled will not enable the exceptions on the configuration file without saving changes on the new connection set.
PRS-413490	When a higher resolution (width and height) is used, the End-user RDP webpage will have a scroll bar and icons are appear bigger.
PRS-413161	Advance HTML5: Post Upgrade to 9.1R16 SSO credentials are not working
PRS-413133	IKE tunnel disconnects in the case of IKE fragmentation and large data transfer.
PRS-412236	Create blacklist option as admin UI to blacklist specific user agent strings to avoid bot requests
PRS-412190	Upgrade to 9.1R16 from 9.1R14.1 fails due to "Archiving Sensor Logs" but it is disabled
PRS-411462	SAML-Server process crashes on 9.1R14.1 due to memory leaks.
PRS-410122	PowerBi Application is loading blank via rewriter.
Release 9.1R17.1 PRs	
PRS-415013	Web profile access using the Launch JSAM option fails in versions 9.1R16 and 9.1R17.
PRS-414662	Users unable to add HTML5 sessions due to field missing from the UI.
PRS-413761	Mouse-related issues seen with scroll and click when using Advanced HTML5.
PRS-413490	Higher resolution in Advance html5 is scaled down and can be viewed without a scrollbar.
Release 9.1R17 PRs	
PRS-413406	Jira application is not working through rewriter after upgrade 9.1R15 to 9.1R16.1
PRS-413734	The sign-in URLs are reordered on ICS upgrade.

Problem Report Number	Summary
PRS-413543	VPN tunneling drops immediately when connected using DHCP scope.
PRS-413367	HTTP Only flag is not set via PTP virtual hostname.
PRS-413102	Breaks seen in the graphs.
PRS-413093	While importing xml file for include-system-config false value is not getting updated.
PRS-413072	Program rewrite-server recently failed.
PRS-412899	REST API based certificate import and mapping to ports failed with PSA 7000 fiber in customer environment.
PRS-412890	Web hits on graph showing constantly at 500M on PSA-7000C.
PRS-412793	PSA7000c unresponsive in Active-Passive cluster with warm restart on 9.1R16.
PRS-412751	PSA3000-V VMware keeps crashing on upgrade to 9.1 R16.
PRS-412651	When multiple users are created through Auth Servers > System Local > Users, usernames are incorrect in User Access logs.
PRS-412335	RDP access over Citrix Storefront through rewriter is not loading the desktop screen.
PRS-412323	Authorization-Only Access not working in 9.1R16.
PRS-412308	Unable to allocate VPN tunnelling IP from static pool.
PRS-412190	"Archiving Sensor Logs" error appears during upgrade, even though the option is disabled and upgrade to 9.1R16 fails.
PRS-412115	Unexpected policies deleted after removing user roles.
PRS-412081	Not able to launch JSAM and Ivanti Secure Access client.
PRS-411521	Slow IPv6 access.
PRS-411357	Multiple DHCP lease request is Initiated by client for same user.

Problem Report Number	Summary
PRS-411134	User logging in from a location that contains special characters in the name of city or country will be prompted for secondary authentication repeatedly.
PRS-411002	Some ports appear to open unexpectedly.
PRS-410965	User configuration Archive fails creating a temp file and taking up disk space under/var/tmp, also causes SNMP alerts.
PRS-410900	NMAP output shows port-5432(UEBA port) as open and not filtered.
PRS-410897	Unable to login to the ICS after changing the Local user/Admin password via REST API
PRS-410519	Upgrade failure to 9.1R15 due to legacy active directory mode configuration
PRS-410212	Import, Cancel, etc. buttons are not displaying due to syntax error.
PRS-410138	After the upgrading to 9.1R14.1, sporadically users are getting redirected with error https://auth/welcome.cgi.
PRS-409932	Citrix JICA/CTS to Storefront 3.1/CTS improvement for admin profile flow.
PRS-409891	Memory Leak on web process leading to process crash and disconnects users.
PRS-409668	"Program cgi-server recently failed." critical log seen frequently.
PRS-409481	Pulse One looping to "Publish Required" while "Trusted Server CA" is the only selected block.
PRS-408157	Facing slowness in Admin GUI while editing Licensing Summary.
PRS-408015	Print function is not working properly with Advanced HTML5
PRS-407793	ICS is not validating the sign in URL in login.cgi.
PRS-406983	PSAL not launched because RPM format PSAL file downloaded on Ubuntu machine.

Problem Report Number	Summary
PRS-404735	Menu button on the Top Left corner is no longer working on Gitlab Website.
PRS-393301	Web bookmark stays in the credential page after providing credentials via rewriter.
PRS-393278	Web bookmark loading as blank page without any data.
Release 9.1R16.1 PRs	
PRS-412751	System: Enabling Kernel protectionmay cause unexpected system crashes on virtual appliances.
PRS-411094	Logging: Login may timeout or is delayed if the roles and realms use more than 4K data.
PRS-412666	An invalid password expiry warning may display when MaxPasswordAge is set to never expire.
PRS-412190	System: Incorrect archiving validation for sensor logs may prevent upgrading to 9.1R16.
PRS-412248	VPN Tunneling: An ACL with wildcard ("*") for port ranges prevents resources access on 9.1R16
PRS-412424	PSAL: Citrix Terminal Services (CTS) client may fail to launch on Chromium-based browsers (with and without the browser extension installed).
PRS-412744	System/Admin UI: The re-branding alert message cannot be dismissed.
PRS-412747	Host Checker/Admin UI: The alert message to increase Host Checker periodic Host Checker evaluation cannot be dismissed.
PRS-412763	System: Browsers configured for Italian may not render messages with proper accents.
Release 9.1R16 PRs	
PRS-411923	Signing-in page got doubled after upgrading the AA cluster to 9.1R15.

Problem Report Number	Summary
PRS-411805	"Password Expiration Prompt" when enabled shows an unusually huge number (say 24855 days).
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-411031	Unable to select the existing VNet while deploying PCS appliance from Azure marketplace due to the /24 subnet enforcement.
PRS-410957	Program dsnetd recently failed (Log improvements added to facilitate RCA in the future).
PRS-410868	For geolocation rules, the Access log does not contain the location of the source IP Address.
PRS-410256	Getting an Error FB-19 while accessing shared sub folder.
PRS-410172	Href instruction output under Sign in Page for End users is showing up extra characters.
PRS-409992	Default Sign-In page instruction is repeated twice in PCS9.1R15.
PRS-409905	HTML5 User added bookmark not visible.
PRS-409894	"ueba-monitor" service restarting frequently after upgrading to 9.1R15.
PRS-409871	cgi-server process crashed when using "Always-on VPN using wizard" feature.
PRS-409778	Upgrade to PCS 9.1R15 caused configuration to be wiped out only on hardware(PSA7K) not on VMs.
PRS-409726	DHCP failure seen after upgrade to 9.1R15 using Infoblox.
PRS-409627	Auth traffic control fails post-upgrade to 9.1R12+ with IPV6 and Management interface only.
PRS-409543	Save All Logs button missing in 9.1R15 in IPS and ICS.

Problem Report Number	Summary
PRS-407681	Named User license does not allow users to login to VPN and gives error "Number of named users (55918) exceeded the system limit (0)" as special characters in the user name are not properly handled in the named license users' functionality.
PRS-409424	Restriction with geolocation feature is not working for UK/Germany IP Addresses.
PRS-409418	PCS/PPS Connection error with Pulse One: Operation timed out after xxx milliseconds with 0 out of -1 bytes received.
PRS-409103	Program Web failed on 9.1R14.
PRS- 408829	Program TNCS failed.
PRS-408573	PCS server deployed on Azure goes unresponsive.
PRS-408542	When using PDC client on Window 11 OS ,authentication report shows Device OS as "Windows" instead of "Windows 11".
PRS-408525	Import of "Enable Pulse Client Components removal Tool for Cert issue Remediation." setting fails.
PRS-408446	Duplication of host checker policy fails if it is configured with the Registry settings.
PRS-408397	User disconnections are not properly logged in the User Access logs giving rise to confusion at times.
PRS-408234	Deprecated SSH Cryptographic Algorithms Supported on Azure.
PRS-406752	Vision Center app not working via re-write.
PRS-408049	Named User Record is not populating in License server Named user repository page.
PRS-407681	Named User license does not allow user to login to VPN and gives error Number of named users (55918) exceeded the system limit (0).
PRS-407644	On 9.1R12 System Software unable to pulldown backup configuration using REST.

Problem Report Number	Summary
PRS-406991	High CPU due to dsserver-tasks on PSA5000-v due to huge file transfers.
PRS-406832	With Static proxy and chrome PSAL+JSAM+Proxy , JSAM is not launching. PSAL is not using static proxy.
PRS-406707	Active Directory authentication server 'XXXX': No logon servers are currently available. Device could not connect to any domain controller of the domain.
PRS-406657	Program Web Failure due to memory leak.
PRS-405934	Users unable to establish tunnel - TUNSETIFF failed with error 16.
PRS-405192	ICS crashes sometimes when using ipv6.
PRS-404710	DMI update of PSAM destination servers takes effect on reconnecting of PDC client.
PRS-404126	Users were unable to connect, existing users got disconnected due to aggressive “Periodic Check” timers.
PRS-403095	HC Logs in User Access shows Local Username instead of VPN Username while using Embedded Browser.
PRS-390142	Outlook via Office365 fails to view or send email for all browsers.
Release 9.1R15 PRs	
PRS-408555	Upgrade failed from 9.1R13.1 to EA build 9.1R15.
PRS-407882	Users unable to access the VPN as the host checker fails with McAfee anti-virus.
PRS-407810	Priority of log SYS31048 (Lost syslog connection to server) is reduced to major from critical.
PRS-407805	Garbled text displayed in IE JSAM Window upon launching bookmark.
PRS-407184	HC re-evaluate Carbon Black virus definition check fails with number of updates.

Problem Report Number	Summary
PRS-407143	Internet Check during HC for EDR products is removed to prevent false-positive scenarios - https://forums.ivanti.com/s/article/KB45142.
PRS-407034	Users are dropped with Dsagentd snapshots generated.
PRS-407029	When saving the Terminal Services Profile, it unchecks the NLA option in the bookmark tab.
PRS-407023	Stales entries in shards is now removed. This will prevent shards from overload.
PRS-407010	Same IP address from IP pool was assigned immediately to different users in short span.
PRS-406654	'Profiler Events' is missing in REST API call.
PRS-406149	XML export on 9.1R13 doesn't contain Local user accounts data.
PRS-405891	Role mapping clash causes connectivity issues for PDC.
PRS-405756	Rewriter application doesn't work via rewriter due to parsing failure (Triple dot and return statement).
PRS-405597	HTML5: File cannot be downloaded if filename contains certain special characters (spec chars $ # % £).
PRS-405494	Full screen mode for multi monitor setup does not match native resolution.
PRS-405462	Top Level DNS domain is not validated properly under connection profiles and console.
PRS-405158	Logs generated on the desktop when accessing the VPN using Internet explorer / MS Edge.
PRS-405155	Events logs generated with wrong source IP address when users tried to connect.
PRS-405102	ICE license does not get auto-disabled.
PRS-404794	Lots of CRL failure entries getting generated in event logs for failed CDPs and it would be there every 5min for each failed CDP.

Problem Report Number	Summary
PRS-404605	Error Invalid Total Maximum Bandwidth "250" Must be between 0 and "0" when attempting to define the "Total Maximum Bandwidth".
PRS-404564	LDAP Domain Name not able to process Truncated TCP DNS response.
PRS-404538	ICS on AWS crash after Disk usage increase.
PRS-404512	Sign-in policy was not getting synched in config-group in pulse one.
PRS-404494	namedusersrestserver.log is filling up causing the HDD 86% usage.
PRS-404178	Intermittent resource access issue (RDP, SSH etc) through PSAM.
PRS-403817	BeyondSSL (Advanced HTML5) logging improvement added like Basic HTML5.
PRS-403588	Importing certificates with system config fails if special characters are part of the password.
PRS-402863	Config option provided for User Record (State Storage) management.
PRS-402627	Pulse One configuration in ICS shows 6 days "Credential Renegotiation Interval" but logs shows every 6 hours.
PRS-402567	Public IP of user in the access logs change when changing password.
PRS-400073	SNMPv3 Engineboots & EngineTime value as 0 with netSNMP lib 5.7.3.
PRS-398595	Modifying IP config using console with VLAN interface fails.
PRS-398358	Disk space getting full resulting in service restart on PSA-V.
PRS-397883	Webpage not loading via ICS.
PRS-396712	PCLS responding to heartbeat request with 404 error.
Release 9.1R14 PRs	
PRS-406149	Data is missing in XML export for Local user accounts in 9.1R13.

Problem Report Number	Summary
PRS-405422	Telnet/SSH: If User localization is JAPANESE, the display screen is garbled.
PRS-405395	Secondary RSA Authentication failing on PDC.
PRS-405370	Super Admin Session is not working when HTTP Only Device Cookie is enabled.
PRS-405203	Admin UI Unable to switch from ICT periodic scan to scheduled scan.
PRS-405082	Core dump generated while rewriting html with xsl stylesheet.
PRS-405071	Resource policy-based detailed rules failure user logs are flooding the User access logs.
PRS-405008	Mac OS Catalina 10.15.7 is failing to pass the HC policy set for File Vault.
PRS-404961	Difference in the GUI and XML export values for Integrity check specifications.
PRS-404839	Radio button on changing the Periodic scan to every 2 hours is not saved.
PRS-404771	User access log was being printed with default username as "System" instead actual username.
PRS-404768	Activity dashboard shows incorrect number of active users over the PCS appliance.
PRS-404713	Issue with high CPU utilization with rewrite-server process snapshot generation.
PRS-404688	User access log prints default username as "System" instead of actual username.
PRS-404264	The ifSpeed default value for physical interface of PSA7000 device is set to 10 Mbps.
PRS-404252	SNMP output of signedinWebUsers, iveConcurrentUsers and clusterConcurrentUsers is returning same value.
PRS-404114	Web Crash in 9.1R12 Version.

Problem Report Number	Summary
PRS-404081	Rewriter URLs ending special characters like (# or |) are not being redirected as the URLs will not be rewritten.
PRS-404016	Session extension with Pre-HC function is enhanced to contain the realm details.
PRS-403945	Background URL mentioned as style attribute not getting rewritten.
PRS-403822	Process SAML-SERVER crash in 9.1R12.
PRS-403777	PCS is not logging useragent string in logs for PDC clients.
PRS-403568	Login issues seen during session extension or during network switching.
PRS-403481	Program dsagentd failed after upgrading to 9.1R12.
PRS-403422	Lockout enforcement not working on PDC when AD is used as authentication source.
PRS-403216	Built in Integrity check scanner tool in PCS version 9.1R12 not accepting 0 in hour field for scheduled scan.
PRS-403208	Issue with Integrity check tool in standalone PSA 300.
PRS-403046	Users face permission denied while browsing file URLs.
PRS-403030	iOS Pulse Mobile users unable to access intranet resources through Per-App VPN after upgrading PCS to 9.1R10 or above
PRS-402559	Seamless Upgrade Helper prompt in Italian Browser does not work as expected.
PRS-402387	System: watchdog restarts cgi-server for at least one hour after changing SSL cipher selection.
PRS-402171	Throughput graph getting cleared on PCS Virtual Appliances.
PRS-401685	Triple dot creates a syntax error while rewriting API.
PRS-399221	A/A Nodes have user record differences.
PRS-398443	Citrix JICA/WI through CTS fails application access after import XML of same resource profile, manually creating fixes issue.

Problem Report Number	Summary
Release 9.1R13.1 PRs	
PRS-404658	Advanced HTML5 SSH Sessions and do not support scroll bar
PRS-404298	Advanced HTML5 Copy/Paste does not work for SSH
PRS-402150	Suddenly new L3 ESP/SSL VPN connection request fails for users due to auto-generation of Dsagentd cores.
Release 9.1R13 PRs	
PRS-403552	Client certificate information (serial number and certificate) is not available in Ivanti Connect Secure user access logs.
PRS-403495	Browser based end user UI error message for invalid credentials is not seen.
PRS-403462	Warn customers to follow mandatory steps before upgrading Ivanti Connect Secure/Ivanti Policy Secure.
PRS-403370	PDF files with streams having no Length attribute create segmentation fault causing rewriter server core.
PRS-403036	Source IP restriction for IPV6 Subnet in Roles restriction is not working.
PRS-403027	Core Access: SSO redirect with concur is not working
PRS-402999	XML import fails when config with the connection set containing option "Connect to URL of this server only" is disabled. This is due to improper initialization
PRS-402922	Improvements for ICT
PRS-402855	Ivanti Connect Secure archiving is not happening on Azure server
PRS-402633	DSDID length is not calculated properly causing Process web crash in FIPS mode.
PRS-402583	ICT page is skewed to left in classic UI but OK in new UI
PRS-402447	The image quality needs improvement for advanced HTML5 RDP.
PRS-402338	"Bookmarks open in new window" option is not exported in XML Export.

Problem Report Number	Summary
PRS-402271	While creating citrix profiles and change the options from java/html5/non-java, the auto policies created are not being handled as expected.
PRS-402253	Display a log message when the Root Partition gets into Read/Write Mode
PRS-402218	Unable to open Sharepoint documents using MS office native apps.
PRS-402075	HTML5: Option needed to hide basic HTML5 bookmarks/RDP launcher
PRS-401872	File download fail as file URL is getting truncated where newline exist in file name.
PRS-401553	When launching the Citrix client, 60 seconds delay is seen with no UI feedback, before PSAL download link appears.
PRS-401376	dsTermServ.exe crashes and unable to access terminal services with Applocker installed.
PRS-401160	Import of configs from older software to 9.1R11.4 may generate some error logs along with 'import done' message.
PRS-400261	REST API incorrectly responding to queries with ascii symbols
PRS-400152	With Recursive DNS domain name resolution for LDAP server is not successful.
PRS-399042	Process dswsd crashed during network fluctuation when some of the variable is not set correctly.
PRS-398648	Enabling/Disabling ICE license on PSA7000 increases the CPU usage
PRS-396540	On the IE browser for the advanced HTML5 intermediate, login page text displays “submit query” instead of submit.
PRS-395709	In MAC Safari browser, Advanced HTML5 sessions clipboard is not available.
PRS-395699	For Advanced HTML5 RDP sessions, video quality can be inconsistent at times.

Problem Report Number	Summary
PRS-392135	Pulse One disconnected from Ivanti Connect Secure after Ivanti Connect Secure upgrade
PRS-390822	Page rendering issue due to Cross-origin Object.
Release 9.1R12.1 PRs	
PRS-403735	Lost connections and dsagent process restarts due to a malformed IKEv2 packet.
PRS-403191	Unable to assign NCIP from the static IP pool in Ivanti Connect Secure 9.1R12.
Release 9.1R12 PRs	
PRS-401930	Authentication fails with no authentication prompt even though “Allow Smartcard with Network Level Authentication” shows enabled in the UI. However, XML export shows it as "Disabled".
PRS-401673	Due to Password Policy Control Changes introduced in 9.1R5, if we do not receive the proper response from LDAP server the authentication fails and associated process crashes.
PRS-401574	Duplicated Named User Licenses as usernames are treated case sensitive.
PRS-401421	Ivanti Connect Secure does not send DSID cookie to Pulse Client (SiteMinder authentication).
PRS-401356	The default admin realm is enabled with source IP restriction which restricts the access from a public network..
PRS-401318	Event log modification from “info to critical” for SYS30948 and from “critical to major” for SYS30912.
PRS- 401294	Log ERR32037 “Server name contains unsupported/unsfe characters”, is seen even if the server name is valid and spelling unsafe is corrected in 9.1R12.
PRS-401213	Web crashes (restart) due to a problem in JSAM/WSAM data path leading to user disconnection and reconnection.

Problem Report Number	Summary
PRS-401185	Multiple Syslog entries are seen under in A/A clusters having more than 2 nodes.
PRS-401064	PSA7000 shows improper interface speeds when VLAN is configured.
PRS-400976	Multiple monitors, sound does not work when HTML5 is configured with NLA and no SSO set.
PRS-400960	Static IP via Radius Attributes not working as expected.
PRS-400951	Static IP allocation fails when there are IP pools which overlap with other IP pools.
PRS-400771	Windows Terminal Services client disconnects the sessions intermittently.
PRS-400725	Windows Terminal Services client disconnects when copying the files.
PRS-400655	Importing certificates from system config fails when there is no password set during config export.
PRS-400631	AP cluster fail-over VIP is taking more time for Cluster VIP reachable.
PRS-400495	Azure Ivanti Connect Secure instance goes unresponsive intermittently.
PRS-400285	Added an event log to monitor internal shard usage.
PRS-400243	VIP status change notification event sent by passive node on reboot is treated as VIP status change notification from Active node, and users notice VPN reconnection.
PRS-400229	Session extension using PDC through SAML authentication server does not work.
PRS-400206	Changes to entity ID and SAML auth server instances are not recorded in the admin access log.
PRS-400067	Windows Pulse Client 9.1r11 with Avaya One-X causes BSOD.

Problem Report Number	Summary
PRS-400023	when User role is duplicated, VPN tunneling option is reset to default options and not updated.
PRS-399963	Impexserver crash is observed when importing Ivanti Connect Secure is having a duplicate certificate.
PRS-399925	Yearly graph shows incorrect data for active user sessions.
PRS-399842	After upgrade to 9.1R11, IP Assignments through LDAP/Radius Attributes is failing but Static Pool works fine.
PRS-399626	PSA7000f server restarts unexpectedly and user connection fails. Additional logs added to determine the Root Cause.
PRS-398621	Enabling "SNMP Diagnostic Logging On" is not working.
PRS-399559	Static IP allocation issue when multi session is enabled.
PRS-399450	Citrix VDI not working in the first attempt, Second attempt starts working and CTS launches and connects.
PRS-399292 (PRS-397227)	Admin URLs are not accessible if administrator logs in with IPv6 address of Ivanti Connect Secure. (PRS-397227 - Fixed in R12 via this PRS-399292.)
PRS-399409	Only ntpd Client service runs going further (Previously both server and client services were run).
PRS-399192	Failed to upload configuration on the newly registered PSA device on pulse one.
PRS-399136	Redirected URLS encoded not passing properly.
PRS-399021	When creating an admin role, User roles in the Users delegation displays incorrect number of selected roles.
PRS-398969	Bandwidth management policy does not work in the SSL Mode.
PRS-398814	guacd process protection mechanism where each instance of guacd instance is monitored and killed if the instance takes 100% CPU till the grace time.
PRS-398703	Healthcheck.cgi does not work from F5 load balancer.

Problem Report Number	Summary
PRS-398600	Named User Record/Database do not show up on license client.
PRS-398371	VLAN details are not removed from VLAN page after removing VLAN ID from management port.
PRS-398348	Ivanti Connect Secure device does not send the SNMPv3 trap out from the device.
PRS-398303	HTML5 bookmarks will not be accessible.
PRS-398270	Expired certificates alarms for deleted certificates.
PRS-398262	Web process failures due to DSEvntTimer observed on Ivanti Connect Secure.
PRS-398002	Limitation on number of realms in sign in URL while connecting through PDC client.
PRS-397693	Compliance report for hostchecker policies mapped against realm/role is generated for user that does not belongs to that realm/role.
PRS-397676	License server low-level protocol error,Code=[6]: Could not resolve host name through external port.
PRS-397664	XML export of Admin/User realms shows the directory-server attribute same as authentication-server even though there is None in the UI.
PRS-397574	With Pre Host checker configured, if the Pulse credentials prompt times out, the session is extended instead of resumption.
PRS-397461	Basic HTML5 : Users not able to use mouse emulation with guacamole RDP sessions on iOS13 iPad.
PRS-397414	Extra fields appear under Role > Web Bookmark for new or existing bookmark prior to upgrade.
PRS-397380	User record synchronisation feature may not occur as-expected across all configured devices.
PRS-397349	User Record Sync clients disconnecting from green to grey status.

Problem Report Number	Summary
PRS-397346	Host Checker Re-Triggers with error message 'ESAP upgrade is needed or Patch Management policy configured' in event logs.
PRS-397290	SAML Single logout is failing.
PRS-397227 (Fixed in R12 via PRS-399292)	Admin URLs are not accessible if administrator logs in with IPv6 address of Ivanti Connect Secure. (Fixed in R12 via PRS-399292.)
PRS-397213	MSSP: watermark does not get reset, even if license client is not leasing licenses from the license server.
PRS-397059	AAA: X-forward-for IP is not evaluated/used when using geoLocationCountry rules.
PRS-397043	One cluster node stops accepting new VPN connections post getting deactivate/activated in cluster.
PRS-396972	Number of MC groups has been increased to 40 & 36 on Linux and Windows respectively.
PRS-396200	Upgrade fails when data partition does not have enough space to hold system configurations.
PRS-396062	Users unable to join hosted pulse collaboration meeting session through IE 11 browser.
PRS-395544	Upgrade failing for one node In A/P cluster.
PRS-395508	User gets disconnected when cert restriction policy is configured and SAML authentication server is used. This has been fixed as part of this PRS.
PRS-395347	Incorrect Source IP address used when sending packets to secondary radius server (When using “Traffic Decoupling” at “Auth Server Level”).
PRS-394657	Pulse Collaboration: Customer gets an error while scheduling the meeting if the localization set to French.
PRS-394572	SNMP alerts shows abnormal increase in device temperature.
PRS-394202	Manual failover takes time to resume user tunnel connections. This is now improved.

Problem Report Number	Summary
PRS-393712	Terminal Session stops working after upgrade to 9.1R8. Adding logs to improve debug ability.
PRS-393675	Failed to send API requests from Ivanti Connect Secure(MDM) to Microsoft Intune for device authorization.
PRS-391871	Openstack KVM deployment - after reboot only local subnet can connect, Ivanti Connect Secure ignoring other packets.
PRS-390315	Fed-Wide session sync delay between Replicas results in user session getting removed from Imported sessions within few minutes.
PRS-380985	Incorrect Interface Status sent by the Ivanti Connect Secure appliance while performing SNMP Walk after upgrade to 9.1R1.
PRS-361501	Sometimes end-user is unable to access backend resources.
Release 9.1R11.5 PRs	
PRS-401116	Pulse Upgrade Helper tool upgrades Pulse Desktop Client once and terminates IE processes during the process.
PRS-400823	State Storage full and Program cache-server failed.
PRS-400746	Unable to see the details of package uploaded into Staging Area in Admin UI
PRS-400717	Improper titles for lines on HTML5 dashboard graph and some titles missing in Concurrent users graph.
PRS-400614	PSAL fails to launch Java Applets.
PRS-400653	In versions 9.1R11.4 and below, if the 'HTTP only cookie' option is enabled for admin role, the super admin session will not work.
PRS-400544	Program web recently failed on 9.1R11.3
PRS-399600	Users are not prompted to enter credentials as well as MFA on successful connection to VPN.
PRS-399576	The localization support is not available for new options on user created advanced HTML5 bookmarks.

Problem Report Number	Summary
PRS-399150	Host header Validation is failing for Virtual hostnames.
PRS-396923	PSA 5000 crashes with no access to UI or Console.
PRS-384770	GARP frames are not being sent under Default VLAN configured on an interface - VIP IP is not accessible after manual failover in A/P cluster.
Release 9.1R11.4 PRs	
PRS-400095	Web crash due to empty session IDs.
PRS-399115	Warm restart of services is observed on two node PSA7K AA cluster when run continuously for multiple days causing L3 and L4 connection drops.
PRS-398510	Error code 1326 displays on Pulse Client when username/password is saved on Client and expired on AD server.
PCS-27395	Custom expression failure messages is flooding User Access Logs.
Release 9.1R11.3 PRs	
PRS-400438	Code signing certificate fails globally when launching HC using browser. The certificate issue is addressed. For information refer KB44781.
Release 9.1R11 PRs	
PRS-398532	During Kernel Panic (System stalls with no access to Admin UI), Ivanti Connect Secure/Ivanti Policy Secure devices will automatically reboot by default.
PRS-397979	Process snapshot gets generated for dsagentd/Web processes in 9.1R10. This issue can happen rarely when Client closes PSAM session with Ivanti Connect Secure server immediately just after closing TCP application connection.
PRS-397324	Dsagentd crashes when Ivanti Connect Secure System load average goes high.
PRS-397190	Rename all the places that contain WSAM keyword on the Admin UI to PSAM.

Problem Report Number	Summary
PRS-397171	Kernel panic is observed sometimes and Ivanti Connect Secure restarts.
PRS-397072	Host Check fails on macOS 11.1 when the policy is enforced. For more information, refer KB44663.
PRS-397046	Background image and recaptcha is not loading through rewriter.
PRS-397000	Supporting corner cases for jquery usage in client side rewriter handling.
PRS-396944	WTS: End users unable to enable MIC on the user interface.
PRS-396921	When a user access basic html5 bookmark, guacd process may restart.
PRS-396870	PDC: Virtual adapter stops intercepting IPv6 packets on Mac/Windows/Linux platforms using PDC 9.1R9 build in ESP mix mode.
PRS-396827	When advanced HTML5 connections are accessed first time, user may see “Failed to connect to gateway” message.
PRS-396773	Host Checker fails after upgrading ESAP version to 3.7.1 or 3.7.2 or 3.7.4 from any previous ESAP version on macOS endpoints (KB44643).
PRS-396710	For advanced HTML5 sessions, REST API count displays invalid values.
PRS-396675	Fixed rewriting for other elements of div tag caused due to Data-srcset support.
PRS-396609	For unsuccessful HTML5 connection, VDS page displays the entry for advanced bookmarks.
PRS-396389	User is not able to configure Azure as backup server in China region.
PRS-396262	Login button is not enabled when accessing web rewriter through IE browser.

Problem Report Number	Summary
PRS-396134	NTP will not synchronize time when default VLAN ID is configured on the interface.
PRS-396116	Browser-based Host checker fails to get launched in 64 Bit Internet Explorer.
PRS-396097	Kernel panic “nf_udp_esp6” may be observed on PSA7000F.
PRS-395982	Rename all the places that contain WSAM keyword on the Admin UI to PSAM.
PRS-395973	User column for SNMP traps does not show the username.
PRS-395902	Pulse Component Set is selected to NONE does not update the “connstore” in spite of changing the connection set. A warning message is displayed to guide configuring the “Connection Set”.
PRS-395813	Disabled DMI Inbound connections setting is not retained after reboot.
PRS-395330	SNMP query for “sysObjectID” is returning PSA7000F for PSA7000C platform.
PRS-395217	Pulse One fails to sync files Windows ACL policies on Target Ivanti Connect Secure from Master Ivanti Connect Secure.
PRS-394382	Handling rewriting of Data URLs at server side code to avoid rewriter crashes.
PRS-393851	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.
PRS-392135	Pulse One disconnected from Ivanti Connect Secure after Ivanti Connect Secure upgrade.
PRS-391999	TOTP Authentication fails for all users.
PRS-391667	Aligned the latest MaxMind DB pointer with local DB for Ueba package upgrade.

Problem Report Number	Summary
PRS-390324	Spikes are observed at regular intervals in the concurrent SSL connections graph.
Release 9.1R10 PRs	
PRS-396733	For advanced HTML5 bookmarks, when the target machine is configured with hostname resource, may not be available at times.
PRS-396149	Web process crashes.
PRS-395696	For Advanced HTML5 sessions, error messages are not displayed.
PRS-395039	License client reports the excess allowed usage while sending the usage to server. This issue is fixed to limit the reported count to maximum lease limit.
PRS-394744	"Error updating data for chart hc_failure_reason/auth_mechanism" log on Ivanti Connect Secure is not seen. The Exception that was causing this error is fixed.
PRS-394586	Administrator can set a guaranteed minimum users on a realm to allow an user from that realm to log into the Ivanti Connect Secure/Ivanti Policy Secure when the licensed concurrent user limit is reached. From Release 9.1R10, guaranteed minimum users is applicable when no ICE license is installed or ICE license is installed and enabled.
PRS-393989	When the current MSP license expires, and customers installs a new MSP license, VLS needs to re-register with PCLS. This was not happening previously, and this resulted in billing against older authcode. In 9.1R10, we have fixed this issue, so that VLS re-registers with the next active MSP license. Hence, the license usage is reported against the new authcode.
PRS-393140	Certificate authentication fails when the option 'Trusted for Client Authentication' is disabled in client CA certificate hierarchy. Added a new user access log and an Admin UI note to alert the Ivanti Connect Secure administrator in such cases.

Problem Report Number	Summary
PRS-389455	Analytics Device OS graph does not show Windows 10 OS information. This issue is fixed in 9.1R10 onwards.
PRS-387059	Unable to publish config when trusted client CA cert (using CRL) is deleted on Master appliance. This issue is fixed in 9.1R10 onwards.
PRS-380696	Predefined Host Checker policy can now be configured with a ignore category based on the vendor.
PRS-390086	End-Points connected through slow internet now will not hit the incomplete ESAP package download scenario.
PRS-395701	Access to advanced HTML5 custom URL is not successful without user logging into Ivanti Connect Secure server. The user is now prompted to log into Ivanti Connect Secure followed by log in prompt to target machine.
PCS-22768	Remote-program, Multi Monitor, Session recording options are not working for end-user created bookmark.
PCS-22757	Advanced HTML5 graph is not implemented.
Release 9.1R9.1 PRs	
PRS-396149	Web process restarts when Client Application profiles are configured under **SAM** --> **Resource Profiles**.
PRS-396441	For advanced HTML5 sessions, web process restarts if the FQDN is not resolved.
PRS-396463	For advanced HTML5 sessions, login may fail if the target machine username or password contain special characters.
Release 9.1R9 PRs	
PRS-395306	“Failed file system integrity check” warning appears on Admin UI when the file “integrity_check” is either not created or deleted. This is addressed in 9.1R9.

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 Connect Secure fails to show Windows OS version with 9.1R8 PDC builds.
PRS-394537	XML export shows virtual Platform for physical license clients. This is addressed in 9.1R9 release.
PRS-394390	Ivanti Connect Secure is not responding to ping with payload size larger than the MTU size.
PRS-394242	Rewriter client side parser issue fixed for DanaGetURLUnencoded API.
PRS-394137	Performance tuning is incorporated for FQDN ACL feature.
PRS-394107	Pulse Client version does not display under "Active Users" tab for mobile devices. The issue is addressed in 9.1R9.
PRS-394075	Pulse Collaboration stops working after Setup Client download fails, after upgrading it to Ivanti Connect Secure 9.1R8.
PRS-393736	Dssecidcheck program fails. This is addressed in 9.1R9.
PRS-393649	If a session is no longer present in the system when the IP lease period is active, then the IP address is released back to the DHCP server.
PRS-393627	Host Checker: Compliance check fails when using Sophos Cloud Endpoint 2.8.6.
PRS-393624	SNMP polling on ifHighSpeed does not return the correct speed of a network interface, if default VLAN is enabled for that interface. This is resolved in 9.1R9.
PRS-393603	File Share: When a big file is uncompressed, Ivanti Connect Secure will ensure that all the chunks are read properly from 9.1R9.
PRS-393544	On the "Virtual Port" view page, if admin clicks "Cancel" button without saving any changes, then Network service is restarted. This is addressed in 9.1R9.

Problem Report Number	Summary
PRS-393437	From 9.1R9, if Ivanti Connect Secure VA is hosted by VMware, then NTP setting at "Date and Time" page will have an extra note which informs admin that the Virtual appliance should have only one source of Time Sync (VMware ESXi or NTP Server, NOT both).
PRS-393313	Web Process crash due to timer Library corruption is addressed in 9.1R9.
PRS-393269	Ivanti Connect Secure was unable to handle "Unknown" OCSP Response. This is addressed in 9.1R9.
PRS-393230	Sometimes, TCP Dump does not start. This is addressed in 9.1R9.
PRS-393146	Host Checker process tncs crash.
PRS-393070	Logical volume support is removed from KVM instances.
PRS-392934	Ivanti Connect Secure does not restrict user logins, even though dsagentd crossed 80% CPU utilization.
PRS-392547	Custom start page takes about a minute to show up when connected from IE with split tunnel and VPN auto-launch enabled. This is addressed in 9.1R9.
PRS-392359	The default password length has been increased and the same has been updated in the Azure ARM Template.
PRS-391949	In spite of installing the Meeting license on a virtual appliance running A/A cluster, the effective count of concurrent meeting users remain zero. This is addressed in 9.1R9.
PRS-391629	PSAL Linux is unable to connect to Ivanti Connect Secure. This is addressed in 9.1R9.
PRS-391573	During domain controller reachability test under LDAP Auth Server, Ivanti Connect Secure does not close the LDAP TCP socket connection with domain controller. This is addressed in 9.1R9.
PRS-391273	When SAML config has both SLS and SSO service types using same Location URL, Import XML fails causing SAML metadata publish to go into loop. This is addressed in 9.1R9.

Problem Report Number	Summary
PRS-389484	Ivanti Connect Secure appliance now sends IPv6 Neighbor Advertisement with correct VLAN tag for user roles mapped with sourceIP as VLAN interface.
PRS-389448	dsagentd process crashes when handling multicast traffic. This is addressed in 9.1R9.
PRS-388972	Session extension fails when custom sign-in page is configured for the sign-in policy. This is addressed in 9.1R9.
PRS-387807	When default VLAN is enabled, virtual port is not considered for the user role while calculating the source IP. So, default IP was assigned as source IP. This is addressed in 9.1R9.
Release 9.1R8.2 PRs	
PRS-394540	A tactical fix was provided as part of 9.1R8.1 (PRS-393243). However, Custom Rule Expression evaluation is now made more robust with thread safety in 9.1R8.2.
PRS-394113	Ivanti Connect Secure can parse and store up to 32 IP addresses returned by DNS server.
PRS-393865	Running TCP Dumps can get the Disk Full as there is no Log Rotation in place. This is addressed in 9.1R8.2.
PRS-393666	Application level integrity check was missing on Ivanti Connect Secure for Fragmented EAP-TLS packets. This is addressed in 9.1R8.2.
PRS-393440	Host Checker fails with Error "Host checker did not get installed properly. Your computer does not meet requirements". This is addressed in 9.1R8.2.
PRS-392873	The desktop settings configured under terminal services bookmarks will not apply if the resource's Operating System is Windows 8 or later. This issue is seen in Pulse Client 9.1R8.1 or earlier. The issue is resolved after implementing new interfaces of the Microsoft MsTscAx component.
PRS-392156	Modified WebRequest code to prevent null pointer (Hprewrite-server) crashes.

Problem Report Number	Summary
PRS-391188	DHCP options disappear upon clicking "Refresh Now" button under Connection Profiles > Proxy Server Settings. This is addressed in 9.1R8.2.
PRS-391141	Duplicate syslog (SYS31407) messages appear in event logs. This is addressed in 9.1R8.2.
PRS-388494	Large Username XML Import now logs proper error message.
PRS-385110	Upgrade failure due to white spaces in the configuration is fixed in 9.1R8.2.
Release 9.1R8.1 PRs	
PRS-393434	Time drift is observed when NTP is configured on Virtual Appliances. This can affect authentication, cluster sync, and cause licensing issues. This is addressed in 9.1R8.1 (KB44558).
PRS-393243	Host Checker policy evaluation fails very intermittently for some time if policy rules need to be evaluated based on Custom Rule expression. This is addressed in 9.1R8.1.
PRS-392995	dsagentd crashes occasionally in load condition during initial data channel establishment. This is addressed in 9.1R8.1.
PRS-392842	The Overview/cockpit graphs representation will now show data similar to the Classic UI (It will omit the duration for which the data is not available).
PRS-392593	Restriction of REST API commands via the internal port is now fixed.
PRS-392254	SNMP polling was not returning false Ivanti Connect Secure Model Number and device type. This is addressed in 9.1R8.1.
PRS-392153	Session Server failures due to cluster instability is fixed in 9.1R8.1.
PRS-392096	Winbindd crash seen due to an exception is fixed in 9.1R8.1.
PRS-391990	SSH/Netconf clients should now be able to connect Ivanti Connect Secure DMI Agent successfully.
PRS-391708	Quick navigation link added to Enable/Disable FQDN ACL. And the following warning message is also added:

Problem Report Number	Summary
	"Ensure that there is no DNS latency/delay in the network to avoid performance issues".
PRS-391690	When a license client surrenders a license, the expiry date of that surrendered license keeps changing in license server to keep the expiry date always as 10 days (default) ahead of current date. The change is reflected in "License Summary" page of license server admin UI. But the change is not always reflected correctly at the "Pool of available licenses" section under the "Configure Clients" tab as there is a sync-up issue. This is addressed in 9.1R8.1.
PRS-391253	When Pulse Desktop client is used, Ivanti Connect Secure server does not provide session ID in User Access log after a successful login. Here "session ID" denotes the last 8 characters of actual session ID in server, and it is used to differentiate a session from other sessions for one user. From 9.1R8.1, Ivanti Connect Secure server will provide this ID for all types of Pulse clients after successful logins.
PRS-390500	From 9.1R8.1, Ivanti Connect Secure end user name will appear as client name (instead of Localhost) in HTML5 RDP session.
PRS-389526	From 9.1R8.1, a warning message will be sent only when the lease request fails or no leasable license is left with the number of users reaching towards maximum concurrent users limit.
PRS-389251	Frequent warning message about "number of concurrent users is nearing system limit" creates confusion about actual issue with concurrent users limit. Form 9.1R8.1, a warning message will be sent only when lease request fails or no leasable license is left and number of users are reaching towards maximum concurrent users.
PRS-387936	Global session configuration values (Users > User Roles > Default Options) are used when individual user role is not configured with session options.
Release 9.1R8 PRs	
PRS-392702 PRS-391725	Additional logging to debug web crashes.

Problem Report Number	Summary
PRS-392244 PRS-388907	Active users were not able to sync to the newly added node on a 3 node Active/Active cluster. This is addressed in 9.1R8.
PRS-392236	Hyper-V 9.1R8 upgrade from earlier versions is not supported.
PRS-392040 PRS-388907	User sessions are not synced across the nodes in an Active/Passive cluster. This is addressed in 9.1R8.
PRS-391902	Invalid packet processing in kernel is addressed in 9.1R8.
PRS-391879	Intermittent audio disconnect issue with HTML5 RDP session is addressed in 9.1R8.
PRS-391837 PRS-380638	tncs process crash with Host Checker caching enabled is addressed in 9.1R8.
PRS-391305	Upgrading Azure images from 9.1R5 to any later releases returns with error message if the factory reset version is 9.1R5.
PRS-391004	The dsunitysamlhandler process crash is addressed in 9.1R8.
PRS-390937	In 9.1R4 to 9.1R7, when multi monitor option is selected under the Terminal Services session/bookmark page as well as under Terminal Services Options page, XML config data shows incorrect value. This is addressed in 9.1R8.
PRS-390916	Kernel panic during upgrade on PSA5000-V running 9.1R3 on Hyper-V. This is addressed in 9.1R8.
PRS-390907	Log rollover is implemented for postgresd so that it does not cause the Disk to get full.
PRS-390831	SAML authentication is now successful when signing is enabled for SAML requests/responses using certificates.
PRS-390828	As dshealthstatsunity process was getting exited due to exceeding process size, data was not being sent to Pulse One for that particular interval and thus calculated cumulative count at Pulse One was incorrect. This issue is addressed in 9.1R8.
PRS-390769	Kernel logging options are added by default for better debuggability.

Problem Report Number	Summary
PRS-390426	As process was getting exited due to exceeding process size, data was not being sent to Pulse One for that particular interval. This issue is addressed in 9.1R8.
PRS-390274	For config elements with unicode characters and having length exceeding 4096 bytes, the config import fails on Pulse One client. This issue is addressed in 9.1R8.
PRS-390217	Tunnels get dropped during connection resumption due to a server error. This is addressed in 9.1R8.
PRS-390106	Inconsistent upgrade issues seen while upgrading Hyper-V images in clustering and single node.
PRS-389927	The TCPDump filter expression can now contain characters from the set "<>|;()[]?#$^&*=\'`"" .
PRS-389897	Kernel Panic hrtimer_interrupt issue is fixed.
PRS-389771	Multiple VIP fail over was seen on Virtual A/P cluster due to the time drift between system clock and hardware clock. This is addressed in 9.1R7 (KB44457).
PRS-389756	The dsagentd process crash during assignment of IP address from DHCP server is addressed in 9.1R8.
PRS-389737	Cluster VIP is not getting migrated to other node when active node's internal interface is not reachable and external port is reachable.
PRS-389642	XML import is failing if configuration file has syslog IPv6 settings.
PRS-389451	TCPDump fails to capture packets when multiple interfaces are selected.
PRS-388630	With current OPSWAT library code, the verification of update functionality was not working. OPSWAT has fixed the issue and provided a new library.
PRS-388104	The top-roles section displayed on dashboard was not showing the roles name in Japanese and other languages. This issue is fixed for both Classic UI and New UI in 9.1R8.

Problem Report Number	Summary
PRS-385646	Whenever a user tries to access the VDI resource, a wrong error code for timeout was written in the logfile. The user sees the message "Missing host name/IP, Invalid host name/IP: " To address the issue: 1. Timeout error ID is passed to write in logfile. 2. A proper validation has been done for the wrong false alarm.
PRS-364693	Bandwidth Management policy not getting enforced for VPN tunneling users is fixed in 9.1R8 - https://forums.ivanti.com/s/article/KB44402/?kA13Z000000L3Dc.
PCS-20480	Ivanti Connect Secure was returning "Incorrect ICE action" error message when trying to execute api/v1license/ice REST API to fetch the current status of ICE. This is addressed in 9.1R8.
PCS-20433	Existing HTML5 active sessions are not displayed under "Active Virtual Desktop Sessions" tab.
PCS-19628	Platform page shows hypervisor information as KVM instead of Alibaba-Cloud-KVM or OpenStack-KVM.
Release 9.1R7 PRs	
PRS-391296	Application access using Citrix Terminal Services through IE browser fails in 9.1R5-9.1R6 Ivanti Connect Secure versions. This is addressed in 9.1R7.
PRS-390778	Host Checker support for OS version check is added for iOS versions 13.4 and 13.4.1.
PRS-390775	Ivanti Connect Secure syslog forwarder does not work if connection to syslog server fails during startup of the syslog forwarder process. This is addressed in 9.1R7.
PRS-390530	Enterprise user onboarding fails in Mac OS Catalina as the filename extension was not populated as '.mobileconfig'. This extension is added in 9.1R7.
PRS-390475	Noticeable slowness was seen in several applications including Citrix HTML5 video rendering in 9.1R3-9.1R6 Ivanti Connect Secure versions. This is addressed in 9.1R7.

Problem Report Number	Summary
PRS-390401	SNMP functionality was not working after cache sync. This is addressed in 9.1R7.
PRS-390234	User access log now shows real-time active HTML5 sessions count.
PRS-390118	In Ivanti Connect Secure A/P cluster split and joined scenario, lease license IDs are validated to reset the stale ID and license client will be able to lease licenses successfully.
PRS-389481	Cloud Platforms: Improved SNAT performance by tuning kernel module parameters based on the memory available in the device.
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.
PRS-388932	From Ivanti Connect Secure 9.1R7, the "Synchronization of last access time in user sessions" option in A/A Cluster mode will be auto-enabled and grayed out when the "Synchronize user sessions" option is enabled (otherwise, it can affect session migration). Existing cluster configuration is not modified during upgrade, so we recommend admins to enable this option for existing configurations as well.
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-382777	Client's original Source IP was not logged if Load Balancer is used. Client's Source IP is now retrieved from 'X-Forwarded-For' header and logged in user access logs.
Release 9.1R6 PRs	
PRS-390370 PRS-390145	Java Script is displayed after the user scans the QR code only during the TOTP user registration.

Problem Report Number	Summary
PRS-390352	Hostname resolution for an FQDN with up to 255 characters was not supported through the L3 tunnel in Ivanti Connect Secure 9.1R5.
PRS-390198	Admin cannot download reports in PDF format for Ivanti Connect Secure.
PRS-389973	HTML5 connections cause memory leak in Guacamole server and result in high memory usage and swap memory usage
PRS-389811	CPU Allocation issue on PSA-7000 (all flavors/varieties) appliances in case of Single-Arm mode VA deployments is now resolved on PSA-7000 HW and ESXi (VMWare) solutions. Refer KB44446 for more details.
PRS-389744	Process snapshot for "dsserver-tasks" is generated while deleting meeting objects for corresponding users.
PRS-389544	Some of the examples listed under "Split Tunneling Networks" policies are not supported.
PRS-389523	External backend resource access using HTTP GET request with username in the URL for the file login.cgi fails through Rewriter.
PRS-389517	Web server crashes and results in User disconnections due to webSocket upgrade related messages during Auth Only URL access.
PRS-389440	User Accounts under TOTP Auth server Users section cannot be exported.
PRS-389406	Delayed or no response from Ivanti Connect Secure for SNMP queries under load condition.
PRS-389276	The corruption of blob during the epupdate results in Host Checker scan failure for users until the next successful epupdate.
PRS-389262	Web process snapshot is generated while sending POST request by REST API with an empty body.
PRS-389127	Garbled text in Citrix VDI profiles page when accessed using bookmark with the Japanese language.

Problem Report Number	Summary
PRS-388796	The dsagentd process (client server process) crashes and frequently disconnects in 9.1R4 when there are more than 1024 tunnels including MobIKE IKEv2 tunnels.
PRS-388645	After upgrading Ivanti Connect Secure/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-388542	Garbled text in file share page when accessed using bookmark with the Japanese language.
PRS-374603	During system downtime activities such as an upgrade, Event IDs such as 20412/20413 are missing in the Syslog server.
Release 9.1R5 PRs	
PRS-389938	9.1R4.3 Radius crashing, unable to authenticate Pulse.
PRS-389550	Intermittently, the system throughput falls drastically and user connections fail.
PRS-389246	"500 Internal Error" is displayed when opening Authentication related pages.
PRS-389212	Intuitive Customer friendly ways and relevant logs to avoid customers configuring single core.
PRS-388958	Idle timeout session is not working, OWA 2016 keepalives not ignored through web-rewrite.
PRS-388885	License Surrendering not happening due to the heartbeat not sent.
PRS-388743	Host Checker :: OS Checks :: MAC :: Add support to configure Minimum Service Pack/Version for MAC Catalina(10.15).
PRS-388734	PSA7000 at 30% total CPU due to two guacd processes at 100% CPU, planning pandemic and wanted to know root cause.
PRS-388536	One node in Cluster is surrendering the licenses to the License server. However, the increment of the surrendered time is not happening.

Problem Report Number	Summary
PRS-388479	PSA5000 : 9.1R4 : A/P Cluster : REST API calls are failing intermittently when they are executed in a loop continuously.
PRS-388429	Text corrected under Log/Monitoring > Admin Access > Settings.
PRS-388421	Ivanti Connect Secure 9.1R4 incorrectly reporting duplicate machine ID.
PRS-388409	Unable to upload config to Pulse One: Configuration changed while preparing configuration to upload.
PRS-388331	After upgrade VA-DTE & PSA-V to 9.1R4, nfqueue unable to create IPTables when VM is configured with 1 CPU core only.
PRS-388244	FileShare:: Customer unable to download direct file from FileShare on 9.1R4 Ivanti Connect Secure version.
PRS-387954	Rewrite: Web page of the maps web applications fails to load via rewrite.
PRS-387780	Registered Ivanti Connect Secure Appliance failing with Pulse one communication after importing user config and shows registration expired error message.
PRS-387641	"Sign Out message" does not properly display unicode text (Japanese, Korean, Chinese, etc.) with Sign-In Pages via browser.
PRS-387359	Unable to authenticate user using certificate. Reason: Wrong Certificate::unsupported name constraint type.
PRS-387349	System: Built-in Trusted Server CAs cannot be removed if they have subCAs.
PRS-387062	PSAM sending unintended traffic via tunnel to VPN in 9.1R3.
PRS-386875	User Sessions get disconnected after upgrading to 9.1R3HF1.
PRS-385747	Program dsdashsummary failing continuously on Ivanti Connect Secure running on 9.0R4.1.
PRS-385466	Sharepoint 2019 is not loading properly through web-rewrite.
PRS-385027	VDI Bookmark would not establish connection to the VDI resource without host entry on the client machine.

Problem Report Number	Summary
PRS-384955	XML Import of trusted server CAs generates a spurious admin log message for each unchanged CA.
PRS-382364	System: Device does not boot up when upgrading from 8.3R7.1 to 9.0R5 with option DELETES all system and user configuration data before installing the service package is selected.
PRS-381972	System : Licensing : "License server low-level protocol error, server=, Code = [6] :Could not resolve host name" populated in event logs of license server.
PRS-381905	After upgrading to iOS 13, HTML5 Access users seems to have broken the on-screen mouse pointer.
PRS-381716	AAA::Issues with host checker when user logs in to a different realm with TOTP auth server enabled.
PRS-381699	Pulse One 2.0.1902: Certificate > Trusted Server CA changes not being distributed (deleted expired CA).
PRS-381678	VIP became unreachable from enforcer when upgrading from 5.4R7 to 9.1R2.
PRS-381046	Rewrite: Dynamic365 menu tabs do not render when on 9.1R1.
PRS-380298	User access log indicates Login failed using auth server LDAP Server (Failed::unable to verify the first certificate) for wrong password.
PRS-380225	"Program fqdnacl recently failed" event failure on Ivanti Connect Secure 9.0R4.
PRS-379752	Reboot failed on PSA7000f.
PRS-379137	Gliffy Plugin in Confluence does not work via Web Rewrite.
PRS-376852	IPV4 Settings change in External or Internal port keeping Default VLAN ID same does not reflect under VLAN tab..
PRS-365669	SNMP: ifAdEntAddr mapped to wrong ifAdEntIndex values.
PCS-18217	License report did not show proper values for older dates (Dec month) after upgrading to 9.1R4 image.
Release 9.1R4.3 PRs	

Problem Report Number	Summary
PRS-389246	"500 Internal Error" is displayed when opening Authentication related pages.
Release 9.1R4.2 PRs	
PRS-380298	User Access log indicates "Login failed using Auth. server LDAP server (Failed: unable to verify the first certificate)" for wrong password.
PRS-387780	Registered Ivanti Connect Secure Appliance fails with Pulse One communication after importing user config and shows "Registration Expired" error message.
Release 9.1R4.1 PRs	
PRS-382268	PDC throws Authentication rejected by server [Error : 1319] when using global Ivanti Connect Secure url.
PRS-387062	PSAM sending unintended traffic via tunnel to VPN in 9.1R3.
Release 9.1R4 PRs	
PRS-365669	SNMP: ifAdEntAddr mapped to wrong ifAdEntIndex values.
PRS-367786	Device locked up and dropped all connections due to Web process consuming CPU.
PRS-375181	VLS does not throw any error if there is no response for Heartbeats sent to PCLS.
PRS-377456	EasyPrint feature using the Premier Java RDP Applet not working.
PRS-379345	Program dsagentd failed.
PRS-379411	Ivanti Connect Secure not sending any Syslog traffic to configured Syslog servers.
PRS-379801	Active Sync stopped working after upgrading the device to 9.0R4.
PRS-382021	Dismiss until next upgrade option is not working for banner related to perpetual licensing.

Problem Report Number	Summary
PRS-381990	During peak hours when multiple users try to do browser-based login on PSA5K, a few users might not be able to connect in the very first attempt.
PRS-380136	Cluster communication and state storage problems on A/A cluster.
PRS-380765	Program dsagentd recently failed after upgrading Ivanti Connect Secure from 9.0R3.2 to 9.0R4.
PRS-380796	Ivanti Connect Secure-VA sending critical SNMP alerts while leasing license.
PRS-380993	DFS: process snapshot generated by snmptrap process.
PRS-381100	Program dsagentd recently failed while running Mixed [V4 and V6] 60K VPN Tunneling ACL's throughput test on PSA5k for secure cache build-3164.
PRS-381579	Sometimes logs are not shown under Log/Monitoring page.
PRS-381366	Multiple users getting disconnected from Pulse Client.
PRS-381403	Sharing Feature is not working in macOS Catalina.
PRS-381579	Sometimes empty logs are seen under "Log/Monitoring".
PRS-381621	9.0R4 and 9.0R5 SPE (PSA-V) do not show the User Record Sync column in Admin UI > Auth Server page.
PRS-381633	Host Checker checking for virus definition file based on Number of updates fails for Sophos Endpoint Security and Control 10.8.4.
PRS-381736	After Upgrade from 8.3R7.1 to 9.1R1, error encountered while upgrading cache (in Host Checker).
PRS-381795	[FQDN ACL / NFQUEUE] Request DEV help in determining why thousand of VPN Tunnels dropped traffic within.
PRS-381960	Facing slowness when accessing web application through Authorization-only access post upgrading to Ivanti Connect Secure OS 9.0R5.

Problem Report Number	Summary
PRS-381963	Group Names in the role mapping rule will get added with &, # and; special character if more than 5 groups are selected with AD as the auth server.
PRS-381984	The cookie setting should be included in the resource profile.
PRS-382001	UI: Description incorrect on default deny in 9.1R3 initial deployment.
PRS-382021	Button to dismiss the banner on Ivanti Policy Secure/Ivanti Connect Secure Dashboard for not accepting Perpetual license is not working.
PRS-382031	Need to replace VA-SPE|PSA-V in "Only EVAL licenses are allowed for manual installation in VA-SPE|PSA-V".
PRS-382035	Proper logging for NFQUEUE full and drops needed, also consider this situation for cluster A/P failover or add to healthcheck.
PRS-382191	Unable to ping the IPv6 VLAN-Gateway from the Ivanti Connect Secure device after changing the Gateway address.
PRS-382240	User dropped from the VPN tunnel connection ##g_dhcp_proxy_ wbuf is maxed!.
PRS-382350	Unknown RAID status in PSA7000f due to no space left on device.
PRS-382804	Active node went unresponsive in A/P cluster and generated multiple Watchdog snapshots.
PRS-384939	“Invalid EKU text” error found while configuring "E-mail protection" under EKU text.
PRS-384963	Host checker: After upgrading to 9.1R3, HC "Successfully loaded" message is garbled when it is initiated in browser with Japanese language.
PRS-384967	healthcheck.api showing incorrect MAXIMUM-LICENSED-USER-COUNT in AA cluster.
PRS-385144	Web Rewrite: Images not loading on the web page for a web resource configured via rewrite.

Problem Report Number	Summary
PRS-385150	Access via SSH port forwarding fails.
PRS-385159	Home page of eTime (Timesheet) Web application is not rendering properly via Rewrite in all web browsers.
PRS-385203	Add iOS check for 13.2, 13.2.1, 13.2.2.
PRS-385496	Adding default policy for Citrix resources.
PRS-385500	VLS should use only MSP Authcode for registering with PCLS.
PRS-385526	Add iOS Check for 13.2.3.
PRS-385550	Users cannot see full display of shared screen, if the size of text, app and other items in the "Scale & layout" in Display settings is set to 150% (Recommended) on the client's machine.
PRS-385721	Unable to restore Local User Accounts Backup on Ivanti Connect Secure 9.0R5.
PRS-387517	DanaLoc appears to be missing when using IE11.
PRS-387541	Web Rewrite: Drop-down menu, Refresh button, Change Password option and Login button not working on the login page.
Release 9.1R3 PRs	
PRS-366490	System| Temperature status value on SNMP server displaying wrong value.
PRS-371351	Citrix sessions drop regularly causing various issues. These issues are observed in Ivanti Connect Secure 9.0 with Citrix port 2598 via JSAM. This issue is not found in 8.2R8.
PRS-371699	Users unable to login as well as dropping users - LMDB full.
PRS-372805	Realm level certificate restriction skipped with SAML Auth.
PRS-372999	Host checker is failing for Host Checker (OS-Check only) for Chrome OS 71.0.3578.127 with Ivanti Connect Secure 9.0R1 firmware version.
PRS-373160	Dropdown option misses internal menu while accessing via web rewrite.

Problem Report Number	Summary
PRS-374124	VDI Session are not showing under Virtual Desktop Sessions.
PRS-374146	UNC path is not handled properly by HOB Applet.
PRS-374318	Ivanti Connect Secure deployed on the AWS Cloud showing speed 10 Mbps.
PRS-374344	Last core dumps being generated at customer after 9.0R2.1HF6 with fixes.
PRS-374603	Syslog missing event logging info when upgrading.
PRS-374765	PSA7000f RAID failed after upgrading.
PRS-374831	Login page is not rendering properly for a web resource configured through rewrite.
PRS-374992	Ivanti Connect Secure using DUO as secondary authentication fails the first authentication attempt after installation.
.PRS-375079	CORE.fqdnacl crashes continues to occur even after 9.0R2.1HF6 (with fix).
PRS-375880	None of the contents in the Azure web portal are loading through rewrite.
PRS-375906	Unable to load a sign-in page getting stuck in loading the web page while accessing a web resource configured through the rewrite.
PRS-376036	Ivanti Connect Secure evaluation of the custom expression "time.dayOfYear" is not working as expected.
PRS-376247	Factory-reset does not work in 9.1R1 instead it boot up Ivanti Connect Secure with current image.
PRS-376249	Logon page of SAP fiori portal displayed as blank in IE11 only via rewrite.
PRS-376343	Mails are not getting synced in Native Email Client in iOS when using SA as ActiveSync Proxy due to stale records present and crash is happening in aseproxy-server service.
PRS-376357	When extending Pulse Client sessions, it causes network drop.

Problem Report Number	Summary
PRS-376429	JSAM stuck on loading forever on IE - Java.
PRS-376458	HOB stuck on loading forever on IE - Java.
PRS-376500	Azure 9.0R3.1 - postgresd service restarts constantly after deployment.
PRS-376520	Host checker fails to detect FireEye Endpoint Agent 29.7.0.
PRS-376840	Running Add command when the Disk is missing will cause a minor error message which requires a reboot.
PRS-376869	Dns_cache process snapshots persist after upgrading to 9.0R4HF6.
PRS-376953	Unable to view PDF files in the myDocuments application.
PRS-377022	File Share accessing issue in 9.0R4.
PRS-377160	HTML-5 -RDP requires additional authentication.
PRS-377482	After upgrading to 9.1R1, host checker word is garbled when it is initiated in browser with Japanese language.
PRS-377681	PSA7000f reports HDDs missing and inactive after upgrade to 9.1R1.
PRS-377825	After upgrading to 9.1R1, the name of the user role displayed in submenu is broken if the language is in Korean.
PRS-377979	When accessing the resources via bookmark, contents are not displayed correctly.
PRS-378049	Failed filesystem integrity check message seen on PSA5K console after upgrading from 9.1R1 to 9.1R2-2119.
PRS-378882	Periodic Snapshot settings via REST fails with error "Modification of Attribute not Allowed".
PRS-378964	When the admin clicks on 'Agent', they receive an error "the page you requested could not be found".
PRS-379125	Pulse One 2.0.1901: With Ivanti Connect Secure 9.0R5 (EA) having failure in target importing SAML using Artifact - empty "Source Artifact Resolution Service URL".

Problem Report Number	Summary
PRS-379336	Chat option not working on the Medical application.
PRS-379773	Syslog - If an appliance is rebooted, it cannot successfully reconnect to a P1 syslog server.
PRS-379974	Critical Events do not get displayed in System > Overview Page.
PRS-380009	REST API calls failing for RDWeb Profiles in Ivanti Connect Secure.
PRS-380148	When syslog server's FQDN resolves to two IP addresses, one of which is reachable, Ivanti Connect Secure/Ivanti Policy Secure may fail to connect.
PRS-380762	Delay during session failover of Ivanti Connect Secure in Active/Active cluster in AWS.
PRS-381014	Japanese words are garbled when we click on the File share bookmark.
PRS-381318	DMI get-config of RDWeb resource profile returns badly formed XML.
Release 9.1R2 PRs	
PRS-367907	FQDNST denied IP is going via tunnel.
PRS-370210	Clear config on PSA 300 fails with unable to mount /webserver partition.
PRS-372439	Post failover, session resumption delayed with Pulse Client.
PRS-373290	Clear config on PSA 300 fails with unable to mount /webserver partition.
PRS-375013	Radius OTP as Secondary authentication fails for the Pulse Client.
PRS-375329	HOB failed to launch through Java in IE.
PRS-375886	JSAM launch failing for IE -JAVA.
PRS-376312	Factory reset from VMware VA console does not load the factory reset version and loads the current version.
PRS-376348	VMWare View 5.1 client does not connect after upgrade.

Problem Report Number	Summary
PRS-376859	Premier Java Applet for Terminal Service failed to download .jar file.
PRS-377945	Publishing for certain block types causes many log messages and other side effects.
Release 9.1R1 PRs	
PCS-5064	Remove legacy mode from Active Directory auth. server.
PRS-375534	JSAM Stats value (Bytes count) is not getting displayed in IE - Activex.
PRS-375067	DNS resolution not working for alternate VPN connections.
PRS-374597	The definition update is not listed for Sentinelone product in "epupdate_hist.xml" file.
PRS-374057	Unable to add the resource <userAttr.Framed-Route> in IPV4 address under Split tunneling policy for Ivanti Connect Secure version 9.0Rx.
PRS-374037	Rewrite: PSAL launching Citrix app multiple times in an infinite loop on all the browsers.
PRS-373948	Contents of a web response are not getting compressed as content encoding header is missing in the response from Ivanti Connect Secure.
PRS-373769	Host Checker IMC detects the Antivirus Change in the client PC and report it to IMV even when Perform Check every min is set to 0.
PRS-373696	Split tunneling FQDN policy with special character, fails to save.
PRS-370953	Unable to edit word documents hosted on SharePoint 2013 via PTP using MS Edge.
PRS-371023	Resource access dropped (RDP, SSH etc.) intermittently on SAW environment.
PRS-373102	Core Access: E-mail web page getting stuck on "login processing".
PRS-373076	Core Access:Web page shows horizontal scrollbars at the bottom of screen.

Problem Report Number	Summary
PRS-372181	DanaLoc fails in case of old window object reference from a new window object.
PRS-372834	PSAM:Pulse SAM takes at least 40 seconds to open custom start up page in UI Options compared to WSAM.
PRS-372677	AAA/Security/Pulse: SAML AuthnRequest leaks data across users with "Reuse NC/Pulse session" enabled.
PRS-372595	User getting same IP address assigned from IP pool in few hours.
PRS-372489	Pulse browser Toolbar is flickering when accessing OWA 2016 resource on iOS device through webrewrite.
PRS-372285	PSA 7000f Frequently reports one of the power supplies is back up.
PRS-372055	Unable to save Citrix listed application using Hostname with port number.
PRS-371973	HC: Compliance fails using Pulse Desktop client 9.0.2 build 1151.
PRS-371970	Users with username in UPN format in System Local Authserver are unable to log in using TOTP after upgrading to 9.0R3.
PRS-371944	Killed user session admin log "ADM23534" does not display admin user but the actual user being terminated.
PRS-371800	Ivanti Connect Secure device is unable to get the enrolled mobile device attribute from MDM server.
PRS-371394	Setting the hash property of location object causes problem in IE, Edge and Firefox browsers because the URL is appended with fragment identifier. In chrome and Safari browsers things work fine.
PRS-371602	Post upgrade to Ivanti Connect Secure 9.0R3, "License server low-level protocol error Code = [47]" error is triggered on license client.
PRS-371513	Page does not load via IE browser.
PRS-371406	"Auto populate domain information" behavior when unchecked: blank first then if wrong password, auto populates domain.
PRS-371357	HTML5 RDP logging do not show realm and shows ().

Problem Report Number	Summary
PRS-371342	Add iOS Check 12.1.1.
PRS-371266	Menu is not loading when accessing the application through web-rewrite.
PRS-371231	Ivanti Connect Secure 9.0 VA-DTE :: Nodes in cluster gets disabled automatically.
PRS-371205	Multicast Traffic not working intermittently in the VPN Tunnel in 8.3R6 / 5.3R6 version and after restarting services, works fine for all users.
PRS-371154	Wrong information in the log messages for Authorization Only Access when source ip restriction is configured on role.
PRS-371114	Add support for adding parameters “client-name’ for HTML5 Access.
PRS-369351	LDAP authorization does not work when using ikev2 tunnel (handle 10K tunnels+few hundred ikev2 clients).
PRS-370138	Read-only admin sessions see an option as disabled that is actually enabled on user roles.
PRS-369960	Page displayed while PSAL downloads to a Mac client shows instruction for Mac; but then references Windows System Tray.
PRS-369200	Logs are not fully displayed if select the date as filter.
PRS-369142	File browsing SSO is not working with user details are given in variable form as well when configured to use system credentials.
PRS-369031	When a configuration object is renamed, not all of the resulting configuration changes are uploaded to Pulse One.
PRS-368927	Web process crashes and logs "ERR31093: Program web recently failed." in the event logs.
PRS-367879	Core Access: Unable to import or download the image using PTP.
PRS-367789	DMI agent not responding to netconf commands as expected.
PRS-367285	System| Active/Passive cluster responding to ICMP request even after shutdown.

Problem Report Number	Summary
PRS-366634	Randomly users are not able to access IPv6 resources through VPN device via VPN tunneling.
PRS-364219	PSA7000f interface status in Network Settings not working.
PRS-366490	System| Temperature status value on SNMP server displaying wrong value.
PRS-371351	Citrix sessions drop regularly causing various issues. These issues are observed in Ivanti Connect Secure 9.0 with Citrix port 2598 via JSAM. This issue is not found in 8.2R8.
PRS-371699	Users unable to login as well as dropping users - LMDB full.

Known Issues

The following table lists the known issues outstanding from previous releases:

Problem Report Number	Release Note
Release 9.1R18.7 PRs	
PRS-417388	**Symptom**: RADIUS service crashes. **Condition**: When logging to ICS through RADIUS. **Workaround**: None.
Release 9.1R18.6 PRs	
No new known issues in this release.	
Release 9.1R18.5 PRs	
No new known issues in this release.	
Release 9.1R18.4 PRs	
No new known issues in this release.	
Release 9.1R18.2 PRs	
PRS-417604	**Symptom**: Virtual ports are not getting mapped automatically to the certificates. **Condition**: when the config is imported. **Workaround**: Map the certificates to the virtual ports manually.
PRS-416867	**Symptom**: Re-valuation of the policies fail on ICS. **Condition**: When user connects through browser. **Workaround**: None.
PCS-44327	**Symptom**: JITC remains enabled when NDcPP and FIPS are in disabled state. **Condition**: When JITC is disabled through console. **Workaround**: Disable the JITC option manually.
Release 9.1R18.1 PRs	
PCS-43061	**Symptom**: Error message is observed once the user log's out. **Condition**: When JSAM with JDK 21 beta version is used on Windows 11 and Mac. **Workaround** : Use JSAM with JDK 17 on windows and Mac OS(Sonoma and Ventura)

Problem Report Number	Release Note
PCS-38894	**Symptom**: Advanced html5 external storage feature will not work. **Condition**: When external storage server contains special characters in the password. **Workaround**: Do not use any special characters in the password.
PRS-416513	**Symptom**: Pulse One sees a configuration change for each end- user login. **Condition**: Due to ICS Sync with Auth servers and reload of end-user configurations. **Workaround**: Add user information to exception list.
Release 9.1R18 PRs	
PCS-41217	**Symptom**: Errors while uploading configuration to ICS. **Condition**: When multiple client packages are available. **Workaround**: Ivanti recommends having only one client package.
PCS-41115	**Symptom**: JSAM logout button throws an internal error message. **Condition**: When open jdk-17 java is installed **Workaround**: No feature impact, click the ok button on the error screen JSAM applet will logout.
PCS-40829	**Symptom**: Citrix listed applications “Failed to connect” message is seen. **Condition** : When SSO is not configured under bookmark page. **Workaround** : Configure the SSO under bookmark page.
PCS-40794	**Symptom**: Launching the Web bookmark via JSAM has issues. **Condition**: When the PSAL is not installed on the client machine. **Workaround**: Create web bookmark to launch via the rewriter engine instead of JSAM.
PCS-39889	**Symptom**: Sometimes session disconnection is observed. **Condition**: When VPN session is left idle for long time without any data transfer. **Workaround**: Disconnect and reconnect the session.
PCS-39791	**Symptom**: Citrix Storefront with CTS client will not launch. **Condition**: When PSAL extension is enabled. **Workaround**: Disable PSAL extension, CSF-CTS client will launch.
PCS-39684	**Symptom**: ICS active users page shows agent type as "Windows 10 Firefox" **Condition**: When user connects from Windows server 2016 Firefox browser.

Problem Report Number	Release Note
	Workaround: None.
PCS-38334	**Symptom**: On a Mobile device, VPN Client fail to establish VPN connection. **Condition**: VPN Client is not connecting to VPN and receiving fatal error from server when session options configured as Idle Timeout: 5, Session Time out: 6 and Reminder Time: 3 **Workaround**: Configure Session Time out as 10 or greater.
PRS-414656	**Symptom**: 9. x ICS 2. x kernel is not supported on the cloud platforms. **Condition**: When 9.x ICS is used on Azure and AWS cloud platforms. **Workaround**: Ivanti recommends to migrate to 22.x ICS.
Release 9.1R17.1 PRs	
No new known issues for this release.	
Release 9.1R17 PRs	
PCS- 39645	**Symptom** : VDI client launch is not working. **Condition** : When upgrading the client from 9.1R15 to 9.1R17 with PSAL extension enabled. **Workaround** : Re-install VDI launch .
PCS-39641	**Symptom** : Intermittently during the Client launch and upgrades, PSAL is not detected in the first attempt. **Condition** : During fresh install or upgrade of client. **Workaround** : Re-launch client.
PCS-39512	**Symptom** : JSAM auto launch is not working. **Condition** : When Host checker is configured. **Workaround** : Manually launch JSAM.
PCS-39271	**Symptom**: Unable to delete the selected username data from Behavioral Analytics User Report **Condition**: When compliant users are listed in the report. **Workaround**: None.
PCS-39227	**Symptom**: After launching JSAM an error displays, "Safari can't find the server." **Condition**: When a user launches JSAM on a MAC Ventura machine using the Safari browser

Problem Report Number	Release Note
	Workaround: Use Chrome browser to launch JSAM
PCS-39265	**Symptom**: HOB auto launch is not working. **Condition**: When Windows is running on a client machine. **Workaround**: Launch manually.
PCS-39073	**Symptom**: JSAM is not launching with a browser extension on MAC devices. **Condition**: Using JSAM and HOB when Browser extension is enabled. **Workaround**: Use custom protocol.
PCS- 38955	**Symptom**: FTP is not working with IPv6 FTP server. **Condition**: When IPv6 FTP server is configured for archival. **Workaround**: Use IPv4 FTP server for archiving.
PCS-38731	**Symptom**: Enterprise onboarding profile push will not work on mobile end point. **Condition**: When a new VPN client is installed on the Mobile end point. **Workaround**: By using MDM server required profiles can be pushed to the mobile end point.
PCS-38455	**Symptom**: Only 'Citrix listed applications' bookmarks is shown in the user home page. **Condition**: when 'Citrix listed applications' is the 1st entry in Users->User Roles->[User-Name]->Terminal Services->Sessions. **Workaround**: Avoid 'Citrix listed applications' as the first entry. Reorder the Terminal Services Sessions from Users->User Roles->[User-Name]->Terminal Services->Sessions page using up-down arrows.
PCS-38218	**Symptom**: Displays error “Failed to contact server , Please check the network connection and try again”. **Condition**: During XML export and import of “Citrix All Listed Application” along with other Citrix bookmarks **Workaround**: Delete the “Citrix all listed application” bookmark and recreate manually using Terminal profile through admin login.
PCS-37845	**Symptom**: VDI-Citrix Xendesktop launch fails. **Condition**: When a user uses Citrix workspace app 2112 or later. **Workaround**: Use Citrix workspace app version 2109.
PCS-37839	**Symptom**: Citrix default ICS launch fails.

Problem Report Number	Release Note
	Condition: When a user uses Citrix workspace app 2112 or later. **Workaround**: Use Citrix workspace app version 2109.
PCS-36999	**Symptom**: Oauth authentication fails in the end user page while using dynamic URL. **Condition**: When creating oauth server with dynamic URL and trying the authentication after upgrade. **Workaround**: 1. To delete existing Oauth configuration and create a new configuration in the latest version 2. Upgrade without using dynamic URL (with manual configuration)
Release 9.1R16.1 PRs	
No new known issues found in this release.	
Release 9.1R16 PRs	
PRS- 412081	**Symptom**: Not able to launch JSAM and PDC client. **Condition**: When an end-user tries from Client Apps page. **Workaround**: Launch the clients from end-user home page.
PCS-37107	**Symptom**: Usernames with special characters sometimes may not get updated in the Named Users Database on the License Server. **Condition**: When Named Users Remote Repo mode is enabled on License Server Username with special characters tries to login to a gateway registered with the License Server **Workaround**: None.
PCS-37024	**Symptom**: Client launch fails on upgrade. **Condition**: When browser extension is enabled. **Workaround**: Reinstall PSAL.
PCS-36513	**Symptom**: When the User Record sync is enabled across nodes and end user creates a HTML5 bookmark in one node .Further when the same enduser logins to other node the created HTML5 bookmark is not present. **Condition**: When User record sync is enabled and enduser creates HTML5 bookmark. **Workaround**: None.

Problem Report Number	Release Note
PCS-36442	**Symptom**: "Failed to contact server" error observed sometimes when auto-launch is enabled. **Condition**: When auto-launch is enabled. **Workaround**: None
PCS- 36282	**Symptom**: JSAM launch is failing for intel-based MAC system with error stating one of the library file may be malicious. **Condition**: JSAM launch fails. **Workaround**: None.
PCS-36088	**Symptom**: RPM based PSAL download instead of DEB based PSAL download in a Debian system. **Condition**: Client installation will not work for Debian based Linux like Ubuntu. **Workaround**: None
Release 9.1R15 PRs	
PRS-408726	**Symptom**: HTML5 Session recording file is not uploaded to SMB server. **Condition**: When the SMB-Server is on a different VLAN than that of ICS. **Workaround**: None.
PRS-408091	**Symptom**: For non-existing remote machine ACL check is passed. **Condition**: When end-user access HTML5 bookmark of non-existing RDP remote machine. **Workaround**: None.
PRS-407815	**Symptom**: Garbled characters are seen in Virtual desktop bookmarks. **Condition**: When language is set as Chinese. **Workaround**: None.
PRS-406983	**Symptom**: PSAL not launched because RPM format PSAL file downloaded on Ubuntu machine. **Condition**: When Firefox version 91.5.0esr (64 bit) is used. **Workaround**: Use Firefox version 68.10.0esr (64 bit) to avoid PSAL launch issue.
PRS-404022	**Symptom**: Second Node upgrade is failing in Cluster setup. **Condition**: when upgrading through Pulse one. **Workaround**: None.

Problem Report Number	Release Note
PCS-35256	**Symptom**: Sometimes one of the nodes in AA cluster deployed in AWS will show as enabled and unreachable after upgrade. **Condition**: When upgrading ICS AA cluster deployed in AWS Environment to 9.1R15. **Workaround**: Reboot the instance in AA cluster from AWS.
PCS-35098	**Symptom**: In end user page Pulse collaboration is shown in the Preferences -> Advanced -> Under upload logs. **Condition**: When admin enabled client-side logging. **Workaround**: None.
PCS-34927	**Symptom**: XML Export for OAuth Servers is missing Traffic port selection settings. **Condition**: Traffic port selection is configured to be at Auth Server Level. **Workaround**: Configure Port Selection for OAuth Server from Admin UI as desired.
PCS-34915	**Symptom**: Role names are not showing for telnet/ssh and unix bookmarks in deprecated list during upgrade for roles configured with telnet/ssh and unix features bookmarks and didn't enable it in roles. **Condition**: Roles configured with telnet/ssh and unix bookmarks and didn't enable telnet/ssh and unix in that role. **Workaround**: Admin has to check for the role and delete the bookmarks.
PCS-34876	**Symptom**: In New Sign-In Policy page meeting content is shown. **Condition**: When admin creates a new sign in policy. **Workaround**: No functionality impact. Ignore the text.
PCS-34845	**Symptom**: ICS client fetches meeting license from the license server. **Condition**: When license server is used to fetch the license. **Workaround**: No functionality impact. Ignore the text.
PCS-34844	**Symptom**: Meeting related information is shown in SNMP MIB file. **Condition**: In the SNMP MIB file. **Workaround**: No functionality impact. Ignore the text.
PCS-34827	**Symptom**: If upgrade (using REST API/DMI/Pulse ONE) fails due to presence of deprecated features, the list of deprecated configurations is not given in upgrade failure message.

Problem Report Number	Release Note
	Condition: When upgrade is done through web UI, a list of deprecated configuration elements to be removed is displayed in the upgrade failure message. - For upgrades through REST API/DMI/PulseOne, the upgrade failure message does not give the list of deprecated features to be removed. **Workaround**: - The list of deprecated features gets displayed in the serial console. - Admin needs to check the serial console for details.
PCS-34694	**Symptom**: Interface is getting disconnected. **Condition**: On configuring static link speed (not Auto), the link is getting disconnected. **Workaround**: The link speed can be set as 'Auto'.
PCS-34528	**Symptom**: Enable Pulse Collaboration integration on this connection is shown in Pulse secure SA connection page. **Condition**: In the SA connection page. **Workaround**: No functionality impact. Ignore the text.
PCS-34322	**Symptom**: ICS on continuous reboot when enabling "Clear all configuration data at this device". **Condition**: When option is enabled. **Workaround**: On admin UI, disable the option under System Maintenance --> Options --> Clear all configuration data at this device.
PCS-33741	**Symptom**: LS cluster: Admin sessions are not getting synced. **Condition**: AA cluster gets set to config-only cluster. **Workaround**: None.
PCS-33735	**Symptom**: Unable to run /etc/adjtimex.sh seen on ICS console on upgrade to 9.1R15. **Condition**: This message is seen predominantly on VMware ESXi. **Workaround**: None.
PCS-33719	**Symptom**: Unable to change VLS cluster type from Active-Passive to Active-Active. **Condition**: When creating cluster on VLS. **Workaround**: None.
PCS-32543	**Symptom**: Pushing sign-in URLs, notifications and pages not supported. **Condition**: When creating any sign-in settings with URL.

Problem Report Number	Release Note
	Workaround: None.
Release 9.1R14 PRs	
PRS-405889	**Symptom**: When creating an Advanced HTML5 RDP bookmark, "Fetch Domain" does not retrieve domain name. **Condition**: When the AD-Server for which the domain is being retrieved is on a different VLAN than that of ICS. **Workaround**: Enter the domain name manually.
PRS-404087	**Symptom**: when end user access L7 rewriter applications and click Home, end user sees "The requested resource is not valid." **Condition**: When Referrer Header Validation under Configuration > Security > Miscellaneous is enabled. **Workaround**: Admin can configure to enable the options to open bookmark in new window or new tab under User role settings for rewriter applications
PRS-404859	**Symptom**: Unable to download the file of type .ps1 with the Advanced HTML5 session. **Condition**: When using chrome browser. **Workaround**: Use Firefox browser.
PRS-405631	**Symptom**: JSAM, Pulse collaboration, Telnet/SSH clients is not working. **Condition**: When client machine is a M1 MacBook **Workaround**: None.
PRS-405680	**Symptom**: The Advanced HTML5 connections graph in the admin UI Overview, takes more time than the duration mentioned in Refresh Interval to display the correct values. **Condition**: When users initiate or close one or more Advanced HTML5 connections, the sessions tab reflects these changes immediately, but takes longer than expected to reflect in the graphs. **Workaround**: None.
PRS-398596	**Symptom**: Modifying IP config using console with VLAN interface fails. **Condition**: After setting Default VLAN ID, when trying to modify, the IP config values are not reflected in cache. **workaround**: None.

Problem Report Number	Release Note
PRS-399744	**Symptom**: XML export/import fails **Condition**: When name field of roles have nested square brackets. **Workaround**: Make sure we rename with no square brackets as workaround.
PCS-31688	**Symptom**: Audio does not work with Google Chrome on Citrix Desktop. **Condition**: When Google Chrome running on Citrix desktop is accessed from PCS browser interface using VDI bookmark. **Workaround**: Pass "--disable-features=AudioServiceOutOfProcess" as arguments when starting Google Chrome. Example: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-features=AudioServiceOutOfProcess Ref: https://discussions.citrix.com/topic/406285-chrome-79-no-audio/page/2/
PCS-31598	**Symptom**: Advance HTML5 user is shown "Number of Advanced HTML5 connections for this session has reached the maximum allowed limit. Please close any unused session(s) and retry." even though user does not have 5 Advanced HTML5 connections. **Condition**: Network disconnect on user side or server side. **Workaround:** Retry after 15 minutes. The connections become available within 1 to 15 minutes from the time of network disconnect.
PCS-31168	**Symptom**: Sometimes WSAM resources is accessed through PCS even though resources has denied in PSAM policy. **Condition**: When changing PSAM/WSAM policy from allow to deny. **Workaround**: None.
Release 9.1R13.1 PRs	
PCS-29121	**Symptom**: Toolbar not visible for bookmarks in PTP mode when using Chrome and Edge browsers. **Condition**: Condition: When web bookmark is configured to access over PTP mode instead of rewriter mode. **Workaround**: Open Ivanti Connect Secure home page URL in a new tab to see the toolbars again. If opening through bookmarks from Ivanti Connect Secure home page, select to open in new tab using right click.
PCS-31811	**Symptom**: UI shows ISA concurrent users for an existing 9.x license client.

Problem Report Number	Release Note
	Condition: When editing an existing 9.x license client on license server running 9.1R13.1. **Workaround**: Ignore the ISA concurrent users field. Leasing functionality is not affected.
Release 9.1R13 PRs	
PRS-404800	**Symptom**: Display of messages like "unregister_netdevice: waiting for tun_0_327 to become free. Usage count = 1". **Condition**: When IPv6 is configured. **Workaround**: None
PRS-403498	**Symptom**:OS check passes on latest Windows 11 machine when checks are configured for "Windows 10-64-Bit". OS check will pass on Windows 10 machine when checks are configured for latest "Windows 11-64-Bit". Windows 11 (preview version) returns version string as Windows 10 in the kernel. **Condition**: OS check policy for Windows 11 systems. **Workaround**: NA
PRS-403270	**Symptom**: Telnet/SSH bookmarks are not working on Windows 11 as IE is deprecated. **Condition**: When using Windows 11 as client machine and accessing Ivanti Connect Secure through browser. **Workaround**: Access Telnet/SSH bookmarks using HTML5 solution.
Release 9.1R12.1 PRs	
No new known issues found in this release.	
Release 9.1R12 PRs	
PRS-402731	**Symptom**: In A/P Cluster, users might notice a delay in the VPN session resumption when restart service triggered on cluster by Admin. **Condition**: In A/P Cluster, delay in user VPN session resumption happens when Admin does restart services on cluster. **Workaround**: It is a delay in session resumption and session shall resume after some time. Admin can restart services during the maintenance window.

Problem Report Number	Release Note
PRS-401279	**Symptom**: Downloading files with 6in4 and 4in6 not working properly in PSA hardware whereas 4in4 and 6in6 are working. **Condition**: ESP mixed mode configured on HW. **Workaround**: Disable "Use ESP tunnel for 6in4 and 4in6 traffic" in Configuration --> VPN Tunneling.
PCS-28369	**Symptom**: VMware tools version shows as Unsupported Older Version. **Condition**: When Ivanti Connect Secure is deployed on ESXi version 7.0. **Workaround**: None. Functionalities such as Reboot, Shutdown, Power Off, NTP sync will continue to work without any issues.
Release 9.1R11.5 PRs	
No new known issues found in this release.	
Release 9.1R11.4 PRs	
PRS-400951	**Symptom**: Static IP allocation fails for both single and multi-session enabled users. **Condition**: Overlapping IP pools are configured in VPN profile. **Workaround**: If the overlapping IP pool is broken up/split up this issue is not seen.
PRS-400802	**Symptom**: Static IP allocation fails for both single and multi-session enabled users. **Condition**: Users having multiple preferred IP addresses and/or multiple users assigned same preferred IP address. **Workaround**: None.
PRS-400668	**Symptom**: Pulse Desktop Client (PDC) always displays upgrade prompt even when client version on the endpoint and the server are same. Clicking on upgrade prompt performs no action (Cosmetic/UI issue). **Condition**: Occurs when the Pulse Desktop Client has Symantec signed binaries and the Ivanti Connect Secure on which it is hosted (9.1R11.3/ 9.1R10.2/ 9.1R9.2/ 9.1R8.4) is signed by Digicert. **Workaround**: Disable End-point upgrade on Ivanti Connect Secure (Ivanti Connect Secure). Enable again only when a higher version of PDC is activated on Ivanti Connect Secure and let the users trigger the client upgrade through the browser.

Problem Report Number	Release Note
PRS-400639	**Symptom**: Sometimes back-end resources are not accessible over L7 VPN. **Condition**: When both L3 & L7 VPN are connected. **Workaround**: Disconnect the L3 VPN & access back-end resources. Connect back to L3 VPN.
Release 9.1R11.3 PRs	
PRS-400509	**Symptom**: The PSAL installation prompts for admin credentials on windows 8.1 for Local user. **Condition**: On Windows 8.1 Endpoints. **Workaround**: Right click on the PSAL **msi**->**Properties** and enable Unblock. Click **Apply** and **OK**. Then install the PSAL.
PRS-400486	**Symptom**: Upgrade prompts missing on connecting to latest Ivanti Connect Secure. **Condition**: When endpoint has PSIS Installed. **Workaround**: Uninstall PSIS.
Release 9.1R11 PRs	
PRS-399842	**Symptom**: Pulse client is assigned an IP address from static pool while configuration is to prefer IP from LDAP/Radius attribute. **Condition**: LDAP/Radius attribute template and static IP address/range is configured in a single user profile as resources. **Workaround**: Split the connection profile into multiple profiles like one Profile with LDAP/Radius attributes/resources and other configuration and another profile with static IP address/range and other configuration. The new profiles can be ordered correctly to maintain the expected order of resources.
PRS-398121	**Symptom**: User sessions are not syncing with one of the node in Active-Active cluster. **Condition**: LMDB related error messages observed. **Workaround**: Clear session data.
Release 9.1R10 PRs	
PRS-397064	**Symptom**: For advanced HTML5 sessions, on administrator UI shows IP address instead of hostname under virtual desktop sessions page. **Condition**: When an advanced HTML5 bookmark is configured with a hostname.

Problem Report Number	Release Note
	Workaround: None.No functionality impact.
PRS-396895	**Symptom**: For basic HTML5 connections file transfer is not working on macOS. **Condition**: When a basic httml5 bookmark is accessed by using Safari browser. **Workaround**: Access basic html5 bookmark using chrome browser.
PRS-396726	**Symptom**: Active user page “Agent Type” shows “Mac OS 10.15" in place of “Mac OS 11.0.1". **Condition**: When using Safari on macOS version BigSur 11.0.1. **Workaround**: None.
PRS-396499	**Symptom:** For advanced HTML5 connections, graph shows invalid values. **Condition:** When user access advanced HTML5 bookmarks. **Workaround:** Check the HTML5 session count on the virtual desktop sessions page.
Release 9.1R9.1 PRs	
PRS-396606	**Symptom:** Ctrl+C (abort) command is not working for advanced html5 sessions. **Condition:** When user access Putty SSH session within Windows 10VM through advanced html5 bookmark. **Workaround:** None.
Release 9.1R9 PRs	
PRS-395925	**Symptom:** “IP Owned by device with HWADDR” messages at MAJOR level seen in Admin logs after upgrade to 9.1R9. **Condition:** These messages are seen during the following sequence: 1. Active Passive Cluster upgrade (Example: Node-1 and Node-2) 2. Upgrade started on Node-1. Node-1 with upgraded version is starting up. 3. Node-2 holds the VIP, till it goes for a reboot. **Workaround:** None. These messages do not cause any impact to the cluster functionality.
PRS-395911	**Symptom:** Pull state from server not leasing licenses to all the nodes in cluster. Following event logs are seen: E.g.: 2020-10-19 17:25:01 - DFS_VA_NODE_115_19 - [127.0.0.1] Root::System()[] - Lease request on behalf of DFS_VA_NODE_115_20 by DFS_VA_NODE_115_19 failed: Not Cluster Member, status code=0x22..

Problem Report Number	Release Note
	Condition: When, occasionally, both the cluster nodes talk to license server to fetch the license clients. **Workaround:** 1. Do XML export of license clients. 2. Delete the affected license clients using admin UI. 3. Re-import the license clients from XML file.
PRS-395722	**Symptom:** For existing HTML5 profiles configuration through REST may not set solution type properly always. **Condition:** While updating the existing HTML5 profile solution type. **Workaround:** Create new profile through REST API.
PRS-395711	**Symptom:** For Advanced HTML5 user's Zoom sessions, audio stream can be inconsistent. **Condition:** When Zoom application is used for meeting session over Advanced HTML5 session. **Workaround:** Use Microsoft Teams application.
PRS-395707	**Symptom:** For Advanced HTML5 RDP sessions, Microsoft Teams video call might disconnect the session. **Condition:** When making a Microsoft Teams video call in Advanced HTML5 RDP session. **Workaround:** None.
PRS-395703	**Symptom:** For Advanced HTML5 sessions, some documents may not invoke print function properly. **Condition:** When printing a text document with Notepad++. **Workaround:** Use default document mode.
PRS-395223	**Symptom:** REST based import of user role fails with the following error: "/sam/sam-options/wsam-autoinstall] Unsupported attribute type 0". **Condition:** 1. User role config obtained from Ivanti Connect Secure running pre-9.1R9 through REST. 2. Admin uses REST PUT|POST to import the config from Step 1 on Ivanti Connect Secure running 9.1R9. **Workaround:** Replace wsam-autoinstall with wsam-autouninstall and use REST based import.

Problem Report Number	Release Note
PRS-393672	**Symptom:** Noticeable slowness seen in upgrade from 9.1R4 to 9.1R8 on AWS platform. **Condition:** When the load on data center is high. Also, depends on the network parameters in the given zone. **Workaround:** Please plan upgrades with sufficient upgrade window.
Release 9.1R8.2 PRs	
PCS-22360	**Symptom:** SAML SLO is not initiated from Ivanti Connect Secure to its IDP when the user's browser-based session is ended. **Condition:** When user is authenticated using any browser to Ivanti Connect Secure with SAML authentication method where Ivanti Connect 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 Connect Secure Admin console. Currently only manual sign out from browser session is supported to send SLO request to IDP from Ivanti Connect Secure side. **Workaround:** Close the browser window and launch a new browser window, so that user is prompted for authentication again for security reasons.
Release 9.1R8.1 PRs	
No new known issues found in this release	
Release 9.1R8 PRs	
PRS-393174	**Symptom:** Local proxy PAC file not working in Internet Explorer 11. **Condition:** When PAC file resides on a local system. **Workaround:** Store the PAC file on an HTTP/HTTPS-accessible server and use that link for Internet Explorer 11 proxy settings.
PRS-393172	**Symptom:** Windows client connecting to Ivanti Connect Secure using Firefox ESR 68.10 intermittently throws error during Compliance check through Proxy configuration. **Condition:** Using Firefox ESR 68.10 version. **Workaround:** Once a successful connection is established from the client to the server using Chrome/IE, try connecting to the server using Firefox ESR. This works as expected.
PRS-392749	**Symptom:** Pulse collaboration client version is not same in Mac and Windows.

Problem Report Number	Release Note
	Condition: When user installs 9.1R8 Pulse collaboration client. **Workaround:** None.
PRS-392345	**Symptom:** Archiving on AWS S3 storage and Azure is failing when DNS server is not reachable from internal interface. **Condition:** When admin trying to Archive using AWS S3 bucket or Azure storage account on management port and DNS server is not reachable through internal port. **Workaround:** Admin has to configure internal port for DNS resolution, Archival interface can be internal/management for archiving on AWS S3 bucket or Azure storage account.
PRS-391947	**Symptom:** Websocket URL is not accessible. **Condition:** When trying to access https://web.whatsapp.com/ URL. **Workaround:** None
PRS-390577	**Symptom:** Active user page is not displaying node details correctly for the users connected in AA cluster after split and join. **Condition:** After cluster split and re-join. **Workaround:** Display issue, user sessions will not get impacted. Newly connected sessions are showing the details correctly.
PRS-390488	**Symptom:** Host checker is getting timed out (can be seen on user access log) and user is getting logged out. **Condition:** When periodic evaluation is enabled. **Workaround:** This issue is not replicable every time, but as a workaround, we have suggested to disable dynamic evaluation or increase the periodic policy evaluation interval.
PRS-384976	**Symptom:** Host Checker installation error found Intermittently while installing Host Checker or Pulse Client [HC enabled] through browser [Chromium Edge/Chrome/Firefox]. **Condition:** Fresh Installation of Host Checker or Pulse Client [Host Checker enabled] through browser [Chromium Edge/Chrome/Firefox] after uninstalling old Host Checker components **Workaround:**

Problem Report Number	Release Note
	• Uninstall the Host Checker/Pulse Client components manually and reboot the system. OR • Manually kill Host Checker process before installing Pulse Client/Host Checker components.
PRS-375138	**Symptom**: Client upload logs fails for Network Connect and JSAM. **Condition**: After launching Network Connect and JSAM on Windows 10, client upload log fails. **Workaround**: None
PCS-21262	**Symptom:** Update in PSAM Resource policies configuration from Admin portal is not getting applied immediately to existing users with UDP PSAM sessions. **Condition:** When Admin changes ACL action from Deny to Allow for a particular UDP based resource (i.e., UDP Server Application) for which user already has UDP PSAM Session active, user will still see access denied and vice-versa. But this condition might occur very rarely in real world scenario. **Workaround:** Admin can choose to delete existing UDP PSAM user sessions for which ACL action changes from Deny to Allow and vice-versa. Alternatively, user can disconnect and connect PSAM UDP based application session.
PCS-20664	**Symptom:** Pulse client is not showing correct error message when there is no bandwidth to allocate for L3 tunnel. Error message in Pulse client - "Unable to allocate IP address". **Condition:** When there is no bandwidth to allocate for L3 tunnel for that specific user. **Workaround:** Display issue, correct error message will get displayed in User Access logs. Error message in User Access logs - "Cannot find a qualified bandwidth management policy for user based on current available bandwidth."
Release 9.1R7 PRs	
Known issues found in this release are resolved.	

Problem Report Number	Release Note
Release 9.1R6 PRs	
Known issues found in this release are resolved.	
Release 9.1R5 PRs	
PRS-389742	**Symptom**: Cannot register the device with Intune to get SCEP profile that has IMEI as common name. **Condition**: The devices like Wi-fi only iPad / Wi-Fi only android tablets that do not have IMEI support or do not have IMEI. **Workaround**: None.
PRS-389737	**Symptom**: Cluster VIP is not getting migrated to other node when active node's internal interface is not reachable and external port is reachable. **Condition**: In AP Cluster configured with both internal and external port, when active node's internal port became unreachable. **Workaround**: Reboot the cluster node having issue with internal interface is unreachable.
PRS-389409	**Symptom**: User sessions will be removed for the session logged in at the time of second node upgrade in AP cluster. **Condition**: During AP cluster upgrade, when the first node comes up after upgrading newer version, it informs other node to upgrade. During this time if any new user logs in, then all those sessions will be removed after second node goes for upgrade. **Workaround**: User needs to re-login.
PRS-388121	**Symptom**: Reliable users may be prompted for secondary authentication despite Adaptive authentication being enabled for the realm. **Condition**: Adaptive Authentication feature may not work in some scenarios where nodes are in the cluster setup. **Workaround**: None.
Release 9.1R4.3 PRs	
No new known issues found in this release	
Release 9.1R4.2 PRs	
No new known issues found in this release	

Problem Report Number	Release Note
Release 9.1R4.1 PRs	
No new known issues found in this release	
Release 9.1R4 PRs	
PCS-18480	**Symptom**: Bookmark based access flow for Cloud based apps does NOT support MFA. **Condition**: When user tries to access any Cloud apps using Bookmark based flow, MFA based Conditional Access policies does Not work and will Deny the access to user. **Workaround**: Access Cloud apps using SP Initiated flow for MFA to work, or do NOT configure MFA for these Bookmark based Cloud apps.
PCS-18002	**Symptom**: Pulse Collaboration meeting is not getting launched with PSAL in macOS Catalina from the second time. **Condition**: In macOS Catalina, Pulse Collaboration meeting can be launched only after the fresh download of the client. If we try to relaunch the meeting, it is getting failed. **Workaround**: Delete the Pulse Collaboration client folder and perform a fresh download before launching the meeting.
PCS-17932	**Symptom**: TOTP server, Certificate server and SAML server authentication do not work for MFA based Conditional Access policy settings. **Condition**: When TOTP server, Certificate server and SAML server are configured as MFA server for Conditional Access. **Workaround**: Any other supported Authentication server can be configured as MFA server.
PCS-17926	**Symptom**: License report doesn't show the software version for one of the members cluster setup. **Condition**: When cluster is in license client **Workaround**: None (Display issue).
PRS-387697	**Symptom**: HOB launch on CentOS failing when Oracle JDK is installed. **Condition**: Oracle JDK installed on CentOS. **Workaround**: Install OpenJDK.

Problem Report Number	Release Note
PRS-387572	**Symptom**: AliCloud Ivanti Connect Secure-7K-V: Watchdog restarting cgi-server auth processes (cgi). **Condition**: Beyond 20K concurrent users under Pulse ESP and PSAM throughput test. **Workaround**: None
PRS-387499	**Symptom**: Hob auto-launch - PSAL failing with error "Failed to contact server". **Condition**: When auto-launch is enabled on HOB bookmark. **Workaround**: Disable auto-launch.
PRS-387452	**Symptom**: SSH does not work after restarting services in AWS and Azure. **Condition**: After performing restart services. **Workaround**: SSH works after a reboot.
PRS-387192	**Symptom**: Rewriter issues with SharePoint 2019 – a few buttons and icons does not load and rename file does not work. **Condition**: When using Ivanti Connect Secure web bookmark for the new SharePoint 2019 server. **Workaround**: Switch to Classic View in SharePoint 2019.
PRS-384976	**Symptom**: Host Checker error found Intermittently while installing Pulse Client via Chromium Edge browser in presence of Host Checker configured. **Condition**: Host Checker configured. **Workaround**: Click on Ignore button.
Release 9.1R3 PRs	
PCS-15327	**Symptom**: When trying to restart Ivanti Connect Secure from vCenter, Ivanti Connect Secure shuts down instead of restart. **Condition:** When trying to restart Ivanti Connect Secure using the Restart Guest option from vCenter. **Workaround**: Restart Ivanti Connect Secure using the PSA-V virtual console.
PRS-382259	**Symptom**: DNS address and domain names are taken from DHCP server when deploying new Ivanti Connect Secure instance in AWS and Azure. **Condition:** When passing DNS address and domain name as parameter for initial configuration, DNS address and domain name are taken from DHCP server. **Workaround**: Reconfigure DNS address and domain in network over view page.

Problem Report Number	Release Note
PRS-382085	**Symptom**: Not able to enable "copy/paste" option for end user created bookmarks after upgrade from 9.1R2 to 9.1R3. **Condition:** After an upgrade, not able to enable "copy/paste" option in the end user created bookmarks. **Workaround**: The user has to delete and create the bookmarks to enable "copy/paste" option.
PRS-382083	**Symptom**: Not able to enable "copy/paste" option via RDP launcher URL. **Condition:** When trying to enable "Copy/paste" option via RDP launcher URL. **Workaround**: • User should use admin created bookmark. • User should use end-user created bookmark.
PRS-382078	**Symptom**: AWS or Azure new Ivanti Connect Secure deployment fails when customer using old templates with admin password is less than 10 characters. **Condition:** When the template contains admin password with less than 10 characters. **Workarounds**: Customer has to provide admin password length with minimum of 10 characters.
PRS-381853	**Symptom**: Azure Ivanti Connect Secure - Network interface speed is showing as “Unknown” in the Network Overview page. **Condition:** When deploying new Ivanti Connect Secure instance in Azure, the network interface speed is showing as “Unknown” in the Network Overview page. **Workaround**: This is just a display issue.
PRS-381707	**Symptom**: Intermittently, Behavioral analytics dashboard page shows "Unable to connect to database" error. **Condition:** Sometimes, when admin navigates to Behavioral analytics dashboard page, "Unable to connect to database" error is seen. **Workaround**: Administrator can reload the Behavioral analytics dashboard page after some time to get the details on the page.
PRS-381554	**Symptom**: When File rule configured for validating a file location using System default Directories <%HOME%> policy evaluation failed on macOS 10.14x or any higher versions.

Problem Report Number	Release Note
	Condition: If file located at System Directories <%HOME%> and configured a Hostcheck policy with File Rule for macOS 10.14.x or higher versions. **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.
PRS-367403	**Symptom**: Pulse collaboration not getting launched in macOS. **Condition:** When the Java version above 8 is installed in the macOS, Pulse collaboration will not launch. **Workaround**: Use Java version 8 for launching the Pulse collaboration in macOS.
Release 9.1R2 PRs	
PRS-14530	**Symptom**: Shutdown of PSA-V deployed on KVM hypervisor does not complete. **Conditions**: • PSA-V is deployed on KVM hypervisor. • Shutdown is initiated from PSA-V virtual console. **Workaround**: None
PRS-374575	**Symptom**: DNS Search Order notes for macOS needs correction as Device only DNS is supported in macOS. **Condition**: macOS supports Device only DNS. **Workaround**: None
PRS-377549	**Symptom**: Older PSIS is not upgrading to 9.1R2 PSIS version. **Condition**: When CTS, WTS and VDI gets upgraded to 9.1R2 in Windows 10 Redstone 5 and later, PSIS is not upgraded to latest version. **Workaround**: None. Old PSIS will continue to work and no impact seen.
PRS-377700	**Symptom**: Using REST API - Archiving Schedule settings change from hourly to specified time does not update the hour/minute setting. **Condition**: None **Workaround**: Apply the same API again the second time.
PRS-378101	**Symptom**: JSAM fails to launch on Mac OS Catalina 10.15. **Conditions**:

Problem Report Number	Release Note
	• Configured a role with Host checker. • Configured JSAM access with auto-launch. **Workaround**: None
PRS-379014	**Symptom**: After single logout with Ivanti Connect Secure as SP, the SP lands on either IdP page or SP page. **Condition**: Ivanti Connect Secure is configured as IdP and another Ivanti Connect Secure configured as SP with single logout enable. **Workaround**: None.
Release 9.1R1 PRs	
PRS-373762	**Symptom**: Named User Remote Repo (NURR) mode does not work when MSSP unlimited license is installed on the License server. **Condition**: MSSP Unlimited License installed on License server. **Workaround**: MSSP customers with MSSP SKU to not use NURR mode.
PCS-11922	**Symptom**: DNS Port selection will not take any effect. DNS traffic will go through Internal Port only. **Condition**: On a Ivanti Connect Secure Virtual Appliance, when Administrative Network is enabled under Traffic Segregation. This issue is not applicable for PSA Hardware Devices. **Workaround**: None
Cloud Secure	
PRS-371781	**Symptom**: Blocked ECP users will not be updated if Generic is selected under LDAP server Type. **Condition**: LDAP server type selected is Generic. **Workaround**: Select the LDAP server type as Active Directory.
PRS-372846	**Symptom**: Blocked ECP users will have a “Blocked till time” of 5 minutes. **Condition**: Request count for a particular user is less than 3. **Workaround**: None
PRS-372861	**Symptom**: Blocked ECP users will not be removed from the ECP reports page based on “Blocked till time”. **Condition**: When a user entry is present in the ECP reports page. **Workaround**: None

Documentation

Ivanti Connect Secure documentation is available at https://help.ivanti.com.

Technical Support

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

- https://forums.ivanti.com/s/welcome-pulse-secure

Call us at +1-888-253-6201

For more technical support resources, browse the support website
https://forums.ivanti.com/s/welcome-pulse-secure