



## **Ivanti Connect Secure Release Notes**

22.1R1-22.7R2.7



# Copyright Notice

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

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

Copyright © 2025, Ivanti, Inc. All rights reserved.

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

---

# Contents

---

<b>Copyright Notice</b>	<b>3</b>
<b>Revision History</b>	<b>5</b>
<b>What's New</b>	<b>7</b>
<b>Introduction</b>	<b>18</b>
<b>Noteworthy Information</b>	<b>19</b>
Caveats	22
<b>Upgrade and Migration</b>	<b>24</b>
Upgrade Path	24
Configuration Migration Path	24
<b>Support and Compatibility</b>	<b>26</b>
Hardware Platforms	26
Virtual Appliance Editions	26
Licensing Types	32
<b>Resolved Issues</b>	<b>34</b>
<b>Security Advisory and Patch Update</b>	<b>50</b>
<b>Known Issues</b>	<b>52</b>
<b>Documentation</b>	<b>78</b>
Technical Support	78

# Revision History

The following table lists the revision history for this document:

Document Revision	Date	Description
8.0	April 2025	Updated with, <a href="#">"Resolved Issues"</a> on page 34, <a href="#">"Noteworthy Information "</a> on page 19, version and build number, <a href="#">"Upgrade and Migration"</a> on page 24 for 22.7R2.7
7.0	February 2025	Updated with <a href="#">"What's New"</a> on page 7, <a href="#">"Resolved Issues"</a> on page 34, <a href="#">"Known Issues"</a> on page 52, <a href="#">"Noteworthy Information "</a> on page 19, version and build number, <a href="#">"Upgrade and Migration"</a> on page 24 for 22.7R2.6
6.0	January 2025	Updated with <a href="#">"What's New"</a> on page 7, <a href="#">"Resolved Issues"</a> on page 34, <a href="#">"Known Issues"</a> on page 52, version and build number, <a href="#">"Upgrade and Migration" on page 24</a> for 22.7R2.5
5.0	December 2024	Updated with <a href="#">"Resolved Issues"</a> on page 34, version and build number, <a href="#">"Upgrade and Migration" on page 24</a> , for 22.7R2.4
4.0	October 2024	Updated with <a href="#">"What's New"</a> on page 7, <a href="#">"Resolved Issues"</a> on page 34, <a href="#">"Known Issues"</a> on page 52, version and build number, <a href="#">"Upgrade and Migration" on page 24</a> for 22.7R2.3
3.0	September 2024	Updated with <a href="#">"Resolved Issues"</a> on page 34, version and build number, <a href="#">"Upgrade and Migration" on page 24</a> , for 22.7R2.2
2.0	July 2024	Updated with <a href="#">"What's New"</a> on page 7, <a href="#">"Resolved Issues"</a> on page 34, <a href="#">"Known Issues"</a> on page 52, version and build number, <a href="#">"Upgrade and Migration" on page 24</a> , <a href="#">Noteworthy Information</a> , and <a href="#">Security Advisory and Patch Update</a> for 22.7R2.1

---

Document Revision	Date	Description
1.0	May 2024	Updated with what's new, known and fixed issues, version and build number, migration and upgrade path for 22.7R2

# What's New

## Release 22.7R2.7

Product Version	Build
ICS 22.7R2.7	4377
ISAC 22.8R1	31437
Default ESAP	4.3.8

## New Features

This release includes [bug fixes](#). There are no new features.

## Version 22.7R2.6

Product Version	Build
ICS 22.7R2.6	3981
ISAC 22.8R1	31437
Default ESAP	4.3.8

## New Features

- **Debug Log Size:** The debug log file size in Virtual Appliances has been increased to 1024 MB for HDDs, which are 80 GB or larger, see [Using the Debug Log](#) and [Supported Virtual Appliances](#). Hardware devices already have this capability.
- **End User Portal:** Enhancements to the appearance and interface in the end-user portal, which includes:
  - Option to enable a background color, see [Configuring Sign-In Pages](#).
  - Confirmation dialog box, which is displayed before the deletion of a bookmark.
  - Increased Logo height on the landing page for better visibility.

- In file browsing after uploading five files, the file upload button is disabled. Only five files can be uploaded at a time.
- For file browsing SSO, when the user enters invalid credentials, an error message is shown.
- **Logging Enhancement:** The user access log displays the country name for geo-location based restriction rules within the user realm, see [Logs](#).

### Release 22.7R2.5

Product Version	Build
ICS 22.7R2.5	3793
ISAC 22.7R4	30859
Default ESAP	4.3.8

### New Features

This release includes [bug fixes](#) and [security fixes](#). There are no new features.

### Release 22.7R2.4

Product Version	Build
ICS 22.7R2.4	3597
ISAC 22.7R4	30859
Default ESAP	4.3.8

### New Features

This release includes only bug fixes and there are no new features.

### Release 22.7R2.3

Product Version	Build
ICS 22.7R2.3	3431



Product Version	Build
ISAC 22.7R4	30859
Default ESAP	4.3.8

## New Features

- **TOTP Server:** Strengthening the TOTP server by adding password authentication checks for importing and exporting a configuration file, with corresponding changes made to the Rest APIs, see [Exporting/Importing TOTP Users](#) and [APIs](#).
- **Hard Disk Monitoring:** Implementing new REST APIs to retrieve disk usage information and perform disk cleaning, see [Disk Usage Monitoring](#) and [Disk Cleanup](#).
- **XML Import/Export:** Strengthening the XML config file import/export process with password authentication checks, and updating Rest APIs accordingly, see [Exporting an XML Configuration File](#) and [Importing an XML Configuration File](#).
- **SNMP Polling:** Improved SNMP functionality to monitor the status of the Power Supply and Fan in ISA 8000 and ISA 6000 devices, see [Displaying Hardware Status](#).
- **SNMP:** Improvements have been made to SNMP to retrieve results showing the current VPN ACL count, see [Configuring SNMP](#).
- **End User Portal:** Enhancements to the appearance and interface in the end-user portal include:
  - Collapsible welcome note on the end user UI.
  - List view for bookmarks, see [Customizing the Welcome Page](#).
  - Option to enable/disable a background image in the Sign-In Page, see [Configuring Sign-In Pages](#).

## Release 22.7R2.2

Product Version	Build
ICS 22.7R2.2	3221
ISAC 22.7R3	30227
Default ESAP	4.3.8

## New Features

This release includes only bug fixes and there are no new features.

### Release 22.7R2.1

Product Version	Build
ICS 22.7R2 .1	3191
ISAC 22.7R3	30227
Default ESAP	4.3.8

## New Features

- **Play Integrity API Checks:** Helps to check that interactions and server requests are coming from the genuine app binary running on a genuine Android device, see [Using the Mobile Options](#).
- **Health Check:** Ensures that the configured NTP and AD in ICS are reachable and also reduces involvement of support and engineering in addressing the customer environment issues, see [Health Check](#).
- **Log Size:** The Maximum Log size is increased to 200MB for VMs and 1GB for ISA hardware devices, see [Configuring Events to Log](#).
- **Read-Only Admin:** On Traffic Segregation, Administrative Network support is removed for Read-Only Admin, see [Traffic Segregation Feature Overview](#).
- **Rest API Auth:** Removal of support for /api/v1/auth API which does not help in enforcing RBAC on REST endpoints. Instead use /api/v1/realm\_auth API for authentication, see [Realm-based Authentication](#).
- **FDQN Support:** Lockdown Mode Exception Rule is added with Remote FDQN Resources to support FDQN, see [Custom-based Resource Access](#).
- **End User Portal:** Bookmark panel on end user portal is enhanced with expand and collapse accordion.
- **Rewriter:** Enhanced Rewriter parser to support Super keyword and Triple dot.

## Release 22.7R2

Product Version	Build
ICS 22.7R2	2615
ISAC 22.7R2	29103
Default ESAP	4.3.8

## New Features

- **Remote Debugging:** Now support center can access system over a secure connection using Remote Debugging server via internal, external, or management port, see [Using Remote Debugging](#).
- **Licensing Server:** ICS Gateway can connect to license server using IPv6 address, from 22.7R2 release onwards, see [License Server](#).
- **Delegated Admin:** From this release onwards, Delegated admin user can login via rest API.
- **Content Security Policy:** CSP is implemented to harden the security by detecting and mitigating certain types of attacks, see [Security Hardening](#).
- **Configuring Administrator Roles:** You can customize the number of records to be displayed per page in a table, see [Creating and Configuring Administrator Roles](#).
- **Integrity Check:** Booting Options on Integrity Check Failure is newly introduced to check integrity check failures during boot up (Disabled by default). Options are added to Reboot, rollback or continue booting if integrity check fails, see [Configuring Miscellaneous Security Options](#).
- **Additional Client package(s):** Now, only the active client package will get exported/carry forwarded, see [Software Upgrade Page](#).
- **MDM Auth Server:** New option is added with interface selection for MDM connections to enable outgoing interface, see [Configuring an MDM Server](#).
- **SAML/ Web Server:** New setting is added to monitor the SAML/Web server, see [Configuring System Maintenance Options](#).
- **TLSv1.3:** Support for Browser based TLSv1.3 certificate authentication using Port Redirection, see [Enabling Inbound SSL Options](#).

- **Mobile Options:** IF-T/TLS NCP knob option is newly added for Mobile, see [Using the Mobile Options](#).
- **Host checker Policy:** Enhancement of Predefined OS Host Check rule for Windows with Service packs/version number.
- **IPv6 support:** New IPv6 Provisioning Parameters added that are required during the deployment of a virtual appliance, see deployment guides [KVM](#), [Hyper-V](#), [VM](#), [Nutanix](#).
- **OpenSSL 3.0:** Upgrading OpenSSL stack with OpenSSL 3.0 which includes a cryptographic module that can be FIPS validated, see [Enabling Inbound SSL Options](#).

## Release 22.6R2

This release is FIPS compliant and includes the following features:

- **Dynamic Disk Size Allocation:** ICS fresh deployment includes 80GB disk size (Default). Admin can modify/increase the disk from 40GB to 80GB on upgrade from prior version, see deployment Guides [Azure](#), [AWS](#), [GCP](#), [KVM](#), [Hyper-V](#), [VM](#).
- VLAN enhanced to Support for Hyper-V, see [Configuring VLAN Ports](#).
- **Inbound Option:** CNSA1.0 is added as new option in Inbound selection list to provide stronger ciphers, see [CNSA1.0](#).
- **DHCPv6 Server:** Support DHCPv6 Subnet option. Enhanced to support IPv6 address, see [IPv6 address assignment in table](#).
- Support SAML as secondary auth Server.
- **LDAP Recovery and Health Monitoring:** Periodic Health Check for server with details in event logs, see [Health Checker](#).
- **Proxy Server:** PCLS host name supports IPv6 address, see [Proxy Server Configuration](#).
- Support added for assigning IPv6 address to IKEv2 based VPN connection and access is enabled to IPv6 based protected resources.

## Release 22.5R2.1

- **DHCPv6 Server:** Enhanced to support IPv6 address. For more details, see [IPv6 address assignment in table](#).

- **Port Probe support for IPv6:** You can verify if TCP and UDP ports for IPv6 destination server is open using IPv6 internal or management source IP. For more details, see [Troubleshooting Tools](#).
- **Advanced HTML5 improvements:** Automatic launch for admin created bookmark on user login is newly added. For more information, see [Advanced HTML5](#).
- **Filter Duplicate Split Tunnel Routes:** Admin gets information message about duplicate configuration entry detection and automatically removed while saving. For more details, see [Split tunnel](#).
- **REST API enhancements:** New set of REST APIs are added for upload, delete and for staging upgrade and also to fetch and save logs. For more details, see [Staging Upgrade](#), [Fetching Logs](#).
- **OAuth Enhancements** to support Encrypted ID Token and Self-Signed Provider Certificates. For more details, see [OAuth](#).

## Release 22.4R2

- **SELinux (Security Enhanced Linux) support:** This feature restricts access to the ICS Linux system so that ICS Linux applications can only access the minimum set of resources they require. SELinux mode is enabled as Enforcing by default. See [Security Enhanced \(SELinux\) Support](#).
- **TLS 1.3 Support:** TLS 1.3 option is newly introduced in this release. See [TLS 1.3 Support](#).

ICS now supports TLS version 1.3 with the following additional cipher suites:

- TLS\_AES\_128\_GCM\_SHA256
- TLS\_AES\_256\_GCM\_SHA384
- TLS\_CHACHA20\_POLY1305\_SHA256

### Limitation:

- End-user certificate authentication feature (Smart Card) is not available when **Accept only TLS 1.3** is enabled in System > Configuration > Inbound Settings for protocol version.
- If you choose **Accept only TLS 1.2 and later** with custom ciphers, then you need to ensure one or more TLS 1.2 ciphers are included.

- **Use Low-Privilege Account instead of Root (NRP):** Web server related processes are executed as non-root user. This prevents malicious code for gaining permissions in the ICS host. This feature is enabled by default.
- **Running Third-Party Tools in Jail:** The ICS applications will run third party tools in a controlled environment where the contained process is not allowed to utilize resources outside of the container such as files, memory space devices, etc. This feature is enabled by default.
- **Kernel rate limiting** is implemented on external interface to prevent unauthenticated DoS and DDoS attack. See [Miscellaneous Security Options](#).



22.4R1 features are supported in 22.4R2.

---

### Release 22.4R1

- IPv6 support for File Resource Profile: This features supports the IPv6 format for the servers IP address and server name. See [Creating a File Resource Profile](#).
- IPv6 support for Log Archiving
- IPv6 support for Host Checker, Download ESAP, Signature files

### Release 22.3R1

- **Pulse One Support:** Beginning with Release 22.3R1, Pulse One support is added. By default, nSA is supported, which is feature rich compared with Pulse One) as a controller for the ISA appliances. If you are not able to use nSA due to certification/federal compliance. You can reach out to Ivanti enterprise support for Pulse One enablement on ICS 22.3R1 or above.
- **IPv6 static routing:** This feature provides static routing for IPv6 address. Static routes are useful for smaller networks with only one path to an outside network and to provide security for a larger network for certain types of traffic or links to other networks that need more control routes are manually configured and define an explicit path between two networking devices.
- **IPv6 in LDAP server:** This feature helps to configure IPv6 on LDAP Server.
- **Support for ICS Deployment on Nutanix:** New Qualification for Nutanix deployment
- **ICS is Qualified on Microsoft Azure F series:** The following Microsoft F series variants are now qualified:
  - F4s\_v2

- F8s\_v2
- F16s\_v2
- **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.
- **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.
- **FQDN IP entries in ACL:** This feature allows to retain FQDN IP entries for lifetime of the FQDN IP in an ACL.
- **Log Enhancements:** This feature allows the admin to enter a custom message to display on the client highlight the host checker compliance errors.

### Release 22.2R3

- This release qualifies certification of FIPS, JITC (DoDIN APL) and NDcPP.
- **JITC Certification**
  - Log Support for detection and prevention of SMURF/SYN Flood/SSL Replay Attack.
  - Disable ICMPv6 echo response for multicast echo request.
  - Disable ICMPv6 destination unreachable response.
  - DSCP Support.
  - Password Strengthening.
  - Notification for unsuccessful admin login attempts.
  - Re-authentication of admin users.
  - Notification on admin status change
- **NDcPP Certification**
  - When NDcPP option is enabled, only NDcPP allowed crypto algorithms are allowed.
  - Device/Client Auth certificate 3072 bit key length support.

- Not allowing Import of Device/Client Auth Certificate if Respective CAs are not in Trusted Stores.
- Not allowing Importing of Device Certificate without Server Authentication EKU (Extended Key Usage).
- Device/Client Auth/CA certificate revocation check during Certificate Import
- Syslog certificate revocation check during TLS connection establishment.
- Not Allowing 1024 bit Public Key Length Server Certificate from Syslog during TLS connection.

### **Release 22.2R1**

- Supports feature parity with 9.1R15. For more information, see [Release Notes](#).
- Platform (Core) License SKUs for ISA platforms are introduced.
- Hyper-V and KVM support for ISA-V devices as below:
  - ISA4000-V
  - ISA6000-V
  - ISA8000-V
- License server can lease core licenses to ISA-V license clients.

### **Release 22.1R1**

- Connect Secure runs on the next generation Ivanti Secure Appliance (ISA) series appliances, which has better performance and throughput due to hardware, software, and kernel optimization.
  - It is available as fixed-configuration rack-mounted hardware.
    - ISA6000
    - ISA8000
  - It can also be deployed to the data center or cloud as virtual appliances.
    - ISA4000-V
    - ISA6000-V



- ISA8000-V
- Supports feature parity with 9.1R14. For more information, see [Release Notes](#).
- This release addresses OpenSSL vulnerability [CVE-2022-0778](#). It is recommended to upgrade all the Gateways to the latest version of Connect Secure.

# Introduction

Ivanti Connect Secure (ICS) is a next generation Secure access product, which offers fast and secure connection between remote users and their organization's wider network. Ivanti Connect Secure modernizes VPN deployments and is loaded with features such as new end user experience, increased overall throughput and simplified appliance management.

This document contains information about what is included in this software release: supported features, fixed Issues, upgrade path, and known issues. If the information in the release notes differs from the information found in the documentation set, follow the release notes.

These are cumulative release notes. If a release does not appear in this section, then there is no associated information for that release.

# Noteworthy Information

## Version 22.7R2.7

- Smart card agent requires to be updated on the client machine to support HTML5 login using smart card authentication. For updating, you must uninstall the older version of Smart card agent on your system and reinstall it by downloading the latest version from ICS End user portal.

## Version 22.7R2.6

- PSAM has been updated to improve security. As a result, the server will validate that the IP address and FQDN being used by the client match the results that the ICS server gets for the same FQDN. If the IP and FQDN do not match, access will be denied. This is most likely to occur with large cloud resources, which are traditionally not handled via PSAM. If access is denied an entry will appear in the access log. Log message: *"Deny connect request to www.xyz.com port 7000. FQDN matched but IP 23.1.3.7 didn't match any resolved IP(s)"*.
- With latest changes by default RADIUS sends the Access Request packet with the Message-Authenticator (80) attribute and does a strict check for the same attribute on the Response packet. If the ICS does not receive the same in response packet, then the connection terminates. Refer the [forum article](#) for more Information.



Verify your RADIUS Server's capability to handle the above scenario before upgrading.

---

- The IF MAP feature is not supported starting from Release 22.7R2.6.
- Beginning with ICS 22.7R2.6 onwards, thumbprint must be used as identifier instead of the serial number in the certificate APIs, see [API Sample](#).

## Version 22.7R2.3

- Functionality provided by the IF-MAP feature has reached a final state. Refer the [forum article](#) for more information.

## Version 22.7R2.1

---



Ivanti Connect Secure 22.7R2.1 will disable the DMI (**System > Configuration > DMI**) feature during upgrade. New installations of this version will also have this disabled by default. This is in line with proactive measures outlined in [KB](#). Enabling this feature in ICS 22.7R2.1 will reintroduce risk associated with the related vulnerability.

---

- Dashboard warning message is implemented in 22.7R2.1 referencing the "Security Certificate validation being enabled or not for the below features"
  - License Server
  - Push Config clients
  - Trusted server enforcement for Ivanti Secure mobile app
  - LDAP Server
  - Trusted Client CA's with CRLs

## Version 22.7R2

- After upgrade , the default ESAP version will be set to 4.3.8.
- Ivanti recommends using `api/v1/realm_auth` instead of `api/v1/auth` as it will not be supported in future release. Update/Modify your REST based scripts to make use of `/api/v1/realm_auth`.
- For advance HTML5 RDP access via smart card, the smart card driver version at client side and RDP Host should be same

## Version 22.6R2

- **ISAC Packages:** Ensure that there is only one client package uploaded along with the default as a best practice. Delete the non-active client package before doing any of the following operations-upgrade, binary export/import and push config. For more details, refer to [Limitations with more than two ISAC packages](#).
- Support added for assigning IPv6 address to IKEv2 based VPN connection and access is enabled to IPv6 based protected resources.
- IPv6 support for Log archiving on AWS is now supported.

- Users upgrading to 22.6R2 with AD servers 2016 or older could see AD domain join failures after upgrade. Refer to the [KB link](#) for details and work around before upgrading.

### Version 22.5R2.1

- The Sign-in policy should be configured with the login URL, if the login URL is different from the Host FQDN to avoid SAML transfer failed issue.

For Release 22.5R2.1, While Configuring SAML/IdP Settings for Cloud Secure set the Signature Algorithm to Sha-256.



SHA-1 is less secure and not supported by Microsoft 365 from 2016 version onwards.

---

### Version 22.4R2

- 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 **User > User Roles > Role > VPN Tunneling** on ICS UI to access all resources.
- Console access using SSH is not available from release 22.4R2 onwards for cloud deployments. The user has to leverage the serial console access instead.
- Enterprise onboarding is not supported in Release 22.4R2.
- Upgrade from 22.5R2/22.4R2 version to R1 version is not supported. Refer the [supported upgrade path forum link](#) for more details.
- Browser based Certificate authentication gets impacted when enforcing TLS 1.3 on 22.4R2. Refer the [forum link](#) for more details.

### Version 22.4R1

- Change in File system type from ext2 to ext3 to avoid power cycle issues for RAID disks.

### Version 22.3R1

- 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.

### Version 22.2R3

- New password must differ from previous 8 password positions (Default) option is newly added under Password options in Local Authentication Settings page.
- Reset Password and Change Password options are newly introduced for Local Authentication Account (User/Admin).

### Version 22.2R1

- Platform (Core) License SKUs for ISA platforms are introduced. Concurrent users is reset to two if core license is not installed or leased.
- Hyper-V and KVM support

## Caveats

Dynamic Disk Size Allocation:

- Admin can modify or increase existing disk size only once.
- In case of an upgrade, increased disk size (40 GB to 80 GB) is applicable only on upgraded ICS images not on rollback and factory reset images.
- If the users are upgrading to 22.6R2 or later, then the disk size change have to be done prior to upgrade on the respective platforms.

The following feature is not supported in this gateway release:

- Analytics Dashboard and Gateway logs are not synchronized with nSA when using an ICS gateway on the cloud running version 22.5R2 or above.
- Users upgrading to 22.6R2 with AD servers 2016 or older could see AD domain join failures after upgrade. Refer to the [KB link](#) for details and work around before upgrading.
- Multicast with IGMP
- Enterprise onboarding is not supported from Release 22.4R2.
- Upgrade from any R2 versions to R1 versions is not supported. Refer the [supported upgrade path forum link](#) for more details.
- Browser based Certificate authentication gets impacted when enforcing TLS 1.3 on 22.4R2. Refer the [forum link](#) for more details.
- Kernel rate limiting cannot be configured from nSA in Release 22.4R2.




The features listed in [KB44747](#) are not supported with 22.x Gateway release. In addition, Pulse Collaboration, HOB Java RDP, and Basic HTML5 are not supported in 22.x Gateway.

---

# Upgrade and Migration

## Upgrade Path


The following table describes the tested upgrade paths, in addition to fresh installation of 22.x for ICS Product.

 Follow the mandatory steps listed in the [KB](#) before staging or upgrading to prevent upgrade related issues.

Upgrade to	Upgrade From (Supported Versions)	Qualified
22.7R2.7	22.7R2.6, 22.7R2.5	Q
22.7R2.6	22.7R2.5, 22.7R2.4, 22.6R2.3	Q
22.7R2.5	22.7R2.4, 22.7R2.3, 22.6R2.3	Q
22.7R2.4	22.7R2.3, 22.7R2.2, 22.6R2.3	Q
22.7R2.3	22.7R2.2, 22.7R2.1, 22.6R2.3	Q
22.7R2.2	22.7R2.1, 22.7R2, 22.6R2.3	Q
22.7R2.1	22.7R2, 22.6R2.3, 22.6R1.2, 22.2R4.2	Q
22.7R2	22.6R2.3, 22.6R1.2, 22.5R2.4, 22.2R4.2	Q

## Configuration Migration Path

The following table describes the tested migration paths. See [PSA-ISA-Migration-Guide](#) and it is mandatory to follow the instructions.

 Before upgrading or config import from 9.x release where deprecated Auth servers is present, it is recommended to delete the deprecated Auth server before upgrade or config-imports. For Siteminder/Netegrity Auth Server, the XML config import and deletion of auth server fails post migration.

Migrate to	Migrate From (Supported Versions)	Qualified
22.7R2.7	9.1R18.9, 9.1R18.8, and 9.1R14.6	Q



Migrate to	Migrate From (Supported Versions)	Qualified
22.7R2.6	9.1R18.9, 9.1R18.8, and 9.1R14.6	Q
22.7R2.5	9.1R18.9, 9.1R18.8, and 9.1R14.6	Q
22.7R2.4	9.1R18.9, 9.1R18.8, and 9.1R14.6	Q
22.7R2.3	9.1R18.9, 9.1R18.8, and 9.1R14.6	Q
22.7R2.2	9.1R18.8, 9.1R18.7, and 9.1R14.6	Q
22.7R2.1	9.1R18.8, 9.1R18.7, and 9.1R14.6	Q
22.7R2	9.1R18.6, 9.1R18.4, 9.1R14.6 and nSA supported 9.1R17.4	Q



Upgrade the servers to the nearest matching version per the table to proceed with Migration if the exact versions are not listed.

# Support and Compatibility

## Hardware Platforms

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

- ISA6000
- ISA8000

## Virtual Appliance Editions

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

### Virtual appliance qualified in Platforms for 22.7R2.7

Limitations:

- Admin can modify or increase existing disk size only once, Admin can create an extra 2 physical disk partitions, which can be added to existing logical volume groups of rollback and currently only for the first time.
- As part of dynamic disk size allocation feature, Increase disk size is applicable only on upgraded ICS image and not on rollback and factory reset image.

Variant	Platform	vCPU	RAM	Disk Space
VMware ESXi 8.0.2 (23305546) ESXi 7.0.3 (23307199)	ISA4000-V	4	8 GB	80 GB
	ISA6000-V	8	16 GB	80 GB
	ISA8000-V	12	32 GB	80 GB

Variant	Platform	vCPU	RAM	Disk Space
Azure-V	ISA4000-V (Standard DS3 V2 - 3NICs)	4	14 GB	80 GB
	ISA4000-V (Standard_D4s_v3 - 2NICs)	4	14 GB	80 GB
	ISA6000-V (Standard DS4 V2 - 3 NICs )	8	28 GB	80 GB
	ISA6000-V (Standard D8s V3)	8	32 GB	80 GB
	ISA8000-V (Standard D16s V3)	16	64 GB	80 GB
	ISA4000-V (F4s_v2)	4	8 GB	80 GB
	ISA6000-V (F8s_v2)	8	16 GB	80 GB
	ISA8000-V (F16s_v2)	16	32 GB	80 GB
AWS-V	ISA4000-V (M5.xlarge - 3 NICs)	4	16 GB	80 GB
	ISA6000-V ( M5.2xlarge - 3 NICs)	8	32 GB	80 GB
	ISA8000-V (M5.4xlarge - 3 NICs)	16	64 GB	80 GB
	ISA4000-V (t3.xlarge - 3 NICs)	4	16 GB	80 GB
	ISA6000-V (t3.2xlarge - 3 NICs)	8	32 GB	80 GB
GCP	ISA4000-V (n2-standard-4 - 3 NICs)	4	16 GB	80 GB
	ISA4000-V (n1-standard-4 - 3 NICs)	4	16 GB	80 GB
	ISA6000-V (n2-standard-8 - 3 NICs)	8	32 GB	80 GB
	ISA6000-V (c2-standard-8 - 3 NICs)	8	32 GB	80 GB
	ISA 8000-V(n2-standard-16 - 3 NICs)	16	64 GB	80 GB

Variant	Platform	vCPU	RAM	Disk Space
OpenStack KVM OpenStack Dalmatian on Ubuntu 24.04.2 LTS	ISA4000-V	4	8 GB	80 GB
	ISA6000-V	8	16 GB	80 GB
	ISA8000-V	12	32 GB	80 GB
Hyper-V Microsoft Hyper-V Server 2022	ISA4000-V	4	8 GB	80 GB
	ISA6000-V	8	16 GB	80 GB
	ISA8000-V	12	32 GB	80 GB

### Virtual appliance qualified in 22.7R2.6, 22.7R2.5, 22.7R2.4, 22.7R2.3, 22.7R2.2, 22.7R2.1

Limitations:

- Admin can modify or increase existing disk size only once, Admin can create an extra 2 physical disk partitions, which can be added to existing logical volume groups of rollback and currently only for the first time.
- As part of dynamic disk size allocation feature, Increase disk size is applicable only on upgraded ICS image and not on rollback and factory reset image.

Variant	Platform	vCPU	RAM	Disk Space
VMware ESXi 8.0.2 (23305546) ESXi 7.0.3 (23307199)	ISA4000-V	4	8 GB	80 GB
	ISA6000-V	8	16 GB	80 GB
	ISA8000-V	12	32 GB	80 GB

Variant	Platform	vCPU	RAM	Disk Space
Azure-V	ISA4000-V (Standard DS3 V2 - 3NICs)	4	14 GB	80 GB
	ISA4000-V (Standard_D4s_v3 - 2NICs)	4	14 GB	80 GB
	ISA6000-V (Standard DS4 V2 - 3 NICs )	8	28 GB	80 GB
	ISA6000-V (Standard D8s V3)	8	32 GB	80 GB
	ISA8000-V (Standard D16s V3)	16	64 GB	80 GB
	ISA4000-V (F4s_v2)	4	8 GB	80 GB
	ISA6000-V (F8s_v2)	8	16 GB	80 GB
	ISA8000-V (F16s_v2)	16	32 GB	80 GB
AWS-V	ISA4000-V (M5.xlarge - 3 NICs)	4	16 GB	80 GB
	ISA6000-V ( M5.2xlarge - 3 NICs)	8	32 GB	80 GB
	ISA8000-V (M5.4xlarge - 3 NICs)	16	64 GB	80 GB
	ISA4000-V (t3.xlarge - 3 NICs)	4	16 GB	80 GB
	ISA6000-V (t3.2xlarge - 3 NICs)	8	32 GB	80 GB
GCP	ISA4000-V (n2-standard-4 - 3 NICs)	4	16 GB	80 GB
	ISA4000-V (n1-standard-4 - 3 NICs)	4	16 GB	80 GB
	ISA6000-V (n2-standard-8 - 3 NICs)	8	32 GB	80 GB
	ISA6000-V (c2-standard-8 - 3 NICs)	8	32 GB	80 GB
	ISA 8000-V(n2-standard-16 - 3 NICs)	16	64 GB	80 GB

Variant	Platform	vCPU	RAM	Disk Space
OpenStack KVM OpenStack Wallaby on Ubuntu 20.04 LTS	ISA4000-V	4	8 GB	80 GB
	ISA6000-V	8	16 GB	80 GB
	ISA8000-V	12	32 GB	80 GB
Hyper-V Microsoft Hyper-V Server 2016 and 2019	ISA4000-V	4	8 GB	80 GB
	ISA6000-V	8	16 GB	80 GB
	ISA8000-V	12	32 GB	80 GB

### Virtual appliance qualified in 22.7R2

Limitations:

- Admin can modify or increase existing disk size only once, Admin can create an extra 2 physical disk partitions, which can be added to existing logical volume groups of rollback and currently only for the first time.
- As part of dynamic disk size allocation feature, Increase disk size is applicable only on upgraded ICS image and not on rollback and factory reset image.

Variant	Platform	vCPU	RAM	Disk Space
VMware ESXi 7.0.3 (23307199) ESXi 6.7.0	ISA4000-V	4	8 GB	80 GB
	ISA6000-V	8	16 GB	80 GB
	ISA8000-V	12	32 GB	80 GB

Variant	Platform	vCPU	RAM	Disk Space
Azure-V	ISA4000-V (Standard DS3 V2 - 3NICs)	4	14 GB	80 GB
	ISA4000-V (Standard_D4s_v3 - 2NICs)	4	14 GB	80 GB
	ISA6000-V (Standard DS4 V2 - 3 NICs )	8	28 GB	80 GB
	ISA6000-V (Standard D8s V3)	8	32 GB	80 GB
	ISA8000-V (Standard D16s V3)	16	64 GB	80 GB
	ISA4000-V (F4s_v2)	4	8 GB	80 GB
	ISA6000-V (F8s_v2)	8	16 GB	80 GB
	ISA8000-V (F16s_v2)	16	32 GB	80 GB
AWS-V	ISA4000-V (M5.xlarge - 3 NICs)	4	16 GB	80 GB
	ISA6000-V ( M5.2xlarge - 3 NICs)	8	32 GB	80 GB
	ISA8000-V (M5.4xlarge - 3 NICs)	16	64 GB	80 GB
	ISA4000-V (t3.xlarge - 3 NICs)	4	16 GB	80 GB
	ISA6000-V (t3.2xlarge - 3 NICs)	8	32 GB	80 GB
GCP	ISA4000-V (n2-standard-4 - 3 NICs)	4	16 GB	80 GB
	ISA4000-V (n1-standard-4 - 3 NICs)	4	16 GB	80 GB
	ISA6000-V (n2-standard-8 - 3 NICs)	8	32 GB	80 GB
	ISA6000-V (c2-standard-8 - 3 NICs)	8	32 GB	80 GB
	ISA 8000-V(n2-standard-16 - 3 NICs)	16	64 GB	80 GB

Variant	Platform	vCPU	RAM	Disk Space
OpenStack KVM OpenStack Wallaby on Ubuntu 20.04 LTS	ISA4000-V	4	8 GB	80 GB
	ISA6000-V	8	16 GB	80 GB
	ISA8000-V	12	32 GB	80 GB
Hyper-V Microsoft Hyper-V Server 2016 and 2019	ISA4000-V	4	8 GB	80 GB
	ISA6000-V	8	16 GB	80 GB
	ISA8000-V	12	32 GB	80 GB
Nutanix AHV 2021	ISA4000-V	4	8 GB	80 GB
	ISA6000-V	8	16 GB	80 GB
	ISA8000-V	12	32 GB	80 GB

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

For more information see [Support Platform Guide](#).

## Licensing Types

License Type	Gateway Licensing Mode	nSA named user Licensing Mode
Platform/Core license	Install license locally or lease license for license server	Register the ICS Gateway with nSA and if the ICS Gateway is using nSA named user licensing mode then the Platform/Core license is not required.
User licensing	Install license locally or lease license for license server	Register ICS Gateway with nSA



License Type	Gateway Licensing Mode	nSA named user Licensing Mode
Feature licenses (Adv HTML5 etc)	Install license locally or lease license for license server	Install license locally on ISA-V

For more information see the [Licensing Management Guide](#)

# Resolved Issues

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

Problem Report Number	Summary
<b>Release 22.7R2.7</b>	
1561342	Web Process stops randomly, generating crashes.
1568828	Smart Card authentication detection failure during advanced HTML5 RDP login.
1558371 1565101 1544108 1544950	One or more web processes get stuck in infinite loop during SSL handshake resulting in High CPU.
1550503	Web process crash leading the user disconnections in ICS 22.7R2.6.
1518863	SMBCONF process crash during AD reset join issue.
1554025	Web Radius EAP crash issues.
1541825	ESP falls back to SSL and after some time the node freezes completely causing all connections to drop.
1535628	Virtual VMWare server running 22.7R2.5 with multiple web process crashes and certain users get disconnected
1527209	Kernel panic is noticed on ICS Version 22.7R2.6 when ESP transport mode is used.
1529008	After upgrading to 22.7R2.6 many users are unable to establish their VPN connection.
1529324	After the upgrade to 22.7R2.6, users started getting error 1132.
<b>Release 22.7R2.6</b>	
1511765	Unable to change background color on Sign-In Page 22.7R2.5.

Problem Report Number	Summary
1498609 1507670 1508201 1505423	Enable Setting view for Role showing unchecked option, when the features ( HTML5,VPN and other option ) for role is enabled.
1486110	Unable to change background color on Sign-In Page 22.7R2.3.
1477394	ICS kernel panic during upgrade.
1476344	With nSA license, few users are not reflecting in users page in the controller.
1427503	PSAM Ivanti Secure access client is not Launching automatically or connecting Automatically.
1384112	Advanced HTML5 Session Recording is Not Working From ICS 22.6R2.3 and Above.
1501125	FQDN based PSAM resources become inaccessible in ICS 22.7R2.4 due to PSAM DNS cache lacking the response for FQDN's.
1503495	PSAM issues in accessing FQDN resources with uppercase letters in ICS 22.7R2.4.
1503731	PSAM FQDN resource access denied despite IP Addresses being present in DNS cache in ICS 22.7R2.4.
1504947	Accessing the Sign-In URL redirects to PSAL helper page with upgrade helper installation prompt In ICS 22.7R2.4.
1302425	Inability to configure custom Radius login Page due to missing Defender.shtml file on 22.x versions.
1436751	Unable to Create Active Directory Server on ICS 22.7R2 and Above When Domain Field Contains ' _ ' Character.
1413083	Issues with SSO and Credential Parsing for Adv HTML5 and unable to access RDP Connection.
1401709	Advanced HTML5 W/ NLA bookmarks overrides settings for the additional NLA bookmarks.

Problem Report Number	Summary
1500990	Special Characters are not allowing in 22.x for selective pushConfig/ImportExport
1450950	Issue with SSH Access to HTML5 Resource on Debian 11: Scrollbar and Mouse Wheel Unresponsive.
1438431	RemoteDir paths containing spaces causing NullPointerException in 22.7R2.1 Advanced HTML5 Bookmark Access.
1428904	File upload in 22.x server allows users to submit more than 5 files but, they can add only 5. If the user adds the 5 files they should be prompted and not given the option to add more than 5.
1456283	Content-Length Header (HTTP) in Health check status full response on loadbalancer shows value as "Zero".
1416037	Unable to delete Staged package starting from 22.7R2 from the UI.
1457548	Unable To Browse the FileShare Resource When a Folder Name has Special Character "&" on ICS 22.7R2.3.
1444327	Kernel Panic is observed on the ICS deployed in Azure running on 22.7R2.
1379005	ICS server running 22.6R2.3 is seeing License Server Low Level Protocol Errors in the event logs.
1433652	REST API for resource throttling providing incorrect response in 22.7R2 and above.
1425143	Interacting with File Share Shortcuts Redirects to Downloading .lnk Files Instead of Folder Browsing on ICS Version 22.7R2.1.
1424576	Issues with SAML-Authentication Server config sync from nSA controller.
1417915	Application Access via Terminal Services Significantly Slower After Migration from PSA Server (9.1R17) to ISA Server (22.6r2.3) despite with same Configuration.
1413166	VPN ACL filtering by port is not working as expected.
1486083	Computer ICON is missing on the browser toolbar after upgrading to 22.7R2.3.

Problem Report Number	Summary
1415379	Cluster Node Hang and Recovery during Active Sync with IKEv2 VPN after migrating to 22.7R2.
<b>Release 22.7R2.5</b>	
1478647	PSAM users experience intermittent disconnections in ICS 22.7R2.3 with the 22.7R3 client version.
1352638	Memory usage increases linearly over time to 100%, causing the device to become unresponsive until it is rebooted.
<b>Release 22.7R2.4</b>	
1474116	Special characters are not permitted in version 22.x for selective pushConfig and ImportExport operations.
1465146	SPI count in debug logs and system snapshot to track memory issues.
<b>Release 22.7R2.3</b>	
1393255	Session Management( idle timeout, max session lifetime, session extension, etc) are not working.
1414793	Intermittent failures in Push Config due to login failure
1394301	End-user certificate (containing UPN name) verification fails when intermediate certificates contains a UPN Name Constraint
1414857	Different users could be assigned the same IPv6 address from DHCP when very specific conditions are met.
1302526	Errors when multiple intermediate CA certificates had the same name
1378157	Sign In Page Localization
1390101	File browser shows black screen when tried to refresh or open in new window.
1366376	File browser shows blank white screen when accessing file share bookmarks through the browser.
1302196	Login Syntax Change Impact on Syslog Agents After Device Upgrade
1352015	Misleading SYS30912 errors appears under user access logs

Problem Report Number	Summary
1376910	Remove postgresQL log files when CLI cleanup option 31 is selected.
1379602	Error Invalid Profile Type 1 when configuring SSH Advanced HTML5 resource
1386705	Session ID not showing as expected in User Access log
1391194	"Custom Settings" for Delegated Admin Role is not working as expected
1355032	Internal ICT scan failure (false positive) with a file nohup.out
1356278	External Integrity Scan and showing pyc files as new (false positive)
1354977	External Integrity Checker showing cert.pem.bak and key.pem.bak(false positive). Also flagging a file name pkgversion.3 (false positive)
1395490	Unable to configure Variable Attributes under Host Details in Terminal Services Configuration
1397105	Improve Watchdog log message to capture the command being executed by /bin/bash
1379860	Unable to enter characters when Chinese Traditional Taiwan language is enabled on local PC and html5 RDP resource.
1413440	Advanced HTML5 : improve pop up messages
1368090	ICS SNMP Unresponsive to 'get' queries
1375437	FTP Archiving failing for user logs
1414845	Program DSWSD recently failed when using certificate authentication
1416142	Process snapshots generated for unityConfigSpli & unityConfigNetc after registering ICS with Pulse One
1413774	License leasing not working correctly for appliances on 22.7Rx when the reserved license is configured as Zero
1411563	UI Issue with Radius Custom Rule Configuration with 22.7R2 and later
1302207	When the Active node shutdown from Active node the Passive node is not taking the VIP.
1429771	PSA7000 generating "First failure for a power supply reading" in the event logs

Problem Report Number	Summary
1428971	Implement log rotation for ive-ec2connect.log AWS deployments.
1383587	AD domain join takes 15 mins to join.
<b>Release 22.7R2.2</b>	
1418051	Improved handling of CA/intermediate certificates that do not have a CN value
1418054	Addressed issues when using two different CA/intermediate certificates that have the same CN and issuer.
1418042	Addressed an issue with swap memory management on ISA8k
1418049	Addressed an issue with swap memory management on VM devices
1395150	UAL license not working for EU region
<b>Release 22.7R2.1</b>	
PRS-418942	Users are having failed realm restrictions even when the location is allowed.
PRS-418576	User access logs displays the wrong Username, when ending a Terminal Session
1379870	Traffic Segregation in Hyper-V is not saving the VLAN ID under available Interface.
1302171	Users session gets disconnected on Windows 10 systems due to the Host Checker time out. For more see <a href="#">KB</a> .
1353427	IPTable rules default policy set to "ACCEPT" allowing all ports.
1302246	User access logs provides 127.0.0.1 address for source IP when an attempt with wrong credentials fails.
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 22.7R2
1352719	External Integrity Scan is Failing on the 22.7R2 server showing 85 mismatched files this occurred in Azure deployment only

Problem Report Number	Summary
1373106	Issue in displaying Special Characters when using French text in Welcome Message on ISA-6000.
1373377	ICS devices deployed in Azure are becoming unresponsive with "No space left on device" errors.
1348873	iveConcurrentUsers count is 0 in SNMP Traps.
1341262	Sometimes, Advanced HTML5 session does not respond to mouse clicks.
1341797	Cluster creation with IPV6 and default VLAN Id is not supported.
<b>Release 22.7R2</b>	
Refer to <a href="#">Security Advisory and Patch Release</a> section to see CVEs fixed.	
PRS-418027	Sending iveMaxConcurrentUsersSignedIn SNMP alert for Leased licenses from License Server.
PRS-419899	Keyboard input is printed twice when host and PC language is Chinese.
PRS-419817	Geolocation based realm restriction failing for user login.
PRS-418576	User access logs Shows wrong Username ,when ending a Terminal Session.
PRS-419357	System State storage size has reached max limit.
PRS-419198	Automatic detection with "unknown Keyboard" as keyboard layout does not work in Advance HTML5 pre-Login
PRS-419162	Wildcard Device certificate deletion with REST API is not working Properly.
PRS-419394	Difficulty in Joining Device to Domain Using Only Reset Join option with AD Authentication.
PRS-419159 PRS-419954 PRS-420242	VPN users dropped suddenly on gateway due to reboot.
PRS-419107	Avoid False Positives in ICT
PRS-419098	High CPU usage is noticed in all of the 12 nodes deployed.





Problem Report Number	Summary
PRS-419086	Import of System config/XML config related to bandwidth Management fails on ICS
PRS-418969	Certificate Auth failing is due to Missing Authority Key Identifier.
PRS-418954	Mitigating login issues through reboot or failover.
PRS-418930 PRS-419505	Certificate Host checker is failing after upgrading to 22.6R2.
PRS-418849	Unable to authenticate user using certificate with "Wrong Certificate::unsupported name constraint type".
PRS-416861	"Dropping the duplicate tunnel session from client" is seen in User Access Logs.
PRS-418161	SNMP Traps are not being generated when the redundant power supply is turned off.
PRS-418682	Singpass (SAML) Authentication fails when Load balancer URL is configured under the "Host FQDN for SAML".
PRS-418443	Not able to update ICS server appliance from 22.4R2 to 22.6R2.
PRS-418434	SSO stoped working for the FileShare Bookmarks after upgrading ICS to 22.6R2 version.
PRS-418392	Rewrite getting blank page via Host-based PTP.
PRS-418219	MDM Setup Issues with Microsoft Intune with Authentication and Authorization Challenges.
PRS-417969	AD join fails with ISA when Domain name has a special character '&'
PRS-418134	SID is not being displayed completely.
PRS-417750	iOS 17 has introduced a change in the IKE code, to make it stricter in compliance with RFC7296
PRS-417300	Ikev2 error messages seen in the User Access logs.
PRS-417319	High CPU usage at 100 % for ICS due to 64K size DNS response.
PRS-417668	Scrolling Bar Accessibility Issue on welcome page in Multiple Browsers.

Problem Report Number	Summary
PRS-417152	Upgrade to 9.1 R18.1 fails due to SSH/Telnet deprecation check.
PRS-417355	Inactivity reminder timeout, when users are using web session post migrating to 22.3R1.
PRS-417140	Failing to get Intune MDM Attribute Intermittently.
PRS-416968 PRS-417276	Chinese characters in file share bookmarks are garbled.
PRS-416896	After migration to ICS the Disk Space is showing as full on the active node in A/P cluster.
PRS-416479	Website loading slow after the upgrade with PassThroughProxy.
PRS-416169 PRS-420178 PRS-419764	Unable to connect to VPN, SAML authentication fails after upgrading the appliance to 22.4R2.
PRS-418524	Unexplained reboots on ISA 8000c A/A Cluster.
PRS-417756	DFS Share access is not working with 22.5R2.1.
PRS-418105	Web process crash on PSA 7000c due to memory leak.
PRS-417933	ICS Azure VM Virtual Wagent showing status not ready and impacting in taking Azure level VM backup in 22.x.
PRS-417302	Database percentage = 99, shard 3 operation above threshold.
PRS-417816	ICS Realm limits are not honored when nSA Named User Licensing mode is used.
PRS-417665	REST-based configuration updates may fail with an HTTP 500 error.
PZT-45037	SNMP trap messages under Event log to be removed.
PZT-44342	Config sync rule on the nSA shows Failed and Pending status.
PZT-44321	Readiness failures observed in Gateway.
PZT-44103	Single node cluster to support config sync and Report generation.
PCS-44875	Event logs are filled with certificate expired error message.

Problem Report Number	Summary
PCS-44362	Failed to save package, cannot copy UEBA package.
<b>Release 22.6R2.1</b>	
PRS-417750	iOS 17 has introduced a change in the IKE code, to make it stricter in compliance with RFC7296
PRS-418167	Program "impexpserver" crashed while importing Connection Profile via XML.
PRS-418021	UEBA option is missing in Pulse one admin UI.
PZT-42378	Peer SP configurations are not getting uploaded to nSA with appropriate title.
PZT-42049	Gateway information not being synced with nSA on 22.5R2.1 version.
PZT-41931	ICS is synchronizing users in Auth Servers to Pulse One.
PZT-41850	ICS Gateway (Event, Admin and user access) Logs are not seen in nSA controller.
PZT-41637	HTTP error 500 after PUT and Unknown errors in Gateway Events Access logs
PZT-41535	Config sync rule on the nSA shows Failed and Pending status.
<b>Release 22.6R2</b>	
PCS-41732	Port probe: Internal port IPv6 address is incorrectly populated when the user selects Management port with family type as IPv6.
PCS-43985	VPN tunneling filter deletion for IPv6 under System > Network > VPN tunneling. IPv6 filter not assigned to VPN clients if no filter is specified.
PCS-35445	Unable to set FIPS mode for web server.
PRS-416742	User Access log may fill quickly.
PRS-417352	Pulse One config sync issue after clearing nSA registration.
PRS-417245	ICT detects random mismatch while integrity scan.
PRS-416118	Host Checker with Certificate check fails due to CRL expiration frequency error.
PRS-416313	Advance HTML5 RDP Access with white space and resolution issue.

Problem Report Number	Summary
PRS-416834	Remote file transfer Advance HTML5 issue is resolved.
PRS-416483	NTP stops working after internal port is set with a default VLAN, though NTP is set to external or management port.
PRS-416460	Folders and files names containing character such as &# does not open in Windows Fileshare.
PRS-416274	PSAM sessions may disconnect frequently after upgrading to 22.4R2 ICS.
PRS-416776	Error on Safari browser searching for browser extension. Added check for Safari browser on 22.x end-user portal with respect to ISAC launch. Now clicking on ISAC launch, will not redirect to browser extension.
PRS-416627	DHCP FQDN's getting truncated in ICS DNS query.
PRS-416157	Lost syslog connection to server.
PRS-415988	Active directory users with HC log links from the active directory page will now redirect to the destination page.
PRS-417128	Unable to fetch device username attribute from Airwatch MDM.
PZT-41472	Config sync template status not progressing and shows as Pending.
PZT-41791	Frequent restarts of Fluent-Bit services.
PCS-43559	AD join from troubleshooting page fails with Error "Failed to find DC for domain <DOMAIN NAME> - Undetermined error".
PCS-42906	Few expired trusted server CA are not getting deleted.
PCS-38894	Advanced HTML5 external storage feature will not work.
PCS-42311	VPN fails to connect with Login Failed Error on Android with Host Checker.
PCS-39986	ICS initial configuration is not getting configured automatically from vApp options.
PCS-41405	VM upgrade and installation progress messages before reboot are not seen on VM serial console.
PCS-40467	On single core CPU platform, web server snapshot can be generated upon Security related configuration change.

Problem Report Number	Summary
PCS-25948	SAML versions and configuration mode.
<b>Release 22.5R2.1</b>	
PRS-416873	<p>Error joining ICS to AD domain if SMBv1 is disabled.</p> <hr/> <p> If you upgrade to 22.5R2.1, with SMBv1 disabled, AD Domain join fails after upgrade. Do a reset join on troubleshooting page post upgrade. For more information, see forum <a href="#">link</a>.</p> <hr/>
PRS-416911	<p>SAML Transfer failed with error message "Relay State does not match with the Server Host name".</p> <hr/> <p> The Sign-in policy should be configured with the login URL, if the login URL is different from the Host FQDN.</p> <hr/>
PRS-416576	An iOS/Android device connected to an ICS gateway with L3 App Visibility enabled and registered with nSA experiences a process crash.
PRS-416513	ICS is synchronizing users in Auth Servers to Pulse One.
PRS-415055	Launch JSAM policy fails to launch JSAM
PRS-416351	HTML Tag's are not working as expected in the Personalized greetings page.
PRS-416032	Unable to download files or folders that contain special characters while using Windows file sharing.
PCS-40794	Launching the Web bookmark via JSAM has issues.
PRS-415997	CGI server process crashing frequently in unique environments and configurations.
PRS-415690	Settings are lost after hard power cycle or power loss - ISA hardware appliance.
PRS-415097	SAML authentication fails with some SAML providers due to formatting errors based on RFC-2045.
PRS-415886	Built in Integrity check scanner tool in ICS does not accept 0 in hour field for scheduled scan so cannot be scheduled between 12 AM and 1 AM.

Problem Report Number	Summary
PRS-414815	File share contents are not available when browsing the file via bookmarks if the file share is only \\server\ and not \\server\share.
PRS-416062	Member of A/A cluster froze with kernel panic error.
PCS-41273	End-users are receiving "VPN Server is busy and unable to accept new connections." on the ISA Client, and unable to access intranet.
PCS-40656	On a Mobile device, if user logged in to web portal via browser and launching VPN connection will fail to establish VPN session.
PCS-41007	ICS does not send logs to remote syslog servers and nSA impacting analytics.
PCS-40006	File browsing with hostname is going through IPV4 address when "Preferred DNS Response:" is configured as IPv6.
<b>Release 22.4R2.1</b>	
PRS-415402	Filename Is Trimmed After Uploading via File Share Server Bookmark in ICS 22.X Versions. See <a href="#">forum link</a> for more details.
PRS-415686	ISAC shows password expiration warning even when the number of days configured in realm for warning is less than the password expiration day for Embedded Browser Sessions.
<b>Release 22.4R1</b>	
PCS-34411	Logs are not pushed from gateways to nSA.
PRS-414033	Boot failure issues with the ISA 8K devices.
PRS-415234	TOTP Remote server fail with REST API error
PRS-415017	Unexpected re-boot on ISA6000-V running 22.2R4
PRS-414999	One of the nodes in APAC region was unresponsive.
PRS-414278	Camera redirection does not work on ICS.
PRS-414111	Sign-out screen is garbled when browser language is Japanese
PRS-414024	Unable to add perpetual license on the ISA device

Problem Report Number	Summary
PRS-412571	Ivanti Connect Secure - Sorting issue for the core access files
PRS-412382	22.1R6 System.J corrupted which causes reboot the device
PCS-36684	Page refresh issue on end user portal.
<b>Release 22.3R1</b>	
PCS-37128	XML import fails in release 22.2R1 version when HTML5 resource profiles exported from release 9.1R15 or R16 .
PCS-35512	User browses to appserver URL with 8083 port (http://appserver:8083/test.asp), it re-directs to some other webpage.
PCS-36787	Certificate validity check shows certificate expired for less than 90 days.
PCS-37104	Downloaded Protected Zip File (1KB) is empty but actual file size is 2.07MB.
PCS-36764	File cannot be downloaded or deleted from the end user UI.
PCS-37090	Black screen is shown when user tries to download PSAL from Safari browser.
PCS-37092	End user Onboarding option is not displaying on MAC OS.
PCS-36675	Panel Preferences for Admin/end user bookmarks is not shown.
<b>Release 22.2R1</b>	
PCS-36319	Save All Logs option missing from Events/User Access/Admin Access Logs
PCS-34870	Clear config data fails with errors.
PCS-33729	Cache cleaner policy is not getting imported when importing XML file for user role configured with cache cleaner policy.
PCS-34546	9.X HLGW : KVM : Post upgrade not able to access GUI
PCS-34530	Rollback via console is not working on KVM appliance.
PCS-34357	Bandwidth consumption is more than configured when downloading files using SSL tunnel mode.
PCS-34870	Reboot fails on selecting clear config from CLI menu.

Problem Report Number	Summary
<b>Release 22.1R6</b>	
PCS-36093	Configuration import fails with reason: software version used to create import file was '9.1R14 (build 16847)' current version of software is '22.1R1 (build 421)'"
<b>Release 22.1R1</b>	
PCS-30919	Copy paste from Advance HTML5 session stops working after a while.
PCS-32765	Flow change seen in End User portal while internal server File Browsing.
PCS-30489	Bandwidth not restricted for the user even though VPN Tunnels Maximum Bandwidth value is set.
PCS-32836	Pulse Client copyright date is not updated with 2022 year.
PCS-32596	Upgrade from 9.1R13 and 9.1R12 GA to 9.1R13.1 is failing at the upload step with Access restricted error.
PCS-32906	ISA VM machine ID getting changed.
PCS-32354	Registration status of ICS is in green color.
PCS-33249	Error message at the end of successful completion of ICS boot.
PRS-407283	Multicast and broadcast packets soft lockup issue observed with ICS Gateway on AWS.
PRS-408401	Configuration import fails on ISA. The Migration Guide is updated with the supported configuration migration path. ICS Release 21.12R1 supports config import from Release 9.1R13 and below
PRS-407958	ICS on VMware console shows watchdog BUG: "soft lockup - CPU#X stuck for XXs!".
PRS-407283	ICS 21.12 soft lockup in AWS.
PRS-407281	Node is not accessible, software lockup issue.
<b>Release 21.12R1</b>	



Problem Report Number	Summary
PRS-405611	Login to PDC to get authentication twice one before HC and one after HC when using DUO-LDAP.
PCS-30626	Failed to update profile for user error is seen in user access logs for every user.
PCS-30694	Number of concurrent users exceeded msg seen, even though licensed through nSA named licensing
PCS-31161	Error updating data messages seen after upgrade to 399.
PCS-31046	XML import from 9.X HLGW to 21.X not working on a specific scenario.
PCS-30652	Host checker failed in Mac OS with server has not received any information for this policy error.
PCS-31213	PDC L3 Multicast with 21.9R1 - IGMPv3 to v2 fallback is not happening automatically.
PCS-31193	health check REST API is returning 500 Internal Server error.
PCS-30658	System Maintenance > Run Diagnostics throws error.
PCS-29657	Kill command seen on the virtual console on fresh deploy of 21.6R2_273.
PCS-30629	Old sign-in page seen if ICS is not able to reach remote TOTP server.
PCS-30854	Push Config of Selective Config fails with error related to HTML5-access sessions.
PRS-406156	Chinese characters on the end user portal page is not appearing properly.
PRS-406805	Issue with VLAN while getting the tunnel IP in A/P cluster.
PCS-31734	Host Checker Compliance Result user access logs have either device_id or browser_id which is mandatory for analytics.
PCS-31730	nSA ICS Overview dashboard Info panel showing empty values.
PRS-404854	ICS Gateway: Temp license is not expired even at 56 days.
PCS-31473	TCP dump not uploaded to nSA
PRS-405612	LDAP: Login in PDC gets authentication twice one before HC and one after HC when using DUO-LDAP

# Security Advisory and Patch Update

Ivanti has released security advisories and mitigations for critical vulnerabilities in the Ivanti Connect Secure gateways. These vulnerabilities impacts all supported versions of ICS (22.x).

The following CVE's have been fixed:

## 22.7R2.6

This release includes important security fixes as part of our ongoing commitment to secure-by-design. There has been no evidence of exploitation in the wild of anything fixed in the release and full details of these security fixes will be available in our next [security advisory](#), scheduled for release on February 11, 2025.

## 22.7R2.5

This release includes important security fixes as part of our ongoing commitment to security. The details of these security fixes can be found in [security advisory blog](#), dated January 8th, 2025.

CVE's	Security Advisory Blog
CVE-2025-0282	For more details, see <a href="#">security advisory</a> blog.
CVE-2025-0283	For more details, see <a href="#">security advisory</a> blog.

## 22.7R2.4

This release includes important security fixes as part of our ongoing commitment to secure-by-design. There has been no evidence of exploitation in the wild of anything fixed in the release and full details of these security fixes will be available in our next [security advisory](#), scheduled for release on December 11, 2024.

## 22.7R2.3

This release includes important security fixes as part of our ongoing commitment to secure-by-design. There has been no evidence of exploitation in the wild of anything fixed in the release and full details of these security fixes will be available in our next [security advisory](#), scheduled for release on November 12, 2024.

22.7R2

CVE's	Ivanti Forum links
CVE-2023-38551	For more details, see <a href="#">Ivanti forum</a> .
CVE-2024-6387	For more details, see <a href="#">Ivanti forum</a> .

# Known Issues


The following table lists the known issues in respective releases:

Problem Report Number	Release Note
<b>Release 22.7R2.6</b>	
1343190	<b>Symptom:</b> Not able to add file share path as user bookmark. <b>Condition:</b> When file share path contains special characters. <b>Workaround:</b> Access via root share path.
1490114	<b>Symptom:</b> Unable to go back to previous folder. <b>Condition:</b> When folder name contains special characters like #. <b>Workaround:</b> Create the folder without special characters.
1518444	<b>Symptom:</b> VDI bookmark is not shown in the End user page and works fine in Admin UI page. <b>Condition:</b> When the Admin imports 9.x XML/user configuration on ICS 22.7R2.6. <b>Workaround:</b> Select the Role and click Save Changes in the UI options page.
1521559	<b>Symptom:</b> Joining node is showing enabled and unreachable when node joins in AP cluster. <b>Condition :</b> When a Node joins a new cluster and switches to AP mode, it receives the cluster VIP. <b>Workaround:</b> Join node in AA cluster mode and then convert into AP cluster mode or reboot the setup.
<b>Release 22.7R2.3</b>	
1383188	<b>Symptom:</b> AD domain join is failing for Windows Server 2025 <b>Condition:</b> AD domain join is failing for Windows Server 2025 with default windows server config. <b>Workaround:</b> None
1435999	<b>Symptom:</b> Cluster Upgrade: Device gets stuck in "started all services" when upgrading to 22.7R2.3 image <b>Conditions:</b> Under rare scenarios, when the vApp options got disabled for the VM on ESXi, and the backup valVEConfig is not in sync with the current config. <b>Workaround:</b> None. Need to do rollback and do RDC, and then remove the backup valVEconfig file.

Problem Report Number	Release Note
1428554	<p><b>Symptom:</b> When a full config export is triggered, xml download progress is not seen.</p> <p><b>Condition:</b> When full config export is triggered the progress bar of the xml download is not seen some times</p> <p><b>Workaround:</b> XML download happens in the background, the progress bar is not visible</p>
1442736	<p><b>Symptom:</b> Folder view is missing in 22.X</p> <p><b>Conditions:</b> For Citrix listed applications.</p> <p><b>Workaround:</b> Currently we support block/list view.</p>
<b>Release 22.7R2.1</b>	
1397724	<p><b>Symptom:</b> ICS upgrade from 22.7R2.1 or later fails through REST API.</p> <p><b>Conditions:</b> Occurs during upgrades from 22.7R2.1 to newer versions.</p> <p><b>Workaround:</b> None. Use Admin UI for upgrades instead.</p>
1387167	<p><b>Symptom:</b> Citrix Storefront web bookmark over HTML5 is not working with 2203/2402 LTSR version.</p> <p><b>Condition:</b> When ICS client access is selected with HTML5.</p> <p><b>Workaround:</b> User can use ICS client access as CTS/WSAM.</p>
1371885	<p><b>Symptoms:</b> Importing mTLS Client Certificates and Keys/bin/tar: tlcerts/cert.pem: Not found in archive message seen on ICS console after upgrade to 22.7R2.1</p> <p><b>Condition:</b> On an upgrade to 22.7R2.1</p> <p><b>Workaround:</b> None. Functionality is not affected. These message can be ignored.</p>
1369802	<p><b>Symptom:</b> Under rare conditions, CPU utilization goes to an average of 30 percent</p> <p><b>Condition:</b> When Adaptive Auth is enabled on the ICS cluster.</p> <p><b>Work around:</b></p> <ul style="list-style-type: none"> <li>• Disable UEBA from <b>System &gt; Configuration &gt; Behavioural Analytics</b>.</li> <li>• Wait for 15 mins</li> <li>• Re-enable <b>UEBA</b>.</li> </ul>
1380280	<p><b>Symptom:</b> Invalid Domain name error seen when AD domain name is having "0"</p>

Problem Report Number	Release Note
	<p><b>Condition:</b> Domain name containing 0 fails to save with error "Invalid Domain name".</p> <p><b>Workaround:</b> Upgrade of ICS from older release will work but need to Reset join. New AD configuration should be without 0 in domain name.</p>
1383587	<p><b>Symptom:</b> AD domain join takes 15 mins to join.</p> <p><b>Condition:</b> Upgrade to 22.7r2 or later.</p> <p><b>Workaround:</b> Save changes of AD config does a AD domain join</p>
1367931	<p><b>Symptom:</b> GCP - Adding management port details of other in cluster is returning with invalid IPv6 gateway error message.</p> <p><b>Condition :</b> When adding the details of management port for another node in cluster environment.</p> <p><b>Workaround:</b> Create cluster with two interfaces (device deployed with internal and external port only).</p>
<b>Release 22.7R2</b>	
PCS-45286	<p><b>Symptom:</b> VDI desktop client launch fails.</p> <p><b>Condition:</b> When user uses latest VDI horizon client 2309.</p> <p><b>Workaround:</b> User must use VDI horizon client 2103.</p>
PCS-47033	<p><b>Symptom:</b> iveConcurrentUsers count is 0 in SNMP Traps.</p> <p><b>Conditions:</b> When max users are signed in to ICS and tries to send iveMaxConcurrentUsersSignedIn SNMP trap. This SNMP trap has the iveConcurrentUsers set to 0.</p> <p><b>Workaround:</b> None.</p>
PCS-47017	<p><b>Symptom:</b> HTML5 RDP login via smart card will not work.</p> <p><b>Conditions:</b> When Windows client machine is configured with windows Hello PIN and Gemalto smart card is used to login via RDP</p> <p><b>Workaround:</b> Disable Windows Hello will work</p>
PCS-47022	<p><b>Symptom :</b> "Total Maximum Bandwidth" configuration is taking more value than interface limit in hyper-v platform</p> <p><b>Condition:</b> In Hyper-V platform when configuring "Total Maximum Bandwidth" in Network overview page</p> <p><b>Work Around:</b> Admin can configure the "Total Maximum Bandwidth" lesser than interface speed limit.</p>

Problem Report Number	Release Note
PCS-46998	<b>Symptom:</b> Kernel stack trace is seen on ICS console. <b>Conditions:</b> Under rare conditions, Kernel stack trace is seen on ICS console. <b>Workaround:</b> None. ICS has to be power cycled.
<b>Release 22.6R2.1</b>	
PCS-44875	<b>Symptom :</b> Event logs are filled with certificate expired error message. <b>Condition :</b> ICS has loaded with Expired trusted server CA. <b>Work around:</b> None, just a display issue.
<b>Release 22.6R2</b>	
PCS-44672	<b>Symptom:</b> PSAL fails to launch JSAM with JDK 21 on MAC Ventura 13.6. <b>Condition:</b> When user try to access JSAM with JDK 21 on MAC Ventura 13.6. <b>Workaround:</b> Use JDK 17 instead of JDK 21.
PRS- 417562 PRS-417355	<b>Symptom:</b> User/WTS session is getting terminated. <b>Condition:</b> When "Enable session timeout warning" option is enabled. <b>Workaround:</b> Disable the "Enable session timeout warning" option.
PCS-44362	<b>Symptom:</b> Failed to save package, cannot copy UEBA package. <b>Condition:</b> Uploading new UEBA package. <b>Workaround:</b> None. Contact Support for assistance.
PCS-43985	<b>Symptom:</b> VPN tunneling filter deletion for IPv6 under System > Network > VPN tunneling. IPv6 filter not assigned to VPN clients if no filter is specified. <b>Condition:</b> Importing binary config from 22.3, 22.4,22.5 releases. <b>Workaround:</b> Add default filter * for IPv6 in System > Network > VPN tunneling
PZT-42049	<b>Symptom:</b> Analytics Dashboard and Gateway logs are not synced with nSA. <b>Condition:</b> ICS Gateways running on cloud with version 22.5R2 or above. <b>Workaround:</b> NA
<b>Release 22.5R2.1</b>	
PCS-43559	<b>Symptom:</b> AD join from troubleshooting page fails with Error "Failed to find DC for domain <DOMAIN NAME> - Undetermined error". <b>Condition:</b> When AD container name contains spaces and was different than the default "Computers". <b>Workaround:</b> Use quotes in the AD configuration page if the AD container name has spaces.

Problem Report Number	Release Note
PCS-42906	<p><b>Symptom</b> : Few expired trusted server CA are not getting deleted.</p> <p><b>Condition</b> : When checking Trusted Server CA Page, using "Show only expired CAs" option enabled.</p> <p><b>Workaround</b> : Admin can import latest CAs if necessary</p>
PCS-41732	<p><b>Symptom</b>: Port probe: Internal port IPv6 address is incorrectly populated when the user selects Management port with family type as IPv6.</p> <p><b>Condition</b>: Interface port is selected first and then family type.</p> <p><b>Workaround</b>: Select family type first and then select the Interface as Internal/Management Port.</p>
PPS-10870	<p><b>Symptom</b>: OAuth token encryption using ECC certificates fails.</p> <p><b>Workaround</b>: Use RSA certificates for Token Encryption</p>
PCS-38894	<p><b>Symptom</b>: Advanced HTML5 external storage feature will not work.</p> <p><b>Condition</b>: When external storage server contains special characters in the password.</p> <p><b>Workaround</b>: Do not use any special characters in the password.</p>
PCS-42593	<p><b>Symptom</b>: Stats for other node are not accessible from the current cluster node.</p> <p><b>Conditions</b>:</p> <ol style="list-style-type: none"> <li>1. Go to <b>System &gt; Status &gt; Overview</b>.</li> <li>2. Select the other node from the drop down in any of the charts.</li> </ol> <p><b>Workaround</b>: None. Login to the other node to get the charts.</p>
PCS-42347	<p><b>Symptom</b>: Multiple authentication successful messages are observed in user access logs when user tries OWA 2016 or above with kerberos SSO.</p> <p><b>Workaround</b>:NA</p>
PCS-42311	<p><b>Symptom</b>: VPN fails to connect with Login Failed Error.</p> <p><b>Condition</b>: When Host checker is configured without enforcing at realm</p> <p><b>Workaround</b>: Enforce same host checker policies at realm also.</p>
<b>Release 22.4R2</b> <hr/> <div>  22.4R1 Known issues are also applicable to 22.4R2. </div> <hr/>	
PCS-37647	<p><b>Symptom</b>: Enterprise on-boarding feature will not work.</p> <p><b>Condition</b>: When end user uses on-boarding feature.</p> <p><b>Workaround</b>: None</p>



Problem Report Number	Release Note
PCS-37637	<b>Symptom:</b> Test enrollment will not work <b>Condition:</b> When end user uses on-boarding feature. <b>Workaround:</b> None
PCS-40086	<b>Symptom :</b> Browser based Certificate authentication is failing when TLS 1.3 is enabled on the ICS <b>Condition:</b> Browser based Certificate authentication fails when admin enables TLS 1.3 on ICS. <b>Workaround:</b> Admin need to enable TLS 1.2 (refer to <a href="#">KB</a> )
PCS-41506	<b>Symptom:</b> KB link for TLS 1.3 client support warning on the dashboard page takes you to a broken link. <b>Condition:</b> Click KB45694 link shown in the dashboard for Client impact with TLS 1.3. <b>Workaround:</b> See <a href="#">KB</a> for details.
PCS-35445	<b>Symptom:</b> Unable to set FIPS mode for web server. <b>Condition:</b> FIPS mode is not supported <b>Workaround:</b> None
PCS-39643	<b>Symptom:</b> Console doesn't respond to user input when selecting "change SELinux mode". <b>Condition:</b> Post cluster upgrade to 22.4R2. <b>Workaround:</b> Restart services from the UI.
PCS-39986	<b>Symptom:</b> ICS initial configuration is not getting configured automatically from vApp options <b>Conditions:</b> After performing clear config operation through VM Virtual Console <b>Workaround:</b> None. Configure ICS initial configuration such as IP address, admin user, self-signed cert details manually
PCS-40824	<b>Symptom :</b> Active user page in cluster nodes are not in sync for connected users, this happens when the cluster splits and joins. <b>Condition :</b> When cluster splits and joins this occurs. <b>Workaround :</b> None, it's just a display issue. In new session it is displayed correctly.
PCS-41405	<b>Symptom :</b> VM upgrade and installation progress messages before reboot are not seen on VM serial console

Problem Report Number	Release Note
	<b>Condition:</b> when upgrade was performed from 22.4r2 to higher release <b>Workaround:</b> None
PCS-41031	<b>Symptom:</b> Kernel rate limiting is not working on config import <b>Condition:</b> During config import from 22.4r2 with Kernel rate limiting enabled to another 22.4R2 setup. <b>Workaround:</b> A change in DOS/DDOS options requires an ICS reboot after config import. As a workaround undo and save the change, then redo and save from the interface.
PCS-40902	<b>Symptom:</b> Active Sync with Cert and Kerberos Constrained Delegation (KCD) does not work. <b>Condition:</b> When TLS 1.3 is enabled on ICS in bound settings. <b>Workaround:</b> Enable TLS 1.2 on ICS in bound settings.
PCS-40467	<b>Symptom:</b> On single core CPU platform, web server snapshot can be generated upon Security related configuration change. <b>Condition:</b> Upon change in Security configuration (such as change in TLS version) old web server process exits with crash <b>Workaround:</b> NA
PCS-40154	<b>Symptom:</b> Sometimes, Advanced HTML5 session does not respond to mouse clicks. <b>Conditions:</b> This issue happens usually when user tries to copy text using mouse on a ssh terminal session within HTML5 session. <b>Workaround:</b> Disconnecting and reconnecting the Advanced HTML5 session solves the issue.
PCS-39794	<b>Symptom:</b> If the server has TLS 1.3 enforced, the existing client connections and upgrades fail. <b>Condition:</b> TLS 1.3 enforced for the secure connections. <b>Workaround:</b> Enable the TLS 1.2 and higher option in the server, connect to the server and upgrade to the latest versions.
PCS-39045	<b>Symptom :</b> TLS 1.3 is not supported on mobile VPN client. <b>Condition:</b> Mobile Authentication will not work when the user enables TLS 1.3 on ICS. <b>Workaround:</b> Select TLS 1.2 on the ICS server.

Problem Report Number	Release Note
PCS-39942	<b>Symptom:</b> DMI based script no longer able to connect to ICS <b>Conditions:</b> After ICS is upgraded to 22.4R2 <b>Workaround:</b> NA.
PCS-38817	<b>Symptom:</b> Test connection for AWS/Azure archival server is showing as "Failed to connect to S3 bucket, WrongBucketLocation" <b>Condition:</b> When configuring AWS or Azure as archival server location. <b>Workaround :</b> Admin can configure SCP or FTP Server for archiving.
PCS-40729	<b>Symptom:</b> Cluster creation with IPV6 and default VLAN Id is not supported. <b>Workaround:</b> NA
PCS-41273	<b>Symptom:</b> End-users are receiving "VPN Server is busy and unable to accept new connections." on the ISA Client, and unable to access intranet. <b>Conditions:</b> When system operations (VIP failover, reboot, restart of services) are performed on the Gateway when users are logged in. <b>Workaround:</b> Perform operations affecting the system such as VIP Failover, Restart of Services, Reboot only during off hours. As a workaround, end-users can re-try after a minute and they would be able to re-establish VPN.
PCS-41014	<b>Symptom:</b> Upgrading from 22.4R2 to R1 builds will not show error when tried via REST API or DMI. <b>Workaround:</b> Upgrade will not happen to R1 builds since it is not a supported upgrade path but no error message will be shown to admin saying that this is not supported.
<b>Release 22.4R1</b>	
PCS-40794	<b>Symptom:</b> Launching the Web bookmark via JSAM has issues. <b>Condition:</b> When the PSAL is not installed on the client machine. <b>Workaround:</b> Create web bookmark to launch via the rewriter engine instead of JSAM.
PCS-40656	<b>Symptom:</b> On a Mobile device, if user logged in to web portal via browser and launching VPN connection will fail to establish VPN session.

Problem Report Number	Release Note
	<p><b>Condition:</b> When Secure Application Manager feature disabled under a user role configuration on ICS then a mobile device user who logged in to web portal via browser at first and then launching VPN connection using VPN bookmark will fail to establish VPN session.</p> <p><b>Workaround:</b> Enable Secure Application Manager feature under a user role configuration on ICS.</p>
PCS-41115	<p><b>Symptom:</b> JSAM logout button throws an internal error message.</p> <p><b>Condition:</b> when openjdk-17 java is installed</p> <p><b>Workaround:</b> No feature impact, click the ok button on the error screen JSAM applet will logout.</p>
PCS-41007	<p><b>Symptom:</b> ICS does not send logs to remote syslog servers and NSA impacting analytics</p> <p><b>Conditions:</b> This is seen in the following scenario:</p> <ol style="list-style-type: none"> <li>1. Preferred mode is set to IPv6</li> <li>2. Hostname is used to specify remote syslog server, and it resolves to both IPv4 and IPv6</li> <li>3. Preferred network to contact NSA is set via Management port</li> <li>4. Management port is configured with IPv6, but in disabled state</li> </ol> <p><b>Workaround:</b></p> <ol style="list-style-type: none"> <li>1. Re-enable IPv6 on management port, if possible (or) Remove IPv6 from management port</li> <li>2. Do restart of services or make a change in any of the syslog server config in Admin UI.</li> </ol>
PCS-40067	<p><b>Symptom:</b> Missing certificate error is not displayed when user connects to Certificate based VPN profile without a mapped certificate in the profile</p> <p><b>Workaround:</b> Map/add user certificate to the profile</p>
PCS-39675	<p><b>Symptom:</b> Start button for JSAM launch in Ubuntu is failing</p> <p><b>Workaround:</b> No workaround</p>
PCS-38989	<p><b>Symptom:</b> Connection with syslog server is failing.</p> <p><b>Workaround :</b> Restart the syslog server.</p>

Problem Report Number	Release Note
PCS-40006	<p><b>Symptom:</b> File browsing with hostname is going through IPV4 address when "Preferred DNS Response:" is configured as IPv6.</p> <p><b>Workaround:</b> Use the IPv6 address instead of host name.</p>
PCS-40007	<p><b>Symptom:</b> File browsing with hostname is not working when DNS response has IPv6 address only.</p> <p><b>Condition:</b> When file server/share is configured with hostname, hostname is not get resolve to IPv6 address. This is because getaddrinfo API is not supporting IPv6 resolution.</p> <p><b>Workaround:</b> NA</p>
PCS-40910	<p><b>Symptom:</b> When file server/share is configured with hostname, hostname will not get resolve to IPv6 address.</p> <p><b>Conditions:</b> File Server/Share configuration with hostname.</p> <p><b>Workaround:</b> Use IPv6 address while configuring instead of hostname.</p>
PPS-10665	<p><b>Symptom:</b> Compliance check fails on MacOSX, while using IPv6.</p> <p><b>Workaround:</b> None</p>
<b>Release 22.3R1</b>	
PCS-37354	<p><b>Symptom:</b> Ping6 with host name is not working.</p> <p><b>Condition:</b> When admin performs ping6 operation using host name.</p> <p><b>Workaround:</b> Admin can perform ping6 using IPv6 address.</p>
PZT-36727	<p><b>Symptom:</b> SNMP timeouts occurring than usual expected rate.</p> <p><b>Condition:</b> When the queries are sent aggressively like around 57 queries/sec timeouts occur.</p> <p><b>Workaround:</b> Increase the querying time for example to 57 queries in 2-3 seconds to see comparatively see less timeouts.</p>
PCS-39623	<p><b>Symptom:</b> Upgrade of cluster node fails with "Unable to extract installer" error message.</p> <p><b>Conditions:</b></p> <ol style="list-style-type: none"> <li>1. Upgrade triggered on a Cluster</li> <li>2. Node-1 upgrades successfully to 22.3R1</li> <li>3. Node-1 asks Node-2 to upgrade</li> </ol>

Problem Report Number	Release Note
	<p>4. Node-2 copies the package from Node-1, but fails to extract the installer. This is due to free disk space constraints on Node-2</p> <p><b>Workaround:</b></p> <ol style="list-style-type: none"> <li>1. Power cycle Node-2</li> <li>2. Press Tab and boot into Standalone mode</li> <li>3. Access the UI and follow the procedure mentioned in <a href="#">KB44877</a> to clean up space</li> <li>4. Reboot and join the cluster. Upgrade of cluster node is done successfully</li> </ol>
PCS-39641	<p><b>Symptom</b> : Intermittently during the fresh install and upgrades of Client launches, PSAL is not getting detected in the first attempt.</p> <p><b>Condition</b> : During fresh install and upgrade of client launches.</p> <p><b>Workaround</b> : Retry to the Client launches, it works.</p>
PCS-39675	<p><b>Symptom</b>: Start button for JSAM launch in Ubuntu is failing</p> <p><b>Workaround</b>: No workaround</p>
PCS-38218	<p><b>Symptom</b> : Error prompts when 'Citrix All Listed Application' is clicked. Failed to contact server, check the network connection and try again.</p> <p><b>Condition</b> : XML export and import of 'Citrix All Listed Application' along with other citrix bookmarks.</p> <p><b>Workaround</b>: Delete the 'Citrix All Listed Application' bookmark and recreate manually using Terminal profile via admin login.</p>
PCS-38455	<p><b>Symptom</b> : Only 'Citrix listed applications' bookmarks is shown in the user home page.</p> <p><b>Condition</b> : Issue is encountered only when 'Citrix listed applications' is the 1st entry in <b>Users &gt;User Roles &gt;[User-Name] &gt;Terminal Services &gt;Sessions</b>.</p> <p><b>Workaround</b>: Reorder the Terminal Services Sessions from <b>Users &gt;User Roles &gt; [User-Name] &gt;Terminal Services &gt;Sessions</b> page using up-down arrows and don't keep 'Citrix listed application' as the 1st entry.</p>
PCS-38731	<p><b>Symptom</b>: Enterprise onboarding profile push will not work on mobile end point.</p> <p><b>Condition</b>: When a new VPN client is installed on the Mobile end point.</p> <p><b>Workaround</b>: By using MDM server required profiles can be pushed to the mobile end point.</p>

Problem Report Number	Release Note
PCS-39459	<p><b>Symptom:</b> Upgrade is not working from 9.1R15(18393)classic to 9.1R17 HLGW (22091)</p> <p><b>Condition:</b> Upgrade from 9.1R15 build 18393 to 9.1R17 HLGW.</p> <p><b>Workaround:</b> Increase the idle timeout and max session length. Set the idle timeout to (300) and the max session length (360) minutes.</p>
PSD-13168	<p><b>Symptoms:</b> When browser extension is enabled, PSAL upgrade to latest might fail.</p> <p><b>Condition:</b> Client launch might fail if PSAL browser extension is enabled on a upgrade scenario.</p> <p><b>Workaround:</b> Reinstall of PSAL will launch clients without a issue.</p>
PCS-39504	<p><b>Symptom:</b> On launching JSAM/HOB, any of the following issues is observed on MAC Ventura machine.</p> <ul style="list-style-type: none"> <li>• "Failed to contact server." error displays</li> <li>• "Detected an internal error, please retry". error displays</li> <li>• Multiple PSAL popups appear.</li> <li>• JSAM/HOB is not launching on first try.</li> </ul> <p><b>Condition:</b> When using a lower PSAL version (22.2R1 or lower) on MAC OS Ventura .</p> <p><b>Workaround:</b></p> <ol style="list-style-type: none"> <li>1. Log out of the browser</li> <li>2. Log in again and cancel the PSAL popup message, "Do you want to allow this page to open PulseApplicationLauncher?"</li> <li>3. The PSAL download page appears after some time.</li> <li>4. Download and install the new version of PSAL.</li> <li>5. Log out and log in again</li> </ol>
PCS-38955	<p><b>Symptom :</b> FTP is not working with IPv6 FTP server</p> <p><b>Condition :</b> When admin configured IPv6 FTP server for archival</p> <p><b>Workaround :</b> Admin can use IPv4 FTP server for archiving</p>
PCS-36442	<p><b>Symptom:</b> "Failed to contact server" error prompted.</p> <p><b>Condition:</b> "Failed to contact server" error observed sometimes when auto-launch is enabled.</p>

Problem Report Number	Release Note
	<b>Workaround:</b> None
PCS-37839	<b>Symptom:</b> Citrix default ICA launch fail. <b>Condition:</b> When a user uses Citrix workspace app 2112 or later. <b>Workaround:</b> User can use Citrix workspace app version 2109.
PCS-37845	<b>Symptom:</b> VDI-Citrix Xendesktop launch fail. <b>Condition:</b> When a user uses Citrix workspace app 2112 or later. <b>Workaround:</b> User can use Citrix workspace app version 2109.
PCS-37219	<b>Symptom:</b> sg_agent is not able to detect the smart card, when end users use MAC OS with smart card redirect support RDP to windows machine. <b>Condition:</b> As per BSSL, since no RDC clients available on MAC, you may not have any solution as of now. <b>Workaround :</b> None.
PCS-39271	<b>Symptom:</b> None of the selected username data is deleted from the Behavioral Analytics User Report list. <b>Condition:</b> When compliant users is listed in report. <b>Workaround:</b> NA
PCS-32175	<b>Symptom:</b> The auth traffic is not following the selection of traffic interface. <b>Condition:</b> Even if admin configures auth traffic to go through management, it still goes through internal interface. <b>Workaround:</b> NA
PCS-36629	<b>Symptom:</b> ESP Throughput is dropping when users logins from two different source IP on Openstack KVM ISA6Kv <b>Condition:</b> With payload of 1300 bytes or higher, you might experience performance drop due to fragmentation. <b>Workaround:</b> With payload of 1300 bytes or lower, you will not hit this issue.
PCS-36937	<b>Symptom:</b> Enduser is not able to receive multicast traffic <b>Condition:</b> When the enduser is connected to VPN in ESP <b>Workaround:</b> NA
PCS-34315	<b>Symptom:</b> AD server will not able to join when default VLAN is enabled. <b>Conditions:</b> Default VLAN is enabled on interfaces.



Problem Report Number	Release Note
	<b>Workaround:</b> Enable Traffic decoupling and Map the setting of system-level interface and interface should be the default-VLAN interface of the internal interface.
PCS-39434	<p><b>Symptom:</b> Time on the ICS gateway goes out of sync, even through configured with NTP servers</p> <p><b>Conditions:</b> When DNS preferred mode is set to IPv6</p> <p><b>Workaround:</b></p> <ol style="list-style-type: none"> <li>1. Set DNS preferred mode to IPv4</li> <li>2. Go to <b>System &gt; Status &gt; Overview</b> page. Click <b>Edit</b> link under <b>System Date &amp; Time</b></li> <li>3. Click <b>Save Changes</b>.</li> </ol>
PCS-39255	<p><b>Symptom :</b> The dashboard graphs for HC failures and OS types are not populated.</p> <p><b>Workaround :</b> Restart services to fix the issue.</p>
PCS-39073	<p><b>Symptoms:</b> When you try to launch JSAM on MAC OS using browser extension you will see an error saying "jnlib file is malicious"</p> <p><b>Condition:</b> By default, browser extension is not enabled and customer do not see any major impact unless they enable browser extension. If browser extension is enabled then it is recommended not to use JSAM and HOB.</p> <p><b>Workaround:</b> Use custom protocol which is the workflow by default.</p>
PCS-39227	<p><b>Symptoms:</b> After launching JSAM an error prompts, "Safari can't find the server."</p> <p><b>Condition:</b> When a user launches JSAM on a MAC Ventura machine using the Safari browser, user may see "Safari can't find the server."</p> <p><b>Workaround:</b> The user can use the Chrome browser for the JSAM launch.</p>
PCS-39265	<p><b>Symptom:</b> HOB auto launch is not working.</p> <p><b>Condition:</b> When a user uses Windows as a client machine.</p> <p><b>Workaround:</b> User can do manual launch.</p>
PCS-38630	<p><b>Symptom:</b> Upgrade from pre-22.3R1 &gt; 22.3R1 appears to be stuck after importing system data.</p> <p><b>Conditions:</b> When upgrading the gateway from pre-22.3R1 &gt; 22.3R1</p> <p><b>Workaround:</b>The issue is seen due to increase in ICS package size. Refer <a href="#">KB</a> on how to workaround this issue.</p>

Problem Report Number	Release Note
PCS-39291	<p><b>Symptom:</b> When Home Icon in Floating tool bar is clicked, the end-user gets 'The page you requested could not be found' error.</p> <p><b>Conditions:</b> When the user clicks on Home Icon in the floating tool bar within a Advanced HTML5 session.</p> <p><b>Workaround:</b> Clear the browser cache and retry.</p>
PCS-36999	<p><b>Symptom:</b> Oauth authentication fails in the end user page while using dynamic URL. Oauth configurations are created using dynamic URL and upgraded to latest version. Authentication fails inconsistently while trying this scenario.</p> <p><b>Condition:</b> When creating Oauth server with dynamic URL and trying the authentication after upgrade.</p> <p><b>Workaround:</b></p> <ul style="list-style-type: none"> <li>• To delete existing Oauth configuration and create a new configuration in the latest version.</li> <li>• Upgrade without using dynamic URL (with manual configuration)</li> </ul>
PCS-38597	<p><b>Symptom :</b> In Dual Stack LDAP Authentication, user authentication fails if Primary server is IPv6 and backup servers are IPv4.</p> <p><b>Condition:</b> Issue exists only when primary server is configured as IPv6 and backup servers are IPv4, only in dual stack case.</p> <p><b>Workaround:</b> Configure IPv4 servers as Primary and IPv6 servers as Backup servers.</p>
PCS-37815	<p><b>Symptom:</b> Upgrade of gateway using DMI fails.</p> <p><b>Conditions:</b> When trying to upgrade gateway using DMI RPCs.</p> <p><b>Workaround:</b> Use Admin UI to upgrade the gateway.</p>
<b>Release 22.2R1</b>	
PCS-37128	<p><b>Symptom:</b> XML import fails in release 22.2R1 version when HTML5 resource profiles exported from release 9.1R15 or R16 .</p> <p><b>Condition:</b> Importing HTML5 resource profiles in to 22.2R1.</p> <p><b>Workaround:</b> NA</p>
PCS-35512	<p><b>Symptom:</b> User browses to appserver URL with 8083 port (http://appserver:8083/test.asp), it re-directs to some other webpage.</p>

Problem Report Number	Release Note
	<p><b>Condition:</b> When the user configure the appserver with kerberos functionality and tries to access the URL: http://appserver:8083/test.asp in end user page.</p> <p><b>Workaround:</b> Instead of browsing end user page, directly browse the login URL: http://appserver:8083/test.asp</p>
PCS-36912	<p><b>Symptom:</b> Displays "Exceeded maximum of 51 write attempts".</p> <p><b>Conditions:</b> During restart/reboot of the system.</p> <p><b>Workaround:</b> None. No functionality impact.</p>
PCS-36787	<p><b>Symptom:</b> Certificate validity check shows certificate expired for less than 90 days.</p> <p><b>Condition:</b> During certificate validity check.</p> <p><b>Workaround:</b> No functional impact, ignore the message.</p>
PCS-37104	<p><b>Symptom:</b> Downloaded Protected Zip File (1KB) is empty but actual file size is 2.07MB.</p> <p><b>Condition :</b> When the user configures the Appserver with protected file share and then downloads any protected file.</p> <p><b>Workaround:</b> Instead of getting files downloaded through zip, download individual file by clicking.</p>
PCS-35628	<p><b>Symptom:</b> Installing Ivanti Secure Access Client through browser fails.</p> <p><b>Condition:</b> After end user login, click on bookmark "PULSE UNIFIED CLIENT" start button, It fails to install Ivanti Secure Access Client.</p> <p><b>Workaround:</b> User to download Ivanti Secure Access Client directly from Server (System &gt; Maintenance &gt; Installers) and install on end point.</p>
PCS-36683	<p><b>Symptom:</b> Setup client uninstall will not work sometimes.</p> <p><b>Condition:</b> When a user tries to uninstall setup client.</p> <p><b>Workaround:</b> User has to reboot the client machine.</p>
PCS-36764	<p><b>Symptom:</b> File cannot be downloaded or deleted from the end user UI.</p> <p><b>Conditions:</b></p> <ul style="list-style-type: none"> <li>• Bookmarks for a file server have to be present in the end user UI.</li> <li>• Files have to be present in the server upon navigating from bookmark to the file server.</li> </ul> <p><b>Workaround:</b> None</p>

Problem Report Number	Release Note
PCS-36556	<p><b>Symptom:</b> Binary configuration import from 9.x classic to 22.2 gateway causes the gateway to disconnected from the nSA and hence no configuration upload happens to the nSA.</p> <p><b>Condition:</b> During Binary configuration import from 9.x classic to a 22.2 gateway, which is already registered to nSA. The configuration import brings the registered ICS device in a gateway not ready state on nSA thereby not updating the newly imported ICS configurations to nSA .</p> <p><b>Workaround:</b> Clear the nSA registration status by navigating to System &gt; Ivanti Neurons for Secure access &gt; Clear config and then Restart the Gateway service from Maintenance &gt; Platform &gt; Restart Services. After restart, register again with nSA.</p>
PCS-37090	<p><b>Symptom:</b> Black screen is shown when user tries to download PSAL from Safari browser.</p> <p><b>Condition:</b> When PSAL is downloaded and installed for the first time.</p> <p><b>Workaround:</b> After PSAL is installed, access the end user page and launch JSAM.</p>
PCS-37092	<p><b>Symptom:</b> End user Onboarding option is not displaying on MAC OS.</p> <p><b>Condition:</b> When a user uses MAC OS.</p> <p><b>Workaround:</b> N/A</p>
PCS-36675	<p><b>Symptom:</b> Panel Preferences for Admin/end user bookmarks is not shown.</p> <p><b>Condition:</b> When a user access the end user Panel Preferences page.</p> <p><b>Workaround:</b> N/A</p>
PCS-36684	<p><b>Symptom:</b> Page refresh issue on end user portal.</p> <p><b>Condition:</b> When a user configures wrong VDI login details and reconfigures with correct login details.</p> <p><b>Workaround:</b> User has to re-login to the end user portal.</p>
<b>Release 22.1R6</b>	
PCS-36319	<p><b>Symptom:</b> Save All Logs option missing from Events/User Access/Admin Access Logs.</p> <p><b>Condition:</b> When Admin navigates to Monitoring &gt; Events &gt; Logs and tries to Save Logs.</p> <p><b>Workaround:</b> NA</p>

Problem Report Number	Release Note
PCS-34870	<p><b>Symptom:</b> Clear config data fails with errors.</p> <p><b>Condition:</b> On ISA8000 platform admin console, when "Clear all configuration data at this Ivanti Connect Secure" is run from the "System Operations" options.</p> <p><b>Workaround:</b> After performing Clear config data, restart the system and choose the "Factory reset" option. This issue will be fixed in the future release.</p>
PCS-35850	<p><b>Symptom:</b> Disk and RAID status appears as Unknown for some time.</p> <p><b>Condition:</b> After adding the disk from console, when user immediately checks Disk and RAID status from UI, it appears asUnknown.</p> <p><b>Workaround:</b> After adding the disk from console, wait for one minute before checking Disk and RAID status from UI. It might take up to one min to sync the status between GUI and console.</p>
<b>Release 22.1R1</b>	
PCS-36093	<p><b>Symptom:</b> Configuration import fails with reason: software version used to create import file was '9.1R14 (build 16847)' current version of software is '22.1R1 (build 421)'.</p> <p><b>Condition:</b> When admin tries to import configuration from release 9.1R14 / 9.1R14.1 to 22.1R1.</p> <p><b>Workaround:</b> NA</p>
PCS-34435	<p><b>Symptom:</b> Third party related error messages seen on VA console.</p> <p><b>Condition:</b> Connect Secure registered with nSA.</p> <p><b>Workaround:</b> None. These messages can be ignored as it does not affect functionality.</p>
PCS-34301	<p><b>Symptom:</b> Connect Secure is not sending Microsoft Intune server request.</p> <p><b>Condition:</b> During the user authentication.</p> <p><b>Workaround:</b> Restart services will restart the MDM services.</p>
PCS-33729	<p><b>Symptom:</b> Cache cleaner policy is not getting imported when importing XML file for user role configured with cache cleaner policy.</p> <p><b>Condition:</b> During XML import of user role with cache cleaner policy.</p>

Problem Report Number	Release Note
	<b>Workaround:</b> None. Assigning cache cleaner policy to a user role is a deprecated feature.
PCS-34315	<b>Symptom:</b> AD server is not able to join when default VLAN is enabled. <b>Condition:</b> Default VLAN enabled on interfaces. <b>Workaround:</b> Enable Traffic decoupling and map the setting of system-level interface and interface to default-VLAN interface of the internal interface.
PCS-34546	9.X HLGW : KVM : <b>Symptom:</b> Post upgrade, not able to access GUI. <b>Condition:</b> After upgrading KVM appliance with gateway build. <b>Workaround:</b> NA
PCS-34530	<b>Symptom :</b> Rollback via console is not working on KVM appliance. <b>Condition:</b> Using rollback option in KVM appliance. <b>Workaround:</b> NA
PCS-34411	<b>Symptom:</b> Logs are not pushed from gateways to nSA. <b>Condition:</b> During 21.9R1 and 21.12R1 gateways upgrade to 22.1R1 and after certificate rotation, logs are not pushed. <b>Work Around:</b> Restarting the gateway services.
PCS-34253	<b>Symptom :</b> Cluster VIP owner details are not in sync between nSA and gateways. <b>Condition :</b> 22.1R1 Connect Secure AP cluster setup registered with nSA. <b>Work Around :</b> Rebooting the cluster setup will resolve the issue.
PCS-34681	<b>Symptom:</b> Roll back option not available in nSA for AA cluster. <b>Condition:</b> Connect Secure status is not updated properly to nSA. <b>Workaround:</b> Reboot the AA cluster.
PCS-34357	<b>Symptom :</b> Bandwidth consumption is more than configured when downloading files using SSL tunnel mode. <b>Condition :</b> Bandwidth policy has configured with minimum and maximum value and assigned to user roles which is having SSL as VPN tunnel mode. <b>Workaround :</b> Configure user roles with ESP tunnel mode for roles configured with bandwidth policy.
PCS-34870	<b>Symptom:</b> Reboot fails on selecting clear config from CLI menu. <b>Condition:</b> Select option 4 and then 6 from CLI menu. <b>Workaround:</b>

Problem Report Number	Release Note
	<ul style="list-style-type: none"> <li>• Factory Reset and proceed or,</li> <li>• If you have saved default config or clean config. Binary import can be done as workaround.</li> </ul>
PCS-34485	<p><b>Symptom:</b> Time track back by ~4 hours on Connect Secure.</p> <p><b>Conditions:</b> After admin restarts system services.</p> <p><b>Workaround:</b> None. Time gets re-synced with NTP servers automatically.</p>
<b>Release 21.12R1</b>	
PCS-32765	<p><b>Symptom:</b>Intermediate file bookmark page is shown when end user tries to access file bookmark.</p> <p><b>Conditions:</b>When end user tries to access Windows file bookmark.</p> <p><b>Workaround:</b> After end user provides credentials to access windows file bookmark, if you see the same file bookmark again, then you need to select the desired file bookmark.</p>
PCS-32717	<p><b>Symptom:</b> XML import fails for UserRecordSync configuration.</p> <p><b>Condition:</b> When UserRecordSync is enabled.</p> <p><b>Workaround:</b> NA</p>
PCS-32594	<p><b>Symptom:</b> Bookmarks are not getting Synced for end user.</p> <p><b>Condition:</b> When UserRecordSync is enabled.</p> <p><b>Workaround:</b> NA</p>
PCS-32543	<p><b>Symptom:</b> Pushing sign-in URLs, notifications and pages not supported.</p> <p><b>Condition:</b> Create any sign-in settings with URL.</p> <p><b>Workaround:</b> NA</p>
PCS-32467	<p><b>Symptom:</b> Latest syslog Server is displayed if entire cluster is selected.</p> <p><b>Condition:</b> Multiple syslog servers must be added in the cluster mode.</p> <p><b>Workaround:</b> NA</p>
PCS-32324	<p><b>Symptom:</b> Error messages related to upgrading cache seen under event logs.</p> <p><b>Condition:</b> After the Connect Secure upgrade.</p> <p><b>Workaround:</b> NA</p>

Problem Report Number	Release Note
PCS-30489	<p><b>Symptom:</b> Bandwidth is not restricted even though minimum and maximum levels are configured.</p> <p><b>Condition:</b> When Admission Privilege Level is configured for bandwidth management in ESP and SSL mode.</p> <p><b>Workaround:</b> NA</p>
PCS-30439	<p><b>Symptoms :</b> End user login fails for users created in Local authentication server with clear text password enabled.</p> <p><b>Condition:</b> Creating local authentication server with clear text enabled.</p> <p><b>Workaround:</b> For Non IKE use cases, do not enable clear text password option.</p>
PCS-29121	<p><b>Symptom :</b> Toolbar not visible for bookmarks in PTP mode when using Chrome and Edge browsers.</p> <p><b>Condition :</b> When web bookmark is configured to be accessed over PTP mode instead of rewriter mode.</p> <p><b>Workaround :</b></p> <ul style="list-style-type: none"> <li>• Open Connect Secure home page URL in new tab to see the toolbars.</li> <li>• While clicking on bookmarks from Connect Secure home page, select to open in new tab.</li> </ul>
PCS-32836	<p><b>Symptom:</b> Pulse Client copyright date is not updated with 2022 year.</p> <p><b>Condition:</b> Pulse Client copyrights year is shown as 2021.</p> <p><b>Workaround:</b> NA</p>
PCS-32596	<p><b>Symptom:</b> Upgrade from 9.1R13 and 9.1R12 GA to 9.1R13.1 is failing at the upload step with Access restricted error.</p> <p><b>Condition:</b> When Administrator session is set to default and an upgrade is initiated using the package file.</p> <p><b>Workaround:</b> Increase idle timeout to 400 and Max Session Length to 600 before starting the upgrade. <b>Administrators &gt; Delegated Admin Roles &gt; Administrators &gt; session timeout</b></p>
PCS-32374	<p><b>Symptom:</b> AD authentication fails with Role based VLAN.</p> <p><b>Condition:</b> When AD authentication is selected.</p> <p><b>Workaround:</b> NA</p>



Problem Report Number	Release Note
PCS-30917	<p><b>Symptom:</b> During session extension from Pulse Client or automatic session extension for the end user portal. New session count is getting incremented for the gateway, but old session is not deleted from nSA.</p> <p><b>Condition:</b> During session extension from Pulse Client or automatic session extension for the end user portal and license count has exhausted.</p> <p><b>Workaround:</b> NA</p>
PCS-32833	<p><b>Symptom:</b> The status info like cluster reboot/ICT/cluster upgrades are not synced between Gateways in nSA cluster.</p> <p><b>Condition:</b> In any cluster, the cluster wide actions status are not synced.</p> <p><b>Workaround:</b> This is only status information, the actually tasks are already performed.</p>
PCS-32906	<p><b>Symptom:</b> ISA VM machine ID getting changed.</p> <p><b>Conditions:</b> Navigate to <b>System&gt;Maintenance&gt;Options</b> and Check/Uncheck the "Enable Virtual Terminal console" check box and then click "<b>save changes</b>".</p> <p><b>Workaround:</b> NA</p>
PCS-32354	<p><b>Symptom:</b> Registration status of Connect Secure is in green color.</p> <p><b>Condition:</b> Importing binary config of existing registered Connect Secure system config.</p> <p><b>Workaround:</b> Clearing and re-registration of nSA.</p>
PCS-32834	<p><b>Symptom:</b> Test connection for AWS/Azure archival server is showing as "Failed to connect to S3 bucket, WrongBucketLocation".</p> <p><b>Condition:</b> When configuring AWS or Azure as archival server location.</p> <p><b>Workaround :</b> Admin can configure SCP or FTP Server for archiving.</p>
PCS-28777	<p><b>Symptom:</b> End User is not able to launch Apps listed in MS RDweb console.</p> <p><b>Condition:</b> End User is using Google Chrome Browser to login.</p> <p><b>Workaround:</b> End User can use MS Edge or Firefox browser to login and launch Apps.</p>
PCS-31245	<p><b>Symptom:</b> Logs from 9.x hlgw setup is not sent to nSA</p> <p><b>Condition:</b> When DNS preferred settings has configured with IPv6 in network overview page.</p> <p><b>Workaround :</b> Admin can configure DNS preferred settings as IPv4 in network overview page.</p>

Problem Report Number	Release Note
PCS-32404	<p><b>Symptom:</b> AP Cluster VIP migration is taking around 2 minutes when cluster VIP configured with IPv6 address</p> <p><b>Condition:</b> When cluster VIP configured with IPv6 address.</p> <p><b>Workaround :</b> None, time is a time delay in cluster VIP migration and cluster VIP migrates to other node.</p>
PCS-33249	<p><b>Symptom:</b> Error message "ERROR: ld.so. object '/home/lib/libdspreload.so' from /etc/ld/so/preload cannot be preloaded:" appears at the end of successful completion of Connect Secure boot</p> <p><b>Condition:</b> After the completion of Connect Secure installation and boot</p> <p><b>Workaround:</b> None. This does not affect the Connect Secure functionality.</p>
<b>Release 21.9R1</b>	
PCS-30626	<p><b>Symptom:</b> Failed to update profile for user error is seen in user access logs for every user.</p> <p><b>Condition:</b> Importing system and user binary configs from 9.x where UEBA is configured.</p> <p><b>Workaround:</b> The UEBA package has to be imported manually for the Adaptive Authentication feature to continue to work fine and stop getting these messages for every user.</p>
PCS-31165	<p><b>Symptom:</b> ESP to SSL session fallback happens randomly on L3 session.</p> <p><b>Conditions:</b> In AA Cluster setup, when VPN Tunneling connection profile is configured with ESP to SSL fallback, sometimes L3-VPN session can fallback to SSL mode after a node leaves and joins the Cluster.</p> <p><b>Workaround:</b> Restarting Services on the Cluster resumes all users VPN session to ESP mode.</p>
PCS-30694	<p><b>Symptom:</b> Number of concurrent users (xx) exceeded the system limit (2) seen in user access logs.</p> <p><b>Conditions:</b> When nSA Named User Mode is enabled in <b>System &gt; Configuration &gt; Licensing</b>.</p> <p><b>Workaround:</b> None. End-user does not see any warning and logins will work.</p>
PCS-31051	<p><b>Symptom:</b> Max Concurrent Users do not get updated immediately.</p> <p><b>Conditions:</b> After installing Connect Secure-EVAL license.</p>

Problem Report Number	Release Note
	<b>Workaround:</b> None. System takes around 3-4 minutes for the page to get updated.
PCS-30919	<p><b>Symptom:</b> In Advanced HTML5 session, Copy paste functionality does not work after a while.</p> <p><b>Conditions:</b>When connected to backend windows machines through Advanced HTML5 session.</p> <p><b>Workaround:</b>Disconnect and Reconnect to Advanced HTML5 session.</p>
PCS-31161	<p><b>Symptom:</b></p> <ul style="list-style-type: none"> <li>Error updating data for chart cloud_secure_roles seen in Admin logs.</li> <li>Dashboard charts are not getting updated.</li> </ul> <p><b>Conditions:</b> After upgrading to 21.9R1 gateway build</p> <p><b>Workaround:</b> None. Dashboard charts get updated after a while.</p>
PCS-30280	<p><b>Symptom:</b> Not able to launch Windows/Citrix terminal services through IPv6 address.</p> <p><b>Condition:</b> When end user enters IPv6 address to launch WTS/CTS.</p> <p><b>Workaround:</b> Launch with IPv4 address.</p>
PCS-31156	<p><b>Symptom:</b> Sessions are not synced between nodes on an AA/AP cluster.</p> <p><b>Condition:</b> Connect Secure failover because of reboot/power cycle.</p> <p><b>Workaround:</b> New sessions after node recovery will be synced across both nodes and data on insights will be accurate.</p>
PCS-31234	<p><b>Symptom:</b> HTML5 graph shows incorrect value for RDP sessions.</p> <p><b>Condition:</b> RDP sessions created on Connect Secure.</p> <p><b>Workaround:</b> No workaround.</p>
PCS-31046	<p><b>Symptom:</b> XML import from 9.x Connect Secure Gateway to 21.x Gateway fails with a directory-server attribute error in a corner condition.</p> <p><b>Condition:</b> When exported XML from 9.x Gateway has a authentication server as system local server and attribute server set to "same as above".</p> <p><b>Workaround:</b>In the XML file either:</p> <ol style="list-style-type: none"> <li>Set &lt;directory-server&gt; attribute value as None: &lt;directory-server&gt;None&lt;/directory-server&gt;.</li> </ol>

Problem Report Number	Release Note
	2. Or remove the <directory-server> attribute, save file, XML import will be successful after that.
PCS-31168	<p><b>Symptom</b> : WSAM resources being accessed through Connect Secure even though resources are denied is PSAM policy.</p> <p><b>Condition</b>: While modifying PSAM/WSAM policy from allow to deny.</p> <p><b>Workaround</b>: NA</p>
PCS-30652	<p><b>Symptom</b>: Antivirus host checker policy fails with error "server has not received any information on Mac OS big sur".</p> <p><b>Condition</b>: When Host checker policy with antivirus is configured on Mac Os big sur for pre-auth/post-auth.</p> <p><b>Workaround</b>: NA</p>
PCS-31058	<p><b>Symptom</b>: On ISA-V or PSA-v VMware platform, spikes in dashboard throughput graph are seen every 5 minutes, when NTP server is configured.</p> <p><b>Condition</b>: If NTP server is configured and there is time drift on gateway.</p> <p><b>Workaround</b>: Change view of graph to 2 days or more. Or use "Sync time with ESX host" in VMware tools and remove NTP server configuration on gateway.</p>
PCS-31213	<p><b>Symptom</b>: Multicast traffic does not flow thru Connect Secure Gateway when using IGMPv3.</p> <p><b>Condition</b>: Only when 3rd party tool send multicast traffic with IGMPv3.</p> <p><b>Workaround</b>: For multicast to work, IGMPv2 should be configured on 3rd party tool.</p>
PCS-30439	<p><b>Symptoms</b> : End user login fails for users created in Local authentication server with clear text password is enabled.</p> <p><b>Condition</b>: Creating local authentication server with clear text enabled.</p> <p><b>Workaround</b>: For Non IKEv2 use cases, use without enabling clear text password.</p>
PCS-31193	<p><b>Symptom</b>: HealthCheck REST API /api/v1/system/healthcheck?status=all returns Security gateway is inaccessible error.</p> <p><b>Conditions</b>: When the default gateway of internal port is NOT reachable.</p> <p><b>Workaround</b>: Make the internal gateway as reachable.</p>
PCS-30658	<p><b>Symptom</b>: Run Gateway Diagnostics option does not return any output.</p> <p><b>Conditions</b>: When triggering Run Gateway Diagnostics option from System Maintenance.</p>

Problem Report Number	Release Note
	<b>Workaround:</b> None. This command is not supported on Connect Secure.
PCS-29657	<b>Symptom:</b> Kill command is seen on ISA-V virtual console. <b>Condition:</b> On a fresh deploy of ISA-V on VMware ESXi, AWS or Azure. <b>Workaround:</b> No functionality is affected. The message can be safely ignored.
PCS-30629	<b>Symptom:</b> End-user sees old sign-in page instead of modernised sign-in page. <b>Conditions:</b> <ol style="list-style-type: none"><li>1. Connect Secure is configured to use Remote TOTP for Secondary Auth.</li><li>2. Remote TOTP server is not reachable.</li></ol> <b>Workaround:</b> None. If the Remote TOTP server is reachable, this page is not seen.
PCS-30854	<b>Symptom:</b> XML Import or Push Config fails with /users/user-roles/user-role [name=xyz-role]/html5-access/sessions. <b>Conditions:</b> When trying to do XML import or Push Config of Selective Config. <b>Workaround:</b> <ul style="list-style-type: none"><li>• XML Import: Remove sessions block under html5-access from XML file and then do XML import.</li><li>• Push Config: There is no workaround.</li></ul>

# Documentation

Ivanti documentation is available at <https://www.ivanti.com/support/product-documentation>.

## Technical Support

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

- <https://forums.ivanti.com/s/contactsupport>
- [support@ivanti.com](mailto:support@ivanti.com)

For more technical support resources, browse the support website  
<https://forums.ivanti.com/s/contactsupport>