Ivanti Policy Secure Release Notes

25.1.2.2

Copyright Notice

Contents

Revision History

The following table lists the revision history for this document:

Document Revision	Date	Description
1.0	July 2026	First version for IPS 25.x

What's New

Version 25.1.2.2

This release supports ISA8500 and ISA6500 hardware devices.

Product Version	Build
IPS 25.1.2.2	691
ISAC 22.8R5	41063
Default ESAP	4.6.4

Note:

- IPS 25.1.2.2 version is a hardware enablement release, the **software package is not available for general download**.
- No new features. This release maintains feature parity with Release 25.1.2.2 .
- ISA6500 and ISA8500 devices shipped after the release of version 25.1.2.2 will have 25.1.2.2 as a base image.
- ISAC 22.8.7.48847 product version is Compatible with Release 25.1.2.2 .
- **Secure Boot with TPM**: The Secure Boot feature offers protection against unauthorized bootloader and kernel images, malware, and rootkits, and ensures compliance with security by design principle while improving boot time.
- **Rotate Internal Storage Key**: This process encrypts sensitive information like passwords when storing them internally and ensures the encryption key is unique and random for every IPS instance.
- **Shared Secret key**: This feature configures a Shared Secret for each source/target pair at time of creation of Push Config Target.
- **Password key Generation**: New API's introduced to generate and fetch the password key.
- **Next Generation Web server**: The Next Generation Web Server has been developed to enhance the performance and scalability of web server infrastructure. Web server logs are implemented for web-related event codes with debug severity.

- **SELinux Security Policy**: The IPS system provides an Enforcing only SELinux capability, ensuring that even the root user or admin cannot switch SELinux to permissive mode without rebooting the system.
- **Verbose Log**: Administrators can toggle SELinux verbose logging to control the detail level of SELinux-related logs.

Introduction

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

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

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

Noteworthy Information

25.1.2.2

- This release supports 8500 and 6500 hardware devices, and this IPS version is embedded in the hardware and is not available for download.
- Starting in early August, all hardware will ship with dual-personality support, allowing devices to boot as either ICS or IPS depending on the selected configuration.
- The Compliance report now shows why the HC compliance is failing . It includes the Policies and rules under the policies based on which device is non -compliant. For more information check Host Checker Configuration Guide.
- Outbound HTTP/HTTPS proxy connections are restricted to a defined allow list of well-known proxy ports to align with Secure by Default.
  Allowed ports: 8080, 8118, 8123, 10001–10010, 10080, 3130, 3445, 8008, 8010, 3128.
- Feature parity with IPS release 22.7R1.14
- SAML Authentication Server configuration using the SAML 1.1 Protocol is deprecated at IPS 25.x versions. From 25.1.2.2 onwards, the system will not allow new SAML 1.1 server configuration and will not allow to import any existing configurations. SAML 2.0 is the option supported. This deprecation was initially notified as part of this
- Before performing a pushConfig operation from an older release to version 25.1.2.2, you must disable the HTTP Only Device Cookie on the target device.
  - For **Admin Roles**: Navigate to **Administrators > Admin Roles > Delegated Admin Roles > Administrators > Session Options**.
  - For **User Roles**: Navigate to **Users > User Roles > [Role Name] > Session Options**.
- Referrer header validation is enabled by default to block CSRF attacks, providing an additional layer of security.
- All cookies will be deleted upon session terminated by default, enhancing security and privacy.
- Content Security Policy (CSP) headers are now implemented for end user pages to provide additional protection against Cross-Site Scripting (XSS) attacks.
- The Next Generation Web Server (Nginx) will restart when performing any of the following certificate-related operations. User connections may drop during this period:

    - Mapping a device certificate to a port.
    - Importing or deleting a trusted client CA.
    - Making changes to inbound TLS versions and cipher suites.
- IPS License Server cann lease licenses to License Clients running version or 25.1.2.2.
- Certificate based authentication will not work after upgrading to 25.1.2.2, if client uses SHA-1 based certificates.
- SSLv3, TLS1.0 and TLS1.1 versions are removed and there are additional cipher changes implemented as part of this release.
- Custom Sign-In pages are deprecated effective from IPS release 25.1.2.2.
- Use of SHA1 for digital signature is not supported, use SHA2 and above:
    - SHA2 is the minimum required version in digital signatures. IPS server will no longer connect or validate with SHA1 in digital signatures.
    - Enable SHA2 as response signature algorithm in OCSP response on OCSP responder.
    - If the IPS only contains SHA1 device signed certificates, the user interface fails to launch. At least one SHA2 signed certificate or any newer version after SHA1 is mandatory.
- **Certificate Validation**: **HTTP/1.1 Enforcement for OCSP Requests** Starting with version 25.1.2.2, certificate validation process now explicitly enforces the use of HTTP/1.1 for Online Certificate Status Protocol (OCSP) requests. This ensures consistent and reliable communication during certificate status checks. For more info refer article.
- For RSA Authentication to work, Add the agent's host name in RSA Auth Manager and configure it in IPS. Ensure the RSA/ACE server has a host entry in IPS.
    - TCP is now enforced as the only supported communication protocol for the RSA SecurID integration. Legacy UDP-based communication is no longer supported.
    - Update firewall rules to allow outbound TCP from IPS to the RSA Authentication Manager on the configured SecurID agent port(s) used in your environment, see KB
    - As TCP is used, hostname-based validation is mandatory. As a result, the Hostname configured in IPS (Network → Overview) must match the Agent Hostname defined in the RSA Authentication Manager.
    - This replaces the earlier flexibility of using internal IP addresses, which was possible with the legacy UDP-based integration.

The above scenarios apply to RSA Authentication Manager 8.7 and below.

- In this release, the /api/v1/healthcheck REST API response has been updated to return content as bytes, which aligns with the default behavior of many web frameworks and libraries when handling API responses. Previously, the response was returned as a string. This change could impact systems or integrations assuming the response would always be a string.
- Upgrade or Binary Import is not supported if SHA-1 certificates are configured on any IPS ports.
- `arping` command no longer resolves hostnames. The command now requires a direct IP address as input. Attempts to use hostnames will result in an error.

  Example error: `Bad Value for ai_flags. Don't use a hostname with arping.`
- The ARP **Maintenance** >**Troubleshooting** >**Tools** >**Commands**>**ARP** option no longer supports hostnames as input. You must now specify a direct IP address when using this command. Attempts to use hostnames will result in following error.
  Example error: `Bad Value for ai_flags. Don't use a hostname with arping.`

Unsupported Features

- Ivanti Policy Secure: Features and Options Becoming Unsupported or Deprecated in 22.7Rx and 25.x, refer to article.

Licenses

An IPS instance running version 25.1.2.2 can be configured as a License Server and is qualified to lease licences to 25.x instances acting as license clients. While an IPS instance running version 25.1.2.2 may technically be able to lease license to 25.x clients, this configuration has not been qualified. Therefore, it is recommended to use IPS version 25.1.2.2 or later when configuring a license server.

Known Limitations

- **Cluster Node Name Restriction**: Cluster node names should not be configured as "localhost2". Using "localhost2" as a node name is not supported and may result in unexpected. behavior.

Upgrade and Migration

Upgrade Path

Please note that there is no direct upgrade path for version 25.1.2.2; this version requires a fresh installation.

Configuration Migration Path

The following table describes the tested migration paths.

Migrate to	ISA Hardware device Migrate From (Supported Versions)
25.1.2.2	22.7R1.13, 22.7R1.12

Support and Compatibility

Hardware Platforms

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

- ISA6500 (hardware only release)
- ISA8500 (hardware only release)

Known Issues

The following table lists the known issues in respective release:

Problem Report Number	Release Note
Release 25.1.2.2	
1770956	**Symptom:** When Antivirus/Firewall remediation is turned on, RTP is not working. **Condition:** When agentless HC is configured on Windows.
1873525	**Symptom**: Active user sessions fail to synchronize to the secondary node. **Condition**: This occurs in Active/Passive (A/P), Active/Acive (A/A) cluster configuration.
1940411	**Symptom**: "Onboard Profiles" are incorrectly visible and need to be hidden. **Condition**: This occurs when a user with a Delegated Admin Role views profiles related to Enterprise Onboarding.
1943009	**Symptom**:Resources located behind the FortiGate firewall become inaccessible. **Condition**: This issue occurs immediately following a cluster fail-over event.
1955982	**Symptom**: The cgi-server process crashes. **Condition**: This happens after a user edits switches that were discovered via SNMP.
1956239	**Symptom**:The "WAF Message" option is incorrectly visible and needs to be hidden. **Condition**:This is seen when viewing Log Settings within IPS.
1958105	**Symptom**: A "502 Bad Gateway" error is displayed. **Condition**: This happens on the AD troubleshooting page when attempting to sign in without providing user credentials.

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