ivanti

Ivanti Connect Secure Release Notes 25.1.3.1

ivanti

CONTENTS

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

1. Ivanti Connect Secure: Release Notes

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.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

2. Revision History

The following table lists the revision history for this document:

Document Revision	Date	Description
4.0	September 2026	Updated what's new, Known Issue for 25.1.3.1
3.0	July 2026	Updated what's new, VM support, and Fixed Issues for 25.1.3.0
4.0	May 2026	Updated what's new and Fixed Issues for 25.1.1.1.
3.0	March 2026	Updated what's new, Known Issue, and Fixed Issues for 25.1.1.0.
2.0	February 2026	Updated what's new and Known Issue.
1.0	September 2025	First version for 25.1.0.0

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

3. What's New

Version 25.1.3.1

Product Version	Build
ICS 25.1.3.1	23681
ISAC 22.8R7 Mobile Client 22.8R8	48847 18981 (Android) 96449 (iOS)
WAF Default CRS	1.0.4
Default ESAP	4.6.4

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

- **RSA Authentication Manager 8.8**: Support for RSA Authentication Manager 8.8 is qualified as part of the validation for ICS 25.x. As a result, users who have upgraded to RSA Authentication Manager 8.8 will be able to use this functionality with ICS 25.1.3.1. For RSA Authentication Manager 8.8 and newer versions, Ivanti recommends using the new RSA (REST API) authentication server, see see **Using a RSA Server (REST API)**.
- **Import XML via REST API** : You can now import XML configuration files through a REST API. The Import XML REST API uses the same validation and processing workflow as the Import XML operation in the Ivanti Connect Secure (ICS) Admin UI, see **Import XML Rest API**.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Version 25.1.3.0

Product Version	Build
ICS 25.1.3.0	22109
ISAC 22.8R7 Mobile Client 22.8R8	48847 18981 (Android) 96449 (iOS)
WAF Default CRS	1.0.4
Default ESAP	4.6.4

- **Rest API Diagnostic Logs**: A new Rest API Diagnostic Logging capability has been added to improve visibility into system health monitoring operations. Administrators can use these logs to assist troubleshooting and operational diagnostics, see Rest API Diagnostic Logs.
- **Windows Hello for Business (WHfB) Single Sign-On Enhancements**: This release includes enhancements to Windows Hello for Business (WHfB) Single Sign-On functionality, providing improved integration with modern authentication workflows and passwordless authentication deployments, see Windows Hello for Business SSO Server.
- **FIDO2 Authentication Enhancements**: ICS has been enhanced to support FIDO2-related authentication improvements, enabling support for modern passwordless authentication methods and strengthening identity security, see FIDO2 support for mobile ISAC .
- **Active User Session API Enhancements**: The Active User Sessions REST API has been enhanced to support filtering session data based on user, see Active User session.
- **WebSocket Support Through HTTP(S) Proxy**: Ivanti Connect Secure (ICS) now supports establishing and maintaining WebSocket connections to backend application servers through a configured HTTP(S) web proxy. This enhancement enables WebSocket-based applications to function seamlessly in environments where proxy routing is required by organizational policies.
- **Automated Certificate Management Environment (ACME) Support**: Ivanti Connect Secure now supports the Automated Certificate Management Environment (ACME) protocol to automate certificate requests, domain validation, certificate issuance, and certificate deployment on the designated interface, see ACME Server.
- **Default VLAN ID Support with IPv6 on Internal Interfaces:** Ivanti Connect Secure now supports the use of the Default VLAN ID when IPv6 is configured on the Internal Interface. This enhancement ensures that the Default VLAN ID remains available and functional when both IPv4 and IPv6 are enabled, see Default VLAN ID.
- **Bulk ACL Management Using REST API**: Ivanti Connect Secure now supports bulk management of Access Control Lists (ACLs) through REST API. Administrators can create, update, and delete multiple ACLs in a single API request, improving scalability and operational efficiency for large enterprise and MSP deployments, see Create Multiple ACLs .
- **Postman Collection for ICS REST APIs**: Ivanti Connect Secure now provides a Postman collection for publicly available REST APIs, enabling administrators and developers to quickly explore, test, and integrate ICS APIs using the Postman client, see Postman Collection.
- **OAuth Group Claims for Role Mapping**: Ivanti Connect Secure (ICS) now supports role mapping based on group claims received from OAuth providers such as Microsoft Entra ID (Azure AD). Administrators can use group information included in the OAuth ID Token or UserInfo response to assign user roles within ICS user realms, see OAuth Group Claims Role Mapping.
- **HTTP/2 Ingress Support in Connect Secure**: Connect Secure has been enhanced to support HTTP/2 for inbound client connections. HTTP/2 provides improved connection efficiency and performance through multiplexing and optimized

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

protocol handling, see **HTTP Protocol Configuration**.

- **Secure Boot and vTPM Support**: GCP, AWS platform now provides secure boot support with vTPM functionality, enhancing security and integrity for virtual machines, see **Secure Boot with TPM/vTPM**.
- **Virtual appliance platforms**: Added support for the new virtual appliance platforms ISA-V 4500, ISA-V 6500, and ISA-V 8500 in Ivanti Connect Secure (ICS) version 25.1.3.0, see **ISA VA Supported Platforms**.
- **Host Header Validation**: Ivanti Connect Secure now provides a console-based option to disable Host Header Validation on the management interface. This enhancement supports deployments where the management interface is accessed through Network Address Translation (NAT), helping ensure administrative access in environments where Host Header Validation may otherwise block requests, see **Host Header Validation**.
- **Configurable Certificate Challenge Timeout**: Administrators can now configure the maximum interval between certificate challenge exchanges during the pre-authentication phase of certificate-based authentication. The timeout value can be set from 1 to 4 minutes, with a default value of **1** minute, see **Certificate Challenge Timeout**.
- **UI Enhancement for Compliance Report**: Failed policies now display the corresponding failed rule names and failure reasons. Additionally, Host Check results are presented in a separate column to improve visibility and reporting clarity, see **Using Host Checker Reports and Logs**.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

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.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

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**.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

4. 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.

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.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

25.1.3.0

- Downgrade operations are no longer supported after the Storage mounting/unmounting capability restriction changes. Administrators must use supported upgrade paths and rollback procedures. Installing older releases by bypassing version validation can result in incompatibilities between installation scripts and platform utilities and may cause installation failures.
- To strengthen security, Ivanti Connect Secure now enables only AES-256, SHA-256, and DH 2048-bit or larger IKEv2 Phase 1 negotiation parameters by default. Administrators must ensure that IKEv2 clients are configured to support these settings. This enhancement applies to new installations, upgrades, and configuration imports (XML and binary) on Ivanti Connect Secure gateways starting with release 25.1.3.0. If compatibility issues are encountered, administrators can manually disable individual negotiation parameters or disable all of them as needed. For configuration imports originating from the same software version, the administrator-configured settings are preserved. For additional information, refer to the **KB** article
- **Secure-by-Default Change for SAML 2.0 SP Signature Validation**: Starting with ICS 25.1.3.0, when Ivanti Connect Secure (ICS) is configured as a SAML 2.0 Service Provider (SP), signature validation of incoming SAML responses is enabled by default. This secure-by-default enhancement aligns with Ivanti's recommended security best practices. To ensure successful SAML authentication, administrators must upload the Identity Provider's (IdP) complete CA certificate chain to the Trusted Client CAs list: Configuration > Certificates > Trusted Client CAs > Import Trusted Client CA This change affects only deployments that use SAML authentication on Ivanti Connect Secure. For additional information, refer to the **KB** article.
- SNMP Configuration Limitations
  - The following limitations apply when configuring SNMP:
    - SNMP v2/v3 usernames can contain only alphanumeric characters.
    - SNMP v3 passwords can contain alphanumeric characters and the following special characters only: ! @ # % ^ & * ( ) \ $
    - The length of SNMP v3 usernames are limited to a maximum of 31 characters.
    - The length of System Name, System Location, and System Contact fields are each limited to a maximum of 254 characters.
- **Secure-by-Default Change for LDAP Server Certificate Validation**: Starting with ICS 25.1.3.0, the Validate Server Certificate option is enabled by default when configuring a new LDAP server. To establish trust, administrators must ensure that the CA certificate required to validate the LDAP server's certificate chain is present in the Trusted Server CAs list on Ivanti Connect Secure. If certificate validation cannot be configured due to technical constraints, administrators can explicitly disable this setting. However, disabling server certificate validation is not recommended. For additional information, refer to the **KB** article.
- **Secure by Default**: To enhance security, the **Delete all cookies at session termination** option is enabled by default under **System > Configuration > Security > Miscellaneous.** When this option is enabled, session cookies are removed when a user session ends. In rare cases, during session migration between Layer 7 access and other client launch types, some web browsers may withhold session cookies, which can prevent certain applications, such as JSAM, from launching successfully. If this behavior is observed, administrators can explicitly disable this setting. For additional information, refer to the **KB** article.
- **Upload Custom Sign-In Pages** feature is temporarily removed in Ivanti Connect Secure 25.1.3.0. The ability to execute scripts from template files has been identified as a security weakness. This feature will be temporarily removed until we re-architect it without this security weakness. Customers will no longer be able to upload and use template-based (THTML)

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

custom sign-in page ZIP packages. Customization on sign-in pages using the previously uploaded template files will also no longer working. Refer the **FAQ** for additional detail.

- When adding or deleting multiple LDAP groups simultaneously, group names containing DC=local (non-builtin groups) may trigger cumulative WAF anomaly scoring, causing the request to be blocked. This behavior is intentional and is not whitelisted to preserve security enforcement. To avoid request blocking, administrators should add or delete LDAP groups containing DC=local individually rather than performing bulk operations.
- If password policy controls are enabled but the configured LDAP server does not support the Password Policy Control extension, error messages similar to the following may appear in the LDAP server logs or console: *slap_global_control: unrecognized control: 1.3.6.1.4.1.42.2.27.8.5.1*

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

- Previously, the same log messages were generated regardless of whether the operation was performed through the Admin UI or the REST API. As a result, operations initiated via the REST API could produce misleading log entries that implied the action was performed from a UI page. The log messages have been revised to use a more generic description, accurately reflecting the operation without referencing a specific interface.

  Previous log format:

```bash
ADM31403 - TOTP User '<username>' account has been unlocked from '<authservername>' auth-server user's page
```

```bash
ADM31403 - TOTP User '<username>' account has been reset from '<authservername>' auth-server user's page
```

  Updated log format:

```bash
ADM31403 - TOTP User '<username>' account on auth-server '<authservername>' has been unlocked
```

```bash
ADM31403 - TOTP User '<username>' account on auth-server '<authservername>' has been reset
```

- A dashboard banner now displays the type of server for which the Server Certificate Validation option is available but not enabled.

25.1.1.1

- This release version includes security enhancement. Ivanti encourages customers to upgrade to this latest version.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

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.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

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

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

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**.
- 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.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

> 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.

Offline and Online Viewer for Advanced HTML5 Recordings

- Advanced HTML5 External Storage recording files for **RDP, SSH, and VNC** sessions can be viewed using the **RemoteSpark Player**. The online player is available through the **RemoteSpark Player** web interface, allowing users to play recorded sessions directly in a browser.
- In addition, **offline player installers for Windows and macOS** are available, enabling users to view recorded session files locally without requiring access to the web-based player or an internet connection.To download the HTML5 Offline Viewer, click the download **link**, sign in to the Ivanti Support portal, and navigate to **Download > Network Security > Ivanti Connect Secure > ICS HTML5 Offline Viewer**.
- **macOS:** `ics_html5_offlineviewer-aarch64.dmg`
- **Windows:** `ics_html5_offlineviewer-x64-en.msi`

RSA Authentication

- 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.

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

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

- **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.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

5. 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)
25.1.3.1	25.1.3.0
25.1.3.0	• 25.1.2.0, 25.1.2.1, 25.1.2.2 on ISA6500 • 25.1.2.2 on ISA8500
25.1.1.1	25.1.1.0, 22.8R2.3
25.1.1.0	25.1.0.1, 25.1.0.0, 22.8R2.3, 22.8R2.2, 22.8R2.1
25.1.0.1	25.1.0.0, 22.8R2
25.1.0.0	22.8R2

Upgrading to ICS GW version 25.1.0.0 is supported only from version 22.8R2 for standalone ISA hardware appliances and ISA-V ESX virtual appliances.

Note that cluster upgrade is not supported from 22.8Rx to 25.x but is supported from 25.1.0.0 and above to 25.1.1.0. For more information, see **Cluster Migration from 22.8Rx to 25.x**. Additionally, upgrades from earlier versions (22.7R2.x and below) to 25.1.0.0 are not supported.

Note:

- Do not initiate upgrade process through external interface of the appliance. Administrative access on external interface has been removed on Ivanti Connect Secure.
- Refer the instructions and notes in the **How to Upgrade**? article before upgrading your ICS.

Configuration Migration Path

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

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Migrate to	ISA Hardware device Migrate From (Supported Versions)	VA Migrate From (Supported Versions)
25.1.3.1	25.1.3.0 , 25.1.2.2, 25.1.1.1, 22.7R2.14	25.1.3.0 , 25.1.2.2, 25.1.1.1, 22.7R2.14
25.1.3.0	25.1.2.2, 25.1.2.1, 25.1.2.0, 25.1.1.1, 25.1.1.0, 22.8R2.4, 22.7R2.14	25.1.2.2, 25.1.2.1, 25.1.2.0, 25.1.1.1, 25.1.1.0, 22.8R2.4, 22.7R2.14
25.1.1.1	25.1.0.1, 25.1.1.0, 22.8R2.3, 22.7R2.12	25.1.0.1, 25.1.1.0, 22.8R2.3, 22.7R2.12
25.1.1.0	25.1.0.1, 25.1.0.0, 22.8R2.3, 22.8R2.2, 22.8R2.1, 22.7R2.12, 22.7R2.11	25.1.0.1, 25.1.0.0, 22.8R2.3, 22.8R2.2, 22.8R2.1, 22.7R2.12, 22.7R2.11
25.1.0.1	25.1.0.0, 22.8R2 and 22.7R2.8	25.1.0.0,22.8R2 and 22.7R2.8
25.1.0.0	22.8R2, 22.7R2.8, and 22.7R2.7	22.8R2, 22.7R2.8, and 22.7R2.7

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

6. Support and Compatibility

Hardware Platforms

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

- ISA6500
- ISA8500

Virtual Appliance Editions

The following table lists the virtual appliance systems qualified with this release:

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Virtual appliance qualified in Platforms for 25.1.3.1

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Variant	Platform	vCPU	RAM
VMware ESXi 8.0U3d	ISA4500-V	4	8 GB
	ISA6500-V	8	16 GB
	ISA8500-V	12	32 GB
AWS	ISA4500-V (c7i.xlarge)	4	8 GB
	ISA6500-V (c7i.2xlarge)	8	16 GB
	ISA8500-V (c7i.4xlarge)	16	32 GB
	ISA4500-V (m7i.xlarge)	4	8 GB
	ISA6500-V(m7i.2xlarge)	8	16 GB
	ISA8500-V (m7i.4xlarge)	16	32 GB
	ISA4500-V (c7i-flex.xlarge)	4	8 GB
	ISA6500-V (c7i-flex.2xlarge)	8	16 GB
	ISA8500-V (c7i-flex.4xlarge)	16	32 GB
	ISA4500-V (m7i-flex.xlarge)	4	8 GB
	ISA6500-V (m7i-flex.2xlarge)	8	16 GB
	ISA8500-V (m7i-flex.4xlarge)	16	32 GB
Azure	ISA4500-V (Standard_D4ds_v6)	4	16 GB
	ISA4500-V (Standard_D4s_v6)	4	16 GB
	ISA6500-V (Standard_D8ds_v6)	8	32 GB
	ISA6500-V (Standard_D8s_v6)	8	32 GB
	ISA8500-V (Standard_D16ds_v6)	16	64 GB
	ISA4500-V (Standard_F4as_v6)	4	16 GB
	ISA6500-V (Standard_F8as_v6)	8	32 GB
	ISA8500-V (Standard_F16as_v6)	16	64 GB
GCP	ISA4500-V (n4-standard-4)	4	16 GB
	ISA6500-V (n4-standard-8)	8	32 GB
	ISA8500-V (n4-standard-16)	16	64 GB

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Variant	Platform	vCPU	RAM
Hyper-V Microsoft Hyper-V Server 2022	ISA4500-V	4	8 GB
	ISA6500-V	8	16 GB
	ISA8500-V	12	32 GB

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

For more information see **Support Platform Guide**.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

7. Resolved Issues

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

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Summary
Release 25.1.3.0	
Logging and Auditing	
1706130	Log improvement to Improve traceability of SML31064 user access log.
1702826	Improve admin logs for SAML SSO Policy configurations during resource policies creation/editing.
1702471	Max Sessions Log Entries Lack Username and Session ID
1718345	Fix the logging context for admin log generated during unlocking of locked TOTP users.
1856647	User Access log shows below message even before TOTP fallback prompt entered in Ivanti Client (only noticed via Ivanti Client based Access
1782798	Connect Secure server running 22.7r2.11 code and faces an issue where host header validation failure logs are wrongly be logged as a Terminal Services user.
1789954	Bandwidth consumed field appears blank in user access logs
1951425	Incorrect details printed in user access logs for host header validation failures.
Authentication and Access Management	
1626252	Fix ISAC behaviour when incorrect RADIUS challenge token is entered during user authentication.
1773336	Unable to create AD Authentication server with Domain name containing Single character in 22.7R2.8 and above
1848336	In case of cert auth configured, Certificate Restriction causing failure even no cert restrictions are configured and fallback not triggered
1863054	ERR24617 is shown in the ICS user access logs, stating that the Kerberos TGT time validity is hardcoded to 5 minutes instead of 10 hours, and therefore fails with an error
1786401	CRLs Automatically Disabled Intermittently, Causing User Connection Issues
1813625	OCSP validation failure in 22.8R2.3 with SELinux enforcing mode
1856666	Missing Eye Icon in Web Browser TOTP Prompt
1856645	LDAP Auth Backup Admin Removal Shows ‘0’ and ‘*’ in ICS Device (Version 25.1.1.0)
VPN and Tunneling	
1974065	iPad users are unable to establish VPN connections. The login process becomes stuck at"Host Checker Loading Components", and the VPN tunnel is never established.
1716929	Users are unable to connect to VPN after upgrading to 22.7R2.8 and above, with the error: "Removing the connection due to IP allocation failure."
1718464	Intermittent IP Allocation Failures Due to TUNSETIFF Error
1841773	IP Allocation Failure on ICS 22.7R2.12
1915919	L3 tunnel fail to establish after authentication over time

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Summary
1800401	Source IP is disabled upon upgrading the server from 22.7R2.9 to 22.7R2.12
Clustering and High Availability	
1724880	Duplicate IP Addresses on Management VLAN Interface While Creating Cluster on 22.8R2.1
HTML5 Access and End User Experience	
1762201	HTML5 RDP Auto-Launch Fails When VPN Tunneling Is Disabled in User Role
1797472	HTML5 RDP session are failing on Connect Secure 22.7R2.12 when the camera is enabled in the bookmark
1801742	Users sessions face an idle timeout issue when the users is using HTML5 RDP on 22.8R2.2
1864473	Login Button in Session Warning Page is Not Clickable on Mobile Devices on 25.1.1.0
Web Rewriting and Bookmarks	
1758145	Internal Links for Alfresco bookmark are not working via rewriter
1753650	Server running 22.8x and is unable to access a site through web rewriter.
1848360	Issue in Editing fields while accessing a web resource after upgrading to 22.8R2.1
1849978	"The requested resource is not valid." Is seen when The Referer Header URL Contains BackSlash "\"
1720879	High CPU / SSL Loop Issues with SharePoint Bookmark on ISA4000-V
File Share and Resource Access	
1695554	FileShare Access Issues Due to Incorrect FileShare AutoPolicy Created by ICS In Certain Condition
1743404	After migrating from 9.1rx PSA Connect Secure to 22.7x ISA Connect Secure, the browser ctrl f search for the file share feature cannot locate all files.
SAML	
1736008	ICS is Providing Corrupted SAML Metadata While Downloading via the Connect Secure Entity ID URL Directly on 22.7R2.9 and Above
REST API and Configuration Management	
1764337	API and XML import not working properly for Mobile OS checks
1763112	Rest API Request to Import Large Number of Users Fails With Error "413 Request Entity Too Large" on ICS 22.8R2.2
1781955	REST API unable to fetch the MAC Address of the ICS interfaces for some devices and shows as blank
1841711	Unable to create syslog server with custom port failed through Rest API

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Summary
1884929	ACL Validation Failure For Virtual Hostname Resources In Certain Condition on 25.1.1.1
1880336	Failure to Add Custom Expressions on 22.7R2.9 Due to Dictionary Memory Limit Exhaustion
Network Services and Protocols	
1730391	Incorrect Interface is used by ICS when HostChecker uses OCSP Traffic Validation for machine cert
1773736	LDAPS Port Support and Port Range Behavior on ISA-6000 (22.8R2.1)
1809448	DMI/Netconf is not working in 22.7R2.11 onwards
System Stability and Performance	
1728074	Memory Utilization Gradually Increasing on Ivanti Connect Secure Nodes – Due to dstaillog Process
1801392	High Memory Usage on ICS 22.8R2.2 due to nginx Worker processes
1847037	NGINX Reload Causing User Disconnections in 22.8R2.3
1809222	Recurring “Program nginx recently failed” Events on ICS 22.8R2.3
1837525	High CPU Utilization and Server Freezes on System Running ICS 25.1.1.0
1800973	Manage Synchronous way of triggering rewriter processes on IP change to avoid duplicates and result in process exhausion
1846861 1849271	Facing internal server error intermittently while accessing admin UI pages after upgrade to nginx
Licensing	
1734668	The system is unable to connect to the local license server and displays the following error: *License server low-level protocol error, server=127.0.0.1:5000, Code=[7]: Could not connect*
1847193	License Leasing Failure on Client Node - 25.1.0.0
Administration and User Interface	
1739404	PSAL version build details displayed on Admin UI is incorrect-25.x
1798083	Config Archiving (Binary vs XML) with password shows a blank box.
1792433	NewUI Enforce Post Upgrading to ICS 22.7R2.12
1713334	Post upgrade to IPS 22.7R1.10 customer is observing web process snapshot and its changing the time on the snapshot page
1781932	500 internal CGI error message shown to users logging in to ICS via web browser after ICS upgraded to 22.7R2.11
JSAM	
1913474	Pop-Up Appears while connecting to JSAM - Error "Cannot find the hosts file. Please contact your Administrator"

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Summary
1859146	JSAM displays a certificate expiration warning/error even though the application was signed with a valid certificate. The validation incorrectly uses the current system date instead of the certificate signing timestamp.
UEBA and Analytics	
1869101	UEBA database appears to be out of date and classifying IP address as wrong country
SCP and Archiving	
1738502	22.7R2.10 Connect Secure server is unable to use SCP Archive to their Windows server that has a P drive set up.
Database / Internal Processing	
1852675	In dsserver execution correct commit while iteration code usage
Networking and Resource Access	
1832217	Intermittent Packet Loss On Internal Interface From Tunnels Leading to Resource Access Failures for All Tunnel Users, fix
1861971	Issues with access backend resources through Passthrough Proxy after upgrading to 25.1.1.0
Secure Access / PSAM	
1835947	PSAM issue persist in 22.7R211
1851546	Unable to Download DSRecord File From ICS When Username Contains the Characters "\" and "@"
Release 25.1.1.1	
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.	

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Summary
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.
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	
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.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Summary
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
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	

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Summary
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.
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.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

8. Known Issues

The following table lists the known issues in respective release:

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Release Note
Release 25.1.3.1	
1999102	**Symptom**: Client log upload fails on macOS when using the JSAM applet. **Condition**: The issue occurs when JSAM is launched on a macOS device. **Workaround**: Upload the client logs manually.
Release 25.1.3.0	
Upgrade and Deployment	
1775958	**Symptom**: Upgrading from a staged package may fail with the following error: "ICS Service Package does not support package version on this device". This error can occur even when an ICS 25.1.2.0 or later package has been successfully uploaded to the staging area. **Conditions**: • The ICS instance is running a version earlier than 25.1.2.0 on a virtual appliance. • An administrator stages an ICS 25.1.2.0 or later package successfully. • The administrator then attempts to perform the upgrade using the staged package. **Workaround**: None. Upgrades to ICS 25.1.2.0 or later are not supported on earlier than 25.1.2.0. Try direct upgrade to get the error immediately.
1970766	**Symptom**: Upgrade from ICS 25.1.3.0 build to any 25.x build fails but the messages on Admin UI says: ICS Package scan completed successfully. **Condition**: This issue occurs when the upgrade is attempted after running Ext ICT on ICS. **Workaround**: After running an Ext ICT, reboot ICS before attempting the ICS upgrade. The upgrade completes successfully after the reboot.
1870595	**Symptom**: During an upgrade, the image displayed on the web interface appears oversized and zoomed in, resulting in a pixelated and misaligned appearance on the page. **Condition**: Occurs while upgrading to Ivanti Connect Secure (ICS) version 25.1.3.0 (build or release). **Workaround**: NA
1939424	**Symptom**: When an ICS custom image is selected on the GCP instance creation page, the Provisioned IOPS value is initially displayed as 2000. **Condition**: This issue occurs while configuring the ICS instance in GCP, under the OS and Storage section, after selecting the custom ICS image. At this stage, the Provisioned IOPS value cannot be edited. **Workaround**: To set the correct Provisioned IOPS value: 1. In the **OS and Storage** section, select the required ICS custom image from the dropdown. 2. The **Provisioned IOPS** value is initially displayed as 2000. 3. Click **Select** to save the configuration. 4. Reopen the configuration by clicking **Change**.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Release Note
	5. The **Provisioned IOPS** value is now displayed as **3480**. 6. Click **Select** again to save the configuration with the updated **Provisioned IOPS** value of **3480**.
Clustering and High Availability	
1921438	**Symptom**: End users may be required to re-authenticate after the VIP Holding Node setting is enabled or disabled in an Active-Passive cluster configuration. **Condition**: This issue occurs when the VIP Holding Node option is enabled or disabled on an Active-Passive cluster. **Workaround**: Use of the VIP Holding Node option is not generally recommended. If it must be enabled or disabled, perform the operation during a planned maintenance window to minimize user disruption and potential re-authentication events.
1969044	**Symptom**: End users can connect to the VIP, but backend resources become inaccessible. This occurs because network packets are no longer tagged after one of the VLAN interfaces goes missing. **Condition**: This issue occurs when multiple VLAN interfaces are configured on a physical interface and VIP failover testing is performed by using the **Failover VIP** button and restarting services. During the failover process, a tentative IPv6 address may be observed intermittently. In some cases, one of the VLAN interfaces may be unexpectedly deleted or may no longer appear in the ifconfig output, resulting in loss of access to end-user resources. **Workaround**: Reboot the affected ICS device to restore the VLAN interface and recover connectivity.
1967862	**Symptom**: Backend resources are not accessible. **Condition**: This issue is seen under the following conditions: Source Port under Roles is set to use VLAN Virtual Port. Use /api/v1/cluster to change the cluster type from AA to AP. **Workaround**: Do Failover VIP so that the VLAN virtual ports get created properly on the other node.
1938819	**Symptom**: EUP login lands in blank page in cluster **Condition**: When logged in as an end user **Workaround**: Clicking on home icon will do
1938796	**Symptom**: SSH, RDP Remote file transfer, RDP print fail to work in cluster **Condition**: When tried in cluster **Workaround**: N/A
1949670	**Symptom**: Deleting a host entry at the cluster level displays the same host entry removal message twice. **Condition**: This issue occurs when a host entry is deleted in a clustered deployment. **Workaround**: NA.
1954185	**Symptom**: The UEBA package is not synchronized to one of the nodes in a cluster. **Condition**: This issue can occur when the UEBA package is uploaded to only one node in the cluster. **Workaround**: Manually upload the same UEBA package to the affected node in the cluster to ensure successful synchronization and availability across all nodes.
1770956	**Symptom**: Antivirus or Firewall remediation actions to enable Real-Time Protection (RTP) do not work.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Release Note
	Condition: This issue occurs when using agentless Host Checker (HC) on Windows endpoints. **Workaround**: NA
Configuration Management	
1933309	**Symptom**: The Push Config feature does not work when pushing configuration from an ICS 25.1.1.0 gateway to an ICS 25.1.3.0 gateway after HTTP/2 is enabled on the target 25.1.3.0 device. **Condition**: This issue occurs because the required HTTP/2 support and associated fix are available only in ICS 25.1.3.0. **Workaround**: Either of the following options can be used: • Upgrade the source gateway to ICS 25.1.3.0 before performing the Push Config operation. • Disable the HTTP/2 feature on the target ICS 25.1.3.0 gateway when the source gateway is running a release earlier than 25.1.3.0.
1925041	**Symptom**: Importing a user configuration fails when the configuration includes Web Proxy settings. **Condition**: Occurs when attempting to import a configuration containing Web Proxy configuration. **Workaround**: Use the XML configuration file to import the Web Proxy settings successfully.
1936818	**Symptom**: There is no option to push HTML5 storage configuration through the configuration push mechanism. **Condition**: This issue occurs when attempting to push HTML5 storage configuration. **Workaround**: Use XML import or user configuration import to transfer the HTML5 storage configuration.
Web Proxy	
1927755	**Symptom**: Web Proxy use cases configured through the REST API are not handled correctly. **Condition**: This issue occurs when Web Proxy configuration or management operations are performed using the REST API. **Workaround**: Use the Admin UI to configure and manage Web Proxy settings.
Monitoring and Logging	
1938472	**Symptom**: TLS Syslog forwarding fails when configured to use a custom port. **Condition**: This issue occurs when TLS Syslog is configured with a custom port instead of the default TLS Syslog port. **Workaround**: Configure TLS Syslog to use the default port. TLS Syslog forwarding works as expected when the default port is used.
1961487	**Symptom**: When an SNMP request is performed for Fan Status or Power Status on ISA6500 or ISA8500 hardware devices, the SNMP MIB browser displays the message"No such object". **Condition**: This issue occurs when querying the Fan Status or Power Status OIDs through an SNMP MIB browser on ISA6500 or ISA8500 hardware platforms. **Workaround**: N/A
Networking	

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Release Note
1951563	**Symptom**: Hostname resolution fails when a hostname is mapped to an IPv6 address. **Condition**: This issue occurs when the hostname contains uppercase letters or special characters. **Workaround**: Use only lowercase letters in the hostname. Hostname resolution works as expected.
1936692	**Symptom**: NFS mounts from the ICS shell may fail when the NFS server is located on a different network than the ICS internal interface. **Condition**: NFS server is reachable only through a different network path. **Workaround**: Add a route that allows the ICS management IP to reach the NFS share through the appropriate internal interface.
User Experience	
1935112	**Symptom**: The Home button displayed on HTML5 maximum connections warning page does not redirect users to the Home page. **Condition**: This issue occurs when users click the Home button on the maximum connections warning page. **Workaround**: Close the tab or use the Home icon
Security and Compliance	
1970177	**Symptom**: External ICT incorrectly detects the file /data/runtime/tt/report_behavioral_analytics_user.thtml.ttc as an anomaly. **Condition**: This issue occurs when Source IP/Location-based restrictions are enabled. **Workaround**: NA
Platform-Specific	
1966605	**Symptom**: The message "generate_grub2_config: failed to stamp SB diagnostic version for system A" is displayed on the console. **Condition**: This message may be observed during a fresh installation on the OpenStack KVM platform. **Workaround**: NA
JSAM	
1971454	**Symptom**: A warning message,"You don't have permission to change host files", is displayed when launching JSAM on Ubuntu.
1679016	**Symptom**: JSAM fails to launch on macOS when accessed through the Safari browser. **Condition**: The issue occurs when users attempt to launch JSAM using Safari on macOS. **Workaround**: Use Microsoft Edge or Google Chrome to launch JSAM.
Release 25.1.1.1	
1879013	**Symptom**: JSAM launch fails on MAC OS **Condition**: When JSAM is launched via all browsers. **Workaround**: There is no workaround

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Release Note
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.
1874029	**Symptom**: End users are prompted to enter secondary authentication every time, even though Adaptive Auth is enabled under Realms. **Condition**: In rare situations, the ICS code fails to establish a connection with the UEBA database, which is required for Adaptive Auth functionality. **Workaround**: Restarting the services resolves the issue.
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	
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.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Release Note
	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
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 & Authenticati	

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Release Note
on	
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.
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. **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..

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Release Note
	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".
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

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Release Note
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. **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	

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

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. **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.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Release Note
	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). **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

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Release Note
REST API	
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. **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.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Release Note
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	
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.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Release Note
1665464	**Symptom**: "IPv6 not enabled on any port" error message is displayed when using troubleshooting commands. **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
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.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

Problem Report Number	Release Note
	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. **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.

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.

9. 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

Copyright © 2026, Ivanti.Inc. All Rights Reserved. Privacy and Legal.