Gluware® User Guide

Version 4.2
February 9, 2022

Copyright © 2022 Gluware, Inc. All rights reserved. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "INFORMATION") IN THIS DOCUMENT ARE PRESENTED "AS IS," WITH ALL FAULTS. GLUWARE, INC. AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL GLUWARE, INC. OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST OF PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE INFORMATION, EVEN IF GLUWARE, INC. OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Gluware, the stylized "[g]uware" logo and the stylized "[g]" logo are registered trademarks of Gluware, Inc. and/ or its affiliates in the United States and certain other countries. All third-party trademarks, registered trademarks, service marks, or registered service marks are the property of their respective owners. All product names and brands mentioned herein are property of their respective owners. All company, product, and service names used in this document are for identification purposes only. Use of these names and brands does not imply endorsement. Reproduction in whole or in part in any form without prior written permission is prohibited. Gluware, Inc. believes the information contained herein to be accurate as of the publication date; such information is subject to change without notice.

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

Table of Contents

About Gluware 4.2 1
Contact us 3
Web 3
Technical support 3
Professional services 3
Training 3
Documentation 4
Product dependencies and compatibility 5
Host operating system 5
Hypervisors 5
Browser 5
Display resolution 5
Security and encryption 6
Dashboards overview 7
Manage dashboards 9
Create a new dashboard 9
Open a dashboard 10
Make a dashboard a favorite 10
Edit a dashboard 10
Change dashboard permissions 10
Search for or filter dashboards 11
Copy a dashboard to another organization 11
Pause dashboard rotation 11
View the properties of a dashboard 11

Delete a dashboard 12
Widget gallery 13
Manage dashboard widgets 8
Add a widget to a dashboard 8
Change the data displayed in a widget 8
Go to a Gluware solution from a widget 8
Search for or filter widgets 9
Manage your device inventory 10
Device Manager quick reference 12
Actions 12
Views 13
Access Status 14
Configurations 14
Example: Importing and managing your inventory 15
Import a list of devices to Device Manager 16
Add devices using network discovery 18
Add individual devices 22
Assign a device to a zone 24
Find and select specific devices 25
Rearrange the display of devices 25
Find specific devices 25
Select devices 26
Run an ad hoc query 27
Discover the hardware and software details of a device 29
View the device log 30
Tips for reviewing the log 30

Change device info 32
Change one device 32
Make the same change to more than one device 32
View a device configuration 33
View the past activities performed on a device 34
View Cisco EoX Bulletins, PSIRT Advisories, and SmartNet contract details 35
Retrieve the latest Cisco support info 35
View the latest Cisco support info for a device 35
View NIST NVD Advisories 37
Retrieve the latest NIST NVD Advisories 37
View the latest NIST NVD Advisories for a device 37
Export a list of devices 38
Delete devices from Gluware 38
Reboot a device 38
Track device configurations 39
Config Drift and Audit quick reference 41
Device actions 41
Device views 42
Audit Policy actions 43
Audit Policy views 44
Example: Checking for configuration changes 45
Example: Auditing an SNMP policy 47
Create an SNMP policy for IOS routers 47
Audit the SNMP policy 48
Take a snapshot 49

Set a default snapshot 50
View configuration snapshots 51
View a device configuration snapshot 51
View all available snapshots for a device 51
View the snapshot log 52
Tips for reviewing the log 52
Compare configuration snapshots 54
Create a policy using Config Drift and Audit 55
Audit your configuration 61
View audit results 63
View and edit policy details 64
View policy history 65
View when a policy was executed 65
View all previous policy activity 65
Export a policy 65
Import a policy 66
Delete a policy 66
OS management overview 67
In File Server 67
In OS Manager 67
File Server quick reference 69
Actions 70
Views 70
File Status 70
Replication Status 70
Add a folder to File Server 71

Rename a folder 71
Move a folder 71
Delete a folder 71
Add an OS image or other file to File Server 72
Move, rename, or delete a file on File Server 73
Rename a file 73
Move a file 73
Delete a file 73
Change the properties of a file 74
Change one file 74
Make the same change to more than one file 74
View the past actions performed on a file 74
OS Manager quick reference 75
Views 75
Actions 76
Plan Status 76
Prepare devices for OS management 78
Management State 78
File Server 78
SSH 78
VRF 79
HA Group 79
Non-disruptive upgrades 79
Add an entry in the OS Catalog 80
Edit an OS Catalog entry 82
Delete an OS Catalog entry 82

Create an OS plan 83
Create the plan 83
Associate an image with a SKU or device 84
Edit an OS plan 85
Associate a new image with a SKU or device 85
Add or remove target devices 85
Move a SKU or device to another OS plan 86
Move devices from one OS plan to another 87
Run an OS plan 88
Best practices 88
Validate and run the OS plan 88
View the device logs 91
Tips for reviewing the log 91
Delete an OS plan 93
Reboot a device 93
Model a configuration 94
Example: Model an SNMP feature 96
Node state assessment 97
Solutions Manager quick reference 98
Install packages 99
Import a capsule 101
Import your own package 102
Create a Feature capsule 102
Import the Feature 102
Workflows quick reference 103
Design a new network Feature type 105

Config Modeling quick reference 107
Export or import a device list in Config Modeling 109
Export a device list 109
Import a device list 109
Add an individual device to Config Modeling 110
Create model instances using Intelligent Model Discovery 112
Run from Config Modeling 112
Run from Workflows 113
Create a Concept Item 116
Create a CLI Command List 119
Create a CLI Command Group 123
Create a Feature 125
Create a Feature Binder 128
Create a Routed Port Map 130
Create your Logical Names 130
Create your Routed Port Maps 130
Create a Switched Port Map 132
Create your Switched Port Naming Profiles 132
Create your Switched Port Maps 132
Create an Assembly 134
Create a CLI State Item 136
Create a CLI State Assessment Policy 141
Create a CLI State Assessment Query 143
Associate an Assembly with a node 145
Associate a CLI State Assessment Policy with an Assembly 146
Test your regular expression 147

View the relationships in your model 151
View a Node Instance Map 151
View referenced instances or types 151
Preview the modeled Feature 152
View a Config Modeling device log 154
Tips for reviewing the log 155
Provision nodes 158
Assign the provisioning type to the node 158
Provision the node using advanced provisioning 158
Provision the node using usbConnect 159
Assess the state of a node 161
Package a Feature for distribution 162
Monitor changes with the gluWatchdog agent 163
Configure a gluWatchdog Feature 163
Cancel a gluWatchdog checkpoint timer 166
See the number of event manager scripts in the queue 166
Stop all event manager scripts and clear the queue 166
Restore the original configuration 167
Disable and enable network interfaces 168
Update the gluWatchdog agent 169
Check for Config Modeling Kit updates 169
Update gluWatchdog 169
Run a workflow in Config Modeling 170
Model an SNMP feature Step 1. Install packages 171
Install (or update) the two packages 171
Model an SNMP feature Step 2. Design an SNMP Feature type 173

Model an SNMP Feature Step 3. Select a Concept Item 178
Model an SNMP feature Step 4. Create a CLI Command List for SNMP 180
Model an SNMP feature Step 5. Create a CLI Command Group for SNMP 182
Model an SNMP feature Step 6. Create a Feature for SNMP.....184
Model an SNMP feature Step 7. Create an Assembly for your IOS routers 186
Model an SNMP feature Step 8. Associate the Assembly with nodes....188
Model an SNMP feature Step 9. View the relationships in your SNMP model 190
Model an SNMP feature Step 10. Preview the SNMP Feature.....191
Network RPA overview 194
Network RPA development states 194
Network RPA views.....195
Data Explorer quick reference.....196
Actions 196
Views 197
Create a report template.....198
Run a Data Explorer report 201
From Data Explorer 201
From Device Manager, Config Drift & Audit, or OS Manager 202
View the Data Explorer report results 203
View Data Explorer report history.....203
Export and import a report template 204
Export a report template 204
Import a report template.....204
Export lists of devices using Data Export.....205

Schedules quick reference....206
Actions....206
Views....207
Schedule types....207
Schedule statuses....207
Last run statuses....207
Manage schedules....208
View the logs of a scheduled action....208
View a schedule's history....208
View future scheduled runs....208
Run a scheduled action now....209
Pause a scheduled action....209
Resume a schedule....209
Modify a schedule....209
Add or remove target devices....210
Delete a schedule....210
System settings overview....211
Add or update organizations....213
Configure Gluware to interact with LDAP....215
Configure Gluware to interact with RADIUS....222
Configure single sign-on authentication....228
Configure SAML authentication....228
Configure OAuth authentication....230
Gluware roles and permissions....233
Assign a Superuser....233
Gluware standard roles....233

Permissions assigned to standard roles....234
Permissions descriptions....241
Install a Gluware license....248
Request a license key from Gluware....248
Install the license....249
Delete a Gluware license....252
View license expiration dates and device counts....254
Add Gluware users....256
Customize roles and permissions....258
Create a custom role....258
Modify a custom role....261
Remove a custom role....262
Set default emails for notifications....263
Set default emails....263
Restrict the devices a role can manage....265
Enable/disable a system banner....267
Enable a system banner....267
Disable a system banner....267
Reset a system banner....267
Customize dashboards....269
Brand your dashboard....269
Change your dashboard theme....269
Enable/disable a dashboard carousel....269
Enable/disable keyboard shortcuts....270
Manage zones for Gluware Zone Engines....271
Add a new zone....272

Set the default zone 272
Disable a zone....272
Configure SMTP and proxy settings....273
Configure SMTP settings....274
Configure proxy settings....274
Manage data retention....275
Data Retention category descriptions....276
Other Data Retention fields....281
Set up custom fields....282
Monitor configurations changes....284
Monitor configuration changes in the syslog....286
Configure devices for syslog monitoring....286
Gluware syslog filters....288
Enable outbound syslog logging....289
Enable logging....289
Configure UDP....289
Configure TCP....289
Configure TLS....290
Outbound syslog messages....290
Messages from the Gluware primary server....301
Set up automatic configuration snapshots....303
Set up Cisco API Console integration....305
Set up NIST NVD API integration....307
Enable NIST NVD API integration....307
Enable GluAPI integration....309
Enable/disable a File Server....311

Troubleshoot a File Server 312
Modify a File Server 314
Delete a File Server 317
Enable the OS Catalog 318
Set up the execution guidelines for OS plans 320
Add your photo to Gluware 323
External access for features and support 324
Gluware system services 326
Manage Gluware system services 328
Services actions 328
Configuration and information actions 329
Data actions 330
Data replica actions 330
OS user management actions 331
Security actions 331
Diagnostics actions 331
Advanced actions 332
Restart Gluware services 334
Set the Gluware system date or time 335
timedatectl actions 335
Create and mount a new file system 336
Change Gluware system passwords 338
Change Gluware system certificates 339
Requesting certificates 339
If using a self-signed certificate 340
If using a PKS#12 certificate 341

Removing the private key password....342
Configuring the web server to use a certificate....342
Configuring IPsec certificates....342
Change Gluware system configurations....343
Gluware engine tuning....344
Performance tuning....347
Back up Gluware systems....348
Scheduled backup....348
Discontinue scheduled backups....350
On demand backup....350
Archive backups....350
Back up Gluware VMs....351
Restore Gluware systems from a backup....352
Promote the Disaster Recovery Server....353
Purge data....355
System reports....355
Upgrade Gluware....356
Extend a virtual drive....358

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 monitor configuration changes over time.
- Create specific compliance rules in **Config 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://youtu.be/bWWqAzsqBoI.

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 4.2.5.

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™ browser, 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

Dashboards overview

Gluware **dashboards** provide a central place to monitor device data and activity. Customize your dashboard widgets to stay on top of important changes like failed upgrades or configuration changes. Notice something you need to investigate? Just click in the widget to open the appropriate Gluware solution in context.

You can also post bulletins, get RSS feeds, and see web pages. And the dashboard is responsive so you can check it on your phone or tablet, or on a communal display in the office.

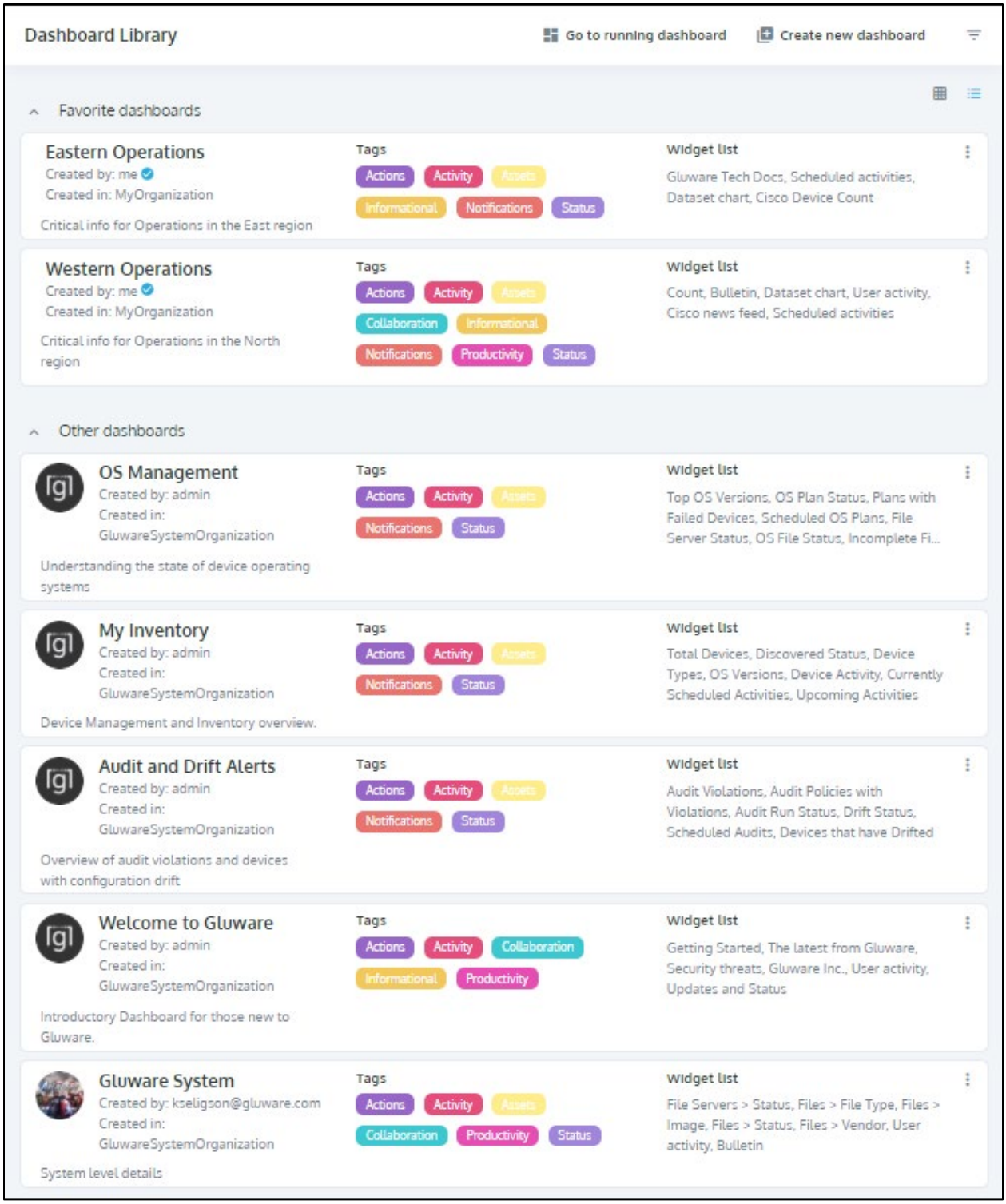
You can see all your dashboards, plus any public dashboard shared with you, in the **Dashboard Library**. Private dashboards are indicated by a lock icon. You can import example dashboards from the Gluware Knowledge Base (https://support.gluware.com/hc/start).

Manage dashboards

Widget gallery

Manage dashboard widgets

Customize dashboards



Watch an overview of Gluware dashboards
https://youtu.be/9rDcBpnvDqo

Manage dashboards

Create a new dashboard

1. Go to **Dashboard** > **Dashboard Library**.
2. Click Create new dashboard

   On a running dashboard, click , then click Create new dashboard
3. Name and describe the dashboard and click **Next**.
4. Do one of the following:
   - Select **Custom Image** and then click to add an image to brand your dashboard. Select a file and click **Open**.
   - Select **Default Image** if one is enabled in system settings.
   - Select **None**.
5. Click **Next**.
6. Do one of the following:
   - Select **Private** if you want to prevent any other users from viewing the dashboard.
   - Select **Public** to allow other users to view the dashboard. Check the box to share the dashboard with users in child organizations.
7. Click **Next**.
8. Add and configure widgets.
9. Click **Publish**.

NOTE: You can also clone an existing dashboard. From the **Dashboard Library**, click on the dashboard you want to clone and then click

Open a dashboard

Keyboard shortcuts to display your favorite dashboards are enabled by default in your profile.

- Go to **Dashboard** > **Running Dashboard**.
- On a running dashboard, click . Then click a dashboard name.
- On a running dashboard, click **Alt**+→ or **Alt**+← to view your favorite dashboards in turn.
- On a running dashboard, click **Alt**+**1** through **Alt**+**9** to display a dashboard in your favorites list.

Make a dashboard a favorite

If a dashboard is shared, it will be a favorite in all organizations it is shared with.

- Go to **Dashboard** > **Dashboard Library**, click and then click Add to favorites.
- On a running dashboard, click Set as favorite and then click **Publish**.

Edit a dashboard

- Go to **Dashboard** > **Running Dashboard** and click

Change dashboard permissions

1. Go to **Dashboard** > **Running Dashboard**.
2. Click and then click Permission settings
3. Do one of the following:
    - Select **Private** if you want to prevent any other users from viewing the dashboard.
    - Select **Public** to allow other users to view the dashboard. Check the box to share the dashboard with child organizations.
4. Save.

Search for or filter dashboards

1. Go to **Dashboard** > **Dashboard Library** and click .
2. Do any of the following:
    - Enter a dashboard name.
    - From the drop-down lists, select a tag, permission level, or shared status.
3. Click **Apply Filters**.

Copy a dashboard to another organization

You can export a dashboard to your Downloads folder and then import it to another organization.

1. Go to **Dashboard** > **Dashboard Library** and click Export dashboards.
2. Check the boxes of the dashboards you want to export.
3. Click **Export**. the dashboard files are sent to your Downloads folder.
4. Go to the organization you want to add the exported dashboard in.
5. Click Import dashboards.
6. Drag and drop the dashboard files you want to import and click **Import**. The dashboards are added to your **Dashboard Library**, Other dashboards list.

NOTE: You can also import example dashboards from the Gluware Knowledge Base at https://support.gluware.com/hc/start.

Pause dashboard rotation

- If you enabled a Dashboard carousel in system settings, you can pause and restart rotation by clicking in the **Dashboard Library**.

View the properties of a dashboard

- Go to **Dashboard** > **Dashboard Library**, click and then click View info

Delete a dashboard

You can delete a dashboard you created. If you have permissions to Moderate Public Dashboards, you can delete any public dashboard.

- Go to **Dashboard** > **Dashboard Library**, click and then click Remove.

Widget gallery

With Gluware, you get a set of generic widget types plus some preconfigured examples such as **The Latest from Gluware** and **Security threats**. The generic widgets are:

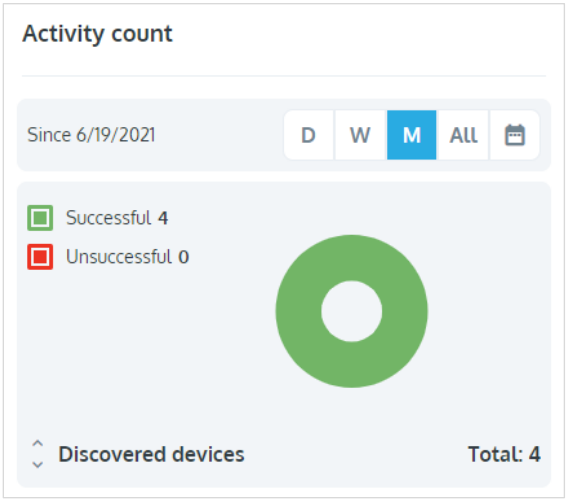
Activity count widget

Display counts for activities performed on devices over the last day, week, month, or all available. You can also select a specific start date from the calendar.

Set the rate to rotate results when more than one activity selected. Select how often to refresh the results.

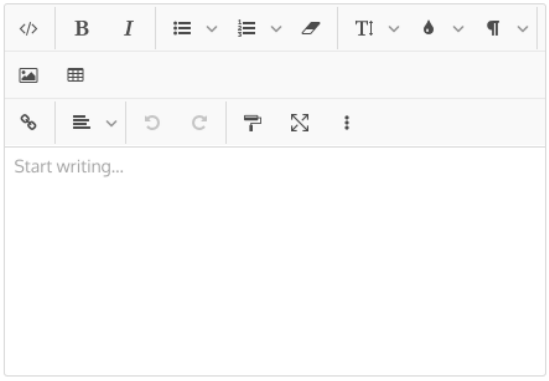
Activities available to display:

- Audited devices
- Captured devices
- Discovered devices
- Provisioned devices
- Upgraded devices



Bulletin widget

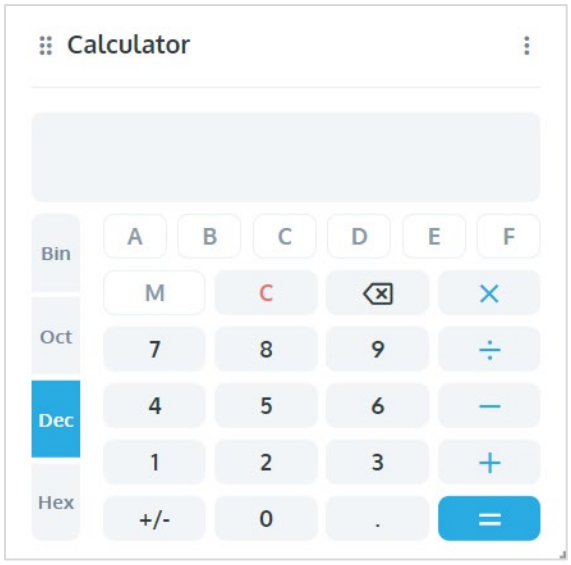
A presentation widget for HTML, rich text, images, and links.



Calculator widget

Calculate binary, octal, decimal, and hexadecimal values. The keyboard is enabled for entries:

Keyboard entry	Result
Numeric key	Number
Delete	Clears entry
+	Addition operation
-	Subtraction operation
*****	Multiplication operation
/	Division operation
Ctrl + **M** **Cmd** + **M**	Clears memory
Ctrl + **R** **Cmd** + **R**	Restores from memory
Ctrl + **C** **Cmd** + **C**	Copies
Ctrl + **V** **Cmd** + **V**	Pastes
F9	Changes sign of the value

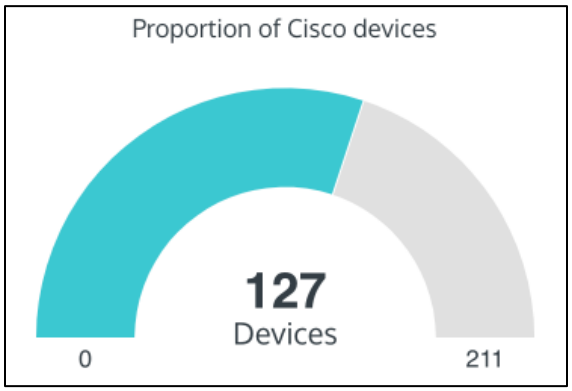


Count widget

The number of the selected data in the current organization with optional filtering. The count or a gauge chart can be displayed.

Data available to display:

- Audit policies
- Devices
- Files
- OS plans
- Schedules

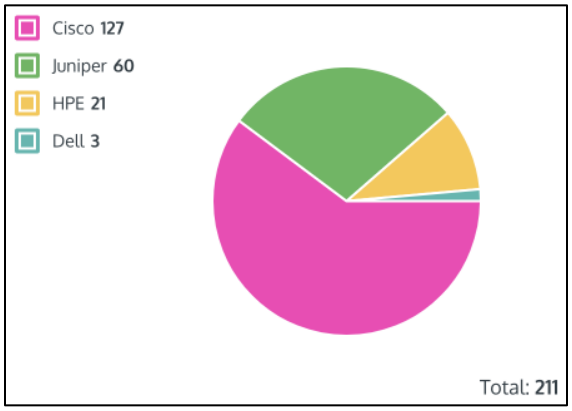


Dataset chart widget

A doughnut or pie chart of the selected property with optional filtering. If the groups of properties exceed the **Number of items** you select, the remainder are represented in an "Other" category.

Data available to display:

- Audit policies
- Devices
- File servers
- Files
- OS plans
- Schedules

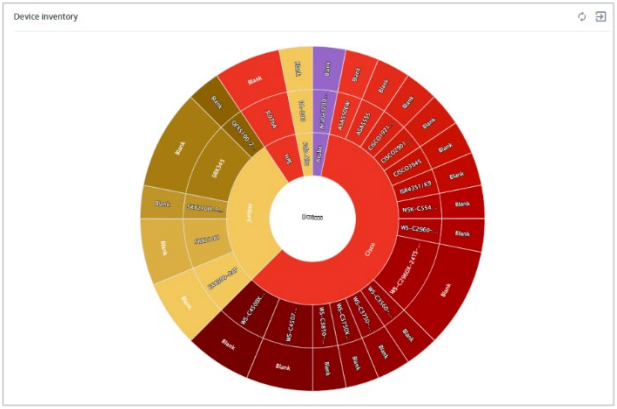


Device inventory widget

A starburst chart of device inventory properties with optional filtering. Select up to three properties to include and how often to refresh the chart. Click on a segment to zoom in on the detail. Click in the center of the starburst to go back.

Properties available to display:

- Access Status
- Captured By
- Configured Info
- Configured Type
- Discovered By
- Discovered Status
- Environment
- File Server
- Last Activity By
- Last Activity Error
- Last Activity Type
- Licensed
- Management State
- OS
- OS Version
- Serial
- SKUs
- Type
- Updated By
- Vendor
- Vendor Operations
- Zone



Grid widget

A simple data grid of the selected items with optional filtering.

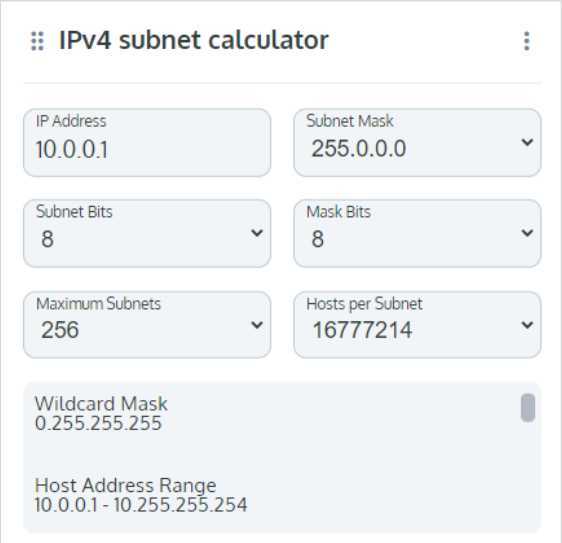
You can double-click a row in the grid and go to that item in the Gluware solution. For example, click on a device in the widget and go to that device in Device Manager. Any filtering applied in the widget is also applied in the Gluware solution.

Data available to display:

- Audit policies
- Devices in Device Manager, Config Drift & Audit, or OS Manager
- File servers
- Files
- OS plans
- Schedules

IPv4 subnet calculator widget

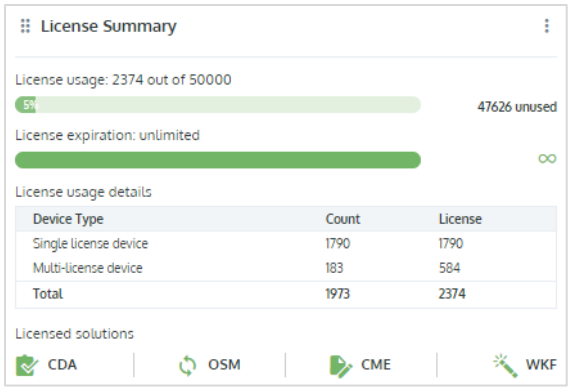
Calculate the subnet network using IP address, subnet mask, subnet bits, mask bits, maximum required IP subnets, and maximum required hosts per subnet.



License summary widget

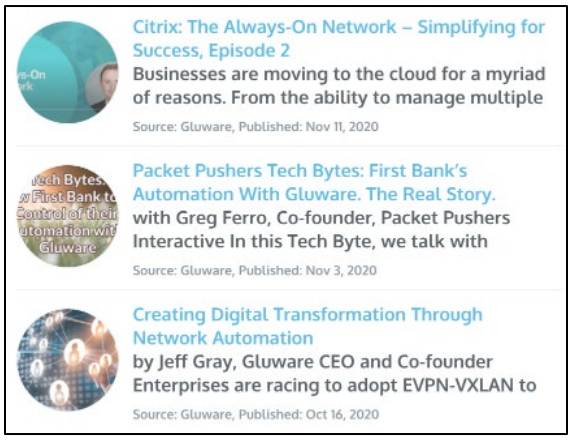
Total number of licenses, number of licenses currently in use, license expiration dates, and the Gluware solutions that are licensed:

CDA – Config Drift & Audit
OSM – OS Manager
CME – Config Modeling
RPA – For future use
TOP – For future use
WKF – Workflows



RSS feed widget

One to five RSS URLs and links to open articles. Select how often to refresh the feeds and how many feeds you want per URL.



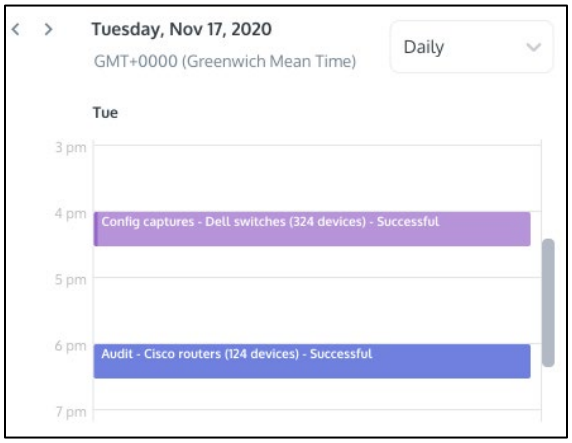
Scheduled activities widget

Upcoming and running scheduled events in list or calendar view. Select a Daily, Weekly, or Monthly schedule.

Scheduled activities available to display:

- All
- Audit
- Capture
- Cisco API
- OS Plan Provisioning
- Reboot
- Data Retention

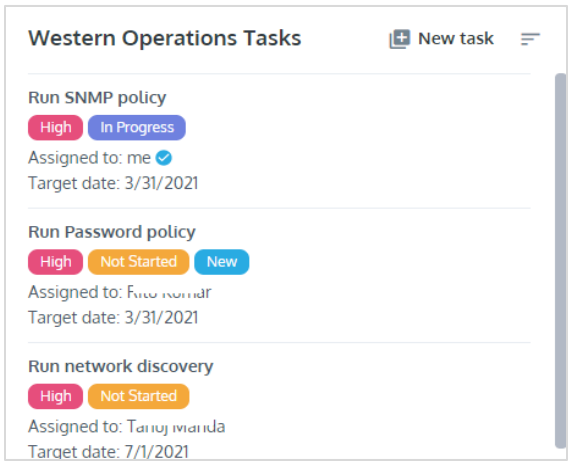
You can only have three scheduled activities widgets on a dashboard.



Task list widget

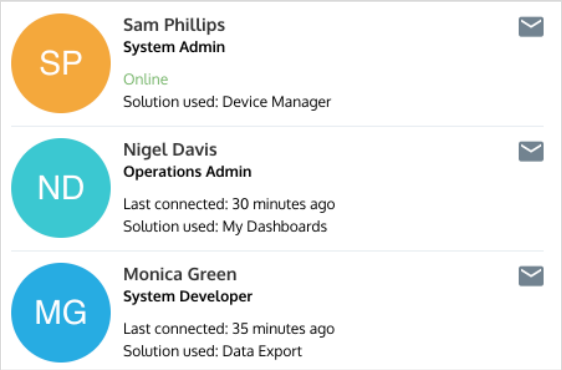
Add tasks for team members, and assign task status, priority, and target completion date. Create a task list to display all tasks or only those assigned to a specific team member. Create a separate task list widget for each team member if you choose.

When the widget is published, you can sort the task list and click to update task status. You can only see tasks you created or are assigned to you.



User activity widget

Up to 10 active Gluware users for the selected organization with optional filtering by role.



Web page widget

The contents of an external web page. Select how often to refresh the page. The web page must support iFrames. You'll see "connection refused" if it does not.

Manage dashboard widgets

Add a widget to a dashboard and configure it to show the data and activity you want to monitor. You can also add pre-configured widgets: Cisco RSS feeds, etc.

Add a widget to a dashboard

1. On a running dashboard, click ⚙.
2. Click Add widget if the side panel is not displayed.
3. Click ⠿ to drag and drop any widget from the side panel onto your dashboard. Or click on the widget's name and then click **Add Widget**.
4. Click **Configure**. Or click ⋮ and then click ⚙.
5. Select what you want the widget to display and then click **Save**.
6. Click **Publish** to save the changes to the running dashboard.

> **NOTE:** You can also add a widget by cloning an existing one. Click ⋮ on the widget you want to clone and then click ⊕

Change the data displayed in a widget

1. On a running dashboard, click ⚙.
2. On the widget you want to change, click ⋮ and then click ⚙.
3. Make your changes and save.

Go to a Gluware solution from a widget

You can jump from a widget to the Gluware solution from which the widget data is drawn. For example, if a widget displays the discovered status of devices in Device Manager, you can jump from the widget to Device Manager.

If the widget has a filter applied, that same filter is applied in the Gluware solution.

You can also jump from a web page widget to that page if your Gluware system has external access.

- On the widget, click .

Search for or filter widgets

- On the side panel, click . Enter a widget name or select a tag and click **Apply Filters**.

Manage your device inventory

Gluware **Device Manager** makes it easy to import your inventory of devices, use network discovery, and add new devices ad hoc. Once your inventory is imported, Gluware can capture connection, hardware, and software details for the devices. You can also view Cisco EoX Bulletins, PSIRT Advisories, and SmartNet contract details in Device Manager.

To use Device Manager, you'll need the **Device Discovery package** installed.

Device Manager quick reference

Import a list of devices

Add devices using network discovery

Add individual devices

Find and select specific devices

Run an ad hoc query

Discover the hardware and software details of a device

View the device log

View a device configuration

Change device info

Assign a device to a zone

View the past activities performed on a device

Monitor configuration changes

View Cisco EoX Bulletins, PSIRT Advisories, and SmartNet contract details

View NIST NVD Advisories

Export a list of devices from Device Manager

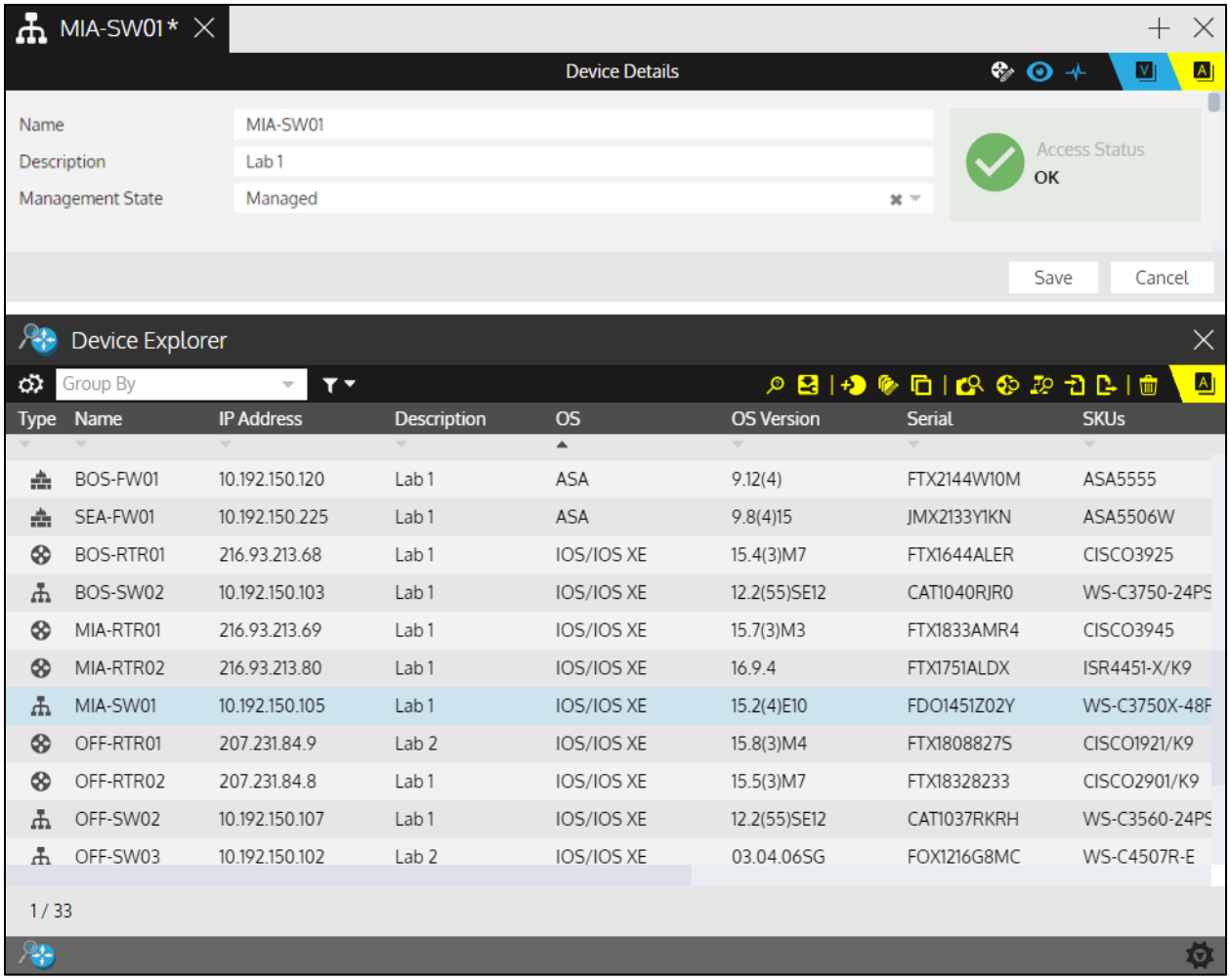
Delete devices from Gluware

Reboot a device

Watch a video introduction to Device Manger at https://youtu.be/QmMthOmxhog

For an example of managing your device inventory, *see* Example: Importing and managing your inventory.

Device Manager quick reference



Actions

Discover Devices – Discover the hardware and software details for the selected network devices

Reboot Devices – Reboot the selected devices

Update Support Data – Get Cisco EoX, PSIRT, and SmartNet details

Add Device – Add a new network device

Edit Devices – Edit the device information

Clone Device – Clone the device details of an existing device to a new device

Ad Hoc Query – Search for a specific string in a device's configuration

Import Devices – Import a list of network devices

Network Discovery – Add devices using network discovery

Export Devices – Export inventory details for all devices in the Device Explorer

Run Report – Run a Data Explorer report on demand or on a schedule

Delete Devices – Delete selected devices and all associated configuration details

Views

Details – View device details

EoX Bulletin – View Cicso EoX Bulletin

Advisory Summary – View Advisory Summary

SmartNet Details – View Cisco SmartNet contract details

Configurations – View the most recent configuration captured for the device

Details – Display the network discovery plan details

Results – Display the network discovery results

Activities – View all previous device actions and associated logs. View all the network discovery plans run in the organization

Access Status

- OK – All is well
- Invalid Credentials – Device has a credential issue
- Undiscoverable – Device can't be identified
- Unknown – Connection not yet attempted
- Unreachable – Device is offline or unreachable

Configurations

– Configuration from discovery

– Configuration from a Config Drift snapshot

– Configuration from a Config Drift snapshot and is the default configuration

Example: Importing and managing your inventory

Importing your device inventory is easy using the template Gluware provides.

1. Ensure you're in the organization that you want to add devices to.
2. Go to Gluware **Device Manager** and click .
3. Click **Download CSV Template** to get a template.
4. Add your device inventory to the template.
    - Column headings are required.
    - The **Name** column is required information.
    - Columns marked with ** are recommended information. **IP Address**, **Username**, **Password** are required if you want to discover the device configuration using Gluware.
    - In the **Manage** column, select **Managed** if you want to model the configuration or use Gluware to upgrade the OS.
5. Drag and drop the CSV file into **Device Manager** and click **OK**.
6. Use **Ctrl**+**A**/⌘+**A** to select all the devices.
7. Click . Gluware discovers the hardware and software details for the selected devices and the status will change in the **Discovered Status** column.
8. Double-click a device and then click to view a log to aid in troubleshooting.

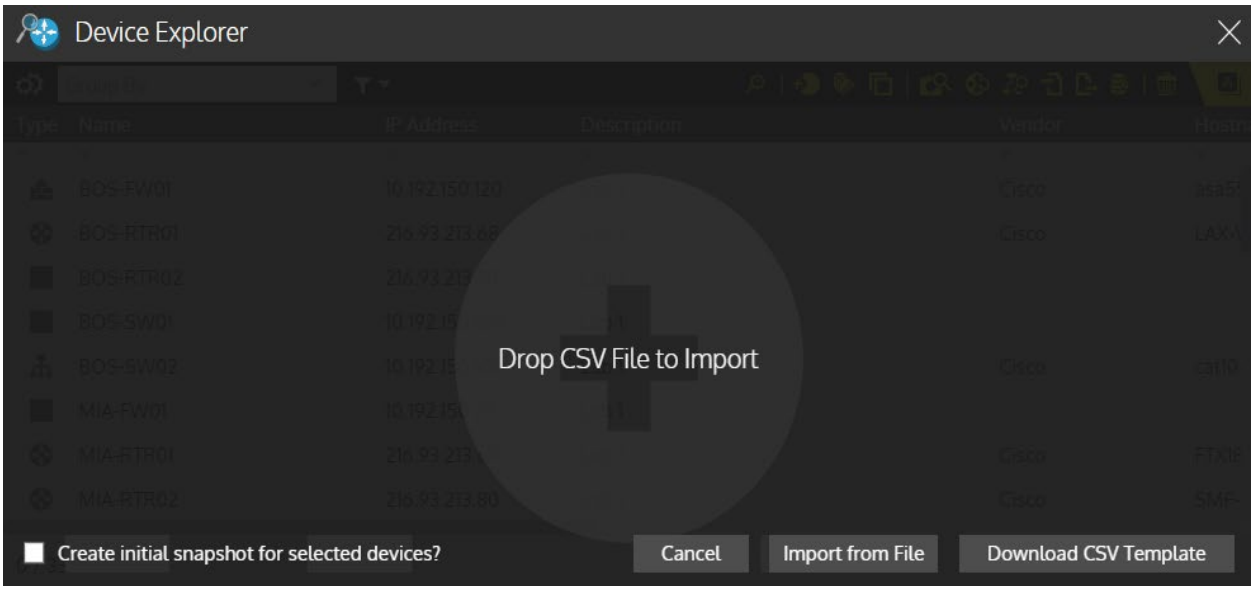
Import a list of devices to Device Manager

Gluware provides a comma-separated values (CSV) template in **Device Manager** that contains the format for importing your list of devices. If any device already exists in Device Manager, the import will update the device details.

> **NOTES:** If your organization uses customized roles, it's possible to import devices that you will not later be able to manage. And if your organization uses customized roles with device filters, you may not be able to import some devices.
>
> GluAPI supports all device management functions.

Column headings must match the column headings in the Device Manager grid. Only the device name is required for import, but connection details (IP address, username, and password) are required if you want to discover the device configuration using Gluware.

1. Go to Gluware **Device Manager** and click .
2. Click **Download CSV Template** to get a template.
3. Add your device inventory to the template.
    - Column headings are required.
    - The **Name** column is required information.
    - Columns marked with ** are recommended information. **IP Address**, **Username**, **Password** are required if you want to discover the device configuration using Gluware.
    - In the **Manage** column, select **Managed** if you want to model the configuration or use Gluware to upgrade the OS.
4. Optional: Check the box if you want Gluware to take a configuration snapshot of each device after importing it.
5. Do one of the following:
    - Drag and drop the CSV file into **Device Manager** and click **OK**.
    - Click **Import from File**, select the template file or the files you want to import, and then click **Open**.


Device Explorer
Drop CSV File to Import
Create initial snapshot for selected devices?
Cancel
Import from File
Download CSV Template

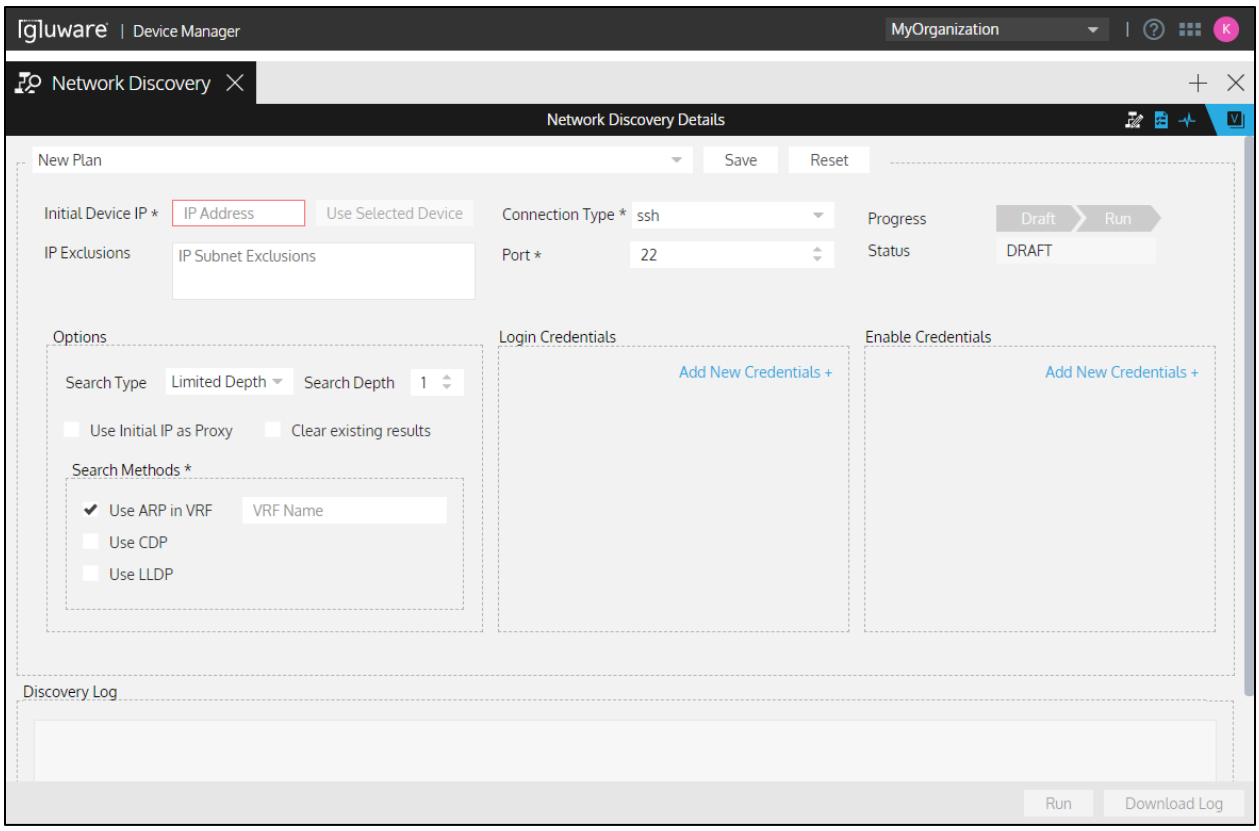
Add devices using network discovery

You can add devices to **Device Manager** by specifying a starting device and allowing Gluware to discover devices using any combination of the ARP, LLDP, and CDP protocols. A unique device is identified by its serial number and SKU.

You can re-run network discovery periodically to discover new devices and import them to **Device Manager**.

Watch a video demonstration of network discovery at https://youtu.be/tdnACfp8EaI.

1. Go to **Device Manager** and click .

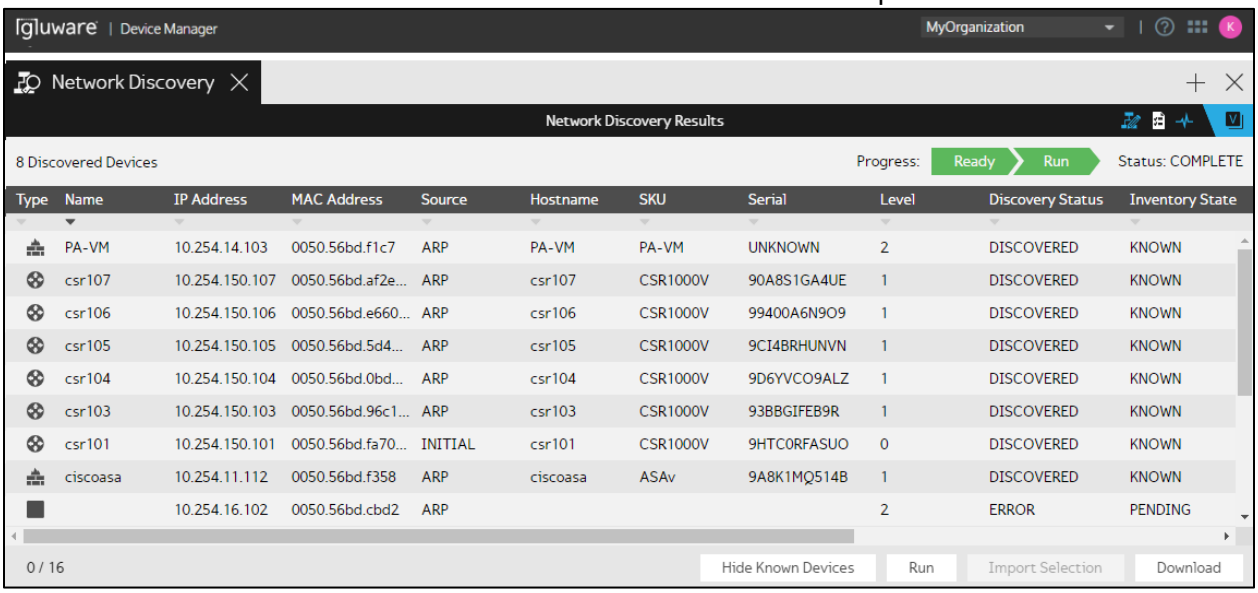


2. Optional: Select a previously saved plan from the drop-down list.
3. Enter the **IP address** of the device you want to start discovery from. Or select a device in the Device Explorer and click **Use Selected Device**. ⚠ indicates that the selected device uses one or more proxies.
4. Optional: To exclude a host or a subnet from discovery, enter an IP address in the **IP Exclusions** field. Example acceptable formats are 10.4.128.3 and 10.4.128.0/27. Enter one IP address per line in the field.
5. Select the **Connection Type** from the drop-down list.
6. Ensure the **Port** is correct for your connection.
7. Select the **Search Type** from the drop-down list:
    - **Limited Depth** – Discovery will be limited to the number of devices distant from the starting device that you specify as the **Search Depth**. This option can help limit the time it will take to search the network.
    - **Exhaustive** – Every device will be explored until no other unique device can be found.
8. Check the **Use Initial IP as Proxy** box if Gluware should proxy via this device during discovery. If this device was selected from your existing inventory and already uses a proxy, then this device will act as a double proxy connection during discovery.
9. Optional: Check the **Clear existing results** box to clear the results of the last network discovery.
10. Check the boxes of the Search Methods to employ. One method is required:
    - **Use ARP** – Collect data from the devices' ARP table. Enter a **VRF name** if Gluware should collect data from the VRF only. If you don't enter a VRF name, Gluware will collect data from the default ARP table only.
    - **Use CDP** – Collect data from the devices' CDP table.
    - **Use LLDP** – Collect data from the devices' LLDP table.
11. Enter at least one **Username** and **Password** to access the devices. Click **Add New Credentials+** to add additional **Usernames** and **Passwords**.
12. Enter the **Enable Password** if applicable. Click **Add New Credentials+** to add additional **Enable Passwords**.

13. Do any of the following:
    - Click **Save**, enter the name for the plan, and click **Save**.
    - Click **Run**. Progress is displayed in the log and the status is displayed at the top of the tab.

After running a plan:

1. Optional: Click **Download Log** to send the discovery log to your Downloads folder.
2. Click . The devices discovered and the status is reported.



Discovery Status: The status of the network discovery process.

- **DISCOVERING** – Network discovery is in process.
- **DISCOVERED** – Network discovery has found complete details about the device.
- **UNREACHABLE** – The device is listed in the MAC table, but Gluware was not able to connect to the device.
- **AUTH FAILURE** – Invalid credentials prevent Gluware from connecting to the device.
- **ERROR** – There was a problem with the network discovery process. Double-click to check the device log for details.

Inventory State: The status of the device in your existing inventory.

- **PENDING** – The device was found in the ARP table but discovery is not yet completed. Or there was a problem during network discovery.
- **NEW** – The device is not in your existing inventory.
- **IMPORTING** – The device is being imported to your inventory.
- **ERROR** – There was a problem importing the device to your inventory.
- **KNOWN** – The device is already in your inventory. If the device details found don't match your existing inventory, for example the OS version is different, your device inventory will be updated.

3. Optional: Click **Hide Known Devices** to display only devices that are new to your **Device Manager** inventory. **Show Known Devices** displays all devices discovered, including those already in your inventory.
4. Optional: Click **Download** to send the list of devices to your Downloads folder. If you have hidden known devices, they are not included in the download.
5. Select the devices you want to import and click **Import Selection**.
6. Click **Confirm**. The selected devices are imported to **Device Manager** and the discovered hardware and software details are included.

NOTE: If your organization uses customized roles with device filters, you may not be able to import some devices.

Add individual devices

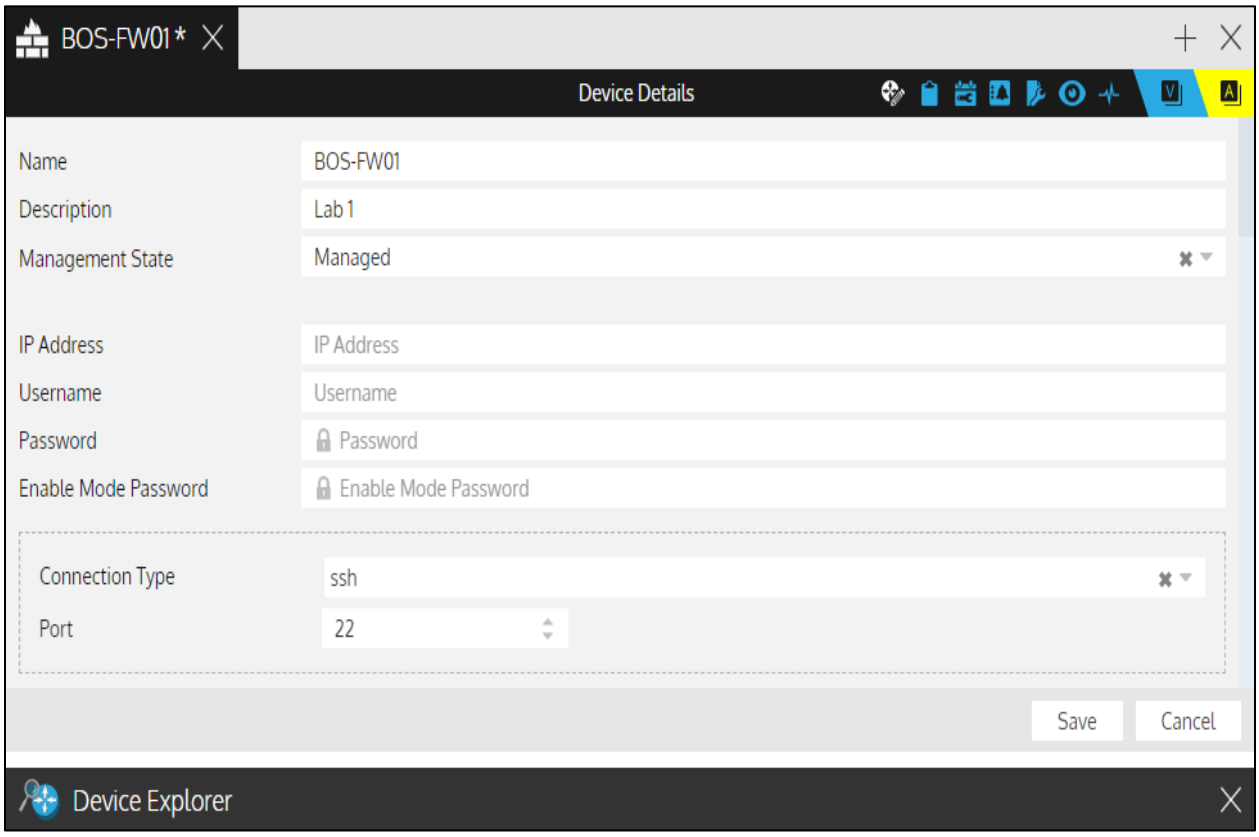
You can add new devices to your inventory, one at a time. Only the device name is required, but connection details (IP address, username, and password) are required if you want to discover the device configuration using Gluware.

1. Go to Gluware **Device Manager** and click .
2. Enter a name for the device and click **Create**.
3. Add a description.
4. Select a **Management State**:
    - **Managed** – The device can be managed in all Gluware solutions (default)
    - **Unmanaged** – The device can be managed only in Device Manager and in Config Drift and Audit
    - **Inventory Only** – The device can be managed only in Device Manager
5. Provide the configuration details for the device: **IP Address**, **Username**, **Password**, **Enable Mode Password** (if required), **Connection Type**, and **Port**.
6. Click **Add Proxy+** to add a proxy and its connection details if applicable.
7. Enter any custom field information. Custom fields are set up in system settings and are unique to an organization. Region, Department, and Restricted are examples of custom fields.
8. If you are using Gluware **OS Manager**, select the **Default File Server** to use for OS plan actions.
9. Save.

NOTES: You can also add a device by cloning an existing device. Simply select a device and click

If your organization restricts the devices users can manage, it's possible to add devices that you will not later be able to manage.

Once devices are discovered, devices may appear or disappear from your device list.



Assign a device to a zone

Each device can be assigned to a zone that has a dedicated **Gluware Zone Engine** to make processing times faster. All jobs on the device will be run on the Zone Engine in that zone when that engine status is ACTIVE. If the Zone Engine is OFFLINE or DISABLED, the device's jobs will run on any other ACTIVE Zone Engine.

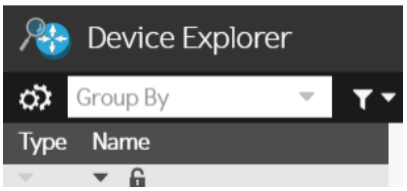
You can lock the device to only run on the engines in a zone. If locked, the device's jobs will not run if the zone's engines are OFFLINE or DISABLED.

1. Go to **Device Manager**.
2. In the **Device Explorer**, select the device or devices and click .
3. Select a **Zone** from the drop-down list.
4. Optional: Check the **Lock** box if you want to restrict the device's jobs only to the Gluware Zone Engine in the assigned zone.
5. Save.

Find and select specific devices

Watch a demo of using the **Device Explorer** at https://youtu.be/3SKREKWxLX4.

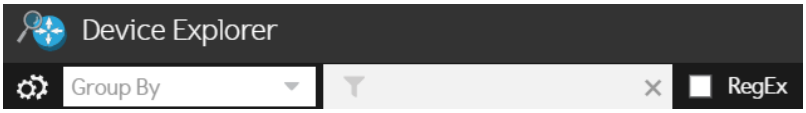
Rearrange the display of devices



- Click and select the columns you want to see in the **Device Explorer** list.
- Drag and drop a column to re-order it.
- Reverse the sort order of the column by clicking under the column title.
- Click to lock the column at the beginning of the row.
- Select an attribute from the **Group By** drop-down list to group like devices. Expand and collapse the groups to show or hide devices.

Find specific devices

- Click and type your search term. Check the **RegEx** box if you want to use a regular expression. Need help with regex? Go to http://regex101.com/



- Click the ▼ next to ▼ for advanced search capabilities.
    - Select a column or snapshot type from the drop-down list, select a condition from the drop-down list, and then enter a search term or string. The search term or string can contain spaces. Selecting **New Snapshot** runs a new snapshot, which can take some time.
    - Click **Add rule** and click **AND** or **OR** to add a logical operator.
    - Click **Add group** to add nested rules.
    - Click **Apply** to implement the search.

- To clear an advanced filter, click **Reset** and then click **Apply**.
- *See also* Run an ad hoc query.

Select devices

Click, **Shift**+**click**, **Ctrl**+**click**/⌘+**click**, or **Ctrl**+**A**/⌘+**A** to select rows.

Run an ad hoc query

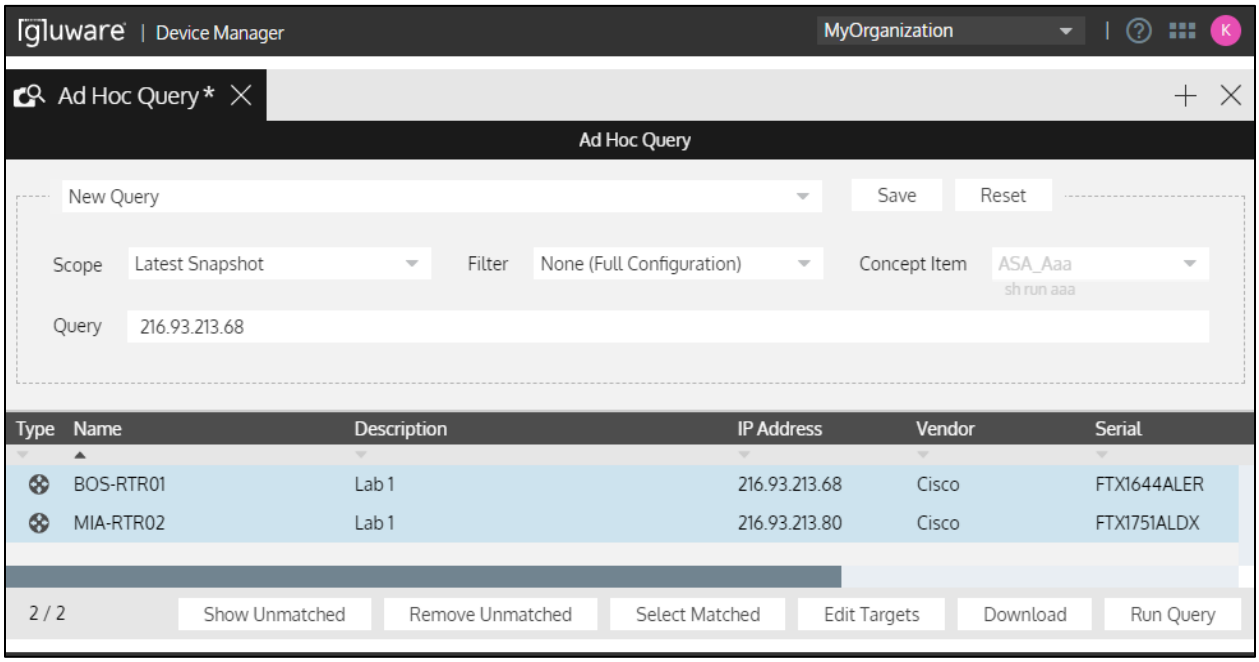
To find devices that contain a specific search string and then inspect the devices' configurations that contain that string, run an ad hoc query.

Watch a demonstration of an ad hoc query at https://youtu.be/iqGEvblOxOE.

1. Go to **Device Manager**, **Config Drift and Audit**, or **OS Manager** > **Devices**.
2. Select one or more devices in the **Device Explorer**.
3. Click .
4. Optional: Select a previously saved query from the drop-down list.
5. Select the source of the query from the drop-down list:
   - **Default Snapshot** – Searches within the default snapshot's configuration.
   - **Latest Snapshot** – Searches within the most recent snapshot's configuration.
   - **Device** – Connects to the device.
6. Select a filter:
   - **None (Full Configuration)** – Searches the entire configuration.
   - **By Concept Item** – Searches only within the Concept Item block you select in the **Concept Item** drop-down list.

     NOTE: If your source is a snapshot and you select a **Concept Item**, a command, for example, a `show` command, is displayed. The command cannot be run on a snapshot; however, the **Concept Item** will extract the same configuration lines that the command would produce.
     If the devices to be queried have several operating systems, create a rule for each OS and select the appropriate **Concept Item**.
   - **By Show Command** – Enter a list of show commands to be executed on the device.
7. Enter the regex search string for the **Query**.
   Need help with regex? Go to http://regex101.com/

8. Click **Run Query**. The **Match Count** shows the number of devices that matched the query.
9. Optional: Do any of the following:
    - Click **Hide Unmatched** to hide devices in the returned list that do not match the query. Click **Show Unmatched** to return the hidden devices to the returned list.
    - Click **Remove Unmatched** to delete devices from the returned list that do not match the query.
    - Click **Select Matched** to select the devices that conform to the query.
    - Double-click to view the device configuration with the search string highlighted.
    - Click **Download** to send a ZIP folder to your Downloads folder that includes the results of the query for the devices selected. If no devices are selected, includes results for all devices queried.
    - Click **Edit Targets** to modify the device list searched. Click **Add**, **Remove**, or **Remove All** to refine the list of devices to search. Then click **Save** and **Back**.
    - Click **Save**, enter the name for the query, and click **Save**.



Discover the hardware and software details of a device

Gluware **Device Manager** uses the connection details for a device to interrogate that device and discover the hardware and software details.

1. Go to **Device Manager** and select one or more devices.
2. Click . Gluware discovers the hardware and software details for the selected devices and the status will change in the **Discovered Status** column.
3. Double-click a device and then click to view a log to aid in troubleshooting.
4. If discovery failed, click to see the error messages.

View the device log

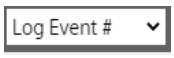
When you discover a device's hardware and software details, a log is created.

1. Go to **Device Manager** and double-click a device.
2. Click .
3. View the log:
    - Point to to quickly skim the log.
    - Double-click on the row to see the log in detail.

> **NOTE:** Any errors appear in red. Common errors include incorrect or missing device credentials (e.g. password, serial number) indicating you're not connected to the device.

4. Optional: Click **Download** to send the log to your Downloads folder.
5. Click **Back** to return to the activity summary.

Tips for reviewing the log

- When you see an error or warning, you may need to inspect the lines above it to determine the cause.
- Click to pause scrolling.
- Click **Show Settings** to:
    - **Search for a text string** – Enter the text string and click **Enter**. Check the **Case-Sensitive** box to make the search case-sensitive. Clear the box to ignore case. Click > and < to see the occurrences found.
    - **Change the line label** – Select a line label from the 

drop-down list. Select from:
Log Event #
Line Number
Timestamp

Time Passed
Event Duration

- **Filter the log** – Click . Check or clear the boxes to display just the levels you want. All levels are displayed by default.
- **See the source code file and line number that produced the log line** – Point to a line.

Log Levels	Description
Error	A problem that must be fixed
Warning	A problem that did not stop the process but should be fixed
Task	The beginning or the end of a step
Checkpoint	A significant point in the code
Info	General info about the process that does not fit in the other logging categories
Response	The raw interaction between the Gluware engine and the device
Debug	Low-level informational log messages usually related to the internal state of code variables. It's specific to how the code is working, as opposed to how the process is proceeding

Change device info

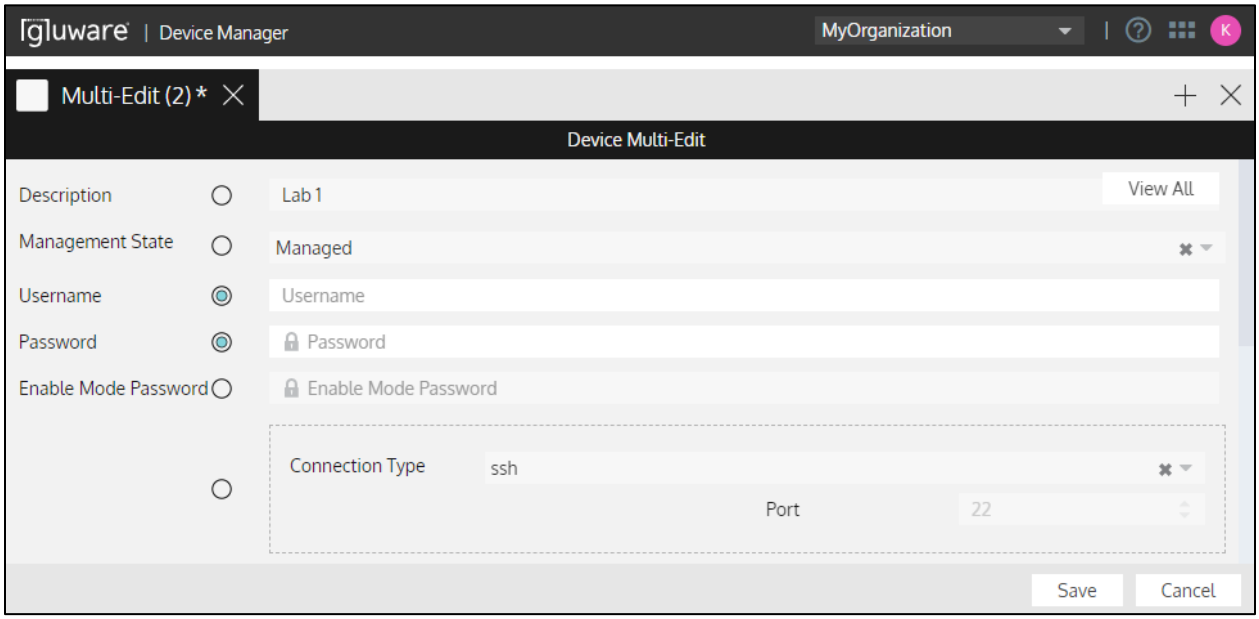
You can make changes to a single device or make the same change to multiple devices.

Change one device

1. Go to Gluware **Device Manager** and select a device.
2. Click .
3. Make changes to the device info in the top of the screen. Some fields are read-only.
4. Save.

Make the same change to more than one device

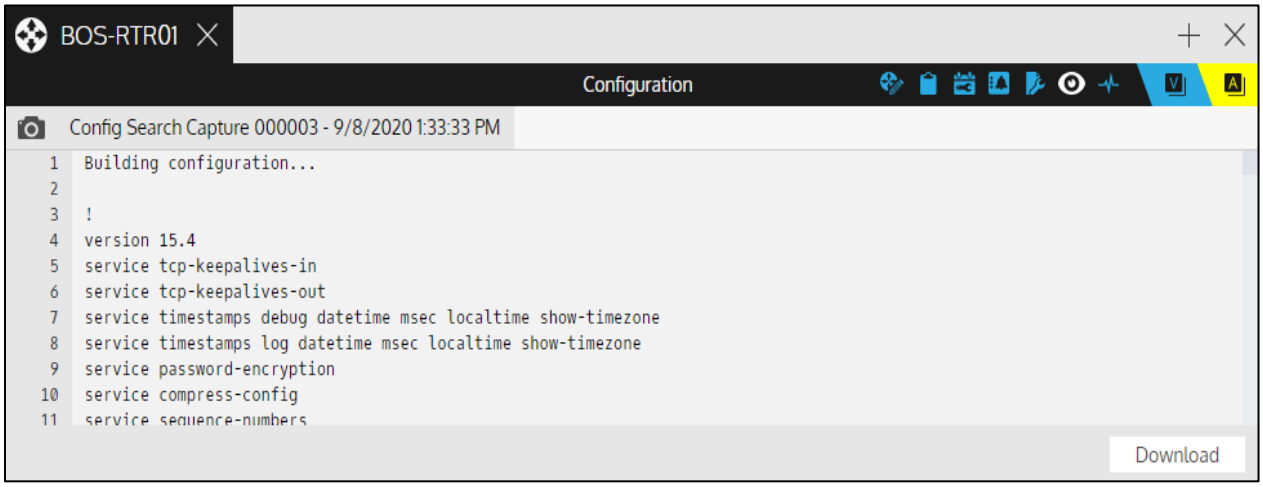
1. Go to Gluware **Device Manager** and select the devices you want to change.
2. Click . A Device Multi-Edit tab opens in the top panel. Click **View All** to see the list of devices you are editing.
3. Click a radio button next to the field and make changes. Some changes are restricted since they would apply to multiple devices.
4. Save.



View a device configuration

Once you have discovered the hardware and software details using **Device Manager,** you can view the last captured configuration of a device.

1. Go to Gluware **Device Manager** and double-click a device to display the device details in the upper panel.
2. Click . In the upper left,
   means the configuration is from discovery
   means the configuration is from a Config Drift snapshot
   means the configuration is from a Config Drift snapshot and is the default configuration
3. Optional: Click **Download** to save the configuration to a file.



View the past activities performed on a device

You can view a list of the actions taken in Gluware for any device.

1. Go to **Device Manager**.
2. Select a device in the **Device Explorer**.
3. Click to view **Activities** related to the device.
4. If there are errors, view the log.

View Cisco EoX Bulletins, PSIRT Advisories, and SmartNet contract details

When enabled in system settings, **Device Manager** can display Cisco Bulletins, Security Advisory counts, and SmartNet contract details. Updates can be retrieved manually or can be scheduled.

> **NOTE:** You must have discovered the hardware and software details on your Cisco devices to view the latest Cisco support info.

Retrieve the latest Cisco support info

1. Go to Gluware **Device Manager**.
2. If not already displayed, click to add the following columns to the **Device Explorer**:
   Critical Advisories
   High Advisories
   Medium Advisories
   EOX Bulletin
   Contract
   Contract End
   End of Sale
   End of Maintenance
   End of Support
   Product ID
3. Select one or more Cisco devices.
4. Click and **Confirm**.

View the latest Cisco support info for a device

1. Go to Gluware **Device Manager**.
2. Double-click a Cisco device.

3. Click to view an EoX Bulletin.
   Click and then click to view an Advisory Summary.
   Click to view SmartNet Details.
4. Click **Download** to save the information to a CSV file.

View NIST NVD Advisories

When enabled in Settings, **Device Manager** can display NIST NVD Advisories. Updates can be retrieved as needed or can be scheduled.

Retrieve the latest NIST NVD Advisories

1. Go to **Device Manager**.
2. If not already displayed, click and select the following columns to add them to the **Device Explorer**:
   Critical Advisories
   High Advisories
   Medium Advisories
3. Select one or more devices.
4. Click and **Confirm**.

View the latest NIST NVD Advisories for a device

1. Go to **Device Manager**.
2. Double-click a device.
3. Click and then click to view an Advisory Summary.
4. Click **Download** to save the information.

Export a list of devices

Device Manager allows you to export your device inventory to a CSV file. If you have filtered your device list, only the devices displayed will be exported.

1. Go to Gluware **Device Manager** and select one or more devices.
2. Click . This exports the list as a CSV file to your Downloads folder.

> **NOTE:** You can also export the list of devices using **Data Export**.

Delete devices from Gluware

When you delete a device, all the related information about the device also gets deleted, including:

- Configuration snapshots
- Device logs
- OS plan results

The device is also removed from any scheduled activities and from any OS plan. And if the device was associated with a Config Modeling node, that node is also deleted.

1. Go to Gluware **Device Manager** and select one or more devices.
2. Click and click **Confirm**.

Reboot a device

1. Go to **Device Manager** or **OS Manager** > **Devices**.
2. In the **Device Explorer**, select one or more devices.
3. Click .
4. Click **Confirm**.

Track device configurations

Config Drift and Audit allows you to take snapshots of device configurations and compare subsequent snapshots to a baseline. Config Drift and Audit also allows you to define what CLI are required and forbidden in the device configuration and audit those policies on specific devices.

To use Config Drift and Audit, you'll need a **Config Drift and Audit license** and the **Config Drift package** installed. Only devices that have a **Management State** of **Managed** or **Unmanaged** appear in **Config Drift and Audit**.

Config Drift and Audit quick reference

Take a snapshot

Set a default snapshot

View configuration snapshots

View the snapshot log

Compare configuration snapshots

Set up automatic snapshots

View the snapshot log

Create a policy using Config Drift and Audit

Audit your configuration

View audit results

View and edit policy details

View policy history

Export a policy

Import a policy

Delete a policy

For examples, *see*:

Config Drift overview video at https://youtu.be/gF5BXPOyyKA

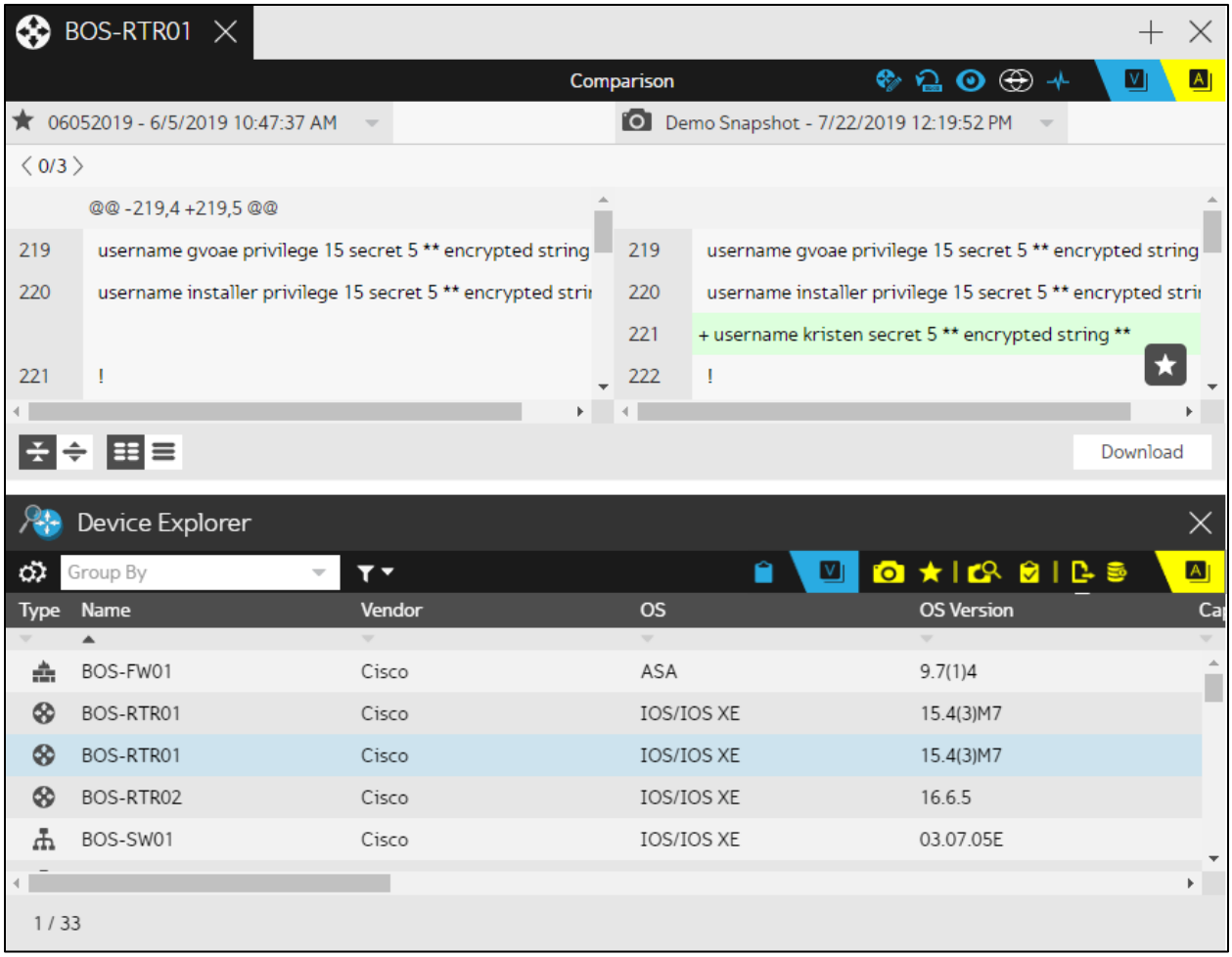
Config Audit overview video at https://youtu.be/LSGTHcsL-Rg

4.2 Config Audit updates video at https://youtu.be/UhQe_8BkNMw

Example: Checking for configuration changes

Example: Auditing an SNMP policy

Config Drift and Audit quick reference



Device actions

Capture Snapshot – Capture a current configuration snapshot from the selected devices, compare it to the baseline configuration for each device, and reflect the status of the comparison in the Captured Status field

Set Default Configuration – Make the most recent snapshot for the selected device the baseline configuration snapshot

Ad Hoc Query – Search for a specific string in a device's configuration

Audit Configuration – Run or schedule an audit for the selected devices

Export Devices – Export the most recent snapshot details for all devices in the Explorer to a CSV file in your Download folder

Run Report – Run a Data Explorer report on demand or on a schedule

Device views

Details – View or modify device details

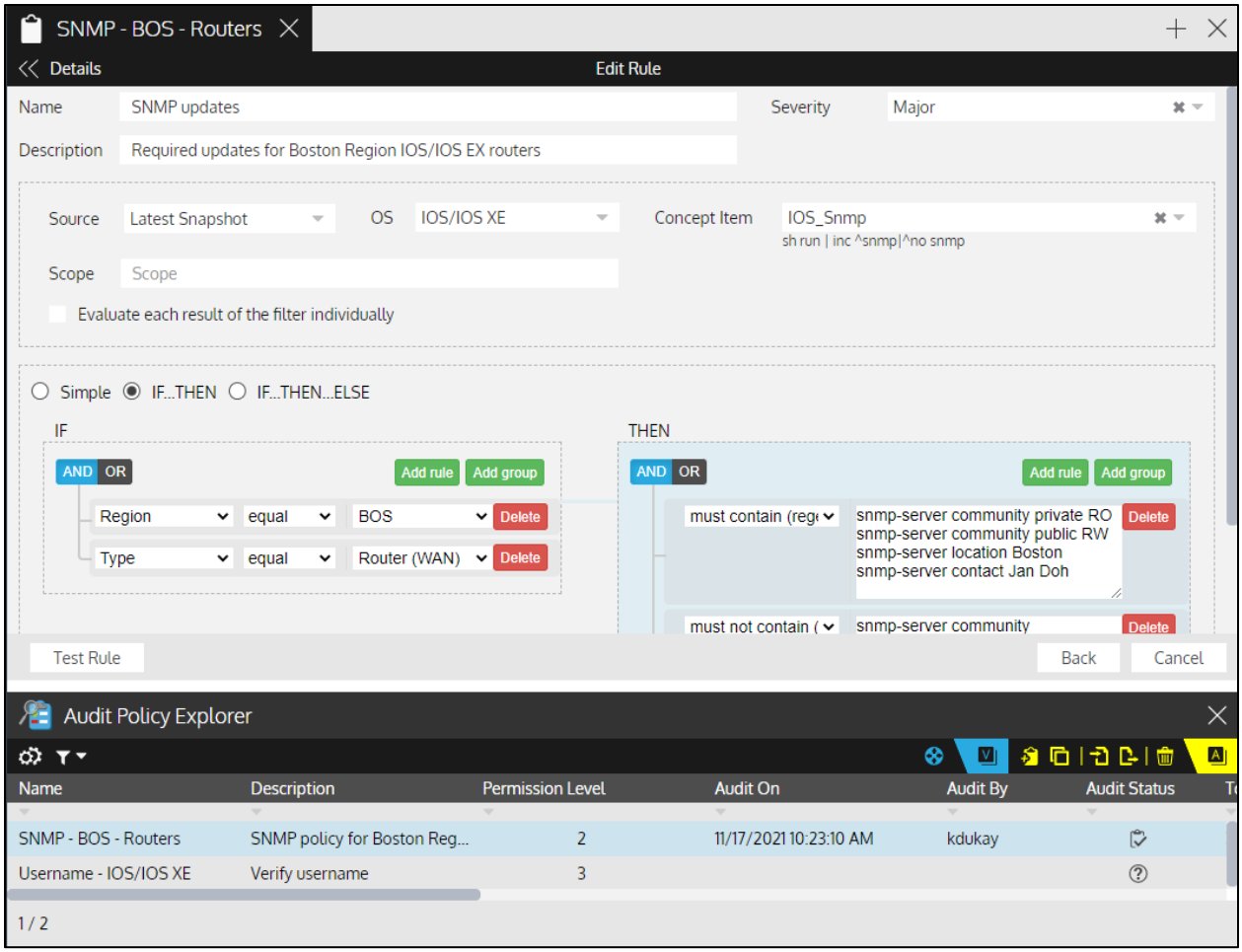
Snapshots – View all available configuration snapshots for a device

Configurations – View a single device configuration snapshot

Comparisons – Compare two configuration snapshots

Activities – View all previous device actions

Audit Policy Explorer – Switch to Audit Policy Explorer



Audit Policy actions

Add Policy – Create a new policy

Clone Policy – Duplicate a selected policy

Import Policy – Import a policy or policies exported from another organization

Export Policy – Export the selected policy or policies for backup or to import to another organization

Delete Policy – Delete the selected policy or policies

Audit Policy views

Details – View or edit policy description and rules

Audit Execution Summary – View when a policy was executed

Audit Policy Results – Display the success or failure of the policy execution for the target devices

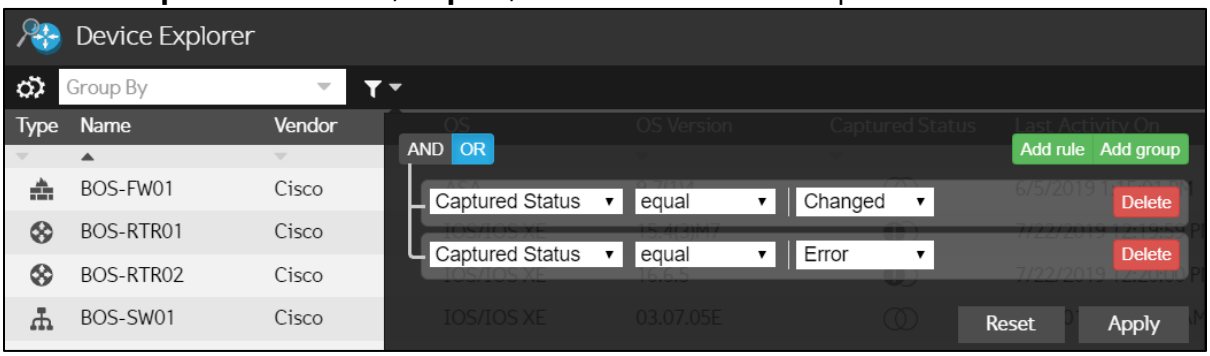
Activities – View all previous policy actions

Device Explorer – Switch to Device Explorer

Example: Checking for configuration changes

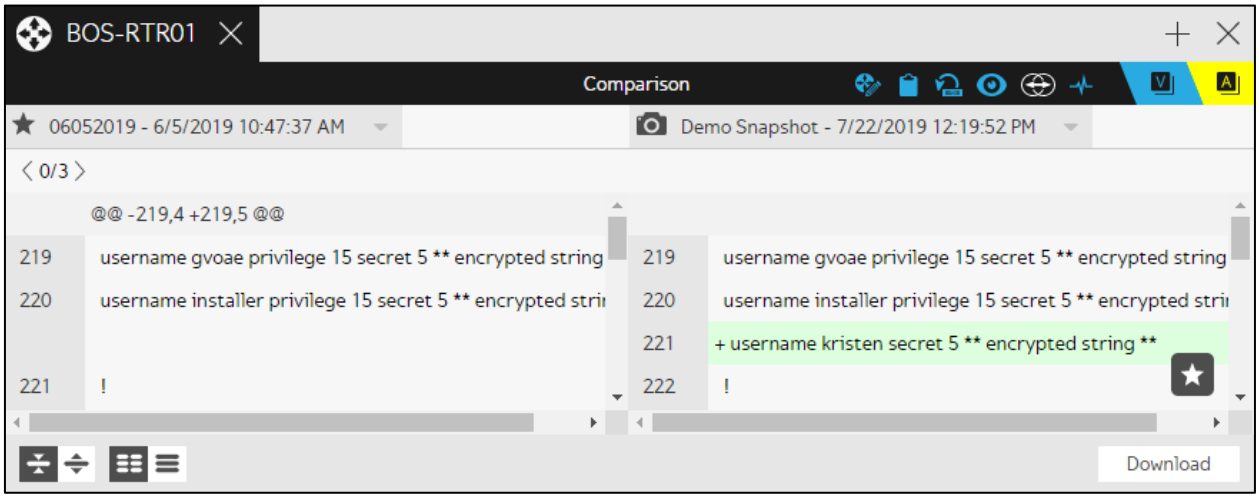
With Gluware, you can check for unauthorized configuration changes. You must have taken an initial snapshot and set a snapshot as the default (baseline) configuration.

1. Go to **Config Drift and Audit** > **Devices**.
2. Use **Ctrl**+**A**/**Command**+**A** to select all the devices and then click to take a new snapshot of the devices' configurations.
3. Name the snapshot.
4. Click **Start Capture**.
5. When the snapshot is complete, click the next to .
6. Select **Captured Status**, **equal**, **Changed** from the drop-down lists.
7. Click **Add rule**.
8. Click **OR**.
9. Select **Captured Status**, **equal**, **Error** from the drop-down lists.



10. Click **Apply**.

11. Double-click a device in the returned list. The comparison between the default and the new snapshot appears in the top pane. Changes are highlighted. **<0/x>** is the number of configuration changes from the baseline snapshot. Click the **>** to see the next change.



12. Use to switch between Expanded and Compact views. Use to switch between Side-by-Side and Line-by-Line views.
13. Click to save the changed configuration as the new default for the device.

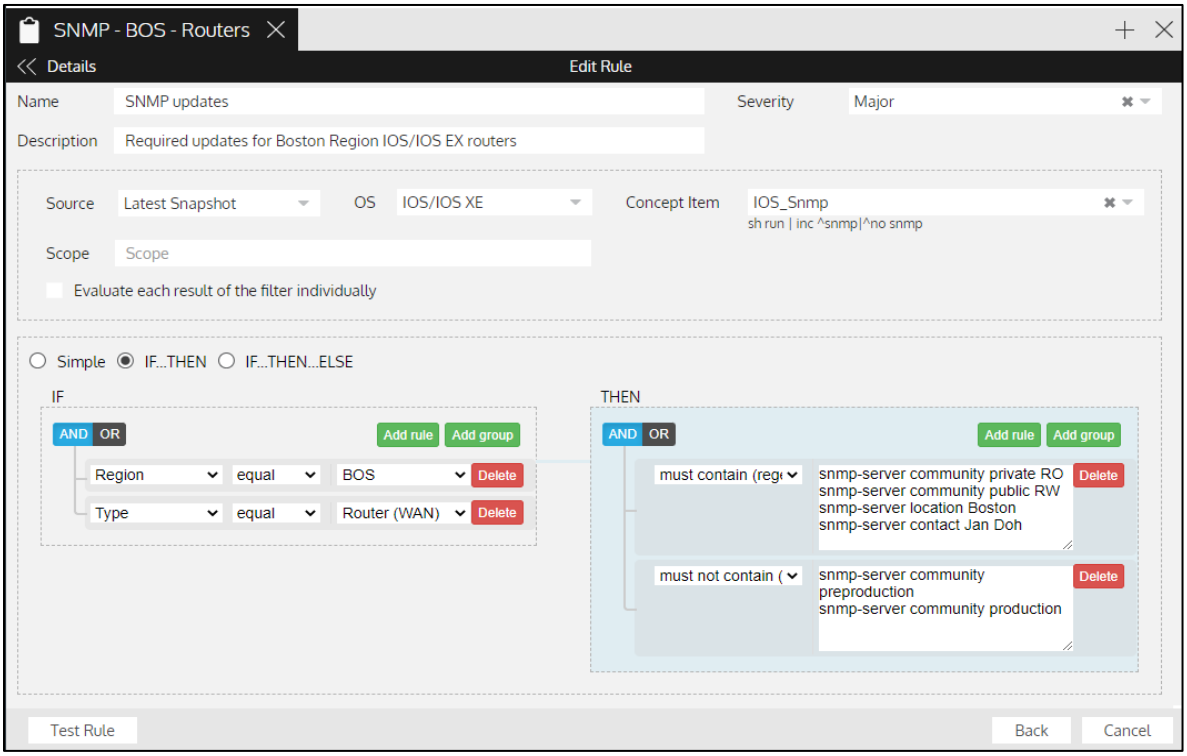
Example: Auditing an SNMP policy

This example policy helps ensure that the SNMP Feature is implemented correctly on all IOS routers.

Create an SNMP policy for IOS routers

1. Go to **Config Drift and Audit** > **Audit Policies**.
2. Click to create the **SNMP Policy** for Boston region routers.
3. Name the policy and click **Create**.
4. Describe the policy.
5. Select permission level 1.
6. Click **Add Rule**.
7. Name the rule and then click .
8. Set the **Severity** of the rule to Major from the drop-down list.
9. Describe the rule as **Required updates for Boston Region IOS/IOS XE routers**.
10. Select **Latest Snapshot** from the **Source** drop-down list. This will run the policy against the latest configuration snapshot.
11. Select the **IOS/IOS XE** operating system as a constraint for the policy.
12. Select the **IOS_Snmp** Concept Item from the **Concept Item** list.
13. Select the **IF…Then** rule type.
14. for the **IF** statement, select **Region**, **equal**, **BOS** from the drop-down lists and then click **Add rule**.
15. Select **Type**, **equal**, **Router (WAN)** from the drop-down lists.
16. For the **THEN** statement, select **must contain (regex)** from the drop-down list.
17. Paste what the policy requires in the box. In our example, we want all Boston-located routers to have:
    ```
    snmp-server community private RO
    snmp-server community public RW
    snmp-server location Boston
    snmp-server contact Jan Doh
    ```
18. Click **Add rule**.
19. Select **must not contain (regex)** from the drop-down list.

20. Define what the policy forbids in the box. In our example, we want to ensure all our old standards have been updated:
    ```
    snmp-server community preproduction
    snmp-server community production
    ```
21. Click **Back**.
22. Save.



Audit the SNMP policy

1. Go to **Config Drift and Audit** > **Devices**.
2. To select the devices you want to audit:
    a. Click and ensure that the **Type** and **Vendor** columns are checked.
    b. Click the **Type** column heading and then select all the Cisco routers you want to audit.
3. Select .
4. Click **Selection**.
5. Select the **SNMP Policy** from the drop-down list.
6. Click **Start Audit**.
7. Click **View Results**.

Take a snapshot

You can capture a snapshot of the current configuration for the selected devices. **Config Drift** compares it to the default snapshot for each device and the result of the comparison is displayed in the **Captured Status** column.

1. Go to **Config Drift and Audit** > **Devices**.
2. Select one or more devices and click .
3. Optional: Name the snapshot.
4. Run or schedule the snapshot:
    - Click **Start Capture** to run the snapshot immediately.
    - Click **Schedule Capture** to define the schedule. Check a **Notification** box to send an email when the snapshot is complete. Select from those listed or add email addresses to **Other recipients**. Separate email addresses with a comma. Then click **Confirm**.
5. When the snapshot is complete, look for changes in the **Captured Status** column.
6. Double-click a device to open the **Device Editor** and click to view details of the snapshot.

You can also set up Gluware to take snapshots automatically in system settings.

Set a default snapshot

Setting a default (baseline) snapshot designates that snapshot as the approved configuration for the device. When you take subsequent snapshots of the configuration, Gluware detects any deviations from the default. If the changes are the result of purposeful action, you can set the new snapshot as the default. If you were unaware of the changes made, you can take corrective action on the device using **Config Modeling**.

1. Go to **Config Drift and Audit** > **Devices**.
2. Select one or more devices.
3. Click and click **Confirm**. This sets the most recent snapshot as the default (baseline).

NOTE: You can also set a new default snapshot when comparing snapshots.

View configuration snapshots

View a device configuration snapshot

1. Go to **Config Drift and Audit** > **Devices**.
2. Double-click a device to open the **Device Editor** and click .
3. Click **Download** to save the information to a file.

View all available snapshots for a device

1. Go to **Config Drift and Audit** > **Devices**.
2. Double-click a device and click .
3. Select a snapshot and click to see the configuration.

View the snapshot log

When you take a snapshot of a device, a log is created.

1. Go to **Config Drift and Audit** > **Devices**.
2. Double-click a device and click to view **Activities** related to the device.
3. View the log:
   - Point to to quickly skim the log.
   - Double-click on the row to see the log in detail.

NOTE: Any errors appear in red. Common errors include incorrect or missing device credentials (e.g. password, serial number) indicating you're not connected to the device.

4. Optional: Click **Download** to send the log to your Downloads folder.
5. Click **Back** to return to the activity summary.

Tips for reviewing the log

- When you see an error or warning, you may need to inspect the lines above it to determine the cause.
- Click to pause scrolling.
- Click **Show Settings** to:
  - **Search for a text string** – Enter the text string and click **Enter**. Check the **Case-Sensitive** box to make the search case-sensitive. Clear the box to ignore case. Click > and < to see the occurrences found.
  - **Change the line label** – Select a line label from the Log Event # drop-down list. Select from:
    Log Event #
    Line Number
    Timestamp
    Time Passed
    Event Duration

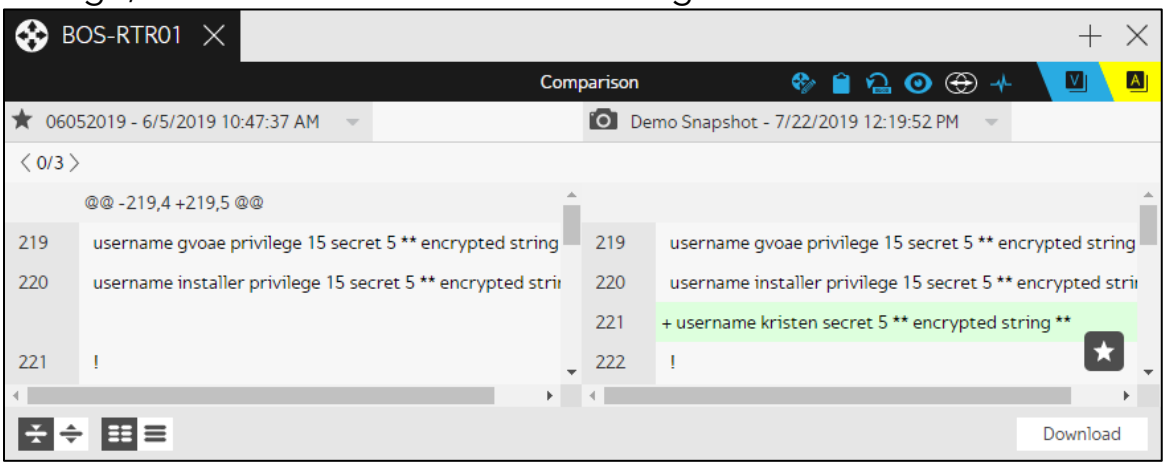
- **Filter the log** – Click . Check or clear the boxes to display just the levels you want. All levels are displayed by default.
- **See the source code file and line number that produced the log line** – Point to a line.

Log Levels	Description
Error	A problem that must be fixed
Warning	A problem that did not stop the process but should be fixed
Task	The beginning or the end of a step
Checkpoint	A significant point in the code
Info	General info about the process that does not fit in the other logging categories
Response	The raw interaction between the Gluware engine and the device
Debug	Low-level informational log messages usually related to the internal state of code variables. It's specific to how the code is working, as opposed to how the process is proceeding

Compare configuration snapshots

You can inspect two configuration snapshots for a device so comparison is easier. Differences are highlighted and four different views are available.

1. Go to **Config Drift and Audit** > **Devices**.
2. Double-click a device that has , a **Changed** status. The comparison between the default and the newest snapshot appears in the top pane. Changes are highlighted. The number of changes appears in angle brackets, e.g., <0/3>. If there is more than one change, click the **>** to see the next change.



3. Use to switch between Expanded and Compact views. Use to switch between Side-by-Side and Line-by-Line views.
4. Download the comparison to review and share.
5. To save the changed configuration as the new default for the device, click .

NOTE: You can compare any two snapshots. Select a different snapshot from the drop-down list at the top of a column.

Create a policy using Config Drift and Audit

You can create company-specific policies for your devices and then run audits against your device configurations to identify configuration policy violations. You can define simple or conditional rules for configuration statements. These rules support native vendor command lines, and filtering by OS, Concept Item show commands, and regular expressions (regex).

Need help with regex? Go to http://regex101.com/

Watch a video on policy-based configuration management at https://youtu.be/LSGTHcsL-Rg

Watch the 4.2 Config Audit updates video at https://youtu.be/UhQe_8BkNMw

1. Go to **Config Drift and Audit** > **Audit Policies**.
2. Click .
3. Name the policy and click **Create**.
4. Add a description of the policy.
5. Select the **Permission level**, 1, 2 or 3, for the policy from the drop-down list. See “Permission descriptions” and “Gluware roles and permissions” for details on how permission level impacts the ability to manage and run the audit policy.
6. Click **Add Rule**. You can also clone an existing rule by clicking
7. Name and describe the rule.
8. Select the **Severity** of the rule (Informational, Minor, Major, or Critical) from the drop-down list. You establish the meaning of each severity level.
9. Select the **Source** configuration to run the rule against.
    - **Latest Snapshot** – The most recent configuration snapshot
    - **Default Snapshot** – The default configuration snapshot

10. Optional: Add one or more constraints.
    - **Operating system** – Filter by operating system
    - **Concept item** – The **Concept Item** filters the configuration snapshot, returning a set of lines and the audit policy is run against the lines returned. The **Concept item** must already exist in Config Modeling.

      NOTE: When you select a **Concept Item**, a command, for example, a `show` command is displayed. The command cannot be run on a snapshot; however, the **Concept Item** will extract the same configuration lines that the command would produce. To see what gets returned using a **Concept Item**, audit a single device. The log for the audit will show what is extracted from the configuration snapshot.

      If the devices to be audited have several operating systems, create a rule for each OS and select the appropriate **Concept Item**.
    - **Scope** – Filter by regex
    - **Evaluate filtered results independently** – If filtering by **Concept Item**, check the box to evaluate each element in the Concept Item results independently. If unchecked, the lines returned by the **Concept Item** are treated as one block. (The Block Name will be ALL in the audit execution summary). Whether you evaluate each result independently or not impacts the number of violations reported. *See* the example below.
10. Define what the policy requires or forbids.
    - Select **Simple** if there are no conditions. Or create conditional statements by selecting **If...Then** or **If...Then...Else**.
    - For **Simple** rules, select a rule type, plain text or regex version:
        - **must contain** – All lines in the rule must occur in the filter results
        - **must not contain** – The lines in the rule **cannot** occur in the filter results
        - **must contain, ordered** – All lines in the rule must occur in the filter results. And the lines in the filter results must appear in the same order as in the rule

    - **must only contain, ordered** – The filter results can **only** contain the lines in the rule. And the lines in the filter results must appear in the same order as in the rule
- For conditional rules, you can define rules specific to certain devices; for example, SKU, OS version, etc. Select from the list of device fields.
- For simple or conditional rules:
    - Click **AND** or **OR** to add a logical operator.
    - Click **Add group** to add nested rules.
- In regex, you can include custom fields. The syntax for including a custom field is `${device.<customfieldname>}`
  Example: For the custom field Bandwidth, `${device.Bandwidth}`
  Make sure you use the correct capitalization of the custom field name. Go to **Settings** > **Custom Fields** to verify names.
- You can include variables that reference the discoverable properties on a device. The syntax for including a discoverable property is `${device.<discoverableproperty>}`
  Example: `${device.detectedHostName}`

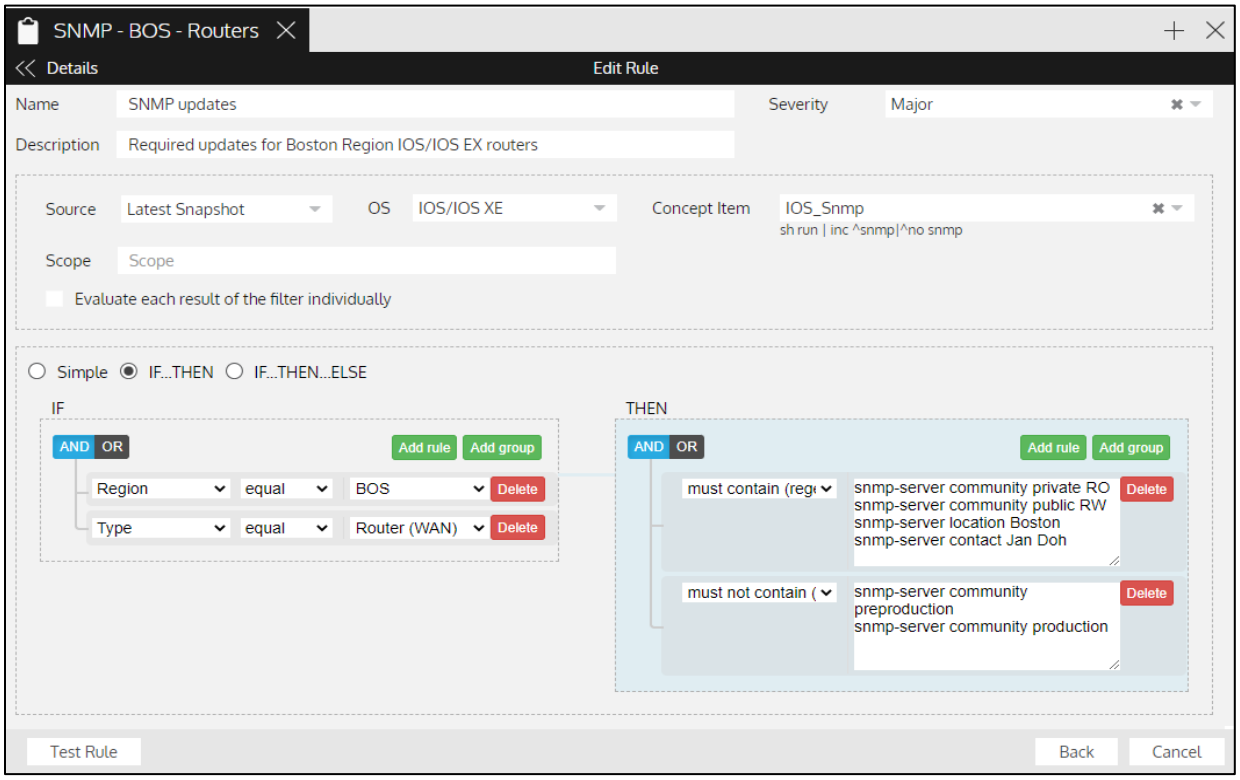
  The discoverable properties on a device are:
  `detectedRawTypeBase`
  `detectedTypeBase`
  `detectedComponents`
  `detectedHostName`
  `detectedOs`
  `detectedRawOs`
  `detectedRawVendor`
  `detectedSerialNumber`
  `detectedSku`
  `detectedSoftwareVersion`
  `detectedStack`
  `detectedTypeName`
  `detectedUptime`
  `detectedVendor`
  `name`

11. Optional: Click **Test Rule** to test the rule offline.
    - Paste the configuration you want to test in the **Test Data** box.
    - In the **Device Properties**, supply the value to test if your rule references a device property variable.
    - Click **Test**.
    - Select from the **Results** drop-down list if your filter returns more than one CLI group.
    - The passed/failed results are displayed in the **Rule** box.
    - Click **Cancel** to go back.
12. Click **Back**.
13. Optional: Click **Add Rule** to add additional rules.
14. Optional: Click ⠿ to drag and re-order any rule.
15. Save.

NOTE: You can also create a policy by cloning an existing policy. Select a policy and click .

You can import example policies from the Gluware Knowledge Base at https://support.gluware.com/hc/start. Click to import.

Example: SNMP policy for IOS routers



Example: Evaluate filtered results independently

The Concept Item IOS_User extracts the lines from the configuration snapshot regarding the local users configured on the device. For example, from a device that has two users defined:

```
{
    "Username": {
        "pod6user": ["username pod6user privilege 15 secret 5
$1$diD6$JEfT7oB3eyvl7jUylbcuz0"],
        "new_sqa": ["username new_sqa privilege 15 secret 5
$1$nUme$z3x7v5Ewp/EBr4.zobhzo0"]
    }
}
```

There is one block per user in this example, where one block is named `pod6user` and the other `new_sqa`. The data that is audited are the lines associated with each block. In this case, each block only has a single line.

If **Evaluate each result of the filter individually** is **not** checked, then the lines of each block are combined and audited as a single unit:

```
"username pod6user privilege 15 secret 5
$1$diD6$JEfT7oB3eyvl7jUylbcuz0"
"username new_sqa privilege 15 secret 5
$1$nUme$z3x7v5Ewp/EBr4.zobhzo0"
```

If a violation is found, it is reported using a Block Name of ALL.

If **Evaluate each result of the filter individually** is checked, then each block is audited separately and a violation may occur for each block. The Block Name in the results will indicate each block that has a violation.

Audit your configuration

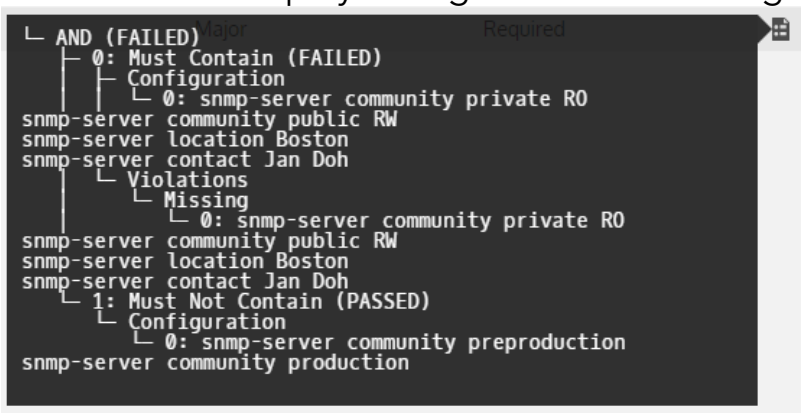
Run a policy audit to ensure that no changes have been made to devices that make them out of compliance.

1. Go to **Config Drift and Audit** > **Devices**.
2. Select the devices you want to audit.
3. Click .
4. Apply the audit to the current selection of devices, the current filter, or all devices. If using a filter and additional devices are added later, those devices will be included the next time the audit is run.
5. Select **Capture new snapshot** to capture a new snapshot for any rule using **Latest Snapshot** as the source. If the **Source** you selected for a rule is **Default Snapshot**, the default configuration will be used as the source.
6. Select the audit policy to run from the drop-down list.
7. Run or schedule the audit:
    - Click **Start Audit** to run the audit immediately.
    - Click **Schedule Audit** to define the schedule. Check a **Notification** box to send an email when the audit is complete. Select from those listed or add email addresses to **Other recipients**. Separate email addresses with a comma. Then click **Confirm**.
8. Click **View Results**.

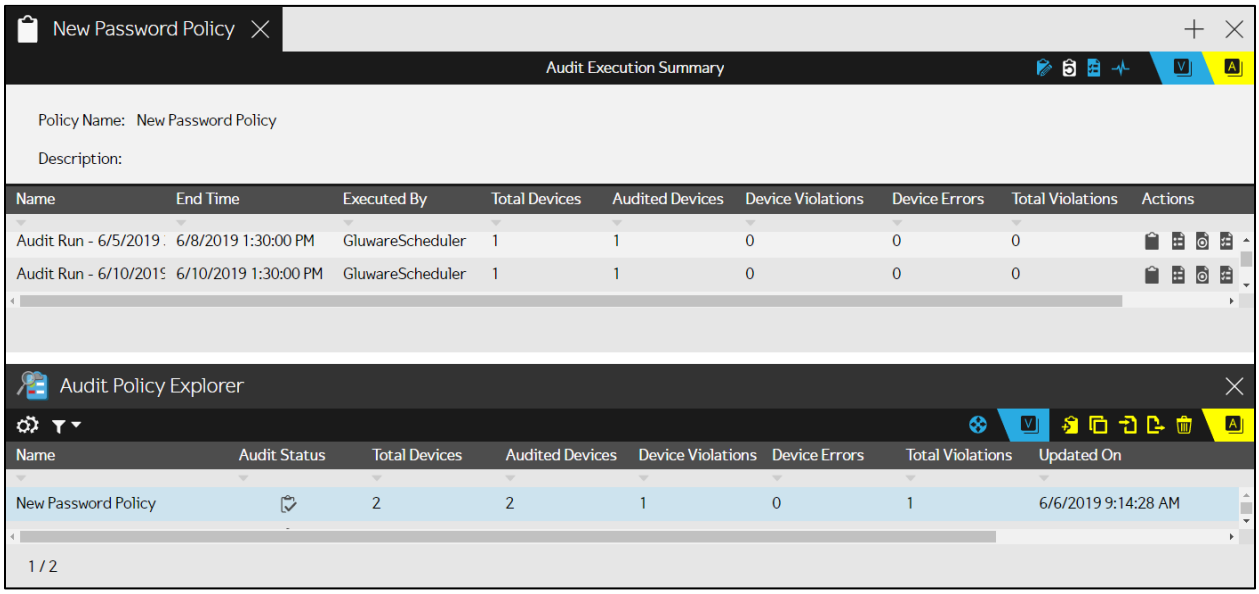
NOTES: It may take some time for the audit to run, so **View Results** may not be immediately available. You can continue to work in Gluware while the audit is run.

9. Click to expand the list of violations on a device.

10. Point to to display a diagram of the rule logic.

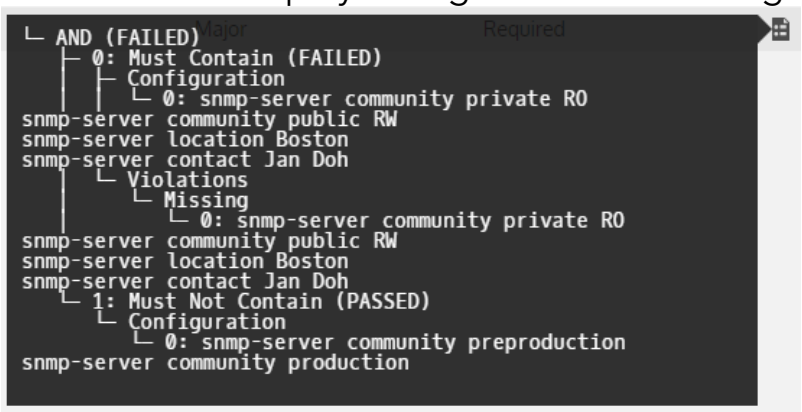


11. Optional: Click **Download Results** for the pass/fail status of each rule in CSV format.
12. Optional: Click **Download Details** to see the results of each rule in JSON format.
13. Click to see the **Audit Execution Summary**.
    - Click to review the audit policy at the time of execution.
    - Click to review the logs of the audit.
    - Click to view the devices that were audited.
    - Click to view the audit results.
14. Optional: Click to run the audit policy against the same set of devices and then click **View Results**.



View audit results

1. Go to **Config Drift and Audit** > **Audit Policies**.
2. Double-click a policy.
3. Click to expand the list of violations on a device.
4. Point to to display a diagram of the rule logic.



5. Optional: Click **Download Results** for a status summary of each rule in CSV format.
6. Optional: Click **Download Details** to see the results of each rule in JSON format.
7. Click to see the **Audit Execution Summary**.
    1. Click to review the audit policy at the time of execution.
    2. Click to review the logs of the audit.
    3. Click to view the devices that were audited.
    4. Click to view the audit results.
8. Optional: Click to run the audit policy against the same set of device and then click **View Results**.

View and edit policy details

1. Go to **Config Drift and Audit** > **Audit Policies**.
2. Double-click a policy and click .
3. Update the name, permission level, or description.
4. Select a rule you want to update and click .
5. Make any changes and click **Back**.
6. Click to drag and re-order any rule.
7. Click **Save**.
8. Click **Download** to export the policy and rules to a JSON file.

View policy history

View when a policy was executed

1. Go to **Config Drift and Audit** > **Audit Policies**.
2. Double-click a policy and click .

View all previous policy activity

1. Go to **Config Drift and Audit** > **Audit Policies**.
2. Double-click a policy and click .

Export a policy

You can export one or more policies from Gluware to a JSON file and then import those policies in another organization or Gluware system.

1. Go to **Config Drift and Audit** > **Audit Policies**.
2. Select one or more policies and click .

Import a policy

You can export a policy to a JSON file, modify it, and import the policy.

> **NOTE:** The import file must have a unique name and any referenced Concept Items must already exist in the organization.
>
> You can import example policies from the Gluware Knowledge Base (https://support.gluware.com/hc/start).

1. Go to **Config Drift and Audit** > **Audit Policies**.
2. Click .
3. Drag and drop the JSON file in to the **Audit Policy Explorer** or click **Import from File**.

Delete a policy

1. Go to **Config Drift and Audit** > **Audit Policies**.
2. Select the policy and click .

OS management overview

The Gluware **File Server** provides a VM server to store and manage OS image, ROMMON, Cisco NX-OS Kickstart, and ASDM files. Gluware **OS Manager** allows you to create and manage OS plans and an optional Catalog of images. These features allow you to perform safe, controlled upgrades or downgrades.

To use File Server and OS Manager, you'll need an **OS Manager license** and the **OS Management package** installed.

Watch a video on OS Manager at https://youtu.be/WAWfhO79rRE

In File Server

File Server quick reference

Add a folder to File Server

Rename, move, or delete a folder on File Server

Add an OS image or other file to File Server

Move, rename, or delete a file on File Server

Change the properties of a file

View the past actions performed on a file

In OS Manager

OS Manager quick reference

Prepare devices for OS management

Add an entry in the OS Catalog

Edit an OS Catalog entry

Delete an OS Catalog entry

Create an OS plan

Edit an OS plan

Delete an OS plan

Move devices from one OS plan to another

Run an OS plan

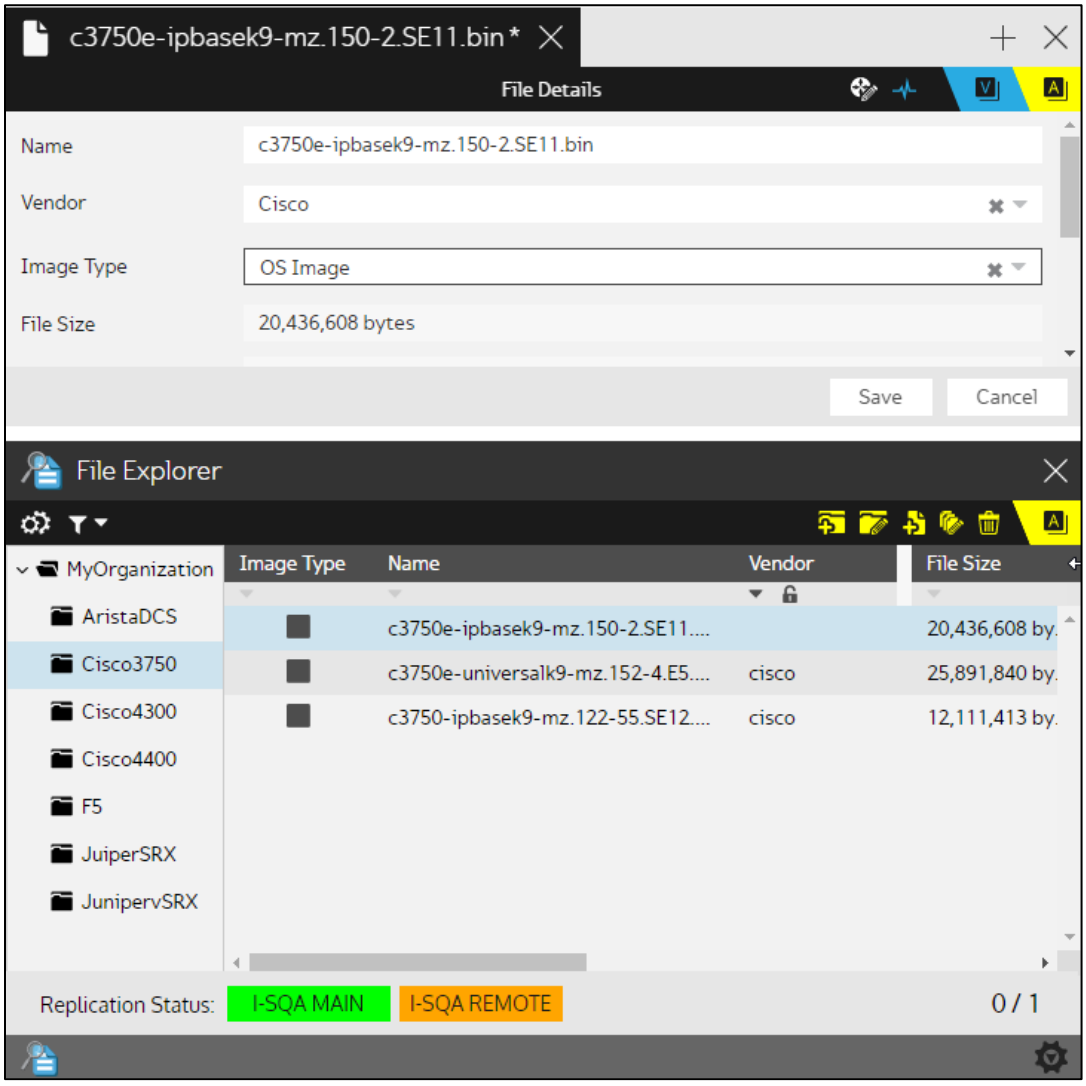
View the device log

Reboot a device

File Server quick reference

The Gluware **File Server** allows you to store and manage OS image, ROMMON, Cisco NX-OS Kickstart, and ASDM files. All standard folder and file operations are available: add, move, rename, delete, and edit properties.

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



Actions

Add Folder – Add a folder or subfolder

Rename Folder – Rename the selected folder

Add File – Upload one or more files

Edit Files – Change the properties of a file or files: the file name, vendor, or image type

Delete Files – Delete the selected files

Views

Details – View the file properties

Activities – View the past activities performed on a file

File Status

UPLOADING – File is being transferred to Gluware

UPLOADED – File has been transferred to Gluware, but not yet to the File Server. If the file stays in this status, delete the file and add it again

SYNCING – File is being transferred from Gluware to the master File Server and remote File Servers

SYNCED – File has been transferred from Gluware to the master File Server and remote File Servers

ERROR – File cannot be transferred. Delete the file and add it again

Replication Status

Server – UNKNOWN, NOT INSTALLED, DISABLED, or CONFIGURING
Server – IN SYNC
Server – SYNCING
Server – OFFLINE
Server – ERROR

Add a folder to File Server

The first folder you add will be the parent folder. You can only have one top-level folder, but you can have as many subfolders as you want.

1. Go to **File Server**.
2. If you are adding a subfolder, select the folder you want to add it to.
3. Click .
4. Name the folder.
5. Save.

Rename a folder

1. Go to **File Server** and select the folder you want to rename.
2. Click .
3. Rename the folder.
4. Save.

Move a folder

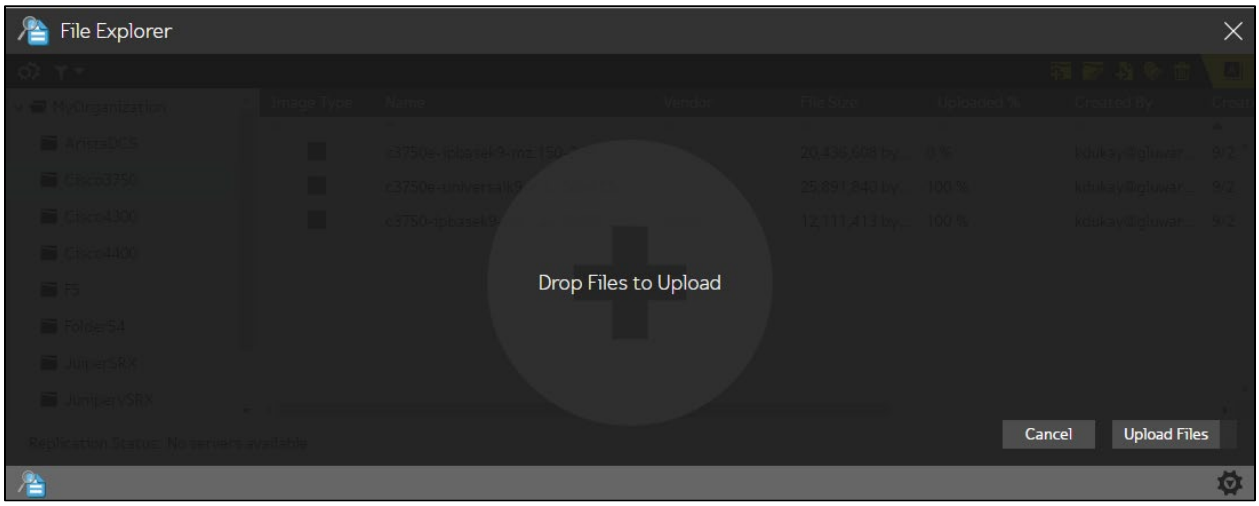
Drag and drop the folder to the new parent folder.

Delete a folder

1. Go to **File Server** and select the folder you want to delete.
2. Click beside the folder name.
3. Click **Confirm**. The folder as well as all the files and subfolders are deleted.

Add an OS image or other file to File Server

1. Go to **File Server** and select the folder you want to add the file or files to.
2. Click .
3. Do one of the following:
    - Drag and drop the file or files into **File Server** and click **Save**.
    - Select **Upload Files**, select the file or files you want to upload, and click **Open**.



4. Optional: Select a vendor from the drop-down list.
5. Optional: Select an image type from the drop-down list.
6. Optional: Select a Catalog Entry from the **Catalog Entry** drop-down list if the Catalog is enabled.
7. Save.

NOTE: If you want to add many files at one time, you can assign vendor, image type, or OS plans to each file later by changing the properties of the file.

Move, rename, or delete a file on File Server

Rename a file

1. Go to **File Server** and select the file you want to rename.
2. Click .
3. Rename the file.
4. Save.

Move a file

Drag and drop the file to the new folder.

Delete a file

1. Go to **File Server** and select the file you want to delete.
2. Click .
3. Click **Confirm**.

Change the properties of a file

In **File Server**, you can change the name, vendor, and image type of a file or make the same change to multiple files.

> **NOTE:** The internal file ID is included in the file details to help you troubleshoot.

Change one file

1. Go to **File Server** and double-click the file in the File Explorer.
2. Make changes to the file info in the top of the screen. Some fields are read-only.
3. Save.

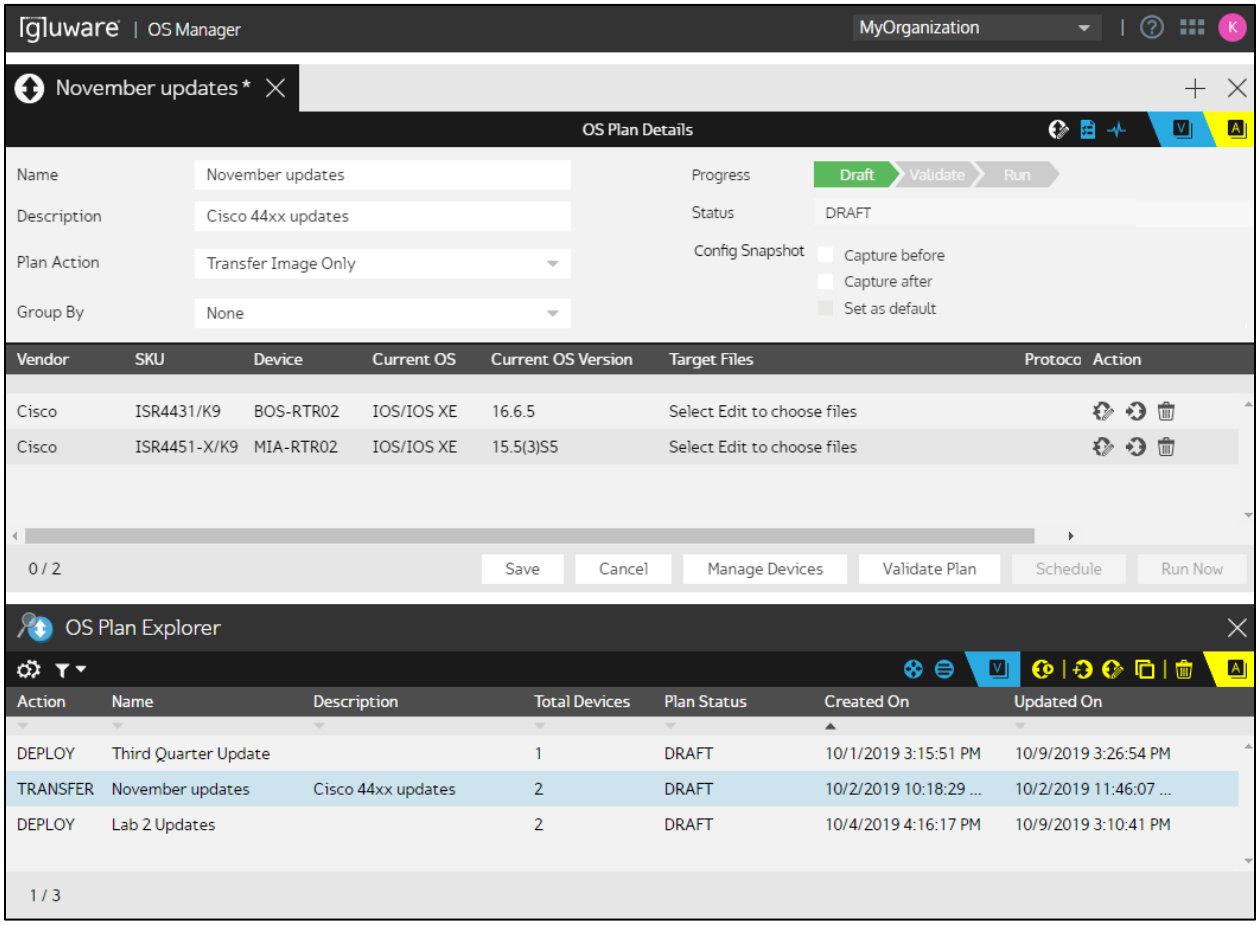
Make the same change to more than one file

1. Go to **File Server** and select the files in the File Explorer.
2. Click . A Multi-Edit tab opens in the top panel. Click **View All** to see the list of files you are editing.
3. Click a radio button next to the field and make changes. Some changes are restricted since they would apply to multiple files.
4. Save.

View the past actions performed on a file

1. Go to **File Server** and double-click the file in the **File Explorer**.
2. Click .

OS Manager quick reference



Views

OS Catalog Explorer – Switch to the OS Catalog Explorer

OS Plan Explorer – Switch to the OS Plan Explorer

Device Explorer – Switch to the Device Explorer

OS Plan Execution

Actions

Add Catalog Entry – Create a new Catalog Entry

Edit Catalog Entry – Change the name, SKUs, or images associated with the selected Catalog Entry

Clone Entry or Plan – Makes a copy of the selected Catalog Entry or OS plan

Run Report – Run a Data Explorer report on demand or on a schedule

Delete Entry or Plan – Delete the selected Catalog Entry or OS plan

Run OS Plan – Run the Plan Action associated with the selected plan

Add OS Plan – Create a new OS plan

Edit OS Plan – Change the name, plan action, devices, or images associated with the associated selected plan

Reboot Devices – Reboot the selected devices

Edit in OS Plan – Change the image associated with the device

Move to Another OS Plan – Move a device from one OS plan to another

Delete From OS Plan – Remove the device from the OS plan

Plan Status

DRAFT – Plan was created and saved but not yet validated

VALIDATING – Validation is running

VALIDATED – Validation was successful. The plan can now be run

INVALID – Validation failed. The plan must be edited and fixed, which will return the plan status to DRAFT

SCHEDULED – Plan now scheduled and will run at the scheduled time

RUNNING – Plan is running

COMPLETE – Plan has successfully run; however, some devices may have failed to be updated

CANCEL PENDING – Processing Cancel request by user

CANCELED – Plan was running and was canceled before the execution was completed

ERROR – Plan execution failed

Prepare devices for OS management

You'll want to verify that the following fields are defined, when appropriate, for the devices you want to manage in OS Manager.

Management State

Only devices that have a **Management State** of **Managed** will appear in **OS Manager**. If a device you want to update does not appear in OS Manager, you'll need to change the Management State in **Device Manager**.

1. Go to **Device Manager**.
2. In the **Device Explorer**, select the device or devices and click .
3. Select **Managed** from the **Management State** drop-down list.
4. Save.

File Server

Ensure that the **File Server** for the device is specified.

1. Go to **Device Manager**.
2. In the **Device Explorer**, select the device or devices and click .
3. Select a **File Server** from the drop-down list.
4. Save.

SSH

If using SCP for file transfers, devices need to be configured for SSH v2.

VRF

If access to File Server will use an interface in a VRF, provide the VRF name.

1. Go to **Device Manager**.
2. In the **Device Explorer**, double-click the device.
3. Enter the **VRF** name in the **VRF** field.
4. Save.

HA Group

Identify an HA pair when applicable. All the devices in the HA Group have to be in the same OS plan and they will all be upgraded.

1. Go to **Device Manager**.
2. In the **Device Explorer**, double-click one of the devices in the HA pair.
3. Click **Add** next to **HA Group**.
4. Select the device that is paired from the list.
5. Save.
6. If in **OS Manager**, click **Back**.

Non-disruptive upgrades

Enable non-disruptive upgrade support for devices that support it.

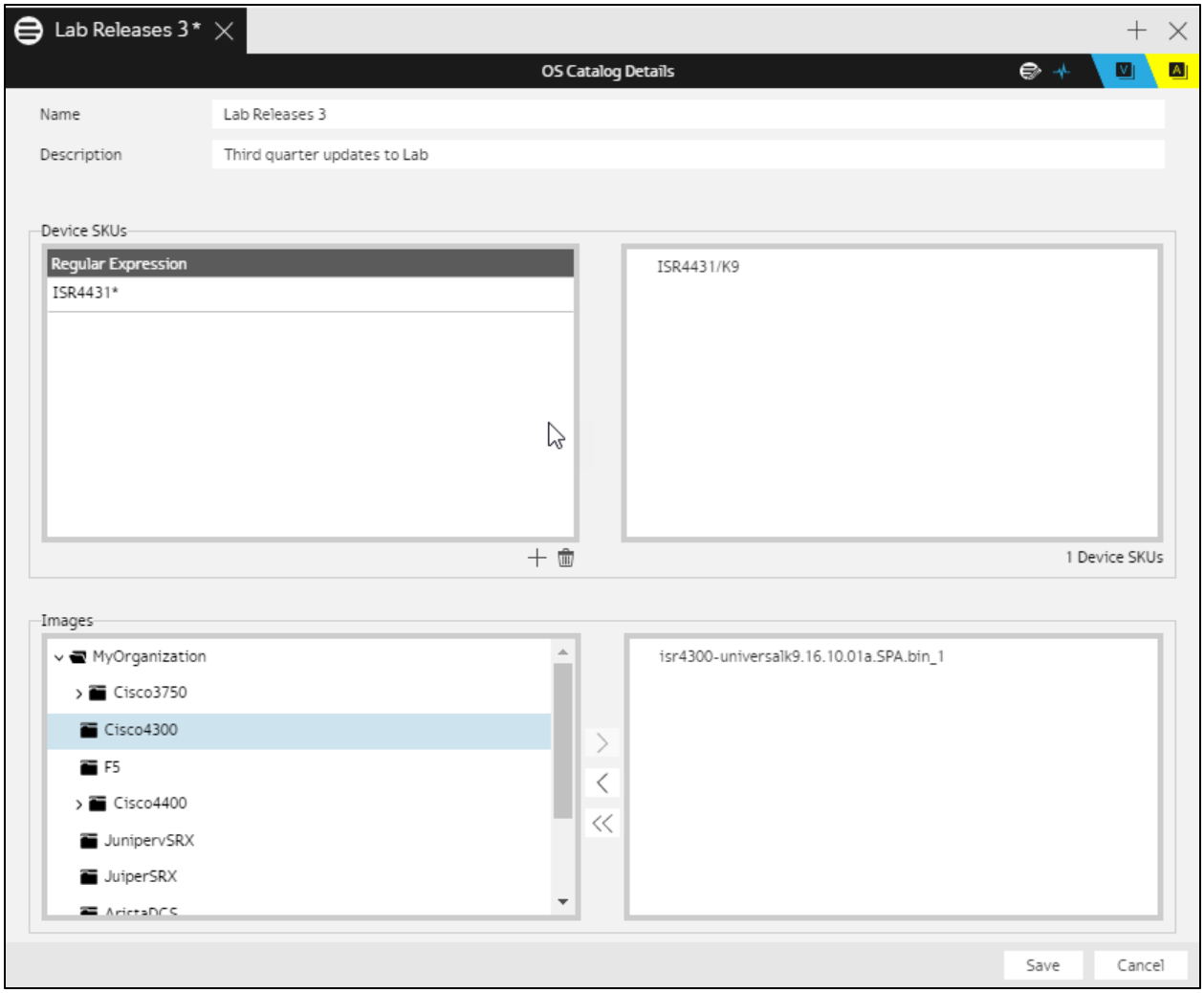
1. Go to **Device Manager**.
2. In the **Device Explorer**, select the device or devices and click .
3. Check the **In-Service Software Upgrade** box.
4. Save.

Add an entry in the OS Catalog

The **OS Catalog** allows you to associate specific OS images with one or more SKUs. Use of the OS Catalog is optional, but its use can help ensure operators only apply approved OS images to devices.

> **NOTE:** The Catalog must first be enabled in system settings and each organization must enable its own Catalog.

1. Go to **OS Manager** > **Catalogs**.
2. Click to add an entry to the OS Catalog.
3. Name the entry and click **Create**.
4. Add a description of the Catalog entry.
5. Click + and enter a regular expression to add a specific SKU or SKUs to the Catalog entry.
6. Click + again to add another regular expression.
7. In the **Images** box, select an image that you want to associate with the SKUs and click .
8. Select any additional images that you want to associate with the SKUs.
9. Save.


Lab Releases 3*
OS Catalog Details
Name
Lab Releases 3
Description
Third quarter updates to Lab
Device SKUs
Regular Expression
ISR4431*
ISR4431/K9
1 Device SKUs
Images
MyOrganization
Cisco3750
Cisco4300
F5
Cisco4400
JunipervSRX
JuiperSRX
isr4300-universalk9.16.10.01a.SPA.bin_1
Save
Cancel

Edit an OS Catalog entry

1. Go to **OS Manager** > **Catalogs**.
2. Select the OS Catalog entry you want to edit and click .
3. Do any of the following:
    - Change the name or description.
    - Click + and enter a regular expression to add a specific SKU or SKUs to the Catalog entry.
    - Select an existing regular expression and click to delete it.
    - In the **Images** box, select an image that you want to associate with the SKUs and click .
    - Select any images you want to remove and click .
4. Save.

Delete an OS Catalog entry

1. Go to **OS Manager** > **Catalogs**.
2. Select the OS Catalog entry you want to delete and click .
3. Click **Confirm**.

Create an OS plan

You'll need to create an OS plan to upgrade or downgrade a device or devices. Only devices that have a **Management State** of **Managed**, that have been discovered in Device Manager, and are supported, appear in **OS Manager**. You can find the devices currently supported at https://gluware.com/supported-platforms/.

Create the plan

1. Go to **OS Manager** > **Devices**.
2. Select the devices that you want to add to the plan. Only devices that have been discovered and are supported in OS Manager are listed in the OS Device Explorer.
3. Click .
4. Name the plan and click **Create**. The **OS Plan Explorer** is displayed.
5. Add a description of the plan in the upper pane.
6. Select the action you want to take from the **Plan Action** drop-down list:
    - **Transfer Image Only**
    - **Deploy New Image**
7. In the **Group By** drop-down list, select **None** if you want to see a list the all the devices instead of a list grouped by SKU.
8. Check a **Config Snapshot** box to take a configuration snapshot:
    - **Capture before** – Takes a configuration snapshot before implementing the plan action
    - **Capture after** – Takes a configuration snapshot before implementing the plan action. If automatic configuration snapshots are set up for OS updates in system settings, this option is selected and cannot be changed
    - **Set as default** – Designates the after snapshot as the default
9. Save.

NOTE: You can also create an OS plan by cloning an existing plan. Simply select a plan and click

Associate an image with a SKU or device

1. Click next to the SKU or device in the OS plan.
2. Select the **Image Source**.
3. Select the image or images to associate with the SKU or device.
4. Click .
5. Save.
6. Click **Back** to return to the OS plan.

Edit an OS plan

NOTE: You can't edit a plan that has a status of COMPLETE.

1. Go to **OS Manager** > **OS Plans**.
2. Double-click the **OS Plan** you want to modify.
3. Do any of the following:
    - Change the plan name or description.
    - Change the **Plan Action**.
    - Change the **Group By** setting.
    - Change the **Config Snapshot** setting.
4. Save.

Associate a new image with a SKU or device

1. Click next to the SKU or device in the OS plan.
2. Select the **Image Source**.
3. Select the image to associate with the SKU or device.
4. Click .
5. Save.
6. Click **Back** to return to the OS plan.

Add or remove target devices

1. Click next to the SKU or device you want to delete.
2. Click **Confirm**.

OR

1. Click **Manage Devices**.
2. Do any of the following:
    - Select an Available Device and click Add
    - Select a Selected Device and click Remove
    - Click Remove All
3. Save.
4. Click **Back** to return to the OS plan.

Move a SKU or device to another OS plan

1. Click next to the SKU or device in the OS plan.
2. Enter a name for a new plan or select an existing plan from the drop-down list.
3. Click **Move**.
4. Save.

Move devices from one OS plan to another

If you have problems when validating a plan, you may want to move the device or devices that are problematic to another plan.

1. Go to **OS Manager** > **OS Plans**.
2. Double-click the OS plan you want to remove the devices from.
3. Click next to the SKU or device in the OS plan.
4. Enter a name for a new plan or select an existing plan from the drop-down list.
5. Click **Move**.
6. Save.

Run an OS plan

Before you run an OS plan,

- Check that the Plan Execution guidelines defined in system settings for your organization are appropriate for the plan.
- Validate the plan before you run it.

Once you run an OS Plan and the status is COMPLETE, the plan becomes read-only and cannot be run again.

Best practices

- Locating your **File Server** close to your devices can reduce transfer time.
- Use of TFTP is recommended. You can enable TFTP in **Settings** > **Organization** > **OS Manager**.
- Download and review the log file for any device that fails.

Validate and run the OS plan

1. Go to **OS Manager** > **OS Plans**.
2. Select the OS plan you want to validate and run and click .

Validate the plan

1. Click **Validate Plan**.
2. Optional: Click **Stop Validation** if you see errors. Click **Validate Plan** to restart validation. Click **Download** to send the log to your Downloads folder.
3. Click **Back** to return to the OS Plan.

Move a SKU or device to another OS plan

If you have problems when validating the plan, you may want to move the device or devices that failed to another plan.

1. Click next to the SKU or device in the plan that you want to move.
2. Enter a name for a new plan or select an existing plan from the drop-down list.
3. Click **Move**.
4. Save.

Run the OS plan now

1. Click **Run Now**. During OS plan execution, there are six possible phases:
   INIT
   TRANSFER
   UPGRADE
   REBOOT
   VERIFICATION
   FINAL
   Not every device goes through all phases. In the INIT phase, Gluware checks the health of the device and will abort the run if the device is in an unhealthy state.

   When the plan has run, the execution status is displayed. The total number of devices impacted by the plan is shown, as well as the number of devices successfully updated and the number of failures.
2. Click or double-click the device to view the execution log for the device.
3. If any devices failed, click **Create New Plan From Failures**, name the new plan, and click **Create**.
4. Optional: Click **Download** to send the device log to your Downloads folder.

Schedule the OS plan

1. Click **Schedule OS Plan**.
2. Set the schedule date and time.
3. Optional: Check the **Notify me when work completes** checkbox.
4. Click **Confirm**.

View the device logs

Once an OS plan has run and its status is COMPLETE, you view the log for each device impacted by the plan.

1. Go to **OS Manager** > **OS Plans**.
2. Double-click the COMPLETE **OS Plan** you want to view the logs for. The total number of devices impacted by the plan is displayed, as well as the number of devices successfully updated and the number of failures.
3. View the log:
    - Click to view the log for a device.
    - Double-click on the row to see the log in detail.

NOTE: Any errors appear in red. Common errors include incorrect or missing device credentials (e.g. password, serial number) indicating you're not connected to the device.

4. Optional: Click **Download** to send the log to your Downloads folder.

Tips for reviewing the log

- When you see an error or warning, you may need to inspect the lines above it to determine the cause.
- Click to pause scrolling.
- Click **Show Settings** to:
    - **Search for a text string** – Enter the text string and click **Enter**. Check the **Case-Sensitive** box to make the search case-sensitive. Clear the box to ignore case. Click > and < to see the occurrences found.
    - **Change the line label** – Select a line label from the Log Event # drop-down list. Select from:
      Log Event #
      Line Number
      Timestamp

Time Passed
Event Duration

- **Filter the log** – Click . Check or clear the boxes to display just the levels you want. All levels are displayed by default.
- **See the source code file and line number that produced the log line** – Point to a line.

Log Levels	Description
Error	A problem that must be fixed
Warning	A problem that did not stop the process but should be fixed
Task	The beginning or the end of a step
Checkpoint	A significant point in the code
Info	General info about the process that does not fit in the other logging categories
Response	The raw interaction between the Gluware engine and the device
Debug	Low-level informational log messages usually related to the internal state of code variables. It's specific to how the code is working, as opposed to how the process is proceeding

Delete an OS plan

1. Go to **OS Manager** > **OS Plans**.
2. Select the OS plan you want to delete and click .
3. Click **Confirm**.

Reboot a device

1. Go to **Device Manager** or **OS Manager** > **Devices**.
2. In the **Device Explorer**, select one or more devices.
3. Click .
4. Click **Confirm**.

Model a configuration

The Gluware **Config Modeling** allows you to standardize network features by leveraging your existing, validated CLI. Once onboarded to the **Config Modeling**, the CLI becomes a feature that can be deployed to network devices and enforced at scale. You can model as many or as few features as you want. You can standardize AAA, NTP, SYSLOG, and other network-wide functions. And you can address pain points such as QoS management.

To use **Config Modeling**, you'll need:

- A license for **Config Modeling**
- The **Config Modeling Foundations** package installed
- The **Config Modeling Kit** packages for your device types installed

If you want to create a custom feature template, you'll also need:

- A license for **Workflows**
- The **Workflows for Config Modeling** package installed

Install packages

Here are the typical steps you take to model and deploy a network feature:

1. In **Workflows**, create a feature template and install it.
   Design a new network Feature type

2. In **Config Modeling**, select existing **Concept Items** or create a new one. Then create **CLI Command Lists**, **CLI Command Groups**, **Features**, and **Assemblies** to fully define the feature. Config Modeling also allows you to preview the feature to ensure it works as intended.
   Create a Concept Item
   Create a CLI Command List
   Create a CLI Command Group

Create a Feature
Create an Assembly
Associate an Assembly with a node
View the relationships in your model
Preview the modeled Feature
Review the logs
Provision nodes

To quickly create model instances, use Intelligent Model Discovery.

3. Create a distribution package containing Feature definitions and instances to be installed on your production environment.
   Package a Feature for distribution

For an example, *see*: Example: Model an SNMP feature

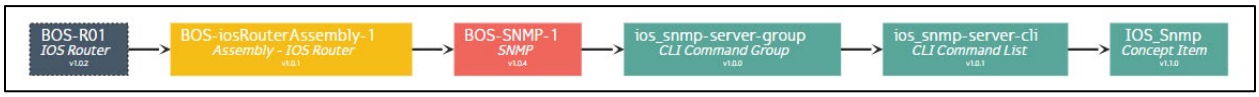
Watch a video about config modeling at
https://youtu.be/pANntfCKTFw

Example: Model an SNMP feature

Modeling a configuration feature involves several steps. We'll take you through an example of modeling an SNMP feature for an IOS Router so you can see how it all fits together.

First, you'll ensure you have the proper packages installed in your organization. Then you create a Feature Set for your organization that will seed required components in **Config Modeling**.

Each model requires, from right to left: a **Concept Item**, a **CLI Command List**, a **CLI Command Group**, a **Feature**, an **Assembly**, and **Nodes** representing devices.



Here's how you create and associate these components into a model:

Step 1. Install packages

Step 2. Design an SNMP Feature type

Step 3. Select a Concept Item

Step 4. Create a CLI Command List for SNMP

Step 5. Create a CLI Command Group for SNMP

Step 6. Create a Feature for SNMP

Step 7. Create an Assembly for your IOS routers

Step 8. Associate the Assembly with nodes

Step 9. View the relationships in your SNMP model

Step 10. Preview the SNMP Feature

Node state assessment

Config Modeling allows you to issue show commands to determine if a device is performing as expected. You can assess the state before and after provisioning or an OS upgrade. You can also assess the state on demand.

To use state assessment, you'll need:

- A license for **Config Modeling**
- The **Config Modeling Foundations** package installed
- The **Config Modeling Kit** packages for your device types installed

Step 1: Create a CLI State Item

Step 2: Create a CLI State Assessment Policy

Optional Step 3: Create a CLI State Assessment Query

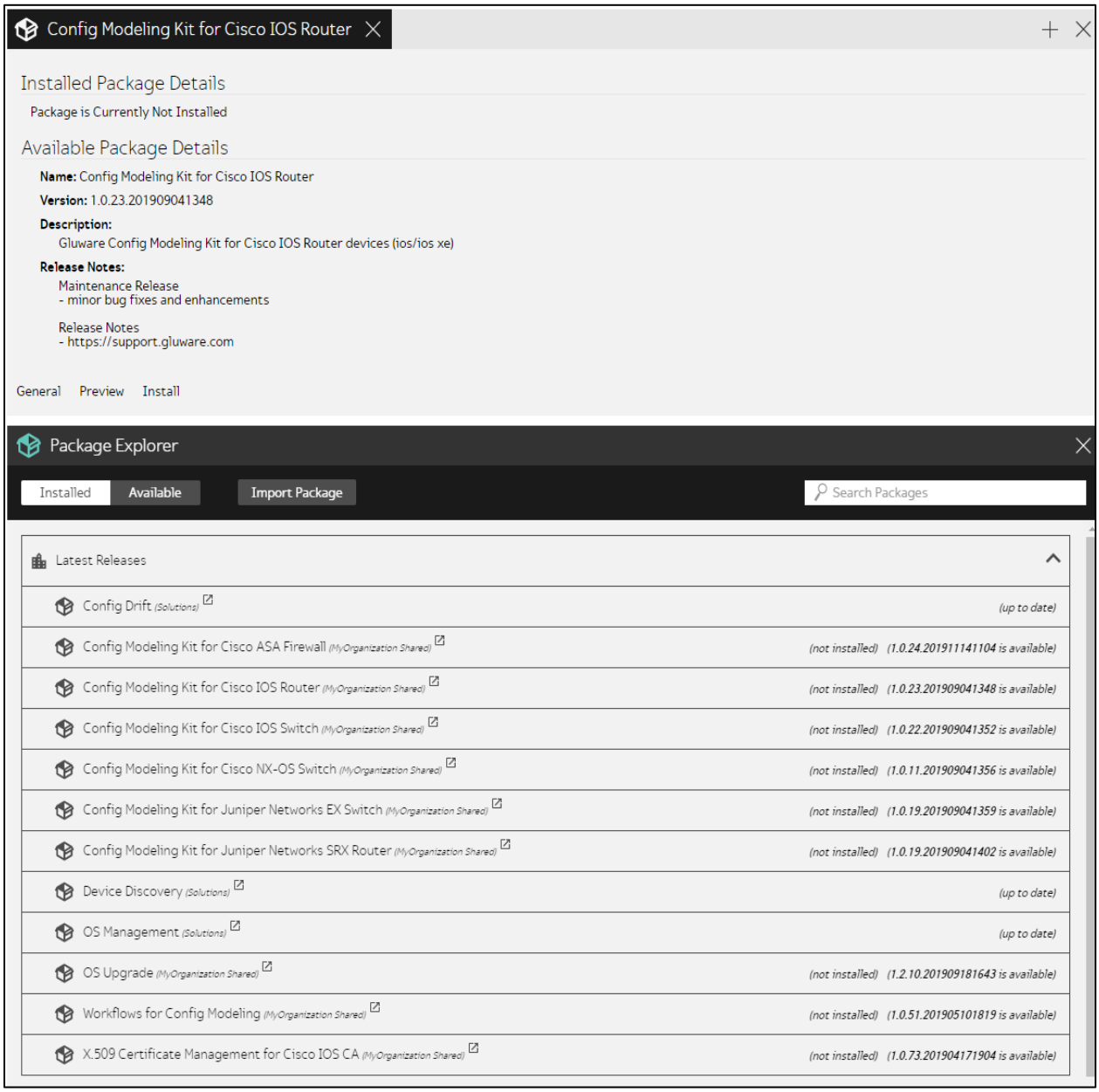
Step 4: Associate a CLI State Assessment Policy with an Assembly

Step 5: Assess the state of a node

Solutions Manager quick reference

Solutions Manager is where you find and install packages from Gluware that provide the basic functionality for **Device Manager**, **Config Drift and Audit**, **OS Manager**, and **Config Modeling**.

Make sure you install packages in the appropriate organization.



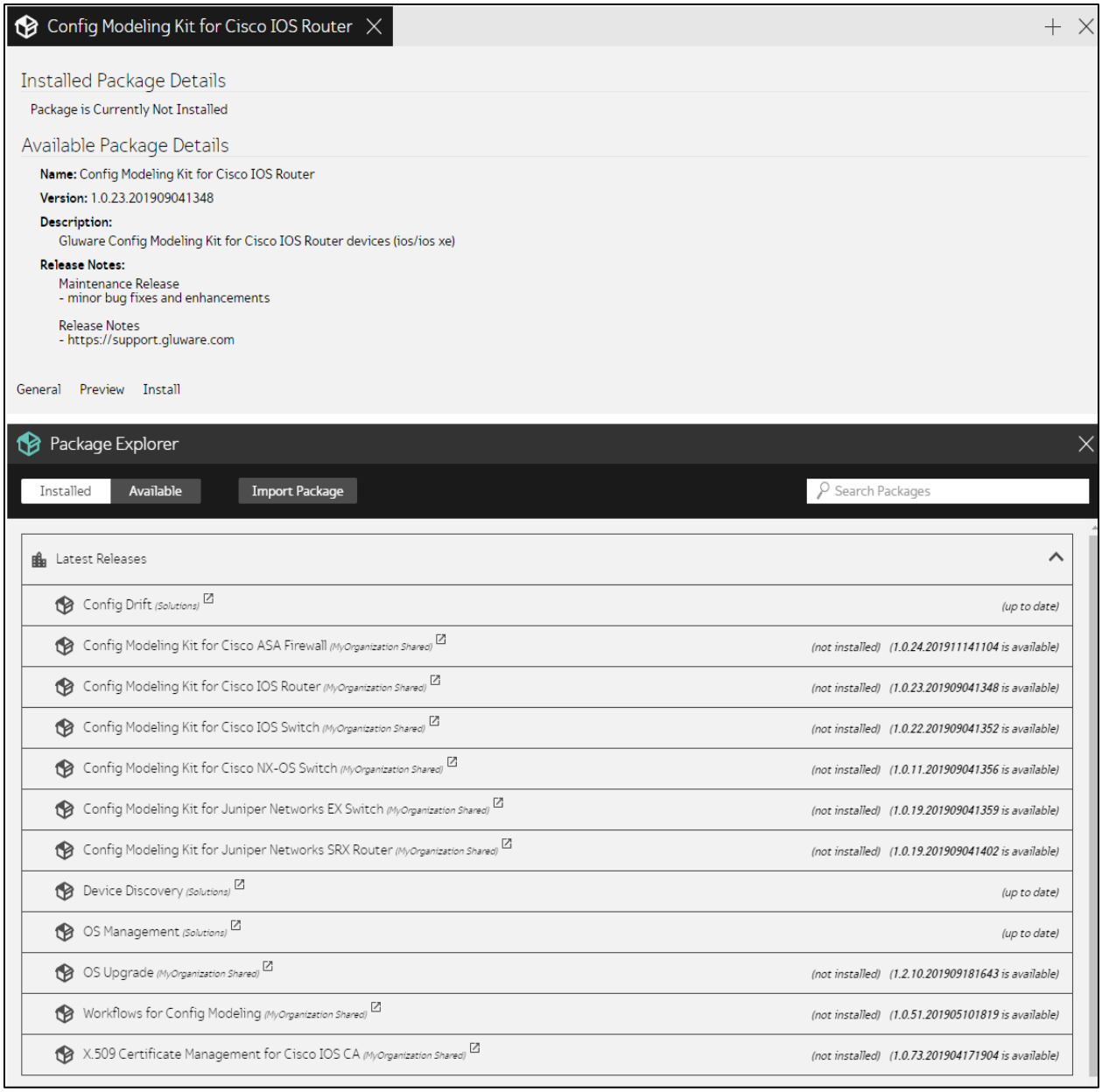
Install packages

Gluware solutions, Config Modeling Kits (CMKs), and Workflows come as packages that you must install. Before installing these packages, make sure your organizations are set up in Gluware. Each relevant package must be installed in the appropriate organization.

Updates to packages are also available.

1. Ensure you're in the organization you want to install the package in.
2. Go to **Solutions Manager** > **Available Packages**.
3. Search for the package you want to install in the **Package Explorer**.
4. Double-click on the name of the package to display the package details. You'll see "Package is Currently Not Installed" in the top pane if the package is not yet installed.
5. Select **Preview** and then click **Preview Package Installation**. This doesn't install the package but can alert you to any potential problems. Look for "Preview Completed!" when the preview script runs successfully. A list of any existing files and/or instances that will be updated are also displayed. Any potential problems with the installation will appear as red error messages. Contact Gluware Support (support@gluware.com) if you can't interpret or resolve errors.
6. Select **Install** and then click **Install Package**. You'll see "Installation Completed!" when the installation is successful. Any problems with the installation will appear as red error messages.

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


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)

Import a capsule

Updates to Gluware On Prem systems are delivered via capsules to be imported in **Solutions Manager**.

1. Ensure you're in the organization you want to install the updates in.
2. Go to **Solutions Manager** and click **Import Package**.
3. Drag and drop the capsule file into the **Package Explorer**. The updated packages will be listed under **Latest Releases** in the **Package Explorer**.

Import your own package

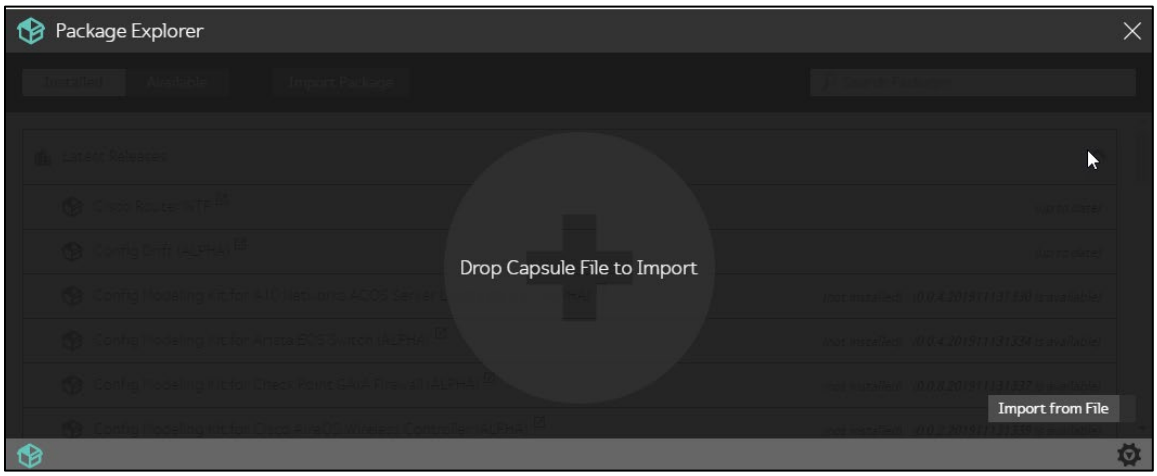
You can copy a network feature created in one organization to a different organization.

Create a Feature capsule

1. Go to **Solutions Manager** > **Installed Packages**.
2. Expand the **Design** folder and double-click the **Network Feature Distribution** workflow.
3. Click **Next**.
4. Select the **Feature Set** you want to copy to another organization from the drop-down list and click **Next**.
5. In the **Options** list, select the **Feature Policies** you want to include and click →. The ↠ selects all the available Feature Policies.
6. Click **Next**.
7. Provide a name, description, and version description, and click **Finish**. The Feature capsule will be added to your Downloads folder.

Import the Feature

1. Ensure you're in the organization in which you want to install the package.
2. Go to **Solutions Manager** and select **Import Package**.
3. Drag and drop the Feature capsule into the **Package Explorer** or click **Import from File**.



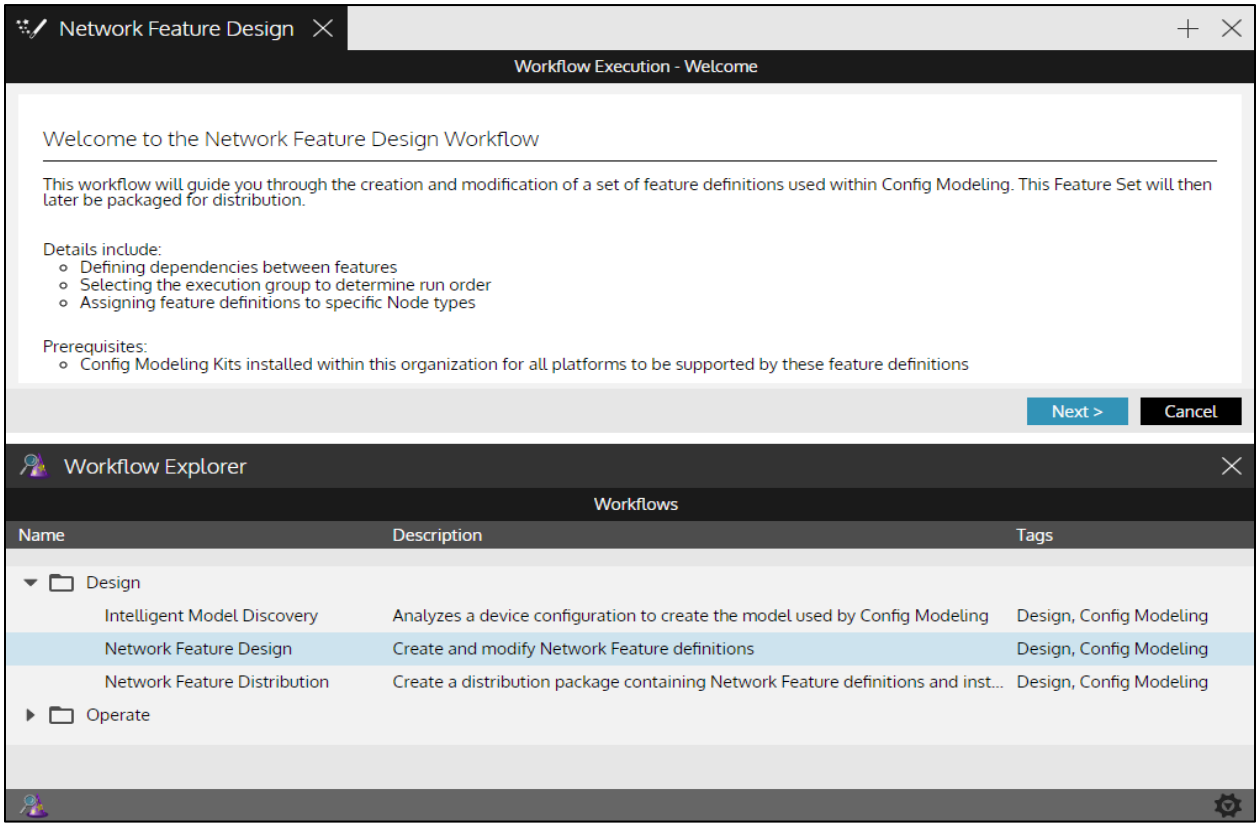
Workflows quick reference

Workflows provide guided execution for a range of different activities applicable to Gluware–based capabilities. Workflows are tied to specific Gluware capabilities. The **Workflow Explorer** provides a list of available workflows for the current organization.

Workflows are only available to Gluware users assigned to a specific standard Gluware role or to a customized role with Workflows permissions.

Category	**Workflow Name**	**Role Assignment**
Design	Network Feature Design	System Admin; Level 4
Design	Network Feature Deployment	System Admin; Level 4
Design	Intelligent Model Discovery	System Admin; Level 4
Operate	CA Manager for Cisco IOS	System Admin; Level 4

The first page of each workflow describes any prerequisites.



Design a new network Feature type

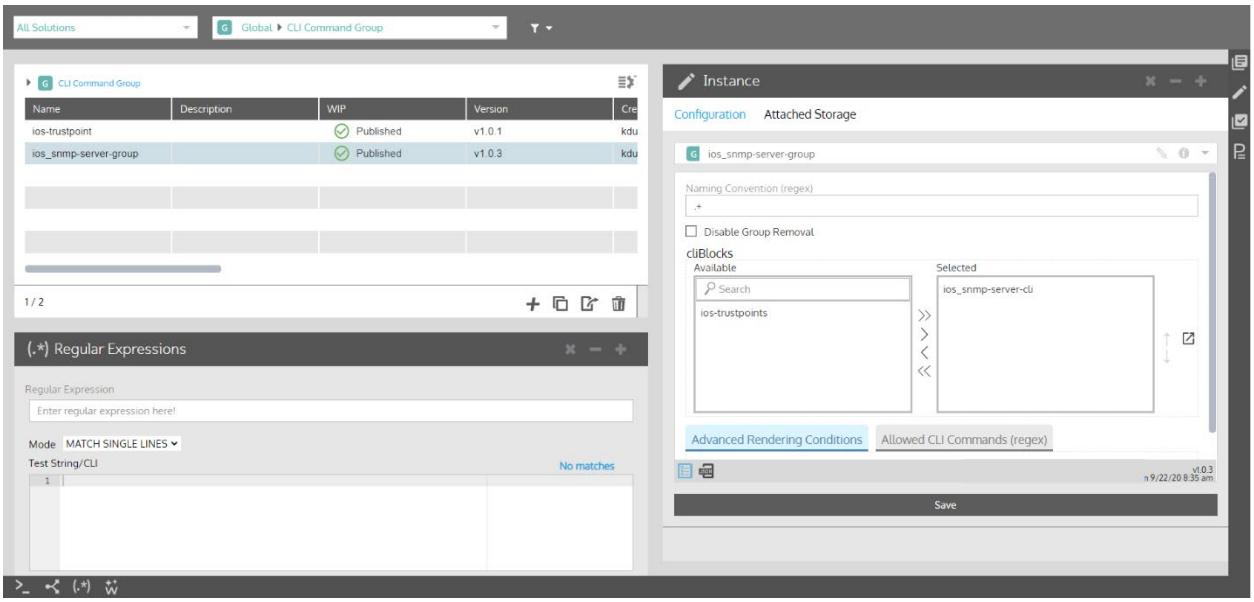
The **Workflows for Config Modeling** wizard guides you through the creation of a set of feature types; for example, NTP, SMTP, QoS. These will be used in **Config Modeling** to create specific feature policies; for example, an SNMP policy for a specific region.

1. Install the **Workflows for Config Modeling** package from **Solutions Manager**.
2. Go to **Workflows**,
3. Expand the **Design** folder, and double-click **Network Feature Design**. You'll see a description of the workflow in the top pane.
4. Click **Next**.
5. Select **Create New Feature Set** and click **Next**.
6. Name and describe the new feature set and click **Next**.
7. Name and describe the feature within the feature set and select a level of execution. **Initial** executes the feature in the first execution group, **Final** executes the feature in the last execution group, **Custom** allows you to assign a numerical order for execution between Initial and Final execution groups.
8. In the **Available** list of node types, select the device types you want the feature to run against and click →. The ↠ selects all the available device types.
9. If the new feature is dependent on another feature, select **Feature Dependencies** and then select from the features in the same execution group.
10. Click **Next**.
11. Optional: To create a form to collect data to be used in the feature rendering, click **Add Section +** and then click **+** to add a row to the form. This is where you can define variables to be used in Command Lists. The variable format in the command line will be *<sectionname>.<fieldname>*, or if an array, *<sectionname>.<fieldname>*[*entry*].*<fieldname>*
    For **Field Type**, select:
    String – Alphanumeric value
    Number – Integer or floating point number

Boolean – True or False
Enum – Enumerated list; a pick list
Array – You'll have more than one value for the variable

12. Optional: Select the row and click to further define the field in the optional form.
    For **Field Type**:
    String – You can define a default value for the field, specify a validation type, and make the field required.
    Number – You can define a default value for the field, specify a validation type, and make the field required.
    Boolean – You can define a default value for the field and make the field required.
    Enum – You can define a default value for the field, valid available values and labels, and make the field required.
    Array – You can define a default values for the field and make the field required.
13. Click **+** to add a row as needed.
14. Click **Add Section +** to the form as needed.
15. Click the **X** in the **Allow Multiple** drop-down list if you want only one group of properties. If you want multiple groups of properties, select a format for the form from the drop-down list.
16. Click **Next** and review the form.
17. Click **Back** to make changes to the form. Click **OK** when you are satisfied with the form.
18. Review the feature set you created and then select **Save** or **Publish**.
19. Provide a package name and description.
20. Optional: To change the version numbering schema, select a schema from the **New Version** drop-down list and provide a version description.
21. Clear the **Install package into current organization** box if you don't want to install the package. Otherwise, the package is published to your organization's local distribution area and can be installed through **Solutions Manager**.
22. Click **Finish**.

Config Modeling quick reference



Select the columns to be displayed in the grid

Create New – Add an instance

Clone Node Instance – Clone the selected instances

Manifest – Download a CSV file that lists all the references and version numbers for the selected instance

Export – Export a CSV file of devices

Delete Node Instance – Delete the selected instances

Terminal – Open the Terminal panel that allows you connect to a node via a secured terminal session to execute native commands

Node Instance Map – View the selected node and related global instances, features, and domains

Regular Expressions – Opens the Regular Expressions panel that allows you to test a regex statement

Workflow – Opens the Regular Expressions panel that allows you to run a custom workflow

Detail – View status and property information about the selected instance, including the other instances that it references

Instance – Open the Instance panel that allows you to edit the properties of an instance

Action – Open the Actions panel that allows you to preview the model and provision the selected node

Provisioning – View a list of the provisioning logs associated with the selected node

Multi-Edit – Make the same updates to all the selected instances

Form View – Display the Instance panel in form view. Available only to those in the System Developer role

JSON View – Display the Instance panel in JSON view. Available only to those in the System Developer role

Export or import a device list in Config Modeling

All devices that have been added in Gluware **Device Manager**, that have been discovered in Device Manager, and that are categorized as **Managed**, will also appear in **Config Modeling**. However, **Config Modeling** maintains additional data elements for each node that will not appear in **Device Manager**. To add the additional data for your devices:

1. Export your device list from **Config Modeling**
2. Add the additional information to the CSV file
3. Then import the device list in **Config Modeling**

Export a device list

1. Ensure you're in the organization you want to export devices from.
2. Go to **Config Modeling** > **Nodes**.
3. Select the type of devices you want to export from the drop-down list. For example, select **IOS Router**.
4. Click . A CSV file is added to your Downloads folder.

Import a device list

1. Ensure you're in the organization you want to import devices into.
2. Go to **Config Modeling** > **Nodes**.
3. Select the type of devices you want to import from the drop-down list. For example, select **IOS Router**.
4. Click .
5. Do one of the following:
    - Select **Download CSV Template** to get a template formatted for **Config Modeling**. The template in **Config Modeling** differs from the template in **Device Manager** and is different for each type of node.
    - Select **Import from File** and click **Open** to import a CSV file.

Add an individual device to Config Modeling

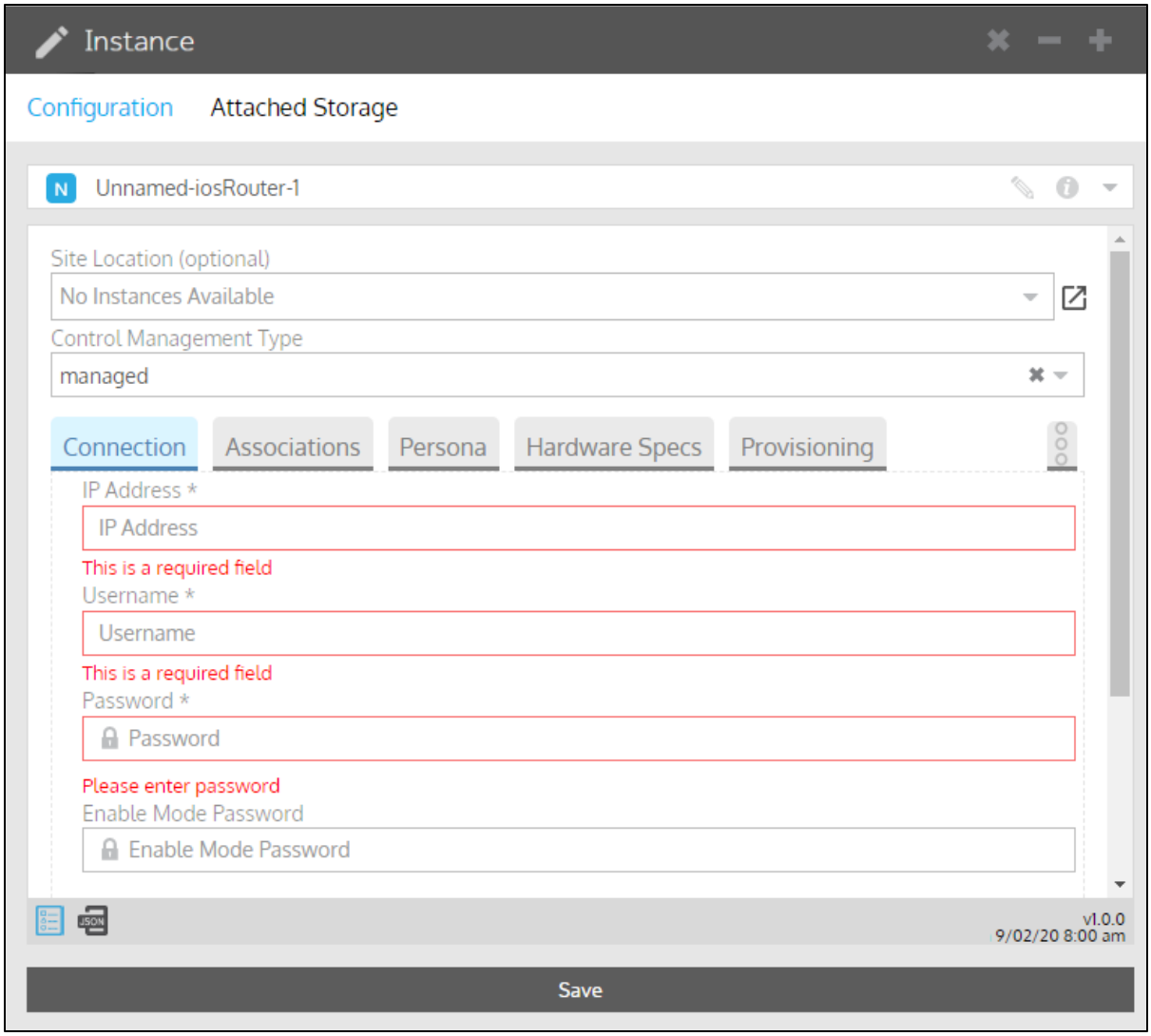
All devices that have been added in Gluware **Device Manager**, that have been discovered in Device Manager, and that are marked **Managed**, will also appear in **Config Modeling**. The **Config Modeling Kit** for the device type must also be installed.

Any nodes added in **Config Modeling**, will also be listed in **Device Manger**. However, **Config Modeling** maintains additional data elements for each node that will not appear in Device Manager.

1. Ensure you're in the organization you want to add devices to.
2. Go to **Config Modeling** > **Nodes**.
3. Select the type of node from the drop-down list.
4. Click ➕.
5. In the Instance panel, click ✎ and name and describe the device.
6. Provide the connection information required for the device.
7. The **Assembly**, on the Associations tab, is required to model the configuration but you can add that later.
8. Save.

NOTES: You can also add a device by cloning an existing device. Simply select a device in the grid list and click ⧉

If your organization uses customized roles, it's possible to add devices that you will not later be able to manage.


Instance
Configuration
Attached Storage
Unnamed-iosRouter-1
Site Location (optional)
No Instances Available
Control Management Type
managed
Connection
Associations
Persona
Hardware Specs
Provisioning
IP Address *
IP Address
This is a required field
Username *
Username
This is a required field
Password *
Password
Please enter password
Enable Mode Password
Enable Mode Password
v1.0.0
9/02/20 8:00 am
Save

Create model instances using Intelligent Model Discovery

You can create all the instances required for Config Modeling from a device with a known configuration. The **Intelligent Model Discovery** (IMD) workflow will create CLI Command Lists, CLI Command Groups, Features, and Assemblies from the device's existing configuration if they don't already exist. You can then use these instances to model other devices in your network.

The required Feature Binder must exist in **Config Modeling** and the Config Modeling Kit for the appropriate vendor device package needs to be installed to use **Intelligent Model Discovery.**

You can run the Intelligent Model Discovery workflow from **Config Modeling** and from **Workflows**.

Run from Config Modeling

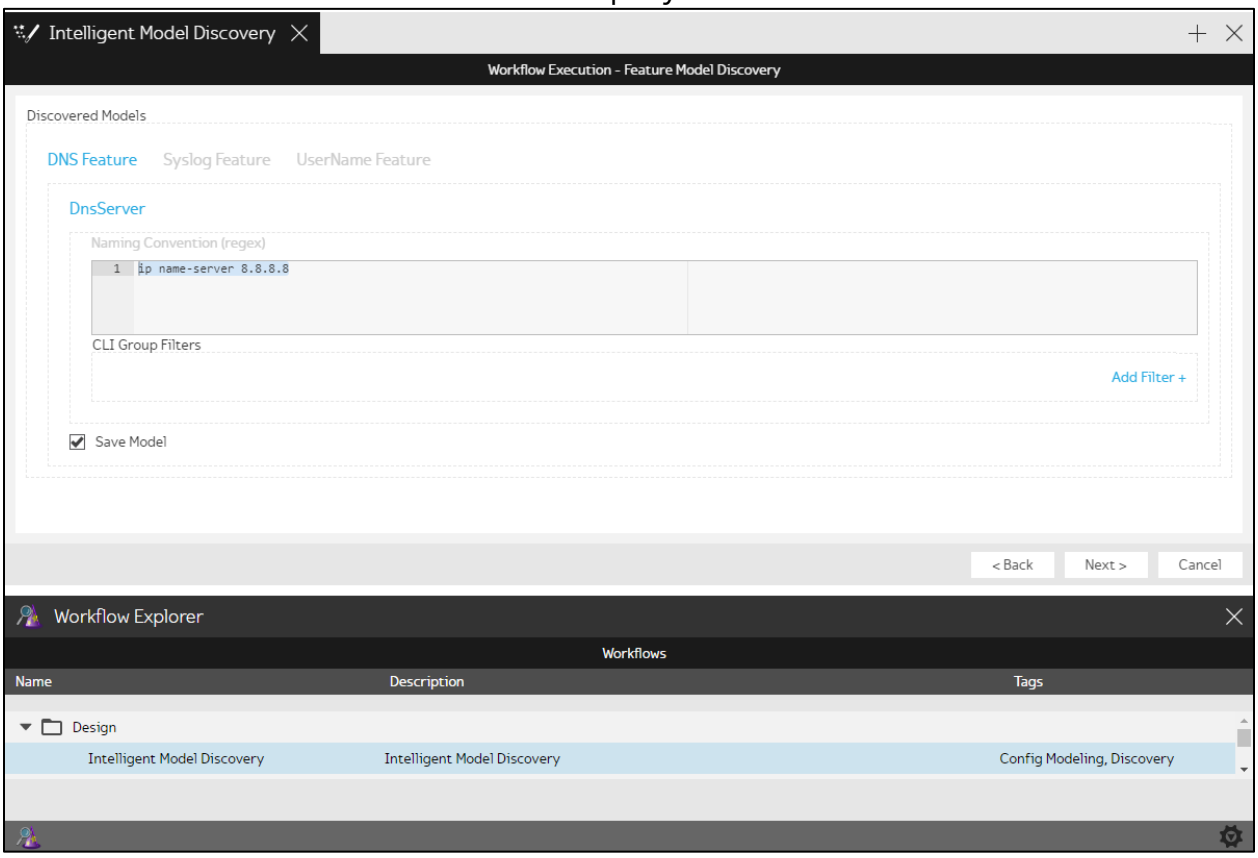
1. Go to **Config Modeling** > **Nodes**.
2. Select the type of node from the drop-down list.
3. Right-click the node in the grid that you want to model and click **Intelligent Model Discovery**. Gluware will connect to the device and parse the configuration into the instances required for modeling. The discovered models are then displayed.
4. For each model discovered:
    - If you want to restrict the CLI commands allowed, click **Add filter +**, select **Allowed CLI Commands (regex)**, and enter the CLI commands. If no commands are entered, Gluware will allow any command to be issued.
    - If you want to render the commands only if the listed elements are found during discovery, click **Add filter +**, select **Discovery Elements**, and list them.
    - Clear the **Save Model** box if you don't want to model the feature.

5. Click **Next**.
6. Confirm the features you want to build by checking the box next to the feature name and click **OK**.
7. Click **Finish**.
8. Click **Cancel**.
9. Click to see the instances that were created or updated by the **Intelligent Model Discovery** workflow.
    - Click and scroll down to reduce the size of the map.
    - Click-and-drag to re-position the map.
    - Double-click on any item in the map to open and inspect the instance details.
10. To download the execution logs, go to **Data Export**, select **Most Recent IMD Workflow Logs** from the drop-down list, and click **Run and Download Export**.

Run from Workflows

1. Go to **Workflows**.
2. Expand the **Design** folder, and double-click **Intelligent Model Discovery**.
3. Click **Next**.
4. Select the **Access Method**:
    - Select **Existing Nodes**. Then select the **vendor**, **node type**, and the **node**.
    - Select **IP & Credentials** if you are running the workflow from **Workflows** and the node you want to model has not already been added to Gluware. Enter the **IP Address**, **username** and **password**, **connection information**, and **proxies** if applicable.
5. Click **Next**. Gluware will connect to the device and parse the configuration into the instances required for modeling.

6. The discovered models are then displayed.



7. For each model discovered:
    - If you want to restrict the CLI commands allowed, click **Add filter +**, select **Allowed CLI Commands (regex)**, and enter the CLI commands. If no commands are entered, Gluware will allow any command to be issued.
    - If you want to render the commands only if the listed elements are found during discovery, click **Add filter +**, select **Discovery Elements**, and list them.
    - Clear the **Save Model** box if you don't want to model the feature.
8. Click **Next**.
9. Confirm the features you want to build by checking the box next to the feature name and click **OK**.
10. Click **Finish**.
11. Click **Cancel**.

12. To download the execution logs, go to **Data Export**, select **Most Recent IMD Workflow Logs** from the drop-down list, and click **Run and Download Export**.

Create a Concept Item

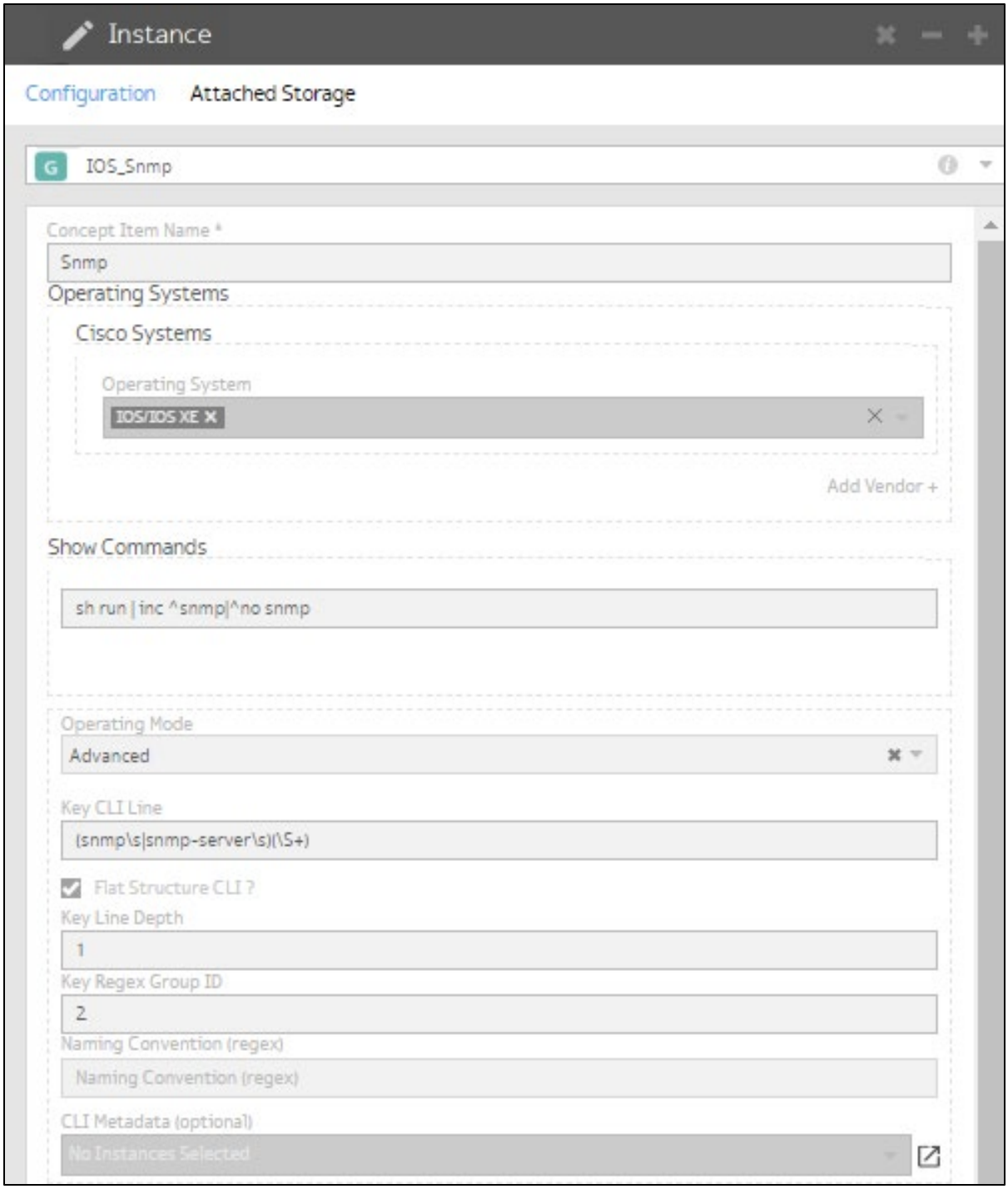
Concept Items are used to discover information from a device before provisioning it. The Concept Item contains the show commands that help define the part of the configuration that will be impacted by a feature in Config Modeling. Concept Items also discover information from devices to place into variables used in CLI Command Lists.

Gluware delivers many of the Concept Items that you will need. You may want to create new Concept Item instance if you want to add your own variables to the show commands or use discovery.

> **NOTE:** You can create a **Concept Item** by cloning an existing one. Simply select a **Concept Item** in the grid and click

1. Ensure you're in the organization you want to create a Concept Item for.
2. Go to **Config Modeling** > **Globals**.
3. Select **Concept Item** from the drop-down list.
4. Click .
5. In the Instance panel, click and name and describe the **Concept Item** instance.
6. Enter the name for the section of the configuration you want to model for the **Concept Item Name**. For example, ACL List.
7. Click **Add Vendor +** and select the **Operating System** (optional). This will allow you to filter the list of Concept Items.
8. Click **Add Command +** and type the list of show commands that will capture the section of the configuration you want to model. Use to re-order or delete lines.
9. Select **Advanced** for the **Operating Mode** when the key line isn't found as the first line in the configuration section or when CLI metadata needs to be added to provide more instruction on how to remove commands, respond to confirmation prompts, etc.
10. Enter the unique identifier of the object you are modeling as the **Key CLI Line**.

11. Select the **Flat Structure CLI** box if the section of the configuration you want to model is at the root level.
12. Optional: If you selected **Advanced** for the **Operating Mode**, provide the **Key Line Depth** (usually 1), **Key Regex Group ID** (usually 1), and select a **CLI Metadata** instance.
13. Optional: Enter the **Start Line (regex)** for the section of the CLI returned that you want to include in the comparison. For example, when a device does not support a "section" command, the entire CLI configuration may come back in the show command. The Start Line tells Gluware where in the CLI that's returned to start to include in the comparison.
14. Optional: Click **Add Element +** and enter a **Field Name** (variable name) if you want to discover it in the configuration. Click **Add Expression +** to define the regex that gets the value for the variable.
15. Optional: To remove objects in the configuration without using the standard "no <*statement*>", click **Add Item +**, enter the regex for the object you want to find as the **Match Expression (regex)**, and then enter what you want to replace it with as the **Remove Expression (regex)**.


Instance
Configuration
Attached Storage
G
IOS_Snmp
Concept Item Name *
Snmp
Operating Systems
Cisco Systems
Operating System
IOS/IOS XE
Add Vendor +
Show Commands
sh run | inc ^snmp|^no snmp
Operating Mode
Advanced
Key CLI Line
(snmp\s|snmp-server\s)(\S+)
Flat Structure CLI ?
Key Line Depth
1
Key Regex Group ID
2
Naming Convention (regex)
Naming Convention (regex)
CLI Metadata (optional)
No Instances Selected

Create a CLI Command List

A **CLI Command List** includes the specific CLI commands to run on the device. The list can contain commands, variables, and information learned from the device during discovery.

1. Ensure you're in the organization you want to create a CLI Command List for.
2. Go to **Config Modeling** > **Globals**.
3. Select **CLI Command List** from the drop-down list.
4. Click ➕.
5. In the Instance panel, click ✎ and name and describe the **CLI Command List** instance.
6. Select a **Concept Item** from the drop-down list.
7. Type the list of command lines for the configuration you want. A reference to both the form and discovered variables can be used and values will be substituted at runtime.
8. Select a **Filter Option** if appropriate: **Compatible OS**, **Compatible OS And Platform SKU**, or **Compatible Platform SKU**. This gives you the option to apply this list only if the specified condition exists. For example, the command lines only apply if the discovered OS version is 15.5 or greater.
9. Save.

> **NOTE:** You can also create a **CLI Command List** by cloning an existing list. Simply select a **CLI Command List** in the grid and click ⧉

Example 1: CLI Command List for SNMP

```
snmp-server community public RO
snmp-server community private RW
snmp-server location America
snmp-server contact Jan Doh
```

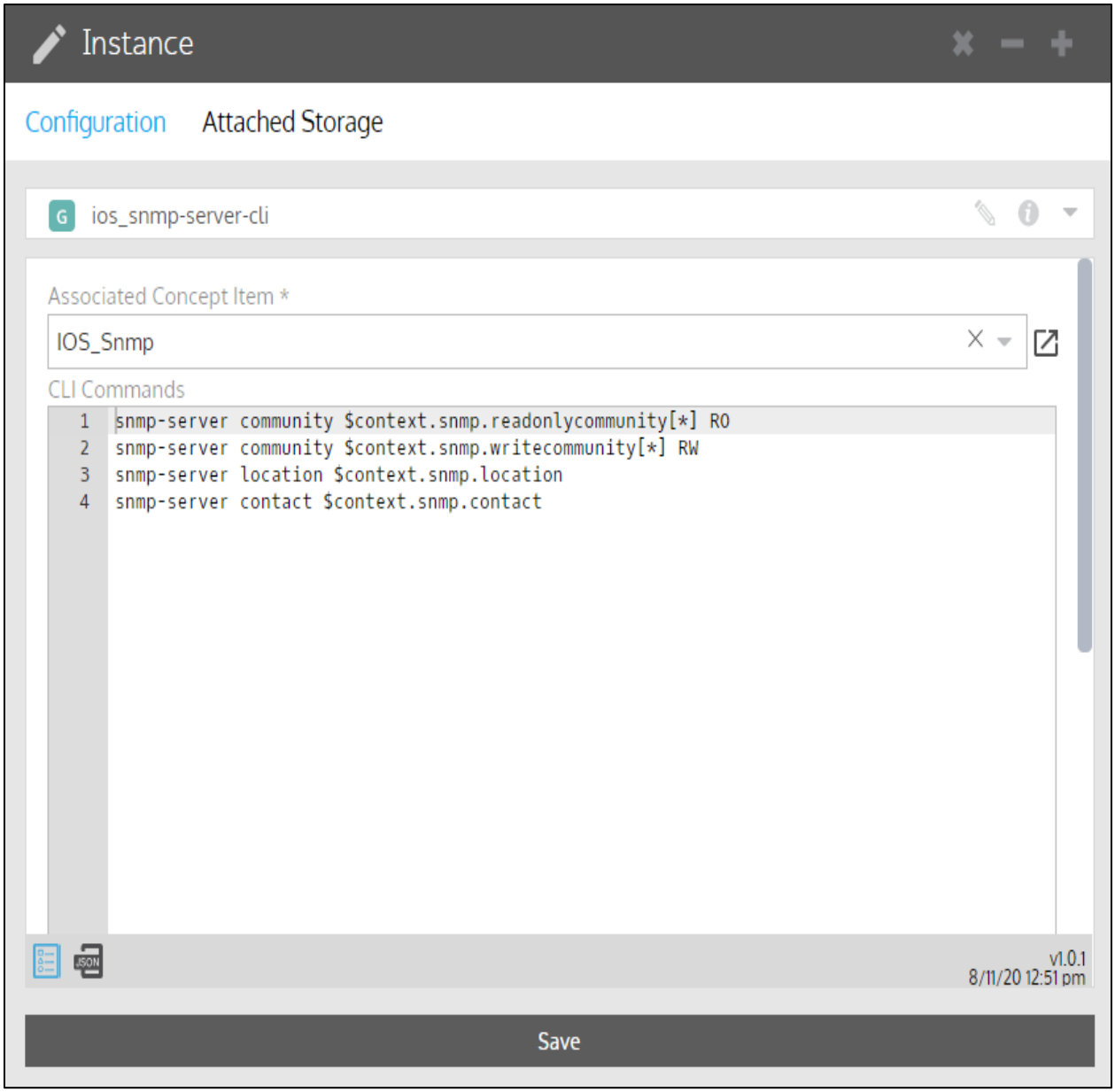
Example 2: CLI Command List for SNMP with form-based variables

NOTE: The variable format in the command line will be <*sectionname*>.<*fieldname*>, or if an array, <*sectionname*>.<*fieldname*>[*entry*].<*fieldname*>

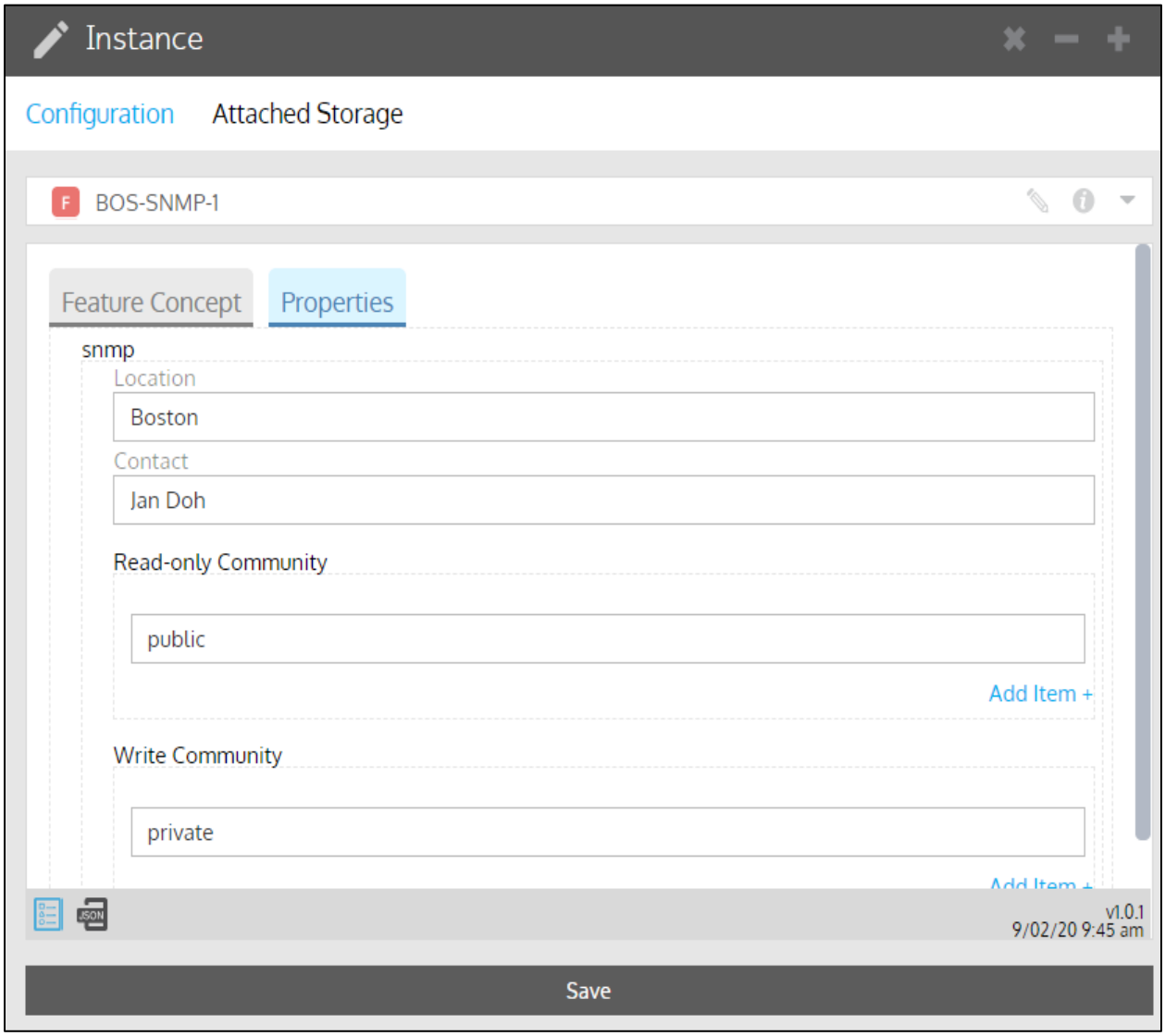
Use `$context` if the command is required. If the line doesn't exist in the configuration it will be added.

Use `#context` if the command is optional. If the line doesn't exist in the configuration it doesn't render at all.

```
snmp-server community
$context.snmp.readonlycommunity[*] RO
snmp-server community $context.snmp.writecommunity[*]
RW
snmp-server location $context.snmp.location
snmp-server contact $context.snmp.contact
```


Instance
Configuration
Attached Storage
ios_snmp-server-cli
Associated Concept Item *
IOS_Snmp
CLI Commands
1 snmp-server community $context.snmp.readonlycommunity[*] RO
2 snmp-server community $context.snmp.writecommunity[*] RW
3 snmp-server location $context.snmp.location
4 snmp-server contact $context.snmp.contact
JSON
v1.0.1
8/11/20 12:51 pm
Save

Feature Properties form for capturing the variables

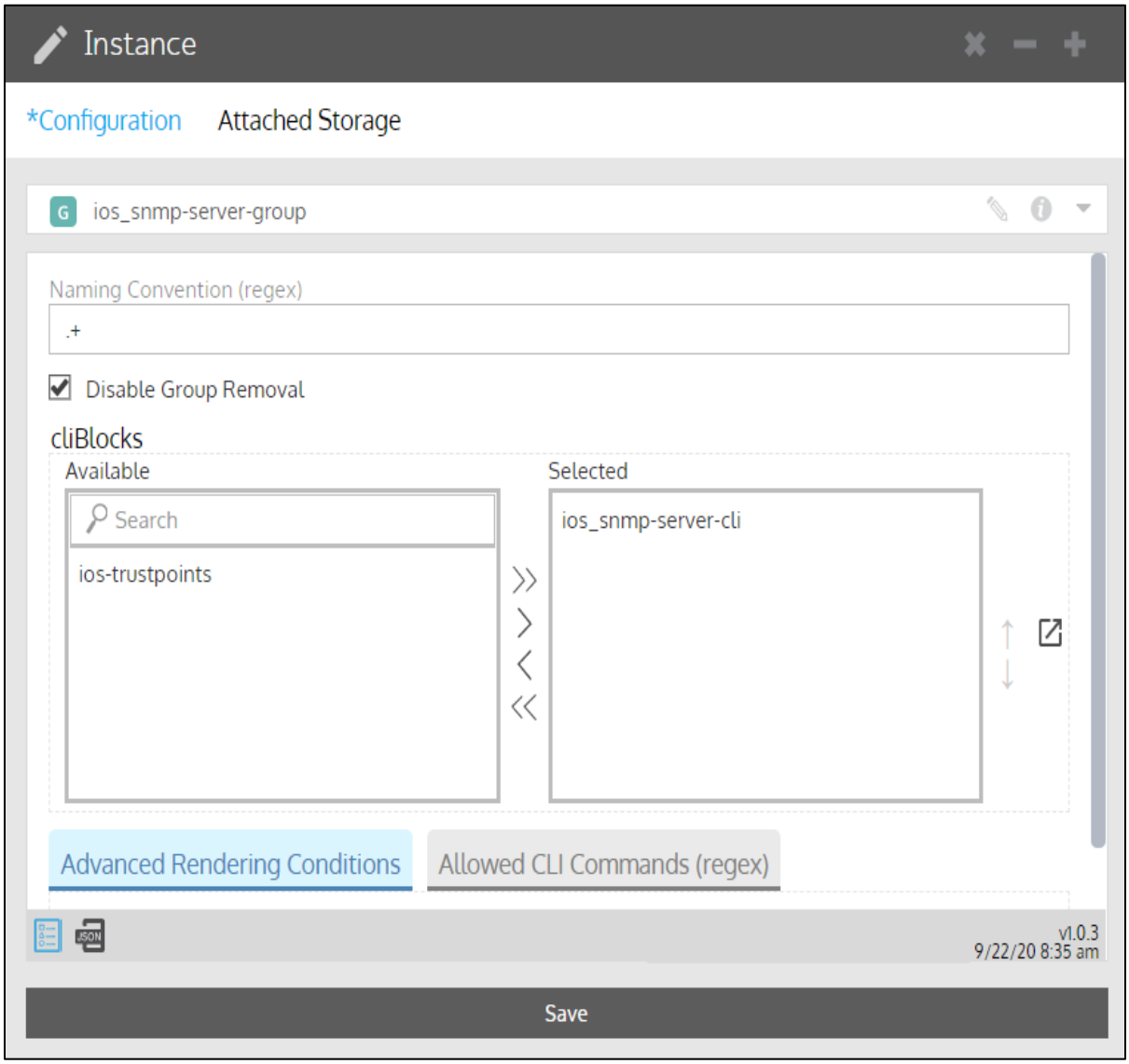


Create a CLI Command Group

A **CLI Command Group** allows you to combine multiple **CLI Command Lists** to achieve a specific configuration. Every **CLI Command List** must be associated with a **CLI Command Group**, so you may have a one-to-one relationship.

1. Ensure you're in the organization you want to create a CLI Command Group for.
2. Go to **Config Modeling** > **Globals**.
3. Select **CLI Command Group** from the drop-down list.
4. Click ➕.
5. In the Instance panel, click ✎ and name and describe the **CLI Command Group** instance.
6. To limit changes to only configuration items with a specific name, enter the regex in **Naming Convention (regex)**. For example, `acl-qos+` limits changes to ACLs that start with `acl-qos`.
   Need help with regex? Go to http://regex101.com/
7. If you want to enable removal of entire CLI groups, clear the **Disable Group Removal** box. Otherwise, if this is selected, modifications can only be made to subcommands.
8. In the **Available** list, select the **CLI Command Lists** you want to include and click →. The ↠ selects all the lists.
9. If you want to render the commands only if the listed elements are found during discovery, list them in **Advanced Rendering Conditions, Discovery Elements**. For example, only apply if the discovered interface description is "WAN Interface."
10. Optional: To add a **Post-Modify Condition** or a **Pre-Modify Condition**, click **Add Item+**, select from the drop-down list, and enter the appropriate regex.
11. Optional: If you want to restrict the CLI commands allowed, enter those in **Allowed CLI Commands (regex)**. If no commands are entered, Gluware will allow any command to be issued.
12. Save.

NOTE: You can also create a **CLI Command Group** by cloning an existing group. Simply select a **CLI Command Group** in the grid and click

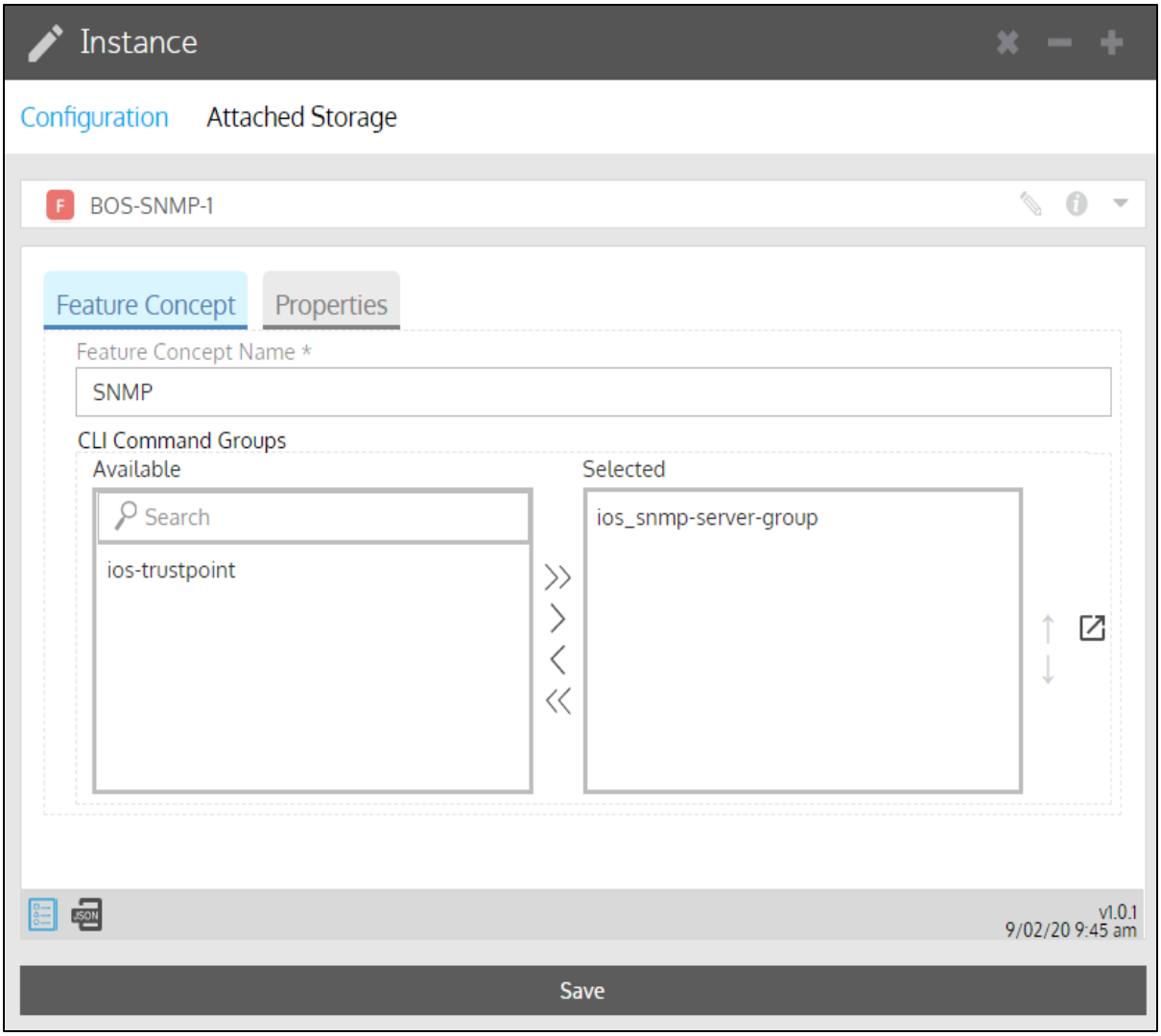


Create a Feature

A **Feature** or **Feature Policy** reflects the structure and syntax of a CLI function on a specific network device.

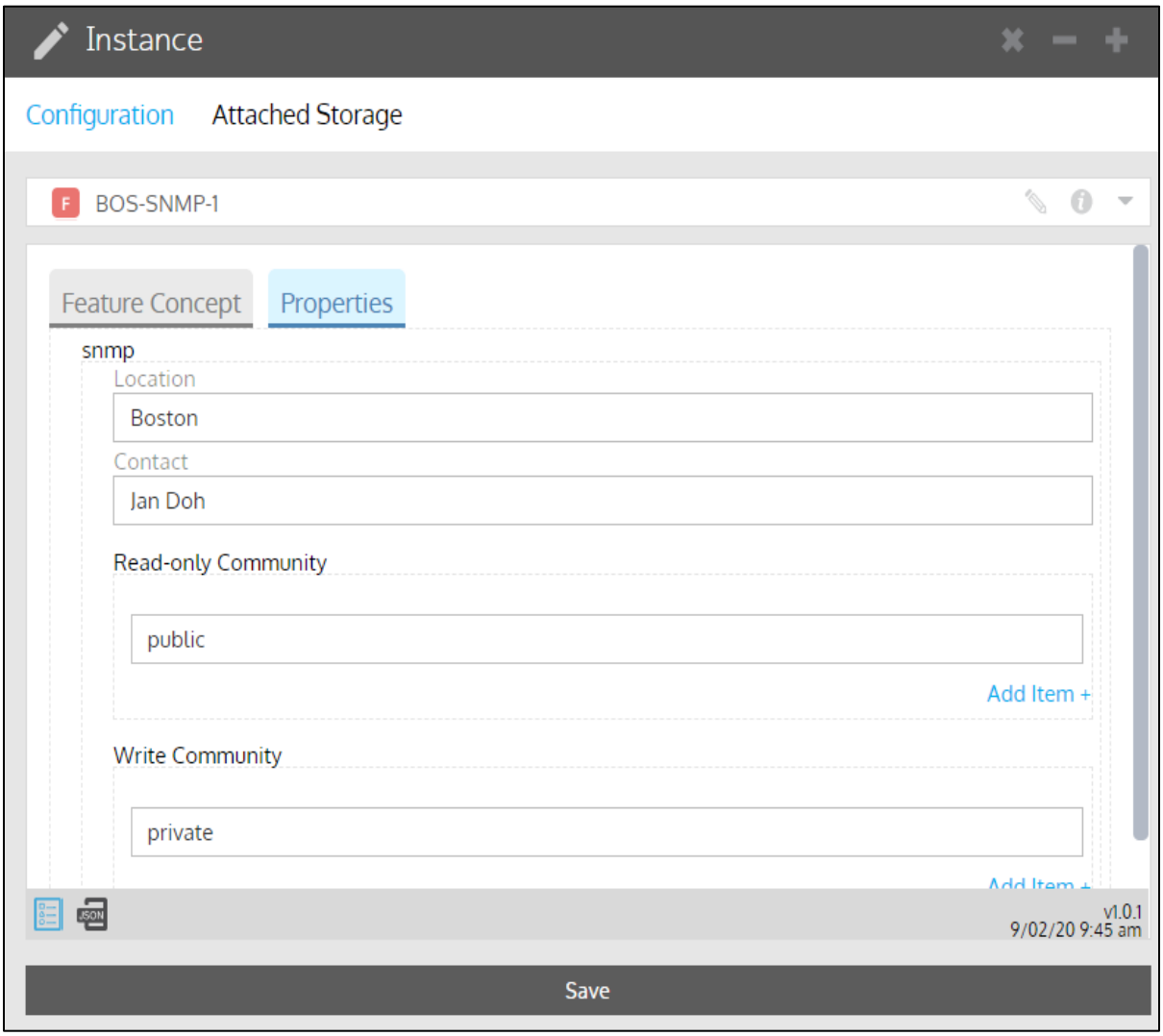
The basic underlying code for a Feature is created using the Workflows wizard. More specific functionality is added using Config Modeling.

1. Ensure you're in the organization you want to create a Feature for.
2. Go to **Config Modeling** > **Features**.
3. Select the type of **Feature** from the drop-down list.
4. Click ➕.
5. In the Instance panel, click ✎ and name and describe the **Feature** instance.
6. Name the **Feature Concept**.
7. In the **Available** list, select the **CLI Command Groups** you want to include and click →. The ↠ selects all the available CLI Command Groups.



8. Select **Properties**.

9. Fill in the form. These are the properties that are used in the CLI Command List.



10. Save.

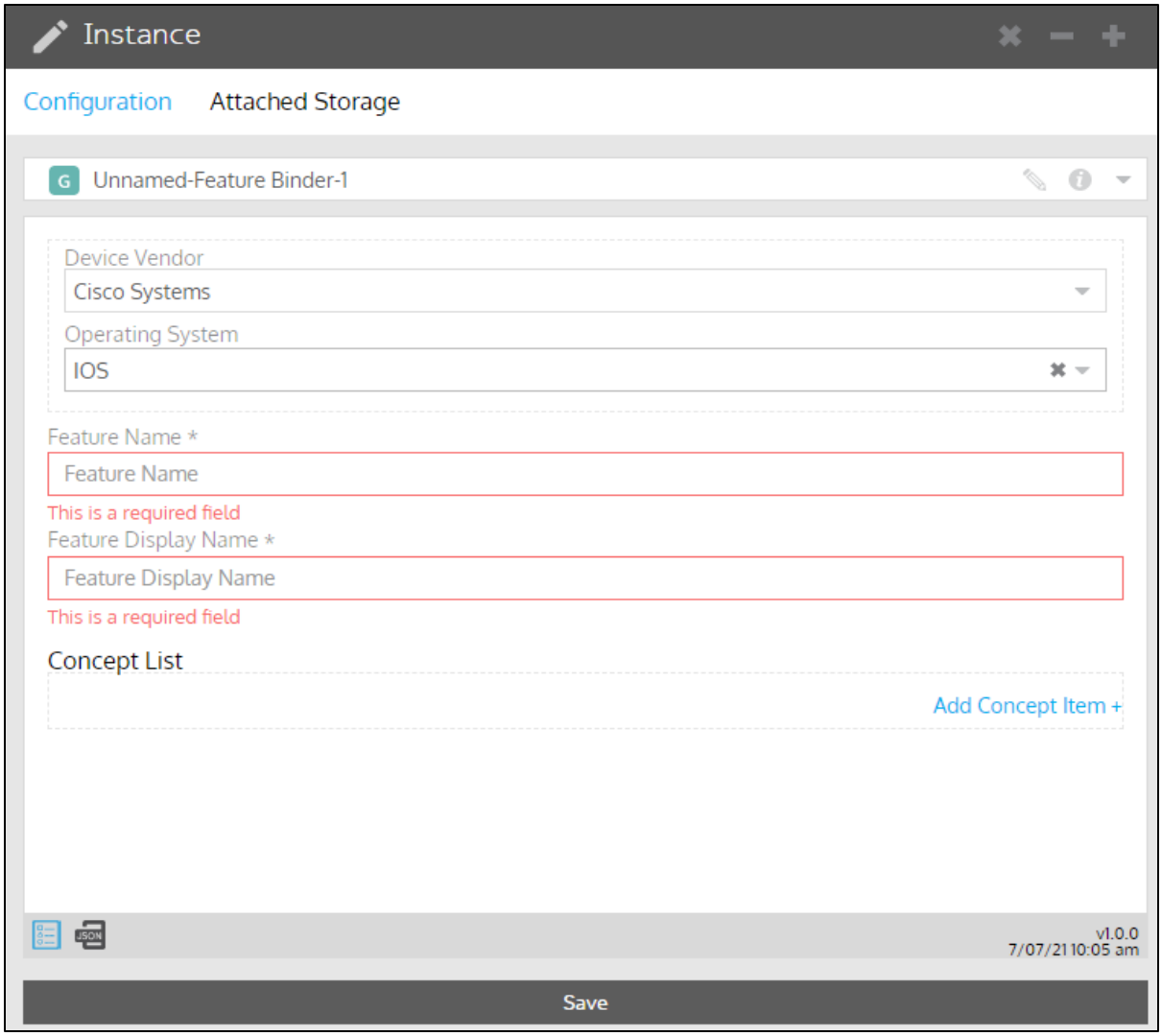
NOTE: You can also:

- Create a Feature instance by cloning an existing one. Simply select a **Feature** in the grid and click
- Import an example Feature from the Gluware Knowledge Base at https://support.gluware.com/hc/start using **Import Package** in **Solutions Manager**.

Create a Feature Binder

A Feature Binder is a collection of Concept Items. A Feature Binder is required if you want to use node state assessment.

1. Go to **Config Modeling** > **Globals**.
2. Select **Feature Binder** from the drop-down list.
3. Click ➕.
4. In the Instance panel, click ✎ and name and describe the **Feature Binder** instance.
5. Select the device vendor from the drop-down list.
6. Select the operating system from the drop-down list.
7. Give the Feature Binder its internal name. The name cannot contain spaces or special characters.
8. Give the Feature Binder a display name.
9. Click **Add Concept Item +** and select a **Concept Item** from the list.
10. Add one or more additional **Concept Items**.
11. Save.


Instance
Configuration
Attached Storage
Unnamed-Feature Binder-1
Device Vendor
Cisco Systems
Operating System
IOS
Feature Name *
Feature Name
This is a required field
Feature Display Name *
Feature Display Name
This is a required field
Concept List
Add Concept Item +
v1.0.0
7/07/21 10:05 am
Save

Create a Routed Port Map

Routed Port Maps allow you to associate a logical name, such as WAN, to similar physical ports on router nodes. Creating **Routed Port Maps** for your network allows you to easily configure like ports with the same CLI.

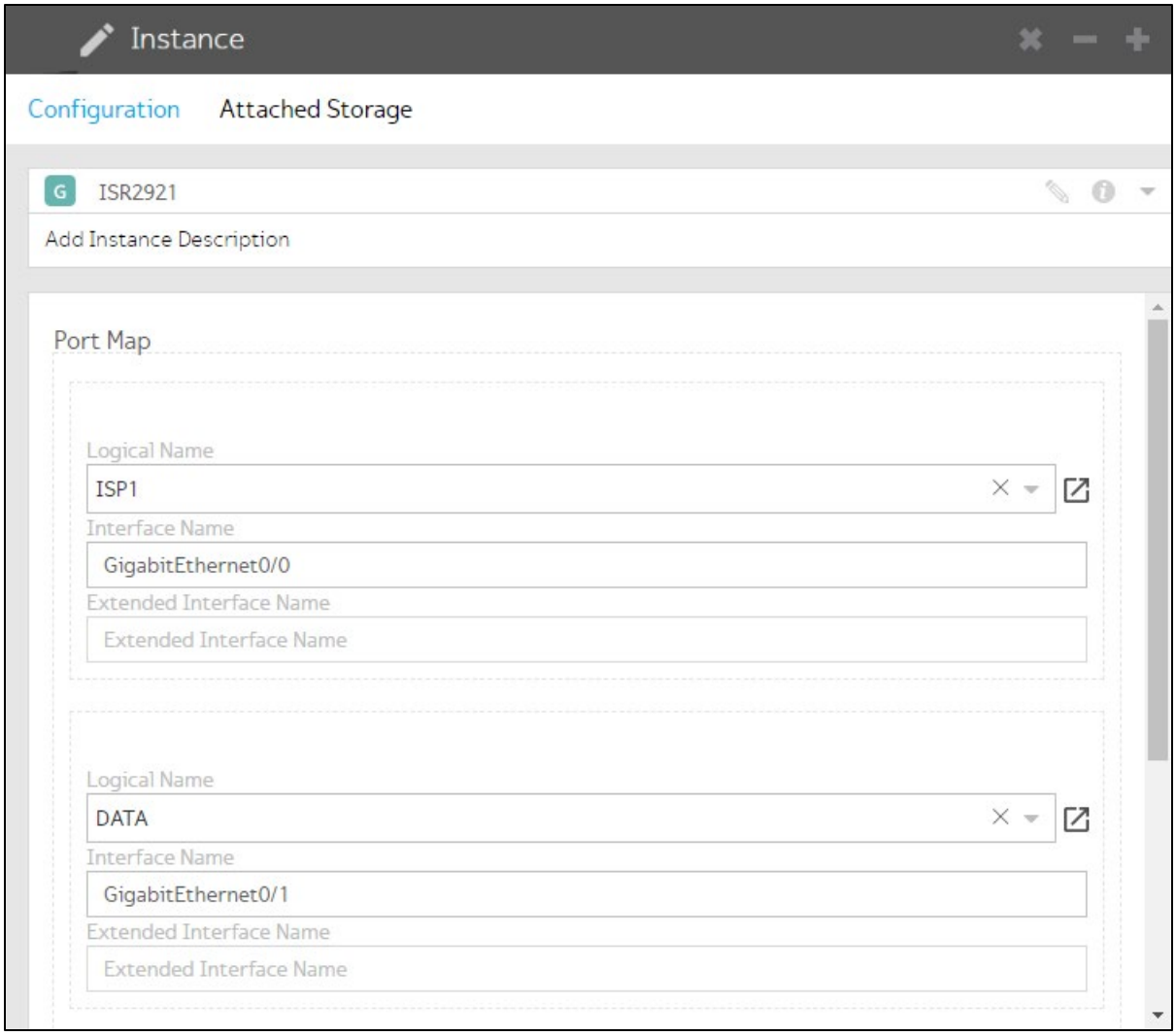
Create your Logical Names

You'll want to decide what logical names make sense for your organization. Some examples are DATA, VOICE, ISP1, ISP2.

1. Go to **Config Modeling** > **Globals**.
2. Select **LAN Interface Name** or **WAN Interface Name** from the drop-down list; for example, DATA or WAN.
3. Click ➕.
4. In the Instance panel, click ✎ and name and describe the instance.
5. Describe the logical name.
6. Save.
7. Create additional logical names as needed.

Create your Routed Port Maps

1. Go to **Config Modeling** > **Globals**.
2. Select **Routed Port Map** from the drop-down list.
3. Click ➕.
4. In the Instance panel, click ✎ and name and describe the **Routed Port Map** instance.
5. Click **Add Port +**.
6. Select a logical name from the drop-down list.
7. Enter the physical interface name for the port that is on the device. For example, GigabitEthernet0/0/0.
8. For Juniper devices, enter the **Extended Interface Name**.
9. Save.


Instance
Configuration
Attached Storage
ISR2921
Add Instance Description
Port Map
Logical Name
ISP1
Interface Name
GigabitEthernet0/0
Extended Interface Name
Extended Interface Name
Logical Name
DATA
Interface Name
GigabitEthernet0/1
Extended Interface Name
Extended Interface Name

Create a Switched Port Map

Switched Port Maps allow you to associate a **CLI Command Group** or Groups to ports on a switch node. Creating these CLI Command Group templates for your network allows you to quickly and easily apply a specific configuration to like ports on your network switches. This not only makes configuration changes easier; it also helps ensure consistency.

Create your Switched Port Naming Profiles

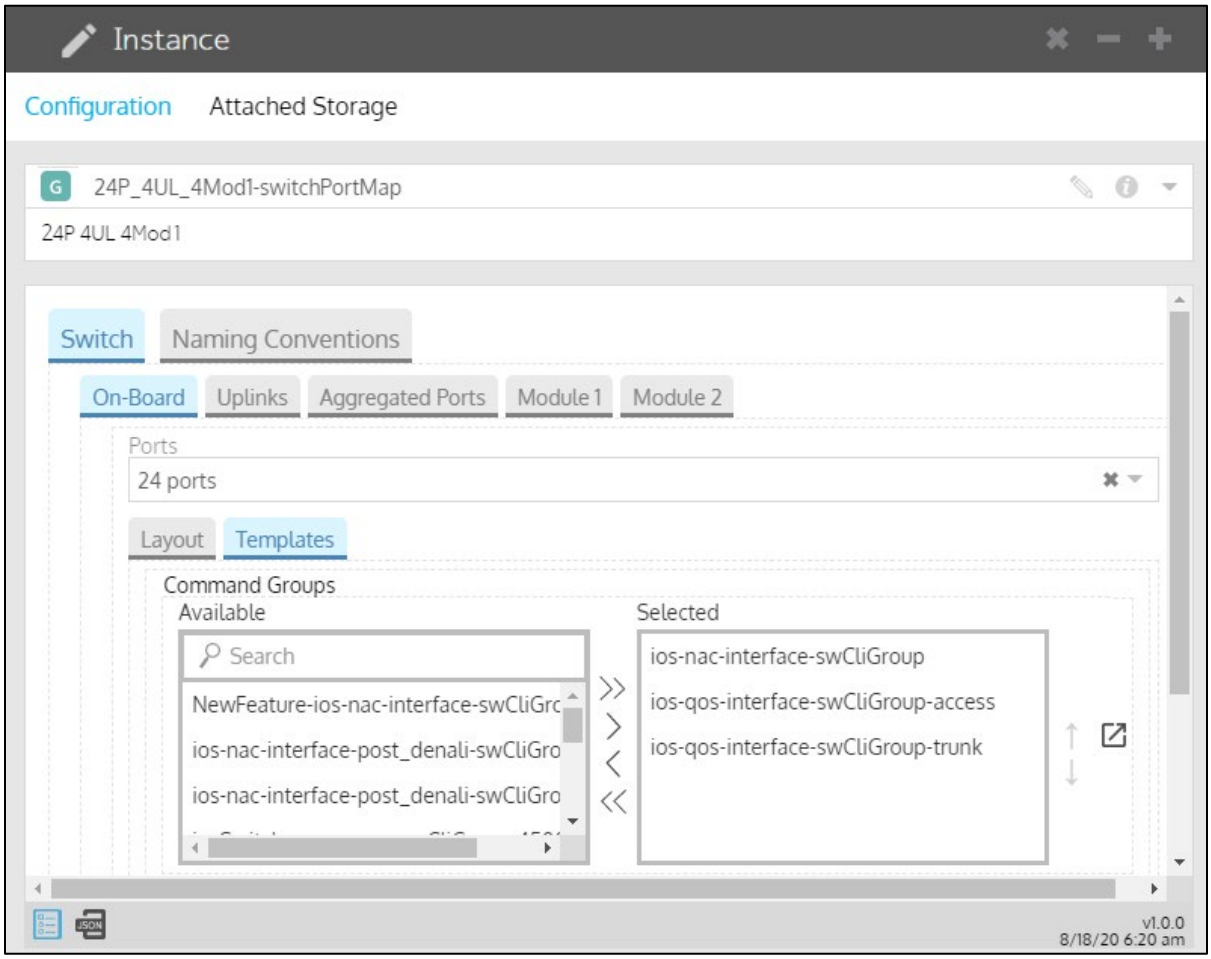
1. Go to **Config Modeling** > **Globals**.
2. Select **Switched Port Naming Profile** from the drop-down list.
3. Click ➕.
4. In the Instance panel, click ✎ and name and describe the profile. Some name examples are onBoarding, uplinks, aggregatedPorts, module1, module2.
5. Select the **Port Type** from the drop-down list.
6. Select the **Mapping Mode** from the drop-down list, usually **inherited (from Switched Port Map)**.
7. Save.
8. Create additional naming profiles as needed.

Create your Switched Port Maps

1. Go to **Config Modeling** > **Globals**.
2. Select **Switched Port Map** from the drop-down list.
3. Click ➕.
4. In the Instance panel, click ✎ and name and describe the **Switched Port Map** instance.
5. Select the number of ports on the node from the drop-down list.
6. Select **Templates**.
7. In the **Available** list, select the **CLI Command Groups** you want to include in the template and click →. The ↠ selects all the lists.
8. In the **Ports** drop-down list, select the ports you want to apply the template to.

9. Save.

NOTE: Alternatively, you can define **Switchport Settings** and then define the **Layout** in the Switched Port Maps. But using the Templates in the Switched Port Maps is faster and easier when there are many ports.



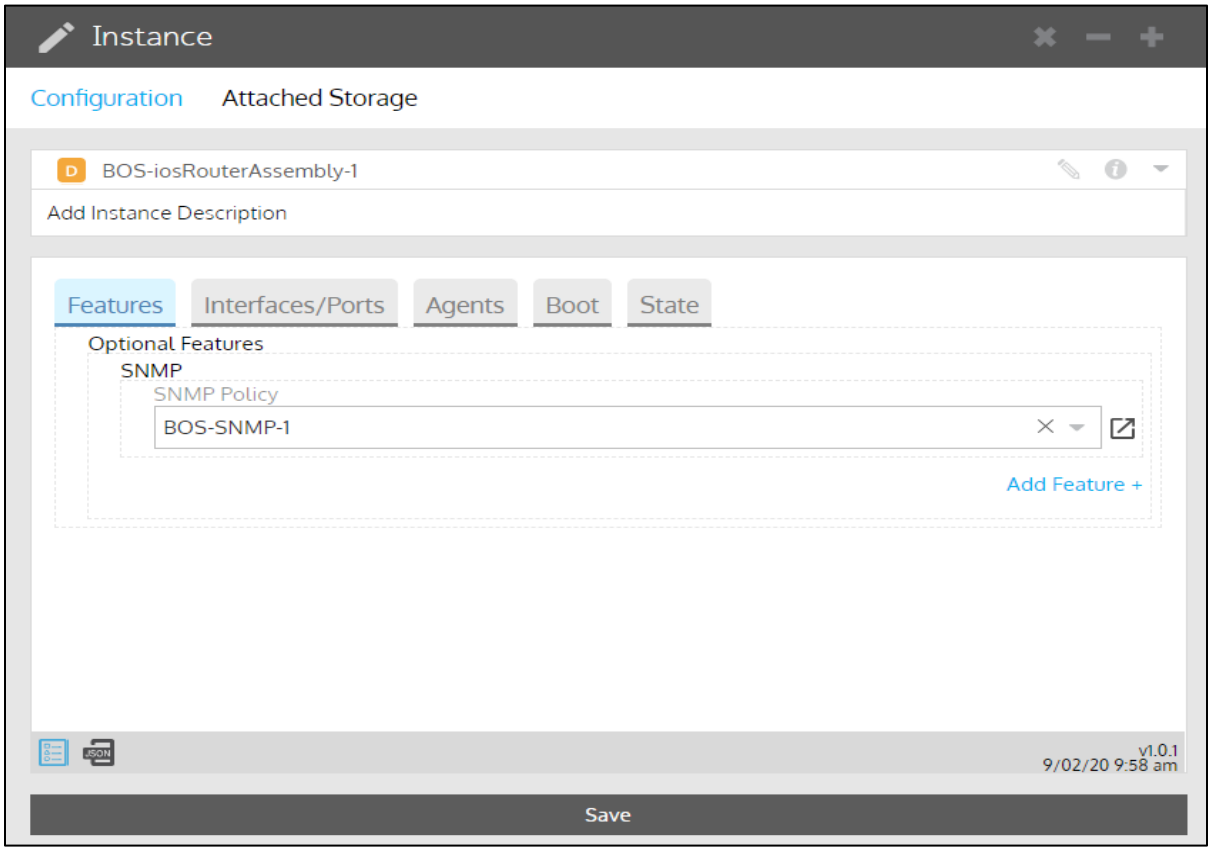
Create an Assembly

Assemblies are the highest-level building block of config modeling and are used to determine how to provision nodes. **Assemblies** are directly attached to nodes and are specific to the device type (switch, router, firewall). Typically, you have as many **Assemblies** as you have individual device roles.

1. Ensure you're in the organization you want to create an Assembly for.
2. Go to **Config Modeling** > **Domains**.
3. Select the type of **Assembly** from the drop-down list.
4. Click +.
5. In the Instance panel, click ✎ and name and describe the **Assembly**.
6. Click **Add Feature +** and select a **Feature Policy** from the list.
7. Add additional **Feature Policies** as appropriate.
8. Select **Interfaces/Ports** and then select a port map and IP address plan from the drop-down lists.
9. Optional: For Cisco IOS/IOSXE routers and switches, select **Agents** and then select a gluWatchdog policy from the drop-down list.
10. Optional: Select **Boot** and then select an upgrade/downgrade policy and firmware catalog from the drop-down lists.
11. Save.

NOTE: You can also create an **Assembly** by cloning an existing one. Simply select an **Assembly** row in the grid and click

Example: IOS Router Assembly



Create a CLI State Item

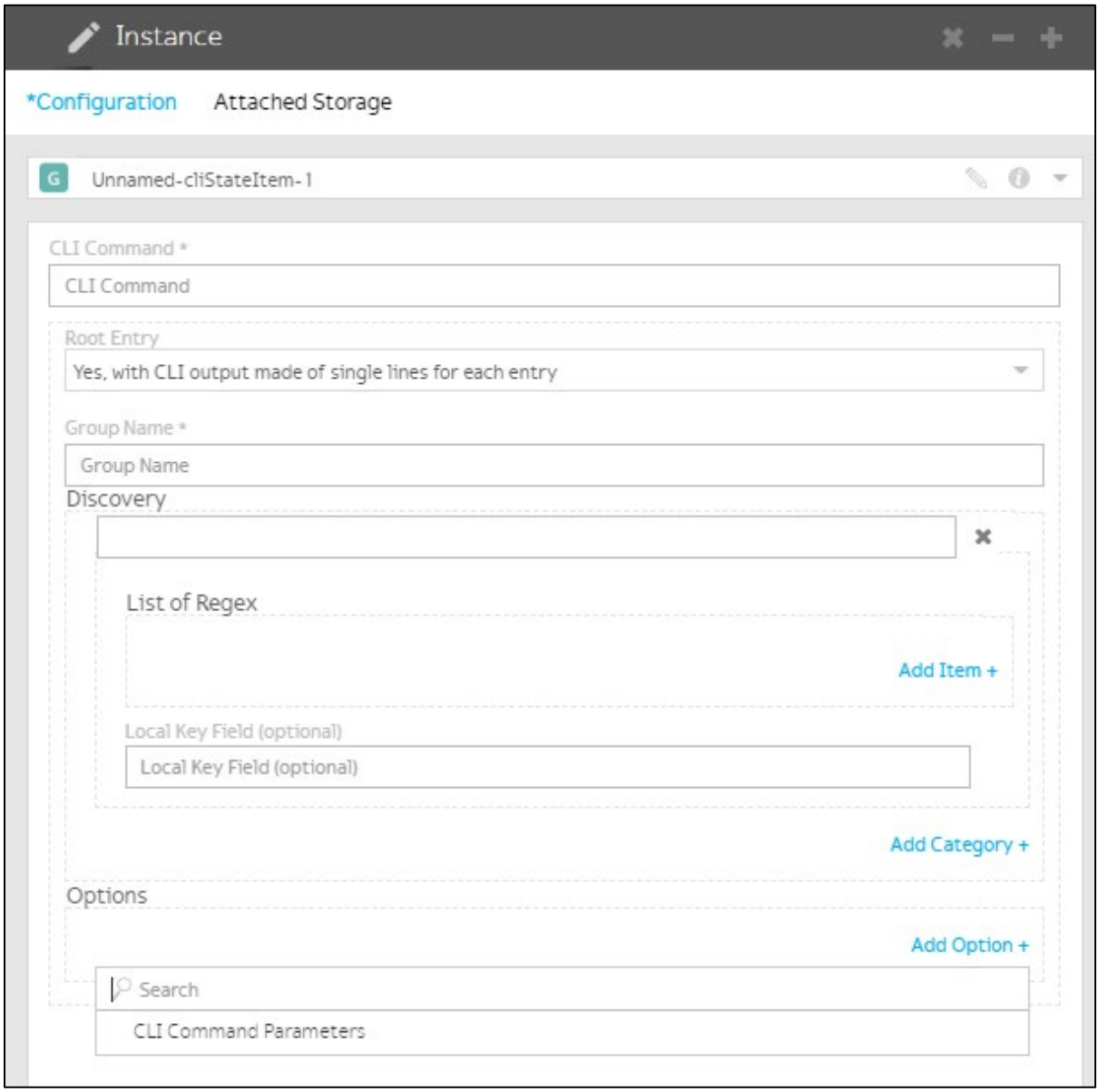
A CLI State Item allows you to define the way you want the show output to be parsed to extract only the relevant data from the output.

1. Go to **Config Modeling** > **Globals**.
2. Select **CLI State Item** from the drop-down list.
3. Click ➕.
4. In the Instance panel, click ✎ and name and describe the **CLI State Item** instance.
5. Enter the CLI Command to extract the relevant information.
6. For the **Root Entry**,
    - Keep **Yes, with CLI output made of single lines for each entry** if the output is a flat structure.
    - Select **No, with CLI output made of distinct paragraphs** if the output is structured in sections/paragraphs.
7. To continue, find the appropriate section below.

Yes, CLI output made of single lines for each entry

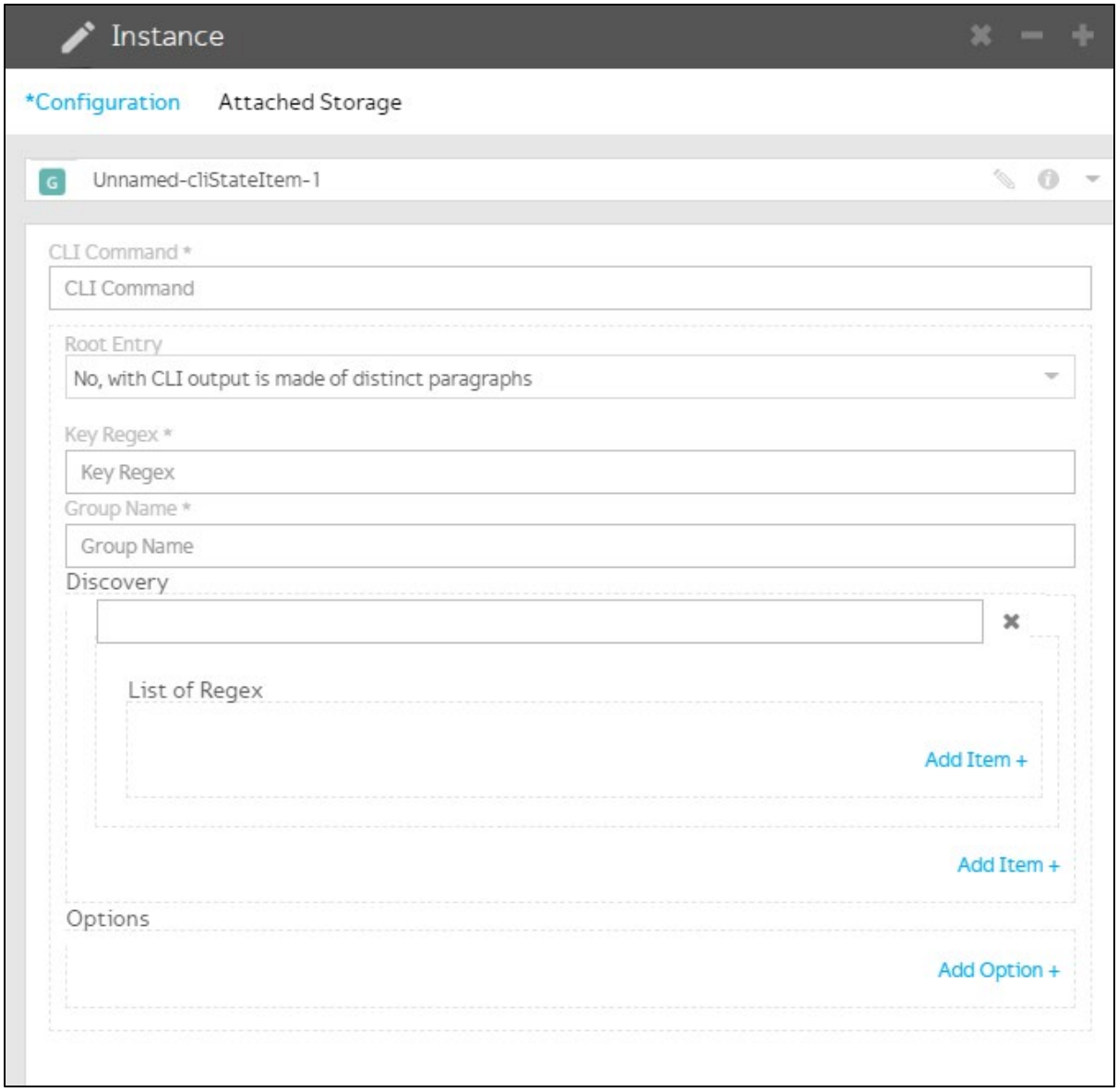
8. Name the group. Each CLI State Item is one group.
9. Click **Add Category +** under **Discovery**.
10. Under Discovery, name the category. Each category includes a list of regex strings that will be applied against the show command output.
11. Click **Add Item +** under **List of Regex**.
12. Enter the regex you want to extract from the show command. All regex backreferences must be named groups. Numbered backreferences are not supported.
13. Optional: For the **Local Key field**, enter the named group that identifies each unique entry (the key). When one named group cannot be used to define the key, you can combine multiple named groups: use the + separator to make the key. You can also use a comma as a separator to define multiple keys. First one found wins.
14. Add additional categories accordingly.

15. Optional: To associate a friendly label to each CLI Command variable, click **Add Option +** under **Options**.
    a. Select **CLI Command Parameters** from the drop-down list.
    b. Click + and enter the variable.
    c. Double-click in the **Label** column and enter the friendly label for the variable.
    d. Optional: Double-click in the **Description** column and enter a tooltip.
    e. Add additional parameters accordingly.
16. Save.

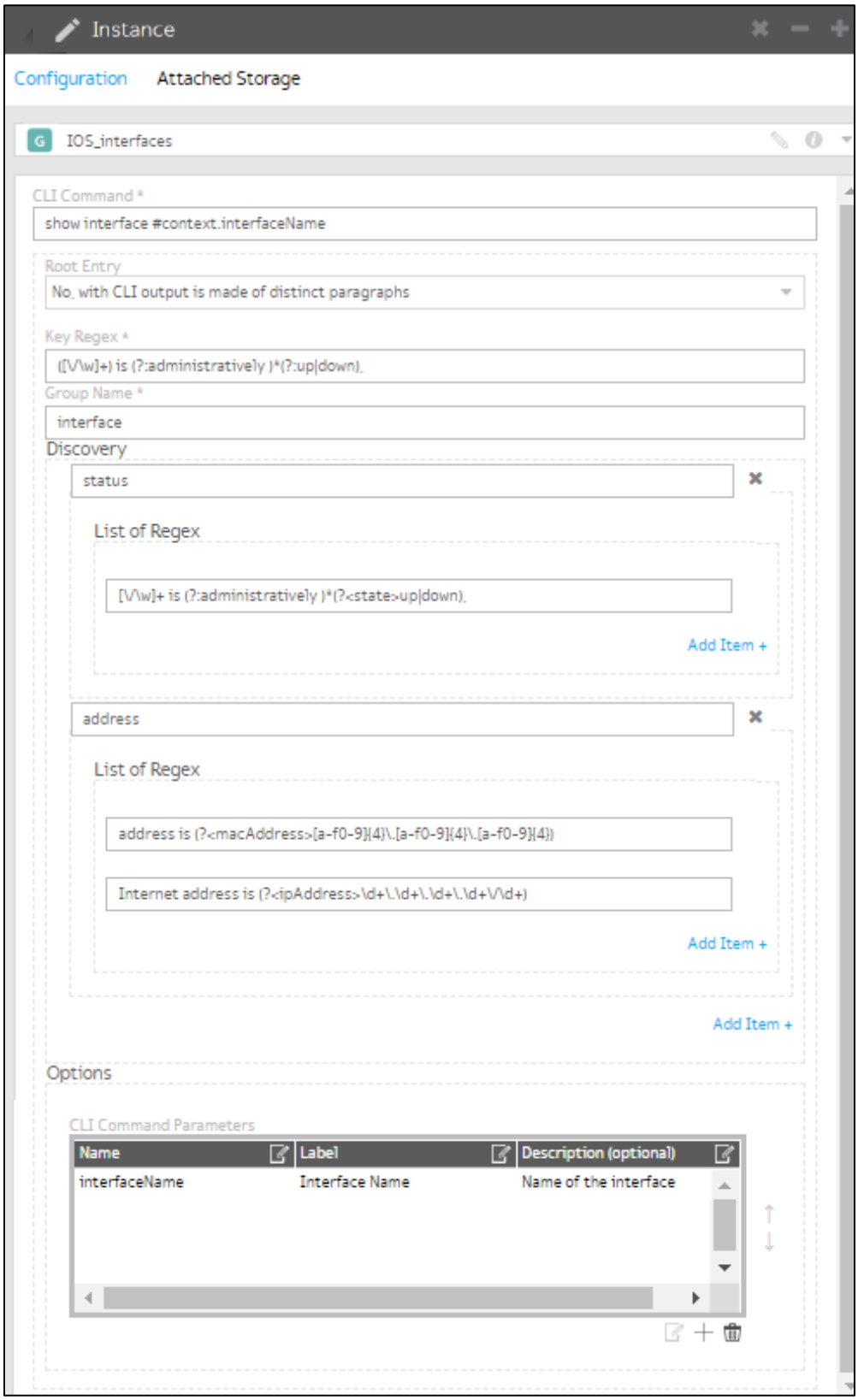


No, CLI output made of distinct paragraphs

8. Enter the regex that identifies each unique entry (the key). This regex can only include one group (backreference).
9. Name the group. Each CLI State Item is one group.
10. Click **Add Category+**.
11. Under **Discovery**, name the category. Each category includes a list of regex strings that will be applied against the show command output.
12. Click **Add Item+**.
13. Enter the regex you want to extract from the show command. All regex backreferences must be named groups. Numbered backreferences are not supported.
14. Add additional categories accordingly.
15. Optional: To associate a friendly label to each CLI Command variable, click **Add Option +** under **Options**.
    a. Select **CLI Command Parameters** from the drop-down list.
    b. Click + and enter the variable.
    c. Double-click in the **Label** column and enter the friendly label for the variable.
    d. Optional: Double-click in the **Description** column and enter a tooltip.
    e. Add additional parameters accordingly.
16. Save.


Instance
*Configuration
Attached Storage
Unnamed-cliStateItem-1
CLI Command *
CLI Command
Root Entry
No, with CLI output is made of distinct paragraphs
Key Regex *
Key Regex
Group Name *
Group Name
Discovery
List of Regex
Add Item +
Add Item +
Options
Add Option +

Example

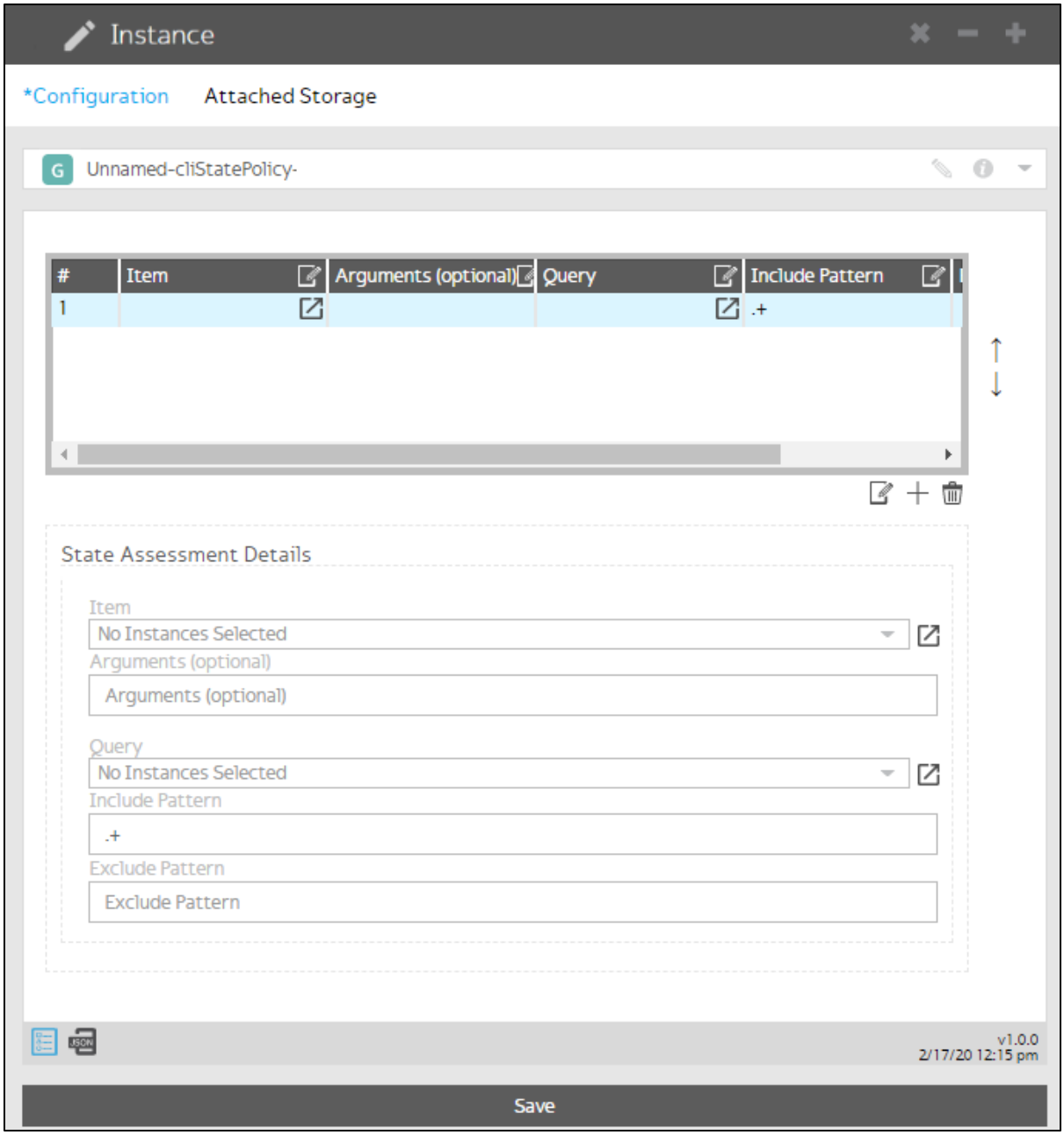

Instance
Configuration
Attached Storage
IOS_interfaces
CLI Command *
show interface #context.interfaceName
Root Entry
No, with CLI output is made of distinct paragraphs
Key Regex *
([\/\w]+) is (?:administratively)*(?:up|down).
Group Name *
interface
Discovery
status
List of Regex
[\/\w]+ is (?:administratively)*(?<state>up|down).
Add Item +
address
List of Regex
address is (?<macAddress>[a-f0-9]{4}\.[a-f0-9]{4}\.[a-f0-9]{4})
Internet address is (?<ipAddress>\d+\.\d+\.\d+\.\d+\/\d+)
Add Item +
Add Item +
Options
CLI Command Parameters
Name
Label
Description (optional)
interfaceName
Interface Name
Name of the interface

Create a CLI State Assessment Policy

You need a CLI State Assessment Policy to assess the running state of a node. Each policy can invoke one or more CLI State Items.

You can assess the state of a node before and after provisioning or an OS upgrade. You can also assess the state on demand. Design your CLI State Assessment Policy with its purpose in mind.

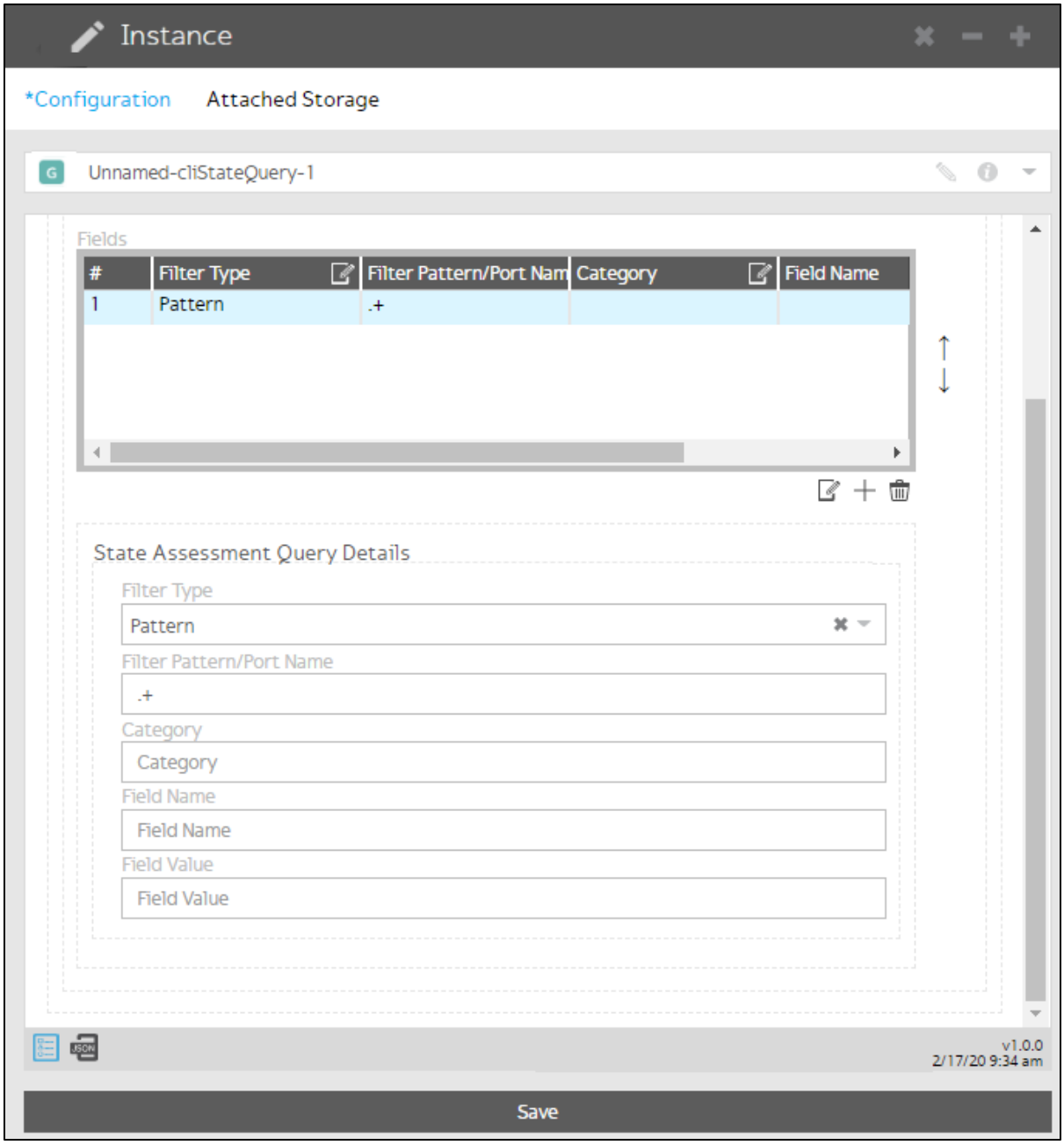
1. Go to **Config Modeling** > **Globals**.
2. Select **CLI State Assessment Policy** from the drop-down list.
3. Click +.
4. In the Instance panel, click and name and describe the **CLI State Assessment Policy** instance.
5. Click + and then click to enter the policy info in a form.
6. Select a **CLI State Item** from the drop-down list.
7. Optional: Specify the optional arguments for the CLI Command associated with the CLI State Item, if any. Use a comma as a separator.
8. Optional: Select a **CLI Assessment Query** from the drop-down list.
9. Optional **Include Pattern**: Define an inclusive regex filter to apply against all the items discovered.
10. Optional **Exclude Pattern**: Define an additional level of filtering to apply against all the items discovered after they have been filtered by the **Include Pattern**.
11. Optional: Click +, click , and select additional **CLI State Items** to add to the policy.
12. Save.


Instance
*Configuration
Attached Storage
Unnamed-cliStatePolicy-
Item Arguments (optional) Query Include Pattern
1 .+
State Assessment Details
Item
No Instances Selected
Arguments (optional)
Arguments (optional)
Query
No Instances Selected
Include Pattern
.+
Exclude Pattern
Exclude Pattern
v1.0.0
2/17/20 12:15 pm
Save

Create a CLI State Assessment Query

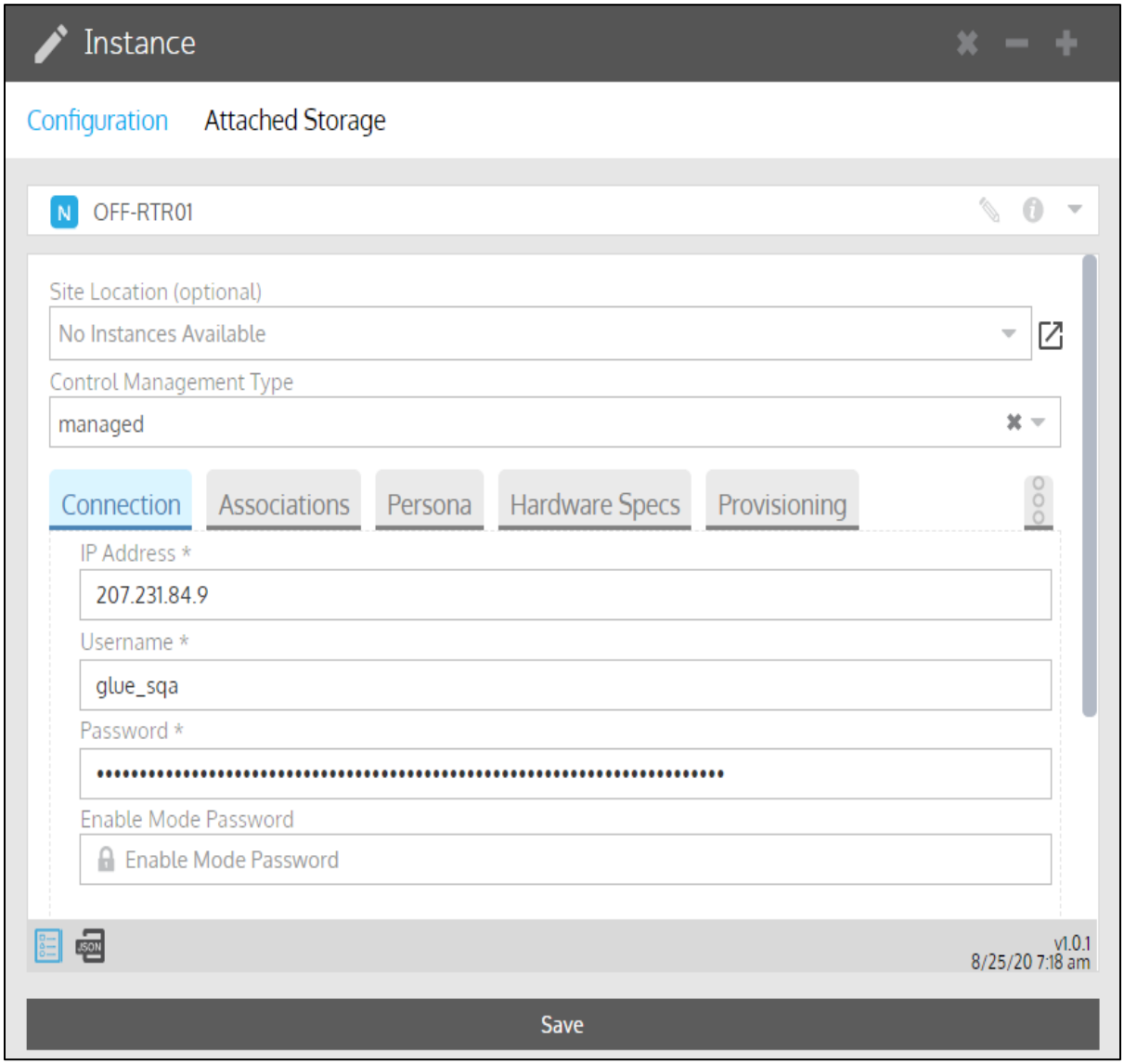
Creating a CLI State Assessment Query is optional. Queries are useful for filtering the results of the state assessment, so you have only the data you want to use.

1. Go to **Config Modeling** > **Globals**.
2. Select **CLI State Assessment Query** from the drop-down list.
3. Click +.
4. In the Instance panel, click ✎ and name and describe the query instance.
5. From the **Mode** drop-down list,
    - Select **Simple** if there is one lookup table.
    - Select **Advanced** if you want multiple, inclusive lookup tables.
6. Select the **Query Type** from the drop-down list:
    - **Count** – Counts all occurrences.
    - **Simple Lookup (at least one match)**
    - **Inclusive Lookup (all need to match)**
7. Click + and then click ✎ to enter the query info in a form.
8. Select the **Filter Type** from the drop-down list,
    - **Pattern** – Refines filtering done by the **CLI State Assessment Policy** for the node.
    - **Port Name** – Filters for a specific port name from the node's **Port Map**.
9. Enter the regex for the key to filter. Or enter the **Port Name**.
10. Enter the **Category** name from the **CLI State Item** for the node.
11. Enter the **Field Value** (the regex) from the **CLI State Item** for the node.
12. Optional: Click +, click ✎, and enter additional query info to the form.
13. Save.


Instance
*Configuration
Attached Storage
Unnamed-cliStateQuery-1
Fields
Filter Type Filter Pattern/Port Nam Category Field Name
1 Pattern .+
State Assessment Query Details
Filter Type
Pattern
Filter Pattern/Port Name
.+
Category
Category
Field Name
Field Name
Field Value
Field Value
v1.0.0
2/17/20 9:34 am
Save

Associate an Assembly with a node

1. Go to **Config Modeling** > **Nodes**.
2. Select the type of **node** from the drop-down list.
3. Select a **node** in the grid list.
4. Click .
5. Click **Associations** and then select an **Assembly** from the drop-down list.
6. Save.



Associate a CLI State Assessment Policy with an Assembly

You can associate a different CLI Assessment Policy for OS Management, Provisioning, or running on demand.

1. Go to **Config Modeling** > **Domains**.
2. Select the type of **Assembly** from the drop-down list.
3. Double-click an **Assembly** in the center grid to open the instance.
4. In the Instance panel, click **State**.
5. Click **Add Item+**.
6. Select when you want to assess the state:
    - **while performing an OS Management**
    - **On-Demand**
    - **while performing a Provisioning**
7. Select the **CLI State Assessment Policy** from the drop-down list.
8. Select from the drop-down list:
    - For OS management:
        - **After OS Management**
        - **Before and After OS Management**
        - **Before OS Management**
        - **Off (no assessment)**
    - For On-Demand:
        - **Abort on Errors**
        - **Ignore Errors**
        - **SYSLOG Message**
    - For Provisioning:
        - **After Provisioning**
        - **Before and After Provisioning**
        - **Before Provisioning**
        - **Off (no assessment)**
9. Save.

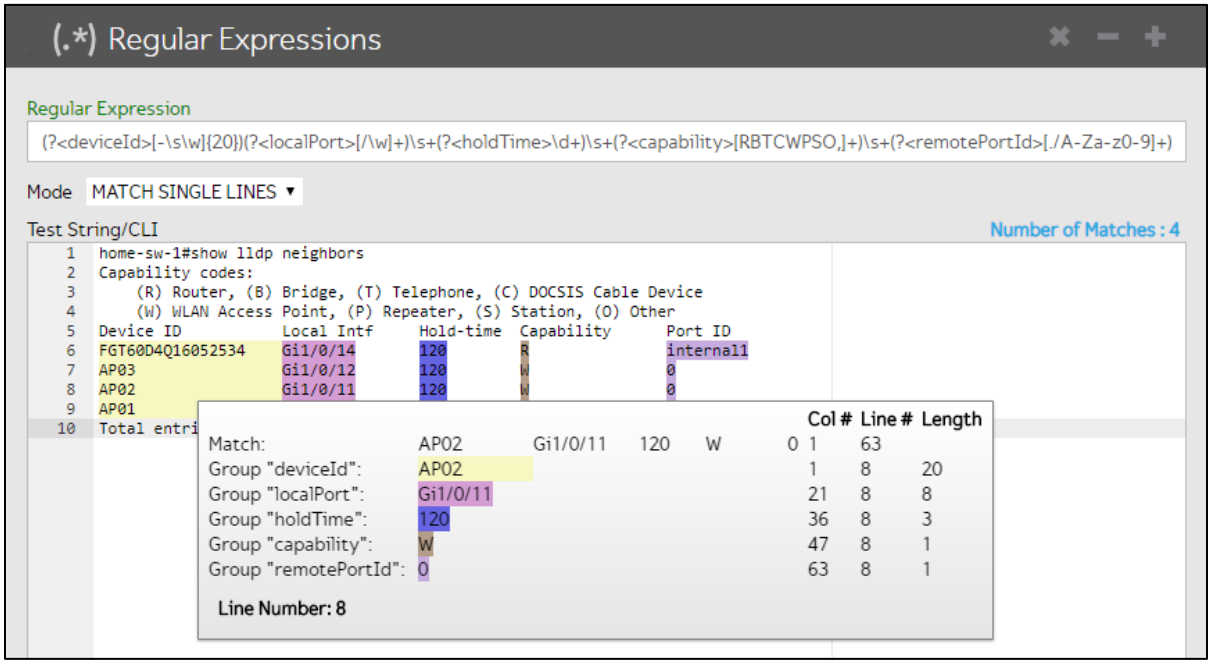
Test your regular expression

A regular expression (regex) is a powerful tool for identifying sections of the configuration to act upon. You can use the Gluware **Regular Expressions validator** to test your regex and ensure it identifies the appropriate sections of the configuration for your purpose. You don't need to provision to see the effect of your regex. Simply paste your regex into the validator to see the section of the configuration that will be impacted. Make changes and immediately see the difference.

You'll need a **Config Modeling** license to use the **Regular Expressions validator**.

1. Go to **Config Modeling** and click (.*) at the bottom of the screen.
2. Enter the regular expression you want to test.
3. Select a view mode:
    - **Match Single Lines** – Finds any single lines in the configuration that match the regex and identifies the named groups by color. You can hover over the results to get details like the line number in the configuration and the length of the string.
    - **Match All Lines** – Finds matches that occur on more than one line.
    - **Match Sections** – Highlights entire sections of the configuration that match the regex. Specify the appropriate section delimiter: **default** (not indented line) or **!**

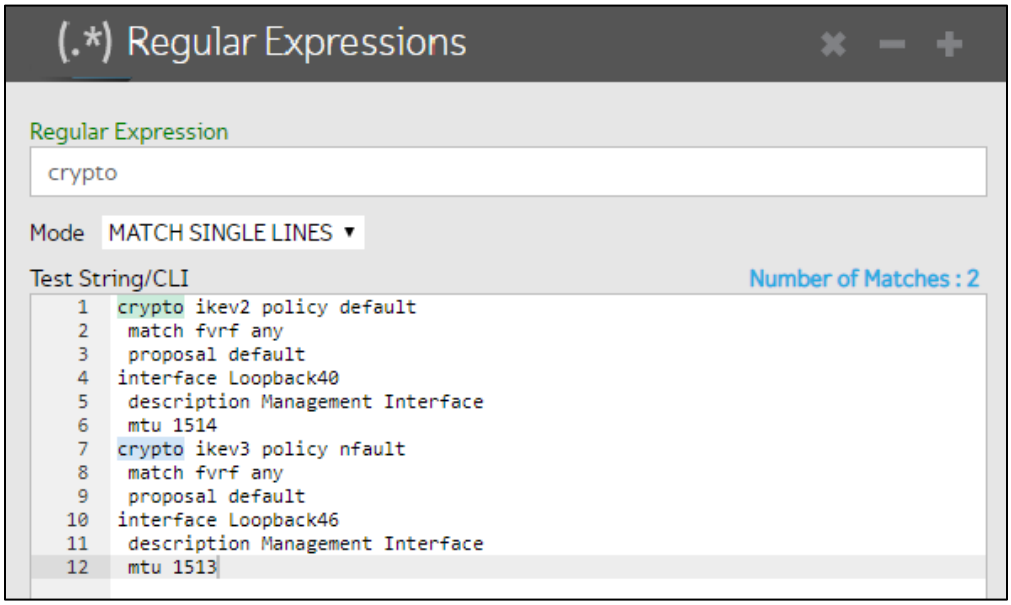
4. Paste or type the text you want to test the regular expression on. The validator will highlight in color the named groups identified in the text. Hover over the highlights to see the details.



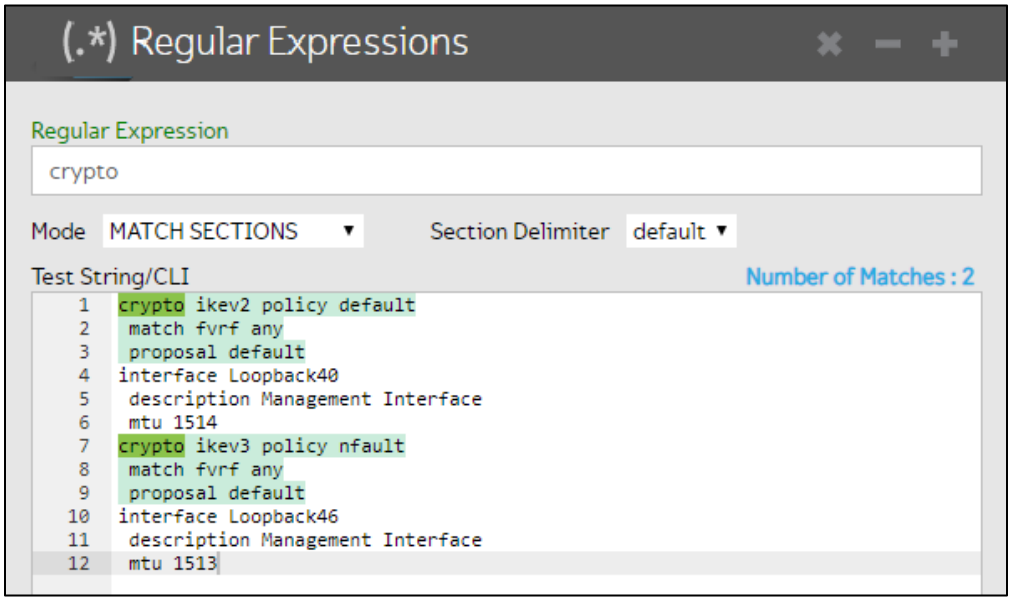
regex refresher

Find a single character x, y, or z: **[xyz]**
Find any character except x, y, or z: **[^xyz]**
Find a character in the range m-z: **[m-z]**
Find a character outside the range m-z: **[^m-z]**
Find a character in the range M-Z or m-z: **[M-Zm-z]**
Find any single character: **.**
Find any white space: **\s**
Find any non-white space character: **\S**
Find any digit: **\d**
Find any non-digit: **\D**
Find any word character: **\w**
Find any non-word character: **\W**
Find everything within: **(...)**
Find either x or z: **(x|z)**
Find zero or one z: **z?**
Find zero or more z's: **z***
Find one or more z's: **z+**
Find five z's: **z{5}**
Find five or more z's: **z{5,}**
Find two to five z's: **z{2,5}**
Start of a string: **^**
End of a string: **$**
Boundary of a word: **\b**
Boundary of a non-word: **\B**
New line: **\n**
Return: **\r**
Tab: **\t**
Null character: **\0**

Match Single Lines example



Match Sections example

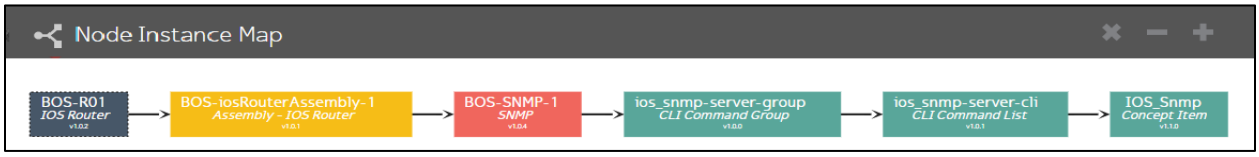


View the relationships in your model

View a Node Instance Map

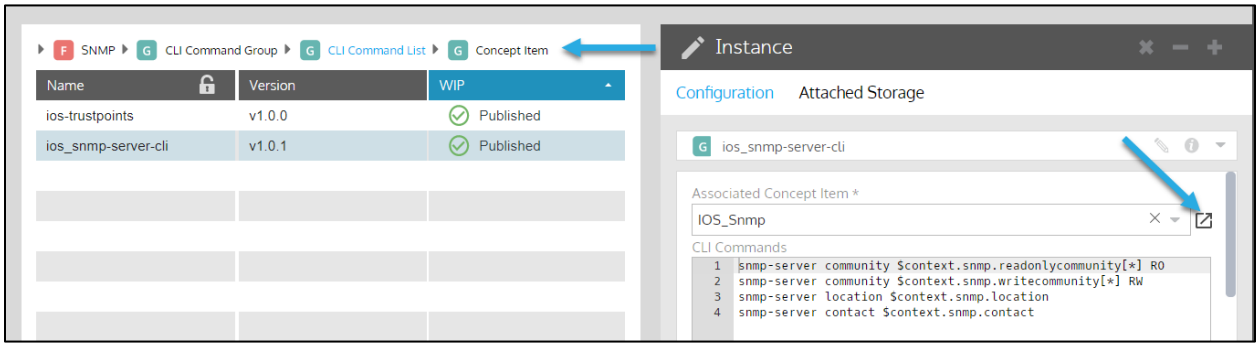
You can see a diagram of the **Assemblies**, **Features**, **CLI Command Groups**, **CLI Command Lists**, and **Concept Items** that are currently associated with a node.

1. Go to **Config Modeling** > **Nodes**.
2. Select the type of node in the drop-down list.
3. Select a node in the grid.
4. Point to the bottom edge of the screen and select to see a **Node Instance Map**.
5. Click-and-drag to reposition the map. Click and scroll up to enlarge the map.
6. Double-click on any item in the map to open and inspect the instance details.



View referenced instances or types

1. In **Config Modeling**, in any instance panel, click . The icon's tooltip explains where you will go.
2. Use the breadcrumbs at the top of the grid to return.



Preview the modeled Feature

Preview will generate the new configuration for review, but not write it to the device. Three preview types are available:

- **Model Validation** – Performs a validation of the model configuration to ensure completeness of required properties and references.
- **Initial Preview** – Validates the model and creates a list of the CLI commands that would be generated to support this model. No analysis of the existing configuration is performed; no connection to the node is required.
- **Connected** – Model validation occurs but, in this case, the existing device configuration is analyzed and the CLI model generated is the difference between the existing CLI and the proposed CLI model. This option requires a connection to the device.

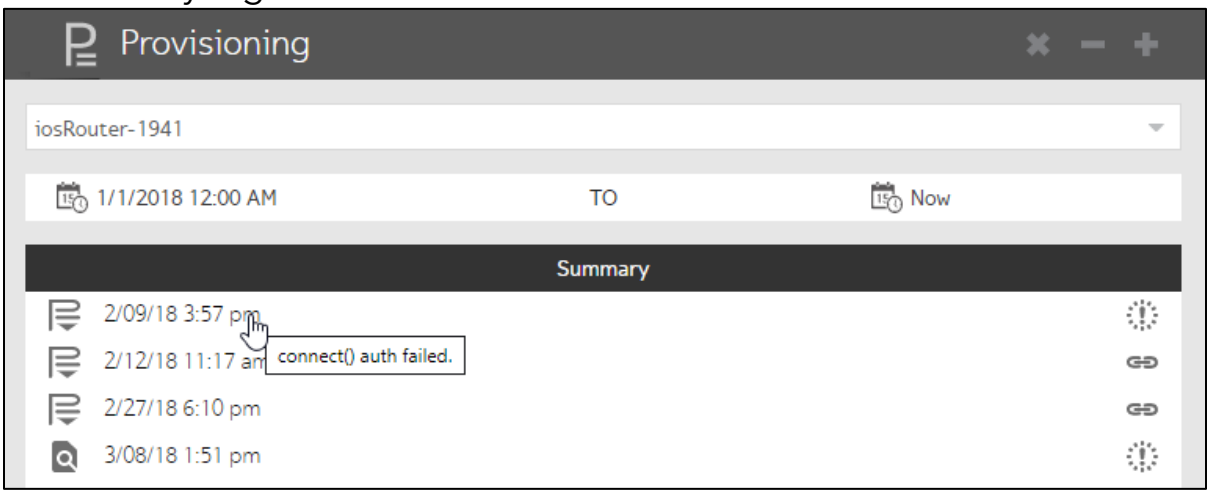
1. Ensure you're in the organization you want to preview the model for.
2. Go to **Config Modeling** > **Nodes**.
3. Select the type of node from the drop-down list or filter the list.
4. Select the node you want to preview the model for in the grid list.
5. Click .
6. Select **Provisioning Utilities** to provision over the network.
7. Select **Preview Features**.
8. To run the preview now:
    a. Click **Start Action**.
    b. Optional: Enter a description to display in the summary.
    c. Select the preview type: **Connected**, **Initial**, or **Model Validation**.
    d. Optional: Enter information to include in the log entry.
    e. Click **Proceed**.

9. To schedule the preview:
    a. Click **Schedule Action**.
    b. Select **One Time** or **Repeating** and the specify the schedule.
    c. Check the boxes of those to receive notification that the preview is complete. Select from those listed or add email addresses to **Other recipients**. Separate email addresses with a comma.
    d. Optional: Enter a description to display in the summary.
    e. Select the preview type: **Connected**, **Initial**, or **Model Validation**.
    f. Optional: Enter information to include in the log entry.
    g. Click **Proceed**.
10. Enter optional identifying information for the **Log Comment**.
11. Click **Start Action**.
12. Click to review the preview log.

View a Config Modeling device log

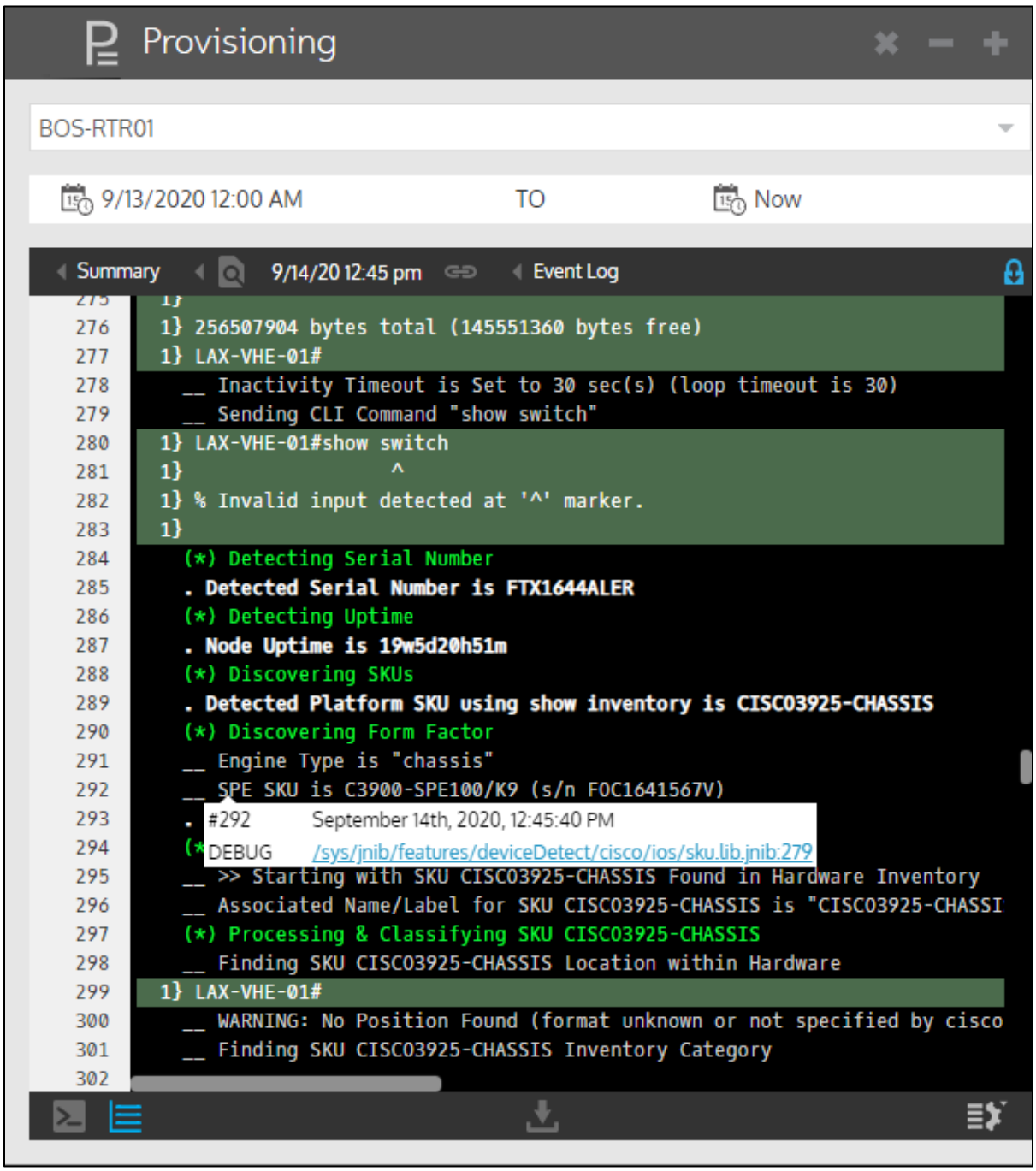
The Config Modeling preview and provisioning logs include both Gluware errors and device errors. Use the logs to review and troubleshoot previews and provisioning.

1. Go to **Config Modeling** > **Nodes**.
2. Select the type of node from the drop-down list or filter the list.
3. Select a node in the grid and click . The **Provisioning** panel **Summary** lists all the logs for the selected node in chronological order. The list might include:
   - Provisioning logs
   - Preview logs including CLI models for the selected Preview mode (Model Validation, Initial, or Connected)
   - Bootstrap logs for usbConnect provisioning
   - OS management logs
4. Specify a date range for logs you want to review. Icons on the right show the status:
   - Provisioning completed
   - Provisioning error
   - Provisioning canceled
5. Point to any log with an error to see the error condition.



6. Double-click a log to review it. Or, if provisioning is successful, go to **Config Drift and Audit** and take a snapshot to ensure the configuration is what you expect.

Tips for reviewing the log



- When you see an error or warning, you may need to inspect the lines above it to determine the cause.
- Click to pause scrolling.
- Click **Show Settings** to:
  - **Search for a text string** – Enter the text string and click **Enter**. Check the **Case-Sensitive** box to make the search case-sensitive. Clear the box to ignore case. Click > and < to see the occurrences found.
  - **Change the line label** – Select a line label from the

drop-down list. Select from:
Log Event #
Line Number
Timestamp
Time Passed
Event Duration
  - **Filter the log** – Click . Check or clear the boxes to display just the levels you want. All levels are displayed by default.
  - **See the source code file and line number that produced the log line** – Point to a line.

Log Levels	Description
Error	A problem that must be fixed
Warning	A problem that did not stop the process but should be fixed
Task	The beginning or the end of a step
Checkpoint	A significant point in the code
Info	General info about the process that does not fit in the other logging categories

Log Levels	Description
Response	The raw interaction between the Gluware engine and the device
Debug	Low-level informational log messages usually related to the internal state of code variables. It's specific to how the code is working, as opposed to how the process is proceeding

- Click to cancel provisioning.
- Click to display the log in CLI view. **Raw** reflects the line-by-line interactions with the device. **Processed** is a summary by feature. CLI view is helpful in troubleshooting errors.
- Click to display the log in list view.
- When you see an error or warning, inspect the lines above it to determine the cause.
- Click to download the provisioning bundle to a ZIP folder. You can add the ZIP folder to a Support ticket if you are not able to resolve all the issues.

Provision nodes

There are two methods of provisioning nodes using Gluware: through a connection from Gluware to the node (**advanced** provisioning) and via a Gluware-configured USB bundle that is downloaded on a USB stick (**usbConnect**). usbConnect is used when the node cannot be accessed by Gluware (e.g., NAT). The connection is established by the node to Gluware.

Best practice: Preview your changes before provisioning nodes.

> **NOTE: usbConnect** only functions on IOS devices and the gluWatchdog Agent Feature must be associated with the device's Assembly.

Assign the provisioning type to the node

1. Ensure you're in the organization you want to provision nodes for.
2. Go to **Config Modeling** > **Nodes**.
3. Select the type of node from the drop-down list or filter the list.
4. Select the node you want to provision in the grid list.
5. Click .
6. Select **Provisioning**.
7. Select **Advanced** or **usbConnect** from the drop-down list.
8. Save.

Provision the node using advanced provisioning

1. Ensure you're in the organization you want to provision nodes for.
2. Go to **Config Modeling** > **Nodes**.
3. Select the type of node from the drop-down list or filter the list.
4. Select the node or nodes you want to provision from the grid list.
5. Click .
6. Check the boxes of the devices you want to provision.

7. Select **Provisioning Utilities** to provision over the network.
8. In the second drop-down list, select **Provision Features** to provision over the network.
9. To provision now:
    a. Click **Start Action**.
    b. Optional: Enter a description to display in the summary.
    c. Optional: Enter information to include in the log entry.
    d. Click **Proceed**.
10. To schedule provisioning:
    a. Click **Schedule Action**.
    b. Select **One Time** or **Repeating** and the specify the schedule.
    c. Check the boxes of those to receive notification that provisioning is complete. Select from those listed or add email addresses to **Other recipients**. Separate email addresses with a comma.
    d. Optional: Enter a description to display in the summary.
    e. Optional: Enter information to include in the log entry.
    f. Click **Proceed**.
11. Click to review the provisioning log.

Provision the node using usbConnect

1. Ensure you're in the organization you want to provision nodes for.
2. Go to **Config Modeling** > **Nodes**.
3. Select the type of node from the drop-down list or filter the list.
4. Select the node or nodes you want to provision from the grid list.
5. Click .
6. Check the boxes of the devices you want to provision.
7. Select **Device Agent Utilities** to provision using a USB.
8. In the second drop-down list, select **Download USB Bundle**.
9. Click **Start Action**. A ZIP folder is downloaded to your Downloads folder.
10. Copy the ZIP folder to a USB.
11. Insert the USB key in the device and reset the device to read the USB on boot. A bootstrapper agent configures the device to establish connectivity to Gluware. Provisioning then begins.

12. Click in Gluware **Config Modeling** to review the provisioning log.

Assess the state of a node

You can assess the state of a node before and after provisioning or an OS upgrade. You can also assess the state on demand. Specify which CLI State Assessment Policy to run by associating the appropriate policy with the node's Assembly.

Watch a demo of state assessment at https://youtu.be/zkXxzMixgmU

1. Go to **Config Modeling** > **Nodes**.
2. Select the type of node from the drop-down list.
3. Select the node or nodes you want to assess from the grid list.
4. Click .
5. Check the boxes of the nodes you want to assess.
6. In the first drop-down list, select **State Assessment Utilities** to test your CLI State Assessment Policy.
7. In the second drop-down list, select one of the following:
   - **Run On-Demand Policy**
   - **Run Provisioning Policy**
   - **Run OS Management Policy**
8. To run the state assessment now:
   a. Click **Start Action**.
   b. Optional: Enter a description to display in the summary.
   c. Optional: Enter information to include in the log entry.
   d. Click **Proceed**.
9. To schedule the state assessment:
   a. Click **Schedule Action**.
   b. Select **One Time** or **Repeating** and specify the schedule.
   c. Check the boxes of those to receive notification that provisioning is complete. Select from those listed or add email addresses to **Other recipients**. Separate email addresses with a comma.
   d. Optional: Enter a description to display in the summary.
   e. Optional: Enter information to include in the log entry.
   f. Click **Proceed**.
10. Click to review the assessment log.

Package a Feature for distribution

You can package a Feature to install it in another organization.

1. Go to **Workflows**.
2. Expand the **Design** folder and double-click **Network Feature Distribution**. You'll see a description of the workflow in the top pane.
3. Click **Next**.
4. Select **the Feature you want to package** and click **Next**.
5. In the **Available** list, select the Feature instances you want to package and click →. The ↠ selects all the available instances.
6. Click **Next**.
7. Provide a package name and description.
8. To change the version numbering schema, select a schema from the **New Version** drop-down list.
9. Provide a version description.
10. Click **Finish**. This creates a capsule file in your Downloads folder. The file can be imported to another organization through Solutions Manager.

Monitor changes with the gluWatchdog agent

The **gluWatchdog** agent is an optional agent for Cisco routers and switches. **gluWatchdog** can:

- Call home at specified intervals to check for a new version and any pending Agent actions
- Roll back provisioning if there is an error
- Monitor devices for unauthorized manual configuration changes
- Monitor IP address changes
- Enable/disable network interfaces
- Monitor SSH services

Configure a gluWatchdog Feature

1. Go to **Solutions Manager** > **Available Packages**.
2. Download a package that includes **gluWatchdog**. You'll find gluWatchdog in the SD-WAN (compatible with Cisco IWAN 2.0), Config Modeling Kit for Cisco IOS Router, and Config Modeling Kit for Cisco IOS Switch packages.
3. Ensure you're in the organization you want to create a **Feature** for.
4. Go to **Config Modeling** > **Features**.
5. Select **gluWatchdog Agent** from the drop-down list.
6. Click ➕.
7. Click ✎ and name and describe the agent instance.

8. Configure the instance:

Field	Description
Automatically Update	When the gluWatchdog agent calls home, it checks the version of the agent on the server. If the agent on the server is newer, it downloads and installs a new agent.
Call Home interval (hours)	How often the agent calls home and checks for a new version and any pending Agent actions.
Checkpoint	Checkpoint can be used to recover a node if connectivity is lost due to a configuration change. If enabled, when you provision a node, it copies the current running config and creates a checkpoint timer when the first feature is started. If there's more than one Feature in your Assembly, it checks to see if half of the time has elapsed and if so, resets the timer and the next Feature executes. If half of the time has not elapsed, it does not reset the timer before the next Feature. At the end of executing all the Features without errors, the checkpoint timer is removed. If the timer expires before the end of a Feature or because provisioning failed, the agent copies the running config to the startup config and reloads the node. If provisioning fails and the node is still reachable by the engine and you restart provisioning, the checkpoint timer is reset.
Checkpoint timeout (minutes)	The checkpoint timer length in minutes. This value should be at least twice the amount of time it will take to run the longest Feature in your Assembly.

Field	Description
Report Configuration changes	Sends the user name and time of the configuration change to the server. This information will be in the grid column, Manual Config Change. Each time the node is provisioned, the information is cleared from the grid for the node. Does not report configuration changes that are made during provisioning.
Report IP Address changes	Sends IP address changes to the Gluware server. This is useful for a directly addressable node using DHCP. If the node's IP changes, the server will not be able to find the node. If you have a fixed IP or the node is NATed and you access it through a tunnel, you do not need this option.
Allow Agent Actions	Allows scheduled agent actions to run on the node. When the agent calls home, checks for pending agent actions (Enable/Disable Network Interfaces, Restore Original Configuration, Cert Renewal). If there are one or more, it will start the action to run.
Monitor SSH Service	Allows the agent to watch for disabled SSH server log message and re-enable SSH server on the node by generating a new SSH key.
SSH Key Size	The SSH key size. Values are 1024, 2048, and 4096. If the agent creates the SSH key, it is created with this byte value. The agent regenerates the key if the SSH server is disabled at reboot or if it gets a log message disabling the SSH server and Monitor SSH Service is selected.

8. Go to **Config Modeling** > **Domains**.
9. Select the type of **Assembly** from the drop-down list.
10. Double-click an **Assembly** instance in the grid, select **Agents** in the Instance panel, and select the **gluWatchdog Feature** instance you configured from the gluWatchdog **Policy** drop-down list.
11. Ensure the node you want to monitor is associated to this Assembly.

Cancel a gluWatchdog checkpoint timer

Sign in to Gluware via a terminal session and enter:

```
event manager run gluWatchdog.tbc
flash:/gluware/cfgs/rollback0.cfg cancelCheckpointTimer
```

See the number of event manager scripts in the queue

Sign in to Gluware via a terminal session and enter:

```
show event manager policy pending
```

Stop all event manager scripts and clear the queue

Sign in to Gluware via a terminal session and enter:

```
event manager scheduler clear all
```

Restore the original configuration

You can reset an IOS device configuration to that which was present on the device when it was first provisioned in Gluware. The original configuration will be restored the next time the **gluWatchdog Agent** calls home, or when the device is reset, whichever occurs first.

> **NOTE:** **Restore Original Configuration** only functions on IOS devices and the gluWatchdog Agent Feature must be associated with the device's Assembly.

1. Go to **Config Modeling** > **Nodes**.
2. Select the type of node from the drop-down list.
3. Select the node instance in the grid.
4. Click .
5. Check the node's box.
6. Select **Device Agent Utilities** from the first drop-down list.
7. Select **Restore Original Configuration** from the second drop-down list.
8. Click **Start Action** or **Schedule Action**.

Disable and enable network interfaces

You can disable all the network interfaces on an IOS device, for example, when preparing a device for shipment to a new location, and then enable them again. These actions will take place the next time the **gluWatchdog Agent** calls home, or when the device is reset, whichever occurs first.

> **NOTE:** Disable/enable is only supported on IOS devices. The gluWatchdog Agent Feature must be associated with the device's Assembly and **Allow Agent Actions** must be enabled in the gluWatchdog policy.

1. Go to **Config Modeling** > **Nodes**.
2. Select the type of node from the drop-down list.
3. Select the node instance in the grid.
4. Click .
5. Check the node's box in the **Action** panel.
6. Select **Device Agent Utilities** from the first drop-down list.
7. Select **Disable Network Interfaces** or **Enable Network Interfaces** from the second drop-down list.
8. Click **Start Action** or **Schedule Action**.

Update the gluWatchdog agent

Check for Config Modeling Kit updates

The **gluWatchdog** agent comes in the **Config Modeling Kit for Cisco IOS Router** and the **Config Modeling Kit for Cisco IOS Switch** packages. Check if an update is available for these packages.

1. Ensure you're in the organization you want to install the package in.
2. Go to **Solutions Manager** > **Available Packages**.
3. Check if an update is available for the IOS router or switch Config Modeling Kits in the **Package Explorer**.
4. Double-click on the name of the package you want to update.
5. Select **Preview** and then click **Preview Package Installation**. Look for “Preview Completed!” when the preview script runs successfully.
6. Select **Install** and then click **Install Package**.

Update gluWatchdog

1. Go to **Config Modeling** > **Nodes**.
2. Select **IOS Router** or **IOS Switch** from the drop-down list.
3. Select a node instance in the grid.
4. Click .
5. Check the node's box in the **Action** panel.
6. Select **Device Agent Utilities** from the first drop-down list.
7. Select **Update gluWatchdog** from the second drop-down list.
8. Click **Start Action**.

Run a workflow in Config Modeling

You can run a workflow in **Config Modeling** that can operate on any Gluware construct (domain, feature, global, or node). Workflows can be designed to capture information, create, modify, edit, or delete. For example, a workflow could assign credentials to one or more nodes or retrieve features from devices.

These packages need to be installed to run workflows in **Config Modeling**:

- Workflows for Config Modeling
- Config Modeling Kit for the appropriate vendor device

1. Ensure you're in the organization the workflow is installed in.
2. Go to **Config Modeling** > **Nodes**, **Domains**, **Features**, or **Globals**, depending on the construct the workflow is designed to act upon.
3. Select the type of instance from the drop-down list.
4. In the grid, right-click an instance to display the workflows available.
5. Click on the name of the workflow. The **Workflows** panel opens to display the first workflow page.
6. Follow the instructions on the workflow pages.

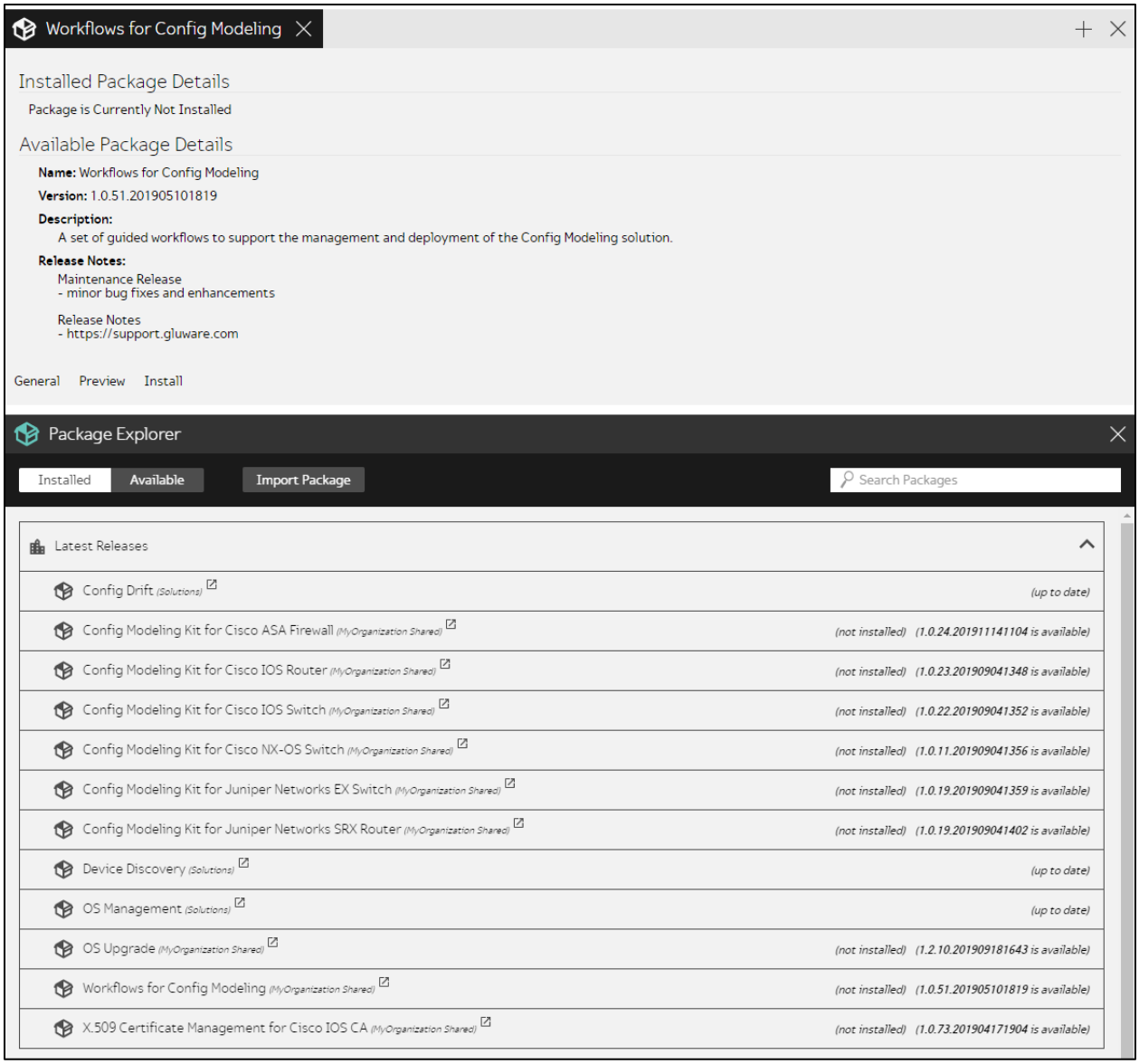
Model an SNMP feature
Step 1. Install packages

To model an SNMP feature for an IOS Router, you'll need to go to **Solutions Manager** and install the following packages in the organization that contains the devices you want to model:

- Workflows for Config Modeling
- Config Modeling Kit for Cisco IOS Router

Install (or update) the two packages

1. Ensure you're in the organization in which you want to install the packages.
2. Go to **Solutions Manager** > **Available Packages**.
3. Open the Latest Releases folder.
4. Double-click the **Workflows for Config Modeling** package.
5. If you see “Package is Currently Not Installed” or "Available Package Details" in the top pane,
    a. Select **Preview** and then click **Preview Package Installation**.
    b. Select **Install** and then click **Install Package**. You’ll see “Installation Completed!” when the installation is successful. Any problems with the installation will appear as red error messages.



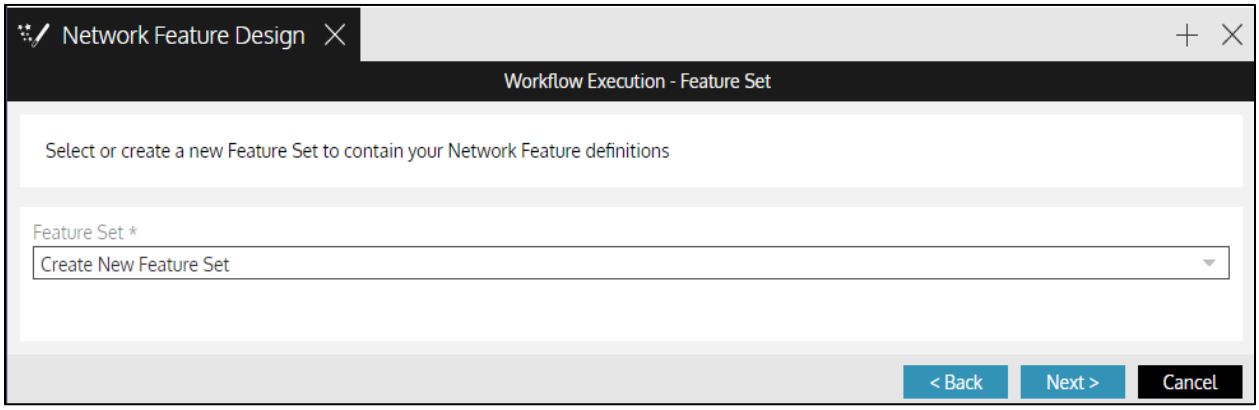
5. In the Package Explorer, double-click the **Config Modeling Kit for Cisco IOS Router** package.
6. If you see “Package is Currently Not Installed” or "Available Package Details" in the top pane,
    a. Select **Preview** and then click **Preview Package Installation**.
    b. Select **Install** and then click **Install Package**.

Next: Step 2. Design an SNMP Feature type

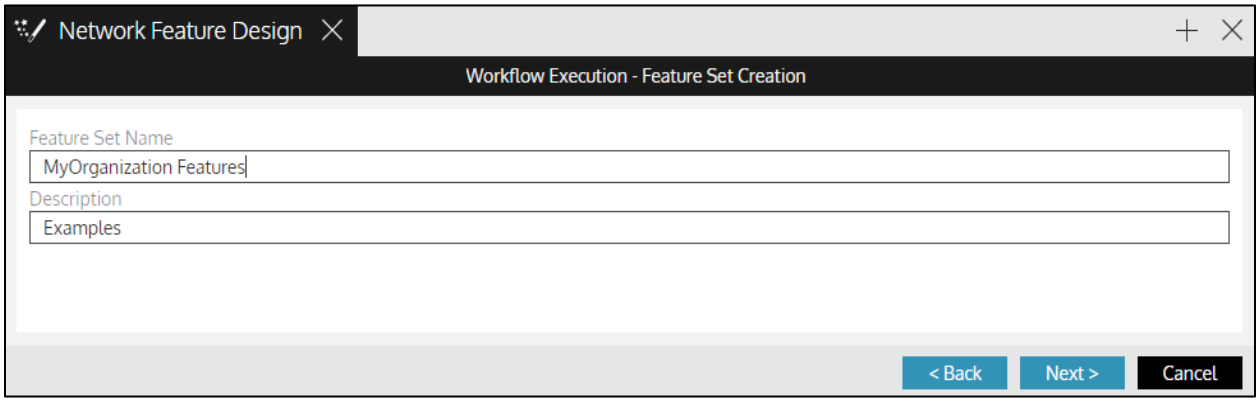
Model an SNMP feature
Step 2. Design an SNMP Feature type

In **Workflows**, you'll set up a **Feature Set** for your organization that includes a form for an SNMP feature. You can add additional feature types to your organization's Feature Set at a later time by modifying the Feature Set.

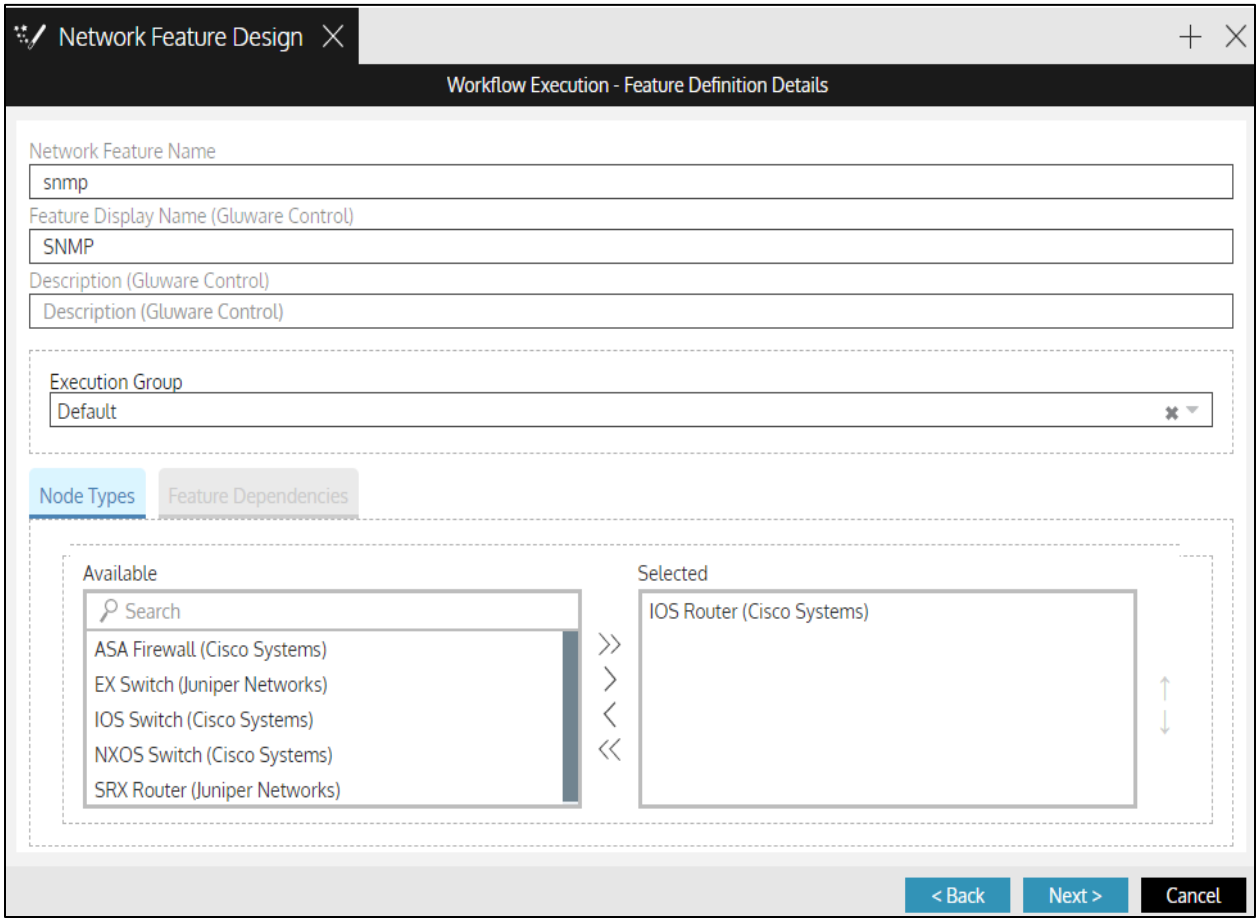
1. Go to **Workflows**.
2. Expand the **Design** folder, double-click **Network Feature Design**, and click **Next**.
3. Select **Create New Feature Set** and click **Next**.



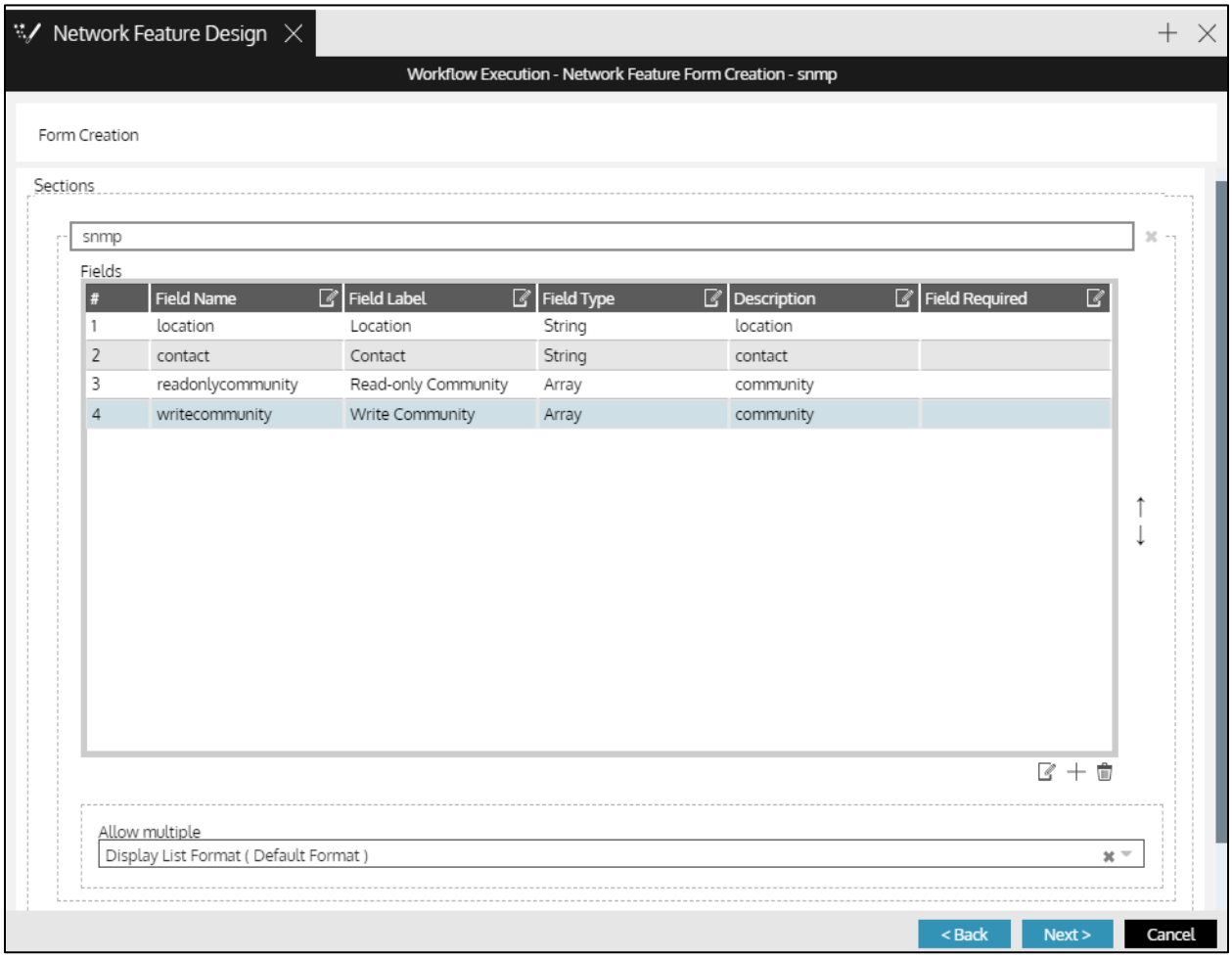
3. Name and describe the Feature Set and click **Next**.



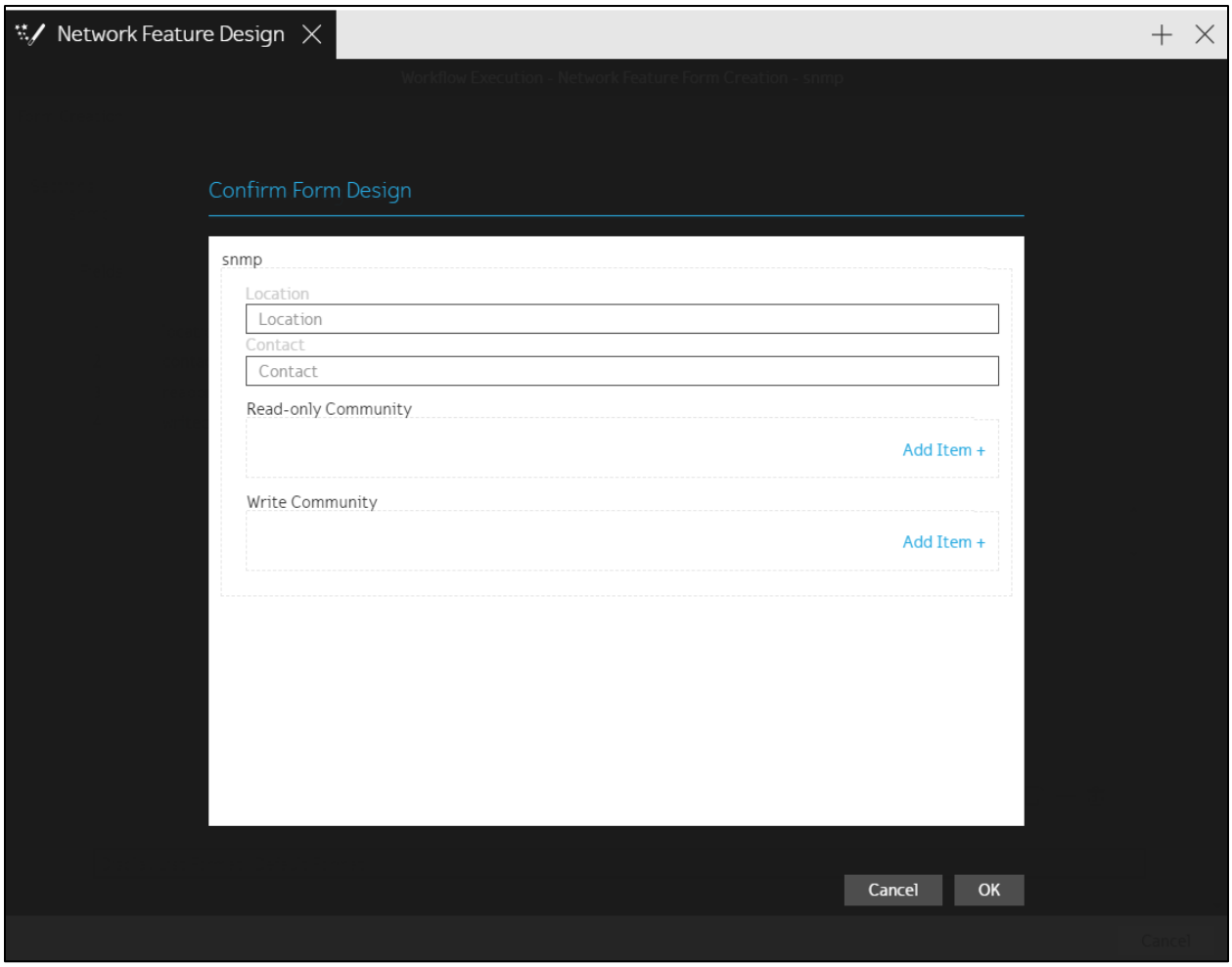
4. Then create the SNMP Feature within the Feature Set: Name the feature, enter a display name, select IOS Router from the nodes list and click →. Then click **Next**.



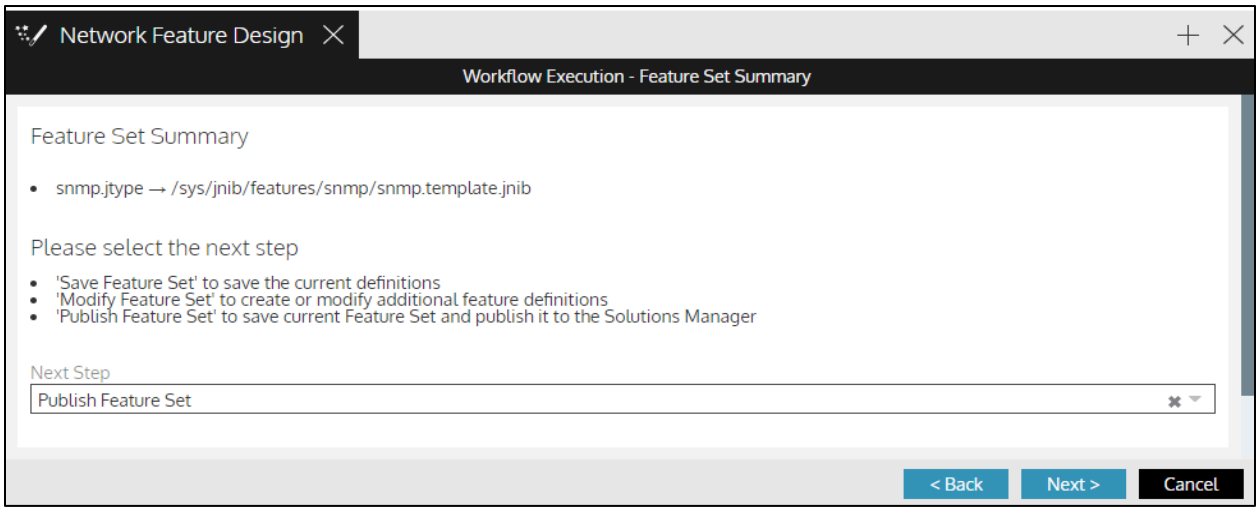
5. Click **Add Section+**.
6. Click the + to set up the fields you want to see on the form for the feature. The field values can then be used within the CLI, allowing rendered values to be dynamic. In our example, Location, Contact, Read-only Community, and Write Community will appear in the feature you create. When you're done, click **Next**.



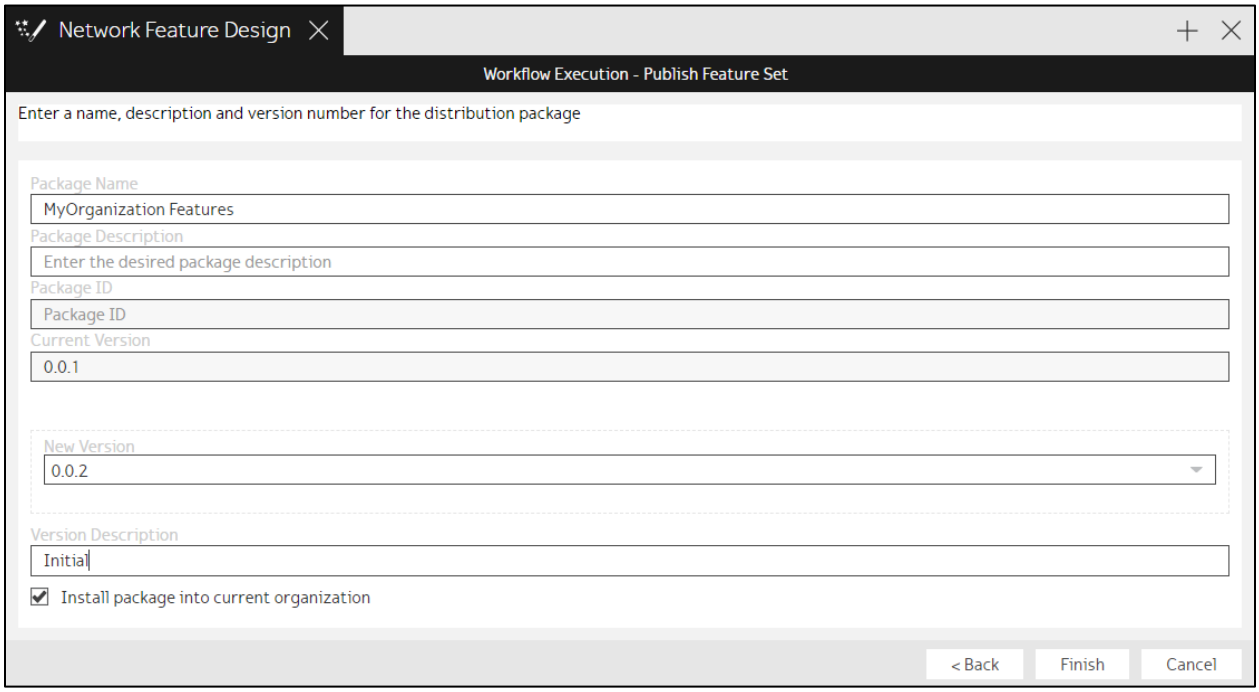
7. Then you get to preview the form you just created. When the form looks good, click **OK**.



8. Publish it to your organization to make it available in **Config Modeling** and click **Next**.

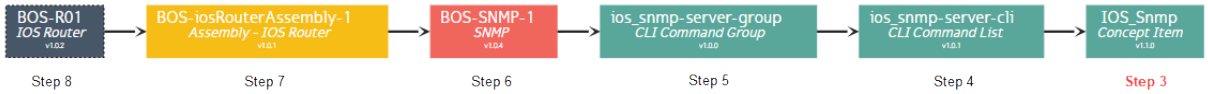


9. Add a version description and click **Finish**.



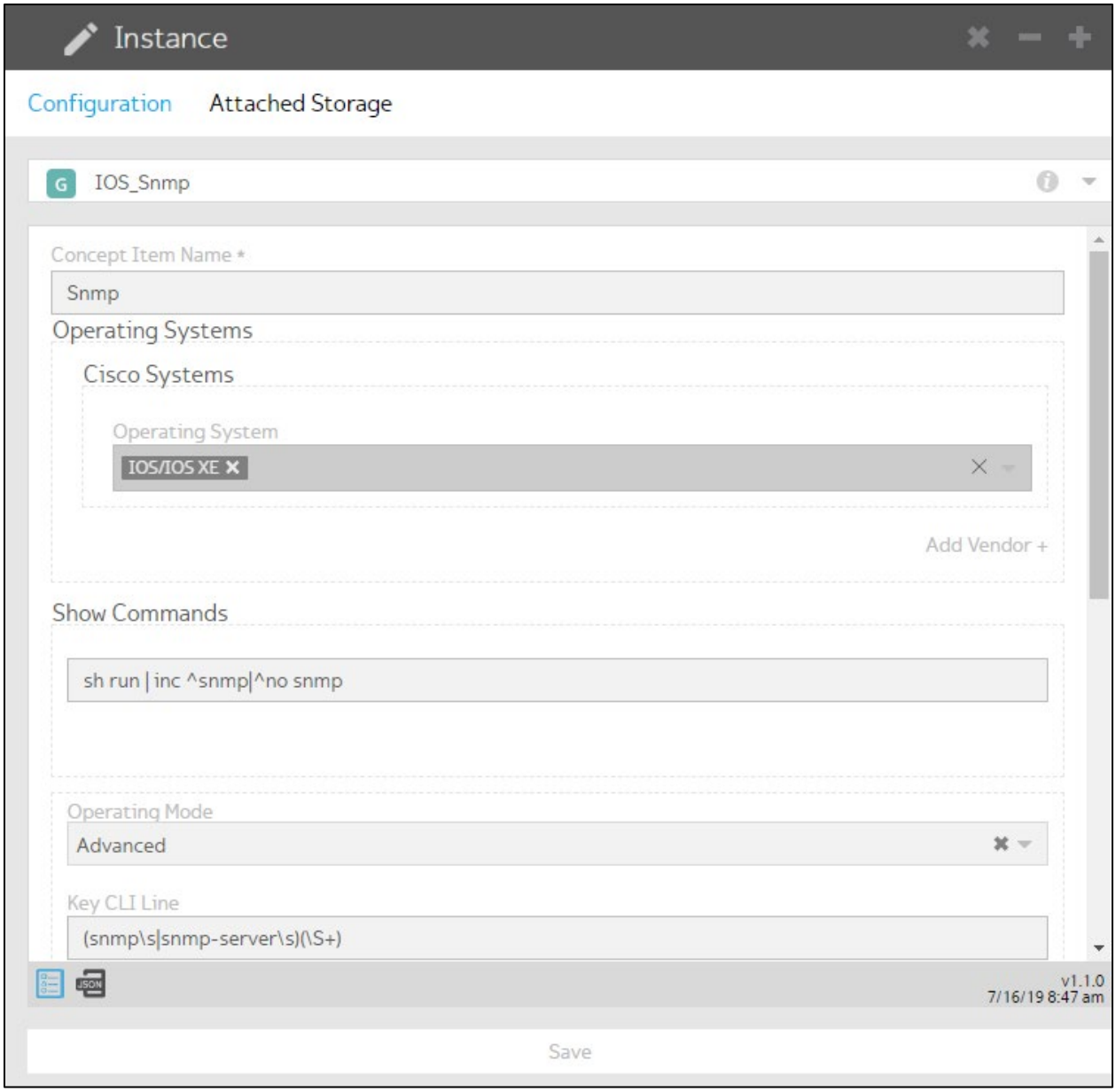
Next: Step 3. Select a Concept Item

Model an SNMP Feature
Step 3. Select a Concept Item



Now you'll go to **Config Modeling** and find the IOS SNMP **Concept Item**. The Concept Item lists the show commands that will be executed on the node. In this case, we ask for everything in the IOS router configuration related to SNMP.

1. Go to **Config Modeling** > **Globals**.
2. Select **Concept Item** from the drop-down list.
3. Double-click the **IOS_Snmp** instance in the grid list to view the details.



Next: Step 4. Create a CLI Command List for SNMP

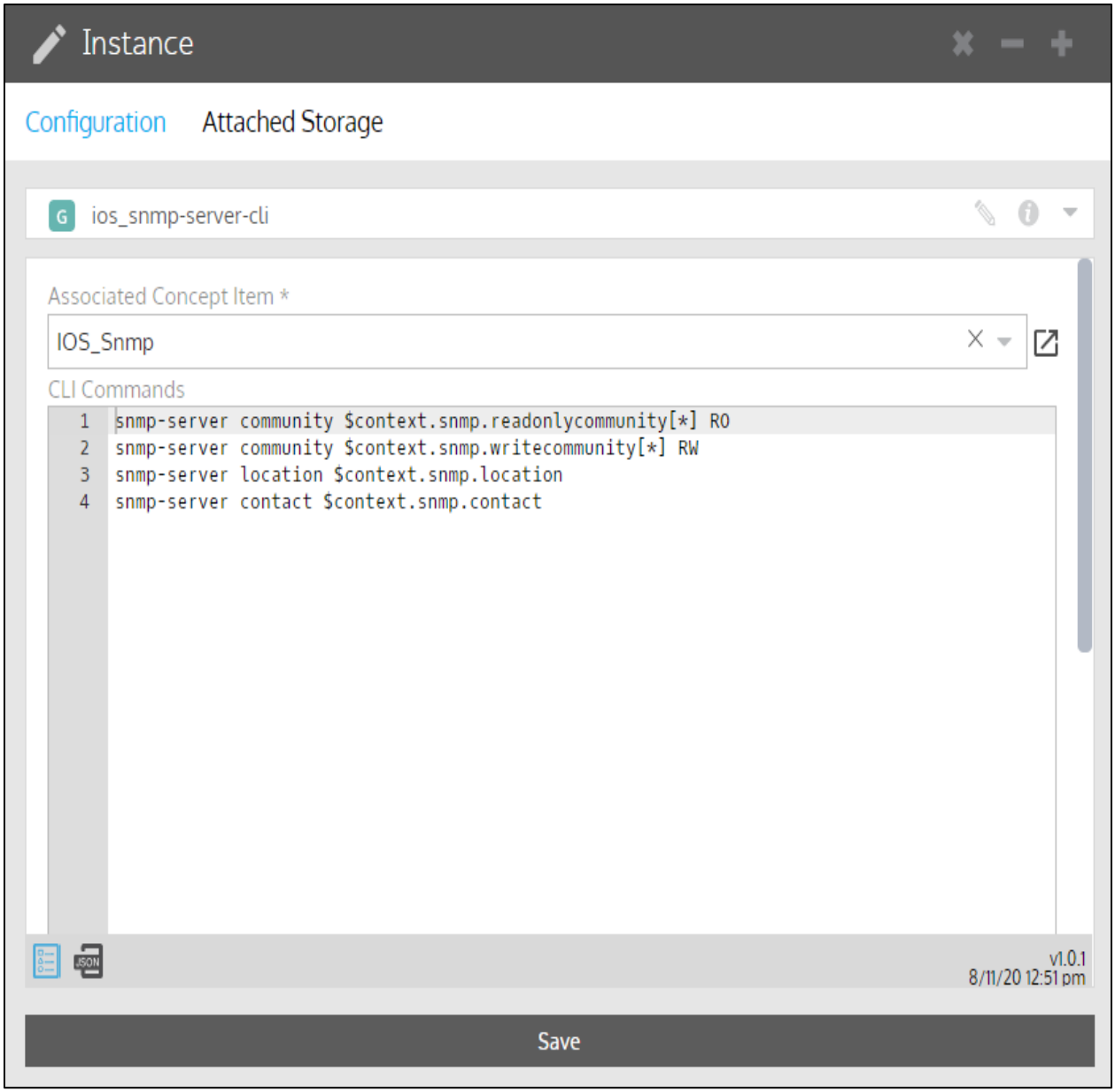
Model an SNMP feature
Step 4. Create a CLI Command List for SNMP

In Config Modeling, create your **CLI Command List** for SNMP. In our example, we are introducing variables:

```
snmp-server community
$context.snmp.readonlycommunity[*] RO
snmp-server community $context.snmp.writecommunity[*]
RW
snmp-server location $context.snmp.location
snmp-server contact $context.snmp.contact
```

These variables will be resolved to the actual commands that will be run on the device.

1. Go to **Config Modeling** > **Globals**.
2. Select **CLI Command List** from the drop-down list.
3. Click ➕.
4. Click ✎ in the Instance panel and name the list **ios_snmp-server-cli**.
5. Select the **IOS_Snmp** Concept Item from the drop-down list.
6. Type the list of CLI Command lines:
   ```
   snmp-server community
   $context.snmp.readonlycommunity[*] RO
   snmp-server community
   $context.snmp.writecommunity[*] RW
   snmp-server location $context.snmp.location
   snmp-server contact $context.snmp.contact
   ```
7. Save.



Next: Step 5. Create a CLI Command Group for SNMP

Model an SNMP feature
Step 5. Create a CLI Command Group for SNMP

Next, create the **CLI Command Group** for SNMP. You can associate more than one **CLI Command List** to a **CLI Command Group** but in our example, we only associate our one SNMP CLI Command List.

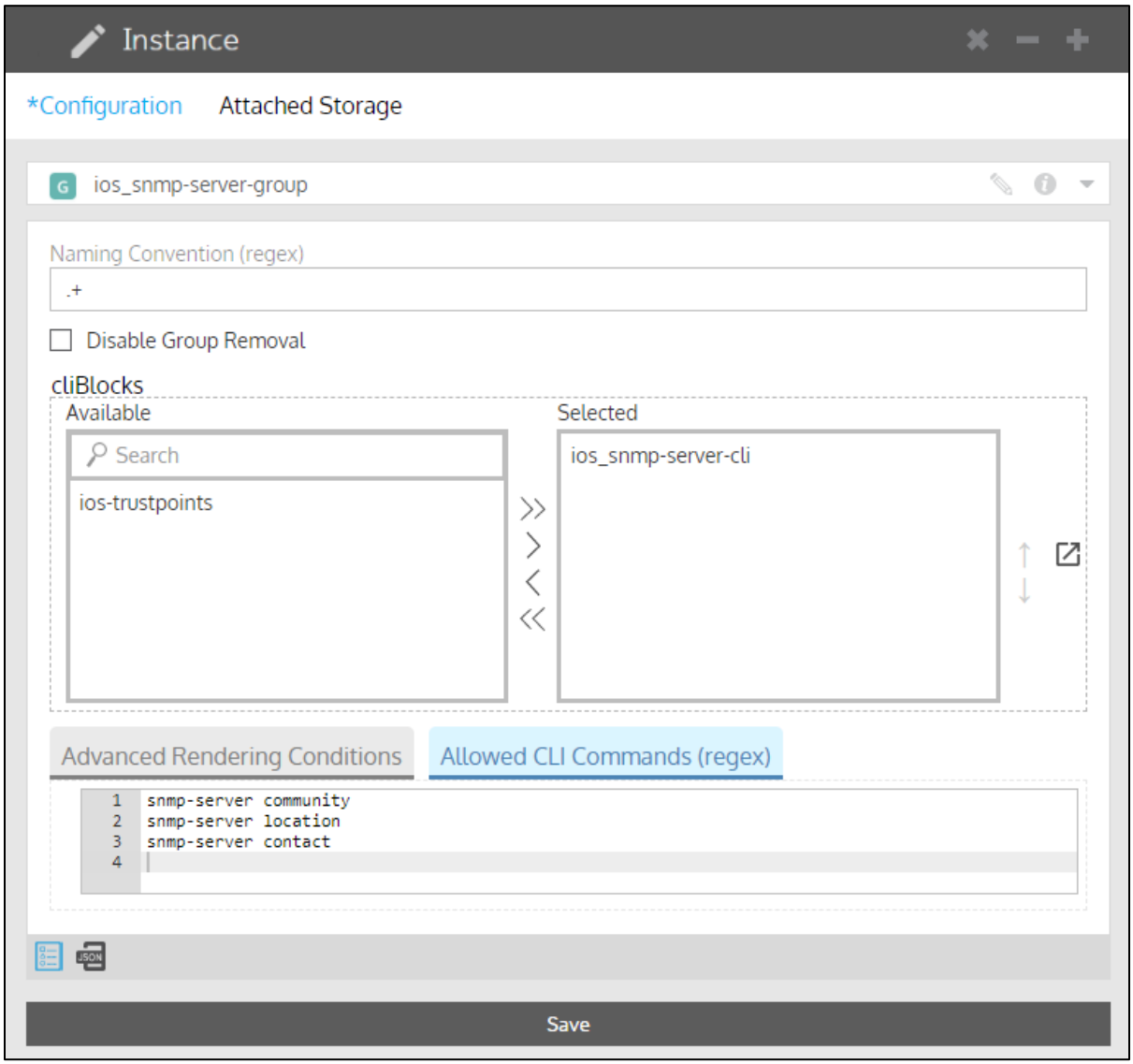
The list of allowed CLI Commands are the only commands that will be impacted if they are found in the configuration:

```
snmp-server community
snmp-server location
snmp-server contact
```

All other lines in the configuration will be left as they are found. If no commands are listed, Gluware will compare the model and the full list of commands returned from the Concept Item.

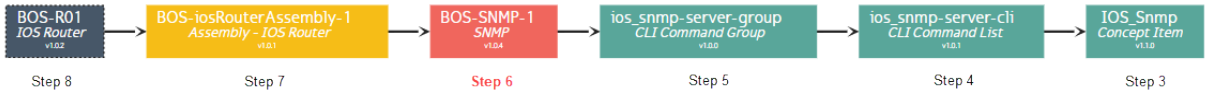
1. Go to **Config Modeling** > **Globals**.
2. Select **CLI Command Group** from the drop-down list.
3. Click ➕.
4. Click ✎ in the Instance panel and name the group **ios_snmp-server-group**.
5. Clear the **Disable Group Removal** box.
6. In the CLI Command **Available** list, select the **ios_snmp-server-cli** and click →.
7. Click **Allowed CLI Commands (regex)** and type these commands in the box:
   ```
   snmp-server community
   snmp-server location
   snmp-server contact
   ```

8. Save.

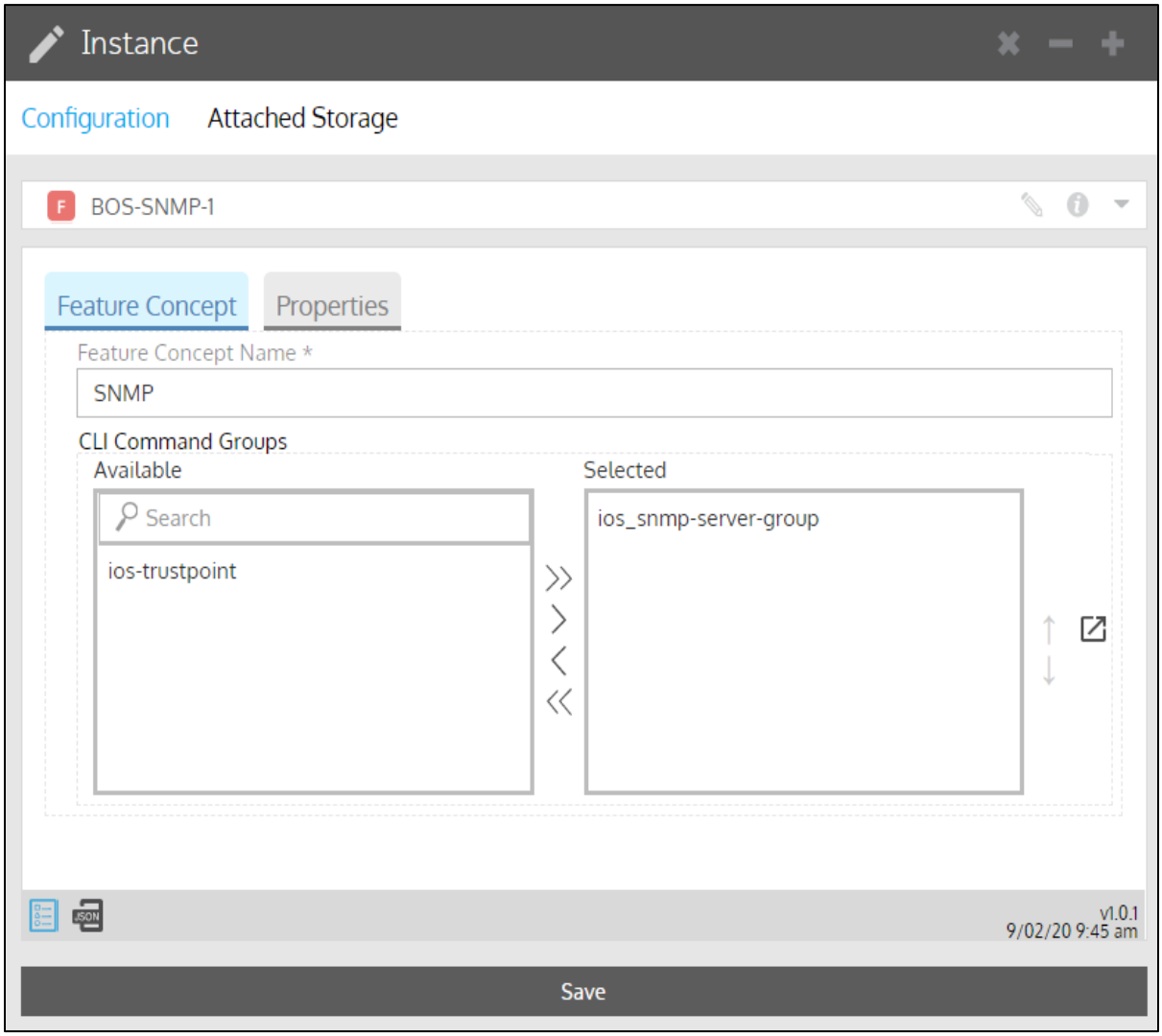


Next: Step 6. Create a Feature for SNMP

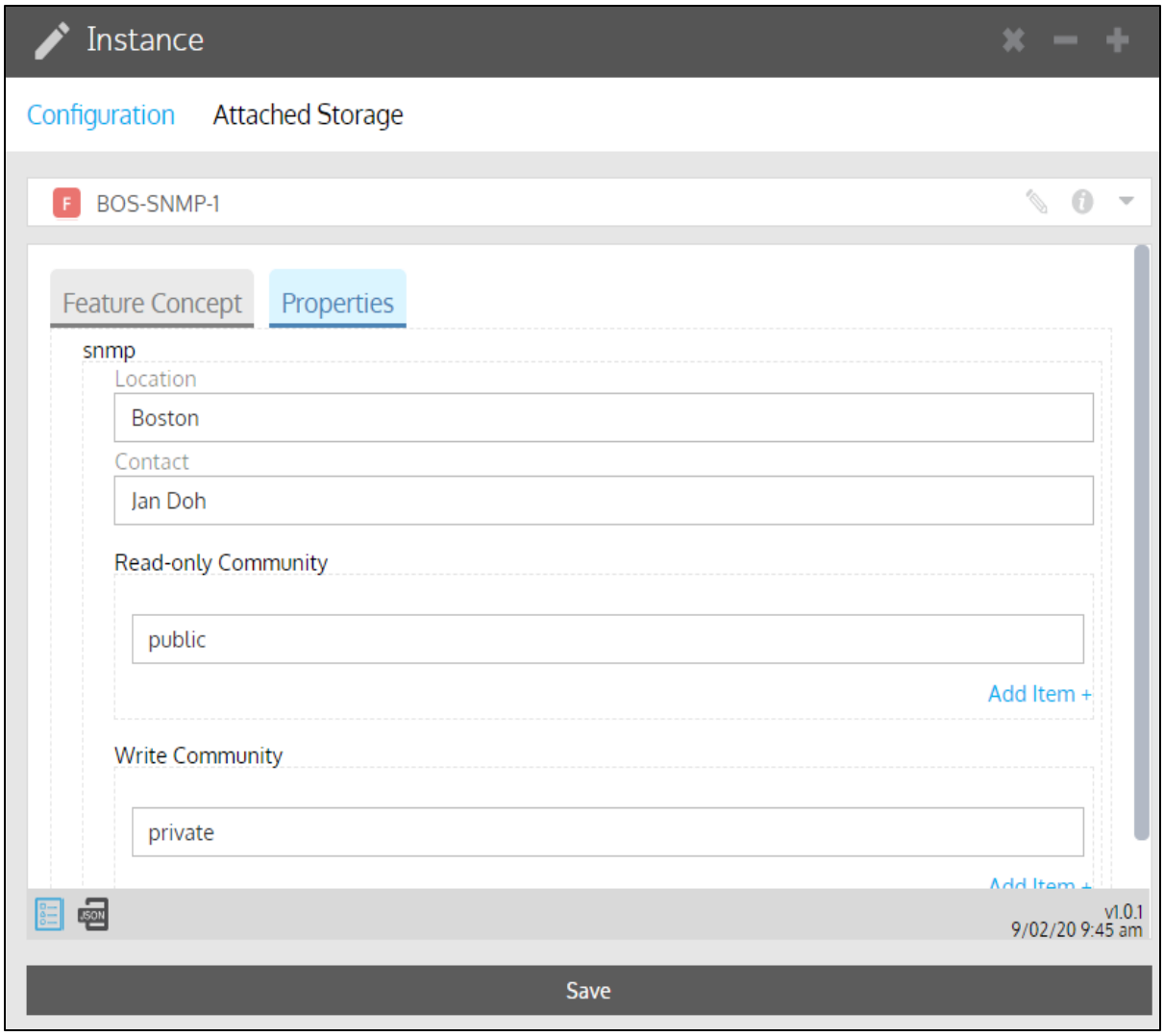
Model an SNMP feature
Step 6. Create a Feature for SNMP



1. Go to **Config Modeling** > **Features**.
2. Select **SNMP** from the drop-down list.
3. Click +.
4. Click ✎ in the Instance panel and name the Feature **BOS-SNMP-1**.
5. Select the **ios_snmp-server-group** CLI Command Group and click >.

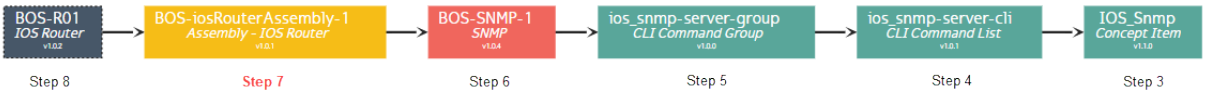


6. Then select **Properties** and fill out the form to specify the values for the variables you want to provision.



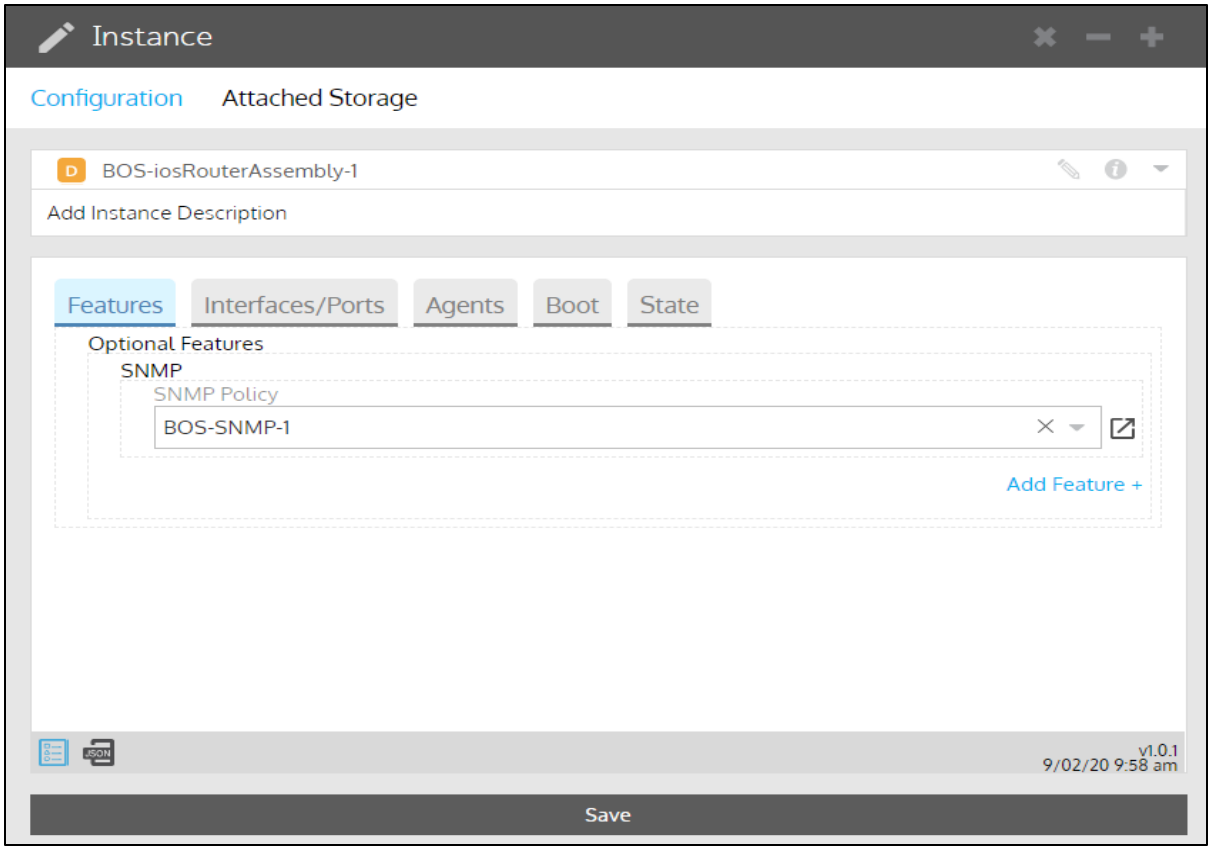
Next: Step 7. Create an Assembly for your IOS routers

Model an SNMP feature
Step 7. Create an Assembly for your IOS routers



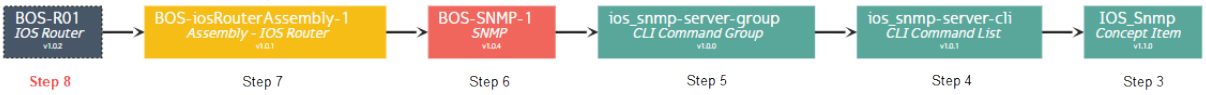
Create the **Assembly** for your IOS routers. The Assembly gathers all the feature policies that you want to standardize on a device. For example, you may have a Banner feature, an NTP feature, and an Interface feature, in addition to the SNMP feature, referenced in your Assembly for your IOS routers. All the features will be provisioned on the nodes that are linked to the Assembly.

1. Go to **Config Modeling** > **Domains**.
2. Select **Assembly - IOS Router (Cisco Systems)** from the drop-down list.
3. Click ➕.
4. Click ✎ in the Instance panel and name the Assembly **BOS-iosRouterAssembly-1**.
5. Click **Add Feature +** and select the **BOS-SNMP-1** feature policy from the list.
6. Save.



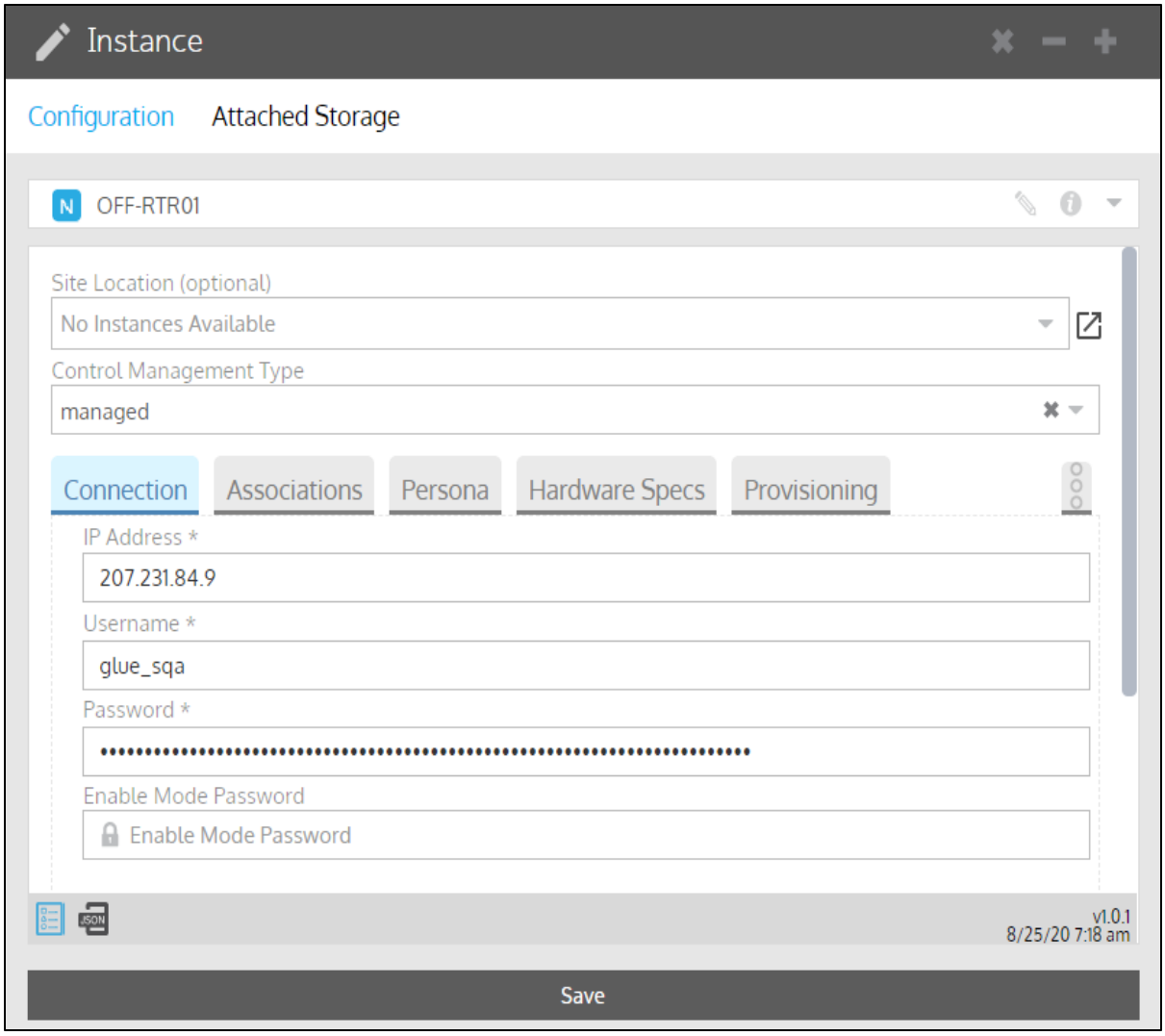
Next: Step 8. Associate the Assembly with nodes

Model an SNMP feature
Step 8. Associate the Assembly with nodes



Now you are ready to associate the IOS router Assembly you created with the nodes that represent your IOS routers. Associate the Assembly with all the router nodes you want provisioned with the SNMP feature policy you created.

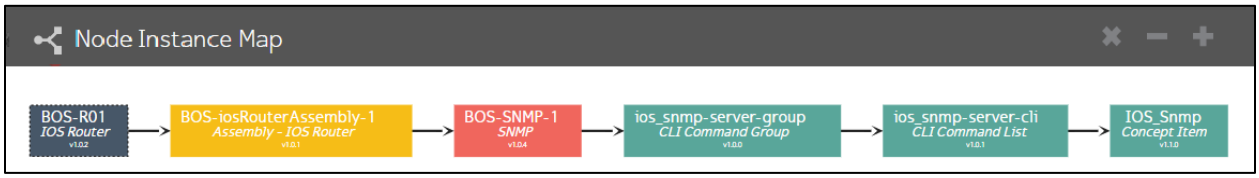
1. Go to **Config Modeling** > **Nodes**.
2. Select **IOS Router (Cisco Systems)** from the drop-down list.
3. Double-click a router node (**BOS-R01** node shown here) in the grid list to open the instance.
4. Select **Associations** and then select the **BOS-iosRouterAssembly-1** Assembly Policy from the drop-down list.
5. Save.



Next: Step 9. View the relationships in your SNMP model

Model an SNMP feature
Step 9. View the relationships in your SNMP model

To check that you have all the required components in your model, with your node selected, point to the bottom of the screen in Config Modeling and click . You'll see a map of the components in your model. It should look something like this:

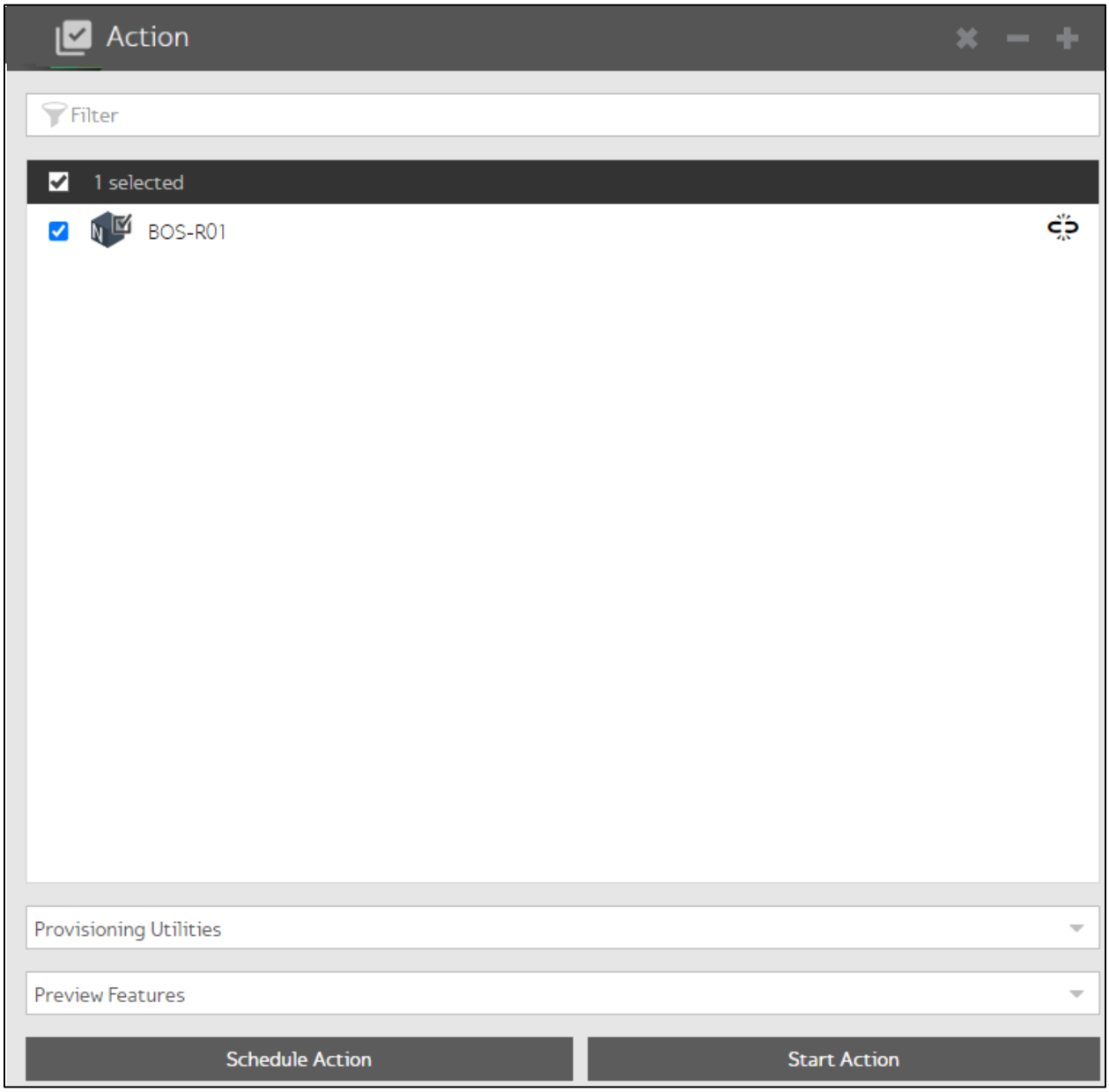


When you have all the components in place, you can preview how the model impacts the node.

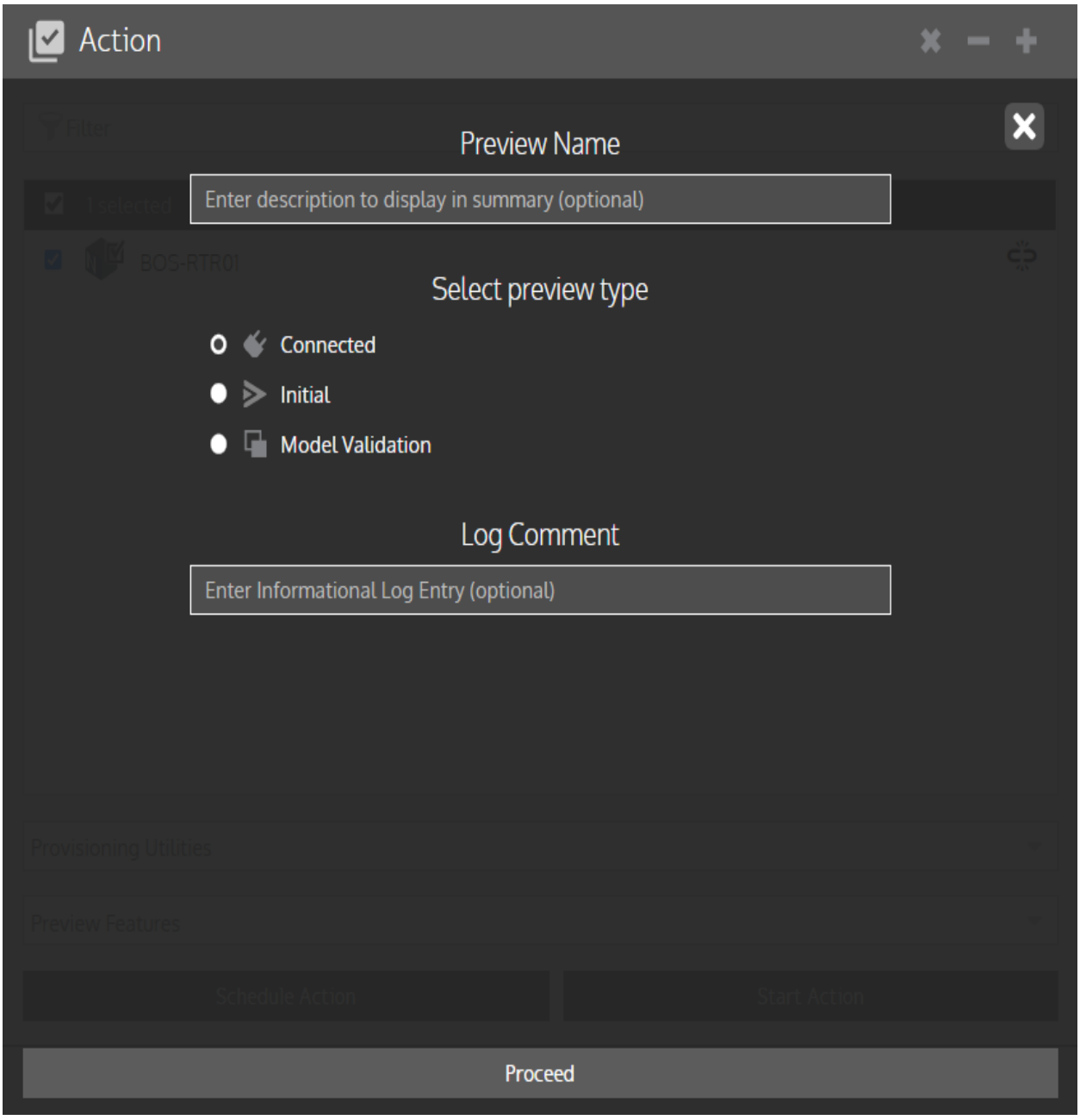
Next: Step 10. Preview the SNMP Feature

Model an SNMP feature
Step 10. Preview the SNMP Feature

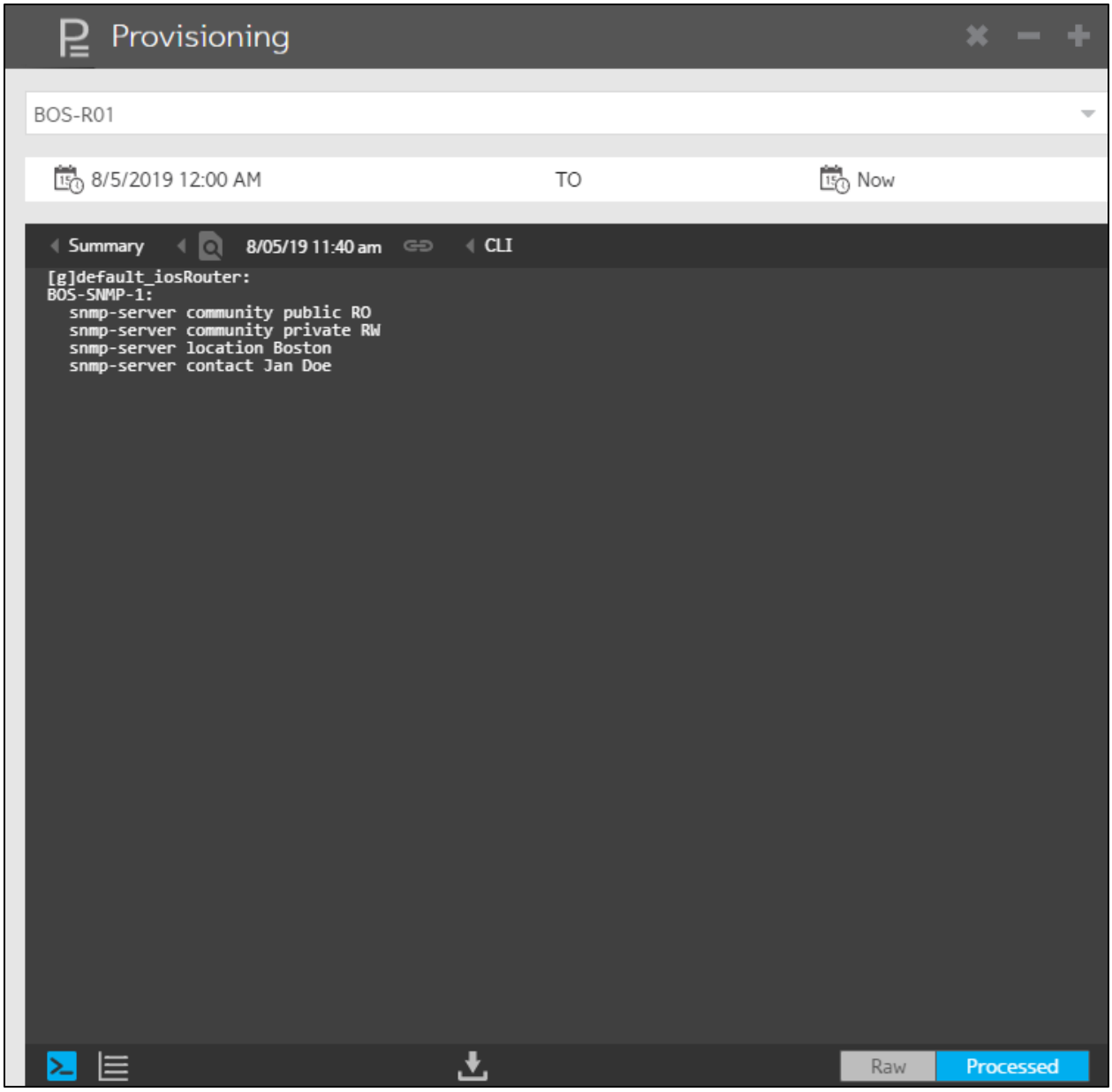
1. With the **BOS-R01** node Instance panel open, click and check the node's box.
2. Select **Provisioning Utilities** and **Preview Features** and click **Start Action**.



3. Select **Connected** and click **Proceed**.



4. Click , double-click on the log listed, click , and then click **Processed**. This shows you what would be placed on the configuration as a result of the model.



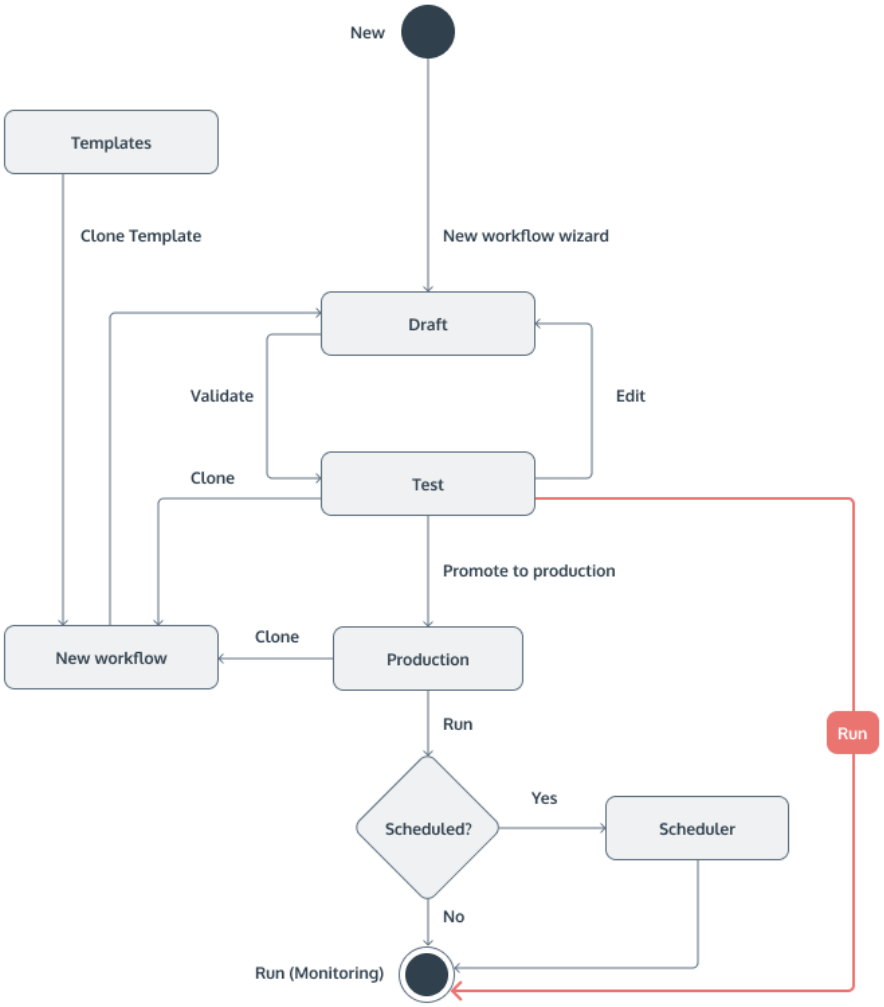
See "Review the logs" for additional views of the log.

When your model is complete and no errors surface when you preview, you can provision the new configuration.

Network RPA overview

Gluware **Network RPA** (robotic process automation) allows you to create workflows that automate simple and complex tasks. No coding is required—simply drag and drop tasks, conditional statements, and establish notifications. Set up test devices to try out the process. And when you're ready to run the workflow in production, easy-to-find logs help you confirm the process was completed successfully or troubleshoot any problems.

Network RPA development states



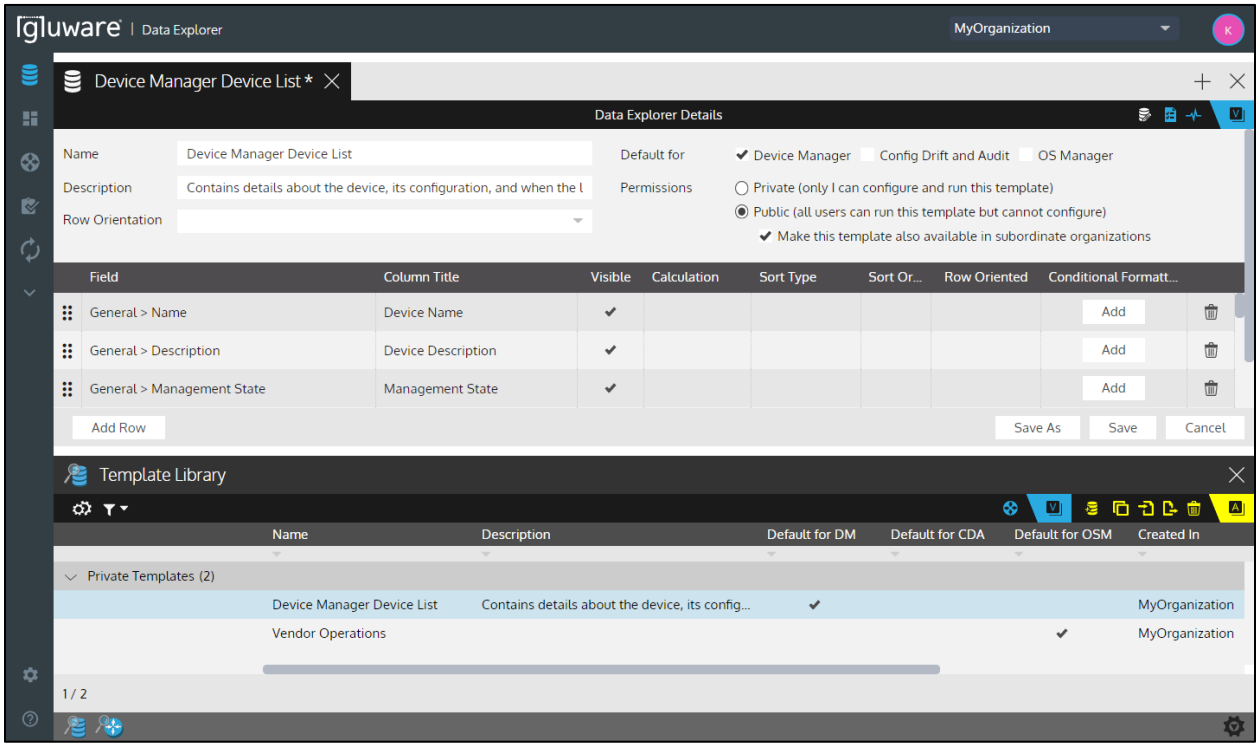
Network RPA views

Workflow Library – Provides workflow management and general information with the ability to import, export, track development levels, and execute workflows. Workflows can be executed on demand, scheduled, or triggered by events.

Workflow Editor – An automation flow designer providing a drag-and-drop user interface. Build end-to-end processes composed of triggers, actions, and events using pre-built tasks along with multi-path decision logic. Add tasks, conditional statements, annotations, and comments. Zoom in or out and re-center as you work. Workflows can be printed and exported in a standard BPMN format.

Workflow Activity – Provides the ability to monitor the workflow execution. View detail and take action at the task or device/endpoint level. Manage workflow states (Pending, Running, Blocked) and view the history and logs.

Data Explorer quick reference



Actions

Add Template – Create a new Data Explorer report template

Clone Template – Clone a Data Explorer report template

Import Template – Import a Data Explorer report template created in another organization

Export Template – Export a Data Explorer report template

Run Report – Run a Data Explorer report on demand or on a schedule

Ad Hoc Query – Search for a specific string in a device's configuration

Views

Data Explorer Details – Display the template details

Data Explorer Results – Display the Data Explorer report results

Activities – View all previous actions related to the template

Create a report template

Gluware **Data Explorer** allows you to create custom, reusable report templates, selecting from data stored by Gluware with flexible layouts. The report templates can be used within other Gluware solutions. Reports can be viewed, downloaded, emailed, and scheduled to run automatically.

With **Data Explorer**, you can:

- Select the fields you want
- Sort by one or more columns
- Group results within a column
- View sum and average values for numeric data
- Specify conditional highlighting of specified values in a column
- Create default reports for exporting from **Device Manager**, **Config Drift and Audit**, and **OS Manager**
- Run reports on demand or on a schedule
- Download reports in CSV, PDF, or JSON format. Rich PDF formatting is available when you run reports on demand from the Data Explorer viewer

Gluware provides a variety of useful report templates in thGluware Knowledge Base (https://support.gluware.com/hc/start) that you can import to **Data Explorer**.

To create a new report template

1. Go to **Data Explorer** > **Template Library**.
2. Click .
3. Name the template and click **Create**.
4. Describe the template.
5. Optional: Check one or more boxes to make the report template your default when you export in **Device Manager**, **Config Drift & Audit**, or **OS Manager**. Any default you set is a personal preference and does not impact other users.
6. Do one of the following:

- Select **Private** if you want to prevent anyone else from using the template.
- Select **Public** to allow other users to use the template. Check the box to share the template with users in child organizations.

7. Click **Add Row**.
8. Select a field from the drop-down list. You can search by field name by typing one or two characters.
9. Do any of the following:
    - Double-click the **Column Title** to rename it.
    - Double-click **Visible** to hide or show the column in the report. You might want to hide the column if you are using it to influence sorting, for example.
    - Double-click **Calculation** to **average** or **sum** number values. An average calculation assumes 0 for null values. If you don't want null values included in the average calculation, you must filter out those devices from your data set.
    - Double-click **Sort Type** and select how to sort the column.
    - Click **Conditional Formatting** to highlight in color specified values in the column.
        1. Click **+ Add rule**.
        2. Select the filter type from the dropdown list, enter a value, and select the highlight color.
        3. Optional: Check the **Stop if true** box if you want no further evaluation if it matches the rule.
        4. Click **OK** to add the conditional formatting to the column.
10. Optional: Click and drag a row to a new position to re-order columns.
11. Optional: If more than one column is to be sorted, click **Sort Order** to prioritize the sorting of the columns. Click and drag a column to the order you want. Then **OK**.
12. Optional: To report on ports, chassis, components, licenses, and stacks, select the type from the **Row orientation** drop-down list. If you don't select **Row orientation** and there is more than one column with the same title, <key#> will be replaced with "1," "2," "3," etc., in the report. *See examples below*.

NOTE: Selecting **Row Orientation** drops the <key#> in default column titles. Customized column titles are unchanged.

13. Save the report template.

Notes: You can also create a report template by:

- Cloning an existing template. Simply select a template and click
- Opening an existing template and clicking **Save As**.
- Importing a template that was created in a different organization.

Example: Report with Row orientation

Name	Component	Component SKU	Component Serial Number
Juniper EX4300-24T PF3715490034	Gbics 0	NON-JNPR	XCW1548S0BD7
Juniper EX4300-24T PF3715490034	Gbics 1	NON-JNPR	XCW1547S02D7
Juniper EX4300-24T PF3715490034	Gbics 2	NON-JNPR	XCW1547S0529
Juniper EX4300-24T PF3715490034	Gbics 3	NON-JNPR	XCW1606S007D
Juniper EX4300-24T PF3715490034	Gbics 4	NON-JNPR	XCW1548S0C51
Juniper EX4300-24T PF3715490034	Gbics 5	NON-JNPR	XCW1605S02BA

Example: Report without Row orientation

Name	Component GBI Cs 0 SKU	Component GBI Cs 0 Serial Number	Component GBI Cs 1 SKU	Component GBI Cs 1 Serial Number	Component GBI Cs 2 SKU	Component GBI Cs 2 Serial Number
Juniper EX4300-24T PF3715490034	NON-JNPR	XCW1548S0BD7	NON-JNPR	XCW1547S02D7	NON-JNPR	XCW1547S0529

Run a Data Explorer report

From Data Explorer

When you run a report from **Data Explorer**, you can view the results, modify the report, and re-run it. You also see any column highlighting you specified and can group the results by any column.

1. Go to **Data Explorer** > **Devices**.
2. Select the devices you want to report on and click .
3. Optional: Rename the file.
4. Optional: Click **Apply current filter** when scheduling a run so that changes in the filtered device list are represented.
5. Select the report template from the drop-down list.
6. Run or schedule the report:
    - Click **Run** to run the report immediately.
    - Click **Schedule** to define the schedule. Check a **Notify on Completion** box to send an email when the report is complete. Select from those listed or add email addresses to **Other recipients**. Separate email addresses with a comma. Select a format for the report and click **Confirm**.
7. Do any of the following:
    - Click **Edit Data Selection** and then run the report again.
    - Click **Email** and enter email recipients separated by commas and then click **Send**.
    - Click **Download** to send the report to your Downloads folder.

NOTE: You can select CSV, PDF, or JSON format for your report. Rich PDF formatting is available when you run reports on demand from the Data Explorer viewer.

From Device Manager, Config Drift & Audit, or OS Manager

If you have specified a Data Explorer report as the default for the solution

- Click . The Data Explorer report is run and sent to your Downloads folder.

To run any Data Explorer report

1. Optional: Select one or more devices in the Device Explorer.
2. Click .
3. Optional: Rename the output file.
4. Select the device to run the report on:
    - **Selected** – Run the report on the devices you selected in the Device Explorer.
    - **Apply current filter** – Run the report on the resulting devices of the filter currently in effect in the Device Explorer. This will include any new devices that satisfy the filter and is a good option when running a report on a schedule.
    - **All** – Run the report on all the devices.
5. Run or schedule the report:
    - Click **Run** to run the report immediately. The report is sent to your Downloads folder.
    - Click **Schedule** to define the schedule. Check a **Notify on Completion** box to send an email when the report is complete. Select from those listed or add email addresses to **Other recipients**. Separate email addresses with a comma. Then click **Confirm**.

View the Data Explorer report results

1. Go to **Data Explorer** > **Template Library**.
2. Double-click a report template.
3. Click .

View Data Explorer report history

1. Go to **Data Explorer** > **Template Library**.
2. Double-click a report template.
3. Click .

Export and import a report template

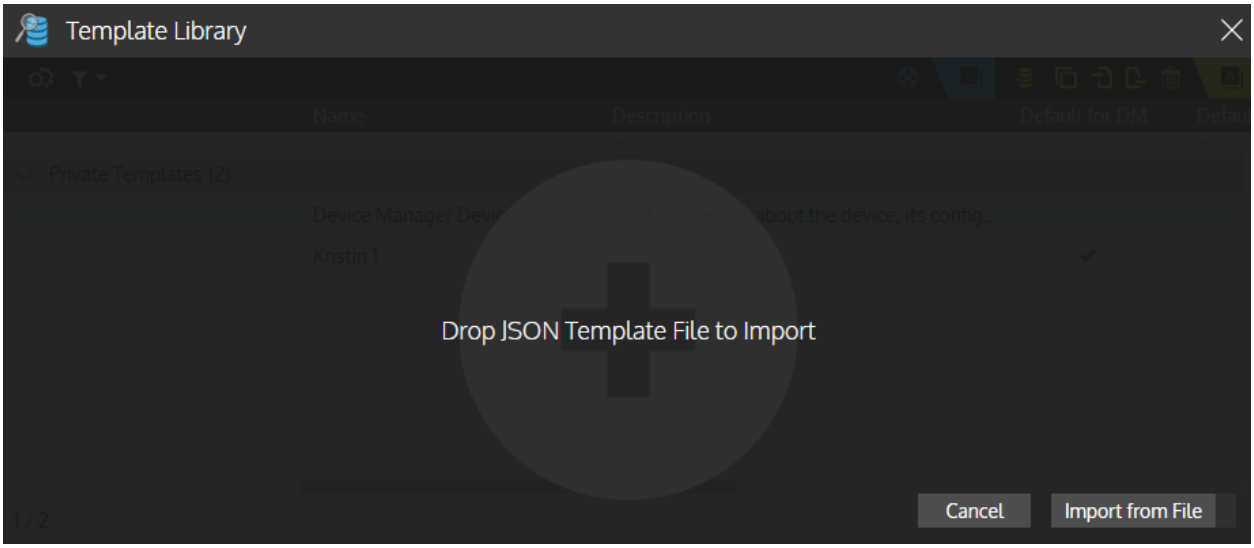
You can share a report template with other organizations, users, and Gluware systems by exporting the template and importing it in a new organization.

Export a report template

1. Go to **Data Explorer** > **Template Library**.
2. Select a report and click . This exports the report as a JSON file to your Downloads folder.

Import a report template

1. Ensure you're in the organization you want to import the template to.
2. Go to **Data Explorer** > **Template Library**.
3. Click .
4. Do one of the following:
    - Drag and drop the JSON template file into the **Template Library** and click **OK**.
    - Click **Import from File**, select the template file or the files you want to import, and then click **Open**.

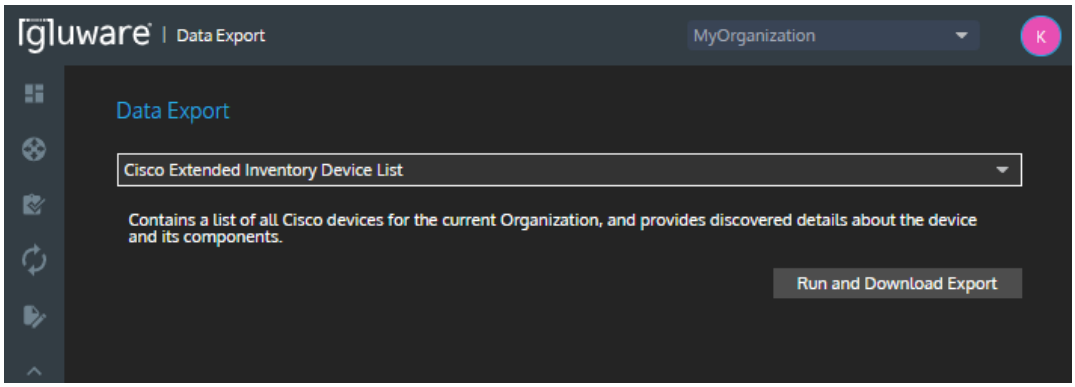


Export lists of devices using Data Export

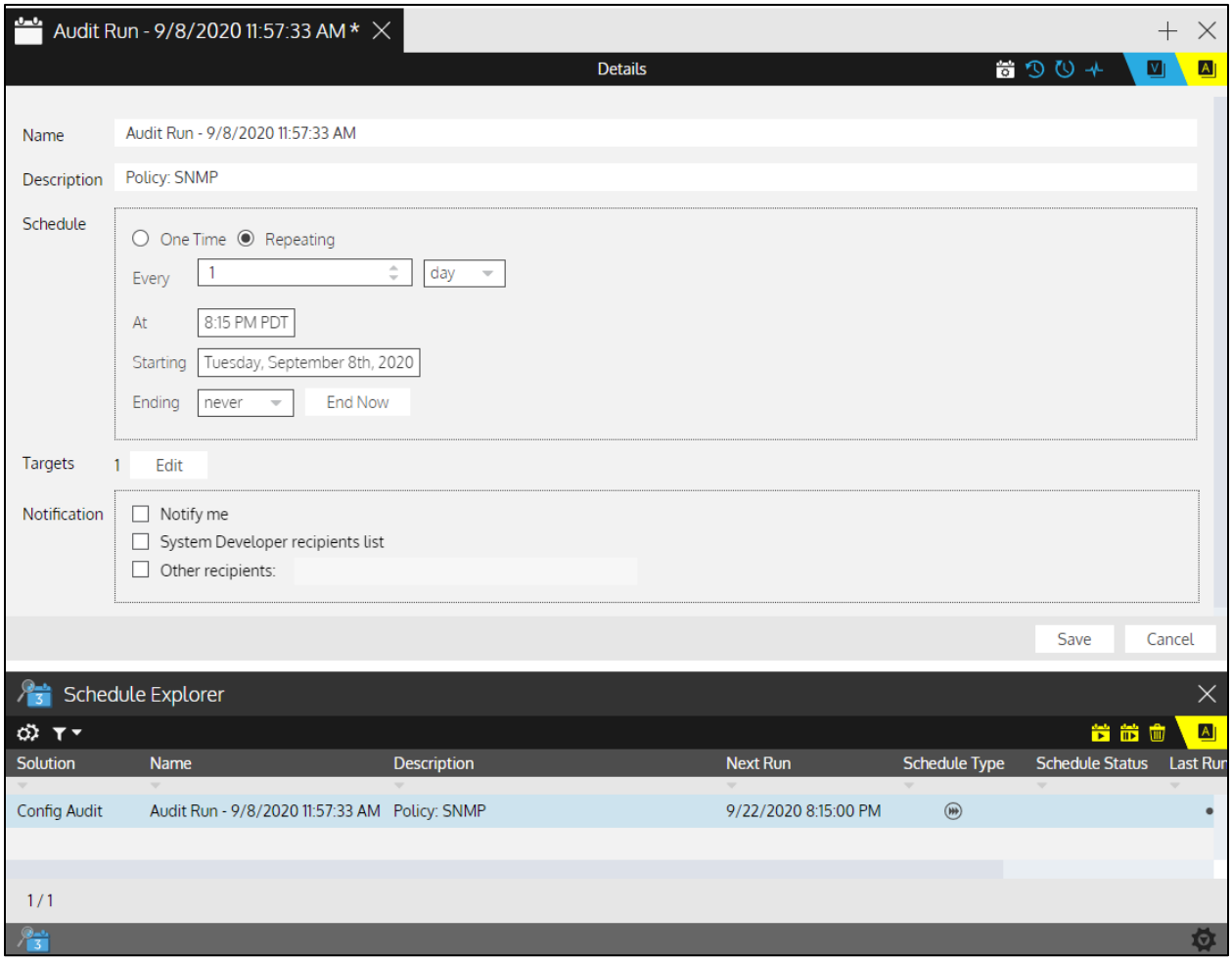
Data Export allows you to export the following types of device lists:

- **Cisco Extended Inventory Device List** – Lists all the Cisco devices in the current organization and provides discovered details about the devices and their components.
- **Config Drift and Audit Device List** – Lists the Config Drift status and last capture dates for all devices.
- **Device Manager Device List** – Lists all the devices that have been added to Device Manager and the hardware and software attributes.
- **IP Numbering List** – Lists all assigned addresses from IPv4 Address Pool instances and all static IP addresses assigned by IP Numbering instances for the organization. The export extracts that information on a node-by-node basis.
- **IP Reservations List** – Lists the IPv4 Address Pools for the current organization, identifies all allocated and currently used IP Address Reservations from each pool, and extracts the details to the export.
- **Most Recent IMD Workflow Logs** – Contains the most recent execution logs from the Intelligent Model Discovery workflow.
- **Node List** – Lists all configured nodes in the current organization that the requester has permissions to manage.

1. Go to Gluware **Data Export** and select the type of list you want to export from the drop-down list.
2. Click **Run and Download Export**. This exports the list as a CSV file to your Downloads folder.



Schedules quick reference



Actions

Run Now – Execute the selected scheduled action immediately

Pause/Resume – Toggle between pausing or resuming the selected scheduled action (only for single schedule selection)

Delete Schedules – Delete the selected schedule

Views

Details – View the configuration details of the selected schedule

Schedule History – View previously executed actions for the schedule

Future Occurrences – View an activity timeline for the next 10 scheduled runs

Activities – View all previous actions involving the schedule

Schedule types

Repeating schedule

One-time schedule

Schedule statuses

Active

Paused

Completed

Last run statuses

Successful

Skipped

Manage schedules

Once you schedule an action, you can manage the schedule in **Schedules**. The actions that support scheduling include:

- Taking a Config Drift snapshot
- Running a Config Audit policy
- Rebooting a device
- Provisioning a device
- Previewing a device provisioning
- Executing a custom script
- Renewing device certificates
- Executing custom scripts
- Performing an OS upgrade
- Assessing the state of a device
- Updating the gluWatchdog agent

View the logs of a scheduled action

1. Go to **Schedules** and double-click a scheduled action.
2. Click to see when the scheduled was run.
3. Click for the action you want to view the log for.
4. Click **Back**.

View a schedule's history

1. Go to **Schedules** and double-click a scheduled action.
2. Click to see when the scheduled was run.
3. Click to see all previous actions involving the schedule.

View future scheduled runs

1. Go to **Schedules** and double-click a scheduled action.
2. Click to see the next 10 scheduled runs.

Run a scheduled action now

1. Go to **Schedules** and select a scheduled action.
2. Click .
3. Click **Confirm**.

Pause a scheduled action

1. Go to **Schedules** and select a scheduled action.
2. Click .
3. Click **Confirm**. The **Schedule Status** changes to .

Resume a schedule

1. Go to **Schedules** and select a paused action. appears in the **Schedule Status** column of the schedule.
2. Click .
3. Click **Confirm**.

Modify a schedule

Data Retention and Cisco API Console schedules can only be modified through system settings. All other schedules can only be modified in **Schedules**. Only schedules that have not ended can be modified.

1. Go to **Schedules** and double-click a scheduled action.
2. Modify the schedule as needed.
3. Check a **Notification** box to send an email when the scheduled action is complete. Select from those listed or add email addresses to **Other recipients**. Separate email addresses with a comma.
4. Click **Save**.

Add or remove target devices

In **Schedules**, you can change the devices that most scheduled actions will act upon.

> **NOTE:** You can't change the target devices for an **OS Manager** plan action (Transfer Image Only or Deploy New Image) in **Schedules**. You'll need to edit the OS plan to change target devices.

1. Go to **Schedules** and double-click a scheduled action.
2. Click if **Details** are not displayed.
3. Click **Edit** next to **Targets** to change the target devices.
4. Do any of the following:
   - Select an **Available Device** and click Add
   - Select a **Selected Device** and click Remove
   - Click Remove All
   - Click **Convert to dynamic target list** and **Confirm** to filter the list of targets. Select a property, relational operator, and value from the drop-down lists.
     - Click **Add rule** and click **AND** or **OR** to add a logical operator.
     - Click **Add group** to add nested rules.
5. Click **Back**.

Delete a schedule

> **NOTE:** Some system schedules cannot be deleted. To disable a **Data Retention** schedule, go to **Settings** > **Data Retention**. To disable **Cisco API Console** updates, go to **Settings** > **Integrations**.

1. Go to **Schedules** and select a scheduled action.
2. Click to delete the schedule.
3. Click **Confirm**.

System settings overview

Gluware systems may include some number of logically separated organizations—typically companies, regions, or service providers. Each organization has users with roles and permissions assigned to them.

Settings is where you create, update, and delete organizations and users, and manage licenses and File Servers.

Watch a video introduction to system settings
https://youtu.be/n-wvgT5H18A

Organization and site management

Add or update organizations

Configure Gluware to interact with LDAP

Configure Gluware to interact with RADIUS

Configuring single sign-on authentication

Gluware roles and permissions

Install a Gluware license

Delete a Gluware license

View license expiration dates and device counts

Add Gluware users

Customize roles and permissions

Set default emails for notifications

Restrict the devices a role can manage

Enable/disable a system banner

Customize dashboards

Manage zones for Gluware Zone Engines

Configure SMTP and proxy settings

Manage data retention

Set up custom fields

Monitor configuration changes

Set up automatic configuration snapshots

Integration

Set up Cisco API Console integration

Set up NIST NVD API integration

Enable GluAPI integration

OS management

Enable/disable a File Server

Troubleshoot a File Server

Modify a File Server

Delete a File Server

Enable the OS Catalog

Set up the execution guidelines for OS plans

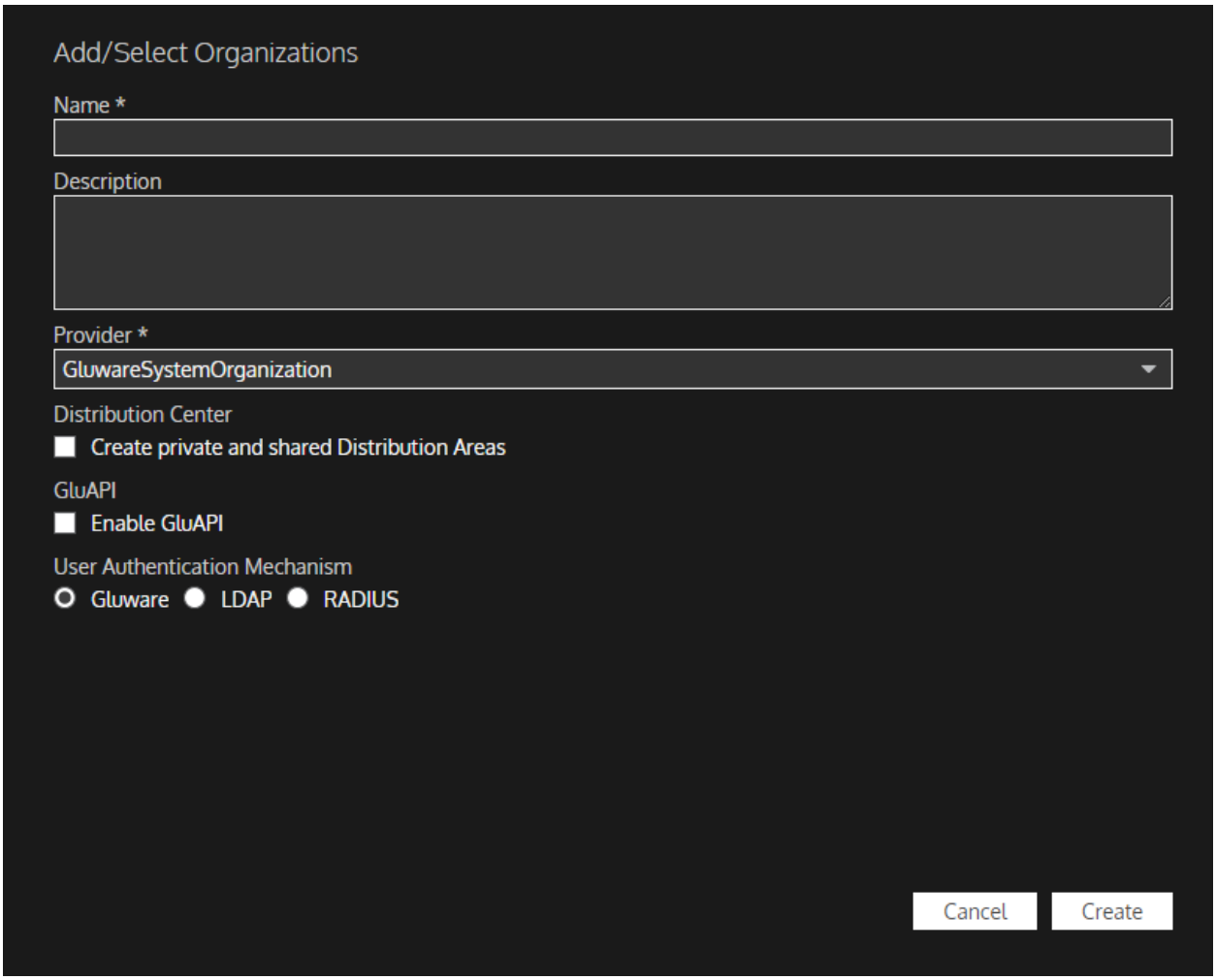
Profile management

Add your photo to Gluware

Add or update organizations

Gluware system settings allows you to add organizational structure to your Gluware system with parent/child relationships. A best practice is to create users in your parent organization and add devices to a child organization.

1. Go to **Settings** > **Organization** > **Organizations**.
2. Select an organization to update from the drop-down list or click **Add Organization** to create a new organization.
3. Enter a name for the organization and a description.
4. Select the parent organization from the **Provider** drop-down list.
5. Optional: Check the **Enable GluAPI** box. *See* "Enable GluAPI integration" for more information on GluAPI.
6. Select a user authentication mechanism:
    - Select **Gluware** to set up users one-by-one in Gluware 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.
7. Click **Create**.
8. 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.
9. Click **OK**.



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

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.

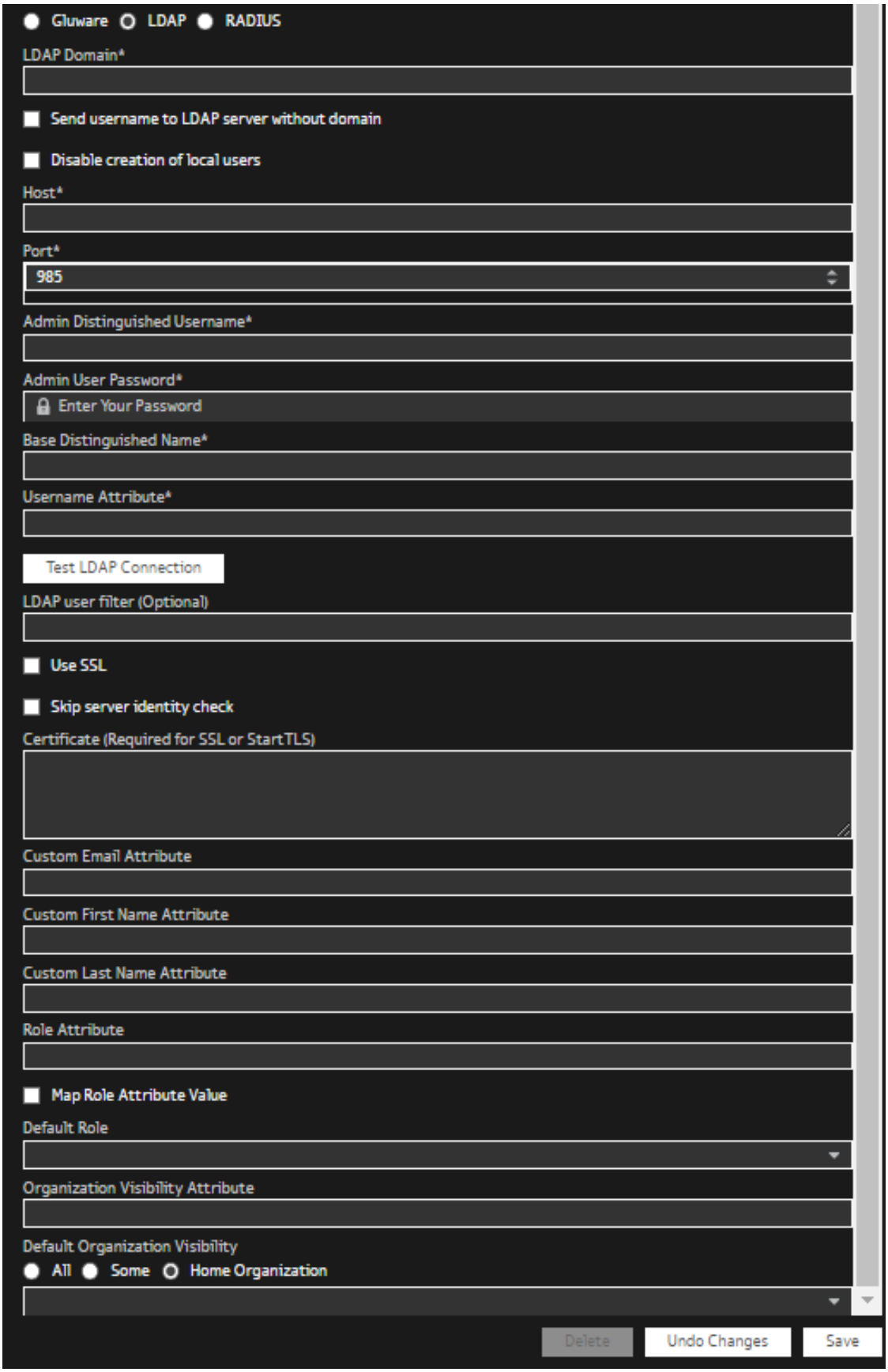
The user authentication process in Gluware determines if, and how, to map an LDAP user with a Gluware user for the following scenarios:

- 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. For example, 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 (*). For example, enter *. The user signs in with jandy.
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

Field	Description
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
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)(member Of=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)

Field	Description
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
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
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

Field	Description
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
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

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.

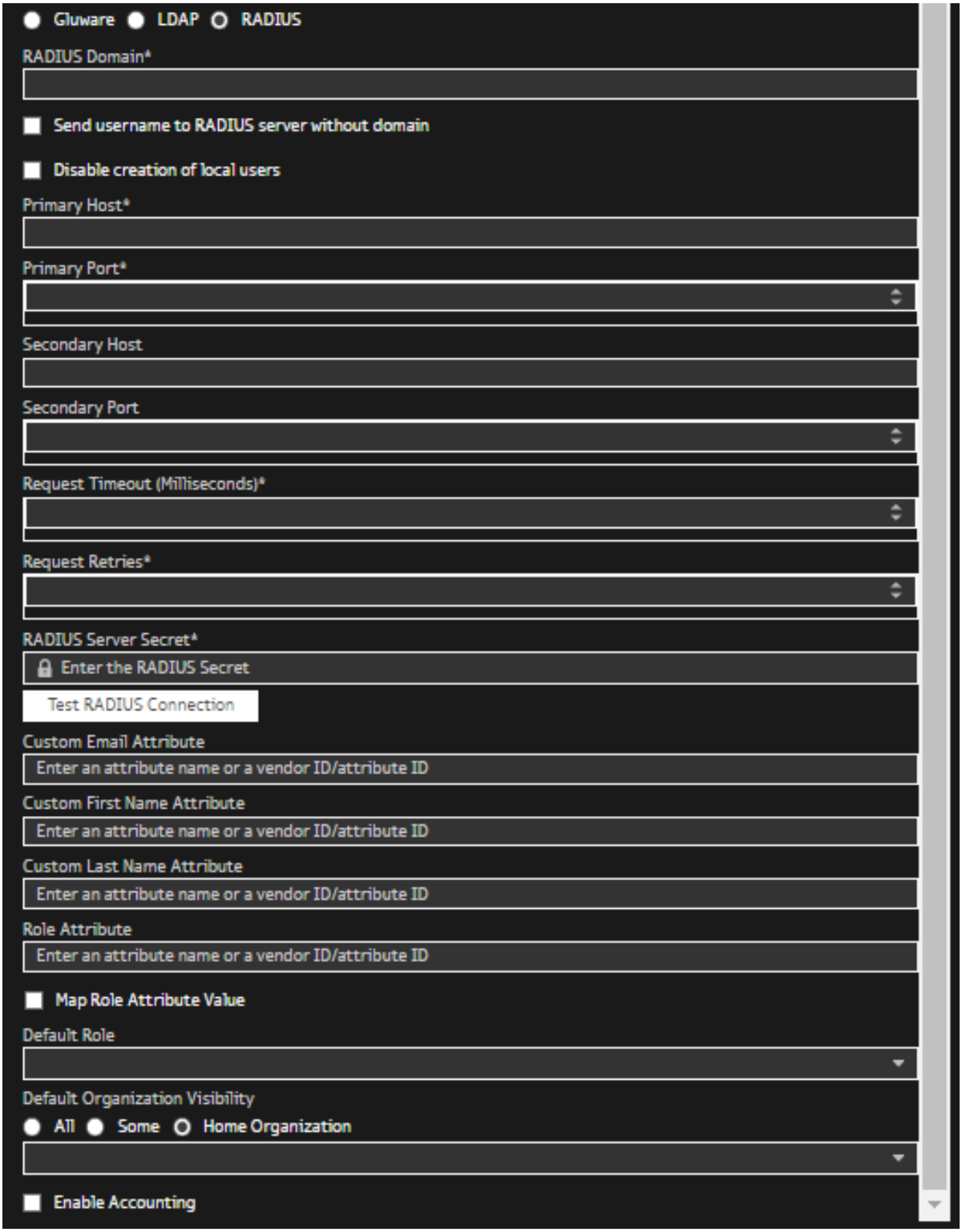
The user authentication process in Gluware determines if, and how, to map a RADIUS user with a Gluware user for the following scenarios:

- 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 a RADIUS domain of gluware.com To require a domain name on sign in, enter the domain name. **Note:** Do not include the @ sign. For example, 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 (*). For example, enter *. The user signs in with jandy.
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

Field	Description
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 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

Field	Description
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 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

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**.

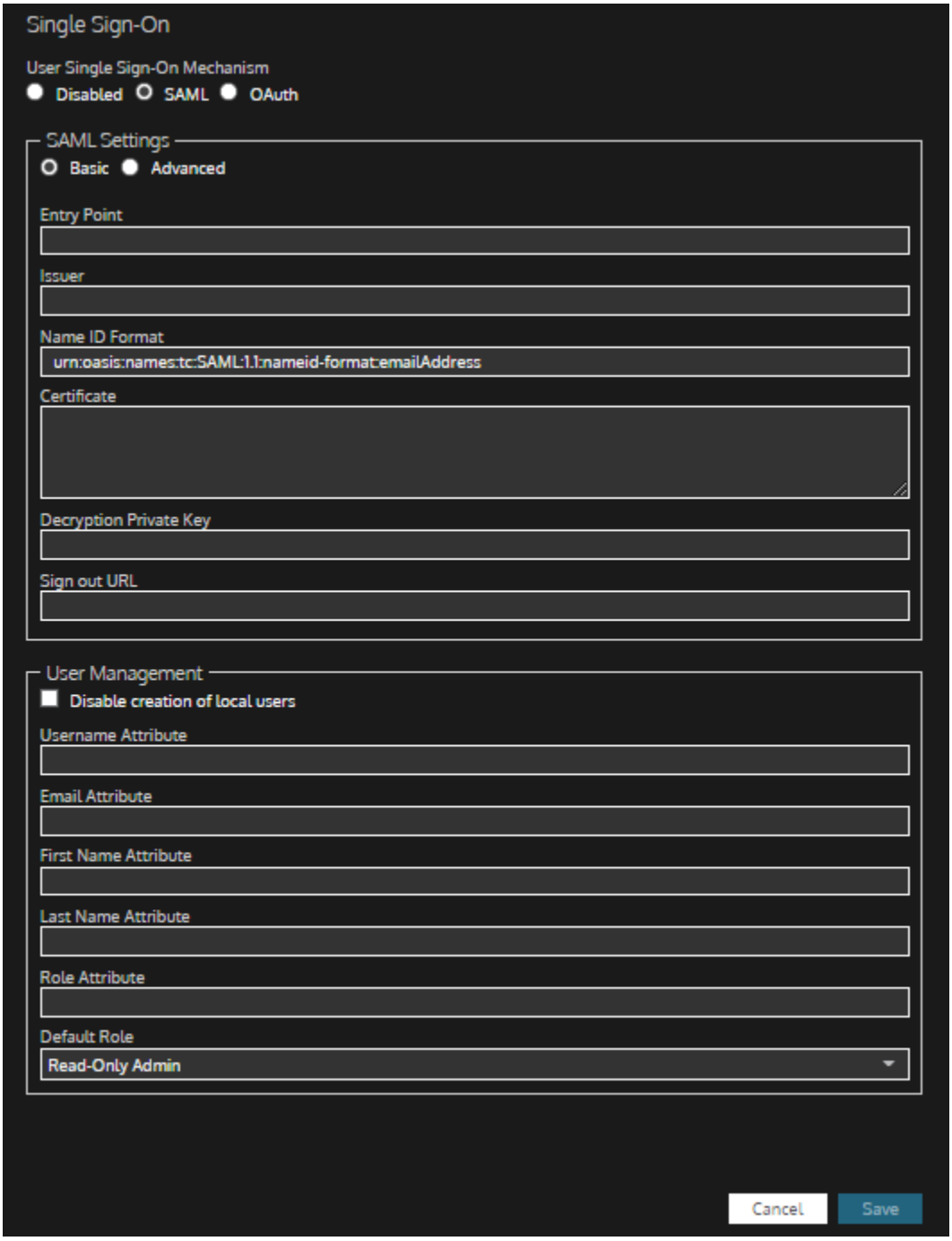
Organization Visibility is set to ALL for all users and can't be modified as part of the single sign-on configuration. To limit **Organization Visibility**, go to ⚙**Settings** > **Users** > **Manage Users**, select a user, and then select **Some** for **Organization Visibility**.

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.

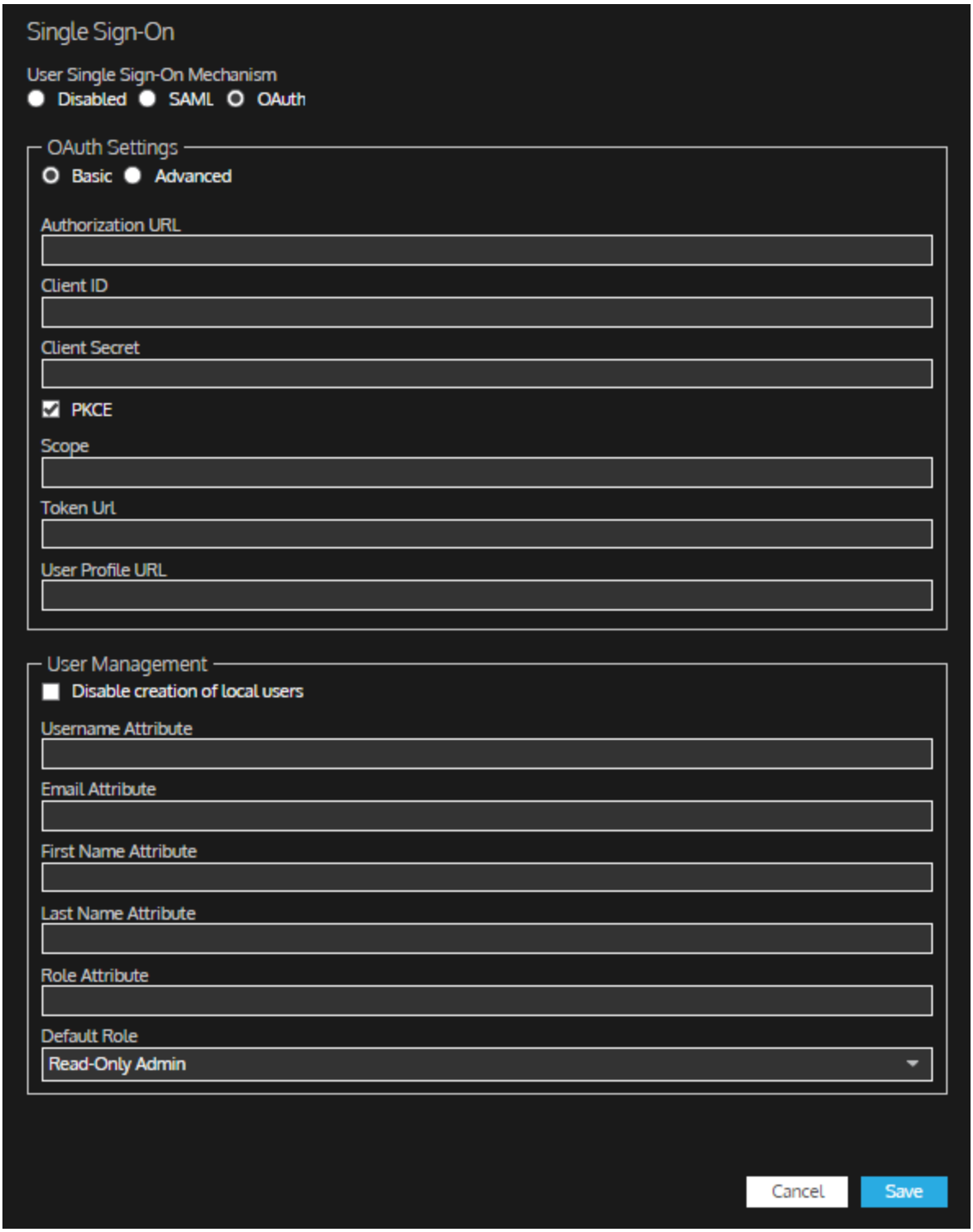
6. Enter the **issuer**, the URL of the identity provider.
7. Enter the **name ID format**, the format for the user identity that will be sent by the identity provider. The default is an email address ("urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress").
8. Paste the public X.509 **certificate** 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.

Gluware roles and permissions

Roles and permissions are assigned in **Settings** > **User** > **Manage Users**. You can use the standard Gluware roles, define custom roles, or use a combination of standard and custom roles.

At least one person in each organization must be a **Superuser**. Superusers can add and remove permissions from any other user in the organization.

> **NOTE:** If roles are defined by LDAP or RADIUS, roles cannot be modified in **Settings** > **User** > **Manage Users**.

Assign a Superuser

1. Ensure you're in the organization you want to assign the Superuser in.
2. Go to **Settings** and select **User** > **Manage Users**.
3. Add a user or search for an existing user.
4. Check the **Superuser Privileges** box.
5. Click **Create** or **Save**.

Gluware standard roles

DV = Dashboard Viewer

RA = Read-Only Admin

OA = Operations Admin

WA = Write Admin

SA = System Admin

SD = System Developer

Permissions assigned to standard roles

Dashboard	**DV**	**RA**	**OA**	**WA**	**SA**	**SD**
Access Dashboard Solution	✔	✔	✔	✔	✔	✔
Create Private Dashboards			✔	✔	✔	✔
Create Public Dashboards				✔	✔	✔
Moderate Public Dashboards					✔	✔
Config Modeling	**DV**	**RA**	**OA**	**WA**	**SA**	**SD**
Access Config Modeling Solution		✔	✔	✔	✔	✔
Create and Edit Globals, Domains, and Features				✔	✔	✔
Create and Delete Nodes			✔	✔	✔	✔
Delete Globals, Domains, Features, and Nodes				✔	✔	✔
Edit Nodes			✔	✔	✔	✔
View JSON Format						✔

Provisioning	**DV**	**RA**	**OA**	**WA**	**SA**	**SD**
Access Actions within Config Modeling			✔	✔	✔	✔
Allow Configuration Changes			✔	✔	✔	✔
View Logs and Download Bundles		✔	✔	✔	✔	✔
Workflows	**DV**	**RA**	**OA**	**WA**	**SA**	**SD**
Access Workflows Solution		✔	✔	✔	✔	✔
Run Level 1 Workflows – custom workflows for Read-Only Admins		✔	✔	✔	✔	✔
Run Level 2 Workflows – custom workflows for Operations Admins			✔	✔	✔	✔
Run Level 3 Workflows – custom workflows for Write Admins				✔	✔	✔
Run Level 4 Workflows – Design and Operate workflows created in the Workflows Solution, plus custom workflows for System Admins					✔	✔
Run Level 5 Workflows – custom workflows for System Developers						✔

Config Drift and Audit	**DV**	**RA**	**OA**	**WA**	**SA**	**SD**
Access Config Drift and Audit Solution		✔	✔	✔	✔	✔
Manage Level 1 Audit Policies				✔	✔	✔
Run and Schedule Level 1 Audit Policies			✔	✔	✔	✔
Manage Level 2 Audit Policies				✔	✔	✔
Run and Schedule Level 2 Audit Policies			✔	✔	✔	✔
Manage Level 3 Audit Policies					✔	✔
Run and Schedule Level 3 Audit Policies					✔	✔
Run and Schedule Device Captures			✔	✔	✔	✔
Data Export	**DV**	**RA**	**OA**	**WA**	**SA**	**SD**
Access Data Export Solution		✔	✔	✔	✔	✔

OS Manager	**DV**	**RA**	**OA**	**WA**	**SA**	**SD**
Access OS Manager Solution		✔	✔	✔	✔	✔
Manage Catalogs					✔	✔
Manage OS Plans					✔	✔
Require Use of Catalogs (when enabled)			✔	✔		
Run and Schedule OS Plans			✔	✔	✔	✔
Device Manager	**DV**	**RA**	**OA**	**WA**	**SA**	**SD**
Access Device Manager Solution		✔	✔	✔	✔	✔
Create and Delete Devices				✔	✔	✔
Edit Devices			✔	✔	✔	✔
Reboot Devices			✔	✔	✔	✔
Run Device Discovery			✔	✔	✔	✔
Update Device Support Data			✔	✔	✔	✔
View Device Vendor Support Data		✔	✔	✔	✔	✔
View and Download Device Activity Logs			✔	✔	✔	✔

Data Explorer	**DV**	**RA**	**OA**	**WA**	**SA**	**SD**
Access Data Explorer Solution			✔	✔	✔	✔
Generate Data From Explorer Templates			✔	✔	✔	✔
Manage Data Explorer Templates					✔	✔
Device API	**DV**	**RA**	**OA**	**WA**	**SA**	**SD**
Include Device Credentials in API Responses						✔
File Server	**DV**	**RA**	**OA**	**WA**	**SA**	**SD**
Access File Server Solution		✔	✔	✔	✔	✔
Manage Files					✔	✔
Schedules	**DV**	**RA**	**OA**	**WA**	**SA**	**SD**
Access Schedules Solution		✔	✔	✔	✔	✔

Settings	DV	RA	OA	WA	SA	SD
Access Organizations Settings		✔	✔	✔	✔	✔
Manage All Users					✔	✔
Manage Auto Capture					✔	✔
Manage Custom Fields					✔	✔
Manage Dashboards					✔	✔
Manage Data Retention Policies					✔	✔
Manage Globals					✔	✔
Manage Integrations					✔	✔
Manage Licenses					✔	✔
Manage Logging					✔	✔
Manage Organizations					✔	✔
Manage OS Management					✔	✔
Manage Roles					✔	✔
Manage Syslog					✔	✔
Manage Zones					✔	✔
Run Data Retention Policies					✔	✔

View All Users	✔	✔	✔	✔	✔	✔
Solutions Manager	**DV**	**RA**	**OA**	**WA**	**SA**	**SD**
Access Solutions Manager Solution		✔	✔	✔	✔	✔
Install Packages					✔	✔

Permissions descriptions

Dashboard	Description
Access Dashboard Solution	Allow use of Gluware dashboards
Create Private Dashboards	Allow the creation of dashboards available only to the creator
Create Public Dashboards	Allow the creation of dashboards available to all users of the organization
Moderate Public Dashboards	Allow allow deletion of other's public dashboards
Config Modeling	
Access Config Modeling Solution	Allow use of Gluware Config Modeling
Create and Edit Globals, Domains, and Features	Allow config modeling constructs to be created and modified
Create and Delete Nodes	Allow nodes to be added and removed
Delete Globals, Domains, and Features	Allow config modeling constructs to be deleted
Edit Nodes	Allow nodes to be modified
View JSON Format	Allow the JSON for config modeling constructs to be viewed in the Config Modeling Instance panel

Provisioning	
Access Actions within Config Modeling	Allow read-only access to Config Modeling and provisioning actions to be run and scheduled
Allow Configuration Changes	Allow configuration changes through provisioning, OS management, and device and state assessment utilities on selected nodes
View Logs and Download Bundles	Review Config Modeling logs and download provisioning bundles
Workflows	
Access Workflows Solution	Allow use of Gluware Workflows
Run Level 1 Workflows	Allow workflows with authorization level wizard-read to be run
Run Level 2 Workflows	Allow workflows with authorization level wizard-write to be run
Run Level 3 Workflows	Allow workflows with authorization level wizard-operate to be run
Run Level 4 Workflows	Allow workflows with authorization level wizard-admin to be run
Run Level 5 Workflows	Allow workflows with authorization level wizard-develop to be run

Config Drift and Audit	
Access Config Drift and Audit Solution	Allow use of Gluware Config Drift and Audit
Manage Level 1 Audit Policies	Allow level 1 audit policies to be created, modified, and deleted
Run and Schedule Level 1 Audit Policies	Allow level 1 audit policies to be scheduled to run and run on demand
Manage Level 2 Audit Policies	Allow level 2 audit policies to be created, modified, and deleted
Run and Schedule Level 2 Audit Policies	Allow level 2 audit policies to be scheduled to run and run on demand
Manage Level 3 Audit Policies	Allow level 3 audit policies to be created, modified, and deleted
Run and Schedule Level 3 Audit Policies	Allow level 3 audit policies to be scheduled to run and run on demand
Run and Schedule Device Captures	Allow configuration snapshots to be scheduled to run and run on demand
Data Export	
Access Data Export Solution	Allow use of Gluware Data Export to download Gluware data reports

OS Manager	
Access OS Manager Solution	Allow use of Gluware OS Management
Manage Catalogs	Allow image catalogs to be created, modified, and deleted
Manage OS Plans	Allow OS plans to be created, modified, and deleted
Require Use of Catalogs (when enabled)	If OS Catalogs are enabled in System Settings, require OS catalogs to be used as the source of images for OS plans
Run and Schedule OS Plans	Allow OS plans to be scheduled to run and run on demand

Device Manager	
Access Device Manager Solution	Allow use of Gluware Device Manager
Create and Delete Devices	Allow devices to be added and removed from Gluware
Edit Devices	Allow devices to be modified
Reboot Devices	Allow devices to be restarted
Run Device Discovery	Allow Discover Devices to be run
Update Device Support Data	If enabled in System Settings, allow Cisco Bulletins, Security Advisory counts, and SmartNet contract details to be retrieved from the Cisco API Console
View Device Vendor Support Data	Allow Cisco Bulletins, Security Advisory counts, and SmartNet contract details to be read
View and Download Device Activity Logs	Allow device logs to be downloaded
Data Explorer	
Access Data Explorer Solution	Allow use of Data Explorer
Generate Data From Explorer Templates	Allow reports to be run from Data Explorer templates
Manage Data Explorer Templates	Allow creation, modification, and deletion of Data Explorer templates

Device API	
Include Device Credentials in API Responses	If GluAPI integration is enabled in System Settings, allow device credentials to be included in the response
File Server	
Access File Server Solution	Allow use of Gluware File Server
Manage Files	Allow image files to be added, modified, and deleted from File Servers
Schedules	
Access Schedules Solution	Allow Gluware schedules to be viewed; allow schedules for tasks the user is allowed to run to be modified and deleted
System Settings	
Access Organizations Settings	Allow use of Gluware System Settings
Manage All Users	Allow Gluware users to be added, modified, and deleted
Manage Auto Capture	Allow automatic configuration snapshots to be set up for selected actions
Manage Custom Fields	Allow custom fields to be added, modified, and deleted
Manage Dashboards	Allow specific dashboard preferences for an organization
Manage Data Retention Policies	Allow data retention policies to be set up, modified, and deleted

Manage Globals	Allow access to global settings
Manage Integrations	Allow access to integration settings
Manage Licenses	Allow Gluware licenses to be installed and removed and expiration dates and device counts to be viewed
Manage Logging	Allow access to logging settings
Manage Organizations	Allow organizations to be added, modified, and deleted
Manage OS Management	Allow access to OS management settings including File Servers
Manage Roles	Allow roles to be created, modified, and deleted
Manage Syslog	Allow monitoring of syslog messages to be set up to catch configuration changes
Manage Zones	Allow zones to be created for Gluware Zone Engines
Run Data Retention Policies	Allow data retention policies to be scheduled to run or run on demand
View All Users	Allows all users in the organization to be viewed
Solutions Manager	
Access Solutions Manager Solution	Allow use of Gluware Solutions Manager
Install Packages	Allow installation of new and updated Gluware packages

Install a Gluware license

Gluware licenses are used to manage:

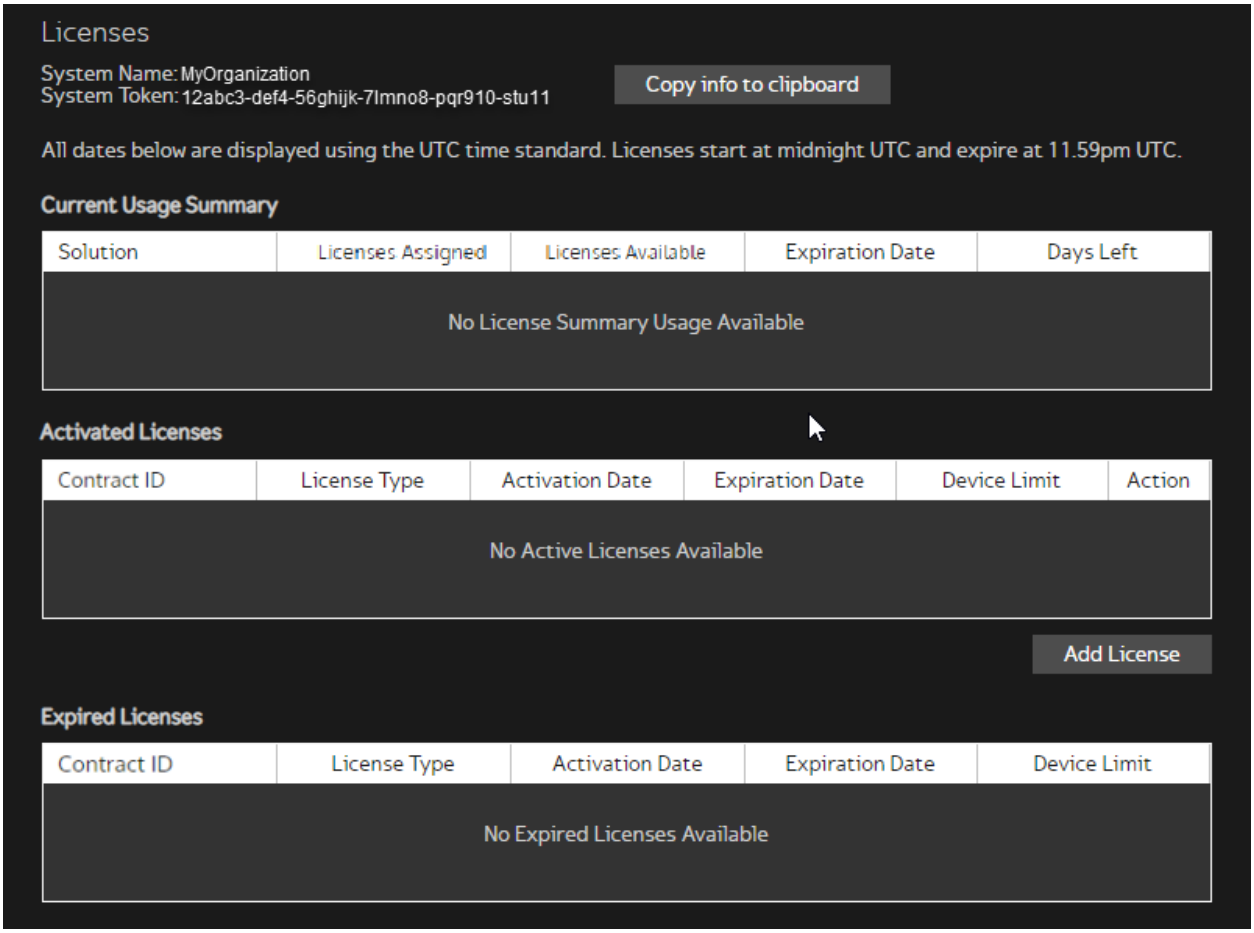
- The Gluware solutions available to you
- The maximum number of devices in your Gluware system
- The expiration date of your evaluation period or product licenses

Only Gluware system settings is available until your license is installed. You'll need to create your organizations and add System Admin users, then install your Gluware license.

> **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 a license key from Gluware

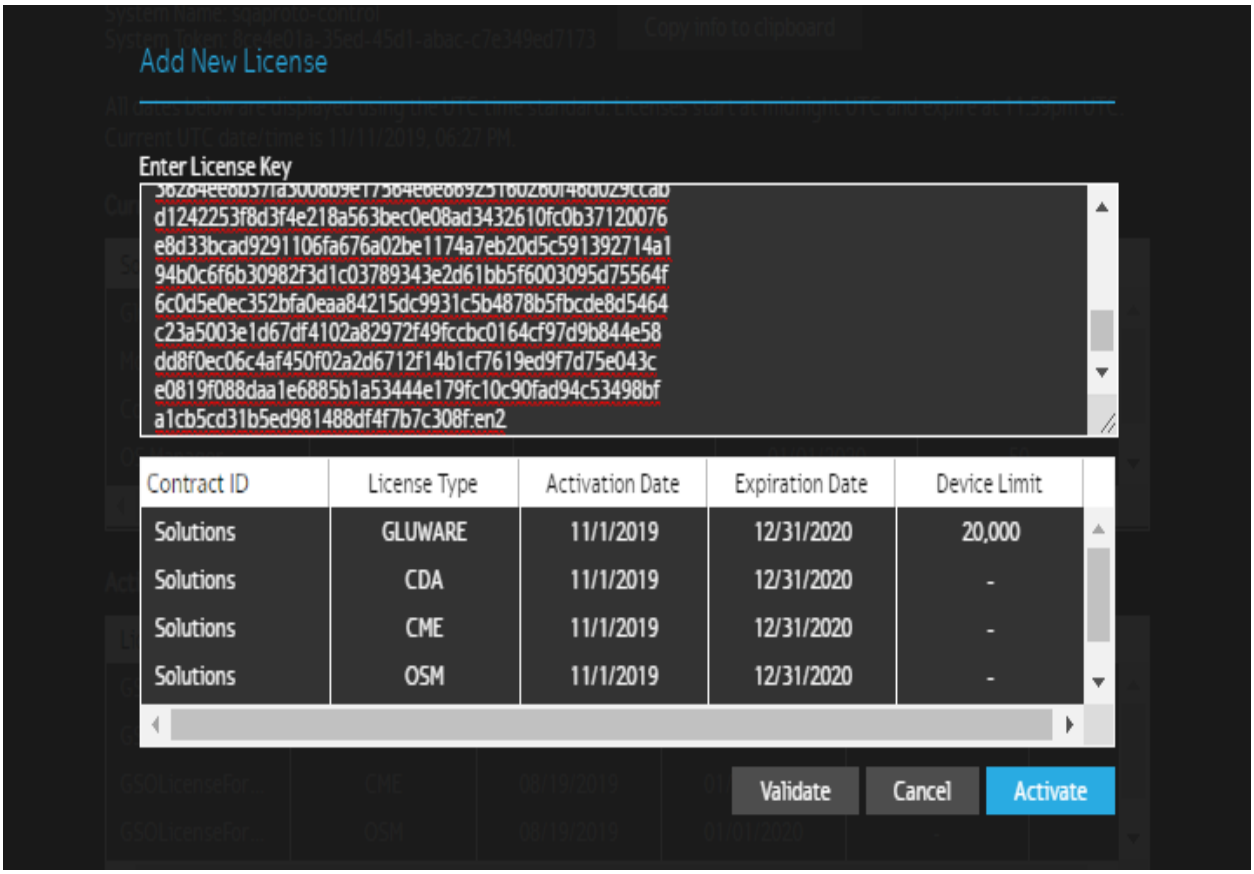
1. Ensure you're in the organization you want to install the license in. This is usually your parent (topmost) organization.
2. Go to **Settings** > **Organization** > **Licensing**. You should see your system name and system token.
3. Click **Copy info to clipboard**. This copies the system name and 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 the license

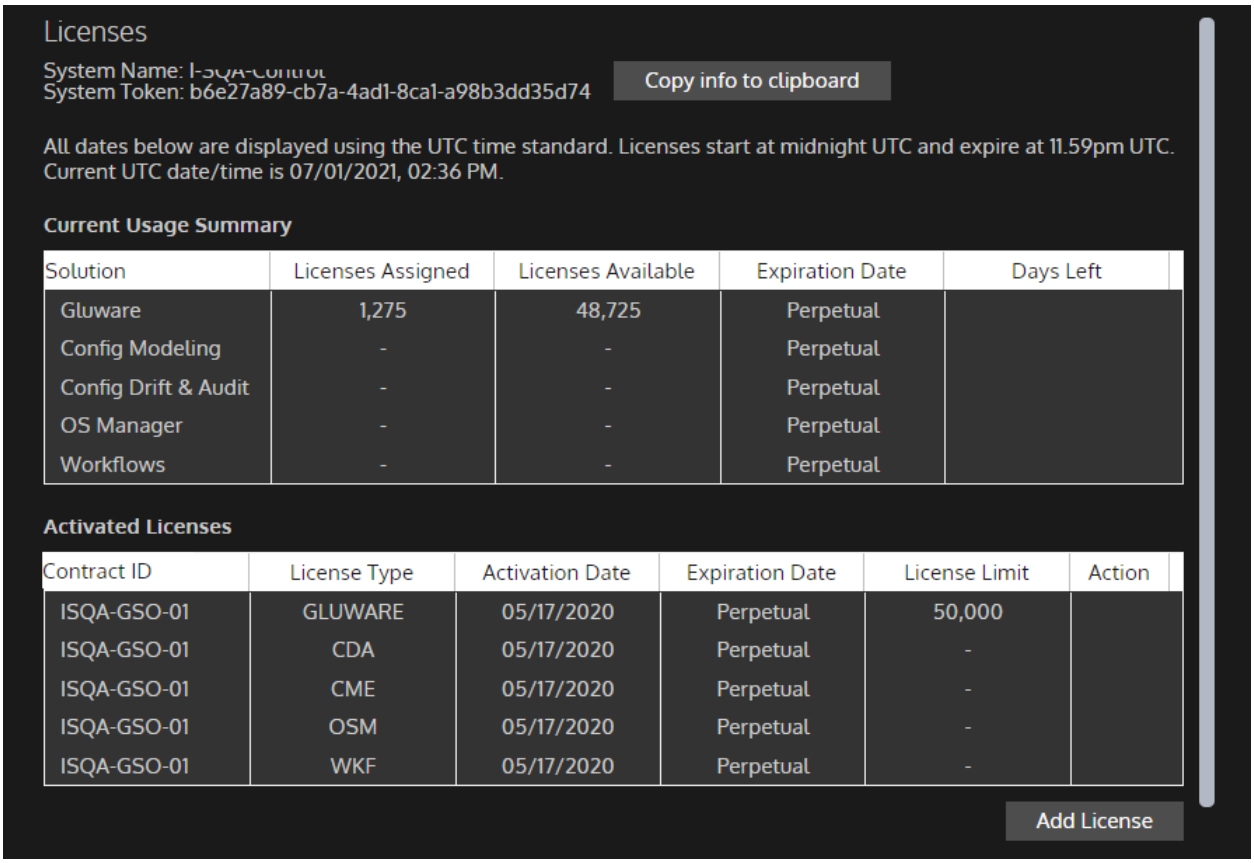
When you receive the license key from Gluware, return to system settings to install it.

1. Ensure you're in the organization you want to install the license in. This is usually your parent (topmost) organization.
2. Go to **Settings** > **Organization** > **Licensing**.
3. Click **Add License**.
4. Paste the contract ID you received from Gluware in the space provided and click **Validate**.



1. **Important**: Verify
    - No error messages 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
2. 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**.

When installed, you'll see the license in the **Activated Licenses** 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.

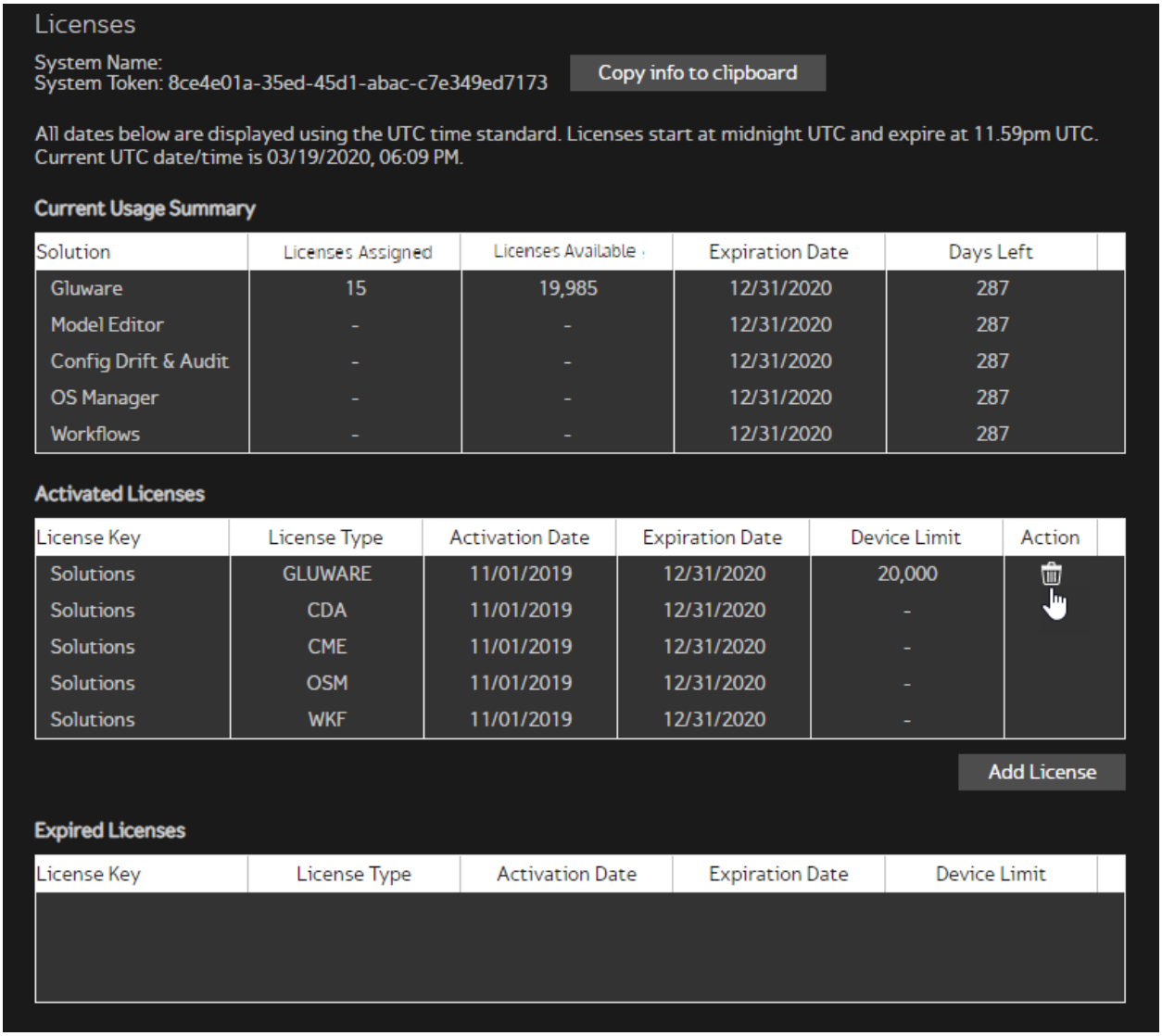

Licenses
System Name: I-SQA-Control
System Token: b6e27a89-cb7a-4ad1-8ca1-a98b3dd35d74
Copy info to clipboard
All dates below are displayed using the UTC time standard. Licenses start at midnight UTC and expire at 11.59pm UTC.
Current UTC date/time is 07/01/2021, 02:36 PM.
Current Usage Summary
Solution
Licenses Assigned
Licenses Available
Expiration Date
Days Left
Gluware
1,275
48,725
Perpetual
Config Modeling
-
-
Perpetual
Config Drift & Audit
-
-
Perpetual
OS Manager
-
-
Perpetual
Workflows
-
-
Perpetual
Activated Licenses
Contract ID
License Type
Activation Date
Expiration Date
License Limit
Action
ISQA-GSO-01
GLUWARE
05/17/2020
Perpetual
50,000
ISQA-GSO-01
CDA
05/17/2020
Perpetual
-
ISQA-GSO-01
CME
05/17/2020
Perpetual
-
ISQA-GSO-01
OSM
05/17/2020
Perpetual
-
ISQA-GSO-01
WKF
05/17/2020
Perpetual
-
Add License

Delete a Gluware license

If you install a Gluware license in the wrong organization, you can delete it. However, you'll need to request a replacement license from licensing@gluware.com if you want to install it in another organization.

WARNING! Deleting a license deletes access to the devices and device information associated with the license.

1. Ensure you're in the organization you installed the Gluware license in.
2. Go to **Settings** > **Organization** > **Licensing**.
3. In the **Active Licenses** list, click beside the license you want to delete.
4. Click **Confirm**.


Licenses
System Name:
System Token: 8ce4e01a-35ed-45d1-abac-c7e349ed7173
Copy info to clipboard
All dates below are displayed using the UTC time standard. Licenses start at midnight UTC and expire at 11.59pm UTC.
Current UTC date/time is 03/19/2020, 06:09 PM.
Current Usage Summary
Solution | Licenses Assigned | Licenses Available | Expiration Date | Days Left
Gluware | 15 | 19,985 | 12/31/2020 | 287
Model Editor | - | - | 12/31/2020 | 287
Config Drift & Audit | - | - | 12/31/2020 | 287
OS Manager | - | - | 12/31/2020 | 287
Workflows | - | - | 12/31/2020 | 287
Activated Licenses
License Key | License Type | Activation Date | Expiration Date | Device Limit | Action
Solutions | GLUWARE | 11/01/2019 | 12/31/2020 | 20,000
Solutions | CDA | 11/01/2019 | 12/31/2020 | -
Solutions | CME | 11/01/2019 | 12/31/2020 | -
Solutions | OSM | 11/01/2019 | 12/31/2020 | -
Solutions | WKF | 11/01/2019 | 12/31/2020 | -
Add License
Expired Licenses
License Key | License Type | Activation Date | Expiration Date | Device Limit

View license expiration dates and device counts

In system settings, you can see:

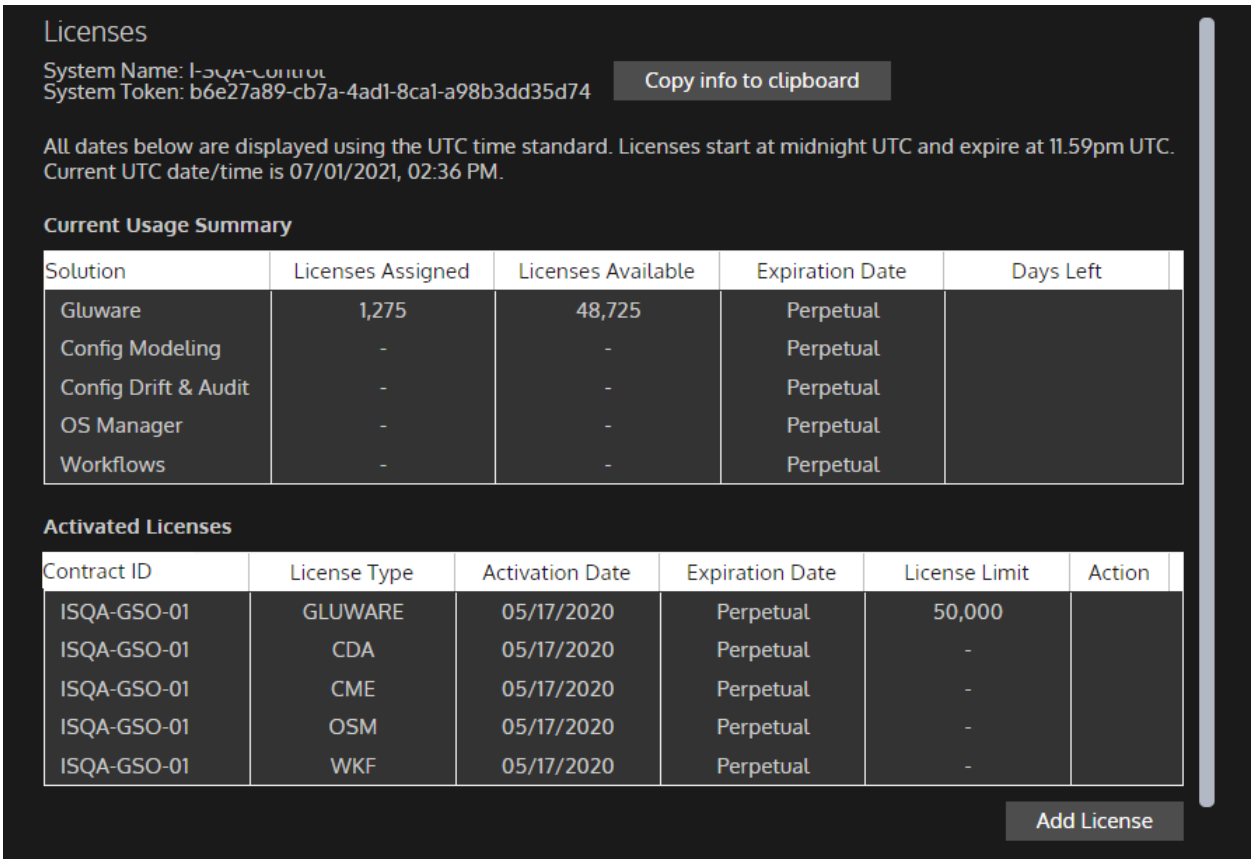
- All the Gluware licenses for the organization
- The number of devices you are licensed for in Gluware
- The number of devices still available for you to add
- The expiration date of each license
- Any expired licenses

NOTES: For licensing purposes, a device is defined to be an individual (physical or virtual) router, firewall, Wide Area Network (WAN) acceleration device or a switch; however, in the case of a switch, each blade will consume one device license. For example, a switch chassis with two blades is equal to two devices, a chassis with four blades will consume four device licenses, etc.

As your license nears expiration or your device count nears the limit, you'll see a warning message. Data is not lost, even if the license expires, but it will no longer be accessible in Gluware.

Licenses expire at 11:59:59 UTC.

1. Ensure you're in the organization you installed the Gluware license in.
2. Go to **Settings** > **Organization** > **Licensing**.


Licenses
System Name: I-SQA-Control
System Token: b6e27a89-cb7a-4ad1-8ca1-a98b3dd35d74
Copy info to clipboard
All dates below are displayed using the UTC time standard. Licenses start at midnight UTC and expire at 11.59pm UTC.
Current UTC date/time is 07/01/2021, 02:36 PM.
Current Usage Summary
Solution | Licenses Assigned | Licenses Available | Expiration Date | Days Left
Gluware | 1,275 | 48,725 | Perpetual
Config Modeling | - | - | Perpetual
Config Drift & Audit | - | - | Perpetual
OS Manager | - | - | Perpetual
Workflows | - | - | Perpetual
Activated Licenses
Contract ID | License Type | Activation Date | Expiration Date | License Limit | Action
ISQA-GSO-01 | GLUWARE | 05/17/2020 | Perpetual | 50,000
ISQA-GSO-01 | CDA | 05/17/2020 | Perpetual | -
ISQA-GSO-01 | CME | 05/17/2020 | Perpetual | -
ISQA-GSO-01 | OSM | 05/17/2020 | Perpetual | -
ISQA-GSO-01 | WKF | 05/17/2020 | Perpetual | -
Add License

Add Gluware users

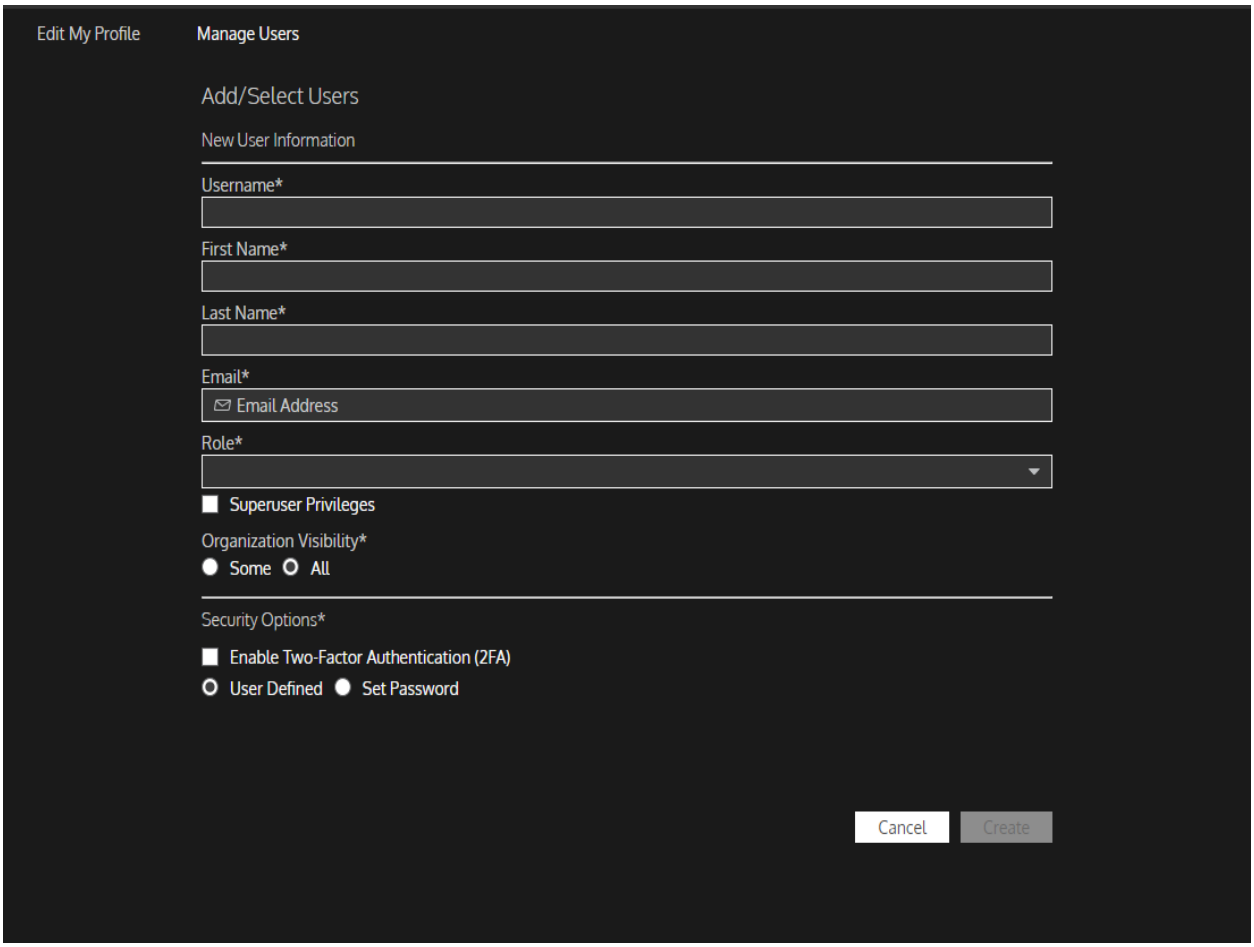
If your organization does not use LDAP or RADIUS to authenticate users, users can be authenticated through the Gluware server. A best practice is to create users in your parent organization and add devices to a child organization.

At least one person in each organization must have **Superuser Privileges**. Superusers can add and remove permissions for any other role in the organization.

> **NOTE:** A user's roles and permissions can have a big impact on what features and actions are available to the user, especially if you customized roles.

1. Go to **Settings** > **User** > **Manage Users**.
2. Click **Add User+**.
3. Enter the user name, first name, last name, and a unique email address.
4. Select a role from the drop-down list to refine the user's permissions.
5. Optional: Check the **Superuser Privileges** box to allow the user to add and remove permissions for all other roles in the organization.
6. To limit the Gluware organization the user has permissions for, select **Some** and then select an organization from the drop-down list. **All** gives access to the current organization and all its child organizations.
7. Optional: Select **Enable 2FA**. Users must enter a 2FA code provided by a third-party authentication application to access devices.

8. Password options:
    - Select **User Defined** if you want the user to establish their password. The user will receive an email with instructions on how to set their password.
    - Select **Set Password** if you want to manage the user's password. Enter a password and confirm it.
9. Click **Create**.



Customize roles and permissions

You can add new roles and refine permissions to meet your organization's needs. Custom roles are then available, along with the standard Gluware roles, to assign to users.

You can restrict access to a Gluware solution that you are licensed for, such as **Config Drift and Audit** or **Config Modeling**. And you can specify view-only or management (read-write) permissions. You can also limit visibility to specific devices and specify email addresses to receive specific notifications. For example, you can create a role to manage only devices in a specific region or from a specific vendor.

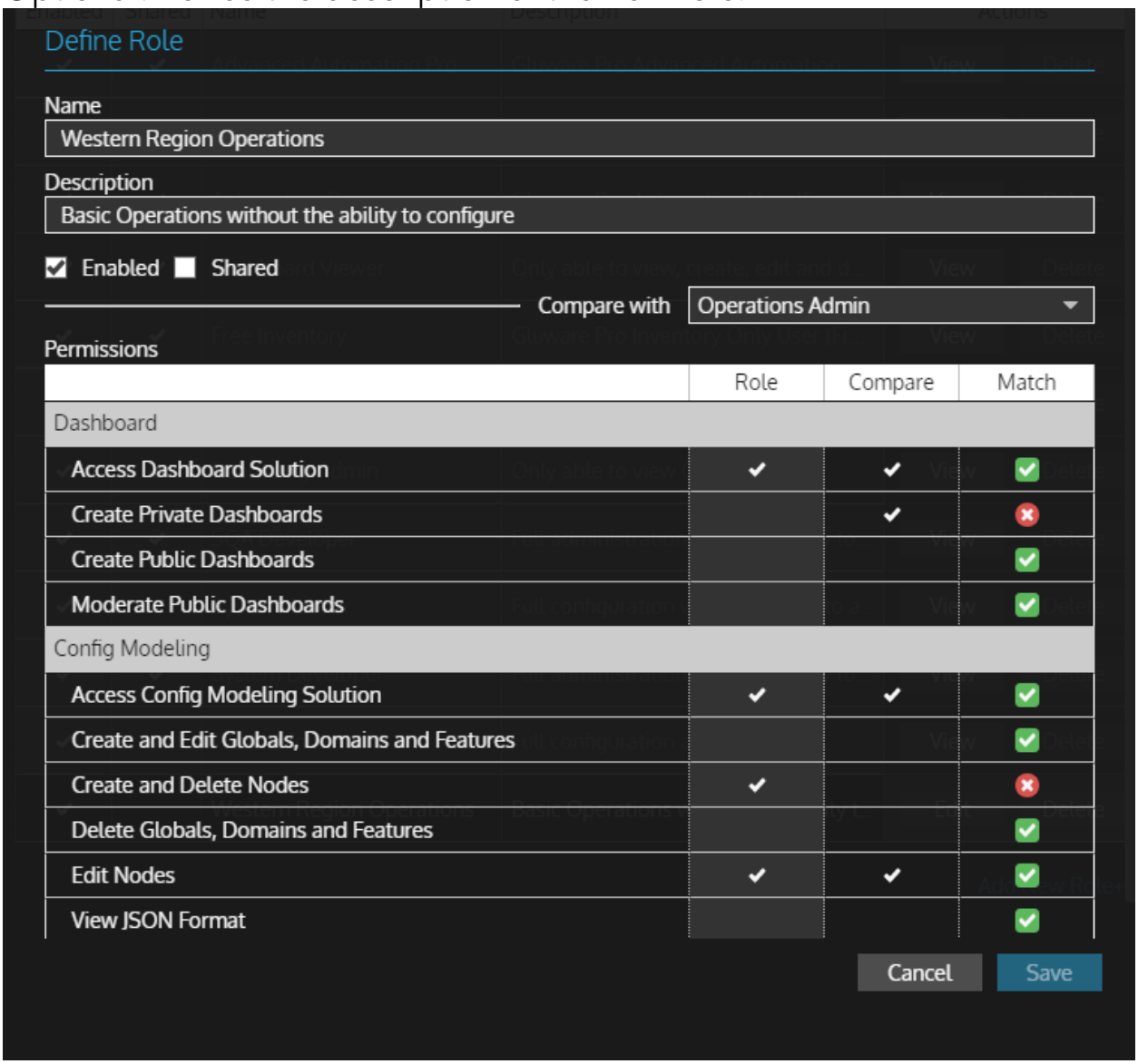
If a custom role is shared, the role is inherited in child organizations. However, roles can only be managed in the organization they are created in.

> **NOTE:** If you add custom roles and use LDAP or RADIUS for authentication, you'll need to add the custom role to the **Map Role Attribute Value** in **Settings** > **Organization** > **Organizations**. You'll also need to add the value in your active directory.

Create a custom role

1. Ensure you're in the organization you want to create the role in.
2. Go to **Settings** > **Organization** > **Roles**.
3. Click **Add New Role +**.
4. Enter a name for the custom role.
5. Optional: Select from the drop-down list a standard Gluware role, or one of your custom roles, to base the new role on. This copies the role's permissions to the custom role you are creating. You can then add or remove permissions to easily customize the new role.
6. Click **Create**.

7. Optional: Revise the description of the new role.



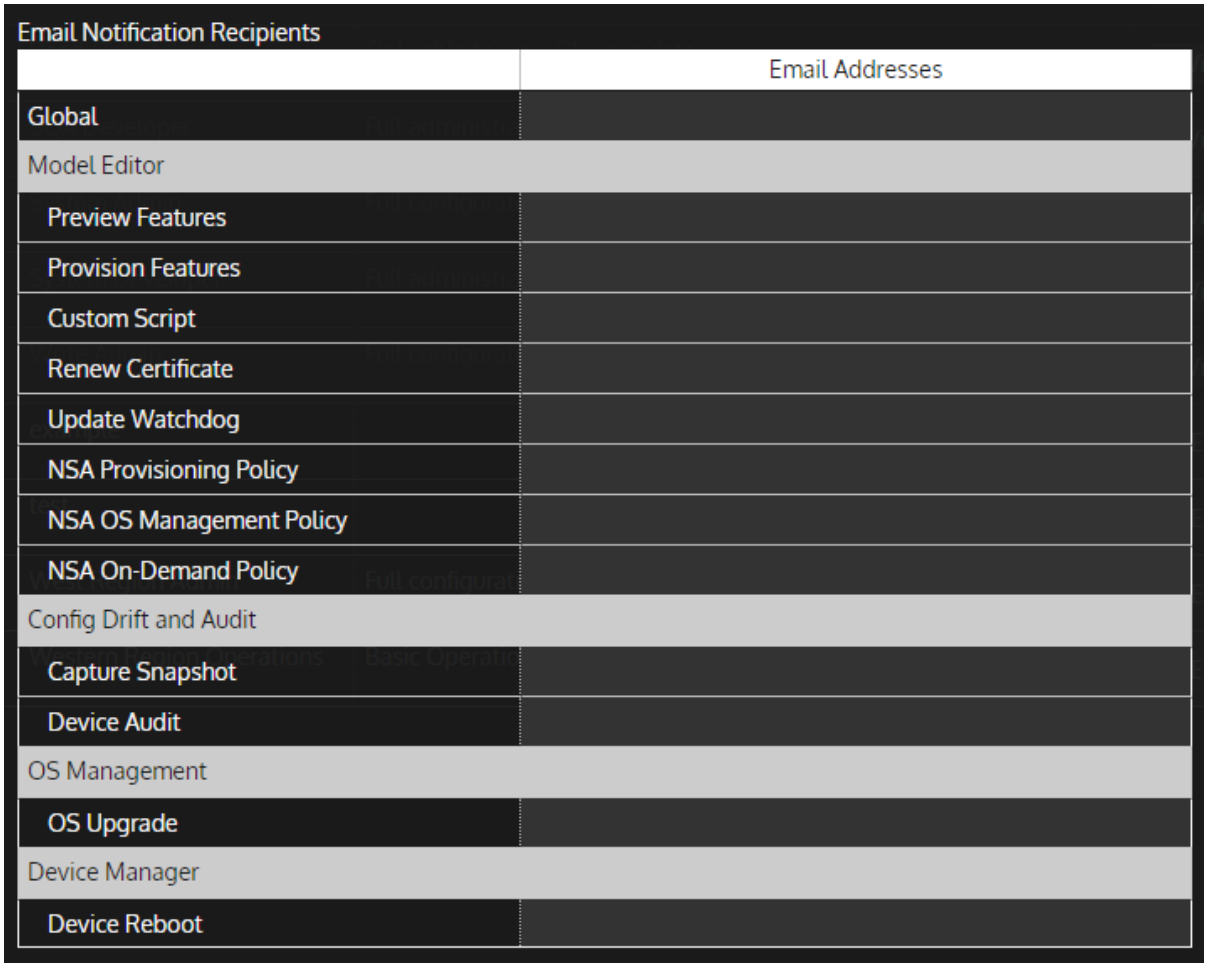
8. Optional: Clear the **Enabled** box if you don't want to assign users to the role at this time.
9. Optional: Check the **Shared** box if you want child organizations to inherit the custom role.
10. Optional: Double-click in the box and clear or check each permission you want to change for the new role. The **Compare with** column shows the permissions for the role selected from the drop-down list. The **Match** column indicates when the new role's permission is the same as the role you are comparing it to.

NOTE: If you prohibit access to a Gluware solution (e.g. Config Modeling), the permissions within that solution will also be prohibited even though they may still be checked in the permissions list.

11. Optional: Use the **Device Filter** to restrict the devices that the role can manage.
    - Select a field from the drop-down list, select a condition from the drop-down list, and then enter a term. Fields will include **Vendor**, **Type**, **Name**, and **Hostname**, and any of the organization's custom fields. Custom fields are shared if the role is also shared.
    - Click **Add rule** and click **AND** or **OR** to add a logical operator.
    - Click **Add group** to add a nested rule.
    - To clear a filter, click **Reset**.

NOTE: If your organization restricts the devices a role can manage, it's possible a user can add devices that the user cannot later manage. Once devices are discovered, devices may appear or disappear from a user's device list.

12. Optional: Double-click, type one or more email addresses to set as the default for a specific notification, and press **Enter**. Separate email addresses with a comma. These default emails assigned to the user's role will be presented as an optional recipient when the action is scheduled.



13. Save.

Modify a custom role

1. Ensure you're in the organization that the custom role was created in.
2. Go to **Settings** > **Organization** > **Roles**.
3. Click **Edit** beside the role you want to change.
4. Clear the **Enabled** box if you want to keep the role but won't use it at this time.

5. Check the **Shared** box if you want child organizations to inherit the custom role. Or clear the box to restrict the role to the current organization.
6. Double-click in the box and clear or check the permission you want to change.
7. Use the **Device Filter** to restrict the devices that the role can manage. Or clear the existing filter.
8. Double-click and add, change, or remove email addresses for each notification you want to change. Press **Enter** after each change.
9. Save.

Remove a custom role

You can't delete a standard Gluware role or a role that has users assigned to it.

1. Ensure you're in the organization that the custom role was created in.
2. Go to **Settings** > **Organization** > **Roles**.
3. Click **Delete** beside the role you want to remove.
4. Click **Confirm**.

Set default emails for notifications

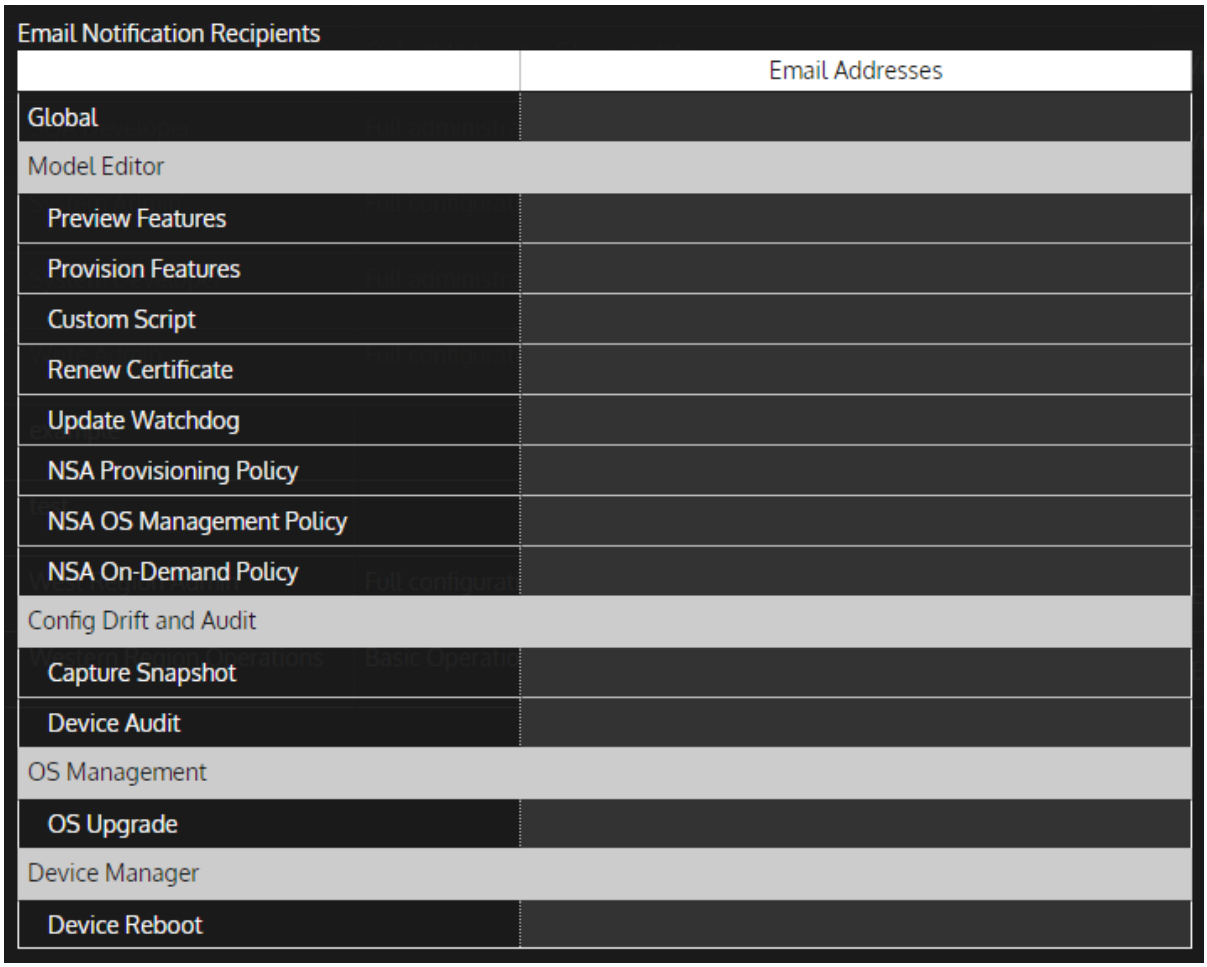
Email notifications may be sent when scheduled actions are completed. The actions that support scheduling and notifications include:

- Taking a Config Drift snapshot
- Running a Config Audit policy
- Provisioning a device
- Previewing a device provisioning
- Renewing device certificates
- Executing custom scripts
- Executing an OS plan
- Transferring OS images
- Transferring OS images and rebooting devices
- Assessing the state of a device
- Updating the gluWatchdog agent

The default email assigned to the user's role will be listed as an optional recipient when the action is scheduled.

Set default emails

1. Ensure you're in the organization that the custom role was created in.
2. Go to **Settings** > **Organization** > **Roles**.
3. Click **Edit** beside the role you want to set default emails for.
4. Double-click, type one or more email addresses, and press **Enter**. Separate email addresses with a comma. These default emails assigned to the user's role will be presented as an optional recipient when the action is scheduled.

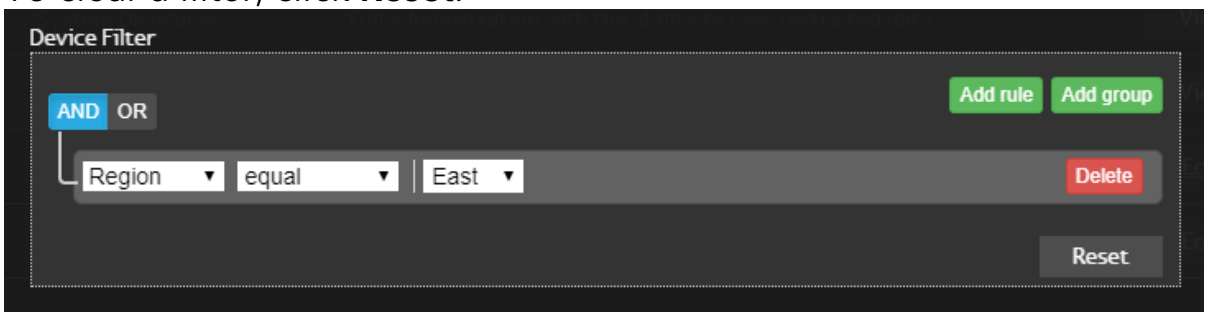

Email Notification Recipients
Email Addresses
Global
Model Editor
Preview Features
Provision Features
Custom Script
Renew Certificate
Update Watchdog
NSA Provisioning Policy
NSA OS Management Policy
NSA On-Demand Policy
Config Drift and Audit
Capture Snapshot
Device Audit
OS Management
OS Upgrade
Device Manager
Device Reboot

5. Save.

Restrict the devices a role can manage

You can limit the devices that a role can manage to specific types of devices or locations of devices. You can use a combination of custom roles and custom fields to restrict management of specific devices to specific users. For example, you can create a role, Operators - East Region, and restrict that role to managing devices assigned the custom field, Region, with a value of East.

1. Ensure you're in the organization that the custom role was created in.
2. Go to **Settings** > **Organization** > **Roles**.
3. Click **Edit** beside the role for which you want to define the devices that can be managed.
4. Use the **Device Filter** to define the devices that the role can manage.
    - Select a field from the drop-down list, select a condition from the drop-down list, and then enter a term. Fields will include **Vendor**, **Type**, **Name**, and **Hostname**, and any of the organization's custom fields. Custom fields are shared if the role is also shared.
    - Click **Add rule** and click to add a logical operator (**AND**/**OR**).
    - Click **Add group** to add a nested rule.
    - To clear a filter, click **Reset**.



5. Save.

NOTE: If your organization restricts the devices users can manage, it's possible a user can add devices that the user cannot later manage. Once devices are discovered, devices may appear or disappear from a user's device list.

Enable/disable a system banner

You can create a custom banner that is displayed on sign-in for all users. For example, you can use the banner for corporate governance policy requirements. You can choose to display it on the user's first sign-in only or on every sign-in.

Enable a system banner

1. Ensure you're in the parent (topmost) organization.
2. Go to **Settings** > **Global** > **Banner**.
3. Check the **Enable System Banner** box.
4. Enter the text to display as the banner using HTML markup. These HTML tags are supported:
   h1, h2, h3, h4, h5, h6, p, span, a, img, i, b, strong, em, ul, ol, li.
5. Define the acceptance and refusal button text.
6. Select how often you want the banner to be displayed:
   - On every sign-in
   - Only on first sign-in per user
7. Click **Preview**.
8. Save.

Disable a system banner

1. Ensure you're in the parent (topmost) organization.
2. Go to **Settings** > **Global** > **Banner**.
3. Clear the **Enable System Banner** box.
4. Save.

Reset a system banner

You can clear all acceptances and re-collect them. For example, if you change the system banner you can ensure all users acknowledge the change.

1. Ensure you're in the parent (topmost) organization.
2. Go to **Settings** > **Global** > **Banner**.

3. Click **Reset User Acknowledgements**.
4. Click **Reset**.

Customize dashboards

Brand your dashboard

You can add an image to the title bar of your dashboards. The image can be inherited by all child organizations or can be specific to each organization.

1. Ensure you're in the organization you want to enable/disable dashboards for.
2. Go to **Settings** > **Organization** > **Dashboards**.
3. Check the **Enable custom Dashboard Images** box.
4. Click , select your image file, and click **Open**.
5. Click and drag or zoom to optimize the image.
6. Click **Add**.
7. Click **Save**.

Change your dashboard theme

The background of your dashboard and widgets can be light or dark. A dark background is often favored for a large communal display.

1. Go to **Settings** > **User** > **Edit My Profile**.
2. Select the **Light** or **Dark** theme.
3. Click **Save**.
4. Click **OK**.

Enable/disable a dashboard carousel

You can have your favorite dashboards rotate in the display.

1. Go to **Settings** > **User** > **Edit My Profile**.
2. Set the **Delay (seconds)** to determine how long each of your favorite dashboards will display. Select **Disable** to view one dashboard at a time.
3. Click **Save**.
4. Click **OK**.

Enable/disable keyboard shortcuts

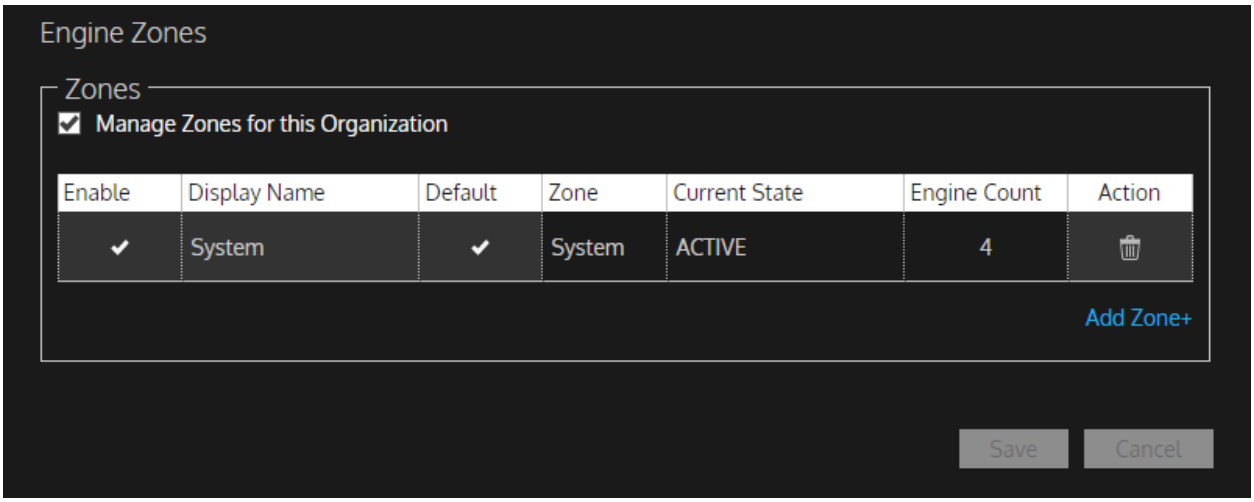
1. Go to **Settings** > **User** > **Edit My Profile**.
2. Check or clear the **Keyboard Shortcuts** boxes.
3. Click **Save**.
4. Click **OK**.

Manage zones for Gluware Zone Engines

If you install Gluware Zone Engines, you can assign these 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.



Add a new zone

1. Recommended: Ensure you're in the organization in which your Gluware licenses are installed.
2. Go to **Settings** > **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.
7. Install the Gluware Zone Engine in this zone. Refer to the *Gluware Installation Guide* for help.

Set the default zone

If devices are not assigned to a zone, jobs will run on the default zone.

1. Ensure you're in the organization in which your zones are managed.
2. Go to **Settings** > **Organization** > **Zones**.
3. Double-click in the **Default** column beside the zone and check the box.
4. Save.

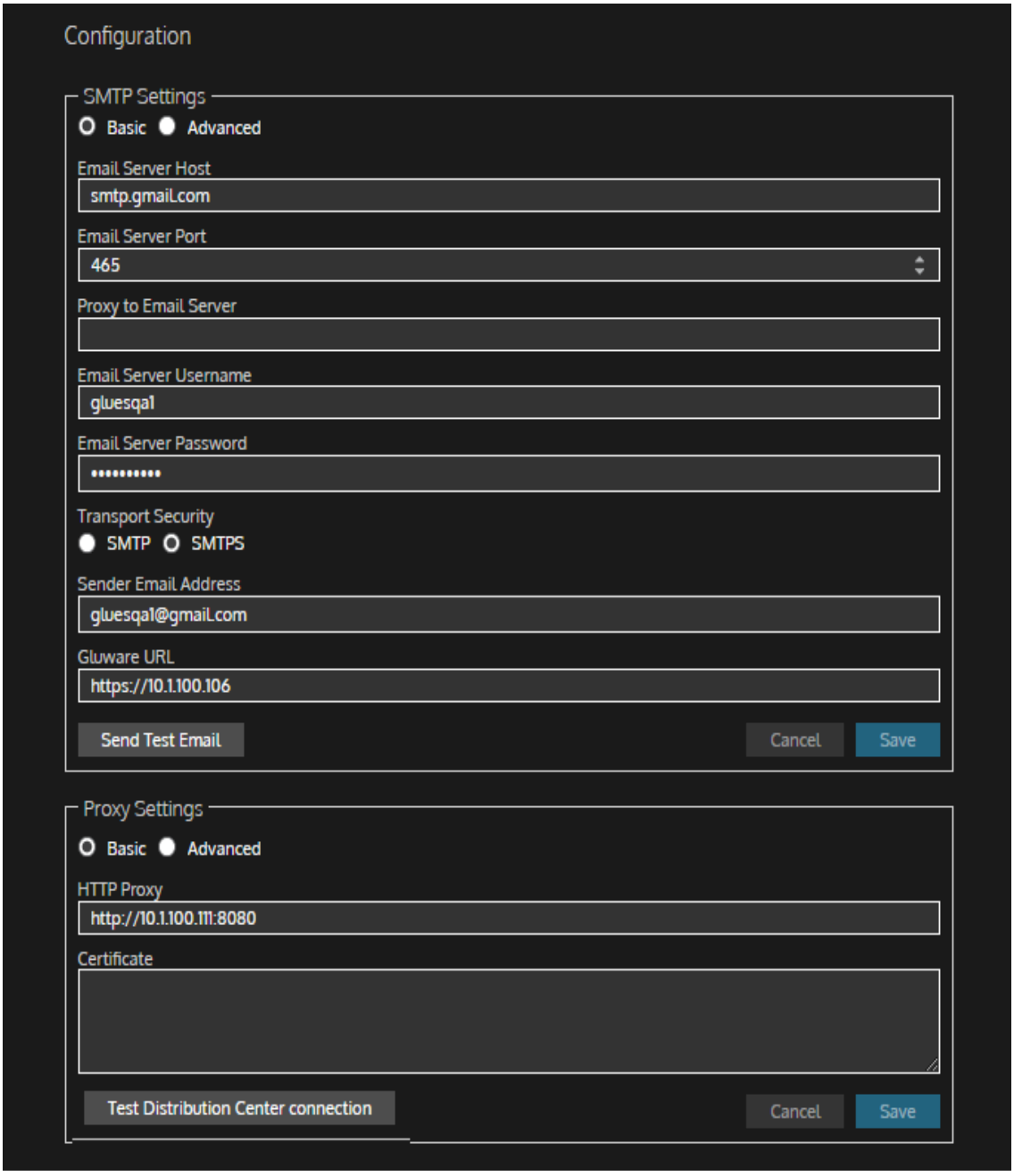
Disable a zone

1. Ensure you're in the organization in which your zones are managed.
2. Go to **Settings** > **Organization** > **Zones**.
3. Clear the **Enable** box beside the zone.
4. Save.

Configure SMTP and proxy settings

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



Configure SMTP settings

Basic SMTP 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 parent topmost (root) organization.
2. Go to **Settings** > **Global** > **SMPT & Proxy**.
3. Enter the **Email Server Host**. This is the mail server host name or IP address for the SMTP server.
4. Enter the **Email Server Port**, the port number for SMTP traffic.
5. Optional: Enter the **Proxy to the Email Server**.
6. Enter the **Email Server Username**. This is the user account used to authenticate with the SMTP server when sending emails.
7. Enter the **Email Server Password**, the password for the SMTP username account.
8. Select the **Transport Security**: **SMTP** or **SMTPS**.
9. Enter the **Sender Email Address**, the return email address for any mail sent from the Gluware server.
10. Verify the **Gluware URL**, the URL of your primary Gluware server (FQDN or IP address)
11. Save.
12. Send a test email:
    a. Click **Send Test Email**.
    b. Enter the recipient's email address.
    c. Click **Send Test Email**.

Configure proxy settings

Basic proxy 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. Enter the **HTTP Proxy**.
2. Enter the PEM encoded X.509 certificate(s) if using HTTPS.
3. Save.
4. Test the connection to the Gluware Distribution Center:
    a. Click **Test Distribution Center connection**.
    b. Click **OK**.

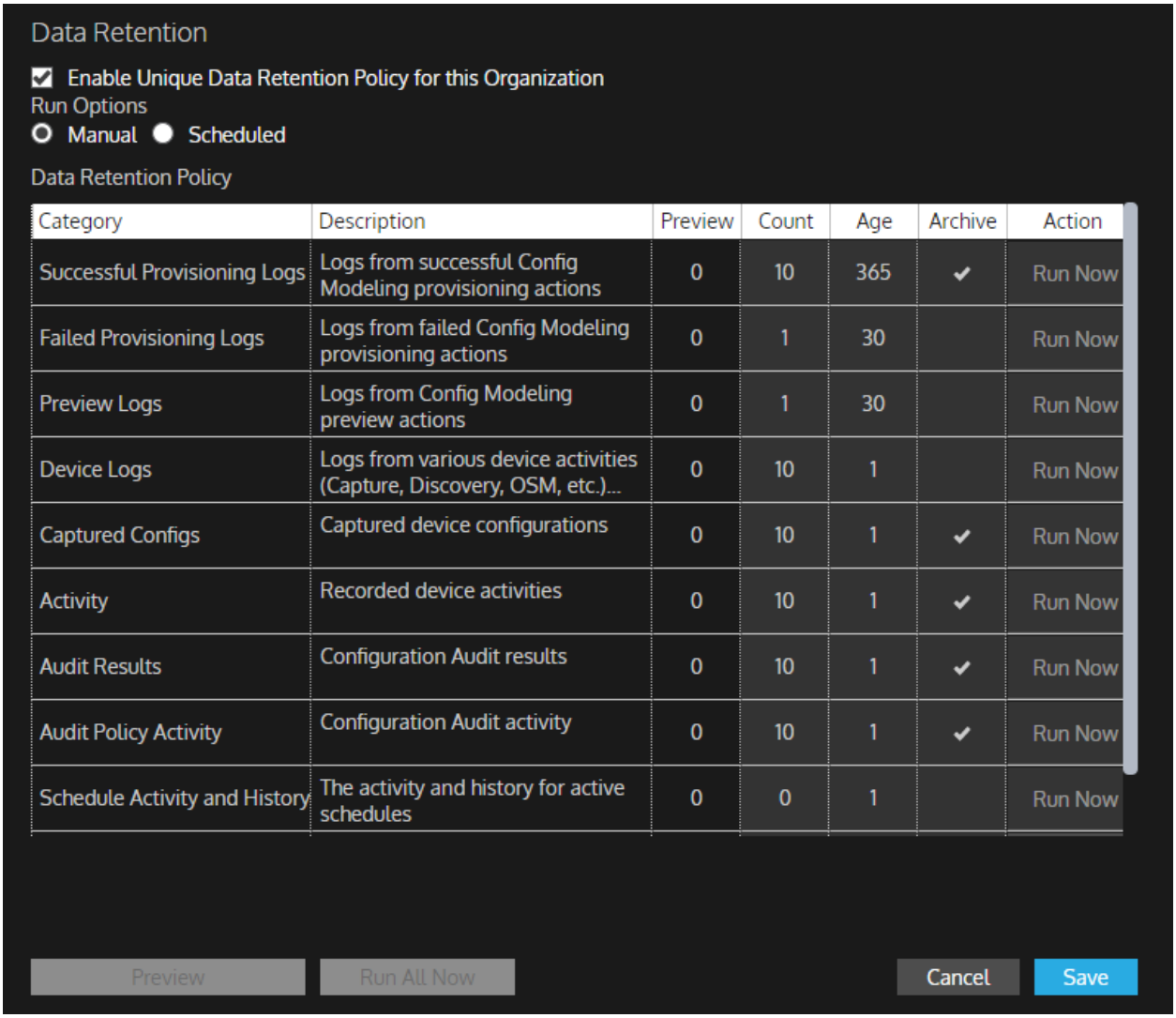
Manage data retention

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 manage data retention for.
2. Go to **Settings** > **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.
    a. Select **Manual** to only run the policy at will.
    b. Select **Scheduled** and set the frequency to automate the policy.
4. Specify the number of records to retain 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 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.



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.

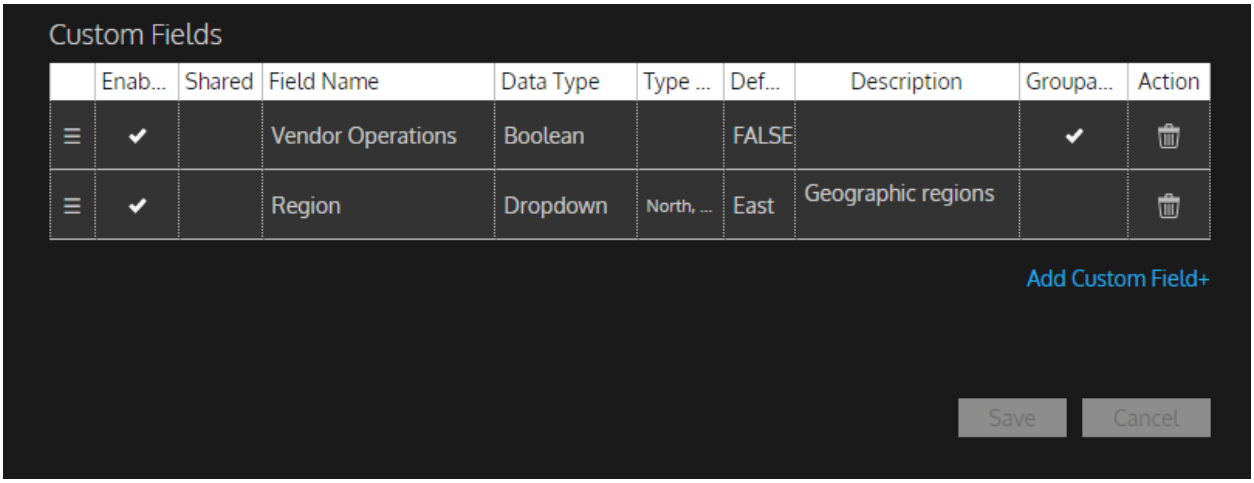
Other Data Retention fields

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

Set up custom fields

Custom fields can be created for each organization or shared from parent to child organizations. Devices in **Device Manager** all maintain their own values for the set of custom fields. The fields can be used to identify aspects of your network or business for use in filtering large numbers of devices in Gluware.

1. Ensure you're in the organization you want to set up custom fields for.
2. Go to **Settings** > **Organization** > **Custom Fields**.
3. Click **Add Custom Field+**.
4. Double-click in each cell of the new row to describe your custom field.
5. To change the order in which the custom field appears in **Device Manager** - **Device Details**, drag the for the custom field to re-order it.
6. Save.



Column	Description
Enabled	Adds this field in **Device Details** for every device in the organization
Shared	Specify whether this field will be shared with subordinate organizations
Field Name	Name for the field
Data Type	Specify the type of the field: **String**, **Boolean**, **Number**, or **Dropdown**
Type Options	For **String** data types, enter optional regex that will be validated against For **Number** data types, specify whether to accept integers only and the range of acceptable numbers For **Dropdown** data types, specify the values that can be selected and click the click check mark to save
Default Value	Optional: displayed default for the field
Description	Displayed field description
Groupable	Add the custom field to the **Group By** option in the **Device Explorer** filter
Action	Deletes the custom field

Monitor configurations changes

Gluware can monitor the syslog to catch configuration changes. Changes are displayed in **Device Manager** in the **Configured Type** column.

The devices currently supported for syslog monitoring are listed at https://gluware.com/supported-platforms/

You'll need to enable syslog monitoring for each organization. We recommend configuring the message logging level **Informational** on devices.

Syslog messages may get dropped if

- We can't match the format (*See the list of Gluware syslog filters below*)
- If the source IP address does not match the IP address of a managed device in the organization

See also "Monitor changes with the gluWatchdog agent"

NOTES:

You can forward syslog messages to Gluware via an intermediary syslog-ng server. You may want to use syslog-ng filters to forward only the appropriate messages. *See* the syslog-ng documentation for details.

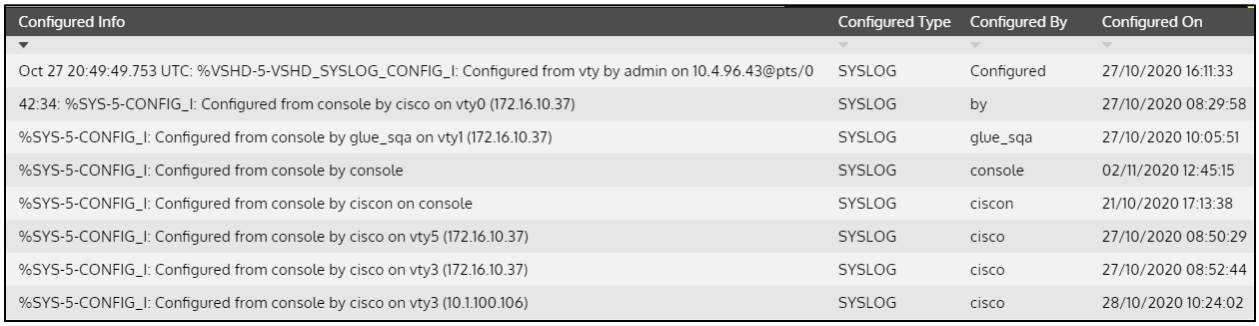
Basic example

```
# Configure syslog server to listen on the network
source s_net {
    network(
        port(514)
        transport("udp")
        flags(no-parse)
    );
};

# Configure Gluware Control as a destination
destination d_gluwareSyslogng {
        syslog-ng(
                server("<gluware control ip address")
                port(<gluware control syslog port for
organization>)
                transport("udp")
        );
};

# Configure syslog server to forward received network traffic to
Gluware Control
log { source(s_net); destination(d_gluwareSyslogng); };
```

Monitor configuration changes in the syslog

1. Ensure you're in the organization you want to monitor configuration changes in.
2. Go to **Settings** > **Organization** > **Events**.
3. Check the **Activate syslog for this organization** box. Gluware assigns the port number that the devices will use to send logs. Port numbers assigned range from 32000 to 32300. Only UDP is supported.
4. If you have **Automatic Configuration Snapshots** enabled for configuration changes monitored by syslog, enter the number of minutes to ignore duplicate syslog messages after the first message is received. Entering 0 does not ignore duplicate messages. The snapshot is taken after the wait time you enter.
5. Save.

When there are configuration changes, SYSLOG appears in the **Configured Type** column in **Device Manager**. The user who made the change, the time of the change, and the message sent are also displayed (**Configured By**, **Configured On**, and **Configured Info**).



Configured Info	Configured Type	Configured By	Configured On
Oct 27 20:49:49.753 UTC: %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by admin on 10.4.96.43@pts/0	SYSLOG	Configured	27/10/2020 16:11:33
42:34: %SYS-5-CONFIG_I: Configured from console by cisco on vty0 (172.16.10.37)	SYSLOG	by	27/10/2020 08:29:58
%SYS-5-CONFIG_I: Configured from console by glue_sqa on vty1 (172.16.10.37)	SYSLOG	glue_sqa	27/10/2020 10:05:51
%SYS-5-CONFIG_I: Configured from console by console	SYSLOG	console	02/11/2020 12:45:15
%SYS-5-CONFIG_I: Configured from console by ciscon on console	SYSLOG	ciscon	21/10/2020 17:13:38
%SYS-5-CONFIG_I: Configured from console by cisco on vty5 (172.16.10.37)	SYSLOG	cisco	27/10/2020 08:50:29
%SYS-5-CONFIG_I: Configured from console by cisco on vty3 (172.16.10.37)	SYSLOG	cisco	27/10/2020 08:52:44
%SYS-5-CONFIG_I: Configured from console by cisco on vty3 (10.1.100.106)	SYSLOG	cisco	28/10/2020 10:24:02

Configure devices for syslog monitoring

You'll need to configure each device that you want to monitor. Here are some examples.

Cisco devices

`logging host` <Gluware IP address> `transport udp port` <Gluware Org port number> `logging trap notifications`

> **NOTE:** Notifications have different levels. `notifications` is a default you can use but you may want a higher or lower level.

Example: `logging host 10.1.100.84 transport udp port 32003`

`logging source-interface` <Mgmt Interface> [vrf <mgmt vrf>]

Example: `logging source-interface FastEthernet0/0 vrf VRF-MGMT`

Juniper devices

```
host <Gluware IP address> {
any notice;
  <Gluware Org port number> ;
    source-address <Mgmt Interface>;
}
```

HPE Aruba devices

```
logging <Gluware IP address> oobm
logging <Gluware IP address> udp <Gluware Org port number>
logging facility syslog
logging severity info
logging notify running-config-change
```

Gluware syslog filters

```
filter f_changeConfigCiscoLike { match("CONFIG_I"
value("MESSAGE")); };
filter f_changeConfigCiscoASALike { match("end configuration"
value("MESSAGE")); };
filter f_changeConfigJuniper { match("UI_COMMIT"
value("MESSAGE")) and
 not match("UI_COMMIT_COMPLETE" value ("MESSAGE")) and not
match("UI_COMMIT_PROGRESS" value ("MESSAGE"));
};
filter f_changeConfigPaloAlto { match(",CONFIG,"
value("MESSAGE")) and match(",commit," value("MESSAGE")); };
filter f_changeConfigFortinet { match("action=Edit"
value("MESSAGE")); };
filter f_changeConfigHpeAruba{
  match("modified" value("MESSAGE")) or match("configuration
changed" value ("MESSAGE"));
};
filter f_rebootCisco { match("REBOOT" value("MESSAGE")) or
match("BOOTTIME" value("MESSAGE")) or
  match("RESTART" value("MESSAGE")) or match("HA_CONFIG_SYNC-6-
BULK_CFGSYNC_SUCCEED" value("MESSAGE")) or
  match("PFMA-2-BOX_ONLINE" value("MESSAGE")) or match("SYS-6-
LOGGINGHOST_STARTSTOP" value("MESSAGE"));
};
filter f_rebootJuniper { match("BOOTPD_VERSION"
value("MESSAGE")); };
```

Enable syslog logging for Gluware activities

Gluware can log user activity, device activity, and system events to a syslog server.

Enable logging

1. Go to **Settings** > **Logging**.
2. Check the **Enable Syslog** box if enabling for a child organization (not for the root or topmost organization).
3. Enter the IP address of the **Destination Host**.
4. Check the boxes for the events that you want to log. Checking the **Events** box selects all User Activity, Device Activity, and System Activity events.

Configure UDP

1. Click **Configuration**.
2. Enter the **Destination Port** number. The default for syslog is 514.
3. Click **Test Syslog Connection** to send a test message to the server. Check your syslog server to verify a message is received.
4. Click **Back**.
5. Save.

Configure TCP

1. Click **Configuration**.
2. Enter the **Destination Port** number. The default for syslog is 514.
3. Select **TCP**.
4. Enter the connection idle **Timeout** in milliseconds.
5. Click **Test Syslog Connection** to send a test message to the server.
6. Click **Back**.
7. Save.

Configure TLS

1. Click **Configuration**.
2. Enter the **Destination Port** number. The default for syslog is 6514.
3. Select **TLS**.
4. Enter the connection idle **Timeout** in milliseconds.
5. Optional: For mutual authentication,
    1. Enter the **Client TLS Key**.
    2. Paste the **Client TLS Certificate**.
6. Click **Add Certificate+**, double-click in the **Certificate** column, and paste the **Server TLS Certificate.** If issued by a certificate authority, include the entire certificate chain.
7. Check the **Skip Server Identity Check** box to accept any certificate offered to Gluware by the syslog server. If not selected, the certificate on the syslog server must match the certificate in the Server TLS Certificate field.
8. Click **Test Syslog Connection** to send a test message to the server.
9. Click **Back**.
10. Save.

Outbound syslog messages

The Gluware Solution names used in these messages are:

Config Drift
Device Explorer
Device Manager
OS Manager
Organization Settings

User activity messages

SystemName: "<SystemName>": EventCode 10101: EventCategory "User Activity": EventSubcategory "General": EventDescription "User Sign In": Username: "<Username>": ClientIp: "<IpAddress>": Message "The user named '<Username>' logged in"

SystemName: "<SystemName>": EventCode 10102: EventCategory "User Activity": EventSubcategory "General": EventDescription "User Sign In Failure": Username: "<Username>": ClientIp: "<IpAddress>": Message "The user named '<Username>' failed login"

SystemName: "<SystemName>": EventCode 10103: EventCategory "User Activity": EventSubcategory "General": EventDescription "User Sign Out": Username: "<Username>": ClientIp: "<IpAddress>": Message "The user named '<Username>' logged out"

SystemName: "<SystemName>": EventCode 10104: EventCategory "User Activity": EventSubcategory "General": EventDescription "User Logout Inactivity": Username: "<Username>": ClientIp: "<IpAddress>": Message "The user named '<Username>' was logged out due to inactivity"

SystemName: "<SystemName>": EventCode 10105: EventCategory "User Activity": EventSubcategory "General": EventDescription "Change Organization": Username: "<Username>": ClientIp: "<IpAddress>": SwitchedFromOrgName "<Org1>": SwitchedToOrgName "<Org2>": Message "The user named '<Username>' switched from org '<Org1>' to '<Org2>'"

SystemName: "<SystemName>": EventCode 10106: EventCategory "User Activity": EventSubcategory "General": EventDescription "Change Solution": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": SwitchedFromSolution "<Solution1>": SwitchedToSolution "<Solution2>": Message "The user named '<Username>' switched from the solution '<Solution1>' to '<Solution2>' in the organization '<OrgName>'"

Device activity messages

SystemName: "<SystemName>": EventCode 20101: EventCategory "Device Activity": EventSubcategory "Device Manager": EventDescription "Run Device Detection": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": TargetCount "<Count>": Message "The user named '<Username>' started device discovery for <Count> devices in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20102: EventCategory "Device Activity": EventSubcategory "Device Manager": EventDescription "Run Network Discovery": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": StartingIp "<IpAddress>": Message "The user named '<Username>' started a network discovery with a starting IP of <IpAddress> in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20103: EventCategory "Device Activity": EventSubcategory "Device Manager": EventDescription "Run Import Devices": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": TargetCount "<Count>": Message "The user named '<Username>' started the import of <Count> devices in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20104: EventCategory "Device Activity": EventSubcategory "Device Manager": EventDescription "Run Reboot Device": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": TargetCount "<Count>": Message "The user named '<Username>' started the reboot of <Count> devices in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20105: EventCategory "Device Activity": EventSubcategory "Device Manager": EventDescription "Run Ad-Hoc Query (show commands only)": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": TargetCount "<Count>": Message "The user named '<Username>' started an ad hoc query for <Count> devices in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20201: EventCategory "Device Activity": EventSubcategory "Config Drift and Audit": EventDescription "Run Audit Device": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": PolicyName "<PolicyName>": DeviceCount "<Count>": Message "The user named '<Username>' started the policy named '<PolicyName>' for <Count> devices in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20202: EventCategory "Device Activity": EventSubcategory "Config Drift and Audit": EventDescription "Run Capture Configuration": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": SnapshotName "<SnapshotName>": DeviceCount "<Count>": Message "The user named '<Username>' started a capture named '<SnapshotName>' for <Count> devices in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20301: EventCategory "Device Activity": EventSubcategory "Config Modeling - Provisioning": EventDescription "Provision Features": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": NodeName "<NodeName>": Message "The user named '<Username>' requested the provisioning of all features on the node named '<NodeName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20302: EventCategory "Device Activity": EventSubcategory "Config Modeling - Provisioning": EventDescription "Execute Custom Script": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": ScriptName "<ScriptName>": NodeName "<NodeName>": Message "The user named '<Username>' executed the script named '<ScriptName>' on the node named '<NodeName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20303: EventCategory "Device Activity": EventSubcategory "Config Modeling - Provisioning": EventDescription "Renew Certificate": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": NodeName "<NodeName>": Message "The user named '<Username>' requested a certificate renewal for the node named '<NodeName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20401: EventCategory "Device Activity": EventSubcategory "Config Modeling - OS Management": EventDescription "Transfer OS Image": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": NodeName "<NodeName>": Message "The user named '<Username>' requested a transfer of an image to the node named '<NodeName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20402: EventCategory "Device Activity": EventSubcategory "Config Modeling - OS Management": EventDescription "Upgrade OS Image and Reboot Device": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": NodeName "<NodeName>": Message "The user named '<Username>' requested an upgrade and reboot of the node named '<NodeName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20403: EventCategory "Device Activity": EventSubcategory "Config Modeling - OS Management": EventDescription "Reboot Device": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": NodeName "<NodeName>": Message "The user named '<Username>' requested the reboot of the node named '<NodeName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20501: EventCategory "Device Activity": EventSubcategory "Config Modeling - Device Agent (gluWatchdog)": EventDescription "Disable Network Interfaces": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": NodeName "<NodeName>": Message "The user named '<Username>' requested to disable the network interfaces of the node named '<NodeName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20502: EventCategory "Device Activity": EventSubcategory "Config Modeling - Device Agent (gluWatchdog)": EventDescription "Enable Network Interfaces": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": NodeName "<NodeName>": Message "The user named '<Username>' requested to enable the network interfaces of the node named '<NodeName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20503: EventCategory "Device Activity": EventSubcategory "Config Modeling - Device Agent (gluWatchdog)": EventDescription "Restore Original Configuration": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": NodeName "<NodeName>": Message "The user named '<Username>' requested to restore the original configuration of the node named '<NodeName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20601: EventCategory "Device Activity": EventSubcategory "OS Manager": EventDescription "Validate Plan": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": PlanName "<PlanName>": TargetCount "<Count>": Message "The user named '<Username>' started the validation of the plan named '<PlanName>' for <Count> devices in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20602: EventCategory "Device Activity": EventSubcategory "OS Manager": EventDescription "Deploy New Image": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": PlanName "<PlanName>": TargetCount "<Count>": Message "The user named '<Username>' started the plan named '<PlanName>' for a deployment to <Count> devices in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 20603: EventCategory "Device Activity": EventSubcategory "OS Manager": EventDescription "Transfer Image Only": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": PlanName "<PlanName>": TargetCount "<Count>": Message "The user named '<Username>' started the plan named '<PlanName>' for a file transfer to <Count> devices in the organization '<OrgName>'"

System activity messages

SystemName: "<SystemName>": EventCode 30101: EventCategory "System Activity": EventSubcategory "Settings": EventDescription "Change Global Settings": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": Message "The user named '<Username>' updated global settings in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30102: EventCategory "System Activity": EventSubcategory "Settings": EventDescription "Add Organization": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": CreatedOrg "<OrgName>": Message "The user named '<Username>' created the organization named '<OrgName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30103: EventCategory "System Activity": EventSubcategory "Settings": EventDescription "Change Organizational Settings": Username: "<Username>": ClientIp: "<IpAddress>": UpdatedOrg "<OrgName>": Message "The user named '<Username>' updated the organization named '<OrgName>'"

SystemName: "<SystemName>": EventCode 30104: EventCategory "System Activity": EventSubcategory "Settings": EventDescription "Delete Organization": Username: "<Username>": ClientIp: "<IpAddress>": DeletedOrg "<OrgName>": Message "The user named '<Username>' deleted the organization named '<OrgName>'"
SystemName: "<SystemName>": EventCode 30105: EventCategory "System Activity": EventSubcategory "Settings": EventDescription "Add User": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": CreatedUsername "<Username>": Message "The user named '<Username>' created the user named '<Username>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30106: EventCategory "System Activity": EventSubcategory "Settings": EventDescription "Change User Settings": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": UpdatedUsername "<Username>": Message "The user named '<Username>' updated the user named '<Username>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30107: EventCategory "System Activity": EventSubcategory "Settings": EventDescription "Delete User": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": DeletedUsername "<Username>": Message "The user named '<Username>' deleted the user named '<Username>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30201: EventCategory "System Activity": EventSubcategory "Solutions Manager": EventDescription "Import Package": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": CapsuleName "<CapsuleName>": Message "The user named '<Username>' started the import of the capsule named '<CapsuleName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30202: EventCategory "System Activity": EventSubcategory "Solutions Manager": EventDescription "Install Package": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": PackageName "<PackageName>": PackageVersion "<PackageVersion>": Message "The user named '<Username>' started the install of the package '<PackageName> <PackageVersion>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30301: EventCategory "System Activity": EventSubcategory "Device Manager": EventDescription "Add/Clone Device": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": DeviceName "<DeviceName>": Message "The user named '<Username>' created the device named '<DeviceName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30302: EventCategory "System Activity": EventSubcategory "Device Manager": EventDescription "Edit Device": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": DeviceName "<DeviceName>": Message "The user named '<Username>' updated the device named '<DeviceName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30303: EventCategory "System Activity": EventSubcategory "Device Manager": EventDescription "Delete Device": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": DeviceName "<DeviceName>": Message "The user named '<Username>' deleted the device named '<DeviceName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30401: EventCategory "System Activity": EventSubcategory "Config Drift and Audit": EventDescription "Set Default Snapshot": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": DeviceCount "<Count>": Message "The user named '<Username>' started the setting of the default configuration for <Count> devices in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30402: EventCategory "System Activity": EventSubcategory "Config Drift and Audit": EventDescription "Add/Clone Audit Policy": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": PolicyName "<PolicyName>": Message "The user named '<Username>' created the policy named '<PolicyName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30403: EventCategory "System Activity": EventSubcategory "Config Drift and Audit": EventDescription "Edit Audit Policy": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": PolicyName "<PolicyName>": Message "The user named '<Username>' updated the policy named '<PolicyName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30404: EventCategory "System Activity": EventSubcategory "Config Drift and Audit": EventDescription "Delete Audit Policy": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": PolicyName "<PolicyName>": Message "The user named '<Username>' deleted the policy named '<PolicyName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30501: EventCategory "System Activity": EventSubcategory "OS Manager": EventDescription "Add/Clone OS Plan": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": PlanName "<PlanName>": Message "The user named '<Username>' created the plan named '<PlanName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30502: EventCategory "System Activity": EventSubcategory "OS Manager": EventDescription "Edit OS Plan": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": PlanName "<PlanName>": Message "The user named '<Username>' updated the plan named '<PlanName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30503: EventCategory "System Activity": EventSubcategory "OS Manager": EventDescription "Delete OS Plan": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": PlanName "<PlanName>": Message "The user named '<Username>' deleted the plan named '<PlanName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30504: EventCategory "System Activity": EventSubcategory "OS Manager": EventDescription "Add/Clone Catalog": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": CatalogName "<CatalogName>": Message "The user named '<Username>' created the catalog named '<CatalogName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30505: EventCategory "System Activity": EventSubcategory "OS Manager": EventDescription "Edit Catalog": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": CatalogName "<CatalogName>": Message "The user named '<Username>' updated the catalog named '<CatalogName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30506: EventCategory "System Activity": EventSubcategory "OS Manager": EventDescription "Delete Catalog": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": CatalogName "<CatalogName>": Message "The user named '<Username>' deleted the catalog named '<CatalogName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30601: EventCategory "System Activity": EventSubcategory "Workflows": EventDescription "Run Workflow": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": WorkflowName "<WorkflowName>": JnbName "<JnibName>": NodeName "<NodeName>": Message "The user named '<Username>' the workflow named '<WorkflowName>' launched the JNIB named '<JnibName>' on the node named '<NodeName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30701: EventCategory "System Activity": EventSubcategory "Config Modeling": EventDescription "Add/Clone Instance": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": Construct "<Construct>": TypeName "<TypeName>": InstanceName "<InstanceName>": Message "The user named '<Username>' created a <Construct> of type '<TypeName>' named '<InstanceName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30702: EventCategory "System Activity": EventSubcategory "Config Modeling": EventDescription "Edit Instance": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": Construct "<Construct>": TypeName "<TypeName>": InstanceName "<InstanceName>": Message "The user named '<Username>' updated a <Construct> of type '<TypeName>' named '<InstanceName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30703: EventCategory "System Activity": EventSubcategory "Config Modeling": EventDescription "Delete Instance": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": Construct "<Construct>": TypeName "<TypeName>": InstanceName "<InstanceName>": Message "The user named '<Username>' deleted a <Construct> of type '<TypeName>' named '<InstanceName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30801: EventCategory "System Activity": EventSubcategory "File Server": EventDescription "Add File": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": FileName "<FileName>": Message "The user named '<Username>' started the upload of the file named '<FileName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30802: EventCategory "System Activity": EventSubcategory "File Server": EventDescription "Edit File": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": FileName "<FileName>": Message "The user named '<Username>' updated information about the file named '<FileName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30803: EventCategory "System Activity": EventSubcategory "File Server": EventDescription "Delete File": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": FileName "<FileName>": Message "The user named '<Username>' deleted the file named '<FileName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30901: EventCategory "System Activity": EventSubcategory "Schedules": EventDescription "Add Schedule": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": ScheduledFrom "<SolutionName>": WorkType "<TaskName>": ScheduleName "<ScheduleName>": Message "The user named '<Username>' created a <ScheduleType> schedule named '<ScheduleName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30902: EventCategory "System Activity": EventSubcategory "Schedules": EventDescription "Edit Schedule": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": ScheduledFrom "<SolutionName>": WorkType "<TaskName>": ScheduleName "<ScheduleName>": Message "The user named '<Username>' updated a <ScheduleType> schedule named '<ScheduleName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30903: EventCategory "System Activity": EventSubcategory "Schedules": EventDescription "Pausing/Resume Schedule": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": ScheduledFrom "<SolutionName>": ScheduleAction "<Paused/Resumed>": ScheduleName "<ScheduleName>": Message "The user named '<Username>' <Paused/Resumed> the schedule named '<ScheduleName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 30904: EventCategory "System Activity": EventSubcategory "Schedules": EventDescription "Delete Schedule": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": ScheduledFrom "<SolutionName>": WorkType "<TaskName>": ScheduleName "<ScheduleName>": Message "The user named '<Username>' deleted a <ScheduleType> schedule named '<ScheduleName>' in the organization '<OrgName>'"

SystemName: "<SystemName>": EventCode 31001: EventCategory "System Activity": EventSubcategory "API": EventDescription "API Access": Organization: "<OrgName>": Username: "<Username>": ClientIp: "<IpAddress>": HttpMethod "<GET>": HttpPath "<URI>": Message "The user named '<Username>' requested the Gluware API with an HTTP <GET> to '<URI>' in the organization '<OrgName>'"

Messages from the Gluware primary server

You can configure any Gluware server to send system secure messages such as SSH logins to your external syslog server using UDP or TCP. TLS is not supported.

1. Open `/var/gluware/gluware_chef_attributes.json` for editing.
2. Look for the following block in the JSON:

```
"rsyslog": {
  "protocol": "udp",
  "Port": 514,
  "server_ip": null
}
```

3. Update the "protocol", "port" and "server_ip" values to configure remote log shipping, for example:

```
"rsyslog": {
  "protocol": "[upd | tcp]",
  "Port": <syslogServerPort>,
  "server_ip": "<syslogServerIP>"
}
```

4. Reconfigure the host: `sudo gluwarectl reconfigure`

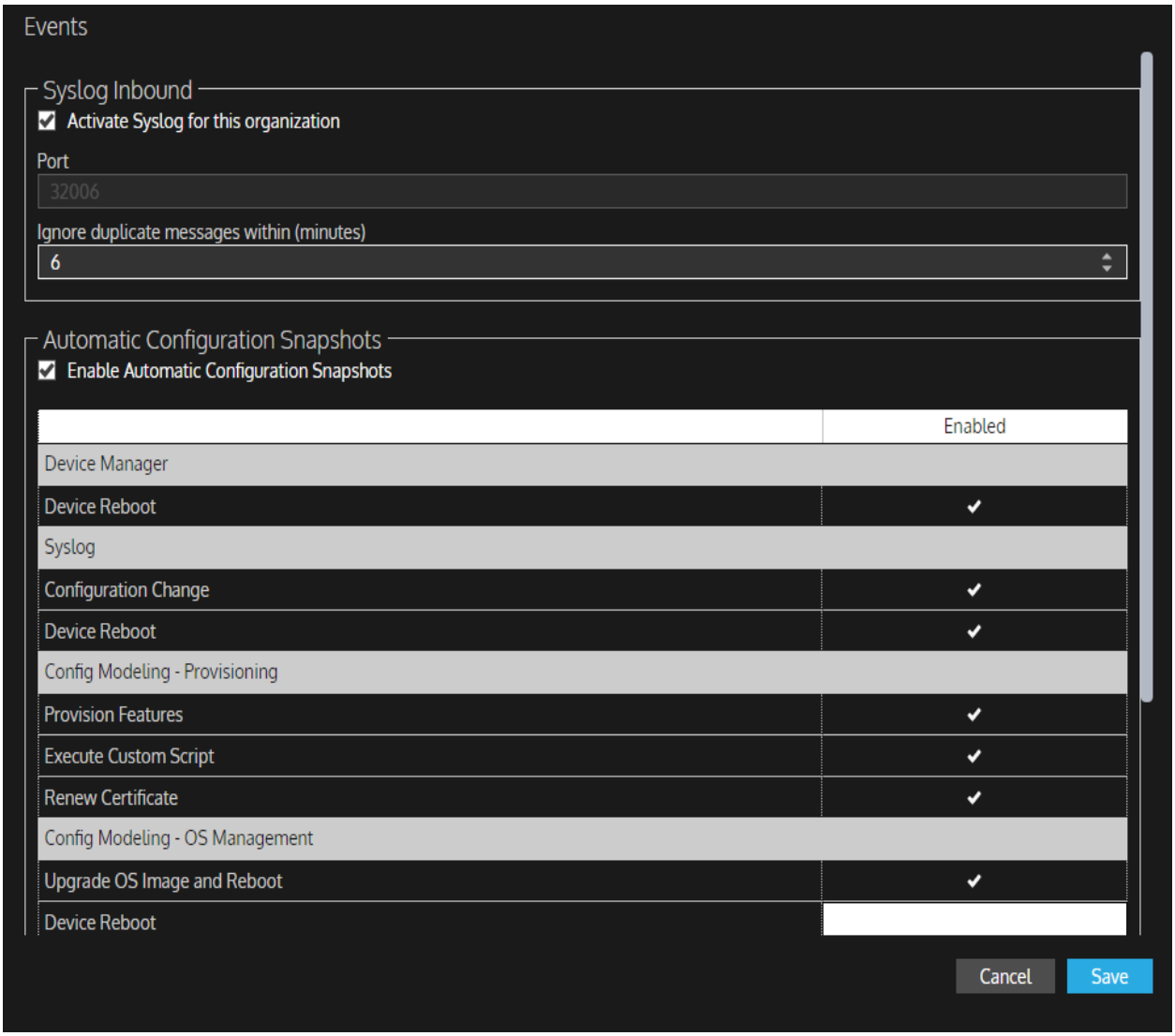
Set up automatic configuration snapshots

You can set up Gluware to take a snapshot automatically after the following actions occur:

- A change recorded in the syslog. Gluware must be set up to monitor syslog changes
- Reboot of devices in **Device Manager**, **Config Modeling**, or **OS Manager**
- Feature provision in **Config Modeling**
- Custom script execution in **Config Modeling**
- Certificate renewal in **Config Modeling**
- OS image deployment in **Config Modeling** or **OS Manager**
- Interface disabled or enabled when the gluWatchdog agent is configured
- Original configuration restoration when the gluWatchdog agent is configured

You can view the snapshots taken in **Config Audit and Drift**.

1. Go to **Settings** > **Events**.
2. Check the **Enable automatic Configuration Snapshots** box.
3. For each action you want to trigger an automatic snapshot, double-click in the Enabled column and check the box.
4. If you enable automatic snapshots for **Syslog – Configuration Change**,
    a. Ensure the **Activate Syslog for this organization** box is checked.
    b. In the **Ignore duplicate messages within (minutes)** field, enter the number of minutes to ignore syslog messages after the first message is received. The snapshot is taken after the wait time you enter. Entering 0 does not ignore duplicate messages and a snapshot is taken after each message.
5. Save.


Events
Syslog Inbound
Activate Syslog for this organization
Port
32006
Ignore duplicate messages within (minutes)
6
Automatic Configuration Snapshots
Enable Automatic Configuration Snapshots
Enabled
Device Manager
Device Reboot
Syslog
Configuration Change
Device Reboot
Config Modeling - Provisioning
Provision Features
Execute Custom Script
Renew Certificate
Config Modeling - OS Management
Upgrade OS Image and Reboot
Device Reboot
Cancel
Save

Set up Cisco API Console integration

When enabled in system settings, Device Manager can display Cisco Bulletins, Security Advisory counts, and SmartNet contract details. Updates can be performed manually or can be scheduled.

You'll first need to register Gluware under **My Applications** in the **Cisco API Console**. Select **Client Credentials** and the following API's:

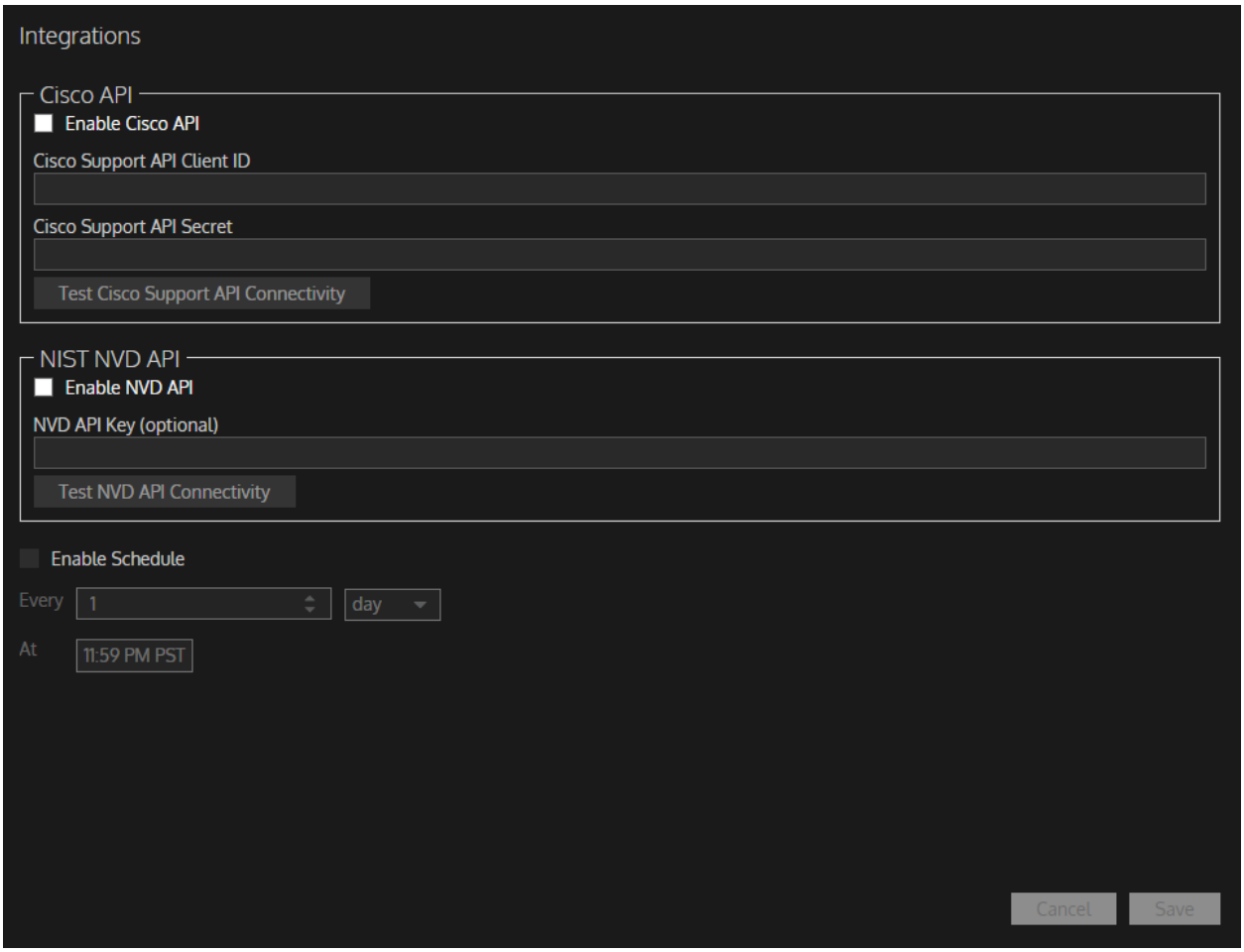
- Cisco PSIRT openVuln API
- Hello API
- Bug API 2.0
- EOX V5 API
- Product Info API 1.0
- Serial Number to Information API Version 2
- Software Suggestion API V2

When you complete the registration, you'll see the **Client Support API Client ID** and **API Secret**. You'll enter them in Gluware system settings.

Watch an overview of Cisco API Console integration
https://youtu.be/lxGV0TVMfnc

To enable Cisco API Console integration:

1. Go to **Settings** > **Organization** > **Integrations**.
2. Check the **Enable Cisco API Console** box and click **Confirm**.
3. Enter the **Client Support API Client ID** and **API Secret**.
4. Click **Test Cisco Support API Connectivity**.
5. To schedule checks for updates, check the **Enable Schedule** box and specify when to check for updates. The schedule will also apply to **NIST NVD API** updates if those are also enabled.
6. Save.


Integrations
Cisco API
Enable Cisco API
Cisco Support API Client ID
Cisco Support API Secret
Test Cisco Support API Connectivity
NIST NVD API
Enable NVD API
NVD API Key (optional)
Test NVD API Connectivity
Enable Schedule
Every
1
day
At
11:59 PM PST
Cancel
Save

Set up NIST NVD API integration

When enabled in **Settings**, **Device Manager** can display NIST (National Institute of Standards and Technology) NVD (National Vulnerability Database) Advisories. Advisories can be retrieved as needed or can be scheduled.

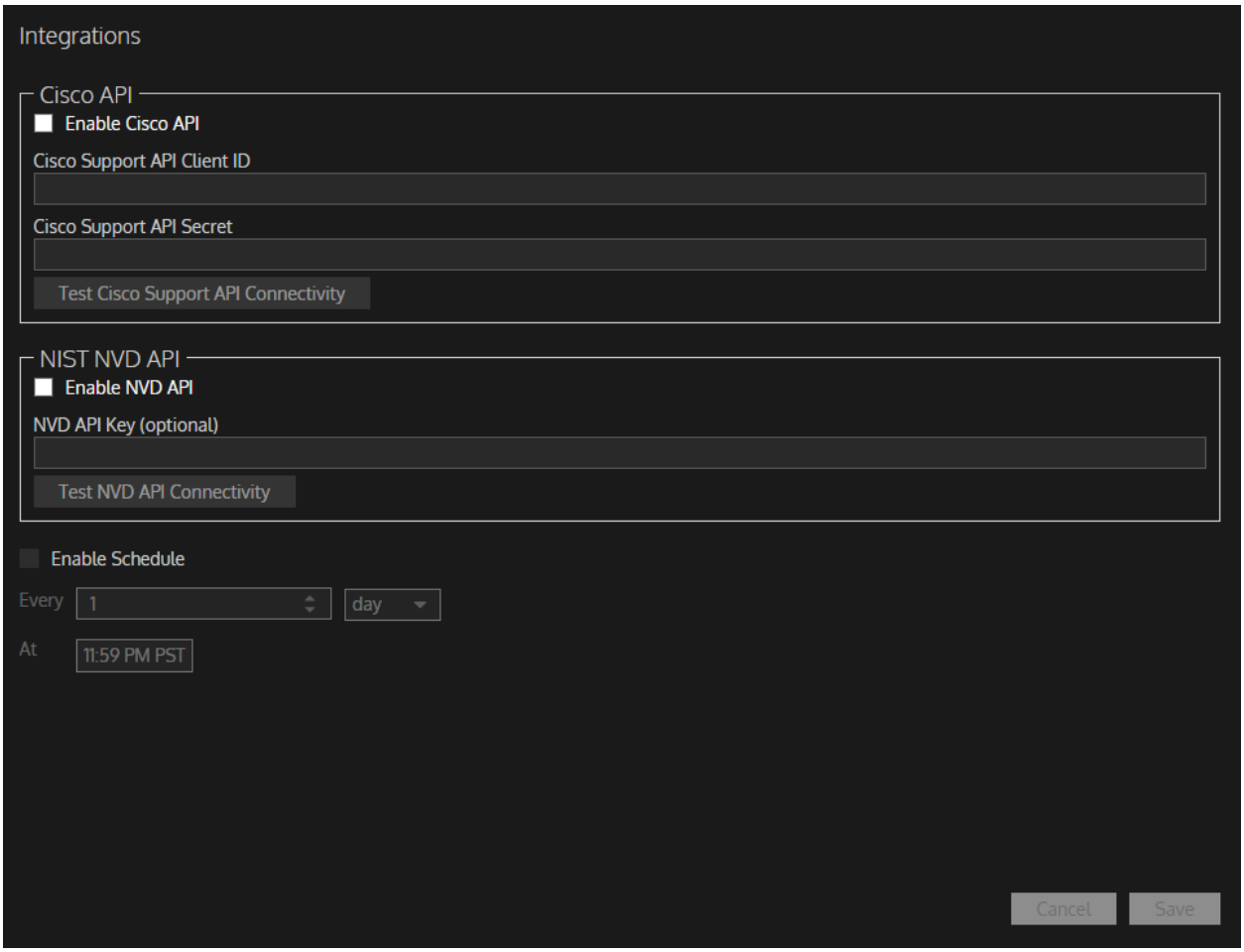
Requesting an NVD API key is optional, but it allows you to make a more API requests. Without the API key, you can make 10 requests in a minute. With the API key, you can make up to 100 requests in a minute.

Go to https://nvd.nist.gov/developers/request-an-api-key to request an API key. When you request an API key, you'll receive an email with your key.

Watch a video about NIST NVD API integration at https://youtu.be/-jHJ293gD6o

Enable NIST NVD API integration

1. Go to ⚙**Settings** > **Organization** > **Integrations**.
2. Check the **Enable NVD API** box and click **Confirm**.
3. Optional: Enter the **NIST NVD API Key**.
4. Click **Test NVD API Connectivity**.
5. To schedule requests for updates, check the **Enable Schedule** box and specify when to requests updates. The schedule will also apply to **Cisco API** updates if those are also enabled.
6. Save.


Integrations
Cisco API
Enable Cisco API
Cisco Support API Client ID
Cisco Support API Secret
Test Cisco Support API Connectivity
NIST NVD API
Enable NVD API
NVD API Key (optional)
Test NVD API Connectivity
Enable Schedule
Every
1
day
At
11:59 PM PST
Cancel
Save

Enable GluAPI integration

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

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

GluAPI documentation can be found on your system at

<*yourGluwareSystem*>`/api-docs/`

or

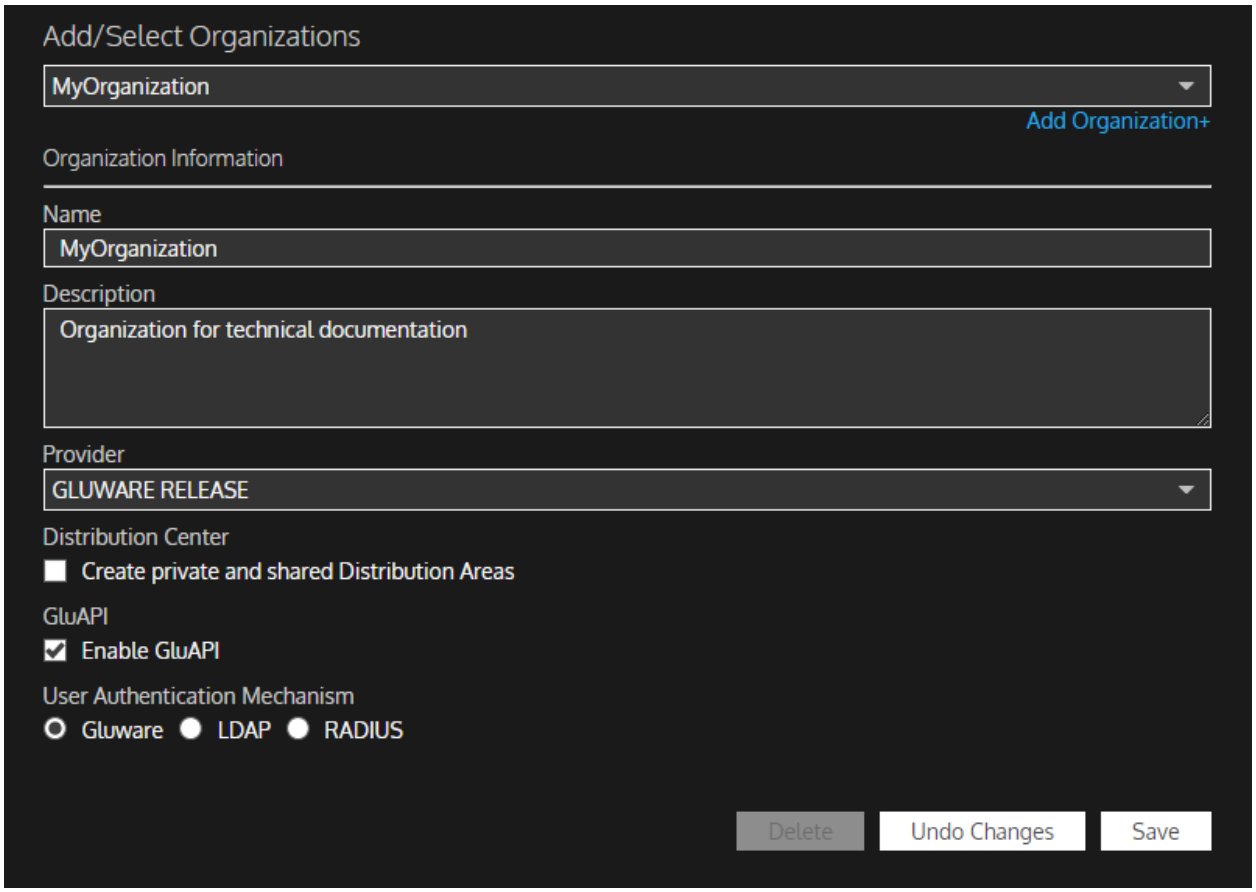
http://api-control.gluware.com/api-docs/

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 ⚙ **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**.


Add/Select Organizations
MyOrganization
Add Organization+
Organization Information
Name
MyOrganization
Description
Organization for technical documentation
Provider
GLUWARE RELEASE
Distribution Center
Create private and shared Distribution Areas
GluAPI
Enable GluAPI
User Authentication Mechanism
Gluware
LDAP
RADIUS
Delete
Undo Changes
Save

Enable/disable a File Server

Once configured, you can enable or disable a File Server any time.

1. Ensure you're in the organization in which the File Server was added.

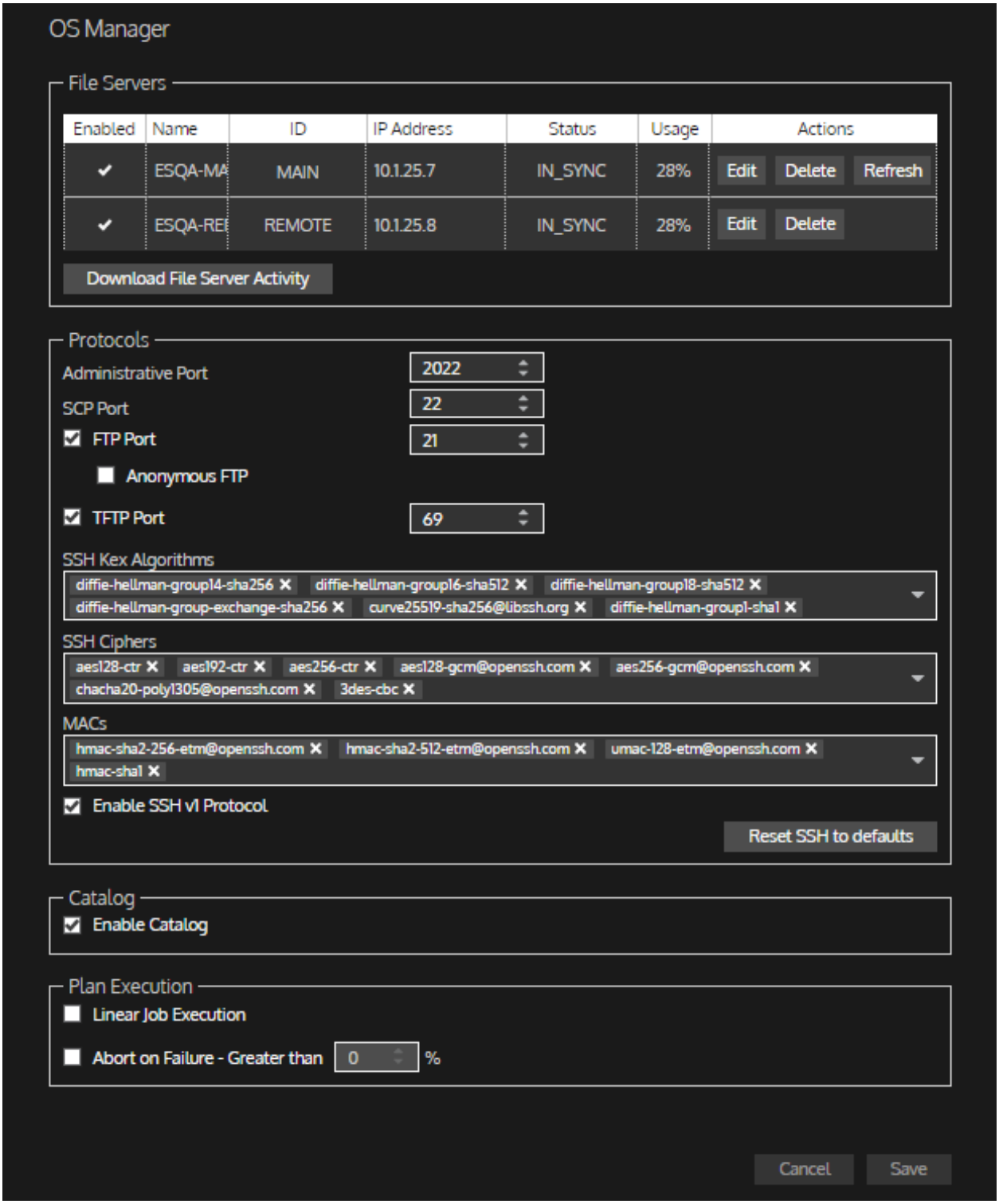
> **NOTE:** You cannot enable or disable a File Server from a child organization.

2. Go to **Settings** > **Organization** > **OS Manager**.
3. Click **Edit** beside the File Server you want to enable or disable.
4. Check or clear the **Enable File Server** box.
5. Save.

Troubleshoot a File Server

Refreshing a master File Server puts it into a configuring state, re-initializes it and its connections to any remote Files Servers, and then restarts syncing.

1. Ensure you're in the organization in which the File Server was added.
2. Go to **Settings** > **Organization** > **OS Manager**.
3. Click **Download File Server Activity**. A CSV file of the last 30 day's activity is sent to your Downloads folder.
4. Click **Refresh** beside the File Server you want to troubleshoot.
5. Click **Confirm**.


OS Manager
File Servers
Enabled
Name
ID
IP Address
Status
Usage
Actions
ESQA-MA
MAIN
10.1.25.7
IN_SYNC
28%
Edit
Delete
Refresh
ESQA-RE
REMOTE
10.1.25.8
IN_SYNC
28%
Edit
Delete
Download File Server Activity
Protocols
Administrative Port
2022
SCP Port
22
FTP Port
21
Anonymous FTP
TFTP Port
69
SSH Kex Algorithms
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group-exchange-sha256
curve25519-sha256@libssh.org
diffie-hellman-group1-sha1
SSH Ciphers
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
3des-cbc
MACs
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
hmac-sha1
Enable SSH v1 Protocol
Reset SSH to defaults
Catalog
Enable Catalog
Plan Execution
Linear Job Execution
Abort on Failure - Greater than
0
%
Cancel
Save

Modify a File Server

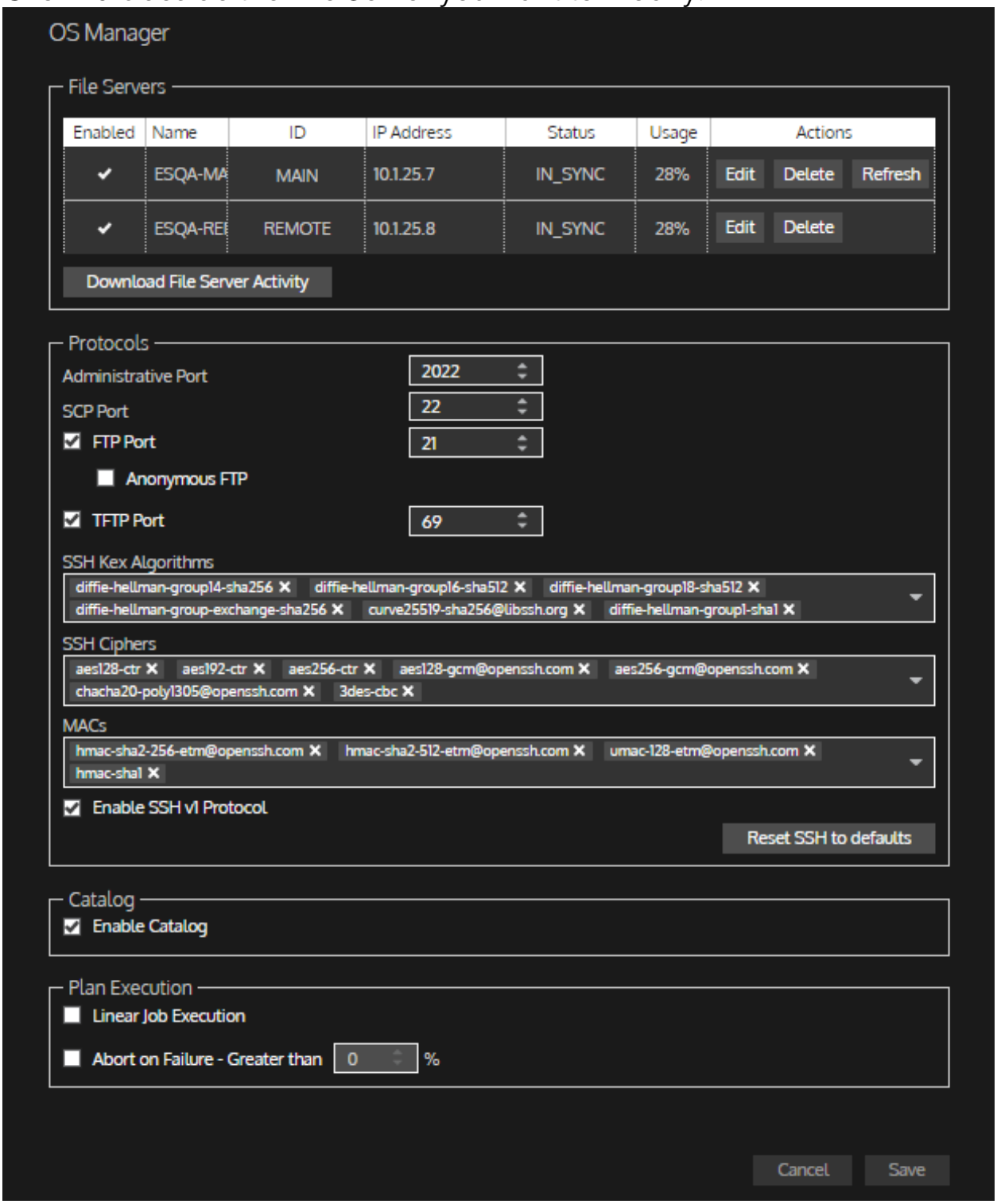
You can enable/disable a File Server, change the name, ID, and IP address. You can also enable or disable ports and change port assignments.

1. Ensure you're in the organization in which the File Server was added.

   > **NOTE:** You cannot modify a File Server from a child organization.

2. Go to **Settings** > **Organization** > **OS Manager**.

3. Click **Edit** beside the File Server you want to modify.



4. Check or clear the **Enable File Server for this Organization** box.
5. Change the name, ID, or IP address.
6. Change port assignments.

7. Check or clear the **FTP Port** box or the **TFTP Port** box to enable or disable those ports. These ports are optional.

NOTE: It takes several minutes for a port to be enabled or disabled in the backend.

8. Only if necessary: Make changes to the encryption algorithms by removing or adding algorithms in the **SSH Kex Algorithms**, **SSH Ciphers**, and **MACs** boxes. Click **Reset SSH to defaults** to return to Gluware's standards.

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

9. Check or clear the **Enable SSH v1 Protocol** box. SSH v2 Protocol is always enabled, regardless of this setting.
10. Save.
11. **If the IP address changed**:
    a. From a command shell on the File Server, run
    `sudo gluwarectl reconfigure`
    b. Return to **Settings** > **Organization** > **OS Manager**.
    c. Click **Refresh** beside the name of the File Server with the updated IP address.
    d. Click **Confirm**.

Delete a File Server

When you delete a master File Server, any Remote File Servers will also be deleted.

1. Ensure you're in the organization in which the File Server was added.

NOTE: You cannot delete a File Server from a child organization.

2. Go to **Settings** > **Organization** > **OS Manager**.
3. Click **Delete** beside the File Server you want to remove.
4. Click **Confirm**.

WARNING! If you delete a master File Server accidentally, you'll need to add the File Server again and then refresh it:

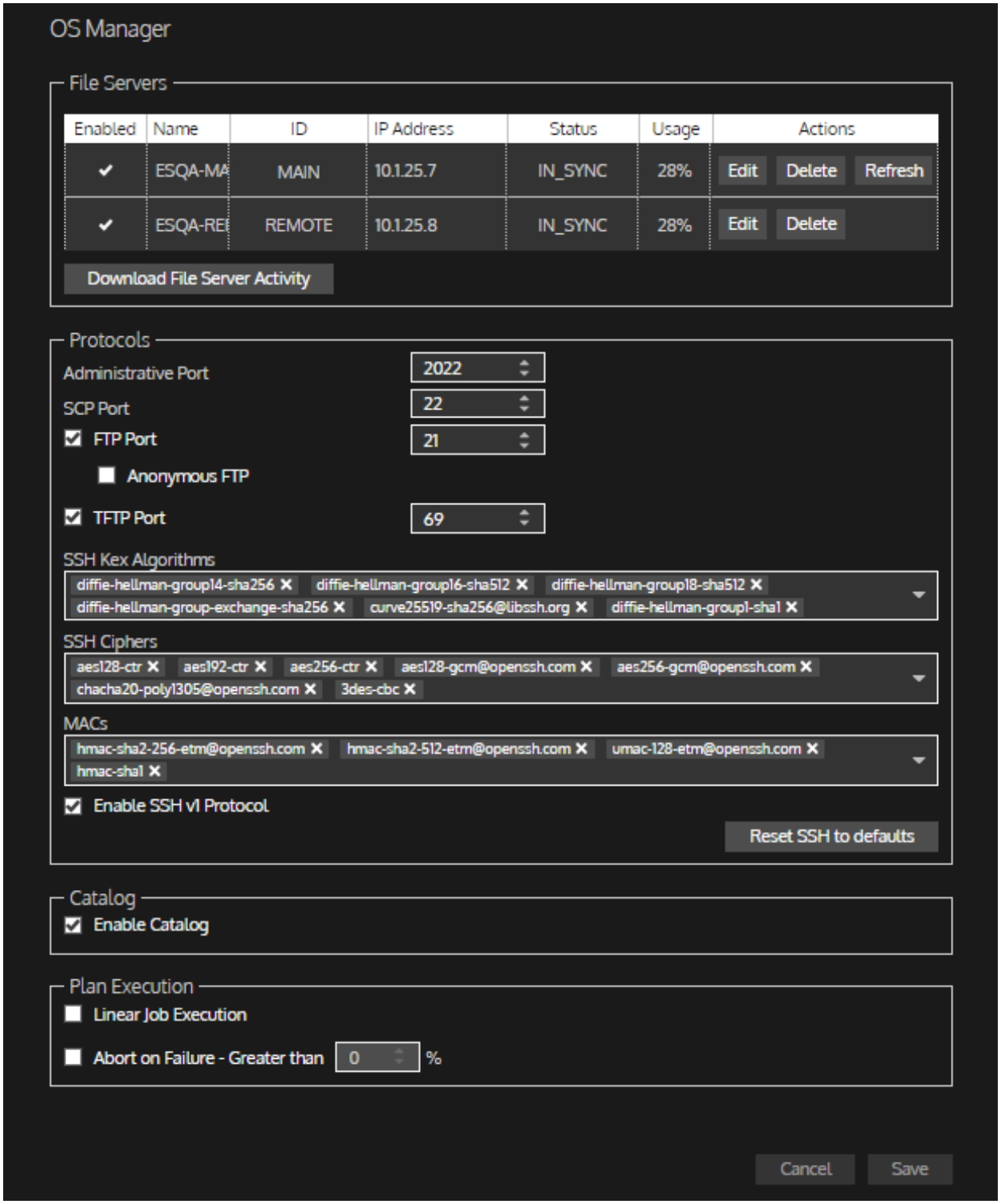
1. Ensure you're in the organization you want to add the master File Server to.
2. Go to **Settings** > **Organization** > **OS Manager**.
3. If you are adding the master File Server in a child organization, check the **Enable New Master File Server for this Organization** box.
4. Ensure the **FTP Port**, **SCP Port**, and **TFTP Port** settings are correct.
5. Click **Add File Server+**.
6. Enter a name and IP address for the server.
7. Save.
8. From a command shell on the File Server, run sudo gluwarectl reconfigure.
9. Return to **Settings** > **Organization** > **OS Manager**.
10. Click **Refresh** beside the name of the File Server.
11. Click **Confirm**.

Enable the OS Catalog

The Catalog allows you to associate files on the File Server with a SKU. This helps ensure that only the files appropriate to a device are available for deployment on that device. The use of a Catalog is optional.

Each organization must enable its own Catalog—you cannot share a Catalog with a child organization.

1. Ensure you're in the organization you want to enable the Catalog for.
2. Go to **Settings** > **Organization** > **OS Manager**.
3. Check the **Enable Catalogs** box.
4. Save.

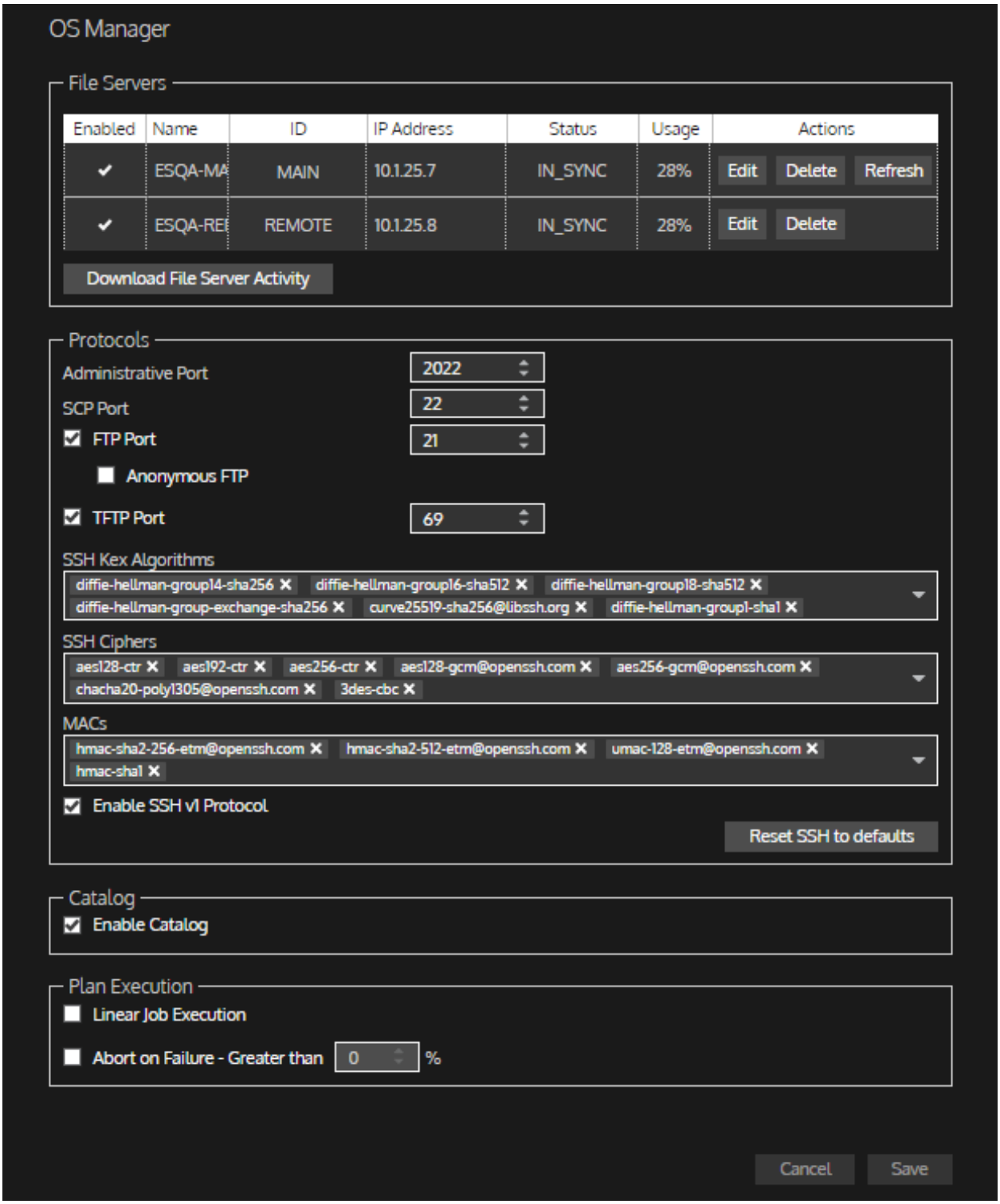

OS Manager
File Servers
Enabled
Name
ID
IP Address
Status
Usage
Actions
ESQA-MA
MAIN
10.1.25.7
IN_SYNC
28%
Edit
Delete
Refresh
ESQA-RE
REMOTE
10.1.25.8
IN_SYNC
28%
Edit
Delete
Download File Server Activity
Protocols
Administrative Port
2022
SCP Port
22
FTP Port
21
Anonymous FTP
TFTP Port
69
SSH Kex Algorithms
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group-exchange-sha256
curve25519-sha256@libssh.org
diffie-hellman-group1-sha1
SSH Ciphers
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
3des-cbc
MACs
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
hmac-sha1
Enable SSH v1 Protocol
Reset SSH to defaults
Catalog
Enable Catalog
Plan Execution
Linear Job Execution
Abort on Failure - Greater than
0
%
Cancel
Save

Set up the execution guidelines for OS plans

Upgrade plans allow you to safely upgrade specific devices. You can schedule upgrades to occur at the optimal time on as many devices as is appropriate.

Each organization must set up its own guidelines—you cannot share guidelines with a child organization.

1. Go to **Settings** > **Organization** > **OS Manager**.



2. Check the **Linear Job Execution** box if you want the devices impacted by the plan to be updated one at a time.

3. Check the **Abort on Failure** box and select a percentage of failures if you want to halt plan execution when a percentage of devices are unable to be updated.
4. Save.

Add your photo to Gluware

You can replace your initials in the Gluware title bar with a photo.

1. Got to **Settings** > **User** > **Edit My Profile**.
2. Click , select your photo file, and click **Open**.
3. Save.

External access for features and support

Using the Gluware On Prem solution can provide isolation from internet access and the related associated exposure and threats. However, there are a few maintenance implications that come from internet isolation including how to update feature packages and how to remotely troubleshoot performance issues.

With these in mind, there are three options for internet access:

- **None.** No internet access throughout the lifetime of Gluware.
- **Intermittent.** Internet access allowed only during limited time frames.
- **Persistent.** Internet access available throughout the lifetime of Gluware.

Feature packages provide the custom- and system-level control types (Feature, Domain, Global, Node, Script) as well as sample configurations that your Gluware users will use to model and configure networks. Access to install or update these packages from the Gluware Distribution Center requires outgoing access through TCP Port 443.

If you have persistent access through your firewall for traffic on this port, then you (or any system developer user of your Gluware system) can update features and sample systems to Gluware from the Gluware Distribution Center at any time.

If you have intermittent access to the internet, you will need to schedule firewall access for allowing outgoing TCP traffic on Port 443. Then you (or any system developer) can install feature packages or sample configurations using the package installer and shut down the firewall access for TCP Port 443 until you need to install or update packages again.

For no access to the internet, follow these instructions to install feature packages locally:

1. Contact Gluware, Inc. and download the supplied **capsule***[unique ID]***.zip** file to a local file system with direct access to the Gluware On Prem system.
2. Copy the supplied capsule file to the **/var/gluware/packagerepo** directory. **Example:**
   `cp capsule`*`[unique ID]`*`.zip /var/gluware/packagerepo`

Once the downloaded feature package has been copied to the **packagerepo** directory on the local On Prem system, you (or any system developer) can install the imported package using the package installer.

When you need Gluware support or troubleshooting help, if sharing logs and errors is not sufficient, scheduling a video conference with support may be necessary. To allow remote access of Gluware desktop to Support during these sessions, plan for VPN access for Support.

Gluware system services

Gluware is configured and built using Chef™, a configuration management tool used to automate the creation and configuration of systems.

There are a handful of core services and transaction types in Gluware. Some background on each will help you understand the relevance of services and logs to your Gluware system performance tuning and system maintenance activities.

Component	Description
Browser	The means by which your Gluware users will interact with Gluware once it is configured and operational
NGINX®	HTTP server used to host the Gluware Web application and to load balance all Web Socket connections and RESTful requests
WS-Eve	The Web Socket container that is used to establish internal Web Socket connections between the server (system) and the client (browser); this socket provides access to all the system functionality except for Provisioning and Provisioning Logs (*see* NIBServer)
HTTP-Eve	The HTTP container that exposes all the internal RESTful services used by Gluware to facilitate interaction with the Agent and JNIB technologies
Agent Manager	The service that communicates with the back end (Mongo, etc.) and processes requests from deployed agents running on nodes

Component	Description
NIBServer	The service responsible for managing Gluware provisioning requests, events, and logging, determining if they are previews that generate logs and CLI, or actual provisioning actions on nodes
RabbitMQ®	The service that provides a messaging queue to coordinate internal events between other Gluware processes
MongoDB®	One of two databases in the Gluware back end that is used to store the highly customizable data models defined by the developer
MySQL®	One of two databases in the Gluware back end that is used to store the relational portions of the system data and allows for ACID (Atomicity, Consistency, Isolation, Durability) reliable database transactions
RADIUS	Provides authentication services that are used for node sign-in authentication
Nodes	The network devices being managed with Gluware

Manage Gluware system services

The combination of services and logs provide your primary means of maintaining Gluware. Status and control of different services are described below.

The format for the utility is:

```
sudo gluwarectl <action> [options]
```

> **NOTE:** Action names are case insensitive; e.g., `radiusSecret` and `radiussecret` produce the same result.

Services actions

`restart [glue|all]`

Restart specified services
`glue` – Only operates on Gluware services such as WSEVE, HTTPEVE, and GluAPI (default)
`all` – All services (Eve, etc.) plus rabbitmq, mongod, mysql, radiusd, and ntpd

`start`

Start all system services

`status`

Display the status for all system services

`stop [glue|all]`

Stop specified services; default is **`glue`**
`all` is glue services (Eve, etc.) and rabbitmq, mongod, mysql, radiusd, and ntpd

Configuration and information actions

`activity`

Display current Gluware Engine job status. Provide a count of engines connected to your Gluware server and current activity by job category (*see* "Gluware engine tuning" for a description of job categories)

`configureProxy [http|https|ftp|all|disable]` <host> <port> <username> <password> <domain>

Reconfigure the proxy used to access external network resources

`configureTimezone <timezone>` or **`configtz <timezone>`**

Set the timezone for the system. Should match a value from **`timedatectl list-timezone`**

`licenseRequestInfo` or **`lic`**

Display information necessary for requesting a Gluware license

`upgradePlatform [-t] <upgrade-bundle file or URL> [bundle-path]`

Upgrade a Gluware server. Use the **`[-t]`** option to download the upgrade bundle but not run the upgrade. If using a URL, specify the optional **`[bundle-path]`** to place the downloaded bundle in that directory. By default, the bundle is downloaded to `/data/tmp`.

`radiusSecret`

Display the system RADIUS token

`reconfigure` or **`rec`**

Reconfigure the system based on the parameters set in the **gluware_chef_attributes.json** file with the option to bypass the confirmation prompt

`setInactivityTimeout` <minutes>

Set the maximum idle time to wait before a Gluware session times out; default is 20 minutes

`showEnvironment`

Display information and status for all servers connected to the Gluware Primary Server (the environment)

`Versions` or **`ver`**

Display all relevant Gluware version information

Data actions

`dataBackup [backup-path]`

Back up all Gluware databases and associated data to a backup set in directory **`[backup-path]`**. If **`[backup-path]`** is not specified, the current working directory is used.

`datarestore` <filename>

Restore the Gluware databases from a specified backup file

`resetDRData`

Resets the MongoDB replicaset data on the Disaster Recovery Server when a `dataRestore` action is performed using a backup that was created in a different Gluware environment

Data replica actions

`promoteDRServer`

Promote a Gluware Disaster Recovery Server instance from standby mode to active

OS user management actions

`addUser` <username>

Create a new system user within the glueadmin group

`deleteUser` <username>

Delete a system user that is a member of the glueadmin group

Security actions

`checkIpsecCaCert`

Check whether the CA certificate is valid. **Enter** displays the certificate text. **CTRL+C** halts the display of the text

`checkIpsecTunnelCert`

Check whether the tunnel/host certificate is valid. **Enter** displays the certificate text. **CTRL+C** halts the display of the text

`updateCert` <cert-file> <key-file>

Replace default self-signed certificate and private key with signed certificate and private key

`updateIpsecCerts` <CAcertfile> <hostcertfile> <hostcertkey>

Replace the CA certificate and host key/cert pair used for IPsec authentication. Be sure to replace the certificate on each VM

Diagnostics actions

`sysCheck` or **`sys`**

Display detailed system and service level status and health indications

`report`

Create an encrypted, compressed archive of all relevant status, logs, and configuration of the system to be sent to Gluware Support while troubleshooting

`clean`

Remove extraneous data and crash dump files

Advanced actions

`allowPing [true|false]`

Allow this system to respond to ping (ICMP) requests
`true` – Allow
`false` – Don't allow

`createDisk` **<device> <mount>**

Create and mount a new filesystem in a Gluware On Prem server
Note: To utilize createDisk you must be familiar with Linux file systems and how to create virtual drives in your hypervisor

`exportOrg [-o|-a]` **<organization-name>** **`[exclude-nodes]`**

Export data from an organization in Gluware to an encrypted data archive file that can be used to import the data to an organization on a different Gluware system, or on the same system with a different name.
`[exclude-nodes]` allows you to export organization instance data without including any node instances
`-o` – Export only instance data (default)
`-a` – Export all data

`gluwareEngineTuning` or **`get`**

Modify performance settings for the locally configured Gluware Zone Engines

importOrg [-o|-a] organization-name organization-name-in-data-archive data-archive-file

Import data from an organization in the data archive file to an organization on a Gluware system
-o – Import only instance data (default)
-a – Import all data

scheduleBackup enable <backuppath> <mailto> <minute> <hour> <day> <month> <dayofweek>

Run data backups on a scheduled basis, as opposed to running gluwarectl data backup manually (uses Linux cron syntax)
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

scheduleBackup disable

Disable a scheduled backup

unmount <mount>

Unmount the device mounted using the createDisk action

Restart Gluware services

You may need to restart services:

- After you make configuration changes
- After you run a configuration upgrade, e.g., `sudo gluwarectl reconfigure`
- When one of the services is stopped or not working. This can be determined by opening a terminal session with Gluware and typing `sudo gluwarectl status`
- When one of the services you believe to be running has stopped listening. You can determine this by opening a terminal session with Gluware and typing `nmap localhost`. This will tell you which ports are currently open. They should be the same ports that you saw the services are listening to in the previous step. For the current system these are port(s) 80, 123, 443, 22, 25, 3306, 8045, 8042, 805x

If in any of these circumstances you determine that your Gluware services need to be started or restarted, open a terminal session with Gluware and enter:

```
sudo gluwarectl [status|stop|start|restart]
```

Set the Gluware system date or time

You can use **`timedatectl`** to display or set the Gluware system date or time. The format for the utility is:

```
sudo timedatectl <action> [options]
```

timedatectl actions

`status`

Show current system clock and RTC settings

`show`

Show current system clock and RTC settings in machine readable form

`set-time` [*time*]

Set the system time in the format 2019-10-30 18:17:16

`set-timezone` [*timezone*]

Specify the system time zone

`list-timezones`

Lists the available time zones

`set-local-rtc [0|1]`

`0` – configures the Gluware system to maintain the RTC in universal time; 0 is the recommended setting.
`1` – maintains the RTC in local time and is not fully supported as it may cause problems, for example, with daylight saving adjustments
Note: This also synchronizes the RTC from the system clock unless you include the **`--adjust-system-clock`** option.

Create and mount a new file system

The **`gluwarectl createDisk`** action enables the creation and mounting of a new file system on a Gluware-based server. The intended use is to extend the capability in an On Prem system for storing data backups, upgrade packages, etc.

The **`createDisk`** action will create a single, primary XFS (Extents File System) partition on a *device* that utilizes all available space on that device (please note that the virtual disk should be sized accordingly). The partition will be made available in *mount* (e.g., the mount point).

`sudo gluwarectl createDisk <device> <mount>`

> **NOTE:** <device> is a block device that maps to a virtual disk, created in the VM host environment, and bound to the Gluware VM (e.g., added as a new disk in the settings). A disk that maps to device must first be created in the VM host environment and attached to the VM. In order to utilize **`createDisk`** you must be familiar with how to create virtual drives in your hypervisor and have familiarity with Linux file systems.

In the VMware console, edit settings for the target system and select **Add hard disk**. Configure the new virtual disk according to Gluware system needs, save settings, and start the system. Sign in as the local user and run **`lsblk`** to obtain the name of the block device that is mapped to the virtual disk

Example:

```
lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
fd0 2:0 1 4K 0 disk
sda 8:0 0 16G 0 disk
-sda1 8:1 0 8G 0 part /
-sda2 8:2 0 1K 0 part
-sda5 8:5 0 8G 0 part
-crypt--data 253:0 0 8G 0 crypt /data
sdb 8:16 0 12G 0 disk
sr0 11:0 1 1024M 0 rom
```

`sdb` in this example is shorthand for `/dev/sdb` and is the new device. Run `sudo gluwarectl createDisk /dev/sdb/mydata` where `/mydata` is the top-level directory name used to access the new file system (e.g., the mount point). Upon completion, a 12 GB partition named /dev/sdb1 will be created and mounted as `/mydata`. In addition, the new entry will be added to `/etc/fstab`.

Running `lsblk` again yields:

```
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
fd0 2:0 1 4K 0 disk
sda 8:0 0 16G 0 disk
-sda1 8:1 0 8G 0 part /
-sda2 8:2 0 1K 0 part
-sda5 8:5 0 8G 0 part
-crypt--data 253:0 0 8G 0 crypt /data
sdb 8:16 0 12G 0 disk
-sdb1 8:17 0 12G 0 part /mydata
sr0 11:0 1 1024M 0 rom
```

Change Gluware system passwords

Use standard Linux commands to change passwords in Gluware. Sign in via a terminal session as the user you created when installing Gluware and enter:

```
passwd
```

If you need further assistance, issue the `man` command.

Change Gluware system certificates

When Gluware and IPsec tunnel certificates expire or are revoked, you can replace them. The Gluware certificate is used for secure web access to the Primary Gluware system. IPsec tunnel certificates are used to establish secure connections between a Gluware Primary Server and a Gluware Disaster Recovery Server or Gluware Zone Engine. Each server in your Gluware configuration needs its own certificate; however, the same certificate on the Gluware Primary Server can be configured for the IPsec tunnel and the web server.

Requesting certificates

In order to facilitate HTTPS connections using SSL/TLS that are fully trusted by browsers, you may need to generate a certificate request to, and subsequently install a signed certificate from, your corporate Certificate Authority (CA) or related security resources in your corporate infrastructure. Contact your security team to identify and follow their existing process for getting your signed certificate.

Alternatively, a best practice is to use the OpenSSL resources on the CentOS based platform to generate a key pair, integrate it into a certificate request (which is forwarded to the appropriate corporate security resource), and then install the signed certificate that is returned by your CA in response to that request. In all the instructions below, where you see a reference to <your FQDN>, you will need to insert the actual FQDN for your Gluware system.

NOTE: The signing process must include the **server_cert** extension.

Also, if you're planning to use the IP address for the box (instead of the FQDN), then you must configure the **SubjectAltName** property and **alt_names options**.

If you're planning to use the certificate to update your IPsec tunnel certificates, then you must ensure that the FQDN, host name, and IP address for each system are listed as Subject Alternate Names. In addition, the IPsec tunnel authorization requires all peer certificates to have the **digitalSignature** or **nonRepudiation keyUsage** flags set.

If using a self-signed certificate

To generate the key pair, sign in to Gluware via a terminal session using the local user account you created. Execute the following commands:

```
mkdir ~/certs
cd ~/certs
mkdir ~/certs/private
openssl genrsa -aes256 -out private/<your FQDN>.key.pem
2048
chmod 400 private/<your FQDN>.key.pem
```

NOTE: You will be prompted to enter a passphrase to protect the key that is generated at this point.

To generate the certificate request, while still signed in to Gluware, execute the following commands:

```
cd ~/certs
openssl req -key private/<your FQDN>.key.pem -new
-sha256 -out  private/<your FQDN>.csr.pem
```

You will then be prompted for the key pair passphrase that you created in the previous step. Once the passphrase has been provided, you will be

prompted for the following information that will be used to populate the certificate request file:

`Country Name (2 letter code) [XX]`: Example - <US>
`State or Province Name (full name) [ ]`: Example - <CA>
`Locality Name (e.g., city) [Default City]`: Example - <Sacramento>
`Organization Name (e.g., company) [Default Company Ltd]`: Example - <Your Org>
`Organizational Unit Name (e.g., section) [ ]`: Example - <Your Org Unit>
`Common Name (e.g., your name or your server's hostname) [ ]`: Example - <your FQDN>
`Email Address [ ]`: Example - <yourOrg.yourCorp.com>
`Optional Attribute: An optional company name [ ]`: Example - <CompanyAlias>

Now that the certificate request has been successfully created, email the file (<your FQDN>`.csr.pem`) to your security team to complete your certificate request.

If using a PKS#12 certificate

You'll need to extract the certificate and private key from the PKS#12 file and save them in PEM format to install Gluware. You'll be prompted for the PKS#12 file password. You can encrypt the private key by removing the `-nodes` flag from the command. Add `-nocerts` or `-nokeys` to output only the private key or certificate.

Execute the following command to extract the certificate from the PKS#12 file:

`openssl pkcs12 -in INFILE.p12 -out` <certificate filename>`.crt -nodes`

Execute the following command to extract the private key from the PKS#12 file:

`openssl pkcs12 -in INFILE.p12 -out` <private key filename>`.key -nodes -nocerts`

Removing the private key password

Once you receive the signed certificate back from your security team, perform the following step.

Because the installed cert will be used by a service, you don't want the installed private key to use a passphrase. It may be useful while the files are in transit; but once it is on the system, you'll want to remove the passphrase, if it exists, by entering the following command:

```
openssl rsa -in onPrem-control.local.key.pem -out
onPrem-control.local.nocrypt.key.pem
```

This will prompt for the passphrase for the existing key file, then write it without a passphrase to a new file.

Configuring the web server to use a certificate

Now, execute the following command to import the certificate into Gluware:

`sudo gluwarectl updateCert` <certificate filename>`.crt` <private key filename>`.key`

Configuring IPsec certificates

Execute the following command on all the Gluware servers (the Gluware Primary Server, the Gluware Disaster Recovery Server, and all Gluware Zone Engines):

`sudo gluwarectl updateipseccerts` <CA-cert> <certificate filename>`.crt` <private key filename>`.key`

Change Gluware system configurations

If you change your Gluware system configuration after the initial installation, for example, after changing host name, IP address, etc., sign in via a terminal session and enter:

```
sudo gluwarectl reconfigure
```

Gluware engine tuning

The Gluware engine processes jobs requested by your Gluware server. These include Previews, Provisioning, Config Drift captures, Device discoveries, OS upgrades, and Workflows that interact with devices. In order to maximize throughput, Gluware places each job in a category (queue) based on size and expected duration and then submits the jobs to one of several message broker queues serviced by the Gluware engine. One or more Gluware engines then process requests by interacting with the message broker.

The job categories are:

Large – Jobs of long duration, such as SDWAN provisioning
Medium – These include Config Modeling provisioning
Small – Config Drift captures and Device Discovery
Extra small – Workflows
OS upgrade – All OS Upgrade requests

Each Gluware engine service uses these requests and can run multiple jobs simultaneously. Because the number of jobs running at any one time can also affect performance, each job category is assigned a prefetch value – this is the number of jobs the engine will process from any given queue at the same time.

The Gluware server runs two Gluware engines by default. More engines can be added to a Gluware server's infrastructure by installing an additional Gluware engine. Each additional Gluware engine runs two engines. The default engine settings are:

Engine 0

Job Category	Enabled/Disabled	Prefetch
Large	Enabled	10 (maximum 10)
Medium	Enabled	30 (maximum 50)
Small	Enabled	30 (maximum 50)
Extra small	Enabled	10 (maximum 50)
OS upgrade	Enabled	10 (maximum 50)
		Total = 90 (maximum 100)

Engine 1

Job Category	Enabled/Disabled	Prefetch
Large	disabled	0 (maximum 10)
Medium	Enabled	30 (maximum 50)
Small	Enabled	30 (maximum 50)
Extra small	Enabled	10 (maximum 50)
OS upgrade	Enabled	10 (maximum 50)
		Total = 80 (maximum 100)

Using the engine tuning action, you can disable engines and queues, and change the number of jobs that will run concurrently on any given queue (the prefetch value).

To change performance parameters for one or more of the locally running engines, while signed in to Gluware or your additional Gluware engine system via a terminal session, enter:

```
sudo gluwarectl gluwareEngineTuning
```

Select the engine to tune, configure the queues within the engine, and then save the engine configuration.

Performance tuning

Adding CPUs and memory to Gluware will improve its performance. For each incremental CPU that is added, another instance of the WS-Events service is spawned, increasing the capacity of Gluware to service user interactions. However, for the new WS-Eve service to be spawned and assigned to the new CPU, Gluware needs to be reconfigured. To reconfigure, sign in to your Gluware system via a terminal session and enter:

```
sudo gluwarectl reconfigure
```

Back up Gluware systems

Back up your Gluware system databases regularly as an important part of system administration. All data is backed up using the `gluwarectl databackup` command (scheduled or on demand), including:

- The entire contents of MongoDB and MySQL DB: instances, models, configurations, schedules, device job and provisioning log files, administrative data (organizations, users, licenses)
- All capsule files located in `/var/gluware/packagerepo`
- All package files managed by Gluware Engines
- Gluware platform information: `/var/gluware/gluware_chef_attributes.json`

Scheduled backup

The **`gluwarectl`** action **`scheduleBackup`** creates or modifies a scheduling task to run data backups on a regular basis.

The supported options are listed below. If either the **path** or **mailto** command line parameters are omitted, the default value will be used. We recommend the **[minute hour day month dayofweek]** options be specifically timed to minimize network performance load for other business needs.

To schedule backups

1. Ensure the local time is accurate on the Gluware Primary Server.
2. Sign in via a terminal session and enter:
   `sudo gluewarectl scheduleBackup enable` **[path mailto minute hour day month dayofweek]**

At least one of the time values must be included in the parameters. The default values are:

path (default is **/var/backup**)
mailto (default is the current user)

[minute, hour, day, month, dayofweek] – Specify at least month and *day* or dayofweek
minute (0–59)
hour (0–23)
day (1–31)
month (1–12 or jan, feb, mar, apr…)
dayofweek (0–6 where Sunday = 0; or sun, mon, tue, wed, thu, fri, sat)

Examples

Schedule a backup to run every day at 10:00 UTC:

```
gluewarectl scheduleBackup enable /mydisk/backups
fred@virtualsys.com 0 10
```

Schedule a backup to run on the 5th day of every month at 10:00 UTC:

```
gluewarectl scheduleBackup enable /mydisk/backups
fred@virtualsys.com 0 10 5
```

Schedule a backup to run on the 5th day of January at 10:00 UTC:

```
gluewarectl scheduleBackup enable /mydisk/backups
fred@virtualsys.com 0 10 5 1
```

Schedule a backup to run every Sunday of every week at 10:00 UTC:

```
gluewarectl scheduleBackup enable /mydisk/backups
fred@virtualsys.com 0 10 "" "" sun
```

Schedule a backup to run every Sunday of every week at 10:00 UTC, using the default backup location and setting email to the current user:

```
gluewarectl scheduleBackup enable "" "" 0 10 "" "" sun
```

Discontinue scheduled backups

To discontinue scheduled backups, enter:

```
gluewarectl scheduleBackup disable
```

On demand backup

To back up both MongoDB and MySQL DB, which includes both system configuration and User/Org data, sign in to your Gluware system via a terminal session and enter:

`sudo gluwarectl databackup [backup path]`

`backup path` – Use an external partition

After execution, the backup will be in have the file name <*Gluware instance name*>.<*date and time*>`.tgz`

Archive backups

Create a script to copy off and delete the backups based on company practices.

Example WINSCP script

```
# Connect
open sftp://user:password@host/ -hostkey=*
# Change remote directory
cd /home/user
# Download file to the local directory d:\
get *.tgz -delete c:\backups
# Disconnect
close
Exit
```

Save the script to the C:\Program Files (x86)\WinSCP\folder. To run the script, enter:

```
Winscp.com /ini=nul /script=downloadBackUp.txt
```

Back up Gluware VMs

Leverage your existing VM infrastructure backup procedures such as VMware Snapshots or the VMware Data Recovery application to ensure that Gluware Control VM server states are backed up.

Restore Gluware systems from a backup

To restore your backup, sign in to Gluware via a terminal session and enter the following command, followed by the fully qualified filename and path to the restore file:

```
sudo gluwarectl datarestore
```

> **NOTE:** You cannot restore the databases from a Gluware Disaster Recovery Server to the Gluware Primary Server. To utilize the data in the Disaster Recovery Server, promote the Disaster Recovery Server.

Promote the Disaster Recovery Server

If the primary Gluware server becomes unresponsive, the Gluware Disaster Recovery Server can be configured as the Gluware Primary Server.

To promote the Disaster Recovery Server to the Gluware Primary Server:

- Sign in to the Disaster Recovery Server as the system administrator and enter
  `sudo gluwarectl promoteDRServer`

Once the Disaster Recovery Server has been promoted to the Gluware Primary Server, it cannot be demoted. The former Primary Server can no longer be used.

To preserve infrastructure relationships (firewall, etc.) and support for processes like USB Provisioning,

1. Sign in to the **Gluware Disaster Recovery Server** (now the **Gluware Primary Server**).
2. Change the IP address to match the IP address that was originally used for the **Gluware Primary Server**.
3. If you have **Gluware Zone Engines** running in the same environment, sign in to each **Gluware Zone Engine** as the system administrator and enter
   `sudo gluwarectl reconfigure`
4. If you have **Gluware file servers** running in the same environment, sign in to each **file server** as the system administrator and enter
   `sudo gluwarectl reconfigure`
5. On the new **Gluware Primary Server**, enter
   `sudo gluwarectl reconfigure`
   All existing configurations that existed for the original **Primary Server** VM are preserved.

To re-establish a Disaster Recovery Server, re-install the Gluware VM image and configure it as a Disaster Recovery instance.

Purge data

1. Go to **Settings** > **Organization** > **Data Retention**.
2. Ensure you are in the organization you want to purge the data for.
3. Optional: Double-click the **Archive** cell and check the box to create an archive file for the data. If **Archive** is not selected, the data will be purged.
4. Click **Run Now** next to the data you want to purge or click **Run All Now** to purge all the data.

System reports

When you need to troubleshoot your Gluware system with Gluware Support, sign in to Gluware via a terminal session and enter:

```
sudo gluwarectl report
```

This creates an encrypted, compressed archive file including all the relevant log and configuration files in the folder you run the utility from. Send this report to Gluware Support (support@gluware.com) to facilitate troubleshooting.

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" for guidance.

Upgrade Gluware from v4.1.x

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 Gluware Zone Engines and File 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.**

Extend a virtual drive

To extend the virtual drive for `/data`:

1. From vCenter, shut down the VM.
2. Remove any snapshots.
3. Increase the size of Hard disk 1.
4. Start the VM.
5. Sign in to the Gluware system via a terminal session using the system administrator local user account credentials.
6. Run **`sudo gluwarectl reconfigure`**.
7. Optional: Depending on your policy, ask the vCenter administrator to take a snapshot of the VM.

NOTES: `/data` will use the size of Hard disk 1 minus 16 GB. Gluware doesn't support multiple drives.

2020 L Street, Suite 130
Sacramento, CA 95811

www.gluware.com

© 2020 Gluware, Inc. All rights reserved.