ivanti

Ivanti Policy Secure Release Notes

22.1R1-22.4R1.1

Contents

Revision History

The following table lists the revision history for this document:

Document Revision	Date	Description
9.1	February 2024	Security Advisory and Patch Release updates for 22.4R1.1 release.
9.0	February 2024	Released security advisories and mitigations for critical vulnerabilities
8.0	November 2023	Updated New features
7.0	August 2023	Updated Known Issues, and Fixed Issues.
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

In 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

In 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.

In 22.2R3

- This release qualifies certification of FIPS, JITC (DoDIN APL) and NDcPP.
- nSA support is not qualified with this release.
- **JITC (DoDIN APL) 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.

In 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.

In 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 the ability to adapt to a 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.

Security Advisory and Patch Update

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

- CVE-2023-46805
- CVE-2024-21887
- CVE-2024-21888
- CVE-2024-21893
- CVE-2024-22024
- CVE-2023-39340
- CVE-2023-41719

For more details, see forum link.

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

Build Details for 22.4R1.1

- IPS 22.4R1.1 Build 463
- Profiler Version (FPDB Version 51)
- ISAC 22.3R1 Build 18209
- 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 993
- 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 22.4R1/22.4R1.1

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

Variant	Platform	vCPU	RAM	Disk Space
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

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 to	Upgrade From (Supported Version)	Qualified
22.4R1.1	22.4R1, 22.3R1 and 22.2R1	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 path is not supported for JITC (DoDIN APL) mode (enabled) from release 22.2R1 or prior releases.

Upgrade can only be done with JITC (DoDIN APL) mode disabled.

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
22.4R1/ 22.4R1.1	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 22.3R1

- 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.

Fixed Issues

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

Problem Report Number	Summary
Release 22.4R1.1	
The following CVE's have been fixed: • CVE-2023-46805 • CVE-2024-21887 • CVE-2024-21888 • CVE-2024-21893 • CVE-2024-22024 • CVE-2023-39340 • CVE-2023-41719 For more details, see forum link.	
Release 22.3R1	
PCS-36787	Certificate validity check shows certificate expired for less than 90 days.
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)'.

Known Issues

The following table lists the known issues in respective releases:

Problem Report Number	Release Note
Release 22.4R1/22.4R1.1	
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

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