Ivanti Connect Secure Release Notes

25.1.2.2

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

Revision History

The following table lists the revision history for this document:

Document Revision	Date	Description
5.0	June 2026	Updated Config and Upgrade Paths.
4.0	May 2026	Updated what's new, Known Issue, and Fixed Issues.
3.0	March 2026	Updated what's new, Known Issue, and Fixed Issues.
2.0	February 2026	Updated what's new and Known Issue.
1.0	September 2025	First version for 25.1.0.0

What's New

Version 25.1.2.2

This release supports ISA8500 and ISA6500 hardware devices.

Product Version	Build
ICS 25.1.2.2	17993
ISAC 22.8R5 Mobile Client 22.8R6	41063 17079 (Android) 5717 (iOS)
WAF Default CRS	1.0.4
Default ESAP	4.6.4

Note:

- ICS 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 25.1.1.0.
- ISA6500 and ISA8500 devices shipped after the release of version 25.1.2.2 will have 25.1.2.2 as a base image.

Version 25.1.2.1

Product Version	Build
ICS 25.1.2.1	15773
ISAC 22.8R5 Mobile Client 22.8R6	41063 17079 (Android) 5717 (iOS)
WAF Default CRS	1.0.4
Default ESAP	4.6.4

This release includes security enhancement and bug fixes. Ivanti encourages customers to upgrade to this latest version.

Version 25.1.2.0

This release supports ISA6500 hardware devices.

Product Version	Build
ICS 25.1.2.0	14001
ISAC 22.8R5 Mobile Client 22.8R6	41063 17079 (Android) 5717 (iOS)
WAF Default CRS	1.0.4
Default ESAP	4.6.4

Note:

- ICS 25.1.2.0 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 25.1.1.0.

Version 25.1.1.1

Product Version	Build
ICS 25.1.1.1	15763
ISAC 22.8R5 Mobile Client 22.8R6	41063 17079 (Android) 5717 (iOS)
WAF Default CRS	1.0.4
Default ESAP	4.6.4

This release includes bug fixes. There are no new features.

Version 25.1.1.0

Product Version	Build
ICS 25.1.1.0	11811
ISAC 22.8R5 Mobile Client 22.8R6	41063 17079 (Android) 5717 (iOS)
WAF Default CRS	1.0.4
Default ESAP	4.6.4

- Feature parity with ICS release 22.8R2.3 and 22.7R2.12
- **Citrix Support**: ICS now supports the use of Device ID as a unique identifier in Citrix Xendesktop LTSR 2507, enabling enhanced device-based authentication and tracking.
- **Secure Boot and vTPM Support**: Hyper-V, Openstack KVM, Azure platform now provides secure boot support with vTPM functionality, enhancing security and integrity for virtual machines, see Deployment Guide.

Version 25.1.0.1

Product Version	Build
ICS 25.1.0.1	10387
ISAC 22.8R5 Mobile Client 22.8R6	41063 17079 (Android) 5717 (iOS)
WAF Default CRS	1.0.4
Default ESAP	4.3.8

There are no new ICS features in this release. This release includes patch for OpenSSL CVE-2025-15467. Feature parity of this release remains same as 25.1.0.0. Refer the KB for more info.

Version 25.1.0.0

Product Version	Build
ICS 25.1.0.0	5663
ISAC 22.8R2 Mobile Client 22.8R3	33497 14 (Android) 95033 (iOS)
Default ESAP	4.3.8

- **Secure Boot with TPM/vTPM**: 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. For more information, see Secure Boot with TPM/vTPM.
- **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 ICS instance, see Rotate Internal Storage Key.
- **Security Enhanced WAF Operation**: This feature protects Connect Secure gateway web applications by filtering and monitoring HTTP traffic, preventing attacks such as SQL injection, cross-site scripting (XSS), and other web exploits, see Configuring Web Application Firewall UI and Security Enhanced WAF Operation console.
- **Shared Secret key**: This feature configures a Shared Secret for each source/target pair at time of creation of Push Config Target, see Configuring Targets.
- **Password key Generation**: New API's introduced to generate and fetch the password key, see APIs.
- **Next Generation Web server**: The Next Generation Web Server has been developed to enhance the performance and scalability of web server infrastructure, see Next Generation Web Server. Web server logs are implemented for web-related event codes with debug severity, see Using the Debug Log.
- **SELinux Security Policy**: The ICS 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, See SELinux Security Policy.
- **Verbose Log**: Administrators can toggle SELinux verbose logging to control the detail level of SELinux-related logs, see SELinux Verbose Log.

Introduction

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

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

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

Noteworthy Information

With Next Generation Web Server enabled, PushConfig operations from releases prior to 22.8Rx (using the legacy web server) to version 25.x are not supported

25.1.2.2

- This release supports 8500 and 6500 hardware devices, and this ICS version is embedded in the hardware and is not available for download.

25.1.2.1

- This release can only be upgraded on ISA 6500 hardware devices.
- This release version includes security enhancement. Ivanti encourages customers to upgrade to this latest version.

25.1.2.0

- This release supports 6500 hardware devices, and this ICS version is embedded in the hardware and is not available for download.

25.1.1.0

- 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 ICS release 22.8R2.3 and 22.7R2.12
- Starting with ICS version 25.1.1.0 the default global **(System > Configuration > Client configuration**) and Role level (**User > User Roles > <name> > VPN tunnelling > Ivanti Secure Access Client Settings**) options for the ISAC Desktop user experience (UX) is set to NeUX for fresh installations of ICS.
  - Ensure your environment allows installation and execution of the React Native Appx bundle used by NeUX.
  - Follow the guidance in the forum article to enable the Appx bundle.

    - Applies to: New installations to ICS 25.1.1.0, and later.
- Cluster setup which is running with version 22.8Rx does not support upgrade to ICS 25.x version. Cluster upgrade supports only on ICS 25.1.0.0 and above to ICS 25.1.1.0.
- SAML Authentication Server configuration using the SAML 1.1 Protocol is deprecated at ICS 25.x versions. From 25.1.1.0 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 KB.
- The username displayed in the End User Portal is always in lowercase, similar to other authentication methods. The correct casing is maintained in the User Access and other logs.
- Before performing a pushConfig operation from an older release to version 25.1.1.0, 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.

25.1.0.1

To enable TLS 1.3 functionality, ensure that the enable_tls_v1_3 Key Value Pair is configured and pushed to ISAC mobile client (Android/iOS) from the MDM server.

Key-Value Pair Setting

- **Configuration Key**: enable_tls_v1_3
- **Value Type**: Boolean
- **Configuration Value**: true

25.1.0.0

- To enable TLS 1.3 functionality, ensure that the enable_tls_v1_3 Key Value Pair is configured and pushed to ISAC mobile client (Android/iOS) from the MDM server.

Key-Value Pair Setting

  - **Configuration Key**: enable_tls_v1_3
  - **Value Type**: Boolean
  - **Configuration Value**: true

- ICS License Server cannot lease licenses to License Clients running versions 22.7Rx, 22.8Rx, or 25.1.x.x. See, forum.
- Certificate based authentication will not work after upgrading to 25.1.0.0, 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. For more information, see Configuring SSL Options.
- Use of SHA1 for digital signature is not supported, use SHA2 and above:
  - SHA2 is the minimum required version in digital signatures. ICS 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 ICS 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 25.1.0.0, 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 KB.

- Cluster upgrade is not supported from 22.8R2 to 25.1.0.0. To upgrade, break the cluster, upgrade and then create the cluster again. For more information, see Cluster Migration from 22.8Rx to 25.x.
- For RSA Authentication to work, Add the agent's host name in RSA Auth Manager and configure it in ICS. Ensure the RSA/ACE server has a host entry in ICS.
    - 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 ICS to the RSA Authentication Manager on the configured SecurID agent port(s) used in your environment, see KB for more details.
    - As TCP is used, hostname-based validation is mandatory. As a result, the Hostname configured in ICS (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 Binay Import is not supported if SHA-1 certificates are configured on any ICS ports.
- Configs with deprecated features will be upgraded or imported to 25,x but will not be qualified. Please refer the KB for more details
- `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.`

With Q1 2026 Release of ICS, the default ESAP version will be 4.6.4. ESAP 4.6.4 has been released in Q2 2025.

Unsupported Features

- Ivanti Connect Secure: Features and Options Becoming Unsupported or Deprecated in 22.7Rx, 22.8Rx, and 25.x, refer to article.

Licenses

An ICS instance running version 22.8R3 can be configured as a License Server and is qualified to lease licences to 22.8Rx and 25.x instances acting as license clients. While an ICS instance running version 22.7Rx may technically be able to lease license to 22.8Rx or 25.x clients, this configuration has not been qualified. Therefore, it is recommended to use ICS version 22.8R3 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.
- **Per-app VPN on iOS in version 25.1.0**: Occasionally, ICS does not fulfill certain requests, resulting in partial functionality for this use case. It is planned to resolve this issue in the upcoming 25.1.1.0 release.

Upgrade and Migration

Upgrade Path

Upgrade Installation is supported on the following ISA Hardware Platforms.

- ISA6500
- ISA8500

The following table describes the tested upgrade paths of 25.x for ICS Product.

Upgrade to	Upgrade From (Supported Versions)
25.1.2.2 (ISA8500/ISA6500 Hardware only) 25.1.2.2 ICS version is embedded in the hardware and is not available for download.	25.1.2.1 (ISA6500 Hardware only)
25.1.2.1 (ISA6500 Hardware only)	25.1.2.0 (ISA6500 Hardware only) 25.1.2.0 ICS version is embedded in the hardware and is not available for download.

Configuration Migration Path

The following table describes the tested migration paths. For more information, see 22.x-25.x-Migration-Guide

Migrate to	ISA Hardware device Migrate From (Supported Versions)
25.1.2.2	25.1.2.1, 25.1.1.1, 25.1.0.1, 25.1.1.0, 22.8R2.4, 22.8R2.3, 22.7R2.13, 22.7R2.12
25.1.2.1	25.1.0.1, 25.1.1.0, 22.8R2.3, 22.7R2.12
25.1.2.0	25.1.1.0, 22.8R2.3, 22.7R2.12

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)

Resolved Issues

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

Problem Report Number	Summary
Release 25.1.2.1	
1832217	Intermittent packet loss on the internal interface from tunnels causes resource access failures for all tunnel users.
1800556	Intermittent IP Allocation Failures in Active/Active Cluster.
1813625	OCSP validation failure in 22.8R2.3 with SELinux enforcing mode.
1792433	Client UI mode **neux** is enforced post upgrading to ICS 22.7R2.12
1800401	Source IP is disabled upon upgrading the server from 22.7R2.9 to 22.7R2.12
1773736	LDAPS Port Support and Port Range Behavior on ISA-6000.
1713264	Unable to Download License via Proxy.
1846861	Navigating through the Admin UI intermittently results in the error "The server had an internal error" on various pages in version 25.1.1.0.
Release 25.1.1.0	
This release also includes the applicable resolved issues from version 22.7R2.12 and 22.8R2.3.	
Authentication & Certificate	
1697123	Users are unable to access core resources because the rate limiting feature restricts connections in certain conditions.
1637539	RADIUS disconnect requests do not terminate the session.
1634055	Encountered an error "Invalid LDAP server IP address".
1622322	OAuth time skew is not functioning according to the configured values.
1651237	WAF issue observed when configuring CRL (Certificate Revocation List).
1648859	ICS allows SHA1 trusted client/server CA certificate to import.

Problem Report Number	Summary
1711706	Switching from TLS 1.2 to TLS 1.3, end users are not prompted to select a user certificate and instead see a "Missing certificate" error.
1772978	3-level hierarchy certificate authentication is not functioning.
1680651	REST API-based authentication fails when the administrator password contains the special character ":", while the same password works correctly via the admin Web GUI.
1739825 1753262	OAuth authentication fails when using PKCE (Proof Key for Code Exchange) on ICS
1742929	OCSP authentication fails as a result of an OpenSSL error.
Bookmark	
1670579	Multiple monitors use case does not work when RDP bookmark created for Smart card VM.
Host Checker	
1664534	Host Checker Component and PSAL is not launching for the remediation scenarios in Edge and Chrome browser.
PSAM	
1790995	Fixed an issue where small file downloads via a Web application failed over a PSAM-connected tunnel on 22.8R2.3, with the ICS device sending RST, ACK. This issue has been resolved in ICS 25.1.1.0.
HTML5	
1641211	RDP print functionality is not working when the print option is enabled in an RDP HTML5.
1777466	Unable to create HTML5 SSH resource profile via REST API.
1778321	File upload fails during an SSH session.
1384221	Advance HTML5 SSH session fails to login via private key.
Active Directory	

Problem Report Number	Summary
1641932	In a cluster setup, UEBA (User and Entity Behavior Analytics) functionality does not work for the first user who accesses the system after an upgrade
1642170	Change Machine Password in Troubleshooting section of AD server configuration does not work.
1624127	On the AD troubleshooting page, DNS resolution checks fail for some AD servers when multiple AD servers are configured. DNS resolution is only successful for the AD server that is also configured as the DNS server.
1634104	AD server uses AES256 encryption type for Kerberos. Authentication protocol even when AES 256 encyption option is not enabled.
1590484	Node secret is not generated on the RSA server, resulting in the absence of the node verification file on the Ivanti Connect Secure (ICS) device.
1546749	Active Directory (AD) traffic segregation is not functioning as expected at both the global and server levels. Specifically, if DNS is configured on a non-internal port, domain join fails, and DNS traffic does not flow through the non-internal port.
User Experience and UI	
1641679	Screen recording for an end-user session fails (recording cannot be saved or downloaded) when the “Screen Recording End User” option is enabled in a bookmark and an end user attempts to utilize session recording.
1574532	An invalid URL is accessed in the end-user login page, clicking the OK button does not redirect or navigate the user to the home page.
1628122	A bookmark is created, the description field automatically includes an extra "0" (zero).
1634866	HTML5 client copy-paste functioality does not work.
1717773	Blank spaces are appended to the NetBIOS name for macOS devices in Host Checker policy results.
1717655	The web login page does not load properly after enabling TLS 1.3.
1664473	Translation errors appears in File Upload and Save Options on End user page

Problem Report Number	Summary
WAF	
1634835	An Admin attempts to delete more than 198 users at once, the Web Application Firewall (WAF) blocks the request.
1634847	No "Upload successful" message is displayed after uploading a WAF ruleset package.
1791256	WAF logs missing the source IP address.
Console	
1641516	File system check (fsck) related messages are seen in the console.
1658693	ICS console shows boot manager screen.
Licensing & Sync	
1634927	Android devices are unable to sync emails using ActiveSync.
1786386	iOS devices using ActiveSync are unable to send or receive emails with attachments after upgrading ICS to version 22.8R2.2.
Nginx & Proxy	
1721222	Nginx process is crashing, resulting in inability to access the Connect Secure server.
1720459	The NGINX program recently failed, causing service disruption.
1756224	Restarting the Nginx process results in all user sessions being dropped on ICS.
1756618	The web page does not display or function as expected when accessed via a pass-through proxy.
API & Web Resource	
1711932	The API PUT request for realm role-mappings fails when there are more than 249 role-mappings included in the request.
1722707	Users receive an ERR_EMPTY_RESPONSE error when attempting to connect directly to PTP (Point-to-Point) resources through the rewriter.

Problem Report Number	Summary
VPN & Session Management	
1691200	VPN sessions disconnect intermittently, displaying the error message "auth check failed, session has expired."
1732180	The Radius process crashes unexpectedly on ICS 22.8R2.1.
1726310	Traffic ceases on SSL VPN tunnels following an upgrade to version 22.8R2.1.
Language, Browser & Windows Terminal Services	
1720290	PSAL fails to launch or operate correctly when the browser language is set to any language other than English.
1743209	Version mismatch between Microsoft DLLs installed by the installer and the system DLLs present on the machine causing Issues in WTS.

Known Issues

The following table lists the known issues in respective release:

Problem Report Number	Release Note
Release 25.1.2.1	
1879013	**Symptom**: JSAM launch fails on MAC OS **Condition**: When JSAM is launched via all browsers. **Workaround**: There is no workaround
1867641	**Symptom**: Copy and paste do not work in VNC. **Condition**: Occurs when using an Ubuntu VNC bookmark. **Workaround**: NA
1861808	**Symptom**: Copy and paste do not work in the HTML5 SSH bookmark. **Condition**: Occurs when attempting to use Ctrl+C and Ctrl+V. **Workaround**: Pasting with right-click works.
Release 25.1.1.0	
Clustering	
1816740	**Symptom**: Internal ICT periodic and scheduled scans do not work in a cluster. **Condition**: Observed in a clustered environment. **Workaround**: NA
Windows Terminal Services	
1819807	**Symptom**: The administrator is unable to enable the options “Deny single sign-on for sessions added by user” and “Enable Remote Desktop launcher”. **Condition**: This issue occurs on the Terminal Services options page. **Workaround**: NA
1820150	**Symptom**: The “Allow users to enable local resources defined below” options are enabled by default. **Condition**: On the Terminal Services page, the administrator is unable to disable these options. **Workaround**: NA
Logging & Debugging	

Problem Report Number	Release Note
1776690	**Symptom**: Process names specified in debug log configuration do not appear in the Admin logs. **Condition**: This issue occurs when process names are included in the debug log settings. **Workaround**: NA
Authentication	
1800576	**Symptom**: End-user logins fail when authenticating against the certificate server. **Condition**: This occurs when users present a certificate issued by a leaf (Subordinate) CA in a three-level certificate hierarchy (SubCA signed by Intermediate CA, which is signed by the Root CA), and OCSP checking is enabled for certificate validation. **Workaround**: Enable TLS 1.3 on the server to restore successful user authentication.
UEBA	
1796977	**Symptom**: Time mismatch observed in UEBA user anomaly reports displayed in the admin UI. **Condition**: The issue occurs when downloading the reports as CSV files. **Workaround**: Convert UTC timestamps to ICS local time, or vice versa, as required.
Backend Access & Domain Info	
1788320	**Symptom**: Hostname and port-based Pass Through Proxy (PTP) does not work. **Condition**: Issue is observed when attempting to connect to backend servers such as VDI. **Workaround**: Accessing the backend server directly via the Rewriter component works.
1776653	**Symptom**: The List Domain Info page displays the same IP address and FQDN for all listed domains. **Condition**: This issue occurs when configuring an AD server that has trusts established with other AD servers. **Workaround**: NA

Problem Report Number	Release Note
WAF	
1799672	**Symptom**: WAF logs are not displayed in the event logs section. **Condition**: This issue occurs when Nginx Fluent Bit is turned off. **Workaround**: Disable and then enable the "WAF message" option under the event logs settings page.
JSAM	
1788311	**Symptom**: PSAL is unable to download, as button is not working, particularly in Ubuntu 24, JSAM is also blocked. **Condition**: Occurs when end users access ISAC options from a client session on Ubuntu 24, resulting in PSAL download failure and JSAM blockage. **Workaround**: None available at this time.
1783670	**Symptom**: A warning pop-up message stating "You don't have permission to change host files" appears when launching the JSAM applet. **Condition**: This issue is observed only when the DSID cookie is enabled at the role level option. **Workaround**: Disable the DSID cookie at the role level option to resolve this issue.
Web Access	
1799537	**Symptom**: 502 Bad Gateway error is observed. **Condition**: Occurs when navigating to Maintenance > Archival > Archiving Servers and entering a valid hostname or IP address, but leaving the destination directory, username, and password fields empty. Selecting any archival component and saving changes triggers the error. **Workaround**: NA
Release 25.1.0.1	
Certificate & Authentication	
1772978	**Symptom**: 3-level hierarchy certificate authentication is not functioning. **Condition**: This occurs when OCSP is enabled for certificate status checking. **Workaround**: None available at this time.

Problem Report Number	Release Note
1711706	**Symptom**: When switching from TLS 1.2 to TLS 1.3, end users are not prompted to select a user certificate and instead see a "Missing certificate" error. **Condition**: This issue occurs when the server is configured to use TLS 1.3. **Workaround**: One of the following workarounds may resolve the issue: • Restart the end user machine. • Restart the ICS server. • Try accessing with a different browser.
HTML5	
1777466	**Symptom**: Unable to create HTML5 SSH resource profile via REST API. **Condition**: While creating resource via REST API. **Workaround**: Works as expected with Admin UI.
1778321	**Symptom**: File upload fails during an SSH session. **Condition**: This issue occurs when attempting to upload files within an HTML5 SSH session. **Workaround**: NA
JSAM	
1751812	**Symptom**: PSAL is unable to launch the Java applet (JSAM) on Mac machines on Safari browser. **Condition**: This occurs when an end user accesses a JSAM bookmark on a Mac machine with "HTTP Only Device Cookie" enabled. **Workaround**: NA
Release 25.1.0.0	
Authentication & User Login	
1625208	**Symptom**: An "Invalid file" error occurs when uploading the sdconf.rec file during ACE server configuration. **Condition**: This issue occurs when the sdconf.rec file is generated from an RSA server running version 8.8 or later. **Workaround**: Use an sdconf.rec file generated from RSA server version 8.7 or lower.
1384221	**Symptom**: Advance HTML5 SSH session fails to login via private key.

Problem Report Number	Release Note
	Conditions:Occurs when attempting login via private key authentication in the web-based SSH client. **Workaround**: Login via password is supported.
1634450	**Symptom** : Java Secure Application Manager (JSAM) does not work on Mac systems.. **Condition**: Occurs when an end user attempts to access the JSAM applet using the Pulse Secure application on a Mac; the application is unable to launch the Java applet. **Workaround**: NA
1628264	**Symptom**: End user login is failing even though file is present in the path and logs are wrong; Host Checker is validating all the unselected policies. **Condition**: If custom File process is selected and file is present in the mentioned path. **Workaround**: Clientless is working.
1634677	**Symptom**: Default admin realm cannot be deleted. **Condition**: When admin tries to delete default admin realm from UI. **Workaround**: NA
1637539	**Symptom**: RADIUS disconnect requests do not terminate the session. **Condition**: Occurs when “processing of RADIUS disconnect requests” is enabled in the RADIUS server configuration. **Workaround**:NA
1642615	**Symptom**: Rarely, admin login fails with "invalid username or password" error message. **Conditions**: Mostly observed when admin is logging in for the first time. **Workaround**: None. Repeated login attempts should resolve the issue
Certificate, CRL, CA & Encryption Configuration	
1561276	**Symptom**: The certificate authentication end-user page becomes inaccessible after enabling the "Advanced Certificate Processing Settings" option under trusted client CA configuration. **Condition**: Occurs when, the “Advanced Certificate Processing Settings” option is enabled for a trusted client CA in the admin UI. **Workaround**: Disable "Advanced Certificate Processing Settings".

Problem Report Number	Release Note
1590484	**Symptom**: Node secret is not generated on the RSA server, resulting in the absence of the node verification file on the Ivanti Connect Secure (ICS) device. **Condition**: After the first end-user login, the ICS device does not display (or contain) the node verification files, indicating that node secret establishment with RSA SecurID is not occurring as expected. There is currently no impact on system functionality. **Workaround**: NA
1590662	**Symptom**: Enabling "Validate Server Certificate" for LDAP connections does not enforce or properly handle certificate validation. **Condition**: Occurs when the "Validate Server Certificate" option is enabled in LDAP configuration. Despite this setting, the system either ignores certificate errors, does not validate the server certificate as expected, or behaves as though the option is disabled. **Workaround**: NA
1622308	**Symptom**: The CRL Setting section is not visible in the Read-Only (RO) admin interface. Additionally, the CRL button is present but not greyed out (i.e., appears enabled) in the RO admin page **Condition:** Occurs when Certificate Revocation List (CRL) checking options are enabled. **Workaround**: NA
1651237	**Symptom**: WAF issue observed when configuring CRL (Certificate Revocation List) checking options in the following scenarios: • Manually configured CDP in Sub CA. • Backup CDP in ROOT CA. • CDP specified in trusted CA. **Condition**: Occurs when configuring CRL checking options and using an IP address in the CRL URL. **Workaround**: Use a domain name instead of an IP address in the CRL URL.
1648859	**Symptom**: ICS allows SHA1 trusted client/server CA certificate to import. **Condition**: Occurs when importing SHA1 certificate under trusted client/server CA.

Problem Report Number	Release Note
	Workaround: NA
Active Directory	
1546749	**Symptom**: Active Directory (AD) traffic segregation is not functioning as expected at both the global and server levels. Specifically, if DNS is configured on a non-internal port, domain join fails, and DNS traffic does not flow through the non-internal port. **Conditions**: • DNS configured on a non-internal port/interface. • AD domain join operation attempted. **Workaround**: NA
1624127	**Symptom**: On the AD troubleshooting page, DNS resolution checks fail for some AD servers when multiple AD servers are configured. DNS resolution is only successful for the AD server that is also configured as the DNS server. **Condition**: When multiple AD servers are configured on the ICS device, the troubleshooting page may show DNS resolution failures for some of the AD servers. **Workaround**:Configure the relevant AD server's IP address as the primary DNS server on the ICS.
1634104	**Symptom**: AD server uses AES256 encryption type for Kerberos. Authentication protocol even when AES 256 encyption option is not enabled. **Condition**: Admin tries to authenticate using AD server and goes for Kerberos Authentication Protocol (default option), with AES 256 option disabled in server configurations (default setting). **Workaround**: NA
1642170	**Symptom**: Change Machine Password in Troubleshooting section of AD server configuration does not work. **Condition**: Occurs when using a Windows AD 2025 server. **Workaround**: Use a Windows AD 2022 server, if possible.
OAuth	

Problem Report Number	Release Note
1642111	**Symptom**: OAuth traffic segregation is not working as expected at either the global or server levels; OAuth traffic is not routed through the configured port as intended. **Condition**: Occurs when traffic segregation policies are applied globally or per authentication server for OAuth traffic. **Workaround**: NA
1622322	**Symptoms**: OAuth time skew is not functioning according to the configured values. **Condition**: OAuth-protected operations (such as token validation) are not honoring the custom time skew settings as specified in the configuration. This can result in unexpected authentication or token validation failures if there is a time difference between the client and server. **Workaround**: NA
UEBA	
1641932	**Symptom**: In a cluster setup, UEBA (User and Entity Behavior Analytics) functionality does not work for the first user who accesses the system after an upgrade **Condition**: This issue occurs only in clustered environments and affects the very first user session after the system is upgraded. **Workaround**: No workaround is needed; from the second user onwards, UEBA functionality resumes and works as expected.
1648442	**Symptom**: After upgrading, User and Entity Behavior Analytics (UEBA) does not show expected logs for the first user session. Subsequent user sessions display logs correctly, and UEBA functionality proceeds as intended. **Condition**: Occurs when accessing UEBA immediately after upgrade. **Workaround**: Accessing UEBA as a second user (or after the first attempt) resolves the issue; all relevant logs are displayed thereafter.
Behavioral Analytics	
1637718	**Symptom**: An error message "Unable to load any data. Try applying valid filters and reload the page." is shown, and no data is displayed. **Condition**: Occurs when user records are filtered by MAC address in the Behavioral Analytics User Report.

Problem Report Number	Release Note
	Workaround: NA
1640860	**Symptom**: Cleared anomalies do not appear in the Behavioral Analytics User Report. **Condition**: Occurs after manually clearing (removing/dismissing) some anomalies and then viewing the Behavioral Analytics User Report.. **Workaround**: NA
Bookmark	
1630234	**Symptom**: JSAM (Java Secure Application Manager) bookmark access does not work when Java Runtime Environment (JRE) 1.8 is installed on the client system. **Condition**: Occurs when an end user attempts to access JSAM profiles using JRE 1.8. **Workaround**:Install Java Development Kit (JDK) 21 instead of JRE 1.8.
1670354	**Symptom**: "Request Header Or Cookie Too Large" message appears when accessing any kind of bookmarks added for the end-user. **Condition**: Occurs when the end-user opens the bookmark and tries to open the child links of the same page. **Workaround**: NA
1669941	**Symptom**: File browsing page refresh is not working. **Condition**: Occurs when user accesses the file share path via the browse option. **Workaround**: User can access admin created bookmark and perform a page refresh to make it work.
1670579	**Symptom**: Multiple monitors use case does not work. **Condition**: Occurs when RDP bookmark created for Smart card VM. **Workaround**: No issue is seen with single monitor.
1677378	**Symptom**: WTS bookmark fails to Autolaunch when end user login successfully. **Condition**: When WTS bookmark is configured with autolaunch enabled and Hostchecker is also enabled. **Workaround**: Disable Hostchecker so that WTS bookmark autolaunchs whenever enduser logins successfully.
1628122	**Symptom**: When a bookmark is created, the description field automatically includes an extra "0" (zero).

Problem Report Number	Release Note
	Condition:Occurs during bookmark creation (no additional specific conditions noted). **Workaround**: NA
1641211	**Symptom**: RDP print functionality is not working. **Condition**: Occurs when the print option is enabled in an RDP HTML5 bookmark. **Workaround**: NA
Host Checker	
1644287	**Symptom** : Host checker version displays as 1.0 in MAC. **Condition** : When a user launches the Host Checker application on Mac, the version shown in installed applications displays as 1.0. **Workaround** : Host Checker functions correctly; only the displayed version is "1.0".
1634866	**Symptom**: HTML5 client copy-paste functioality does not work. **Condition**: Occurs when a user attempts to use Command+C/Command keyboard shortcuts for copy-paste operations on a Mac. **Workaround**: Select the required content in the HTML5 client, then right-click and use the context menu to copy and paste the content on the local machine.
1664534	**Symptom**: Host Checker Component and PSAL is not launching for the remediation scenarios in Edge and Chrome browser. **Condition**: If 3 or more HC policies configure (Custom or Predefined). **Workaround**: Use Firefox browser or enable browser extension for Chrome/Edge.
1641387	**Symptom**: Host Checker Policies are empty in the remediation > Enable Custom Actions field. **Condition**: In all conditions, it is empty. **Workaround**: NA
1657227	**Symptom**: 502 bad gateway message is seen. **Condition**: When user clicks "Profile" hyperlink in the HC page. **Workardound**: N/A
REST API	

Problem Report Number	Release Note
1612333	**Symptom**: "IP Pool cannot be empty" error observed when switching from DHCP-based IP assignment to Pool-based for VPN Connection Profiles via REST API. **Condition**: Occurs when the "ip-address-pool" attribute is provided before the "ip-address-assignment" attribute in the request body. **Workaround**: Provide "ip-address-assignment" before the "ip-address-pool" attribute in the request body.
1601479	**Symptom**: Configuring FQDN based lockdown exception rule for a connection set fails when attempted via the REST API. **Condition**: Occurs when attempting to configure an FQDN-based lockdown exception rule for a connection set using the REST API. **Workaround**: Configure the FQDN-based lockdown exception rule manually via the Ivanti Connect Secure (ICS) administrative user interface.
1634397	**Symptom**: Exception rule creation when using rest API failed. **Condition**: Occurs during attempts to create an exception rule via REST API. **Workaround**: None
1658685	**Symptom**: REST API call to set FIPS is failing with error: "Non FIPS Cipher is selected when FIPS mode is on (Outbound)". **Condition**: Occurs when enabling FIPS using REST API and TLS 1.3 is selected in In-Bound settings. **Workaround**: Configure FIPS manually from Admin UI page.
Upgrade	
1634850	**Symptom**: Bind failed related logs are seen for few seconds. **Condition**: During ICS upgrade. **Workaround**: NA
1640944	**Symptom**:The error message /bin/tar: tlscerts/cert.pem: Not found in archive is displayed on the console. **Condition**: Occurs during the Ivanti Connect Secure (ICS) upgrade process. **Workaround**: NA
1658693	**Symptom**: ICS console shows boot manager screen. **Condition**: Occurs while performing an upgrade.

Problem Report Number	Release Note
	Workardound: Perform a reset or reboot from the boot manager; the upgrade will restart.
1600182	**Symptom**: The message "Unable to synchronize time, either NTP server(s) are unreachable or provided symmetric key(s) are incorrect" appears in the system logs. **Conditions**: This occurs after a system upgrade or a reboot. **Workaround**: NA
Config Import	
1641516	**Symptom**: File system check (fsck) related messages are seen in the console. **Condition**: Occurs when an administrator performs a reboot or clears the device configuration. **Workaround**: No functionality impact observed.
1666021	**Symptom**: Push config fails for custom port syslog server config. **Condition**: Occurs when configuration is pushed from a lower build ICS to the latest. **Workaround**: Configure using the ICS Gateway UI.
1666027	**Symptom**: Syslog XML import fails for custom port syslog server config. **Condition**: Occurs when exported from ICS lower build and imported to latest ICS build. **Workaround**:Configure using the ICS Gateway UI.
1664557	**Symptom**: Blank screen appears when attempting to use a custom sign-in page imported via XML or binary. **Condition**: Due to Perl modules upgrade, stricter rules are applied in handling HTML files. **Workaround**: Import the custom sign-in page as a zip file format; UI will display any errors encountered. Resolve the errors, then re-upload the custom sign-in pages.
1669912	**Symptom**: HTML5 storage config is not getting imported. **Condition**: Occurs when importing binary HTML5 config. **Workaround**: : Configure using the ICS Gateway UI.
WAF	

Problem Report Number	Release Note
1634835	**Symptom**: When an Admin attempts to delete more than 198 users at once, the Web Application Firewall (WAF) blocks the request. **Condition**: Occurs during the deletion of more than 198 users in a single operation. **Workaround**: Delete users in smaller batches of up to 150 users at a time to avoid WAF blocking.
1634847	**Symptom**: No "Upload successful" message is displayed after uploading a WAF ruleset package. **Condition**: Occurs when an administrator uploads a WAF ruleset package through the UI. **Workaround**: Check the admin logs to confirm the status of the upload.
1665495	**Symptom**: WAF messages are seen in event logs. **Condition**: When accessing HTML5 bookmarks via REST API. **Workaround**: NA
Network Operations	
1616321	**Symptom**: Bandwidth management does not work. **Conditions**: Occurs when SSL is used. **Workaround**: Use ESP protocol instead of SSL.
1637651	**Symptom**: Traceroute output displays %int0, %ext0, %mgt0. **Condition**: NA **Workaround**: NA
1648583	**Symptom**: Pushing config does not works using IPv6. **Workaround**: Use IPv4 for push config functionality to work.
1663938	**Symptom**: Unable to view the charts for Concurrent Users, Hits Per Second, etc in Overview Page. **Conditions**: Occurs when attempting to view stats for another member in the cluster. **Workaround**: View stats from the Admin UI of the respective cluster node. Impacted Functionality: Graphs on Admin UI page.
1665464	**Symptom**: "IPv6 not enabled on any port" error message is displayed when using troubleshooting commands.

Problem Report Number	Release Note
	Condition: Occurs when VLAN ports are configured with IPv6 address, but internal, external, and management ports are not configured with IPv6 address. **Workaround**: This is a display issue and does not impact functionality.
1665457	**Symptom**: Portprobe is not working with management port VLAN. **Condition**: Occurs when admin attempts to perform portprobe using VLANs created on the management port. **Workaround**: NA
1628560	**Symptom**:Ivanti Connect Secure (ICS) is sending syslog messages (for both TCP and UDP) over the management port. **Conditions**: This occurs when syslog is configured with default settings. **Workaround**: Disable the management port.
UI	
1641679	**Symptom**:Screen recording for an end-user session fails (recording cannot be saved or downloaded). **Condition**: Occurs when the "Screen Recording End User" option is enabled in a bookmark and an end user attempts to utilize session recording. **Workaround**: Open the browser's developer tools console and enter $rdp.close( ). This triggers a pop-up allowing the user to save the session recording to the client device.
1574532	**Symptom**: When an invalid URL is accessed in the end-user login page, clicking the OK button does not redirect or navigate the user to the home page. **Condition**: Occurs when a user browses to any invalid URL on the end-user login page and interacts with the error prompt by clicking "OK". **Workaround**: NA
1679335	**Symptom**: Sample template files related to Kiosk and SoftID are not working for custom sign-in pages. **Condition**: Seen on both Kiosk and SoftID templates. **Workaround**: NA
1648229	**Symptom**: Error 403 is seen while enabling/disabling/vip failover node in AP cluster with NSA 22.8R1.4 and 25.1.0.0 gateway. **Workaround**: Try performing enable/disable/vip failver from the gateway UI

Problem Report Number	Release Note
LDAP	
1634055	**Symptoms**: Encountered an error "Invalid LDAP server IP address". **Condition**: This occurs when attempting to configure an LDAP server using an IPv6 address. **Workaround**: NA
1634087	**Symptom**: When configuring a Backup LDAP server, an error “Invalid admin Credentials” is encountered. **Condition**: Occurs while entering the Backup LDAP Server IP and Base DN during server configuration. **Workaround**: NA
JSAM	
1566054	**Symptom**: JSAM is not accessible on Ubuntu; an error "Application launcher is not installed" is seen. **Condition**: JSAM is not accessible on Ubuntu. **Workaround**: NA
1635741	**Symptom**: Unable to access the intranet server "tools-svr.engdevroot.com" using JSAM. **Condition**: Occurs when trying to access "tools-svr.engdevroot.com" using JSAM. Workaround : NA
Deployment	
1671089	**Symptom**: Assuming ownership of connection set fails after turning on FIPS mode where TLS 1.3 is enabled. **Condition**: Next generation service restart causes the failure. **Workaround**: Add sleep time after enabling FIPS mode.
1670033	**Symptom**: ICS returns blank page when public sites are accessed. **Condition**: When public sites are enabled with CSP. **Workaround**: NA
1674580	**Symptom**: Package upload fails for 2nd node. **Condition**: During cluster upgrade.

Problem Report Number	Release Note
	Workaround: It automatically tries to upload package again and cluster upgrade proceeds further.
1669339	**Symptom**: Login through Rest API fails with TLS 1.3 enabled after Lockdown Exception rules are configured. **Condition**: Occurs when REST API is triggered. **Workaround**: Login using Admin UI.
Logs	
1676718	**Symptom**: Failed to update profile for user message seen in Event logs. **Conditions**: Messages are seen under the following conditions:: • Secondary auth is enabled for a User Realm • Adaptive Authentication is enabled for the User Realm • End user trying to login using ISAC **Workaround**: None. Adaptive Auth functionality is not affected.

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