



Ivanti Connect Secure Release Notes
22.5R1.3-22.1R1

Copyright Notice

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

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

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

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

Contents

| | |
|--|-----------|
| Revision History | 4 |
| Introduction | 5 |
| Security Advisory and Patch Update | 5 |
| Caveats | 9 |
| Hardware Platforms | 9 |
| Virtual Appliance Editions | 9 |
| Licensing Types | 15 |
| Upgrade Path | 15 |
| Configuration Migration Path | 16 |
| Noteworthy Information | 17 |
| What's New | 19 |
| Fixed Issues | 24 |
| Known Issues | 30 |
| Documentation | 53 |
| Technical Support | 53 |

Revision History

The following table lists the revision history for this document:

| Document Revision | Date | Description |
|-------------------|---------------|--|
| 12.0 | February 2024 | Updated with Security Advisory and Patch Release updates for 22.x releases. |
| 11.0 | Aug 2023 | Updated version and build number with migration path for 22.5R1 and added with new features. |
| 10.0 | July 2023 | Updated version and build number with migration path for 22.5R2 and added with new features. |
| 9.0 | June 2023 | Updated version and build number with migration path for 22.4R2.1 |
| 8.0 | April 2023 | Updated New Features, Known issue in 22.4R1 and Fixed issue in 22.4R1 |
| 7.0 | January 2023 | Updated with new client version |
| 6.0 | November 2022 | Updated New Features, Known issue in 22.3R1 and Fixed issue in 22.3R1 |
| 5.0 | July 2022 | Updated Known issue in 22.2R1 and Fixed issue in 22.2R1 |
| 4.0 | June 2022 | Update Known issue in 22.1R1 and Fixed issue in 22.1R6 |
| 3.0 | April 2022 | Updated Known and fixed issues for 22.1R1 |
| 2.0 | January 2022 | Updated Known issues for 21.12R1 |
| 1.0 | October 2021 | Initial Publication for 21.9R1 |

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.

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:

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

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

The build details of ICS Gateways, which includes CVE fixes are listed below:

Build Details for 22.5R1.3

- ICS 22.5R1.3 Build 2213

- ISAC 22.3R3 Build 19959
- Default ESAP version 4.0.5

Build Details for 22.5R1.2

- ICS 22.5R1.2 Build 2213
- ISAC 22.3R3 Build 19959
- Default ESAP version 4.0.5

Build Details for 22.5R1

- ICS 22.5R1 Build 2037
- ISAC 22.3R3 Build 19959
- Default ESAP version 4.0.5

Build Details for 22.4R2.4

- ICS 22.4R2.4 Build 2169
- ISAC 22.3R1 Build 18209
- Default ESAP version 4.0.5

Build Details for 22.4R2.3

- ICS 22.4R2.3 Build 2159
- ISAC 22.3R1 Build 18209
- Default ESAP version 4.0.5

Build Details for 22.4R2.1

- ICS 22.4R2.1 Build 1725
- ISAC 22.3R2 Build 19787
- Default ESAP version 4.0.5

Build Details for 22.4R2

- ICS 22.4R2 Build 1531
- ISAC 22.3R1 Build 18209
- Default ESAP version 4.0.5

Build Details for 22.4R1.2

- ICS 22.4R1.2 Build 2173
- ISAC 22.3R1 Build 18209
- Default ESAP version 4.0.5

Build Details for 22.4R1.1

- ICS 22.4R1.1 Build 2165
- ISAC 22.3R1 Build 18209
- Default ESAP version 4.0.5

Build Details for 22.4R1

- ICS 22.4R1 Build 1439
- ISAC 22.3R1 Build 18209
- Default ESAP version 4.0.5

Build Details for 22.3R1.2

- ICS 22.3R1.2 Build 2075
- ISAC 22.3R1 Build 1295
- Default ESAP version 4.0.5

Build Details for 22.3R1.1

- ICS 22.3R1.1 Build 2071
- ISAC 22.3R1 Build 1295

- Default ESAP version 4.0.5

Build Details for 22.3R1

- ICS 22.3R1 Build 1647
- ISAC 22.3R1 Build 1295
- Default ESAP version 4.0.5

Build Details for 22.2R4.2

- ICS 22.2R4.2 Build 1481
- ISAC 22.2R1 Build 1295

Build Details for 22.2R4.1

- ICS 22.2R4.1 Build 1475
- ISAC 22.2R1 Build 1295

Build Details for 22.2R3

- ICS 22.2R3 Build 1283
- ISAC 22.2R1 Build 1295

Build Details for 22.2R1

- ICS 22.2R1 Build 657
- nSA GW 9.1R15 Build 18393
- PDC 9.1R15 Build 15819
- ISAC 22.2R1 Build 1295
- Default ESAP version 3.7.5

Build Details for 22.1R6.1

- ICS 22.1R6.1 Build 893

Build Details for 22.1R6

- ICS 22.1R6 Build 575

Build Details for 22.1R1

- ICS 22.1R1 Build 421
- nSA GW 9.1R14 Build 18099
- PDC 9.1R14 Build 13525
- Default ESAP version 3.7.5

Caveats

The following feature is not supported in this gateway release:

- Multicast with IGMP
- Enterprise onboarding is not supported in Release 22.4R2.
- Upgrade from 22.5R2.1/22.4R2 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.
- 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.

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 22.5R1, 22.5R2.1, 22.4R2.1, 22.4R2, 22.4R1 and 22.3R1

| Variant | Platform | vCPU | RAM | Disk Space |
|---|--------------------------------------|------|-------|------------|
| VMware ESXi 7.0.2 (17867351) ESXi 6.7.0 | ISA4000-V | 4 | 8 GB | 40 GB |
| | ISA6000-V | 8 | 16 GB | 40 GB |
| | ISA8000-V | 12 | 32 GB | 40 GB |
| Azure-V | ISA4000-V (Standard DS3 V2 - 3NICs) | 4 | 14 GB | 40 GB |
| | ISA4000-V (Standard_D4s_v3 - 2NICs) | 4 | 14 GB | 40 GB |
| | ISA6000-V (Standard DS4 V2 -3 NICs) | 8 | 28 GB | 40 GB |
| | ISA6000-V (Standard D8s V3) | 8 | 32 GB | 40 GB |
| | ISA8000-V (Standard D16s V3) | 16 | 64 GB | 40 GB |
| | ISA4000-V (F4s_v2) | 4 | 8 GB | 40 GB |
| | ISA6000-V (F8s_v2) | 8 | 16 GB | 40 GB |
| | ISA8000-V (F16s_v2) | 16 | 32 GB | 40 GB |
| AWS-V | ISA4000-V (M5.xlarge - 3 NICs) | 4 | 16 GB | 40 GB |
| | ISA6000-V (M5.2xlarge - 3 NICs) | 8 | 32 GB | 40 GB |
| | ISA8000-V (M5.4xlarge - 3 NICs) | 16 | 64 GB | 40 GB |
| | ISA4000-V (t3.xlarge - 3 NICs) | 4 | 16 GB | 40 GB |
| | ISA6000-V (t3.2xlarge - 3 NICs) | 8 | 32 GB | 40 GB |

| Variant | Platform | vCPU | RAM | Disk Space |
|---|-------------------------------------|------|-------|------------|
| GCP | ISA4000-V (n2-standard-4 - 3 NICs) | 4 | 16 GB | 40 GB |
| | ISA4000-V (n1-standard-4 - 3 NICs) | 4 | 16 GB | 40 GB |
| | ISA6000-V (n2-standard-8 - 3 NICs) | 8 | 32 GB | 40 GB |
| | ISA6000-V (c2-standard-8 - 3 NICs) | 8 | 32 GB | 40 GB |
| | ISA 8000-V(n2-standard-16 - 3 NICs) | 16 | 64 GB | 40 GB |
| OpenStack KVM OpenStack Wallaby on Ubuntu 20.04 LTS | ISA4000-V | 4 | 8 GB | 40 GB |
| | ISA6000-V | 8 | 16 GB | 40 GB |
| | ISA8000-V | 12 | 32 GB | 40 GB |
| Hyper-V Microsoft Hyper-V Server 2016 and 2019 | ISA4000-V | 4 | 8 GB | 40 GB |
| | ISA6000-V | 8 | 16 GB | 40 GB |
| | ISA8000-V | 12 | 32 GB | 40 GB |
| Nutanix AHV 2021 | ISA4000-V | 4 | 8 GB | 40 GB |
| | ISA6000-V | 8 | 16 GB | 40 GB |
| | ISA8000-V | 12 | 32 GB | 40 GB |

Virtual appliance qualified in 22.2R1

| Variant | Platform | vCPU | RAM | Disk Space |
|---|--------------------------------------|------|-------|------------|
| VMware ESXi 7.0.2 (17867351) ESXi 6.7.0 | ISA4000-V | 4 | 8 GB | 40 GB |
| | ISA6000-V | 8 | 16 GB | 40 GB |
| | ISA8000-V | 12 | 32 GB | 40 GB |
| Azure-V | ISA4000-V (Standard DS3 V2 - 3NICs) | 4 | 14 GB | 40 GB |
| | ISA4000-V (Standard_D4s_v3 - 2NICs) | 4 | 14 GB | 40 GB |
| | ISA6000-V (Standard DS4 V2 -3 NICs) | 8 | 28 GB | 40 GB |
| | ISA6000-V (Standard D8s V3) | 8 | 32 GB | 40 GB |
| | ISA8000-V (Standard D16s V3) | 16 | 64 GB | 40 GB |
| AWS-V | ISA4000-V (M5.xlarge - 3 NICs) | 4 | 16 GB | 40 GB |
| | ISA6000-V (M5.2xlarge - 3 NICs) | 8 | 32 GB | 40 GB |
| | ISA8000-V (M5.4xlarge - 3 NICs) | 16 | 64 GB | 40 GB |
| | ISA4000-V (t3.xlarge - 3 NICs) | 4 | 16 GB | 40 GB |
| | ISA6000-V (t3.2xlarge - 3 NICs) | 8 | 32 GB | 40 GB |

| Variant | Platform | vCPU | RAM | Disk Space |
|---|-------------------------------------|------|-------|------------|
| GCP | ISA4000-V (n2-standard-4 - 3 NICs) | 4 | 16 GB | 40 GB |
| | ISA4000-V (n1-standard-4 - 3 NICs) | 4 | 16 GB | 40 GB |
| | ISA6000-V (n2-standard-8 - 3 NICs) | 8 | 32 GB | 40 GB |
| | ISA6000-V (c2-standard-8 - 3 NICs) | 8 | 32 GB | 40 GB |
| | ISA 8000-V(n2-standard-16 - 3 NICs) | 16 | 64 GB | 40 GB |
| OpenStack KVM OpenStack Wallaby on Ubuntu 20.04 LTS | ISA4000-V | 4 | 8 GB | 40 GB |
| | ISA6000-V | 8 | 16 GB | 40 GB |
| | ISA8000-V | 12 | 32 GB | 40 GB |
| Hyper-V Microsoft Hyper-V Server 2016 and 2019 | ISA4000-V | 4 | 8 GB | 40 GB |
| | ISA6000-V | 8 | 16 GB | 40 GB |
| | ISA8000-V | 12 | 32 GB | 40 GB |

Virtual appliance qualified in 22.1R1

| Variant | Platform | vCPU | RAM | Disk Space |
|---|-----------|------|-------|------------|
| VMware ESXi 7.0.2 (17867351) ESXi 6.7.0 | ISA4000-V | 4 | 8 GB | 40 GB |
| | ISA6000-V | 8 | 16 GB | 40 GB |
| | ISA8000-V | 12 | 32 GB | 40 GB |

| Variant | Platform | vCPU | RAM | Disk Space |
|---------|---------------------------------------|------|-------|------------|
| Azure-V | ISA4000-V (Standard DS3 V2 - 3NICs) | 4 | 14 GB | 40 GB |
| | ISA4000-V (Standard_D4s_v3 - 2NICs) | 4 | 14 GB | 40 GB |
| | ISA6000-V (Standard DS4 V2 - 3 NICs) | 8 | 28 GB | 40 GB |
| | ISA6000-V (Standard D8s V3) | 8 | 32 GB | 40 GB |
| | ISA8000-V (Standard D16s V3) | 16 | 64 GB | 40 GB |
| AWS-V | ISA4000-V (M5.xlarge - 3 NICs) | 4 | 16 GB | 40 GB |
| | ISA6000-V (M5.2xlarge - 3 NICs) | 8 | 32 GB | 40 GB |
| | ISA8000-V (M5.4xlarge - 3 NICs) | 16 | 64 GB | 40 GB |
| | ISA4000-V (t3.xlarge - 3 NICs) | 4 | 16 GB | 40 GB |
| | ISA6000-V (t3.2xlarge - 3 NICs) | 8 | 32 GB | 40 GB |
| GCP | ISA4000-V (n2-standard-4 - 3 NICs) | 4 | 16 GB | 40 GB |
| | ISA4000-V (n1-standard-4 - 3 NICs) | 4 | 16 GB | 40 GB |
| | ISA6000-V (n2-standard-8 - 3 NICs) | 8 | 32 GB | 40 GB |
| | ISA6000-V (c2-standard-8 - 3 NICs) | 8 | 32 GB | 40 GB |
| | ISA 8000-V(n2-standard-16 - 3 NICs) | 16 | 64 GB | 40 GB |

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

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 |
| 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*

Upgrade Path

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

- i Follow the mandatory steps listed in the [KB44877](#) before staging or upgrading to prevent upgrade related issues.
- i Upgrade from 22.5R2.1/22.4R2 version to R1 version is not supported. Refer the [supported upgrade path forum link](#) for more details.
- i Upgrade path is not supported for FIPS mode (enabled) from release 22.3R1 or prior releases. Upgrade can only be done with FIPS mode disabled.

| Upgrade to | Upgrade From (Supported Versions) | Qualified |
|------------|-----------------------------------|-----------|
| 22.5R1 | 22.4R1, 22.3R1 | Q |

| Upgrade to | Upgrade From (Supported Versions) | Qualified |
|--------------|-----------------------------------|-----------|
| 22.5R2.1 | 22.4R2.1, 22.4R2, 22.4R1, 22.3R1 | Q |
| 22.4R2.1 | 22.4R2, 22.4R1, 22.3Rx and 22.2Rx | Q |
| 22.4R2 | 22.4R1, 22.3Rx and 22.2Rx | Q |
| 22.4R1(FIPS) | 22.3Rx and 22.2Rx | Q |
| 22.3R1 | 22.2Rx and 22.1Rx | Q |
| 22.2R1 | 22.1R1 and 21.12R1 | Q |
| 22.1R6 | 22.1R1 and prior releases | Q |
| 22.1R1 | 21.12R1 and 21.9R1 | Q |

Upgrade Path in 22.2R3

| Upgrade to | Upgrade From (Supported Version) | Qualified |
|------------|----------------------------------|-----------|
| 22.2R3 | 22.2R1 and 22.1R1 | Q |




FIPS mode supports fresh installation and upgrade for VMware images and only upgrade for Cloud (AWS, Azure, GCP) images.

Configuration Migration Path

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

| Migrate to | Migrate From (Supported Versions) | Qualified |
|------------|---|-----------|
| 22.5R1 | 9.1R18.1, 9.1R18, 9.1R14.3 and nSA supported 9.1R17 | Q |
| 22.5R2.1 | 9.1R18.1, 9.1R18, 9.1R14.3 and nSA supported 9.1R17 | Q |
| 22.4R2.1 | 9.1R17 and nSA supported 9.1R18 | Q |
| 22.4R2 | 9.1R18, 9.1R17.1, 9.1R17, 9.1R16.2, 9.1R14.3 and nSA supported 9.1R17 | Q |


| Migrate to | Migrate From (Supported Versions) | Qualified |
|------------|---|-----------|
| 22.4R1 | 9.1R18, 9.1R17.1, 9.1R17, 9.1R16.2, 9.1R14.3 and nSA supported 9.1R17 | Q |
| 22.3R1 | 9.1R17, 9.1R16, 9.1R15, 9.1R14, and nSA supported 9.1R15 | Q |
| 22.2R1 | 9.1R15, 9.1R14.1, 9.1R13.2, and nSA supported 9.1R14 | Q |
| 22.1R6 | 9.1R14.1 or prior releases | Q |
| 22.1R1 | 9.1R13.2 or prior releases | Q |
| 21.12R1 | 9.1R13.2 or prior releases | Q |
| 21.9R1 | 9.1R12 or prior releases | Q |

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

Noteworthy Information

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 22.5R2.1/22.4R2 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

What's New

22.5R1

- **Subnet Options for DHCPv6 address assignment in Connection Profiles:** ICS now supports options specifying the subnet from which DHCPv6 servers need to assign IPv6 address to Remote users. This option allows ICS to specify the subnet on which to allocate an IPv6 address. You can specify the IPv6 prefix address, which defines the range of IPv6 addresses to be assigned by the DHCPv6 server for the Remote users. For more details, see [IPv6 address assignment in table](#).
- **Host Checker Timeout** can be configured to accommodate the network responsiveness under various conditions. For more information, see [Host Checker Configuration Guide](#).



22.5R2.1 features are supported in 22.5R1.

22.5R2.1

- **DHCPv6 Server:** Enhanced to support IPv6 address. For more details, see [IPv6 address assignment in table](#).
- **Port Probe support for IPv6:** Port probing method now supports both IPv4 and IPv6 addresses with improved reliability. 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](#).

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.

22.4R1

- IPv6 support for File Resource Profile: This feature 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

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.

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.

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.



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.

Fixed 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 |
|-------------------------|--|
| Release 22.5R1 | |
| PRS-416576 | Application crash issue when iOS/Android client accessing IPv4 resources using ICS server with Application visibility enabled is now resolved. |
| PRS-416513 | ICS is synchronizing users in Auth Servers to Pulse One |
| PRS-415055 | Launch JSAM policy fails to launch JSAM |
| PRS-416032 | Unable to download files or folders that contain special characters while using Windows file sharing. |
| PRS-415997 | CGI server process crashing frequently in unique environments and configurations. |
| 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. |
| 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-416351 | HTML Tag's are not working as expected in the Personalized greetings page. |
| Release 22.5R2.1 | |
| PZT-40529 | " cgi-server" process may crash when syncing the configurations from nSA. |
| PZT-40223 | Communication issue between nSA and ICS gateway causing user login failure. |
| PRS-416873 | Error joining ICS to AD domain if SMBv1 is disabled. |

| Problem Report Number | Summary |
|-------------------------|---|
| | <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 link.</p> |
| PRS-416911 | <p>SAML Transfer failed with error message "Relay State does not match with the Server Host name".</p> <p> The Sign-in policy should be configured with the login URL, if the login URL is different from the Host FQDN.</p> |
| 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. |
| 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. |
| 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. |
| Release 22.4R2.1 | |

| Problem Report Number | Summary |
|------------------------------|---|
| PRS-415402 | Filename Is Trimmed After Uploading via File Share Server Bookmark in ICS 22.X Versions. See forum link 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. |
| Release 22.4R1 | |
| 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 |
| PRS-412571 | Ivanti Connect Secure - Sorting issue for the core access files |
| PRS-412382 | 22.1R6 System.J corrupted which causes reboot the device |
| Release 22.3R1 | |
| 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. |

| Problem Report Number | Summary |
|------------------------------|---|
| PCS-37092 | End user Onboarding option is not displaying on MAC OS. |
| PCS-36675 | Panel Preferences for Admin/end user bookmarks is not shown. |
| Release 22.2R1 | |
| 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. |
| Release 22.1R6 | |
| 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)'" |
| Release 22.1R1 | |
| PCS-30919 | Copy paste from Advance HTML5 session stops working after a while. |
| PCS-32765 | Flow change seen in End User portal while DFS 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. |

| Problem Report Number | Summary |
|------------------------------|---|
| 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. |
| Release 21.12R1 | |
| 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 | DFS: 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 | DFS: health check REST API is returning 500 Internal Server error. |
| PCS-30658 | System Maintenance > Run Diagnostics throws error. |

| Problem Report Number | Summary |
|------------------------------|---|
| PCS-29657 | Kill command seen on the virtual console on fresh deploy of 21.6R2_273. |
| PCS-30629 | DFS: 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 |

Known Issues

The following table lists the known issues in respective releases:

i For the complete list of current Known Issues, see [here](#).

i 22.4R1 Known issues are also applicable to 22.4R2.

| Problem Report Number | Release Note |
|-------------------------|--|
| Release 22.5R1 | |
| PCS-43061 | <p>Symptom: Error message is observed once the user log's out.</p> <p>Condition: When JSAM with JDK 21 beta version is used on Windows 11 and Mac.</p> <p>Workaround: Use JSAM with JDK 17 on windows and Mac OS(Sonoma and Ventura)</p> |
| PCS-43282 | <p>Symptom: Integrity scanner could detect mismatch files randomly or occasionally.</p> <p>Condition: After upgrading the ICS, sometimes Integrity scanner detects mismatch file.</p> <p>Workaround: Do a rollback and re-upgrade.</p> |
| PCS-38894 | <p>Symptom: Advanced HTML5 external storage feature will not work.</p> <p>Condition: When external storage server contains special characters in the password.</p> <p>Workaround: Do not use any special characters in the password.</p> |
| PCS-41732 | <p>Symptom: Port probe: Internal port IPv6 address is incorrectly populated when the user selects Management port with family type as IPv6.</p> <p>Condition: Interface port is selected first and then family type.</p> <p>Workaround: Select family type first and then select the Interface as Internal/Management Port.</p> |
| PPS-10870 | <p>Symptom: OAuth token encryption using ECC certificates fails.</p> <p>Workaround: Use RSA certificates for Token Encryption</p> |
| Release 22.5R2.1 | |

| Problem Report Number | Release Note |
|-----------------------|---|
| PCS-43559 | <p>Symptom: AD join from troubleshooting page fails with Error "Failed to find DC for domain <DOMAIN NAME> - Undetermined error".</p> <p>Condition: When AD container name contains spaces and was different than the default "Computers".</p> <p>Workaround: Use quotes in the AD configuration page if the AD container name has spaces.</p> |
| PCS-42906 | <p>Symptom : Few expired trusted server CA are not getting deleted.</p> <p>Condition : When checking Trusted Server CA Page, using "Show only expired CAs" option enabled.</p> <p>Workaround : Admin can import latest CAs if necessary</p> |
| PCS-41732 | <p>Symptom: Port probe: Internal port IPv6 address is incorrectly populated when the user selects Management port with family type as IPv6.</p> <p>Condition: Interface port is selected first and then family type.</p> <p>Workaround: Select family type first and then select the Interface as Internal/Management Port.</p> |
| PPS-10870 | <p>Symptom: OAuth token encryption using ECC certificates fails.</p> <p>Workaround: Use RSA certificates for Token Encryption</p> |
| PCS-38894 | <p>Symptom: Advanced HTML5 external storage feature will not work.</p> <p>Condition: When external storage server contains special characters in the password.</p> <p>Workaround: Do not use any special characters in the password.</p> |
| PCS-42593 | <p>Symptom: Stats for other node are not accessible from the current cluster node.</p> <p>Conditions:</p> <ol style="list-style-type: none"> 1. Go to System > Status > Overview. 2. Select the other node from the drop down in any of the charts. <p>Workaround: None. Login to the other node to get the charts.</p> |
| PCS-42347 | <p>Symptom: Multiple authentication successful messages are observed in user access logs when user tries OWA 2016 or above with kerberos SSO.</p> <p>Workaround:NA</p> |
| PCS-42311 | <p>Symptom: VPN fails to connect with Login Failed Error.</p> |

| Problem Report Number | Release Note |
|-----------------------|--|
| | <p>Condition: When Host checker is configured without enforcing at realm</p> <p>Workaround: Enforce same host checker policies at realm also.</p> |
| Release 22.4R2 | |
| PCS-37647 | <p>Symptom: Enterprise on-boarding feature will not work.</p> <p>Condition: When end user uses on-boarding feature.</p> <p>Workaround: None</p> |
| PCS-37637 | <p>Symptom: Test enrollment will not work</p> <p>Condition: When end user uses on-boarding feature.</p> <p>Workaround: None</p> |
| PCS-40086 | <p>Symptom : Browser based Certificate authentication is failing when TLS 1.3 is enabled on the ICS</p> <p>Condition: Browser based Certificate authentication fails when admin enables TLS 1.3 on ICS.</p> <p>Workaround: Admin need to enable TLS 1.2 (refer to KB)</p> |
| PCS-41506 | <p>Symptom: KB link for TLS 1.3 client support warning on the dashboard page takes you to a broken link.</p> <p>Condition: Click KB45694 link shown in the dashboard for Client impact with TLS 1.3.</p> <p>Workaround: See KB for details.</p> |
| PCS-35445 | <p>Symptom: Unable to set FIPS mode for web server.</p> <p>Condition: FIPS mode is not supported</p> <p>Workaround: None</p> |
| PCS-39643 | <p>Symptom: Console doesn't respond to user input when selecting "change SELinux mode".</p> <p>Condition: Post cluster upgrade to 22.4R2.</p> <p>Workaround: Restart services from the UI.</p> |
| PCS-39986 | <p>Symptom: ICS initial configuration is not getting configured automatically from vApp options</p> <p>Conditions: After performing clear config operation through VM Virtual Console</p> |

| Problem Report Number | Release Note |
|-----------------------|--|
| | Workaround: None. Configure ICS initial configuration such as IP address, admin user, self-signed cert details manually |
| PCS-40824 | <p>Symptom : Active user page in cluster nodes are not in sync for connected users, this happens when the cluster splits and joins.</p> <p>Condition : When cluster splits and joins this occurs.</p> <p>Workaround : None, it's just a display issue. In new session it is displayed correctly.</p> |
| PCS-41405 | <p>Symptom : VM upgrade and installation progress messages before reboot are not seen on VM serial console</p> <p>Condition: when upgrade was performed from 22.4r2 to higher release</p> <p>Workaround: None</p> |
| PCS-41031 | <p>Symptom: Kernel rate limiting is not working on config import</p> <p>Condition: During config import from 22.4r2 with Kernel rate limiting enabled to another 22.4R2 setup.</p> <p>Workaround: 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.</p> |
| PCS-40902 | <p>Symptom: Active Sync with Cert and Kerberos Constrained Delegation (KCD) does not work.</p> <p>Condition: When TLS 1.3 is enabled on ICS in bound settings.</p> <p>Workaround: Enable TLS 1.2 on ICS in bound settings.</p> |
| PCS-40467 | <p>Symptom: On single core CPU platform, web server snapshot can be generated upon Security related configuration change.</p> <p>Condition: Upon change in Security configuration (such as change in TLS version) old web server process exits with crash</p> <p>Workaround: NA</p> |
| PCS-40154 | <p>Symptom: Sometimes, Advanced HTML5 session does not respond to mouse clicks.</p> <p>Conditions: This issue happens usually when user tries to copy text using mouse on a ssh terminal session within HTML5 session.</p> <p>Workaround: Disconnecting and reconnecting the Advanced HTML5 session solves the issue.</p> |

| Problem Report Number | Release Note |
|-----------------------|---|
| PCS-39794 | <p>Symptom: If the server has TLS 1.3 enforced, the existing client connections and upgrades fail.</p> <p>Condition: TLS 1.3 enforced for the secure connections.</p> <p>Workaround: Enable the TLS 1.2 and higher option in the server, connect to the server and upgrade to the latest versions.</p> |
| PCS-39045 | <p>Symptom : TLS 1.3 is not supported on mobile VPN client.</p> <p>Condition: Mobile Authentication will not work when the user enables TLS 1.3 on ICS.</p> <p>Workaround: Select TLS 1.2 on the ICS server.</p> |
| PCS-39942 | <p>Symptom: DMI based script no longer able to connect to ICS</p> <p>Conditions: After ICS is upgraded to 22.4R2</p> <p>Workaround: NA.</p> |
| PCS-38817 | <p>Symptom: Test connection for AWS/Azure archival server is showing as "Failed to connect to S3 bucket, WrongBucketLocation"</p> <p>Condition: When configuring AWS or Azure as archival server location.</p> <p>Workaround : Admin can configure SCP or FTP Server for archiving.</p> |
| PCS-40729 | <p>Symptom: Cluster creation with IPV6 and default VLAN Id is not supported.</p> <p>Workaround: NA</p> |
| PCS-41273 | <p>Symptom: End-users are receiving "VPN Server is busy and unable to accept new connections." on the ISA Client, and unable to access intranet.</p> <p>Conditions: When system operations (VIP failover, reboot, restart of services) are performed on the Gateway when users are logged in.</p> <p>Workaround: 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.</p> |
| PCS-41014 | <p>Symptom: Upgrading from 22.4R2 to R1 builds will not show error when tried via REST API or DMI.</p> <p>Workaround: 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.</p> |
| Release 22.4R1 | |

| Problem Report Number | Release Note |
|-----------------------|--|
| PCS-40794 | <p>Symptom: Launching the Web bookmark via JSAM has issues.</p> <p>Condition: When the PSAL is not installed on the client machine.</p> <p>Workaround: Create web bookmark to launch via the rewriter engine instead of JSAM.</p> |
| PCS-40656 | <p>Symptom: On a Mobile device, if user logged in to web portal via browser and launching VPN connection will fail to establish VPN session.</p> <p>Condition: 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>Workaround: Enable Secure Application Manager feature under a user role configuration on ICS.</p> |
| PCS-41115 | <p>Symptom: JSAM logout button throws an internal error message.</p> <p>Condition: when open jdk-17 java is installed</p> <p>Workaround: No feature impact, click the ok button on the error screen JSAM applet will logout.</p> |
| PCS-41007 | <p>Symptom: ICS does not send logs to remote syslog servers and NSA impacting analytics</p> <p>Conditions: This is seen in the following scenario:</p> <ol style="list-style-type: none"> 1. Preferred mode is set to IPv6 2. Hostname is used to specify remote syslog server, and it resolves to both IPv4 and IPv6 3. Preferred network to contact NSA is set via Management port 4. Management port is configured with IPv6, but in disabled state <p>Workaround:</p> <ol style="list-style-type: none"> 1. Re-enable IPv6 on management port, if possible (or) Remove IPv6 from management port 2. Do restart of services or make a change in any of the syslog server config in Admin UI. |
| PCS-40067 | <p>Symptom: Missing certificate error is not displayed when user connects to Certificate based VPN profile without a mapped certificate in the profile</p> <p>Workaround: Map/add user certificate to the profile</p> |

| Problem Report Number | Release Note |
|-----------------------|---|
| PCS-39675 | Symptom: Start button for JSAM launch in Ubuntu is failings Workaround: No workaround |
| PCS-38989 | Symptom: Connection with syslog server is failing. Workaround : Restart the syslog server. |
| PCS-40006 | Symptom: File browsing with hostname is going through IPV4 address when "Preferred DNS Response:" is configured as IPv6. Workaround: Use the IPv6 address instead of host name. |
| PCS-40007 | Symptom: File browsing with hostname is not working when DNS response has IPv6 address only. Condition: 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. Workaround: NA |
| PCS-40910 | Symptom: When file server/share is configured with hostname, hostname will not get resolve to IPv6 address. Conditions: File Server/Share configuration with hostname. Workaround: Use IPv6 address while configuring instead of hostname. |
| PPS-10665 | Symptom: Compliance check fails on MacOSX, while using IPv6. Workaround: None |
| Release 22.3R1 | |
| PCS-37354 | Symptom: Ping6 with host name is not working. Condition: When admin performs ping6 operation using host name. Workaround: Admin can perform ping6 using IPv6 address. |
| PZT-36727 | Symptom: SNMP timeouts occurring than usual expected rate. Condition: When the queries are sent aggressively like around 57 queries/sec timeouts occur. Workaround: Increase the querying time for example to 57 queries in 2-3 seconds to see comparatively see less timeouts. |
| PCS-39623 | Symptom: Upgrade of cluster node fails with "Unable to extract installer" error message. |

| Problem Report Number | Release Note |
|-----------------------|--|
| | <p>Conditions:</p> <ol style="list-style-type: none"> 1. Upgrade triggered on a Cluster 2. Node-1 upgrades successfully to 22.3R1 3. Node-1 asks Node-2 to upgrade 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>Workaround:</p> <ol style="list-style-type: none"> 1. Power cycle Node-2 2. Press Tab and boot into Standalone mode 3. Access the UI and follow the procedure mentioned in KB44877 to clean up space 4. Reboot and join the cluster. Upgrade of cluster node is done successfully |
| PCS-39641 | <p>Symptom : Intermittently during the fresh install and upgrades of Client launches, PSAL is not getting detected in the first attempt.</p> <p>Condition : During fresh install and upgrade of client launches.</p> <p>Workaround : Retry to the Client launches, it works.</p> |
| PCS-39675 | <p>Symptom: Start button for JSAM launch in Ubuntu is failing</p> <p>Workaround: No workaround</p> |
| PCS-38218 | <p>Symptom : Error prompts when 'Citrix All Listed Application' is clicked. Failed to contact server, check the network connection and try again.</p> <p>Condition : XML export and import of 'Citrix All Listed Application' along with other citrix bookmarks.</p> <p>Workaround: Delete the 'Citrix All Listed Application' bookmark and recreate manually using Terminal profile via admin login.</p> |
| PCS-38455 | <p>Symptom : Only 'Citrix listed applications' bookmarks is shown in the user home page.</p> <p>Condition : Issue is encountered only when 'Citrix listed applications' is the 1st entry in Users >User Roles >[User-Name] >Terminal Services >Sessions.</p> <p>Workaround: Reorder the Terminal Services Sessions from Users >User Roles > [User-Name] >Terminal Services >Sessions page using up-down arrows and don't keep 'Citrix listed application' as the 1st entry.</p> |
| PCS-38731 | <p>Symptom: Enterprise onboarding profile push will not work on mobile end point.</p> |

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

| Problem Report Number | Release Note |
|-----------------------|---|
| PCS-36442 | <p>Symptom: "Failed to contact server" error prompted.</p> <p>Condition: "Failed to contact server" error observed sometimes when auto-launch is enabled.</p> <p>Workaround: None</p> |
| PCS-37839 | <p>Symptom: Citrix default ICA launch fail.</p> <p>Condition: When a user uses Citrix workspace app 2112 or later.</p> <p>Workaround: User can use Citrix workspace app version 2109.</p> |
| PCS-37845 | <p>Symptom: VDI-Citrix Xendesktop launch fail.</p> <p>Condition: When a user uses Citrix workspace app 2112 or later.</p> <p>Workaround: User can use Citrix workspace app version 2109.</p> |
| PCS-37219 | <p>Symptom: 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.</p> <p>Condition: As per BSSL, since no RDC clients available on MAC, you may not have any solution as of now.</p> <p>Workaround : None.</p> |
| PCS-39271 | <p>Symptom: None of the selected username data is deleted from the Behavioral Analytics User Report list.</p> <p>Condition: When compliant users is listed in report.</p> <p>Workaround: NA</p> |
| PCS-32175 | <p>Symptom: The auth traffic is not following the selection of traffic interface.</p> <p>Condition: Even if admin configures auth traffic to go through management, it still goes through internal interface.</p> <p>Workaround: NA</p> |
| PCS-36629 | <p>Symptom: ESP Throughput is dropping when users logins from two different source IP on Openstack KVM ISA6Kv</p> <p>Condition: With payload of 1300 bytes or higher, you might experience performance drop due to fragmentation.</p> <p>Workaround: With payload of 1300 bytes or lower, you will not hit this issue.</p> |
| PCS-36937 | <p>Symptom: Enduser is not able to receive multicast traffic</p> <p>Condition: When the enduser is connected to VPN in ESP</p> <p>Workaround: NA</p> |

| Problem Report Number | Release Note |
|-----------------------|---|
| PCS-34315 | <p>Symptom: AD server will not able to join when default VLAN is enabled.</p> <p>Conditions: Default VLAN is enabled on interfaces.</p> <p>Workaround: Enable Traffic decoupling and Map the setting of system-level interface and interface should be the default-VLAN interface of the internal interface.</p> |
| PCS-39434 | <p>Symptom: Time on the ICS gateway goes out of sync, even through configured with NTP servers</p> <p>Conditions: When DNS preferred mode is set to IPv6</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Set DNS preferred mode to IPv4 2. Go to System > Status > Overview page. Click Edit link under System Date & Time 3. Click Save Changes. |
| PCS-39255 | <p>Symptom : The dashboard graphs for HC failures and OS types are not populated.</p> <p>Workaround : Restart services to fix the issue.</p> |
| PCS-39073 | <p>Symptoms: When you try to launch JSAM on MAC OS using browser extension you will see an error saying "jnlib file is malicious"</p> <p>Condition: 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>Workaround: Use custom protocol which is the workflow by default.</p> |
| PCS-39227 | <p>Symptoms: After launching JSAM an error prompts, "Safari can't find the server."</p> <p>Condition: 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>Workaround: The user can use the Chrome browser for the JSAM launch.</p> |
| PCS-39265 | <p>Symptom: HOB auto launch is not working.</p> <p>Condition: When a user uses Windows as a client machine.</p> <p>Workaround: User can do manual launch.</p> |
| PCS-38630 | <p>Symptom: Upgrade from pre-22.3R1 > 22.3R1 appears to be stuck after importing system data.</p> <p>Conditions: When upgrading the gateway from pre-22.3R1 > 22.3R1</p> |

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

| Problem Report Number | Release Note |
|-----------------------|--|
| PCS-35512 | <p>Symptom: User browses to appserver URL with 8083 port (http://appserver:8083/test.asp), it re-directs to some other webpage.</p> <p>Condition: 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>Workaround: Instead of browsing end user page, directly browse the login URL: http://appserver:8083/test.asp</p> |
| PCS-36912 | <p>Symptom: Displays "Exceeded maximum of 51 write attempts".</p> <p>Conditions: During restart/reboot of the system.</p> <p>Workaround: None. No functionality impact.</p> |
| PCS-36787 | <p>Symptom: Certificate validity check shows certificate expired for less than 90 days.</p> <p>Condition: During certificate validity check.</p> <p>Workaround: No functional impact, ignore the message.</p> |
| PCS-37104 | <p>Symptom : Downloaded Protected Zip File (1KB) is empty but actual file size is 2.07MB.</p> <p>Condition : When the user configures the Appserver with protected file share and then downloads any protected file.</p> <p>Workaround: Instead of getting files downloaded through zip, download individual file by clicking.</p> |
| PCS-35628 | <p>Symptom: Installing Ivanti Secure Access Client through browser fails.</p> <p>Condition: After end user login, click on bookmark "PULSE UNIFIED CLIENT" start button, It fails to install Ivanti Secure Access Client.</p> <p>Workaround: User to download Ivanti Secure Access Client directly from Server (System > Maintenance > Installers) and install on end point.</p> |
| PCS-36683 | <p>Symptom: Setup client uninstall will not work sometimes.</p> <p>Condition: When a user tries to uninstall setup client.</p> <p>Workaround: User has to reboot the client machine.</p> |
| PCS-36764 | <p>Symptom: File cannot be downloaded or deleted from the end user UI.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • Bookmarks for a file server have to be present in the end user UI. • Files have to be present in the server upon navigating from bookmark to the file server. |

| Problem Report Number | Release Note |
|-----------------------|--|
| | Workaround: None |
| PCS-36556 | <p>Symptom: 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>Condition: 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>Workaround: Clear the nSA registration status by navigating to System > Ivanti Neurons for Secure access > Clear config and then Restart the Gateway service from Maintenance > Platform > Restart Services. After restart, register again with nSA.</p> |
| PCS-37090 | <p>Symptom: Black screen is shown when user tries to download PSAL from Safari browser.</p> <p>Condition: When PSAL is downloaded and installed for the first time.</p> <p>Workaround: After PSAL is installed, access the end user page and launch JSAM.</p> |
| PCS-37092 | <p>Symptom: End user Onboarding option is not displaying on MAC OS.</p> <p>Condition: When a user uses MAC OS.</p> <p>Workaround: N/A</p> |
| PCS-36675 | <p>Symptom: Panel Preferences for Admin/end user bookmarks is not shown.</p> <p>Condition: When a user access the end user Panel Preferences page.</p> <p>Workaround: N/A</p> |
| PCS-36684 | <p>Symptom: Page refresh issue on end user portal.</p> <p>Condition: When a user configures wrong VDI login details and reconfigures with correct login details.</p> <p>Workaround: User has to re-login to the end user portal.</p> |
| Release 22.1R6 | |
| PCS-36319 | <p>Symptom: Save All Logs option missing from Events/User Access/Admin Access Logs.</p> <p>Condition: When Admin navigates to Monitoring > Events > Logs and tries to Save Logs.</p> |

| Problem Report Number | Release Note |
|-----------------------|---|
| | Workaround: NA |
| PCS-34870 | <p>Symptom: Clear config data fails with errors.</p> <p>Condition: On ISA8000 platform admin console, when "Clear all configuration data at this Ivanti Connect Secure" is run from the "System Operations" options.</p> <p>Workaround: 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>Symptom: Disk and RAID status appears as Unknown for some time.</p> <p>Condition: After adding the disk from console, when user immediately checks Disk and RAID status from UI, it appears asUnknown.</p> <p>Workaround: 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> |
| | |
| Release 22.1R1 | |
| PCS-36093 | <p>Symptom: 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>Condition: When admin tries to import configuration from release 9.1R14 / 9.1R14.1 to 22.1R1.</p> <p>Workaround: NA</p> |
| PCS-34435 | <p>Symptom: Third party related error messages seen on VA console.</p> <p>Condition: Connect Secure registered with nSA.</p> <p>Workaround: None. These messages can be ignored as it does not affect functionality.</p> |
| PCS-34301 | <p>Symptom: Connect Secure is not sending Microsoft Intune server request.</p> <p>Condition: During the user authentication.</p> <p>Workaround: Restart services will restart the MDM services.</p> |
| PCS-33729 | <p>Symptom: Cache cleaner policy is not getting imported when importing XML file for user role configured with cache cleaner policy.</p> |

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

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

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

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

| Problem Report Number | Release Note |
|-----------------------|--|
| PCS-32404 | <p>Symptom: AP Cluster VIP migration is taking around 2 minutes when cluster VIP configured with IPv6 address</p> <p>Condition: When cluster VIP configured with IPv6 address.</p> <p>Workaround : None, time is a time delay in cluster VIP migration and cluster VIP migrates to other node.</p> |
| PCS-33249 | <p>Symptom: 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>Condition: After the completion of Connect Secure installation and boot</p> <p>Workaround: None. This does not affect the Connect Secure functionality.</p> |
| | |
| Release 21.9R1 | |
| PCS-30626 | <p>Symptom: Failed to update profile for user error is seen in user access logs for every user.</p> <p>Condition: Importing system and user binary configs from 9.x where UEBA is configured.</p> <p>Workaround: 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>Symptom: ESP to SSL session fallback happens randomly on L3 session.</p> <p>Conditions: 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>Workaround: Restarting Services on the Cluster resumes all users VPN session to ESP mode.</p> |
| PCS-30694 | <p>Symptom: Number of concurrent users (xx) exceeded the system limit (2) seen in user access logs.</p> <p>Conditions: When nSA Named User Mode is enabled in System > Configuration > Licensing.</p> <p>Workaround: None. End-user does not see any warning and logins will work.</p> |
| PCS-31051 | <p>Symptom: Max Concurrent Users do not get updated immediately.</p> <p>Conditions: After installing Connect Secure-EVAL license.</p> |

| Problem Report Number | Release Note |
|-----------------------|---|
| | Workaround: None. System takes around 3-4 minutes for the page to get updated. |
| PCS-30919 | <p>Symptom: In Advanced HTML5 session, Copy paste functionality does not work after a while.</p> <p>Conditions:When connected to backend windows machines through Advanced HTML5 session.</p> <p>Workaround:Disconnect and Reconnect to Advanced HTML5 session.</p> |
| PCS-31161 | <p>Symptom:</p> <ul style="list-style-type: none"> • Error updating data for chart cloud_secure_roles seen in Admin logs. • Dashboard charts are not getting updated. <p>Conditions: After upgrading to 21.9R1 gateway build</p> <p>Workaround: None. Dashboard charts get updated after a while.</p> |
| PCS-30280 | <p>Symptom: Not able to launch Windows/Citrix terminal services through IPv6 address.</p> <p>Condition: When end user enters IPv6 address to launch WTS/CTS.</p> <p>Workaround: Launch with IPv4 address.</p> |
| PCS-31156 | <p>Symptom: Sessions are not synced between nodes on an AA/AP cluster.</p> <p>Condition: Connect Secure failover because of reboot/power cycle.</p> <p>Workaround: New sessions after node recovery will be synced across both nodes and data on insights will be accurate.</p> |
| PCS-31234 | <p>Symptom: HTML5 graph shows incorrect value for RDP sessions.</p> <p>Condition: RDP sessions created on Connect Secure.</p> <p>Workaround: No workaround.</p> |
| PCS-31046 | <p>Symptom: 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>Condition: 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>Workaround:In the XML file either:</p> <ol style="list-style-type: none"> 1. Set <directory-server> attribute value as None: <directory-server>None</directory-server>. |

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

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

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

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