Ivanti Neurons for Zero Trust Access

Release Notes

v22.3R4

Published	Feb 15, 2023
Document Version	1.0
Document Build	Update-22.3R4-ICS-RN 4886188

Ivanti
10377 South Jordan Gateway
Suite 110
South Jordan, Utah 84095
https://www.ivanti.com

END USER LICENSE AGREEMENT

Contents

Release Notes v22.3R4

Introduction

Ivanti Neurons for Secure Access (nSA) v22.3R4 contains a number of functionality enhancements and bug fixes.

nSA is a cloud-based SaaS (Software as a Service) application that provides fully-managed zero-trust authentication and access control for an organization's application infrastructure. To learn more about nSA operation and administration, refer to the Ivanti Neurons for Secure Access documentation. For more details, see *Documentation and Technical Support* (page 18).

Note: If the information in these Release Notes differs from the information found in the online documentation, refer to the Release Notes as the source of the most accurate information.

Client, Platform & Gateway Version Support

Client Versions Supported In This Release

The Ivanti Secure Access Client Desktop/Mobile versions listed below are the supported versions to use with Ivanti Neurons for Secure Access for this release.

TABLE 1.1 : Clients Supported

Client	Recommended Versions	Supported Versions
macOS	22.3R1-18209	22.3R1-18209 22.2R1-1295 9.1R14-15521 9.1R13-13865
Windows	22.3R1-18209	22.3R1-18209 22.2R1-1295 9.1R14-15521 9.1R13-13865
Linux	22.3R1-18209	22.3R1-18209 22.2R1-1295 9.1R14-15521 9.1R13-13865
Android	22.3.1(r824030.23)	22.3.1(r824030.23)
iOS Client	22.3.1(91069)	22.3.1(91069)

Platforms Supported In This Release

The platform OS and browser versions listed below are supported for this release.

TABLE 1.2 : Platforms Supported

Platform	Operating System	Web Browser
Windows	nSA is compatible with: • Windows 11 22H2 • Windows 10 22H2 • Windows 10 Version 20H2 • Windows 10 Version 2004 • Windows 10 Version 1909 • Windows 11 • Windows 8.1 Enterprise, 64 bit • Windows Server 2012 and 2016	nSA is compatible with: • Chrome 103.0.5060.53(64-bit) • Firefox 102.0.1 (64-bit) • Edge 103.0.1264.44 (64bit)

Continued on next page

TABLE 1.2 – continued from previous page

Platform	Operating System	Web Browser
macOS	nSA is compatible with: • macOS 10.15.6, 64 bit • macOS 10.15.1, 64 bit • macOS 10.14, 64 bit • macOS 10.13, 64 bit • macOS Big Sur 11.0.1, 64 bit • macOS Monterey 12.0.1, 64 bit • macOS Ventura 13.0	nSA is compatible with: • Safari 15.2, 14.1.2, 13.1.2, 12.x • Chrome 103.0.5060.114 (x86_64) • Firefox 102.0 (64-bit) • Edge 103.0.1264.51 (64bit)
Linux	nSA is compatible with: • Ubuntu 18.04 LTS • Ubuntu 18.04.1 LTS • Ubuntu 18.04.2 LTS • Ubuntu 20.04 LTS (fully supported) • Ubuntu 20.04.1 LTS • Fedora 32 • Fedora 31 • Fedora 34 • Debian 10 • Centos8/RHEL8	nSA is compatible with: • N/A
Android	nSA is compatible with: • Android 13 • Android 12 • Android 11 These were tested on: • One Plus 6 • Samsung Galaxy S10 • Samsung Galaxy S20 • Samsung Galaxy S21 • Samsung Galaxy Note 10 • Google Pixel 6 • Google Pixel 5	nSA is compatible with: • Chrome • Firefox • Duckduckgo Ensure that you use the latest versions of your browser for your operating system.
iOS	nSA is compatible with: • Qualified: – iPhone 15.7, 15.7.1,15.5,16.0,16.1 – iPad 14.7.1 • Compatible: – 15.x, 14.x, 13.x	nSA is compatible with: • Safari • Chrome Ensure that you use the latest versions of your browser for your operating system.

ZTA Gateway Versions Supported In This Release

The ZTA Gateway versions listed below are the supported versions to use with nSA for this release.

Note: For details pertaining to Ivanti Connect Secure (ICS) Gateways, refer instead to the "ICS Gateway Release Notes".

TABLE 1.3 : ZTA Gateway Versions Supported

Gateway	Recommended Versions	Supported Versions
ZTA Gateway	22.3R4-883 22.3R1-821	22.3R4-883 22.3R1-821 22.2R1-361 22.1R1-75 21.12R1-95

Usage of ZTA Gateway from nSA Versions Prior to 20.10

If you are using a base ZTA Gateway image supplied with nSA versions earlier than v20.10, the license agreement prompt can appear on the Gateway console following a reboot causing the Gateway to appear as unavailable until the agreement is accepted. If you encounter this issue, replace the Gateway with a new instance at the latest available version.

ZTA Gateway Templates Supported In This Release

Note: Download a local copy of the Gateway template files listed here and save to a location that is accessible from the hypervisor or cloud management interface you are using. Refer to the *Tenant Admin Guide* for full details of how to deploy your Gateways.

- **On-Premises VMware vSphere**:

  The following OVF template is applicable to this release:

  https://pulsezta.blob.core.windows.net/gateway/ISA-V-VMWARE-ZTA-22.3R4-883.1.zip

- **On-Premises KVM**:

  OpenStack distribution qualified: OpenStack Stein release.

  The following KVM template is applicable to this release:

https://pulsezta.blob.core.windows.net/gateway/ISA-V-KVM-ZTA-22.3R4-883.1.zip

- **Amazon Web Services (AWS)**:

  The following JSON template files are applicable to this release:

  - To deploy in an existing VPC:

    Nitro Hypervisor

    https://pulsezta.blob.core.windows.net/gateway/templates/AWS/23-2-883/Nitro/ivanti-zta-2-nics-existing-vpc.json
    https://pulsezta.blob.core.windows.net/gateway/templates/AWS/23-2-883/Nitro/ivanti-zta-3-nics-existing-vpc.json

  - To deploy in a new VPC:

    Nitro Hypervisor

    https://pulsezta.blob.core.windows.net/gateway/templates/AWS/23-2-883/Nitro/ivanti-zta-2-nics-new-network.json
    https://pulsezta.blob.core.windows.net/gateway/templates/AWS/23-2-883/Nitro/ivanti-zta-3-nics-new-network.json

  ZTA Gateway AMIs are available in all AWS regions (except China). To obtain the AMI applicable to your region, follow these steps:

  1. Log into the AWS console.
  2. Navigate to **EC2 > Images > AMIs**.
  3. Select "Public Images".
  4. Search for the image corresponding to your selected hypervisor:
     - Nitro: ISA-V-NITRO-ZTA-22.3R4-883.1-SERIAL-nitro.img
  5. Make a note of the corresponding AMI ID.

- **Microsoft Azure**:

  The following JSON template files are applicable to this release:

  - To deploy in an existing VNET:

    https://pulsezta.blob.core.windows.net/gateway/templates/Azure/23-2-883/ivanti-zta-2-nics-existing-vnet.json
    https://pulsezta.blob.core.windows.net/gateway/templates/Azure/23-2-883/ivanti-zta-3-nics-existing-vnet.json

  - To deploy in a new VNET:

    https://pulsezta.blob.core.windows.net/gateway/templates/Azure/23-2-883/ivanti-zta-2-nics.json https://pulsezta.blob.core.windows.net/gateway/templates/Azure/23-2-883/ivanti-zta-3-nics.json

  The following Azure VHD images are applicable to this release. Use the link most suitable for your geographic location:

  - Americas:

https://pulsezta.blob.core.windows.net/gateway/ISA-V-HYPERV-ZTA-22.3R4-883.1-SERIAL-hyperv.vhd

  - APJ:

    https://pulseztaapj1.blob.core.windows.net/gateway/ISA-V-HYPERV-ZTA-22.3R4-883.1-SERIAL-hyperv.vhd

  - Europe:

    https://pulseztaeurope.blob.core.windows.net/gateway/ISA-V-HYPERV-ZTA-22.3R4-883.1-SERIAL-hyperv.vhd

- **Google Cloud Platform**:

  The following template files are applicable to this release:

  - To deploy in an existing VPC:

    https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-2-883/ivanti-zta-2-nics-existing-vpc.zip
    https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-2-883/ivanti-zta-3-nics-existing-vpc.zip

  - To deploy in a new VPC:

    https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-2-883/ivanti-zta-2-nics-new-vpc.zip
    https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-2-883/ivanti-zta-3-nics-new-vpc.zip

  The following GCP gateway image is applicable to this release:

  https://pulsezta.blob.core.windows.net/gateway/ISA-V-GCP-ZTA-22.3R4-883.1.tar.gz

What's New

22.3R4

- Management port support on ZTA Gateway. With this feature, ZTA Gateway can use management interface to communicate with controller and NTP Server.

22.3R1

- Optimal Gateway Selection (OGS)
- End User UX Improvements
- Simplified Configuration Users and Secure Access Policy configurations
- Actionable Insights: Step up Authentication, Subsequent login and Chart Visibility
- Device Risk Assessment: RiskSense integration, Default Device Policy
- Application Visibility Improvements: Secure Access Policy for discovered applications

- Lookout SWG/CASB Forward Proxy integration
- External Browser support
- Minimum Client Version
- Lock Down mode support
- PSAL with Browser Extension

For a list of the issues resolved in this release, see the information that follows.

Important Notice for v22.1R1 and Later

nSA 22.1R1 includes updates to address the OpenSSL vulnerability described in CVE-2022-0778. Ivanti recommends upgrading your Gateways and Clients to the *Recommended Version* listed in this document at your earliest convenience.

Limitations

The following limitations apply to this release:

- Okta and PingID SAML authentication methods are supported for Ivanti Secure Access Client MacOS and Windows variants only.
- Each application can only be accessed with ping/SSH using the addressing method specified when registering it. That is, if you registered the application using an FQDN, you cannot access it using an IP address.
- PZT-24825: Tenants wanting to use their own Public Key Infrastructure with device certificates (known in this document as BYOC - Bring Your Own Certificate), the following limitations apply:
  - For existing tenants, to convert from a non-BYOC tenant to a BYOC tenant is not supported. This is supported only for newly-created tenants.

    Note: After tenant creation, the admin must configure the tenant as BYOC before registering a gateway or enrolling an end-user device.
  - For existing tenants, to convert from a BYOC tenant to a non-BYOC tenant is not supported as the tenant needs at least one customer CA.

    Note: If all customer CAs are removed after gateways or devices have been enrolled, those existing gateways and devices will not function properly.
  - A CA is not permitted to be used by more than one BYOC tenant.

Upgrading Ivanti Secure Access Client Windows Variants to Version 21.6 or Later

Ivanti is aware that Windows-based desktop devices that have Ivanti Secure Access Client installed from a previous nSA release (9.1R11 and earlier) can fail during

upgrade to the version applicable to nSA release 21.6 or later. This is due to a certificate expiry issue in the client.

To remedy this situation, please refer to the instructions and helper files contained at https://pulsezta.blob.core.windows.net/client/21.6/Pulse_Client_Upgrade_Helper.zip

Note: Administrators using Microsoft Intune for MDM services should instead refer to this document: https://pulsezta.blob.core.windows.net/client/21.6/Intune_Pulse_client_Upgrade.docx

Fixed Issues

The following table describes the issues resolved.

TABLE 1.4 : Fixed Issues

Problem Report	Description
Release 22.3R4	
PZT-36792	If a SAP is created with stand-alone non-ready gateways then that can trigger skipping of all the applications that have OGS.
PZT-37610	When Admin navigates to SAP page and expands two App groups, same Apps are shown for both App groups.
PZT-37611	When Admin navigates to SAP page, performing App group expansion and changing records per page leads to disappearance of expand option in SAP policy groups.
Release 22.3R2	
PZT-37228	Error while loading the Secure Access Policies page.
Release 22.3R1	
PZT-26902	Dynamic tunnel IP: NAT rules are not seen on Gateways when a newly added Gateway is added to a Gateway Group.
PZT-29624	The MSP admin portal UI is throwing an error when kept idle, and then not redirecting to the login page.
PZT-31679	An unregistered Gateway's status should show as Offline in the "Gateway By Status" chart drill-down view when log grouping is applied, and also on the Landing page gateway detailed view.

Continued on next page

TABLE 1.4 – continued from previous page

Problem Report	Description
PZT-32217	Search API triggered multiple times with different payload due to which the logs are not getting filtered intermittently when navigating from Insight Logs to Gateway Logs and vice-versa.
PZT-33284	If SAML user authentication is configured before enabling a custom domain, the SAML policy remains configured with the standard domain URL.
PZT-35770	nZTA:Invalid Client Certificate Error 1147 is seen during user connection.
PZT-36790	No alert generated for Policy configured on Enrollment URLs.
PRS-412051	The user is prompted multiple times to switch to the new UI when upgrading Ivanti Secure Access Client.
Release 22.2R1	
PZT-15594	Client configuration: Disable Splash screen option is not working.
PZT-22198	Mac Intune Client is not launching automatically after the client installation.
PZT-23470	CEF EUP on mac: With system local auth, some SSO apps are not launching with Safari as the default system browser, with a certificate prompt appearing twice.
PZT-24993	Linux Windows multi sign-in: Changing the user sign-in URL from one URL to another is not prompting for fresh credentials.
PZT-26431	Certificate rotation on macOS: When the device certificate expires and the end-user attempts to connect, "Error 1151" is not prompting properly.
PZT-27640	Summary ribbon tile charts are not aligned properly.
PZT-28838	Gateways Overview: An L4 dashboard should display only the chart and table data based on the drop-down selected on the originating L2 dashboard chart. For example, selecting to view "Major Errors" should not show other error severity levels in the L4 view.
PZT-28841	Logs in the Gateways Overview L4 dashboard for the "Gateway Stats" chart shows only the current state (active view) logs despite the parent L2 dashboard page having a non-active view time period set.
PZT-28844	Unable to use the group-by feature with all the keys on the Gateways Overview L4 dashboards of "Top 10 gateways by Errors", "Access Trend" and "Gateway Stats".

Continued on next page

TABLE 1.4 – continued from previous page

Problem Report	Description
PZT-29143	Unable to filter and search with "Gateway Status" set to "offline" and "Gateway Version" set to "pre-22.1" on the Gateways Overview L4 dashboard of "Gateway Stats".
PZT-29281	Gateways Overview "Top 10 Gateways by Health" chart displays the gateway statistics only for pre-22.1 ZTA Gateways for "Previous Day" and "Previous Week" historic views.
PZT-29811	Log Export might fail if the number of logs to be exported is more than 400K.
PZT-32742	Gateways older than the version provided with nZTA 22.2R1 are entering a bad state due to the inability to apply journal updates. After 15 minutes, the Gateway will do a full config pull and recover.
Release 22.1R1	
PZT-21416	EUP: Accessing RDP and SSH application links does not pick the default application installed on the device.
PZT-21813	Regression - Bookmarks API Response is fluctuating between 200 success and 500 error HTTP response codes under certain scenario.
PZT-24098	Global Device Preferences - the nZTA client is not honoring "Allow Delete Connection".
PZT-24546	Multi sign-in URLs: Login behavior is different for Ivanti Secure Access Client with standard login and non-standard multiple sign-in login URLs when no Secure Access Policy (SAP) is configured on the nSA Controller.
PZT-27300	In a location device rule, it is not possible to update the City field by just typing locations rather than selecting them from the drop-down list fields.
PZT-27538	Date-picker is popping out of the main dashboard on the Connected Clients chart L4 detailed logs page, as the title of the chart is long.
PZT-27546	Policy Failure page summary strip is populated by data for the previous day when the weekly historic view is selected.
PZT-27593	Configuring a SAML auth server using the manual method while leaving "IDP Slo Service" field empty can cause a 500 status code error.
PZT-27743	Due to low network bandwidth availability, upgrading a Gateway to the 21.12R1-95 build fails (the event logs shows "HTTP error 409 after PUT" messages continuously).

Continued on next page

TABLE 1.4 – continued from previous page

Problem Report	Description
PZT-27999	CA rotation breaks leaf renewal for Ivanti Secure Access Client 21.9.3 12679.
Release 21.12R1	
PZT-26604	Sessions are not timing out on the Controller even when there is no corresponding user session on a client device.
PZT-27416	Handle the Policy Failure by Locations chart visibility on Policy failures page.
Release 21.6R1	
PZT-20309	Error while installing the client.
Release 21.1R1	
PZT-15937	”dsunitytaskd” process failed in ESXI 189 gateway while upgrading to 131.
Release 20.12R1	
PZT-15533	Client Configuration - Save User credentials option does not work.
Release 20.10R1	
PZT-10907	Configuring single user rule to match multiple values is not supported.
Release 20.9R1	
PZT-11677	SAML Authentication fails if the azure metadata is uploaded for first time.

Known Issues

The following table describes the open issues with workarounds where applicable.

TABLE 1.5 : Known Issues

Problem Report	Description
Release 22.3R4	
PZT-31655	**Symptom**: MFA Support : signing in an older version client through a MFA device policy with TOTP enabled causes a *loading components* page or loop after TOTP registration in the end-user portal. **Workaround**: TOTP is supported for client versions applicable to the 22.2R1 release only. Make sure your client software is up-to-date.
PZT-35144	**Symptom**: Admin rules cannot be deleted when attached to an admin group. **Workaround**: Select only rules that are not associated with any admin groups for deletion.
PZT-35194	**Symptom**: Applications page lacks row level actions. **Workaround**: Scroll to top after selection to edit/delete.
PZT-36050	**Symptom**: Sign in button is visible for the end user even when the UEBA score has crossed the threshold and user is denied login. **Workaround**: N/A
PZT-36753	**Symptom**: Subscription page gateway filters don't work under some conditions. **Workaround**: None
PZT-36884	**Symptom**: Sankey chart does not show the exact path for application being accessed with respect to user group. **Workaround**: N/A
PZT-37424	**Symptom**: When ICS and ZTA components already 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. **Workaround**: Deep clean endpoint with all client components and do fresh installation.
PZT-37536	**Symptom**: Non-compliance cards not seen on the Analytics Dashboards for Application types - SSH, Telnet, RDP and IPv4. **Workaround**: N/A
PZT-37765	**Symptom**: Authentication URL gives error as 'SAP is not configured' when trying to open from browser. **Workaround**: Navigate to Secure Access > Manage Users > User Groups. Edit the user group and save it again.

Continued on next page

TABLE 1.5 – continued from previous page

Problem Report	Description
PZT-37803	**Symptom**: The page appears broken when visiting Gateway Logs in Chrome browser. **Workaround**: Please follow these steps in your Chrome browser: 1. Go to chrome://settings/system. 2. Enable hardware acceleration by clicking on the "Use hardware acceleration when available" switch. 3. Relaunch the browser.
PZT-37841	**Symptom**: Report format CSV/JSON has the epoch timestamp instead of human readable. **Workaround**: N/A
PZT-37912	**Symptom**: Auth Failure messages with the username as SYSTEM are observed in the Top Auth Failures chart on L2 All Users Dashboard when authentication method is SAML and the user has crossed the UEBA threat score threshold configured as a part of Actionable Insights. **Workaround**: N/A
PZT-37966	**Symptom**: When IP resource is added with FQDN sub-domain, FQDN sub-domain is not sent for the client. **Workaround**: Add FQDN as main resource and add IP as sub-domains.
PZT-37981	**Symptom**: Time Of Day Device policy cannot be enforced while creating Secure Access Policy when gateway selectors are used. **Workaround**: Use standalone gateways or gateway groups instead of gateway selectors.
PZT-38101	**Symptom**: If 22.2R1 or below version of gateways are present & OGS feature is configured, older gateways may not go to ready state. **Workaround**: Upgrade gateways to 22.3R1 and above to use OGS feature.
PZT-38173	**Symptom**: User name with %40 is shown in Tenant access log when SAML-based authentication and device policy are enabled at Secure Access Policy (SAP). **Workaround**: N/A
Release 22.3R3	
PZT-6921	**Symptom**: After un-enrollment of nZTA profile, the VPN connection should be disconnected instantly and the profile should be removed from Ivanti Secure Access Client. **Workaround**: Open Ivanti Secure Access Client and move between the screens. A pop-up message should appear warning that the certificate is revoked. The profile is removed automatically.

Continued on next page

TABLE 1.5 – continued from previous page

Problem Report	Description
PZT-7581	**Symptom**: nZTA VOD: Ivanti Secure Access Client is not notifying the end user when Notification is turned off. **Workaround**: Enable Notification for the Ivanti Secure Access Client in iOS Device settings.
PZT-8610	**Symptom**: Simultaneous connections: After switching to a new user, Ivanti Secure Access Client shows the nZTA enrollment details. **Workaround**: N/A
PZT-8740	**Symptom**: OS check for Android is failing while updating the policy dynamically. **Workaround**: None
PZT-8866	**Symptom**: Dynamic policy update is not working when the same iOS OS device policy is updated for deny and allow access. **Workaround**: None
PZT-9926	**Symptom**: ESAP Upgrade for nZTA sometimes does not work when classic VPN and nZTA connections use different ESAP versions. **Workaround**: Make sure classic VPN and nZTA connections use the same ESAP version.
PZT-9979	**Symptom**: Captive portal detection is not working with nZTA connection. **Workaround**: Open a browser window. The user should then be re-directed to the Captive portal for Guest authentication.
PZT-10287	**Symptom**: Resource access is not going over nZTA when chrome is enabled with Secure DNS feature. **Workaround**: Disable the Secure DNS option on chrome settings or use the DNS server which supports 443. https://en.wikipedia.org/wiki/Public_recursive_name_server
PZT-10340	**Symptom**: [Windows] Simultaneous connections: With the bng-vpn and nZTA (corporate) connections both active, Microsoft Outlook is not reachable. **Workaround**: N/A
PZT-10600	**Symptom**: [Windows] nslookup with non-nZTA FQDNs is always forwarded to the ZTA Gateway DNS server. **Workaround**: N/A
PZT-10946	**Symptom**: 9.2.0 nZTA On-Demand : nZTA will be triggered only when the per-app application is being used to access the nZTA resources. **Workaround**: N/A (Use Classic Per-app VPN applications to access the nZTA resources to get connect with nZTA).

Continued on next page

TABLE 1.5 – continued from previous page

Problem Report	Description
PZT-10971	**Symptom**: 9.2.0 nZTA Transition : Update MDM profile and push disconnects the nZTA connection. **Workaround**: N/A (MDM always set its latest update configuration as default and it is limitation).
PZT-12681	**Symptom**: Ivanti Secure Access Client for Windows 10 prompts for credentials when the device is unenrolled. **Workaround**: Post-enrollment, wait for approximately 2 minutes and try to connect to the nSA controller. The user will get the Certificate revoke message, and after accepting the warning the nZTA profile and certificates are deleted.
PZT-14224	**Symptom**: If you have a classic OnDemand VPN connection and your nZTA connection is in monitoring mode, when you attempt to access a nZTA resource, Ivanti Secure Access Client connects to the classic OnDemand VPN profile and displays a transition notification to the user. **Workaround**: N/A
PZT-14316	**Symptom**: ZTA Gateway fails with *Error-1111* when a classic VPN fails to resolve the ZTA Gateway FQDN. **Workaround**: The user must disconnect both classic and nZTA connections, then connect nZTA first followed by the classic VPN. Alternatively, set the client DNS IP address to public to facilitate resolving classic and nZTA connections.
PZT-14581	**Symptom**: When Ivanti Secure Access Client for Desktops is uninstalled, stale certificates are not cleaned up. **Workaround**: Manually delete certificates from the Cert/Key Store.
PZT-15072	**Symptom**: The AAA service should send only one alert for one object error. **Workaround**: N/A
PZT-15278	**Symptom**: Client config- Mac- Delete and Add connection not allowed, but the Add and Delete button is not shown as disabled. **Workaround**: N/A
PZT-19786	**Symptom**: Login not happening immediately after resetting password for account lock cases. **Workaround**: N/A

Continued on next page

TABLE 1.5 – continued from previous page

Problem Report	Description
PZT-20681	**Symptom**: "subject_name_format" and subject_name" SAML attributes are displayed under the SAML config table, and custom attributes are displayed under the SAML app attributes table as expected. Once configured, these attributes are not deleted even if the admin tries to delete them through the UI. We are still allowing deletion since we have to allow the admin to change the values if needed. **Workaround**: N/A
PZT-23409	**Symptom**: CEF EUP on mac: Network error message is thrown in the CEF-based EUP post-authenticating with nZTA. **Workaround**: Close the CEF portal and launch it again.
PZT-25360	**Symptom**: Gateway service REST API: Dynamic tunnel configuration values are incorrectly exposed. **Workaround**: Updated APIs are targeted to be made available in v21.11.
PZT-26083	**Symptom**: A resource or application is intermittently not accessible when the nZTA connection resumes from the Connect-Idle state. **Workaround**: Close the web browser and Launch the application through the nZTA end-user portal.
PZT-26394	**Symptom**: In some scenarios, logs are not visible in the Controller for an ESXi gateway. **Workaround**: Perform a warm restart of the Gateway from the console.
PZT-26399	**Symptom**: Ivanti Secure Access Client sometimes gets stuck in a connect requested state. **Workaround**: N/A
PZT-27820	**Symptom**: Windows 11: An internet application is blocked when the same DNS IP address is configured on both the client device's physical network interface and in the ZTA Gateway DNS settings. **Workaround**: Use a different DNS IP address for the physical interface and for the ZTA Gateway DNS settings.
PZT-29002	**Symptom**: Manual configuration of a SAML authentication server is not supported with Gateways older than v21.12. **Workaround**: Upgrade all Gateways to v21.12 or later. Alternatively, for Gateways older than v21.12, use only the metadata file based configuration method.
PZT-29280	**Symptom**: In some circumstances, Gateways are not being automatically upgraded as per the configured maintenance schedule. **Workaround**: If a scheduled update fails, update the Gateway manually.

Continued on next page

TABLE 1.5 – continued from previous page

Problem Report	Description
PZT-31744	**Symptom**: Application Groups filter is not shown correctly and is hidden behind another panel. Unable to view the filtered application fully in the chip below. **Workaround**: None
PLD-952	**Symptom**: Unable to take a nZTA connection to the state where On-Demand functionality is initiated. **Workaround**: N/A
Release 22.3R1	
PZT-27457	**Symptom**: Policy failure dashboard shows compliance and network rule failures when any one of the rule is passing on the client machine having a common policy enforced which comprises of network and compliance rules together. **Workaround**: None
PZT-34006	**Symptom**: Even when default policy evaluation fails, controller to client connection will be intact and not disconnected. **Workaround**: None
PZT-35683	**Symptom**: CARTA Message appears in Client Window, while searching any Non Compliance application in search engine. **Workaround**: Disable this prefetching feature in the browser (For example, Google Chrome).
PZT-36083	**Symptom**: ISAC Uninstallation will be stuck with Certificate deletion prompt on Windows for nZTA connections. **Condition**: On uninstalling ISAC with nZTA client connection. **Workaround**: None
PZT-36623	**Symptom**: Allowed domains added under any configured application shows IP address instead of the application name when accessed on Analytics dashboards. **Workaround**: None
PZT-36639	**Symptom**: Session Details not reported on nSA and logs are not generated. **Workaround**: None. Do not edit the JSON filter manually.
PZT-36750	**Symptom**: Lockdown enable/disable done on tenant, taking 3-9 minutes to reflect in client connstore.dat file. **Condition**: When we make changes with respect to lockdown in the tenant. **Workaround**: None

Continued on next page

TABLE 1.5 – continued from previous page

Problem Report	Description
PZT-36813	**Symptom**: Risk Sense evaluation for Windows 10 22H2 endpoints is returning as 'Not Available'. **Workaround**: Install any VLC app.
PZT-36911	**Symptom**: Top Risky Applications chart does not show any data when gateway filter is applied on All Users dashboard. **Workaround** : N/A
PZT-36976	**Symptom**: Internet Traffic might be blocked during nZTA reconnection after recovering from sleep. **Workaround**: Restart the dsAccessService using Activity monitor or restart the machine.
PZT-36977	**Symptom**: nZTA connection shows "Limited connectivity" and "Invalid client Certificate" messages. **Workaround**: In the Ivanti Secure Access Client UI, delete the nZTA connection and then add the connection manually.
PCS-38630	**Symptom**: Upgrade from pre-22.3R1 to 22.3R1 appears to be stuck after importing system data. **Condition**: When upgrading the gateway from pre-22.3R1 to 22.3R1. **Workaround**: The issue is seen due to increase in ICS package size. Refer https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44877/?kA13Z000000L3Z5
PCS-39165	**Symptom**: For realms with TOTP enabled as secondary auth server. Authentication may fail with an Internal error occurred log. **Workaround:** • Go to Users Realm > Realm Name > Secondary Auth server. • Select any other Auth server available in the list and save. • Select the previously selected Auth server.
PCS-39291	**Symptom**: When Home Icon in Floating tool bar is clicked, the end-user gets "The page you requested could not be found" error. **Conditions**: When the user clicks on Home Icon in the floating tool bar within an Advanced HTML5 session. **Workaround**: Clear the browser cache and re-try.

Documentation and Technical Support

nSA documentation for administrators is available from the Tenant Admin portal. If you are an administrator, login to the portal using the URL provided in your welcome email after setting up your product subscription. To access product help and documentation links, click the "?" help icon in the navigation bar:

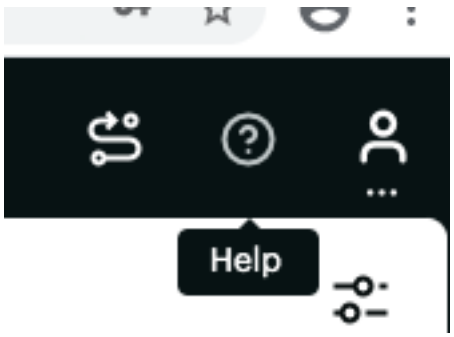

FIGURE 1.1 : For documentation links, click the Help icon in the navigation bar.

From the drop-down list of Help options, click "Go to NZTA Documentation":

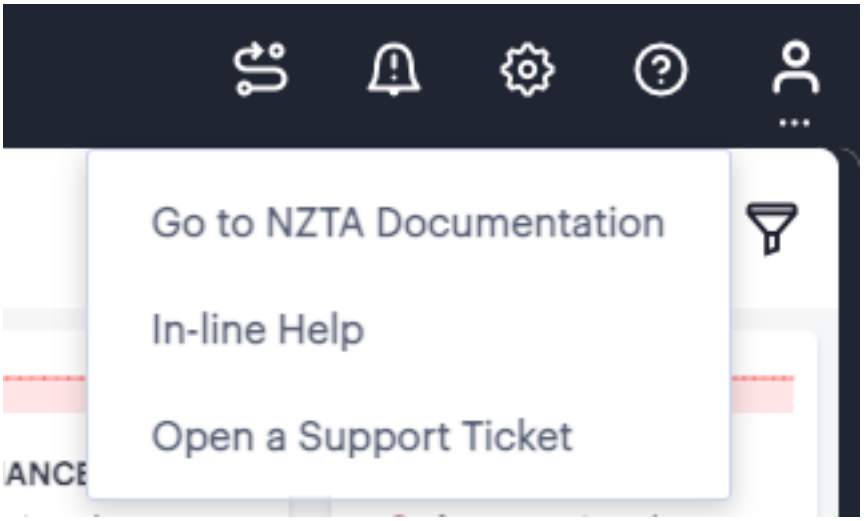

FIGURE 1.2 : Select the "Go to NZTA Documentation" option

The nSA documentation cover page opens in a separate browser window. Use this page to browse through the available guides.

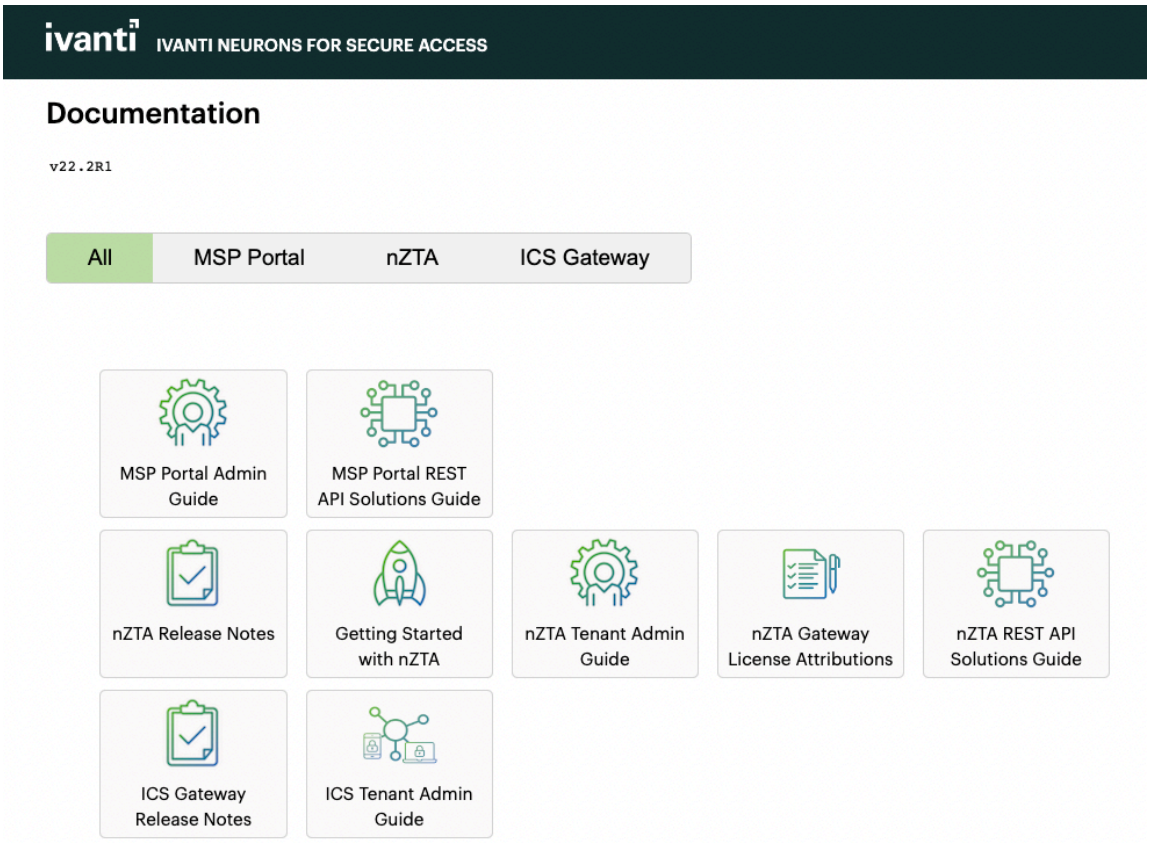

FIGURE 1.3 : The nSA documentation cover page

Note: To access nSA documentation, you must be logged in to the Tenant Admin portal.

For other Ivanti products, documentation is available at https://help.ivanti.com/

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@pulsesecure.net. Find CSC offerings: https://support.pulsesecure.net

Technical Support

When you need additional information or assistance, you can contact Ivanti Technical Support:

- https://support.pulsesecure.net
- support@pulsesecure.net

- Call us at 1-844-751-7629 (toll-free USA)

Revision History

The following table lists the revision history for this document.

Revision	Revision Date	Description
1.4	November 2022	22.3R1 release notes
1.3	October 2022	22.2R5 release notes
1.1	October 2022	22.2R4 release notes created
1.0	July 2022	22.2R1 release notes created