Ivanti Connect Secure Release Notes

22.8R2

Copyright Notice

Contents

Revision History

The following table lists the revision history for this document:

Document Revision	**Date**	**Description**
1.0	July 2025	First version for 22.8R2.

What's New

Version 22.8R2

Product Version	Build
ICS 22.8R2	14015
ISAC 22.8R2	33497
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 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

- Security hardening features are not supported on IPS.
- The checkbox under the option **Booting Options on Integrity Check Failure** at **System > Configuration > Security > Miscellaneous** becomes irrelevant. Boot time integrity checks performed by SecureBoot will stop the system booting if failure is detected.
- Enable **Prevent System Overload** to proactively protect your Connect Secure infrastructure from heavy load or resource spikes. This is a best practice for mission-critical or high-utilization VPN environments.

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

- Admin Access via External Interface is no longer supported in Ivanti Connect Secure (ICS) from Version 22.7R2.9, refer to article.
- Ivanti Connect Secure: Features and Options Becoming Unsupported or Deprecated in 22.7Rx, 22.8Rx, and 25.x, refer to article.
- Deprecation of TDI Fail-Over Option for Pulse SAM Connection, refer to article.
- ICS running version 22.8R2 cannot be configured as a License Server, see Known Issues. However, a License Server running version 22.7Rx can still provide licenses to an ICS 22.8R2 instance acting as a license client.

Upgrade

Upgrade Path

Upgrade Installation is supported only on the following ISA Hardware Platforms.

- ISA6000
- ISA8000

The following table describes the tested upgrade paths, in addition to fresh installation of 22.x for ICS Product.

Upgrade to	Upgrade From (Supported Versions)
22.8R2	22.7R2.8 and 22.7R2.7

Note:

- 22.7R2.9 users must upgrade to future versions of 22.8Rx, but not to the current 22.8R2 version for feature parity with ICS 22.7R2.9.
- 22.8R2 is a SecureBoot enabled ICS version. Once migrated, the VM and Hardware appliances cannot be rolled back to non-SecureBoot ICS versions (22.7x).
- This appliance will also lose dual-personality functionality and cannot be re-purposed for IPS.
- Upgrade to ICS version 22.8R2 is supported only for Hardware appliance. Refer to Upgrade section for upgrade path from ICS 22.7x.
- ICS virtual appliances require fresh installation.
- 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.

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 22.8R2

Only Fresh ICS Installation is supported on VMware Platform and other virtual/cloud platforms are not supported in this Release.

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.

Licensing Types

License Type	Gateway Licensing Mode
Feature licenses (Adv HTML5 etc)	Install license locally. ⓘ ICS running version 22.8R2 cannot be configured as a License Server, see Known Issues. However, a License Server running version 22.7Rx can still provide licenses to an ICS 22.8R2 instance acting as a license client.

For more information see the Licensing Management Guide

Known Issues

The following table lists the known issues in respective release:

Problem Report Number	Release Note
Release 22.8R2	
1590662	**Symptom**: Enabling “Validate Server Certificate” for LDAP connections does not enforce or properly handle certificate validation. **Conditio**n: Occurs when the “Validate Server Certificate” option is used in LDAP configuration. **Workaround**: N/A
1562767	**Symptom**: Users are unable to change their AD passwords via the preference page. **Condition**: This occurs during password change attempts from enduser page. **Workaround**: N/A
1561276	**Symptom**: The certificate authentication end-user page becomes inaccessible after enabling the "Advanced Certificate Processing Settings" option under trusted client CA configuration. **Condition**: This 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".
1558753	**Symptom**: AAA traffic segregation is not working as expected at both the global and server levels. Authentication attempts to AD or OAuth servers do not use the configured segregated port, resulting in all AAA traffic being sent via the internal port. **Condition**: Occurs when segregation policies are set globally or per-auth server, but the system continues to use default paths for all authentication traffic. The issue is observed on both AD and OAuth authentication flows in the current platform version. **Workaround**: N/A
1624414	**Symptom**: ICS is not sending logs to remote syslog server **Conditions**: When ICS is configured to send logs to remote TLS syslog server **Workaround**: Use TCP syslog server, if possible.

Problem Report Number	Release Note
1628538	**Symptom**: SharePoint bookmark access throws"The page you requested could not be found." message. **Workaround**: N/A
1624127	**Symptoms**: On the AD troubleshooting page, DNS resolution checks fail if multiple AD servers are configure. DNS resolution is success for the AD which is configured as a DNS server. **Condition**: Configuring multiple AD servers on the ICS, Some of the AD severs DNS resolution may fail in trouble shooting page. **Workaround**: Configure the AD server IP as a primary DNS.
1622322	**Symptoms**: OAuth time skew is not working as per the configured values. **Workaround**: N/A
1624093	**Symptoms**: When configure an LDAP server, it fails with the error "Invalid server address," **Condition**: when configuring an LDAP server. **Workaround**: N/A
1607526	**Symptom**: Admin UI is not accessible. **Condition**: When configured V6 address is wrong. **Workaround**: Disable Next Gen Web Server from console, access the admin page and correct the IP address. Then enable Next Gen Web Server again from console.
1611707	**Symptom**: WAF package version is missing in the admin log. **Condition**: When rollback is done for WAF package. **Workaround**: N/A
1611987	**Symptom**: Debug log download is not working. **Condition**: When Next Gen Web Server is disabled. **Workaround**: Turn off the 'debug logging on' and 'include logs' fields, 'save' and then download the logs.
1628212	**Symptoms**: Cloud secure configuration fails with the error message: "Failed, no metadata". **Condition**: This occurs when configuring the Office 365 application in Cloud Secure. **Workaround**:

Problem Report Number	Release Note
	1. Download the Microsoft Office 365 (Azure AD) SAML metadata XML directly from Microsoft. 2. Save the file to your local machine. 3. In the **Cloud Secure** admin portal, choose to manually import SAML metadata, and upload the file you downloaded.
1627526	**Symptom**: Android ISAC client connection to ICS gateway fails with 'Server's security certificate is not trusted'. **Conditions**: ICS is running 22.8R2. **Workaround**: Disable **Server certificate trust enforcement** option under **System > Configuration > Mobile**.
1626143	**Symptom**: Creation of delegated admin role fails. **Conditions**: When trying to create a delegated admin role via Rest API. **Workaround**: Add the rule IDs 920170, 930120 in WAF exclude rule ID list, and then execute the REST API.
1626107	**Symptom**: Restore of binary config via /api/v1//system/binary-configuration REST API fails. **Condition**: When the REST API is executed against ICS running 22.8R2 and later. **Workaround**: Use Admin UI to backup and restore binary config.
1626479	**Symptom**: One of the node in the cluster is not accessible after doing restart services **Condition**: After restarting services **Workaround**: Restart the Services or reboot the node with the issue.
1624778	**Symptom**: Sometimes 502 bad gateway message is seen. **Condition**: When File browsing bookmark is accessed. **Workaround**: Trying accessing second time, it will work.
1617191	**Symptom**: After creating the AD server in an Active/Passive (A/P) cluster, the AD username and password fields are empty, even though the 'Save Credentials' setting is enabled. **Condition**: The appliance is running with 22.8R2 version and the device is configured in an Active/Passive (A/P) cluster mode with 'Save Credentials' option enabled on the AD authentication server.

Problem Report Number	Release Note
	Workaround: On each login, manually enter the AD credentials (since autofill/save is not working).
1601479	**Symptom**: Configuring FQDN based lockdown exception rule for a connection set failing through Rest API. **Condition**: While configuring FQDN based lockdown exception rule for a connection set through Rest API. **Workaround**: Configuring the FQDN based lockdown exception manually in ICS.
1601128	**Symptom**: ISAC Connection using IPv6 is disconnecting when custom UDP port **Condition**: When custom IPv6 UDP port is configured **Workaround**: None
1621990	**Symptom**: System/User Binary import/XML import is failing with 22.8R2 gateway registered to the latest NSA controller. **Workaround**: System/User binary/XML import to be done from Gateway UI.
1600324	**Symptom**: ISAC client Disconnection is taking more time. **Condition**: When SLO is enabled. **Workaround**: Disable SLO.
1600229	**Symptom**: `/bin/cp cannot create regular file` message is seen on console. **Condition**: Reboot. **Workaround**: None. Error message is harmless. It can be ignored.
1600243	**Symptom**: L3 Tunnel fails to connect using NCP for mobile clients (Android and iOS). **Condition**: When NCP is chosen as Communication Protocol. **Workaround**: Select IFT/TLS as the Communication Protocol instead of NCP.
1621721	**Symptom**: HTML5 copy paste will not work. **Condition**: On MAC when user use Command C/V operations. **Workaround**: Select the required content & do right click and Copy. Paste the content in the local machine.
1590178	**Symptom**: Importing xml file with archival config settings is returning with password related error message.

Problem Report Number	Release Note
	Workaround: If the exported XML is of 22.8R2.x or higher version, then the Proper strength password (as defined in default Authentication Server) for the following archival configs should be provided before import: • System configuration • User accounts • Administrative Network Configuration • Archive XML configuration
1618213	**Symptom**: JSAM bookmark access will not work when JRE 1.8 is installed. **Condition**: When enduser accesses JSAM profiles with JRE 1.8. **Workaround**: Install JDK instead of JRE1.8 .
1600813	**Symptom**: Unable to lease licenses from license server. **Conditions**: 22.8R2 license client is configured to lease license from license server running 22.8R2 **Workaround**: Use a license server running 22.7R2.x latest version.
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**: This 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.
1610000	**Symptom**: ISAC connection not disconnecting immediately after SESSION_TIMEOUT **Condition**: Configure SESSION_TIMEOUT from session options as 6 min which is minimum value **Workaround**: None
1609890	**Symptom**: Switch to serial console on VM doesn't bring up Admin/End user UI. **Condition**: If serial port is not attached to VM and convert Virtual Terminal to serial console. **Workaround**: Attach serial port to VM to access UI.

Problem Report Number	Release Note
1570129	**Symptom**: System boots up slow compared to previous version. **Condition**: Reboot. **Workaround**: None available.
1611701	**Symptom**: WAF package version is missing in the admin log. **Condition**: When WAF package is uploaded. **Workaround**: N/A
1617997	**Symptoms**: User login is successful even if we disable client Certificate Negotiation. **Condition**: When we disable "Trusted for Client Authentication" and "Participate in Client" on the trusted client CA. **Workaround**: Delete the client CA certificate which we want to disable the participate in client certificate negotiation from the ICS.
1590685	**Symptom**: During upgrade bind failed related logs seen for few seconds. **Condition**: Upgrade, Enable/Disable Next Generation Webserver. **Workaround**: NA
1562419	**Symptom**: Unable to attach vTPM if vTPM is detached manually. **Condition**: If vTPM is detached and want to re-attach then VMware VCD does not provide option to re-attach vTPM. **Workaround**: None. Removing vTPM makes vICS non recoverable. vTPM is mandatory component.
1506788	**Symptom**: Upload successful message is not populated **Condition**: When WAF ruleset package is uploaded. **Workaround**: Refer the admin logs.
1499053	**Symptom**: WAF functionality will not work. **Condition**: When admin enables Next Gen Web Server from console options. **Workaround**: From ICS admin UI disable and enable the WAF, then WAF functionality will work.
1449031	**Symptom** : When admin tries to delete more than 198 users, WAF is blocking it. **Condition**: Deletion of more than 198 users. **Workaround**: Delete 150 users at one time.

Problem Report Number	Release Note
1614488	**Symptom**: 22.8R2 can be staged on a VMware appliance running on 22.7Rx but upgrade fails. **Condition**: On VMware, 22.8R2 may be staged from 22.7Rx but upgrade cannot process as upgrade from 22.7Rx to 22.8R2 is not allowed on VMware. **Workaround**: Use direct upgrade instead of Staged Upgrade..
1600939	**Symptom**: When trying to create or update an Admin Realm through REST API, ICS returns “Unknown Element” error. **Conditions**: When the json input in the post body contains “allow-admin-signin-external-port”. **Workaround**: Remove “allow-admin-signin-external-port” attribute. It is no longer supported in ICS 22.8R2 and later releases.
1621181	**Symptom**: Upgrade aborts with error “ADM23397: This appliance cannot be upgraded to 22.8R2.” **Workaround**: No workaround. This indicates that the upgrade cannot proceed because there is insufficient disk space in the boot partition because the factory reset version is very old. Contact Ivanti Support for error.

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