gluware®

Gluware® Installation Guide

Version 4.2
March 3, 2022

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

Table of Contents

About Gluware 4.2

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 **Workflows**.
- Model and manage configurations for devices with **Config Modeling**.
- 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**.
- Monitor unauthorized changes, ensure connectivity, and enable rollback with **gluWatchdog**, an optional agent for Cisco IOS/IOSXE routers and switches.

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 Modeling**
- **Workflows**
- **Network RPA** – For future use
- **Topology** – For future use

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://youtube.com/playlist?list=PL2EJzW0a2Z_OfbnhP9pS-F1wME_55EbNO

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 4.2.6.

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

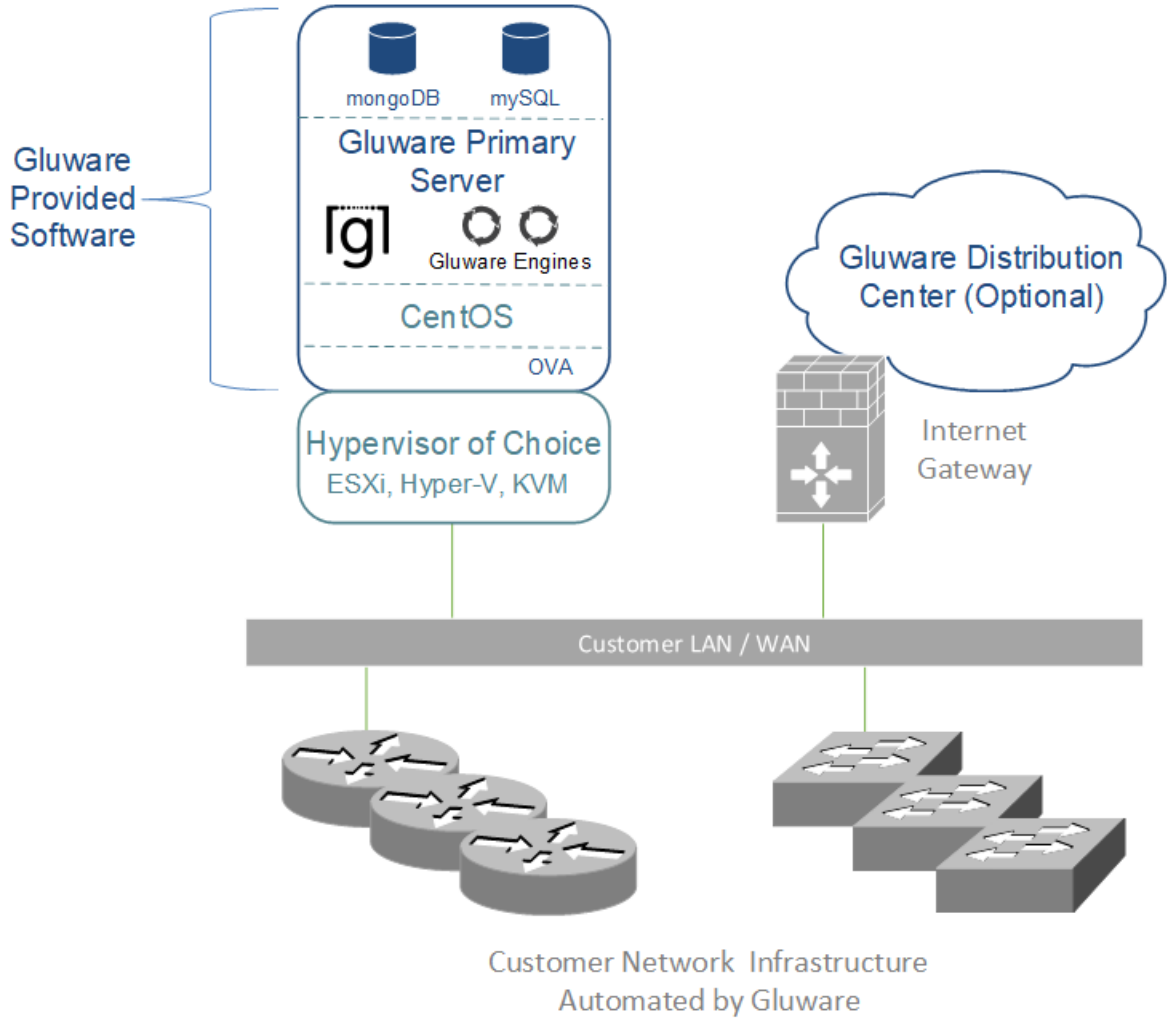
Before you begin to install Gluware, determine if you will use a Gluware Disaster Recovery Server and any Gluware Zone Engines. Once you determine your optimal Gluware configuration, ensure you have adequate platform resources.

Here are the steps involved:

Step 1. Determine your configuration and resources required

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	64 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

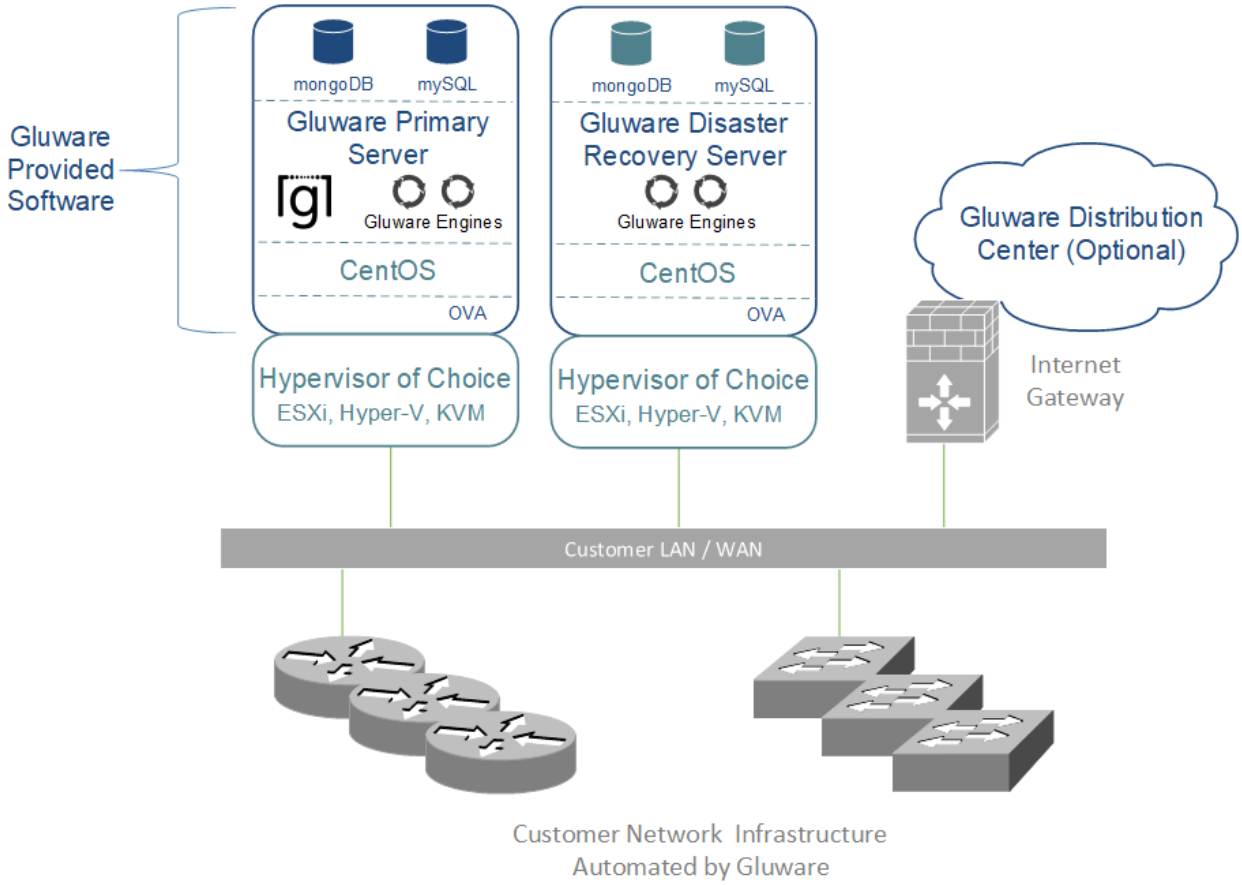
Website	URL
Gluware Distribution Center	https://glulab.gluware.com/
Cisco API Console*	https://cloudsso.cisco.com/as/token.oauth2 (to authenticate) https://api.cisco.com/ (for data retrieval)
NIST NVD*	https://services.nvd.nist.gov/

*If integration enabled.

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

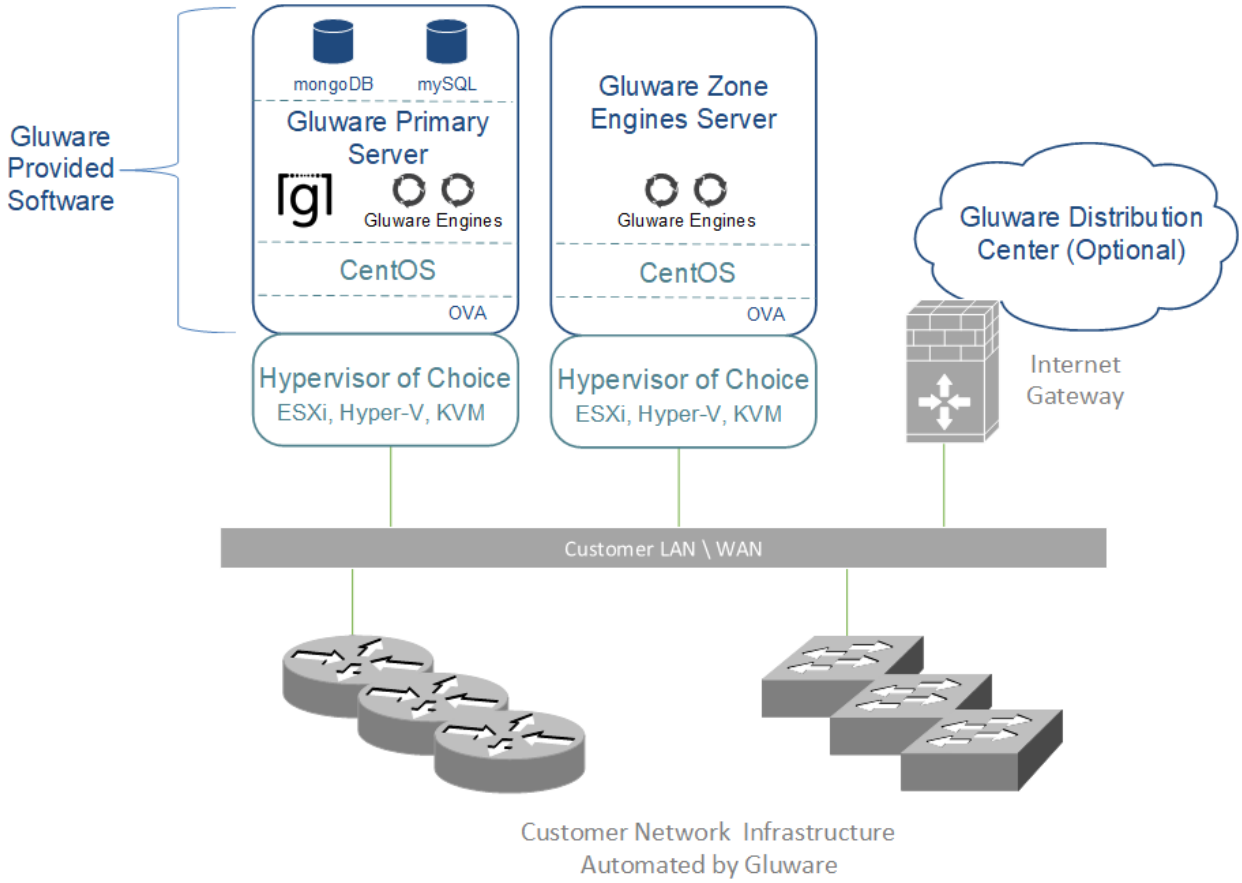
*Default, user-configurable

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	64 GB*	At least 64 GB*
Memory	4 GB	8 GB
CPUs/vCPUs	2 CPUs, 2.4 GHz	2 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

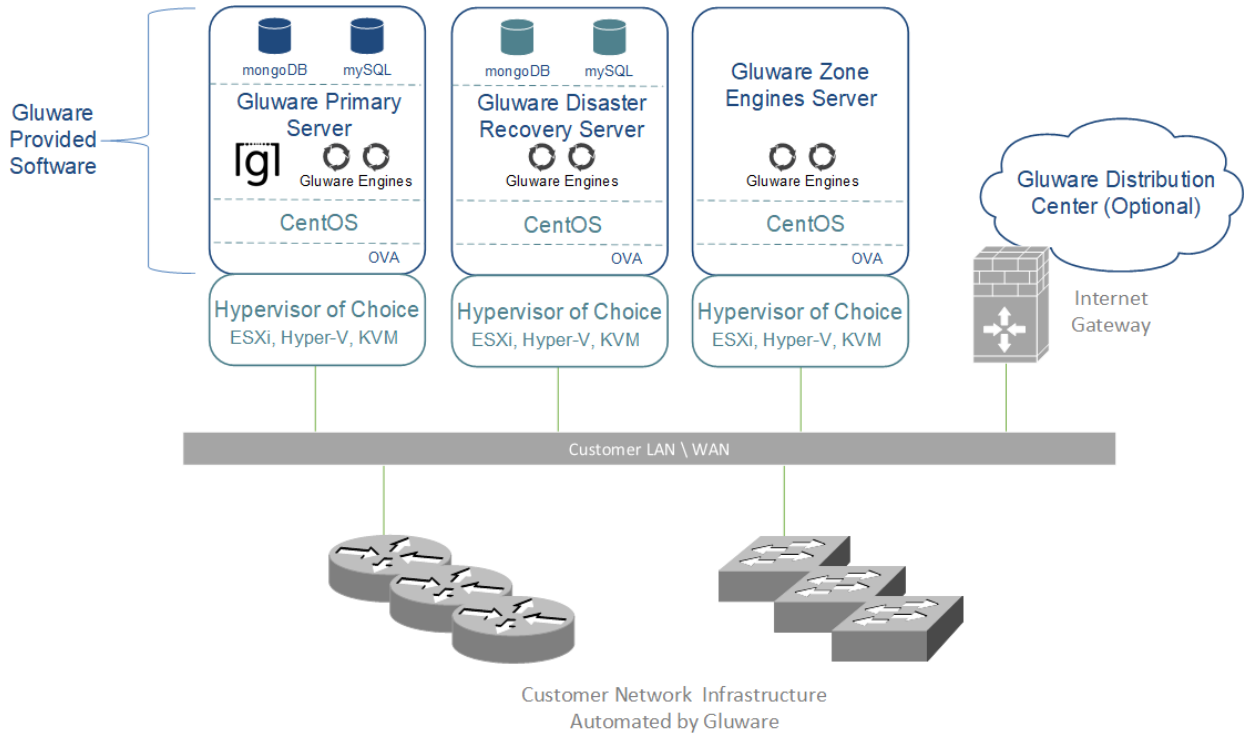
Device	Protocol	Port
Network device	SSH or Telnet	TCP 22 or TCP 23*
Gluware Primary Server	RabbitMQ, MongoDB, and HTTPS, ESP	TCP 5672, UDP 5672, TCP 27017, TCP 8042
Gluware Disaster Recovery Server	RabbitMQ, MongoDB, and HTTPS, ESP	TCP 5672, UDP 5672, TCP 27017, TCP 8042
Customer NTP server	NTP	UDP 123

*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:

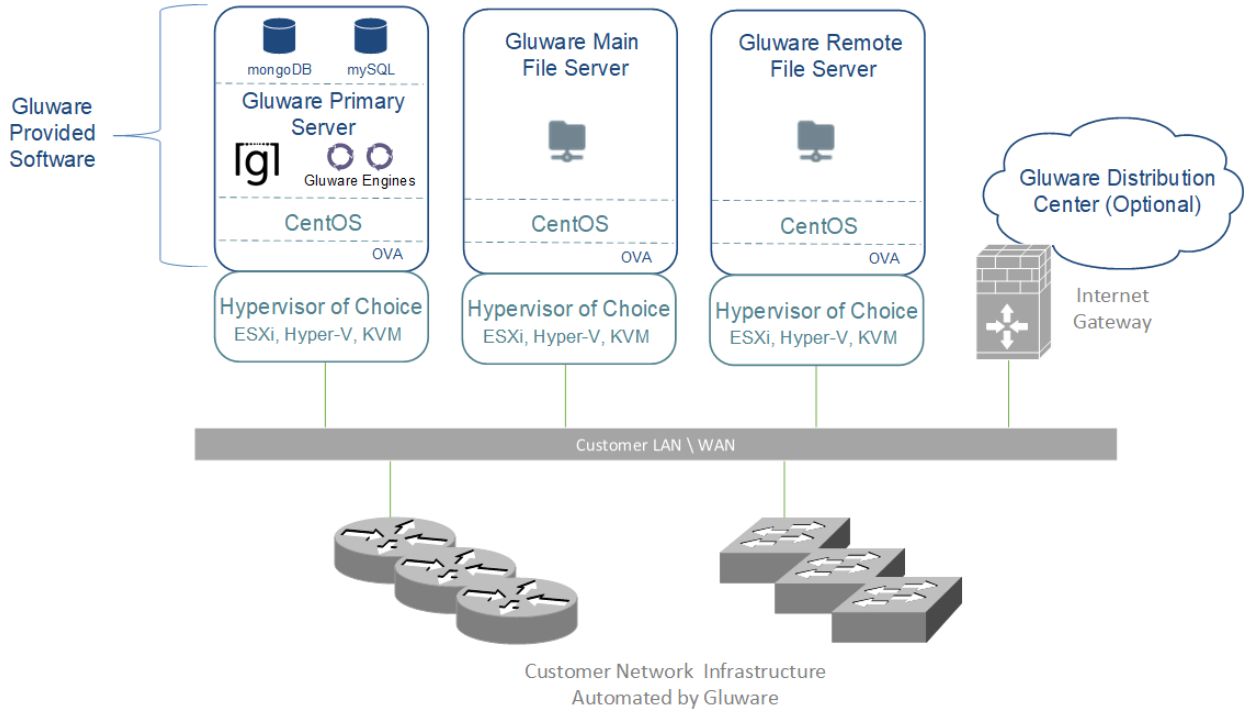
- Gluware Primary Server
- Gluware Disaster Recovery Server
- 1–*n* Gluware Zone Engines



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	2 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 64 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

Gluware® Installation Guide for Microsoft® Azure®

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

Step 11. 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

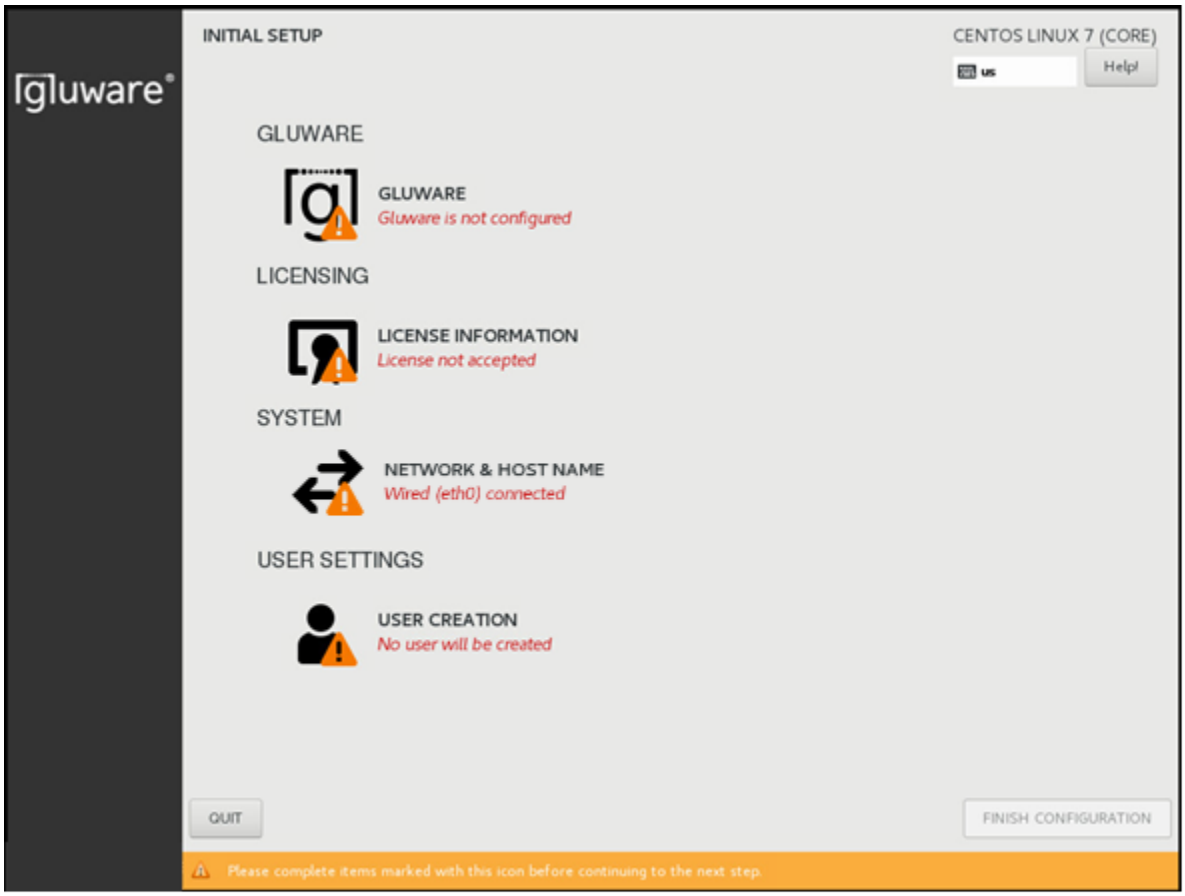
Configure Gluware Zone Engines

Configure a main File Server

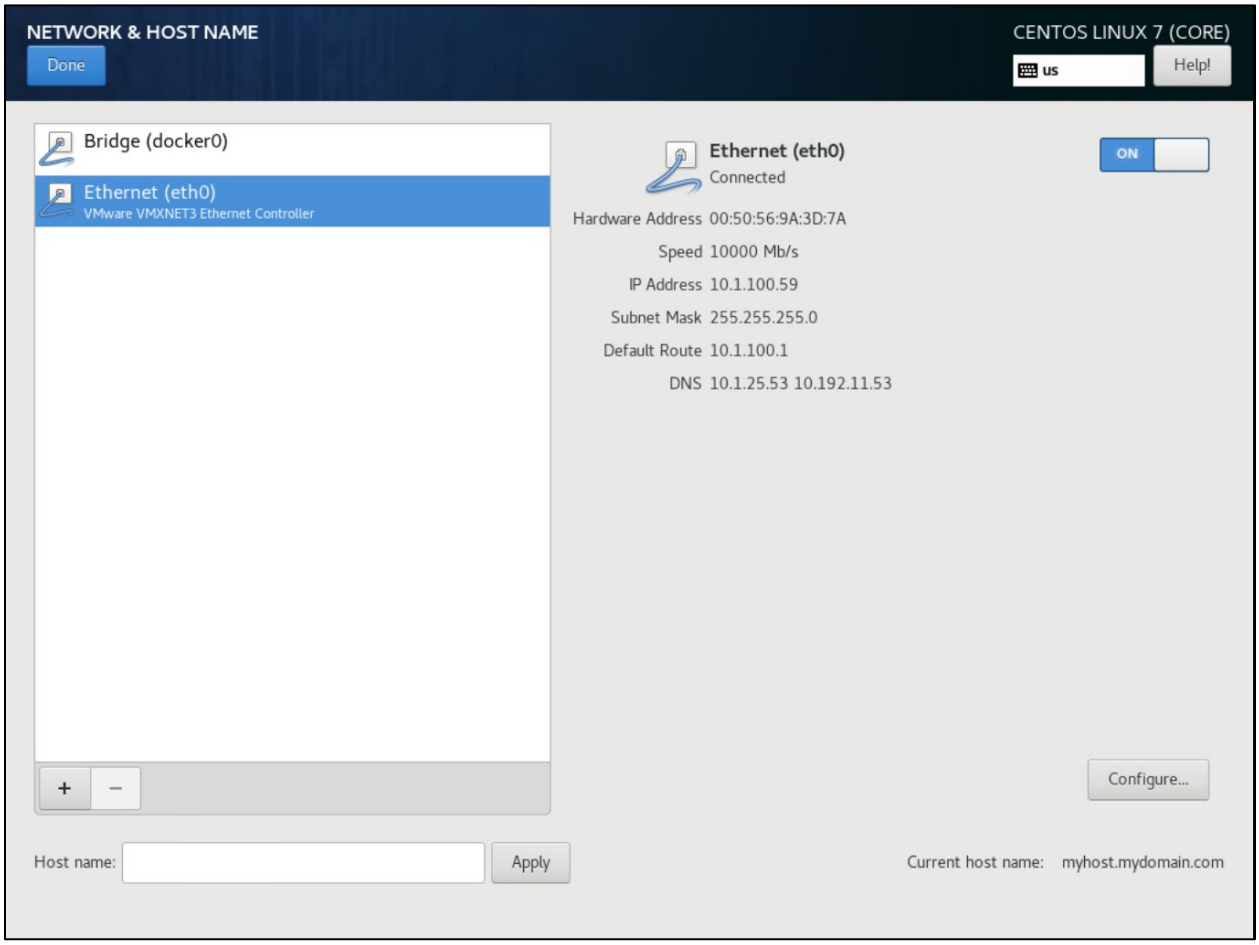
Configure a remote File Server

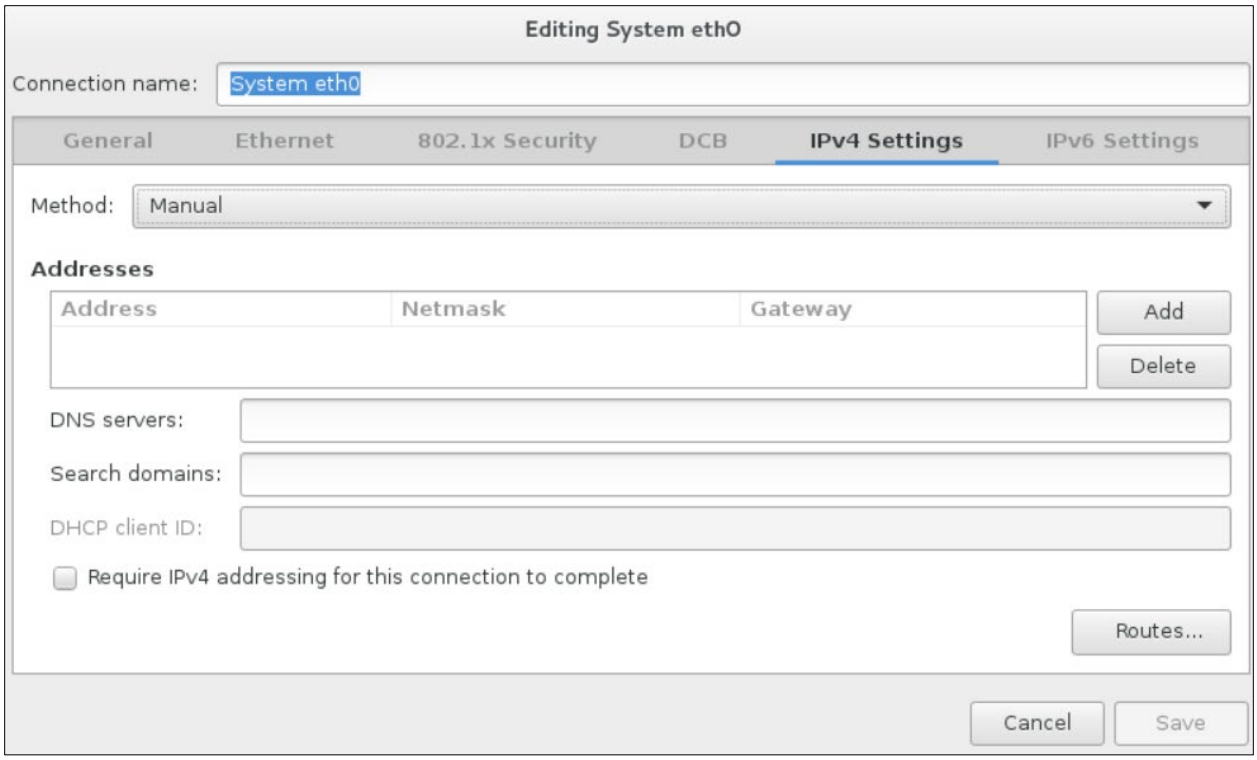
Step 1. Configure network settings

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



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.

   NOTE: A static IP address is recommended. Use of DHCP is not recommended.

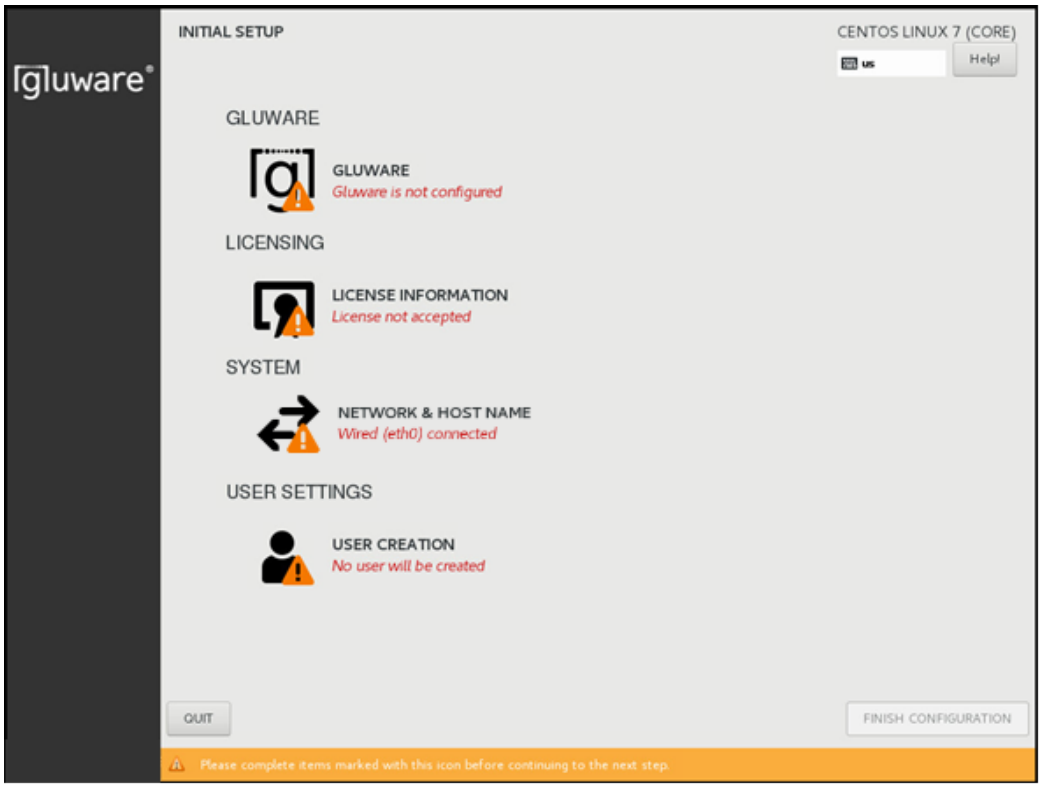
9. Click **Save** to store your network configuration and then click **DONE** to complete your network definition.

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.

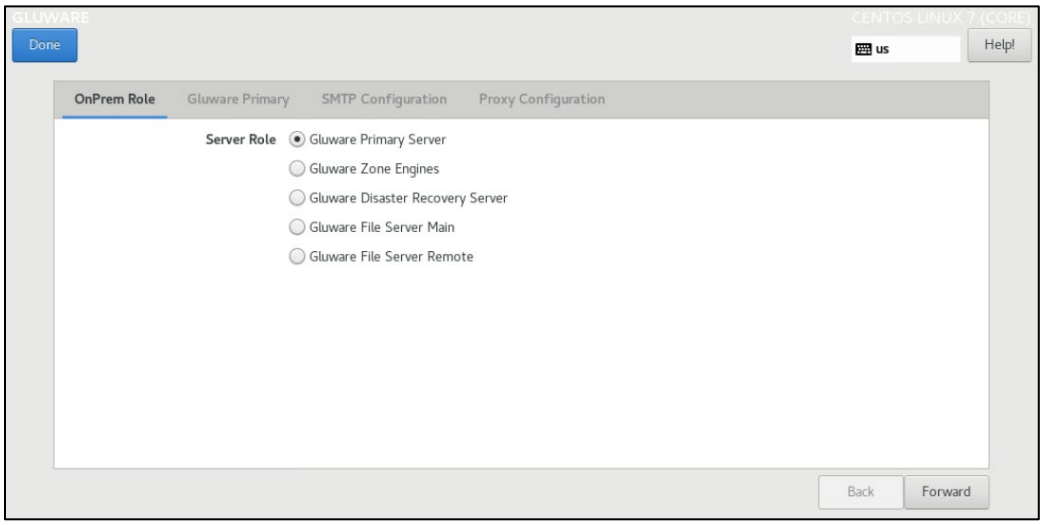
Next step: Configure the Gluware Primary Server

Step 2. Configure the Gluware Primary Server

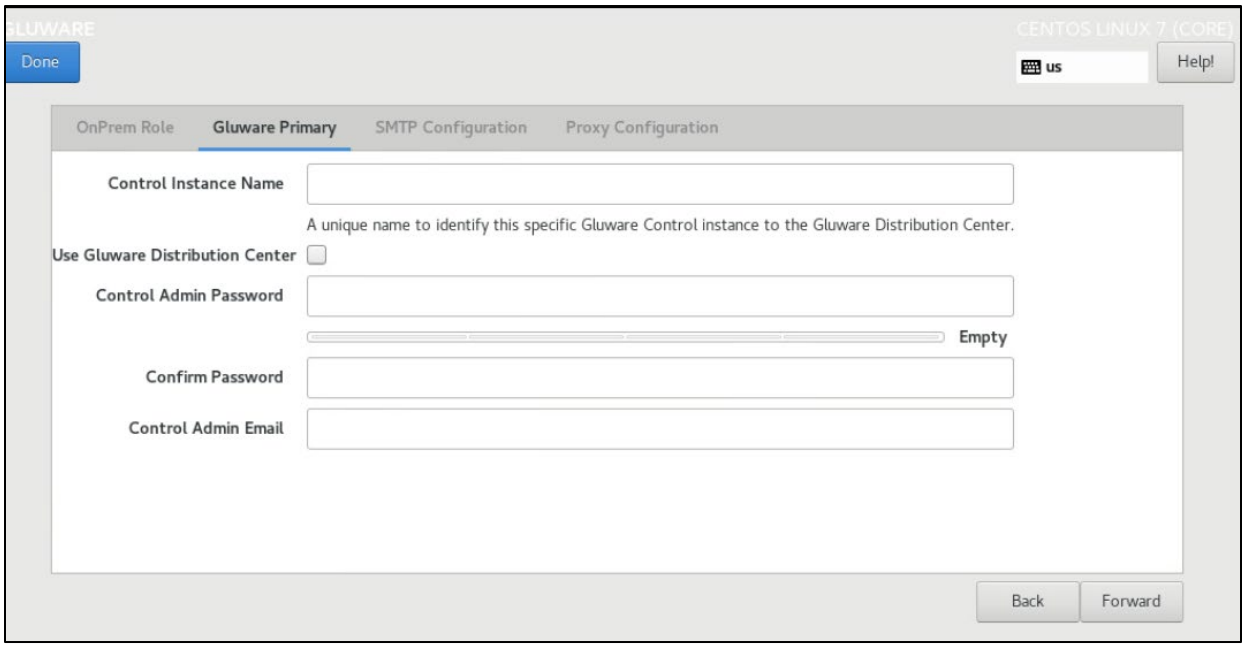
1. On the **INITIAL SETUP** screen, select **GLUWARE**.



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



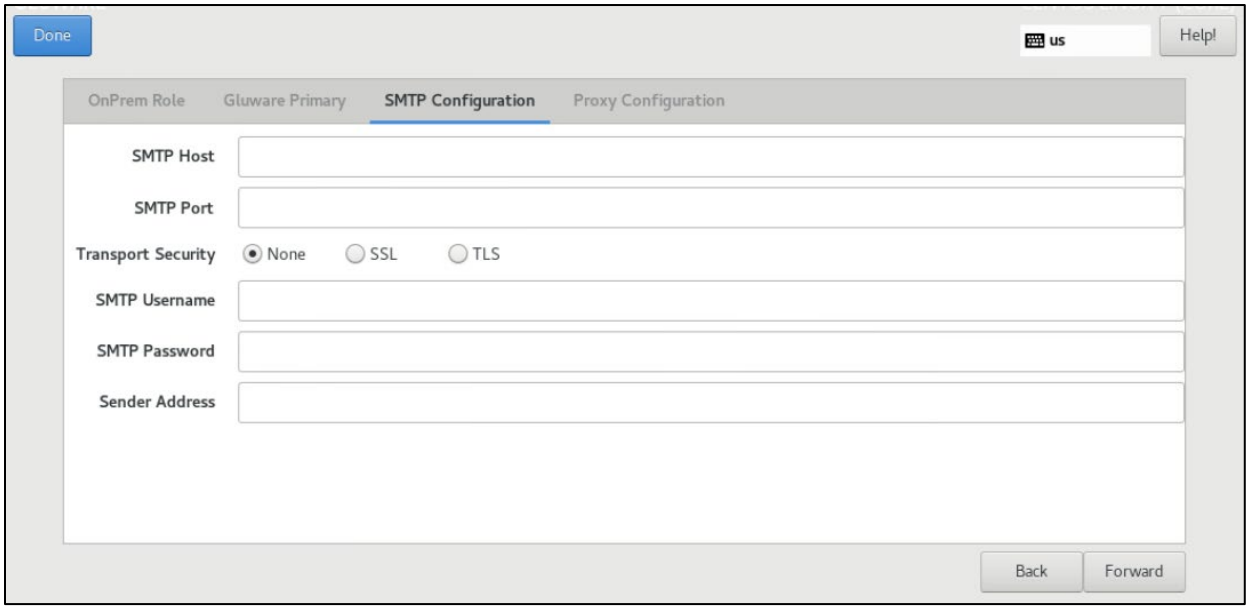
3. On the **Gluware Primary** tab, define the Gluware system name and the primary admin password and then click **Forward**.



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)
Use Gluware Distribution Center	Select this option if you will be using the Gluware Distribution Center for Feature updates (recommended)
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

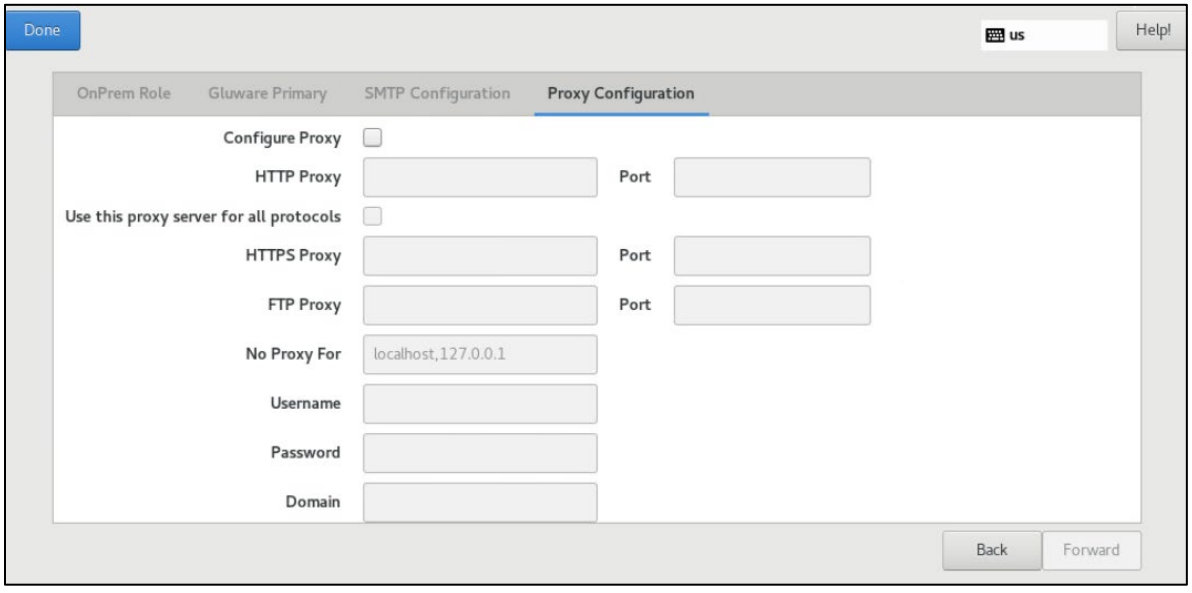
4. On the SMTP tab, specify the SMTP configuration details.

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.



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.



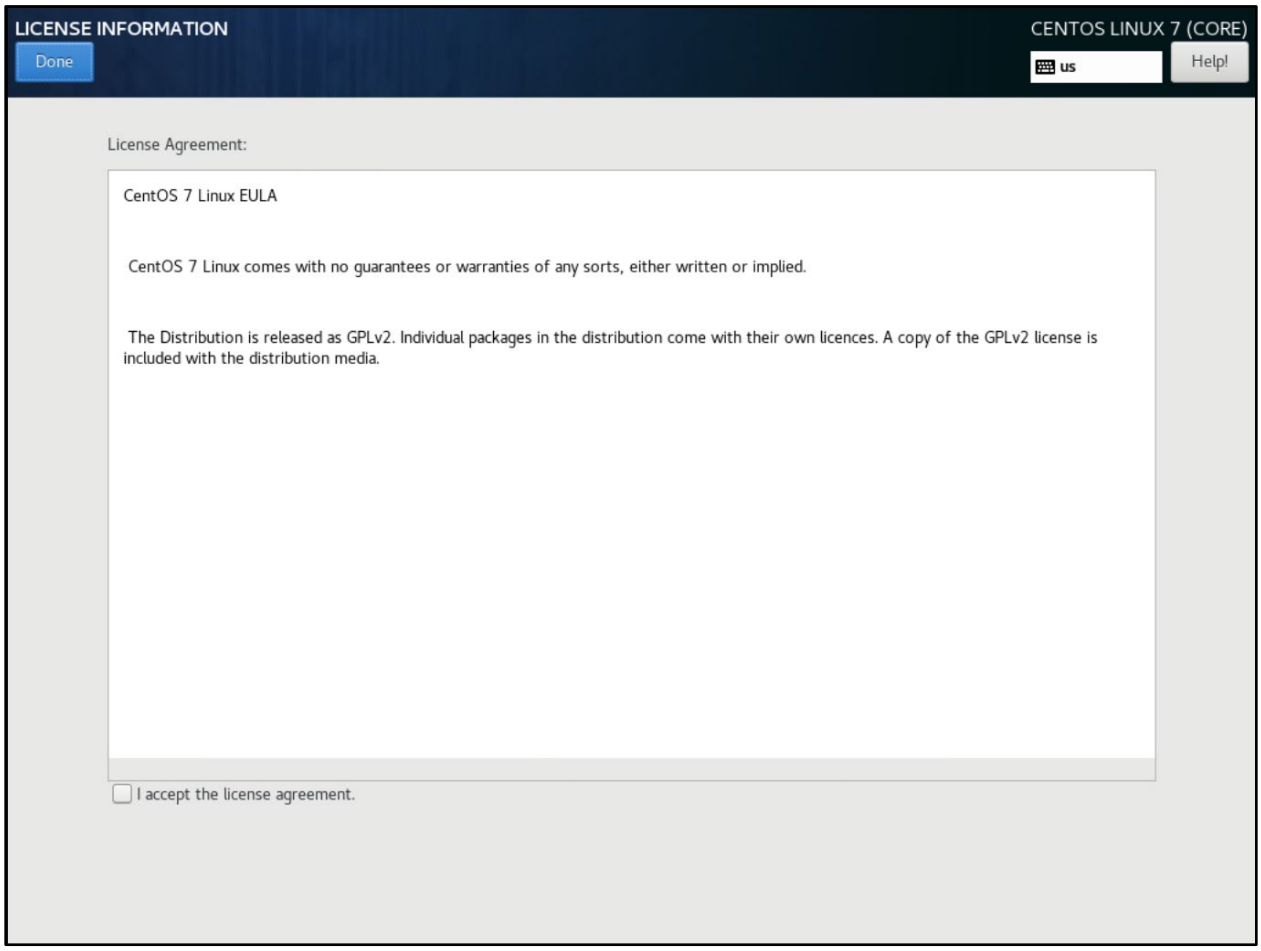
Property	Description
HTTP Proxy and Port	Host name or IP address for the HTTP proxy server. Port number for the HTTP proxy server
Use this proxy for all protocols	Check the box to use the HTTP proxy for all protocols
HTTPS Proxy and Port	Host name or IP address for the HTTPS proxy server. Port number for the HTTPS proxy server
FTP Proxy and Port	N/A
No Proxy For	N/A
Username	User account used to authenticate with the proxy server, if needed
Password	Password for the proxy server username account, if needed
Domain	The Active Directory domain associated with the username and password, 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**.

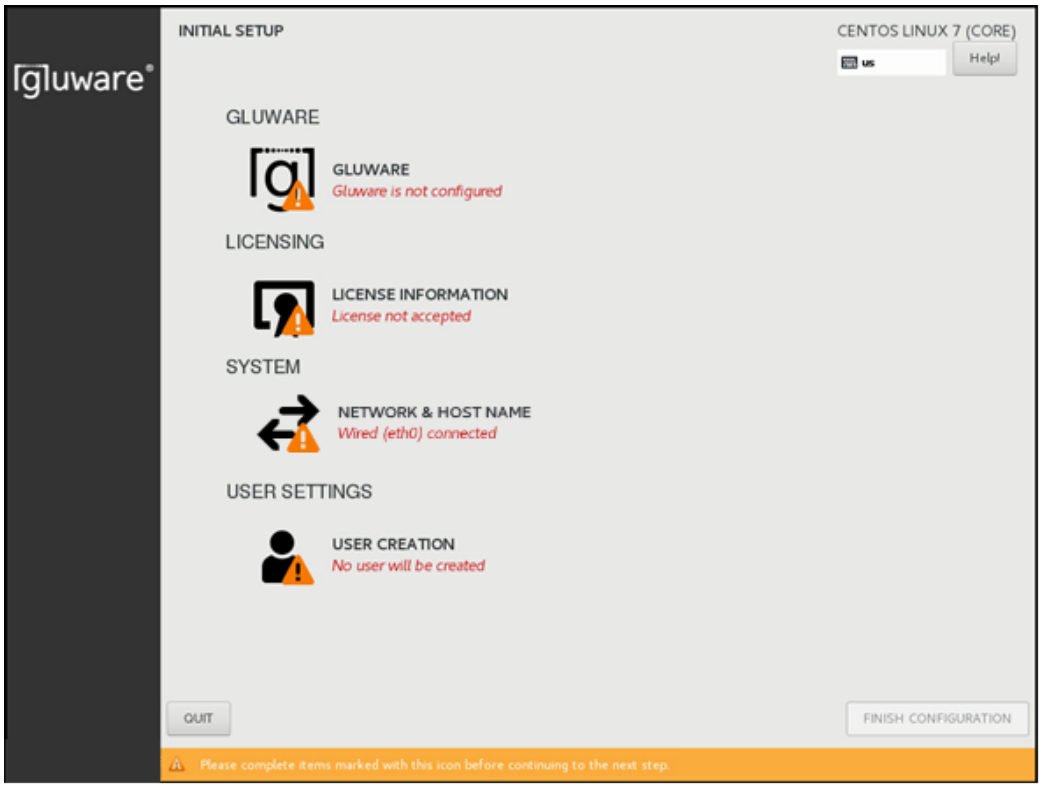


Next step: Create the local user

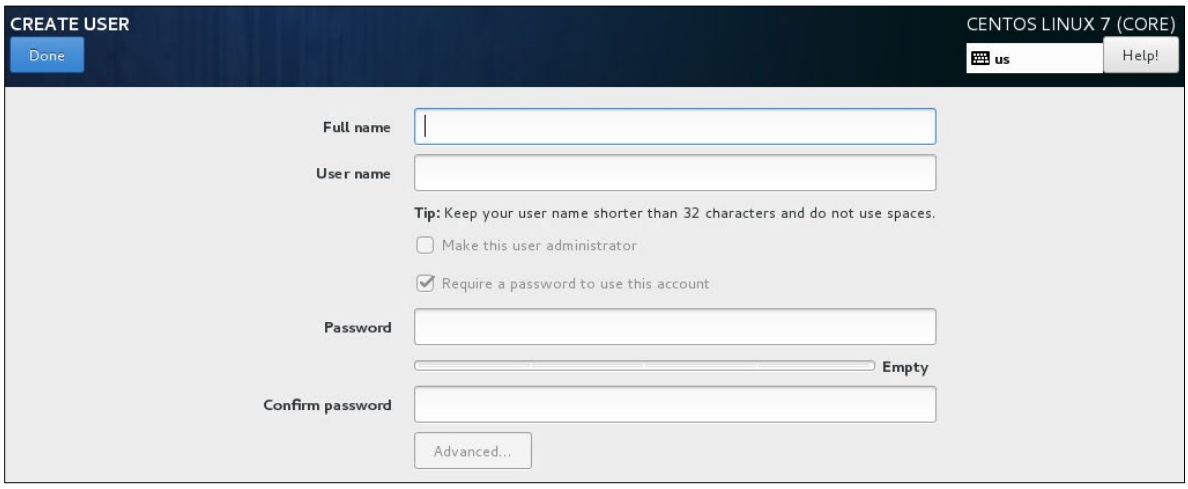
Step 4. Create the local user

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**.



2. Enter the CentOS user's first and last name (**Full name**).



3. 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.
4. Confirm the password and click **DONE**.
5. 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 step: Set up organizations and user authentication

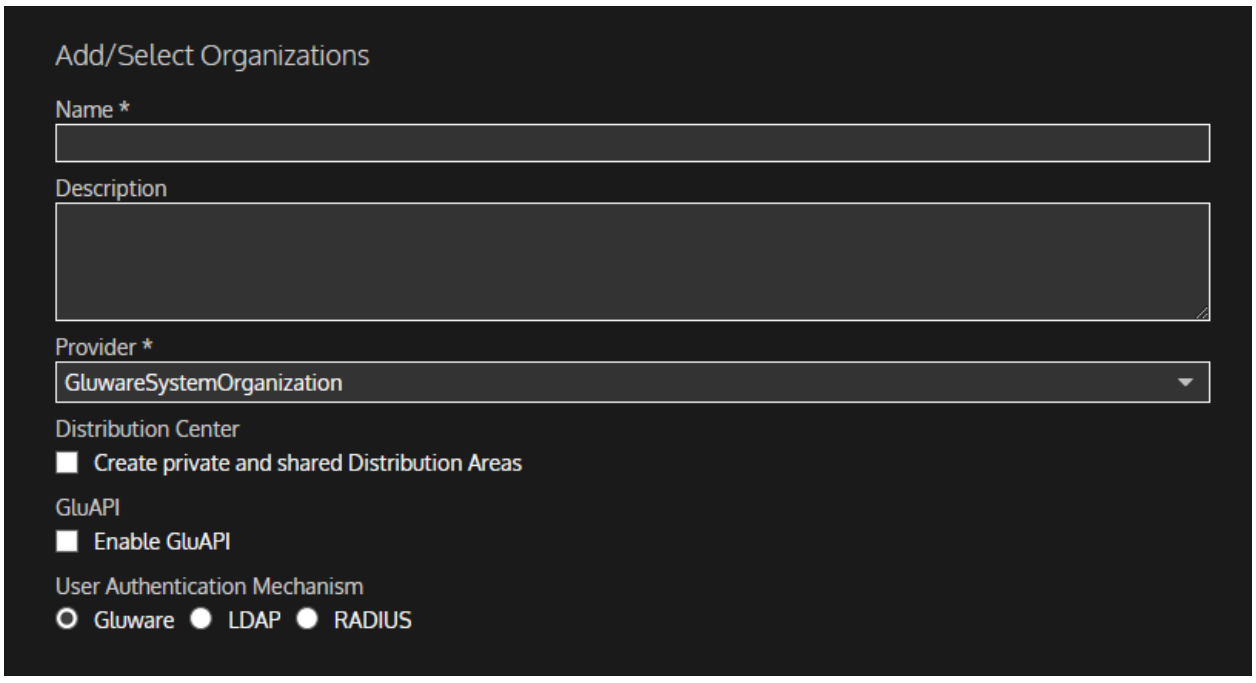
Step 6. Set up organizations and user authentication

Gluware system settings allows you to add organizational structure to your Gluware system with parent/child relationships.

NOTES: You can rename the default organization (GluwareSystemOrganization) instead of adding an organization.

A best practice is to create users in your parent organization and add devices to a child organization.

1. Sign in to Gluware using the username "admin" and the Gluware administration password you created in Step 2.
2. Go to **Settings**.
3. Select **Organization** > **Organizations**.
4. Click **Add Organization+** to create a new organization.



5. Enter a name for the organization and a description.
6. Select the parent organization from the **Provider** drop-down list.

NOTE: Only check the **Create private and shared Distribution Areas** box if Gluware asks you to.

7. Optional: Check the **Enable GluAPI** box to enable integration.
8. Select a user authentication mechanism:
    - Select **Gluware** to set up users one-by-one or if you are using single sign-on. *See* "Add Gluware users" or "Configure single sign-on authentication" for details.
    - Select **LDAP** or **RADIUS** to use your existing user credentials. *See* "Configure Gluware to interact with LDAP" or "Configure Gluware to interact with RADIUS" for details.
9. Click **Create**.
10. Click **Yes** to add the base level Gluware Solution packages to your organization. Click **No** if you want to create the organization with no packages installed, for example for testing a Beta package.
11. Click **OK**.

Configure Gluware to interact with LDAP

If your network implements LDAP, configure Gluware to interact with your LDAP implementation. Gluware lets you access your LDAP servers from Gluware systems and leverage your existing LDAP implementations to organize and manage user access and privileges within Gluware.

LDAP users will be mapped to Gluware users during the Gluware user authentication process. This means that a corresponding user in Gluware is not created until the user successfully signs in to Gluware for the first time. This also means that if your company is already LDAP-enabled, once you have established a business relationship with Gluware, you can create your Gluware user accounts on an as-needed basis.

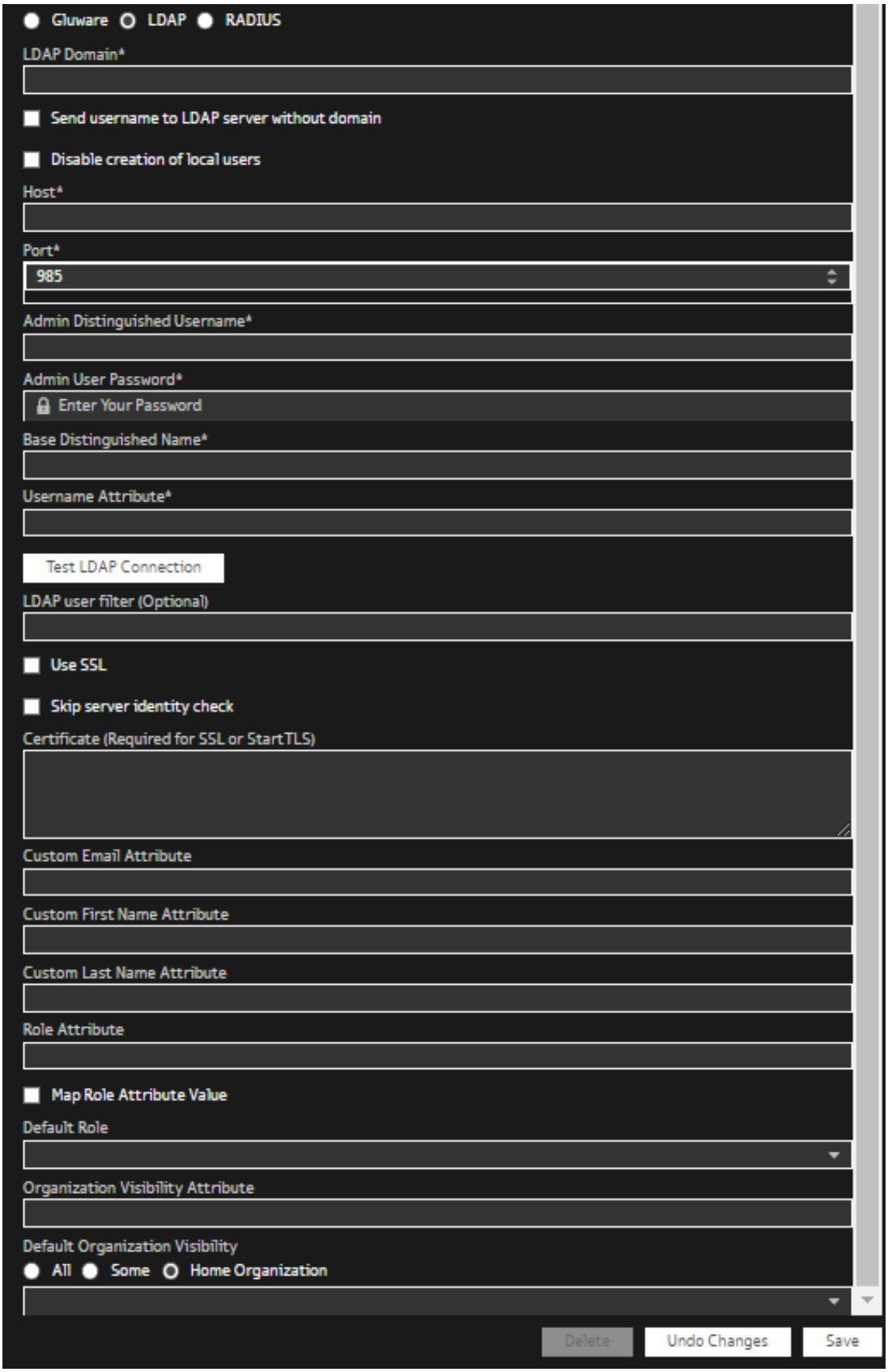
The user authentication process in Gluware determines if, and how, to map an LDAP user with a Gluware user for the following scenarios:

- If the user already exists in the Gluware database, and the user is not flagged as coming from LDAP, Gluware will authenticate the entered password against the password stored in Gluware.
- If the user already exists in the Gluware database, and the user is flagged as coming from LDAP, Gluware will establish a connection with the LDAP server for the user's Gluware organization. It will then search for the user on the LDAP server, and
- If the user exists in LDAP, the user will be authenticated by attempting to bind to the user entry in LDAP using the supplied password. If this succeeds, then Gluware checks the user LDAP entry for any updates to mapped attributes and updates the user in Gluware appropriately.
- If the user no longer exists in LDAP, then Gluware flags the user as deactivated.
- If the user does not exist in the Gluware database, and the user name includes the domain name (for example, user@domain.org), and a Gluware organization is found with a matching domain name,

Gluware will connect to the LDAP server for the org and search for the user. If the user exists in LDAP, it will bind to the user using the supplied password. If the bind succeeds, then Gluware will create a user with the appropriate LDAP attributes.

The @domain.org portion of the user name entered by the user will always be included in the user name in the Gluware system, even if it is stripped off for LDAP authentication. If an LDAP entry for a user does not have an email address to map to the Gluware user, then the user name (along with the @domain.org) will be used as the user's email address in Gluware.

If an LDAP configuration is removed for an organization and a user flagged as coming from LDAP tries to sign in to Gluware, then the user will be updated as deactivated. If a user that came from LDAP is marked as deactivated in Gluware and later that user attempts to sign in and is successfully authenticated with LDAP, then the user will be reactivated.


Gluware
LDAP
RADIUS
LDAP Domain*
Send username to LDAP server without domain
Disable creation of local users
Host*
Port*
985
Admin Distinguished Username*
Admin User Password*
Enter Your Password
Base Distinguished Name*
Username Attribute*
Test LDAP Connection
LDAP user filter (Optional)
Use SSL
Skip server identity check
Certificate (Required for SSL or StartTLS)
Custom Email Attribute
Custom First Name Attribute
Custom Last Name Attribute
Role Attribute
Map Role Attribute Value
Default Role
Organization Visibility Attribute
Default Organization Visibility
All
Some
Home Organization
Delete
Undo Changes
Save

Field	Description
LDAP Domain	The unique domain name all users of the organization include in their username when signing in to Gluware. For example, the user jandy@gluware.com has an LDAP Domain of gluware.com To require a domain name on sign in, enter the domain name. **Note:** Do not include the @ sign. E.g., enter gluware.com. The user signs in with jandy@gluware.com To require only the user without the domain name on sign in, enter an asterisk (*). E.g., enter *. The user signs in with jandy
Send username to LDAP server without domain	Strips the domain name (@yourcompany.com) off the username. Users still sign in to Gluware using user@yourcompany.com
Disable creation of local users	Limits new users to only those in LDAP. Any existing users remain
Host	Host name or IP address of the LDAP server. If you are using LDAPS, this name must match the server certificate
Port	Port of the LDAP server: 389 or 636 (SSL)
Admin Distinguished Username	Username used to search for user entries; for example, CN=gluServiceAccount,CN=Users,DC=contoso,DC=local
Admin User Password	Password used to bind to the Admin Distinguished Username

Field	Description
Base Distinguished Name	Location where the server will look for user accounts; for example, CN=Users,DC=contoso,DC=local
Username Attribute	LDAP attribute name where the user name is stored in a user entry. Additional entries can be used if proxies are needed to access a device
Test LDAP Connection	Allows you to test the LDAP configuration and connection for an org before saving it
LDAP user filter (Optional)	An optional LDAP filter applied to the search when searching for a user entry to bind to; for example, (&(objectCategory=person)(memberOf=CN=securityGroup,CN=Users,DC=contoso,DC=local)) Need help with LDAP filters?
Use SSL	Select if you are using LDAPS
Skip server identity check	When selected, accepts any certificate offered to Gluware. If not selected, the certificate on the LDAP server must match the certificate in the Certificate field (below)
Certificate (Required for SSL or Start TLS)	The certificate for the LDAP server. If the connection to the LDAP server is encrypted using TLS, then this is a string in PEM format of the TLS certificate
Custom Email Attribute	The LDAP attribute that contains the user's email address, for example, mail. If you don't specify an email address, Gluware will use the username and domain name since this is a required field. **Note**: If you supply a value for Custom Email Attribute, the field will NOT be editable, and you cannot override the value pulled from LDAP

Field	Description
Custom First Name Attribute	The LDAP attribute that contains the user's first name. **Note**: If you supply a value for Custom First Name Attribute, the field will NOT be editable, and you cannot override the value pulled from LDAP
Custom Last Name Attribute	The LDAP attribute that contains the user's last name. **Note**: If you supply a value for Custom Last Name Attribute, the field will NOT be editable, and you cannot override the value pulled from LDAP
Role Attribute	Optional LDAP attribute used to set the role; for example, memberOf. If Role Attribute is assigned, the role cannot be modified in Gluware **Settings** > **Users** > **Manage Users**
Map Role Attribute Value	When selected, allows you to create up to five LDAP security groups and map each group to a role
Default Role	If the role is not specified, or the LDAP user entry does not include the Role Attribute, then this will be the default role given to a new Gluware user and the role can be modified in Gluware **Settings** > **Users** > **Manage Users**
Organization Visibility Attribute	An optional LDAP attribute, including vendor-specific attributes, that contains a string of "ALL," a comma-separated string of organization names, or the "HOME" organization; for example, you can use the "info" attribute and enter Org1,Org2, Org3 in the Users Notes field on the Telephones tab in Active Directory

Field	Description
Default Organization Visibility	If the Organization Visibility Attribute is not specified, or the LDAP user entry does not include the Organization Visibility Attribute, then this is the Organization Visibility given to a new Gluware user. **All** – The organization the user is created in and any child organizations **Some** – Select one or more organizations from the drop-down list **Home** – Only the organization the user is created in

Next step: Install your Gluware licenses

Configure Gluware to interact with RADIUS

If your network implements RADIUS, configure Gluware to interact with your RADIUS implementation. Gluware lets you access your RADIUS servers from Gluware systems and leverage your existing RADIUS implementations to organize and manage user access and privileges within Gluware.

RADIUS users will be mapped to Gluware users during the Gluware user authentication process. This means that a corresponding user in Gluware is not created until the user successfully signs in to Gluware for the first time. This also means that if your company is already RADIUS-enabled, once you have established a business relationship with Gluware, you can create your Gluware user accounts on an as-needed basis.

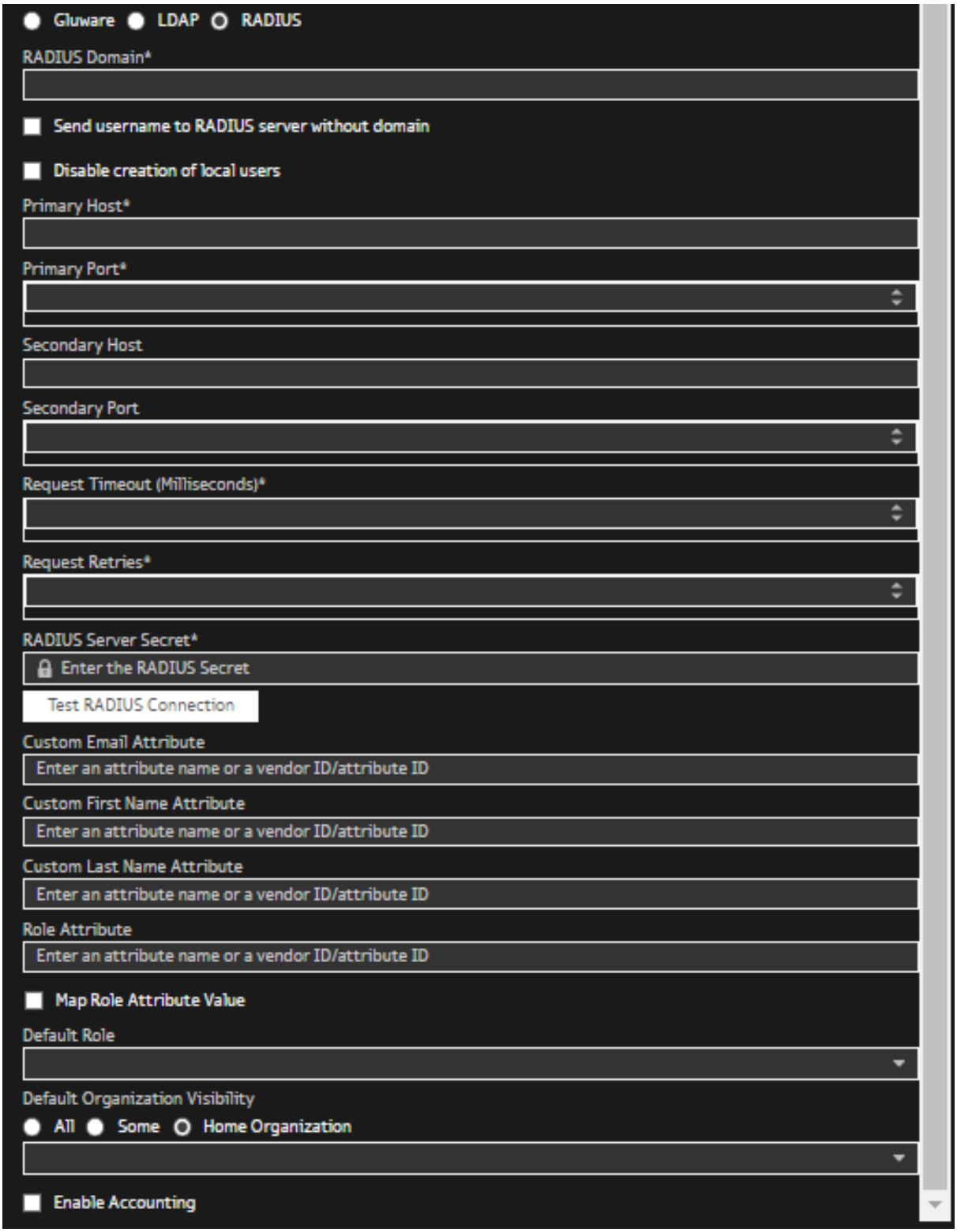
The user authentication process in Gluware determines if, and how, to map a RADIUS user with a Gluware user for the following scenarios:

- If the user already exists in the Gluware database, and the user is not flagged as coming from RADIUS, Gluware will authenticate the entered password against the password stored in Gluware.
- If the user already exists in the Gluware database, and the user is flagged as coming from RADIUS, Gluware will establish a connection with the RADIUS server for the user's Gluware organization. It will then search for the user on the RADIUS server, and
- If the user exists in RADIUS, the user will be authenticated by attempting to bind to the user entry in RADIUS using the supplied password. If this succeeds, then Gluware checks the user RADIUS entry for any updates to mapped attributes and updates the user in Gluware appropriately.
- If the user no longer exists in RADIUS, then Gluware flags the user as deactivated.

- If the user does not exist in the Gluware database, and the user name includes the domain name (for example, user@domain.org), and a Gluware organization is found with a matching domain name, Gluware will connect to the RADIUS server for the org and search for the user. If the user exists in RADIUS, it will bind to the user using the supplied password. If the bind succeeds, then Gluware will create a user with the appropriate RADIUS attributes.

The @domain.org portion of the user name entered by the user will always be included in the user name in the Gluware system, even if it is stripped off for RADIUS authentication. If a RADIUS entry for a user does not have an email address to map to the Gluware user, then the user name (along with the @domain.org) will be used as the user's email address in Gluware.

If a RADIUS configuration is removed for an organization and a user is flagged as coming from RADIUS tries to sign in to Gluware, then the user will be updated as deactivated. If a user that came from RADIUS is marked as deactivated in Gluware and later that user attempts to sign in and is successfully authenticated with RADIUS, then the user will be reactivated.


Gluware
LDAP
RADIUS
RADIUS Domain*
Send username to RADIUS server without domain
Disable creation of local users
Primary Host*
Primary Port*
Secondary Host
Secondary Port
Request Timeout (Milliseconds)*
Request Retries*
RADIUS Server Secret*
Enter the RADIUS Secret
Test RADIUS Connection
Custom Email Attribute
Enter an attribute name or a vendor ID/attribute ID
Custom First Name Attribute
Enter an attribute name or a vendor ID/attribute ID
Custom Last Name Attribute
Enter an attribute name or a vendor ID/attribute ID
Role Attribute
Enter an attribute name or a vendor ID/attribute ID
Map Role Attribute Value
Default Role
Default Organization Visibility
All
Some
Home Organization
Enable Accounting

Field	Description
RADIUS Domain	The unique domain name all users of the organization include in their username when signing in to Gluware. For example, the user jandy@gluware.com has an RADIUS Domain of gluware.com To require a domain name on sign in, enter the domain name. **Note:** Do not include the @ sign. E.g., enter gluware.com. The user signs in with jandy@gluware.com To require only the user without the domain name on sign in, enter an asterisk (*). E.g., enter *. The user signs in with jandy
Send username to RADIUS server without domain	Strips the domain name (@yourcompany.com) off the username. Users still sign in to Gluware using user@yourcompany.com
Disable creation of local users	Limits new users to only those in RADIUS. Any existing users remain
Primary Host	Host name or IP address of the RADIUS server
Primary Port	Port of the RADIUS server
Secondary Host	Host name or IP address of the secondary RADIUS server
Secondary Port	Port of the secondary RADIUS server
Request Timeout (Milliseconds)	Time allowed for the request to the RADIUS server to respond
Request Retries	Number of times a connection to the RADIUS server will be attempted

Field	Description
RADIUS Server Secret	Shared secret of the RADIUS server for the Gluware RADIUS client
Test RADIUS Connection	Allows you to test the RADIUS configuration and connection for an Org before saving it
Custom Email Attribute	Username used to search for user entries. **Note**: If you supply a value for Custom Email Attribute, the field will NOT be editable, and you cannot override the value pulled from RADIUS
Custom First Name Attribute	The RADIUS attribute that contains the user's first name. **Note**: If you supply a value for Custom First Name Attribute, the field will NOT be editable, and you cannot override the value pulled from RADIUS
Custom Last Name Attribute	The RADIUS attribute that contains the user's last name. **Note**: If you supply a value for Custom Last Name Attribute, the field will NOT be editable, and you cannot override the value pulled from RADIUS
Role Attribute	A RADIUS attribute, including vendor-specific attributes, that contains the role for the user. If Role Attribute is assigned, the role cannot be modified in Gluware **Settings** > **Users** > **Manage Users**
Map Role Attribute Value	When selected, allows you to create up to five RADIUS security groups and map each group to a role

Default Role	If the role is not specified, or the RADIUS user entry does not include the Role Attribute, then this will be the default role given to a new Gluware user and the role can be modified in Gluware **Settings** > **Users** > **Manage Users**
Default Organization Visibility	This is the Organization Visibility given to a new Gluware user. **All** – The organization the user is created in and any child organizations **Some** – Select one or more organizations from the drop-down list **Home** – Only the organization the user is created in
Enable Accounting	Enables record keeping of sign in/sign off activity

Next step: Install your Gluware licenses

Configure single sign-on authentication

Gluware supports SAML (Security Assertion Markup Language) and OAuth (Open Authorization) authentication.

Your identity provider can usually provide an XML or JSON metadata document that contains the information you need for configuring SSO.

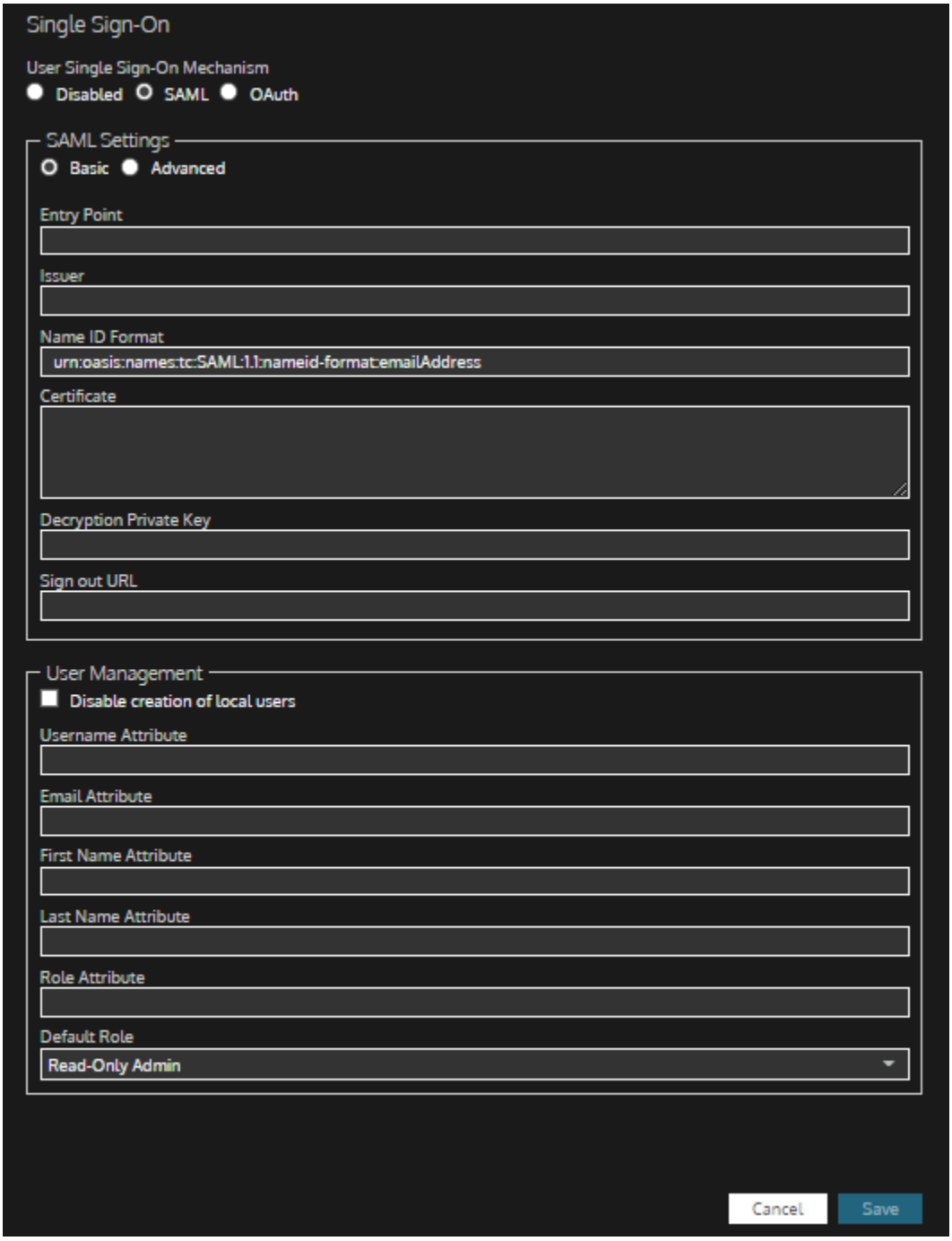
> **NOTES:** In Gluware 4.1, single sign-on is implemented at the global level and will apply to all your organizations. If you are updating Gluware and have organizations configured to use LDAP or RADIUS authentication, disable those by selecting **Gluware** authentication in ⚙**Settings** > **Organization** > **Organizations**.
>
> **Organization Visibility** is set to ALL for all users and can't be modified as part of the single sign-on configuration. To limit **Organization Visibility**, go to ⚙**Settings** > **Users** > **Manage Users**, select a user, and then select **Some** for **Organization Visibility**.

Configure SAML authentication

You'll need to provide the following information to the identity provider:

Audience (Entity ID): `https://<Gluware-FQDN>/sso/saml/metadata`
ACS (Consumer) URL Validator: `https://<Gluware-FQDN>/.*`
ACS (Consumer) URL: `https://<Gluware-FQDN>/saml/callback`
Single Logout URL: `https://<Gluware-FQDN>/sso/saml/logout`
Login URL: `https://<Gluware-FQDN>/saml/login`

Basic SAML settings work for most implementations. If the **Basic** settings aren't sufficient, contact Gluware support at support@gluware.com for help using **Advanced** settings.



1. Ensure you're in the topmost (root) organization.
2. Go to **Settings** > **Global** > **Single Sign-On**.
3. Select **SAML**.
4. Select **Basic**.
5. Enter the **Entry Point**, the URL used to initiate a Single Sign On (SSO) with the identity provider.

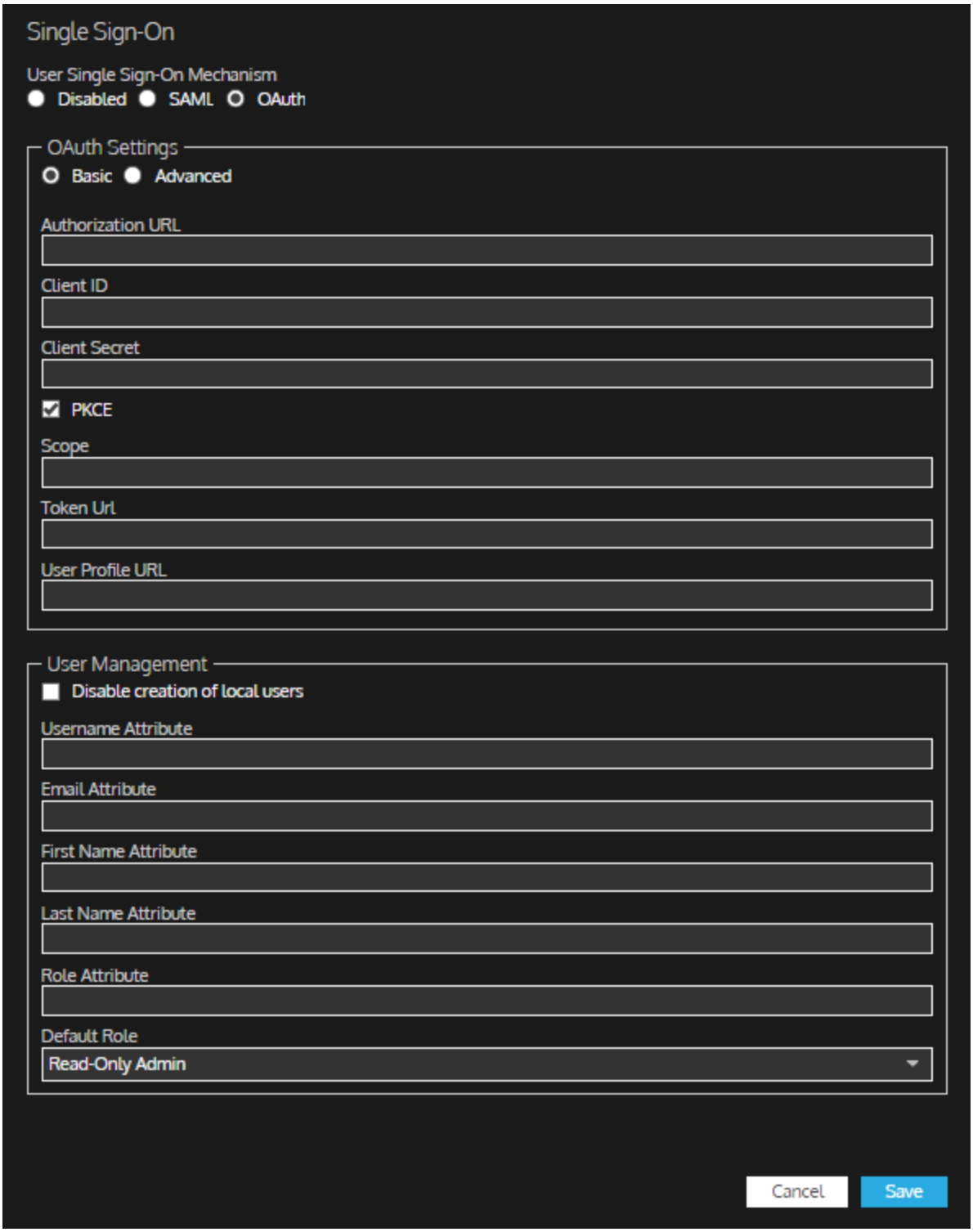
6. Enter the **issuer**, the URL of the identity provider.
7. Enter the **name ID format**, the format for the user identity that will be sent by the identity provider. The default is an email address ("urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress").
8. Paste the public X.509 **certificate** in Base-64 encoded format for the identity provider.
9. Optional: Enter the private **decryption private key** used to secure the communication between the identity provider and Gluware.
10. Enter the **sign-out URL**, the URL used to initiate a Single Log Out (SLO) with the identity provider.
11. Optional: Click in the **Disable creation of local users** box to limit new users to only those in SAML. Any existing users remain.
12. Enter the SAML attribute name where the username is stored in a user entry. Additional entries can be used if proxies are needed to access a device.
13. Enter the SAML attribute that contains the user's email address; for example, `mail`. If you don't specify an email address, Gluware will use the username and domain name since this is a required field.
14. Enter the SAML attribute that contains the user's first name.
15. Enter the SAML attribute that contains the user's last name.
16. Optional: Enter the SAML attribute used to set the role; for example, `memberOf`. If **Role Attribute** is assigned, the role cannot be modified in Gluware **Settings** **Users** > **Manage Users**.
17. Enter the default role to assign to the new user if the role is not specified or the SAML user entry does not include the Role Attribute. The role can be modified in Gluware **Settings** > **Users** > **Manage Users**.
18. Save.

Configure OAuth authentication

You'll need to provide the following information to the identity provider:

Sign-in redirect URI: `https://<Gluware-FQDN>/sso/oauth/callback`

Basic OAuth settings work for most implementations. If the **Basic** settings aren't sufficient, contact Gluware support at support@gluware.com for help using **Advanced** settings.



1. Ensure you're in the topmost (root) organization.
2. Go to ⚙**Settings** > **Global** > **Single Sign-On**.
3. Select **OAuth**.
4. Select **Basic**.

5. Enter the **Authorization URL**, The URL used to initiate a Single Sign On (SSO) with the identity provider.
6. Enter the **Client ID**, the public identifier generated by the identity provider to uniquely identify Gluware.
7. Enter the **Client Secret**, the shared secret generated by the identity provider.
8. Check the **PKCE** box if using Proof Key for Code Exchange to provide additional security.
9. Enter the **Scope**, the scope assigned to users that allows them to sign in to Gluware using OAuth2 as defined in the identity provider.
10. Enter the **Token URL**, the URL used to request access tokens from the identity provider.
11. Enter the **User Profile URL**, the URL to retrieve user profiles from the identity provider.
12. Optional: Click in the **Disable creation of local users** box to limit new users to only those in OAuth. Any existing users remain.
13. Enter the OAuth attribute name where the username is stored in a user entry. Additional entries can be used if proxies are needed to access a device.
14. Enter the OAuth attribute that contains the user's email address; for example, `mail`. If you don't specify an email address, Gluware will use the username and domain name since this is a required field.
15. Enter the OAuth attribute that contains the user's first name.
16. Enter the OAuth attribute that contains the user's last name.
17. Optional: Enter the OAuth attribute used to set the role; for example, `memberOf`. If **Role Attribute** is assigned, the role cannot be modified in Gluware **Settings** > **Users** > **Manage Users**.
18. Enter the default role to assign to the new user if the role is not specified or the OAuth user entry does not include the Role Attribute. The role can be modified in Gluware **Settings** > **Users** > **Manage Users**.
19. Save.

Step 7. Install your Gluware licenses

After you have created your organization structure, obtain and activate your Gluware licenses. Gluware licenses are used to manage:

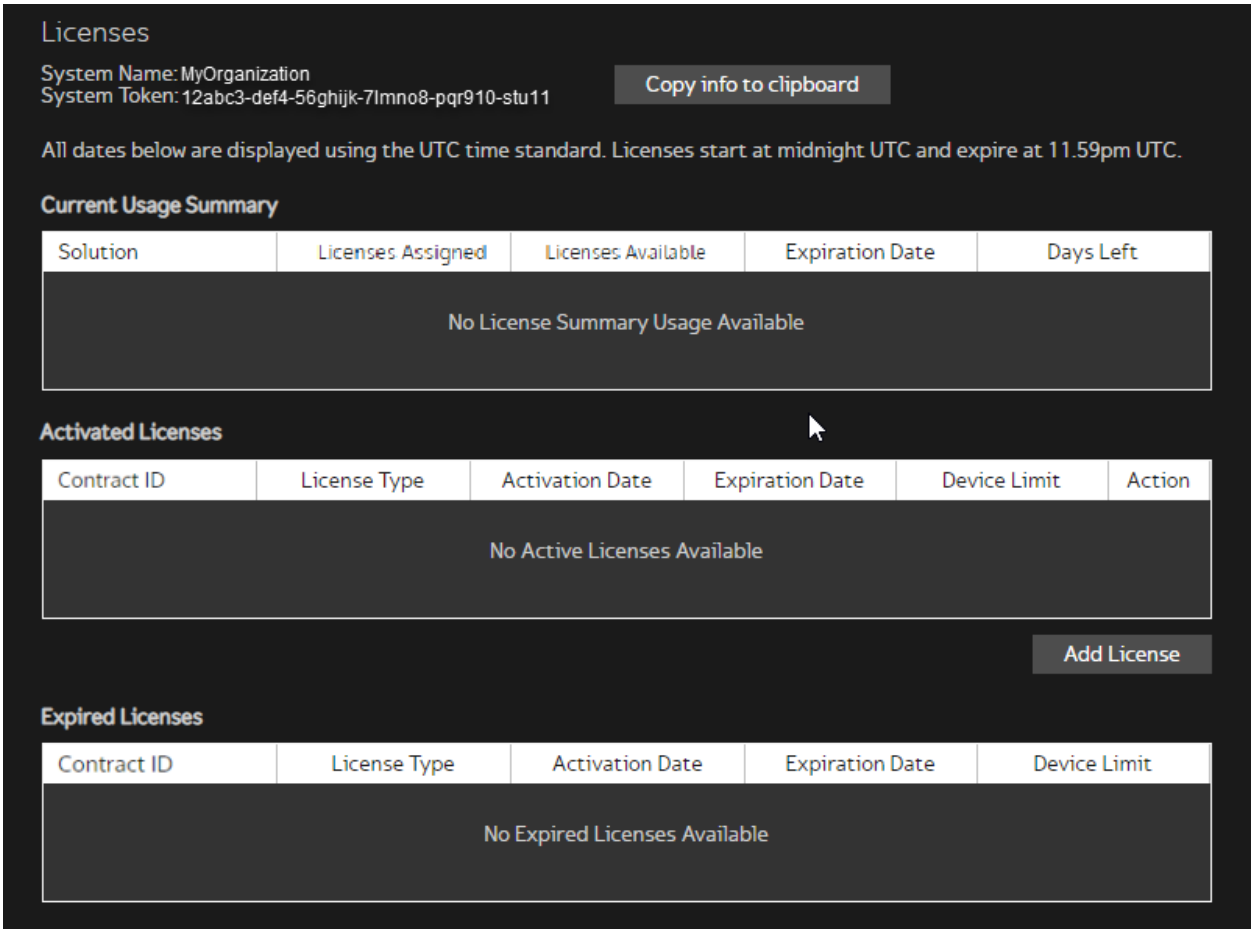
- The Gluware solutions available to you
- The maximum number of devices in your Gluware system
- The expiration date of your evaluation period or product licenses

IMPORTANT: You usually install your Gluware licenses in your parent (topmost) organization. All child organizations share these licenses and the pool of devices. If you install a license in a child organization, licenses from the parent organization no longer apply to the child organization.

Once you install a license in an organization, you cannot move it to a different organization.

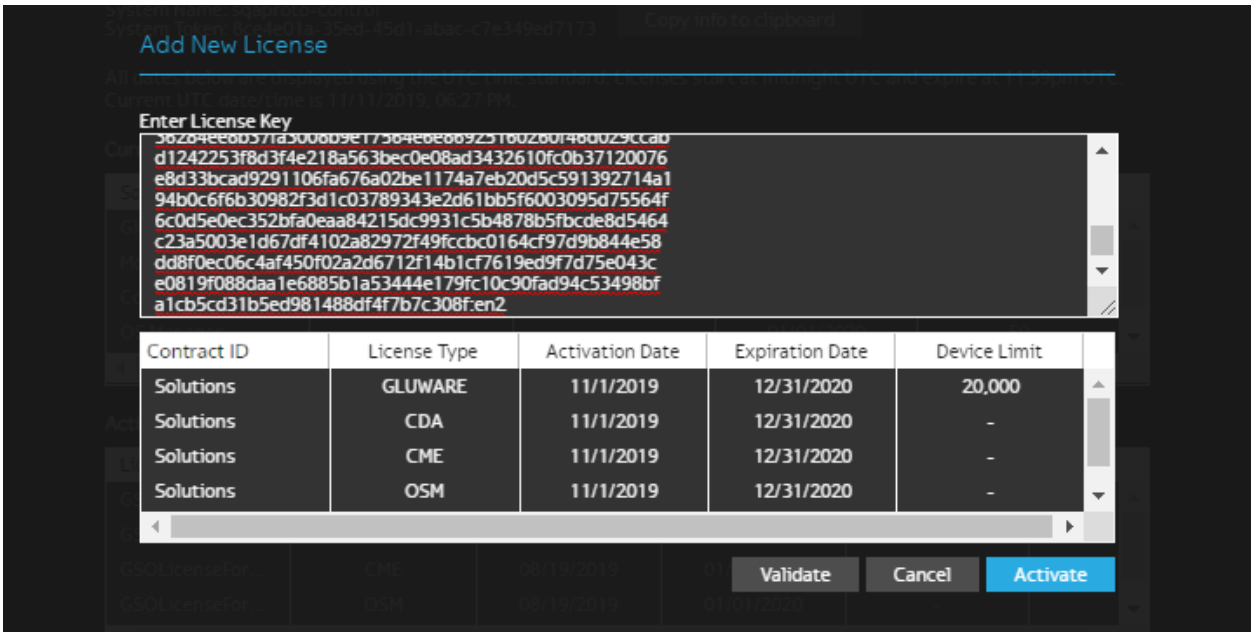
Request your contract ID from Gluware

1. Ensure you're in the organization you want to install the license in. This is usually your parent (topmost) organization. You can see the organization you are in, and navigate to other organizations, at the top right of the screen.
2. Go to **Settings** and select **Organization** > **Licensing**. At the top of the screen you'll see your System Name and System Token.
3. Click **Copy info to clipboard**. This copies the system name and token to your clipboard.
4. Send an email to licensing@gluware.com that includes:
    - The **System Name** and **System Token** that you copied
    - The **name**, **email**, and **phone number** of the person to receive the license via email



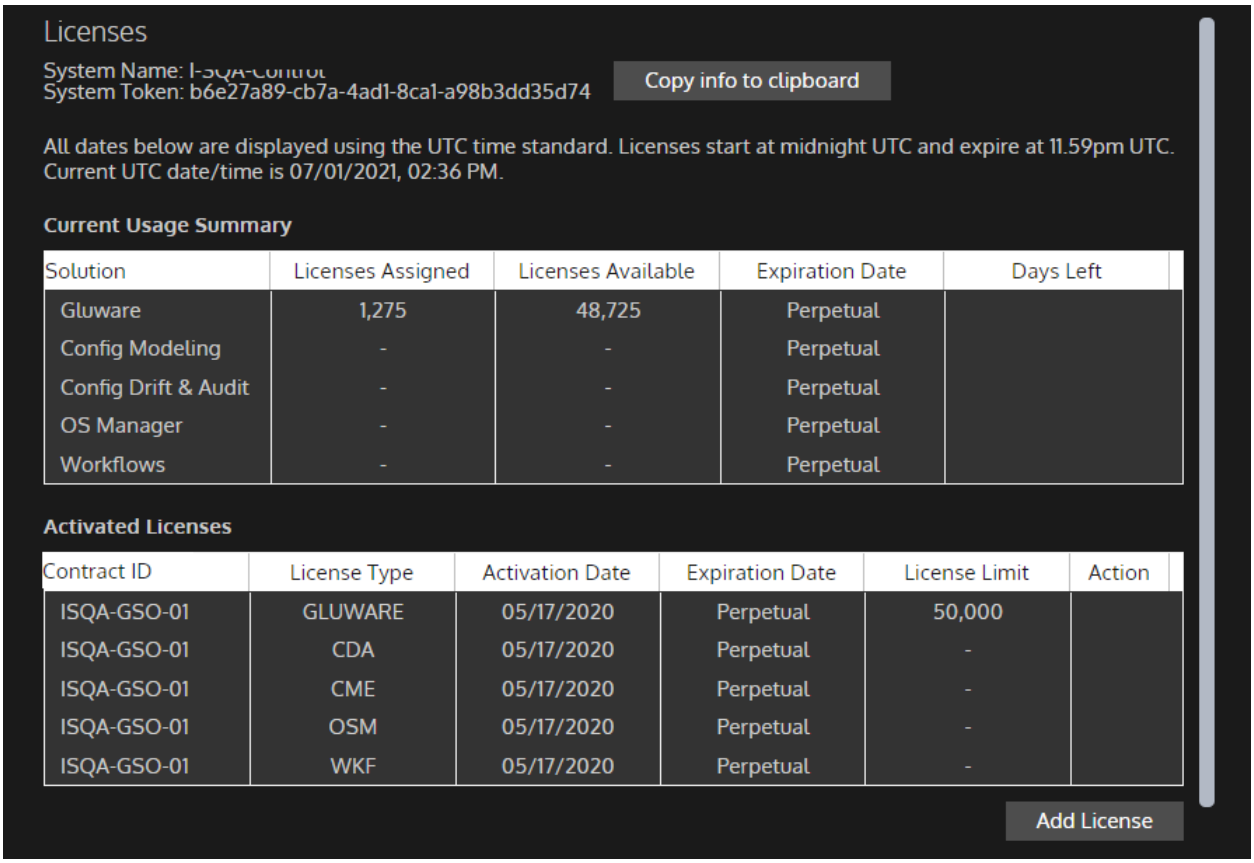
Install your license

1. Ensure you're in the organization you want to install the license in. This is usually your parent (topmost) organization. You can see the organization you are in, and navigate to other organizations, on the right side of the home bar.
2. Go to **Settings** and select **Organization** > **Licensing**.
3. Click **Add License**.
4. Paste the contract ID you received from Gluware in the space provided and click **Validate**.



5. **Verify these three important items**:
   - No errors are displayed
   - The organization displayed at the top of the screen is the organization you want to install the license in
   - The license information displayed matches your sales order
6. If there are any error messages you can't resolve or any info is incorrect, click **Cancel** and contact licensing@gluware.com immediately. If all looks correct, click **Activate**.

You'll see your newly installed licenses in the **Activated License** list. As a license nears expiration or your device count nears capacity, a warning message will notify you. Your data is not lost, even if the license expires, but it will no longer be accessible through Gluware.



Next step: Set up data retention

Step 8. Set up data retention

IMPORTANT: Set up data retention to keep Gluware running smoothly by eliminating outdated and ephemeral information from the Gluware database.

Think carefully about what makes sense for your organization to reduce confusion and keep Gluware running optimally. For example, while compliance may require that you retain logs from successful provisioning of a device for 6 months or more, failed provisioning logs are only needed until troubleshooting is complete and could be eliminated after a few days or weeks.

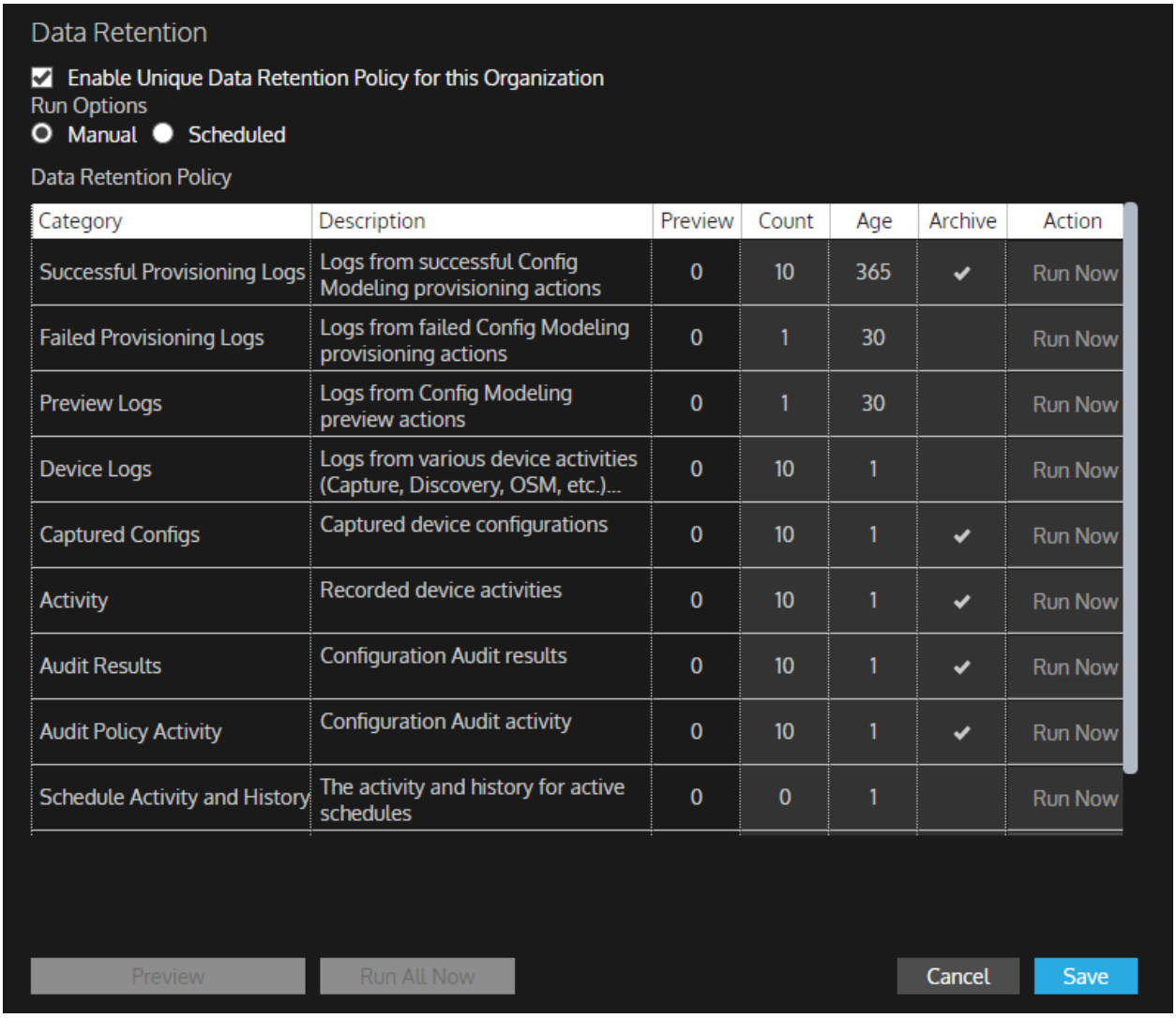
By default, the policy specified in the parent organization is inherited in all child organizations. However, each organization can have their own policy, schedule settings, and data retention settings.

1. Ensure you're in the organization you want to set up data retention for.
2. Go to Gluware **Settings** and select **Organization** > **Data Retention**.
3. Check the **Enable Unique Data Retention Policy for this Organization** box if you want a unique policy for this organization. Otherwise, the policy inherited from the parent organization is displayed.
4. Select **Manual** to only run the policy at will. Select **Scheduled** and set the frequency to automate the policy.
5. Specify the number of records to retain by double-clicking the **Count** cell.
6. Specify the maximum age of the records to be retained by double-clicking the **Age** cell. Entering **0** for **Age** disables age-based retention.

7. Double-click the **Archive** cell and check the box to create a text file of the purged data in /var/gluware/archive. If **Archive** is not selected, no text file is created when the data is purged.

NOTE: Archive is not recommended. Archive files are not backup files that can be reinstalled or used by Gluware. They are text files for offline use. To create a backup, *see* Set up scheduled backups.

8. Save.



Data Retention category descriptions

Deleted organizations

When an organization is deleted in **Settings** > **Organization** > **Organizations**, the data belonging to the organization is marked as deleted and remains in the database until you run Data Retention. The organization data includes:

Custom field settings
Dashboard settings
Data retention settings
Event settings (syslog and automatic configuration snapshots)
Integration settings (Cisco support API credentials)
Gluware licenses
Organization settings
OS Manager settings
Custom role settings
Zone settings
Users
Dashboards
Devices and device activity
Discovered and captured device configurations
Network discovery details, results, and activity
Config Audit policies, executions, results, and activity
File server directory names, file names and associated metadata
OS Catalogs and activity
OS Manager plans, executions, and activity
Data Explorer templates, results, and activity
Schedule details, future occurrences, history, and activity
Ad Hoc queries and results
Work results and logs
Job logs
Loaded solution packages
Config Modeling nodes, features, globals, domains, and scripts
Provisioning logs

The **Deleted Organizations** category is only available at the topmost Gluware organization. An organization that is a provider of one or more

other organizations cannot be deleted, so there is no risk of data retention deleting data that is actively being shared, such as Custom Fields and Roles, with child organizations.

Data that is shared by a parent organization with a child organization belongs to the parent organization and will not be deleted when Data Retention removes the data for a deleted child organization.

If a child organization is deleted followed by the deletion of the parent organization, running Data Retention processes the child organization first. A subsequent execution cleans up the parent organization's data.

Deleted Instances

When Config Modeling nodes, features, globals, domains, and scripts are deleted they are marked as deleted but remain in the database. Running data retention permanently removes these instances based on the count and age criteria.

This category is only available at the topmost Gluware organization and applies to deleted instances in all organizations in the Gluware system.

Successful Provisioning Logs

Deletes successful provisioning logs that match the count and age criteria. The count criteria is the minimum number of the most recent logs retained per node. The provisioning types are:

Provision Features
Renew Certificate
Revoke Certificate
All OS Management provisioning

This category only applies to logs associated with devices in the organization where data retention is run.

Failed Provisioning Logs

Deletes failed provisioning logs that match the count and age criteria. The count criteria is the minimum number of the most recent logs retained per node. The provisioning types are:

Provision Features
Renew Certificate
Revoke Certificate
All OS Management provisioning

This category only applies to logs associated with devices in the organization where data retention is run.

Preview Logs

Deletes failed preview provisioning logs that match the count and age criteria. The count criteria is the minimum number of the most recent logs retained per node.

This category only applies to logs associated with devices in the organization where data retention is run.

Device Logs

Deletes all job logs associated with a device, including network discovery, device discovery, snapshots, ad hoc queries, policy audits, reboots, etc. that match the count and age criteria. The count criteria is the minimum number of the most recent logs retained per node.

This category only applies to logs associated with devices in the organization where data retention is run.

Captured Configs

Deletes configuration snapshots from captures that match the count and age criteria. The count criteria is the minimum number of the most recent snapshots retained per node. The configuration marked as default is always retained.

This category only applies to snapshots associated with devices in the organization where data retention is run.

Activity

Deletes activity events of devices that match the count and age criteria. The count criteria is the minimum number of the most recent activity events retained per device.

This category only applies to activity associated with devices in the organization where data retention is run.

Audit Results

Deletes data related to the execution of audit policies, including results, work logs, work results, and work reports that match the count and age criteria. The count criteria is the minimum number of the most recent audit results retained per audit policy.

This category only applies to audit results associated with devices in the organization where data retention is run.

Audit Policy Activity

Deletes activity events of audit policies that match the count and age criteria. The count criteria is the minimum number of the most recent activity events retained per audit policy.

This category only applies to audit policy activity associated with devices in the organization where data retention is run.

Schedule Activity and History

Deletes activity and history of scheduled tasks that match the count and age criteria. This includes the work logs, work results and work reports associated with the scheduled tasks associated with the schedule history. The count criteria is the minimum number of the most recent activity events and historical executions retained per schedule.

This category only applies to schedule activity and history associated with devices in the organization where data retention is run.

Exhausted Schedules

Deletes schedules that no longer have future occurrences that match the count and age criteria. This includes schedule details, schedule activity, schedule history, and the work logs, work results, and work reports associated with the scheduled tasks' history. The count criteria is the minimum number of exhausted schedules retained for the organization.

This category only applies to exhausted schedules associated with devices in the organization where data retention is run.

Other Data Retention fields

Field	Description
Preview	Number of records that would be archived and removed or simply removed based on the current retention policy. Populated by clicking **Preview**
Count	Minimum number of records to retain for each device. For a device-specific category, number of records to retain for the category for each device
Age	Maximum age for the record to be retained (e.g., If age = 30, then entries older than 30 days will be archived and removed or only removed). 0 disables retention by age
Archive	Records that meet the criteria will be archived as a text file and removed from the database
Action	Run the data retention policy for the category
Preview	Populate the count for the current organization in the Preview column on this screen

Function	Description
Run All Now	Runs the data retention policy for all categories for the current organization and any child organizations that inherit it

Next step: Set up scheduled backups

Step 9. Set up scheduled backups

Schedule regular backups of your Gluware system.

To set up backups, sign in to Gluware via a terminal session using the local user account you created. Execute the following command:

`sudo gluwarectl scheduleBackup enable` <backupPath> <mailto> <minute> <hour> <day> <month> <dayofweek>

backupPath – Location where data backups will be written
mailto – Email address for sending task notifications
minute – 0-59; minute of the hour the task will start
hour – 0-23; hour during a day the task will start
day – 1-31 or *; day during a month the task will start. * is every day
month – 1-12; month during a year the task will start
dayofweek – 0-6; day of the week the task will start. 0 is Sunday

Best practices

While the use of backups is strongly encouraged, backups can be large and, based on frequency, fill disk space quickly. Selecting a <backupPath> that is outside of Gluware, such as an external drive, is strongly recommended.

Next step: Install packages

Step 10. Install packages

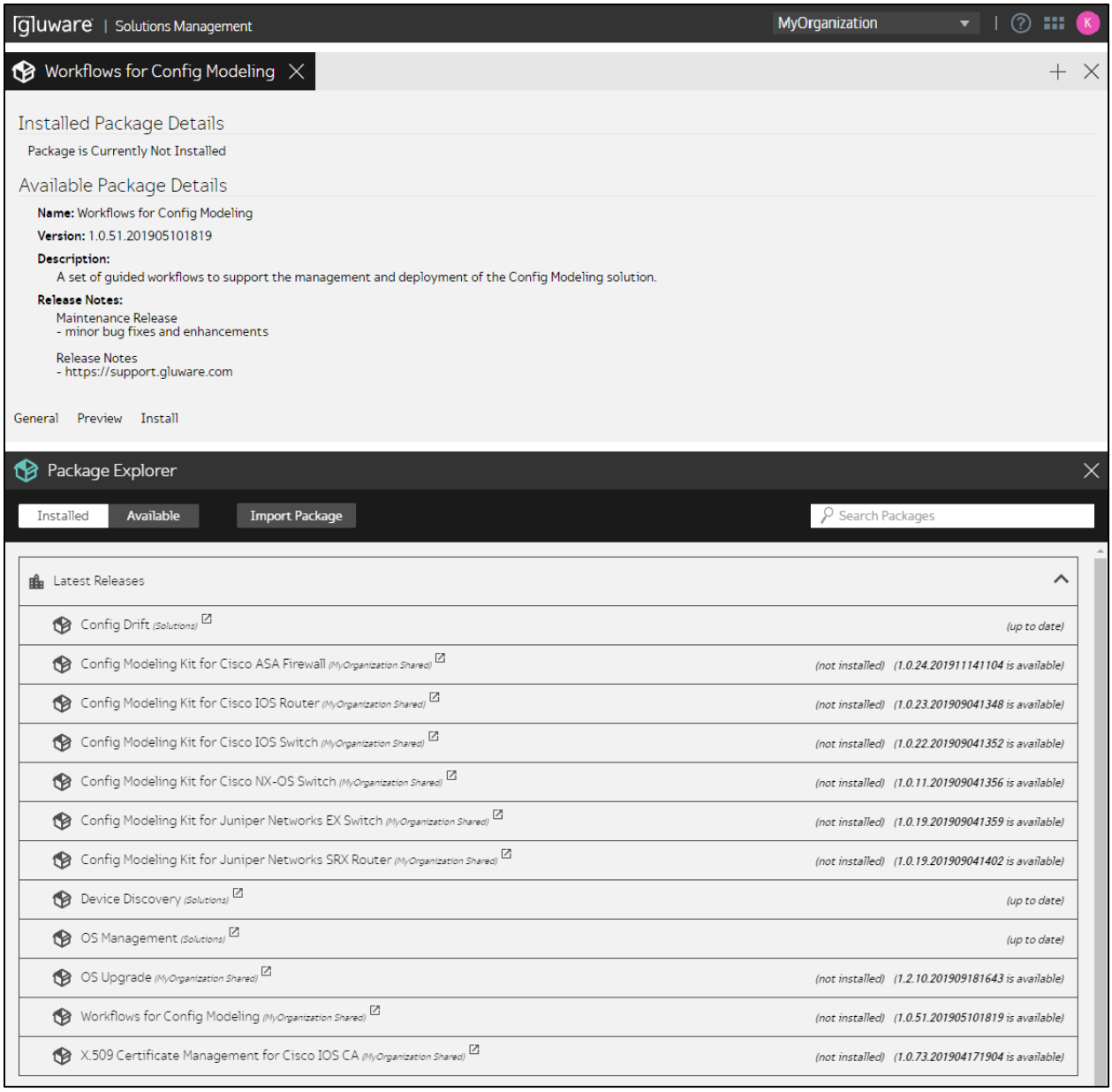
You can install any combination of features and capabilities you have licensed from Gluware in any organization you have created.

- To use Device Manager, you'll need the **Device Discovery package**.
- To use Config Drift and Audit, you'll need the **Config Drift package**.
- To use OS Manager, you'll need the **OS Management package**.

> **NOTE:** Packages must be installed one at a time. The organization will be locked until the installation is complete.

1. Ensure you are in the organization you want to install the package in.
2. Go to Gluware **Solutions Manager** and double-click the package you want to install.
3. Select **Preview** to preview the installation details.
4. Select **Install**.
5. Click **Install Package**.

If you are licensed for and want to use **Config Modeling** or **Workflows**, you'll need the **Workflows for Config Modeling** package and the **Config Modeling Kit** packages for your device types. These are available from the Gluware Distribution Area or from Gluware if you do not have internet access from your primary Gluware system.


gluware | Solutions Management
MyOrganization
Workflows for Config Modeling
Installed Package Details
Package is Currently Not Installed
Available Package Details
Name: Workflows for Config Modeling
Version: 1.0.51.201905101819
Description:
A set of guided workflows to support the management and deployment of the Config Modeling solution.
Release Notes:
Maintenance Release
- minor bug fixes and enhancements
Release Notes
- https://support.gluware.com
General
Preview
Install
Package Explorer
Installed
Available
Import Package
Search Packages
Latest Releases
Config Drift (Solutions) (up to date)
Config Modeling Kit for Cisco ASA Firewall (MyOrganization Shared) (not installed) (1.0.24.201911141104 is available)
Config Modeling Kit for Cisco IOS Router (MyOrganization Shared) (not installed) (1.0.23.201909041348 is available)
Config Modeling Kit for Cisco IOS Switch (MyOrganization Shared) (not installed) (1.0.22.201909041352 is available)
Config Modeling Kit for Cisco NX-OS Switch (MyOrganization Shared) (not installed) (1.0.11.201909041356 is available)
Config Modeling Kit for Juniper Networks EX Switch (MyOrganization Shared) (not installed) (1.0.19.201909041359 is available)
Config Modeling Kit for Juniper Networks SRX Router (MyOrganization Shared) (not installed) (1.0.19.201909041402 is available)
Device Discovery (Solutions) (up to date)
OS Management (Solutions) (up to date)
OS Upgrade (MyOrganization Shared) (not installed) (1.2.10.201909181643 is available)
Workflows for Config Modeling (MyOrganization Shared) (not installed) (1.0.51.201905101819 is available)
X.509 Certificate Management for Cisco IOS CA (MyOrganization Shared) (not installed) (1.0.73.201904171904 is available)

Step 11. 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

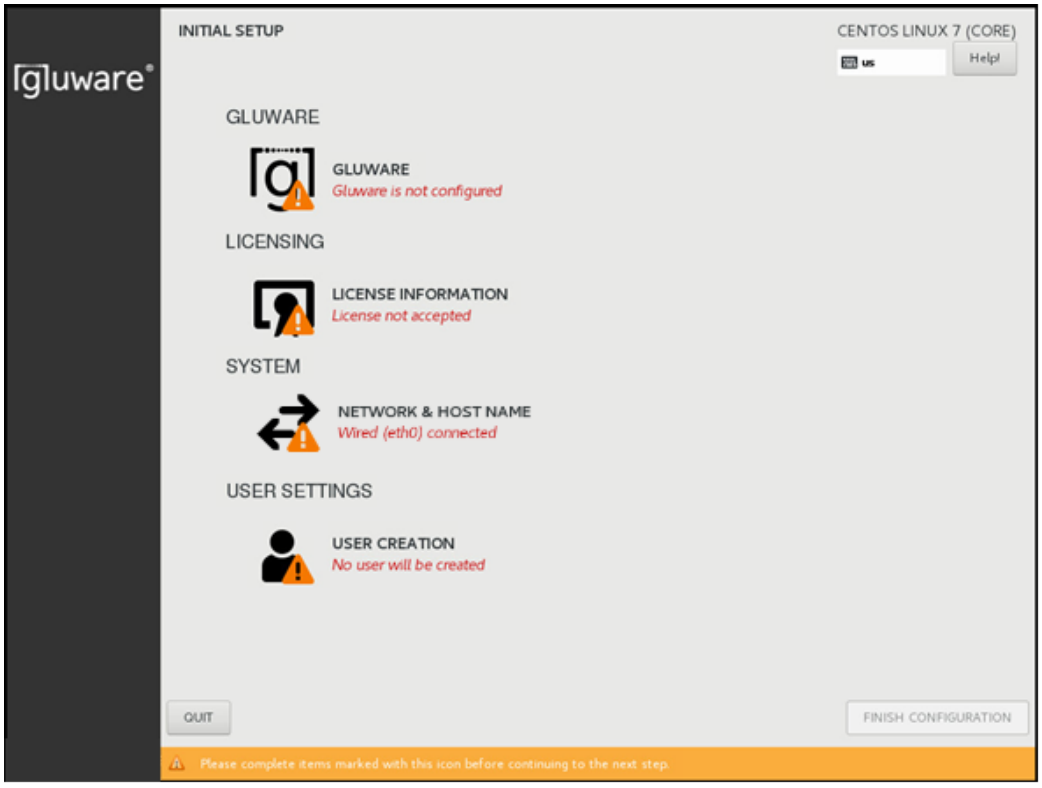
Set up the Gluware Primary Server completely before you configure the Disaster Recovery Server.

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

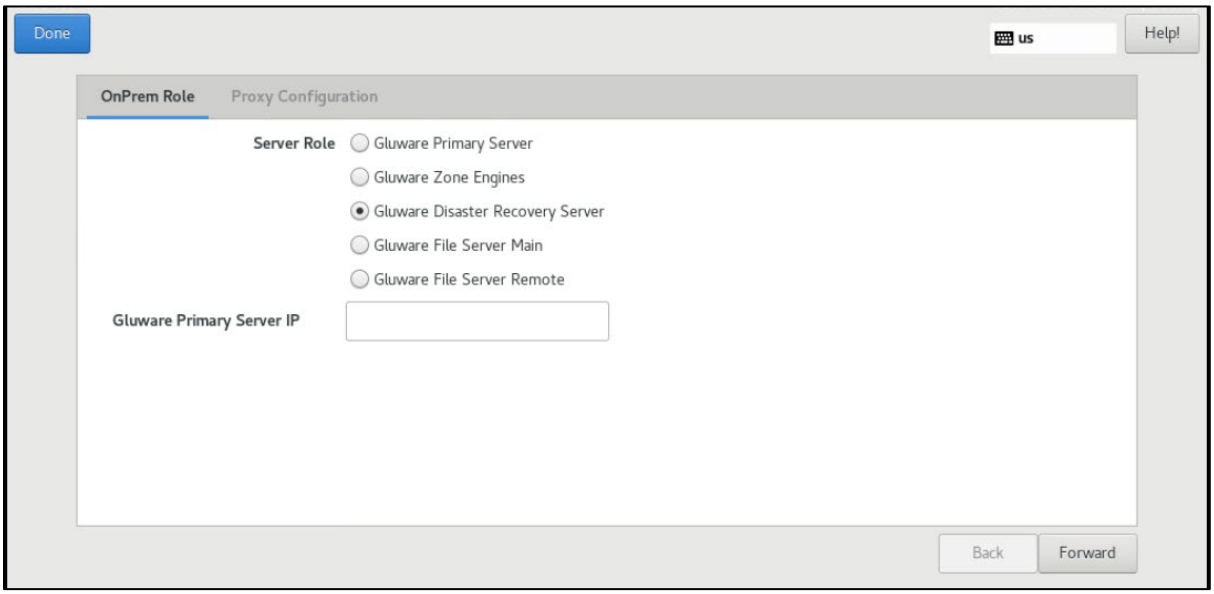
1. Open the **VMware Console**.
2. On the **INITIAL SETUP** screen, **first** select **NETWORK & HOST NAME**.



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.



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.

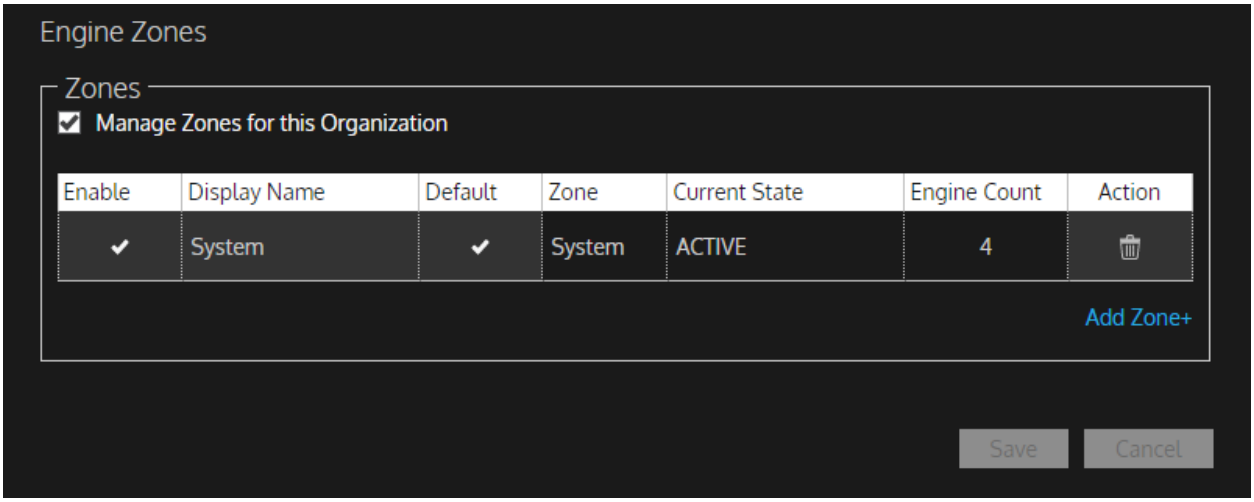
When you install a Gluware Zone Engines Server, you can assign the engines to a zone. Then each device can preferentially run jobs on the zone's engine or engines when they are ACTIVE.

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



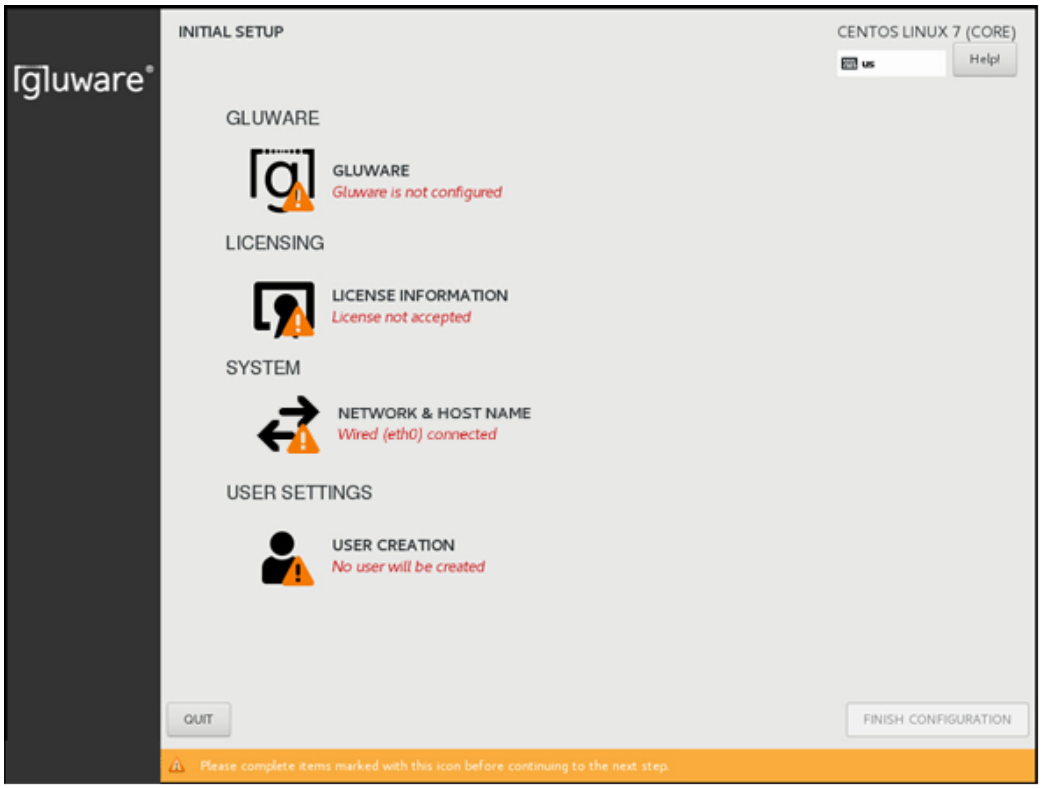
Add a zone in Gluware system settings

Add one or more zone in Gluware system 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

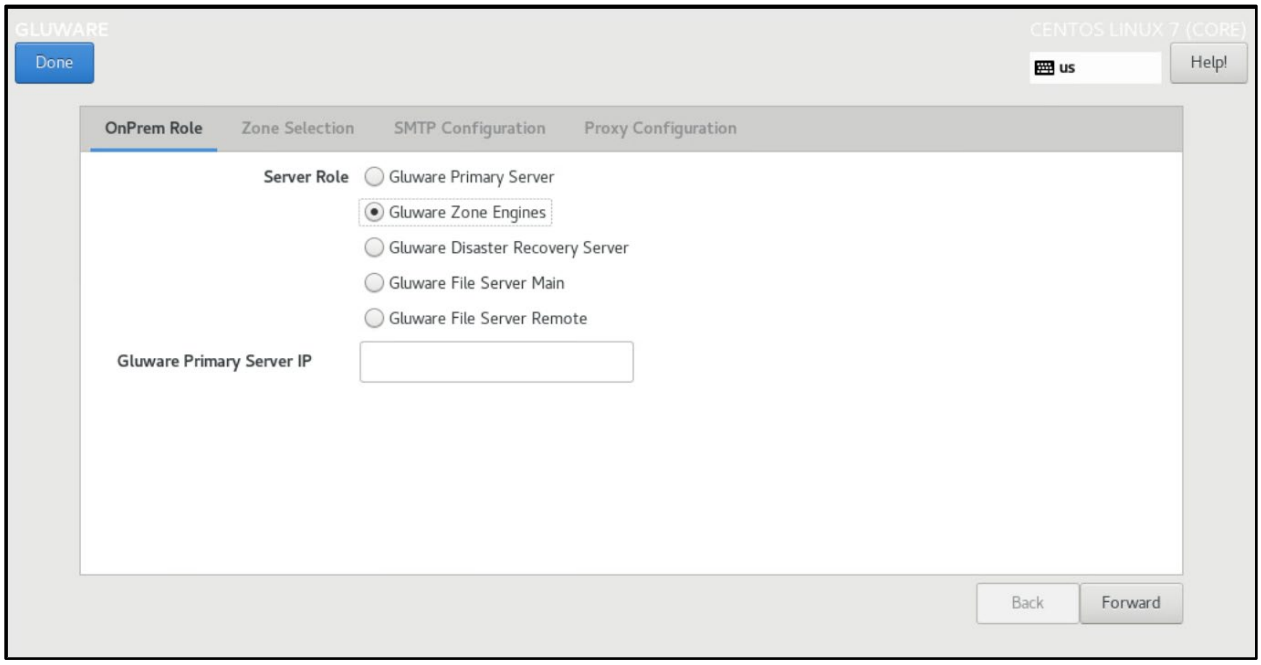
1. Open the **VMware Console**.
2. On the **INITIAL SETUP** screen, **first** select **NETWORK & HOST NAME**.



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

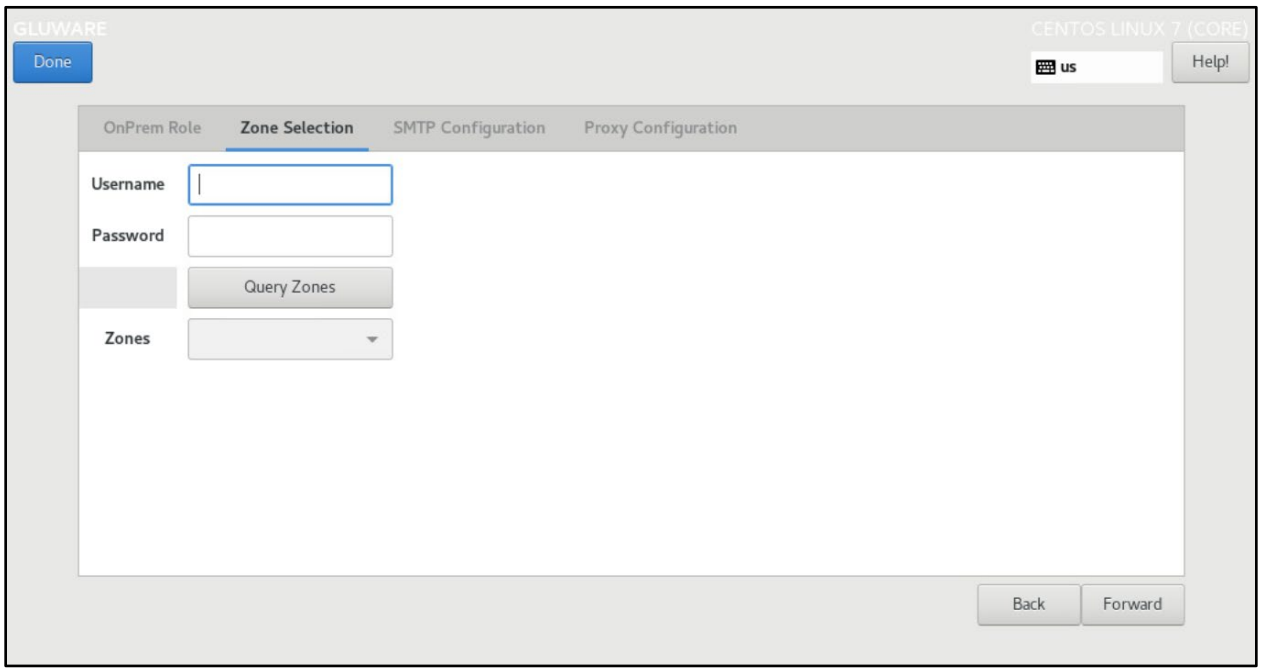
10. On the **INITIAL SETUP** screen, select **GLUWARE**.
11. On the **OnPrem Role** tab, select **Gluware Zone Engines**.
12. Enter the IP address for the Gluware Primary Server. At this point, the address is validated, and a connection is tested.
13. Do one of the following:
    - If you are only using 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.



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 Modeling 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

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.

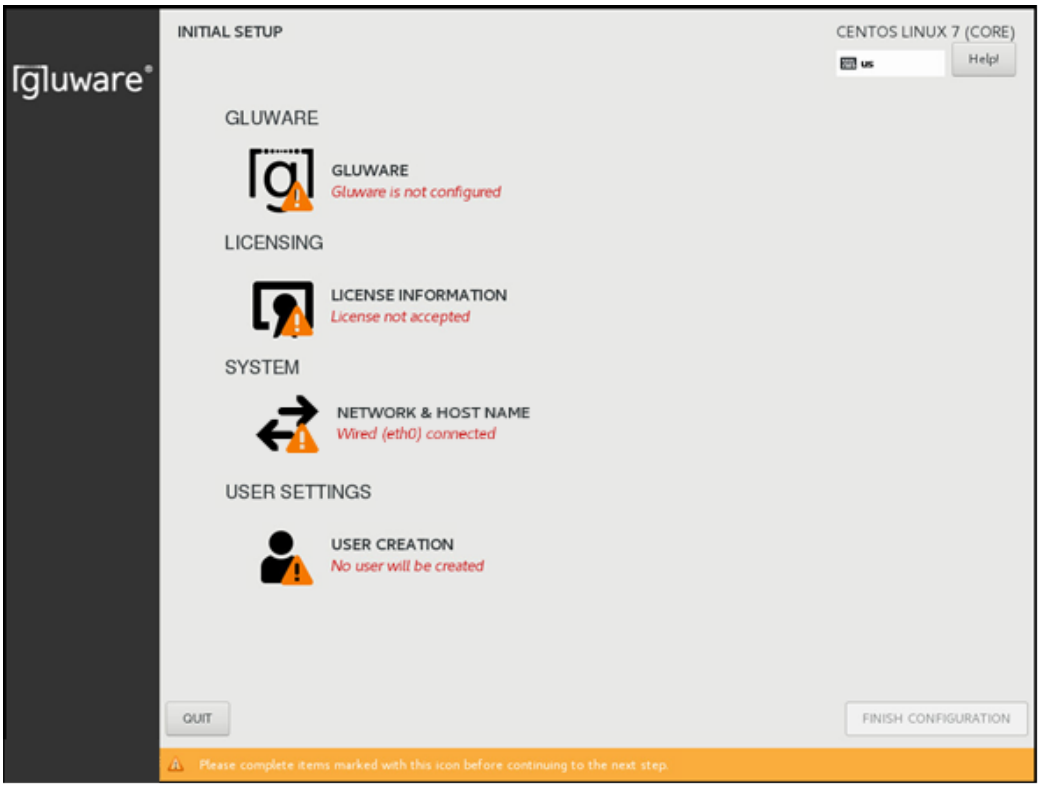
To configure the main File Server, ensure you have the following information:

- 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

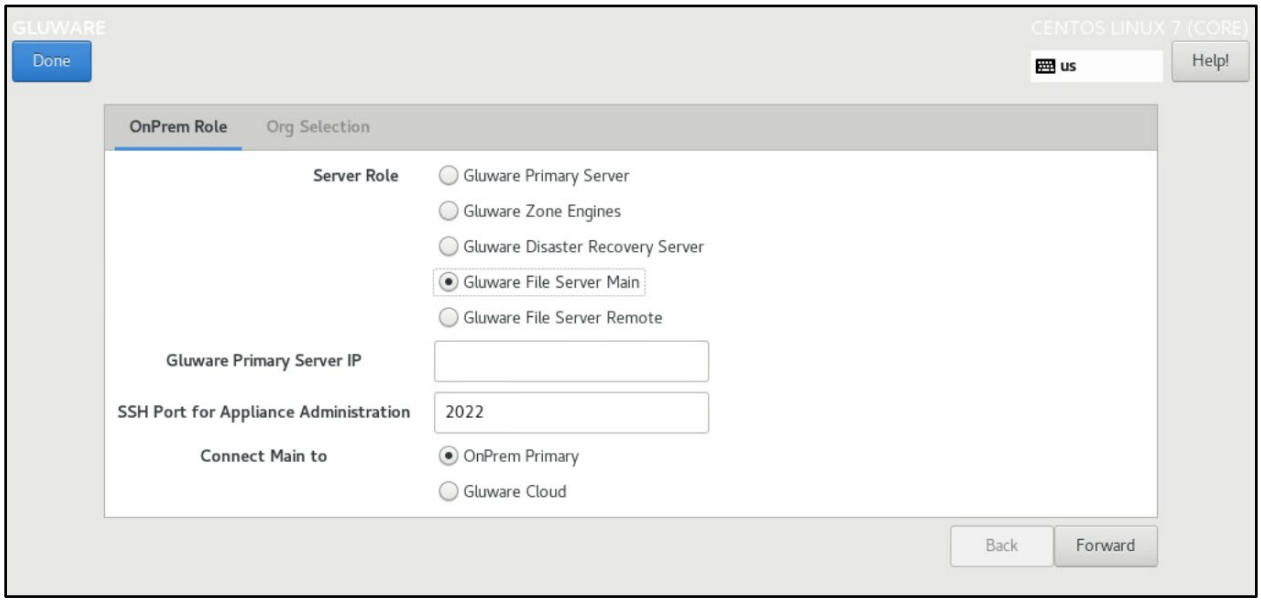
1. Open the **VMware Console**.
2. On the **INITIAL SETUP** screen, **first** select **NETWORK & HOST NAME**.



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

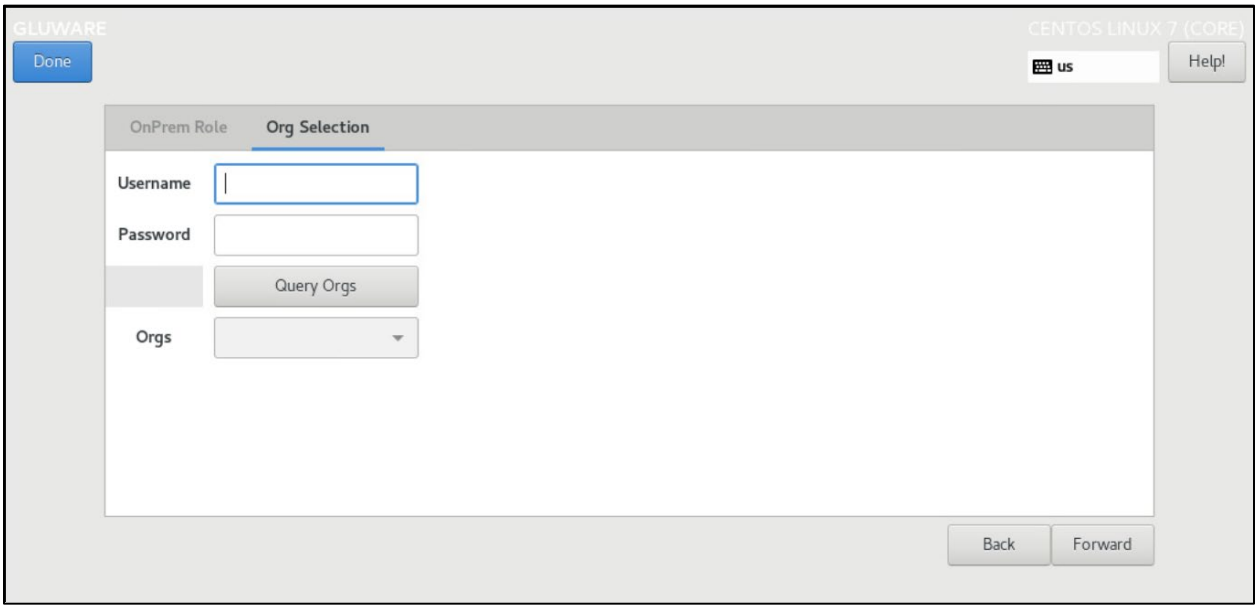
10. On the **INITIAL SETUP** screen, select **GLUWARE**.
11. On the **OnPrem Role** tab, select **Gluware File Server Main**.



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.

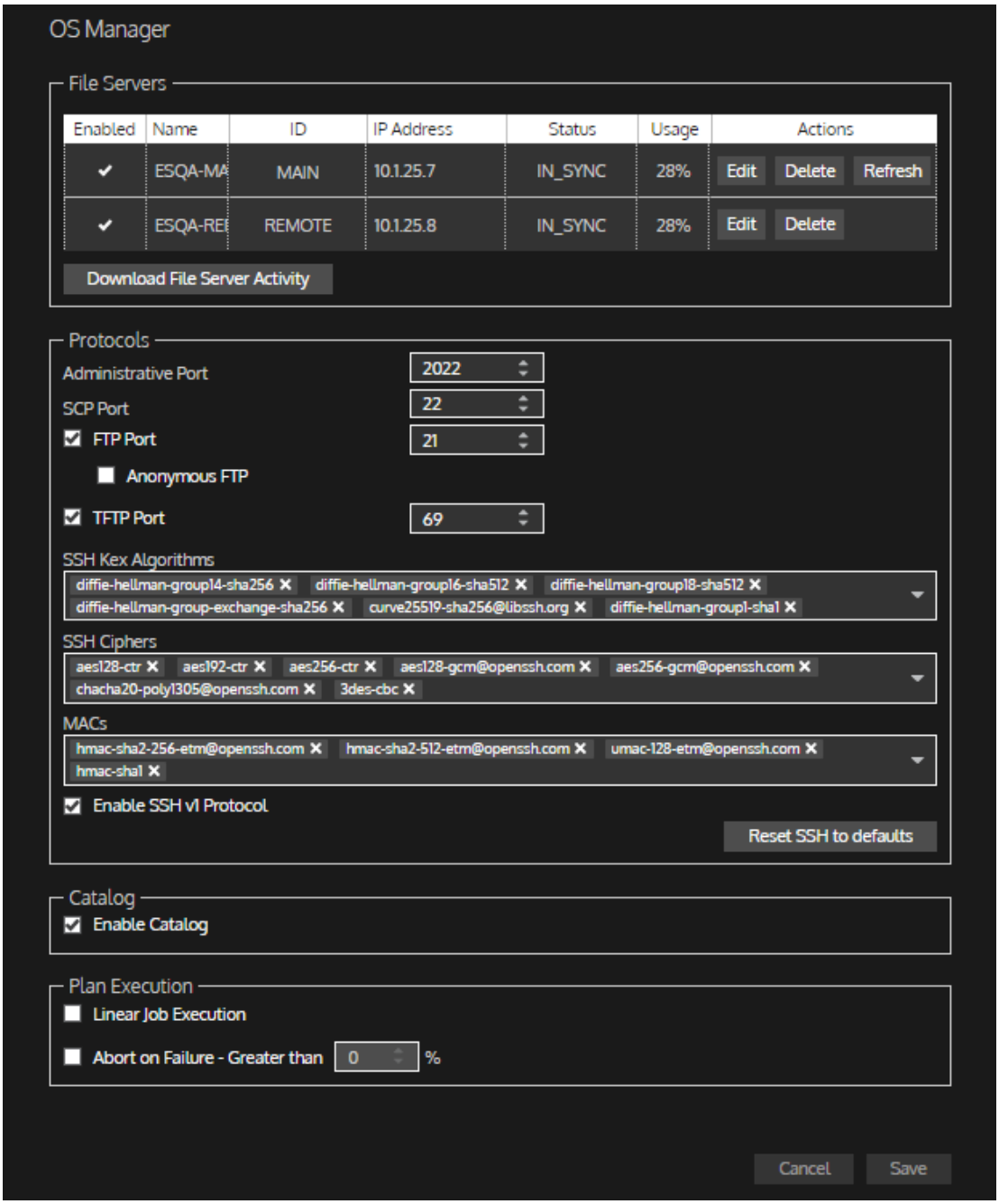
24. Confirm the password and click **DONE**.
25. On the **INITIAL SETUP** screen, click **FINISH CONFIGURATION**.
26. Sign off CentOS and sign in again to ensure the appropriate permissions take effect.

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.



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.

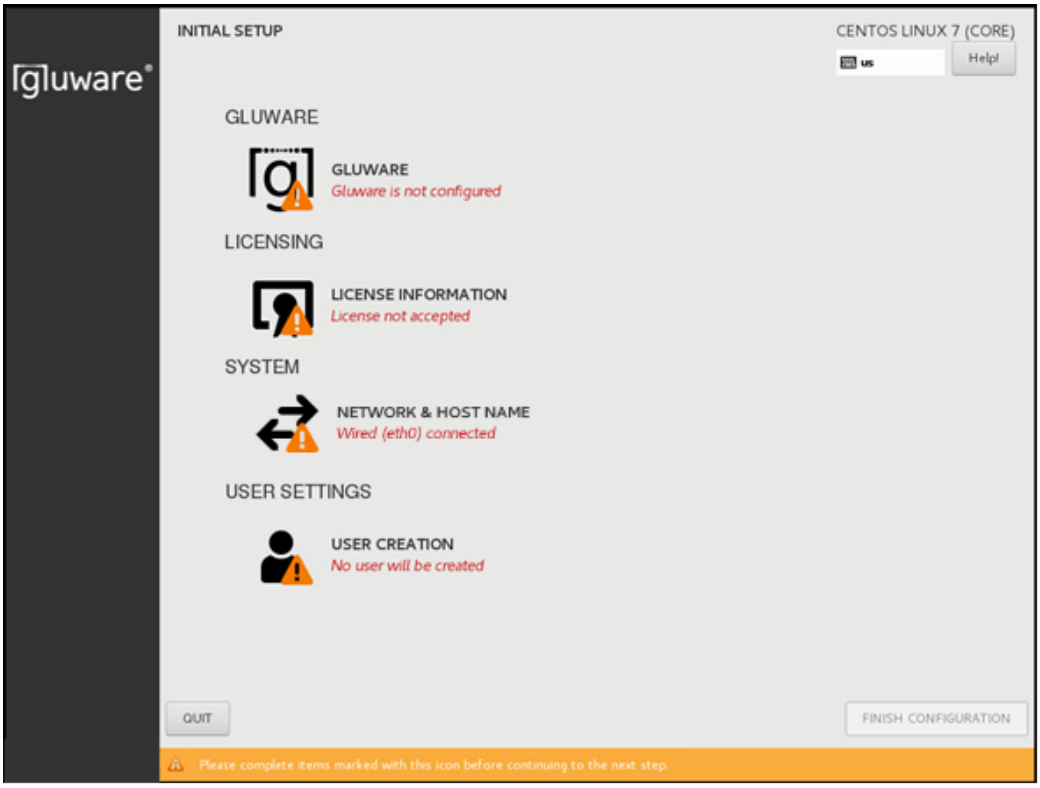
To configure a remote File Server, ensure you have the following information:

- 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**.

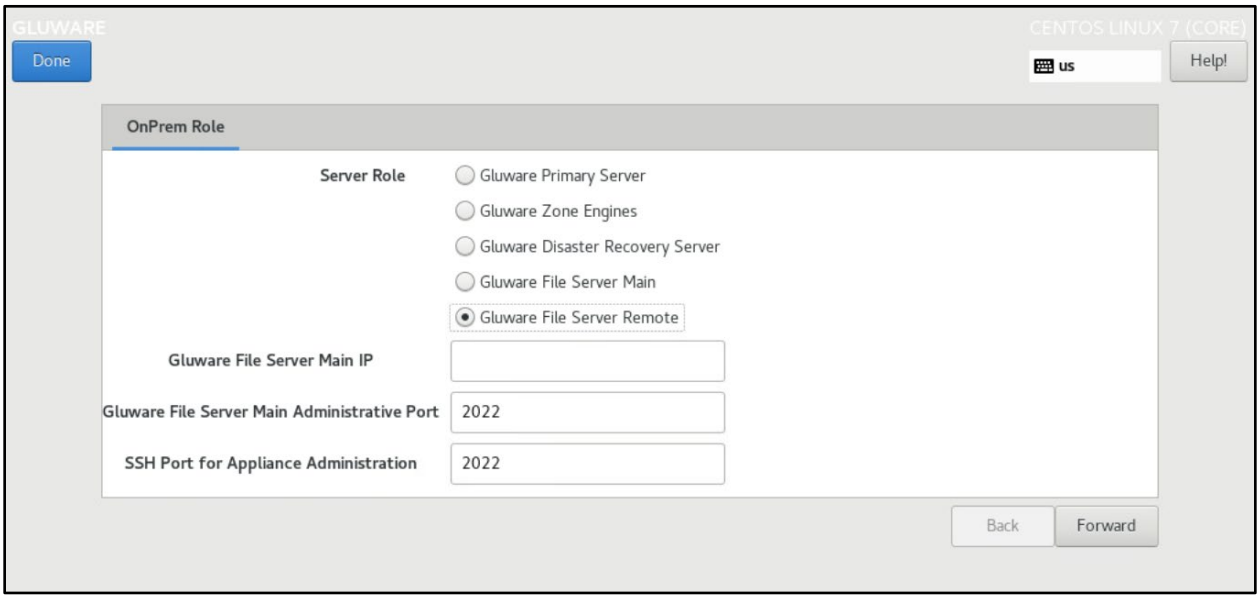


3. Ensure that **Ethernet (eth0)** is selected. (Don't change the **Bridge (docker0)** settings.)
4. Enter the fully qualified host name you want for this host and click **Apply**.
5. Click **Configure** to define your network configuration on the eth0 adapter.
6. Select the **IPv4 Settings** tab.
7. 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**.



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

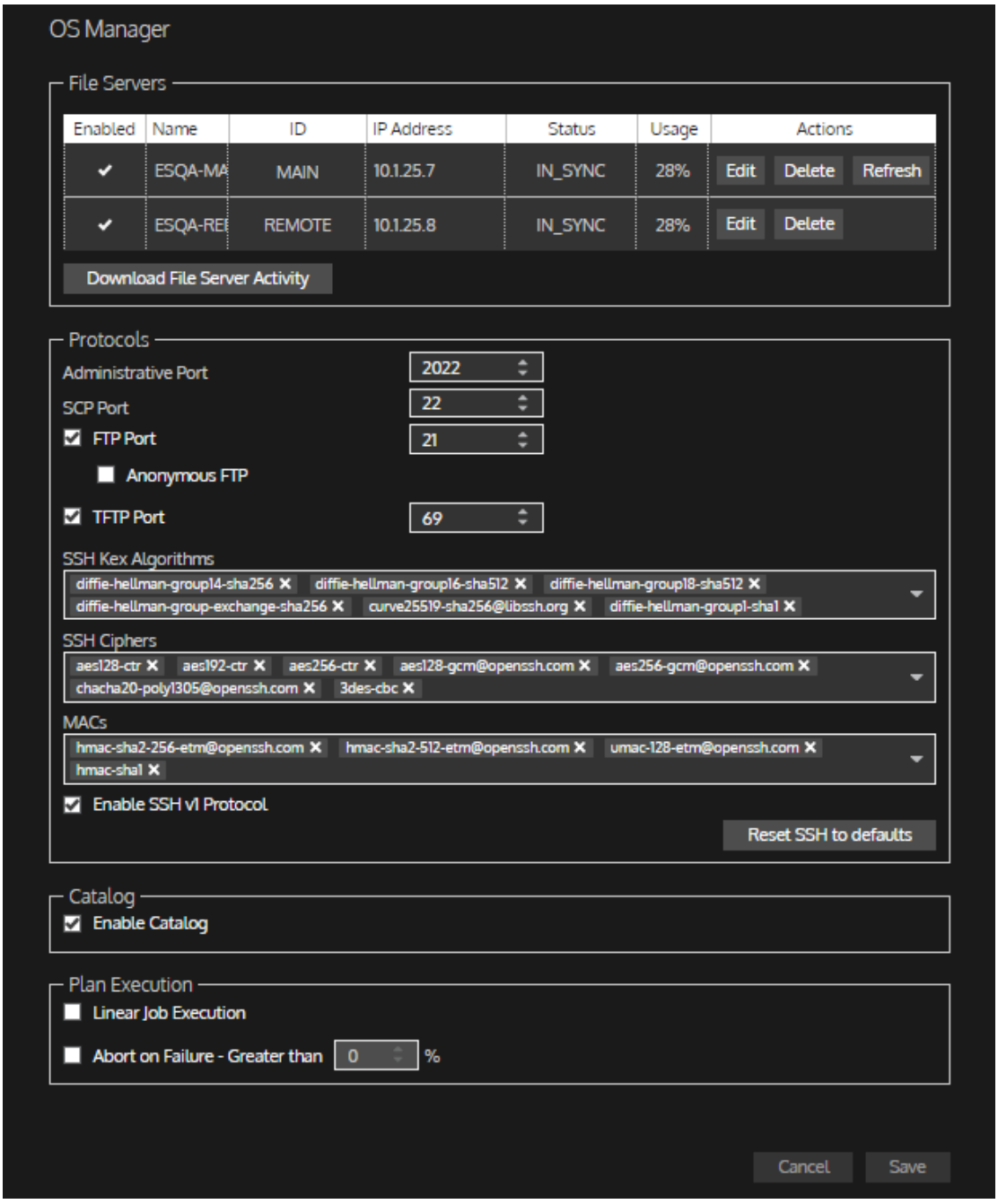
18. On the **INITIAL SETUP** screen, select **USER CREATION**.
19. Enter the CentOS user's first and last name (**Full name**).
20. Provide the **User Name** and **Password** the CentOS user will use to administer the Gluware system. Create a strong password to protect access to Gluware.
21. Confirm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



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 instruction 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" in Gluware online Help 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.
3. Do one of the following:
    - Download the upgrade package **gluware-control-upgrade-4.2.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-4.2.250.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-4.2.250.tar.gz.enc /myDirectory`
4. Check the upgrade results by issuing the **`sudo gluwarectl status`** command. 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
5. In your browser, clear cache and cookies using **Ctrl**+**Shift**+**R**/ ⌘+**Shift**+**R**.

Enable GluAPI

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/

Watch a video about GluAPI at https://youtu.be/P1ac5UgClOM

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

To enable GluAPI

1. Go to Gluware ⚙**Settings** > **Organization** > **Organizations**.
2. Select the organization you want to enable GluAPI integration for from the drop-down list.
3. Check the **Enable GluAPI** box.
4. Click **Confirm**.
5. Click **Save** and **OK**.

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