ivanti

nSA Release Notes

22.7R1

Copyright Notice

Contents

Introduction

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 22.7R1
- nSA-managed ICS 22.4R2.4 Build 2169
- nSA-managed ICS 22.5R2.4 Build 2229
- nSA-managed ICS 22.6R2.3 Build 2719
- nSA-managed ICS 9.1R18.5 Build 25187

References

• For nSA-managed ICS 9.1R18.5, refer to: Release Notes

• For nSA-managed ICS 22.6R2.3 Gateway release notes, refer to: Release Notes

Supported Gateway Templates

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

9.x Gateways

9.1R18.5

9.x Package: https://pulsezta.blob.core.windows.net/gateway/nsa/9.1R18.5-25187.pkg

9.1R18.4

- 9.x Package: https://pulsezta.blob.core.windows.net/gateway/nsa/9.1R18.4-25055.pkg

9.1R18.3

- 9.x Package: https://pulsezta.blob.core.windows.net/gateway/nsa/9.1R18.3-24995.pkg

9.1R18.2

- 9.x Package: https://pulsezta.blob.core.windows.net/gateway/nsa/9.1R18-nSA-package-24467.1.pkg

On-Premises VMware vSphere:

The following OVF template is applicable to this release:

- https://pulsezta.blob.core.windows.net/gateway/nsa/PSA-V-VMWARE-ICS-9.1R18.2-24467.1.zip

On-Premises KVM:

OpenStack distribution qualified: OpenStack Stein release.

The following KVM template is applicable to this release:

- https://pulsezta.blob.core.windows.net/gateway/nsa/PSA-V-KVM-ICS-9.1R18.2-24467.1.zip

Amazon Web Services (AWS):

The following JSON template files are applicable to this release:

To deploy in an existing VPC on Nitro Hypervisor:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-9-24467/ivanti-2nic-existing-vpc.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-9-24467/ivanti-3nic-existing-vpc.json

To deploy in a new VPC on Nitro Hypervisor:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-9-24467/ivanti-2nic-new-vpc.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-9-24467/ivanti-3nic-new-vpc.json

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

1. Log into the AWS console.
2. Navigate to EC2 > Images > AMIs.
3. Select "Public Images".
4. Search for the image corresponding to your selected hypervisor: XEN: PSA-V-XEN-ICS-9.1R18.2-24467.1-SERIAL-xen.img
5. Make a note of the corresponding AMI ID.

Microsoft Azure:

The following JSON template files are applicable to this release:

To deploy in an existing VNET:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-9-24467/ivanti-2nic-existing-vnet.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-9-24467/ivanti-3nic-existing-vnet.json

To deploy in a new VNET:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-9-24467/ivanti-2nic-new-vnet.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-9-24467/ivanti-3nic-new-vnet.json

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

- Americas: https://pulsezta.blob.core.windows.net/gateway/nsa/PSA-V-HYPERV-ICS-9.1R18.2-24467.1-SERIAL-hyperv.vhd

Google Cloud Platform:

The following template files are applicable to this release:

To deploy in an existing VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-9-24467/ivanti-ics-2-nics-existing-vpc.zip
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-9-24467/ivanti-ics-3-nics-existing-vpc.zip

To deploy in a new VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-9-24467/ivanti-ics-2-nics-new-vpc.zip
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-9-24467/ivanti-ics-3-nics-new-vpc.zip

The following GCP gateway image is applicable to this release:

- https://pulsezta.blob.core.windows.net/gateway/nsa/PSA-V-GCP-ICS-9.1R18.2-24467.1.tar.gz

9.1R18.1

- 9.x Package: https://pulsezta.blob.core.windows.net/gateway/nsa/9.1R18.1-nSA-package-23821.1.pkg

On-Premises VMware vSphere:

The following OVF template is applicable to this release:

- https://pulsezta.blob.core.windows.net/gateway/nsa/PSA-V-VMWARE-ICS-9.1R18.1-23821.1.zip

On-Premises KVM:

OpenStack distribution qualified: OpenStack Stein release.

The following KVM template is applicable to this release:

- https://pulsezta.blob.core.windows.net/gateway/nsa/PSA-V-KVM-ICS-9.1R18.1-23821.1.zip

Amazon Web Services (AWS):

The following JSON template files are applicable to this release:

To deploy in an existing VPC on Nitro Hypervisor:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-7-23821/ivanti-2nic-existing-vpc.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-7-23821/ivanti-3nic-existing-vpc.json

To deploy in a new VPC on Nitro Hypervisor:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-7-23821/ivanti-2nic-new-vpc.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-7-23821/ivanti-3nic-new-vpc.json

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

1. Log into the AWS console.
2. Navigate to EC2 > Images > AMIs.
3. Select "Public Images".
4. Search for the image corresponding to your selected hypervisor: XEN: PSA-V-XEN-ICS-9.1R18.1-23821.1-SERIAL-xen.img
5. Make a note of the corresponding AMI ID.

Microsoft Azure:

The following JSON template files are applicable to this release:

To deploy in an existing VNET:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-7-23821/ivanti-2nic-existing-vnet.json

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-7-23821/ivanti-3nic-existing-vnet.json

To deploy in a new VNET:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-7-23821/ivanti-2nic-new-vnet.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-7-23821/ivanti-3nic-new-vnet.json

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

- Americas: https://pulsezta.blob.core.windows.net/gateway/nsa/PSA-V-HYPERV-ICS-9.1R18.1-23821.1-SERIAL-hyperv.vhd

Google Cloud Platform:

The following template files are applicable to this release:

To deploy in an existing VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-7-23821/ivanti-ics-2-nics-existing-vpc.zip
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-7-23821/ivanti-ics-3-nics-existing-vpc.zip

To deploy in a new VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-7-23821/ivanti-ics-2-nics-new-vpc.zip
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-7-23821/ivanti-ics-3-nics-new-vpc.zip

The following GCP gateway image is applicable to this release:

- https://pulsezta.blob.core.windows.net/gateway/nsa/PSA-V-GCP-ICS-9.1R18.1-23821.1.tar.gz

9.1R18

- 9.x Package: https://pulsezta.blob.core.windows.net/gateway/nsa/9.1R18-nSA-package-23345.1.pkg

- VMware vSphere:

  The following OVF template is applicable to this release:

  - https://pulsezta.blob.core.windows.net/gateway/nsa/PSA-V-VMWARE-ICS-9.1R18-23345.1.zip

- KVM:

  The following KVM template is applicable to this release:

  - https://pulsezta.blob.core.windows.net/gateway/nsa/PSA-V-KVM-ICS-9.1R18-23345.1.zip

- Nutanix:

  The following KVM Nutanix template is applicable to this release:

  - https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-NUTANIX-ICS-9.1R18-23345.1.zip

- Hyper-V:

  The following Hyper-V template is applicable to this release:

  - https://pulsezta.blob.core.windows.net/gateway/nsa/PSA-V-HYPERV-ICS-9.1R18-23345.1.zip

Cloud Deployments:

- Amazon Web Services (AWS):

  The following JSON template files are applicable to this release:

  To deploy in an existing VPC:

  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-4-23345/ivanti-2nic-existing-vpc.json
  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-4-23345/ivanti-3nic-existing-vpc.json

  To deploy in a new VPC:

  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-4-23345/ivanti-2nic-new-vpc.json

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-4-23345/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-9.1R18-23345.1-SERIAL-nitro.img"

- Microsoft Azure:
  - Image : https://pulsezta.blob.core.windows.net/gateway/nsa/PSA-V-HYPERV-ICS-9.1R18-23345.1-SERIAL-hyperv.vhd

  The following JSON template files are applicable to this release:

  To deploy in an existing VNET:

  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-4-23345/ivanti-2nic-existing-vnet.json
  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-4-23345/ivanti-3nic-existing-vnet.json

  To deploy in a new VNET:

  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-4-23345/ivanti-2nic-new-vnet.json
  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-4-23345/ivanti-3nic-new-vnet.json

22.x Gateways

22.6R2.3

- 22.6R2.3 Package: https://pulsezta.blob.core.windows.net/gateway/nsa/22.6R2.3-2719.pkg

22.4R2.4

- 22.5R2.4 Package: https://pulsezta.blob.core.windows.net/gateway/nsa/22.5R2.4-2229.pkg

22.4R2.4

- 22.4R2.4 Package: https://pulsezta.blob.core.windows.net/gateway/nsa/22.4R2.4-2169.pkg

22.6R2.2

- 22.6R2.2 Package: https://pulsezta.blob.core.windows.net/gateway/nsa/22.6R2.2-2677.pkg

22.6R2.1

- 22.6R2.1 Package: https://pulsezta.blob.core.windows.net/gateway/nsa/22.6R2.1-nSA-package-2487.1.pkg

VMware vSphere:

The following OVF template is applicable to this release:

- https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-VMWARE-ICS-22.6R2.1-2487.1.zip

KVM:

The following KVM template is applicable to this release:

- https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-KVM-ICS-22.6R2.1-2487.1.zip

Cloud Deployments:

Amazon Web Services (AWS):

The following JSON template files are applicable to this release:

To deploy in an existing VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-11-2487/ivanti-2nic-existing-vpc.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-11-2487/ivanti-3nic-existing-vpc.json

To deploy in a new VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-11-2487/ivanti-2nic-new-vpc.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-11-2487/ivanti-3nic-new-vpc.json

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

1. Log into the AWS console.
2. Navigate to EC2 > Images > AMIs.
3. Select "Public Images".
4. Search for the image corresponding to your selected hypervisor: Nitro: ISA-V-NITRO-ICS-22.6R2.1-2487.1.img
5. Make a note of the corresponding AMI ID.

Microsoft Azure:

Image : https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-AZURE-ICS-22.6R2.1-2487.1.vhd

The following JSON template files are applicable to this release:

To deploy in an existing VNET:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-11-2487/ivanti-2nic-existing-vnet.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-11-2487/ivanti-3nic-existing-vnet.json

To deploy in a new VNET:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-11-2487/ivanti-2nic-new-vnet.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-11-2487/ivanti-3nic-new-vnet.json

Google Cloud Platfrom:

The following GCP gateway image is applicable to this release:

- https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-GCP-ICS-22.6R2.1-2487.1.tar.gz

The following templates are applicable to this release:

To deploy in existing VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-11-2487/ivanti-ics-2-nics-existing-vpc.zip
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-11-2487/ivanti-ics-3-nics-existing-vpc.zip

To deploy in new VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-11-2487/ivanti-ics-2-nics-new-vpc.zip
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-11-2487/ivanti-ics-3-nics-new-vpc.zip

22.6R2

- 22.6R2 Package: https://pulsezta.blob.core.windows.net/gateway/nsa/22.6R2-nSA-package-2365.1.pkg

VMware vSphere:

The following OVF template is applicable to this release:

- https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-VMWARE-ICS-22.6R2-2365.1.zip

KVM:

The following KVM template is applicable to this release:

- https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-KVM-ICS-22.6R2.1-2365.1.zip

Cloud Deployments:

Amazon Web Services (AWS):

The following JSON template files are applicable to this release:

To deploy in an existing VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-9-2365/ivanti-2nic-existing-vpc.json

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-9-2365/ivanti-3nic-existing-vpc.json

To deploy in a new VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-9-2365/ivanti-2nic-new-vpc.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-9-2365/ivanti-3nic-new-vpc.json

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

1. Log into the AWS console.
2. Navigate to EC2 > Images > AMIs.
3. Select "Public Images".
4. Search for the image corresponding to your selected hypervisor: Nitro: ISA-V-NITRO-ICS-22.6R2-2365.1.img
5. Make a note of the corresponding AMI ID.

Microsoft Azure:

Image : https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-HYPERV-ICS-22.6R2-2365.1-SERIAL-hyperv.vhd

The following JSON template files are applicable to this release:

To deploy in an existing VNET:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-9-2365/ivanti-2nic-existing-vnet.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-9-2365/ivanti-3nic-existing-vnet.json

To deploy in a new VNET:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-9-2365/ivanti-2nic-new-vnet.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-9-2365/ivanti-3nic-new-vnet.json

Google Cloud Platform:

The following GCP gateway image is applicable to this release:

- https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-GCP-ICS-22.6R2-2365.1.tar.gz

The following templates are applicable to this release:

To deploy in existing VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-9-2365/ivanti-ics-2-nics-existing-vpc.zip
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-9-2365/ivanti-ics-3-nics-existing-vpc.zip

To deploy in new VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-9-2365/ivanti-ics-2-nics-new-vpc.zip
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-9-2365/ivanti-ics-3-nics-new-vpc.zip

22.5R2.3

22.5R2.3 Package: https://pulsezta.blob.core.windows.net/gateway/nsa/22.5R2.3-2215.pkg

22.5R2.1

- 22.5R2.1 Package: https://pulsezta.blob.core.windows.net/gateway/nsa/22.5R2-nSA-package-2035.1.pkg

VMware vSphere:

The following OVF template is applicable to this release:

- https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-VMWARE-ICS-22.5R2.1-2035.1.zip

KVM:

The following KVM template is applicable to this release:

- https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-KVM-ICS-22.5R2.1-2035.1.zip

Cloud Deployments:

Amazon Web Services (AWS):

The following JSON template files are applicable to this release:

To deploy in an existing VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-8-2035/ivanti-2nic-existing-vpc.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-8-2035/ivanti-3nic-existing-vpc.json

To deploy in a new VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-8-2035/ivanti-2nic-new-vpc.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-8-2035/ivanti-3nic-new-vpc.json

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

1. Log into the AWS console.
2. Navigate to EC2 > Images > AMIs.
3. Select "Public Images".
4. Search for the image corresponding to your selected hypervisor: Nitro: ISA-V-NITRO-ICS-22.5R2.1-2035.1.img
5. Make a note of the corresponding AMI ID.

Microsoft Azure:

Image : https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-HYPERV-ICS-22.5R2.1-2035.1-SERIAL-hyperv.vhd

The following JSON template files are applicable to this release:

To deploy in an existing VNET:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-8-2035/ivanti-2nic-existing-vnet.json

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-8-2035/ivanti-3nic-existing-vnet.json

To deploy in a new VNET:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-8-2035/ivanti-2nic-new-vnet.json
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-8-2035/ivanti-3nic-new-vnet.json

Google Cloud Platform:

The following GCP gateway image is applicable to this release:

- https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-GCP-ICS-22.5R2.1-2035.1.tar.gz

The following templates are applicable to this release:

To deploy in existing VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-8-2035/ivanti-ics-2-nics-existing-vpc.zip
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-8-2035/ivanti-ics-3-nics-existing-vpc.zip

To deploy in new VPC:

- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-8-2035/ivanti-ics-2-nics-new-vpc.zip
- https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-8-2035/ivanti-ics-3-nics-new-vpc.zip

22.4R2.3

22.4R2.3 Package: https://pulsezta.blob.core.windows.net/gateway/nsa/22.4R2.3-2159.pkg

22.4R2.2

- 22.4R2.2 Package: https://pulsezta.blob.core.windows.net/gateway/nsa/22.4R2.2-2149.pkg

22.4R2.1

- 22.4R2.1 Package: https://pulsezta.blob.core.windows.net/gateway/nsa/22.4R2.1-1725.pkg

22.4R2

- 22.4R2 Package: https://pulsezta.blob.core.windows.net/gateway/nsa/22.4R2-nSA-package-1531.1.pkg

To upgrade to Release 22.4R2, 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-22.4R2-1531.1.zip
- KVM
  KVM Template applicable to this release:
  https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-KVM-ICS-22.4R2-1531.1.zip

Cloud Deployments:

- Amazon Web Services (AWS):

  The following JSON template files are applicable to this release:

  To deploy in an existing VPC:

  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-4-1531/ivanti-2nic-existing-vpc.json
  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-4-1531/ivanti-3nic-existing-vpc.json

  To deploy in a new VPC:

  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-4-1531/ivanti-2nic-new-vpc.json
  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/AWS/23-4-1531/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-22.4R2-1531.1-SERIAL-nitro.img

- Microsoft Azure

  Image applicable to this release:

  - https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-HYPERV-ICS-22.4R2-1531.1-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/23-4-1531/ivanti-2nic-existing-vnet.json
  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-4-1531/ivanti-3nic-existing-vnet.json

  To deploy in a new VNET:

  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-4-1531/ivanti-2nic-new-vnet.json
  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/Azure/23-4-1531/ivanti-3nic-new-vnet.json

- Google Cloud Platform

  The following GCP gateway image is applicable to this release:

  - https://pulsezta.blob.core.windows.net/gateway/nsa/ISA-V-GCP-ICS-22.4R2-1531.1.tar.gz

  To deploy in an existing VPC

  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-4-1531/ivanti-ics-2-nics-existing-vpc.zip
  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-4-1531/ivanti-ics-3-nics-existing-vpc.zip

  To deploy in new VPC

  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-4-1531/ivanti-ics-2-nics-new-vpc.zip
  - https://pulsezta.blob.core.windows.net/gateway/nsa/templates/GCP/23-4-1531/ivanti-ics-3-nics-new-vpc.zip

What's New

22.7R1

- **Admin Experience Enhancements**: To enhance the administrative experience, there have been improvements in the form of table modernization for both Admin Management and Session Management. For details, see nSA Administration.
- **Password Strengthening for Local Authentication Server**: The local authentication server has stronger password restrictions. For details, see Workflow: Creating a Local Authentication Policy.

22.6R1

- **IPv6 L3 VPN Application Visibility** (Supported only for 22.x ICS Gateway): Support for IPV6 L3 VPN visibility in nSA. You can view both IPv4 and IPv6 applications for L3 user sessions from the Applications overview page. For details, see Using the Applications Filter Bar.
- **nSA Named User License Normalization** (Supported only for 22.6R2 ICS Gateway with 22.6R1 ISAC Client and later versions): Normalization of license seat reservation across devices and users. Single license is consumed instead of two through associating devices with users for Machine Cert Authentication and subsequent User Authentication. For details, see nSA Licensing/Subscription.
- **Licensing Enhancements for named user licenses (UAL)**: Support added to perform out of band license checks. The subscription page in nSA tenant admin portal will be updated with few minutes of delay from the new user login.
- **nSA Feature parity with 22.6R2 ICS gateway**
  - Resource policies > VPN Tunnelling > Connection Profile > DHCP Subnet - 22.x
  - HTML5 Bookmark - Enable Auto Resolution Option - 22.x and 9.x
  - User Roles Options - Enable Auto Resolution Option - 22.x and 9.x
  - System > Configuration > SAML > New SAML > Hide PDP Option - 22.x
  - Hide Authentication > Auth Servers > LDAP server > Health check - Test username, Test Password and Validate User Credential fields - 9.x

  - Authentication > Auth Servers > LDAP server > Health check - Test username, Test Password and Validate User Credential fields - 22.x
  - System > Configuration > Security > Miscellaneous > Relay state option - 22.x
- **Support SAML Authentication server as a secondary authentication server when configuring Certificate Authentication server** (Supported only for 22.x ICS Gateway): nSA now supports configuration of Certification Authentication server with SAML Authentication server as a secondary authentication server. For details, see Configuring Certificate Authentication Server.
- Admin experience enhancements to L4, Gateway Logs, and Logs Tables in terms of selection and resizing, pagination, and text copy/paste

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

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

For details, see Using the Top Active Breakdown Charts and Filtering the Logs.

22.5R1

- **Auto Selecting Dependent Configurations as part of Config Sync**: While creating config sync rule, if there is any dependency mismatch, admin can review dependent configurations and select them before creating/editing rule. For details, see Config Synchronization.

  For example, If realm configuration is mapped to Authentication server and if config sync rule is created with only realm. The dependent configuration is highlighted (Auth server). Realm configuration is highlighted with i icon and when dependencies are reviewed, Authentication server is mentioned in the dependency tree.
- Preview of changes done in source gateway before config sync. This feature is available only with Manual sync.

Preview before sync will work only when one manual config sync rule is triggered.

- 22.5R2 ICS configuration parity in nSA.
- **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 Creating Admin Policies.
- **nSA Licensing Enhancements**: When nSA licensing is enabled on Gateway, and if there is connectivity issue between gateway and controller, grace period of 24 hours is applied for new user logins up to platform limit.

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

22.4R1

- **Analytics: Historical View**: Analytics supports data visualization in Active View. Admin can see the historic data on different time windows. Admin's can find all connections details for different time frames past 30 days. For details, see Using the Filter Bar
- **Config Sync Rule Status**: This feature allows a user to view the config sync rule status of all target gateways. For details, see Config Synchronization.
- **nSA named user licensing normalization**: This feature allows a user to use different login formats - Domain\username, Common Name (CN), and User Principal Name (UPN) - from different devices, but consumes only one seat for the user. For details, see nSA Licensing/Subscription.

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.

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 and Later

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: KB44877.

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:

- Analytics Dashboard and Gateway logs are not synchronized with nSA when using an ICS gateway on the cloud running version 22.5R2 or above.
- Gateway ESAP package version 4.1.6 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

- 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.
- 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.

Additional Notes

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

Fixed Issues

The following table describes the issues resolved.

Problem Report	Description
22.7R1	
PZT-44896	ICS Gateway Packages Release Date shown is incorrect under Installation Packages.
PZT-44862	License Subscription expired message shown for user with Active subscription.
PZT-44311	Gateway connectivity issues and the intermittent log uploading issue seen with nSA.
PZT-44103	Config synchronization and Report Generation issue with Single Node cluster.
9.1R18.5/22.6R2.3 (ICS GW)	
PZT-43145	When the client connection set was chosen, certificates were indicated as dependencies.
PZT-43104	Event Log Issues related to external syslog server connection reset.
PZT-43095	Gateway is in nSA licensing mode but unable to connect to Ivanti Neurons for Secure Access' to fetch user license
PZT-43035	The new user registration process should dispatch the authentication URL instead of the enrollment URL.
PZT-42338	The configuration upload to nSA or Pulse one will be initiated again incase there are additional users logging in. If there are constant new users logging in, the full configuration upload will take longer.
PZT-41970	Config rule push status for the failed gateway will be in "pending" state in nSA Admin UI.
PZT-41961	Config sync push fails if /configuration/system/maintenance/options/gro-on-off is selected.
PZT-42809	Gateway status constantly changes from not ready to ready on the nSA platform.
PZT-41472	The status of the configuration synchronization template is stuck in the Pending state.

Problem Report	Description
PZT-43133	Number of Users exceeds Realm Capacity error seen with nSA Licensing Mode enabled.
22.6R1.2	
PZT-37841	Report format CSV/JSON has the epoch timestamp instead of human readable.
PZT-42285	Incorrect selected user roles displayed for Split tunneling policies.
PZT-42378	Peer SP configurations are not getting uploaded to nSA with appropriate title.
PZT-42049	Gateway information not being synced with nSA on 22.5R2.1 version.
PZT-41931	ICS is synchronizing users in Auth Servers to Pulse One.
PZT-41850	ICS Gateway (Event, Admin and user access) Logs are not seen in nSA controller.
PZT-41637/PZT-41354	HTTP error 500 after PUT and Unknown errors in Gateway Events Access logs
PZT-41535	Config sync rule on the nSA shows Failed and Pending status.
PZT-42012	Unsupported attribute type 0' errors in Gateway Admin Access logs during config sync operation
PZT-41970	Config rule push status for the failed gateway will be in "pending" state in nSA Admin UI.
22.6R1	
PZT-41418	nSA Subscription users page is not listing users when the number of reserved license seats are more than 20K. Pagination is now added on User Table UI page along with new UX table changes.
PZT-41470	SAML authentication server configuration with incorrect values.
PZT-41471	Configuration changes made through the nSA UI to the ‘source’ gateway do not reflect or have a very long delay in being reflected in Multinode Config Synchronization templates.
PZT-41473	Incorrect selected user roles displayed for Split tunneling policies.
PZT-41334	Pagination not working with user roles in nSA.

Problem Report	Description
PZT-40864	nSA Reports: Dropdown shows max 100 options (all dropdowns).
PZT-38774	When multiple client packages are present in gateway, errors are seen while uploading configurations to nSA.
PZT-36639	ICS not sending logs to nSA and sessions are not reported.
22.5R1.3	
PZT- 41484	Data is not loading under Insight > Applications.
22.5R1.2	
PZT-41074	Upload ESAP Packages issue on nSA is fixed.
PZT-40843	Fixed log swap issue between the gateway and timestamp fields
22.5R2.1 (ICS GW)	
PZT-40795	As part of logs optimization, Optimized (reduced) the number of API calls triggered from gateways to controller.
PZT-40794	As part of logs optimization, Optimized the critical log message in Gateway Readiness API calls from gateways.
PZT-40730	As part of logs optimization, fixed Gateway getting disconnected and connection error due to SSL read error log messages.
PZT-40706	Fixed issue where sometimes Config upload was triggered quite frequently with no config change done on the gateway.
PZT-40843	Log swap issue, where Gateway and Timestamp fields are interchanged after line #1001 is fixed.
22.5R1	
PZT-40361	ICS is shown as Default upon first login after tenant creation.
PZT-40068	When Terminal Service Profile had special characters the config upload fails.
PZT-38883/38860	Log enhancements in event logs for failure cases.
22.4R2.1 (ICS GW)	

Problem Report	Description
PZT-39635	Program unityConfigSpli fails after gateway reboot and config upload.
PZT-39366	Program jsonConfigHelpe failed, error message is displayed during cofig upload.
22.4R2	
PZT-38102	Program failed after upgrading to latest 22.4R2 builds.
22.4R1	
PZT-38859	Unable to create terminal services profile from nSA
PZT-37709	Pushing full configuration to blank target does not happen.
PZT-38837	Entire config sync is failing with 'Node 'bookmark' identifier count mismatch' error.
PZT-38827	Trying to modify configurations on ICS through nSA Interface, then you have to submit the configuration change multiple times.
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.
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.

Problem Report	Description
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	
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.

Problem Report	Description
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.

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

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

Problem Report	Description
22.6R1.2	
PZT-42338	**Symptom**: The configuration upload to nSA or Pulse one will be initiated again incase there are additional users logging in. If there are constant new users logging in, the full configuration upload will take longer. **Workaround**: None
22.6R1	
PZT-41640	**Symptom**: SAML dependencies check does not include all checks, while creating the config sync rule. **Condition**: When any configuration is dependent on the SAML Auth server, whether it is being used as a service provider or identity provider. **Workaround**: Manually select all the SAML dependencies.
PZT-41354	**Symptom**: HTTP error 500 after PUT and Unknown errors in Gateway Events Access logs **Condition**: Observed during Gateway rollback. **Workaround**: No functional impact. Config upload works fine upon retrying.
PZT-42049	**Symptom**: Analytics Dashboard and Gateway logs are not synced with nSA. **Condition**: ICS Gateways running on cloud with version 22.5R2 or above. **Workaround**: NA
PZT-42012	**Symptom**: 'Unsupported attribute type 0' errors in Gateway Admin Access logs during config sync operation. **Condition**: Observed when config sync operation is performed where source gateway is running on R1 build (FIPS) and target gateway is running R2 build (Non FIPS) **Workaround**: Exclude security settings from config sync rule.

Problem Report	Description
PZT-41970	**Symptom**: Config rule push status for the failed gateway will be in "pending" state in nSA Admin UI. **Condition**: Config sync rule might fail for one of the target gateways, if entire config sync is pushed to multiple gateways. **Workaround**: Delete the failed gateway entry from the config rule and create new config rule for the failed gateway only.
PZT-41961	**Symptom**: Config sync push fails if /configuration/system/maintenance/options/gro-on-off is selected. **Condition**: This issue can be seen for both Hardware appliances as well Virtual appliances. **Workaround**: Avoid selecting this option while creating a config sync rule.
22.5R1	
PZT-40105	**Symptom**: Dependency check for resources policies. **Condition**: When resource policies are part of config sync rule. **Workaround**: Do not include resource policies in selective config sync rule or skip dependency check.
PZT-40644	**Symptom**: HTTP PUT errors observed in logs. **Condition**: When Gateway is registered with nSA sometimes HTTP put errors observed in Events logs. **Workaround**: NA
22.4R3	
PZT-39636	**Symptom**: When RBAC user navigates to Config Sync rule page, you may not see config sync rules properly. **Condition**: While creating RBAC role with connect secure Gateway permissions, user does not select GW's under selected Gateways list which are part of Config Sync rule.

Problem Report	Description
	Workaround: Make sure to select all GW's under selected Gateways which are part of config sync rule while creating RBAC role.
22.4R2	
PZT-39635	**Symptom**: Program unityConfigSpli fails after gateway reboot. **Condition**: When gateway is registered with nSA and upon gateway reboot. **Workaround**: NA
22.4R1	
PZT-39310	**Symptom**: Config upload post Gateway reboot fails when configurations with resource profile name containing unicode characters. For example but not limited to : ¯, ß, ð, ƒ, ©, þ. **Workaround**: Identify the unicode characters in resource profile and remove them from gateway.
PZT-38809	**Symptom**: Admin may not find all application names in the sanky chart which are listed in the access trend chart. **Workaround**:NA
PZT-38806	**Symptom**: Admin may see some text and labels in lower case and some in upper case **Workaround**: NA
PZT-38774	**Symptom**: When multiple client packages are present in gateway, errors are seen while uploading configurations to nSA. **Workaround**: It is recommended to have only one client package in Gateway.

Problem Report	Description
PZT-38670	**Symptom**: Binary config import from a Gateway, which is registered to a different nSA, client certificates are getting replaced. After the import is successful, as the client certificates are getting replaced GW is trying to communicate to a different nSA due to which GW is going to "not ready" state. **Workaround**: After the binary configuration import is successful, we need to remove the client certificates and re-register the GW.
PZT-38714	**Symptom**: If one of the gateways goes down in a cluster, nSA is not showing the active session with another gateway, it still shows connected with the gateway which is down. **Workaround**: NA
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.

Problem Report	Description
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: 1. Power cycle Node-2. 2. Press Tab and boot into Standalone mode. 3. Access the UI and follow the procedure mentioned in https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44877/?kA13Z000000L3Z5 to clean up space. 4. Reboot and join the cluster. Upgrade should now go through fine.
22.2R1	
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.

Problem Report	Description
	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
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.

Problem Report	Description
	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.

Problem Report	Description
	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.
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.

Problem Report	Description
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.
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%.

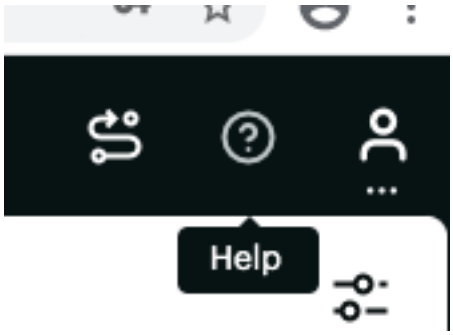
Problem Report	Description
	Condition: Admin starts Gateway upgrade from nSA, and then observes the download percentage. **Workaround**: Wait for package download operation to complete, even if the % goes to around 120%.
PCS-31734	**Symptom**: nSA ICS Overview dashboard Info panel shows empty values 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.
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

Problem Report	Description
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
PCS-30305	**Symptom**: Cluster Table is not getting updated when user tries to destroy the registered Virtual ICS/ PCS Gateway from ESXi server.

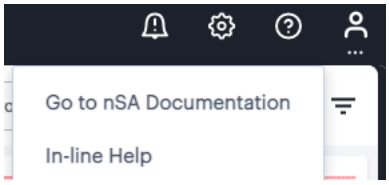
Problem Report	Description
	Condition: Destroy the Gateway in ESXi server without deleting the Cluster. **Workaround**: Delete the created Cluster and then destroy the virtual Gateways in ESXi server.
PCS-30802	**Symptom**: nslookup with TXT query returns large response then 403 error is seen in Admin 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.

Documentation and Technical Support

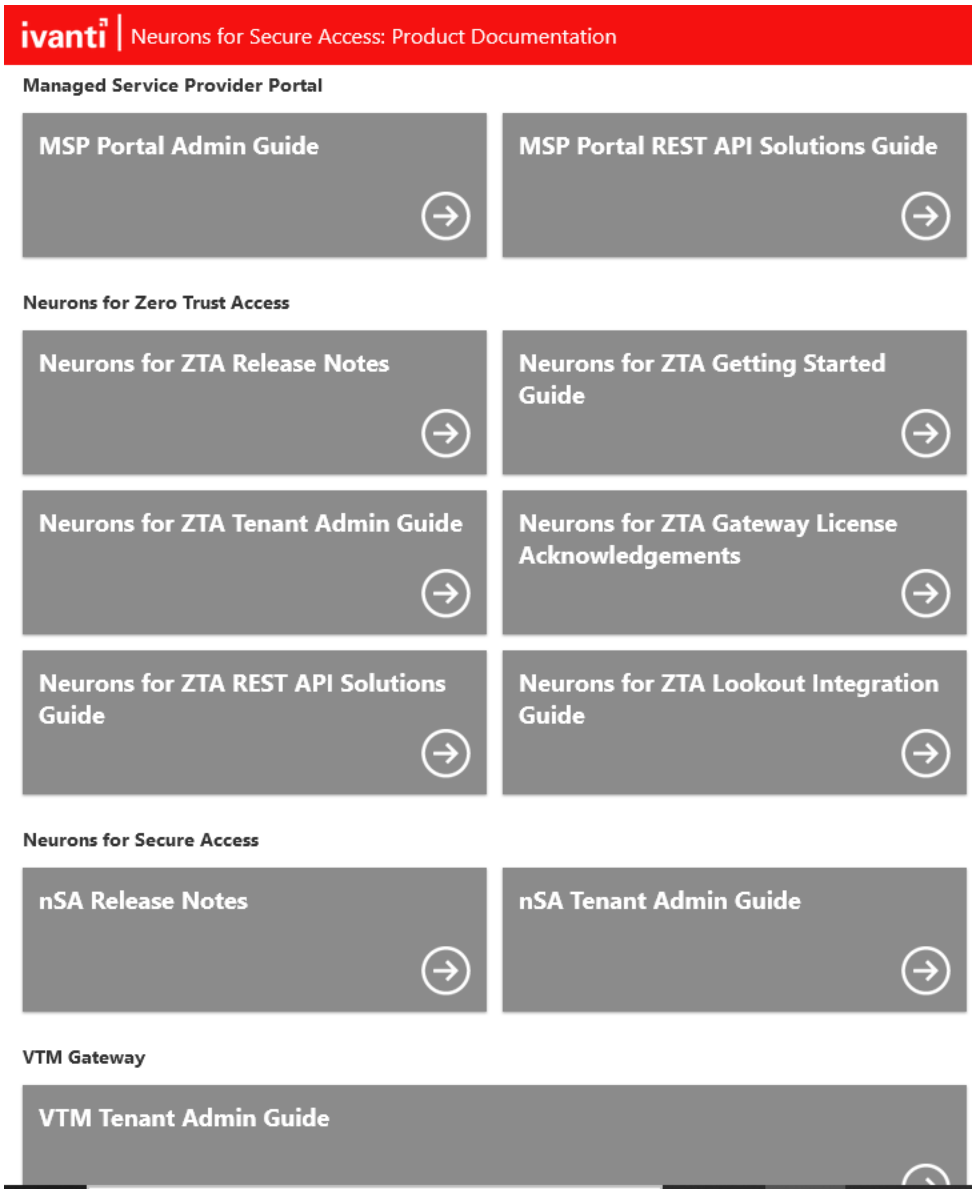
nSA documentation for administrators is available from the Tenant Admin portal. If you are an administrator, login to the portal using the URL provided in your welcome email after setting up your product subscription. To access product help and documentation links, click the "?" help icon in the navigation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



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



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



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 https://help.ivanti.com/. 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

Revision History

The following table lists the revision history for this document.

Revision	Revision Date	Description
2.3	April 2024	Fixed Issues list is updated for 22.7R1
2.2	March 2024	22.7R1 release notes created
2.1	February 2024	22.6R1.7 release notes created
2.0	February 2024	22.6R1.6 release notes created
1.9	January 2024	22.6R1.5 release notes created
1.8	October 2023	22.6R1 release notes created
1.7	July 2023	22.5R1 release notes created
1.6	June 2023	22.4R3 release notes created
1.5	April 2023	22.4R1 release notes created
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