Ivanti Connect Secure Release Notes

25.1.0.0

Copyright Notice

Contents

Revision History

The following table lists the revision history for this document:

Document Revision	Date	Description
1.0	September 2025	First version for 25.1.0.0

What's New

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

- 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.
- 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.

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 and VMware.

- ISA6000
- ISA8000

The following table describes the tested upgrade paths, in addition to fresh installation of 25.x for ICS Product.

Upgrade to	Upgrade From (Supported Versions)
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 upgrades are not supported. 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

Migrate to	Migrate From (Supported Versions)
25.1.0.0	22.8R2, 22.7R2.8, and 22.7R2.7

Support and Compatibility

Hardware Platforms

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

- ISA6000
- ISA8000

Virtual Appliance Editions

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

Virtual appliance qualified in Platforms for 25.1.0.0

Fresh ICS Installation and upgrade is supported on VMware Platform and other platforms are not supported.

Variant	Platform	vCPU	RAM	Disk Space
VMware ESXi 8.0U3d ESXi 7.0.3 (23307199)	ISA4000-V	4	8 GB	80 GB
	ISA6000-V	8	16 GB	80 GB
	ISA8000-V	12	32 GB	80 GB

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

For more information see Support Platform Guide.

Known Issues

The following table lists the known issues in respective release:

Problem Report Number	Release Note
Release 25.1.0.0	
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.
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
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".
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
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.

Problem Report Number	Release Note
	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
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
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.
1616321	**Symptom**: Bandwidth management does not work. **Conditions**: Occurs when SSL is used. **Workaround**: Use ESP protocol instead of SSL.
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

Problem Report Number	Release Note
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
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.
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
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.
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.
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

Problem Report Number	Release Note
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
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
1634397	**Symptom**: Exception rule creation when using rest API failed. **Condition**: Occurs during attempts to create an exception rule via REST API. **Workaround**: None
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
1634677	**Symptom**: Default admin realm cannot be deleted. **Condition**: When admin tries to delete default admin realm from UI. **Workaround**: NA
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.

Problem Report Number	Release Note
	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.
1634850	**Symptom**: Bind failed related logs are seen for few seconds. **Condition**: During ICS upgrade. **Workaround**: NA
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.
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
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
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
1641211	**Symptom**: RDP print functionality is not working. **Condition**: Occurs when the print option is enabled in an RDP HTML5 bookmark.

Problem Report Number	Release Note
	Workaround: NA
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.
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.
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.
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
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.
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.

Problem Report Number	Release Note
	Workaround : Host Checker functions correctly; only the displayed version is "1.0".
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
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.
1648583	**Symptom**: Pushing config does not works using IPv6. **Workaround**: Use IPv4 for push config functionality to work.
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
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.
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.

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.
1637651	**Symptom**: Traceroute output displays %int0, %ext0, %mgt0. **Condition**: NA **Workaround**: NA
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.
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
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
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.
1657227	**Symptom**: 502 bad gateway message is seen. **Condition**: When user clicks "Profile" hyperlink in the HC page. **Workardound**: N/A
1665495	**Symptom**: WAF messages are seen in event logs. **Condition**: When accessing HTML5 bookmarks via REST API. **Workaround**: NA
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
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.
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.

Problem Report Number	Release Note
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.
1669912	**Symptom**: HTML5 storage config is not getting imported. **Condition**: Occurs when importing binary HTML5 config. **Workaround**: : Configure using the ICS Gateway UI.
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.
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
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.
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.
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.

Problem Report Number	Release Note
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.
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.
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.
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
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.
1641387	**Symptom**: Host Checker Policies are empty in the remediation > Enable Custom Actions field. **Condition**: In all conditions, it is empty. **Workaround**: NA

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