Gluware®
Installation Guide for Microsoft® Azure®

Version 3.6
June 10, 2020

NOTE: The information in this guide supersedes the installation and configuration information in Gluware online Help.

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

Table of Contents

About Gluware 3.6

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.
- Support process-oriented activities across devices with **Workflows**.
- Model and manage configurations for devices with **Model Editor**.
- Install the latest OS on one or many devices using **File Server** and **OS Manager**.
- 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 Export**, and **Solutions Management**
- **Config Drift and Audit**
- **OS Manager** – Includes **File Server**
- **Workflows**
- **Model Editor**

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.

Contact us

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

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 are 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 3.6.a.

Product dependencies and compatibility

Host Operating System

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

Browser

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

Other browsers may work, but the user experience may vary. Users experiencing issues with other browsers should verify their issue on the most recent version of Google Chrome before contacting support.

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 replica server and any standalone Gluware servers. Once you determine your optimal Gluware configuration, ensure you have adequate platform resources.

Here are the steps involved:

Step 1. Determine your configuration and resources required

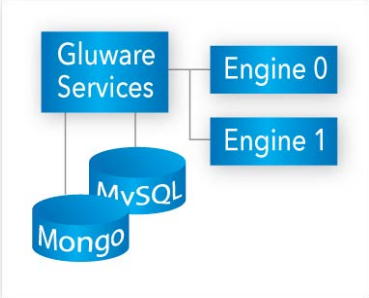
Step 2. Gather platform details

Step 3. Create the primary Gluware server

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	16 GB	32 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.

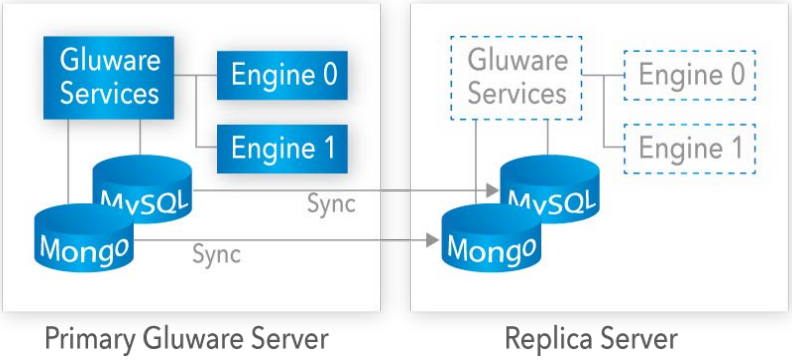
*OS and applications need a minimum of 20 GB. The rest is intended for data.

Port	**Use**
80/443 TCP	Gluware system
1812-1813 UDP & TCP	RADIUS (if using Gluware RADIUS)
465	Outgoing SMTP mail over SSL
123	NTP (if using Gluware NTP)
25	SMTP non-encrypted
22	SSH
5672 and 27017	Inbound communication if connecting to a standalone Gluware engine

Gluware primary server + replica server

Adding a replica server provides a backup of your Gluware primary server and is a disaster recovery option. The replica 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
- Replica server



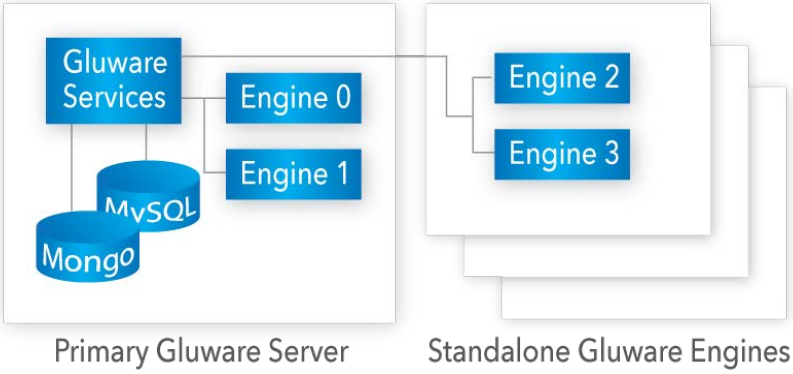
A replica server can be added to your Gluware implementation at any time. The resources required for the replica server must match those of your Gluware primary server.

Gluware primary server + standalone Gluware engine(s)

Adding standalone Gluware engines offers scalability. Standalone engines help improve Gluware performance on large networks by increasing the number of simultaneous jobs that can be run. However, there is no advantage to adding standalone engines in different regions. And distributing them geographically could potentially slow down provisioning.

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

- Gluware primary server
- 1–*n* standalone Gluware engines(s)



Standalone engines can be added to your Gluware system when the need for faster processing arises. You'll need the following resources for each standalone engine 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.

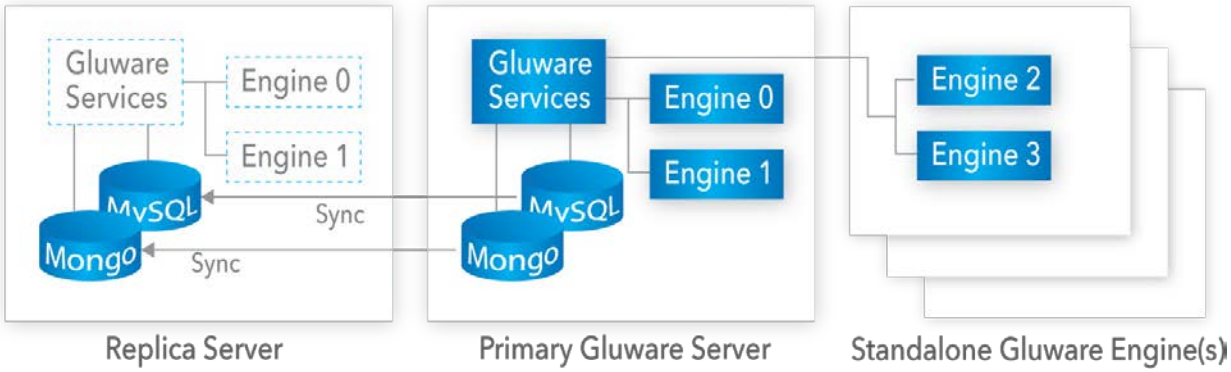
*OS and applications need a minimum of 20 GB. The rest is intended for data.

Port	Use
80/443 TCP	Gluware system
22	SSH

Gluware primary server + replica server + standalone Gluware engine(s)

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

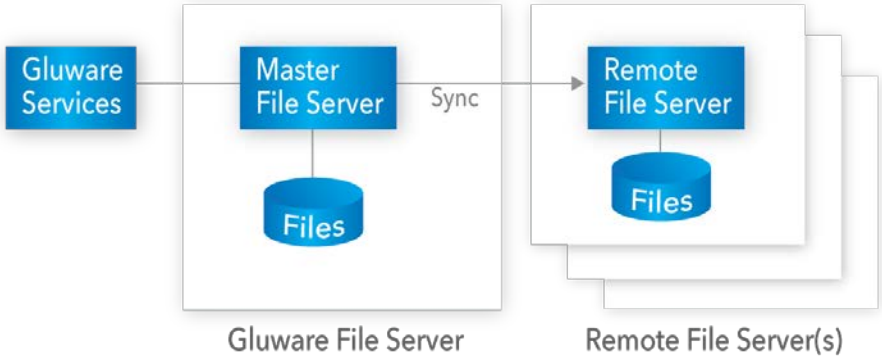
- Gluware primary server
- Replica server
- 1–*n* standalone Gluware engines(s)



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 master file server
- 0–*n* remote file servers



NOTE: Remote **file servers** cannot also be used as standalone engines since they must be on two different VMs.

For each **file server** (master 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

Port	**Use**
22	SSH
21	FTP
60/UDP	TFTP
2022 or user-specified	SSH for server administration

Step 2. Gather platform details

For the **primary Gluware server** installation and configuration, you'll need the following:

Component	Specifications
Public Key	SSH key for the gluadmin user's authentication to the Gluware server
Microsoft Azure virtual network, subnet, and resource group	The virtual network, subnet, and resource group need to be created in the same region in which you will create the primary Gluware server, prior to creating the server
Gluware System Name	The name that will uniquely identify this Gluware system
Gluware Administrative Password	The password used by the system administrator to access the Gluware system
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
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 the Gluware system

For **replica server** and **standalone Gluware engine** configurations, collect the following information:

Component	**Specifications**
Public Key	SSH key for the gluadmin user
IP Address for the primary Gluware server	The private IP address for the primary Gluware server when it was first installed and configured – NOT the CentOS Host System IP Address of the standalone Gluware engine

Next step: Create the primary Gluware server

Step 3. Create the primary Gluware server

Before creating the Gluware VM in the Azure Marketplace, you'll need to have the following in Microsoft Azure:

- Your virtual network
- Subnet
- Resource group

In creating the VM for the primary Gluware server, you'll be configuring the general Gluware administrative settings, including:

- The system administrator account to access the Gluware system, replica server, or standalone engine
- Security and IP address
- SMTP mail details used for notifications from Gluware during runtime

> **NOTE:** You must fully configure the primary Gluware server before configuring a replica server, standalone engine, or file server.

Get the Gluware offer

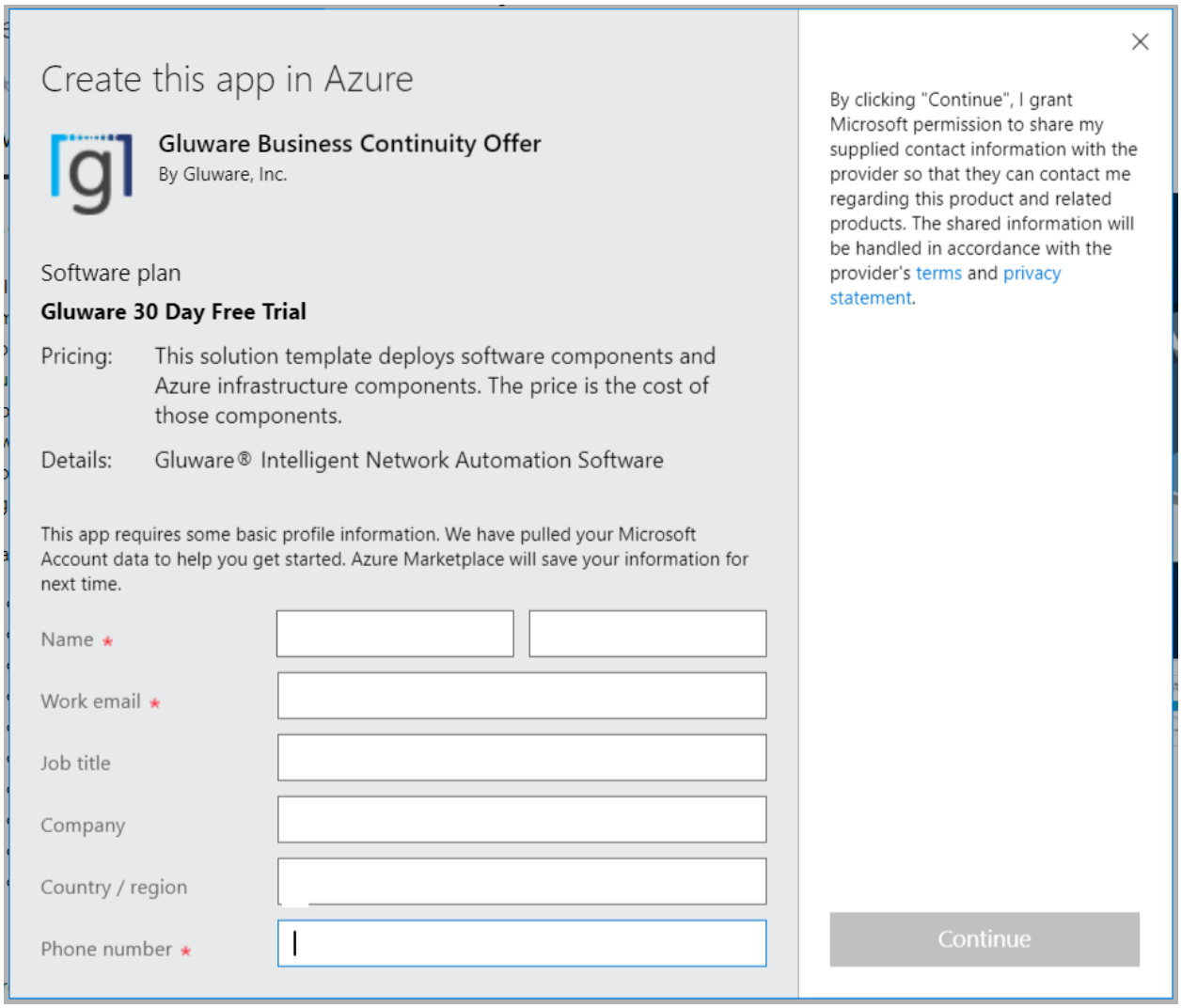
If you are an existing Microsoft Azure customer, get the Gluware offer from the Azure Portal. Otherwise, get the offer from the Azure Marketplace.

From the Azure Portal

1. Sign in to the Azure Portal (https://portal.azure.com/).
2. Search for **Marketplace**.
3. Search for **Gluware**.
4. Click on the **Gluware Business Continuity Offer** for your Primary Gluware server and number of devices.
5. On the Overview page, click **Create**.

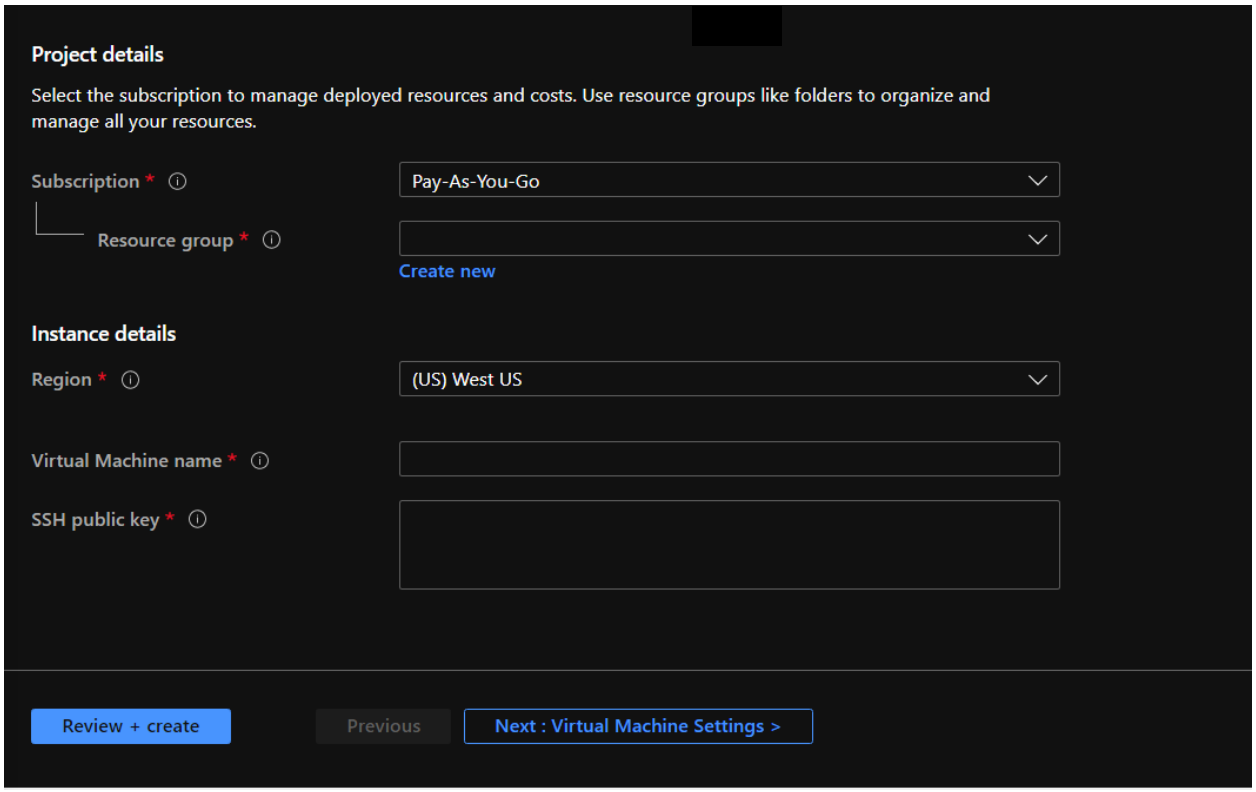
From the Azure Marketplace

1. Go to the Azure Marketplace (https://azuremarketplace.microsoft.com/en-us/).
2. Search for **Gluware**.
3. Find the **Gluware Business Continuity Offer** for your Primary Gluware server and number of devices and click **Get it now**.
4. Click **Continue**.



5. Provide your contact details including your first and last name, work email address, and phone number.
6. Click **Continue**.
7. On the Overview page, click **Create**.

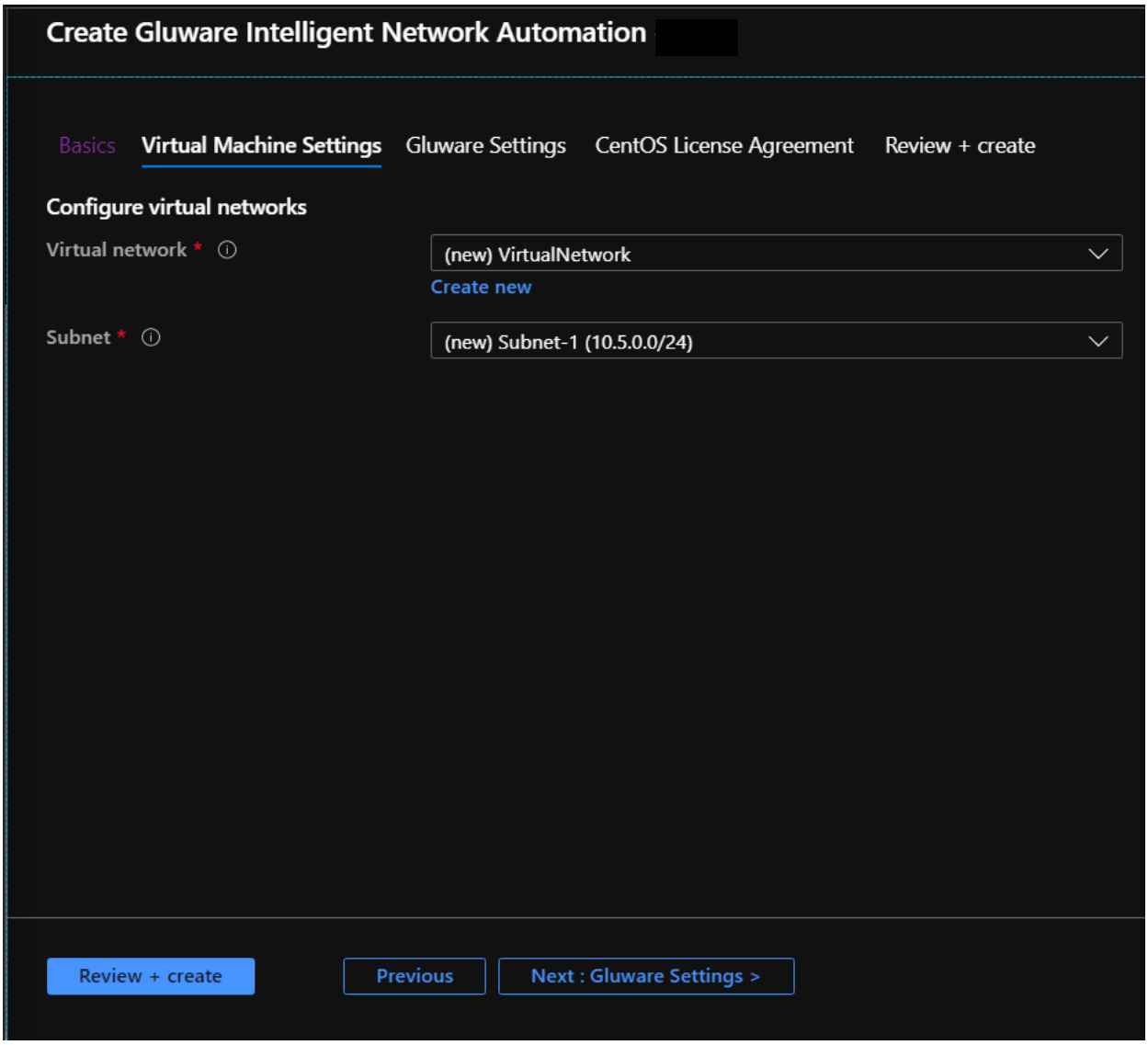
Create the VM



1. Select your resource group.

WARNING! Do not select **Create new**.

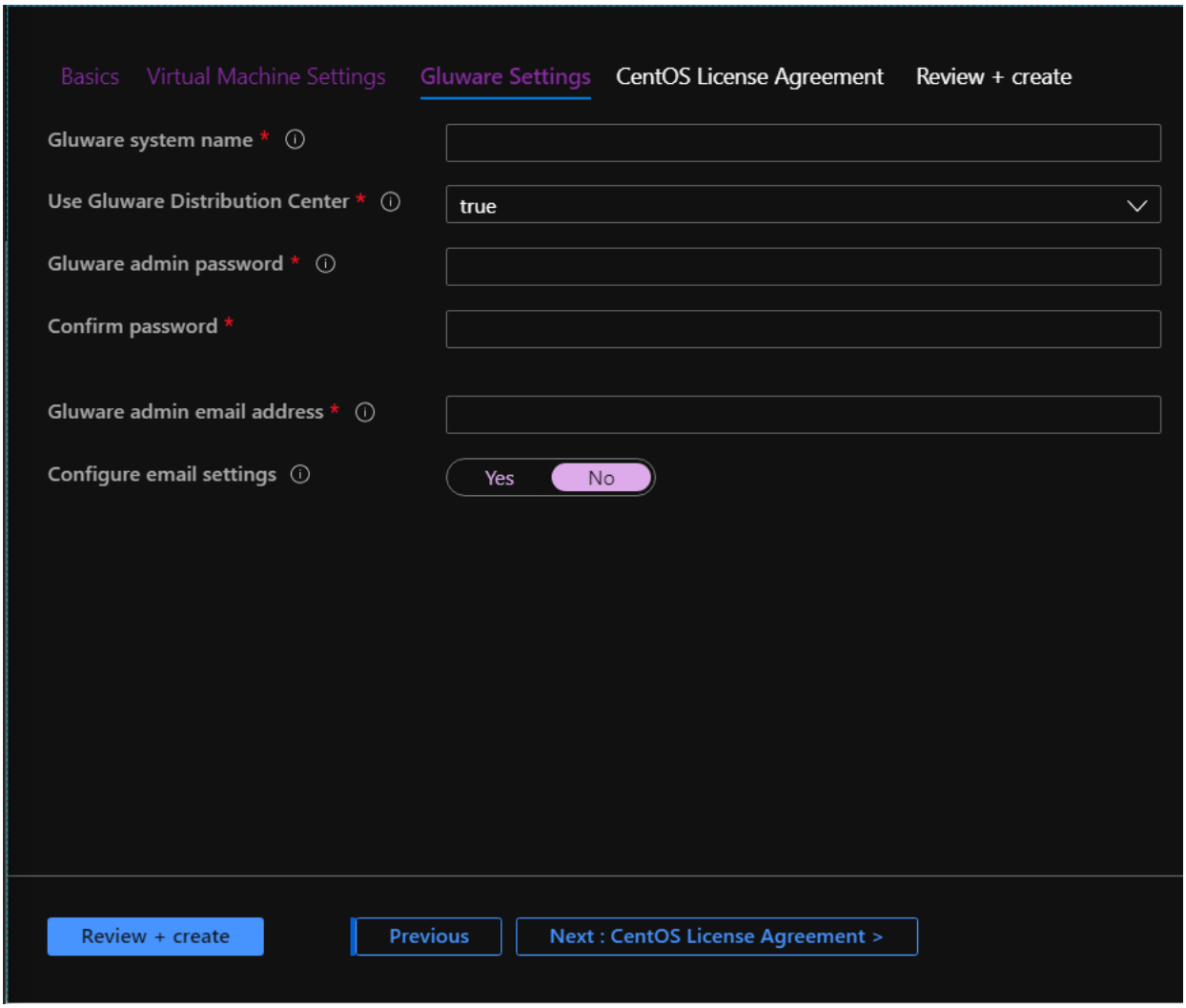
2. Select the region that corresponds to the resource group.
3. Name your virtual machine. The name **cannot** contain uppercase letters.
4. Enter the **SSH public key** for authentication to the Gluware server. You'll need to generate your SSH public key. For example, use PuTTYgen (https://www.ssh.com/ssh/putty/windows/puttygen).
5. Click **Next: Virtual Machine Settings**.



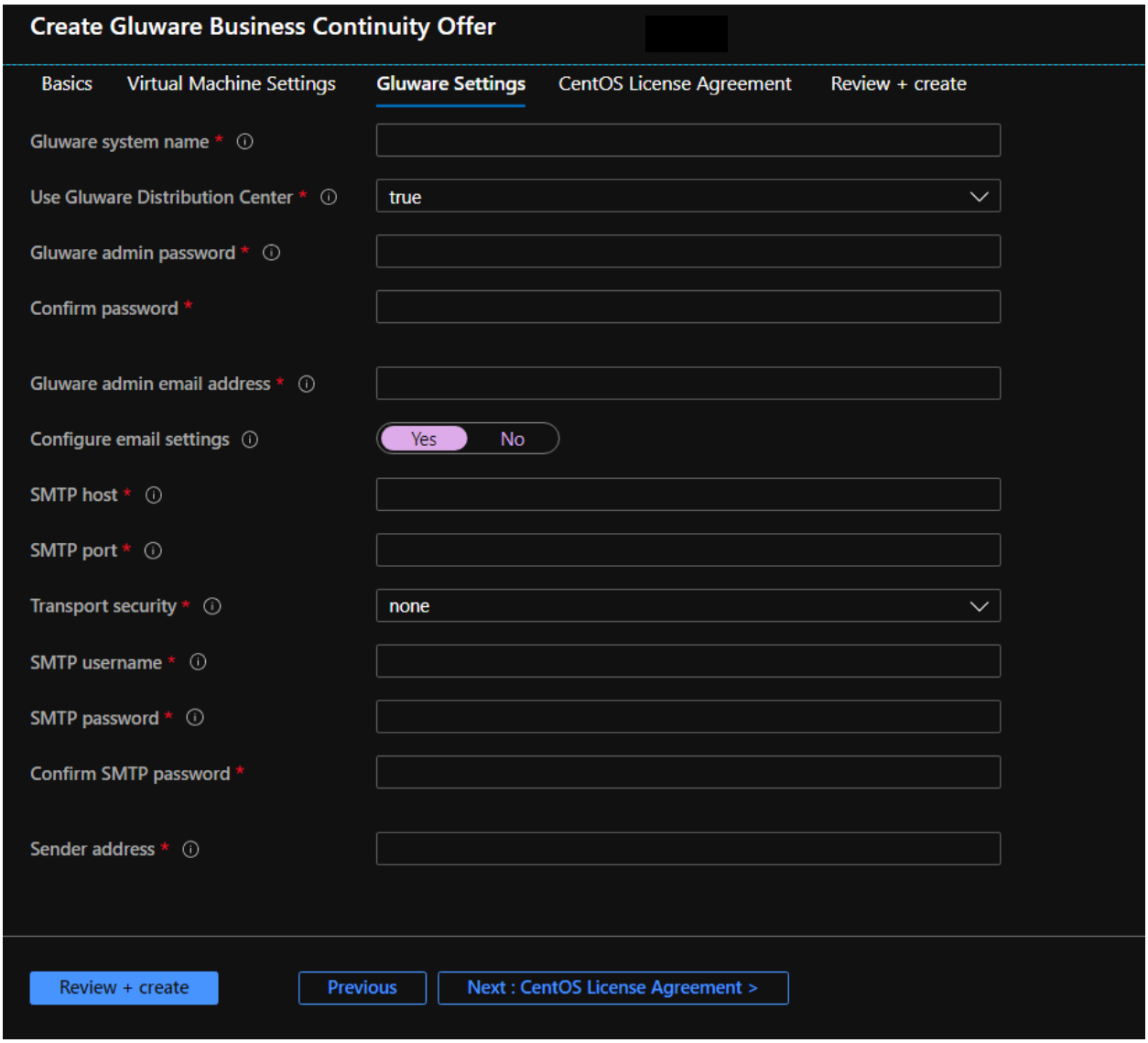
6. Select your virtual network from the drop-down list.

WARNING! Do not select **Create new**.

7. Select a subnet from the drop-down list.
8. Click **Next: Gluware Settings**.



9. Enter the **Gluware system name.** This is the name used to identify this Gluware system.
10. Select **Use Gluware Distribution Center** if you will be using the Gluware Distribution Center for Feature updates (recommended).
11. Enter the **Gluware admin password**. This is the password for the Gluware admin user. Choose a strong password to protect access to the Gluware system.
12. Confirm the password.
13. Enter the **Gluware admin email address**. This is the email address for the Gluware admin user.



14. Click **Yes** to configure Gluware email settings.

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*>. For example, Gluware <notify@yourcorp.com>. The user would receive the email from Gluware, but the reply would go to notify@yourcorp.com.

a. Enter the **SMTP host**. This is the host name or IP address for the mail server.

b. Enter the **SMTP port**, the port number for SMTP traffic.
c. Select the **Transport security** (SSL or TLS encryption) to secure traffic.
d. Enter the **SMTP username**. This is the user account used to authenticate with the SMTP server when sending emails.
e. Enter the **SMTP** password, the password for the SMTP username account.
f. Confirm the SMPT password.
g. Enter the **Sender** address, the return email address for any mail generated from Gluware.

15. Click **Next: CentOS license Agreement**. By clicking **Next** on this screen, you accept the CentOS License Agreement.
16. Click **Next: Review + create**. Your settings are validated.
17. Click **Create**.
18. Wait until you see the message, "Your deployment is complete."
19. Optional: Click **Download** to see the Deployment details.
20. Go to https://portal.azure.com/#home.
21. Select **Virtual Machines** and then select the VM you created to see the details.
22. Copy the **Public IP address**. This is the address you'll use to connect to Gluware using your Chrome browser.
23. Click on **Networking** under **Settings**. Review the inbound and outbound firewall settings and make changes as necessary.

NOTES: It takes a few minutes to complete the installation of Gluware once the VM is created.

To use SSH to connect to the primary Gluware server, use the username "gluadmin" and the SSH public key.

Gluware configuration overview

Step 1. Set up organizations and user authentication

Step 2. Install your Gluware licenses

Step 3. Set up data retention

Step 4. Set up scheduled backups

Step 5. Install packages

Then, depending on your configuration, install and configure the following additional servers:

Gluware replica server

Standalone Gluware engine

Master file server

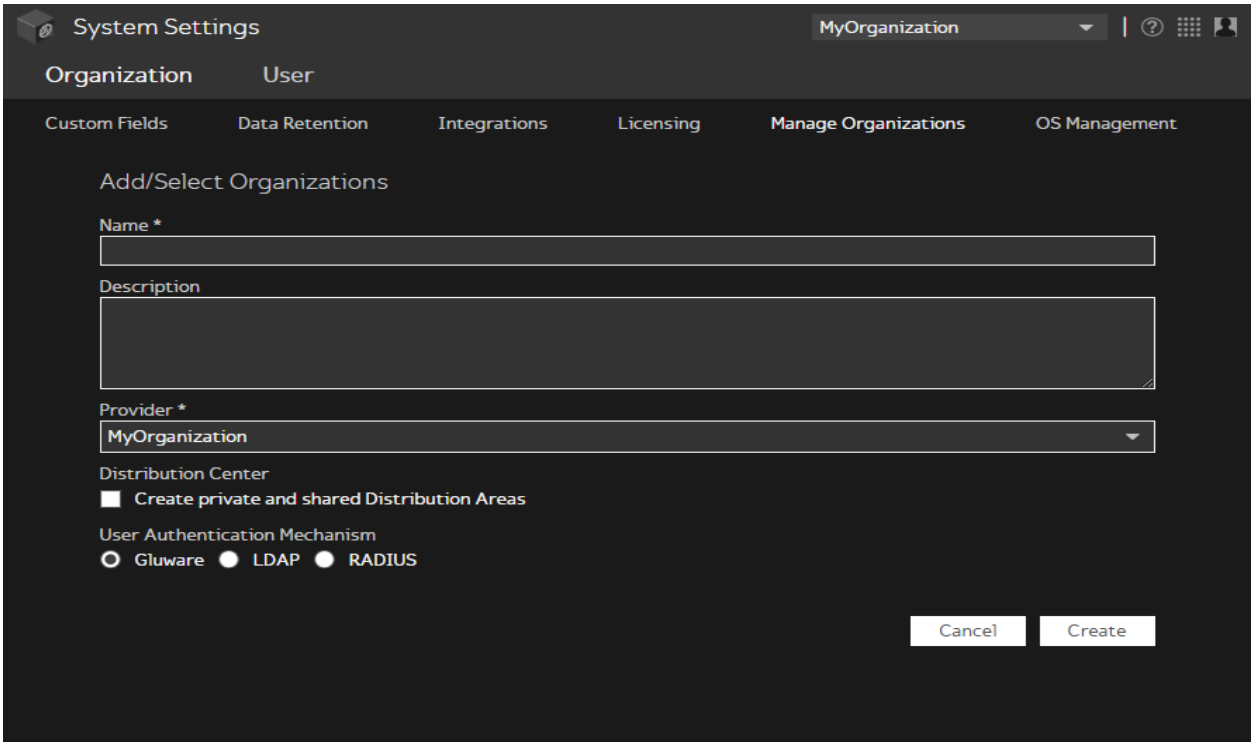
Remote file server

Step 1. 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.
2. Go to **System Settings**.
3. Select **Organization** > **Manage 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. Select a user authentication mechanism:
    - Select **Gluware** to set up users one-by-one and click **Create**. **Next:** Install your Gluware licenses
    - Select **LDAP** or **RADIUS** to use your existing user credentials and continue to Configure Gluware to interact with LDAP or Configure Gluware to interact with RADIUS.

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.

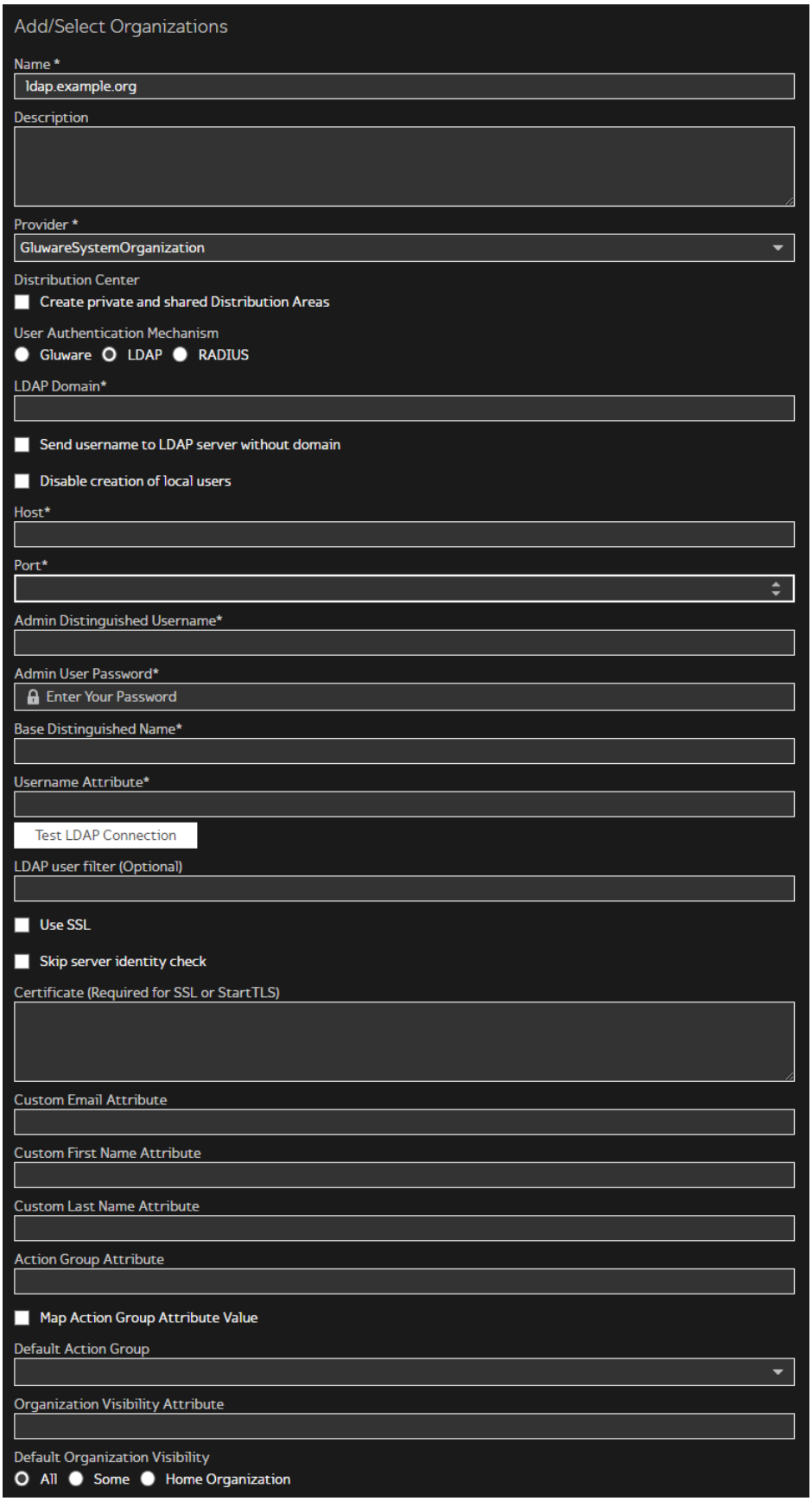
The user authentication process in Gluware determines if, and how, to map an LDAP user with a Gluware user for the following scenarios:

- 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.


Add/Select Organizations
Name *
ldap.example.org
Description
Provider *
GluwareSystemOrganization
Distribution Center
Create private and shared Distribution Areas
User Authentication Mechanism
Gluware
LDAP
RADIUS
LDAP Domain*
Send username to LDAP server without domain
Disable creation of local users
Host*
Port*
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
Action Group Attribute
Map Action Group Attribute Value
Default Action Group
Organization Visibility Attribute
Default Organization Visibility
All
Some
Home Organization

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
Send username to LDAP server without domain	Strips the @domain.org off the username. Users still sign in to Gluware using user@domain.org.
Disable creation of local users	Limits new users to only those in LDAP
Host	Host name or IP address of the LDAP server. If you are using LDAPS, this name should match the server certificate
Port	Port of the LDAP server: 389 or 636 (SSL)
Admin Distinguished Username	Read-only Admin Distinguished 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
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

Field	Description
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))
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
Custom First Name Attribute	LDAP attribute name where a user's first name is stored in a user entry. **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

Field	Description
Custom Last Name Attribute	LDAP attribute name where a user's last name is stored in a user entry. **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
Action Group Attribute	Optional LDAP attribute used to set the Gluware Action Group; for example, memberOf
Map Action Group Attribute Value	When selected, allows you to create up to five LDAP security groups and map each group to a Gluware Action Group
Default Action Group	If the Action Group is not specified, or the LDAP user entry does not include the Action Group Attribute, then this will be the default Action Group given to a new Gluware user
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
Default Organization Visibility	If the Control Org Visibility is not specified, or the LDAP user entry does not include the Org Visibility Attribute, then this will be the default Org Visibility given to a new Gluware user. This can be a string with a value of "ALL" or "HOME" or an object with organization IDs as its keys

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.

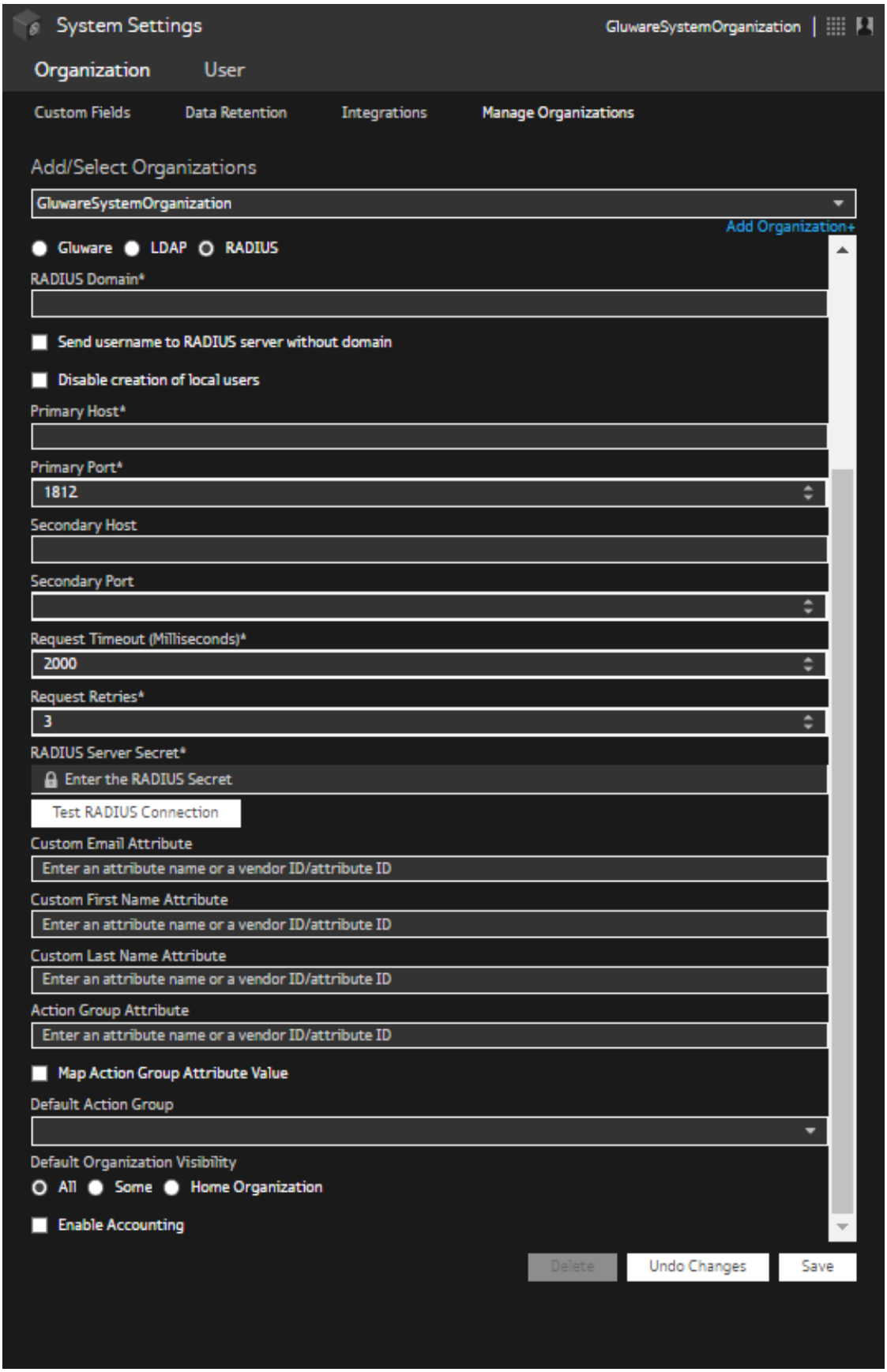
The user authentication process in Gluware determines if, and how, to map a RADIUS user with a Gluware user for the following scenarios:

- 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.


System Settings
GluwareSystemOrganization
Organization
User
Custom Fields
Data Retention
Integrations
Manage Organizations
Add/Select Organizations
GluwareSystemOrganization
Add Organization+
Gluware
LDAP
RADIUS
RADIUS Domain*
Send username to RADIUS server without domain
Disable creation of local users
Primary Host*
Primary Port*
1812
Secondary Host
Secondary Port
Request Timeout (Milliseconds)*
2000
Request Retries*
3
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
Action Group Attribute
Enter an attribute name or a vendor ID/attribute ID
Map Action Group Attribute Value
Default Action Group
Default Organization Visibility
All
Some
Home Organization
Enable Accounting
Delete
Undo Changes
Save

Field	Description
RADIUS Domain	The unique domain name all users of the organization include in their username when signing in to Gluware. For example, t the user jandy@gluware.com has an RADIUS domain of gluware.com
Send username to RADIUS server without domain	Strips the @domain.org off the username. Users still sign in to Gluware using user@domain.org.
Disable creation of local users	Limits new users to only those in RADIUS
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
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	Read-only Admin Distinguished Username used to search for user entries. **Note**: If you supply a value for Custom Email Attribute, the field will NOT be editable,

Field	Description
	and you cannot override the value pulled from RADIUS
Custom First Name Attribute	A RADIUS attribute, including vendor-specific attributes, where a user's first name is stored. **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	A RADIUS attribute, including vendor-specific attributes, where a user's last name is stored. **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
Action Group Attribute	Optional LDAP attribute used to set the Gluware Action Group; for example, memberOf
Map Action Group Attribute Value	When selected, allows you to create up to five LDAP security groups and map each group to a Gluware Action Group
Default Action Group	If the Action Group is not specified, or the LDAP user entry does not include the Action Group Attribute, then this will be the default Action Group given to a new Gluware user
Default Organization Visibility	If the Control Org Visibility is not specified, or the RADIUS user entry does not include the Org Visibility Attribute, then this will be the default Org Visibility given to a new Gluware user. This can be a string with a value of "ALL" or "HOME" or an object with organization IDs as its keys
Enable Accounting	Enables record keeping of sign in/sign off activity

Step 2. Install your Gluware licenses

Gluware licenses are used to manage:

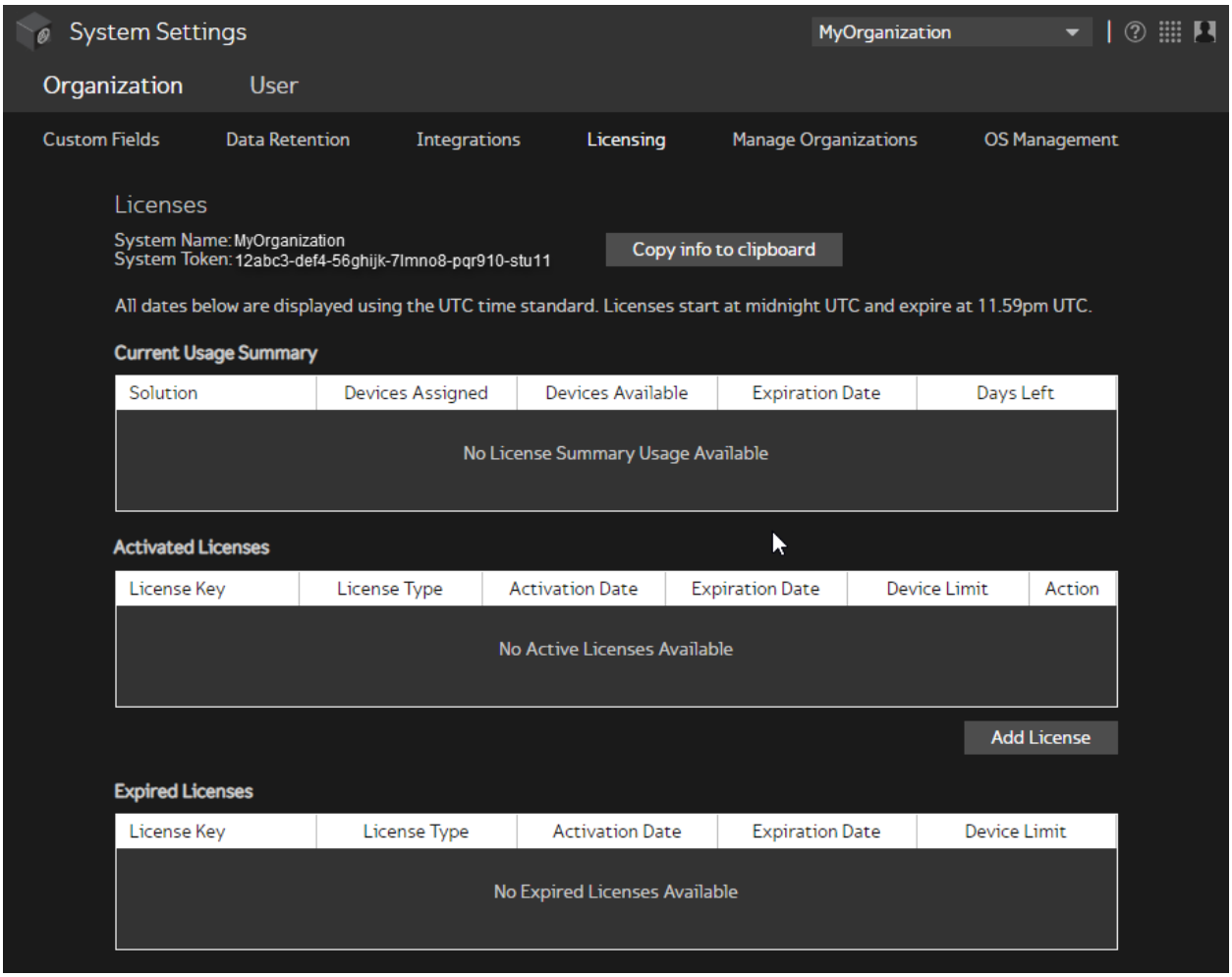
- The Gluware solutions available to you
- The maximum number of devices in your Gluware system
- The expiration date of your evaluation period or product licenses

Install Gluware and create your organization structure. Then obtain one or more Gluware licenses and activate the 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.

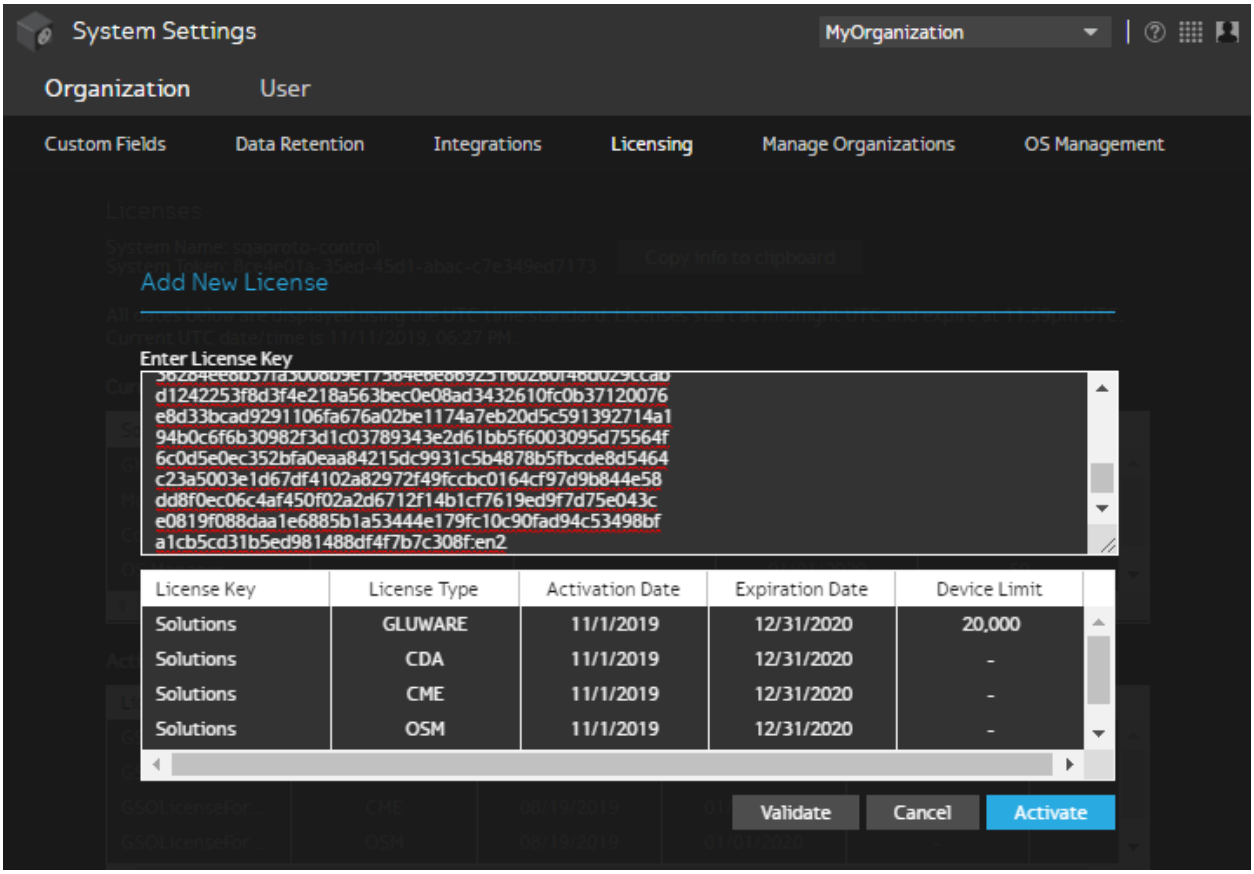
Request your license key from Gluware

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 **Systems 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



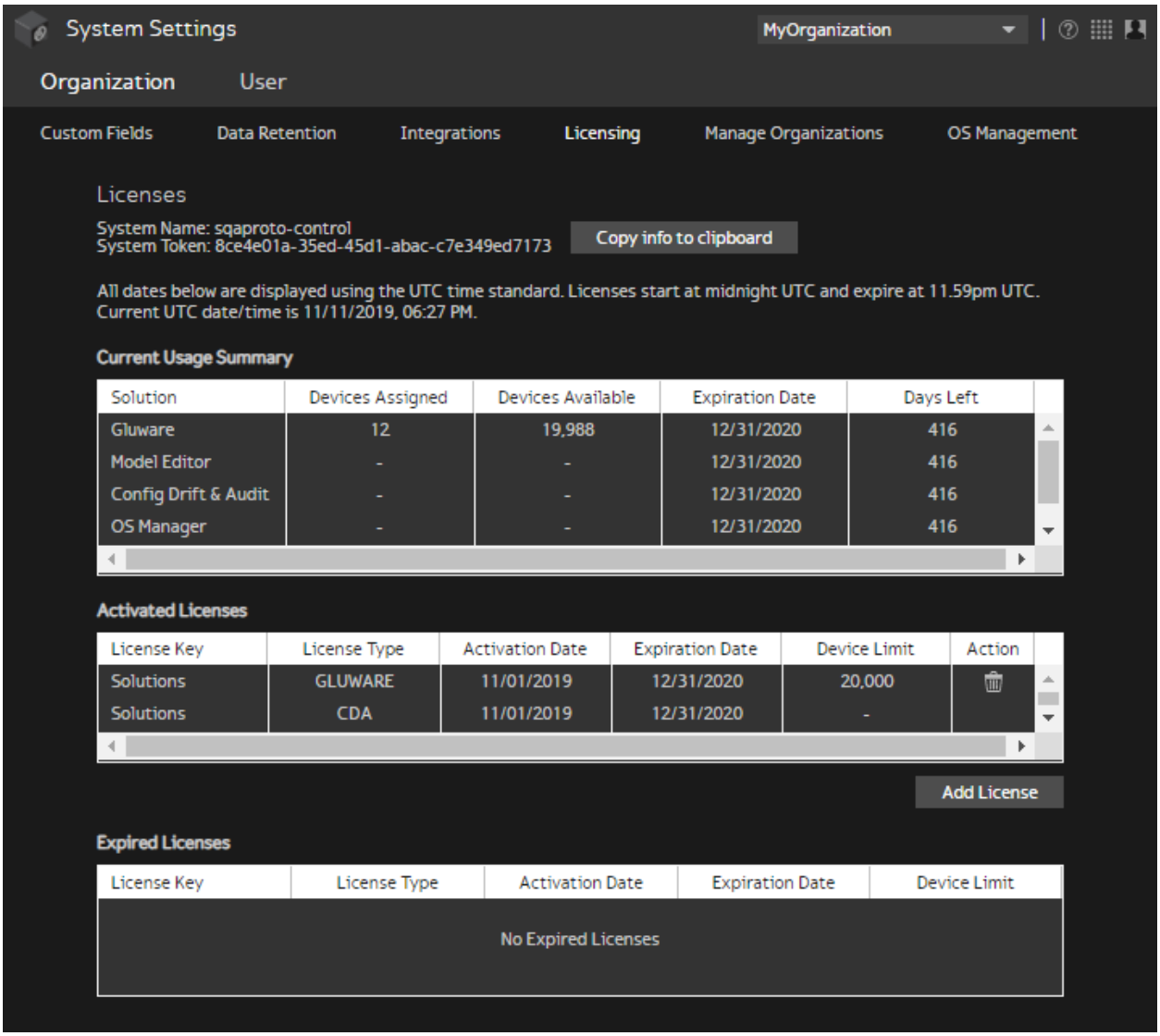
Install your license key

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 **Systems Settings** and select **Organization** > **Licensing**.
3. Click **Add License**.
4. Paste the license key 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 3. Set up data retention

Set up data retention and archiving for key activities. 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 are in the organization you want to set up data retention for.
2. Go to Gluware **System 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.
    - Select **Manual** to only run the policy at will.
    - Select **Scheduled** and set the frequency to automate the policy.
4. Specify the maximum number of records to retain for a device by double-clicking the **Count** cell.
5. Specify the maximum age of the records to be retained by double-clicking the **Age** cell. Entering **0** for **Age** disables age-based retention.
6. Double-click the **Archive** cell and check the box to create a text file of the purged data. If **Archive** is not selected, no text file is created when the data is purged.
7. Save.

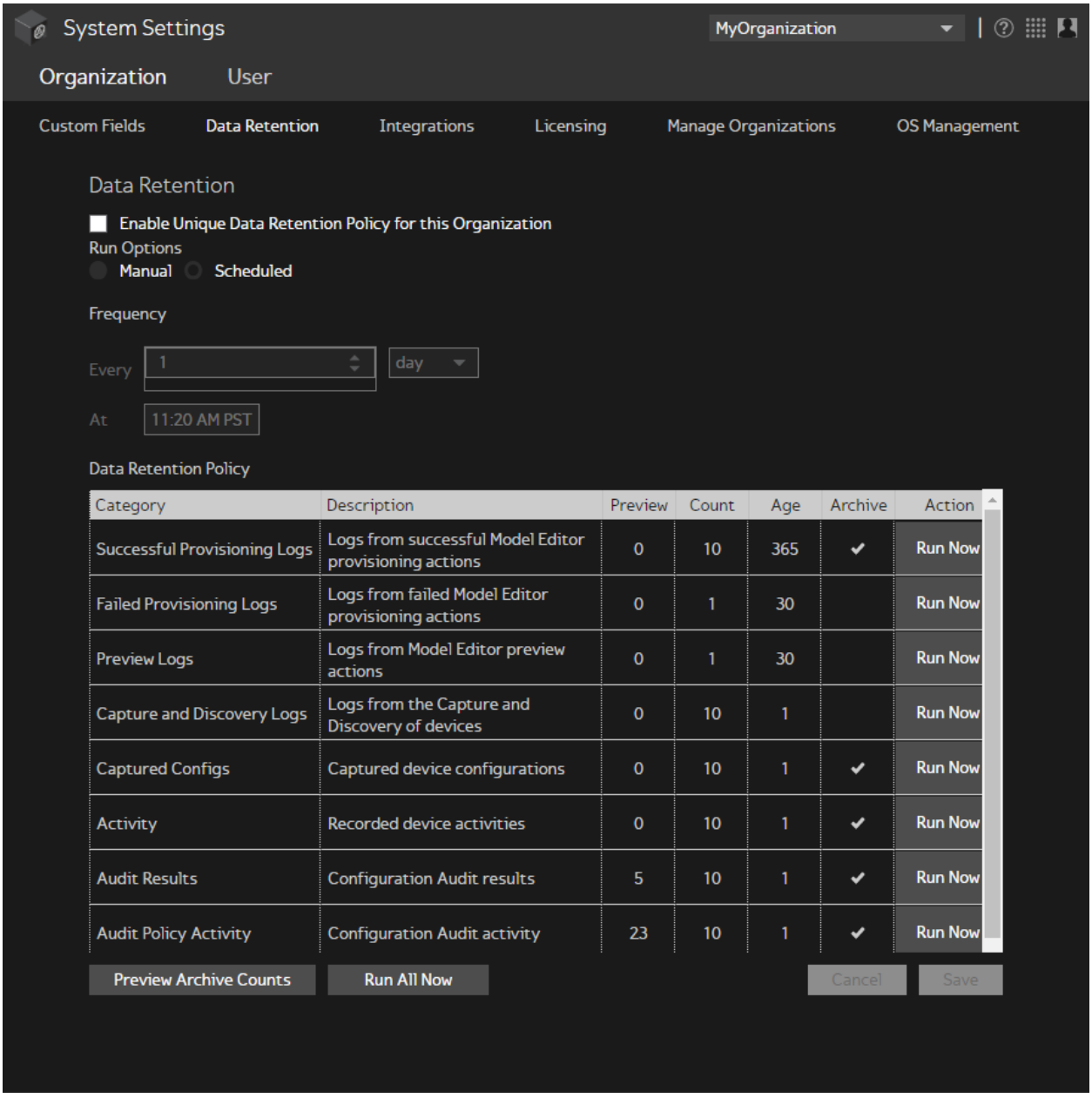
> **NOTE:** Archive files generated by data retention are not backup files that can be reinstalled or used by Gluware. They are text files for offline use.

Best practices

The use of Data Retention is strongly encouraged, as it eliminates much of the ephemeral data generated because of testing or failures. As an 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.

Think carefully about what makes realistic sense for your organization to reduce confusion and keep Gluware running optimally.



Function	Description
Category	Activity or status that details and logs are stored for: **Successful Provisioning Logs** started in Model Editor **Failed Provisioning Logs** started in Model Editor **Preview Logs** started in Model Editor **Capture and Discovery Logs** started in Config Drift or in Device Manager **Captured Configs** started in Config Drift **Activity** started in Config Drift and Audit or in Device Manager **Audit Results** started in Config Audit **Audit Policy Activity** started in Config Audit **Schedule Activity and History** for any scheduled activity **Exhausted Schedules** history
Description	Details for the category
Preview	Number of records that would be archived and purged or simply purged based on the current retention policy. Populated by clicking **Preview Archive Counts**
Count	Maximum number of records to retain for each device (e.g., If count = 10, then the 11th and subsequent entries will be archived and purged or simply purged)
Age	Maximum age for the record to be retained (e.g., If age = 30, then entries older than 30 days will be archived and purged or only purged) 0 disables retention
Archive	Specifies whether records that meet the criteria will be archived as a text file and purged (deleted)
Action	Runs the archive-and-purge or purge-only action now. Double-click in the cell and then click **Confirm**
Preview Archive Counts	Populates the count in the Preview column

Function	Description
Run All Now	Runs the entire data retention policy for the current organization

Next step: Set up scheduled backups

Step 4. 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 username “gluadmin” and the public key. 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 5. Install packages

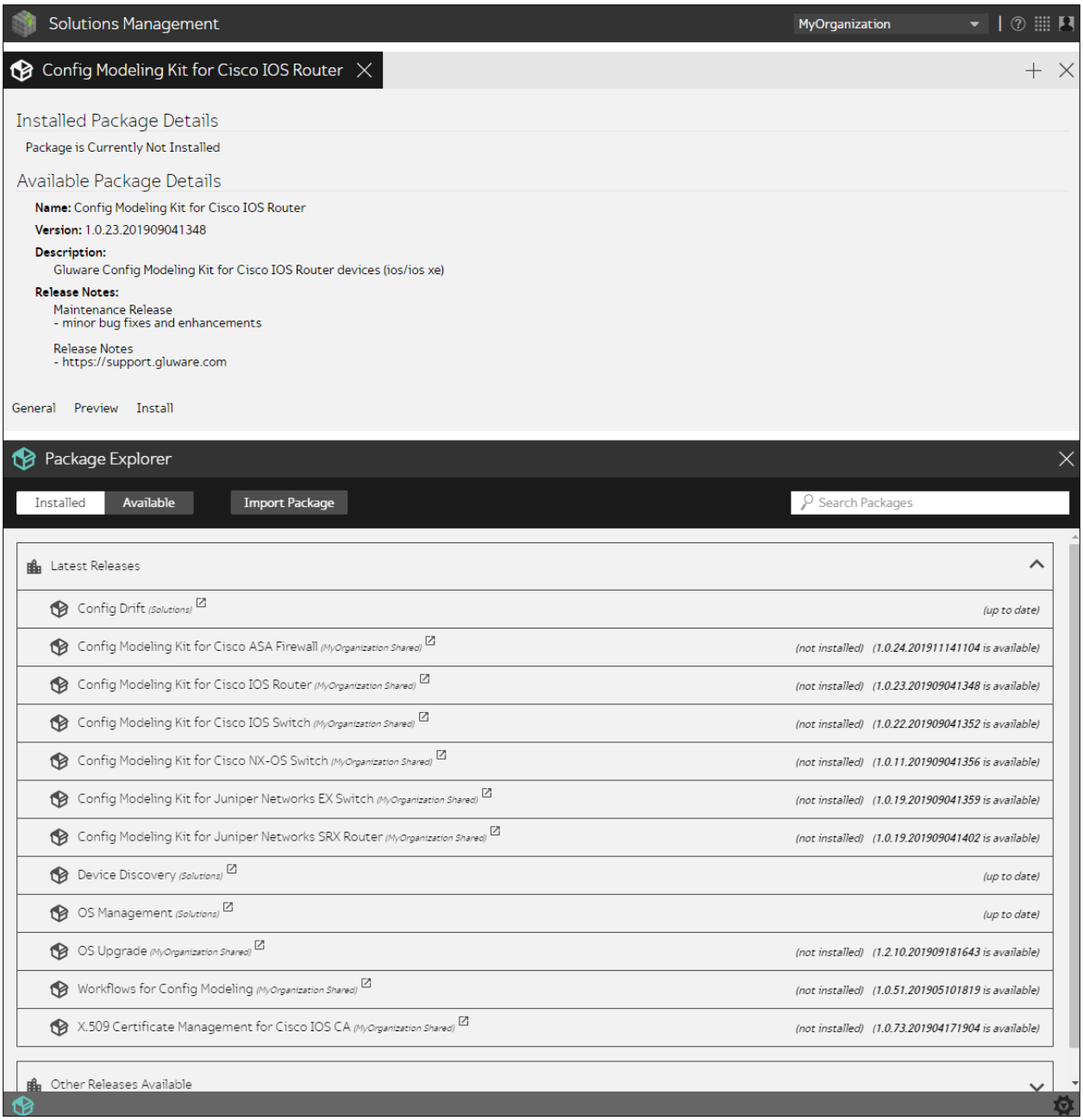
You can install any combination of features and capabilities you have licensed from Gluware in any organization you have created.

- 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 Management** 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 **Model Editor** 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.


Solutions Management
MyOrganization
Config Modeling Kit for Cisco IOS Router
Installed Package Details
Package is Currently Not Installed
Available Package Details
Name: Config Modeling Kit for Cisco IOS Router
Version: 1.0.23.201909041348
Description:
Gluware Config Modeling Kit for Cisco IOS Router devices (ios/ios xe)
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)
Other Releases Available

Configure a Gluware replica server

Set up the primary Gluware server completely before you configure the replica server.

Get the Gluware offer

If you are an existing Microsoft Azure customer, get the Gluware offer from the Azure Portal. Otherwise, get the offer from the Azure Marketplace.

From the Azure Portal

1. Sign in to the Azure Portal (https://portal.azure.com/).
2. Search for **Marketplace**.
3. Search for **Gluware**.
4. Click on the **Gluware Business Continuity Offer** for your Gluware replica server and number of devices.
5. On the Overview page, click **Create**.

From the Azure Marketplace

1. Go to the Azure Marketplace (https://azuremarketplace.microsoft.com/en-us/).
2. Search for **Gluware**.
3. Find the **Gluware Business Continuity Offer** for your Gluware replica server and click **Get it now**.
4. Provide your contact details including your first and last name, work email address, and phone number.
5. Click **Continue**.
6. On the Overview page, click **Create**.

Create the VM

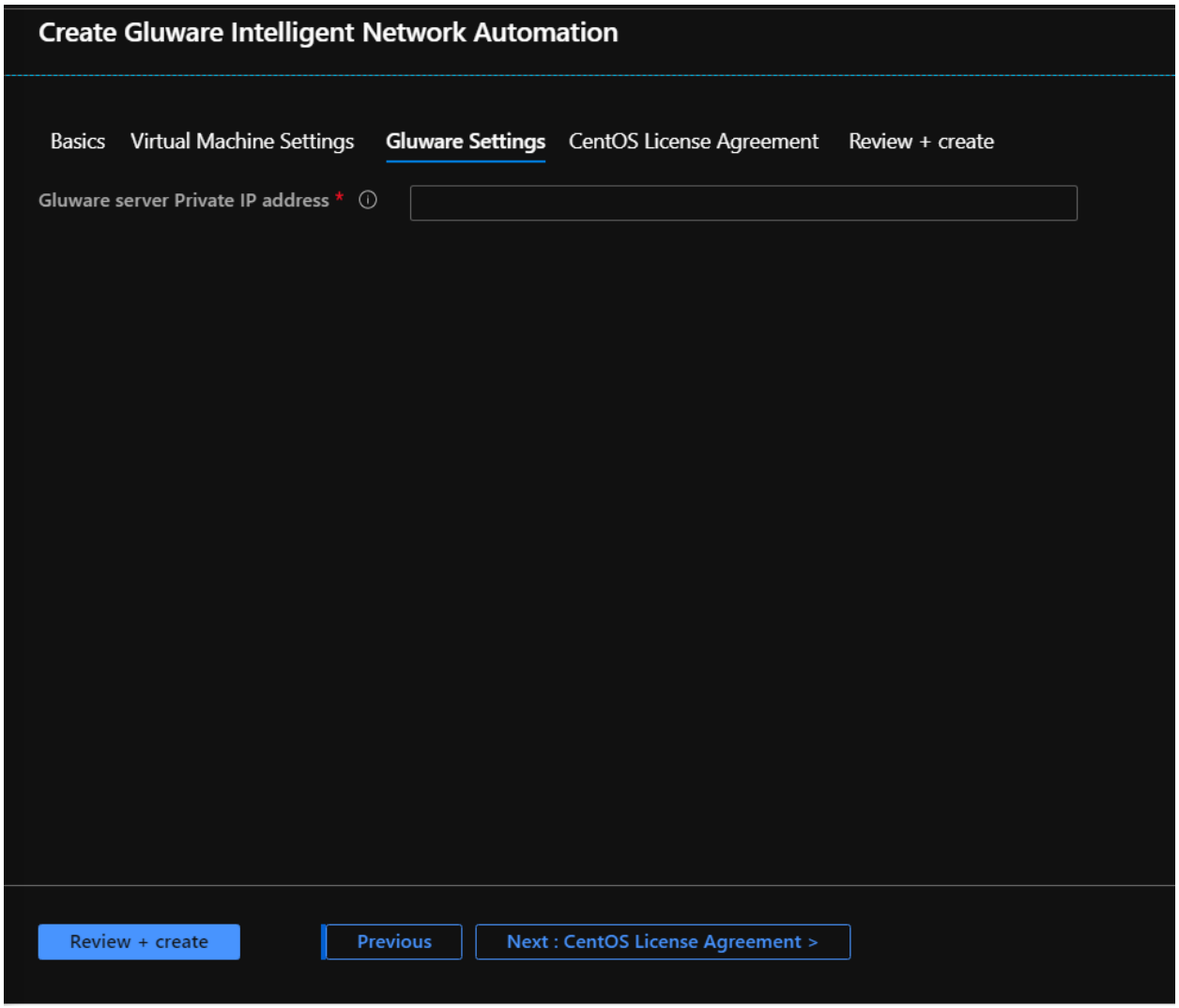
1. Select your resource group.

> **WARNING!** Do not select **Create new**.

2. Select the region that corresponds to the resource group.
3. Name your virtual machine. The name **cannot** contain uppercase letters.
4. Enter the **SSH public key** for authentication. You'll need to generate your SSH public key. For example, use PuTTYgen (https://www.ssh.com/ssh/putty/windows/puttygen).
5. Click **Next: Virtual Machine Settings**.
6. Select your virtual network from the drop-down list.

> **WARNING!** Do not select **Create new**.

7. Select a subnet from the drop-down list.
8. Click **Next: Gluware Settings**.



9. Enter the private IP address for the primary Gluware server.
10. Click **Next: CentOS license Agreement**. By clicking **Next** on this screen, you accept the CentOS License Agreement.
11. Click **Next: Review + create**. Your settings are validated.
12. Click **Create**.
13. Wait until you see the message, "Your deployment is complete."
14. Optional: Click **Download** to see the Deployment details.
15. Go to https://portal.azure.com/#home.
16. Select **Virtual Machines** and then select the VM you created to see the details.
17. Click on **Networking** under **Settings**. Review the inbound and outbound firewall settings and make changes as necessary.

18. Sign in to the primary server via a terminal session and issue the `gluwarectl reconfigure` command for the replica server to be initialized and configured for standby mode.

Configure a standalone Gluware engine

Set up the primary Gluware server completely before you configure a standalone Gluware engine.

Get the Gluware offer

If you are an existing Microsoft Azure customer, get the Gluware offer from the Azure Portal. Otherwise, get the offer from the Azure Marketplace.

From the Azure Portal

1. Sign in to the Azure Portal (https://portal.azure.com/).
2. Search for **Marketplace**.
3. Search for **Gluware**.
4. Click on the **Gluware Business Continuity Offer** for your standalone Gluware engine.
5. On the Overview page, click **Create**.

From the Azure Marketplace

1. Go to the Azure Marketplace (https://azuremarketplace.microsoft.com/en-us/).
2. Search for **Gluware**.
3. Find the **Gluware Business Continuity Offer** for your standalone Gluware engine and click **Get it now**.
4. Provide your contact details including your first and last name, work email address, and phone number.
5. Click **Continue**.
6. On the Overview page, click **Create**.

Create the VM

1. Enter the private IP address for the primary Gluware server.
2. Click **Next: CentOS license Agreement**. By clicking **Next** on this screen, you accept the CentOS License Agreement.
3. Click **Next: Review + create**. Your settings are validated.
4. Click **Create**.
5. Wait until you see the message, "Your deployment is complete."
6. Optional: Click **Download** to see the Deployment details.
7. Go to https://portal.azure.com/#home.
8. Select **Virtual Machines** and then select the VM you created to see the details.
9. Click on **Networking** under **Settings**. Review the inbound and outbound firewall settings and make changes as necessary.
10. Sign in to the primary server via a terminal session and issue the `gluwarectl reconfigure` command to enable the standalone Gluware engine.

We recommend that you tune the additional 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 master file server

Each organization can have one **master file server** and any number of **remote file servers**. If an organization does not have a master 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.

Get the Gluware offer

If you are an existing Microsoft Azure customer, get the Gluware offer from the Azure Portal. Otherwise, get the offer from the Azure Marketplace.

From the Azure Portal

1. Sign in to the Azure Portal (https://portal.azure.com/).
2. Search for **Marketplace**.
3. Search for **Gluware**.
4. Click on the **Gluware Business Continuity Offer** for your Gluware master file server.
5. On the Overview page, click **Create**.

From the Azure Marketplace

1. Go to the Azure Marketplace (https://azuremarketplace.microsoft.com/en-us/).
2. Search for **Gluware**.
3. Find the **Gluware Business Continuity Offer** for your Gluware master file server and click **Get it now**.
4. Provide your contact details including your first and last name, work email address, and phone number.
5. Click **Continue**.

6. On the Overview page, click **Create**.

Create the VM

1. Enter the private IP address of the Primary Gluware Control Server.
2. Enter the SSH port for VM administration. Do not use the same SSHP port used for file transfers.
3. Click **Next: CentOS license Agreement**. By clicking **Next** on this screen, you accept the CentOS License Agreement.
4. Click **Next: Review + create**. Your settings are validated.
5. Click **Create**. The file server configuration begins. During this time, it requires communication with the Gluware server. If it can't communicate with Gluware, the configuration will fail.
6. Wait until you see the message, "Your deployment is complete."
7. Optional: Click **Download** to see the Deployment details.
8. Go to https://portal.azure.com/#home.
9. Select **Virtual Machines** and then select the VM you created to see the details.
10. Click on **Networking** under **Settings**. Review the inbound and outbound firewall settings and make changes as necessary.

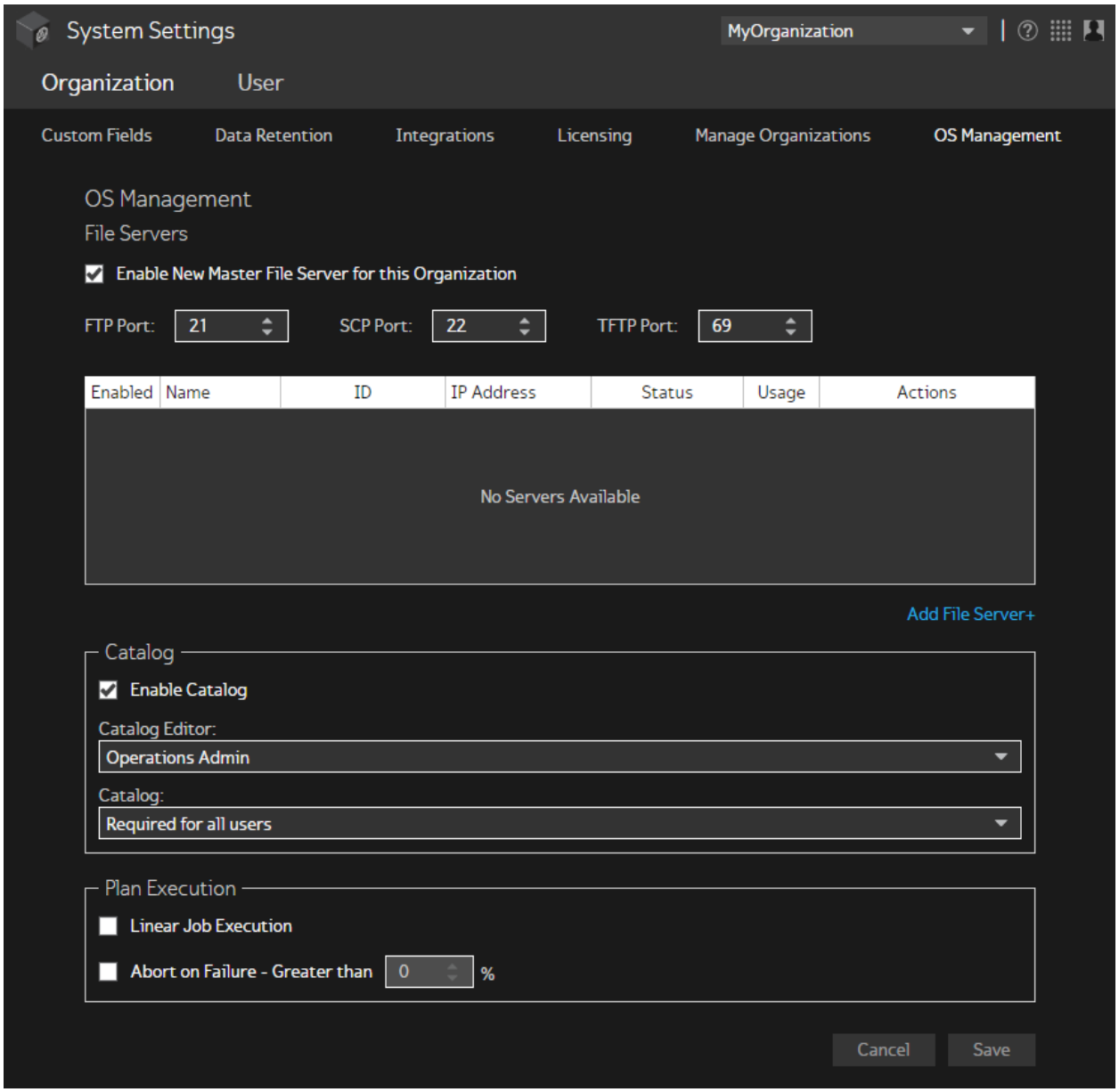
When the configuration of the file server is complete, go to Gluware **System Settings** to set up the file server in Gluware.

Add the file server in Gluware System Settings

1. Go to Gluware **System Settings** and ensure you're in the organization you want to add the master file server to.

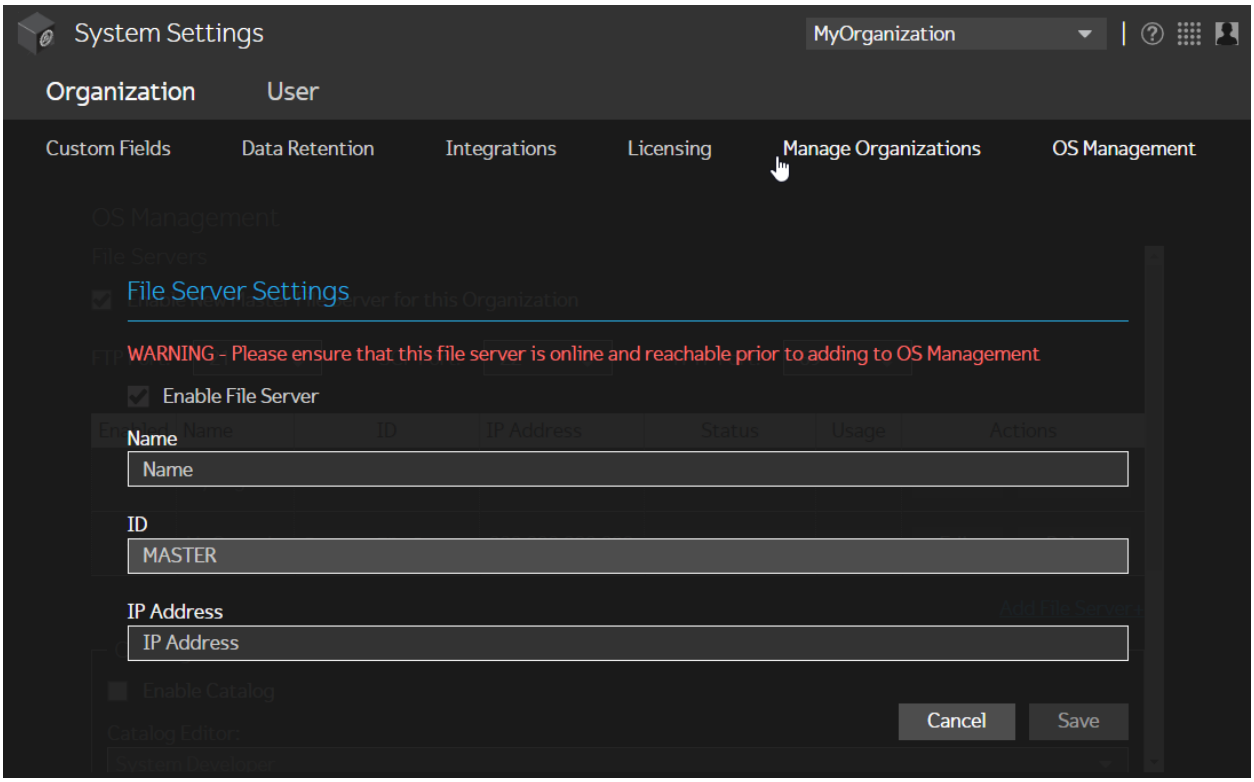
> **NOTE:** The file server will be used by all child organizations unless they have their own file server.

2. Select **Organization** > **OS Management**.



3. If you are adding the master file server in a child organization, check the **Enable New Master File Server for this Organization** box.
4. Ensure the **FTP Port**, **SCP Port**, and **TFTP Port** settings are correct.
5. Click **Add File Server+**.

6. Enter a name and IP address for the master file server.
7. Save.



Configure a remote file server

Configure the master file server before configuring any remote Files Servers.

Get the Gluware offer

If you are an existing Microsoft Azure customer, get the Gluware offer from the Azure Portal. Otherwise, get the offer from the Azure Marketplace.

From the Azure Portal

1. Sign in to the Azure Portal (https://portal.azure.com/).
2. Search for **Marketplace**.
3. Search for **Gluware**.
4. Click on the **Gluware Business Continuity Offer** for your Gluware remote file server.
5. On the Overview page, click **Create**.

From the Azure Marketplace

1. Go to the Azure Marketplace (https://azuremarketplace.microsoft.com/en-us/).
2. Search for **Gluware**.
3. Find the **Gluware Business Continuity Offer** for your Gluware remote file server and click **Get it now**.
4. Provide your contact details including your first and last name, work email address, and phone number.
5. Click **Continue**.
6. On the Overview page, click **Create**.

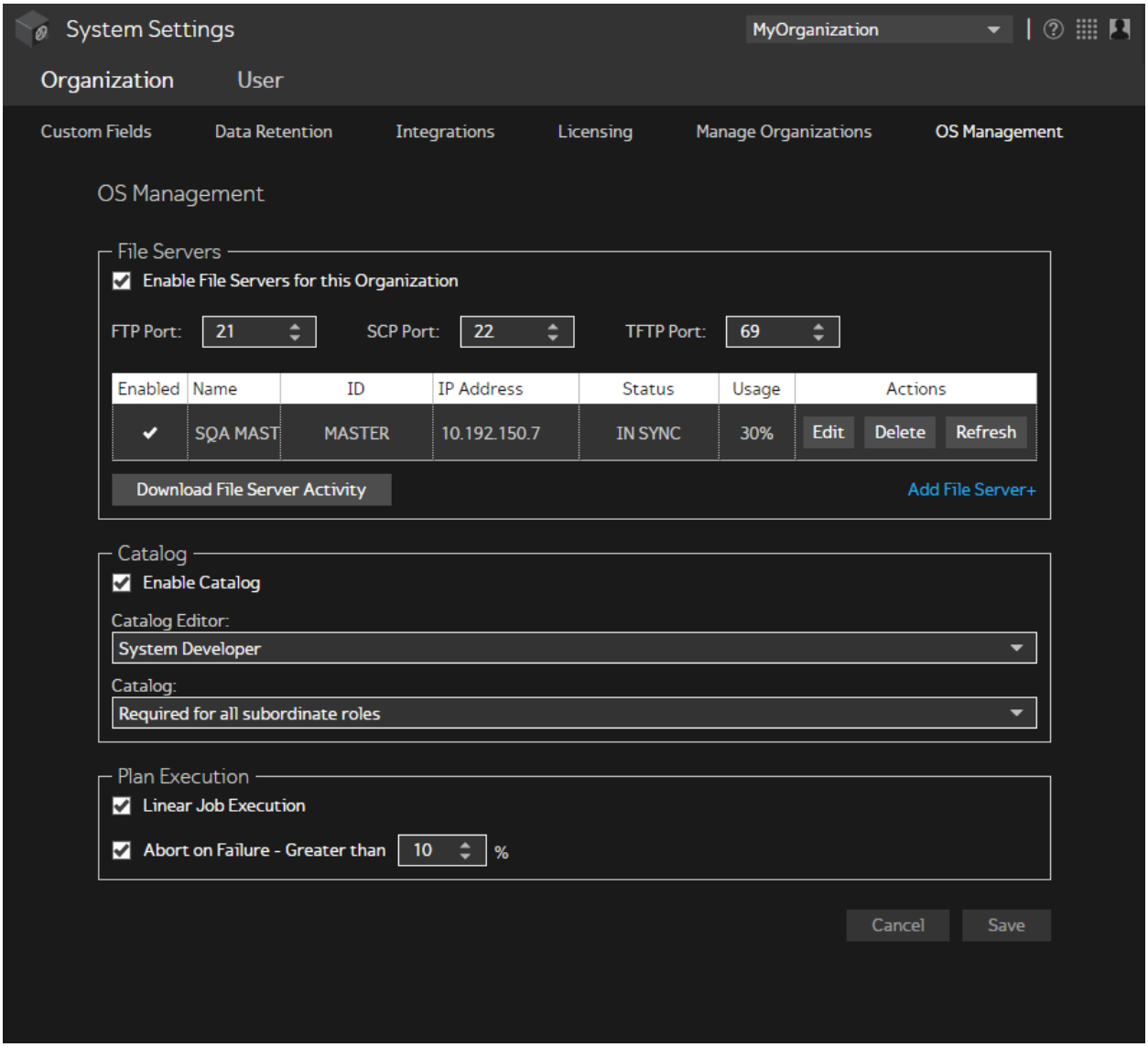
Create the VM

1. Enter the private IP address of the master file server.
2. Enter the SSH administrative port number you specified for the master file server as the **Gluware File Server Master Administrative Port**.
3. 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.
4. Click **Next: CentOS license Agreement**. By clicking **Next** on this screen, you accept the CentOS License Agreement.
5. Click **Next: Review + create**. Your settings are validated.
6. Click **Create**. The file server configuration begins. During this time, it requires communication with the Gluware server. If it can't communicate with Gluware, the configuration will fail.
7. Wait until you see the message, "Your deployment is complete."
8. Optional: Click **Download** to see the Deployment details.
9. Go to https://portal.azure.com/#home.
10. Select **Virtual Machines** and then select the VM you created to see the details.
11. Click on **Networking** under **Settings**. Review the inbound and outbound firewall settings and make changes as necessary.

When the configuration of the file server is complete, go to Gluware **System Settings** to set up the file server in Gluware.

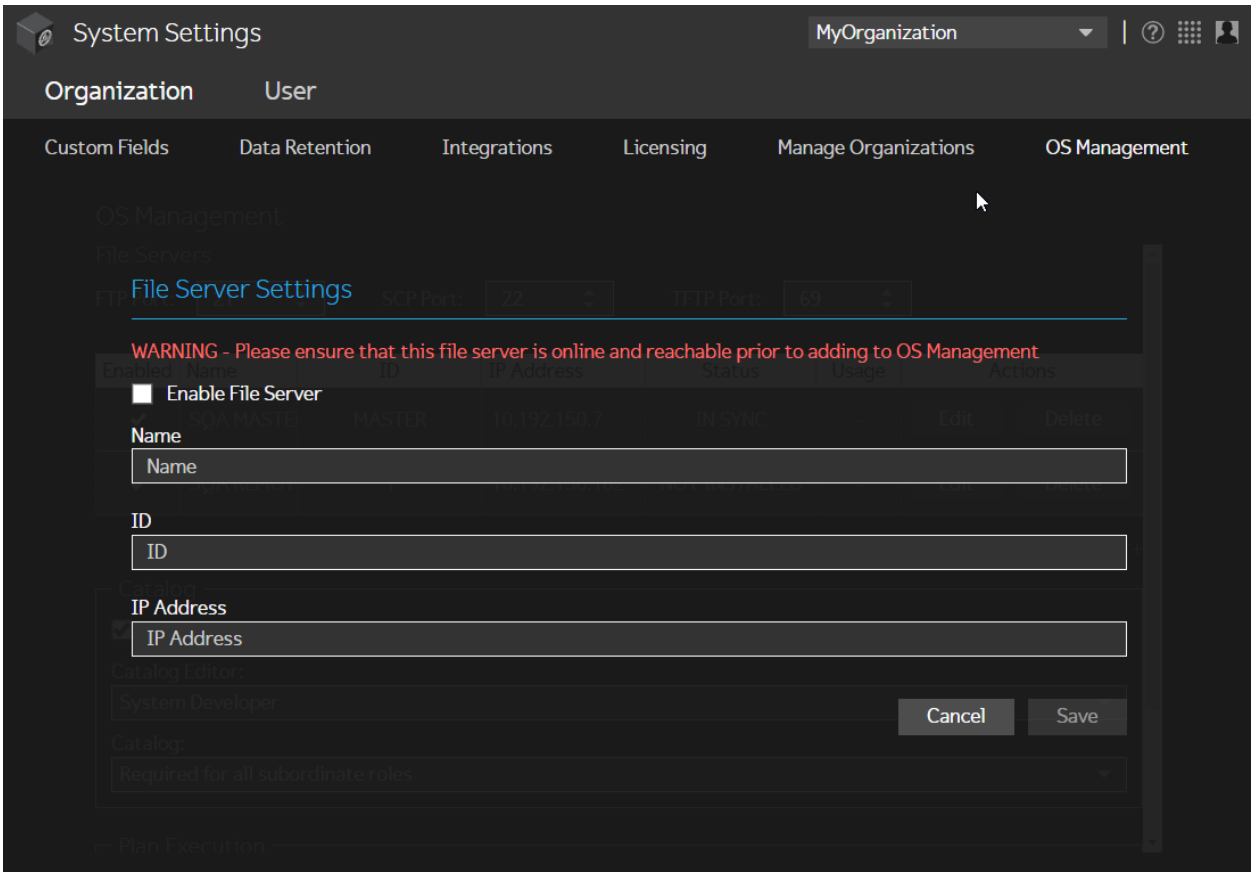
Add the file server in Gluware System Settings

1. Go to Gluware **System Settings** and ensure you're in the organization you want to add the remote file server to.
2. Select **Organization** > **OS Management**.



3. Click **Add File Server+**.

4. Optional: Check the **Enable File Server** box. You can enable or disable the remote file server at any time.
5. Enter a name, unique ID, and IP address for the server.
6. Save.



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/.

Examples of GluAPI usage are available on GitHub.

To enable GluAPI

1. Go to Gluware **System Settings** and select **Organization** > **Manage 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**.

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