nZTA Release Notes

22.8R1.3

Copyright Notice

Contents

Revision History

The following table lists the revision history for this document.

Revision	Revision Date	Description
3.4	May 2025	22.8R1.3 Release Notes created Updated "Support and Compatibility" on page 14
3.3	April 2025	22.8R1.2 Release Notes created Updated "Support and Compatibility" on page 14 and "Resolved Issues" on page 18 .
3.2	February 2025	22.8R1.1 Release Notes created Updated "Support and Compatibility" on page 14 and "Resolved Issues" on page 18 .
3.1	January 2025	22.8R1 Release Notes created Updated "Support and Compatibility" on page 14
3.0	November 2024	22.7R1.6 Release Notes
2.9	October 2024	22.7R1.5 Release Notes
2.8	August 2024	22.7R1.4 Release Notes
2.7	July 2024	22.7R1.3 Release Notes created Updated the following topics: What's New Support and Compatibility Limitations Resolved Issues Known Issues
2.6	June 2024	22.7R1.2-HF2 Fixed issues list is updated.
2.5	May 2024	22.7R1.2 Release Notes created
2.4	March 2024	22.7R1 Release Notes created
2.3	February 2024	22.6R1.7 Release Notes created

Revision	Revision Date	Description
2.2	February 2024	22.6R1.6 Release Notes created
2.1	January 2024	22.6R1.5 Release Notes created
2.0	November 2023	22.6R1.2 Release Notes created
1.9	October 2023	22.6R1 Release Notes created
1.8	July 2023	22.5R1 Release Notes created
1.7	June 2023	22.4R3 Release Notes created
1.6	April 2023	22.4R1 Release Notes created
1.5	February 2023	22.3R4 Release Notes created
1.4	November 2022	22.3R1 Release Notes created
1.3	October 2022	22.2R5 Release Notes created
1.1	October 2022	22.2R4 Release Notes created
1.0	July 2022	22.2R1 Release Notes created

What's New

22.8R1.2

This release includes bug fixes. There are no new features.

22.8R1.1

This release includes bug fixes. There are no new features.

22.7R1.6

- **Admin experience enhancements**: "Group by" option is added in the Gateway List page to filter the list based on Gateway Type, Connection status, Version or Region.

22.7R1.4

- **Admin UI user experience enhancements**: Column reordering is newly added in the Users L3 and L4 pages. To move a column, a user can click the header and drag to its new position. For more details, see Using the Insights Menu to Monitor User Activity and Service Usage.

22.7R1.3

- **Consolidated landing page**: Drill down support for the Sankey chart is newly added on the consolidated landing page. With each chart, the View all link provides a page with detailed log records for that category. For more details, see Consolidated Landing Page, see Consolidated Landing Page.
- **All Gateways Counter**: - All Gateways counter is newly added on ZTA and nSA specific analytics landing page. For more details, see Reviewing Your Network Activity.

22.7R1.2

- **(Preview) Consolidated landing page**: A new unified landing page allows tenant admin to examine the shared Analytics tables and charts for nZTA and ICS Gateways. For more details, see Consolidated Landing Page.
- **Admin UI user experience enhancements**: Improvements to the admin experience (Modernize the table view for session management and log view). Advanced filter on the page for managed users. For more details, see:

  - Checking the Logs
  - Viewing Gateway Logs
  - Viewing and Terminating User Sessions

- **Sync Now**: A new Sync Now page allows the tenant admin to implement changes made and correct any configuration problems based on the alerts. For more details, see Synchronizing the Configuration.

22.7R2

22.7R2 ZTA Gateway version is the security hardened version with CentOS updates.

22.7R1

- **Configurable MTU size for gateways**: Tenant admin can now define MTU size for ZTA gateways depending on their requirements and underlying network infrastructure.

For details, see:

  - Adding a VMware vSphere Gateway
  - Adding an AWS Gateway
  - Adding an Azure Gateway
  - Adding a KVM Gateway
  - Adding a GCP Gateway
  - Adding an Oracle Gateway

- **Password Strengthening for Local Authentication Server**: The local authentication server has stronger password restrictions. For details, see Workflow: Creating a Local Authentication Policy.
- **Renewed ZTA IDP metadata in release 22.7R1**: To ensure continued compatibility, download the renewed ZTA IDP metadata from the ZTA tenant application configuration page and subsequently apply the updated information to the SaaS SAML SSO configurations.

22.6R1.2

- **Integrating NMDM with ZTA**: Ivanti Neurons for MDM provides compliance check and simplified onboarding experience for nZTA end users connecting via mobile. For details, see. For details see Integrating Ivanti Neurons for MDM with nZTA.
- **Hardened custom sign-in policies and login URLs**: As part of hardening custom sign-in policies and login URLs, the following changes are implemented:
  - Instead of requiring administrators to configure enrollment policies, administrators will only need to configure user policies. As a default, all configured user policies support enrollment.
  - Single SAML authentication server for user authentication and enrollment.

  For details, see:

  - Workflow: Creating a SAML Authentication Policy With Azure AD
  - Workflow: Creating an Authentication Policy for On-Premises ICS SAML
  - Workflow: Creating a SAML Authentication Policy for Okta
  - Workflow: Creating a SAML Authentication Policy for Ping Identity
  - Workflow: Creating a Local Authentication Policy

22.6R1

- **Oracle Cloud Platform support for ZTA Gateway**: ZTA Gateway now supports deployment on Oralce Cloud Platform. For details see Workflow: Creating a Gateway in Oracle Cloud Platform.
- **Launching the Windows Edge/Webview2 browser**: In a typical enrollment, upon successful authentication to the Controller, Ivanti Secure Access Client automatically shows the end-user portal applications page through a Windows Edge/Webview2 browser. This feature is supported with ISAC client version 22.6R1. For details. see Enrolling a Windows Device.
- **Reusable custom icon to associate with application**: The create application page provides an option to upload your own icon, which can be used to associate with more than one application. For details. see Adding Applications to the Controller.
- **Enhancements to L4, Gateway Logs, and Logs Tables**:

  The following list shows the enhancements to L4, Gateway Logs, and Logs Tables.

    - Column resizing across ZTA pages
    - Cell content copy text from Table
    - Pagination across ZTA pages
    - Minimum number of columns in all the tables in L4 dashboards
    - Enhancement to Advanced Filter

  For details. see Viewing Detailed Logs for a Chart and Filtering the Logs.

- **Simplifying device rules and policies, and global device preferences**: Admin experience is enhanced by simplifying the device rules and policies For details, see Creating Device Policies, Setting Global Device Preferences.

22.5R1.2

Suppress EUP Auto Launch: Allows Admin to suppress the auto launch of the End User portal. This option is enabled by default and works with ISAC 22.5R1 and later. For details, see Setting Global Device Preferences.

22.5R1

- Admin Access Control based on location, Host Checker, and Network: Checks the Admin's device geographic location/network/host checker compliance for admin sign-in policy before providing access to admin login. For details, see Configuring Default Device Policy for Users.
- Enhancements to Non Compliance and Anomalies L4 Drill Down logs:
    - The Anomalies L4 table now includes MAC Address and Source IP Address columns.
    - The Non-compliances L4 table now includes Acknowledged, Non-compliant Policy Type, Non-compliance Policy reason, MAC Address and Source IP Address columns.
    - For details, see Using the Active Anomaly and Non-Compliance Charts.
- Log export options to the admin from Gateway and L4 (drill down view) logs: In any of the L4 pages, export the displayed log as a CSV or JSON text file, or create schedules to set up log export jobs. For details, see Viewing Detailed Logs for a Chart.
- Exporting logs from L4 (drill down view) logs and Gateway logs. For details see Exporting logs.

- Gateway Creation Config UI Simplification: Create ZTA Gateway and Create ZTA Gateway Group are grouped under Create. For details, see Adding a vSphere Gateway.
- Acknowledge non-compliance in the non-compliance info panel on the Landing page: Acknowledge individual non-compliances and remove them from the active total. Filter on acknowledged, unacknowledged (active), or all non-compliances. For details, see Using the Summary Ribbon.

22.4R3

- **Role Based Access Control for Admin Users**: With Role-based access control (RBAC), organizations can easily add admins and assign them specific roles, with differing levels of access to the nSA Admin Portal. In addition to an existing set of default roles, Administrators can now create custom granular roles for specific functions within the nSA admin portal. For details, see Role-based Access Control for Admin Users
- **HTTP Proxy Support**: Support Proxy configuration in gateway to connect to ZTA.

For details, see:

- Adding a vSphere Gateway
- Adding an AWS Gateway
- Adding an Azure Gateway
- Adding a KVM Gateway
- Adding a GCP Gateway

22.4R1

- **Applications and Application Groups UI change**: Group together multiple applications for which a single secure access policy is required. Adding Applications to the Controller and Adding Application Groups to the Controller.
- **ZTA Gateway Connection Control for Trusted Networks**: ZTA Gateway can sometimes be bypassed so that users can connect directly to specific applications. For example, you might want users to bypass ZTA for a specific application if they are connected directly to your trusted corporate network. ZTA gateway tunnel creation will be bypassed on the endpoint since resource access will go through the physical interface.

  For details, see Configuring a Default Gateway for Application Discovery.

- **Gateway Re-registration**: ZTA Gateway can now be re-registered in case if the Gateway Registration was not successful and can edit gateway configuration parameters. On registration failures, admin can trigger the registration manually along with the current debugging options such as networking tools, reboot etc. You can also regenerate and download the gateway init config from the controller admin interface as when required. The Admin can also use Registration error report, which provides insight about the registration failure and suggest solutions to overcome it.

  For details, see Re-registering a VMware vSphere Gateway, Re-registering an Amazon Web Services Gateway and Re-registering a GCP Gateway.

  Limitations : Azure and KVM does not allow the user to update configuration after the gateway is deployed. So, if any config update is needed in Azure or KVM gateways (ZTA) ,we need to redeploy the ZTA gateway.

- **Location/Network rule support in default device policy**: Location/Network policy based enforcement can be applied for any user policy. For details, see Options for Location Rules and Options for Network Rules.

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

Security Advisory and Patch Update

Ivanti has released security advisories and mitigations for critical vulnerabilities in the Ivanti ZTA Gateway. These vulnerabilities impacts all supported versions of ZTA Gateway.

The following CVE's have been fixed:

22.8R2

This release includes important security fixes as part of our ongoing commitment to security. The details of these security fixes can be found in security advisory blog, dated January 8th, 2025.

CVE's	Security Advisory Blog
CVE-2025-0282	For more details, see security advisory blog.
CVE-2025-0283	For more details, see security advisory blog.

Support and Compatibility

Supported Client Versions

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

Client	Recommended Versions	Qualified Versions
macOS	22.8R1-8135	22.8.2.33497
Windows	22.8R1-8135	22.8.2.33497
Linux	22.8R1-8135	22.8.2.33497
Android	22.8.1.16	22.8.2.13
iOS	22.8.1.94401	22.8.2.94733

Supported ESAP Versions

The ESAP versions listed below are the supported versions to use with Ivanti Neurons for Zero Trust Access for this release.

	Recommended Versions	Qualified Versions
ESAP	4.6.1	4.6.1 4.5.4 4.5.1 4.3.8 4.3.1

Supported Platforms and Browsers

For Platform and Browser Compatibility with ISAC, refer ISAC SPG.

Supported ZTA Gateway Versions

The ZTA Gateway versions listed below are the supported versions to use with nSA for this release. Download the ZTA Gateway image and template files from the Software Download Portal.

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

Gateway	Recommended Versions	Supported Versions
ZTA Gateway	22.8R2.2- 579 22.8R2.1- 543 22.8R2- 539 22.7R1.2- 525	22.8R2.2- 579 22.8R2.1- 543 (available with controller upgrade) 22.8R2- 539 22.7R1.2- 525

Release and Upgrade Notes

Noteworthy Changes: 22.7R1.3

- CASB/SWG options does not support HTTP PAC files. The support is only for HTTPS PAC files.

Noteworthy Changes: 22.6R1

- Default ESAP version is 4.1.6 or the manually selected previous version will be retained. The newer version of ESAP must be manually enabled from the ZTA controller. In case of any config error after selecting the new version, the admin must delete any unsupported versions (See the Admin logs for any unsupported versions). For more information, see https://forums.ivanti.com/s/article/ESAP-Package-Selection-Behaviour-Changes-Starting-from-ZTA-22-6R1-Release
- ESAP Version 3.9.3 is deprecated in this release. If the deprecated version is previously selected it will be upgraded with ESAP version 4.1.6.
- Default ISAC version is 22.5R1 (25375) or the manually selected previous version will be retained. The newer version of ISAC must be manually enabled from the ZTA controller. For more information, see https://forums.ivanti.com/s/article/Ivanti-Secure-Access-Client-ISAC-Behaviour-Changes-Starting-from-ZTA-22-6R1-Tenant-Release
- ISAC Client 22.3R1 18209 is deprecated in this release. If the deprecated version is previously selected it will be upgraded with ISAC version 22.5R1 (25375).

Noteworthy Changes: 22.5R1

UI changes in Application Create/Edit page:

- Admin can choose to continue creating another application in Create page.
- Admin can change the name of an existing application in Edit page.

Noteworthy Changes in 22.4R3

- App configuration supports configuring subnets and ports. For example, 192.168.1.0/24:443.

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

Important Notice for v22.1R1 and Later

Release 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.

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

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

Resolved Issues

The following table describes the issues resolved.

Problem Report	Description
Release 22.8R1.2	
1525094	Schedule Log export fails to generate an export(CSV/JSON) if it is scheduled for a week.
Release 22.8R1.1	
1391923	The admin might notice discrepancies between the device counts in the Summary Panel and the Table view when clicking on the counter.
1512873	Fixed the issue with report jobs failing when creating an Adhoc/Scheduled job and sharing the report with any admin user in the tenant has been resolved.
1509852	The issue with Deleting Domains from Manage Application page is now resolved.
Release 22.8R2.1 (ZTA GW)	
1505663	The issue with the unresponsive state of ZTA Gateway due to Disk Space issues on Azure is resolved.
Release 22.7R1.6	
1431458	The issue with certificate renewal for ZTA Gateways using Controller is now resolved.
1447143	The issue with the active users information not shown in the nSA license subscription page is now resolved.

Problem Report	Description
Release 22.7R1.4	
1375681	Application logo will be blank when trying to install the Ivanti Secure Access Client from the web browser flow just before it starts downloading the Client.
Release 22.7R1.3	
1350330	Consolidated overview data for all ZTA gateways is not reflecting. No data on Neurons for ZTA > Insights > Overview page.
1341772	Sankey chart does not show the exact path for application being accessed with respect to usergroup.
1375846	Unable to Acknowledge all active anomalies under Overview Page.
1378162	Overview Page should display all the Gateways registered with the controller.
Release 22.7R1.2-HF2	
1350400	Observing slowness when navigating to Secure Access Policy creation and applications pages.
1350442	Gateway Configuration tasks from controller are stuck in pending state.
1350471	Auto-Delete of users failing in ZTA Controller after 30 days of inactivity.
1350376	Configuration sync not working with SNMP configuration.
1349527	Unable to create multiple User Groups when mapped with same rules.
Release 22.7R1.2	

Problem Report	Description
PZT-37411	CEF browser is restricted by domain/group policies, you need external browser support for SAML based Enrollment and authentication.
PZT-43982	Error in adding SSO URL with ":" while creating SAML Auth server.
Release 22.7R1	
PZT-42710	If a user group has a SAML attribute user rule mapped to it, changing SAML auth to local auth in the user policy should alert with a warning.
PZT-42721	Analytics dashboard shows the MDM device attribute failure if there is a hybrid device policy(Location, HC, MDM) enforced on Secure Access Policy wherein the non-compliance is actually due to HC/Location failures.
PZT-41958	ZTA Gateway shows upgrade failed and shows a different version on the Secure Access Gateways dashboard when upgraded to latest version but the console of the gateway is successfully upgraded.
PZT-41821	Gateway UI will not validate IP address /subnet and subnet Gateway info while creating ZTA Gateway under Manage Gateways.
PZT-43953	If the vendor name field is left blank in a Windows Firewall device rule, it will result in the AAA journal version being decremented to -1.

Problem Report	Description
Release 22.6R1.2	
PZT-41502	Add/Delete Gateway in the Gateway Group is not working.
PZT-42203	While editing an existing FQDN app policy with App Discovery enabled to a URL based policy, App Discovery checkbox gets greyed out and not editable.
PZT-41797	Upgrade/Downgrade of ESAP might cause bad config state, if configured product not present in old release.
Release 22.6R1	
PZT-41452	Fixed wildcard with unsupported FQDN format.
PZT- 41443	ZTA Gateway Upgrade issue with VMware ESX.
PZT- 41414	Error when loading end user login or any other sign-in policy page.
PZT-38904	New GW deployment loses the interface configuration and controller registration details upon reboot from GCP Instance options.
PZT-41401	Unauthorized error 401 is displayed when trying to login as readonly/cxo/netadmin to the controller not having any Gateways registered.
PZT-41264	Page not found when trying to login with the pre-canned Network admin role configured under System >Admin Roles

Problem Report	Description
PZT-40857	Non-compliance policy failure reason is empty on the drill down log view dashboard when non-compliance is reported while accessing RDP/Ipv4 application type.
PZT-40518	Endpoint connection to the controller will fail and show the status as 'Failed' when Rule requirement >custom expression is configured under Secure Access > Manage Devices >Device Policies due to AAA journal version failure.
PZT-38858	After upgrading MOD AAA to latest build, assigned roles are missing in cache and admin login might fail.
PZT-38428	Location Device rule does not save properly when denying access from a specific city but allowing access from the same country.
PZT-38625	Controller UI should show error while creating Gateway Group if one of the Gateway in the Gateway Group is mapped with a known network tag in Gateway Selector configuration.
PZT-36750	Lockdown enable/disable done on tenant, taking 3-9 minutes to reflect in client connstore.dat file.
PZT-36813	Risk Sense evaluation for Windows 10 22H2 endpoints is returning as 'Not Available'.
Release 22.5R1.3	

Problem Report	Description
PZT-41314	The connection status is shown as Connecting and some users are not able to establish the connection.
PZT-41403	Data is not loading on Insights > Overview page.
Release 22.5R1.2	
PZT-40843	Fixed log swap issue between the gateway and timestamp fields.
PZT-41180	Page not found error while clicking on **Administration > Admin Management > Admin Roles** with read-only admin (pre-canned role) logging in.
Release 22.5R1	
PZT-39870	Multiple SAP policies having Device policy configured with AV rule results in incorrect cache on AAA.
PZT-37841	Report format CSV/JSON has the epoch timestamp instead of human readable
Release 22.4R3	
PZT-38599	When device rule is edited, corresponding sign-in policy does not get updated with new policy.
PZT-39103	Issue in downloading logs from nSA is now resolved.
PZT-39050	New gateway deployed in GCP looses it's configuration upon first reboot from GCP Instance options.
PZT-39351	Application details with Kerberos/LDAP/NTP not detecting when migrating from ICS to ZTA.

Problem Report	Description
PZT-29634	After upgrade or rollback Gateway certificate is shown wrongly in gateway group.
Release 22.4R1	
PZT-37223	ZTA connection fails with Invalid Client Certificate error.
PZT-38173	User name not displayed properly in tenant access logs.
PZT-38101	If 22.2R1 or below version of gateways are present and OGS feature is configured, older Gateways may not go to ready state.
PZT-35144	Admin rules cannot be deleted when attached to an admin group.
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.

Problem Report	Description
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.
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	: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 .
Release 22.2R1	
PZT-15594	Client configuration: Disable Splash screen option is not working.
PZT-22198	Mac Intune Client is not launching

Problem Report	Description
	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".

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 s 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 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 client is not honoring "Allow Delete Connection".
PZT-24546	Multi sign-in URLs: Login behavior is different for with standard login and non-standard multiple sign-in login URLs when no Secure Access Policy (SAP) is configured on the Controller.
PZT-27300	In a location device rule, it is not possible

Problem Report	Description
	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).
PZT-27999	CA rotation breaks leaf renewal for 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	

Problem Report	Description
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.

Problem Report	Description
Release 22.8R1.2	
1567059	**Symptom**: The UI screen appears blank when the endpoint machine is non-compliant with Host Check (HC). **Condition**: End point machine non complaint with HC. **Workaround**: Close and reopen the ISAC.
1565991	**Symptom**: McAfeeAntiVirusHigh default AV import issue. **Workaround**: • Unmap default McAfeeAntivirushigh device policy in auth policy or in secure access policy if configuration import error in Admin logs or warning in device policy page. • Create custom AV policy for McAfeeAntiVirusHigh and map it for the policy.
1553286	**Symptom**: Syslog forwarding configuration with "via Gateways" on ZTA may impact syslog forwarding for nSA/ZTA. **Cause**: System tries to forward logs "via Controller" also even with configuration "via Gateways" on ZTA. **Workaround**: On ZTA, Configure Syslog Server for ZTA "via Controller" only.
1546793	**Symptom**: Unicodes are seen sometimes in the Tenant UI instead of Icons. **Condition**: While using the Tenant using Chromium browser. **Workaround**: No functional impact. Reopen the App in another tab in the browser, issue will not be seen.
Release 22.8R1	
1512873	**Symptom**: Report job fails when creating a report adhoc or scheduled, and an admin configures it to share with any admin user in the tenant. **Workaround** : NA
Release 22.7R1.6	

Problem Report	Description
1474762	**Symptom**: The tenant might go into config error state when new ESAP 4.5.1 is enabled and the existing Antivirus/Antispyware/FIREWALL/HD encryption polices has removed products. **Workaround**: Edit the existing device polices rules , unselect existing vendors/products and reselect and save. For example, COMODO Security Solutions corresponding product and vendor removed.
Release 22.7R1.5	
1442614	**Symptom**: Error while trying to reset TOTP user account from nSA controller under Administration > Admin Management > Authentication Servers if secondary auth is configured for the sign-in policy **Workaround**: No workaround
1440328	**Symptom**: TCP dump action under Gateway Troubleshooting in nSA/ZTA fails to upload the dump to Troubleshooting overview. This issue happens intermittently when Admin is unable to stop the TCP dump. **Workaround**: Try re-triggering TCP dump action.
Release 22.7R1.4.2	
1425921	**Symptom** : Ivanti Secure Access Client page under Administration > Installation Packages does not respond when we turn off "Always auto update to latest version" option without selecting the client package version. **Workaround** : Select appropriate client package version and save before switching "Always auto update to latest version" option.
Release 22.7R1.4	
1410360	**Symptom** : The consolidated landing page (ZTA+nSA) is currently in preview mode, you may see some discrepancies between the chart counts and the logs/table views of the corresponding charts. **Workaround** : No workaround
1384267	**Symptom**: nSA will allow to add any number of nodes to the cluster with hardware devices while it is restricted to 2 nodes for virtual (ISA-V) gateways registered to controller. **Workaround**: Limit number of nodes to not more than 4 while registering hardware devices to nSA for classic ICS while forming a cluster. Only 2 nodes are supported for 22.x ICS.

Problem Report	Description
Release 22.7R1.3	
1350201	**Symptom** : nSA log export for any L4 dashboard shows the active view data for the previous four days. When performing the log export, it exports the log data for only the previous 1 hour. **Workaround** : To display the correct logs in the csv/json export, select the custom time range that is needed for data export.
1387881	**Symptom**: Data mismatch will be seen in the active view (last hour) as a result of the ZTA Overview page and Consolidated dashboard (NSA+ZTA) displaying data from different time stamps. **Workaround**: To display data inside a certain time range, a workaround is required to filter the data using the desired time range.
1370506	**Symptom**: Active view(last 1 hour) Home page showing consolidated data for NSA+ZTA will show only the active user count activity and not all the user activity in the last 1 hour. **Workaround** : The overall user activity for the ZTA users in the last 1 hour (Active view) will be reflected in the Overview page of ZTA.
1389307	**Symptom**: nSA 'All Gateway' count on the Overview page as well as Insight > Gateways summary strip shows the registered and online gateways count only in the historic views. **Workaround** : NA
1375681	**Symptom** : Application logo will be blank when trying to install the Ivanti Secure Access Client from the web browser flow just before it starts downloading the Client. **Workaround** : NA (No impact on installing ISAC from web browser flow).
1391936	**Symptom**: On the Consolidated Landing Page, the Current Day view (Displayed as Last X hours) may show a count mismatch between the Summary Panel and the Table. **Condition**: When admin wants to view details of current day's data. **Workaround**: The admin can utilise the custom view to observe data for the same time range.
1392136	**Symptom**: On the consolidated Landing Page Sankey Chart, the gateways shown in the Gateways Column might not correspond to the Active Gateways count.

Problem Report	Description
	Condition: When a user connects to a gateway but does not access any application through it. **Workaround**: Regard the Summary Panel gateways count as the accurate Active gateways count.
1391923	**Symptom**: The admin might notice discrepancies between the device counts in the Summary Panel and the Table view when clicking on the counter. **Condition**: Endpoints without a device identification number or share the same device identification number. **Workaround**: Consider the Summary Panel count as the accurate count.
1393507	**Symptom** : Consolidating landing page(ZTA+nSA) is in preview mode and hence there could be data mismatch between the counts on the chart compared to the logs/table view of corresponding charts. **Workaround** : No workaround
1393596	**Symptom**: Admins might observe a slight difference in the CPU, Swap Memory, Disk Usage and Network Throughput values shown on the tooltip forTop Gateways by Health chart under nSA > Insight > Gateways and the table view logs for respective gateways. **Workaround** : No workaround
1393987	**Symptom**: ZTA historic overview /users/applications is not properly displayed in few tenants. **Workaround**: Use the custom time range option to get the historic data.
1393374	**Symptom**: The count shown for specific gateway version might differ between the Gateway by version chart and the table view under Insights > Gateways in nSA. Workaround : No workaround
Release 22.7R1.2	
PZT-45006	**Symptom**: Firewall device policy fails on endpoint when the advance settings are enabled on the firewall device rule with Microsoft product on Windows endpoint. **Workaround**: NA
PZT-43989	**Symptom**: For pre-canned roles login user, navigating to some pages shows not found message if the page is not meant for that role.

Problem Report	Description
	Workaround: NA
PZT-39046	**Symptom** : End user logins will be blocked and admin login will show 401 error when AAA journal version is in bad state once a new ESAP version is activated under Administration > Installers > ESAP **Workaround** : Edit the already configured Device Policy and remove the unsupported products from it and add the supported products. This applies for all the OPSWAT based device policies (AntiVirus, Firewall, Patch, AntiSpyware) irrespective whether these device policies are enforced on a specific Secure Access Policy
PZT-45091	**Symptom** : ZTA data mismatch on the Home page (ZTA+NSA consolidated) as compared to the Overview page showing only ZTA specific data in the controller. **Workaround** : NA
PZT-45016	**Symptom** : User Access/Event logs not updated intermittently in the Gateways due to which analytics dashboards will not show relevant data once the gateway is upgraded to 22.7R2/22.7R1.2 **Workaround** : Reboot Gateway to get the user access/event logs along with Analytics data.
1327244	**Symptom** : Log export does not carry forward the advance filter, sort, search applied on the user access, event and admin logs under Insights **Workaround** : NA
1332914	**Symptom**: ZTA gateways showing FIPS version in the display of gateway console when gateway is upgraded to 22.7R1 from 22.5R1.x or 22.6R1.x although no functionality impact in end user application access. **Workaround**: NA
Release 22.6R1.2	
PZT-42473	**Symptom**: 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. **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.

Problem Report	Description
PZT-42710	**Symptom**: If a user group has a SAML attribute user rule mapped to it, changing SAML auth to local auth in the user policy should alert with a warning. **Workaround**: Remove user rule which has SAML attribute before changing user authentication server from SAML auth to local authentication server.
PZT-42722	**Symptom**: MDM device rule should not be added to the device policy which is enforced on the Admin sign-in URL under User Policies. **Workaround**: NA
PZT-42721	**Symptom**: Analytics dashboard shows the MDM device attribute failure if there is a hybrid device policy(Location, HC, MDM) enforced on Secure Access Policy wherein the non-compliance is actually due to HC/Location failures. **Workaround**: NA
PIOS-6533	**Symptom**: Re-authentication using login to Ivanti Secure Access is not working. **Workaround**: Click on 'connect' button manually.
Release 22.6R1	
PZT-42203	**Symptom**: While editing an existing FQDN app policy with App Discovery enabled to a URL based policy, App Discovery checkbox gets greyed out and not editable. **Workaround**: • Uncheck the App discovery first and then edit the application URL. • Convert wildcard to URL.
PZT-41958	**Symptom** : ZTA Gateway shows upgrade failed and shows a different version on the Secure Access Gateways dashboard when upgraded to latest version but the console of the gateway is successfully upgraded. **Workaround** : None. End to end use case when connecting to the gateway is not impacted as the gateway is already upgraded to the latest version.
PZT-41797	**Symptom**: Upgrade/Downgrade of ESAP might cause bad config state, if configured product not present in old release.

Problem Report	Description
	Workaround: If new product is configured with new ESAP version and downgraded to older version where that product is not available. Admin has to manually delete that product to get back the tenant in normal state. For example, when upgrading from ESAP 4.1.6 to ESAP 4.2.6, admin has to manually remove the vendor name "Broadcom" and product name "Symantec Endpoint Protection (0.0.x)" from the configured AV/AS/Firewall device policies.
PZT-41821	**Symptom**: Gateway UI will not validate IP address /subnet and subnet GW info while creating ZTA Gateway under Manage Gateways. **Workaround**: Admin has to provide the correct interface IP/subnet and subnet default Gateway info while configuring ZTA Gateway.
PZT-41719	**Symptom**: UEBA Threat data for the user in the ZTA analytics dashboards as compared to the UEBA Threat report is different for the same timestamp. **Workaround**: NA
PZT-41837	**Symptom**: UEBA Threat score and UEBA Threat rank is not showing accurate for the users in active and historic view on the Analytics dashboards in case of simultaneous (ICS + ZTA) scenario. **Workaround**: NA
Release 22.5R1.2	
PZT-41401	**Symptom**: Error 401 un-authorized when trying to login to the tenant with any of the pre-canned role like read-only, cxo and net admin if there are no gateways registered in the controller. **Workaround**: Register ZTA gateway in the tenant controller and login.
PZT-41264	**Symptom**: Page not found when trying to login with the pre-canned Network admin role configured under System >Admin Roles **Workaround** : Create a custom admin role with only permissions to view the Manage Gateways dashboard which serves the purpose of the Network admin role.
PZT-41319	**Symptom**: After a fresh installation of the client, it closes unexpectedly. **Condition**: Manual or browser installation of the client. **Workaround**: Open the client from the system tray.
Release 22.5R1	

Problem Report	Description
PZT-40857	**Symptom** : Non-compliance policy failure reason is empty on the drill down log view dashboard when non-compliance is reported while accessing RDP/Ipv4 application type. **Workaround** : NA
PZT-40739	**Symptom**: Non-compliance policy failure reason on L4 (drill down) log dashboard states all the strings related to host check (HC) failures instead of a specific string, which caused the failure for that specific application access. **Workaround**: NA
PZT-37613	**Symptom**: The timestamp displayed under the cards in the User Info panel on Landing page is incorrect in the historic view. **Workaround**: NA
PZT-39046	**Symptom**: End user logins will be blocked and admin login shows 401 error when AAA journal version is in bad state once a new ESAP version is activated under Administration> Installers > ESAP. **Workaround**: Edit the already configured Device Policy and remove the unsupported products from it and add the supported products. This applies for all the OPSWAT based device policies (Antivirus, Firewall, Patch, Antispyware) irrespective whether these device policies are enforced on a specific Secure Access Policy.
PZT-40518	**Symptom**: Endpoint connection to the controller will fail and show the status as 'Failed' when Rule requirement > custom expression is configured under Secure Access > Manage Devices > Device Policies due to AAA journal version failure. **Workaround**: Edit the device policy with custom expression and save again so AAA journal version will recover.
Release 22.4R3	
PZT-38904	**Symptom** : Tenant admin UI will be logged out frequently with 401 error and end user connections will be blocked due to incorrect cache in AAA. **Workaround** : Find the XML import failure log in **Insight > Admin logs** and remove the unsupported product version from the device rule and save it.

Problem Report	Description
PZT-39870	**Symptom**: Multiple SAP policies with having Device policy configured with AV rule results in incorrect cache on AAA. **Workaround**: NA
Release 22.4R1	
PZT-39050	**Symptom**: Intermittently it is observed inconsistency in historic view data in analytics dashboards **Workaround**: NA
PZT-38904	**Symptom** : GCP gateway is not in the connected state after reboot. Using the GCP VM control options (Reset and Stop/Start) **Workaround**: Post deploying the gateway instance in GCP after the successful registration of gateway to the controller, reboot from serial console of the instance once to avoid the issue. Also we dont recommend to use hard reset to reboot the cloud gateways.
PZT-39351	**Symptom** : Application details with Kerberos/LDAP/NTP or unknown port numbers not detecting while creating Secure Access Policy when migrating from ICS to ZTA. **Workaround** : Admin need to modify the application details manually by adding the relevant port number at the end of FQDN/IP. For example in case of LDAP, ldap://<FQDN> need to be changed to <FQDN>:389 and for Kerberos, kerberos://<IP> need to be changed to <IP>:88
PZT-29634	**Symptoms**: Ivanti client is not able to connect to the gateway and fails with error 1147 - Invalid client certificate during upgrade/rollback of a standalone or gateway group **Workaround**: If it is a standalone gateway, then the gateway need to be added to a gateway group and removed back to perform certificate renewal and reboot the gateway. If a gateway is already a part of gateway group, then it needs to be removed and added back to the gateway group.
PZT-38904	**Symptom** : GCP gateway is not in the connected state after reboot using the GCP VM control options (Reset and Stop/Start) **Workaround** : Post deploying the gateway instance in GCP after the successful registration of gateway to the controller, reboot from serial console of the instance once to avoid the issue. Also we dont recommend to use hard reset to reboot the cloud gateways.

Problem Report	Description
PZT-39046	**Symptom**: End user logins will be blocked and admin login will show 401 error when AAA journal version is in bad state once a new ESAP version is activated under Administration > Installers > ESAP. **Workaround**: Edit the already configured Device Policy and remove the unsupported products from it and add the supported products. This applies to all the OPSWAT based device policies (AntiVirus, Firewall, Patch, AntiSpyware) irrespective whether these device policies are enforced on a specific Secure Access Policy.
PZT-39002	**Symptom**: At end of every end UEBA Threat Score is recalculated and there could be a change in the Threat Score **Workaround**: NA
PZT-38858	**Symptom**: After upgrading MOD AAA to latest build, assigned roles are missing in cache and admin login might fail. **Workaround**: After upgrading edit admin groups and then save.
PZT-38995	**Symptom** : Enrollment/Auth is blocked when connection is made from an endpoint which does not have the source_IP listed in allow/block criteria in the Network device policy which is enforced on User policy. **Workaround** : Create Network Device policy to allow the source_IP/s instead of denying as the default action is to deny.
PZT-38975	**Symptom** : 500 error intermittently seen on the dashboard when un-enrolling clients from 'Manage Devices' and new device enrollment will fail on the endpoint due to connectivity issue between the client service and redis. **Workaround** : Restart client service on the controller.
PZT-38722	**Symptom**: Non-compliance count mismatch on the analytics dashboards in the summary strip and non-compliance info panel in historic view when non-compliances are reported in the same hour from the same user. **Workaround**: No workaround
PZT-38718	**Symptom**:CARTA check failing on MAC OSX for the predefined and custom device policies. **WorkAround**: Disconnect and connect again to re-evaluate the compliance and perform remediation accordingly.

Problem Report	Description
PZT-38717	**Symptom**: Firewall device policy not evaluated on the endpoint when default Microsoft product is configured while having 'Rule options' and rule monitoring on. **Workaround**: No workaround
PZT-38690	**Symptom**: If previously selected Client package version is not present after upgrade, latest version will be set to default with auto upgrade enabled. **Workaround**: Select the required client version if the admin don't want to use latest client version after upgrade.
PZT-38619	**Symptom**: RiskSense Notify device policy blocks enrollment via web browser when applied on the Enrollment User sign policy. **Workaround**: Device policy should be configured with multiple device rules apart from RiskSense notify policy OR Connect to ZTA connection profile directly from Ivanti client already installed on the endpoint.
PZT-38618	**Symptom**: UI misaligned when host checker policy fails in the web browser and 'Try Again' button is clicked on Windows endpoint **Workaround**: No workaround
PZT-38599	**Symptom**: Device policy enforced on the sign-in policy does not get updated when any device rule is modified to that corresponding device policy. **Workaround**: Navigate to Secure Access->Manage Users->User Policies and EDIT the User policy where the device policy is enforced and 'Update User policy'.
PZT-38502	**Symptom**: Non-compliance card shown on Analytics dashboard for applications having device policy enforced which is configured for one Operating System and the non-compliance is reported on another Operating System. **Workaround**: No workaround
PZT-38501	**Symptom**: SAML user with error "invalid assertion" received on the endpoint frequently in the CEF browser when connecting to ZTA. **Workaround**: Click on 'Sign-in' and re-try on getting the error dialog with "invalid assertion".
PZT-38428	**Symptom**: Location Device rule does not save properly when denying access from a specific city but allowing access from the same country. **Workaround**:Delete the location rule and add a new one.

Problem Report	Description
PZT-38327	**Symptom**: No error string or instruction displayed on the Ivanti client when Network/Location/RiskSense policy is enforced on User Enrollment/Authentication Sign in URL and the compliance fails on the endpoint due to any of these device policies. **Workaround**: Navigate to Insight->Logs->Access logs to view the compliance logs for admin. No workaround for the end user.
PZT-38315	**Symptom**: ZTA gateway console may show Register as one of the option in the menu, even though the Gateway is already registered. **Condition**: Sometimes with Cloud it is taking a while for the registration process to get completed. Hence when the console options are displayed after registration process is triggered , the register option is still present in the console menu. **Workaround**: Pressing enter key after few secs the register option won't be present in the gateway console menu.
PZT-38265	**Symptom**: Controller UI should show error while creating Gateway Group if one of the Gateway in the Gateway Group is mapped with a known network tag in Gateway Selector configuration. **Workaround**:No workaround
PZT-38256	**Symptom**: Session Migration from one network to another still shows the session with the older source IP under Insights->Users-> Active Sessions. **Workaround**: No workaround
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-37841	**Symptom**: Report format CSV/JSON has the epoch timestamp instead of human readable. **Workaround** : No workaround
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.
PZT-37613	**Symptom**The timestamp displayed under the cards in the User Info panel on Landing page is incorrect in the historic view.

Problem Report	Description
	Workaround: No workaround
PZT-36884	**Symptom**: Sankey chart does not show the exact path for application being accessed with respect to user group. **Workaround**: No workaround
PZT-36623	**Symptom**: Allowed domains added under any configured application shows IP address instead of the application name when accessed on analytics dashboards. **Workaround**: No workaround
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**: No workaround
PZT-29634	**Symptom**: Ivanti client will not be able to connect to the gateway and fails with error 1147 - Invalid client certificate. **Workaround**: Remove gateway from the gateway group and then add it back.
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**: No workaround
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.

Problem Report	Description
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.
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

Problem Report	Description
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 profile, the VPN connection should be disconnected instantly and the profile should be removed from . **Workaround**: Open and move between the screens. A pop-up message should appear warning that the certificate is revoked. The profile is removed automatically.
PZT-7581	**Symptom**: VOD: is not notifying the end user when Notification is turned off. **Workaround**: Enable Notification for the in iOS Device settings.
PZT-8610	**Symptom**: Simultaneous connections: After switching to a new user, shows the enrollment details. **Workaround**: N/A
PZT-8740	**Symptom**: OS check for Android is failing while updating the policy dynamically.

Problem Report	Description
	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 sometimes does not work when classic VPN and connections use different ESAP versions. **Workaround**: Make sure classic VPN and connections use the same ESAP version.
PZT-9979	**Symptom**: Captive portal detection is not working with 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 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 (corporate) connections both active, Microsoft Outlook is not reachable. **Workaround**: N/A
PZT-10600	**Symptom**: [Windows] nslookup with non- FQDNs is always forwarded to the DNS server. **Workaround**: N/A
PZT-10946	**Symptom**: 9.2.0 On-Demand : will be triggered only when the per-app application is being used to access the resources. **Workaround**: N/A (Use Classic Per-app VPN applications to access the resources to get connect with).
PZT-10971	**Symptom**: 9.2.0 Transition : Update MDM profile and push disconnects the connection. **Workaround**: N/A (MDM always set its latest update configuration as default and it is limitation).
PZT-12681	**Symptom**: for Windows 10 prompts for credentials when the device is unenrolled.

Problem Report	Description
	Workaround: Post-enrollment, wait for approximately 2 minutes and try to connect to the controller. The user will get the Certificate revoke message, and after accepting the warning the profile and certificates are deleted.
PZT-14224	**Symptom**: If you have a classic OnDemand VPN connection and your connection is in monitoring mode, when you attempt to access a resource, connects to the classic OnDemand VPN profile and displays a transition notification to the user. **Workaround**: N/A
PZT-14316	**Symptom**: fails with *Error-1111* when a classic VPN fails to resolve the FQDN. **Workaround**: The user must disconnect both classic and connections, then connect first followed by the classic VPN. Alternatively, set the client DNS IP address to public to facilitate resolving classic and connections.
PZT-14581	**Symptom**: When 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
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 .

Problem Report	Description
	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 connection resumes from the Connect-Idle state. **Workaround**: Close the web browser and Launch the application through the 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**: 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 DNS settings. **Workaround**: Use a different DNS IP address for the physical interface and for the 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.
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 connection to the state where On-Demand functionality is initiated. **Workaround**: N/A

Problem Report	Description
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 connections. **Condition**: On uninstalling ISAC with 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 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
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

Problem Report	Description
PZT-36976	**Symptom**: Internet Traffic might be blocked during reconnection after recovering from sleep. **Workaround**: Restart the dsAccessService using Activity monitor or restart the machine.
PZT-36977	**Symptom**: connection shows "Limited connectivity" and "Invalid client Certificate" messages. **Workaround**: In the UI, delete the 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.

Limitations

The following limitations apply to this release:

- 22.7R2.2 ZTA gateway version is not supported with Oracle and AWS platforms.
- nslookup is not supported on Windows and Mac OS.
- RBAC: If the tenant has both nSA and ZTA gateway, setting any common permissions while creating an Custom RBAC Admin Role applies to both nSA and ZTA gateway. For example, if custom admin role has modify permission for ZTA gateway then the same applies to nSA gateway also.
- Okta and PingID SAML authentication methods are supported for 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.

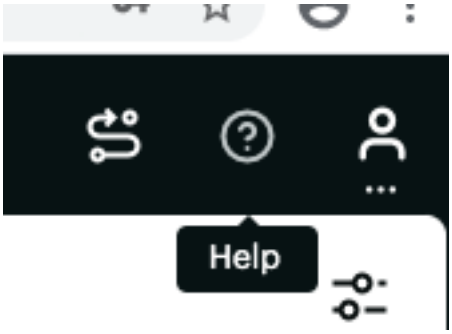
      After tenant creation, the admin must configure the tenant as BYOC before registering a gateway or enrolling an end-user device.
    - For existing tenants, to convert from a BYOC tenant to a non-BYOC tenant is not supported as the tenant needs at least one customer CA.

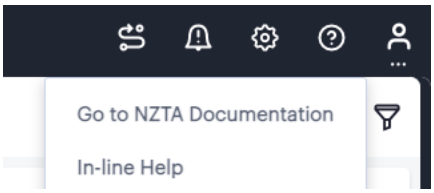
      If all customer CAs are removed after gateways or devices have been enrolled, those existing gateways and devices will not function properly.
    - A CA is not permitted to be used by more than one BYOC tenant.

Documentation and Technical Support

nZTA 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:



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



To access nZTA 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. Find CSC offerings: https://forums.ivanti.com/s/contactsupport

Technical Support

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

- https://forums.ivanti.com/s/contactsupport
- support@ivanti.com