Ivanti Neurons for Secure Access

ICS Gateway 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

nSA ICS Release Notes

Introduction

With enterprises embracing cloud, digitalization, and proliferation of a mobile workforce, users need access to resources and applications from any device, any location, and at any time. Ivanti Connect Secure provides secure and compliant access to resources in hybrid IT environments.

Ivanti Neurons for Secure Access (nSA) simplifies ICS Gateway management and enhances security by providing end-to-end visibility, analytics, centralized troubleshooting, and Gateway lifecycle management from a single pane, and empowers IT administrators to optimize Secure Access policies.

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.

The information in this Release Notes relates to the following releases:

- nSA 22.3R4
- nSA-managed ICS 22.3R1 Build 1647
- nSA-managed ICS 9.1R17 Build 22397

References

- For nSA-managed ICS 9.1R17, refer to: https://help.ivanti.com/ps/help/en_US/ICS/9.1RX/rn-9.1R17/landingpage.htm
- For nSA-managed ICS 22.3R1 Gateway release notes, refer to: https://help.ivanti.com/ps/help/en_US/ICS/22.x/rn/landingpage.htm

Gateway Templates Supported In This Release

Download the image and template files from the links provided below:

- **9.x Package**

  https://pulsezta.blob.core.windows.net/gateway/nsa/9.1R17-nSA-package-22397.1.pkg

- **22.x Package**

  https://pulsezta.blob.core.windows.net/gateway/nsa/22.3R1-nSA-package-1647.1.pkg

  Note: To upgrade to Release 22.3R1, you should first deploy the fresh VM's using the below images:

- **VMware**

  OVF Template applicable to this release: https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-VMWARE-ICS-22.3R1-1647.1.zip

- **KVM**

  KVM Template applicable to this release: https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-KVM-ICS-22.3R1-1647.1.zip

- **Hyper-V**

  Template applicable to this release: https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-HYPERV-ICS-22.3R1-1647.1.zip

- **AWS (JSON)**

  To deploy in an existing VPC:

  https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/22-12-1647/ivanti-2nic-existing-vpc.json

  https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/22-12-1647/ivanti-3nic-existing-vpc.json

  To deploy in a new VPC:

  https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/22-12-1647/ivanti-2nic-new-vpc.json

  https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/22-12-1647/ivanti-3nic-new-vpc.json

  ICS gateway AMIs are available in all AWS regions (except China):

  Nitro Hypervisor Image - Search for the AMI name in the public image:

  ISA-V-NITRO-ICS-22.3R1-1647.1.img

- **Microsoft Azure**

  Image applicable to this release:

  https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-HYPERV-ICS-22.3R1-1647.1-SERIAL-hyperv.vhd

  JSON template files applicable to this release:

  To deploy in an existing VNET:

https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/22-12-1647/ivanti-2nic-existing-vnet.json

https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/22-12-1647/ivanti-3nic-existing-vnet.json

To deploy in a new VNET:

https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/22-12-1647/ivanti-2nic-new-vnet.json

https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/22-12-1647/ivanti-3nic-new-vnet.json

- **Google Cloud Platform**

  Image applicable to this release:

  https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-GCP-ICS-22.3R1-1647.1.tar.gz

  To deploy in an existing VPC:

  https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/22-12-1647/ivanti-ics-2-nics-existing-vpc.zip

  https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/22-12-1647/ivanti-ics-3-nics-existing-vpc.zip

  To deploy in new VPC:

  https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/22-12-1647/ivanti-ics-2-nics-new-vpc.zip

  https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/22-12-1647/ivanti-ics-3-nics-new-vpc.zip

What's New

22.3R4

- Configuring ZTA Policy to an ICS Application - Administrators can now configure ICS application with ZTA secure access policy from the nSA-ICS Applications page.
- nSA Named User Licensing - Freeing named user licenses automatically - Users who have not logged in to the ICS Gateway for the last 30 days can be deleted automatically from the Users list.
- Addition of a new alert "Config Sync Target Cluster Deleted" - This alert is generated when the Target Cluster, which is in any of the Config Sync rule gets deleted.

Note: Configuration template functionality is consolidated into Configuration sync feature.

22.3R3

- Actionable Insights: Step up Authentication, Subsequent login and Chart Visibility.

22.3R1

- Enhanced Admin experience
- Config Sync enhancements
- Alerts and Notification enhancements
- nSA UI parity with 9.1R16 and R17
- L3 VPN App Visibility
- Config Replace/reorder

Important Notice for v22.3R1

To prevent any upgrade related issues and to clean up the disk space, follow the mandatory steps listed in the KB article before staging or upgrading: https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44877/?kA13Z000000L3Z5

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 to version 22.1R1 at your earliest convenience.

Caveats

The following caveats are applicable to this release:

- Gateway ESAP package version 4.0.5 is default.
- Config group management works best with ESAP version 4.0.5. The ESAP version on the Gateway can be upgraded to desired version.
- For uploading the ESAP package, you must have the package in ESAP<version>_Prod.pkg format.
- Config Synchronization feature:
  - Active ESAP versions must be same on both Source and Target Gateways.
  - Admin Realms, Admin Sign-In URLs, Device certificates and Client Auth certificates are not supported.
  - During Config Synchronization, the configurations will be getting merged from Source Gateway to Target Gateway and hence the delete operation is not supported.

- nSA accepts only certificates in PEM format, DER format certificates are not supported from nSA.
- nSA custom validation is not supported through Configuration Templates. The UI may accept invalid configuration parameters.
- Remote profiler and OAuth server are not supported through Configuration templates.
- Always on VPN wizard is not supported on nSA.
- Dark theme for nSA ICS admin UI is not supported.
- ICS Cluster creation with IPv6 address from nSA is not supported.

Limitations

- The ICS upgrade time from nSA depends on the network bandwidth and latency. If the downloading of package takes more than 4 hours then the upgrade process is marked as failed.
- Cluster creation from nSA takes few minutes to create cluster and add/join members.
- The time taken for Config Synchronization process from source to target Gateway depends on the configuration size.

Fixed Issues in This Release

The following table describes the fixed issues in this release.

TABLE 1.1 : Fixed issues

Problem Report	Description
22.3R1	
PZT-33001	Config template: SAML settings XML import fails if FQDN is not configured.
PZT-32924	Config Synchronization fails with error.
PCS-36871	Configuration upload is not happening after rebooting the Gateway from nSA.
PZT-33341	Config Template: Adding local auth server for 22.1R1 template fails.
PZT-33708	During Config Synchronization operation, you see 'The system log file is corrupt. Contact Support immediately entry in GW Admin access logs.

Continued on next page

TABLE 1.1 – continued from previous page

Problem Report	Description
PCS-36976	Device attribute is not present in role mapping when MDM server is used for device attribute.
PZT-33343	On cluster nodes Network > Overview, Port status may appear as incorrect such as blank, Not connected.
PCS-35938	Once Client package download starts from nSA to ICS Gateway, any other operations in nSA (For example, Role/Realm creation, any config modification)
PCS-36969	"Add to all VLAN route tables" option is not present in nSA.
PCS-36971	Mac address and link local address are not present for internal/external/management port in nSA.
PCS-36720	TOTP User status is shown as Unlocked, even after unlocking from nSA.
PCS-36747	Role name not present in "Applies to Role" for any Auto Resource policies.
PCS-36757	Internal server error is observed while deleting the user roles.
PZT-32806	Delay in creating User roles from nSA.
PZT-31534	Gateways are not getting listed in nSA after deleting and re-registered.
PZT-31512	The edit name functionality for SAML Authentication server is not working.
PCS-36700	Binary User configuration file import not supported from nSA for file size above 300 MB.
PZT-32799	Unable to delete multiple sign-in URLs on a gateway.
PCS-35403	Test Enrollment is not working in Enterprise Onboarding.
PZT-31275	'Enable periodic password change of machine account' text-box value of AD server is not getting updated/pushed to Gateway from nSA.
PZT-31693	The status of 9.x Gateway in A/P cluster is shown incorrect in nSA, even though they are online and both notification channel and registration.
PCS-34028	Logs not related to configuration done from configuration template is visible under Config Template > Logs.
PZT-29269	The configuration is not pushed to the Gateway, when adding a disconnected state Gateway to the configuration template.
22.2R1	

Continued on next page

TABLE 1.1 – continued from previous page

Problem Report	Description
PZT-29298	nSA UI must indicate to Admin if the template configuration is modified using Gateway Admin UI.
PCS-33427	Test Connection to LDAP and Remote TOTP authservers fail, when executed from nSA UI.
PZT-29259	When invalid file (.rec) is uploaded while creating ACE server, which affects the entire config group management feature.
PCS-33546	Activated/Default Ivanti Secure Access Client package details are not displayed in nSA.
PCS-33308	Ivanti Secure Access Client > Components page in nSA displays different client package versions details when compared with ICS Gateway.
PCS-33633	The Trusted Server List popup is displayed incorrectly.
PCS-33873	Entity ID is not fetched for SAML metadata provider settings.
PCS-33881	User Role fails to push to Gateway with NFS file attribute errors.
PCS-33394	UI issues observed in Always On VPN wizard.
PCS-33859	Unable to download the MIB file in SNMP tab in log settings.
PCS-33219	Post Registration and during config upload, authentication realms admin related logs printed in Gateway event logs.
PCS-33268	Test Connection functionality in MDM Auth Server is not working properly in the Gateway.
PCS-34214	IP address configuration getting pushed from nSA to Gateway but not visible in nSA.
PCS-34122	Not able to create any type of MDM Auth Server.
PCS-33486	Search option is not available in users list for system local auth server.
PCS-34233	Internal server error is displayed when user realm configured from nSA with multiple Auth servers.
PCS-31552	Under the code signing page, delete certificates functionality is not working properly.
PCS-33407	"Not found" error is seen on Hostchecker options page when connection control policy is not configured.
22.1R1	
PZT-27718	View All link from the "Gateways Access Trend chart" from *Insights > Gateways* page, shows incorrect total rows count on the table.

Continued on next page

TABLE 1.1 – continued from previous page

Problem Report	Description
PCS-31198	Adding a Gateway to a cluster in GW UI does not add the cluster as a group on nSA.
PCS-32081	nSA shows L4 connection as WSAM instead of PSAM connection.
PCS-30330	Cluster is not deleted from nSA on deleting the same cluster from Gateway UI.
PCS-32923	User can see same Host Checker (HC) policy with multiple entries (one with space and the other without) on the Gateway Overview page.
PCS-31061	nSA shows "Gateway status not ready" due to an error encountered in ICS.
PCS-31164	When HTML5 bookmark backend resource is not reachable from the Gateway, nSA insights doesn't show the HTML5 bookmark access details.
PCS-31139	9.x PCS: When the user opens internal directories/files for a particular file bookmark of 9.x, an additional active application count is observed on nSA.
PCS-31232	Default "Meeting Sign-In Page" is missing at "Authentication > Signing In > Sign-In Pages" on VMware VM in 9.12.
PCS-31169	9.x PCS: WELF filter is missing in the filters section, and two JSON filters are present.
PCS-31229	Unable to create Resource profile file of type Unix.
PCS-31230	Default welcome banner shows up the text "Connect Secure" when upgraded from version 9.1R12-14139 to 9.1R12-15707.
PZT-25667	ICS Gateway: The source IP of an end-user session is sometimes seen as 127.0.0.1 under **Insights**.
PCS-31180	9.x PCS: The Telnet/SSH application count is coming as 0 on the nSA.

Known Issues in This Release

The following table describes the open issues in this release, with workarounds where applicable.

TABLE 1.2 : Known issues

Problem Report	Description
22.3R4	
PCS-39826	**Symptom**: Failure logs are seen multiple times during config sync operation. **Condition**: When config sync rule fails, it is observed that failure logs are seen multiple times. **Workaround**: Skip configuration, which is failing from config sync rule and trigger same rule again.
22.3R1	
PZT-33008	**Symptom**: Uploaded device certificate is not visible on the nSA. **Condition**: When using nSA to import device certificate onto the ICS gateway. **Workaround**: Wait for at least 10 seconds, and then refresh the page.
PZT-36639	**Symptom**: ICS not sending logs to nSA and sessions are not reported. **Condition**: When Admin configures the JSON filter. **Workaround**: Remove JSON filter, which was created manually.
PCS-39623	**Symptom**: Upgrade of cluster node fails with "Unable to extract installer" error message. **Condition**: • When upgrade triggered on a cluster: – Node-1 upgrades successfully to 22.3R1 and prompts Node-2 to upgrade. – Node-2 copies the package from Node-1, but fails to extract the installer. – This is due to free disk space constraints on Node-2. **Workaround**: • Follow the below procedure: – Power cycle Node-2. – Press Tab and boot into Standalone mode. – Access the UI and follow the procedure mentioned in https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44877/?kA13Z000000L3Z5 to clean up space. – Reboot and join the cluster. Upgrade should now go through fine.
22.2R1	

Continued on next page

TABLE 1.2 – continued from previous page

Problem Report	Description
PCS-36834	**Symptom**: Radius Auth server User Attributes do not display code/number associated with them on nSA UI. **Condition**: Creating/Editing a Role Mapping rule based on User Attributes under a User Realm with Radius auth server. **Workaround**: The code/number associated with the attributes can be viewed on GW UI.
PCS-36937	**Symptom**: Enduser is not able to receive multicast traffic. **Condition**: When the enduser is connected to VPN in ESP. **Workaround**: Not applicable
PZT-33361	**Symptom**: Config Template: Adding MDM server for 22.1R1 template fails. **Condition**: When Admin tries to add an MDM server for 22.1R1 template it shows this element is not expected. **Workaround**: Upgrade the Gateways to 22.2R1 and add this Gateway to 22.2R1 template and create the configuration.
PZT-32568	**Symptom**: Configuration values in Security Settings > Miscellaneous page is not retained. **Condition**: When nSA admin tries to configure values in Security Settings > Miscellaneous page. **Workaround**: No functionality impact, configs are pushed successfully.
PZT-33401	**Symptom**: Second node in the cluster is shown as disconnected. **Condition**: Upgrade from older release to 22.2R1 build, through nSA. **Workaround**: Navigate to the cluster through nSA and check the status.
PCS-36458	**Symptom**: Default and Factory version name is not displayed for default Ivanti Secure Access Client package. **Condition**: Admin selects the gateway and accesses Ivanti Secure Access Client Components. **Workaround**: Not applicable
PCS-34681	**Symptom**: Roll back option not available in nSA for AA cluster. **Condition**: When Admin tries to do a roll back from nSA. **Workaround**: Reboot the AA cluster.
PCS-36458	**Symptom**: Default and Factory Version labeling name is not displayed for default Client package. **Condition**: Select gateway and access Client Components in nSA. **Workaround**: Not applicable

Continued on next page

TABLE 1.2 – continued from previous page

Problem Report	Description
PCS-34067	**Symptom**: Resource not exists is displayed while trying to delete Internal, external, management port. **Condition**: Select a gateway > Navigate to Network > Vlan > Internal, external, management > virtual port. **Workaround**: Perform the Configuration using Gateway Admin UI.
PCS-36695	**Symptom**: Unable to configure cluster when License server configured on both nodes. **Condition**: When License server is configured on Gateways used to create cluster. **Workaround**: Remove License server configuration from Gateways and create cluster.
PZT-32537	**Symptom**: When admin tries to filter out logs in Template> logs page. **Condition**: When controller logs filter is set to true. **Workaround**: None
PZT-32981	**Symptom**: XML Import of SAML SSO 1.1 policy and creation from nSA fails. **Condition**: Import of SAML SSO 1.1 policy and policy creation. **Workaround**: Use the Gateway Admin UI.
PZT-32749	**Symptom**: "Unknown Error" is displayed on the nSA Admin UI, while adding gateway to configuration template. **Condition**: When admin tries to add gateway with many large configurations. For example, many Host Checker policies. **Workaround**: Ignore the error as the Gateway is added to template and config is pushed to gateway.
PZT-31008	**Symptom**: Expired certificate is getting imported on nSA from Config Template > Trusted Server page. **Condition**: When Admin tries to import an expired CA certificate in nSA. **Workaround**: Ensure that the certificate is valid before importing it on nSA.
PZT-30913	**Symptom**: Editing the configuration name is not working on nSA. **Condition**: Create an new component set for Client Components, edit the name of the component set and the edited name is not being reflected in nSA but it is successfully pushed to ICS Gateway. **Workaround**: No functionality impact.

Continued on next page

TABLE 1.2 – continued from previous page

Problem Report	Description
PZT-31638	**Symptom**: Updating ESAP package to cluster will not work when one node is in connected state and other is in disconnected state. **Condition**: When user tries to update the ESAP package to a cluster. **Workaround**: Update ESAP package from the active node configuration.
PZT-29300	**Symptom**: Reconcile configuration takes few seconds. **Condition**: Select a Gateway or cluster, which exists in the configuration template and click Reconcile configuration. **Workaround**: None
PZT-29049	**Symptom**: Deletion time is high while deleting the config in configuration template. **Condition**: Deleting many server configurations at a time. **Workaround**: Deleting minimal amount of configuration or server config from template.
PCS-33870	**Symptom**: File upload fails to push to Gateway for VMware and Citrix download configurations. **Condition**: Admin tries to upload large size file. **Workaround**: Use the Gateway Admin console to upload the configuration.
PCS-36464	**Symptom**: ICS gateway model details not updated correctly on nSA. **Condition**: When licenses are installed on Gateway after nSA registration. **Workaround**: Install all required licenses before registering to nSA.
PZT-33115	**Symptom**: Deleting AD Auth server shows internal server error in nSA. **Condition**: Deleting AD Auth server from nSA. **Workaround**: Refreshing the page shows AD AUTH is deleted.
22.1R1	
PZT-29523	**Symptom**: nSA is not reachable using web browser. **Condition**: When the Admin refreshes the Configuration template page. **Workaround**: None. nSA becomes reachable in few minutes.
PZT-28842	**Symptom**: While navigating to the Gateway list page user might get 'Request failed with status code 500' error. **Condition**: When more then 100+ Gateways are registered with nSA, sometimes navigating to Gateway list page results in above mentioned error. **Workaround**: Waiting or refreshing the page resolves the issue.

Continued on next page

TABLE 1.2 – continued from previous page

Problem Report	Description
PCS-34551	**Symptom**: Reconciliation fails with a config group template having a CA certificate, which already exists on the Gateway. **Condition**: Admin tries to perform a Reconciliation in nSA. **Workaround**: Delete the duplicate certificate from the Gateway before trying reconciliation again.
PCS-34477	**Symptom**: Configuration status of one or more Gateways on Configuration template shows "pending configuration". Host Checker configuration made on configuration template is not pushed to particular Gateways. **Condition**: Gateways are added to configuration template and Host checker configurations (Policy and Rules) done using configuration template. **Workaround**: Select all Gateways in "pending configuration status" and do reconciliation.
PCS-34333	**Symptom**: Download percentage towards end shows more then 100%. **Condition**: Admin starts Gateway upgrade from nSA, and then observes the download percentage. **Workaround**: Wait for package download operation to complete, even if the % goes to around 120%.
PCS-31734	**Symptom**: nSA ICS Overview dashboard Info panel shows empty values for some users. **Condition**: Issue is seen for the sessions, whose Host Checker logs generated by Gateway do not have both device_id and browser_id values. **Workaround**: None
21.12	
PZT-27477	**Symptom**: nSA Insights page displays Users/Sessions as active when session is suspended in client. **Condition**: When the user VPN connection is suspended from the client. **Workaround**: None
PCS-32827	**Symptom**: The ICT changes are not sent through passive node of cluster. **Condition**: In Active/Passive cluster, the configuration change for ICT is not sent through passive node. **Workaround**: Admin needs to send the ICT related changes to active node in cluster.

Continued on next page

TABLE 1.2 – continued from previous page

Problem Report	Description
PCS-32833	**Symptom**: The status info like cluster reboot/ICT/cluster upgrades are not synced between Gateways in nSA cluster. **Condition**: In any cluster, the cluster wide actions status are not synced. **Workaround**: None
PCS-32741	**Symptom**: When Admin sends ICT config, Gateway logs shows interval is seen in seconds instead of hours/minutes format. **Condition**: When ICT configuration is sent from nSA. **Workaround**: None
PZT-27506	**Symptom**: Gateway certificate Renewal Failed" error messages seen on nSA. **Condition**: When registering release 21.9 Gateway devices in release 21.12 nSA. **Workaround**: Upgrade the Gateway to release 21.12.
PCS-32890	**Symptom**: One of the upgraded node in Active/Passive cluster will intermittently be showing the old version in nSA. **Condition**: During the Active/Passive cluster upgrade. **Workaround**: Rebooting the problematic device will fix the issue in nSA.
PCS-32842	**Symptom**: The first time changes to ICT are not pushed to ICS Gateway. **Condition**: Post registration to nSA, the first time configuration changes are not pushed to Gateway. **Workaround**: Admin needs to reconfigure the ICT with different values.
PCS-32382	**Symptom**: In nSA application access count is incremented, even though application is not accessed. **Condition**: When resource is not reachable or disconnected from the internal port of ICS or internal VLAN port of ICS. **Workaround**: None
21.9	
PZT-22115	**Symptom**: ICS Gateway: Gateway selection at the top of the page is not applicable for **Insights** pages. **Workaround**: Apply a global Gateway filter on the dashboard.
PCS-29171	**Symptom**: ICS Gateway: **Insights > Users > Session types chart > View All** - device type is missing for IF-MAP imported sessions in table view. **Workaround**: None

Continued on next page

TABLE 1.2 – continued from previous page

Problem Report	Description
PCS-30305	**Symptom**: Cluster Table is not getting updated when user tries to destroy the registered Virtual ICS/ PCS Gateway from ESXi server. **Condition**: Destroy the Gateway in ESXi server without deleting the Cluster. **Workaround**: Delete the created Cluster and then destroy the virtual Gateways in ESXi server.
PCS-30802	**Symptom**: nslookup with TXT query returns large response then 403 error is seen in Admin UI events log. **Condition**: nslookup with TXT query returning large response. **Workaround**: Use the Gateway nslookup query.
PCS-30648	**Symptom**: Use proxy gets enabled on System > Ivanti Neurons for Secure Access, though set to no in REST API. **Condition**: When using /api/v1/nsa/register REST API to register ICS Gateway with nSA. **Workaround**: If not going to use proxy, do not send proxy related config in the POST body.
PCS-31166	**Symptom**: After cluster upgrade to 9.1R12, node details, tunnel type, tunnel IP details are not updating in user access logs. **Condition**: In AA Cluster, upgrading cluster nodes when 5K users (or more users) connected and traffic is on, user might see node details, tunnel type, tunnel IP details are not updating in user access logs. **Workaround**: Do the upgrade process during, off-peak hours.
PCS-30439	**Symptom**: End user login fails for users created in Local authentication server with clear text password enabled. **Condition**: Creating local authentication server with clear text enabled. **Workaround**: For Non IKE use cases use without enabling clear text password.

Additional Notes

- Rollback - When we rollback to previous versions of 9.1Rx (where nSA is not supported), the status in nSA shows disconnected.

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:

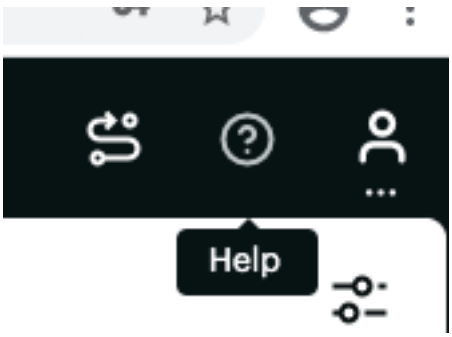

FIGURE 1.1 : For documentation links, click the Help icon in the navigation bar

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

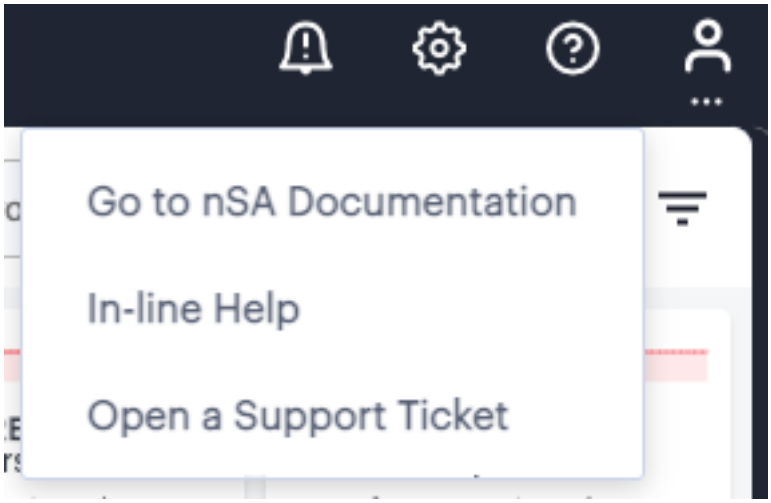

FIGURE 1.2 : Select the "Go to nSA Documentation" option

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

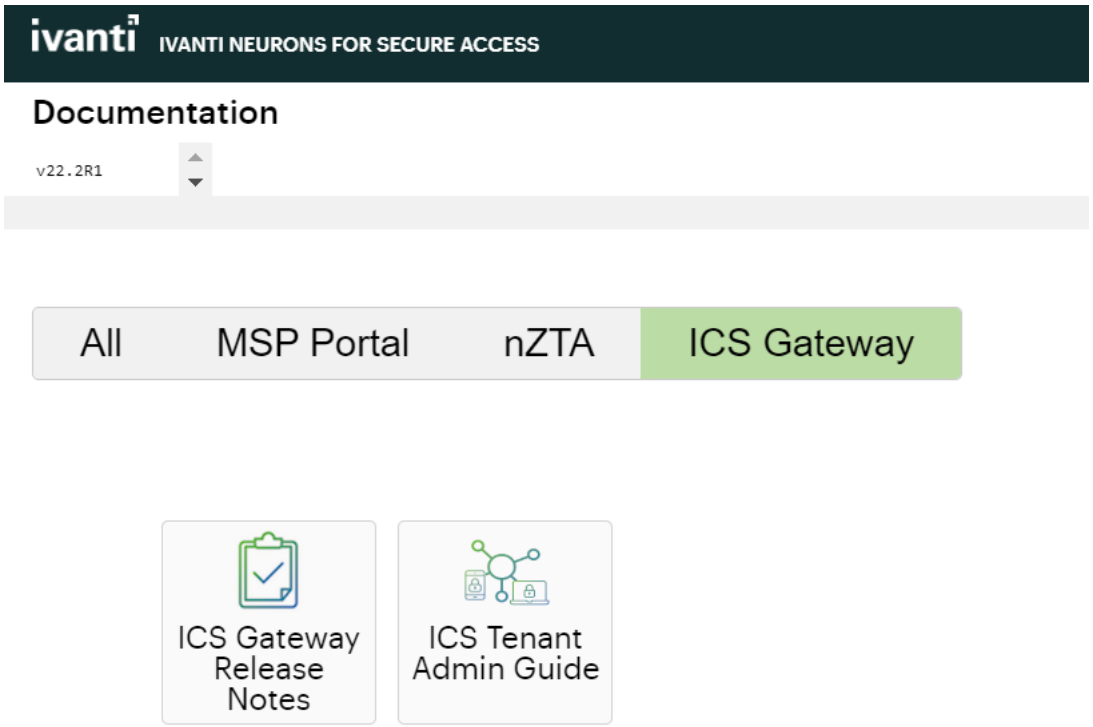

FIGURE 1.3 : The nSA documentation cover page

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 created
1.3	July 2022	22.2R1 release notes created
1.2	April 2022	22.1R1 release notes created
1.1	January 2022	21.12 release notes created
1.0	October 2021	21.9 release notes created