ivanti

Ivanti Policy Secure Release Notes

22.1R1-22.7R1.2

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.

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

Contents

Ivanti Policy Secure: 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.

What's New

Revision History

View as PDF

Revision History

The following table lists the revision history for this document:

Document Revision	Date	Description
10.0	November 2024	Updated Noteworthy section
9.0	October 2024	Updated known issue and Fixed issues
8.0	May 2024	"Security Advisory and Patch Update" on page 24
7.0	March 2024	Updated New Features and Upgrade Path for in 22.7R1
6.0	April 2023	Updated New Features and Upgrade Path for in 22.4R1
5.0	January 2023	Updated New Features and Upgrade Path for in 22.2R3
4.0	November 2022	Update known issue in 22.3R1 and Fixed issue in 22.3R1
3.0	July 2022	Update known issue in 22.2R1 and Fixed issue in 22.2R1
2.0	June 2022	Update known issue in 22.1R1 and Fixed issue in 22.1R6
1.0	April 2022	Initial Publication 22.1R1

What's New

These are cumulative release notes. If a release does not appear in this section, then there are no associated new features.

22.7R1.2

Product Version	Build
IPS	1485
Profiler Version	FPDB Version 54
ISAC 22.7 R4	30859
Default ESAP	4.3.8

No new features.

22.7R1.1

Product Version	Build
IPS	1321
Profiler Version	FPDB Version 54
ISAC 22.7R3	30777
Default ESAP	4.3.8

No new features.

22.7R1

Product Version	Build
IPS	907
Profiler Version	FPDB Version 52
ISAC 22.7R3	26825
Default ESAP	4.3.8

TLS1.3 support

TLS 1.3 support is newly introduced in this release.

IPS now supports TLS version 1.3 with the 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 unavailable 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, see TLS 1.3 Support.htm
- **Host checker Policy**: Host checker policies-based Predefined OS check the operating systems and their respective service packs/ version.

  - **IPv6 Support**: In this release IPv6 is supported for fresh deployment of IPS on Hyper-v, VMware, and KVM.
  - **MDM Auth Server**: New option is added with interface selection for MDM connections to enable outgoing interface, see configuring_with_mdm_servers.htm
  - **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.
  - **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 IPS host. This feature is enabled by default.
  - **Running Third-Party Tools in Jail**: The IPS 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.

22.6R1

- You can now set the **Minimum Version** check in Host checker for the Custom Command rule for Mac OS. For more information, see Configuring Custom Command Rule.
- NMAP scan subnet increased to 1000 enabling faster scan capability for MAC OS. For more information, see Subnets Configuration
- Dynamic Disk Size Allocation: IPS 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, KVM, Hyper-V, VM.

22.5R1

- Host Checker Timeout can be configured to accommodate the network responsiveness under various conditions. For more information, see Specifying General Host Checker Options.

22.4R1

- Pulse One enablement on IPS 22.4R1 or above. This feature is not enabled by default and has to be enabled through CLI.
- IPS is qualified on Azure cloud and Hyper-V platforms.
- IPv6 support for Host Checker, Download ESAP, Signature files.
- IPv6 support for Log Archiving

22.3R1

- **Allow Host checker policy on certificate expiry**: This feature allows the administrators to pass host checker policies on endpoints after the user certificate expiry. The Administrator can assign endpoints to have remediation roles, so that users can renew certificate.
- **Log Enhancements**: This feature allows the admin to enter a custom message to display on the client highlight the host checker compliance errors.
- **Report scheduling enhancements**: This feature supports scheduling multiple reports of the same type. Allows scheduling report notification on a customized time of a day/month/week.
- **Compliance report enhancements**: The dashboard displays the chart for the compliant and non-compliant devices. The compliance report is enhanced to display the compliant devices.

22.2R3

- This release qualifies certification of FIPS, JITC (DoDIN APL) and NDcPP.

JITC (DoDIN APL) Certification

  - Log Support for detection and prevention of SMURF/SYN Flood/SSL Replay Attack.
  - Password Strengthening.
  - Notification for unsuccessful admin login attempts.

- **NDcPP Certification**
  - When NDcPP option is enabled, only NDcPP allowed crypto algorithms are allowed.
  - 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 release. For more information, see Release Notes
- **OAuth/OpenID support for authentication**: Ivanti Policy Secure (IPS) supports OAuth as an Auth Server, which can be added and configured for End User authentication. OAuth is an open-standard authorization framework that describes how unrelated servers and services can safely allow authenticated access to their assets, without sharing the initial, related, or single logon credentials. OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. This feature allows users to authenticate with any standard OpenID Provider like Google, OKTA, Azure AD, to connect to IPS.
- **Support deployment of IPS on AWS cloud platform**: IPS can now be deployed on AWS cloud platform.

- **IPv6 enforcement support for Palo Alto Networks (PAN) firewall**: IPS supports IPv6 resources access through PAN firewall.

22.1R1

- Policy Secure runs on the next generation Ivanti Secure Appliances (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 release. For more information, see Release Notes.
- The following are some of the sample SKU's introduced in this release:
  - IPS-SVC-GLD-1000U-1YR
  - IPS-SVC-GLD-1000U-3YR
  - IPS-SVC-GLD-1000U-5YR
  - IPS-PROFILER-LG-3YR

The features listed in https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44747 are not supported with 22.1 GW release. In addition, Pulse Collaboration, HOB Java RDP, Basic HTML5 and Pulse One are not supported in 22.1 Gateway.

Introduction

Ivanti Policy Secure (IPS) is a next generation Secure access product, which offers customers to adapt to zero trust network access security model. Enterprises use Policy Secure to enforce endpoint policy compliance for employees, guests and contractors regardless of location, device type or device ownership. Users enjoy greater productivity and the freedom to work anywhere without limiting access to authorized network resources and applications. BYOD onboarding optimizes the user experience by allowing workers to use their preferred device. Policy Secure provides complete visibility of managed and unmanaged network devices.

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

The IPS Gateway versions listed below are the supported versions to use with Gateway for respective releases.

Build Details for 22.6R1.2

- IPS 22.6R1.2 Build 673
- Profiler Version (FPDB Version 52)
- ISAC 22.3R3 Build 19959
- Default ESAP version 4.0.5

Build Details for 22.6R1.1

- IPS 22.6R1.1 Build 669
- Profiler Version (FPDB Version 52)
- ISAC 22.3R3 Build 19959
- Default ESAP version 4.0.5

Build Details for 22.6R1

- IPS 22.6R1 Build 595
- Profiler Version (FPDB Version 52)
- ISAC 22.3R3 Build 19959

- Default ESAP version 4.0.5

Build Details for 22.5R1

- IPS 22.5R1 Build 553
- Profiler Version (FPDB Version 52)
- ISAC 22.3R3 Build 19959
- Default ESAP version 4.0.5

Build Details for 22.4R1

- IPS 22.4R1 Build 373
- Profiler Version (FPDB Version 51)
- ISAC 22.3R1 Build 18209
- Default ESAP version 4.0.5

Build Details for 22.3R1

- IPS 22.3R1 Build 469
- Profiler Version (FPDB Version 51)
- ISAC 22.2R1 Build 1295
- Default ESAP version 4.0.5

Build Details for 22.2R3

- IPS 22.2R3 Build 1049
- ISAC 22.2R1 Build 1295

Build Details for 22.2R1

- IPS 22.2R1 Build 461
- Pulse Profiler Version (FPDB Version 48)
- PDC 9.1R15 Build 15819

- ISAC 22.2R1 Build 1295
- Default ESAP version 3.7.5

Build Details for 22.1R6

- 22.1R6 Build 281

Build Details for 22.1R1

- IPS 22.1R1 Build 211
- Pulse Profiler Version (FPDB Version 48)
- PDC 9.1R14 Build 13525
- Default ESAP version 3.7.5

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 22.7R1

Variant	Platform	vCPU	RAM	Disk Space
OpenStack Wallaby on Ubuntu 20.04 LTS	(4 vCPUs / ISA4000-v), (8 vCPUs,ISA6000-v), (12 vCPUs, ISA8000-v)	4	8 GB	80 GB
VMware ESXi 7.0.3	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
AWS	ISA4000-V (M5.xlarge)	4	16 GB	80 GB
	ISA6000-V (M5.2xlarge)	8	32 GB	80 GB
	ISA8000-V (M5.4xlarge)	16	64 GB	80 GB
Azure	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
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 22.6R1

Variant	Platform	vCPU	RAM	Disk Space
OpenStack Wallaby on Ubuntu 20.04 LTS	(4 vCPUs / ISA4000-v), (8 vCPUs,ISA6000-v), (12 vCPUs, ISA8000-v)	4	8 GB	40 GB

Variant	Platform	vCPU	RAM	Disk Space
VMware ESXi 7.0.3	ISA4000-V	4	8 GB	40 GB
	ISA6000-V	8	16 GB	40 GB
	ISA8000-V	12	32 GB	40 GB
AWS	ISA4000-V (M5.xlarge)	4	16 GB	40 GB
	ISA6000-V (M5.2xlarge)	8	32 GB	40 GB
	ISA8000-V (M5.4xlarge)	16	64 GB	40 GB
Azure	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
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 22.5R1

Variant	Platform	vCPU	RAM	Disk Space
VMware ESXi 7.0.3	ISA4000-V	4	8 GB	40 GB
	ISA6000-V	8	16 GB	40 GB
	ISA8000-V	12	32 GB	40 GB
AWS	ISA4000-V (M5.xlarge)	4	16 GB	40 GB
	ISA6000-V (M5.2xlarge)	8	32 GB	40 GB
	ISA8000-V (M5.4xlarge)	16	64 GB	40 GB
Azure	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
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 22.4R1

Variant	Platform	vCPU	RAM	Disk Space
VMware ESXi 7.0.3	ISA4000-V	4	8 GB	40 GB
	ISA6000-V	8	16 GB	40 GB
	ISA8000-V	12	32 GB	40 GB
AWS	ISA4000-V (M5.xlarge)	4	16 GB	40 GB
	ISA6000-V (M5.2xlarge)	8	32 GB	40 GB
	ISA8000-V (M5.4xlarge)	16	64 GB	40 GB
Azure	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
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 22.2R3

Variant	Platform	vCPU	RAM	Disk Space
VMware ESXi 7.0.3	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, 22.2R1, and 22.3R1

Variant	Platform	vCPU	RAM	Disk Space
VMware ESXi 7.0.3	ISA4000-V	4	8 GB	40 GB
	ISA6000-V	8	16 GB	40 GB
	ISA8000-V	12	32 GB	40 GB
AWS	ISA4000-V (M5.xlarge)	4	16 GB	40 GB
	ISA6000-V (M5.2xlarge)	8	32 GB	40 GB
	ISA8000-V (M5.4xlarge)	16	64 GB	40 GB

Virtual appliance qualified in 22.1R1

Variant	Platform	vCPU	RAM	Disk Space
VMware ESXi 7.0.3 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

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

Upgrade Path

The following table describes the tested upgrade paths, in addition to fresh installation of 22.1R1 and 22.1R6 for IPS Product.

Upgrade path is not supported for FIPS mode (enabled) from release 22.1R1 or prior releases.

Upgrade can only be done with FIPS mode disabled.

Upgrade to	Upgrade From (Supported Version)	Qualified
22.7R1/22.7R1.1/22.7R1.2	22.6R1, 22.4R1 and 22.5R1	Q
22.6R1.2	22.6R1, 22.4R1 and 22.5R1	Q
22.6R1	22.4R1 and 22.5R1	Q
22.5R1	22.4R1 and 22.3R1	Q
22.4R1	22.3R1 and 22.2R1	Q
22.3R1	22.2R1 and 22.1R1	Q
22.2R1	22.1R6 and 22.1R1	Q
22.1R6	22.1R1	Q

Upgrade Path in 22.2R3

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

JITC (DoDIN APL) supports fresh installation and upgrade for VMware images and only upgrade for cloud (AWS) images.

Configuration Migration Path

The recommended and qualified import option is using Binary Config.

The following table describes the tested migration paths.

Migrate to	Migrate From (Supported Versions)	Qualified
22.7R1/22.7R1.1/22.7R1.2	9.1R18.2, 9.1R18.1	Q
22.6R1/22.6R1.2	9.1R18.2, 9.1R18.1	Q
22.5R1	9.1R18, 9.1R17, 9.1R16.2	Q

Migrate to	Migrate From (Supported Versions)	Qualified
22.4R1	9.1R18, 9.1R17, 9.1R16.2, 9.1R14.3	Q
22.3R1	9.1R17, 9.1R16, 9.1R16.2, 9.1R15, 9.1R14	Q
22.2R1/ 22.2R3	9.1 R15, 9.1 R14.1, 9.1 R13.2	Q
22.1R6	9.1R14.1 or prior releases	Q
22.1R1	9.1R13.2 or prior releases	Q

Noteworthy Information

Version 22.7R1

- Functionality provided by the IF-MAP feature has reached a final state. Refer the forum article for more information.
- Dot1x Authentication with certification auth is not supported with TLS 1.3 on Windows 11.
- Layer 3 Enforcement communication with Juniper SRX is not supported as this functionality is not supported by Juniper SRX.
- Ivanti recommends to use api/v1/realm_auth instead of api/v1/auth as it will not be supported in future release. Update your REST based scripts to make use of /api/v1/realm_auth
- After upgrade to 22.7R1, ESAP 4.3.8 is set by default.

Version 22.3R1

- Host checker on the Ubuntu OS is not supported on Firefox browser.

Version 22.2R3

- New password must differ from previous 8 password positions 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

- For MAC spoof detection based on NMAP, the classification change counter is configurable. To configure, you must navigate to **Profiler Configuration > Settings > Advance Configuration**.
- Platform (Core) License SKUs for ISA platforms are introduced. Concurrent users are reset to two if core license is not installed or leased.

Resolved Issues

The following table lists release numbers and the PRS numbers with the summary of the issue fixed during that release. If a release does not appear in this section, then there are no associated resolved issues.

Problem Report Number	Summary
Release 22.7R1.2	
PPS-11485	When you upgrade to 22.7R1 the following features do not work: • Profiler SSH collector • SNMP ACL Enforcement • MySQL
1302207	When the Active node shutdown from Active node the Passive node is not taking the VIP.
Release 22.7R1.1	
PPS-11485	MySQL not working when you upgrade to 22.7R1.
1382786	"Program RADIUS recently failed" issue has been fixed.
Release 22.7R1	
PRS-418197	End-user login fails when admin configures multiple MAC OS in a rule for Host Checker.
PRS-417156	SSH discovery not working for Paloalto firewalls with ipV4
PRS-417370	Host checker fails for McAfee LiveSafe Version: 1.9.253
PRS-417568	DDR Page is not updated for Remote Profiler once an end-user connects to ICS
PRS-417155	SSH Profiling not working for Plaoalto firewalls
PRS-416067	Browser-based user login page is not displaying the "instruction message" for localized language in IPS 22.x version.
PRS-417882	Added improvements in scripts which cleans up stale/incomplete sessions.
Release 22.6R1	

Problem Report Number	Summary
PRS-417065	Unable to upload ISAC 22.3R3 pkg file on the 22.4R1 server.
PRS-416740	Export Device Data to a backup file - CSV format is not downloading completely from the 22.5R1 Server.
PRS-415662	Browser-based user login page is not displaying correctly in IPS 22.x version.
Release 22.5R1	
PRS-415034	After upgrading to 9.1 R17 version, Profiler DDR shows 5 filters were applied by default.
PRS-415336	SBR auth process not recovering on its own after being overloaded
Release 22.3R1	
PCS-36787	Certificate validity check shows certificate expired for less than 90 days.
Release 22.2R3	
Refer to the Security Advisory and Patch Release section to see CVEs fixed.	
Release 22.2R1	
PRS-410550	Native supplicant 802.1x authentication fails with Local Auth Server with Error "Invalid Credentials"
Release 22.1R6	
PCS-36093	Configuration import fails with reason: software version used to create import file was '9.1R14.1' current version of software is '22.1R1 (build 211)'.

Security Advisory and Patch Update

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

22.7R1.2

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.

22.6R1.1

CVE-2024-21887

CVE-2023-46805

22.5R2.2

CVE-2024-21893

22.5R1.2

CVE-2024-21887

CVE-2024-22024

22.5R1.1

CVE-2024-21893

CVE-2024-22024

22.4R1.1

CVE-2024-21887

CVE-2023-46805

22.2R3

CVE-2024-21887

CVE-2023-46805

CVE-2024-21893

CVE-2024-22024

General

CVE-2024-21894

CVE-2024-22052

CVE-2024-22053

CVE-2024-22023

CVE-2024-29205

For more details, see Ivanti forum KB.

Known Issues

The following table lists the known issues in respective releases. If a release does not appear in this section, then no associated new known issues were added to this document for that release.

Problem Report Number	Release Note
Release 22.7R1.2	
1374589	**Symptom** :Device sponsor works only if unclassified devices are assigned "Other OS" as category. Newly discovered by default will have category as empty "". **Workaround**: To manually approve unclassified devices with missing category, the admin needs to create a group with a rule under Profiler Configuration > Profile Groups with category= "" .
1432313	**Symptom**: When updating 22.7R1.2 the spread Process fails **Workaround**:None
1325637	**Symptom** : dsunity Process fails in 22.7R1.2 **Workaround**: None
1444387	**Symptom** : XML fails during Import **Workaround**: Import the user configuration
Release 22.7R1.1	
No Known Issues.	
Release 22.7R1	
PPS-11998	**Symptom** Native Supplicant with TLS 1.3 is not working against Windows 11 while Cert-Auth Perform. For more information , see 000092310 **Workaround**: None
PPS-11512	**Symptom** TLS13 CGI Process crashing during KerberosSSO authentication. **Workaround**: None
Release 22.6R1	
No Known Issues.	
Release 22.5R1	

Problem Report Number	Release Note
PPS-10915	**Symptom**: When logging into IPS 22.5R1, the browser header displays Ivanti Connect Secure for a second. **Workaround**: None
Release 22.4R1	
PPS-10665	**Symptom**: Compliance check fails on MacOSX, while using IPv6. **Workaround**: None
PPS-10670	**Symptom**: With SNMP enabled, the XML import/export fails. **Workaround**: Default VLAN must be entered manually.
PPS-10768	**Symptom**: Captive portal redirection page requests an URL and upon providing the URL it throws an internal Server error. **Workaround**: Open the URL in New Tab and access resources.
PPS-10744	**Symptom**: Config Import from Pulse One fails with an error message. **Workaround**: Currently there is no workaround for this issue as Import configuration is not supported from Pulse One.
PPS-10702	**Symptom**: Click here to register with Pulse One." from the page Auth Servers > New MDM Server. Upon clicking it throws error 500. **Workaround**: There is no workaround and no functional impact.
Release 22.3R1	
PPS-10343	**Symptom**: Upgrade fails due to disk space issue. **Condition**: When the IPS VM diskspace is full. **Workaround**: Reboot and upgrade, or delete the unused, system-snapshots, debug logs and ESAP packages not in use, and then try upgrade again. Follow the mandatory steps listed in the KB44877 before staging or upgrading to prevent any upgrade related issues.
PPS-10292	**Symptom**: In Chinese language, machine certificate rule failed message showing in English. **Condition**: When using Chinese language on Firefox ESR browser. **Workaround**: None.
Release 22.2R1	

Problem Report Number	Release Note
PCS-36787	**Symptom**: Certificate validity check shows certificate expired for less than 90 days. **Condition**: During certificate validity check. **Workaround**: No functional impact, ignore the message.
Release 22.1R1	
PCS-36093	**Symptom**: Configuration import fails with reason: software version used to create import file was '9.1R14.1' current version of software is '22.1R1 (build 211)'. **Condition**: When admin tries to import configuration from release 9.1R14.1 to 22.1R1. **Workaround**: NA
PRS-410550	**Symptom**: Native supplicant 802.1x authentication fails with Local Auth Server with Error "Invalid Credentials" **Condition**: When user configures Local Auth Server for native dot1x authentication. **Workaround**: Use any other supported server to authenticate native dot1x connection.
For the list of current Known Issues, see here.	

Documentation

Pulse documentation is available at https://www.ivanti.com/support/product-documentation.

Technical Support

When you need additional information or assistance, you can contact:

- https://forums.ivanti.com/s/contactsupport
- support@ivanti.com

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