



# ICE Server Air Gap Installation Guide

Product guide for prerelease

Copyright © 2024, Instant Connect Software, LLC. All rights reserved.

Document version 1841, produced on Friday, September 06, 2024.

main 90adc8bf40040649230176bbdd465f6261a2d8e0

ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. STA GROUP DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL INSTANT CONNECT LLC OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF STA GROUP OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Trademarks mentioned in this document are the properties of their respective owners.

## Contents

<b>1</b>	<b>Document History</b>	<b>6</b>
<b>2</b>	<b>Overview</b>	<b>7</b>
<b>3</b>	<b>Pre-installation</b>	<b>8</b>
<b>4</b>	<b>Virtualization Guidance</b>	<b>9</b>
<b>5</b>	<b>Create a virtual machine (VM) to run ICE OS</b>	<b>11</b>
<b>6</b>	<b>Start up the ICE OS VM</b>	<b>13</b>
<b>7</b>	<b>ICE OS terminal screens</b>	<b>14</b>
7.1	Start . . . . .	14
7.2	Node Config . . . . .	15
7.3	Access Code . . . . .	16
<b>8</b>	<b>ICE OS Configuration Wizard</b>	<b>17</b>
8.1	Verify connection . . . . .	17
8.2	Wizard UI overview . . . . .	17
8.3	Profile . . . . .	21
8.4	Network . . . . .	21
8.5	Storage . . . . .	22
8.6	Kubernetes . . . . .	23
8.7	Version . . . . .	23
8.8	TLS Certs . . . . .	24
8.9	Server . . . . .	25
8.10	Telephony . . . . .	26
8.11	External Log Store . . . . .	27
8.12	Monitoring . . . . .	27
8.13	Finish . . . . .	28
<b>9</b>	<b>Post-installation</b>	<b>30</b>
9.1	Retrieve initial passwords for superuser and Grafana accounts . . . . .	30
9.2	ICE Desktop: Setup the superuser account . . . . .	31
9.2.1	Change the superuser password . . . . .	31
9.3	ICE Desktop: Apply your ICE license . . . . .	35
9.3.1	Request a license . . . . .	36

9.3.2	Apply the ICE Server license . . . . .	36
9.4	Grafana: System monitoring . . . . .	37
9.4.1	Login to Grafana . . . . .	37
9.4.2	Grafana dashboards . . . . .	37
<b>10</b>	<b>Next steps...</b>	<b>39</b>
<b>11</b>	<b>Appendix A: Generate an SSH-RSA key</b>	<b>39</b>
11.1	For Windows . . . . .	40
11.2	For MacOS . . . . .	41
<b>12</b>	<b>Appendix B: Log retention using Vector</b>	<b>42</b>
12.1	ICE Server configuration for the Vector agent . . . . .	42
12.2	Vector configuration for ICE Server . . . . .	44
12.3	Example configuration . . . . .	45
<b>13</b>	<b>Appendix C: Installation status processes</b>	<b>45</b>
<b>14</b>	<b>Appendix D: Installing local patch server or static reflector</b>	<b>47</b>
14.1	Installing local patch server on Ubuntu via docker . . . . .	47
14.2	Installing local static reflector on Ubuntu via docker . . . . .	48

## List of Tables

## 1 Document History

---

Date	Release	Notes
May 28, 2024	3.5.1	Updated ICE version reference to 3.5.41629.
April 15, 2024	3.5.0	Updated ICE version reference to 3.5.41160. The 'ICE OS terminal screens' and 'ICE OS Configuration Wizard' have been significantly updated.
January 29, 2024	3.4.0	Added a note regarding geo-redundancy to the 'Hosting' bullet in the 'Virtualization Guidance' section.
October 27, 2023	3.4.0	Added <i>'Appendix D: Installing local patch server or static reflector'</i> section.
October 23, 2023	3.4.0	Updated airgap version to <a href="#">iceos-airgap-release-3.4.0-3.4.31412-652</a> .
October 11, 2023	3.4.0	Minor updates to <i>Network</i> , <i>Kubernetes</i> , and <i>TLS Certs</i> sections.
October 10, 2023	3.4.0	Updated X.509 certificate validity period to 397 days (13 months) or less. Added note to use VMware <i>EXSi</i> , instead of <i>vCenter Server</i> , to set VM latency sensitivity setting to 'Medium'.
September 20, 2023	3.4.0	Updated ICE Server version reference to 3.4.30527. The 'ICE OS terminal screens' and 'ICE OS Configuration Wizard' have been significantly updated.
July 27, 2023	3.3.0	Updated ICE Server version reference to 3.3.28975. 'ICE Desktop: Apply your ICE license': Added explanation that some features are not accessible until an appropriate license is applied.
July 24, 2023	3.3.0	Updated ICE Server version reference to 3.3.28856. The 'Virtualization Guidance' and 'ICE OS Configuration Wizard' have been significantly updated.
April 25, 2023	3.2.0	Updated ICE Server version reference to 3.2.26273.
March 17, 2023	3.2.0	Updated instructions to identify, download, and mount the correct ISO file(s) for the VM.
February 13, 2023	3.2.0	Updated VM latency sensitivity setting to 'Medium' (previously was 'High').

Date	Release	Notes
January 30, 2023	3.2.0	Added additional settings for 'CPU' when creating a VM, updated virtualization guidance and VM creation information.
January 13, 2023	3.2.0	Updated screenshots to reflect current UI, updated installation and configuration steps to reflect current UI, updated settings and guidance for VMs, removed 'Appendix B: Nginx Load Balancer Example' and added it to the <b>ICE Server Installation with Kubespray Guide</b> .
December 1, 2022	3.2.0	Updated screenshots to reflect current UI, added 'Appendix B: Nginx Load Balancer Example' (from the <b>ICE Server Administration Guide</b> ) in support of the 'Reverse Proxy Access' feature. Added virtualization hardware guidance for snapshots and disk consolidation. Added 'Appendix C: Log retention using Vector'. Added note on blocking port 80.
September 26, 2022	3.1.2	Renamed document to <b>ICE Server Air Gap Installation Guide</b> (formerly <b>ICE OS Air Gap Installation Guide</b> ). Added/updated virtualization hardware guidance, new fields, HTTPS, Telephony, ICE license activation, DHCP support, Grafana dashboards.
June 15, 2022	3.1.1	Document created.

## 2 Overview

**ICE OS** is a proprietary Linux-based operating system which allows for a streamlined installation of **ICE Server** as single node Kubernetes cluster, including support for air gapping. This document walks through the installation process:

1. Pre-installation
2. Create and startup an ICE OS virtual machine (VM).
3. Begin ICE OS configuration via the terminal screens.
4. Finish ICE OS configuration via the web browser-based 'ICE OS Configuration Wizard'.
5. Post-installation

### 3 Pre-installation

In preparation for the installation, please complete the following checklist:

1. Download the latest ISO files from the Instant Connect Support Portal:
  1. Navigate to: <https://support.instantconnectnow.com/s/downloads>
  2. Select the 'Instant Connect Enterprise Software' folder.
  3. Select the 'ICE 3.5.1 Software' folder.
  4. Select the 'Download' button for both of the following:
    - 3.5.1 [ICE Server Installer](#): The downloaded ZIP folder is named `iceos-3499-release-3.5.1.zip`.
    - 3.5.1 [ICE Server for Airgap Installation](#): The downloaded ZIP folder is named `iceos-airgap-release-3.5.1-3.5.41629-41630.zip`.
  5. Extract the following ISO files from the ZIP folders:
    - `iceos-release-3-5-1-git-3641870-3499.iso`
    - `iceos-airgap-release-3-5-1-41629.41630.iso`
2. Acquire a public/private key pair for secure shell protocol (SSH). You will need enter the public key certificate during the installation process.

#### Notes:

- All X.509 certificates used for Instant Connect must expire in 397 days (13 months) or less. This includes server certificates, intermediate CA, root CA, etc. Certificates whose expiration dates exceed this validity period will not be accepted by Instant Connect clients, resulting in 'Cannot connect to server' error messages.
- Per industry standard best practice, it is recommended to block port 80 when using certificates. This is done via the following command:

```
/sbin/iptables -A INPUT -p tcp --destination-port 80 -d X.X.X.X -j DROP
```

(If using the ICE Cisco IP Phone XML client, though, a firewall rule will need to be implemented allowing access to port 80.)

3. Verify that the computer used when accessing the 'ICE OS Configuration Wizard' is accessible on the ICE OS VM's network.



4. Verify that both a working DNS server (or servers) and an NTP server are accessible on the ICE OS VM's network. ICE OS requires both in order to install and maintain the ICE Server. The DNS lookup time must be 5 seconds or less.

To verify a DNS server is working, run the `nslookup` command.

- If the response resolves a hostname, reverse lookups an IP, or says 'host not found', then the DNS server is working.
- If there is a timeout error, then the DNS server is *NOT* working.

**Note:** The DNS server does *NOT* need:

- An internet connection.
- To resolve hosts on the internet.
- To resolve cluster hostnames.
- To perform reverse IP lookups.

**Note:** If there is no DNS server, as a workaround, give the DNS the exact same address as the ICE server.

5. Verify that port 8999 is available, e.g., not blocked by a firewall.

## 4 Virtualization Guidance

Please consult the documentation for your virtualization platform and hardware for best practices and specific configuration recommendations, e.g., VMware product documentation.

- **Deployment size:** Specify the deployment size and verify the availability of minimum virtual machine requirements (more is *always* better):

Size	CPU cores	Memory	Disk space
Lite	4	16Gb	250Gb
Small	8	32Gb	500Gb
Medium	12	48Gb	750Gb
Large	16	64Gb	1Tb

**Notes:** The web browser-based install wizard will ask you to specify one of the above deployment sizes and will then verify that the minimum system requirements are available, if it is not, then you will be unable to proceed with the installation.

- **Solid state drive (SSD):** Verify the host server's hard drives are sufficient. We *strongly* recommend using an SSD to host the ICE Server VM. ICE Server performance and stability are heavily dependent on (minimal) disk I/O latency, so an SSD is essential for successful deployment. Disk storage for the VM should be created by thick provisioning with highest shares allowed. Please see: VMware: Resource Allocation Shares.

Since traditional spinning drives (HDD) are not recommended, if a customer is using one, then we can only provide support if the ICE Server VM is the only VM running on it. The ICE Server VM cannot be competing with other VMs for disk access. Also, if any drive does not pass the disk performance (speed) test, which is conducted during installation, then the drive is not capable of running ICE Server and the installation will fail. This is likely to be an issue for non-SSD hard drives.

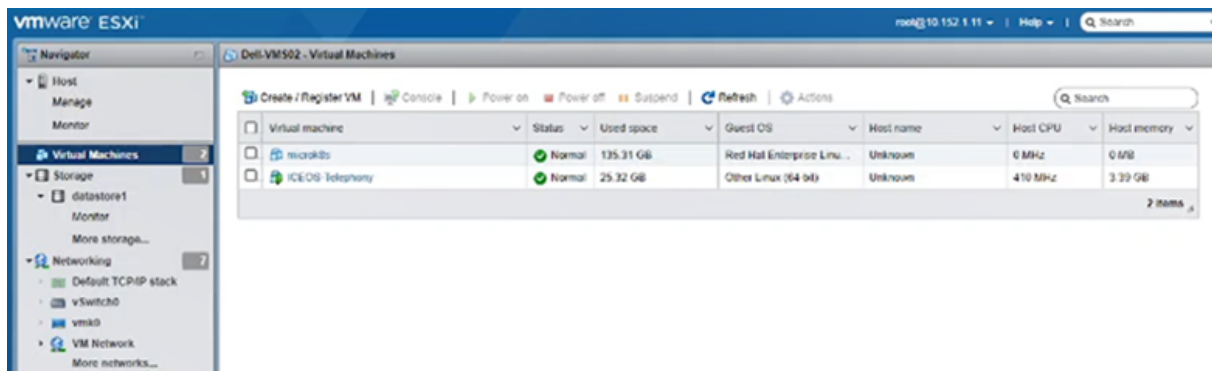
- **Memory:** Memory must not be oversubscribed. As a starting point, assume an amount equal to 25% of total VM memory usage should be allocated for memory overhead. For example, if there are two VMs on a host, and each uses 32Gb of memory (64Gb in total), then allocating an additional 16Gb (at least) for overhead is prudent. Please consult VMware or your virtualization hardware vendor for guidance on appropriate memory overhead based on VM size and type.
- **Processing:** If hyperthreading, then the number of vcpus (cores) used must not be oversubscribed. As a starting point, assume an amount equal to 25% of total vcpus in use should be allocated for hyperthreading overhead. For example, if there are 2 VMs on a host, and each uses 8 vcpus (16 vcpus in total), then allocating an additional 4 vcpus (at least) for overhead is prudent. For hyperthreading, a minimum of 20 vcpus are recommended.
- **Hosting:** Avoid deploying the ICE Server VM on virtualization hardware which also hosts other I/O intensive VMs, e.g., database servers, otherwise the installation will fail.

**For geo-redundancy:** The VMs for DC1 and DC2 should not share the same virtualization hardware host nor be on the same subnet.

- **VM snapshot:** Limit the ICE Server VM to two snapshots. Disk space equal to twice the size of the ICE deployment size should be available for the snapshots. For example, a medium sized ICE deployment of 750Gb, requires at least 1.5Tb of disk space for two snapshots. Delete snapshots after 48 hours. Follow this same guidance for other VMs sharing the same hardware. A build up of snapshots may result in adverse disk I/O performance due to lack of free disk space.

- **Virtual disk consolidation:** If the ESXi console displays the *VMware virtual machine disks consolidation is needed* error message, please address the situation.
- **Virtual disk write cache configuration:** When possible, always set the virtual disk write cache policy to **write-back**, rather than the default of **write-through**. Please consult VMware or your virtualization hardware vendor for additional information.
- **RAID controller firmware:** It is essential to keep the RAID controller firmware up-to-date. Please consult VMware or your virtualization hardware vendor for additional information.

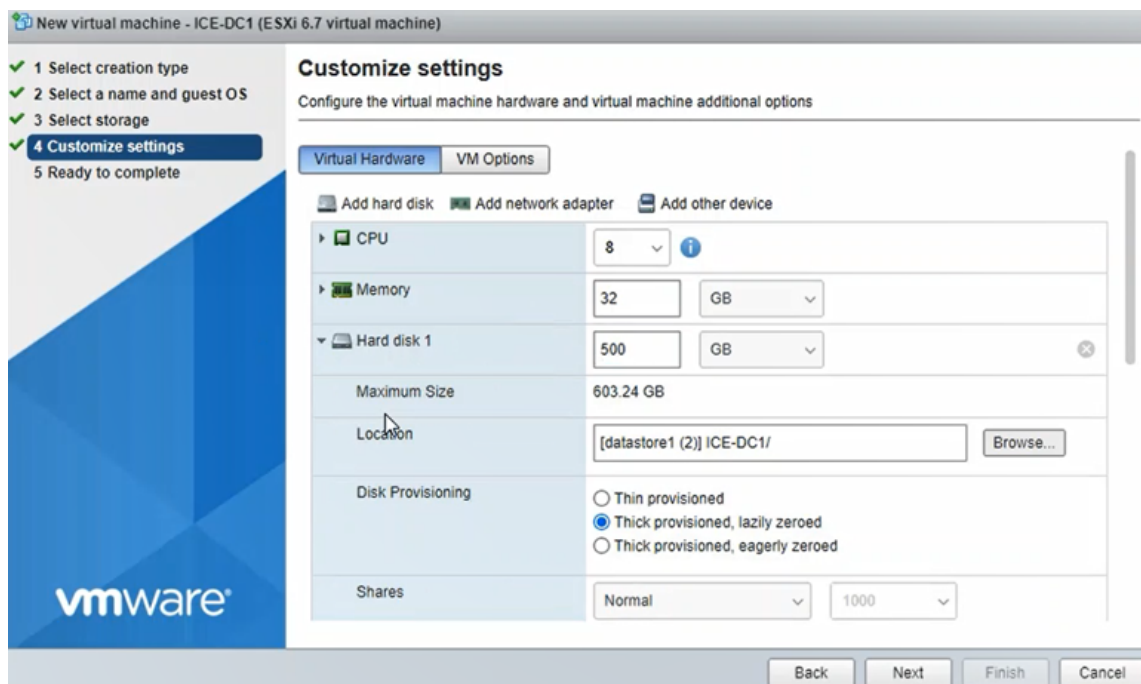
## 5 Create a virtual machine (VM) to run ICE OS



**Note:** We recommend loading all ISOs to a datastore and booting them from there. While ICE OS can be booted from live media (e.g., DVD), we do not recommend that, as the live media always needs to be mounted, otherwise the OS will crash.

1. Open VMware.
  2. Click 'Create / Register VM' to open the 'New virtual machine' wizard.
  3. From the 'Select creation type' screen, select 'Create a new virtual machine', then click 'Next'.
  4. From the 'Select a name and guest OS' screen:
    - Name the VM.
    - Compatibility = ESXi 6.5 (or later) virtual machine.
- Note:** Older versions are *not* recommended. Instant Connect does not support the use of obsolete hypervisors, such as VMware ESXi versions older than 6.5. Instant Connect cannot provide installation, performance, or server-related support to customers using these virtualization products.
- Guest OS family = Linux

- Guest OS version = Other Linux (64-bit)
  - When complete, click 'Next'.
5. From the 'Select storage' screen, select the datastore which contains the ISO files. Make sure at least the minimum required space is available (based on the deployment size specified in your pre-installation planning), then click 'Next'.
  6. From the 'Customize settings' screen (below is an example of a medium deployment):



**Note:** The storage cannot be resized once the VM is created, so verify the appropriate space is available before proceeding.

- CPU = 4, 8, 12, or 16 (minimum based on lite, small, medium, or large deployment size)
  - Cores per Socket = Same as for 'CPU' or as close as possible.
  - Limit = Unlimited
  - Shares = High
- Memory = 16Gb, 32Gb, 48Gb, or 64Gb (minimum based on lite, small, medium, or large deployment size)
  - Reservation = Same as for 'Memory'. Also select 'Reserve all guest memory (All locked)'.
- Hard disk = 250Gb, 500Gb, 750Gb, or 1Tb (minimum based on lite, small, medium, or large deployment size)

- Disk Provisioning = Thick Provisioned, Eagerly Zeroed (recommended), Thick Provisioned, Lazily Zeroed (acceptable)
- Shares = High. If ‘Limit - IOPS’ is configured, then set ‘Shares’ to the maximum allowed.
- Network Adapter 1 = The selected network must have a working DNS server. Also select ‘Connect At Power On’.
- CD/DVD Drive 1 = Select ‘Datastore ISO file’. From the ‘Datastore browser’, select `iceos-release-3-5-1-git-3641870-3499.iso`. Also select ‘Connect At Power On’.
- CD/DVD Drive 2 = Select ‘Datastore ISO file’. From the ‘Datastore browser’, select `iceos-airgap-release-3-5-1-41629.41630.iso`. Also select ‘Connect At Power On’.

**Note:** ‘Drive 1’ must be for the ‘iceos-git’ ISO file. ‘Drive 2’ must be for the ‘airgap’ ISO file. You may need to add a second drive to the VM:

1. Select ‘Add other device’.
2. Select ‘CD/DVD drive’.
3. The second drive is added to the VM.

**Note:** VMware may list the drives in reverse order, so check the drives’ details. One drive is designated as ‘master’ and the other as ‘slave’. The ‘iceos-git’ ISO is for the ‘master’ drive and the ‘airgap’ ISO is for the ‘slave’ drive.

- When complete, click ‘Next’.
7. From the ‘Ready to complete’ screen, click ‘Finish’.
  8. Wait for the VM to be created. Due to the ‘Disk Provisioning’ setting, the disk provision is written at this time.
  9. From the VMware directory, right-click on the newly created ICE OS VM, and select ‘Edit Settings’.
  10. VM Options > Advanced > Latency Sensitivity = Medium
    - Note:** If using VMware’s *vCenter Server*, the ‘Medium’ option may not appear, so instead use their *ESXi* to access the VM and select ‘Medium’.
  11. VM > Boot Options > Firmware = BIOS

## 6 Start up the ICE OS VM

1. From the VMware directory, click the ICE OS VM.

2. From the ICE OS VM details screen, click 'Power on' to start up the VM.
3. The VM opens in a new terminal window displaying the ICE OS terminal screens.

## 7 ICE OS terminal screens

There are three terminal screens to navigate: 'Start', 'Node Config', and 'Access Code'.

**Note:**

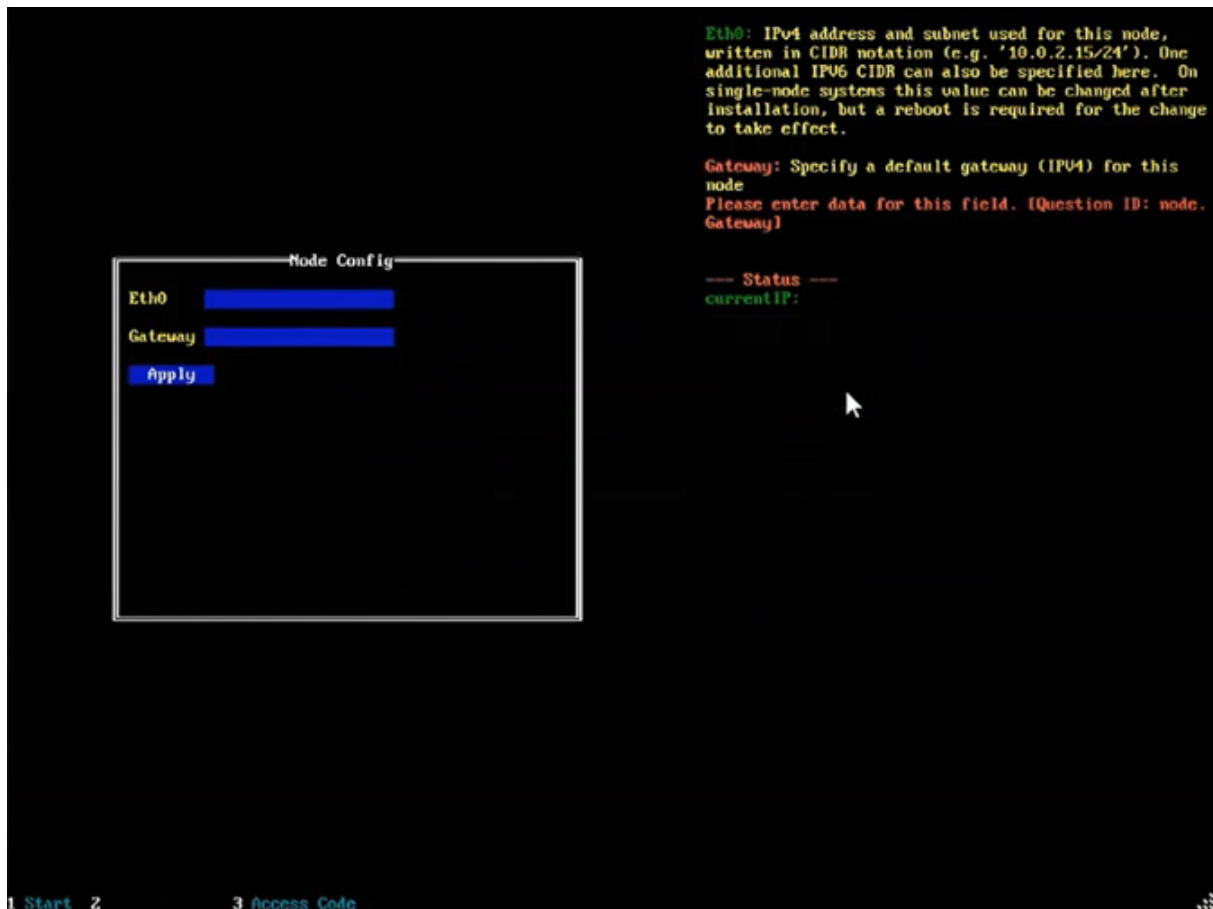
- Use the 'Tab' key on your keyboard to advance through the fields on a screen.
- As you proceed through the UI, please refer to the top, right corner of each screen for helpful configuration information.

### 7.1 Start



From the 'Start' screen, hit 'Ctrl+N' on your keyboard to advance to the 'Node Config' screen.

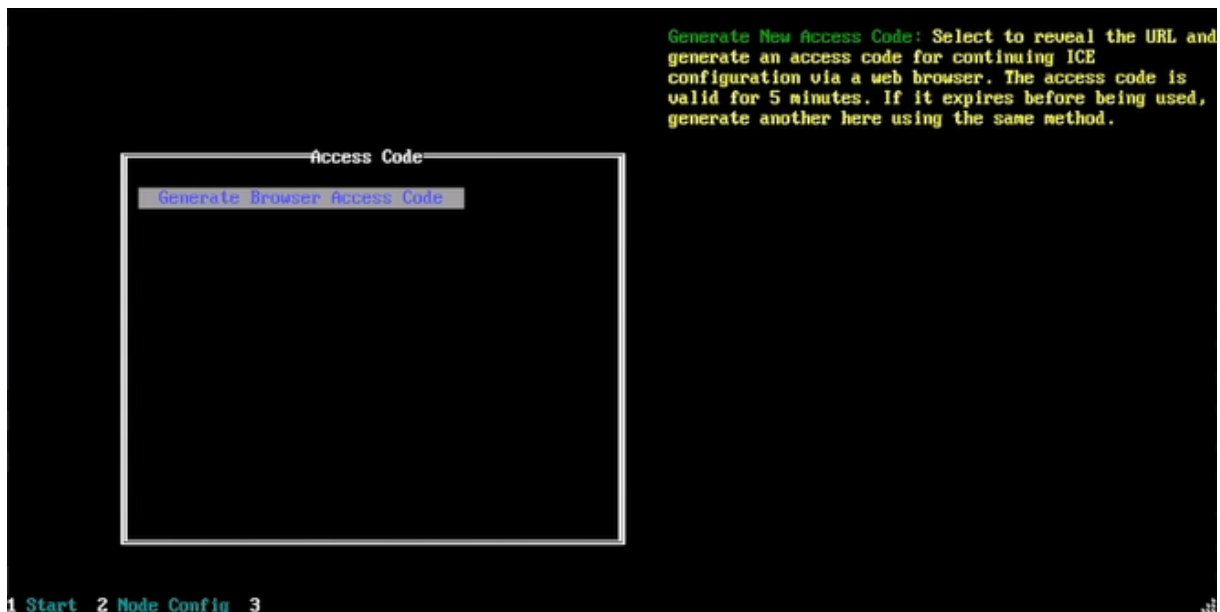
## 7.2 Node Config



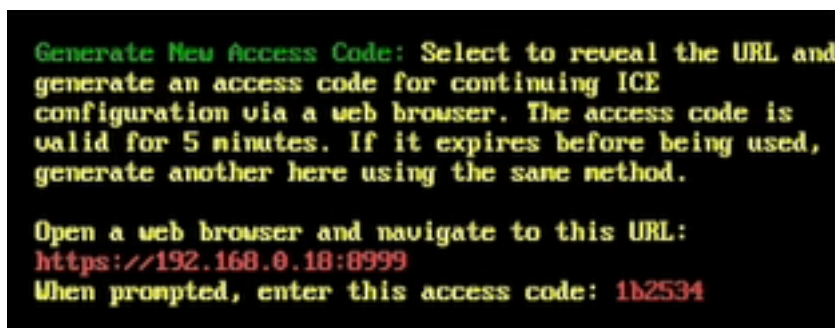
**Note:** ICE Server supports use of Dynamic Host Configuration Protocol (DHCP) for IP address assignment, but does *NOT* support IP address change by lease renewal on the DHCP server, ICE OS on premise, or AWS / Azure. The DHCP service should reserve the assigned IP address exclusively for the ICE OS VM. ICE Server will become inaccessible if the DHCP service assigns a different IP address at any time post-installation. The ICE OS VM's IP address should *NOT* be changed:

- ...after a reboot
  - ...if the DHCP has expired on its own, and got auto-renewed
  - ...if the network administration forces a DHCP renewal
- Eth0 = The IPv4 or IPv6 address for the host node, use CIDR notation. The note on the right will turn from red to green once a valid value is entered.
  - Gateway = The IPv4 address for the default gateway. The note on the right will turn from red to green once a valid value is entered.
  - Apply = To advance to the next screen, tab to the 'Apply' button, then hit the 'Enter' key. This applies the values on the current screen and advances you to the 'Access Code' screen.

### 7.3 Access Code



- Generate Browser Access Code = Hit the 'Enter' key to generate a URL ([https://\[IP address of the VM\]:8999](https://[IP address of the VM]:8999)) and an access code. Both are displayed in the top, right corner of the screen.



The access code is valid for 5 minutes. If it expires before being used, simply return to the above page and generate a new browser access code. The URL will remain the same.

- Open a web browser and navigate to the URL to access the 'ICE OS Configuration Wizard' for the VM.

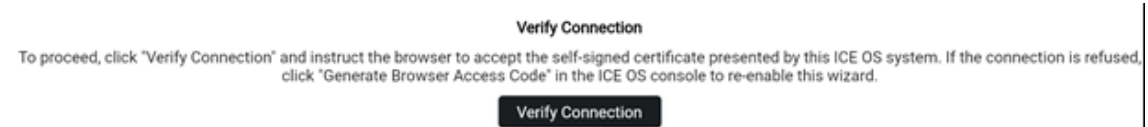
**Note:** From the browser, you may get a 'Your connection is not private' warning, please advance past that.



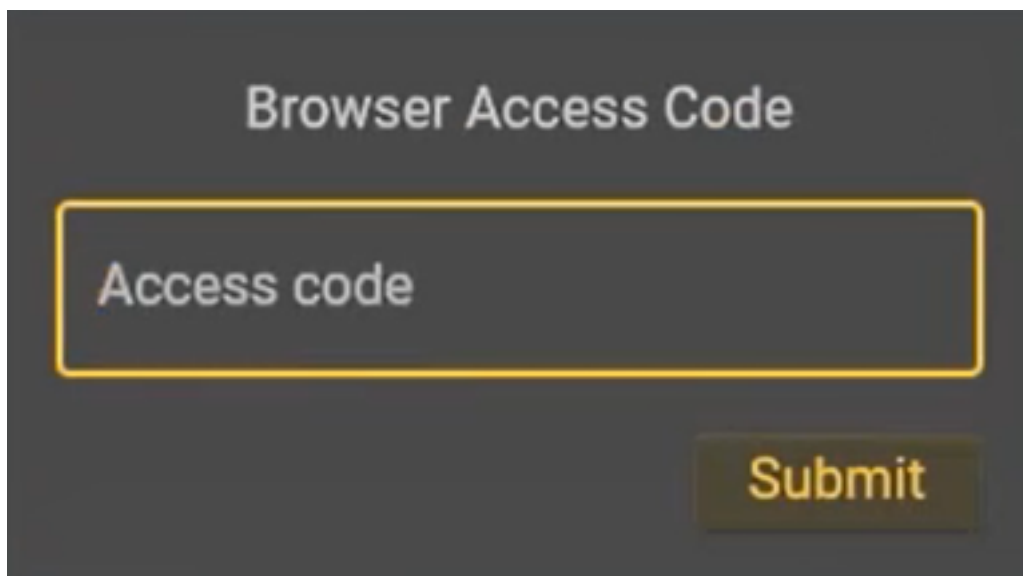
## 8 ICE OS Configuration Wizard

### 8.1 Verify connection

1. Select 'Verify Connection'.



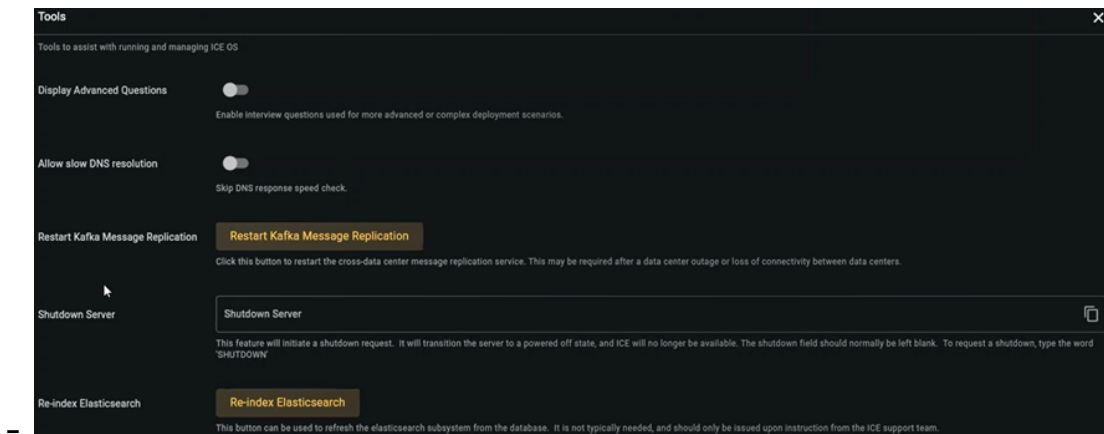
2. From the resulting popup, enter the access code, then select 'Submit'.




3. You now see the 'ICE OS Configuration Wizard' user interface.

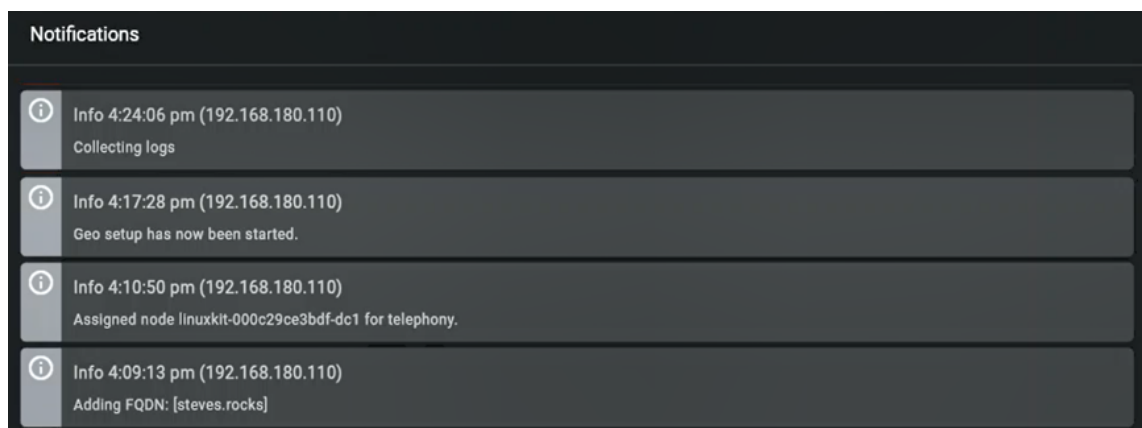
### 8.2 Wizard UI overview

- **Toolbar** (🔧): Select this button to open the 'Tools' popup:



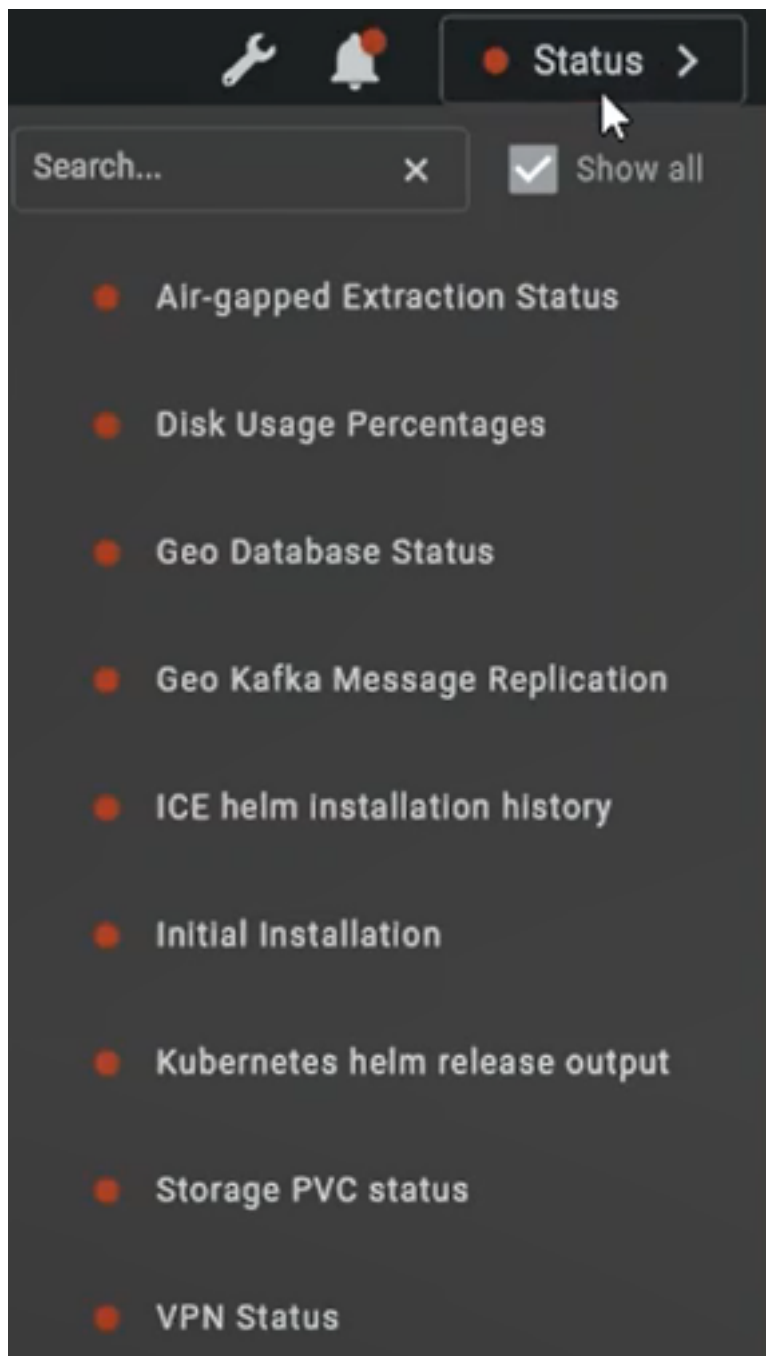
- ★ Display advanced questions = Enabling this tool adds fields to certain screens:
  - Server: 'Install Headlamp' and 'Install KafkaUI' fields will display.
  - Telephony: 'SIP Ports Specification' fields will display.
- ★ Allow slow DNS resolution
- ★ Disable Configuration Wizard
- ★ Shutdown server
- ★ Collect debug logs
- ★ Run database backup
- ★ Restart helm operator
- ★ Remove failed job status messages

- **Notifications** (  ): Select this button to open the 'Notifications' popup, which displays a running list of notifications received during the current session.



- **Status**: Select this button to open the 'Status' dropdown, which displays the status of ICE OS processes as you proceed through the wizard. It is important to keep an eye on this section as some steps should not proceed until certain processes indicate they are ready. See 'Appendix

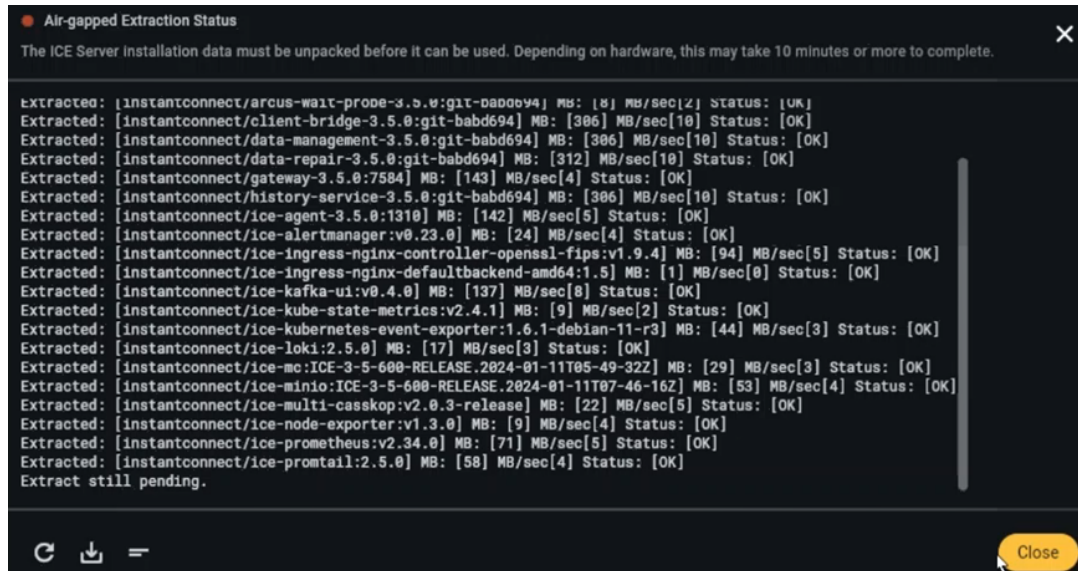

C: Installation status processes' for a full list.




**- Colors:**

- \* Green = Running or done.
- \* Yellow = Paused or waiting to start due to a dependency (e.g., another process must complete first).

\* Red = Not running yet or crashed. Crashes are called out in the log.

- **Refresh** (

In the example above, we see a typical display of a process in progress. The status logs can be downloaded () , which is useful for analysis when troubleshooting issues.

**Note:** As you advance through the screens of the wizard, if you encounter a screen that is not fully displaying all expected fields, then do the following:

1. Go back to the prior screen and advance again, the screen should fully render, if not...
2. Use the browser refresh button to re-render the screen.

### 8.3 Profile

The screenshot shows the 'Profile' configuration screen. It includes fields for 'System Name', 'Use Profile', 'Deployment Profile', and 'Kubernetes CIDR'. Each field has a description and a 'Please enter data for this field' message. There is a 'Check Disk Performance' button at the bottom.

Profile

Provide information about the use and utilization of this system.

System Name

System Name

Provide a name for this system. This value is used only to identify this system, it has no operational impact on the software.  
Please enter data for this field. [Question ID: identify.customerName]

Use Profile

Select option

Choose the profile that matches the licensed size of this system. This value will be used to validate that your host has sufficient resources available to it. This value cannot be changed after Kubernetes has started.  
Please enter data for this field. [Question ID: identify.systemUsage]

Deployment Profile

Select option

Choose the deployment profile matching your architecture. For single data center deployments, choose Solo. For geo-redundant systems, one system should be GeoDC1 and the other GeoDC2. This value cannot be changed after leaving this tab.  
Please enter data for this field. [Question ID: identify.deploymentProfile]

Kubernetes CIDR

10.99.0.0/16

This value specifies the local network address range used internally by Kubernetes. This must be a /16 bit range (255.255.0.0). Most users should not need to change this value, however all addresses within this range must be reserved for this cluster. This value cannot be changed after Kubernetes has started.

Check Disk Performance

Check Disk Performance

ICE OS is very sensitive to disk performance. An under-performing storage system can produce a full system failure. Verify the speed of your disks by clicking this button.

- System Name = Recommend same as ICE OS VM machine.
- Use Profile = Based on your ICE license: Lite, Small, Medium, Large. Once you select a value, the wizard will check if the required minimum space is available.
- Deployment Profile = Select 'Solo'.
- Kubernetes CIDR = Internal to the node and not accessible via the internet.
- Check Disk Performance = Recommended, see 'Virtualization Hardware Guidance' in the *Pre-installation* section above.
- Apply = Select to apply these values and proceed to the next screen.

### 8.4 Network

**Note:** We recommend using SSH.

The screenshot shows the 'Network' configuration screen. It includes fields for 'DNS servers', 'NTP servers', 'SSH Authorized Key', and 'SSH Login Message'. Each field has a description and a 'Please enter data for this field' message. There is a 'Check Disk Performance' button at the bottom.

Profile

Network

Ancillary network settings (ssh/ntp/dns). To allow access to this host via SSH, an SSH key must be provided. For security, ICE OS does not allow SSH access using a password credential.

DNS servers

DNS servers

Specify one or more space-delimited DNS nameservers (e.g. '8.8.8.8.4.4'). For environments without access to a DNS server, use '127.0.0.1'.  
Please enter data for this field. [Question ID: node.Nameservers]

NTP servers

pool.ntp.org

Specify one or more space-delimited network time protocol (NTP) servers.

SSH Authorized Key

SSH Authorized Key

To enable SSH access to this host, provide the public key of the authorized user (typically by cutting and pasting the value of ~/.ssh/id\_rsa.pub). This value should begin with 'ssh-rsa'. Leave this value empty to disable SSH access. Most users will not require SSH access.

SSH Login Message

ICE OS

Enter a message that will be displayed to users who SSH into this system. This is typically used to display compliance, security or regulatory information related to system access.

- DNS servers = The DNS server(s), enter multiple values as space delimited.

- NTP servers = The NTP server(s), enter multiple values as space delimited.
- SSH Authorized Key = Only required if using SSH.

**Note:** Please see ‘Appendix A: Generate an SSH-RSA key’ at the end of this document for more information, if needed.

- SSH Login Message = A free-form text field for a message to display to users when they SSH into the system, e.g., a message alerting a user they are accessing a Government Information System.
- Apply = Select to apply these values and proceed to the next screen.

### 8.5 Storage

Profile	Network	Storage
These values define the storage space allocations assigned to various system components. Default storage allocations are sufficient for most users, but may be adjusted to suite specific needs. Note that once an allocation has been applied the value cannot be reduced, only increased.		
Log Storage (GBs)	10	
The amount of disk space, in gigabytes, reserved for storing system log files. This value cannot be less than the default value and the sum total of all storage allocations cannot exceed the size of the disk.		
File Storage (GBs)	65	
The amount of disk space, in gigabytes, reserved for storing files shared by users as chat message attachments and channel recording archives. This value cannot be less than the default value and the sum total of all storage allocations cannot exceed the size of the disk.		
Backup Storage (GBs)	19	
The amount of disk space, in gigabytes, reserved for storing database backups. This value cannot be less than the default value and the sum total of all storage allocations cannot exceed the size of the disk.		
Database Storage (GBs)	18	
The amount of disk space, in gigabytes, reserved for database storage. This value cannot be less than the default value and the sum total of all storage allocations cannot exceed the size of the disk.		
Search Index Storage (GBs)	30	
The amount of disk space, in gigabytes, reserved for storing search indices. This value cannot be less than the default value and the sum total of all storage allocations cannot exceed the size of the disk.		
System Storage (GBs)	250	

Here you can adjust the amount of disk space for different storage categories, which are prepopulated with recommended default values:

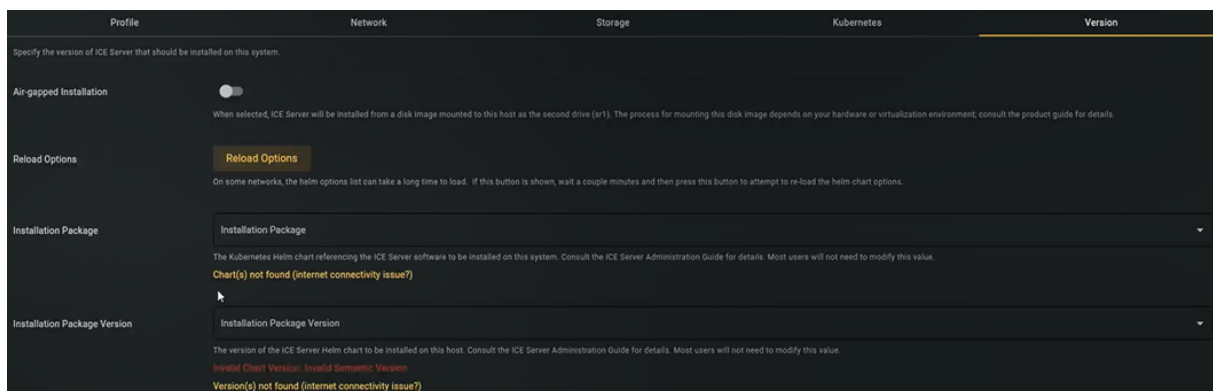
- Log Storage (GBs)
- File Storage (GBs)
- Backup Storage (GBs)
- Database Storage (GBs)
- Search Index Storage (GBs)
- System Storage (GBs)
- Apply = Select to apply these values and proceed to the next screen. A ‘Requested Storage allocation [XXX GB] within provisioned size [YYY GB]’ notification displays.

### 8.6 Kubernetes



- Node Name = This field is prepopulated, but may be edited.
- Apply = Select to apply these values and proceed to the next screen.

### 8.7 Version



- Air-gapped Installation = Toggle on this feature (if not air gapping, leave it toggled off). If enabled, the following field appears:
  - Air Gap Package URL = Default value points to the ‘airgap’ ISO file mounted to the VM (see the *Create a virtual machine (VM) to run ICE OS* section above).
- Reload Options = Follow the instructions if this button appears.
- Installation Package = From the dropdown, select the following value: `ice-release-helm/ice-helm-operator-release-3-5-1`
- Installation Package Version = From the dropdown, select the following value: `3.5.41629`
- Apply = **Check the ‘Status’ dropdown and wait for ‘Pod Status’ to turn green before proceeding to the next screen.**

**For air gap:** An ‘Airgap Extract started’ notification displays.

## 8.8 TLS Certs

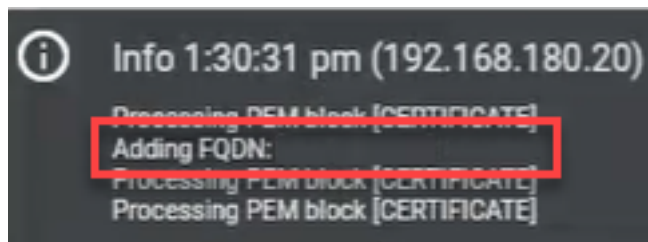
Profile	Network	Storage	Kubernetes	Version	TLS Certs
Use of HTTPS requires that an X.509 server identity certificate be installed. The certificate may identify a single host, or any host within a specific domain (known as a "wildcard certificate").					
ICE TLS	<div>Enable TLS <input type="checkbox"/></div> <div>Enable TLS on the ICE Ingress. This will provide secure connectivity between ICE clients and this ICE server.</div> <div>ICE TLS related questions</div>				
Ldap TLS	<div>Specify LDAP Server Certificate <input type="checkbox"/></div> <div>Enable this option when using secure LDAP communications (ldaps://) with LDAP server identity certificate that was not issued by a well-known (public) certificate authority. Leave disabled if using unsecured connection (ldap://), or if LDAP server's identity certificate was issued by a well-known (public) certificate authority.</div> <div>Ldap TLS related questions</div>				

**Note:** Certificates must be valid for more than 60 days, at least. Open 'Status' > 'Client TLS Certificates' to check the validity of loaded certificates.

**Note:** If a certificate contains an IP address prefaced by <http> or <https>, then do *NOT* list that IP address in the 'Cluster Ingress Hostname' field on the 'Server' screen.

- Enable TLS = If enabled, the following fields appear:
  - Site Certificate Private Key = Enter the private (host) key. X.509 certificate in PEM format.
  - Site Certificate Chain = Enter the public key. X.509 certificate in PEM format. The certificate chain is as follows: server certificate > intermediate certificate(s) (if any) > certificate authority (CA). When using the 'File upload' option, the certificate chain must be uploaded as a single file.

**Note:** After entering both the private and public keys, an 'Adding FQDN: [XXX]' notification displays. Open the 'Notifications' screen and review the 'Adding FQDN' line of that notification to verify the domain is correct.



**Note:** The ICE Desktop web client (enabled on the 'Server' screen) requires certificates be entered here, otherwise, navigating to the web client address results in the following notification: 'Instant Connect is not available in this browser context. Contact your system administrator for more information.'

- Specify LDAP Server Certificate = If enabled, the following field appears:
  - LDAP Certificate = Enter the LDAP server's identity certificate in PEM format.



- Apply = **Check the ‘Status’ dropdown and wait for ‘Node Status’ to turn green *before* proceeding to the next screen.**

**For air gap: Also wait for ‘Air-gapped Extraction Status’ to turn green *before* proceeding to the next screen.**

**Note:** If you advance to the next screen *before* ‘Node Status’ turns green, an error message may display. If this occurs, wait for ‘Node Status’ to turn green, and the error will resolve itself.

### 8.9 Server

Profile Network Storage Kubernetes Version TLS Certs **Server**

Specify options for configuring your ICE Server deployment.

Cluster Ingress Hostname

Enter the scheme, host and domain name in lowercase that ICE clients will use to connect to this system. This value must start with `http://` or `https://`. For example, `https://ice.domain.com`. When more than one address can be used to access this system, enter each address on a separate line placing the primary address on the first line. When providing multiple addresses, the scheme (`http` or `https`) must be the same for each address. IP address is allowed only when using `http://`.

Reverse Proxy Access ☐

Enable this if users will access this system through a reverse proxy (common in many IT environments). An incorrect setting will impact the audit log's ability to display the IP address from which clients are connecting to the system.

Enable Crash Reporting ☒

When enabled, server components that support it will report crashes and other serious errors to Instant Connect. This value does not affect crash reporting of ICE Mobile or ICE Desktop. Instant Connect never collects personal information, user data, or usage patterns.

Install Patch Server ☒

A patch server is used to bridge audio between channels. When checked, a patch server will be installed on this host. This component is unnecessary if your license does not include patch capabilities.

- Cluster Ingress Hostname = Required. The address must be entered in lowercase.
- Reverse Proxy Access = Requires `https://` in the ‘Cluster Ingress Hostname’, otherwise this button is greyed out. If enabling, see ‘Appendix B: Nginx Load Balancer Example’ for information on Nginx load balancer configuration.
- Enable Crash Reporting = Disable if not sharing crash logs.
- Install Patch Server = Disable if not using the Patch Server feature (see the *ICE Server Administration Guide* for more information).
- Install ICE Desktop for Web = Disable if not using the ICE Desktop web client.
- IP Desk Phone Support = Do *NOT* enable unless this feature is included in your ICE product license. Doing so may cause performance issues.

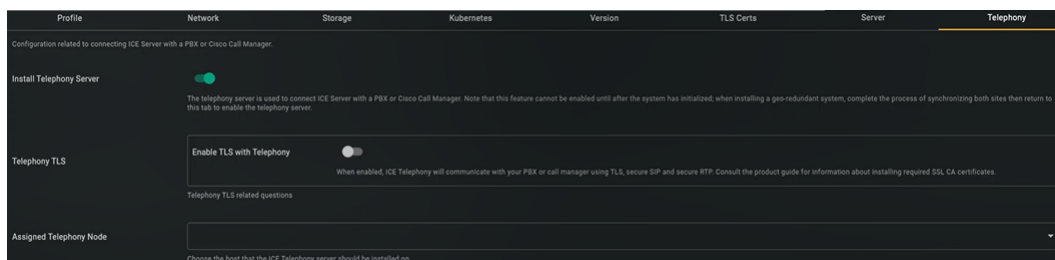
**Note:** This feature is unavailable for ‘Lite’ installations.

- Install Archive Server = Do *NOT* enable unless this feature is included in your ICE product license. Doing so may cause performance issues.

**Note:** This feature is unavailable for 'Lite' installations.

- Concurrent AI Transcribers = Select the desired number of concurrent AI transcribers.
- Install Static Reflector = Enable if using reflections (see the *ICE Server Administration Guide* for more information). If enabled, the following field appears:
  - Network Interface = Must be populated. Default value = `eth0`.
- Install Swagger (OpenAPI) = Enable for API documentation.
- Install KafkaUI = Only displays if the 'Advanced Questions' tool is enabled.
- Install Headlamp = Only displays if the 'Advanced Questions' tool is enabled.
- Enable MinIO Console = Enable to manage backups via this web app.
- Apply = Select to apply these values and proceed to the next screen.

### 8.10 Telephony



- Install Telephony Server = Do *NOT* enable unless this feature is included in your ICE product license. If enabled, an 'Assigned node XXX for telephony' notification displays, also the following fields appear:
  - Enable TLS with Telephony = If enabled, the following fields appear:
    - ★ Telephony Certificate Private Key = Required.
    - ★ Telephony Certificate Chain = Required.
- Assigned Telephony Node = Prepopulated with the ICE host name, which is pulled from the value entered in the 'Node Name' field on the 'Network' screen.
- SIP Ports Specification = Only displays if the 'Advanced Questions' tool is enabled.
  - SIP TCP Port
  - SIP UDP Port
  - SIP TLS Port
  - SIP TCP6 Port

## ICE Server Air Gap Installation Guide

- SIP UDP6 Port
- SIP TLS6 Port
- Apply = Select to apply these values and proceed to the next screen.

### 8.11 External Log Store

The screenshot shows the 'External Log Store' configuration page. At the top, there's a navigation bar with tabs: Profile, Network, Storage, Kubernetes, Version, TLS Certs, Server, Telephony, and External Log Store (which is active). Below the navigation bar, there's a section titled 'Configuration related to sending ICE Server logs to external log repository.' The main content area has three sections: 1. 'Install Vector agent' with a toggle switch turned on and a note: 'Vector agent is used to send ICE Server logs to external log repository.' 2. 'Vector Sink type' with a dropdown menu showing 'Select option'. Below the dropdown, it says: 'Choose from one of the following supported sink type: Amazon CloudWatch Logs, Azure Monitor Logs, or Splunk HEC (HTTP Event Collector) Logs. Please enter data for this field. [Question ID: ice.vector.sink.type]' 3. 'Remote Log Repository TLS' with a toggle switch turned off. Below the toggle, it says: 'Enable this option when using TLS communications (https://) with external log repository on which its identity certificate was not issued by a well-known (public) certificate authority. Leave disabled if using unsecured connection (http://), or if external log repository's identity certificate was issued by a well-known (public) certificate authority. Remote Log Repository TLS related questions'.

- Install Vector Agent = If enabled, the following fields appear:
  - Vector Sink Type = Select the appropriate value, then the following fields appear:
    - \* Endpoint = The URL for the server type selected above.
    - \* Access Token = The token for the server type selected above.
  - Remote Log Repository TLS = Enable if using TLS with the external log repository.

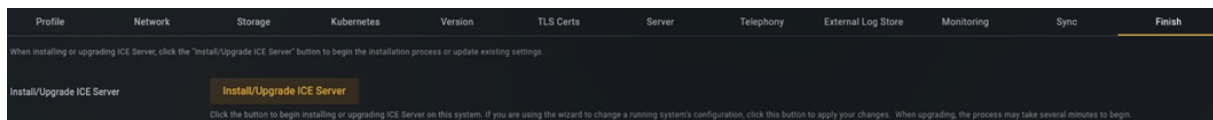
### 8.12 Monitoring

**Note:** This screen is unavailable for 'Lite' installations.

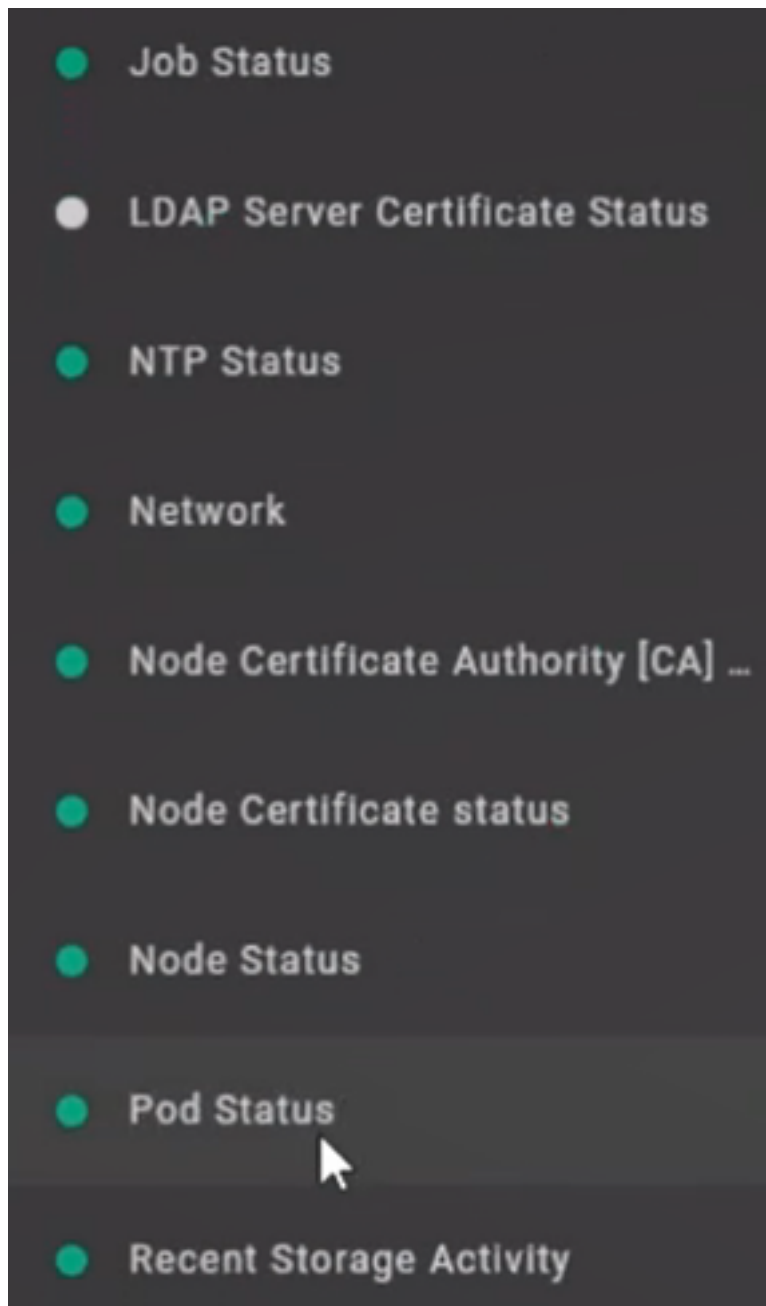
The screenshot shows the 'Monitoring' configuration page. At the top, there's a navigation bar with tabs: Profile, Network, Storage, Kubernetes, Version, TLS Certs, Server, Telephony, External Log Store, and Monitoring (which is active). Below the navigation bar, there's a section titled 'These values are used to configure an email relay server that Grafana will utilize to send email alerts. Contact your IT department or mail administrator for assistance. Be aware that configuring an email server does not, by itself, result in email alerts being delivered. Consult the product guide for information about configuring alerts.' The main content area has four sections: 1. 'Enable Email Alerting' with a toggle switch turned on and a note: 'Toggle this value on to configure a mail server that will be used by Grafana as an email notification channel.' 2. 'Alert Email Reply-To Address' with a text input field containing 'Alert Email Reply-To Address' and a copy icon. Below the field, it says: 'Specify the reply-to email address of the user for email notifications. Please enter data for this field. [Question ID: grafana.emailcontact]' 3. 'Alert Email Reply-To Name' with a text input field containing 'Alert Email Reply-To Name' and a copy icon. Below the field, it says: 'Specify the Reply-To display name of the user for email notifications. Please enter data for this field. [Question ID: grafana.emailuser]' 4. 'Email Server Address' with a text input field containing 'Email Server Address' and a copy icon. Below the field, it says: 'Enter the IP address or host name of the SMTP server that will be used to relay email messages. Please enter data for this field. [Question ID: grafana.smtpserver]' 5. 'SMTP port' with a text input field containing 'SMTP port' and a copy icon. Below the field, it says: 'Enter the TCP port number that the SMTP server communicates on (25 for insecure, 587 for TLS). Please enter data for this field. [Question ID: grafana.smtpport]'.

- Enable Email Alerting = If enabled, the following additional fields appear:
  - Alert Email Reply-To Address
  - Alert Email Reply-To Name
  - Email Server Address
  - SMTP Port
  - SMTP Service Username
  - SMTP Service Password
- Apply = Select to apply these values and proceed to the next screen.

### 8.13 Finish

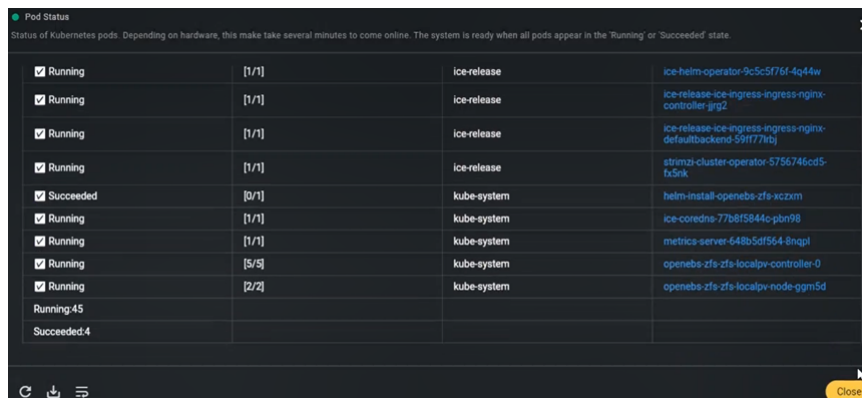


- Before doing *anything* on this screen, open the 'Status' dropdown and verify that *all* of the following are green:
  - Air-gapped Extraction Status
    - Note:** If you accidentally select 'Install/Upgrade' before the air gap extraction completes, then wait for the extraction to complete, then re-select 'Install/Upgrade'.
  - DNS Status
  - Network
  - Node Status
  - NTP Status
  - Pod Status



If any are *NOT* green, wait until they are. Select their 'Refresh' button, to get their latest status, or open their status window to see their progress. Do *NOT* use the web browser refresh.

- Install/Upgrade ICE Server = Select to apply all the configuration settings. A 'Beginning System setup' notification displays. Track progress by opening the 'Status' dropdown. The process is complete when 'Pod Status' returns to green, expanding it will show the following:



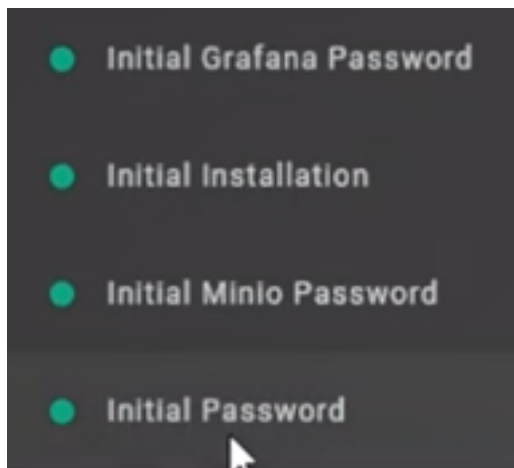
Running	[1/1]	ice-release	ice-helm-operator-9c5c5f76f-4q44w
Running	[1/1]	ice-release	ice-release-ice-ingress-ingress-nginx-controller-vgz2
Running	[1/1]	ice-release	ice-release-ice-ingress-ingress-nginx-defaultbackend-59tt77lrcj
Running	[1/1]	ice-release	strimzi-cluster-operator-5756746cd5-fx5nk
Succeeded	[0/1]	kube-system	helm-install-openebs-zfs-sczzm
Running	[1/1]	kube-system	ice-coredns-77b6f5844c-pbn98
Running	[1/1]	kube-system	metrics-server-648b5df564-8nqpl
Running	[5/5]	kube-system	openebs-zfs-zfs-localpv-controller-0
Running	[2/2]	kube-system	openebs-zfs-zfs-localpv-node-pgm5d
Running:45			
Succeeded:4			

*Congratulations!* This means the ICE Server installation is complete. Please continue with the ‘Post-installation’ section below.

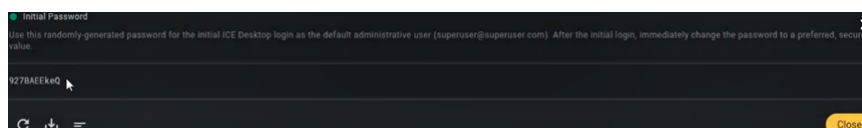
## 9 Post-installation

### 9.1 Retrieve initial passwords for superuser and Grafana accounts

From the ‘Finish’ screen, retrieve the initial passwords for your ICE Server ‘superuser’ and Grafana dashboards accounts.



- Initial Password = Select to open, which reveals your initial superuser account password. Please take note of it for use in the *Setup the superuser account* section below.



- Initial Grafana Password = Select to open, which reveals your initial Grafana account password. Please take note of it for use in *System monitoring* section below.

### 9.2 ICE Desktop: Setup the superuser account

**Note:** Please refer to the *Desktop User Guide* to install the client and activate your license.

ICE Server is installed with a special *superuser* account. This account has normal administrative-level privileges, but also has the unique property that it does not require or consume a license. This makes it essential for bootstrapping a system that does not yet have a license file installed.

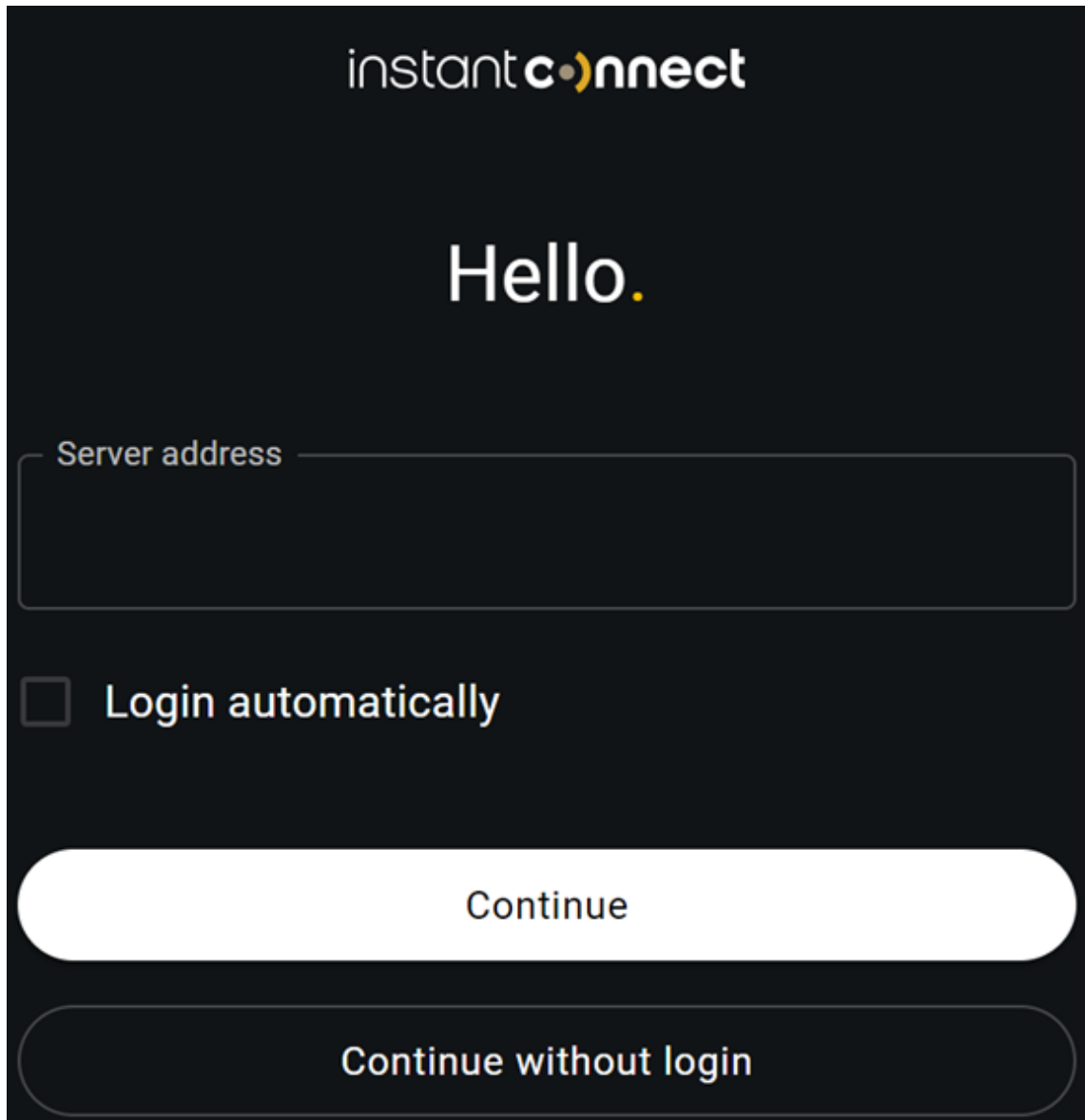
In this section, we'll use this account to connect to ICE Server using the ICE Desktop client to install a license file and provision other users.

The superuser account username is `superuser@superuser.com` and the initial password is available on the 'Finish' screen of the 'ICE OS Configuration Wizard' (see the *Retrieve initial passwords for superuser and Grafana accounts* section above).

#### 9.2.1 Change the superuser password

While not required, we recommend that site administrators change the randomly generated ICE Server superuser password to a value of your choosing. To do so, use the ICE Desktop application to login to ICE Server using the superuser login.

1. Open the ICE Desktop, then enter the hostname or IP address of your ICE Server.

The image shows a dark-themed login interface for 'instantconnect'. At the top, the logo 'instantconnect' is displayed in white, with the 'c' and 'n' connected by a yellow dot. Below the logo, the word 'Hello.' is written in a large, white, sans-serif font. Underneath, there is a text input field with the placeholder text 'Server address' in a light gray font. Below the input field, there is a checkbox followed by the text 'Login automatically' in a light gray font. At the bottom of the form, there are two large, rounded buttons. The top button is white with the text 'Continue' in black. The bottom button is dark gray with the text 'Continue without login' in white.

instantconnect

Hello.

Server address

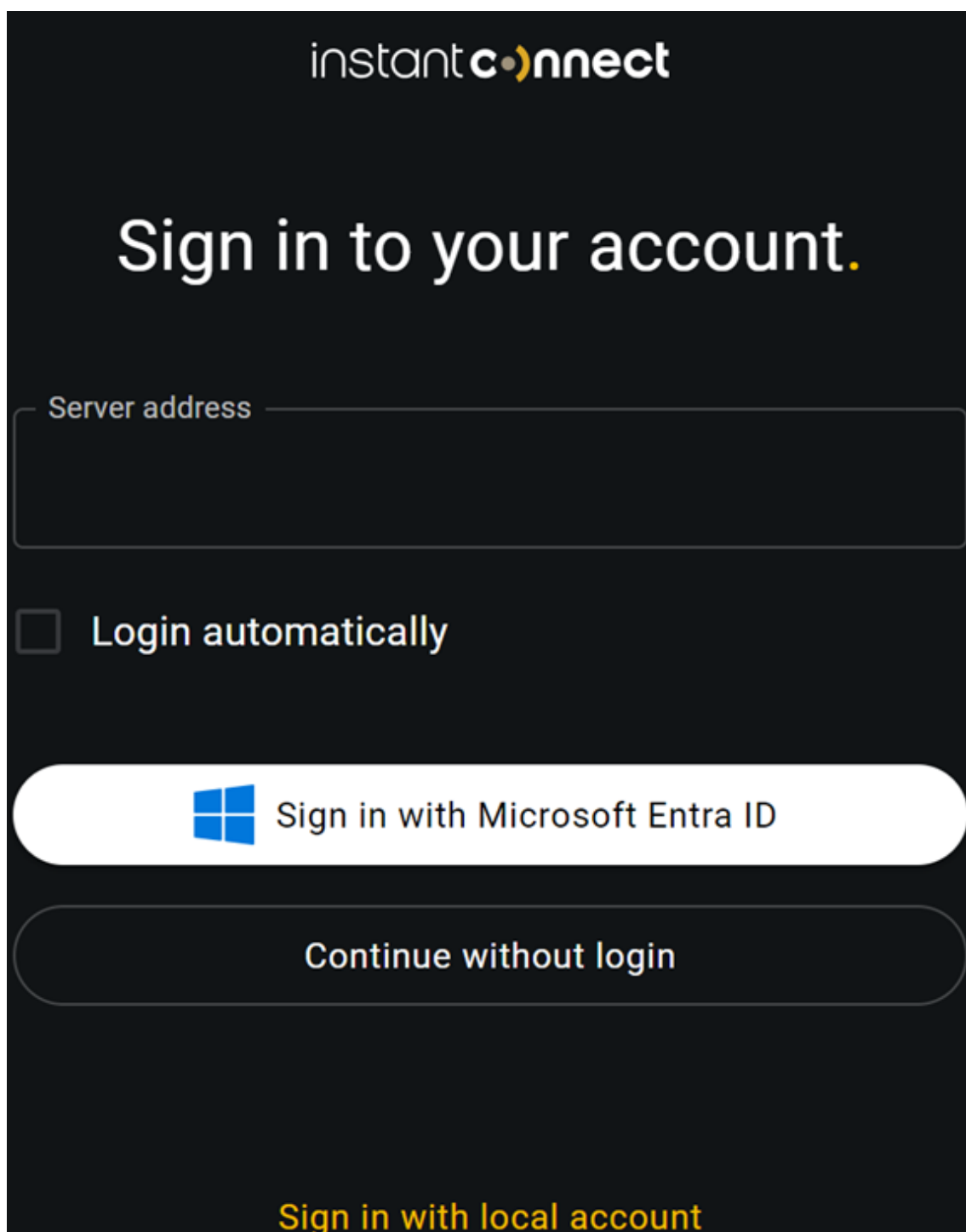
☐ Login automatically

Continue

Continue without login

2. Select 'Continue'.
3. Select 'Sign in with local account' (Enterprise mode).






The image shows a login interface for 'instantconnect'. At the top is the logo 'instantconnect' in white on a dark background. Below it is the heading 'Sign in to your account.' in large white text. There is a text input field labeled 'Server address'. Below the input field is a checkbox labeled 'Login automatically'. There are two buttons: a white button with a blue Windows logo and the text 'Sign in with Microsoft Entra ID', and a dark button with the text 'Continue without login'. At the bottom, the text 'Sign in with local account' is displayed in yellow.

instantconnect

## Sign in to your account.

Server address

☐ Login automatically

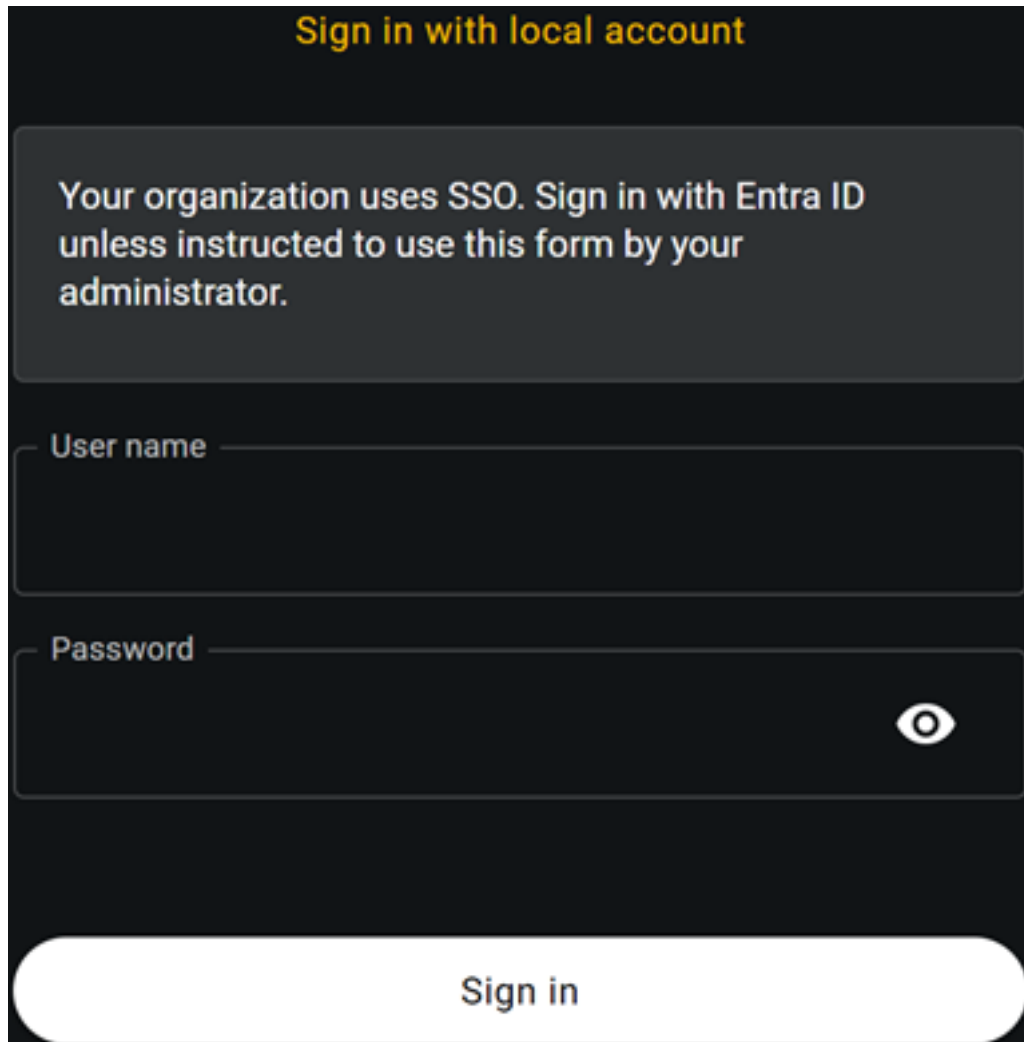
 Sign in with Microsoft Entra ID

Continue without login

Sign in with local account

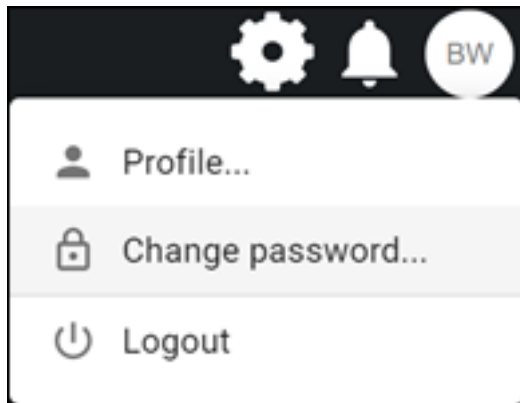
4. Enter the hostname or IP address of your ICE Server, the superuser user name (`superuser@superuser.com`), and the previously retrieved password.

**Note:** If https is not enabled, enter <http://> before the hostname.



The image shows a dark-themed sign-in interface. At the top, the text "Sign in with local account" is displayed in orange. Below this, a dark gray box contains the message: "Your organization uses SSO. Sign in with Entra ID unless instructed to use this form by your administrator." Underneath the message are two input fields. The first is labeled "User name" and the second is labeled "Password". The password field includes a white eye icon on the right side, used for toggling password visibility. At the bottom of the form is a large, white, rounded rectangular button with the text "Sign in" in black.

5. Select 'Sign in'.
6. From the ICE Desktop, select 'Change Password' from the top-right corner of the window.



7. In the pop-up window that appears, re-enter the initial ICE Server superuser password, and then enter the new superuser password twice.

A screenshot of a password change dialog box titled 'Change your Instant Connect Enterprise password:'. It contains three text input fields: 'Current password', 'New password', and 'Confirm password'. Each field is filled with a series of asterisks to represent masked text. At the bottom right of the dialog are two buttons: a 'Cancel' button and a 'Change password' button.

8. Select 'Change Password'.
9. You are then logged out of ICE Desktop. To log in again, use the new password.

**Note:** A forgotten password can only be reset by an administrator. Therefore, the site administrator is recommended to create other administrative accounts for regular day-to-day use.

### 9.3 ICE Desktop: Apply your ICE license

A valid ICE license is required for users other than the superuser to log into the server.

Each ICE license is locked to a unique ID generated during install that's unique to each ICE Server

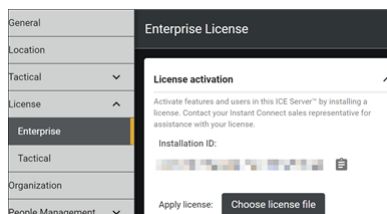
installation. Be warned that licenses are not transferrable; a license issued for use on one installation cannot be used on another. Similarly, re-installing a system from scratch will invalidate its license file. Please contact Instant Connect sales support if you need to transfer your license to another system.

For some features, even though they were enabled in the configuration wizard, they will not be accessible until an appropriate license is applied. Examples include IP phone, archived recordings, and telephony.

### 9.3.1 Request a license

To request an ICE license, you will need to reference your unique installation ID. To find the installation ID:

1. Log in to ICE Desktop as an administrator (i.e., superuser).
2. Go to Settings > License > Enterprise > License activation.



3. Take note of the 'Installation ID' displayed.
4. Contact your Instant Connect sales representative and report this installation ID to them. They will issue you a license file (.lic) that unlocks the features and capabilities per your purchase agreement.

### 9.3.2 Apply the ICE Server license

The license file is typically distributed as an email attachment with the installation ID embedded in the filename, for example: `license-b1d9fdbd-f058-49bb-9204-6ebea5f29c5e-mycompany.lic`

**Do not alter the contents of the license file in any way.**

The license file is cryptographically signed and cannot be modified. Any change to the license file will invalidate it.

1. Save the license file attachment to a location accessible by the ICE Desktop.
2. Back on the 'License' screen, from which you retrieved the installation ID, select 'Choose license file'.

3. Select the saved license file.
4. Each licensed feature will display on the 'License' screen.

## 9.4 Grafana: System monitoring

As part of the installation process, the following tools are automatically configured and deployed to support live system monitoring and alert notifications:

- Prometheus: An open source tool used for event monitoring and alerting, records real-time metrics in a time series database, with flexible queries and real-time alerting.
- Grafana: Serves as the presentation layer for Prometheus. An open source analytics and interactive visualization web application providing charts, graphs, and alerts for the web when connected to supported data sources.
- [ICE Monitoring](#) chart: Configures Grafana to pull data from Prometheus for populating dashboards.

### 9.4.1 Login to Grafana

Access and manage the Grafana dashboards for a cluster via the IP address or hostname of any node in that cluster:

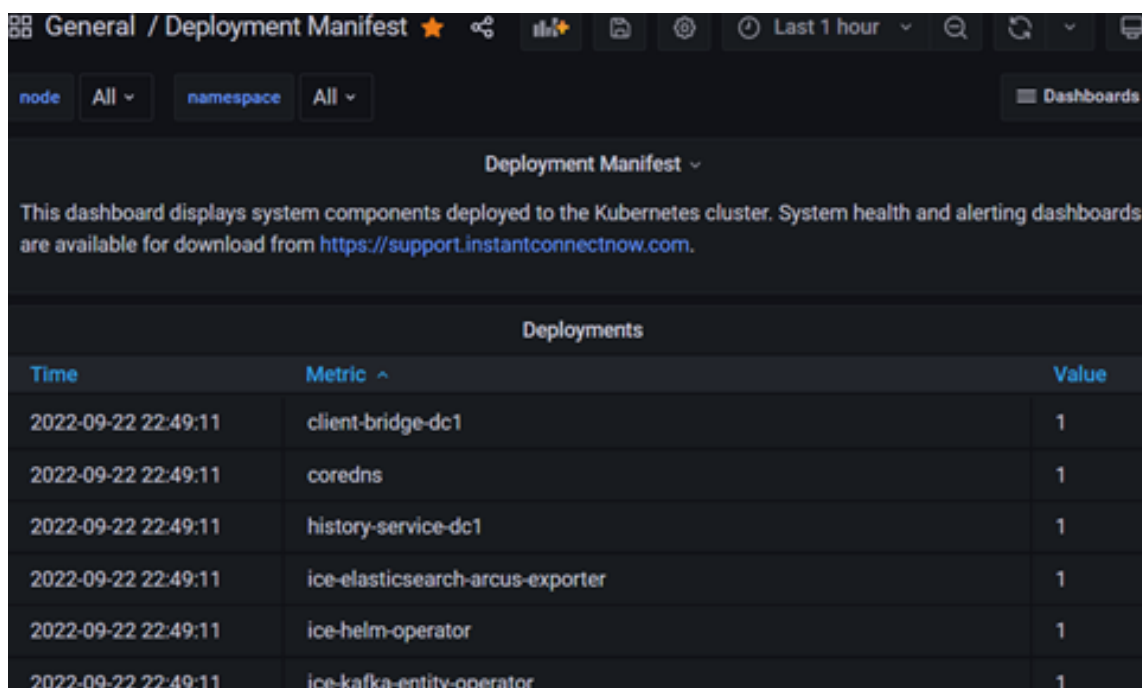
- URL template: `https://CLUSTER_FQDN/grafana/login`
- Default credentials:
  - Username: admin
  - Password: The initial password is available on the 'Finish' screen of the 'ICE OS Configuration Wizard' (see the *Retrieve initial passwords for superuser and Grafana accounts* section above).

### 9.4.2 Grafana dashboards

**Note:** When viewing a dashboard for multiple nodes, be sure to check all of the nodes (not just the initial one displayed), by using the 'Host' dropdown at the top of the dashboard screen.

There are two pre-built dashboards available within Grafana by default:

- **Manifest:** Lists the software components deployed on the cluster.



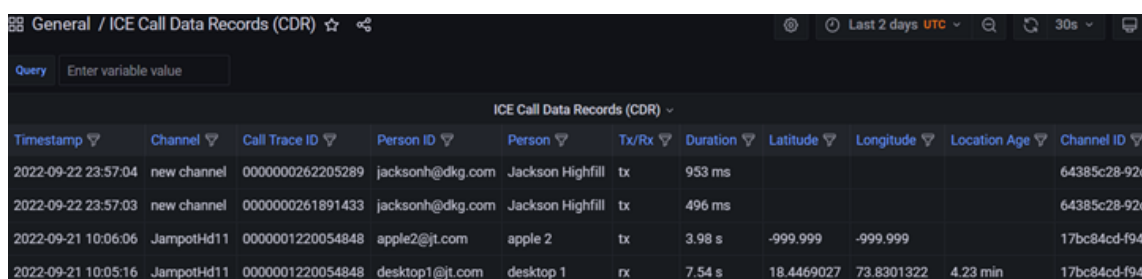
General / Deployment Manifest

This dashboard displays system components deployed to the Kubernetes cluster. System health and alerting dashboards are available for download from <https://support.instantconnectnow.com>.

Deployments

Time	Metric	Value
2022-09-22 22:49:11	client-bridge-dc1	1
2022-09-22 22:49:11	coredns	1
2022-09-22 22:49:11	history-service-dc1	1
2022-09-22 22:49:11	ice-elasticsearch-arcus-exporter	1
2022-09-22 22:49:11	ice-helm-operator	1
2022-09-22 22:49:11	ice-kafka-entity-operator	1

- **Call Data Records:** Shows each person who transmitted audio or made a phone call, and the individuals who received the transmission. For more information on this dashboard, see the ‘Call Data Records (CDR)’ section of the *ICE Desktop User Guide*.



General / ICE Call Data Records (CDR)

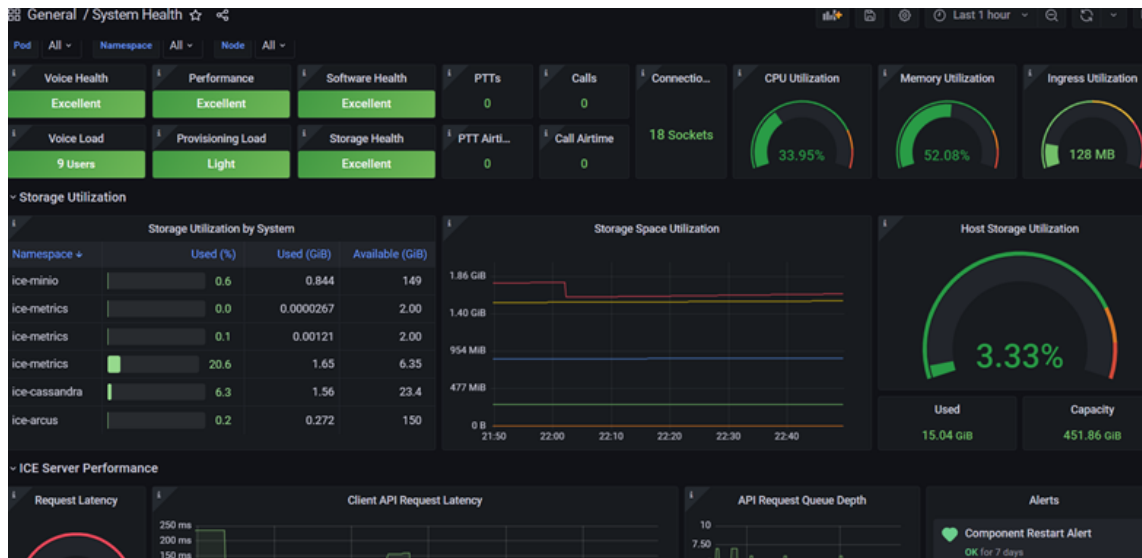
ICE Call Data Records (CDR)

Timestamp	Channel	Call Trace ID	Person ID	Person	Tx/Rx	Duration	Latitude	Longitude	Location Age	Channel ID
2022-09-22 23:57:04	new channel	0000000262205289	jacksonh@dkg.com	Jackson Highfill	tx	953 ms				64385c28-92d
2022-09-22 23:57:03	new channel	0000000261891433	jacksonh@dkg.com	Jackson Highfill	tx	496 ms				64385c28-92d
2022-09-21 10:06:06	JampotHd11	0000001220054848	apple2@jt.com	apple 2	tx	3.98 s	-999.999	-999.999		17bc84cd-f94
2022-09-21 10:05:16	JampotHd11	0000001220054848	desktop1@jt.com	desktop 1	rx	7.54 s	18.4469027	73.8301322	4.23 min	17bc84cd-f94

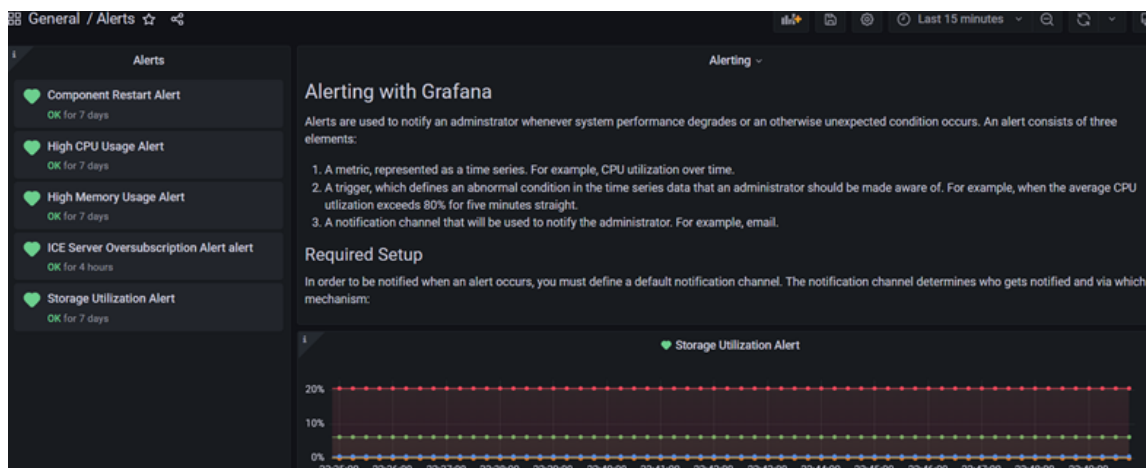
Additionally, there are two other dashboards which can be downloaded from the Instant Connect Support Portal (<https://support.instantconnectnow.com/s/downloads>) and then imported to Grafana.

- **System Health:** Provides live system monitoring. When viewing this dashboard, hover over the ‘i’ (information) icons to see more information on each panel.

## ICE Server Air Gap Installation Guide



- **Alerts:** Provides some predefined alerting conditions.



## 10 Next steps...

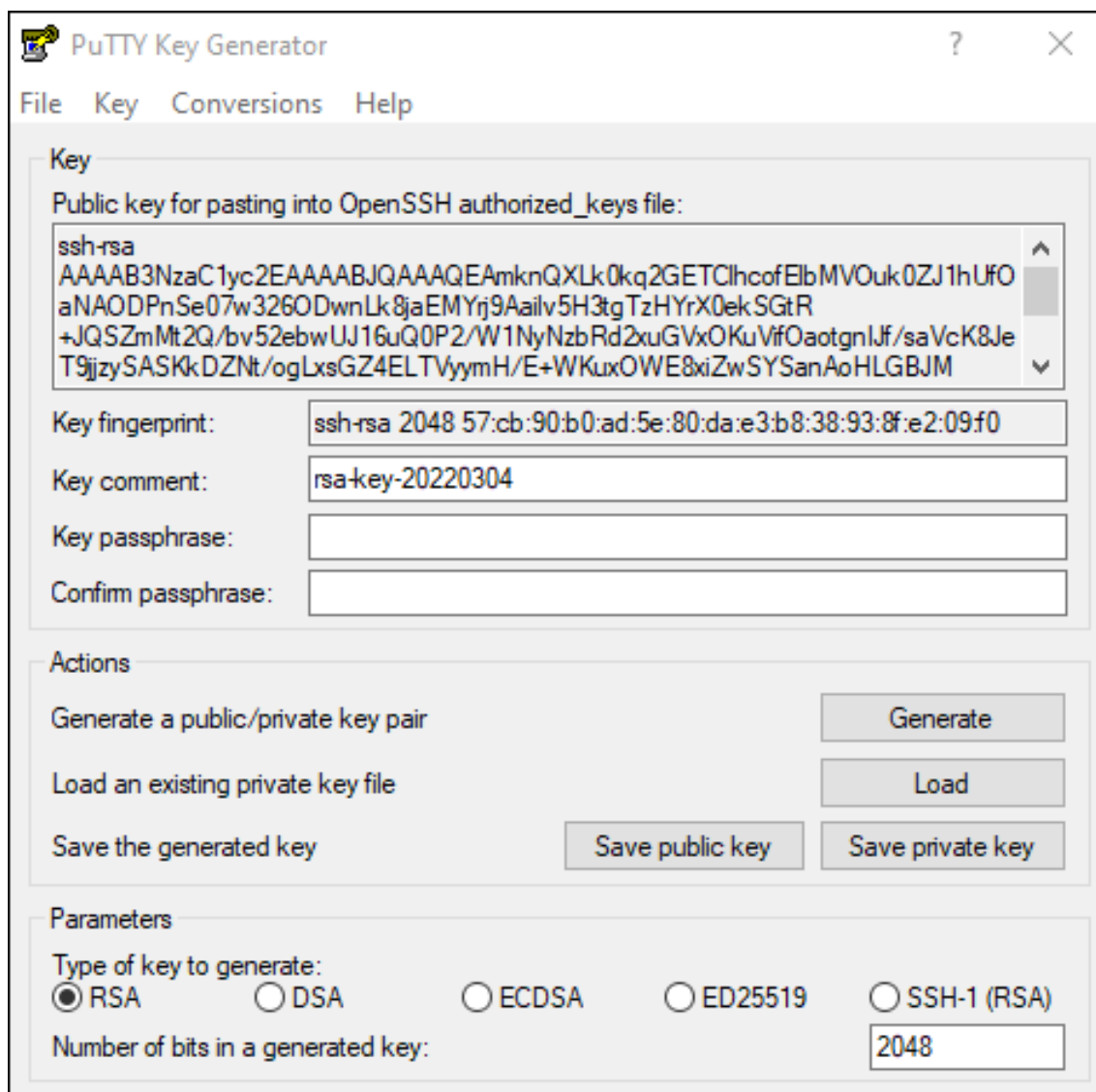
- Please refer to the *LDAP Configuration on ICE Server Guide* to configure the LDAP (Lightweight Directory Access Protocol) service, enable CAC cards, etc.
- Please refer to the *Desktop User Guide* to configure channels, setup users, etc.

## 11 Appendix A: Generate an SSH-RSA key

If you do not have an existing SSH-RSA key, you can generate one.

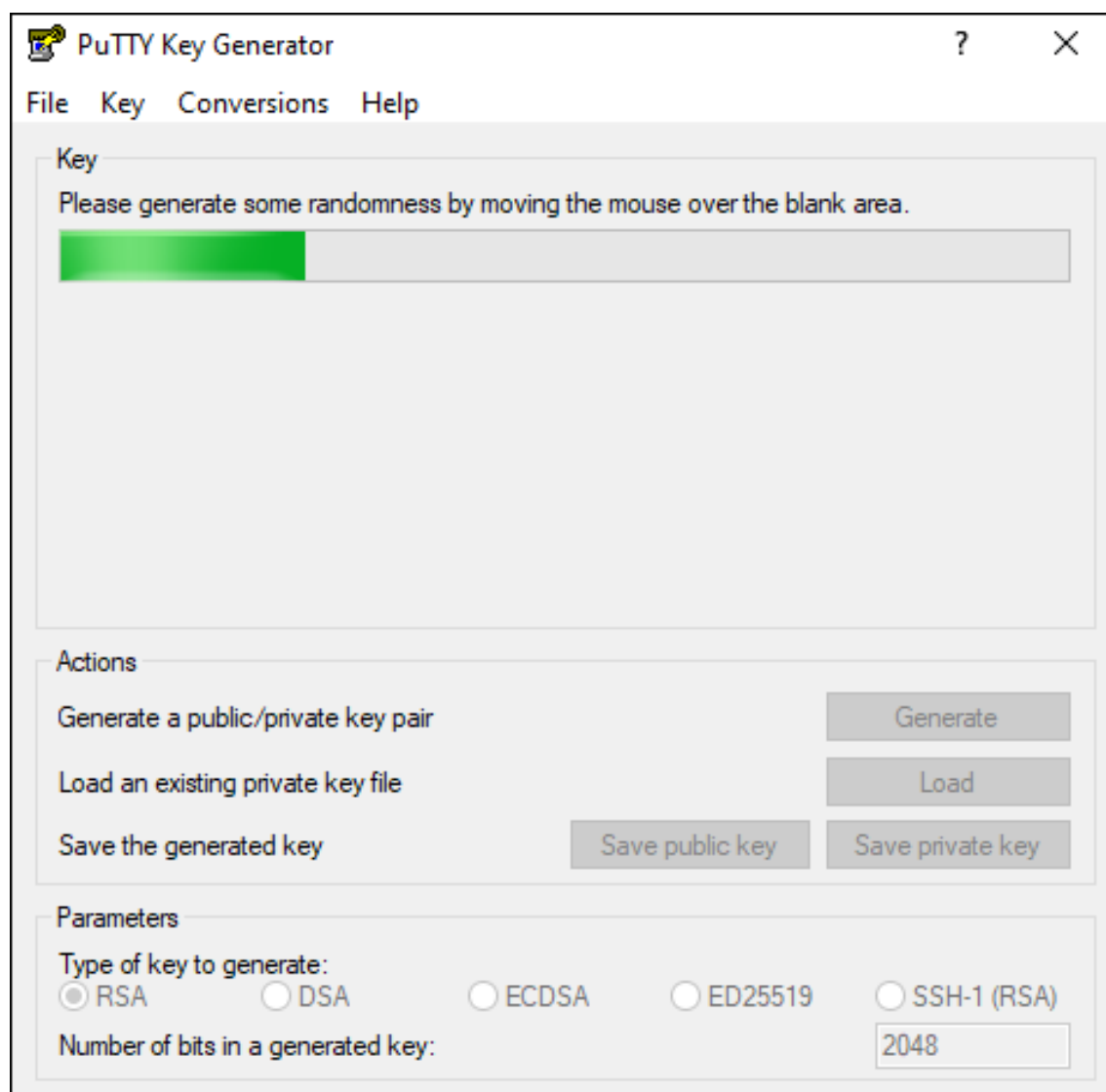
## 11.1 For Windows

1. Open PuTTY Key Generator. The login is `ice-admin`.
2. From the 'PuTTY Key Generator' screen, select 'Generate'.



3. PuTTY generates the public and private keys.





4. Save the private key.
5. Paste the public key into the 'SSH Authorized Key' field of the 'SSH' screen of the configuration wizard.

## 11.2 For MacOS

1. Run the following command in OpenSSH to generate the keypair:

```
ssh-keygen -t rsa -f id_rsa.pub; echo $?  
2048 SHA256:GjtgH3vZCcd2imzH8witAU3zjRz06Z6k00X2BtyMl+g icetadmin@icet  
-test-licenseserver.instantconnectenterprise.com (RSA)  
0
```

2. Paste the content of `~/ .ssh/id_rsa.pub` into the 'SSH Authorized Key' field of the 'SSH' screen of the configuration wizard.

## 12 Appendix B: Log retention using Vector

You can set up ICE Server to forward logs to Vector. For more information on Vector, a third-party log manager, please refer here: <https://vector.dev/docs/reference/configuration/sources/>

### 12.1 ICE Server configuration for the Vector agent

Deploy the Vector agent using `helm`:

1. Add the Vector `helm` repo:

```
helm repo add vector https://helm.vector.dev
helm repo update
```

2. Create a `vector_values.json` for the Vector agent on ICE Server:

```
cat <<- 'VALUES' > ~/vector_values.json
{
  "role": "Agent"
}
VALUES
```

3. Deploy Vector on ICE Server:

```
helm install vector vector/vector \
  --namespace vector \
  --create-namespace \
  --values ~/vector_values.yaml
```

4. Change the default output from `stdout` to the remote Vector server:

1. Edit the vector configmap on the ICE Server in a `vi` editor:

```
kubectl -n vector edit cm vector
```

2. Look for the `sinks` section:

```
sinks:
  prom_exporter:
    type: prometheus_exporter
    inputs: [host_metrics, internal_metrics]
    address: 0.0.0.0:9090
```

```
stdout:
  type: console
  inputs: [kubernetes_logs]
  encoding:
    codec: json
```

3. Replace `stdout` with your preferred name for the Vector output, e.g., `my_vector_sink` :

```
my_vector_sink:
  type: console
  inputs: [kubernetes_logs]
  encoding:
    codec: json
```

4. Update `type` from `console` to `vector`:

```
my_vector_sink:
  type: vector
  inputs: [kubernetes_logs]
  encoding:
    codec: json
```

5. Delete the `codec` line:

```
my_vector_sink:
  type: vector
  inputs: [kubernetes_logs]
  encoding:
```

6. Replace the `encoding` line with `address: remote_vector_fqdn_or_IP:9000`:

```
my_vector_sink:
  type: vector
  inputs: [kubernetes_logs]
  address: 192.168.1.144:9000
```

7. If TLS is enabled on the remote server, you must also enable it on the agent with the FQDN name of the Vector server by adding a `tls` section:

```
my_vector_sink:
  type: vector
  inputs: [kubernetes_logs]
  address: vector.icnow.app:9000
  tls:
    enabled: true
```

8. Restart the Vector agent on ICE Server:

```
kubectl -n vector delete pods --all
```

## 12.2 Vector configuration for ICE Server

1. Add a section in `/etc/vector/vector.toml`:

```
#
# In this example, we are collecting all kubernetes logs
# from ICE OS VM 192.168.0.198
#
# "sources.K8S_CLUSTER" : User-friendly name of ICE Server
#
# "sinks.DATA_SOURCE_NAME" : User-friendly name of data source
#   output
# "inputs" : It should point to "sources.K8S_CLUSTER"
#   "
# "path" : Location of sink's output file

[sources.ice_192_168_0_198_vector]
type = "vector"
address = "0.0.0.0:9000"

[sinks.ice_192_168_0_198_vector_out]
type = "file"
inputs = ["ice_192_168_0_198_vector"]
path = "/var/log/vector/k8s/ice_192_168_0_198.log"
encoding.codec = "raw_message"
```

2. For TLS:

1. Add the following in the `source` section:

```
tls.enabled = true
tls.ca_file = "/etc/vector/tls/tls.vector.ca_file"
tls.crt_file = "/etc/vector/tls/tls.vector.crt_file"
tls.key_file = "/etc/vector/tls/tls.vector.key_file"
```

2. `tls.ca_file` should point to a .PEM file containing the root certificate and the intermediate certificate, if applicable.
3. `tls.crt_file` should point to a .PEM file containing the Vector server certificate.
4. `tls.key_file` should point to a private key file corresponding to `tls.crt_file`.

3. Start/restart Vector:

```
sudo systemctl restart vector
```

4. You should see ICE Server logs streaming to: `/var/log/vector/k8s/ice_192_168_0_198.log`

### 12.3 Example configuration

**Note:** The `splunkhec_logs` component was previously named `splunkhec`. Update your Vector configuration to accommodate the name change:

```
[sinks.my_splunkhec_logs_sink]
+type = "splunkhec_logs"
-type = "splunkhec"
```

```
CommonAdvanced
TOMLYAMLJSON
[sinks.my_sink_id]
type = "splunkhec_logs"
inputs = [ "my-source-or-transform-id" ]
endpoint = "https://http-inputs-hec.splunkcloud.com"
host_key = "hostname"
indexed_fields = [ "field1" ]
compression = "none"
default_token = "${SPLUNK_HEC_TOKEN}"
[sinks.my_sink_id.encoding]
codec = "json"
```

## 13 Appendix C: Installation status processes

---

Component	Summary
Air-gapped Extraction Status	The ICE Server installation data must be unpacked before it can be unused. Depending on hardware, this may take 10 minutes or more to complete.
Client TLS Certificates	Monitor validity of client Ingress and Telephony X509 TLS Certificates.
Disk Usage Percentages	Disk Usage should not exceed 80% in order to prevent disk related outages.
DNS Status	The DNS server is an important and integral part of network communication. Correct operation of DNS servers is very critical.
Geo Database Status	Indicates the Geo sync status of the ICE Server database.
Geo Kafka Message Replication	Kafka message replication status info intended for use by ICE support personnel.

Component	Summary
Geo Sync Status	Synchronizing geo-redundant systems may take several minutes or as long as an hour. Status of the synchronization process will be displayed here. Contact support for assistance.
Helm Repo Load Status	Loading helm Repo via slow internet connections can be slow. Completion Status will display here.
ICE helm installation history	Display versions of timing of ICE installations.
ICE helm upgrade results	Display versions of timing of ICE installations.
Initial Grafana Password	Use this randomly-generated password for the initial Grafana login as the default administrative user (admin). After the initial login, immediately change the password to a preferred, secure value.
Initial Installation	This status is an indication of whether the user has completed all of the initial interview setup questions
Initial Minio Password	Use this randomly-generated password for the initial Minio login as the default administrative user (iceminio). After the initial login, immediately change the password to a preferred, secure value.
Initial Password	Use this randomly-generated password for the initial ICE Desktop login as the default administrative user (superuser@superuser.com). After the initial login, immediately change the password to a preferred, secure value.
Job Status	A Job creates one or more Pods and will continue to retry execution of the Pods until a specified number of them successfully terminate. As pods successfully complete, the Job tracks the successful completions.
Kubernetes helm release output	ICE helm release info intended for use by ICE support personnel.
LDAP Server Certificate Status	Indicates whether LDAP server certificate have been synchronized from the UI.
Network	Address of the network interface. IP, subnet and gateway are defined in the ICE OS console.

Component	Summary
Node Certificate Authority (CA)	Status of Kubernetes X509 self signed certificate authority. It is valid for 10 years from original installation and will then need to be rotated. It will NOT rotate automatically.
Node Certificate status	Status of Kubernetes X509 self signed certificate. It will automatically renew when the server is restarted and the certificate is within 90 days of expiration.
Node Status	Status of the Kubernetes node. Depending on hardware, this may take several minutes to come online.
NTP Status	Network time protocol is used to set the date and time of this system. Maintaining accurate time is crucial for system operation.
Pod Status	Status of Kubernetes pods. Depending on hardware, this make take several minutes to come online. The system is ready when all pods appear in the 'Running' or 'Succeeded' state.
Recent Storage Activity	Insight into the percentage of time the hard drive for this system has been busy.
Storage PVC status	Verifies that expected PVC's exist.
Telephony Certificate Status	Indicates whether telephony certificates have been synchronized from the UI.
VPN DNS Status	Status of the cluster DNS system. Contact support for assistance.
VPN Status	Status of the Wireguard VPN used to link geo-redundant systems together. Contact support for assistance.

## 14 Appendix D: Installing local patch server or static reflector

**Note:** The following require Docker to already be installed. For instructions on installing Docker, please refer to the '*Install Docker*' section in the '**ICE Telephony Administration Guide**'.

### 14.1 Installing local patch server on Ubuntu via docker

To install a local patch server, first stop any existing one (ignore warning message if it is not running):

```
docker stop patch && docker stop patch-agent
```

Remove existing patch server volumes, if any:

```
docker volume rm patch-config \
    && docker volume rm patch-status
```

Run `curl` from the patch server generated via ICE Desktop admin account on your local Ubuntu machine:

- **DEBUG=1:** You may remove for normal installs.
- **TOKEN:** The server link/token will be different for every patch server.

```
curl https://ICE_SERVER_URL:443/remote-installer/install_engagebridge.sh | \
    \
    DEBUG=1 \
    TOKEN=..... \
    SERVERBRIDGE_URL=https://ICE_SERVER_URL:443/server-bridge/\
    bash -
```

**Note:** If your cluster is not using certificate, replace `https` with `http`.

### 14.2 Installing local static reflector on Ubuntu via docker

**Note:** You should determine the network interface name (`REFLECTOR_NIC`) for multicast on the static reflector host by running `ifconfig -a`, `ip a` or `nmcli`.

To install a local static reflector, first stop any existing one (ignore warning message if it is not running):

```
docker stop reflector && docker stop reflector-agent
```

Remove existing reflector volumes, if any:

```
docker volume rm reflector-config && docker volume rm reflector-status
```

Run `curl` from the static reflector generated via ICE Desktop admin account on your local Ubuntu machine that sits with the radios in the same multicast domain:.

- **DEBUG=1:** You may remove for normal installs.
- **TOKEN:** The server link/token will be different for every static reflector.

```
curl https://ICE_SERVER_URL:443/remote-installer/install_reflector.sh | \
    \
    DEBUG=1 \
    MULTICAST_INTERFACE=REFLECTOR_NIC \
```



```
TOKEN=..... \  
SERVERBRIDGE_URL=https://ICE_SERVER_URL:443/server-bridge/  
bash -
```

**Note:** If your cluster is not using certificate, replace [https](#) with [http](#).