



Ivanti Secure Access Client Release Notes

22.8R1 Build 31437

22.7R4 Build 30859

22.7R3 Build 30227

22.7R2 Build 28777

22.7R1.1 Build 29163

22.7R1 Build 28369

22.6R1.2 Build 27593

22.6R1 Build 26825

22.5R1.1 Build 26249

22.5R1 Build 25375

22.3R3.1 Build 20175

22.3R3 Build 19959

22.3R2 Build 19787

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.

Copyright © 2025, Ivanti, Inc. All rights reserved.

Protected by patents, see <https://www.Ivanti.com/patents>.

Contents

Copyright Notice	2
Revision History	5
What's New	6
Overview	12
Noteworthy Information	12
Security Advisory and Patch Update	15
Upgrade Instructions	16
Upgrade Paths	16
Installer List on Ivanti Connect Secure	16
Support and Product Compatibility	17
Resolved Issues	18
Release 22.8R1	18
Release 22.7R4	18
Release 22.7R3	19
Release 22.7R2	20
Release 22.7R1	21
Release 22.6R1	22
Release 22.5R1	23
Release 22.3R3	24
Release 22.3R2	24
Release 22.3R1	26
Release 22.2R1	27
Known Issues	30
Release 22.8R1	30
Release 22.7R4	30
Release 22.7R3	30
Release 22.7R2	31
Release 22.7R1	31
Release 22.6R1	32
Release 22.5R1	33
Release 22.3R3	34
Release 22.3R2	34
Release 22.3R1	35
Release 22.2R1	37
Product Codes (GUIDs) for SCCM Deployments	43
Release 22.8R1	43
Release 22.7R4	43
Release 22.7R3	44
Release 22.7R2	44
Release 22.7R1	45
Release 22.6R1	45
Release 22.5R1	46

Release 22.3R3	47
Release 22.3R2	48
Release 22.3R1	49
Release 22.2R1	50
Documentation	52
Technical Support	52

Revision History

The following table lists changes made to this document:

Date	Revision
February 2025	Updated What's New , Known issues , and Resolved issues as applicable to 22.8R1.
January 2025	Added a Known issue 1481530.
October 2024	Updated for Windows 24H2 qualification, What's New , Known issues , and Resolved issues as applicable to 22.7R4.
September 2024	Updated for macOS 15 qualification.
July 2024	Updated What's New , Known issues , and Resolved issues as applicable to 22.7R3.
May 2024	Updated What's New , Known issues , and Resolved issues as applicable to 22.7R2.
January 2024	Updated What's New , Known issues , and Resolved issues as applicable to 22.7R1.
October 2023	Updated What's New , Known issues , and Resolved issues as applicable to 22.6R1.
July 2023	Updated What's New , Known issues , and Resolved issues as applicable to 22.5R1.
June 2023	Updated What's New , Known issues , and Resolved issues as applicable to 22.3R3.
May 2023	Updated What's New , Known issues , and Resolved issues as applicable to 22.3R2.
January 2023	Updated What's New , Known issues , and Resolved issues as applicable to 22.3R1.
July 2022	22.2R1; Initial release as Ivanti Secure Access Client; Previously Pulse Secure Client.

What's New

Release 22.8R1

Build: 31437

- **Silent deep clean script:** For Windows endpoint, Ivanti Secure Access Client now supports to run deep clean script silently in the background and avoid any user intervention during the process. For script and more information, see [Deep Clean Script for ISAC Management](#).

Release 22.7R4

Build: 30859

- **Single Stack IPV6 connection:** Ivanti Secure Access Client now supports Single Stack IPv6 tunnel connections. It supports connecting to an ICS configured with a Single Stack IPv6 tunnel Connection Profile for ISAC 22.7.4 Windows endpoints only.
- **Search device DNS only for IPv6:** When the Search device DNS only option is selected, DNS on the end user's system is replaced with device DNS. This option is recommended to avoid ISP's DNS hijacking. This feature was previously supported for IPv4, now it is enhanced to IPv6 Windows endpoints only.
- **Bypass client proxy settings:** This feature allows the administrator to bypass the client proxy settings in certain conditions using Advanced client configuration.
- **FQDN Support for Lockdown Exceptions:** This feature allows admins to block or allows FQDN hostnames based lockdown exception. This feature is supported on macOS and for IPv4 resources only. This feature is already available on Windows.
- **Support for Windows 11 24H2:** Ivanti Secure Access Client is now supported with Windows 11 24H2.
- **Support for macOS15 sequoia:** Ivanti Secure Access Client is now supported with macOS15 sequoia.
- **Support for RHEL 9:** Ivanti Secure Access Client is now supported with RHEL 9.

Release 22.7R3

Build: 30227

- **Support for macOS15 sequoia:** Ivanti Secure Access Client is now supported with macOS15 sequoia.
- **FQDN Support for Lockdown Exceptions:** This feature allows admins to block or allows FQDN hostnames based lockdown exception. This feature is supported on Windows and for IPv4 resources only.
- **Support on Windows Server version 2022:** Ivanti Secure Access Client now supports Windows Server version 2022.
- **Support for M3 chip based macOS:** Ivanti Secure Access Client is now supported on M3 chip based macOS.

Release 22.7R2

Build: 29103

- **Embedded browser DNS resolution when TTL is minimal:** For macOS, this feature ensures that embedded browser and client application gets same IP for the gateway and communicate FQDN to same gateway server.To enable this feature, on installing the , run the following command:
`defaults write net.pulsesecure.Pulse-Secure.plist EnableGWDnsCacheResponse-bool true.`
- **FQDN Split Tunneling with Traffic Enforcement:** This feature enables strict enforcement of traffic routes using FQDN split-tunneling rules configured in the Ivanti Connect Secure.
- **Split DNS parity for nZTA gateways:** On windows, this feature enables the DNS requests corresponding to a specific list of domains, sent to specific list of DNS servers through the corresponding virtual adapters.Ensure that the ZTA gateway DNS server do not conflict with DNS servers of the virtual or physical adapter.
- **Display last login details:** ISAC now displays the details of the last successful login. Under the Advanced Details tab in Connection Details, you can find the following three values related to the Last Login:
 - Last Login Time (Time and Date)
 - Last Login Device (hostname/FQDN) This field is not available for browser login
 - Last Login Agent Type (OS details)

- **Default enabling of DNS caching:** On windows, this feature enables DNS caching of VPN Gateway FQDN for SAML based embedded browser by default. For more information, refer Admin Guide.

Release 22.7R1.1

Build: 29163

No new features introduced in this release.

Release 22.7R1

Build: 28369

- **Select Session Command:** The CLI provides an option to connect or cancel new sessions.
CLI format: `pulselauncher.exe -sessionselection <connect|cancel> -url <url_of_server> -u<username> -p <password> -r <realm>`
 - `sessionselection connect:` Terminates the previous session and establishes a new session. When the maximum concurrent sessions are reached, the first session in the existing sessions will be terminated.
 - `sessionselection cancel :` Maintains the previous session without establishing a new session. It is equivalent to not utilizing the `sessionselection` parameter.
- **Support re-sizing of embedded browser:** This feature allows the user to set the default size of the embedded browser as small or large.
- **Configurable MTU Size:** This feature allows administrators to configure the MTU size on the gateway. The default value is set to 1400, the values can range from 576 to 1500.

Release 22.6R1.2

Build 27593

No new features introduced in this release.

Release 22.6R1

Build 26825

- **EdgeWebView2 support for nZTA:** EdgewebView2 is used as the embedded browser on nZTA connections for SAML authentication and End-user portal.Single Sign-On for the nZTA connections (using the same Idp as windows), enhances end-user experience.
- **Network Manager support on Debian Linux Client:** Network Manager is supported on ISAC clients running on Linux OS.This feature uses Network manager service to set DNS server and domains without modifying the configuration file.
- **Support on Windows 11 23H2:** Ivanti Secure Access Client now supports Windows 11 Windows 23H2 (OS Build 22631.2506)
- **Support on macOS 14 Sonoma:** Ivanti Secure Access Client now supports macOS 14 Sonoma.

Release 22.5R1.1

Build 26249

No new features introduced in this release.

Release 22.5R1

Build 25375

- **End User Portal Auto launch Suppression :** This feature provides an option for admin to control the auto launch of the End User Portal.On nZTA controller configure the option under **Managed Devices --> Global Device Preferences --> Application control.**
- **Enhanced Host checker validation:** This feature provides an option for admin to enable enhanced host checker validation for an ISAC connection.

Release 22.3R3.1

Build 20175

No new features introduced in this release.

Release 22.3R3

Build 19959

No new features introduced in this release.

Release 22.3R2

Build 19787

No new features introduced in this release.

Release 22.3R1

Build 18209

- **Support on Windows 11 22H2:** Ivanti Secure Access Client now supports Windows 11 22H2
- **Support on Windows 10 22H2:** Ivanti Secure Access Client now supports Windows 10 22H2
- **Support on macOS 13 Ventura:** Ivanti Secure Access Client now supports macOS 13 Ventura.
- **Support on Ubuntu 22.04:** Ivanti Secure Access Client now supports Ubuntu 22.04.
- **Embedded browser DNS resolution when TTL is minimal:** This feature ensures that embedded browser and client application gets same IP for the gateway and communicate FQDN to same gateway server.

Release 22.2R1

Build 1295

- **Edge as External Browser:** Ivanti Secure Access Client uses Microsoft Edge as external browser by default on all Windows platforms.
- **FIDO2 Password less Support:** Ivanti Secure Access Client uses Microsoft Edge WebView2 based Embedded browser, on all Windows platforms, for Captive portal, SAML, Custom sign-in, and SAML Single Logout (SLO). The embedded browser also supports FIDO2 passwordless Authentication. Ivanti recommends downloading the Evergreen Bootstrapper software and run it on the endpoints. Software Download available at: <https://developer.microsoft.com/en-us/microsoft-edge/webview2/#download-section>.
- **PSAL Browser Extension:** This feature allows communication through browser extension instead of PSAL custom protocol. The browser extension allows to communicate to native host application installed on the client machine. The combination of native host application with the browser extension serves as the Pulse Secure Application Launcher (PSAL).

- **Replace OpenSSL FIPS module with wolfEngine/wolfSSL:** OpenSSL FIPS module is now replaced with wolfSSL through wolfEngine. This feature allows single client installer for FIPS and non-FIPS users.
- **Debian 11 qualification:** Ivanti Secure Access Client is qualified on Debian 11 platform.
- **Ivanti Secure Access Client upgrade through browser:** This feature allows administrators to control role level auto upgrade of Ivanti Secure Access Client on browsers.


Overview

This is the release-notes document for Ivanti Secure Access Client . This document provides a cumulative list of all enhancements, fixes and known issues for 22.X Releases. If the information in the release notes differs from the information found in the documentation set, follow the release notes.



The dot releases 22.3R3.1, 22.5R1.1, 22.6R1.2, 22.7R1.1 , and 22.7.2 supports latest code signing certificate. Upgrade to latest dot release before upgrading to 22.7R3 and later releases. Refer [Noteworthy information in dot releases](#) for more information.



Pulse Secure Client is re-branded as Ivanti Secure Access Client. Complete UX rebranding and the UI upgrade is implemented. There is also an option to switch between the Classic UI and New-UI to maintain user experience. The Pulse Secure client icon is replaced by Ivanti Secure Access Client icon . For more information refer [KB45301](#).

For information on End of Life (EOL) and End of Support of the Ivanti Secure Access Client, Ivanti connct secure, and Ivanti Policy Secure see, [EOL Matrix](#).

Download the Ivanti Secure Access Client from [Software Download Portal](#). You need to have the login credentials to access the portal.

Ivanti Secure Access Client provides a secure and authenticated connection from an endpoint device (either Windows, macOS or Linux) to a Ivanti gateway (either Ivanti Connect Secure or Ivanti). For a complete description of the capabilities of Ivanti Secure Access Client, see online help within Ivanti Secure Access Client itself, or *Ivanti Secure Access Client Administration Guide*.

Noteworthy Information

These are cumulative release notes. If a release does not appear in this section, then there were no associated noteworthy information or enhancements.

Noteworthy Information in 22.8R1

- ISAC launch through URL is disabled by default, this feature can be enabled by administrators from Advanced client configuration or by using installer command line options. This feature is supported for windows only. For more information, see [Ivanti Secure Access Client NachoVPN mitigation](#).
- For windows, Dynamic certificate trust is disabled by default, administrators can enable using ICS UI or through installer command line. For more information, see [Ivanti Secure Access Client NachoVPN mitigation](#).
- For TDI driver deprecation information refer to [Deprecation of TDI Fail-Over Option](#).

Noteworthy Information in 22.7R3

- From Release 22.7R3, JAM commands for user mode are not supported. However for admin mode, there are no changes.
- Auto upgrade or browser base upgrade is not supported from Release 22.7R1 or earlier versions to 22.7R3. Refer [Noteworthy upgrade path](#).

Noteworthy Information in dot releases 22.3R3.1, 22.5R1.1, 22.6R1.2, 22.7R1.1, and Release 22.7.2

- Due to code signing certificate expiry on Windows, the auto upgrade and browser based scenarios of Ivanti Secure Access Client is impacted. ISAC 22.7.3 and later releases uses updated code signing certificate.
To upgrade from 22.7R1 or earlier releases to 22.7R3 and later ISAC releases, first upgrade to the latest respective dot release (22.3R3->22.3R3.1) before upgrading to required release version. For detailed upgrade procedure, refer to [Upgrade Procedure for Ivanti Secure Access Client \(ISAC\) for Windows Desktop due to change in code signing certificate](#).

Code signing certificate expiry does not impact ISAC upgrade through SCCM. Users can directly upgrade to required main release version.

Noteworthy Information in 22.7R2

- Ivanti Secure Access Client is upgraded to OpenSSL version 3.2.
- CentOS 7 is not supported.
- On Ubuntu 22, Ivanti Secure Access Client does not support CEF and SAML.

Noteworthy Information in 22.7R1

- Ivanti Secure Access Client does not support Windows 32-bit (x86). Latest ICS do not list the x86 installers.
- On existing version of ICS when 22.7.1 ISAC packages are updated, Windows 32-bit (x86) installers link will not work and when a user connects to ICS, an upgrade prompt displays but the upgrade fails.
- Auto upgrade is not supported for Windows 32-bit (x86) platform. An upgrade prompt may display but the upgrade fails on Windows 32-bit systems. Refer [Deprecation of Windows X86/32-Bit](#).
- macOS Big Sur is not supported from 22.7R1.
- When AOVPN and nZTA connections co-exists, users can access any resources by connecting to either the lockdown connection (L3) or the nZTA connection. If one connection is active, the client lifts the lockdown irrespective of other connection.

Noteworthy Information in 22.6R1

- Ivanti Secure Access Client is not supported on macOS Catalina.
- Ivanti Secure Access Client installer is enhanced to support dynamic Windows ISAC driver Interface IfType Ethernet/Virtual.
- The dynamic driver type functionality does not work when the client is auto-upgraded or upgraded through the Web Browser from 22.5Rx or older builds to 22.6R1.


Noteworthy Information in 22.3R3

- Ivanti Secure Access Client is enhanced to fix security issues. For more information, refer [Security Article CVE-2023-34298](#).

Noteworthy Information in 22.3R1

- On macOS13 Venture, PSAL/Setup client upgrade with the browser does not work. Manually click Download and install to install the client.
- Ivanti Secure Access Client may trigger infinite browser tabs when "Allow user to override connection policy" is set to false when using SAML authentication. Use embedded browser when using SAML authentication or set the "Allow user to override connection policy" to true.

Noteworthy Information in 22.2R1

- Pulse Secure Client is re-branded as Ivanti Secure Access Client. Complete UX rebranding and the UI upgrade is implemented. There is also an option to switch between the Classic UI and New-UI to maintain user experience. The Pulse Secure client icon is replaced by Ivanti Secure Access Client icon . For more information refer [KB45301](#).
- No FIPS specific client is available from release 22.2R1.
- Cache-cleaner, IE ActiveX are deprecated from release 22.2R1.
- Increased number of Split tunneling networks from 512 to 1024.
- DSA Certificate Authentication is not supported in FIPS mode.

Security Advisory and Patch Update

Security-related issues are not normally covered in release notes. To learn more about security advisories affecting Ivanti products, see the [Ivanti security advisory page](#).

Upgrade Instructions

Upgrade Paths

The following table describes the tested upgrade paths.

Release	Description
22.7R4 and previous 22.x releases	You can upgrade directly to 22.8R1.

- Client upgrades are not supported to or from beta releases or Hot-Fix releases.
- Auto upgrade or browser base upgrade is not supported from Release 22.7R1 or earlier version to 22.7R3 and later.

Installer List on Ivanti Connect Secure

The **Maintenance** --> **System** --> **Installers** page on Ivanti Connect Secure User Interface displays the list of installers.

From 22.7R1, Windows 32-bit (x86) installers are not available.

Support and Product Compatibility

See the latest [Ivanti Secure Access Client Supported Platforms Guide](#) for supported versions of operating systems, browsers, and servers in this release. The platforms with default factory settings are qualified and advanced features are not considered.

Resolved Issues

The following table lists issues that are fixed and are resolved by upgrading to this release.

Problem Report Number	Summary
Release 22.8R1	
1493774	Unable to launch Mac client after upgrade to 22.7R4 from 22.5R1.
1485632	Resource Not Accessible issue observed when accessing any application that is accessed via PSAM with L3 coexistence.
1451782	ISAC keeps trying to connect back to VPN and doesn't give up when the connectivity is lost with VPN Gateway.
1444880	ISAC 22.7R3 freezes on MAC OS Ventura.
1442039	User Access shows Local Username instead of VPN Username while using SAML with EB.
1435950	MacOS users with ISAC 22.7R3 are unable to access backend resources with .127 IPs through PSAM.
1419515	PSAM displays "'pcp max no of connections limit (63) reached for a user session" for Mac users.
Release 22.7R4	
1302201	Authentication fails. No option to choose the RSA token in new GUI ISAC.
1385123	Ivanti Client New UI invoks powershell command without any explicit info on execution mode
1376762	Ivanti Client feature "Randomize URL list order" not working as expected, and traffic to one gateway is specifically more than other.
1378417	When trying to connect to a ZTA connection on ISAC, CEF download is prompted. On clicking "OK" the download fails INTERMITTENTLY with the error "CEF package download failed. Error:getpeername() failed".
1378084	Physical Interface DNS not getting restored after disconnecting from the

Problem Report Number	Summary
	VPN, waking from sleep mode, or logging off.
1408565	ISAC is not downloading the proxy.pac file when automatically detect proxy settings are enabled on Windows.
1389111	[mac-sequoia] Browser based ISAC installation fails.
1395992	Invalid ICS prompts observed on macOS systems.
1426115	Installation issue observed with ISAC 22.7R3 on Windows 10 and 11.
Release 22.7R3	
1302186	User gets authentication rejected by server error 1319.
1302268	The attempt to load the session start script fails when switching the URL between two different servers.
1302274	Optimize SSL for Cisco Umbrella.
1302279	ISAC client disconnection with error "Invalid ICS URL, disconnection. Enter a valid ICS URL".
1302304	PSAM Resources Not Accessible on mac OS Sonoma with ISAC 22.7R1.
1302374	ISAC 22.7.1 takes min 15-20 mins to load post PC reboot.
1302383	Unable to launch ISAC 22.7R1 in second user profile.
1302881	After upgrading the ISAC to 22.7R1 a PulseSecureService.exe dump is observed.
1302883	PulseSecureService.exe is crashing on Ivanti Secure Access Client 22.7R1.
1315266	DNS cache response not working on IPV6 for A and AAAA Records.
1368561	Ivanti Client Failed to Register VPN IP - DDNS [IPv4 Only].
1380272	Unable to copy files using SFTP through PSAM connection on ISAC 22.7R1 on mac OS Sonoma.

Problem Report Number	Summary
PSD-17652	The VPN connection goes into a loop (connect/disconnect) when Location Awareness rules are configured for DNS servers on the Physical adapter, and the same DNS server is configured on the ICS.
PSD-17824	The Pulse Secure Installer Service (PSIS) installation is failing.
PSD-16989	Ivanti secure Access Client prompts for authentication post upgrade.
Release 22.7R2	
PRS-420202	The branding logo is not placed correctly on Ivanti Secure Access Client on macOS even when PulseMac.pulsebranding was re-created with the latest branding tool.
PRS-419929	Chinese language localization issue noticed with linux client while using RADIUS challenges.
PRS-419887	Ivanti client is considering virtual adapter MTU value instead of physical adapter.
PRS-419802	When upgrading Windows machines from 9.1R15 to 22.7R1 some users machines are facing failure.
PRS-419606	Rollback observed during upgrade from 9.1R15.1 to 22.5R1.
PRS-419391	DNS resolution issues observed with WFP driver PSAM.
PRS-419189	TDIUtility.exe did not support silent switch.
PRS-418957	Session roaming with The DNS Load balancer ICS setup should resume the session without Re-Authentication.
PRS-418927	Ivanti Client Embedded Browser allow users to browse internet websites.
PRS-418785	Users experiencing network disruptions post the CISCO umbrella installation when the ISAC client is in a connected state.
PRS-418682	Singpass (SAML) Authentication fails when Load balancer URL is configured under the "Host FQDN for SAML".

Problem Report Number	Summary
PRS-418673	FQDN DNS Response being upper case and split tunnel route creation failed.
PRS-418667	Certificate Selection Popup issue in recent ISAC Client Versions on Mac OS during SAML Authentication.
PRS-417828	Intermittent DNS error message noticed with PSAM and IPv6 enabled in 22.x version.
PRS-417571	22.5R1 auto-connect is not working, location awareness issue.
Release 22.7R1	
PRS-418768	Unable to upgrade client through SCCM/msiexec from 9.1R15 to ISAC 22.6R1.
PRS-418645	Unable to upgrade client from 9.1.15 to 22.3.3.
PRS-418634	ISAC Client on MAC OS Sonoma unable to complete connection and crashes.
PRS-418193	Invalid Server Certificate on macOS Workstations with ISAC 22.5R1 caused by JAM UI Plugin Loading Issue.
PRS-418164	HC Logs in User Access shows Local Username instead of VPN Username while using Embedded Browser.
PRS-418158	Secure DNS Blocking fails after upgrading to 22.6R1.
PRS-417897	Heap Corruption due to repeated connect/disconnect of PSAM using pulselauncher.exe.
PRS-417598	Uninstall ISAC 22.5R1 fails and rollback.
PRS-417589	Delayed response/disconnection to backend resource application after upgrade to ISAC client on Mac OS (Ventura).
PRS-417520	Crash observed often when using connect/disconnect to PSAM repeatedly through pulselauncher.exe

Problem Report Number	Summary
PRS-417288	Ivanti Desktop Client menu responsiveness between Dock and taskbar issue on Mac.
PRS-416723	BSOD observed on 22.3.2.19787 when PSAM is enabled.
PRS-416402	Ivanti client on Mac prompts for upgrade when any of the components on the user machine are lower than the server.
PRS-415882	Crash noticed in PSAM access through Pulse launcher.
Release 22.6R1	
PRS-417416	ISAC client installation/uninstallation issue is observed when upgrading to latest version.
PRS-417410	Embedded browser is allowing file downloads through Captive Portal.
PRS-417373	Unable to upgrade client through SCCM from 9.1R15 to ISAC 22.3R3
PRS-416994	Customized Branding LOGO size is not proportionate for ISAC client.
PRS-416852	Wireless 802.1x session not resuming when machine wakes up from sleep.
PRS-416790	Slow Login Prompt Presentation on ISAC After Clicking 'Connect' on Mac Machine.
PRS-416426	While installing 22.3R2, Outlook dependencies / Files In Use warning displays.
PRS-416383	On 22.3 client, automatic selection of user certificate fails certificate authentication with YubiKey-based certificates.
PRS-416363	RDP Connection Drops consistently with ISAC 22.3.2 (FIPS).
PRS-416310	VM crashes when ISAC is installed and PSAM based access mechanism is used by VPN users.
PRS-416166	When the Hyper-V feature is enabled on Windows 11 (Enterprise), ISAC disables the WLAN functionality.

Problem Report Number	Summary
PRS-415197	Client log collection prompts for admin credential as standard user on Mac OS.
PRS-414982	Sign-out command only works with first matched URL.
PZT-40377	When powering on back from sleep/suspend, the ISAC UI crashes with the message "The application PulseUI has closed unexpectedly".
PZT-38894	Disable splash screen not working in ISAC 22.3R1
Release 22.5R1	
PRS-416363	RDP Connection drops consistently with ISAC 22.3.2 (FIPS)
PRS-416133	Ivanti secure access client gives Server certificate trust error when connecting using the IP address which is already present in SAN.
PRS-416019	The LDAP authentication in ISAC 22.Rx is not functioning properly when used in conjunction with the primary SAML server.
PRS-415808	End-users are not able to connect to VPN due to Captive Portal issues when using with Always-On-VPN.
PRS-415790	When New UX for ISAC client is selected, on reboot auto launches the UI.
PRS-415778	Session script does not execute on MacOS if set to run at the end of the session.
PRS-415108	Split DNS: excluded split tunneling resources are being resolved by IVE DNS first.
PRS-414373	[macOS] Hostname changes after connecting to the ISAC.
PSD-13884	[macOS] internet traffic is getting blocked and save logs is not working after sleep and resume when SSID changes.
PSD-14514	[macOS] SAML Certificate Based Authentication fails via Embedded Browser
PSD-14358	[macOS] Not prompting proper error messages while downgrading the client.

Problem Report Number	Summary
PZT-39506	MTU size varies for Virtual adapter when connecting to ZTA gateways, causing packet loss.
PZT-40652	Windows clients enrolment always fails on the corporate machine but works on private machine.
Release 22.3R3	
PRS-416363	RDP Connection Drops consistently with ISAC 22.3.2 (FIPS)
Release 22.3R2	
PRS-416175	[Windows] VPN stop script not honored for Always On VPN.
PRS-415674	[Windows] SplitDNS Proxy functionality does not work with Apex One Personal Firewall Service.
PRS-415370	[Windows] When using the Edge embedded browser, in a proxy environment, the captive portal may not display correctly to allow the user to authenticate/login to the captive portal.
PRS-414083	[Windows] When using the Edge embedded browser, in a proxy environment, the captive portal may not display correctly to allow the user to authenticate/login to the captive portal.
PRS-415263	[Windows] Intermittently observed the BSOD issue when the Skyhigh antivirus is installed on the endpoint with ISAC client.
PRS-415223	[Windows] When Split DNS is enabled and system hibernates, after resume VPN shows as connected but resources are not accessible.
PRS-415194	[Windows] Switching NIC causes the secondary connection to be unstable.
PRS-415161	[Windows] Wi-Fi connection does not re-connect automatically and fails with unknown error when the system wakes from sleep mode.
PRS-415073	[Windows] On upgrade, the RDP session in full screen mode does not display properly.

Problem Report Number	Summary
PRS-414885	[Windows] When using the Edge embedded browser, in a proxy environment, the captive portal may not display correctly to allow the user to authenticate/login to the captive portal.
PRS-414879	[Windows] Pulse Secure Service crash observed intermittently.
PRS-414801	[Windows] Preconfig file not getting deployed on the client PC using msixexec command.
PRS-414668	[macOS] ISAC interface launches on MACOS after reboot.
PRS-414512	[Windows] ISAC 22.3.1 crash observed on Windows 10.
PRS-414355	[Windows] User Tunnel with SAML Authentication is showing error with ISAC 22.x when multiple realms are configured using same sign-in policy.
PRS-414262	[Windows] On some machines, when client version is manually downgraded (uninstall and revert to an older version) the connection is stuck in "Securing Connection" phase.
PRS-414210	When using Cert Auth with LDAP as secondary, unable to complete authentication on the linux client or New UI with Windows or Mac.
PRS-414164	[Windows] Ivanti Secure Access Client fails to connect with FIPS enabled on the connection store.
PRS-414098	[Windows] PSAM Based FQDN Deny resource while accessing shows Internal Error in 9.1R15 Client.
PRS-414083	[Windows] When using the Edge embedded browser, in a proxy environment, the captive portal may not display correctly to allow the user to authenticate/login to the captive portal.
PRS-413929	[Windows] Connect Button is greyed out in New-UX when SAML is the primary authentication method and TOTP is secondary authentication method.
PRS-413897	[Windows] The Host Checker plugin fails to initialize, resulting in the failure of login to the VPN server.

Problem Report Number	Summary
PRS-413858	[Windows] PulseSecureService crashes post enabling DDNS registration.
PRS-413631	[Windows] After user connected to VPN and got assigned to IPv4/IPv6 Dual stack, occasionally the IPv6 address changed from "Preferred" to "Duplicate".
PRS-413610	[Windows] Crash (BSOD) on Windows (Dell laptops) while powering on back from hibernate mode when using ISAC -22.2R1
PRS-413597	[macOS] Packet loss and latency spikes are noticed with Ivanti Client 9.1R13 and above when Split tunnel and proxy pac is used on Mac OS.
PRS-413549	[Windows] Embedded Browser fails to detect the Secondary Monitor position (Left or Right Side).
PRS-413382	[macOS] Ivanti Secure Access Desktop Client fails Signature check when verifying with SuspiciousPackage.
PRS-413376	[Windows] ISAC hung in Disconnecting state.
PRS-412774	[Windows] Pulse Secure Service crashes intermittently.
PRS-412097	[Windows] ISAC deployment through SCCM fails when the setup client installation fails with any issue.
PRS-411934	[Windows] Location awareness evaluation may not work as expected when switching the network interfaces LAN to Wi-Fi and vice versa.
Release 22.3R1	
PRS-414036	Resizing of ISAC default view on Embedded Browser.
PRS-413521	[Mac OS] Ivanti Secure Access Client interrupt's shutdown during initial attempt.
PRS-413518	[Mac OS] Ivanti Secure Access Client UI issue in German Version.
PRS-413455	Host checker takes long time in phase checking compliance.
PRS-413442	[Mac OS] Memory leak seen after upgrading client to PDC 9.1R15 on mac OS Monterey.

Problem Report Number	Summary
PRS-413412	Ivanti clients from ICS 22.2R1 Build 1295 is identified as older client than ICS9.1R15 build 15819 in VMware workspace one UEM
PRS-413424	[Mac OS] Ivanti secure access client unable to stop Startup application on Mac.
PRS-413212	Yubikey not able wrap the keys
PRS-413036	Ivanti Secure Access client crash with IveConnMethod.dll
PRS-412811	Inconsistencies in ISAC 22.2R1 UI for Chinese language (Traditional and Simplified)
PRS-412732	The UI mode option is disabled when the ReactNative package fails to install.
PRS-412692	[Mac OS] Authentication Rejected by server on using Custom Sign-in page.
PRS-412216	Service (dsTMSservice.dll) crashes intermittently and the user faces disconnection.
PRS-412127	[Mac OS] Memory leak on PDC 9.1R15 on mac OS Monterey.
PRS-411912	Credential Provider doesn't start immediately after boot.
PRS-411613	Ivanti Secure Access Client fails to download PAC file.
PRS-411465	SSH is not working when TOS bit is enabled on ICS.
PRS-410919	Accessing resources consume more data/bandwidth, the connection to the resources fails with TCP errors and connectivity to those devices are intermittently timing out.
PRS-410910	Suspend button grayed out when connection is present.
PRS-401785	[Windows] Client Embedded browser DNS resolution fails if TTL is minimal.
Release 22.2R1	

Problem Report Number	Summary
PRS-410847	[Windows] Unable to access the PSAM resource after upgrading to 9.1R15-Windows 10 and 11
PRS-410284	[MacOS] When content filter profile is pushed through MDM, the content provider is still preserved after uninstalling the sysext. When the content filter provider is installed manually the content provider is deleted after uninstalling the sysext.
PRS-410075	[Linux] CEF Browser get aborted in Linux Distro.
PRS-409902	[Windows] Even if "sso-cached-credential" option is enabled,Ivanti Secure Access Client is again prompting for username/password (post getting the desktop).
PRS- 409751	[MacOS] Issue with PDC on Mac Monterey 12.3.0 or 12.3.1, Big Sur (11.6.2) with getting connected when the session times out or, the user mahcine goes to sleep.
PRS-409677	[Linux] Ivanti Secure Access Client service is getting crashed, during the download of a large file.
PRS-409362	Ivanti Secure Access Client route events flooding the debug logs.
PRS-408862	[MacOS] MacOS Workgroup changes from Domain to Hostname when connecting with Ivanti Secure Access Client.
PRS-408843	[MacOS] Client Service crashes on macOS with Ivanti Secure Access Client 9.1R15 EA.
PRS-408632	[Windows] SAML login window is hidden for users - embedded browser.
PRS-408516	The Browser based HC was getting corrupted due to Heap corruption during a 3rd party NHC rule evaluation.
PRS-408513	[MacOS] MacOS User's traffic bypassing lockdown.
PRS-408487	[Linux] Duplicating "WebKitWebProcess" consuming endpoint memory with R14 client.

Problem Report Number	Summary
PRS-408199	[Windows] Unable to download Proxy Pac from 9.1R12 when "Transfer-Encoding: chunked" header is present.
PRS-408159	[Windows] Embedded browser pop-up gets hidden on windows machine intermittently during launch.
PRS-407376	[Windows] PAC file download fails when content-type Header is not present.
PRS-406670	[MacOS] ESP-Keep-Alive Fails after upgrading to 9.1R13.1 Ivanti Secure Access Client.
PRS-406469	[MacOS] FIPS MacOS universal client support for Native ARM (M1) instead of Rosetta.
PRS-403095	HC Logs in User Access shows Local Username instead of VPN Username while using Embedded Browser.

Known Issues

The following table lists Known Issues in the current release.

Problem Report Number	Summary
Release 22.8R1	
1517114	Symptom: ISAC tunnel falls back from ESP to SSL during configuration import with a combination of XML and Rest API on ICS 22.7R2.6. Workaround: Try one of the following: <ul style="list-style-type: none"> • Restart ICS services • Reboot ICS • Open Connection profile and save without any changes
1516939	Symptom: DNS Resolution issue observed when using "Device Only DNS with Split Tunneling in VPN" on Mac Sonoma. Workaround: Enable IPv6 on the physical interface or remove the specific allow policy on the ICS.
Release 22.7R4	
1481530	Summary: Sometimes, launching of ISAC will be stuck in full screen mode on Windows 10 22H2 when using CLI. Workaround: Exit and relaunch ISAC.
Release 22.7R3	
1389111	Summary: [mac-sequoia] Browser based ISAC installation fails. Workaround: None. Fix will be available in ISAC 22.7R4 (October 2024)
1390566	Summary: [mac-sequoia] Upgrade prompt appears after upgrade to latest version. Workaround: Click Cancel on upgrade prompt. Fix will be available in ISAC 22.7R4 (October 2024)
1381258	Summary: Intermittently observed the Ivanti secure access client (ISAC) crash on macOS Sonoma while upgrading to the 22.7R3 ISAC client. Workaround: None, ISAC recovers automatically.

Problem Report Number	Summary
1378417	<p>Summary: When trying to connect to a ZTA connection on ISAC, CEF download is prompted. On clicking "OK" the download fails INTERMITTENTLY with the error "CEF package download failed. Error:getpeername() failed".</p> <p>Workaround: Unload and Load dsAccessService or Restart the machine.</p>
Release 22.7R2	
PSD-17652	<p>Summary: The VPN connection goes into a loop (connect/disconnect) when Location Awareness rules are configured for DNS servers on the Physical adapter, and the same DNS server is configured on the ICS.</p> <p>Workaround: Enable the registryKey [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Pulse Secure] "DisableNotifyInterfaceUpdate"=dword:00000001.</p>
PSD-17446	<p>Summary: Unable to connect to internet after a secure connection fails.</p> <p>Workaround: Restart the machine.</p>
PSD-17824	<p>Summary: The Pulse Secure Installer Service (PSIS) installation is failing.</p> <p>Workaround: Install the earlier version (22.7R1/22.6R1) PSIS for the fresh ISAC installation scenarios via browser.</p>
PSD-16702	<p>Summary: Ivanti Secure Access Client registers its DNS proxy Provider network extension with the system for some feature like TE FQDN and minTTL and stops working if any other application with DNS Proxy provider runs simultaneously. As per Apple, only one "DNS proxy Provider" network extension can be present on the machine.</p> <p>Workaround: Uninstall applications with DNS Proxy provider network extension before Installing Ivanti Secure Access Client</p>
PSD-16989	<p>Summary: Ivanti secure Access Client prompts for authentication post upgrade.</p> <p>Workaround: Re-authenticate and continue to use Ivanti Secure Access Client.</p>
Release 22.7R1	
PSD-15911	<p>Summary: Client freezes on the Role Selection window during timeout phase and does not allow user to select any Role.</p> <p>Workaround: Close the client from the tray and reopen.</p>

Problem Report Number	Summary
PZT-43203	<p>Summary: Intermittently users are unable to access the backend resources when both ZTA and VPN connections are connected.</p> <p>Workaround: Open ISAC UI from tray, disconnect ZTA connection and reconnect.</p>
PZT-43108	<p>Summary: Client is not honoring new GW MTU when GW failover happens in GW group if GWs are having different MTUs.</p> <p>Workaround: None.</p>
PZT-42473	<p>Summary: Enrollment fails from browser and will give error "SAP is not configured for /login /login/enroll" when device policy is enforced on the user sign-in policy and the same device policy is modified.</p> <p>Workaround : Navigate to Secure Access->Manage Users->User Policies and need to edit/save the user policy on which device policy is mapped post changing the device policy.</p>
Release 22.6R1	
PSD-14144	<p>Summary: Multiple instances of ISAC UI observed. User input is accepted in all instances.</p> <p>Workaround: None</p>
PSD-15296	<p>Summary: On rare occurrences, client UI closes during manual connect or disconnect of connections.</p> <p>Workaround: Use system tray to launch Client UI.</p>
PSD-15380	<p>Summary: Pulse setup client is not installing/upgrading. The client does not display the client upgrade prompt when connecting to the ICS server with http connection.</p> <p>Workaround: Use https Sign-in URL to connect to ICS server.</p>
PSD-15384	<p>Summary: During simultaneous (nZTA + VPN) connection, Auth failure message '1319' displays for VPN connection for a brief period.</p> <p>Workaround: Connect nZTA first and then initiate VPN connection or vice versa.</p>
PSD-15502	<p>Summary: On rare occurrences, connection fails due to CEF browser crash.</p> <p>Workaround: Restart dsAccessService.</p>
PSD-15540	<p>Summary: CEF browser crashes on Mac OSX when resuming from sleep.</p>

Problem Report Number	Summary
	Workaround: None.
PSD-15637	Summary: User not able to connect to VPN. Workaround: Close and re-launch client from spotlight.
PZT-35720	Summary: Download triggers before clicking "Upgrade" button on the upgrade message window when auto-upgrade is enabled. Workaround: None.
PZT-41329	Summary: User sees an embedded browser white blank screen while reconnecting SAML auth for few seconds. Workaround: None.
PZT-41880	Summary: During Simultaneous (nZTA + VPN) connection, one of the connections might take slightly longer time to connect. Workaround: Connect first to nZTA and the VPN or vice-versa.
PZT-41927	Summary: When user clicks to connect to ZTA, the connection does not start. This is specific to ZTA connections and is seen to happen during machine start of machine left idle for long time with ZTA in disconnected state Workaround: Restart the machine or delete and re-enroll the client again.
PZT-41967	Summary: The ZTA connections reconnect at random times. Workaround: None.
Release 22.5R1	
PSD-15039	Summary: When ZTA and Classic connections exist simultaneously, the classic gateway connection gets stuck in "Checking Compliance" state Workaround: Restart the client and establish either ZTA or classic connection.
PSD-14785	Summary: When ZTA is connected and ISAC crashes, it is noticed on recovery the DNS resolution is blocked on the machine. Workaround: Only if ZTA workflow crashes, create a registry key HKLM\SOFTWARE\Pulse Secure\Pulse DWORD key AutoUnloadWFP with value 1.
PZT-40370	Summary: Linux ISAC is unable to download CEF browser and ISAC crashes. Workaround: Manually install CEF.

Problem Report Number	Summary
PZT-37424	<p>Summary: With pre-configured ICS and all client components installed on the endpoint, auth re-directs to default login URL instead of custom SAML auth URL when trying to enroll with multi sign-in URL.</p> <p>Workaround: Deep clean endpoint for all client components and perform a fresh installation.</p>
Release 22.3R3	
No new Known Issues in this release.	
Release 22.3R2	
PRS-414909	<p>Symptom: PIN prompt for the FIDO Authentication is not displayed for Linux users.</p> <p>Condition: When FIDO password Authentication is enabled.</p> <p>Workaround: None</p>
PSD-14142	<p>Symptom: Rarely users come across a BSOD while resuming the machine from Hibernation.</p> <p>Condition: When a machine is in Hibernate mode.</p> <p>Workaround: None.</p>
PSD-14501	<p>Symptom: Rarely users come across a BSOD while upgrading the client.</p> <p>Condition: When split DNS is enabled.</p> <p>Workaround: None.</p>
PSD-14512	<p>Symptom: ISAC Client help shows release version as 22.4.</p> <p>Condition: When help is accessed through ISAC 22.3R2</p> <p>Workaround: None.</p>
PSD-14514	<p>Symptom: VPN SAML Authentication fails on Mac OS with Embedded browser.</p> <p>Condition: When Azure SAML IdP is configured with certificate-based login.</p> <p>Workaround: Enable FIDO2 U2F for SAML authentication option under connections to use CEF browser for SAML with certificate-based authentication.</p>
PZT-39936	<p>Symptom: Upgrade to latest ISAC version fails.</p> <p>Condition: Cisco Any Connect software is installed and running.</p> <p>Workaround: Stop the Cisco Any Connect from services.msc</p>

Problem Report Number	Summary
Release 22.3R1	
PRS-414801	Symptom: Preconfig file is not deployed on the client PC. Condition: When using msixexec command. Workaround: None.
PRS-412169	Symptom: The display name on Windows Task Manager differs compared to OS versions prior to Win 11 22H2. Condition: Windows OS version is Win 11 22H2 or higher. Workaround: None.
PRS-411820	Symptom: Ivanti Secure Access Client disconnects randomly on Windows. Condition: When Ivanti Secure Access Client and a combination of Windows Connection Manager is used. Workaround: None.
PSD-13174	Symptom: PSAL download prompt appears multiple times on macOS 13. Condition: When installing client using browser. Workaround: Ignore the message and click 'Download' to proceed.
PSD-13172	Summary: Random user observed ZTA onboarding failed. Condition: While Enrolling ZTA connection. Workaround: Uninstall and reinstall the client.
PSD-13168	Symptom: PSAL and setup client launch fails when ICS is upgraded from 9.1R15. Condition: When PSAL browser extension is enabled. Workaround: Download and launch PSAL again.
PSD-13030	Summary : While upgrading to the 22.3R1 client prompts to close some applications. Condition: Upgrading the client to the 22.3R1 version from older version. Workaround: Ignore the prompt and proceed with the upgrade.
PSD-13021	Symptom: User cannot disconnect the active VPN session. Condition: L3 and ZTA connections are used on macOS 13. Workaround: Re-launch UI.
PSD-13014	Symptom: On upgrading client to 22.3R1, during the first UI launch, the UI crashes.

Problem Report Number	Summary
	Condition: On Windows machines having 15 or more connections configured Workaround: Launch the client UI again from start menu.
PSD-12930	Symptom: EdgeWebView2 Runtime installation mandates a minimum of 2GB free disk space even when not actually utilized. Condition: Ivanti Secure Access Client requires to use Embedded Browser (SAML, Custom Sign-in pages) etc Workaround: The minimum free disk space requirement is a pre-requisite to ensure seamless working of Edge based Embedded Browser.
PSD-12409	Symptom: Switching from classic UI to NEUX, launches Ivanti Secure Access Client in full screen mode. Conditions: When L2 and L3 connections are used. Workaround: None.
PSD-8514	Symptom: Add and Remove program has both classic and React UI present. Condition: When Client is installed. Workaround: None.
PZT-40784	Summary: when the machine wakes up after a long sleep, sometimes the Client UI shows the error "Failed to setup virtual adapter". Condition: When a ZTA connection is attempted on Linux OS. Workaround: Click Retry and attempt to connect again.
PZT-36977	Symptom: Server CA fails to install on the end points. Condition: Randomly happens on some MAC machines. Workaround: Delete the existing connection and add new ZTA connection.
PZT-36750	Symptom: Lockdown enable/disable on tenant takes more time to reflect in client connstore.dat file. Condition: When we make changes with respect to lockdown on the tenant. Workaround: None
PZT-36426	Symptom: dsAccess service crashed after system sleep. Condition: When using ZTA and ICS tunnel on Mac Book Pro Ventura 13.0. Workaround: Restart Ivanti Secure Access Client services.
PZT-35824	Symptom: Error 1107 observed when using browser based enrollment. Condition: When security enabled POD is running.

Problem Report Number	Summary
	Workaround: Reconnect the connection.
PZT-35807	Symptom: Ivanti Secure Access Client does not move to Connected state. Condition: On Minimum Client Version upgrade. Workaround: None.
PZT-35360	Symptom: Pop-up blocked for the enrollment URL Condition: When using PSAL browser extension is enabled. Workaround: Close and open the browser again.
PZT-34750	Symptom: System preferences popup does not appear until machine reboot/re-login. Condition: When using Always-ON VPN with lock-down connection. Workaround: None.
PZT-34534	Symptom: Every disconnect and connect installs the Lookout forward proxy certificate on macOS. Condition: When trying to establish a connection. Workaround: None.
PZT- 36969	Symptom: Error 1147 observed after uninstalling (with save configuration) and re-installing ISAC for ZTA . Condition: When ZTA connection details are saved previously. Workaround: Re-enroll the connection.
Release 22.2R1	
PCS-38008	Symptom: PSAL failed to launch JAVA applets on MAC M1 Ventura 13. Condition: When end-user launches JSAM. Workaround: None.
PCS-37311	Symptom: The Ivanti Secure access client on Windows or macOS machines establishes the VPN session with the Ivanti Connect Secure displayed as the FIPs client under the Active users' page. Condition: The 22.2R1 client is used for establishing the session Workaround: None.
PRS-412672	Symptom: DMG package on Ventura platform shows the file was downloaded on an unknown date and is damaged.

Problem Report Number	Summary
	<p>Condition: When Host checker is configured, the client fails to launch through browser or browser based connection.</p> <p>Workaround: None.</p>
PRS-412216	<p>Symptom: Ivanti Secure Access Client Service (dsTMSservice.dll) crashes intermittently and the user faces disconnection.</p> <p>Condition: When a DNS response contains very long CNAME entries and the payload is compressed, there is a chance of a parsing error, resulting in a crash.</p> <p>Workaround: None.</p>
PRS-412144	<p>Symptom: A Warning displays, "Uninstall is damaged can't be opened" on MAC Ventura 13.0.</p> <p>Condition: During Ivanti Secure Access Client uninstallation.</p> <p>Workaround: None.</p>
PRS-412025	<p>Symptom: Smart card login fails when used on custom sign-in page.</p> <p>Condition: Custom sign-in page is mapped to VPN sign-in URL.</p> <p>Workaround: Map default sign-in page to the VPN sign-in URL or VPN sign-in can be performed through chrome browser and then Ivanti Secure Access Client connection can be started from browser</p>
PRS-411750	<p>Symptom: Ivanti Secure Access Client rebranded package creation through ConfigureInstaller python script fails.</p> <p>Condition: Ivanti Secure Access Client rebranded package creation is performed on Big Sur or Monterey.</p> <p>Workaround : Perform ISAC rebranded package creation on Catalina.</p>
PRS-411746	<p>Symptom: "Securing Connection" status is not seen on New-UX.</p> <p>Condition: When using New-UX client.</p> <p>Workaround: None.</p>
PRS-411741	<p>Symptom: Mac- With ICS and IPS connections, for each disconnection of VPN, Un-expected UI switch happens. This happens when a different Admin Setting is enabled for Client UI Mode than the existing display in the Client UI.</p> <p>Condition: When user tries to connect to two connections in the client, that is ICS and IPS connections.</p> <p>Workaround: None.</p>

Problem Report Number	Summary
PRS-411632	<p>Symptom: UI Switch as per Admin Settings does not work for the second connection in desktop client.</p> <p>Condition: When there exist two ICS connections, ICS and IPS connections, or for tunnel in tunnel case.</p> <p>Workaround: None</p>
PRS-411599	<p>Symptom : Set-up client error pop up seen when connecting to an older server.</p> <p>Condition : New Client connecting to older Server.</p> <p>Workaround: Install the client manually or upgrade the client by connecting to Ivanti Connect Secure using client.</p>
PRS-411593	<p>Symptom: Ivanti VPN Web page stuck at "Searching for PSAL" even after L3 VPN session established.</p> <p>Condition: Custom sign-in pages mapped to corresponding VPN Sign-in URL and end-user launches L3 VPN connection from browser VPN session.</p> <p>Workaround: Click "Please click here to go back" on the PSAL search page when L3 VPN session is started.</p>
PRS-411556	<p>Symptom: No notification to user when New-UX is asking for credentials. This eventually leads to User Input timeout.</p> <p>Condition: When user does not enter credentials.</p> <p>Workaround: Need to check New-UX to enter credentials.</p>
PRS-411510	<p>Symptom: "Searching for Application Launcher Page" displays even after successful Install and connecting to VPN.</p> <p>Condition: The installation/launch of Ivanti Secure Access Client using Firefox.</p> <p>Workaround: Refresh the browser.</p>
PRS-411478	<p>Symptom: VPN Connection may fail to establish in proxy environment where automatic PAC URL is configured.</p> <p>Condition: Web server send the PAC file without http response header content-length instead sends transfer-encoding: chunked.</p> <p>Workaround: Configure web server hosting PAC file to send content-length in http response header.</p>
PRS-411380	<p>Symptom: Accessibility feature does not work on New-UX.</p> <p>Condition: When using New-UX.</p> <p>Workaround: Use classic UI.</p>

Problem Report Number	Summary
PRS-411350	<p>Symptom: May observe the Ivanti Secure Access Client crash while establishing an L4 connection on macOS.</p> <p>Condition: The 9.1R15 client connecting to 9.1R16 which is upgraded from 9.1R15 to R16 with macOS PSAM configurations configured on the R15.</p> <p>Workaround: Upgrade the client to 22.2R1 or delete and recreate the new macOS PSAM configurations after the upgrade.</p>
PRS-411341	<p>Symptom: If New-UX client is minimized to windows taskbar, it does not open if user selects to open the client from Tray.</p> <p>Condition: New-UX client minimized to Windows taskbar.</p> <p>Workaround: Manually select the taskbar icon and open the New-UX client.</p>
PRS-411006	<p>Symptom: CPU usage might increase when Auto-Refresh is enabled on New-UX.</p> <p>Condition: When Auto-Refresh is enabled on NEUX.</p> <p>Workaround: Disable Auto-Refresh.</p>
PRS-410987	<p>Symptom: No system sound to notify the end user that user input is required while User Credentials input screen is displayed.</p> <p>Condition: User Sign in workflow.</p> <p>Workaround: None.</p>
PRS-410877	<p>Symptom: During Ivanti Secure Access client installation, the installation time exceeds by a noticeable margin.</p> <p>Condition: This is dependent on current load at the endpoint; However, mostly noticeable during all installations and upgrades.</p> <p>Workaround: None.</p>
PRS-410024	<p>Symptom: Sometimes valid error message not shown.</p> <p>Condition: In some scenarios, whenever the MessageCatalog file got into some issue, unable to get the corresponding error message.</p> <p>Workaround: None.</p>
PRS-409774	<p>Symptom: Not able to launch New-UX on Vanilla Windows 20H2 OS Build 19042.1110 and windows server 2022.</p> <p>Condition: During Ivanti Secure Access Client installation or auto-upgrade.</p> <p>Workaround: None, use Classic UI.</p>

Problem Report Number	Summary
PRS-409484	Symptom: Server certificate error is shown repeatedly for untrusted certificates. Condition: When ISAC connects to ICS (Directly \ through Hotspot) having untrusted certificates then certificate exception page will be shown repeatedly. Workaround: End user must click continue to <server> link on the certificate error page.
PRS-409465	Symptom: "This Extension is not trusted by Enhanced Security Browser" warning prompts during the Ivanti Secure Access Extension installation. Condition: While launching or installing the clients via Browser. Workaround: None.
PRS-409302	Symptom: Chromium embedded framework (CEF) based browser will be used by 22.2R1+ clients only during credential provider SAML login. Condition: ISAC connection set is enabled for Embedded browser for Authentication with Edge Webview2 browser engine and credential provider. Workaround: ISAC is already handling the credential provider use case with CEF browser.
PSD-11610	Symptom: Uninstall fails to remove UI component for New-UX client. Condition: During client uninstallation. Workaround: None.
PSD-11560	Symptom: Diagnostic tool is not opening using Ctrl+F2 on New-UX client. Condition: When invoking Diagnostic tool from client. Workaround: Open diagnostic tool manually.
PSD-10736	Symptom: New-UX client controls, labels and text are misaligned clipped. Condition: When client window is resized. Workaround: None.
PSD-10356	Symptom: Auto retry of User Input Timeout is not working in New-UX. Condition: User Input timeout error. Workaround: Manually Retry user input.
PSD-9938	Symptom: Ivanti Secure Access Client not responding after some days of usage. Condition: On Ivanti Secure Access Client usage for some days. Workaround: Restart the application or reboot the system.

Problem Report Number	Summary
PSD-9538	Symptom: Splash screen off setting if selected on the server is not reflecting on the New-UX client. Condition: New-UX fresh launch. Workaround: None.
PSD-8631	Symptom: Memory Usage may gradually increase when using New-UX. Condition: When auto-refresh is enabled. Workaround: Disable auto-refresh.
PSD-8591	Symptom: New-UX client on Windows 2022 Server is not available due to missing dependencies. Condition: When New-UX client is used on Windows 2022 Server. Workaround: None.
PSD-6971	Symptom: Keyboard Navigation is not supported for New-UX client. Condition: When using keyboard navigation. Workaround: None.

Product Codes (GUIDs) for SCCM Deployments

If you deploy Ivanti Secure Access Client using Microsoft System Center Configuration Manager (SCCM, formerly SMS), it can be helpful to know the Product Codes (GUIDs) of Ivanti Secure Access Client installation bundles. SCCM uses these codes to determine whether products are already installed. The table below gives the product codes for the corresponding release of Ivanti Secure Access Client for the given the architecture (32-bit or 64-bit) and locale (language environment).



From 22.7R1 onwards, ISAC do not be support Win32 platform and installation bundles will not include x86 installers.

Language	Product Codes (GUIDs)
Release 22.8R1	
PulseSecure.x64.msi	
English	{38C3F131-9536-4896-8819-F4B1DBC4A10}
Chinese (Taiwan)	{2D6ADC91-9D67-43C2-B640-43E7B822FB5F}
German	{16B9F3F0-81C1-4BF4-A130-3464E29DCE60}
Spanish	{830F838D-AB8B-48D3-BF49-9443B6DE2431}
French	{559B4FB9-797D-4122-85D5-D728B3966DC5}
Italian	{3E28E254-6096-4DC4-A620-79BB6256CCE3}
Japanese	{839E66EB-11CE-4139-9E13-88AF80F72DCE}
Korean	{E58EC2A0-D8E8-4FF1-8A15-100AEDE57B61}
Polish	{A5ED784F-90AB-49F5-A378-AE38B764C503}
Chinese (China)	{3F46A596-62AD-4271-A981-BC627F3A24A7}
Release 22.7R4	
PulseSecure.x64.msi	
English	{307DE272-CE5B-43C1-8A33-DB173A7EA289}

Language	Product Codes (GUIDs)
Chinese (Taiwan)	{C73EE4BC-E50F-44A1-B02F-2CBA0C8A018C}
German	{D32B8C32-017C-497E-AA6E-751BED43A19E}
Spanish	{0BE71D9D-D2CB-421C-9C80-DF272ED1ABF8}
French	{BEF1668A-F37F-482F-B607-1CAFEC3D5D07}
Italian	{C8A322C1-BDAC-43D1-9475-8B97F066DF80}
Japanese	{F6BC4A8E-BACF-4F37-8D83-FEF99CED10B0}
Korean	{8C5A6591-2FF8-49AB-9E4D-CA7E0CC01B36}
Polish	{E5B49D1B-E8C1-4F25-A459-7F8072844AF2}
Chinese (China)	{0663846C-6547-4608-A0A4-7D3A171BD368}
Release 22.7R3	
PulseSecure.x64.msi	
English	{FF1DA951-E681-4031-974E-7D66780AFD32}
Chinese (Taiwan)	{0647129F-05FB-4E26-9DAA-A5AC2466E427}
German	{B888E99B-732C-4643-A4FF-21046112430D}
Spanish	{72F3F325-F068-4F47-9AC1-EAE9872C26D7}
French	{3D4E2A87-F316-4FC0-97D7-40A6E8A51D29}
Italian	{7F535C46-71A5-4F19-8272-A3D9C8B07308}
Japanese	{36A9DD0E-47AB-416F-BEBA-A92413DBACE4}
Korean	{F45CECA4-B9A0-43AD-A0EB-F88FCB4CE67E}
Polish	{1A6F067B-16B2-4448-A782-F9035D9B9659}
Chinese (China)	{0CF2CCF3-6AE9-4C0D-894B-3960C906A432}
Release 22.7R2	
PulseSecure.x64.msi	

Language	Product Codes (GUIDs)
English	{DB2D711D-C598-4080-B68F-4FDFACD13D2D}
Chinese (Taiwan)	{9721FAAD-8DAF-4702-B1BC-48F679A41B08}
German	{D585F321-5BA6-46BA-8882-E83F57ECA1AE}
Spanish	{C1624D1D-7625-4330-9688-313FA8D07B8A}
French	{3A7DC9F4-DC7B-4611-B257-136580C9506F}
Italian	{F3ECFB93-3DDA-4010-9C7D-DA5EA355E820}
Japanese	{6115FCF2-64D9-41F9-ABA5-32C6C3AD6298}
Korean	{3938262A-0814-46CD-B854-F5FD27ACEDA7}
Polish	{0E62322D-5790-41AF-A385-85E3DB5808D4}
Chinese (China)	{9A40EE04-4808-451E-8E00-C35B5E482201}
Release 22.7R1	
PulseSecure.x64.msi	
English	{21D9DE1D-F8FF-45ED-9E78-42CD9A6D4851}
Chinese (Taiwan)	{AD8A78E8-B0FD-4E01-8F53-F0B3AA5876CA}
German	{905ECF99-8408-4BCD-ACDF-F80BFA3FC1F5}
Spanish	{8BAB0CFE-FC51-416C-A4B3-C38DBFEB5BA6}
French	{4D708090-D8D3-4E80-BEC1-0B40557D23CF}
Italian	{EE707187-48A3-409C-8928-6CFB220948F7}
Japanese	{42EB2DE8-E298-4BFC-A2CB-18B621FC9330}
Korean	{7E69B3A3-039F-4E20-8B10-1898B43D8862}
Polish	{24DDA274-DC06-48B2-82CB-207FCDADB38C}
Chinese (China)	{854BF5C8-2074-485C-836E-DCDC46B5A90C}
Release 22.6R1	

Language	Product Codes (GUIDs)
PulseSecure.x86.msi	
English	{DB84DE57-05FE-4D33-A4A6-37FDF7C8D310}
Chinese (Taiwan)	{E4DF4BC5-5933-4BE9-89D4-970E3CD081A4}
German	{F7054C58-1853-4DDD-868A-8791FF39481F}
Spanish	{8E1E2589-3B9C-414F-857F-F8F08EFA2C55}
French	{30947CCF-DF50-4482-AC34-81F17F0CFEFE}
Italian	{DA41DFBC-144C-449D-ABD2-1A61B25082F1}
Japanese	{DF5CF3E4-C505-42E0-AAA0-19A0B6DFE0B1}
Korean	{E32BED46-915C-4371-A0E3-25FC195EF68E}
Polish	{F86B6E8E-3B8E-49A7-9F44-C8CE935C3658}
Chinese (China)	{341C8EA9-108F-47A9-B83D-CC046FE1A88B}
PulseSecure.x64.msi	
English	{0513E7B6-B058-4B6B-A198-F850C5F49C6D}
Chinese (Taiwan)	{F6547D88-2FCC-425D-8F6F-E0F00C905A69}
German	{A55FAE18-7A2A-4722-99DE-E3F5C4FEA564}
Spanish	{D103A5F3-0A8A-4256-8F2D-0053FB036AEF}
French	{12D258BE-0E43-4F95-982A-33AD6BBBF1BA}
Italian	{575667F8-CB4D-4518-8DE3-307C64306CC9}
Japanese	{2FD77C05-18C7-45EA-A7FA-3105400597E4}
Korean	{4F5D1DBE-FE71-46EC-B2BC-D4A1A9F60DCA}
Polish	{9C091EF7-424B-4D66-B577-3707A6437E0A}
Chinese (China)	{29A6AF66-2838-441D-81C2-5D18277426D6}
Release 22.5R1	

Language	Product Codes (GUIDs)
PulseSecure.x86.msi	
English	{7A4EE38D-D694-4BB9-B76A-33387EB1189B}
Chinese (Taiwan)	{DC7E2455-65E5-45C8-94FA-7D95F6E1A151}
German	{C2404EE0-A9E3-46E0-B0E2-A07E85D90602}
Spanish	{30599545-FED2-4A47-BC36-0A98AAAF1DEF}
French	{EC981283-EF60-433C-8B85-3157C7B86043}
Italian	{BD0B82F4-CF7F-435E-B717-71909CE98CE1}
Japanese	{7CBEB940-C10A-4AEE-A45E-B2E702052090}
Korean	{3C44FAD6-0AAA-454F-B3C8-1D91126FBBAE}
Polish	{4379EB27-D42B-4A88-94AA-3E6188E652E5}
Chinese (China)	{3BCA7B63-64A6-4E05-8ECE-DD4390BB9043}
PulseSecure.x64.msi	
English	{BA3A8806-53FB-4F9C-95EF-904CFD2C8192}
Chinese (Taiwan)	{A4770DC5-D6D5-4D99-805D-43F64FBFBD5F}
German	{9F5E50A0-1732-4A17-9BAC-A126EFEB41DD}
Spanish	{CD0D806F-4E49-46FF-8561-05CDC5824F67}
French	{0F353AAF-D3A6-497E-8A99-53556CE818DA}
Italian	{9C6CB838-95E8-41F8-9161-E546B0A63564}
Japanese	{A415E700-07AB-401E-9599-596A23626740}
Korean	{792A529A-25AA-4CB4-9FA5-3244D1B0E7DD}
Polish	{84C087F2-0A19-4E29-9BCC-83F88DAADAD7}
Chinese (China)	{4429376D-D31D-49A3-870C-D46F5F7C1D46}
Release 22.3R3	

Language	Product Codes (GUIDs)
PulseSecure.x86.msi	
English	{6719115C-D5A4-47A5-9DCE-8D313D1FF981}
Chinese (Taiwan)	{E8288AD1-7599-496A-A05F-8F6D789496A8}
German	{79DB9B1B-1A42-4117-A2BD-8068316FCACB}
Spanish	{4A974EB5-90AF-4C3D-9341-535E7E24B4AA}
French	{CA1B874D-1422-4484-B697-5681F1057266}
Italian	{9A00908B-A970-4368-8D81-CCA2973383B8}
Japanese	{FCF7EC0C-6F2E-4590-9897-5AEF23D87780}
Korean	{3B9B63E5-0F11-49D4-BB01-573A1069F13F}
Polish	{E0EAAE0B-74B7-44F3-A981-D19AABB6FFD9}
Chinese (China)	{B3174ADF-9374-484F-A256-53BB2CF2C3E4}
PulseSecure.x64.msi	
English	{B9EFDE88-2F0D-426B-8521-1ADE01A960D8}
Chinese (Taiwan)	{FFCF3D23-5DA4-4500-96EB-1CC786A8B8A0}
German	{E2544AF6-DF35-47C8-8592-5EC3BC105909}
Spanish	{853BA0FD-E417-4990-8787-2A32E7314C5E}
French	{33ABC6F4-B87A-4010-B448-65CCC29DC23E}
Italian	{5333AB2A-0B49-468D-80F3-2AA239AB4FE2}
Japanese	{33E7A12A-E708-4367-AFC5-3460E1461966}
Korean	{BA39B791-DDE9-4BBA-8982-908B775CA7AB}
Polish	{71FB40A4-C91F-4762-93FE-CFD4C9DCF061}
Chinese (China)	{A8F6E901-C1F4-4280-8951-67DA5236AD5D}
Release 22.3R2	

Language	Product Codes (GUIDs)
PulseSecure.x86.msi	
English	{5BE10637-F29F-4051-9C8C-683513C6EED6}
Chinese (Taiwan)	{8B689C04-5DA5-43D9-B5ED-2B0C68A10A5B}
German	{EF55C7DC-D85B-409B-BBD0-CAC2AC7F0B38}
Spanish	{696CE3BE-CD8F-4B4D-9EBE-07418FDCDA05}
French	{39EF62A4-644D-419E-BBF2-0AE4B7719796}
Italian	{987C3524-80AD-4B44-B472-1BCBA627A99E}
Japanese	{2222EA6E-14B8-4CA3-8D7C-EEABD2606718}
Korean	{19B69A5B-3C2B-43EF-9B00-744392D15F84}
Polish	{C46DB6FF-DA76-4EAE-BA14-5CA2359478B3}
Chinese (China)	{1B7E7721-67B1-4560-9580-A026143BA877}
PulseSecure.x64.msi	
English	{486081CA-2D4C-4F94-837E-01B379B3133C}
Chinese (Taiwan)	{C75505FD-6FFA-47A7-A3E0-04015CD03C50}
German	{DE96FE68-665D-4166-95E5-AA5F4D101877}
Spanish	{E3B7C0A7-0924-4466-82B9-64F76EA70DD1}
French	{08A1C28D-65FC-406F-928E-A2B5CE2F112D}
Italian	{CEA853DC-6F4F-41A3-94C4-CB70A273C5F5}
Japanese	{EEE9C393-80DA-4927-9600-911C133A4AE8}
Korean	{1D18D80F-6456-4B55-AF6F-F503D3AB49EE}
Polish	{9B0775B3-3650-41A3-A42A-A2AEE96D2D5F}
Chinese (China)	{4DAC8D05-9FB4-410C-9BC4-DB6FC43B04B1}
Release 22.3R1	

Language	Product Codes (GUIDs)
PulseSecure.x86.msi	
English	{EB1BE1CE-C5D8-4EF2-B8D2-87622ED63A80}
Chinese (Taiwan)	{85221D6B-EB49-4CB1-9B39-C784FA75F24D}
German	{8D83F898-DD5F-4D0C-A51C-059DC2AC9D72}
Spanish	{992EC617-B393-404E-AD9D-644520BCDAC0}
French	{38D4227D-2464-4626-9779-84E0CA391C0D}
Italian	{40F4F506-4D6E-432D-BC08-DFAF52709D20}
Japanese	{0BE5C2C7-3BA0-4E0A-8B02-2C5200B707A4}
Korean	{ABD88E90-DE39-4DD7-9995-34E9B4C4FBCF}
Polish	{E0E58494-0943-4C5E-AF04-BD21BE3B5334}
Chinese (China)	{4C30C791-C02E-4D16-B196-CCDCF5D3A89A}
PulseSecure.x64.msi	
English	{31FD6281-CD18-439F-8970-1F2EDBD9C139}
Chinese (Taiwan)	{73D59F8D-C9A8-4452-8B6F-7D15F2EE633A}
German	{021D93C8-676F-419F-9DBF-02D05DA67464}
Spanish	{03E50D16-AAF5-4BFF-980B-19FE600D2B92}
French	{9274EF41-1330-4A0C-8A31-0A6EEDBE0CC2}
Italian	{1F7418EF-B4A1-4A6D-B6BA-D497FC8E7B6E}
Japanese	{2FE5E463-1D49-428A-83B6-F458F17CB7E2}
Korean	{329EC6FF-084B-4383-83B2-A99F7494F734}
Polish	{4F9DBE29-9FEC-49FC-BE2D-321801D2C642}
Chinese (China)	{0EB07AB9-0218-4395-B1D5-E3ABF6F5E5AC}
Release 22.2R1	

Language	Product Codes (GUIDs)
PulseSecure.x86.msi	
English	{F1C5C420-A0DE-4B3D-86EB-787747A1DCB4}
Chinese (Taiwan)	{2E2ED4E6-9E15-4226-BBA7-F48237437030}
German	{169CE007-DDC4-4821-8A6C-B3B1A02F245B}
Spanish	{90369A50-E63B-4B4A-9EC6-89F9CF9571F8}
French	{95447240-98F4-40B7-BB98-C3BB5D54B382}
Italian	{CF52EBE9-38A5-43CA-A38A-D2A61E7D3A6C}
Japanese	{46513EC4-BED9-4D56-A31B-CBA1AFB197A7}
Korean	{CFD702C4-DDD8-4553-A73D-3A84F3AE0234}
Polish	{8838A4A3-A143-4AC2-A469-71B267EF3FE5}
Chinese (China)	{AB0D6C08-626D-44A6-92D6-3A001589796F}
PulseSecure.x64.msi	
English	{1519A65B-7016-42C6-9213-6BFF49D1F659}
Chinese (Taiwan)	{024DE5E4-7DE1-46E6-902E-022E3EB6A43A}
German	{CA8DA038-8979-470A-89C1-B4A3F8214871}
Spanish	{190C6D0C-8375-47E6-BC73-9ACDE170125C}
French	{5B342340-B6CE-4514-84B1-942BC36778FD}
Italian	{6C9D927B-D59F-466A-A629-663B19087A44}
Japanese	{6B599EA7-E458-449E-88AA-F91E23E83FF4}
Korean	{CB8FB4BB-29CD-4042-8B2B-CCE63FB99BFD}
Polish	{19F91F39-17A0-494B-8820-D2698693B530}
Chinese (China)	{2BECB654-0804-4BA3-AACD-28BA7FF28F1F}

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 Ivanti Support Center:

- <https://forums.ivanti.com/s/welcome-pulse-secure>
- support@ivanti.com

Call us at +1-888-253-6201

For more technical support resources, browse the support website <https://forums.ivanti.com/s/welcome-pulse-secure>.