gluware®

Gluware® Installation Guide

Version 5.2
25 October, 2023

gluware®

2020 L Street, Suite 130 | Sacramento | CA | 95811
+1 916 913 8062 | www.gluware.com

Table of Contents

About Gluware 5.2

Gluware automates network life cycle management on existing networks, allowing you to roll out a robust suite of advanced network and security features while reducing manual deployment and support costs. It simplifies network configuration and change management, enables compliance checking, and implements security policies.

Gluware provides powerful tools that allow you to monitor and update to your network devices.

- Create and maintain a hardware and software inventory of devices using **Device Manager**.
- Take configuration snapshots in **Config Drift and Audit** and monitor configuration changes over time.
- Create specific compliance rules in **Config Drift and Audit** to ensure policies are maintained on all devices.
- Monitor device data and activity in one place with **Dashboards**.
- Support process-oriented activities across devices with **Network RPA** workflows.
- Keep your network diagrams up-to-date and simplify troubleshooting with Gluware **Topology**.
- Model and manage configurations for devices with **Config Model Editor**.
- Install the latest OS on one or many devices using **File Server** and **OS Manager**.
- Create robust report templates and run reports on demand or on a schedule with **Data Explorer**.

Gluware is licensed per solution:

- **Gluware** – Includes **Device Manager**, **Schedules**, **Data Explorer**, **Data Export**, **Dashboards**, and **Solutions Manager**
- **Config Drift and Audit**
- **OS Manager** – Includes **File Server**
- **Config Model Editor**
- **Workflows**
- **Network RPA**
- **Topology**

The **Gluware license** is for a specific device count for the organization it is installed in and any child organizations. Each license, including the Gluware license, has an activation and expiration date.

An unlicensed system can be installed, but only the system settings configuration functions are available until the Gluware license is installed.

Watch Gluware introductory videos at https://gluware.com/videos/product-videos/

Contact us

Please contact Gluware, Inc. directly for further information or if you have any questions.

Web

For help with Gluware, and to learn more about Gluware, Inc. products, visit https://www.gluware.com

Technical support

We're here to deliver the support and service you need to get the most from your investment in Gluware. If you need support for Gluware, contact the Gluware Support and Service team. Technical support requires a valid support and maintenance agreement with Gluware, Inc.

Email: support@gluware.com

Web Support: https://support.gluware.com

Professional services

Gluware, Inc. has a staff of professionals who can help you with installation, provisioning, project management, custom designs, project design, and custom solutions. Contact your account manager or Gluware, Inc. Sales for a quote at sales@gluware.com.

Training

If you're new to our software solution, or seek to advance your skills, we offer an extensive range of training to help you accomplish your goals and make the most of your Gluware, Inc. investment. Gluware, Inc.'s training courses are tailored to fit specific skill levels, from beginner through advanced, covering our core solutions. We can also create custom courses to meet your specific training needs. If you would like more information about training options, email training@gluware.com and we can discuss the most suitable option for your organization.

Documentation

Gluware, Inc. strives for continual refinement and improvement in the quality and usability of Gluware documentation. We regularly update our documents and if you have any comments, suggestions, or information that you believe we should include, send documentation comments to techpubs@gluware.com. Reference version 5.2.4.

Product dependencies and compatibility

Host operating system

CentOS v7.6 is the base operating system for the virtual machine on which Gluware runs.

Hypervisors

Supported Hypervisors: VMWare ESXi™ v6.0, or above; Microsoft® Hyper-V™ v2012 R2, or above

Other Hypervisors are not recommended for production installations and are not validated with this Gluware version. Installation results attempted on other platforms may vary significantly. Please contact Gluware, Inc. for more information regarding demonstration of other hypervisor proof-of-concepts and lab testing.

Browser

Supported Browser: Google Chrome™, desktop versions (not iOS)

Other browsers may work, but the user experience may vary.

Display resolution

Recommended: 1920 x 1080 pixels
Minimum: 1280 x 1024 pixels

Security and encryption

The Gluware SSH engine supports the following:

Supported SSH ciphers

aes256-ctr
aes192-ctr
aes128-ctr
aes256-cbc
aes192-cbc
aes128-cbc
3des-ctr
Arcfour
arcfour128
arcfour256

Supported key exchange mechanisms

diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
diffie-hellman-group1-sha1

Supported signatures

ssh-rsa
ssh-dss

Supported encryption algorithms

aes128-ctr
aes128-cbc
3des-ctr
3des-cbc
blowfish-cbc

Supported integrity algorithms

hmac-sha2-256
hmac-sha1
hmac-sha1-96
hmac-md5-96 (deprecating soon)
hmac-md5 (deprecating soon)

Supported authentication mechanisms

Password
keyboard-interactive

Installation overview

Before you begin to install Gluware, determine if you will use a Gluware Disaster Recovery Server and any Gluware Zone Engines. Once you determine your optimal Gluware configuration, ensure you have adequate platform resources.

Here are the steps involved:

Step 1. Determine your configuration and resources required

Step 2. Gather platform details

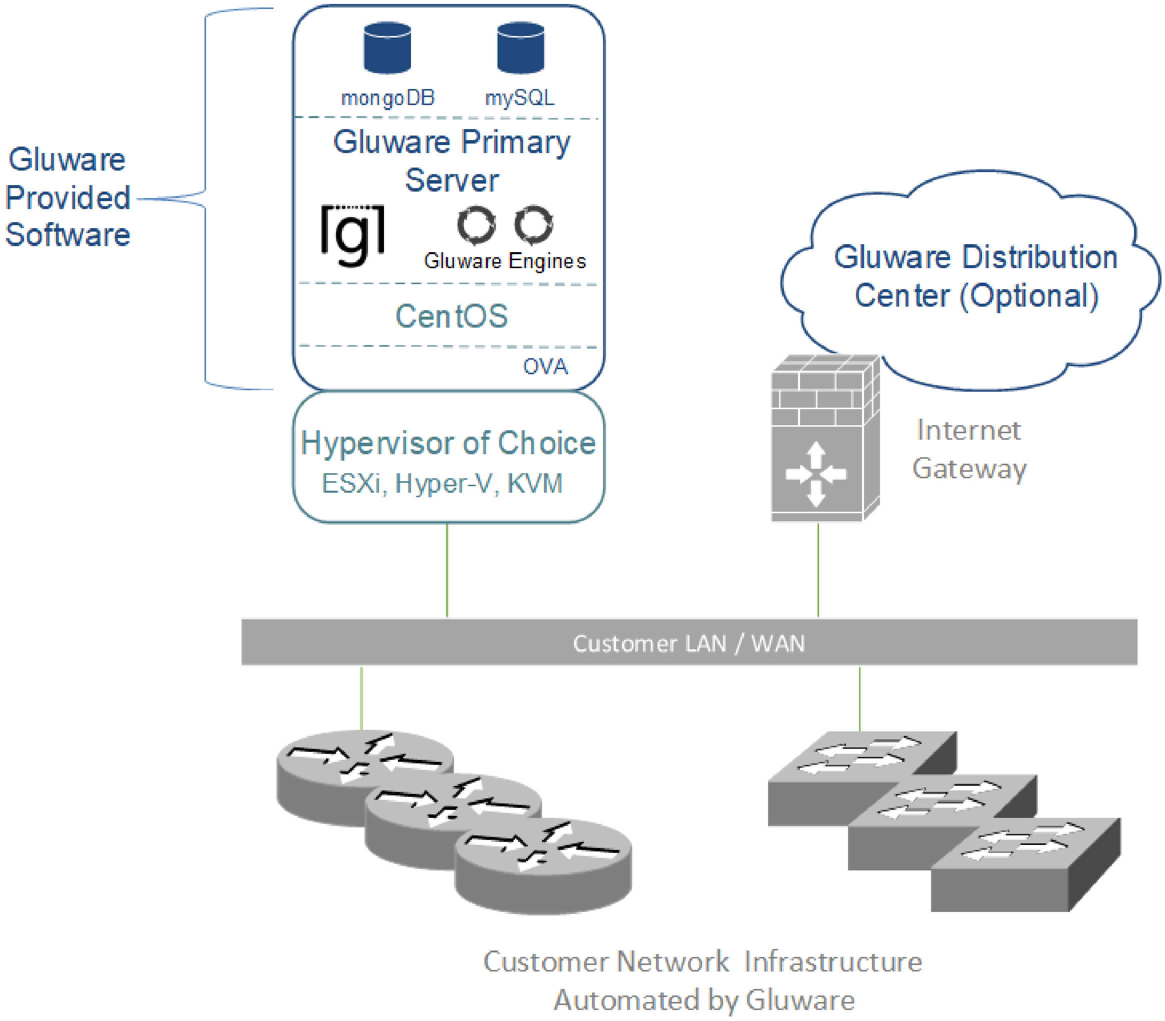
Step 3. Configure your VM

Step 4. Install Gluware

Step 1. Determine your configuration and resources required

Basic Gluware system

The **Gluware Primary Server** performs all Gluware functions and stores all the logs and data archives that Gluware generates. Thoughtful scheduling of backups and regular purging or offloading of logs and data archives using Data Retention can help maintain performance of your Gluware server. However, you might consider adding an additional disk for storing backups.



For the Gluware Primary Server, you'll need the following resources:

Component	Minimum requirements	Large scale recommendations
Disk space	128 GB*	At least 500 GB*
Memory	32 GB	64 GB
CPUs/vCPUs	4 CPUs, 2.4 GHz	8 CPUs, at least 2.4 GHz
Other	Unique static IP address. SSL certificate and private key or self-signed certificate.	Unique static IP address. SSL certificate and private key or self-signed certificate.

*OS and applications need a minimum of 20 GB. The rest is intended for data.

Gluware Primary Server communications

Device	Protocol	Port
Network device	SSH or Telnet	TCP 22 or TCP 23*
Gluware Disaster Recovery Server	MongoDB, IPSec, and ESP	TCP 27017, UDP 500, and UDP 4500
Gluware Zone Engines	RabbitMQ	TCP 5672 and UDP 5672
Gluware distribution center	SSL	TCP 443
Customer SMTP server	SMTP or SMTP over SSL	TCP 25 or TCP 465
Customer LDAP server	LDAP or LDAPS	TCP 389* or TCP 636*
Customer RADIUS server	RADIUS	TCP 1812* and TCP 1813*
Customer NTP server	NTP	UDP 123
Customer web sign-in	HTTPS	TCP 443

*Default, user-configurable

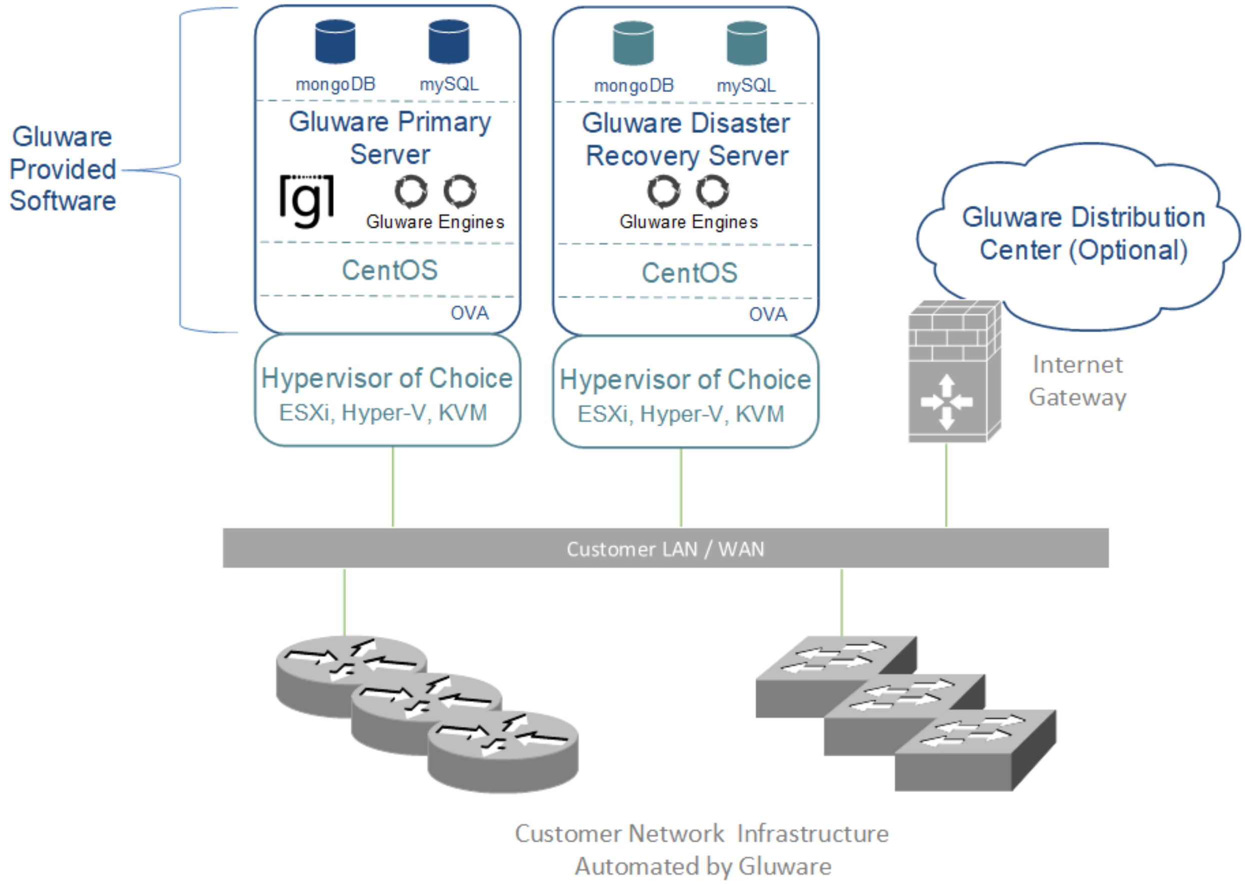
External access required — If enabled

Website	**URL**
Gluware Distribution Center	https://glulab.gluware.com
Cisco API Console	https://cloudsso.cisco.com/as/token.oauth2 to authenticate https://api.cisco.com/ for data retrieval
NIST NVD	https://services.nvd.nist.gov/
StackStorm	Requires access to the IP and port of your StackStorm instance
Cisco Meraki API	https://api.meraki.com/

Gluware Primary Server + Gluware Disaster Recovery Server

Adding a Gluware Disaster Recovery Server provides a backup of your Gluware Primary Server and is a disaster recovery option. The Gluware Disaster Recovery Server is a cold standby intended for catastrophic failure of the Gluware Primary Server. It does not provide high availability failover. For this configuration, you'll need two servers:

- Gluware Primary Server
- Gluware Disaster Recovery Server



A Gluware Disaster Recovery Server can be added to your Gluware implementation at any time. The resources required for the Gluware Disaster Recovery Server must match those of your Gluware Primary Server.

Gluware Disaster Recovery Server communications

Device	Protocol	Port
Network device	SSH or Telnet	TCP 22 or TCP 23*
Gluware Primary Server	MongoDB, IPSec, and ESP	TCP 27017, UDP 500, and UDP 4500
Gluware Zone Engines	RabbitMQ	TCP 5673 and UDP 5673
Gluware distribution center	SSL	TCP 443
Customer SMTP server	SMTP or SMTP over SSL	TCP 25 or TCP 465
Customer LDAP server	LDAP or LDAPS	TCP 389* or TCP 636*
Customer RADIUS server	RADIUS	TCP 1812* and TCP 1813*
Customer NTP server	NTP	UDP 123
Customer web sign-in	HTTPS	TCP 443

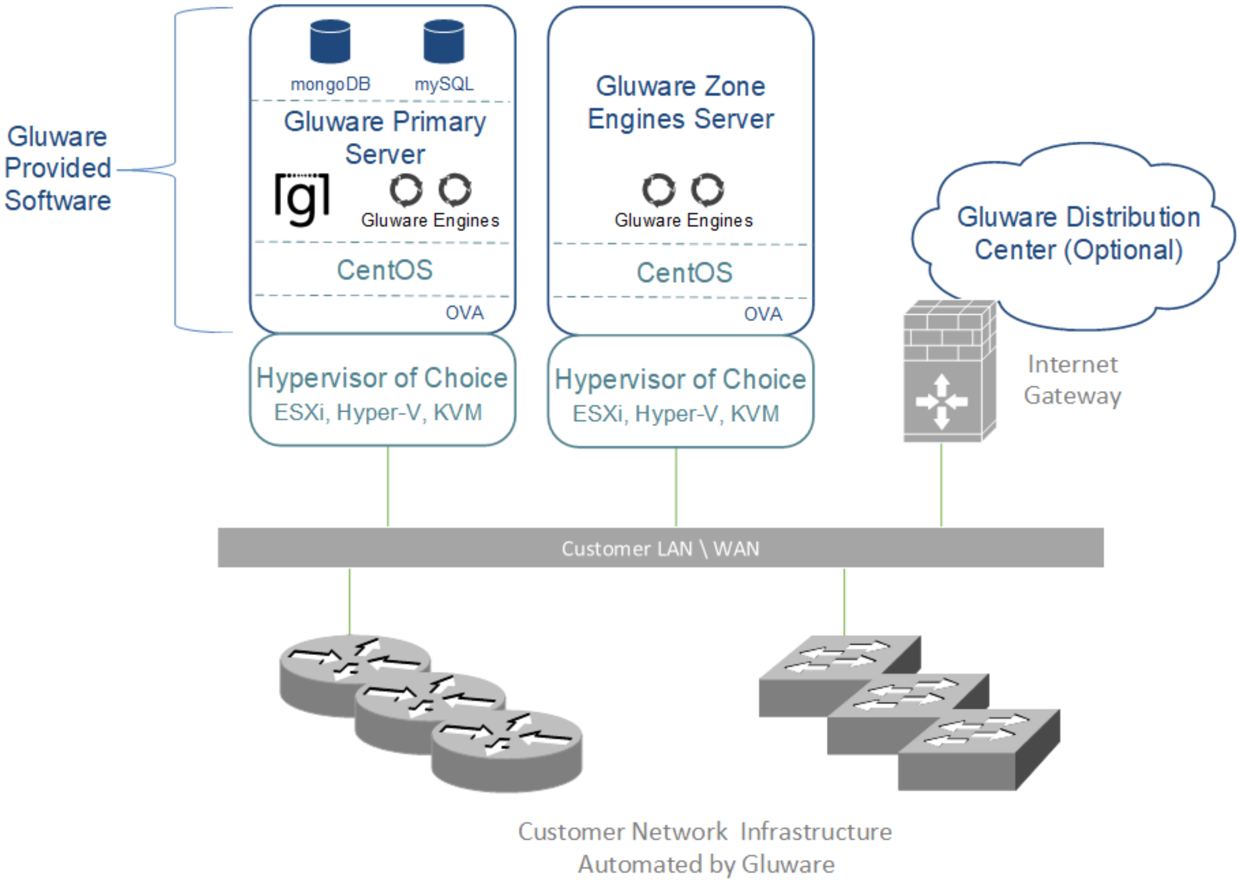
*Default, user-configurable

Gluware Primary Server + Gluware Zone Engines

Adding Gluware Zone Engines offers scalability. Zone Engines help improve Gluware performance on large networks by increasing the number of simultaneous jobs that can be run. To optimize performance and reduce latency in a distributed geographical design, devices must be assigned to a zone. *See* “Assign a device to a zone” in online Help or the *Gluware Enterprise User Guide*.

For this configuration, you'll need two or more servers:

- Gluware Primary Server
- 1–*n* Gluware Zone Engines



Zone Engines can be added to your Gluware system when the need for faster processing arises. You'll need the following resources for each you add:

Component	Minimum requirements	Large scale recommendations
Disk space	128 GB*	At least 128 GB*
Memory	16 GB	32 GB
CPUs/vCPUs	2 CPUs, 2.4 GHz	4 CPUs, at least 2.4 GHz
Other	Unique static IP address. SSL certificate and private key or self-signed certificate.	Unique static IP address. SSL certificate and private key or self-signed certificate.

*OS and applications need a minimum of 20 GB. The rest is intended for data.

Gluware Zone Engines communications

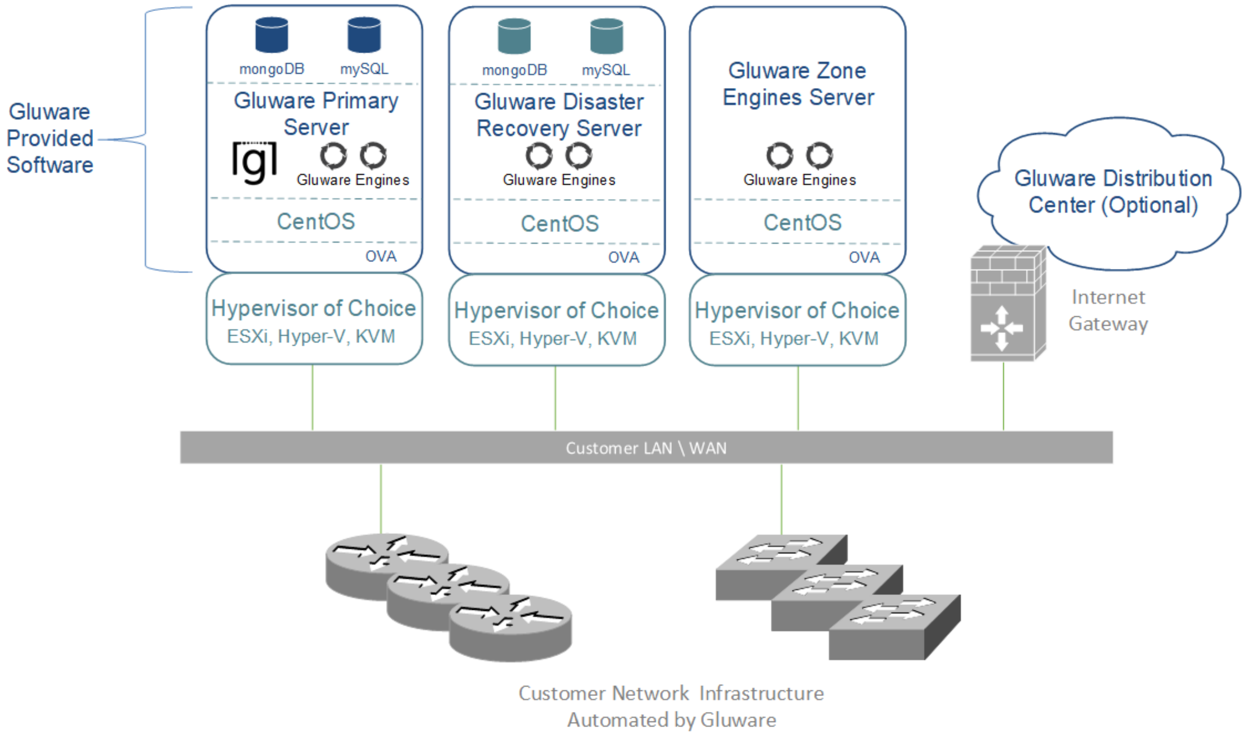
Device	Protocol	Port
Network device	SSH or Telnet	TCP 22 or TCP 23*
Gluware Primary Server	RabbitMQ, MongoDB, and HTTPS, ESP	TCP 5672, UDP 5672, TCP 27017, TCP 8042
Gluware Disaster Recovery Server	RabbitMQ, MongoDB, and HTTPS, ESP	TCP 5672, UDP 5672, TCP 27017, TCP 8042
Customer NTP server	NTP	UDP 123

*Default, user-configurable

Gluware Primary Server + Gluware Disaster Recovery Server + Gluware Zone Engines

This configuration combines the disaster recovery option and addresses performance. For this configuration, you'll need three or more servers:

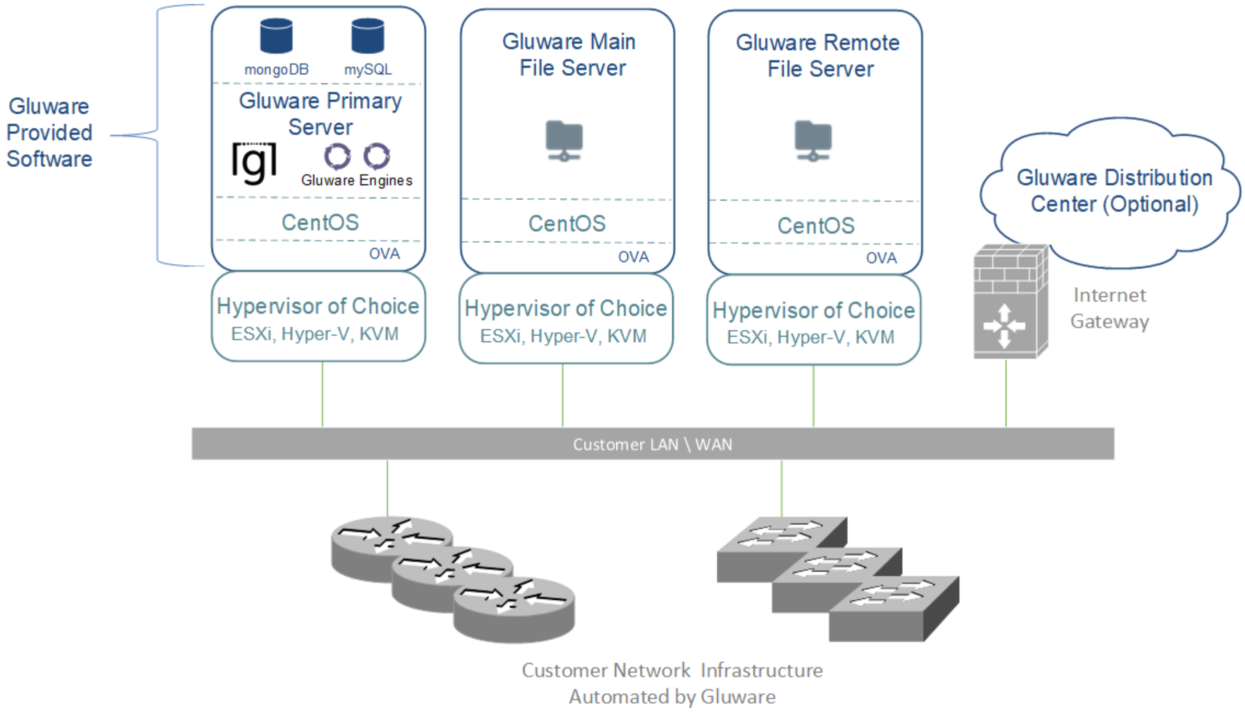
- Gluware Primary Server
- Gluware Disaster Recovery Server
- 1–*n* Gluware Zone Engines



Any of the above configurations + Gluware File Server + remote File Servers(s)

If you purchase a Gluware OS Manager license, you'll need a Gluware File Server. You can add as many remote File Servers as you need, for example, to better support different geographies.

- Gluware main File Server
- 0–*n* remote File Servers



Note: Remote **File Servers** cannot also be used as Gluware Zone Engines since they must be on two different VMs.

For each **File Server** (main or remote) you plan to use, you'll need:

Component	Minimum requirements
Disk space	To meet enterprise needs for OS images
Memory	4 GB
CPUs/vCPUs	2 CPUs
Other	Unique static IP address

Gluware main File Server communications

Device	Protocol	Port
Gluware remote File Server	SSH	TCP 22*
Gluware Primary Server	RabbitMQ HTTPS	TCP 5672 TCP 443

*Default, user-configurable

Gluware remote File Server communications

Device	Protocol	Port
Gluware main File Server	SSH Rabbit MQ HTTPS	TCP 22* TCP 5672 TCP 443

*Default, user-configurable

Step 2. Gather platform details

Gluware Primary Servers

For the **Gluware Primary Server** installation and configuration, collect the following information:

Component	**Specifications**
Gluware system name	The name that will uniquely identify this Gluware system
Gluware administrative password	The password used by the system administrator to access Gluware
System email	The email address used for actions like password reset of the system administrator and overrides the default (admin@gluware.com)
SMTP host name	Host name of an existing email subsystem you would like used for Gluware notification email (e.g., password reset email)
SMTP user name and password	User name and password for the email system referenced above
CentOS user and password	The CentOS user name and password that the system administrator will use to administer the CentOS system hosting Gluware
IP address for the CentOS host	The external IP address for the system that Gluware is hosted on, which is used to configure network traffic to and from Gluware

Gluware Disaster Recovery Server and Gluware Zone Engines

For **Gluware Disaster Recovery Server** and **Gluware Zone Engines** configurations, collect the following information:

Component	Specifications
CentOS user name and password	The CentOS user name and password that the system administrator will use to administer the CentOS system hosting the Gluware Disaster Recovery Server or Gluware Zone Engines. There is no requirement for this to be the same as the Gluware system CentOS user name and password
IP address for the Gluware Primary Server	The IP address that was configured for the Gluware Primary Server when it was first installed and configured – NOT the CentOS Host System IP Address of the Gluware Disaster Recovery Server or the Gluware Zone Engines

Main and remote File Servers

For **main** and **remote File Server** configurations, collect the following information:

Component	Specifications
CentOS user name and password	The CentOS user name and password that the system administrator will use to administer the CentOS system hosting the File Server. There is no requirement for this to be the same as the Gluware system CentOS user name and password
IP address for the Gluware Primary Server and main File Server	The IP address that was configured for the Gluware Primary Server when it was first installed and configured – NOT the CentOS Host System IP Address of the File Server. For remote File Servers, the IP address for the main File Server

Step 3. Configure your VM

Disk space considerations

The default virtual disk configured for the Gluware VM image is 128 GB. 46 GB is reserved for database storage for **Gluware Primary Servers**, **Gluware Disaster Recovery Server**, and OS images for **File Servers**. Expanding the size of the default virtual disk is best done at deployment time. (VMware will only allow size changes when there are no snapshots of the VM.)

Determining your disk space needs for Gluware is dependent on many factors: number of devices, organizations, scheduled tasks, and types of jobs such as configuration snapshots and audits, and provisioning of config models. In addition, a good **data retention policy** can keep the database from growing rapidly.

The default drive size for a **Gluware Primary Server** will support thousands of devices with configuration snapshots and audits, but only if a good data retention policy is enabled and run regularly. *See* configuration "Step 8: Set up data retention" in this guide.

For future-proofing, increasing the drive to 256 GB or higher and creating a good data retention policy will ensure adequate disk space for the database indefinitely. However, you should reassess your space usage at some interval–say, every six months– to determine if your current disk size is adequate.

Best Practices

For a **Gluware Primary Server**:

- Don't store database backups on the default drive for a long time. Use an additional virtual drive (see below) or an offsite data backup tool. *See* configuration "Step 9. Set up scheduled backups" in this guide.
- Don't enable data retention **archiving** as it uses the default drive.

For a **Gluware Disaster Recovery Server**:

- Set the default virtual drive size identical to the Gluware Primary Server.

For a **Gluware Zone Engines**:

- Very little disk space is consumed by this server type. The default setting will work in all scenarios.

For a **File Server**:

- The size needed is wholly dependent on the number of OS images you plan to store on the system. All image files are stored in the directory `/data` and are not compressed by Gluware.

Additional virtual drives can be created for the VM and activated as mounted partitions. *See* configuration "Step 11: Optional: Make a new virtual drive". A good use for an additional partition is for storing database backups. However, the space can be used for anything: upgrade bundles, capsule files, etc.

Configure the VM

Once the virtual machine image has been downloaded, complete the configuration of the virtual machine if you haven't already done so.

References

Configure VMware at https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.html.hostclient.doc/GUID-DBBF8810-D721-4672-8C20-87AEC68C518D.html

Configure Microsoft Hyper-V at https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/deploy/export-and-import-virtual-machines#import-a-virtual-machine

Step 4. Install Gluware

Gluware virtual machine images are provided by Gluware, Inc. for a variety of hypervisors. The images provide the complete default specification for the Gluware system. For VMWare, this includes the required CPU, memory, networking, storage, and virtual disk requirements. For Hyper-V, this is the virtual disk requirements.

Note: The VMWare image is delivered in OVA format and can be used as is. The image is several gigabytes in size and depending on network speeds, may take considerable time to download.

The Hyper-V image is delivered as a compressed (ZIP) file and must be uncompressed after downloading.

Gluware configuration overview

Once the Gluware Primary Server virtual machine image is loaded, power on the virtual machine and open the Console tab. The installation agent will run as soon as the virtual machine powers up.

You'll configure the general administrative settings, including:

- IP address, default gateway, and subnet mask
- The system administrator account to access the Gluware system, Gluware Disaster Recovery Server, or Gluware Zone Engines
- SMTP mail details used for notifications from Gluware during runtime

Note: For new Gluware installations, you must fully configure the Gluware Primary Server before configuring a Gluware Disaster Recovery Server, Gluware Zone Engine, or File Server.

Gluware VM configuration includes these steps:

Step 1. Configure networking settings

Step 2. Configure the Gluware Primary Server

Step 3. Accept CentOS licensing terms

Step 4. Create the local user

Step 5. Sign off and sign in again

Step 6. Set up organizations and user authentication

Step 7. Install your Gluware licenses

Step 8. Set up data retention

Step 9. Set up scheduled backups

Step 10. Install packages

Optional: Make a new virtual drive

When the Gluware Primary Server is fully configured, and depending on your configuration, configure the following additional servers:

Configure a Gluware Disaster Recovery Server

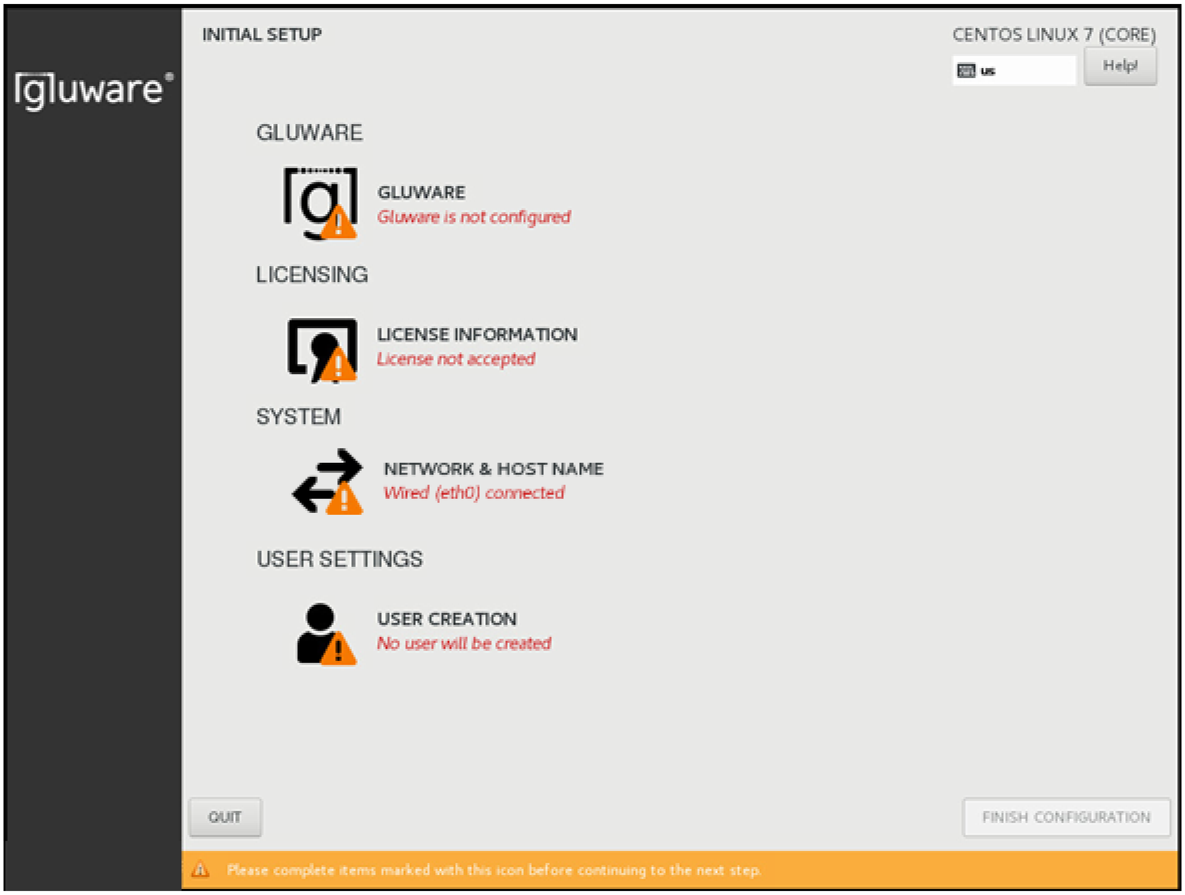
Configure Gluware Zone Engines

Configure a main File Server

Configure a remote File Server

Step 1. Configure network settings

1. Open the **VMware Console**.
2. On the **INITIAL SETUP** screen, **first** select **NETWORK & HOST NAME**.



GLUWARE

GLUWARE
Gluware is not configured

LICENSING

LICENSE INFORMATION
License not accepted

SYSTEM

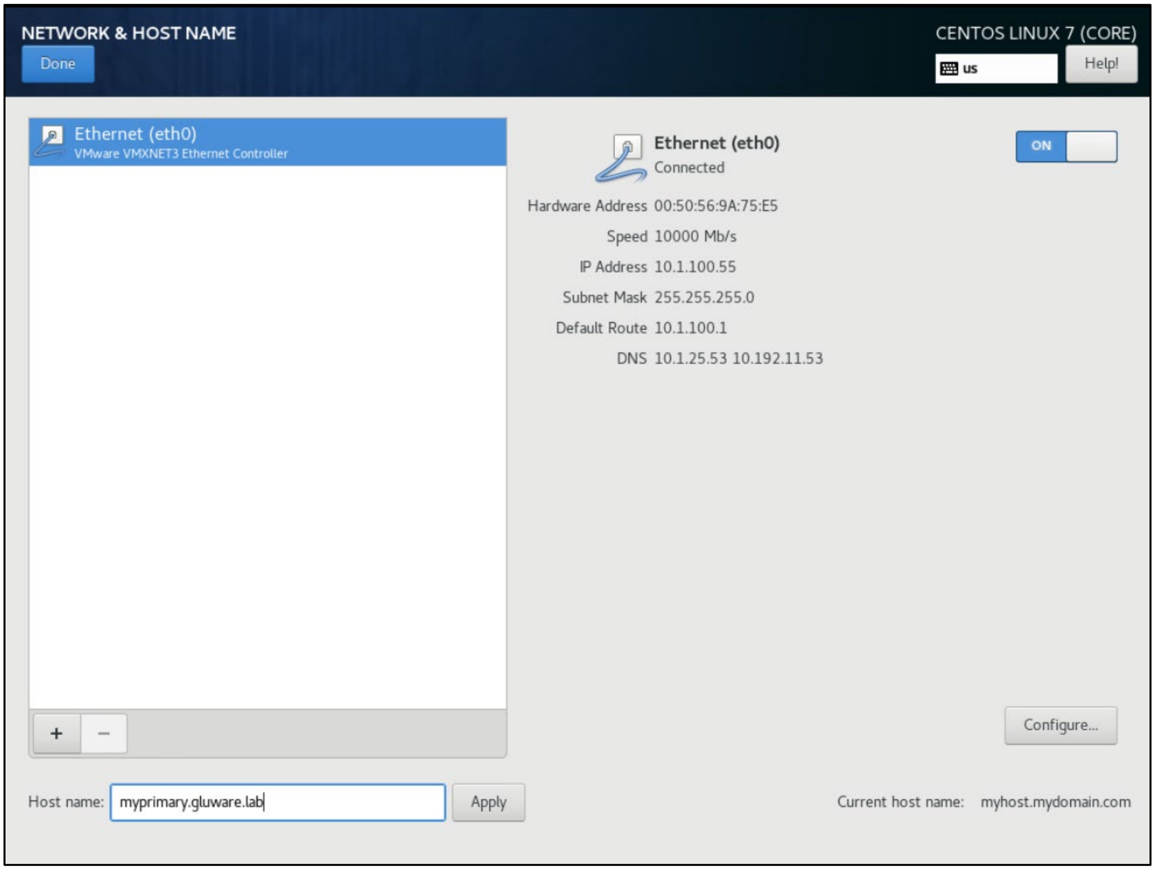
NETWORK & HOST NAME
Wired (eth0) connected

USER SETTINGS

USER CREATION
No user will be created

⚠ Please complete items marked with this icon before continuing to the next step.

3. Ensure that **Ethernet (eth0)** is selected. (Don't change the **Bridge (docker0)** settings.)
4. Enter the fully qualified host name you want for this host and click **Apply**.
5. Click **Configure** to define your network configuration on the eth0 adapter.



NETWORK & HOST NAME

CENTOS LINUX 7 (CORE)

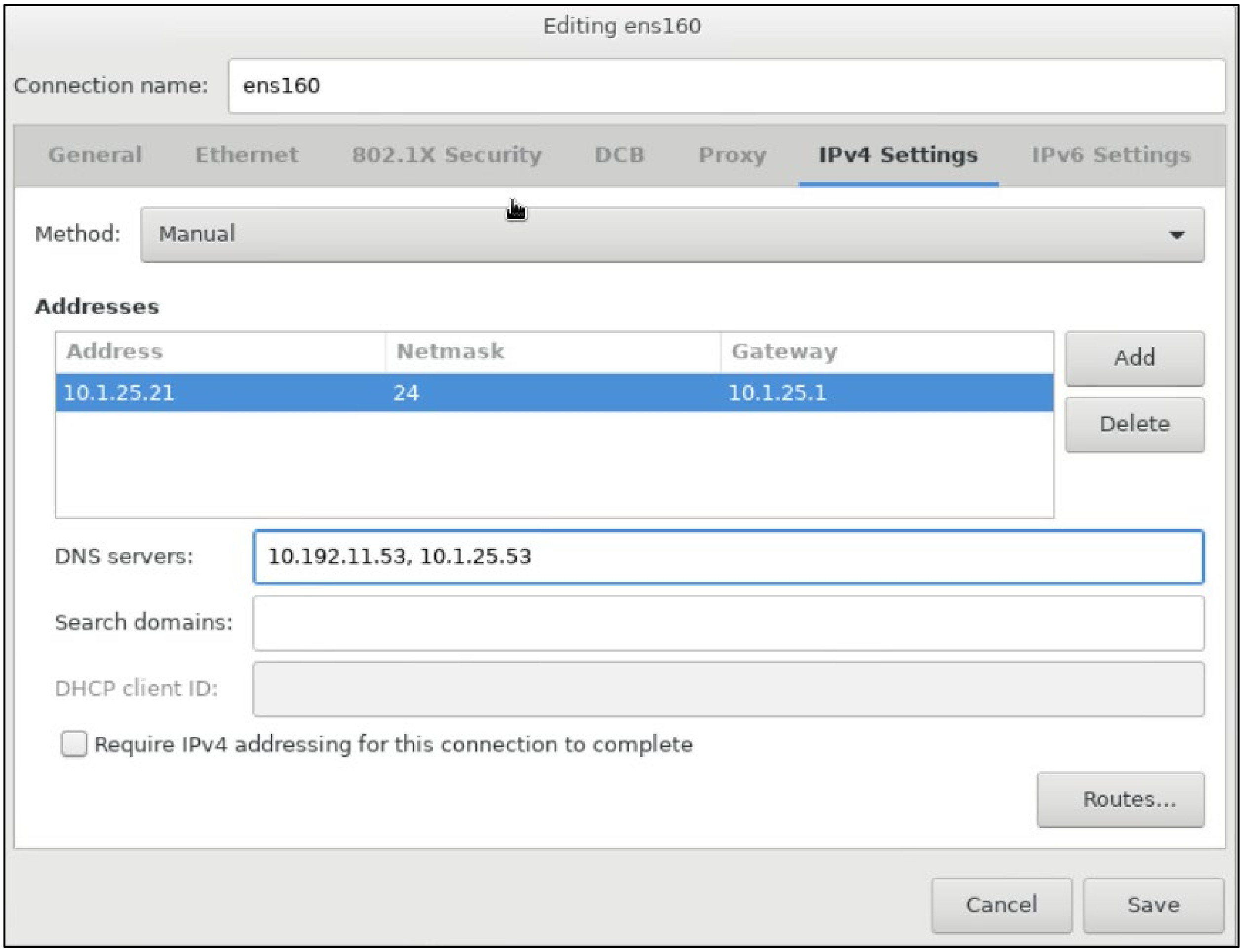
Ethernet (eth0)
VMware VMXNET3 Ethernet Controller

Ethernet (eth0)
Connected

Hardware Address 00:50:56:9A:75:E5
Speed 10000 Mb/s
IP Address 10.1.100.55
Subnet Mask 255.255.255.0
Default Route 10.1.100.1
DNS 10.1.25.53 10.192.11.53

Host name: myprimary.gluware.lab

Current host name: myhost.mydomain.com



Editing ens160

Connection name: ens160

Method: Manual

Addresses

Address	Netmask	Gateway
10.1.25.21	24	10.1.25.1

DNS servers: 10.192.11.53, 10.1.25.53

Search domains:

DHCP client ID:

□ Require IPv4 addressing for this connection to complete

6. Select the **IPv4 Settings** tab.
7. Select **Manual** from the **Method** drop-down list.
8. Click **Add** and enter your network definition: the IP **Address**, **Netmask**, and **Gateway** to assign for this host. It must be consistent with the virtual switch that was assigned for this host when setting up the virtual machine.
9. Enter the **DNS server** names or IP addresses. Separate them with a comma or a space.

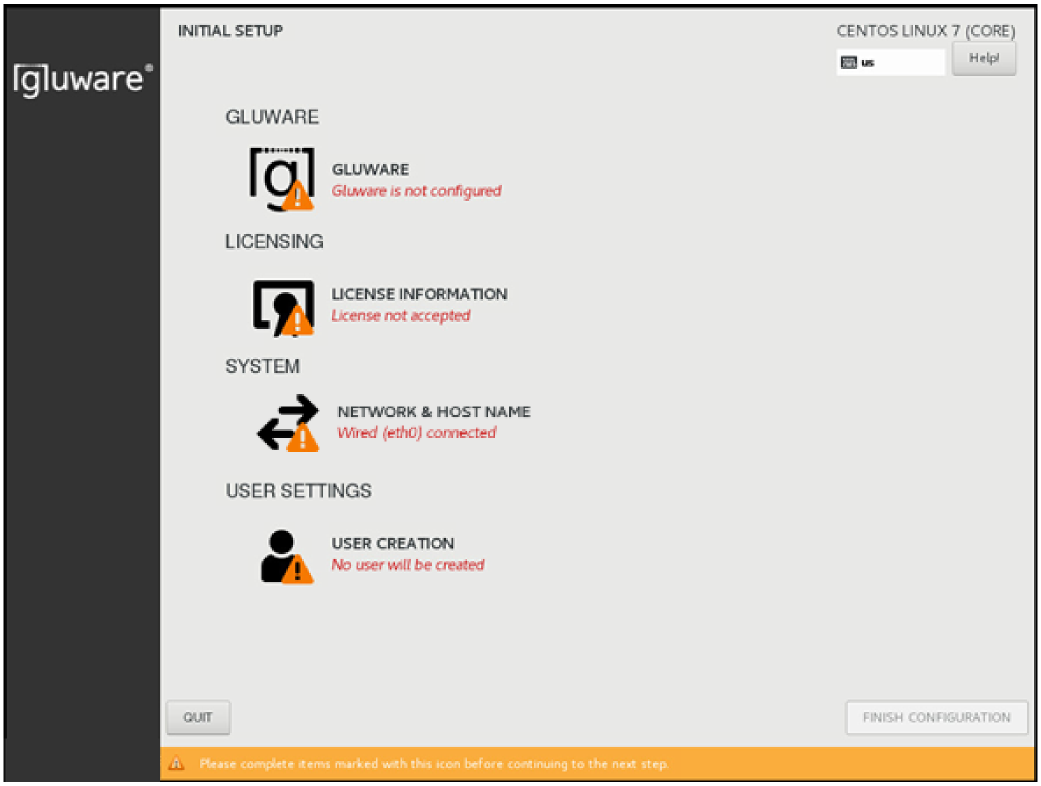
> **Note:** A static IP address is recommended. Use of DHCP is not recommended.

10. Click **Save** to store your network configuration and then click **DONE** to complete your network definition.

The Ethernet (eth0) setting is based on the hypervisor virtual network setup on which the CentOS image has been built. If you need to change the Ethernet settings in CentOS for any reason, from the CentOS desktop select **Applications** > **System Tools** > **Settings** > **Network**, where the network settings can be adjusted for the CentOS system.

Step 2. Configure the Gluware Primary Server

1. On the **INITIAL SETUP** screen, select **GLUWARE**.



GLUWARE

GLUWARE
Gluware is not configured

LICENSING

LICENSE INFORMATION
License not accepted

SYSTEM

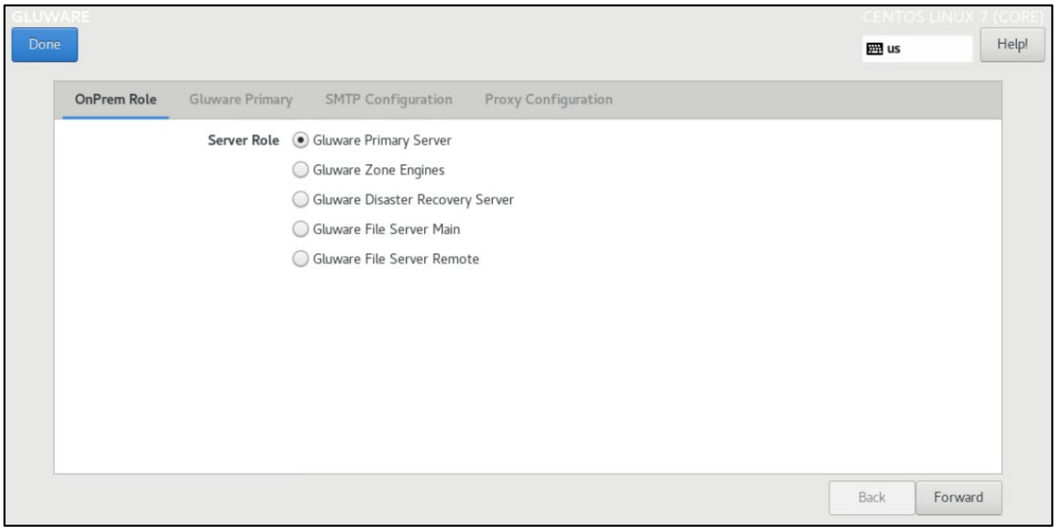
NETWORK & HOST NAME
Wired (eth0) connected

USER SETTINGS

USER CREATION
No user will be created

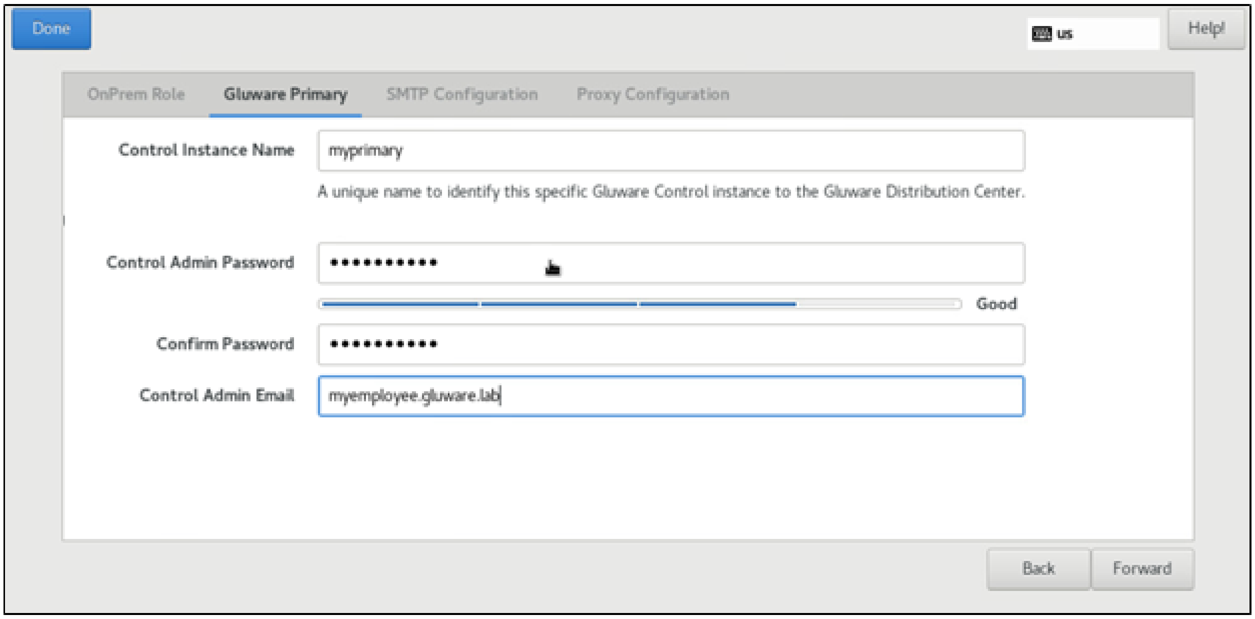
⚠ Please complete items marked with this icon before continuing to the next step.

2. On the **OnPrem Role** tab, make sure **Gluware Primary Server** is selected, and click **Forward**.



Server Role
● Gluware Primary Server
○ Gluware Zone Engines
○ Gluware Disaster Recovery Server
○ Gluware File Server Main
○ Gluware File Server Remote

3. On the **Gluware Primary** tab, define the Gluware system name and the primary admin password and then click **Forward**.



Control Instance Name: myprimary

A unique name to identify this specific Gluware Control instance to the Gluware Distribution Center.

Control Admin Password: ••••••••••• Good

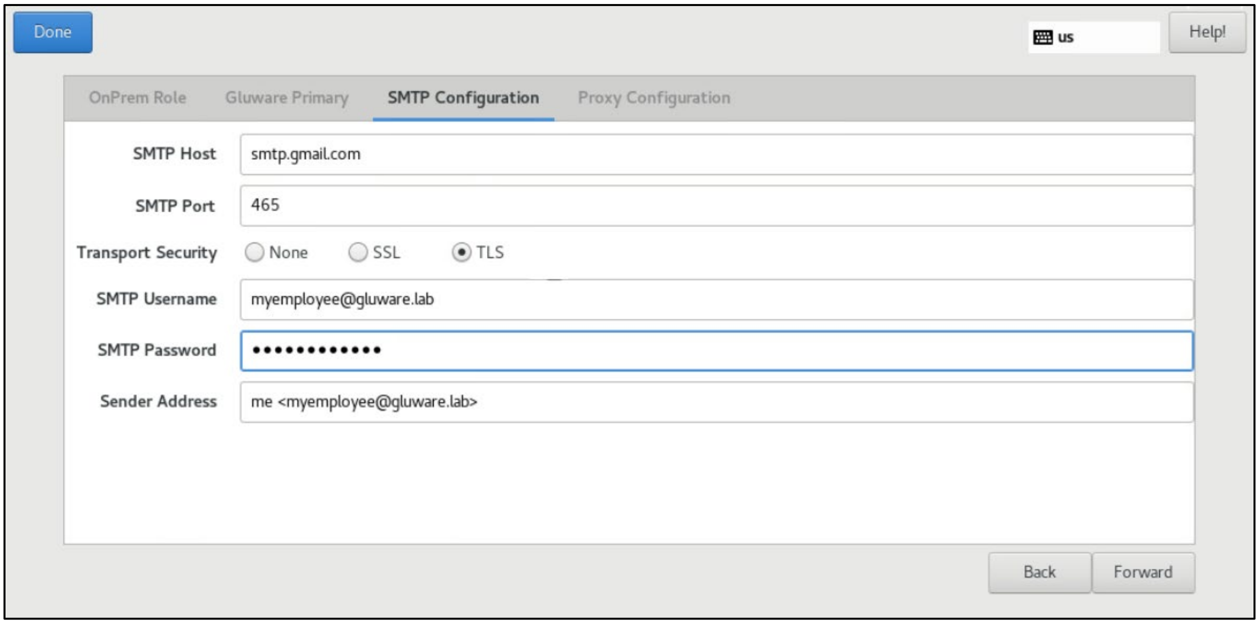
Confirm Password: •••••••••••

Control Admin Email: myemployee.gluware.lab

Property	Description
Control Instance Name	Name used to identify this Gluware system. It is NOT the host name of the machine. It is good practice to include the company name. (e.g., AcmeLabEast)
Control Admin Password	Password for the Gluware admin user. We recommend strong password best practices (min 8 char, a-z, 0-9, #!@, etc.) to protect access to the Gluware system
Confirm Password	Confirm the administrative password
Gluware Admin Email	Email address for the Gluware admin user

4. On the SMTP tab, specify the SMTP configuration details.

Note: Without SMTP options set, Gluware cannot send emails such as password reset and system notifications but will otherwise operate successfully. The format for email sent by Gluware is *displayName <emailAddress>*, e.g., Corp <notify@yourcorp.com>. The user receives the email from Gluware, but the reply goes to notify@yourcorp.com.



SMTP Host: smtp.gmail.com

SMTP Port: 465

Transport Security: ○ None ○ SSL ● TLS

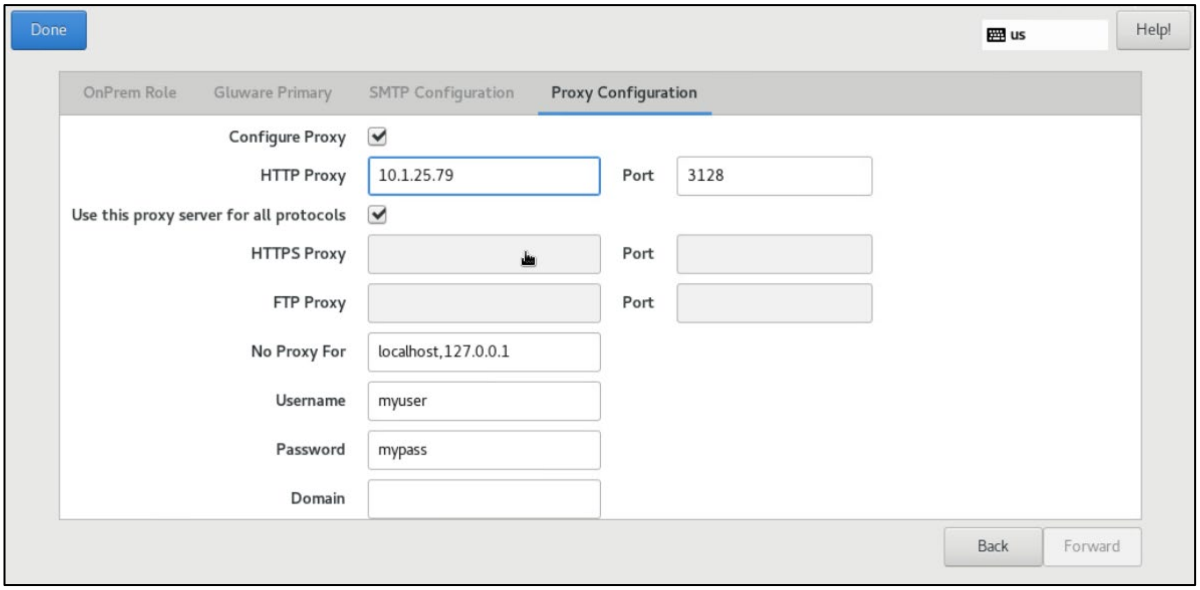
SMTP Username: myemployee@gluware.lab

SMTP Password: ••••••••••••

Sender Address: me <myemployee@gluware.lab>

Property	**Description**
SMTP Host	Host name or IP address for the mail server
SMTP Port	Port number for SMTP traffic
Transport Security	Enable SSL or TLS encryption to secure traffic
SMTP Username	User account used to authenticate with the SMTP Server when sending emails
SMTP Password	Password for the SMTP username account
Sender Address	Email address in the From field of any mail generated from Gluware, such as reset password

5. Do one of the following:
    - Click **Forward** if you intend to use the Gluware Distribution Center and your Gluware Primary Server requires a proxy to access the internet.
    - Otherwise, click **DONE**. **Then continue to the next step:** Accept CentOS licensing terms.
6. Check the **Configure Proxy** box and specify the proxy details.



Configure Proxy ☑

HTTP Proxy 10.1.25.79 Port 3128

Use this proxy server for all protocols ☑

HTTPS Proxy Port

FTP Proxy Port

No Proxy For localhost,127.0.0.1

Username myuser

Password mypass

Domain

Property	**Description**
HTTP Proxy and Port	Host name or IP address for the HTTP proxy server. Port number for the HTTP proxy server
Use this proxy for all protocols	Check the box to use the HTTP proxy for all protocols
HTTPS Proxy and Port	Host name or IP address for the HTTPS proxy server. Port number for the HTTPS proxy server
FTP Proxy and Port	N/A
No Proxy For	N/A

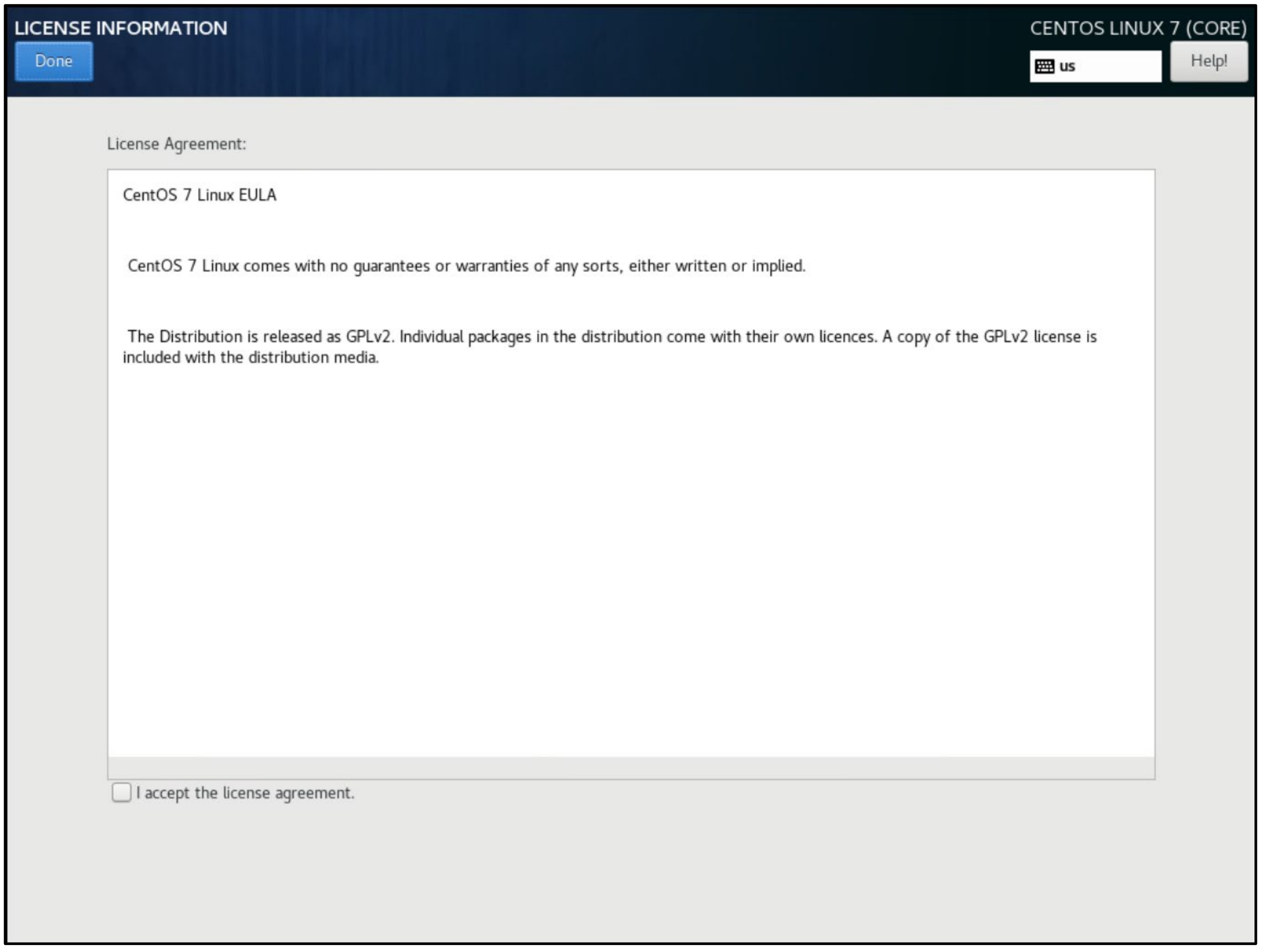
Property	**Description**
Username	Active Directory domain and user account used to authenticate with the proxy server, if needed, in the format *DOMAIN\username*
Password	Password for the proxy server username account, if needed

7. Click **DONE**.

Next step: Accept CentOS licensing terms

Step 3. Accept CentOS licensing terms

1. On the **INITIAL SETUP** screen, select **LICENSE INFORMATION**.
2. Check the box to accept the CentOS license agreement and click **DONE**.



License Agreement:

CentOS 7 Linux EULA

CentOS 7 Linux comes with no guarantees or warranties of any sorts, either written or implied.

The Distribution is released as GPLv2. Individual packages in the distribution come with their own licences. A copy of the GPLv2 license is included with the distribution media.

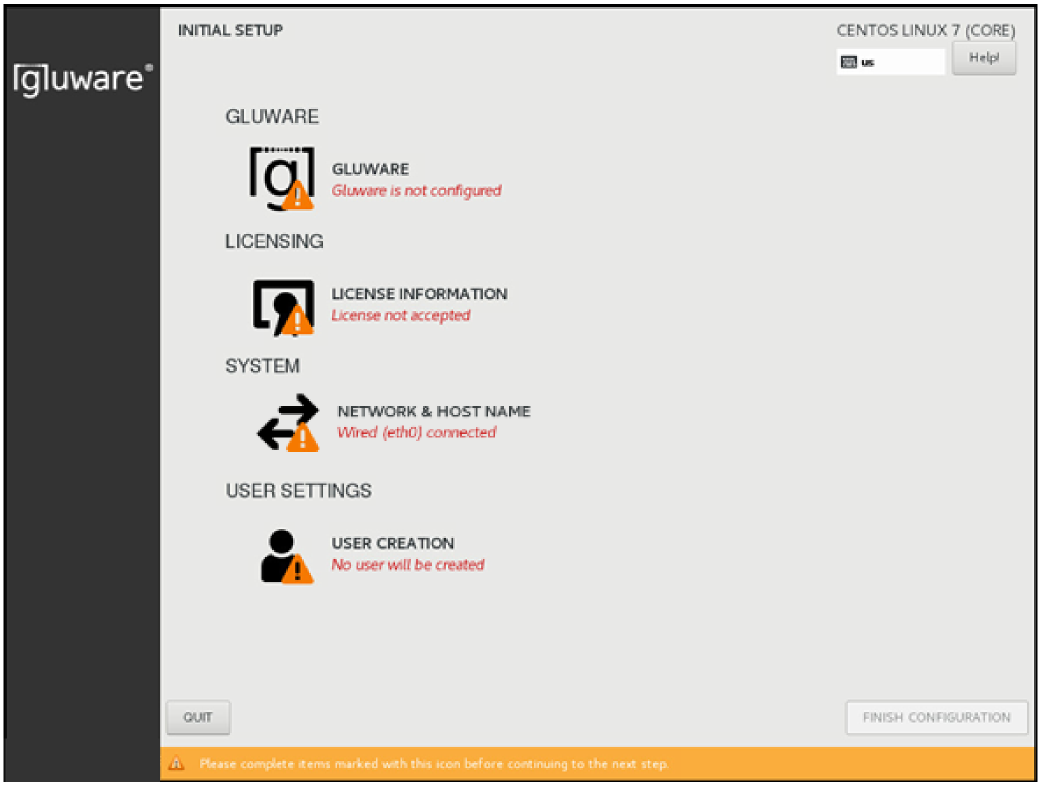
□ I accept the license agreement.

Next step: Create the local user

Step 4. Create the local admin user

The system administrator local user account needs to be created. This isn't a Gluware user—it's the CentOS user that will administer the Gluware system.

1. On the **INITIAL SETUP** screen, select **USER CREATION**.



GLUWARE

GLUWARE
Gluware is not configured

LICENSING

LICENSE INFORMATION
License not accepted

SYSTEM

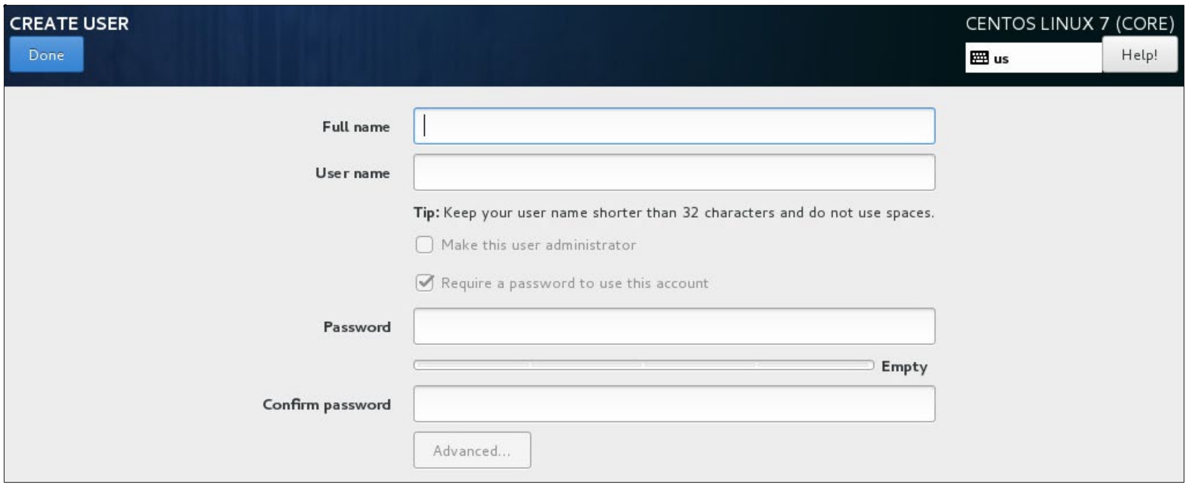
NETWORK & HOST NAME
Wired (eth0) connected

USER SETTINGS

USER CREATION
No user will be created

⚠ Please complete items marked with this icon before continuing to the next step.

2. Provide the **User Name** and **Password** the CentOS user will use to administer the Gluware system. Create a strong password to protect access to Gluware. The password is encrypted using SHA512. Note that the User Name will be copied to the Full Name field.



Tip: Keep your user name shorter than 32 characters and do not use spaces.

□ Make this user administrator

☑ Require a password to use this account

3. Confirm the password and click **DONE**.
4. On the **INITIAL SETUP** screen, click **FINISH CONFIGURATION**.

The installation process takes several minutes to apply the configuration. During this time, you can open a terminal in the console or connect to the system via SSH (using PuTTY or another tool).

The background installation writes to the /var/log/chef-client.log. You can watch the contents of this file to determine when configuration is complete.

The last lines of a successful install are:

```
"INFO: Chef Run Complete in xxx.xxx seconds"
"INFO: Running Report Handlers"
"INFO: Report handlers complete"
```

Gluware is now ready to run and you can sign in using a browser at https://control.*yourcorp*.com.

You can also confirm successful installation on the CentOS desktop. The "Configuring…" status will disappear when installation is complete.

Next step: Sign off and sign in again

Step 5. Sign off and sign in again

Sign off CentOS, either via the console or SSH, and sign in again to ensure the appropriate permissions take effect. Any subsequent steps may fail if you do not have the appropriate permissions.

Next steps

Sign in to Gluware using your admin username and password. Using online **Help**, finish setting up your Gluware system.

Installation note

It's recommended that you sign in to Gluware and complete steps 6–10 before configuring a Disaster Recovery Server, Gluware Zone Engine, or Gluware File Server (main and or remote). However, if you prefer to configure these servers now, before your Gluware licenses are installed, you must accept the default organization, GluwareSystemOrganization, during configuration. If you install Gluware File Servers, you won't be able to change the name of the default organization later.

Step 6. Set up organizations and user authentication

See the following **Help** topics for details:

- Add or update organizations
- Configure single sign-on authentication
- Configure Gluware to interact with LDAP
- Configure Gluware to interact with RADIUS
- Add Gluware users

Step 7. Install your Gluware licenses

See the following **Help** topic:

- Install a Gluware license

Step 8. Set up data retention

See the following **Help** topic:

- Manage data retention

Step 9. Set up scheduled backups

See the following **Help** topic:

- Back up Gluware systems

Step 10. Install packages

See the following **Help** topic:

- Install packages

Optional: Make a new virtual drive

If you added an additional virtual drive when configuring the VM, use the `gluwarectl createDisk` action to register the drive with the OS.

Sign in to Gluware via a terminal session using the local user account you created. Execute the following command:

`sudo gluwarectl createDisk` <device> <mount>

Note: To utilize `createDisk` you must be familiar with Linux file systems and how to create virtual drives in your hypervisor.

Configure a Gluware Disaster Recovery Server

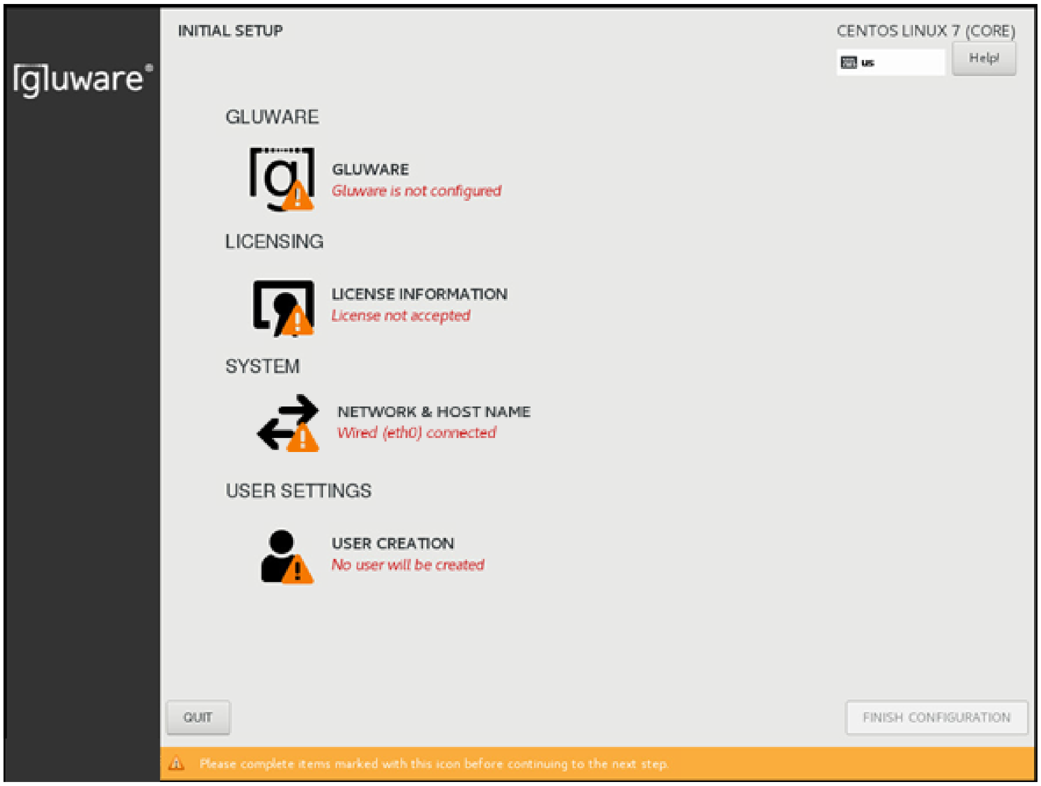
Set up the Gluware Primary Server completely before you configure the Disaster Recovery Server.

To configure the Gluware Disaster Recovery Server, ensure you have the following information:

- A unique IP address for this VM (the Gluware Disaster Recovery Server)
- The IP address of the Gluware Primary Server
- The CentOS user name and password for this VM

Confirm network settings

1. Open the **VMware Console**.
2. On the **INITIAL SETUP** screen, **first** select **NETWORK & HOST NAME**.



GLUWARE

GLUWARE
Gluware is not configured

LICENSING

LICENSE INFORMATION
License not accepted

SYSTEM

NETWORK & HOST NAME
Wired (eth0) connected

USER SETTINGS

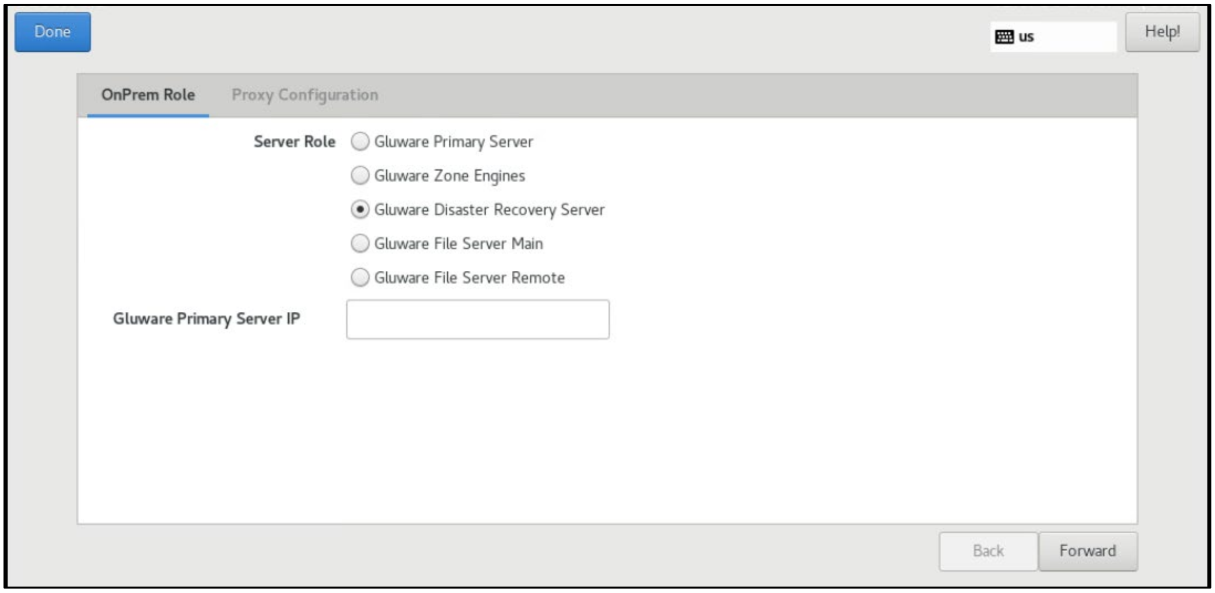
USER CREATION
No user will be created

Please complete items marked with this icon before continuing to the next step.

3. Ensure that **Ethernet (eth0)** is selected. (Don't change the **Bridge (docker0)** settings.)
4. Enter the fully qualified host name you want for this host and click **Apply**.
5. Click **Configure** to define your network configuration on the eth0 adapter.
6. Select the **IPv4 Settings** tab.
7. Select **Manual** from the **Method** drop-down list.
8. Click **Add** and enter your network definition: the IP **Address**, **Netmask**, and **Gateway** to assign for this host. It must be consistent with the virtual switch that was assigned for this host when setting up the virtual machine.
9. Click **Save** to store your network configuration and then click **DONE** to complete your network definition.

Configure the Gluware Disaster Recovery Server

10. On the **INITIAL SETUP** screen, select **GLUWARE**.
11. On the **OnPrem Role** tab, select **Gluware Disaster Recovery Server**.
12. Enter the IP address for the Gluware Primary Server. At this point, the address is validated, and a connection is tested.



Server Role
○ Gluware Primary Server
○ Gluware Zone Engines
● Gluware Disaster Recovery Server
○ Gluware File Server Main
○ Gluware File Server Remote

Gluware Primary Server IP

13. Click **DONE**.

Accept CentOS licensing terms

14. On the **INITIAL SETUP** screen, select **LICENSE INFORMATION**.
15. Check the box to accept the CentOS license agreement and click **DONE**.

Create the local user

16. On the **INITIAL SETUP** screen, select **USER CREATION**.
17. Enter the CentOS user's first and last name (**Full name**).
18. Provide the **User Name** and **Password** the CentOS user will use to administer the Gluware system. Create a strong password to protect access to Gluware.
19. Confirm the password and click **DONE**.
20. On the **INITIAL SETUP** screen, click **FINISH CONFIGURATION**.

Final steps

21. Sign off CentOS and sign in again to ensure the appropriate permissions take effect.
22. **IMPORTANT:** After the VM installation is complete for the Gluware Disaster Recovery Server, sign in to Gluware via a terminal session using the local user account you created and issue the `sudo gluwarectl reconfigure` command on the Primary Server for the Gluware Disaster Recovery Server to be initialized and configured for standby mode.

Configure Gluware Zone Engines

Set up the Gluware Primary Server completely before you configure Gluware Zone Engines. It's also recommended that you set up organizations and install Gluware licenses before configuring Gluware Zone Engines. However, if you prefer to configure Gluware Zone Engines before your Gluware licenses are installed, you must accept the default organization, GluwareSystemOrganization, during configuration.

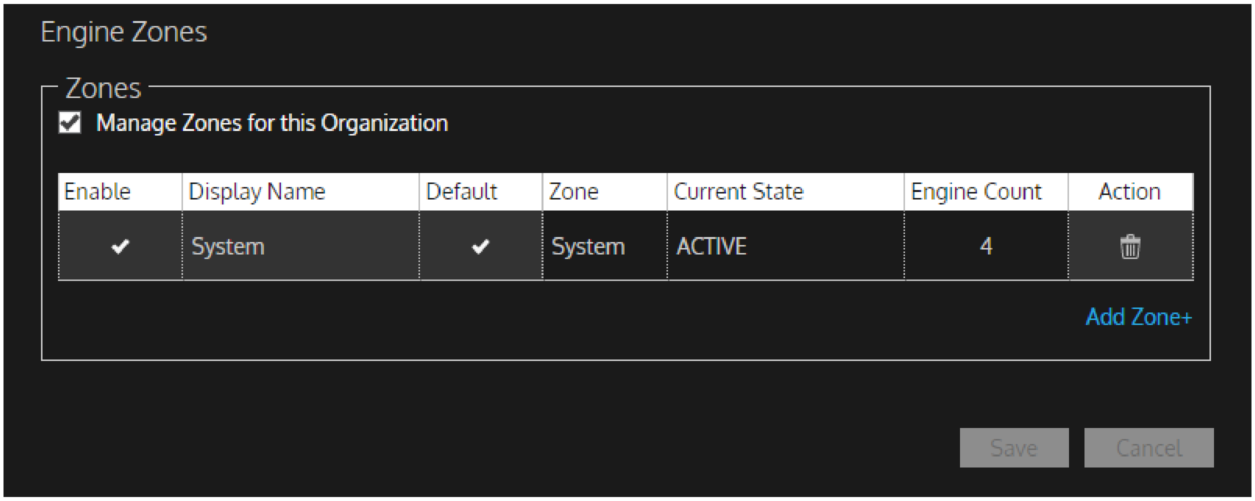
When you install a Gluware Zone Engines Server, you can assign the engines to a zone. Then each device can preferentially run jobs on the zone's engine or engines when they are ACTIVE.

If a device is **locked** to a zone, jobs will only run on the engines in that zone. Should those engines become INACTIVE, jobs will not run until the engines are ACTIVE again.

> **Note:** All child organizations share the zone. It's best to add the zone in the same organization that your Gluware licenses are installed in so that devices in all child organizations can use the zone. If you enable a zone in a child organization, zones from the parent organization can be disabled in the child organization.

To configure Gluware Zone Engines, ensure you have the following information:

- A unique IP address for this VM (the Gluware Zone Engines)
- The IP address of the Gluware Primary Server
- The CentOS user name and password for this VM



Engine Zones

Zones

☑ Manage Zones for this Organization

Enable	Display Name	Default	Zone	Current State	Engine Count	Action
✓	System	✓	System	ACTIVE	4	🗑

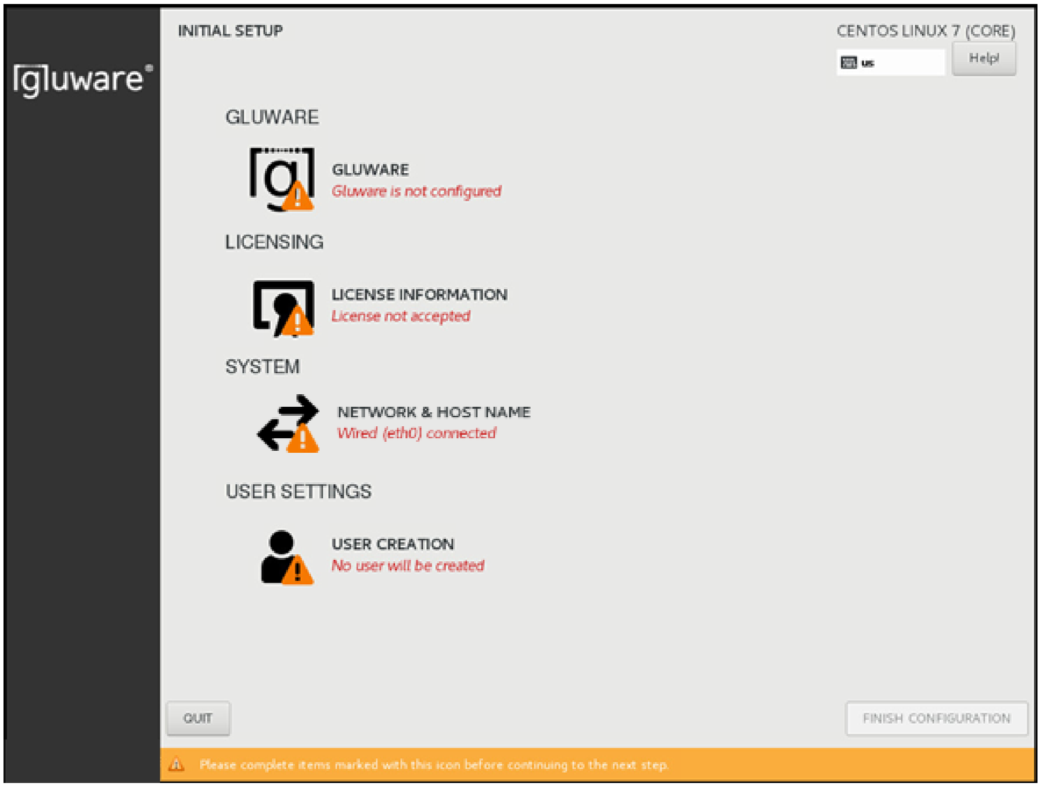
Add a zone in Gluware Settings

Add one or more zone in Gluware Settings if you want to create and use zones other than the default zone (System). If you will only use the System zone, skip this step.

1. Recommended: Ensure you're in the organization in which your Gluware licenses are installed.
2. Go to Gluware ⚙ **Settings** and select **Organization** > **Zones**.
3. Check the **Manage Zones for this Organization** box.
4. Click **Add Zone+**.
5. Name the zone and provide a display name.
6. Save.

Confirm network settings

1. Open the **VMware Console**.
2. On the **INITIAL SETUP** screen, **first** select **NETWORK & HOST NAME**.



Gluware is not configured

License not accepted

Wired (eth0) connected

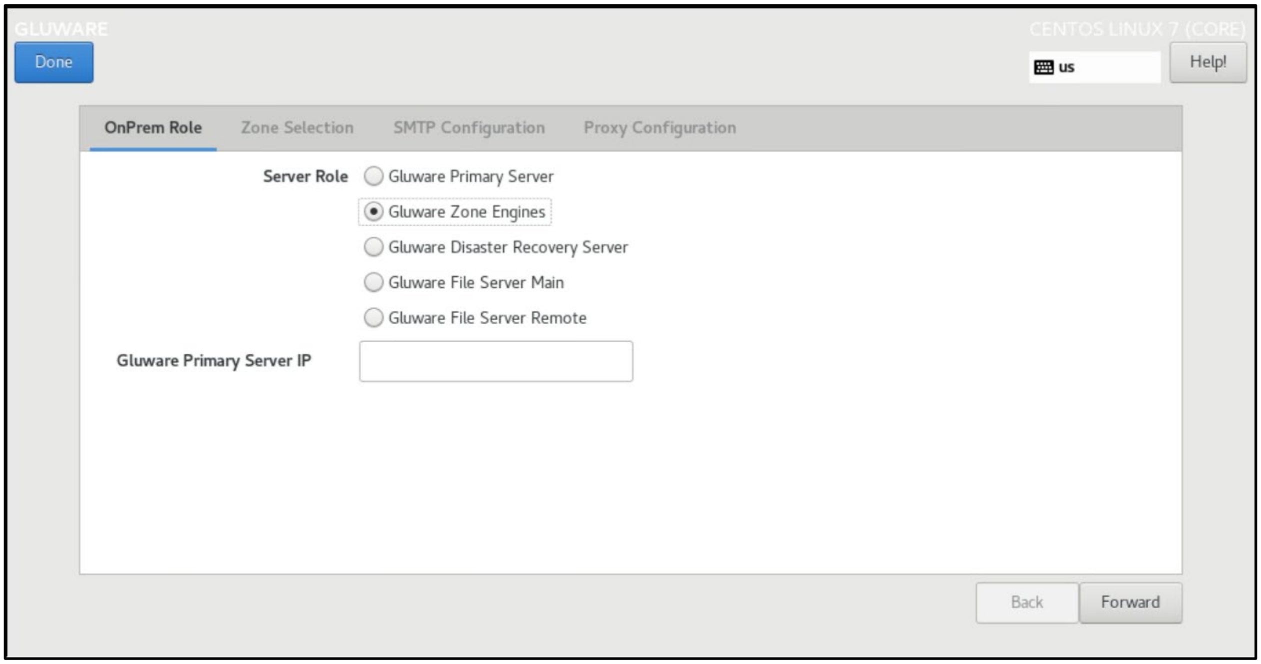
No user will be created

Please complete items marked with this icon before continuing to the next step.

3. Ensure that **Ethernet (eth0)** is selected. (Don't change the **Bridge (docker0)** settings.)
4. Enter the fully qualified host name you want for this host and click **Apply**.
5. Click **Configure** to define your network configuration on the eth0 adapter.
6. Select the **IPv4 Settings** tab.
7. Select **Manual** from the **Method** drop-down list.
8. Click **Add** and enter your network definition: the IP **Address**, **Netmask**, and **Gateway** to assign for this host. It must be consistent with the virtual switch that was assigned for this host when setting up the virtual machine.
9. Click **Save** to store your network configuration and then click **DONE** to complete your network definition.

Configure the Gluware Zone Engines Server

10. On the **INITIAL SETUP** screen, select **GLUWARE**.
11. On the **OnPrem Role** tab, select **Gluware Zone Engines**.
12. Enter the IP address for the Gluware Primary Server. At this point, the address is validated, and a connection is tested.
13. Do one of the following:
    - If you are only using the System zone (the default zone), click **DONE**. **Then continue to the next step:** Accept CentOS licensing terms.
    - If you set up one or more additional zones in Gluware system settings, click **Forward** to specify the zone for these Zone Engines.



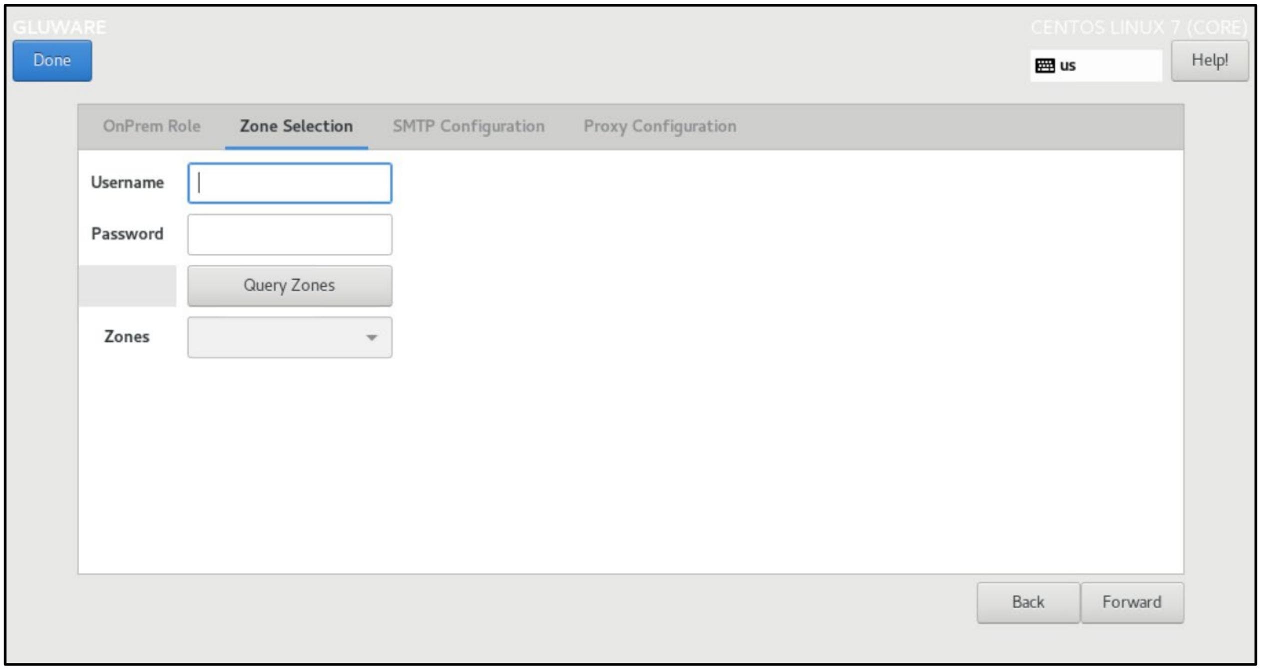
Server Role
○ Gluware Primary Server
● Gluware Zone Engines
○ Gluware Disaster Recovery Server
○ Gluware File Server Main
○ Gluware File Server Remote

Gluware Primary Server IP

Select a zone

If you added zones in Gluware system settings, specify the zone for the Zone Engines Server.

14. On the **Engine Zone Selection** tab, enter a **Gluware username** and **password**. Only Gluware superusers, System Admins, and System Developers can configure additional zones
15. Click **Query Zones**. CentOS retrieves the zones that you added in Gluware system settings.
16. Select the zone for this Zone Engines Server from the drop-down list.



17. Click **DONE**.

Accept CentOS licensing terms

18. On the **INITIAL SETUP** screen, select **LICENSE INFORMATION**.
19. Check the box to accept the CentOS license agreement and click **DONE**.

Create the local user

20. On the **INITIAL SETUP** screen, select **USER CREATION**.
21. Enter the CentOS user's first and last name (**Full name**).
22. Provide the **User Name** and **Password** the CentOS user will use to administer the Gluware system. Create a strong password to protect access to Gluware.
23. Confirm the password and click **DONE**.
24. On the **INITIAL SETUP** screen, click **FINISH CONFIGURATION**.

Final steps

25. Sign off CentOS and sign in again to ensure the appropriate permissions take effect.
26. **IMPORTANT:** After the VM installation is complete for the Gluware Zone Engines, sign in to Gluware via a terminal session using the local user account you created and issue the `sudo gluwarectl reconfigure` command on the Primary Server for Gluware Zone Engines to be utilized.

Best practices

We recommend that you tune the Zone Engines and queues for the types of workload you forecast running on your Gluware system over time (Config Drift captures, OS upgrades, Config Model Editor provisioning, etc.). *See* the "Gluware Engine Tuning" topic in online Help for details of the `gluwareEngineTuning` and `queue` operations of the `gluwarectl` utility.

Configure a main File Server

Set up the Gluware Primary Server completely before you configure Gluware File Servers. It's also recommended that you set up organizations and install Gluware licenses before configuring Gluware File Servers. However, if you prefer to configure these servers before your Gluware licenses are installed, you must accept the default organization, GluwareSystemOrganization, during configuration. You won't be able to change the name of default organization later.

Each organization can have one **main File Server** and any number of **remote File Servers**. If an organization does not have a main File Server, it inherits the File Servers from the parent organization. You can configure multiple File Servers if you need separation of peer organizations and data.

Gluware **File Server** is required to use **OS Manager** and an **OS Manager license** is required.

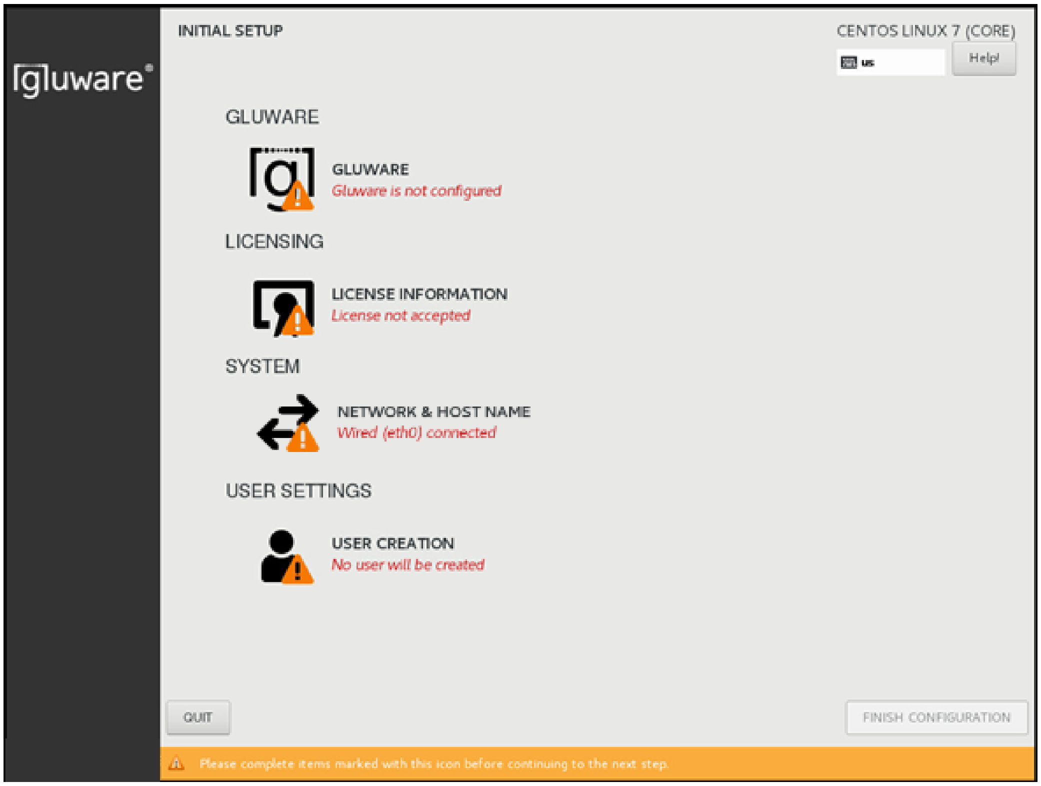
To configure the main File Server, ensure you have the following information:

- A unique IP address for this VM (main File Server)
- The IP address of the Gluware Primary Server
- The CentOS user name and password for this VM
- The SSH port for the administration of the main file server VM
- Port assignments for the SSH/SCP port
- Port assignments for the FTP and TFTP ports, if used

On the main File Server

Confirm network settings

1. Open the **VMware Console**.
2. On the **INITIAL SETUP** screen, **first** select **NETWORK & HOST NAME**.



INITIAL SETUP

CENTOS LINUX 7 (CORE)

GLUWARE

GLUWARE
Gluware is not configured

LICENSING

LICENSE INFORMATION
License not accepted

SYSTEM

NETWORK & HOST NAME
Wired (eth0) connected

USER SETTINGS

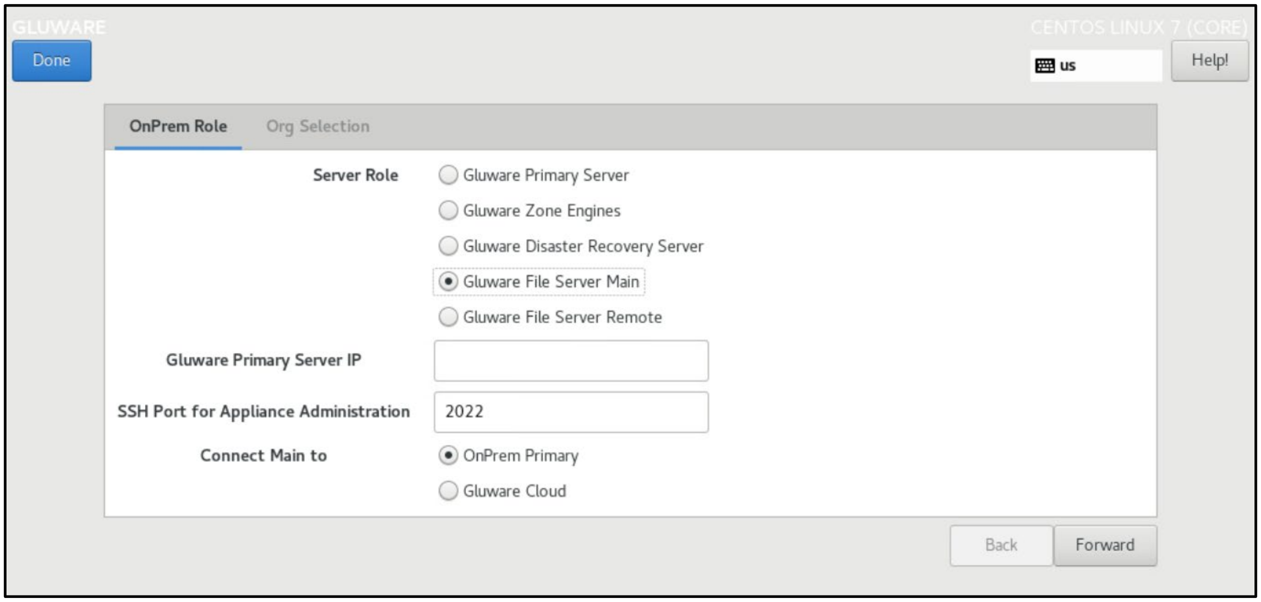
USER CREATION
No user will be created

Please complete items marked with this icon before continuing to the next step.

3. Ensure that **Ethernet (eth0)** is selected. (Don't change the **Bridge (docker0)** settings.)
4. Enter the fully qualified host name you want for this host and click **Apply**.
5. Click **Configure** to define your network configuration on the eth0 adapter.
6. Select the **IPv4 Settings** tab.
7. Select **Manual** from the **Method** drop-down list.
8. Click **Add** and enter your network definition: the IP **Address**, **Netmask**, and **Gateway** to assign for this host. It must be consistent with the virtual switch that was assigned for this host when setting up the virtual machine.
9. Click **Save** to store your network configuration and then click **DONE** to complete your network definition.

Configure the main File Server

10. On the **INITIAL SETUP** screen, select **GLUWARE**.
11. On the **OnPrem Role** tab, select **Gluware File Server Main**.



Server Role
○ Gluware Primary Server
○ Gluware Zone Engines
○ Gluware Disaster Recovery Server
● Gluware File Server Main
○ Gluware File Server Remote

Gluware Primary Server IP

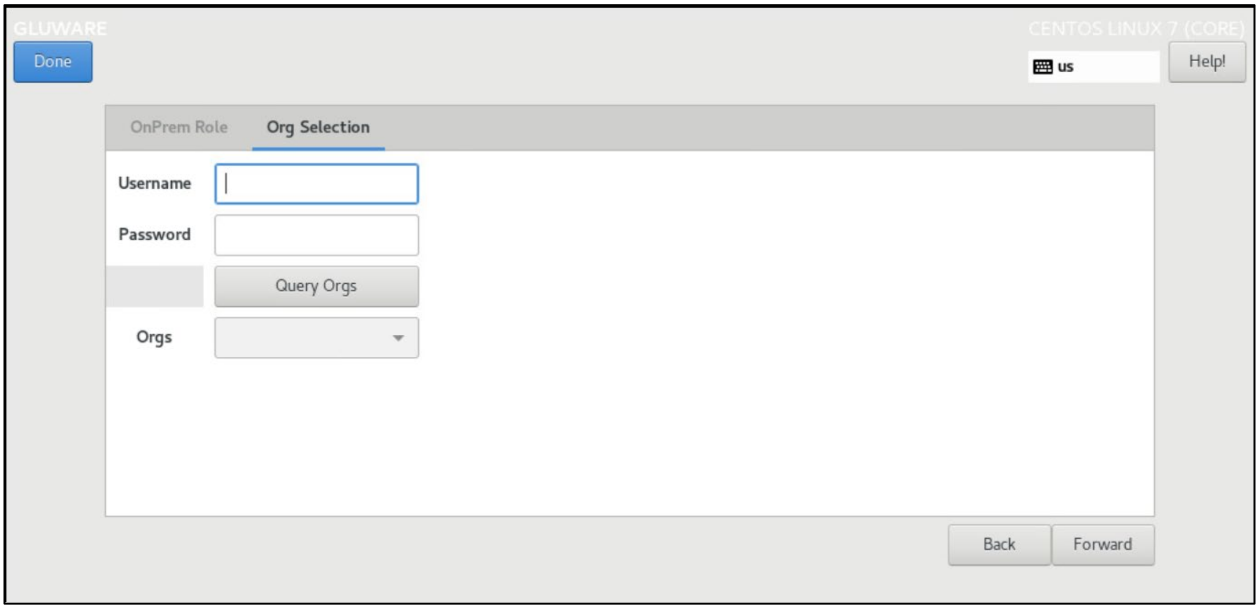
SSH Port for Appliance Administration: 2022

Connect Main to
● OnPrem Primary
○ Gluware Cloud

12. Enter the IP address of the Gluware Primary Server. At this point, the address is validated, and a connection is tested.
13. Enter the SSH port to use for the administration of the VM. You cannot use port 22 as that port is used to respond to SCP requests for file transfers.
14. Click **Forward**.

Select an organization

15. On the **Org Selection** tab, enter a **Gluware username** and **password**. Only Gluware superusers, System Admins, and System Developers can configure File Servers.
16. Click **Query Orgs**.
17. Select the organization for this Gluware main File Server from the drop-down list.



18. Click **DONE.**

Accept CentOS licensing terms

19. On the **INITIAL SETUP** screen, select **LICENSE INFORMATION**.
20. Check the box to accept the CentOS license agreement and click **DONE**.

Create the local user

21. On the **INITIAL SETUP** screen, select **USER CREATION**.
22. Enter the CentOS user's first and last name (**Full name**).
23. Provide the **User Name** and **Password** the CentOS user will use to administer the Gluware system. Create a strong password to protect access to Gluware.

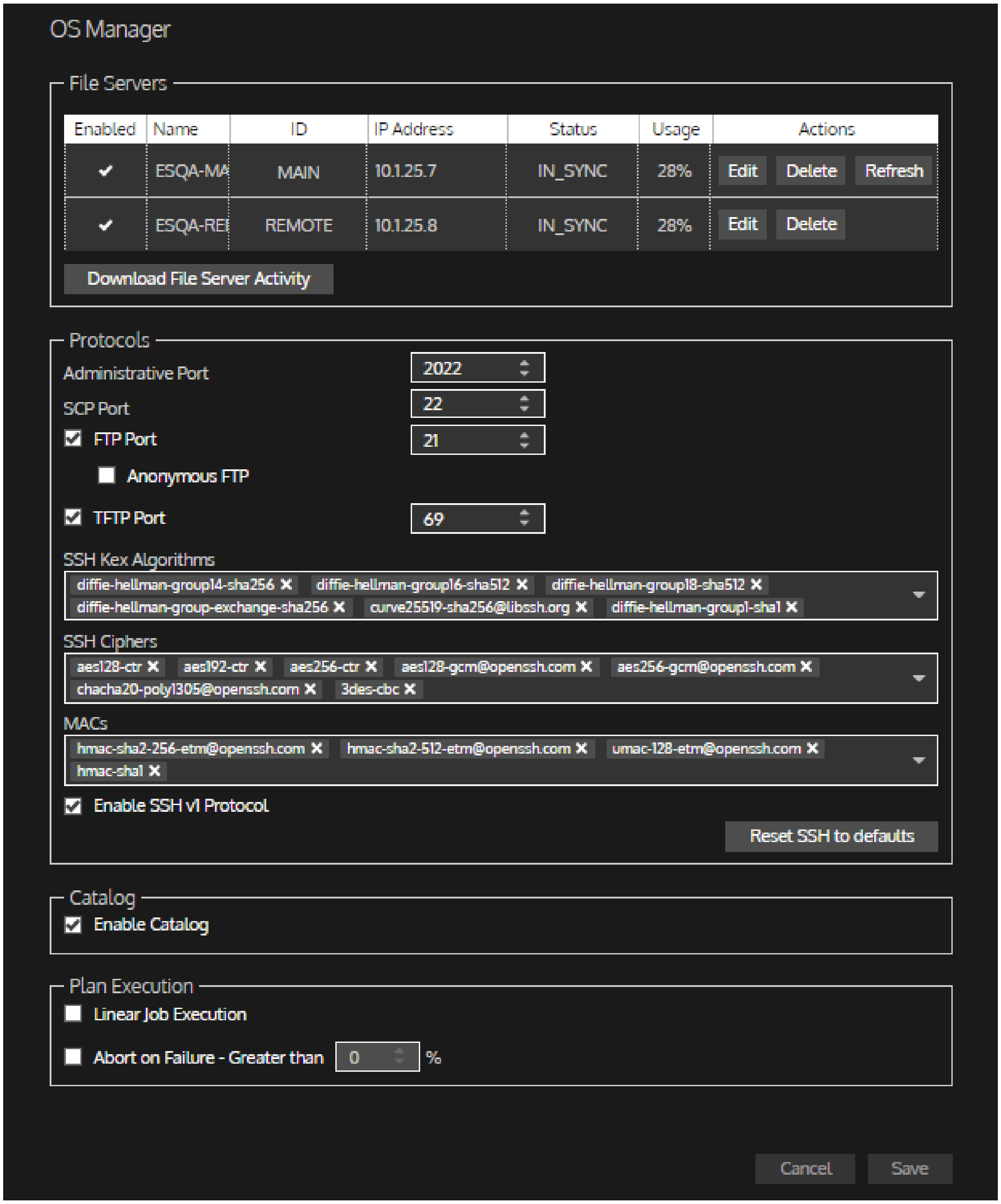
24. Confirm the password and click **DONE**.
25. On the **INITIAL SETUP** screen, click **FINISH CONFIGURATION**.
26. Sign off CentOS and sign in again to ensure the appropriate permissions take effect.

When the configuration of the File Server is complete, go to Gluware **Settings** to set up the File Server in Gluware.

Verify the File Server in Gluware Settings

Once you configure the VM for the main File Server, it is registered in Gluware system settings.

1. Go to Gluware ⚙ **Settings** > **Organization** > **OS Manager** and ensure you're in the organization that you added the main File Server to.



OS Manager

File Servers

Enabled	Name	ID	IP Address	Status	Usage	Actions
✓	ESQA-MA	MAIN	10.1.25.7	IN_SYNC	28%	Edit Delete Refresh
✓	ESQA-RE	REMOTE	10.1.25.8	IN_SYNC	28%	Edit Delete

Protocols

Administrative Port: 2022

SCP Port: 22

☑ FTP Port: 21

□ Anonymous FTP

☑ TFTP Port: 69

SSH Kex Algorithms: diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group-exchange-sha256, curve25519-sha256@libssh.org, diffie-hellman-group1-sha1

SSH Ciphers: aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com, chacha20-poly1305@openssh.com, 3des-cbc

MACs: hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha1

☑ Enable SSH v1 Protocol

Catalog

☑ Enable Catalog

Plan Execution

□ Linear Job Execution

□ Abort on Failure - Greater than 0 %

2. If you are adding the main File Server in a child organization, check the **Enable New Main File Server for this Organization** box.

Note: The File Server will be used by all child organizations unless they have their own File Server.

3. Ensure the **Enable File Server** box is checked.
4. Verify the name and IP address for the main server.
5. Ensure the **Administrative Port** and **SCP Port** assignments are correct.
6. Optional: Clear the **FTP Port**, **TFTP Port**, or the **Anonymous FTP** box to disable the port. These ports are not required. Ensure the enabled port assignments are correct.
7. Only if necessary: Make changes to the encryption algorithms by removing or adding algorithms in the **SSH Kex Algorithms**, **SSH Ciphers**, and **MACs** boxes.

WARNING! Some encryption algorithms may expose security vulnerabilities but may be required by older devices or firmware.

8. Optional: Clear the **Enable SSH v1 Protocol** box. SSH v2 Protocol is always enabled, regardless of this setting.
9. Save.

Configure a remote File Server

Configure the main File Server before configuring any remote File Servers.

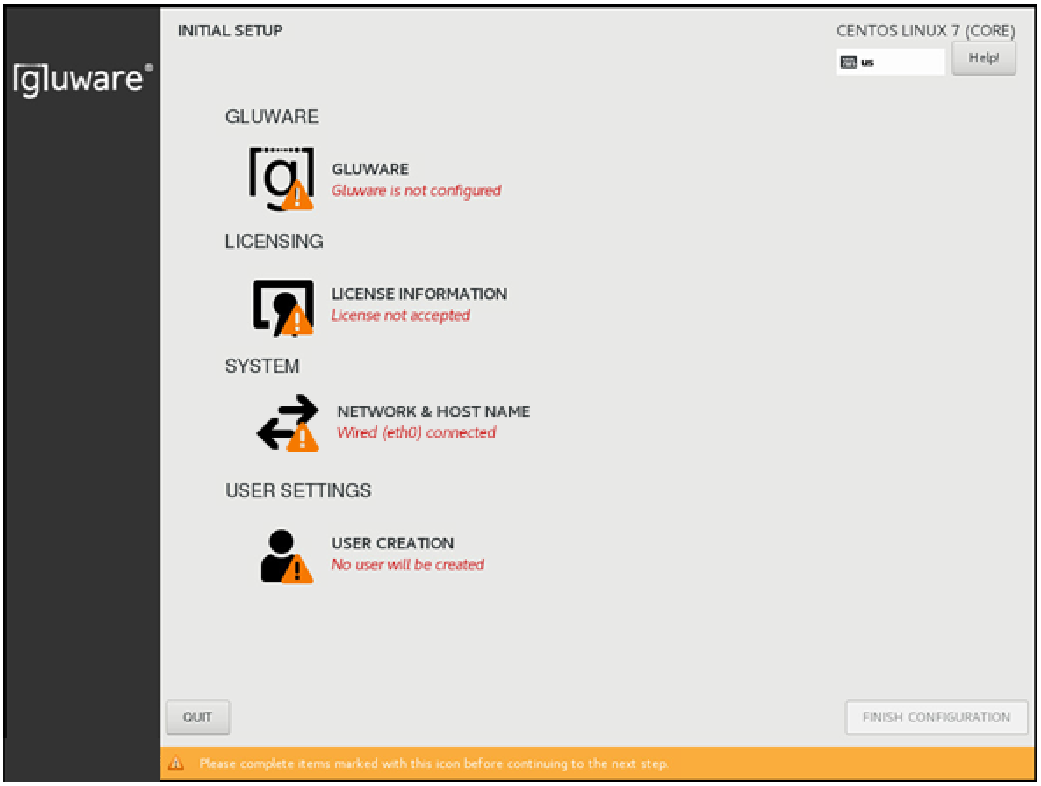
To configure a remote File Server, ensure you have the following information:

- A unique IP address for this VM (remote File Server)
- The IP address of the main File Server
- The CentOS user name and password for this VM
- The SSH port number you specified for the main File Server as the **Gluware File Server Main Administrative Port**
- The port number for the remote File Server's **SSH Port for Appliance Administration**

On the remote File Server

Confirm network settings

1. Open the **VMware Console**.
2. On the **INITIAL SETUP** screen, **first** select **NETWORK & HOST NAME**.



INITIAL SETUP

CENTOS LINUX 7 (CORE)

gluware

GLUWARE

GLUWARE
Gluware is not configured

LICENSING

LICENSE INFORMATION
License not accepted

SYSTEM

NETWORK & HOST NAME
Wired (eth0) connected

USER SETTINGS

USER CREATION
No user will be created

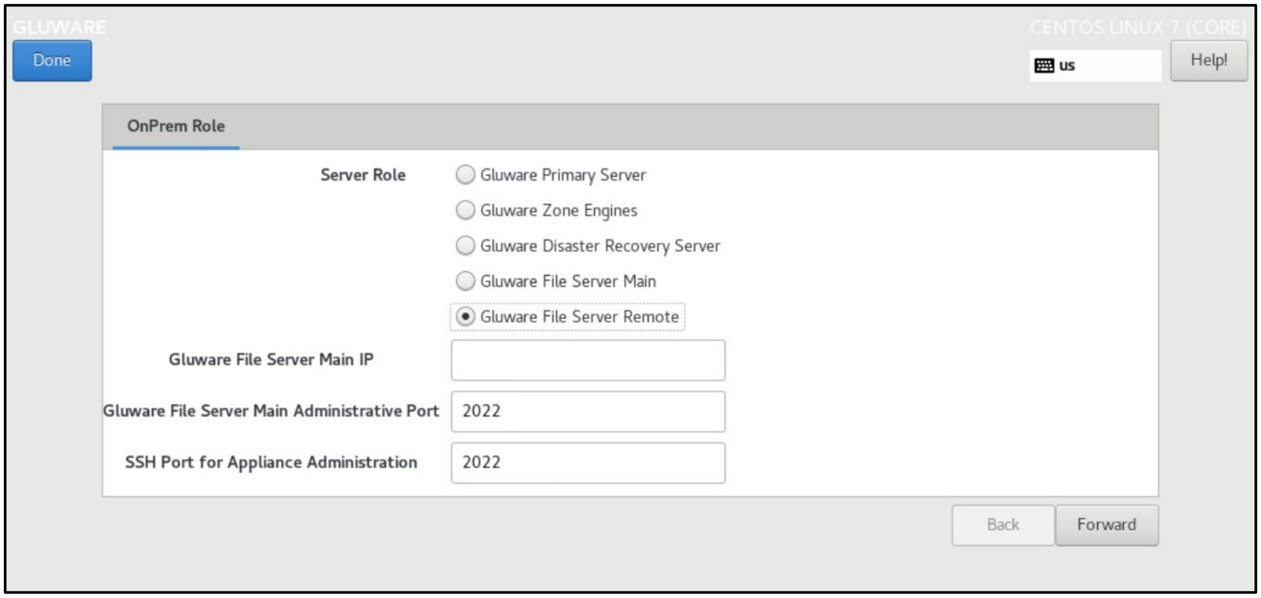
Please complete items marked with this icon before continuing to the next step.

3. Ensure that **Ethernet (eth0)** is selected. (Don't change the **Bridge (docker0)** settings.)
4. Enter the fully qualified host name you want for this host and click **Apply**.
5. Click **Configure** to define your network configuration on the eth0 adapter.
6. Select the **IPv4 Settings** tab.
7. Select **Manual** from the **Method** drop-down list.
8. Click **Add** and enter your network definition: the IP **Address**, **Netmask**, and **Gateway** to assign for this host. It must be consistent with the virtual switch that was assigned for this host when setting up the virtual machine.

9. Click **Save** to store your network configuration and then click **DONE** to complete your network definition.

Configure the remote File Server

10. On the **INITIAL SETUP** screen, select **GLUWARE**.
11. On the **OnPrem Role** tab, select **Gluware File Server Remote**.



Server Role
○ Gluware Primary Server
○ Gluware Zone Engines
○ Gluware Disaster Recovery Server
○ Gluware File Server Main
● Gluware File Server Remote

Gluware File Server Main IP:

Gluware File Server Main Administrative Port: 2022

SSH Port for Appliance Administration: 2022

12. Enter the IP address of the main File Server. At this point, the address is validated, and a connection is tested.
13. Enter the SSH port number you specified for the main File Server as the **Gluware File Server Main Administrative Port**.
14. Enter the port number for the remote File Server as the **SSH Port for Appliance Administration**. You cannot use port 22 as that port is used to respond to SCP requests for file transfers.
15. Click **DONE**.

Accept CentOS licensing terms

16. On the **INITIAL SETUP** screen, select **LICENSE INFORMATION**.
17. Check the box to accept the CentOS license agreement and click **DONE**.

Create the local user

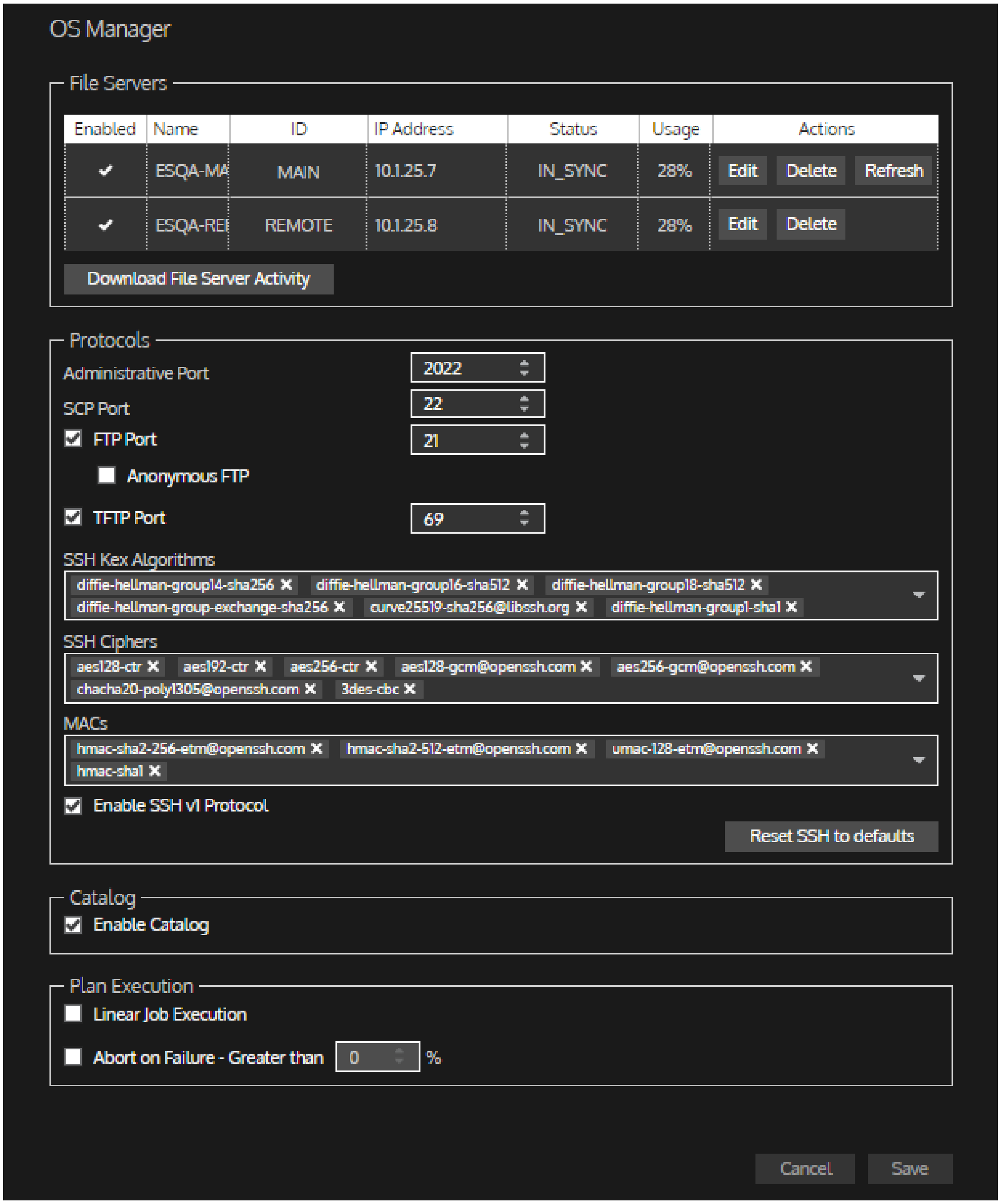
18. On the **INITIAL SETUP** screen, select **USER CREATION**.
19. Enter the CentOS user's first and last name (**Full name**).
20. Provide the **User Name** and **Password** the CentOS user will use to administer the Gluware system. Create a strong password to protect access to Gluware.
21. Confirm the password and click **DONE**.
22. On the **INITIAL SETUP** screen, click **FINISH CONFIGURATION**.
23. Sign off CentOS and sign in again to ensure the appropriate permissions take effect.

When the configuration of the File Server is complete, go to Gluware system settings to add the remote File Server to Gluware.

Verify the File Server settings in Gluware

Once you configure the VM for the remote File Server, it is registered in Gluware system settings.

1. Go to Gluware **Settings** > **Organization** > **OS Manager** and ensure you're in the organization that you added the remote File Server to.



OS Manager

File Servers

Enabled	Name	ID	IP Address	Status	Usage	Actions
✓	ESQA-MA	MAIN	10.1.25.7	IN_SYNC	28%	Edit Delete Refresh
✓	ESQA-RE	REMOTE	10.1.25.8	IN_SYNC	28%	Edit Delete

Download File Server Activity

Protocols

Administrative Port 2022

SCP Port 22

☑ FTP Port 21

□ Anonymous FTP

☑ TFTP Port 69

SSH Kex Algorithms: diffie-hellman-group14-sha256 ✕ diffie-hellman-group16-sha512 ✕ diffie-hellman-group18-sha512 ✕ diffie-hellman-group-exchange-sha256 ✕ curve25519-sha256@libssh.org ✕ diffie-hellman-group1-sha1 ✕

SSH Ciphers: aes128-ctr ✕ aes192-ctr ✕ aes256-ctr ✕ aes128-gcm@openssh.com ✕ aes256-gcm@openssh.com ✕ chacha20-poly1305@openssh.com ✕ 3des-cbc ✕

MACs: hmac-sha2-256-etm@openssh.com ✕ hmac-sha2-512-etm@openssh.com ✕ umac-128-etm@openssh.com ✕ hmac-sha1 ✕

☑ Enable SSH v1 Protocol

Catalog

☑ Enable Catalog

Plan Execution

□ Linear Job Execution

□ Abort on Failure - Greater than 0 %

2. If you are adding the remote File Server in a child organization, check the **Enable New Main File Server for this Organization** box.

Note: The File Server will be used by all child organizations unless they have their own File Server.

3. Ensure the **Enable File Server** box is checked.
4. Verify the name and IP address for the main server.
5. Ensure the **Administrative Port** and **SCP Port** assignments are correct.
6. Optional: Clear the **FTP Port**, **TFTP Port**, or the **Anonymous FTP** box to disable the port. These ports are not required. Ensure the enabled port assignments are correct.
7. Only if necessary: Make changes to the encryption algorithms by removing or adding algorithms in the **SSH Kex Algorithms**, **SSH Ciphers**, and **MACs** boxes.

WARNING! Some encryption algorithms may expose security vulnerabilities but may be required by older devices or firmware.

8. Optional: Clear the **Enable SSH v1 Protocol** box. SSH v2 Protocol is always enabled, regardless of this setting.
9. Save.

Upgrade Gluware

We'll notify you of a system version upgrade or an emergency patch when it becomes available. You'll be instructed how to obtain a copy of the upgrade bundle and be provided with release notes describing the impact and detailed instructions for performing the upgrade.

Before installing the upgrade:

- Check that your system continues to meet the minimum requirements for Gluware operation and use.
- Save any unsaved work and close any open software (this doesn't include any of the Gluware services). The Gluware services can remain running and the upgrade process will manage them collectively.
- **IMPORTANT** Perform a full backup of your system and specific configuration. *See* "Back up Gluware systems" for guidance.

Perform the steps below for each Gluware server that comprises your infrastructure. The best practice is to upgrade your Gluware servers in the order below; however, once the Gluware primary server is upgraded, you can upgrade your other servers concurrently.

1. Gluware Primary Server
2. Disaster Recovery Server
3. Gluware Zone Engines
4. Gluware File Servers

To upgrade:

1. Sign in to the Gluware server you are updating via a terminal session using the system administrator local user account credentials. (This is the CentOS user that the system administrator uses to administrate the Gluware system.)
2. Assess the health of the Gluware environment by issuing the `sudo gluwarectl showEnvironment` command on the **Gluware Primary Server** or the **Disaster Recovery Server**. The status of each

of the servers in your Gluware environment are displayed. If there is an error or warning for any server, investigate and correct the problem before upgrading by issuing the `sudo gluwarectl status` command on the server.

- Download the upgrade package `gluware-control-upgrade-5.2.xxx.tar.gz.enc` and copy it to the Gluware server you are updating. Then issue the `sudo gluwarectl upgradePlatform` <upgrade-bundle-filename> command.
  Example: `sudo gluwarectl upgradePlatform gluware-control-upgrade-5.2.250.tar.gz.enc`
- Download and upgrade in one operation by specifying the upgrade bundle URL: Issue the `sudo gluwarectl upgradePlatform` <upgrade-bundle-URL> [bundle-path] command. By default, the upgrade bundle is placed in `/data/tmp`.
  Example: `sudo gluwarectl upgradePlatform URL/gluware-control-upgrade-5.2.250.tar.gz.enc /myDirectory`

3. Check the upgrade results. If errors are reported or you notice errors during the upgrade, consult the upgrade results log file named `Upgrade_<server type>.<datetime>.log`, where <server type> is one of the following:
   - `Primary` for a Gluware Primary Server
   - `DisasterRecovery` for a Gluware Disaster Recovery Server
   - `ZoneEngines` for a Gluware Zone Engine
   - `MainFileServer` for a main File Server
   - `RemoteFileServer` for remote File Servers
4. In your browser, clear cache and cookies using **Ctrl**+**Shift**+**R**/ ⌘+**Shift**+**R**.

GluAPI integration

GluAPI allows you to write scripts to access Gluware device and organization data. GluAPI adheres to REST architectural principles, has predictable, resource-oriented URLs, and uses HTTP response codes to indicate API errors. Built-in HTTP features, like HTTP authentication and HTTP verbs, are understood by off-the-shelf HTTP clients.

GluAPI supports cross-origin resource sharing, allowing you to interact securely with the API from a client-side web application. JSON is returned by all GluAPI responses, including errors.

GluAPI documentation can be found at
<yourGluwareSystem>/`api-docs`/

or
http://api-control.gluware.com/api-docs/

Examples of GluAPI usage are available on GitHub at
http://github.com/gluware

Access to GluAPI functionality depends on your role and permissions.

Gluware Ansible Integration

To install **Gluware Ansible Integration** and modules on the system that is running Ansible, run the command line

```
pip install gluware-ansible-inventory
```

To update GluAPI to a newer version, run the command line

```
pip install -I gluware-ansible-inventory
```

To see the documentation for each module, run the command line

```
ansible-doc -t module {{ module_name }}
```

Note: Ansible does not run directly on Windows: it needs to run on a UNIX file system such as Linux or Mac. For Windows, it will run under Cygwin. Trying to use `pip install` only works in an environment Ansible can run on.

2020 L Street, Suite 130
Sacramento, CA 95811

www.gluware.com