Ivanti Connect Secure Release Notes

22.8R2.2

Copyright Notice

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as “Ivanti”) and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.Ivanti.com.

Protected by patents, see https://www.ivanti.com/patents.

Contents

Revision History

The following table lists the revision history for this document:

Document Revision	Date	Description
3.0	January 2026	Updated What's new, Noteworthy Info, and Resolved issue for 22.8R2.2.
2.0	November 2025	Updated What's new, Noteworthy Info, and Resolved issue for 22.8R2.1.
1.0	July 2025	First version for 22.8R2.

What's New

Version 22.8R2.2

Product Version	Build
ICS 22.8R2.2	18481
ISAC 22.8R5	41063
Default ESAP	4.6.4

New Features

- This release includes resolved issues from 22.8R2.2 and features from 22.7R2.11.

Version 22.8R2.1

Product Version	Build
ICS 22.8R2.1	16479
ISAC 22.8R4	38767
Default ESAP	4.3.8

New Features

This release includes resolved issues from 22.8R2 and features from 22.7R2.10. There are no new ICS features in this release.

Version 22.8R2

Product Version	Build
ICS 22.8R2	14015
ISAC 22.8R2	33497
Default ESAP	4.3.8

New Features

- **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

22.8R2.2

- **Secondary SessionID verification enforcement for Secure VPN Authentication**: Secondary SessionID verification enforcement ensures ICS server to strictly validate HTTP Only Device Cookie on all L3 and L4 workflows. This provides an additional layer of session validation, enhancing overall security, see Configuring Miscellaneous Security Options.
- Feature parity with ICS release 22.7R2.11
- The Next Web Server 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.
- The Classic UI of Ivanti Secure Access Client (ISAC) will be deprecated in the Q3 release (July 2026) of Ivanti Secure Access Client for both Desktop and Mobile. The option to switch between Classic and New UI will be removed both from ISAC user-interface and ICS admin UI. Ivanti recommends customers to migrate to New UI of Ivanti Secure Access for better user experience and enhanced security. For more details, see forum link.

22.8R2.1

- Feature parity with ICS release 22.7R2.10 and 22.7R2.9.
- After a node joins the cluster, it may take up to 60 seconds for the correct VIP owner to be reflected. This delay ensures accuracy in cluster state reporting.
- The External ICT package introduced with the ICS 22.8R2.1 release is not compatible with previous versions of ICS, due to changes made for SELinux inclusion. New releases after 22.8R2.1 will remain compatible with 22.8R2.1, but cannot be used with older ICS versions. For more info refer KB.
- The option to disable Web Application Firewall (WAF) and the Next Generation Web Server (Nginx) has been removed. WAF will now run continuously on ICS, ensuring protection. For more info refer KB.

- Upgrading from 22.8R2 to 22.8R2.1 on hardware appliances ensures that the factory reset partition is updated along with the active partition. For more information, see KB.

- A secure-by-default configuration change is introduced to enable the host header validations on fresh deployment/upgrade in this release. To ensure successful hostname-based requests, administrators must provision certificates with appropriate Subject Alternative Name (SAN) entries matching all intended host header values.

- This release includes important security enhancements as part of our ongoing commitment to secure-by-design. Ivanti encourages customers to upgrade to this latest version.

- Added validation checks to verify the file-type in `/api/v1/system/maintenance/upgrade`, when passing the file to the API. Modify your scripts to include the file-type as ‘`application/octet-stream`’.

Code snippet for python provided by Postman App.

```
import requests

url = "https://<ICS-IP>/api/v1/system/maintenance/upgrade"

payload = {}
files=[
  ('file',('package.pkg',open
('/C:/Users/qa1/Downloads/<package.pkg>','rb'),'application/octet-stream'))
]
headers = {
  'Authorization': '••••••'
}

response = requests.request("POST", url, headers=headers, data=payload, files=files)

print(response.text)
```

22.8R2

- 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.

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.

Caveats

- Active Directory (AD) 2025 and above will not be supported on 22.8R2 releases due to incompatibility issues with Samba versions. For AD 2025 support, upgrading to release 25.x is required.

Upgrade and Migration

Upgrade Path

Upgrade Installation is supported only on the following platforms.

- ISA6000
- ISA8000
- VMware

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)
22.8R2.2	22.8R2.1 (VM, Hardware), 22.8R2 (VM, Hardware), 22.7R2.11 (Hardware) and 22.7R2.10 (Hardware)
22.8R2.1	22.8R2 (VM, Hardware), 22.7R2.9 (Hardware) and 22.7R2.10 (Hardware)
22.8R2	22.7R2.8 and 22.7R2.7 (Only Hardware)

Note:

- 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 22.8R2.2 is supported with both Hardware and virtual platforms.
  - The Factory Reset version for Hardware will change to 22.8R2.2 post upgrading to 22.8R2.2.
- 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.

Migrate to	Migrate From (Supported Versions)
22.8R2.2	22.8R2.1, 22.8R2, 22.7R2.11, and 22.7R2.10
22.8R2.1	22.8R2, 22.7R2.9, and 22.7R2.10
22.8R2	22.7R2.8, 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 22.8R2.2

Only VMware Platform is supported and other virtual/cloud platforms are not supported in this release.

Variant	Platform	vCPU	RAM	Disk Space
VMware ESXi 8.0U3d	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.

Resolved Issues

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

Problem Report Number	Summary
Release 22.8R2.2	
This release also includes the applicable resolved issues from version 22.7R2.11.	
Access & Connectivity	
1699625	Applications configured with non-standard TCP ports are not accessible through the PSAM tunnel when the Nginx Web Server is enabled in version 22.8R2.
1708733	Web bookmarks are not functioning on ICS 22.8R2, caused by issues with JSESSION ID passthrough rewrite.
1716243	Users are experiencing unexpected disconnections after upgrading to version 22.7R2.10.
1701632	Users are unable to access specific resources through PSAM after upgrading ICS to version 22.8R2.
Web Server & Performance	
1697005	Nginx crashes frequently observed on ICS 22.8R2, affecting web access features.
Authentication & Security	
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.
1720853	TOTP user reset functionality does not work when WAF is enabled in Protection Mode.
HTML5	
1621721	HTML5 copy paste will not work.
1733551	Advanced HTML5 sessions remain active even after the end user logs out.

Problem Report Number	Summary
1384221	Advanced HTML5 SSH session fails to log in when using a private key.
End User Portal	
1708517	A black screen is displayed when accessing a file share bookmark created by the end user.
Web Application Firewall (WAF)	
1711109	The WAF package reverts to version 1.0.0.
1709370	XML import/push config fails with the error message: "Can't download crs package '1.0.0' from controller as gateway is not registered with controller."
1712905	WAF issues are observed in the following configurations: • Manually configured CDP in Sub CA for CRL checking. • Backup CDP configured in Root CA. • CRL checking options set to use CDP specified in the trusted CA.
Cluster Management	
1703177	Event logs display the message "administrator manual failover" when VIP failover occurs due to the active node rebooting.
Release 22.8R2.1	
Authentication (AD/LDAP)	
1624093	When configure an LDAP server, it fails with the error "Invalid server address".
1562767	Users are unable to change their AD passwords via the preference page.
1617191	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.
1622322	OAuth time skew is not working as per the configured values.
VPN/Resource Access	
1693993	VPN ACL configuration push fails with the error message: "Invalid IPv4 address specified."

Problem Report Number	Summary
1688316	Users are unable to access the URL https://compliance.login.globalrelay.com/ using a web bookmark and encounter a JavaScript error.
1687912	Attempting to access SharePoint results in the error message: "The page you requested could not be found."
Webserver	
1600885	The Nextgen Webserver service crashes while performing DFS operations.
1696296	The Nextgen Webserver crashes frequently observed on systems running version 22.8R2.
1611547	"Program nginx recently failed." is observed when uploading a file of 800 MB.
1658196	Program Nextgen Webserver recently failed after upgrading to 22.8R2.
Certificates	
1617997	User login is successful even if we disable client Certificate Negotiation.
1628212	Cloud secure configuration fails with the error message: "Failed, no metadata".
1641444	The Android ISAC client fails to connect to DFS and displays the error message "Server's security certificate is not trusted." when the next generation server is enabled.
1666634	The PSAL client displays the error "Detected Incorrect Data From Server because ICS is not sending the SrvCertMd5 value.
UI/Platform	
1641921	Some UI pages are inaccessible after upgrading the ISA8K.
1609890	Switch to serial console on VM does not bring up Admin/End user UI.
Web Application Firewall (WAF)	
1611707 1611701	WAF package version is missing in the admin log.

Known Issues

The following table lists the known issues in respective release:

Problem Report Number	Release Note
Release 22.8R2.2	
Web Application Firewall (WAF) & Configuration	
1449031	**Symptom** : When admin tries to delete more than 600 users, WAF is blocking it. **Condition**: Deletion of more than 600 users. **Workaround**: Delete 600 users at one time.
Cluster Management & Upgrade	
1503708	**Symptom**: Upgrade of a lower version node fails during the "Verifying Package Integrity" step. **Condition**: This issue occurs in the following scenario: 1. Create a cluster on pre-22.8R2 version. 2. Upgrade to 22.8R2. 3. Remove the cluster in 22.8R2. 4. Roll back node-1 and upgrade again to 22.8R2. 5. After the upgrade of node-1 is successful, roll back node-2. 6. When node-2 is coming up, it joins the cluster and attempts to upgrade to 22.8R2, at which point the error occurs. **Workaround**: Boot the device in standalone mode and then perform the upgrade.
Authentication	
1753244	**Symptom**: The TOTP fallback server fails to function when used in conjunction with an LDAP authentication server. **Condition**: This issue occurs when configuring TOTP as a fallback for LDAP based authentication. **Workaround**: N/A
End User Experience & Access	
1700995	**Symptom**: When using the Safari browser, PSAL is not detected and the end user is prompted to download and install PSAL. **Condition**: This issue occurs when attempting to log in via the Safari browser.

Problem Report Number	Release Note
	Workaround: Use Chrome instead of Safari for successful detection and login with PSAL.
1739513	**Symptom**: Web VDI bookmark access occasionally does not work. **Condition**: This issue occurs when two Web VDI bookmarks are configured. **Workaround**: Configure only one VDI bookmark and use it for access.
1751812	**Symptom**: PSAL is unable to launch Java applet (JSAM) on MAC machines. **Condition**: This issue occurs when an end user accesses a JSAM bookmark on a MAC device. **Workaround**: Disable the **HTTP Only Device Cookie** option under User **Roles > Users > General > Session Options**. After disabling this setting, PSAL will be able to launch the JSAM applet.
1758504	**Symptom**: SAM internal resources are not passed through the configured proxy server. **Condition**: This issue occurs when a PSAM proxy is configured with SAM resource policies. **Workaround**: NA
Release 22.8R2.1	
HA/Cluster	
1703177	**Symptom**: Event logs display the message "administrator manual failover" when VIP failover occurs due to the active node rebooting. **Condition**: This happens when the active node (holding the cluster VIP) undergoes a reboot. **Workaround**: When this message appears, check the Admin logs to determine if the reboot was initiated by an administrator. Look for entries such as "Server Reboot requested by Admin/Administrators" to verify the source of the reboot.
1708187	**Symptom**: In an Active-Passive cluster configured with virtual ports on VLANs, backend resources within a VLAN become inaccessible following a cluster VIP failover. **Conditions**: This issue is observed under the following circumstances: • The user role is configured with Source IP set to the VLAN virtual port.

Problem Report Number	Release Note
	- VIP failover from the active to passive node is triggered by ICS code due to events such as gateway not reachable, system reboot, or an admin-initiated VIP failover. **Workaround**: Reboot the entire cluster to restore access to backend resources.
End User Portal	
1697623	**Symptom**: The browser bar in the End User Portal (EUP) displays "URL is invalid." **Condition**: This occurs when the "Mask hostnames while browsing" option is enabled. **Workaround**: Disable "Mask hostnames while browsing" and use the browser bar.
1708517	**Symptom**: A black screen is displayed when accessing a file share bookmark created by the end user. **Condition**: This occurs when the bookmark is created through the file browse option. **Workaround**: - End user can access admin created bookmark & bookmark the required path to access. - Attempt to access the required file share path directly from the file browse option.
1710328	**Symptom**: End user receives the error message: "Invalid username or password. Please re-enter your user information" when attempting to log in to ICS. **Conditions**: This error occurs when: - The end user already has an active session with ICS. - The end user tries to log in again from another device or browser. **Workaround**: Close any existing sessions and log in again.
Authentication	
1708860	**Symptom**: End-users occasionally receive the error message "Unable to perform TOTP auth." **Conditions**:

Problem Report Number	Release Note
	• When user realm is configured with Remote TOTP as the secondary authentication method. • When error typically occurs when multiple users attempt to login simultaneously. **Workaround**: Enable Adaptive Authentication, if possible. This will reduce the frequency of secondary authentication requests and help prevent the error.
1698364	**Symptom**: Active Directory authentication may offer or advertise vulnerable ciphers during SSL/TLS negotiation. **Condition**: This occurs when an enduser authenticates with Active Directory. **Workaround**: N/A
RDP/ File Transfer	
1696607	**Symptom**: HTML5 RDP connection is terminated unexpectedly. **Condition**: This occurs when an end user attempts to send or receive files larger than 1 GB using the remote file transfer feature. **Workaround**: N/A.
Web Application Firewall (WAF)/Config Import	
1711109	**Symptom**: The WAF package reverts to version 1.0.0. **Condition**: This occurs when the admin performs an Entire Push Config or System.cfg import from 22.8R2 GA. **Workaround**: • Perform a WAF reset; the package will be restored to the default version 1.0.3. • If any exclude rule IDs are configured, the admin must reconfigure those rule IDs after the reset.
1709370	**Symptom**: XML import/push config fails with the error message: "Can't download crs package '1.0.0' from controller as gateway is not registered with controller." **Condition**: This occurs when the admin performs a selective push config/XML import that includes WAF configuration. **Workaround**: Admin can use system configuration (cfg) upload as an alternative.

Problem Report Number	Release Note
1712905	**Symptom**: WAF issues are observed in the following configurations: • Manually configured CDP in Sub CA for CRL checking. • Backup CDP configured in Root CA. • CRL checking options set to use CDP specified in the trusted CA. **Condition**: This issue occurs when an IP address is used in the CRL URL during CRL checking configuration. **Workaround**: Use a domain name in the CRL URL instead of an IP address.
System Upgrade / Cache	
1688577	**Symptom**: Event logs display the following message: "Error encountered while upgrading cache (Key: vc0/federateClientSettings/serverURL, Value: Created: 1)" **Condition**: This occurs during the upgrade process. **Workaround**: N/A
TLS/Certificates	
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.
PSAM	
1699625	**Symptom**: Backend resources are not accessible through the PSAM tunnel when non-standard TCP ports are used. **Condition**: This occurs when applications are configured with non-standard TCP ports in PSAM. **Workaround**: NA
Release 22.8R2	
Authentication (AD / LDAP / OAuth / Certificates)	

Problem Report Number	Release Note
LDAP	
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 used in LDAP configuration. **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
Active Directory (AD)	
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
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.
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. **Workaround**: On each login, manually enter the AD credentials (since autofill/save is not working).
Traffic Routing	

Problem Report Number	Release Note
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
OAuth	
1622322	**Symptoms**: OAuth time skew is not working as per the configured values. **Workaround**: N/A
Certificates	
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".
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.
Role/Access Control (Admin/User/Delegated)	
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.
Web Application Firewall (WAF)	
1611707	**Symptom**: WAF package version is missing in the admin log.

Problem Report Number	Release Note
	Condition: When rollback is done for WAF package. **Workaround**: N/A
1611701	**Symptom**: WAF package version is missing in the admin log. **Condition**: When WAF package is uploaded. **Workaround**: N/A
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.
1624455	**Symptom**: When attempting to push either selected or entire configuration to multiple targets in a single push job, the operation fails if the targets are configured with different Shared Secret Keys. **Condition**: This issue occurs when multiple targets have different Shared Secret Keys configured and a single push job is used to deploy configurations to these targets (either selected or entire configuration). **Workaround**: To successfully push configurations to multiple targets in one push job, ensure that all selected targets are configured with the same Shared Secret Key.
Clustering / High Availability	
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.
REST API	
1626107	**Symptom**: Restore of binary config via /api/v1//system/binary-configuration REST API fails.

Problem Report Number	Release Note
	Condition: When the REST API is executed against ICS running 22.8R2 and later. **Workaround**: Use Admin UI to backup and restore binary config.
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.
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.
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.
Admin UI / Console / Web Server	
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.
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.
Cloud Secure Config	

Problem Report Number	Release Note
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**: 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.
ISAC/Mobile Client / VPN Issues	
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.
1601128	**Symptom**: ISAC Connection using IPv6 is disconnecting when custom UDP port **Condition**: When custom IPv6 UDP port is configured **Workaround**: None
1600324	**Symptom**: ISAC client Disconnection is taking more time. **Condition**: When SLO is enabled. **Workaround**: Disable SLO.
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
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**.
Bookmark / File Browsing / Portal/End User UI	

Problem Report Number	Release Note
1628538	**Symptom**: SharePoint bookmark access throws"The page you requested could not be found." message. **Workaround**: N/A
1624778	**Symptom**: Sometimes 502 bad gateway message is seen. **Condition**: When File browsing bookmark is accessed. **Workaround**: Trying accessing second time, it will work.
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 .
License and Export/Import Issues	
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.
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.
1590178	**Symptom**: Importing xml file with archival config settings is returning with password related error message. **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
vTPM / VM / VMware	
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.

Problem Report Number	Release Note
	Workaround: None. Removing vTPM makes vICS non recoverable. vTPM is mandatory component.
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.
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. **Workaround**: None. Upgrade from 22.7Rx to 22.8R2 is not allowed.
Miscellaneous / System	
1570129	**Symptom**: System boots up slow compared to previous version. **Condition**: Reboot. **Workaround**: None available.
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.
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.
Upgrade	
1590685	**Symptom**: During upgrade bind failed related logs seen for few seconds. **Condition**: Upgrade, Enable/Disable Next Generation Webserver. **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