System administrator (traditional)

System administrators are in charge of the following tasks.

- Logging in to the application server operating system and Jama Connect as root user
- Installing, updating, and maintaining the Jama Connect platform
- Setting up the database and application servers
- Installing the admin console and Jama Connect
- Configure settings such as authentication and mail servers
- Regular maintenance such as updates and uploading custom reports

Ideally a system administrator has expertise in these areas of administration:

- **Database**
  System administrators set up and administer the database including database sizing, resource allocation, recommended backups, and availability of the database engine.
- **Linux**
  Jama Connect must be installed on a Linux based system. System administrators need to use Command Line Interface (CLI) for basic navigation, file manipulation, permissions, and network configuration when they are installing, upgrading, allocating resources, and maintaining availability and security of the server.
- **Directory server**
  If you're not using Jama Connect native authentication, system administrators must perform setup and administration or your organization's supported directory server [27].
- **Mail server**
  If you're using these functions in Jama Connect, system administrators perform setup and administration of your organization's mail server.

System administration are necessary for customers who are self-hosting Jama Connect. For cloud customers, Jama Software manages system administration. If you're interested in an implementation that doesn't require system administration at your organization, contact your sales representative regarding our cloud solution.

Configuring the Admin Console settings (traditional)

Jama Connect uses Replicated technology to deliver all microservices to self-hosted customers. Replicated software is a container orchestration tool that provides the interface, **Admin Console**, for Jama Connect.

Replicated and Jama Connect are hosted on the same application server, running on different ports.

The Admin Console stores settings, such as SSL certificates and database connection information, that Jama Connect uses to start and run correctly. Some of its functions include:

- Manage the run state of Jama Connect
- Perform upgrades
- Synchronize license renewals

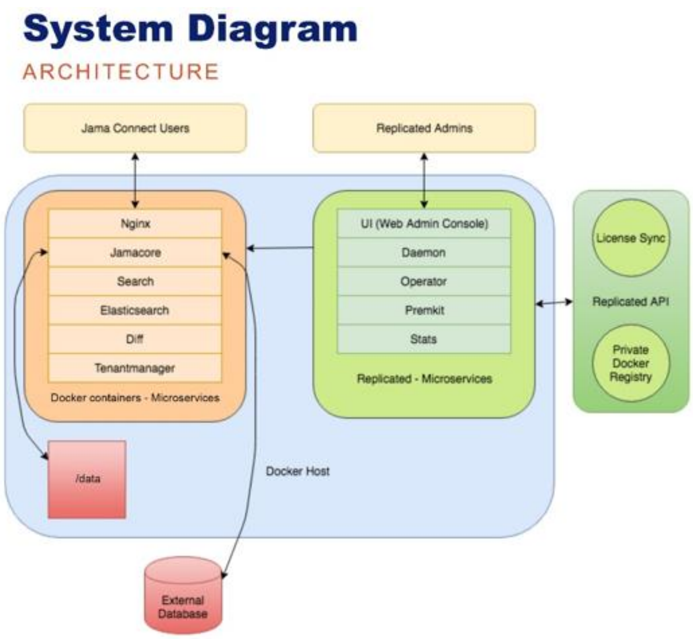
Many of the settings for the Admin Console are configured during installation. However, you can make changes to the settings whenever you need.

Application server overview

Your application server hosts the Jama Connect application, Docker containers, and the Admin Console (Replicated software). It also stores data such as attachments, images, reports, and a micro-service cache.

Docker containers — A standalone executable package of software that includes code, runtime, system tools, system libraries, and settings. See https://www.docker.com/resources/what-container for details.

Replicated — A container-based platform for easily deploying cloud native applications inside customers' environments to provide greater security and control. The Admin Console is the user interface for installing the Jama Connect application. See https://www.replicated.com/ for details.



- Jama Connect users access Jama Connect by browsing to the instance URL (https://jamainstanceurl.customer.com/).
- System administrators access the Admin Console by browsing to the same instance URL, but on port 8800 (https://jamainstanceurl.customer.com:8800/).
- Replicated updates Jama Connect and the license via API calls for internet-enabled environments. Our airgap option removes the need for remote API calls.
- Any content added to your Jama Connect instance is stored in the database. Uploaded artifacts are stored in the file system in the /data directory.

Restart the Admin Console (traditional)

Occasionally, you might need to restart the Admin Console. For example, when you need to sync a new license.

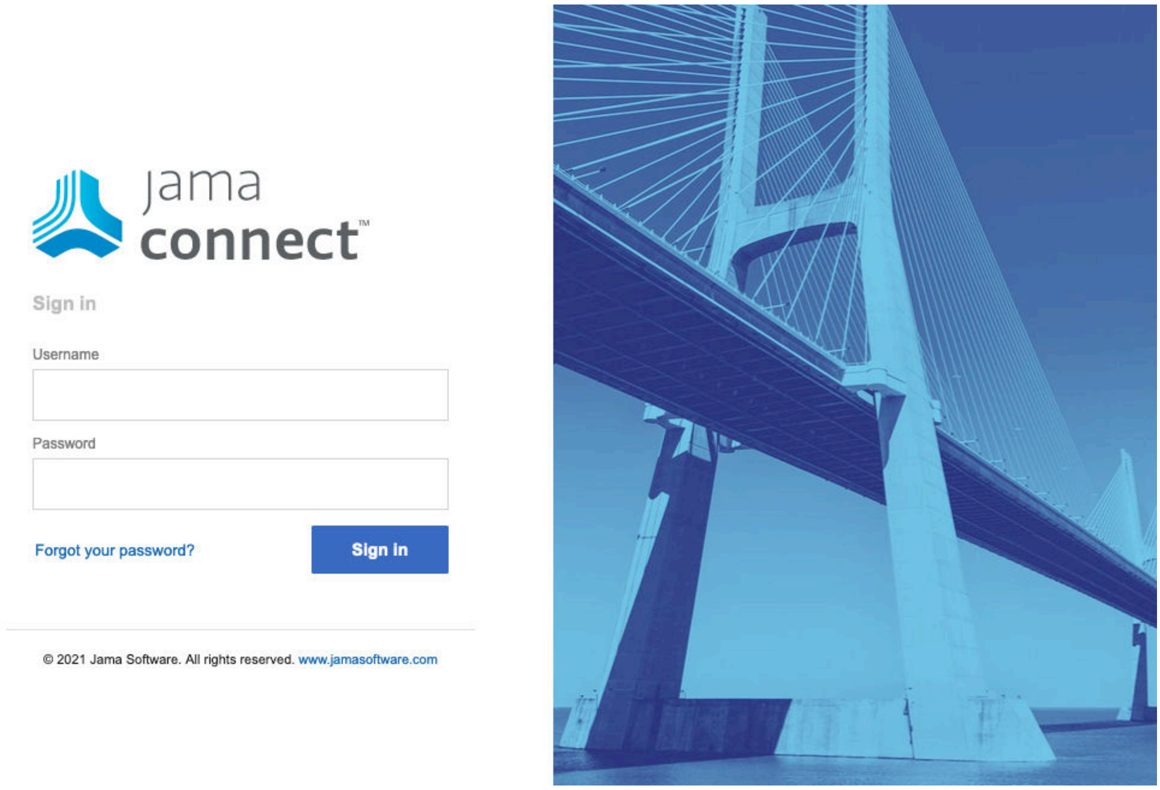
The commands to restart the Admin Console depend on the flavor of Linux you're using.

1. To restart the Admin Console on **Debian** or **Ubuntu** systems, execute these commands:

   ```
   sudo service replicated restart
   sudo service replicated-ui restart
   sudo service replicated-operator restart
   ```
2. To restart the Admin Console on **CentOS**, **RHEL**, or **Fedora** systems, execute these commands:

   ```
   sudo systemctl restart replicated replicated-ui replicated-operator
   ```

Once restarted, the Admin Console displays the login page.


jama
connect™
Sign in
Username
Password
Forgot your password?
Sign in
© 2021 Jama Software. All rights reserved. www.jamasoftware.com

Create a Replicated snapshot (traditional)

A Replicated snapshot is a backup of the Admin Console environment. It includes the Replicated database, registry images, and container volumes (when specified).

A Replicated snapshot can be taken while Jama Connect is running without interruption.

> **IMPORTANT**
>
> Replicated snapshots don't include the contents of the Jama Connect database, the contents of the /data directory, or the log files. To back up those items, see Back up to .jama or XML file [46].

When to create a snapshot

- When migrating Jama Connect to new hardware [62]. When you replace one server with another (create a clone), you can perform a fresh installation of Docker and Replicated, then restore from the snapshot.
- During disaster recovery.
- Before upgrading your software (Jama Connect or Replicated).

Snapshot location

By default, Replicated snapshots are stored in this location:

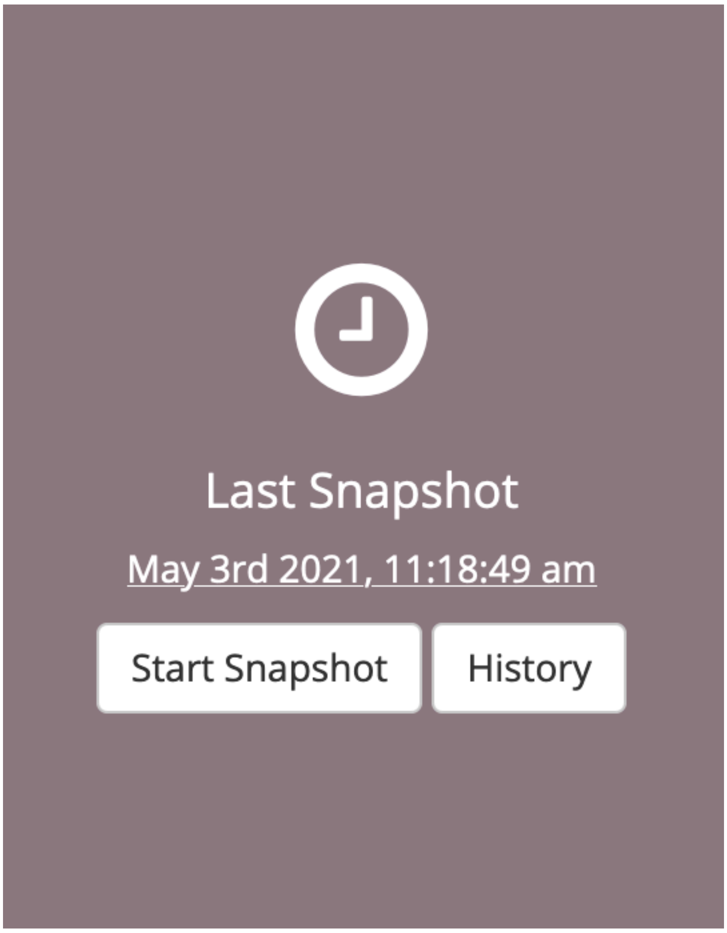
```
/var/lib/replicated/snapshots
```

To include the Replicated snapshots in your regular backups of Jama Connect, you can change the location for the snapshots, like this:

```
/data/replicated/snapshots
```

To create a Replicated snapshot:

1. (Optional) Identify and configure a custom directory for your snapshots: Select **Admin Console > Settings** (gear icon) **> Console Settings > Snapshots**.
2. Create a snapshot: Open the Admin Console and select **Start Snapshot**.
   Snapshots Enabled changes to **Snapshotting** and a progress spinner appears while it backs up the registry data and container volumes. When the snapshot is ready, you see a timestamp for the last snapshot.



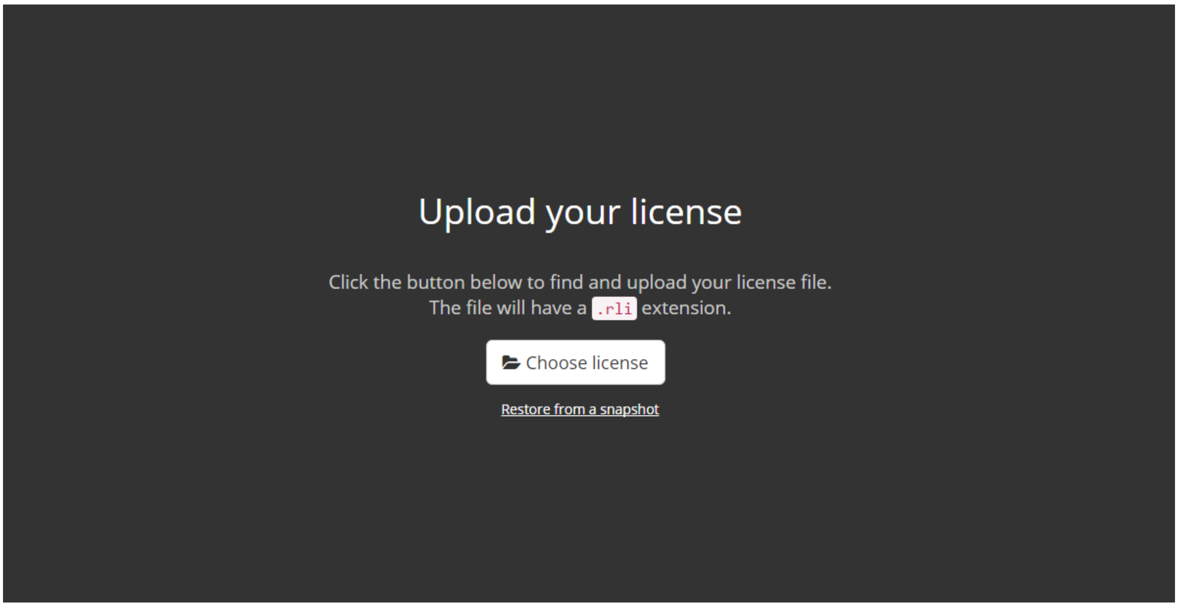
If the Replicated snapshot fails, the dashboard displays an error message with technical detail of the failure, including the file or folder involved. This error message is generated from the underlying file system (for example, readdirent: errno 523), which means the problem is likely with the underlying file system and not the Jama Connect installation.

Restore all settings from a Replicated snapshot (traditional)

When you set up a new application server for Jama Connect, you can restore the Admin Console settings that you saved in a Replicated snapshot.

Snapshots include the Replicated database, registry images, and container volumes (when specified).

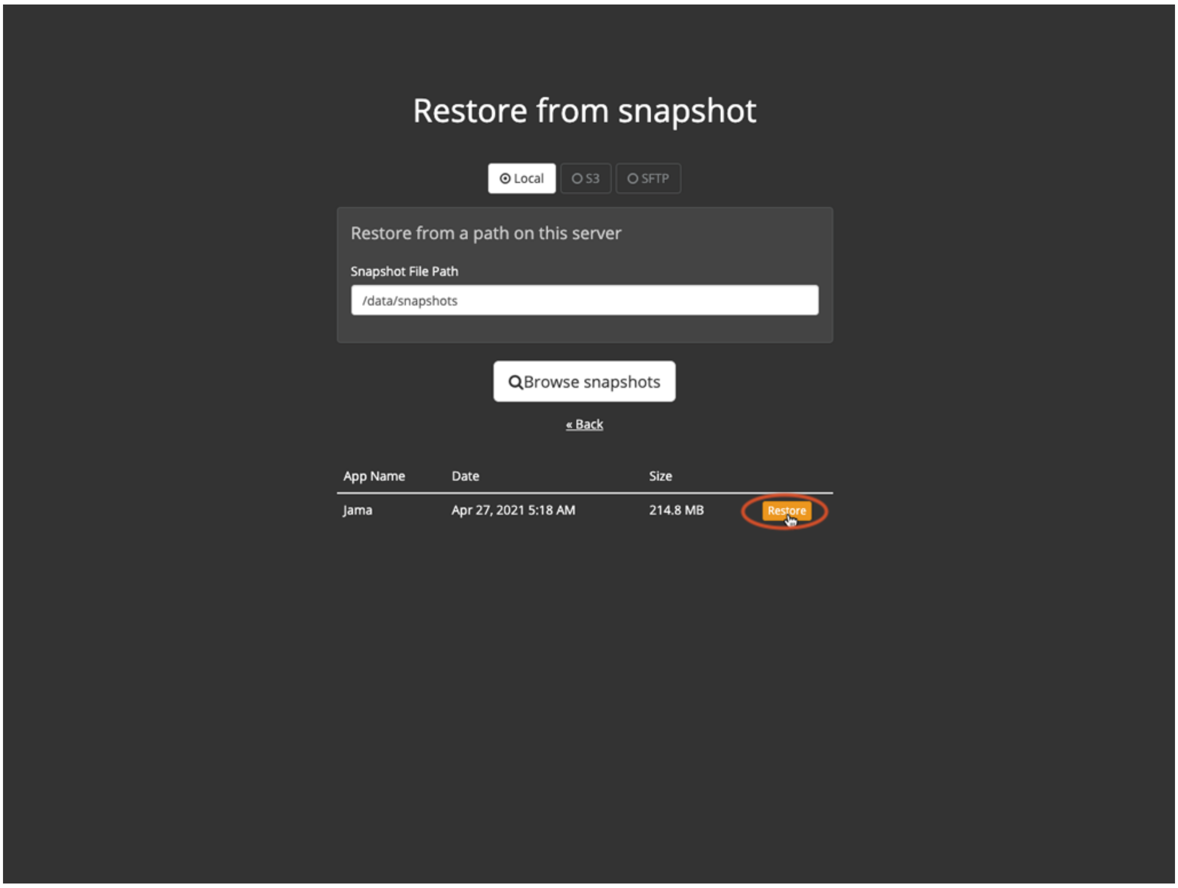
1. Install Jama Connect on the new server.
2. When the page Upload your license is displayed, select **Restore from a snapshot**.



Upload your license

Click the button below to find and upload your license file.
The file will have a `.rli` extension.

3. When the Restore from snapshot page is displayed, enter the path to your snapshot and click **Restore**.
   Use the same path on the new server as you did on the old server. For example, **/var/lib/replicated/snapshots** or **/data/snapshots**.



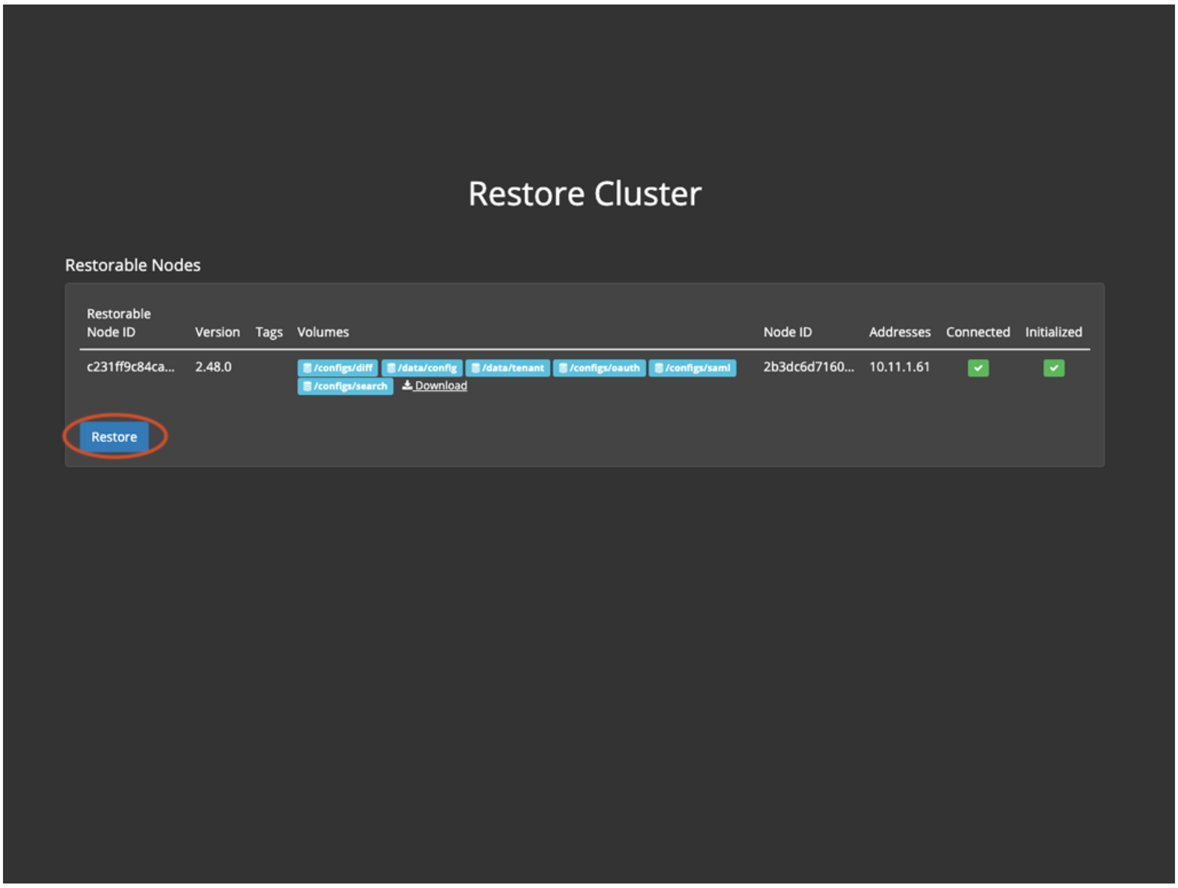
Restore from snapshot

Restore from a path on this server

Snapshot File Path: /data/snapshots

App Name	Date	Size	
Jama	Apr 27, 2021 5:18 AM	214.8 MB	Restore

4. On the Restore Cluster page, click **Restore**.

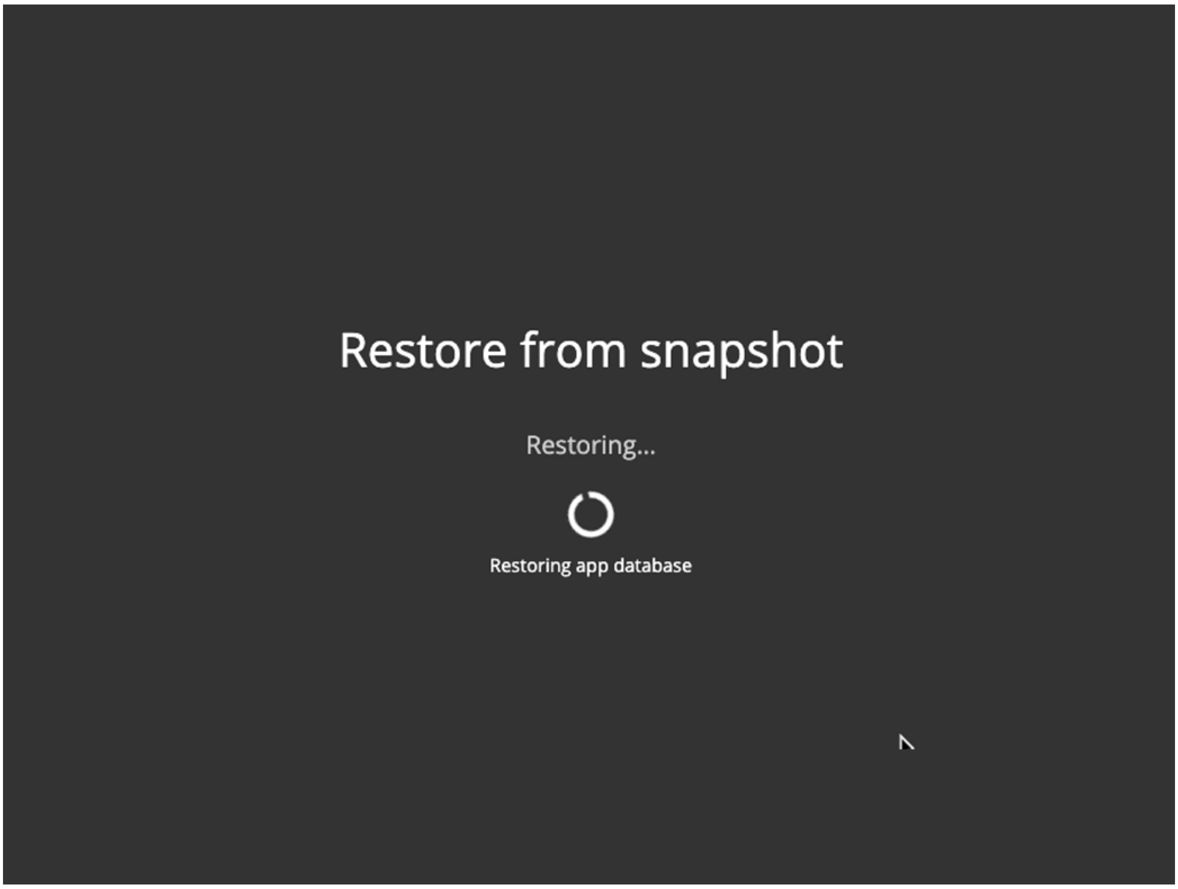


Restore Cluster

Restorable Nodes

Restorable Node ID	Version	Tags	Volumes	Node ID	Addresses	Connected	Initialized
c231ff9c84ca...	2.48.0		/configs/diff /data/config /data/tenant /configs/oauth /configs/saml /configs/search Download	2b3dc6d7160...	10.11.1.61	✓	✓

The system displays a progress page as it restores your data from the snapshot.



Restore from snapshot

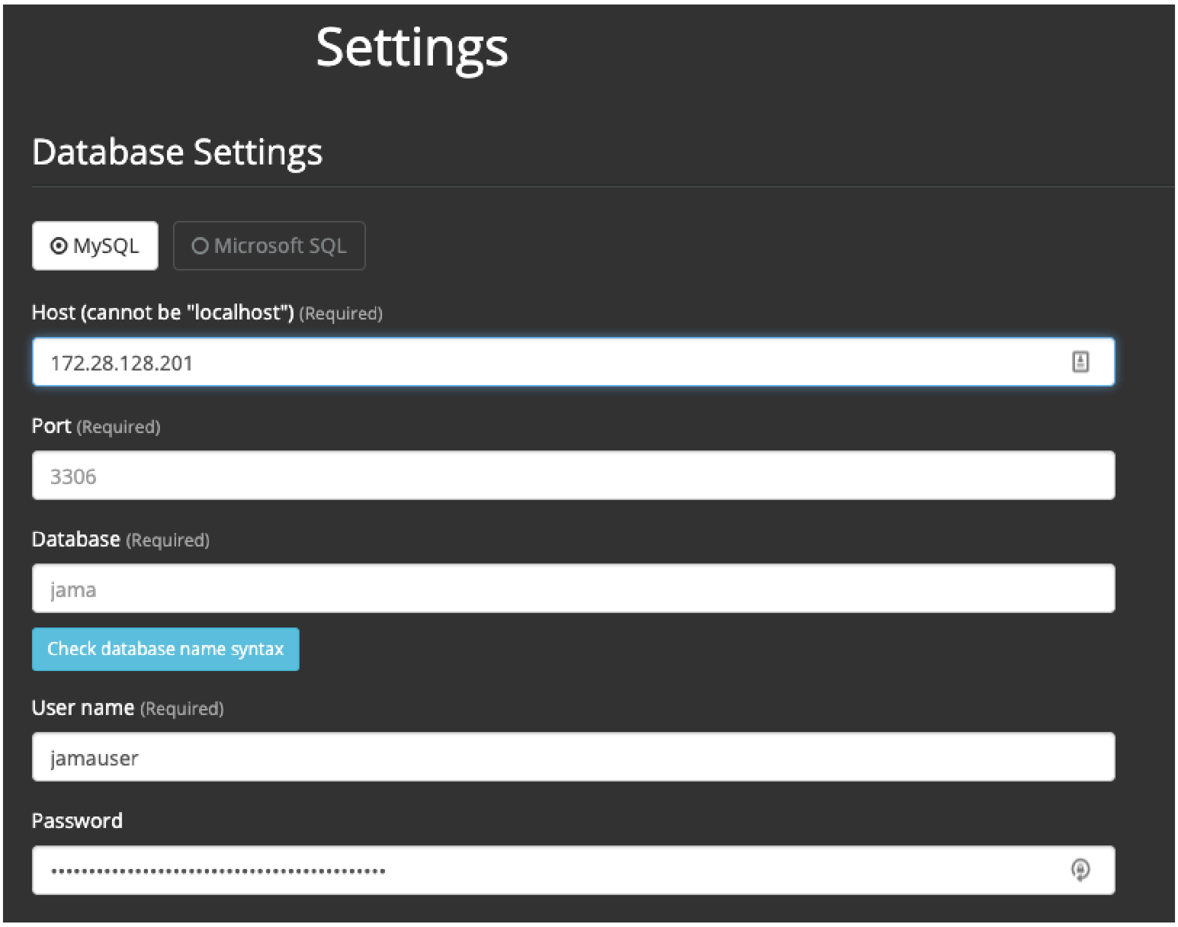
Restoring...

Restoring app database

Configure database settings (traditional)

Database settings can be configured as part of your initial installation of Jama Connect or any time you need to make changes.

1. In the header of the Admin Console, select **Settings** to open the Settings page.
2. Scroll to the **Database Settings** section of the page.



Settings

Database Settings

● MySQL ○ Microsoft SQL

Host (cannot be "localhost") (Required)

172.28.128.201

Port (Required)

3306

Database (Required)

jama

User name (Required)

jamauser

Password

••

3. Select the type of database you're using, MySQL or Microsoft SQL, then complete or change the database settings as needed.
4. (Optional) If you need to connect to your database through an SSL-encrypted connection, provide additional connection string parameters. These parameters specify key/value pairs in the format appropriate to your database.
   - **MySQL**

     ```
     useSSL=true&requireSSL=tru
     ```
   - **SQL Server**

     ```
     ssl=require;appName=jama;bufferMinPackets
     ```

     More options are available for MySQL and SQL Server
5. Scroll to the bottom of the page and click **Save**. A message confirms that your settings were saved.
6. To apply settings, you must restart the application:
   - Immediately — Select **Restart now**.
   - Later — Select **Cancel** and **Restart later**.

Configure web server settings (traditional)

Web server settings can be configured as part of your initial installation of Jama Connect or any time you need to make changes.

The web server configuration allows the use of SSL (TLS) or plain text connections.

1. In the header of the Admin Console, select **Settings** to open the Settings page.
2. Scroll down to the **Web Server** section of the page.
3. Enter the context path for Jama Connect, for example, https://<hostname>. Don't use this configuration unless you need to specify a sub-path or sub-directory.
4. (Optional) Select **Check context path syntax**.
5. (Optional) Set the TLS and plain text port as needed.
6. Scroll to the bottom of the page and click **Save**. A message confirms that your settings were saved.
7. To apply settings, you must restart the application:
   - Immediately — select **Restart now**.
   - Later — Select **Cancel** and **Restart later**.

Configure host name (traditional)

Your Host Name settings can be configured as part of your initial installation of Jama Connect or any time you need to make changes.

If possible, choose a host name that's meaningful to users. Be sure the domain name matches your TLS certificate.

If you need to change this host name, you must also change the base URL [55].

1. In the header of the Admin Console, select **Settings** to open the Settings page.
2. Scroll down to the **Host Name** section of the page.
3. Enter or change the host name.
4. (Recommended) Select **Reuse admin console TLS configuration** to use the same certificate configured in the Admin Console.
5. Scroll to the bottom of the page and click **Save**. A message confirms that your settings were saved.
6. To apply settings, you must restart the application:
   - Immediately — Select **Restart now**.
   - Later — Select **Cancel** and **Restart later**.

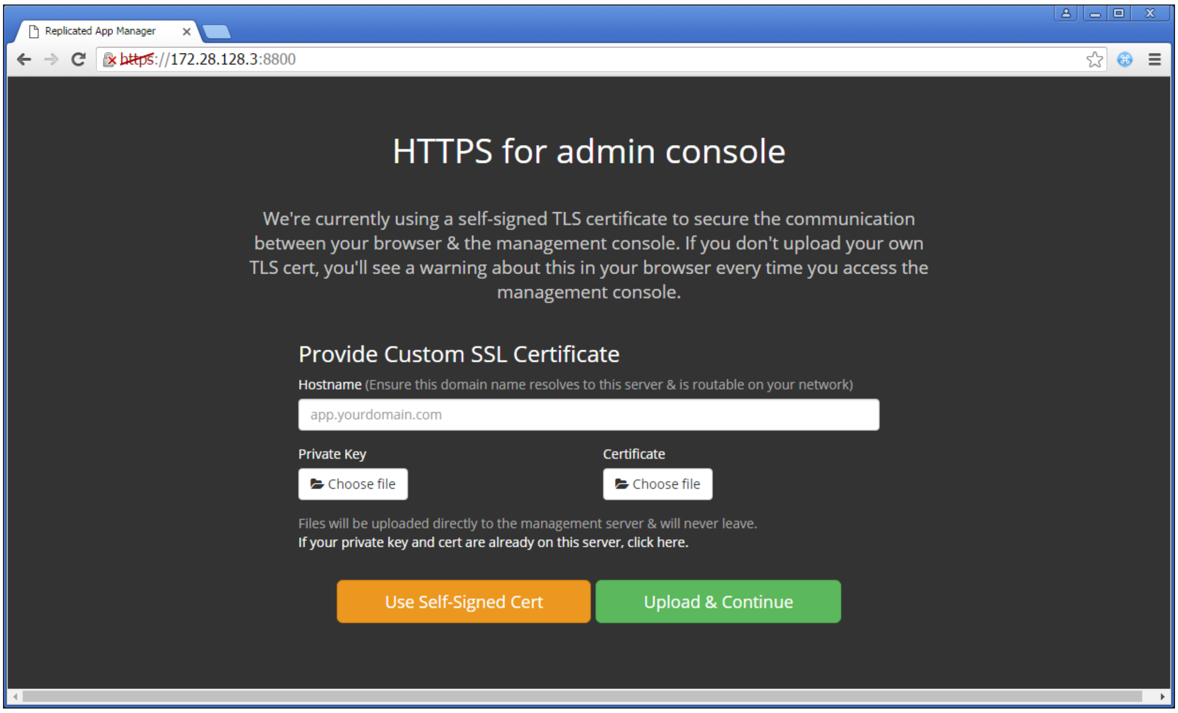
Bypass browser TLS warning (traditional)

A Transport Layer Security (TLS) or Secure Sockets Layer (SSL) certificate is required to establish a link between the Admin Console (Replicated) and your browser.

When configuring the Admin Console for the first time, you see a TLS warning with an option to bypass it with a self-signed certificate. If you have a trusted certificate, you can configure the certificate at any time [9]. If you continue with the self-signed certificate, you see a warning every time you access the Admin Console.

You can upload a TLS certificate and provide a private key if you have one. Private keys can't be password-protected. The key and primary certificate must be in PEM format, that's a base64 encoded x509 certificate.

1. In the header of the Admin Console, select **Settings** to open the Settings page.
2. Scroll down to the **Bypass Browser TLS Warning** section of the page.
3. Click **Continue to Setup** to upload a TLS certificate.



HTTPS for admin console

We're currently using a self-signed TLS certificate to secure the communication between your browser & the management console. If you don't upload your own TLS cert, you'll see a warning about this in your browser every time you access the management console.

Provide Custom SSL Certificate

Hostname (Ensure this domain name resolves to this server & is routable on your network)

app.yourdomain.com

Private Key

Choose file

Certificate

Choose file

Files will be uploaded directly to the management server & will never leave.
If your private key and cert are already on this server, click here.

Use Self-Signed Cert | Upload & Continue

4. Click **Choose file** to select the key and certificate, then click **Upload & Continue**.
5. Scroll to the bottom of the page and click **Save**. A message confirms that your settings were saved.
6. To apply settings, you must restart the application:
   - Immediately — Select **Restart now**.
   - Later — Select **Cancel** and **Restart later**.

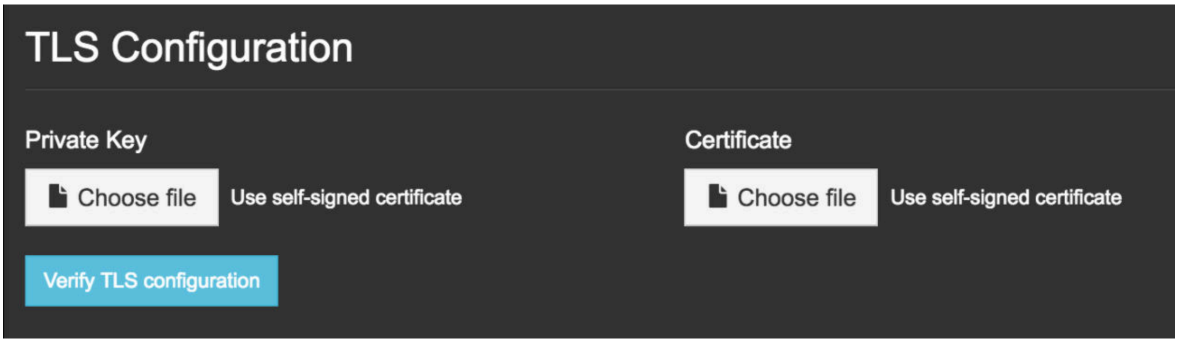
Configure TLS certificate (traditional)

The settings for the TLS certificate can be configured as part of your initial installation of Jama Connect or any time you need to make changes.

You can provide custom private key and TLS certificates to secure the application, or you can reuse the Admin Console certificate. You can also update your certificate [54] if it expires.

The certificate ensures that Jama Connect trusts the issuer.

1. In the header of the Admin Console, select **Settings** to open the Settings page.
2. Scroll down to the **TLS Configuration** section of the page.



TLS Configuration

Private Key

Choose file Use self-signed certificate

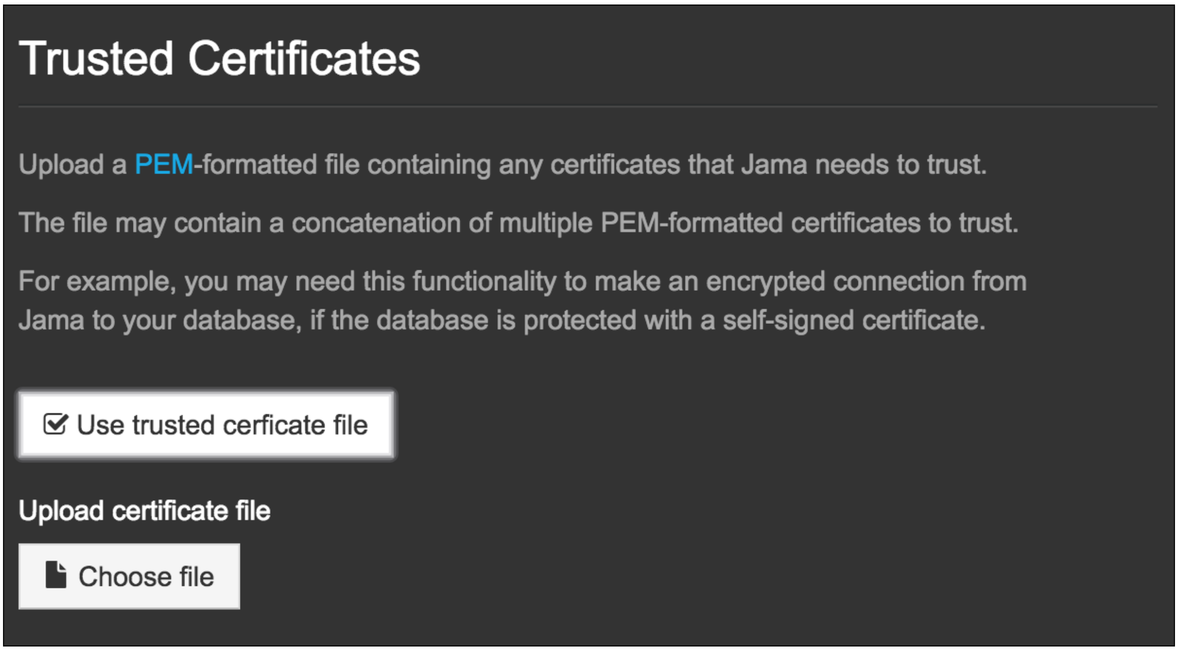
Certificate

Choose file Use self-signed certificate

Verify TLS configuration

3. To link Jama Connect to a service protected by a certificate (self-signed or issued by a local authority):
   - **Private Key** — Click **Choose file** and select your private key.
   - **Certificate** — Click **Choose file** and select your self-signed certificate.
4. Select **Use trusted certificate file** to upload a PEM-formatted public certificate or multiples that are concatenated into a single file. These certificates are added to the default Java trust store. You

might need this functionality to connect to your MySQL, SQL Server, LDAP, Crowd, IMAP, SMTP, or other internal servers from Jama Connect.



Trusted Certificates

Upload a PEM-formatted file containing any certificates that Jama needs to trust.

The file may contain a concatenation of multiple PEM-formatted certificates to trust.

For example, you may need this functionality to make an encrypted connection from Jama to your database, if the database is protected with a self-signed certificate.

5. Scroll down to the bottom of the page and click **Save**. A message confirms that your settings were saved.
6. To apply settings, you must restart the application:
   - Immediately — Select **Restart now**.
   - Later — Select **Cancel** and **Restart later**.

Configure memory settings (traditional)

Memory settings can be configured as part of your initial installation of Jama Connect or any time you need to make changes.

Use the advanced memory settings to change the memory allocation of containers that are running Java processes.

jamacore service	Uses 6.5 GB plus a portion of the remaining total memory. *Recommended:* 6.5 GB + ($total-15 GB)*50%
Search service	Uses 1 GB plus a portion of the remaining total memory. *Recommended:* 1 GB + ($total-15 GB)*5%
Diff service	Default recommendation is 128 MB.
Elasticsearch	Uses 3.5 GB plus a portion of the remaining total memory. *Recommended:* 3.5 GB + ($total-15 GB)*20%
SAML service	Uses 1 GB plus a portion of the remaining total memory.
OAuth service	Uses 512 MB plus a portion of the remaining total memory.

Memory settings can be expressed as a simple formula, using:

Operators	+ - / *
Brackets	( ) to specify order of operations
Variable	$total to reference the total memory of the application server
Numbers	with units KB, MB, or GB
Numbers	with percentages %

NOTE

When changing memory settings, make sure you don't over-allocate the total memory of the application server. Monitor usage [50] and make sure to leave enough memory for system processes to run smoothly. For information, see Resource sizing for your application server.

To configure memory settings:

1. In the header of the Admin Console, select **Settings** to open the Settings page.
2. Scroll down to the **Advanced Memory Settings** section of the page.
3. Use the default values. If you have performance issues, contact Support for help configuring these values.
4. Scroll to the bottom of the page and click **Save**. A message confirms that your settings were saved.
5. To apply settings, you must restart the application:
    - Immediately — Select **Restart now**.
    - Later — Select **Cancel** and **Restart later**.

Configure advanced startup settings (traditional)

Startup settings can be configured as part of your initial installation of Jama Connect or any time you need to make changes.

Enable Java Management Extensions (JMX) and set additional Java Virtual Machine JVM options (JAVA_OPTS) for the following containers that are running Java processes:

- The jamacore application
- Search service
- Elasticsearch

IMPORTANT

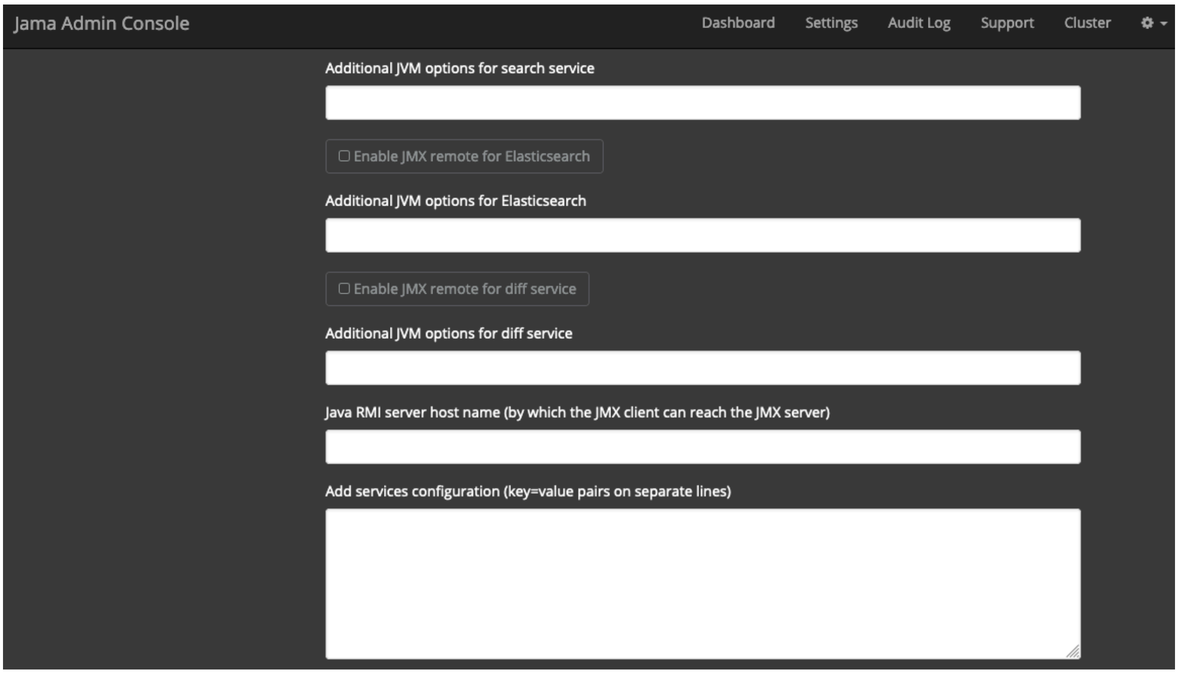
Each of these containers already adds a number of their own JVM options that might clash with additional JVM options configured here.

Use JMX support in a secure environment, because JMX ports have no authentication on the JMX ports when JMX is enabled. A formula can also be used [10] to set an exact memory amount.

To configure advanced startup settings:

1. In the header of the Admin Console, select **Settings** to open the Settings page.
2. Scroll down to the **Advanced Startup Settings** section of the page.
3. Select **Enable JMX remote for core Jama application**.
4. Enter the JMX remote port number for the core Jama application.

   Don't overlap JMX ports between containers and don't overlap other ports that are already in use on the application server.
5. (Optional) Enter additional Java JVM options for Jama core, search service, and Elasticsearch.



Additional JVM options for search service

□ Enable JMX remote for Elasticsearch

Additional JVM options for Elasticsearch

□ Enable JMX remote for diff service

Additional JVM options for diff service

Java RMI server host name (by which the JMX client can reach the JMX server)

Add services configuration (key=value pairs on separate lines)

6. Enter a Java RMI server hostname.
   A single Java RMI server hostname can be given that works across all containers that have JMX enabled. The host IP address is used by default. However, if the host IP address isn't accessible by the JMX client for the configured JMX ports, the public hostname or the public host IP is set here. If an SSH tunnel is used, set the hostname to "localhost."
7. (Optional) In the **Add services configuration** field, add services configuration specific to Jama Connect, such as throttling.
8. Scroll to the bottom of the page and click **Save**. A message confirms that your settings were saved.
9. To apply settings, you must restart the application:
   - Immediately — Select **Restart now**.
   - Later — Select **Cancel** and **Restart later**.

TIP

Garbage collection logging (GC logging) is automatically enabled for containers that are running Java processes. GC log files are available alongside other log files for the respective container [59]. When you restart Jama Connect [49], previous GC log files are packaged as a ZIP file. Typically, the default GC logging configuration is sufficient, but it's possible to override GC logging parameters through the **Additional JVM options for Jama core** field in admin console advanced startup settings [11].

Configure Advanced Search Settings (traditional)

Advanced Search settings can be configured as part of your initial installation of Jama Connect or any time you need to make changes.

Configure index settings for Elasticsearch. Making changes to these settings requires re-indexing.

1. In the header of the Admin Console, select **Settings** to open the Settings page.
2. Scroll down to the **Advanced Search Service Settings** section of the page.
3. Accept the default values.
4. Scroll to the bottom of the page and click **Save**. A message confirms that your settings were saved.

5. To apply settings, you must restart the application:
   - Immediately — Select **Restart now**.
   - Later — Select **Cancel** and **Restart later**.

Set a custom location for the MathType Equations Editor (Traditional)

Settings for the MathType Equations Editor can be configured as part of your initial installation of Jama Connect or any time you need to make changes.

> **NOTE**
>
> The MathType Equations Editor requires a separate license. After your organization has purchased the license, and the system administrator sets up a location for the editor, users can access the editor in the Rich Text Editor in Jama Connect.

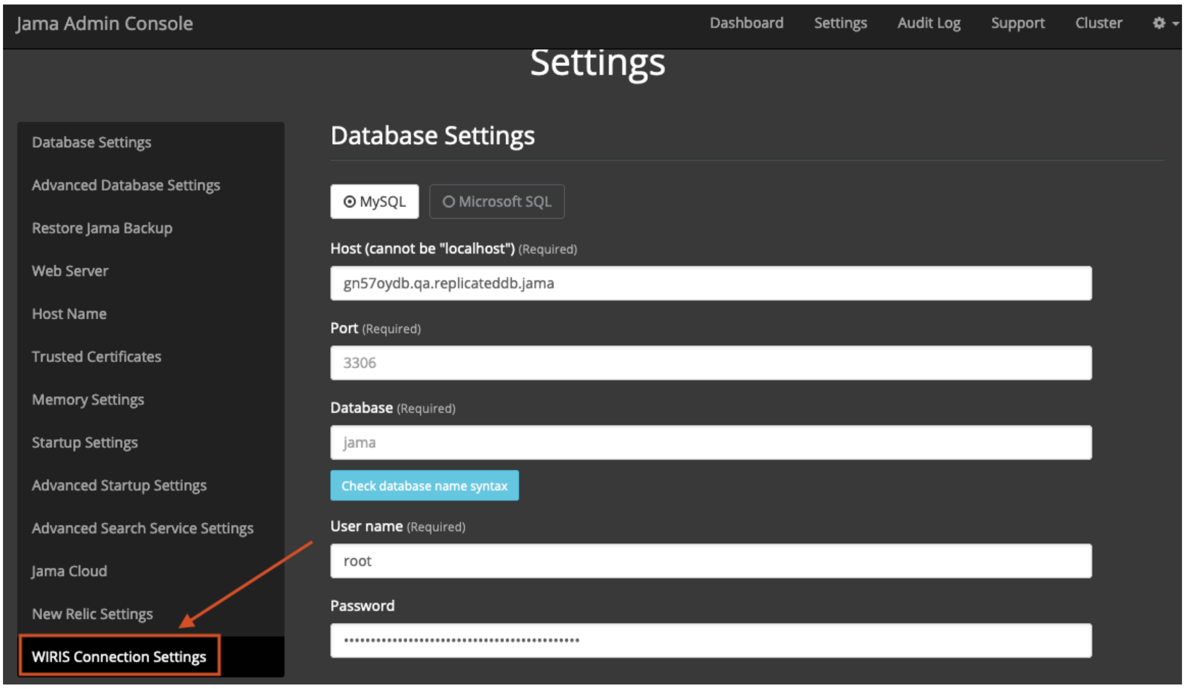
Airgap or self-hosted instances of Jama Connect can add math and chemical equation options to the rich text editor without making calls to an external server.

Before enabling the MathType Equations Editor, you must:

- Designate a server inside your environment that can listen for MathType calls and responses. Check for the latest supported version on the Community.
- Acquire a MathType license from Jama Software.

To configure settings for MathType Editor:

1. Log in to the Admin Console.
2. In the side panel, select **WIRIS Connection Settings**.



Database Settings

● MySQL ○ Microsoft SQL

Host (cannot be "localhost") (Required): gn57oydb.qa.replicateddb.jama

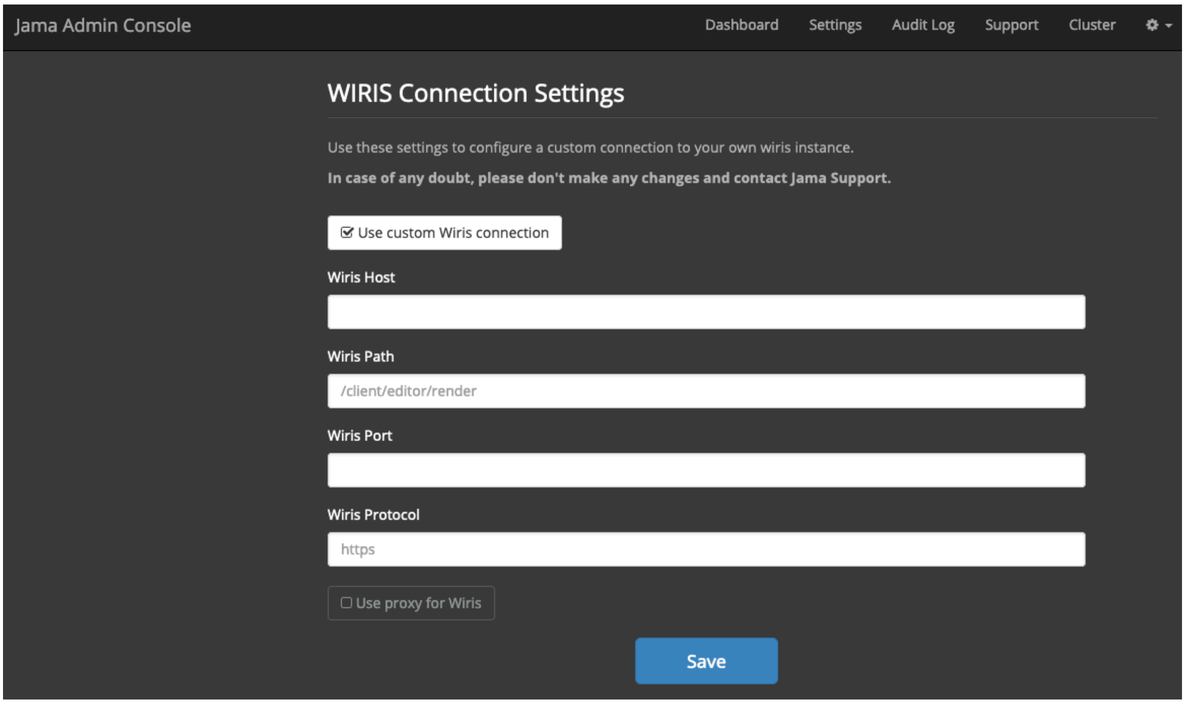
Port (Required): 3306

Database (Required): jama

User name (Required): root

Password: ••

3. Select **Use custom WIRIS connection** to override default settings for communication with the WIRIS cloud servers.



WIRIS Connection Settings

Use these settings to configure a custom connection to your own wiris instance.

In case of any doubt, please don't make any changes and contact Jama Support.

☑ Use custom Wiris connection

Wiris Host

Wiris Path: /client/editor/render

Wiris Port

Wiris Protocol: https

□ Use proxy for Wiris

4. Enter the following information for your designated MathType server:
   - **WIRIS host** (Required) — Enter the hostname of your MathType server. This must be accessible from both the Jama Connect application server and the user's browser. Don't include the port or protocol.
   - **WIRIS path** — Enter the context path followed by "render." Depending on how your server is set up, it might look like this:

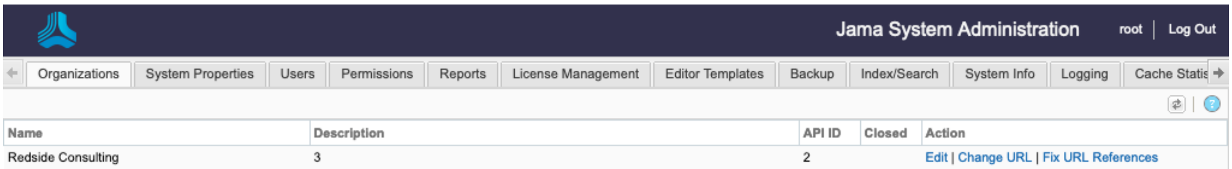
     ```
     /editor/render
     ```
   - **WIRIS port** — The defaults are 80 for http and 443 for https. You can override these values by entering a different port number.
   - **WIRIS protocol** — This is https or http. If you use https to link to Jama Connect, you must also use https for WIRIS.

     > **NOTE**
     >
     > Additional settings for proxy are available but haven't been fully tested. You can use these settings if your Jama Connect instance needs to use a proxy to connect to the MathType server. However, these settings don't change how your browser connects to the MathType server.
5. Scroll to the bottom of the page and click **Save**. A message confirms that your settings were saved.
6. To apply settings, you must restart the application:
   - Immediately — Select **Restart now**.
   - Later — Select **Cancel** and **Restart later**.

Setting up Jama Connect (traditional)

Once you finish installing Jama Connect, continue with a few tasks for the initial setup of the application.

When logged in as root, you can access the System Administration page. From there you can complete the tasks for setting up and maintaining Jama Connect.



Name	Description	API ID	Closed	Action
Redside Consulting	3	2		Edit | Change URL | Fix URL References

Administrator tasks

System administrators complete basic setup and maintenance tasks in the System Administration page. Some of these tasks can also be completed by an organization administrator.

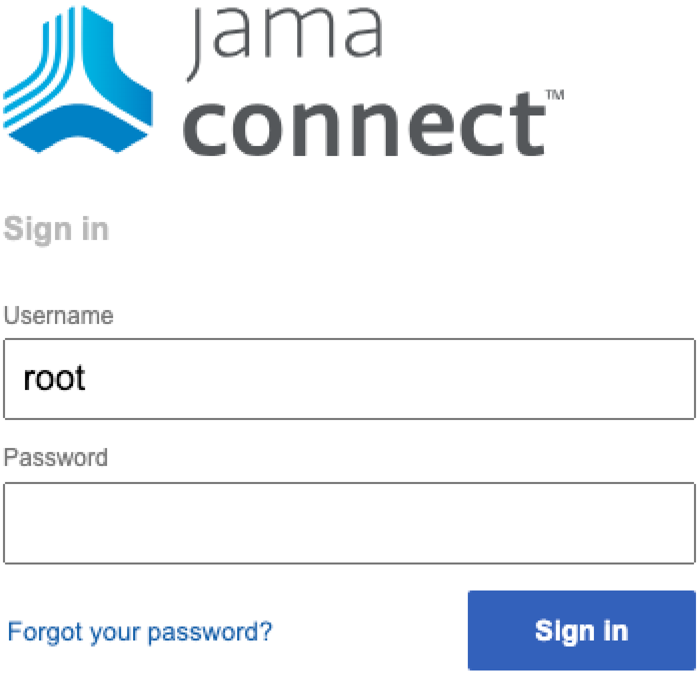
Task	System admin	Org admin
Modify organization details [23]	X	
Configure general properties [24]	X	
Configure authentication properties [27]	X	
Manage users	X	X
Manage permissions	X	X
Manage reports	X	
Monitor license usage	X	X
Create editor templates	X	X
Create a backup [42]	X	
Reindex search [59]	X	
View log and profile [65]	X	
Clear cache [58]	X	
View scheduled jobs [58]	X	
View applied patches [58]	X	

Log in as root for the first time (traditional)

As a system administrator, you are the root user with a unique set of permissions that allow you to access the System Administration page in Jama Connect.

The first time you log in as root, change the default password for the root user and edit any details in the My Profile page, such as email address, phone number, or location.

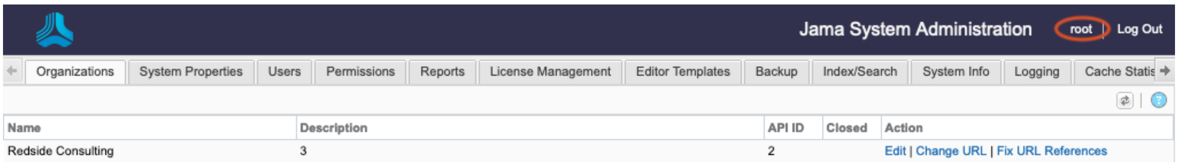
1. At the Jama Connect login page, enter the default credentials for root, then select **Sign In**.
   - **Username** = root
   - **Password** = password



Username: root

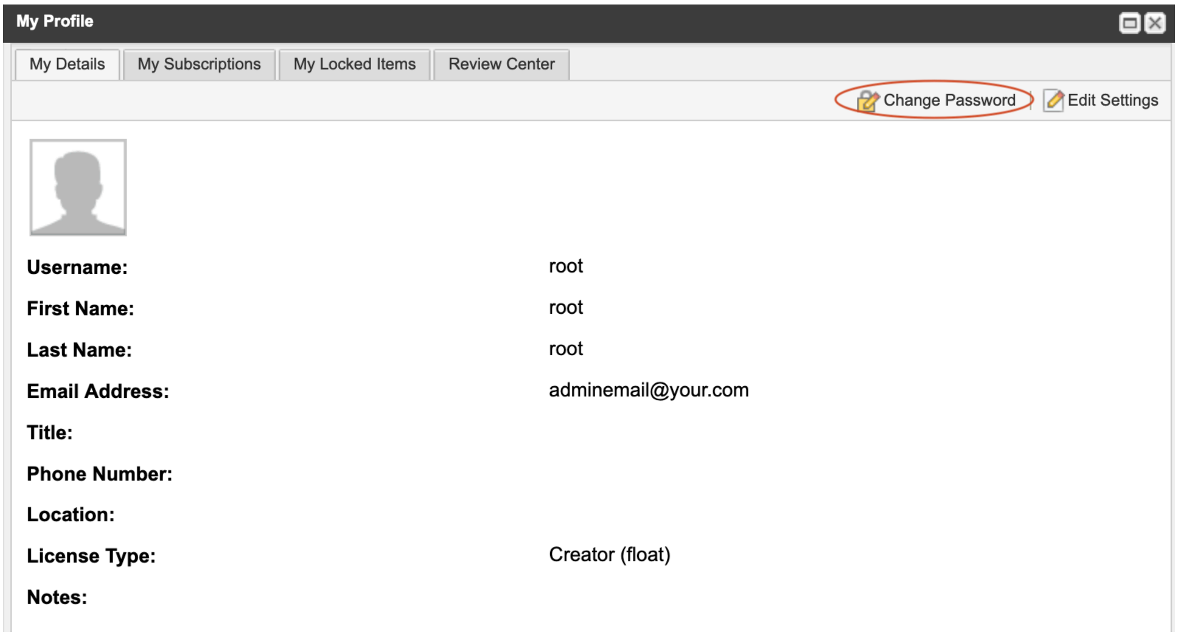
Password:

2. In the top right header, select **root**.



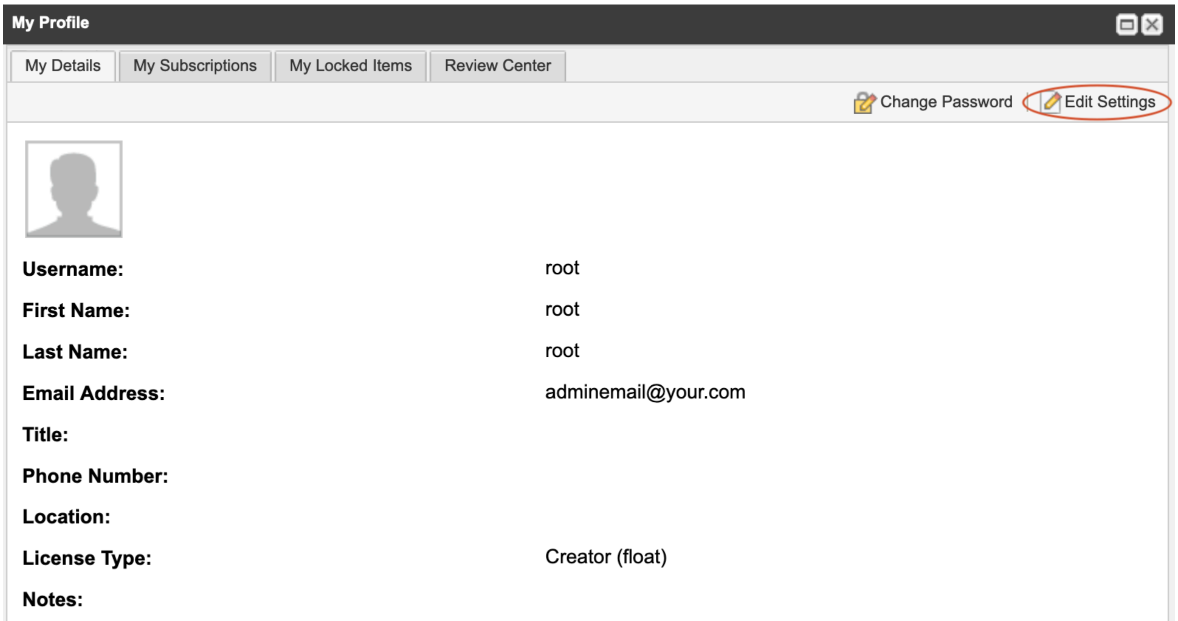
Name	Description	API ID	Closed	Action
Redside Consulting	3	2		Edit | Change URL | Fix URL References

3. On the root user's My Profile page, select **Change Password**.

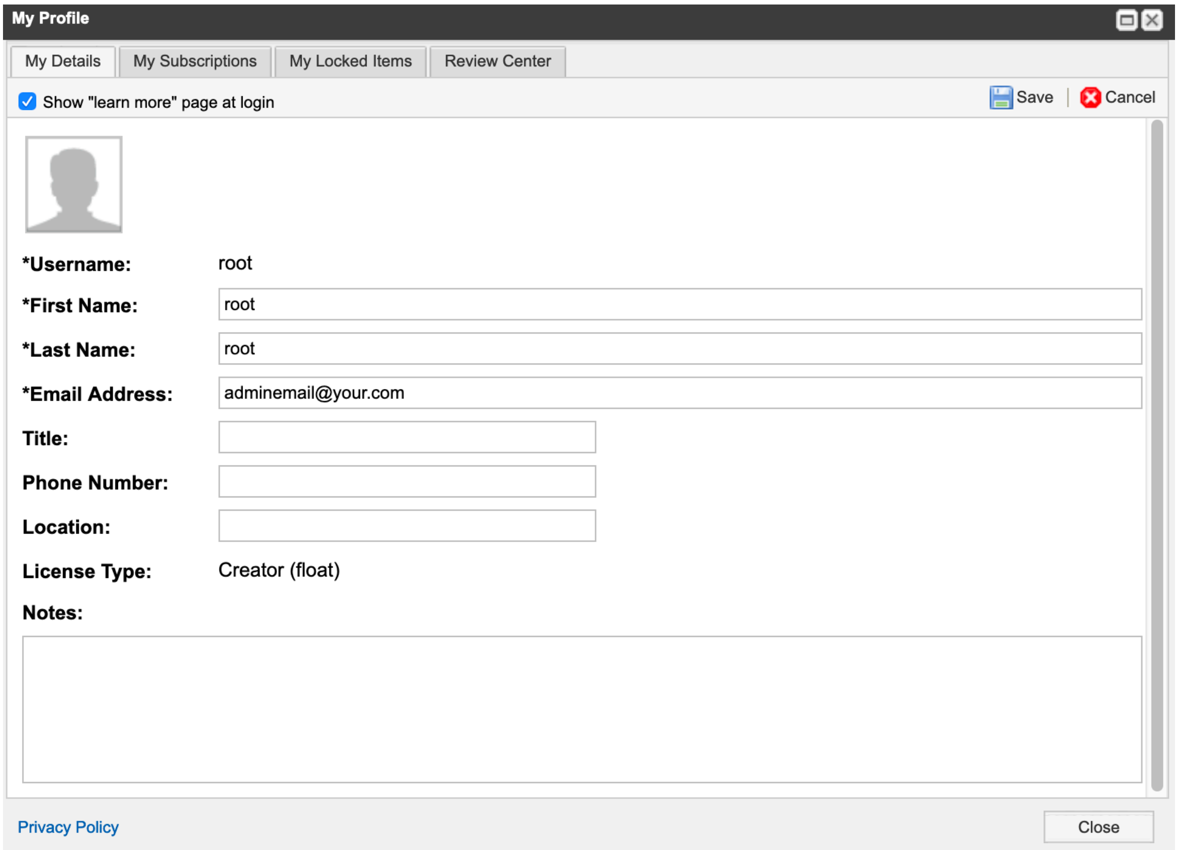


Username:	root
First Name:	root
Last Name:	root
Email Address:	adminemail@your.com
Title:	
Phone Number:	
Location:	
License Type:	Creator (float)
Notes:	

4. Enter the existing password, enter and confirm a new secure password, then select **Save**.
5. (Optional) Select **Edit Settings** to configure the root user email and any other details as needed.



Username:	root
First Name:	root
Last Name:	root
Email Address:	adminemail@your.com
Title:	
Phone Number:	
Location:	
License Type:	Creator (float)
Notes:	



☑ Show "learn more" page at login

***Username:**	root
***First Name:**	root
***Last Name:**	root
***Email Address:**	adminemail@your.com
Title:	
Phone Number:	
Location:	
License Type:	Creator (float)
Notes:	

6. Select **Save**, then select **Close**

Organization administrator's role for setup (traditional)

A *role* is a set of permissions or responsibilities granted to a user. Permissions allow a user to perform a particular job. The role of *organization administrator* controls all aspects of configuring Jama Connect, its users, and its groups.

Only system and organization administrators can assign roles or grant permissions to other users.

The role of organization admin can be assigned to an individual or to a group.

Important considerations

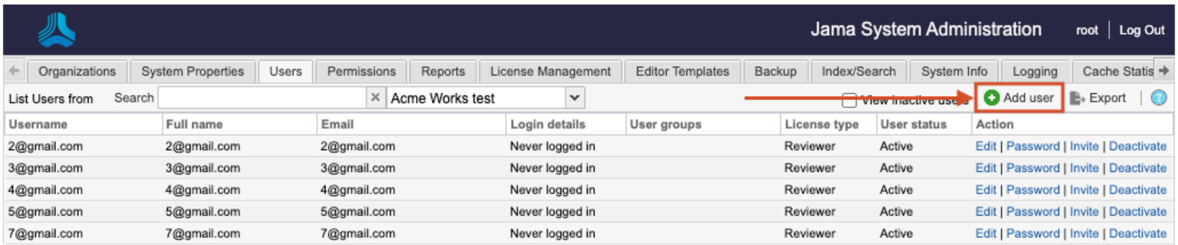
- Configure one or more users as organization admins right after you install Jama Connect, so they can work with you to set up your environment.
- If you have multiple organization admins, include them in a group like the default Organization Admin group, and assign permissions to the group instead of the individual.

Assign a new user as organization admin (traditional)

Only system and organization administrators can assign roles or grant permissions to other users. If you configure an organization admin right after you install Jama Connect, you can share the tasks of setting up user accounts and permissions.

You must be have system administrator permissions to complete this task.

1. Log in to Jama Connect as the root user [15] or as an organization admin.
2. Select **Users > Add user**.



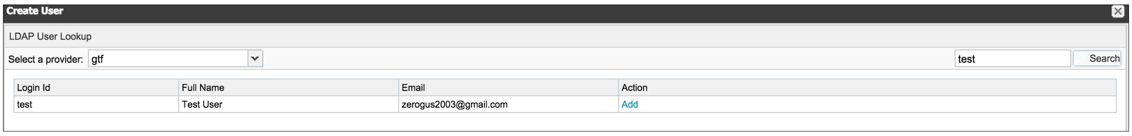
Username	Full name	Email	Login details	User groups	License type	User status	Action
2@gmail.com	2@gmail.com	2@gmail.com	Never logged in		Reviewer	Active	Edit | Password | Invite | Deactivate
3@gmail.com	3@gmail.com	3@gmail.com	Never logged in		Reviewer	Active	Edit | Password | Invite | Deactivate
4@gmail.com	4@gmail.com	4@gmail.com	Never logged in		Reviewer	Active	Edit | Password | Invite | Deactivate
5@gmail.com	5@gmail.com	5@gmail.com	Never logged in		Reviewer	Active	Edit | Password | Invite | Deactivate
7@gmail.com	7@gmail.com	7@gmail.com	Never logged in		Reviewer	Active	Edit | Password | Invite | Deactivate

3. Select a user if LDAP is enabled [33]:
   1. From the LDAP column that is added, select **Add user from LDAP**, enter the name of an existing LDAP user in the search box, then press **Enter**.

      TIP

      You can add wildcards to a search but don't add them at the beginning of a search term. Wildcards at the beginning can result in slow performance. For large directories, expect several minutes.

   2. From the search results, choose a user, then select **Add**.

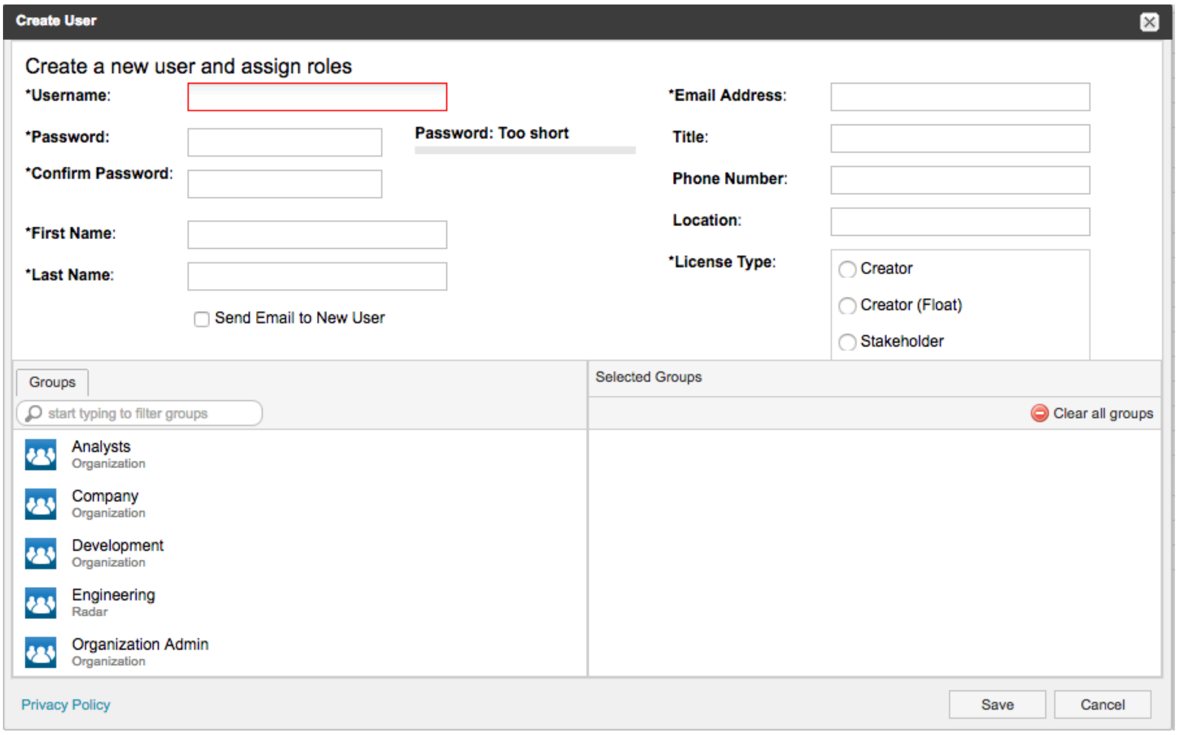


Select a provider: gtf

test

Login Id	Full Name	Email	Action
test	Test User	zerogus2003@gmail.com	Add

4. Select a user if LDAP isn't enabled — Select **Add user**.
5. In the Create User page that opens, complete the information for a single user.



Create User

Create a new user and assign roles

*Username:		*Email Address:	
*Password:	Password: Too short	Title:	
*Confirm Password:		Phone Number:	
*First Name:		Location:	
*Last Name:		*License Type:	○ Creator ○ Creator (Float) ○ Stakeholder

□ Send Email to New User

Groups

start typing to filter groups

- Analysts – Organization
- Company – Organization
- Development – Organization
- Engineering – Radar
- Organization Admin – Organization

Selected Groups

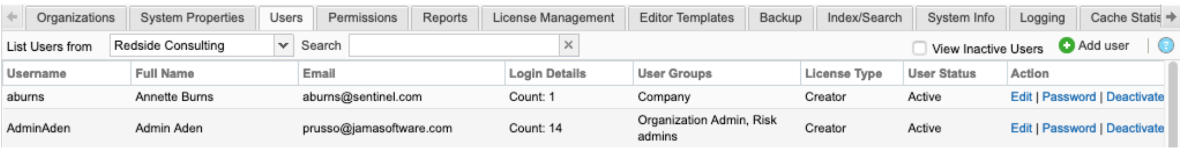
6. For License Type, select **Creator**.
7. Under Groups, select **Organization Admin** from the list.
8. Select **Save**.

Assign an existing user as organization admin (traditional)

Only system and organization administrators can assign roles or grant permissions to other users. If you configure an organization admin right after you install Jama Connect, you can share the tasks of setting up user accounts and permissions.

You must be a system or organization admin to complete this task.

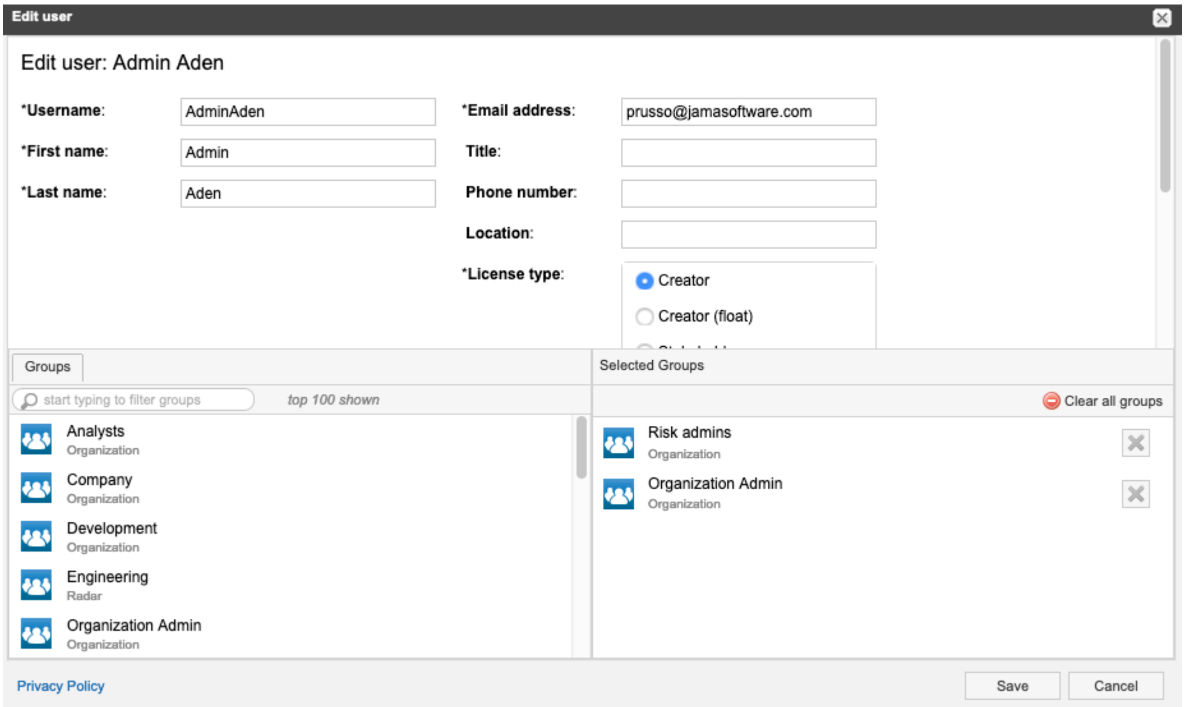
1. Log in to Jama Connect as the root user [15] or as an organization admin.
2. Select **Users** to display the list of existing users.



List Users from: Redside Consulting Search □ View Inactive Users Add user

Username	Full Name	Email	Login Details	User Groups	License Type	User Status	Action
aburns	Annette Burns	aburns@sentinel.com	Count: 1	Company	Creator	Active	Edit | Password | Deactivate
AdminAden	Admin Aden	prusso@jamasoftware.com	Count: 14	Organization Admin, Risk admins	Creator	Active	Edit | Password | Deactivate

3. Choose a user and select **Edit** from the Action list.
   The Edit user page opens.



Edit user

Edit user: Admin Aden

*Username:	AdminAden	*Email address:	prusso@jamasoftware.com
*First name:	Admin	Title:	
*Last name:	Aden	Phone number:	
		Location:	
		*License type:	● Creator ○ Creator (float)

Groups — start typing to filter groups — *top 100 shown*

- Analysts — Organization
- Company — Organization
- Development — Organization
- Engineering — Radar
- Organization Admin — Organization

Selected Groups — Clear all groups

- Risk admins — Organization
- Organization Admin — Organization

Privacy Policy

4. Under Groups, select **Organization Admin** from the list.
5. Select **Save**.

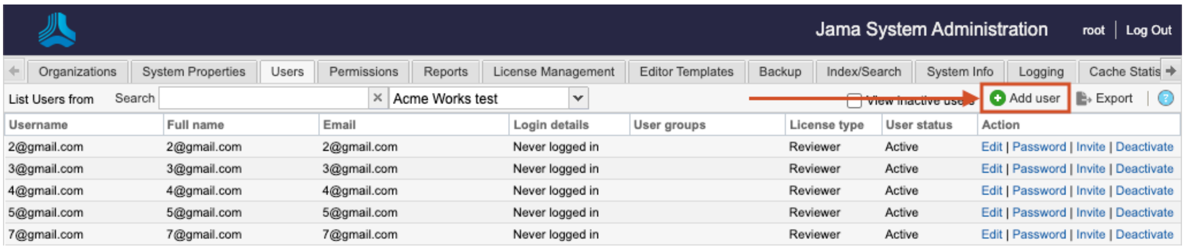
Add a user (traditional)

An important part of building and maintaining your Jama Connect environment is creating accounts for your users.

You must be a system or organization admin to complete this task.

> **NOTE**
>
> If you have a user import plugin, an organization administrator can add a single user, a group, or multiple users.

1. Log in to Jama Connect as the root user [15] or as an organization admin.
2. Select **Users > Add user**.



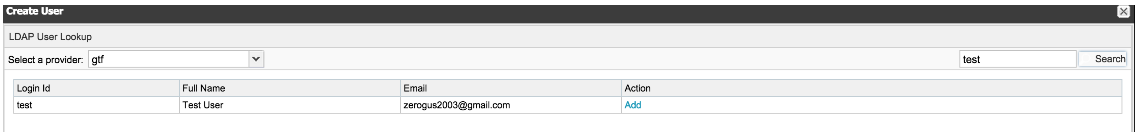
List Users from Search Acme Works test

Username	Full name	Email	Login details	User groups	License type	User status	Action
2@gmail.com	2@gmail.com	2@gmail.com	Never logged in		Reviewer	Active	Edit | Password | Invite | Deactivate
3@gmail.com	3@gmail.com	3@gmail.com	Never logged in		Reviewer	Active	Edit | Password | Invite | Deactivate
4@gmail.com	4@gmail.com	4@gmail.com	Never logged in		Reviewer	Active	Edit | Password | Invite | Deactivate
5@gmail.com	5@gmail.com	5@gmail.com	Never logged in		Reviewer	Active	Edit | Password | Invite | Deactivate
7@gmail.com	7@gmail.com	7@gmail.com	Never logged in		Reviewer	Active	Edit | Password | Invite | Deactivate

3. Select a user if LDAP is enabled [33]:
   a. From the LDAP column that is added, select **Add user from LDAP**, enter the name of an existing LDAP user in the search box, then press **Enter**.

> **TIP**
>
> You can add wildcards to a search but don’t add them at the beginning of a search term. Wildcards at the beginning can result in slow performance. For large directories, expect several minutes.

b. From the search results, choose a user, then select **Add**.



Create User

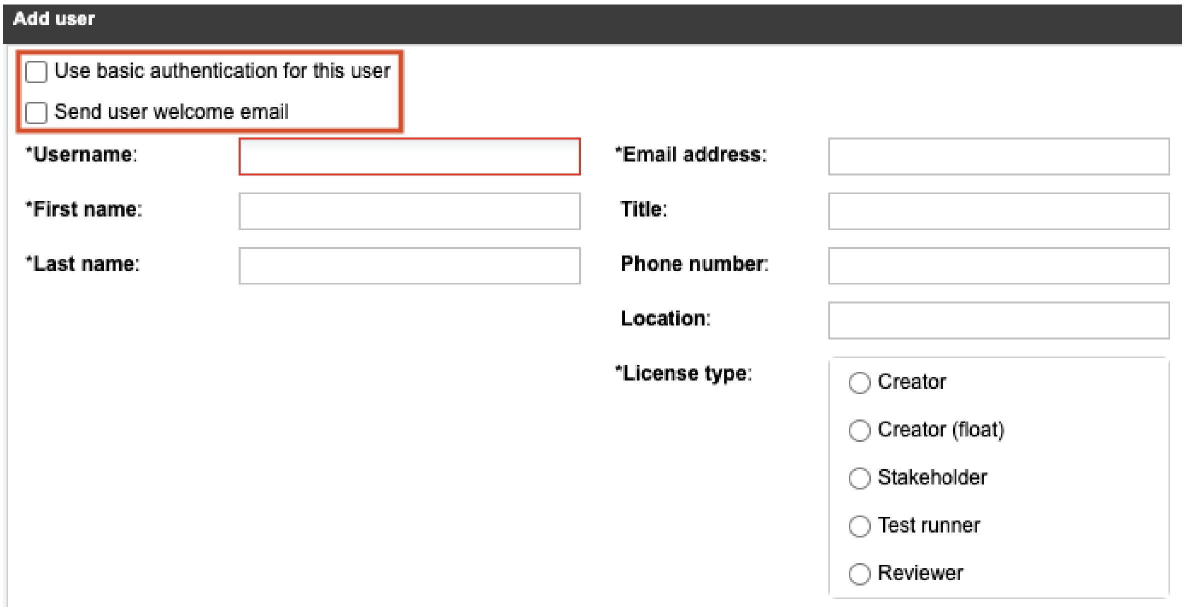
LDAP User Lookup

Select a provider: gtf

test

Login Id	Full Name	Email	Action
test	Test User	zerogus2003@gmail.com	Add

4. Select a user if LDAP isn’t enabled — Select **Add user**.
5. In the page that opens, complete the information for a single user.



Add user

☐ Use basic authentication for this user

☐ Send user welcome email

*Username:		*Email address:	
*First name:		Title:	
*Last name:		Phone number:	
		Location:	
		*License type:	○ Creator ○ Creator (float) ○ Stakeholder ○ Test runner ○ Reviewer

- **Username** — Must be unique, like an email address (recommended).
- **License type** — When assigning license types, consider how many licenses you purchased and the expected usage.
- **Groups** — Assign the user to groups according to how you use groups to manage users, permissions, and security.

6. Select **Save**.

Grant permissions to users (traditional)

Permissions allow users access to create, read, and edit items. They are granted at different levels in your environment.

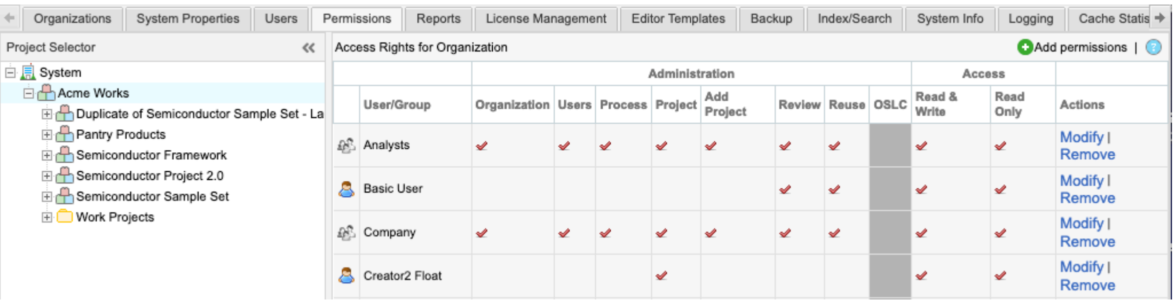
Types of permissions	Level	Notes
Roles and access permissions	Organization level	Org-level permissions are passed on to lower levels.
Project admin permissions	Project level	
Access permissions	Container level and above	

TIP

Organization admin permissions can’t be overridden. In releases prior to Jama Connect 8.62, there was the appearance that you could control an organization admin’s access. However, that user could still see all projects and content, and if they wanted they could give themselves access. The addition of User, Process, and Add project roles decreases the need for a large group of organization admins. No updates or overrides that you created in the past have been removed, so we recommend that you remove them as your organization adopts these new admin roles.

You can create new permissions for a user or group as well as modify existing permissions.

1. Log in to Jama Connect as the root user [15] or as an organization admin.
2. Select **Admin > Permissions**.

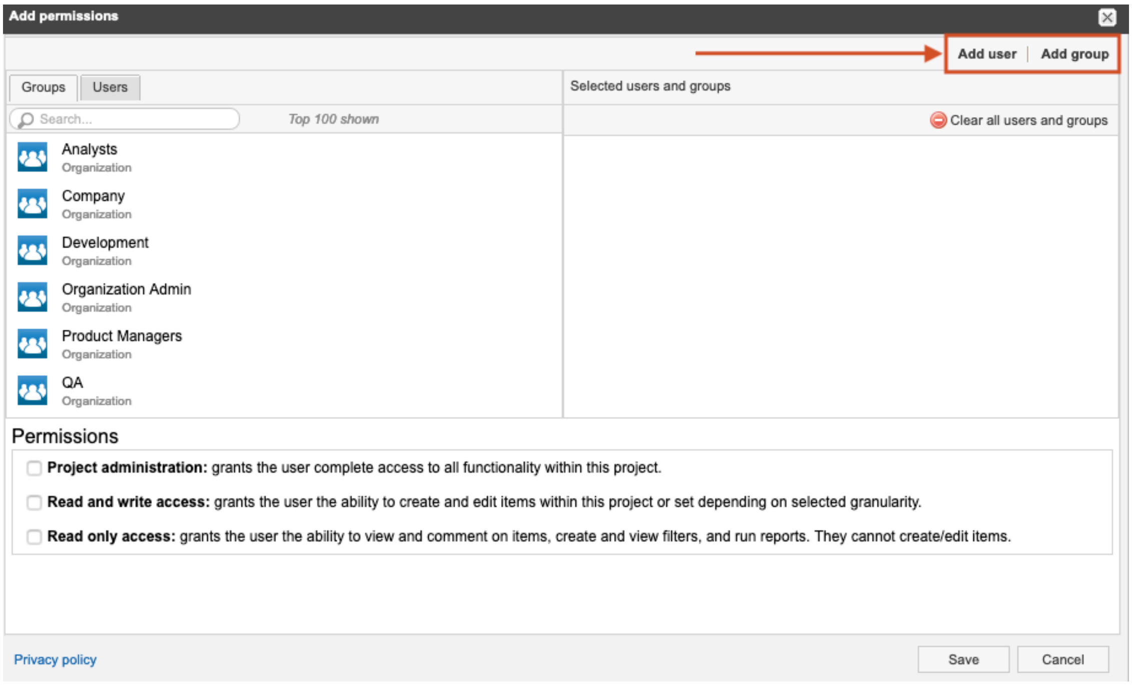
   

   Access Rights for Organization

	Administration								Access		
User/Group	Organization	Users	Process	Project	Add Project	Review	Reuse	OSLC	Read & Write	Read Only	Actions
Analysts	✓	✓	✓	✓	✓	✓	✓		✓	✓	Modify | Remove
Basic User						✓	✓		✓	✓	Modify | Remove
Company	✓	✓	✓	✓	✓	✓	✓		✓	✓	Modify | Remove
Creator2 Float				✓					✓	✓	Modify | Remove

3. In the Project Selector on the left, choose the level where you want to access permissions.
   - Organization (**System**)
   - Individual project
   - Container

   The main page displays current permissions.
4. To change existing permissions for a user or group:
   1. Select **Modify** in the row of the user or group you want to change, select the permissions you want to include, and deselect what you don't want to include.
   2. Select **Remove** in the row of the user or group where you want to delete permissions.
5. To add permissions for a user or group:
   1. Select **Add permissions** in the top right.
   2. In the Add permissions page that opens, select **Add user** or **Add group**.



Analysts
Organization

Company
Organization

Development
Organization

Organization Admin
Organization

Product Managers
Organization

QA
Organization

Permissions

□ **Project administration:** grants the user complete access to all functionality within this project.

□ **Read and write access:** grants the user the ability to create and edit items within this project or set depending on selected granularity.

□ **Read only access:** grants the user the ability to view and comment on items, create and view filters, and run reports. They cannot create/edit items.

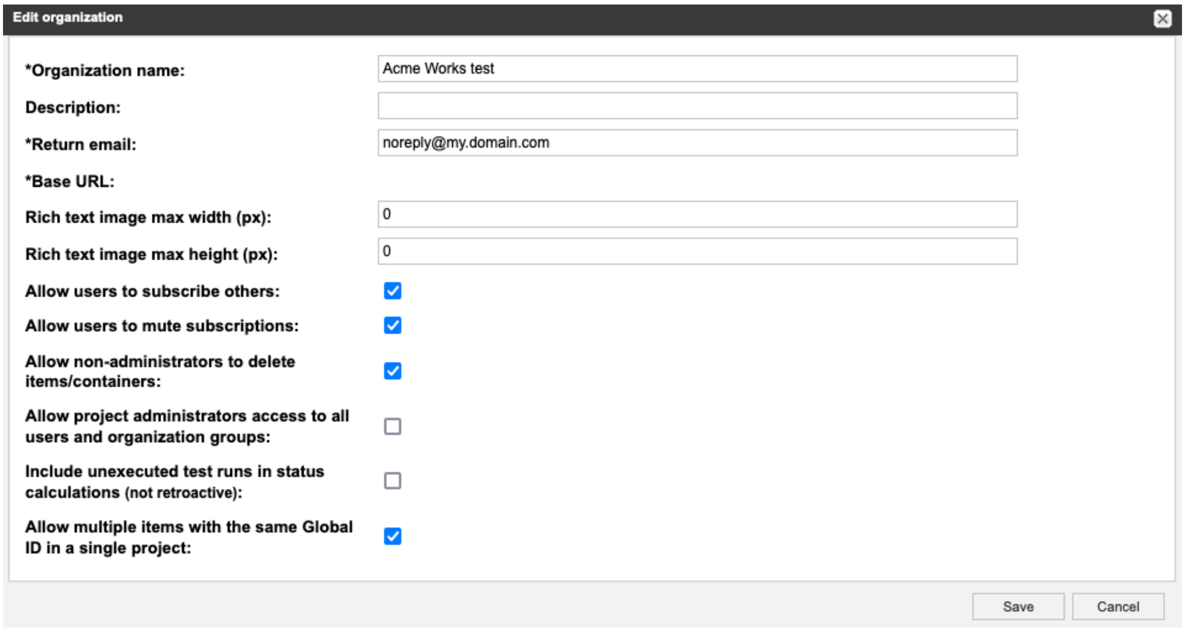
- **Existing user or group** — Select a user or group from the list on the left, then under Permissions, select the role (access permissions) for that user or group.
- **New user or group** — Select **New user** or **New group** in the top right corner of the page. Then under Permissions, select the role or access permissions for that user or group.

3. Select **Save**.

Edit organization details (traditional)

As a system administrator, you can change your organization's information such as the name, description, or return email address.

1. Log in to Jama Connect as the root user [15].
2. Select **Organizations > Edit**.



*Organization name:	Acme Works test
Description:	
*Return email:	noreply@my.domain.com
*Base URL:	
Rich text image max width (px):	0
Rich text image max height (px):	0
Allow users to subscribe others:	☑
Allow users to mute subscriptions:	☑
Allow non-administrators to delete items/containers:	☑
Allow project administrators access to all users and organization groups:	□
Include unexecuted test runs in status calculations (not retroactive):	□
Allow multiple items with the same Global ID in a single project:	☑

3. Enter or change any of the following information:
   - **Organization name** — Typically the name of your company or team. This name appears in the application as well as in reports.

- **Description** — Additional information about your company.
- **Return email** — Email notifications automatically sent by the application. Typically, the organization administrator's email address is used or noreply@example.com.
- **Base URL** — The base URL is used to create URLs sent in email notifications and embed images in exports.
- **Rich text image max width (px)** — Maximum pixel width setting that shrinks all images embedded into rich text fields. Default 0 means no max width is applied.
- **Rich text image max height (px)** — Maximum pixel height setting that shrinks all images embedded into rich text fields. Default 0 means no max height is applied.

  > **NOTE**
  >
  > Images retain their aspect ratio when adjusted to fit the maximum setting of height or width. The adjustment only happens during an upload or document import. Images that already exist on the server are not adjusted. Compression is based on the width and height setting applied.

- **Allow project admins to subscribe to others** — Allows project administrators to subscribe other users to items.
- **Allow users to mute subscriptions** — Allows users to turn off a subscription that was subscribed to by another user.
- **Allow non-administrators to delete items/containers** — Allows a user to delete items even if they don't have organization admin permissions. Default is On.
- **Include unexecuted test run in status calculations (Not retroactive)** — Jama Connect uses all associated test runs to automatically calculate test case status.

  > **NOTE**
  >
  > For test cases associated with a single plan, test case status reflects the status of the test run with the *most recent activity*, which includes unexecuted tests (if enabled). When the case is associated with multiple plans, the *most urgent status* is chosen in this priority order: unexecuted, failed, blocked, scheduled, passed.

  Select this box to include unexecuted test runs in the calculation of test case status (default). Uncheck this box to remove unexecuted test runs from the status priority order.

  If you don't include unexecuted test runs and there are no executed test runs, the system defers to including unexecuted test runs.
- **Allow multiple items with the same Global ID in a single project** — Allows items to be reused multiple times within one project. Default is off.

Configure general properties (traditional)

The general properties need to be configured for all Jama Connect installations. Properties include configuring email and any messages you want to display on the login page.

1. Log in to Jama Connect as the root user [15].
2. Select the **System properties** tab in the System Administration panel, then select **Edit** in the top, right corner.
3. Change any of the following settings.
   - **Enable HTML Tag Security Cleaning** — Prevents suspicious HTML tags from being added to new and modified rich text fields and test steps. Doesn’t clean up data retroactively. Enabled by default.
   - **SMTP Settings** — Settings that affect notifications and subscriptions.

SMTP Enabled	Select **Yes** to use SMTP.
SMTP Host	The domain address of your SMTP server.
SMTP Port	The port for SMTP access.
SMTP User	User account to access SMTP.
SMTP Password	Password for the user account.
Authorization Required	Select **Yes** if authorization is required for the SMTP server.
Use TLS?	Select **Yes** if your mail server uses TLS. Jama Connect supports only Explicit (Opportunistic) SSL/TLS connections for SMTP.

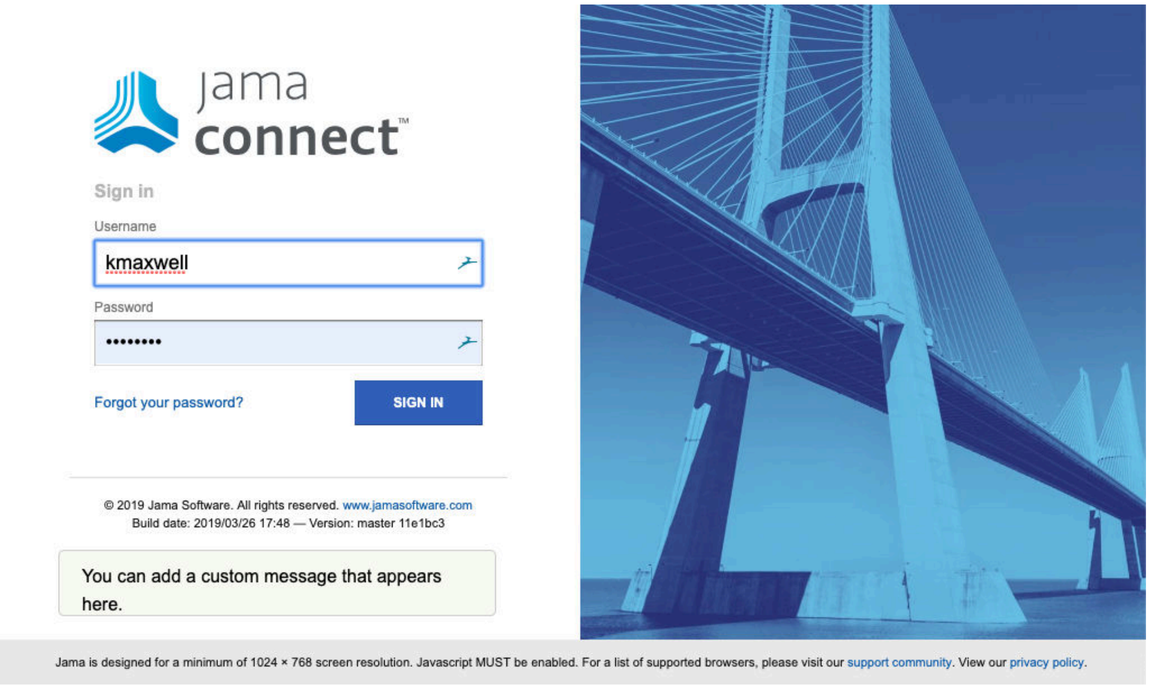
- **System "From" address** — Enter an address for the system to use when it sends notifications or other system messages (for example, info@mycompany.com).
- **Collaboration "From" address** — IMAP must be supported to enable reply-to e-mails in the stream. The Collaboration "From" address must match the email address used for IMAP, so replies to stream emails are sent to the same account that processes incoming mail (for example, replyto@mycompany.com). To enable IMAP, see Configure Inbound email (IMAP) settings [26].
- **Allow Project Administrators to add groups** — Select **Yes** for project administrators to add groups. Otherwise, only system and organization administrators can add groups.
- **Allow Project Administrators to set project permissions** — Select **Yes** for project administrators to grant project permissions. Otherwise, only system and organization administrators can grant permissions.
- **Allow access to REST API** — Enables users to perform actions in Jama Connect from outside the user interface.
- **Attachment file extensions** — List of file types (lowercase, separated by commas, periods, spaces, or newline characters) that can be uploaded as an attachment.

  NOTE

  Files are rejected if the content of the file doesn’t match the file extension, or if the MIME type is not understood by the system, even if the file type is listed here. To allow files of an unknown type, set the option to a blank string.

  File extensions must be lowercase even if the actual extension on the file is uppercase. Learn more.

- **Notice on login page** — Displays a notice to users below the login page and in a yellow bar at the base of the application page.



Username: kmaxwell

Password: ••••••••

© 2019 Jama Software. All rights reserved. www.jamasoftware.com
Build date: 2019/03/26 17:48 — Version: master 11e1bc3

You can add a custom message that appears here.

Jama is designed for a minimum of 1024 × 768 screen resolution. Javascript MUST be enabled. For a list of supported browsers, please visit our support community. View our privacy policy.

NOTE
This login page might not be visible if you are using SSO or SAML logins.

- **Maintenance mode** — Logs out and locks out all users except the root user until this option is disabled.
- **Set header color** — Helps to differentiate test or staging instances from the production instance of Jama Connect.
- **Set Batch Synchronous Index Limit** — Select a limit that determines whether items in a batch update are indexed synchronously or asynchronously. Synchronous indexing can add time to the index process, so the default value is set to 1000. The added time depends on the number of items and the complexity of fields for those items.
  - **Synchronous indexing** — The number of items in a batch update is equal to or less then the limit.
  - **Asynchronous indexing** — The number of items in a batch update is greater than the limit.

4. Select **Save**.

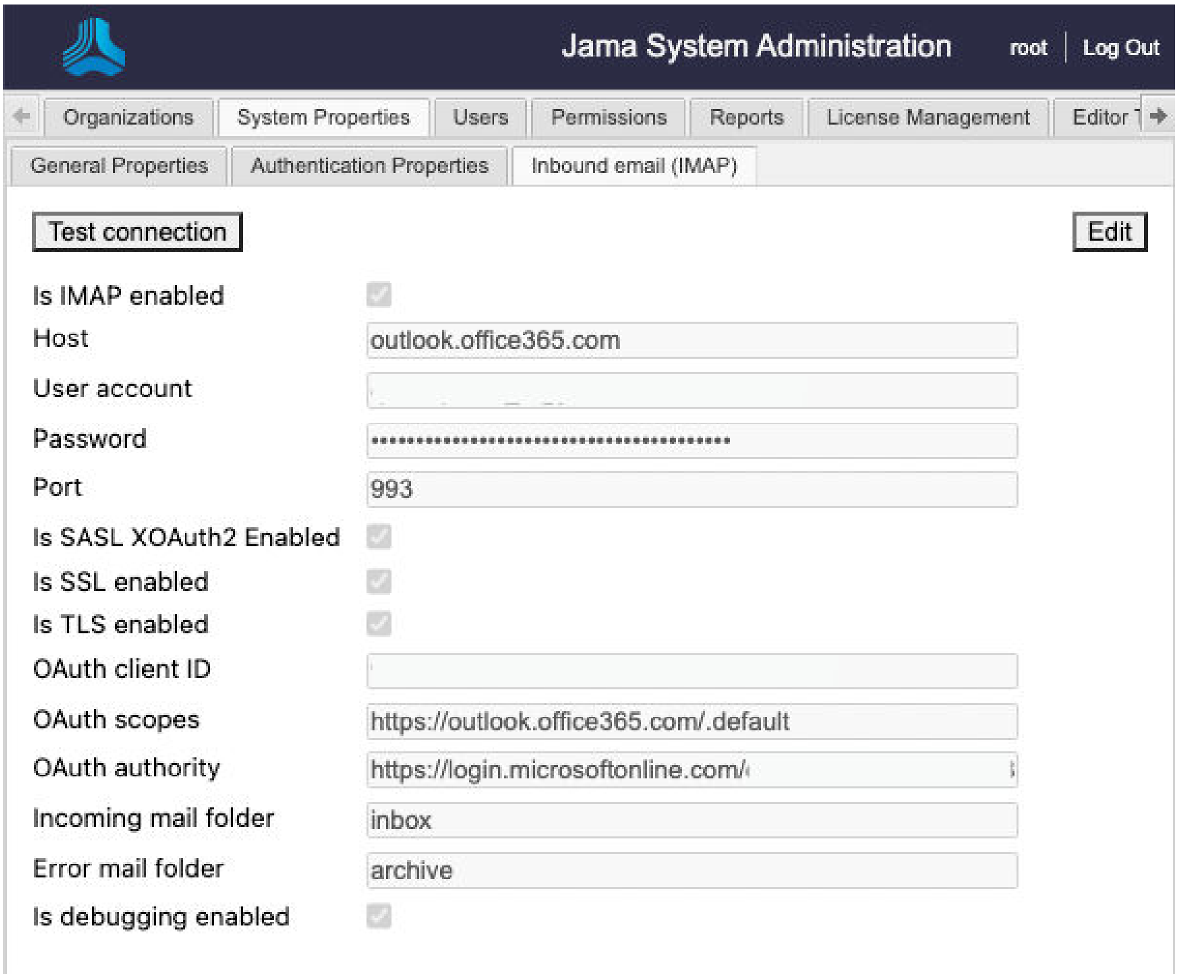
Configure Inbound email (IMAP) settings (traditional)

Before configuring IMAP, verify that your email server supports IMAP. Your server must support IMAP to enable reply-to emails in the stream.

For more information, see Authenticate an IMAP, POP or SMTP connection using OAuth.

To configure IMAP:

1. Log in to Jama Connect as root user [15].
2. Select **System Properties > Inbound email (IMAP)**.
3. Click **Edit**, then select **Is IMAP enabled**.
4. Configure the following settings:



Is IMAP enabled ☑

Host: outlook.office365.com

User account:

Password: **

Port: 993

Is SASL XOAuth2 Enabled ☑

Is SSL enabled ☑

Is TLS enabled ☑

OAuth client ID:

OAuth scopes: https://outlook.office365.com/.default

OAuth authority: https://login.microsoftonline.com/

Incoming mail folder: inbox

Error mail folder: archive

Is debugging enabled ☑

Host	Enter the IMAP server URL.
User account	Enter a user account for someone with access to the folder where IMAP emails are saved.
Password	Enter the password for the user account or the OAuth secret.
Port	The port for IMAP connection, typically different from SMTP. Standard ports are Non-SSL:143, SSL:993.
Is SASL XOAuth2 Enabled	Select to enable OAuth authentication and token-based authorization for Microsoft based IMAP connections.
Is SSL Enabled	Select to enable SSL IMAP connections.
Is TLS Enabled	Select to enable TLS IMAP connections.
OAuth Client ID	Enter the client ID (Microsoft AAD Application ID).
OAuth scopes	Enter the resource URLs defining the token authorization request.
OAuth authority	Enter the URL of the authenticating authority or security token service. Microsoft security token service example: https://login.microsoftonline.com/{microsoft_tenant_id}
Incoming mail folder	(Required) Enter the name of the mail folder to read collaboration replies from.
Error mail folder	(Required) Enter the name of the mail folder to move unknown emails to. Unknown emails are non-collaboration emails.
Is debugging enabled	Select to enable debug level logging for failing IMAP connections. After enabling, check the server logs and test the connection.

5. Click **Save**.

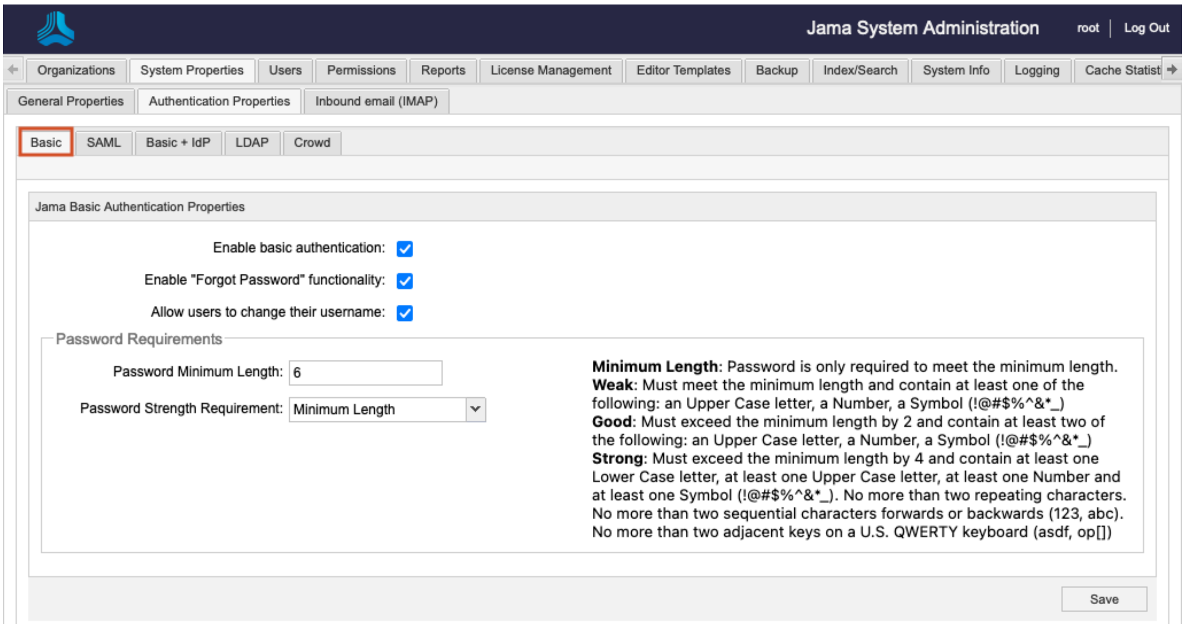
Configure Basic authentication (traditional)

The default authentication method is Jama Connect Basic, which authenticates users by their username and password that are stored in the Jama Connect database. Passwords are encrypted before they are stored in the database.

NOTE
You must be a system administrator to complete this task.

To configure the Basic authentication properties:

1. Log in to Jama Connect as the root user [15].
2. Select **System Properties > Authentication Properties > Basic**.



Jama Basic Authentication Properties

Enable basic authentication: ☑

Enable "Forgot Password" functionality: ☑

Allow users to change their username: ☑

Password Requirements

Password Minimum Length: 6

Password Strength Requirement: Minimum Length

Minimum Length: Password is only required to meet the minimum length.
Weak: Must meet the minimum length and contain at least one of the following: an Upper Case letter, a Number, a Symbol (!@#$%^&*_)
Good: Must exceed the minimum length by 2 and contain at least two of the following: an Upper Case letter, a Number, a Symbol (!@#$%^&*_)
Strong: Must exceed the minimum length by 4 and contain at least one Lower Case letter, at least one Upper Case letter, at least one Number and at least one Symbol (!@#$%^&*_). No more than two repeating characters. No more than two sequential characters forwards or backwards (123, abc). No more than two adjacent keys on a U.S. QWERTY keyboard (asdf, op[])

3. Configure the authentication properties for the method you are using.
   - **Enable basic authentication** — Enabled by default. You must deselect this option to use LDAP or Crowd.
   - **Enable "Forgot Password" functionality** — Users who forget their password can request a new password without notifying the system admin.
   - **Allow users to change their username** — Users can change their username when they manage their profile.
   - **Password requirements** — Set the required password strength for all future passwords. New user passwords must meet the required password strength to be saved. Changes to these settings do not affect passwords already in the system.
4. Click **Save**.

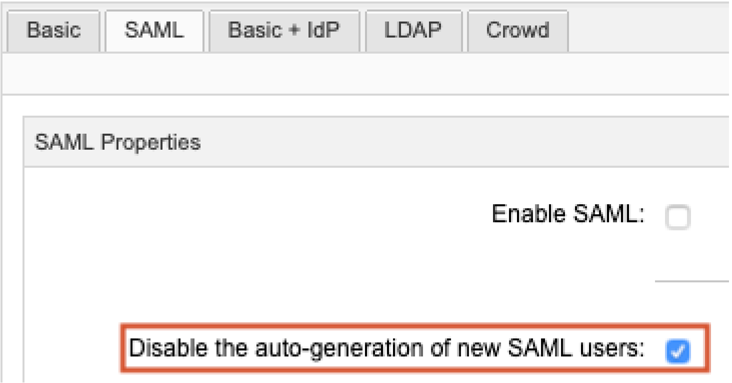
Configure SAML authentication (traditional)

To configure SAML authentication, you must first update the authentication properties.

Important considerations

- To connect multiple instances of Jama Connect to the SAML service, you must create unique metadata or applications for each instance through the identity provider. This is true for any combination of production, sandboxes, or self-hosted instances. The entity ID is a unique value that allows the service and identity provider to locate each other and send users to the correct Jama Connect instance.
- We recommend testing an integration instance before using SAML on a production instance. For example, disable a sandbox instance from SAML before connecting on a production instance.

- Starting with Jama Connect 8.48, organizations that use SAML can use electronic signatures, which are enabled by default. If your identity provider (IdP) can't process the re-authentication, you can disable signatures.
- You can enable a different authentication method at any time. If you do, SAML is disabled.
- You can control the auto-provisioning of new SAML users in both single SAML and multi-mode. If your users are set up in SAML but not yet added to your Jama user table, this option allows you to control whether users can auto-provision in Jama Connect.
  When this option is selected and properties are saved, your SAML users (SAML and multi-mode) can’t sign in to Jama Connect until you add them to the Jama user table. A message tells them to finish the authentication process with their administrator.
  This option is selected by default after you upgrade to 8.62.



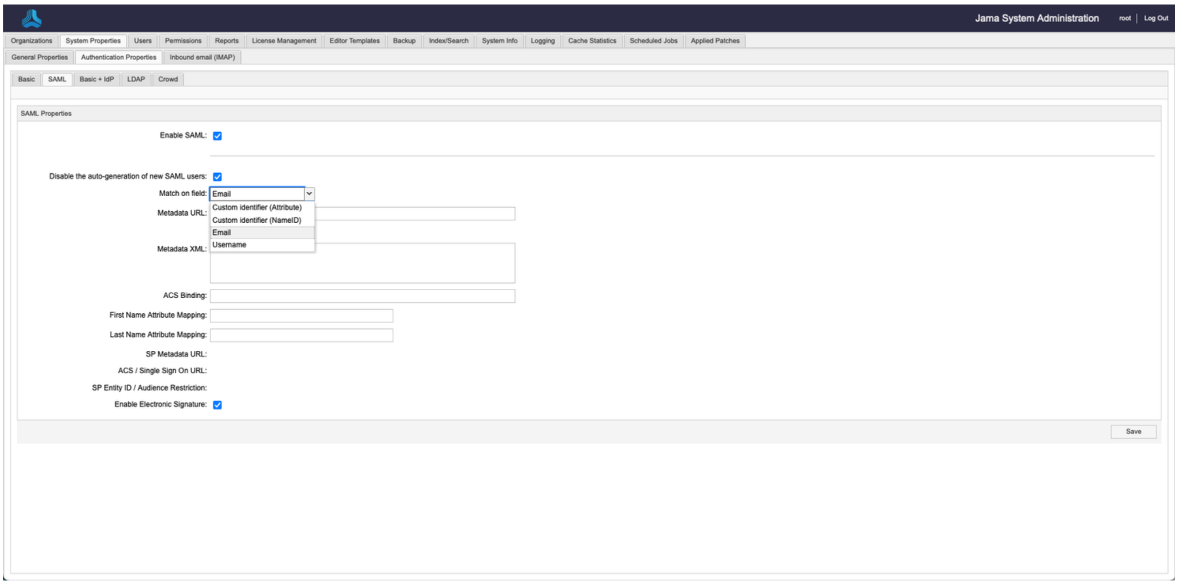
SAML Properties

Enable SAML: □

Disable the auto-generation of new SAML users: ☑

To configure SAML authentication:

1. Log in to Jama Connect as the root user [15].
2. Select **System Properties > Authentication Properties > SAML**.
3. *Before you enter data*, select **Enable SAML**, then click **Save**.



SAML Properties

Enable SAML: ☑

Disable the auto-generation of new SAML users: ☑

Match on field: Email

Metadata URL:

Metadata XML:

ACS Binding:

First Name Attribute Mapping:

Last Name Attribute Mapping:

SP Metadata URL:

ACS / Single Sign On URL:

SP Entity ID / Audience Restriction:

Enable Electronic Signature: ☑

NOTE

The following selections for the **Match on field** configuration are beta features that are under development: **Username**, **Custom identifier (NameID)**, and **Custom identifier (Attribute)**. For now, use the default **Email** selection. If you're interested in beta testing the **Username** or **Custom identifier** selections, contact your account manager.

4. Contact your identity provider for the metadata URL or XML, then paste it in the appropriate field.
   If a connection is established, the last three read-only fields are auto-populated with a URL.
   - **SP metadata URL** — https://saml-or.jamacloud.com/saml/metadata/alias/defaultAlias
   - **ACS / single-sign-on URL** — https://saml-or.jamacloud.com/saml/SSO/alias/defaultAlias
   - **SP entity ID / Audience restriction** — https://saml-or.jamacloud.com/saml/metadata/alias/defaultAlias

   If the connection doesn't work, you might need to adjust the information in the **ACS binding**, **First name attribute mapping**, and **Last name attribute mapping** fields or contact support.

   > **TIP**
   >
   > The mapping fields serve as the key that connects user identity between Jama Connect and your identity provider. If name attribute mapping fields aren't specified, then a new user's full name defaults to their email address.

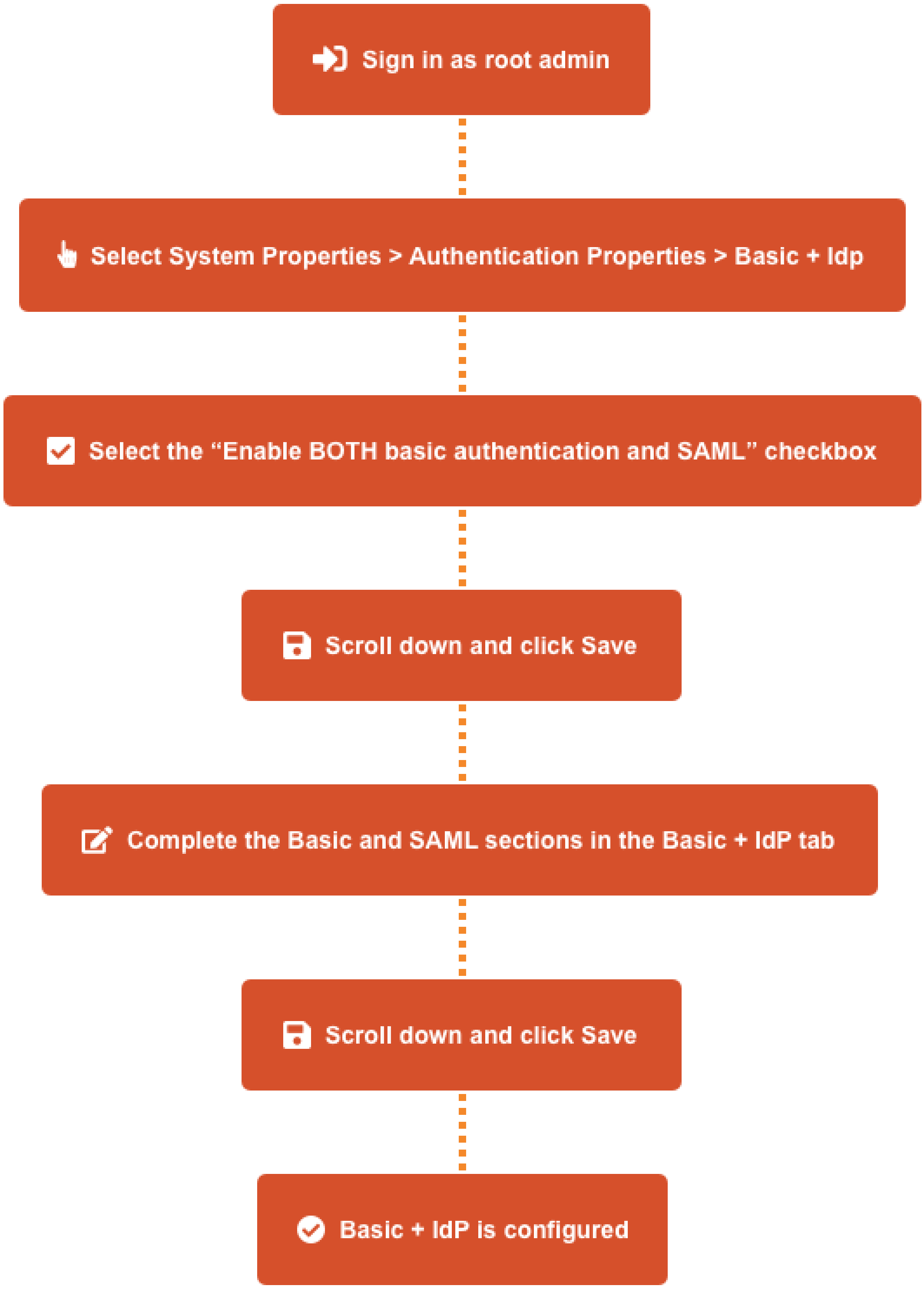
5. Click **Save**.

Once SAML is enabled, Jama Connect redirects all users to the identity provider's login page. The Jama Connect login page is only accessible for system administrators if they log in as the root user with this URL:

```
https://your-jama-url/casper/login.req
```

Configure multi-mode authentication (traditional)

The combination of Jama Connect Basic and SAML authentication (**Basic + IdP**) provides extra security by separating your internal users from external partners.



Sign in as root admin

Select System Properties > Authentication Properties > Basic + Idp

Select the “Enable BOTH basic authentication and SAML” checkbox

Scroll down and click Save

Complete the Basic and SAML sections in the Basic + IdP tab

Scroll down and click Save

Basic + IdP is configured

To configure multi-mode authentication:

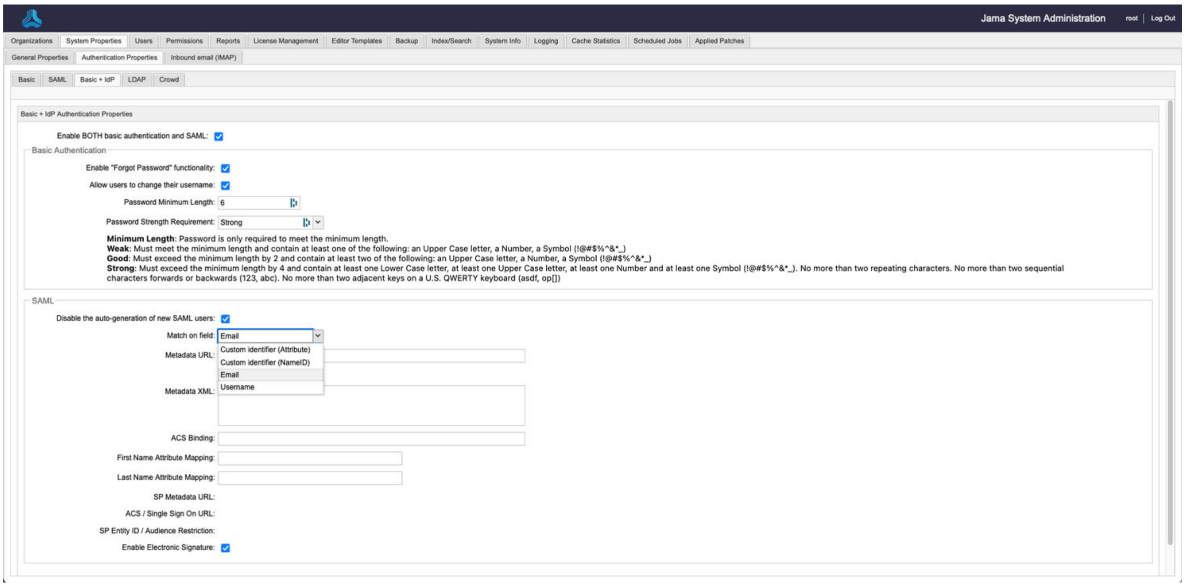
1. If you haven't entered the SAML metadata in the root menu, go to the SAML tab and enter it there.
   - Contact your identity provider for the metadata URL or XML, then paste it in the appropriate field. If a connection is established, the last three read-only fields are auto-populated with a URL.
     - **SP metadata URL** — https://saml-or.jamacloud.com/saml/metadata/alias/defaultAlias
     - **ACS / single-sign-on URL** — https://saml-or.jamacloud.com/saml/SSO/alias/defaultAlias

- **SP entity ID / Audience restriction** — https://saml-or.jamacloud.com/saml/metadata/alias/defaultAlias

  If the connection doesn't work, you might need to adjust the information in the **ACS binding**, **First name attribute mapping**, and **Last name attribute mapping** fields or contact support.

> **TIP**
>
> The mapping fields are the key that connects user identity between Jama Connect and your identity provider. If name attribute mapping fields aren't specified, a new user's full name defaults to their email address.

2. Log in to Jama Connect as the root user [15].
3. Select **System Properties > Authentication Properties > Basic + IdP**.



Basic + IdP Authentication Properties

Enable BOTH basic authentication and SAML: ☑

Basic Authentication

Enable "Forgot Password" functionality: ☑

Allow users to change their username: ☑

Password Minimum Length: 6

Password Strength Requirement: Strong

Minimum Length: Password is only required to meet the minimum length.
Weak: Must meet the minimum length and contain at least one of the following: an Upper Case letter, a Number, a Symbol (!@#$%^&*_)
Good: Must exceed the minimum length by 2 and contain at least two of the following: an Upper Case letter, a Number, a Symbol (!@#$%^&*_)
Strong: Must exceed the minimum length by 4 and contain at least one Lower Case letter, at least one Upper Case letter, at least one Number and at least one Symbol (!@#$%^&*_). No more than two repeating characters. No more than two sequential characters forwards or backwards (123, abc). No more than two adjacent keys on a U.S. QWERTY keyboard (asdf, op[])

SAML

Disable the auto-generation of new SAML users: ☑

Match on field: Email

Custom identifier (Attribute)
Custom identifier (NameID)
Email
Username

Metadata URL:

Metadata XML:

ACS Binding:

First Name Attribute Mapping:

Last Name Attribute Mapping:

SP Metadata URL:

ACS / Single Sign On URL:

SP Entity ID / Audience Restriction:

Enable Electronic Signature: ☑

4. Select **Enable BOTH Basic authentication and SAML**, then click **Save**.

   The Basic + IdP tab transitions can now accept input. While the Basic and SAML tabs are now read-only This type of input is the same on both tabs: Basic and SAML.
5. Complete the Basic and SAML sections in the Basic + IdP tab:

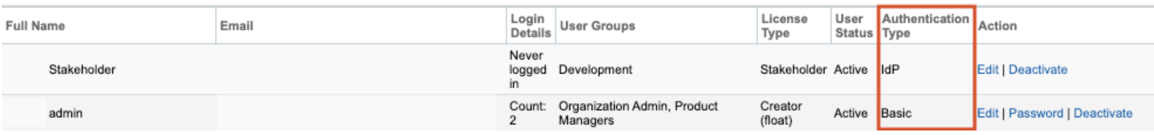
   Basic — Fill out the the Basic Authentication section.

   SAML — If you haven't entered the SAML metadata in the root menu, complete the following steps in the SAML section of the Basic + IdP tab.

> **NOTE**
>
> The following selections for the **Match on field** configuration are beta features that are under development: **Username**, **Custom identifier (NameID)**, and **Custom identifier (Attribute)**. For now, use the default **Email** selection. If you're interested in beta testing the **Username** or **Custom identifier** selections, contact your account manager.

6. Click **Save**.
7. Confirm the configuration was successful.
   - Select the **Users** tab, then verify that the Authentication Type column appears in the table.

     If you see the Authentication Type column, Basic + IdP authentication is now enabled.



Full Name	Email	Login Details	User Groups	License Type	User Status	Authentication Type	Action
Stakeholder		Never logged in	Development	Stakeholder	Active	IdP	Edit | Deactivate
admin		Count: 2	Organization Admin, Product Managers	Creator (float)	Active	Basic	Edit | Password | Deactivate

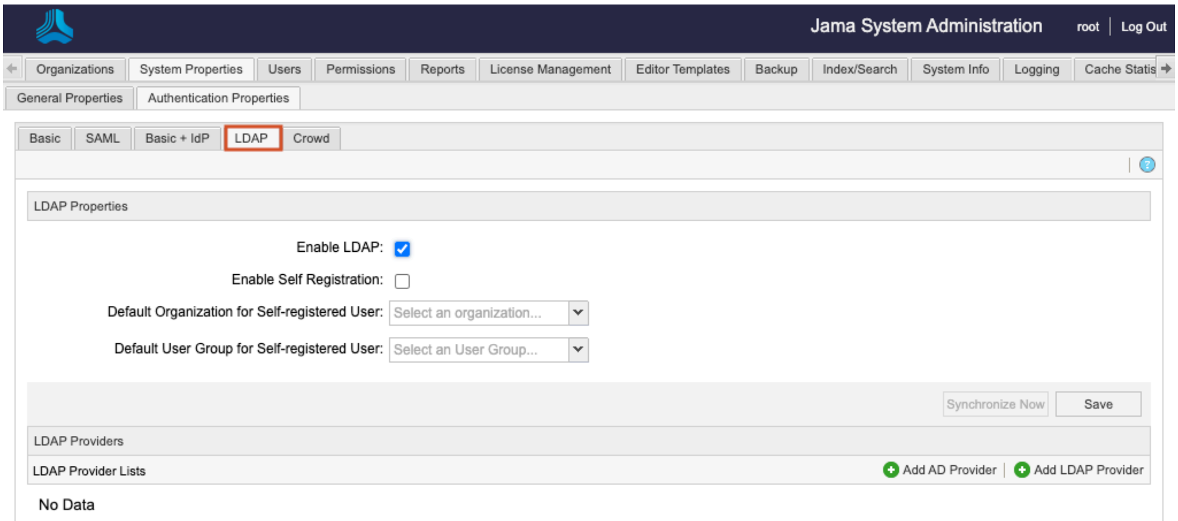
Configure LDAP authentication (traditional)

LDAP (Lightweight Directory Access Protocol) is a tool for organizations to centralize the management of user accounts. Jama Connect includes a built-in integration for LDAP and Microsoft Active Directory.

LDAP must be configured before it can be used in Jama Connect to authenticate users against your LDAP server.

To configure LDAP authentication:

1. Log in to Jama Connect as the root user [15].
2. Select **System Properties > Authentication Properties > LDAP**.



Enable LDAP: ☑

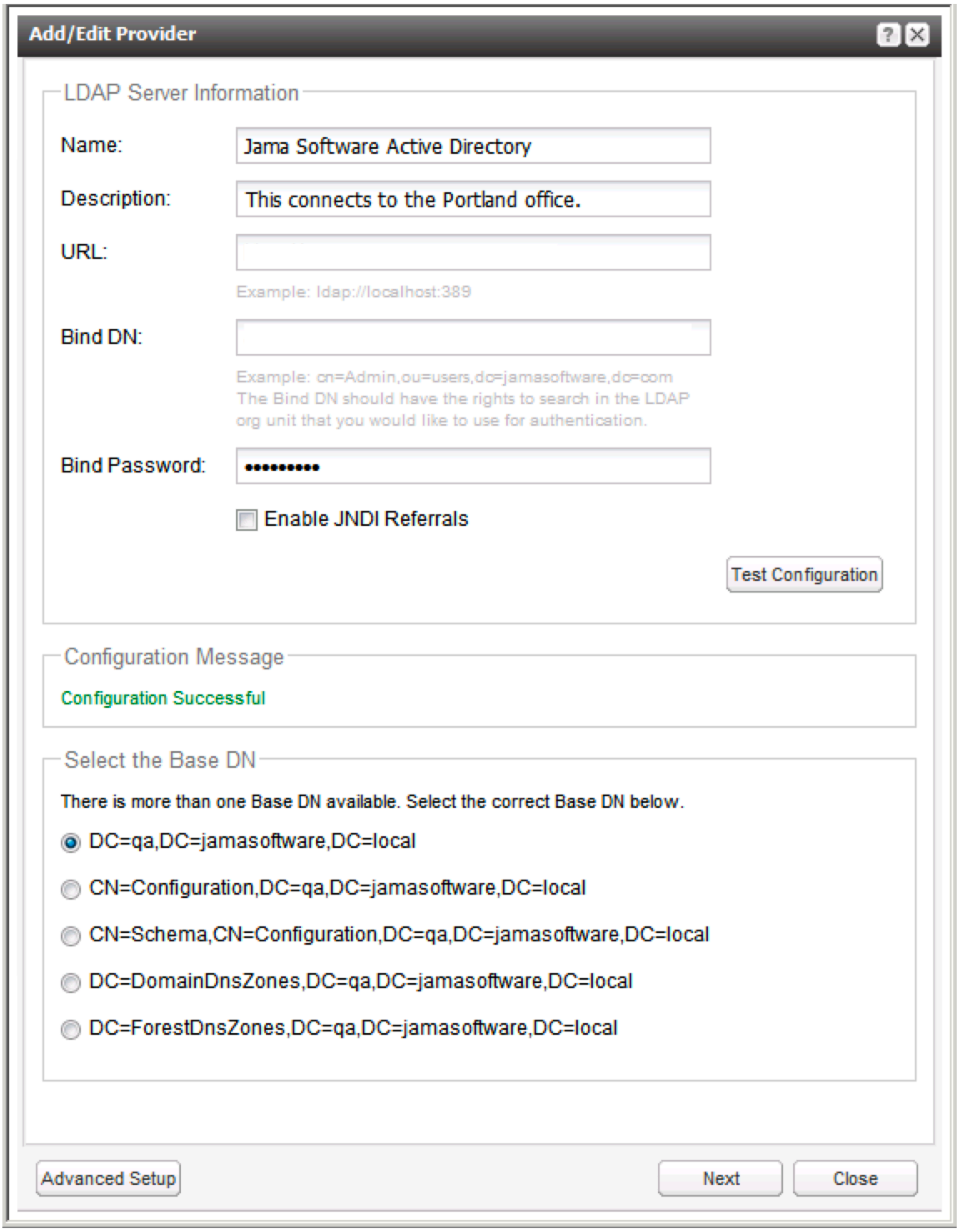
Enable Self Registration: □

Default Organization for Self-registered User: Select an organization...

Default User Group for Self-registered User: Select an User Group...

No Data

3. Configure the authentication properties for the method you are using.
   - **Enable LDAP** — Select this to enable LDAP and disable the default Jama Connect authentication. Save the settings for changes to take effect.
   - **Enable Self Registration** — Users can register themselves by logging in to Jama Connect using their LDAP credentials. If successfully authenticated, they get a prompt to register for Jama Connect. Without self-registration, users must be added manually by an organization administrator. Once registered, users will be assigned a license type based the rules below. An organization or project administrator must then assign permissions for that user.
     - If there are available creator licenses, they are assigned a creator license.
     - If there are no named creator licenses, users are assigned floating creator licenses (shared among others).
     - If there are no creator or floating creator licenses available, you can still create users, but they are set to inactive. An organization administrator must manually assign the user an active license when one becomes available.
   - **Default organization for self-registered user** — Select the organization that self-registered users are assigned by default. There should only be one option.
   - **Default user group for self-registered user** — Select the default group to which a self-registered user should be assigned. Organization administrators will need to assign permissions to self-registered users.
4. You can configure multiple directories with LDAP authentication. To add a new provider, select **Add AD Provider** or **Add LDAP Provider**, depending on the LDAP tool you use.
5. In the window that opens, provide the following server information used to connect to the Active Directory or LDAP server, then click **Next**.



Name: Jama Software Active Directory

Description: This connects to the Portland office.

URL:

Example: ldap://localhost:389

Bind DN:

Example: cn=Admin,ou=users,dc=jamasoftware,dc=com
The Bind DN should have the rights to search in the LDAP org unit that you would like to use for authentication.

Bind Password: ●●●●●●●●●●

□ Enable JNDI Referrals

Configuration Successful

There is more than one Base DN available. Select the correct Base DN below.

● DC=qa,DC=jamasoftware,DC=local

○ CN=Configuration,DC=qa,DC=jamasoftware,DC=local

○ CN=Schema,CN=Configuration,DC=qa,DC=jamasoftware,DC=local

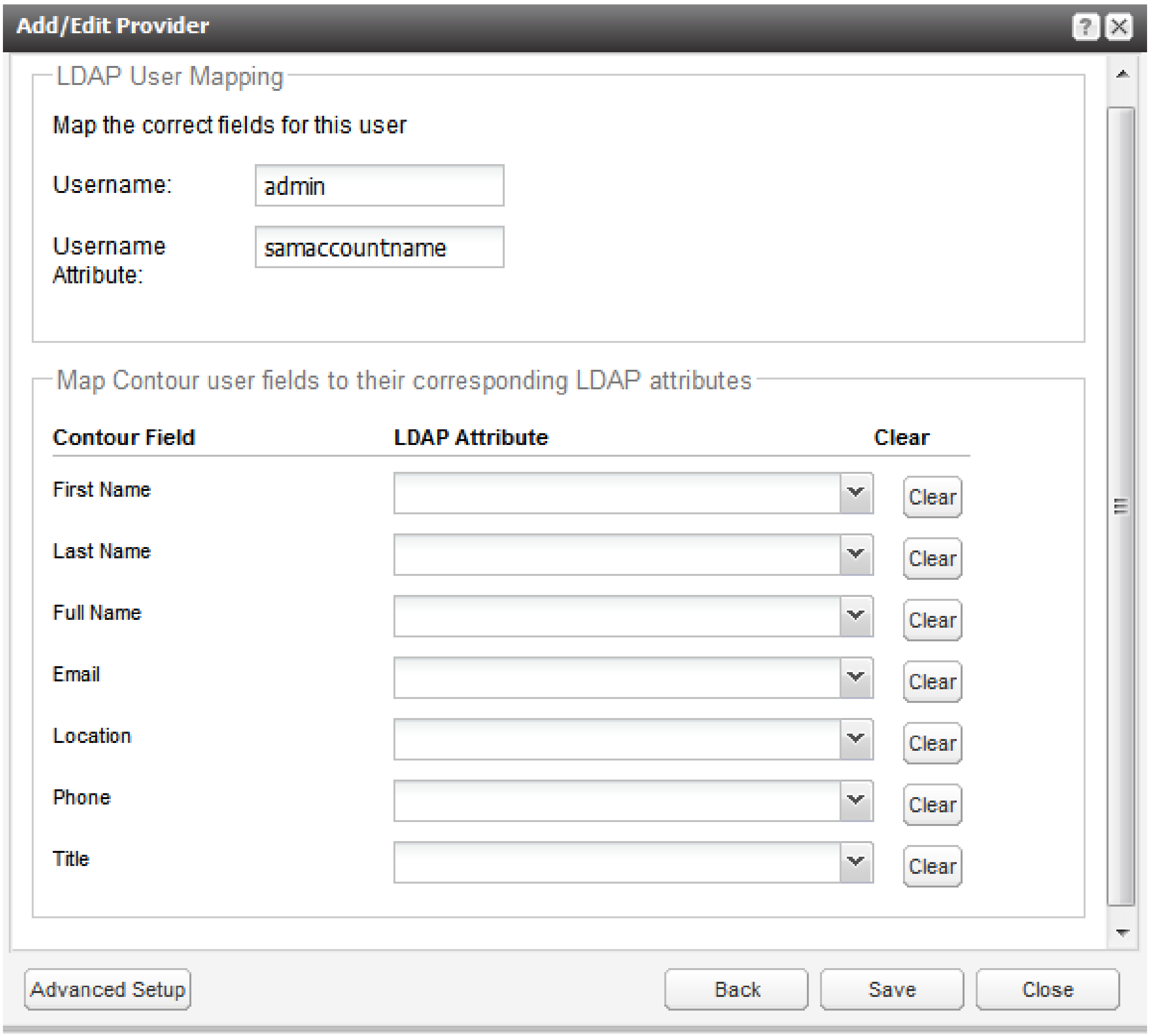
○ DC=DomainDnsZones,DC=qa,DC=jamasoftware,DC=local

○ DC=ForestDnsZones,DC=qa,DC=jamasoftware,DC=local

- **Name** — Name of the connection that will appear in the Jama Connect interface.
- **Description** — Description of the connection that will appear in the Jama Connect interface.
- **URL** — The URL to the Active Directory or LDAP server.
- **Bind DN** — The reference to the account that Jama Connect will use to perform all actions against the Active Directory or LDAP server. This field accepts the Distinguished Name of the account ("cn=John Doe,ou=Users,dc=jamasoftware,dc=com").
  Some Active Directory servers support the use of Full Name ("John Doe") or Email ("jdoe@domain.com").
- **Bind Password** — The password of the Bind DN account.

- **Test Configuration** — Select **Test configuration** to test for a successful connection to the specified server and bind account information. If successful, a "Configuration Successful" message will display in the window and the Base DN selection screen will expand.
- **Select the Base DN** — The Base DN is the directory where users in Active Directory or LDAP exist that need to be added to Jama. Successfully tested configurations will load a radio button selection list of all available Base DNs.

6. Specify the attributes in Active Directory and LDAP that automatically populates the Jama Connect user attributes.



Add/Edit Provider

LDAP User Mapping

Map the correct fields for this user

Username: admin

Username Attribute: samaccountname

Map Contour user fields to their corresponding LDAP attributes

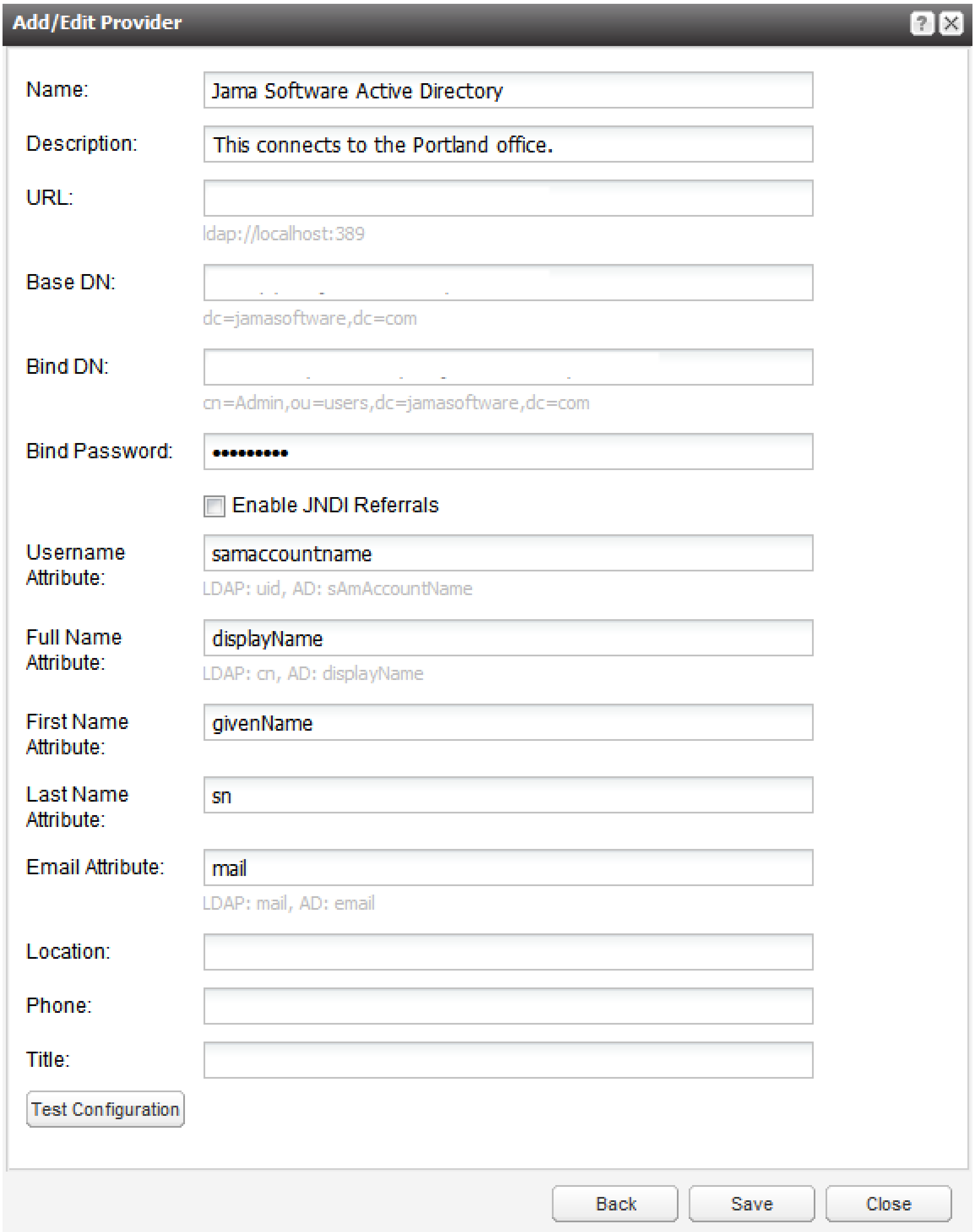
Contour Field	LDAP Attribute	Clear
First Name		Clear
Last Name		Clear
Full Name		Clear
Email		Clear
Location		Clear
Phone		Clear
Title		Clear

- **Username** — Enter the username of a sample user that exists in the specified Base DN.
- **Username Attribute** — Enter the attribute where the username value is stored (for example, Active Directory commonly uses "samaccountname").

7. Select **Next** to validate that the provided username and username attribute exist. If successful, the window expands to show a selection list of all available attributes for each of the Jama Connect user attributes.

- **Jama User Attributes** — First Name, Last Name, Full Name, Email, Location, Phone, Title.
- **LDAP attribute** — The selection drop-down shows all available directory attributes that are connected to the provided username. Select the correct value in the selection list that matches the Jama Connect user attribute.

8. Select **Advanced setup** if you know all the details of the connection and user attribute values. If you choose this option, you must add the **Full Name Attribute** or errors will result.



Add/Edit Provider

Name: Jama Software Active Directory

Description: This connects to the Portland office.

URL:

ldap://localhost:389

Base DN:

dc=jamasoftware,dc=com

Bind DN:

cn=Admin,ou=users,dc=jamasoftware,dc=com

Bind Password: ●●●●●●●●●

□ Enable JNDI Referrals

Username Attribute: samaccountname

LDAP: uid, AD: sAmAccountName

Full Name Attribute: displayName

LDAP: cn, AD: displayName

First Name Attribute: givenName

Last Name Attribute: sn

Email Attribute: mail

LDAP: mail, AD: email

Location:

Phone:

Title:

9. After saving the connection, select **Synchronize Now** to manually sync all existing users in Jama Connect to LDAP. This updates user information with attributes from LDAP.

Any Jama Connect users who are not registered in LDAP are deactivated. Users in LDAP that do not already exist in Jama Connect aren't synchronized. New users must be added manually [18] with existing LDAP credentials.

Troubleshooting LDAP errors (traditional)

If any errors occurred during installation, use this table to troubleshoot the issues.

Error message	Reason
Unable to communicate with LDAP server; nested exception is javax.naming.CommunicationException: localhost:389 [Root exception is java.net.ConnectException: Connection refused: connect]	Can't connect to the server. Check the URL and make sure port 389 is open.
Operation failed; nested exception is javax.naming.AuthenticationException: [LDAP: error code 49 - Invalid Credentials]	The BindDn or password is incorrect.
Can't find user	Indicates that the Base Dn, Bind Dn, and Bind Password can be connected to accurately (a good connection to LDAP). Either the Login Name Attribute was not filled in correctly or the Sample User does not exist in the Base Dn indicated.
Can't authenticate user	The sample user password is incorrect. However, this message indicates a successful connection to LDAP and that the sample user was found in the Base Dn.
Operation failed; nested exception is javax.naming.PartialResultException: Unprocessed Continuation Reference(s); remaining name	The cause is usually the base URL is incomplete (too broad).
Operation failed; nested exception is javax.naming.ServiceUnavailableException: adunit:636; socket closed. Port 636 is for SSL.	Either SSL isn't supported by Spring LDAP or the certificate is incorrect. Solution: Try using ldap protocol. For example: ldaps://myserver.example.com:636.

Make sure you entered the correct information for the type of LDAP you are configuring:

- **Active Directory**
  URL: 'ldap://localhost:389'
  Base Dn: 'ou=Users,dc=<domainname>,dc=com'
  Bind Dn: 'cn=Admin,ou=Admin Users,dc=<domainname>,dc=com'
  Bind Password: 'password'
  Login Name Attribute: 'sAmAccountName'
  Email Attribute: 'email'
  User Name Attribute: 'displayName'
  Sample User: 'admin'
  Sample User Password: 'password'
- **LDAP**
  URL: 'ldap://localhost:389'
  Base Dn: 'ou=Users,dc=<domainname>,dc=com'
  Bind Dn: 'cn=Admin,ou=Admin Users,dc=<domainname>,dc=com'
  Bind Password: 'password'
  Login Name Attribute: 'uid'
  Email Attribute: 'mail'
  User Name Attribute: 'cn'
  Sample User: 'admin'
  Sample User Password: 'password'

IMPORTANT

If you are using SSL, you must use the ldaps protocol. For example, ldaps://myserver.example.com:636

The Base Dn and Bind Dn values won't accept a domain-only value. At least one additional level is required, such as the 'ou=Users' shown in the example above.

Take note of the "Can't find/authenticate user" errors. Errors often indicate a successful connection, but the Sample User/Password are incorrect.

IMPORTANT

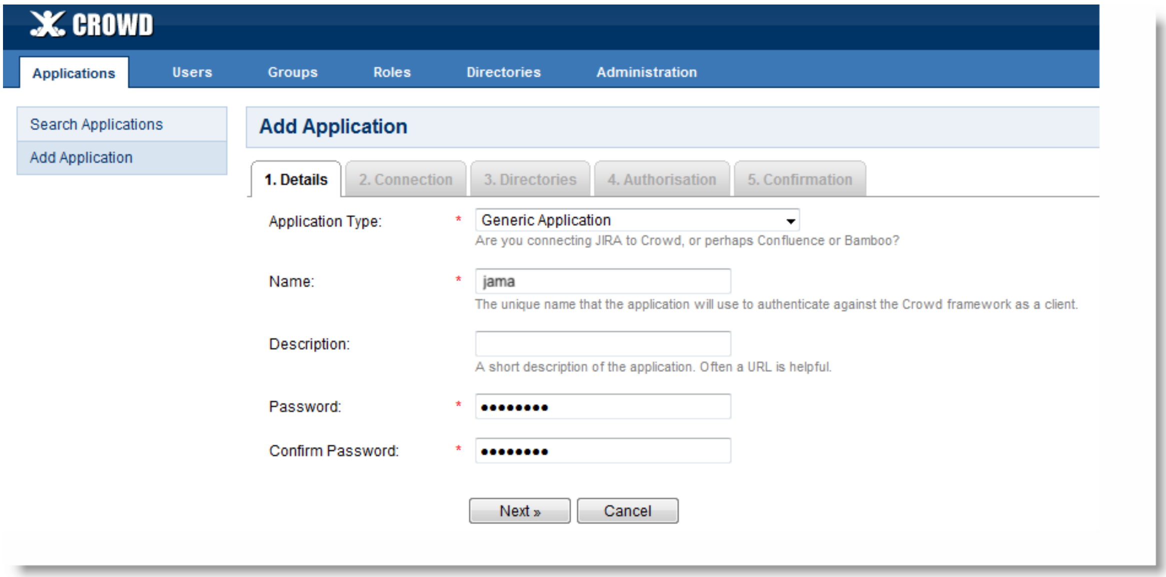
The Sample User and Password fields are deleted every time the configuration window is closed.

Configure Crowd authentication (traditional)

Use Crowd to manage users and groups within a single system. Jama Connect can accept user details from Crowd and sync them with authentication data in Jama Connect.

To configure Crowd authentication:

1. Log in to Crowd as an administrator.
2. Select **Applications > Add Application**, fill in the fields for a new application and select **Next**.



Add Application

Application Type: * Generic Application
Are you connecting JIRA to Crowd, or perhaps Confluence or Bamboo?

Name: * jama
The unique name that the application will use to authenticate against the Crowd framework as a client.

Description:
A short description of the application. Often a URL is helpful.

Password: * ••••••••

Confirm Password: * ••••••••

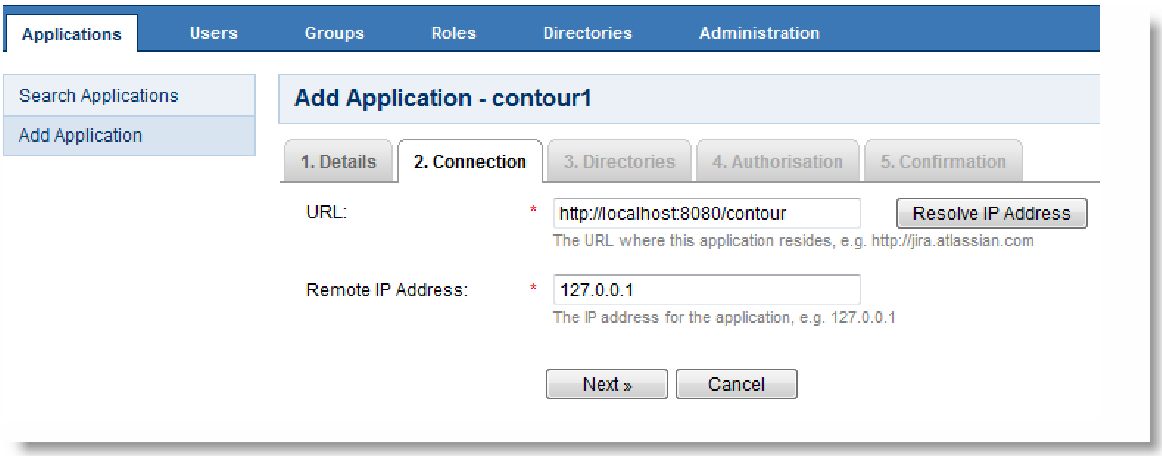
- **Application type** — Generic Application.
- **Name** — "jama" or any other unique name that identifies Jama Connect as the application.

NOTE

The name must match. For example, lower case "jama" in the above example.

- **Description** — (Optional) Provide a short description of the application.
- **Password** — Create a new password that Jama Connect uses to access Crowd.

3. Enter the URL and IP address for Jama Connect, then select **Next**.



Add Application - contour1

URL: * http://localhost:8080/contour

The URL where this application resides, e.g. http://jira.atlassian.com

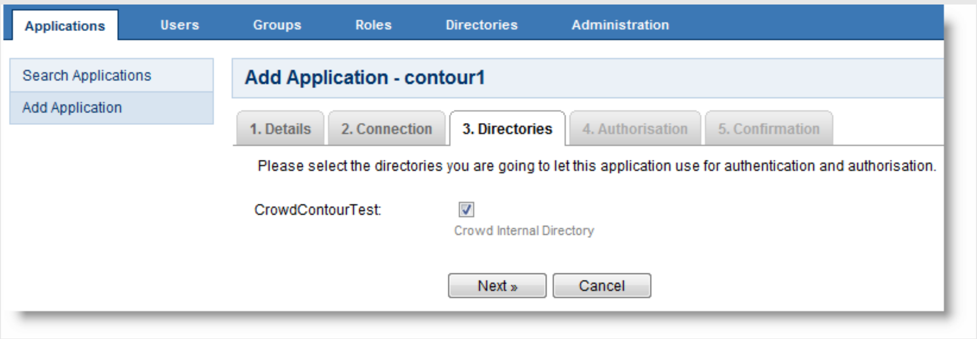
Remote IP Address: * 127.0.0.1

The IP address for the application, e.g. 127.0.0.1

4. Select the directories that control access to Jama Connect, then select **Next**.

NOTE

These directories must exist prior to inclusion.



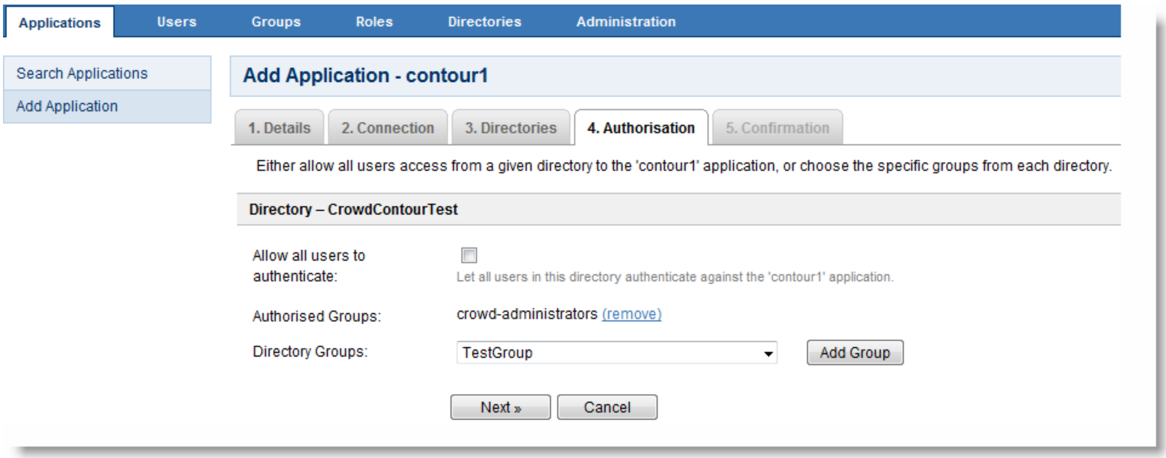
Add Application - contour1

Please select the directories you are going to let this application use for authentication and authorisation.

CrowdContourTest: ☑

Crowd Internal Directory

5. Select the particular groups in the Crowd Directory you want to have access to Jama Connect, or choose "all users in the directory" if you want all users to have access, then select **Next**.



Add Application - contour1

Either allow all users access from a given directory to the 'contour1' application, or choose the specific groups from each directory.

Directory – CrowdContourTest

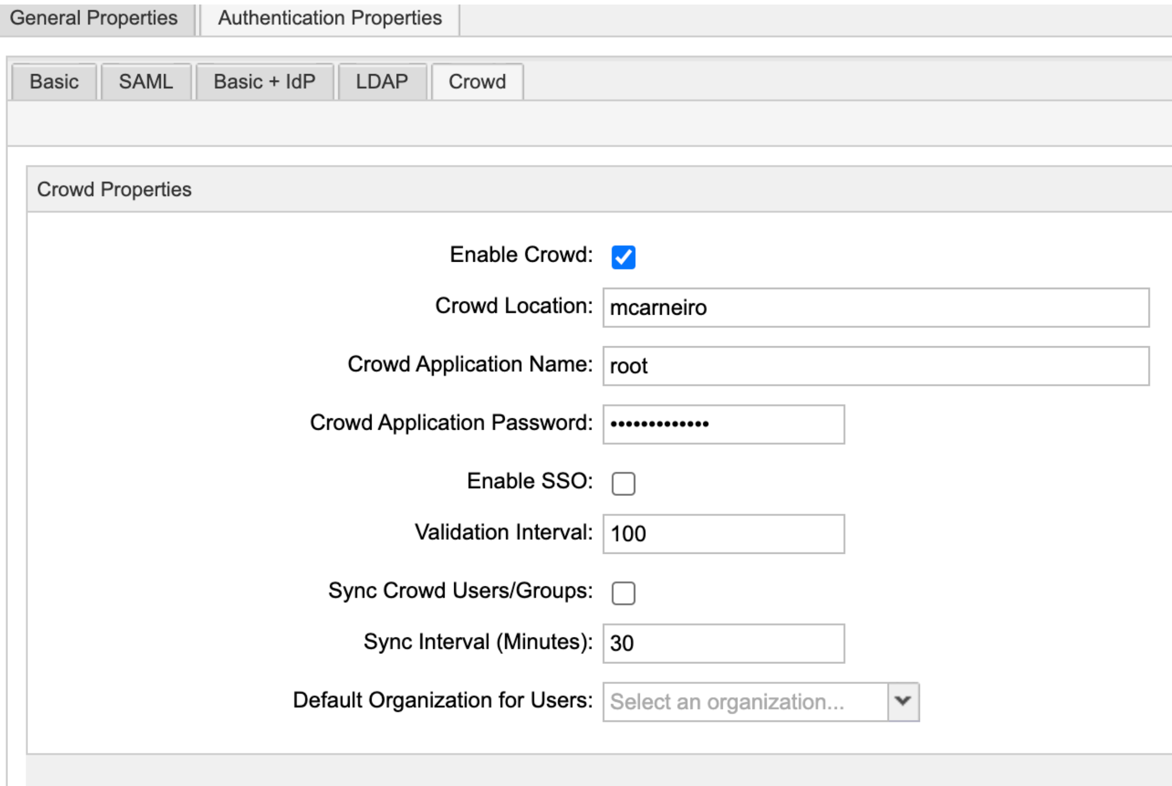
Allow all users to authenticate: □

Let all users in this directory authenticate against the 'contour1' application.

Authorised Groups: crowd-administrators (remove)

Directory Groups: TestGroup

6. Review your configuration, then select **Save**.
7. Log in to Jama Connect as the root user [15].
8. Select **System Properties > Authentication Properties** and complete the following fields.



Enable Crowd: ☑

Crowd Location: mcarneiro

Crowd Application Name: root

Crowd Application Password: •••••••••••••

Enable SSO: □

Validation Interval: 100

Sync Crowd Users/Groups: □

Sync Interval (Minutes): 30

Default Organization for Users: Select an organization...

- **Enable Crowd** — Select to enable or disable Crowd Connector. When disabled, the Jama Connect database is used for users and passwords.
- **Crowd location** — Enter the URL for the Crowd server.
- **Crowd application name** — Name of the application created in step 2 above.
- **Crowd application password** — Enter the password for Jama Connect that was created in Crowd.
- **Validation interval** — The amount of times a user can access the application prior to re-authenticating. The larger the number, the less communication with Crowd.
- **Sync Crowd users and groups** — Select this option to push Crowd Groups and Users into Jama Connect at regular intervals. Make sure you understand how users and groups in Crowd interact with Jama Connect [41] before you do this.

  When syncing with Crowd, Jama Connect assigns licenses as follows:
  - If there are available named creator licenses, users are assigned a named creator license.
  - If there are no available creator licenses, users are assigned a float license.
  - If there are no available creator or float licenses, the user is skipped and it appears in the log.

  When Crowd is synced, Jama Connect runs through its list of users, adds new users, and modifies existing users in the Jama Connect userbase. When that's complete, Jama Connect runs through the list again to see if there are any existing users in the Jama Connect userbase that need to be deactivated.

  Since Jama Connect makes two passes at adding and deactivating users, you might need to sync twice consecutively for it to work. For example, if you reach your license threshold, don't use float licenses, try adding a new user and deactivating an existing user, or must sync twice consecutively before the new user is given a named license.

IMPORTANT

You can also select **Manual Sync** at the bottom of the window to manually synchronize all users and groups. Manual sync removes all Jama Connect configured Users and Groups and insert Crowd users and groups.

  - **Sync interval** — Enter the timing interval you would like for Crowd to synchronize groups and users with Jama Connect. This defaults to 30 minutes.
  - **Default Organization for User** — Only required when multiple organizations are setup with Jama Connect.

9. Select **Save**.
10. Select **Test Connection** to test if the configuration values are valid.

Users who are registered in Jama Connect, but not in Crowd, can't access Jama Connect. Other users won't be able to add disabled users to reviews or notifications.

How users and groups work in Crowd (traditional)

How users and groups function is impacted when you synchronize users and groups in Crowd connector [38].

The following actions change:

- All groups and users in Crowd that aren't in Jama Connect are added to Jama Connect. New users are assigned the most licenses available. When no licenses are available, users are created and **Inactive**.
- All groups in Jama Connect that aren't in Crowd are removed.
- All users that are in Jama Connect, but not in Crowd, are deactivated.
- Going forward, all user and organizational group management activities are performed in Crowd.
- Organization administrators no longer create or edit users and organizational groups in Jama Connect because they are automatically created from Crowd.

The following actions stay the same:

- Organization administrators retain the ability to assign a license type to users.
- Users can continue to upload avatar icons.
- Organization administrators and project administrators continue to manage project groups within individual projects.

> **IMPORTANT**
> Project level project groups are only managed in Jama Connect and aren't visible in Crowd.

- An organization or project administrator continues to manage user and group permissions in Jama Connect.

Action in Crowd	Result in Jama Connect
Group(s) added to “Jama” Application in Crowd	Group created. The name of the group is reused if it already exists.
Users added to the "Jama" group in Crowd	Users added. Attributes in Jama Connect are overwritten by values from Crowd if a user already exists.
Group attributes modified	Group attributes are modified.
User attributes modified	User attributes are modified.
User added to group	User is added to group.
User removed from group	User is removed from group.
Group deleted	Group is deleted.
User is deactivated	User is deactivated.

Action in Crowd	Result in Jama Connect
User activated	User is activated. If the user doesn't exist, a new user is created. The new user is assigned the highest available license. If a license isn't available, the user is inactive.

Backing up and restoring your data (traditional)

Backing up your data is an essential part of maintaining and securing your self-hosted environment. With regular backups, you can easily restore settings and content when you update your application server hardware or if you lose data.

NOTE

This information applies to self-hosted environments only.

You can back up and restore your data using several methods:

- **Replicated snapshot** — A function of Replicated software that creates a backup of the Admin Console environment. It includes all Admin Console settings, the Replicated database, Docker images, and Docker container volumes.
- **.jama or XML file** — A method with built-in automation, recommended for migrations and refreshes. A .jama file includes the database and /data directory. An XML file includes only the database.
- **Native database backup** — The proprietary backup/restore system for MySQL and SQL Server databases. Recommended only if your database is extremely large.
- **Backup of user data directories [59]** — Where all physical artifacts [59] are stored.

IMPORTANT

Create a backup regularly: daily, weekly, or monthly. Include in your regular backup a Replicated snapshot (Admin Console environment) and a .jama or XML file backup (database and /data directory).

Create a Replicated snapshot (traditional)

A Replicated snapshot is a backup of the Admin Console environment. It includes the Replicated database, registry images, and container volumes (when specified).

A Replicated snapshot can be taken while Jama Connect is running without interruption.

IMPORTANT

Replicated snapshots don't include the contents of the Jama Connect database, the contents of the /data directory, or the log files. To back up those items, see Back up to .jama or XML file [46].

When to create a snapshot

- When migrating Jama Connect to new hardware [62]. When you replace one server with another (create a clone), you can perform a fresh installation of Docker and Replicated, then restore from the snapshot.
- During disaster recovery.
- Before upgrading your software (Jama Connect or Replicated).

Snapshot location

By default, Replicated snapshots are stored in this location:

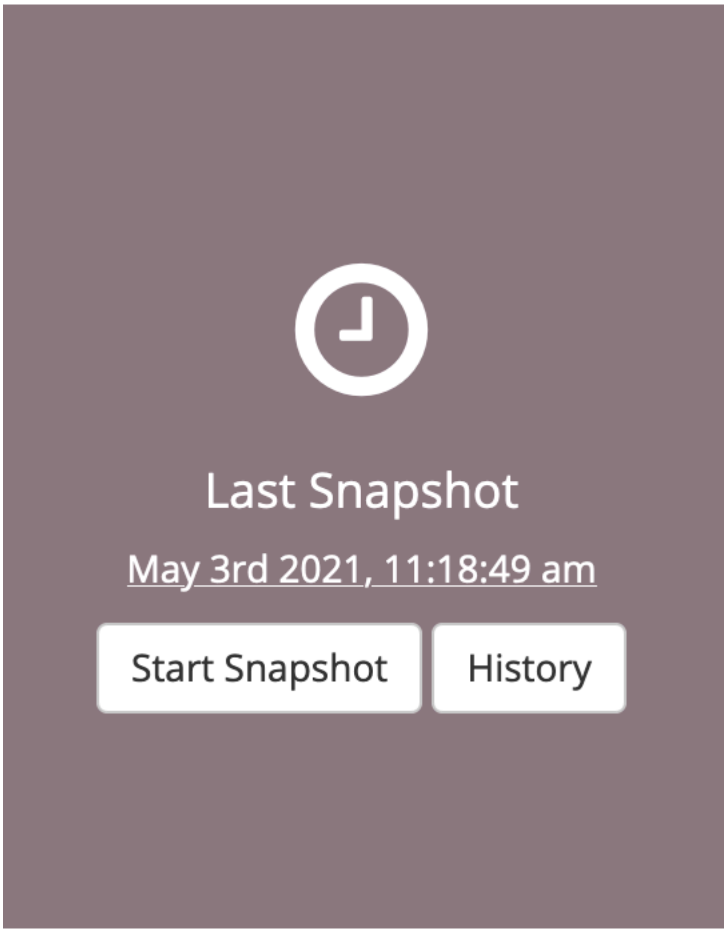
```
/var/lib/replicated/snapshots
```

To include the Replicated snapshots in your regular backups of Jama Connect, you can change the location for the snapshots, like this:

```
/data/replicated/snapshots
```

To create a Replicated snapshot:

1. (Optional) Identify and configure a custom directory for your snapshots: Select **Admin Console > Settings** (gear icon) **> Console Settings > Snapshots**.
2. Create a snapshot: Open the Admin Console and select **Start Snapshot**.
   Snapshots Enabled changes to **Snapshotting** and a progress spinner appears while it backs up the registry data and container volumes. When the snapshot is ready, you see a timestamp for the last snapshot.



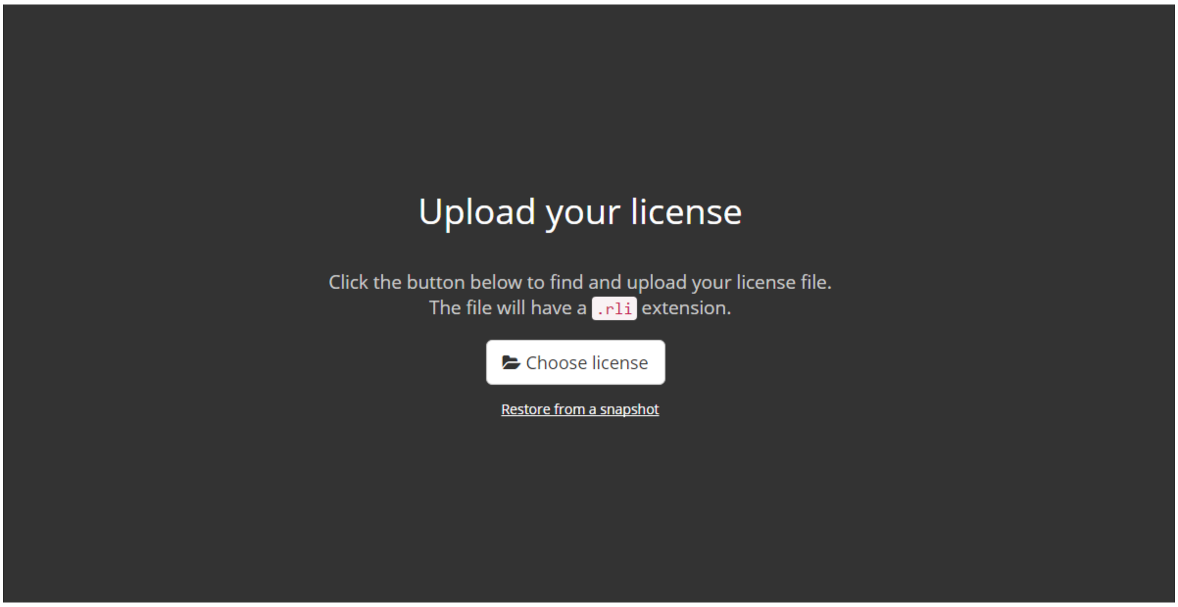
If the Replicated snapshot fails, the dashboard displays an error message with technical detail of the failure, including the file or folder involved. This error message is generated from the underlying file system (for example, readdirent: errno 523), which means the problem is likely with the underlying file system and not the Jama Connect installation.

Restore all settings from a Replicated snapshot (traditional)

When you set up a new application server for Jama Connect, you can restore the Admin Console settings that you saved in a Replicated snapshot.

Snapshots include the Replicated database, registry images, and container volumes (when specified).

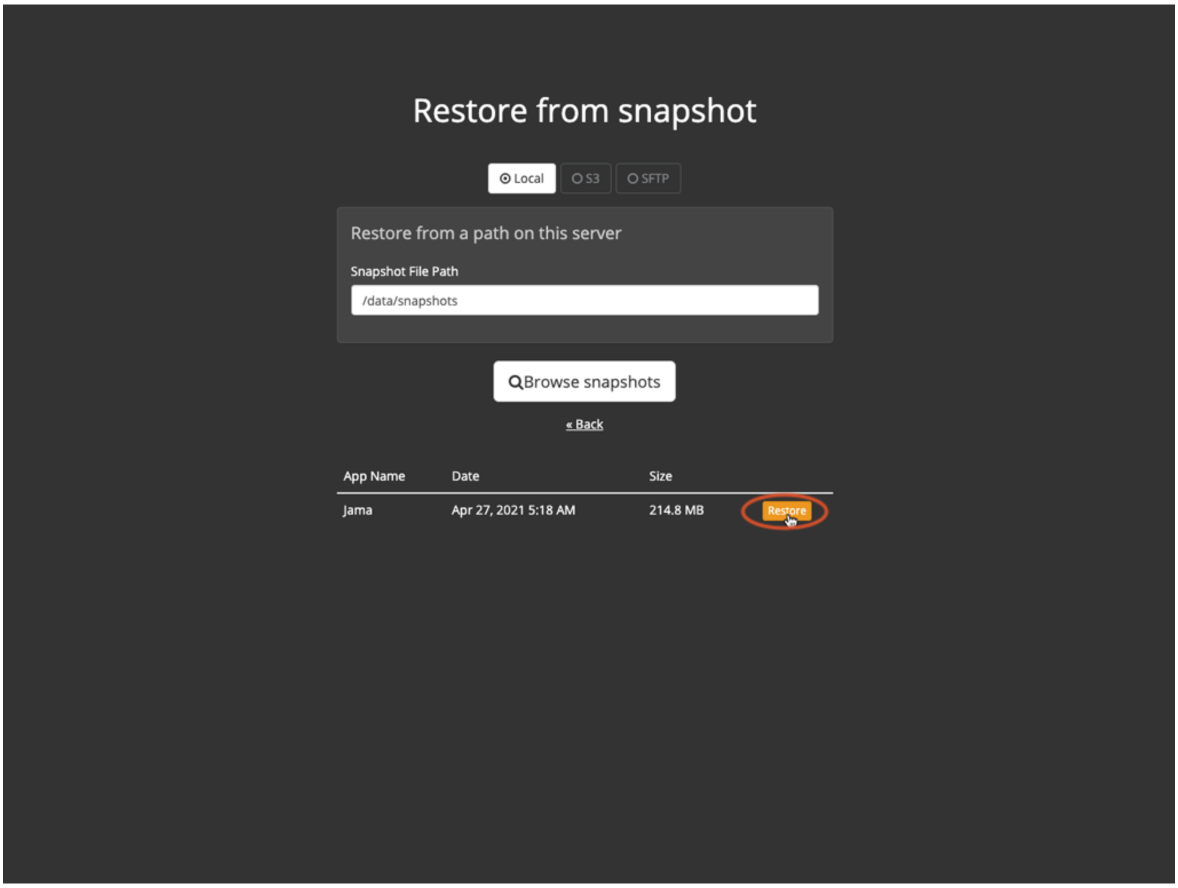
1. Install Jama Connect on the new server.
2. When the page Upload your license is displayed, select **Restore from a snapshot**.



Upload your license

Click the button below to find and upload your license file.
The file will have a `.rli` extension.

3. When the Restore from snapshot page is displayed, enter the path to your snapshot and click **Restore**.
   Use the same path on the new server as you did on the old server. For example, **/var/lib/replicated/snapshots** or **/data/snapshots**.



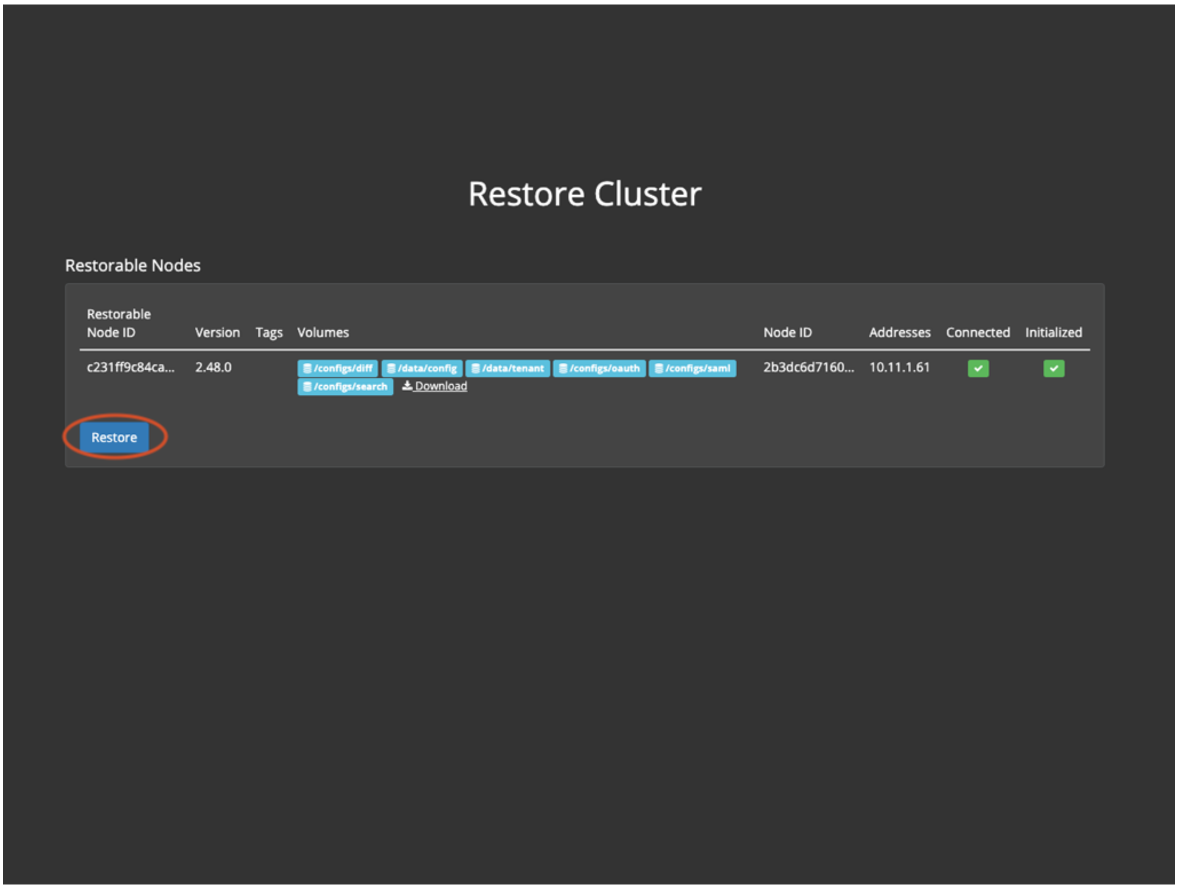
Restore from snapshot

Restore from a path on this server

Snapshot File Path: /data/snapshots

App Name	Date	Size	
Jama	Apr 27, 2021 5:18 AM	214.8 MB	Restore

4. On the Restore Cluster page, click **Restore**.

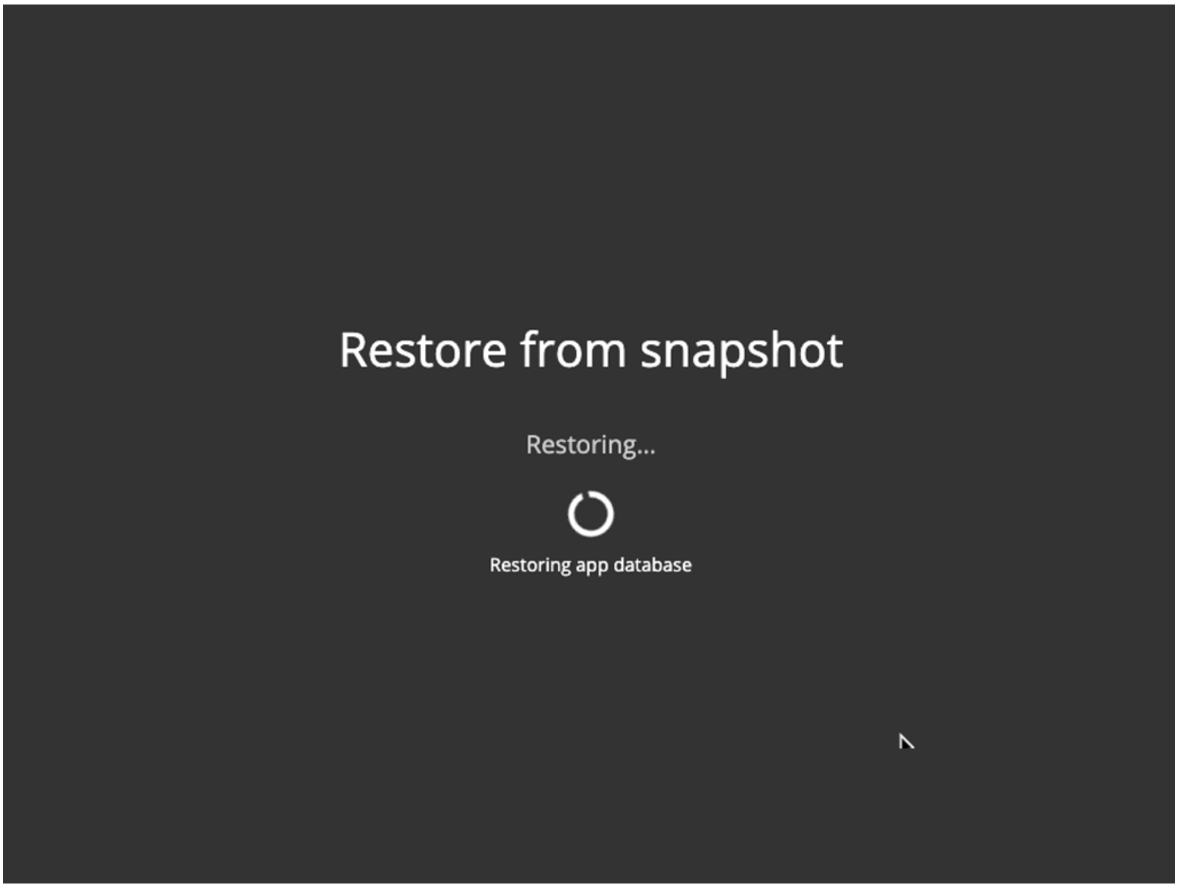


Restore Cluster

Restorable Nodes

Restorable Node ID	Version	Tags	Volumes	Node ID	Addresses	Connected	Initialized
c231ff9c84ca...	2.48.0		/configs/diff /data/config /data/tenant /configs/oauth /configs/saml /configs/search Download	2b3dc6d7160...	10.11.1.61	✓	✓

The system displays a progress page as it restores your data from the snapshot.



Restore from snapshot

Restoring...

Restoring app database

Back up to .jama or XML (traditional)

We recommend backing up to a .jama or XML file for migrations and refreshes because this method has built-in automation. You can avoid manual changes which can impact the integrity of the data.

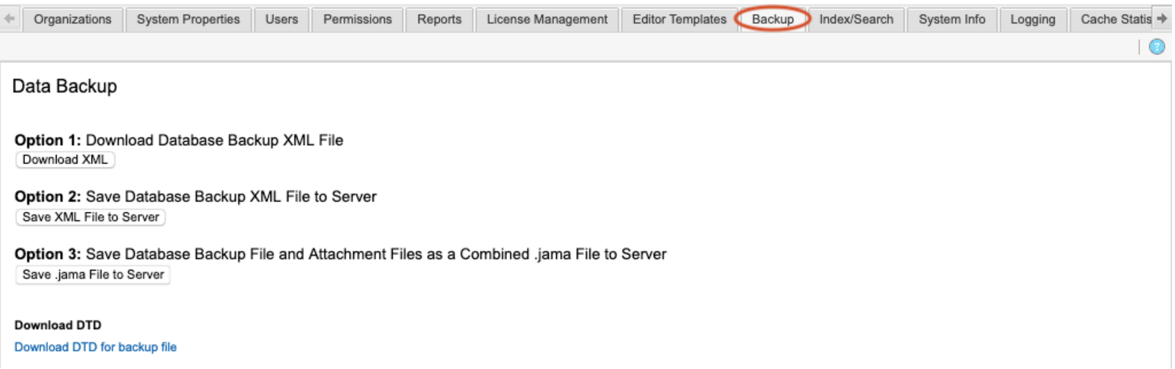
A .jama file backup includes the database and /data directory. An XML file backup includes only the database.

Important considerations

- If SAML is enabled, disable it before backing up your data. After you restore your instance of Jama Connect, you must re-enable SAML.
- Backups must be done manually; they can't be scheduled automatically.
- Make sure you have enough available disk space [50].
- Make sure Jama Connect is in maintenance mode [24] before you create a backup.
- If you are using a version of Jama Connect prior to version 8, generate backups during a maintenance window and inform users, including API users, not to use the application.
- Regardless of what version you are using, all integrations must be disabled.

To back up to a .jama or XML file:

1. Log in to Jama Connect as the root user [15].
2. Select the **Backup** tab to see the backup options.



Data Backup

Option 1: Download Database Backup XML File

Download XML

Option 2: Save Database Backup XML File to Server

Save XML File to Server

Option 3: Save Database Backup File and Attachment Files as a Combined .jama File to Server

Save .jama File to Server

Download DTD

Download DTD for backup file

3. Choose a backup method (listed here in recommended order).

Method	Scenario	Select...
Save .jama file to the application server.	Migrating between versions later than 8.0.	**Save .jama File to server**
Save XML file to the application server.	• Migrating between different types of databases [63] • Migrating version earlier than 8.0	**Save XML File to Server**
Download XML database backup to your workstation.	• If you can't access the application server • For smaller databases	**Download XML**
Download document type definition (DTD) to your workstation.	If all other methods fail	**Download DTD**

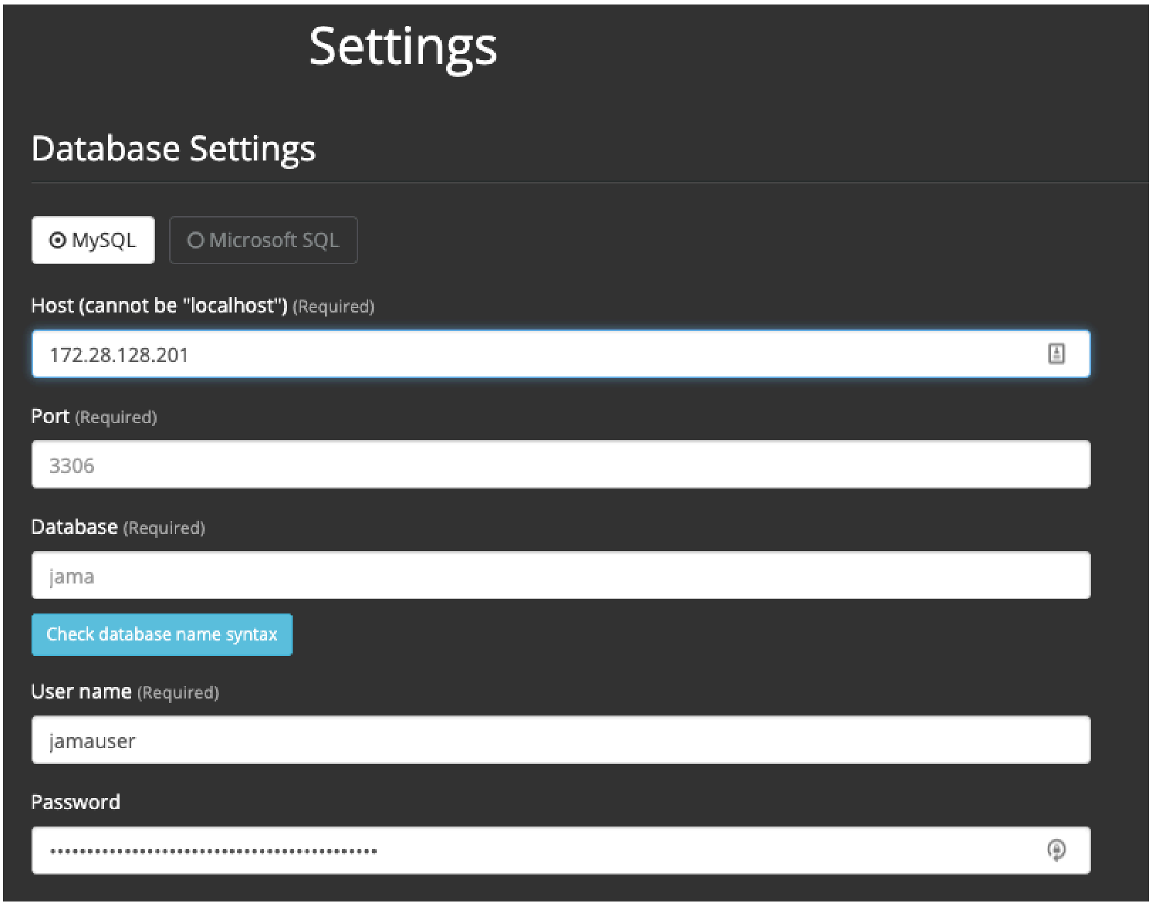
The backup process is complete.

Restore to a new server from .jama or XML (traditional)

When you set up a new server, you can install Jama Connect and restore data using the .jama or XML file backup you created. See Back up to .jama or XML file [46].

> **IMPORTANT**
>
> If you use SAML in your environment, it was disabled before you created the .jama or XML backup. When you install Jama Connect on a new server, it will be running Basic authentication. You must re-enable SAML to use that authentication method.

1. Log in to Jama Connect as the root user on the new server.
2. Install Jama Connect:
   - On the Settings page under **Database settings**, select the database you are using: **MySQL** or **SQL Server**.



Settings

Database Settings

● MySQL ○ Microsoft SQL

Host (cannot be "localhost") (Required)

172.28.128.201

Port (Required)

3306

Database (Required)

jama

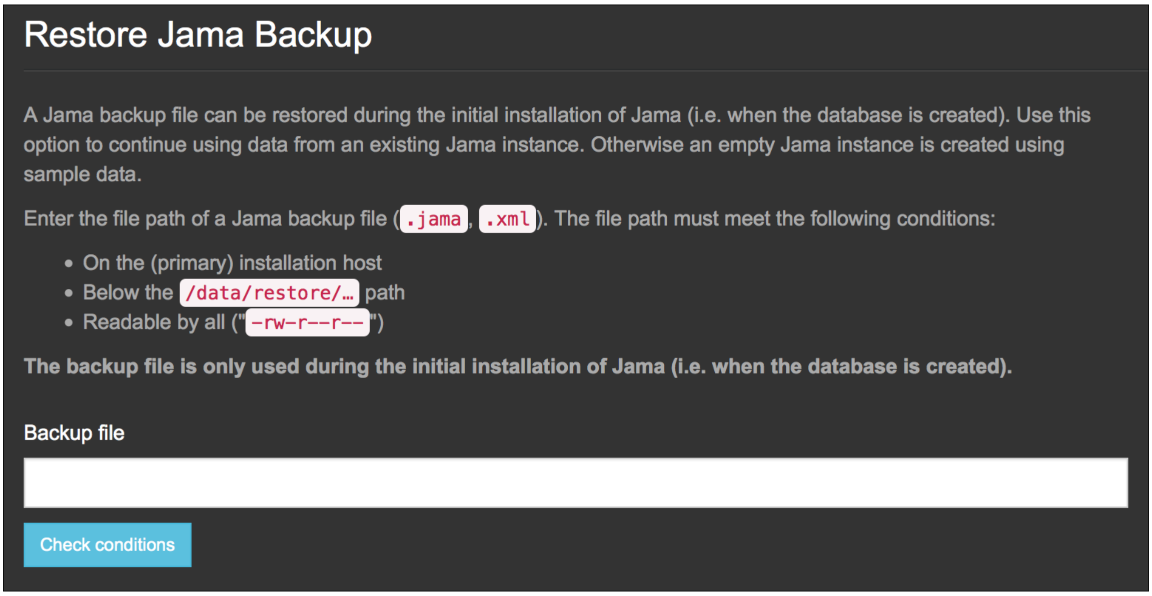
User name (Required)

jamauser

Password

••

- Under **Restore Jama Backup**, enter the file path for the backup you created, (for example, /data/restore/your_backup.xml). Select Check conditions to make sure the path to your backup file meets the conditions listed onscreen.



Restore Jama Backup

A Jama backup file can be restored during the initial installation of Jama (i.e. when the database is created). Use this option to continue using data from an existing Jama instance. Otherwise an empty Jama instance is created using sample data.

Enter the file path of a Jama backup file (`.jama`, `.xml`). The file path must meet the following conditions:

- On the (primary) installation host
- Below the `/data/restore/…` path
- Readable by all ("`-rw-r--r--`")

The backup file is only used during the initial installation of Jama (i.e. when the database is created).

Backup file

IMPORTANT

You must have an empty database for the restore process to complete.

3. For non-.jama file backups: Move existing data folders to the new application server.
4. Save and restart Jama Connect [49].

5. Log in to Jama Connect as the root user [15].
6. If your new application server has a different URL than the old one, update the base URL to reflect the change.
7. To sync your indexes with the database, index all items.

Backing up MySQL or SQL Server database (traditional)

If your MySQL or SQL Server database is extremely large, use the native backup method that comes with your database. Doing so avoids possible data corruption.

Follow instructions for whichever system you are using, MySQL or SQL Server.

> **IMPORTANT**
>
> If you are migrating from one type of SQL server to another, for example SQL Server to MySQL, use the .jama or XML file backup [46].

Maintaining your Jama Connect environment (traditional)

A system administrator is responsible for keeping the system up and running and at peak performance.

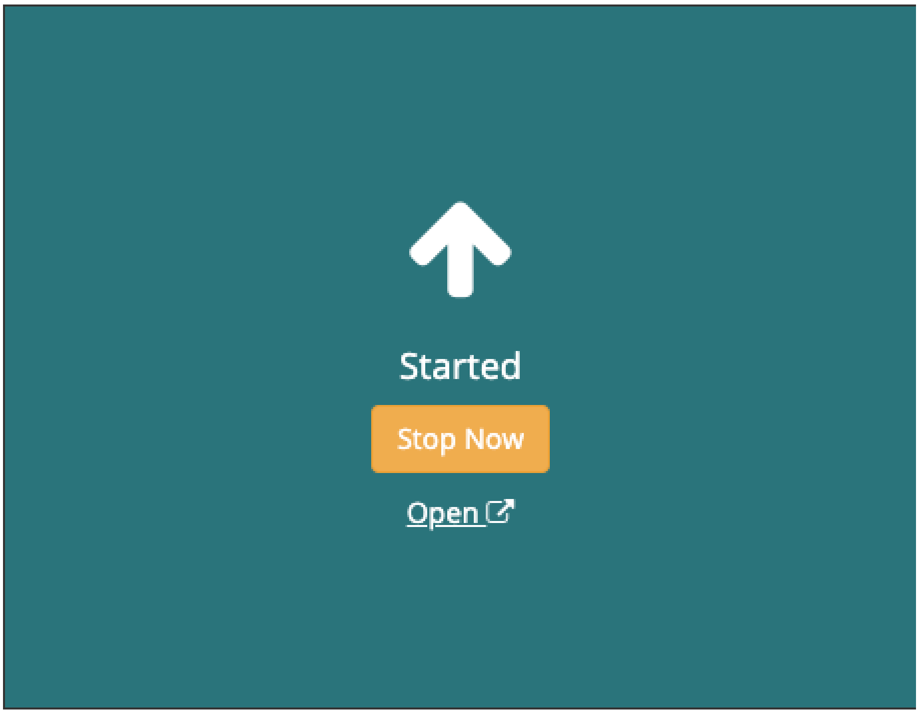
Maintaining your environment consists of ongoing tasks that are done regularly and important tasks that are done infrequently.

Ongoing/regular tasks	Infrequent but important tasks
• Monitor memory usage [50] • Maintaining your Jama Connect database [51] • Back up your data [42] • View scheduled jobs [58] • Clear cache [58] • Remove old Docker images [57] • View applied patches [58] • Stop and restart Jama Connect services (traditional) [49] • Reset Admin Console password (traditional) [52] • Deactivate and reactivate users (traditional) [51]	• Update the license (internet [52], airgap [53], or KOTS) • Update the certificate [54] • Update the application's IP address [54] • Change [55] or fix URL [56] • Delete an organization [57] • Reindex all items [59] • Upgrade the Admin Console • Upgrade Jama Connect

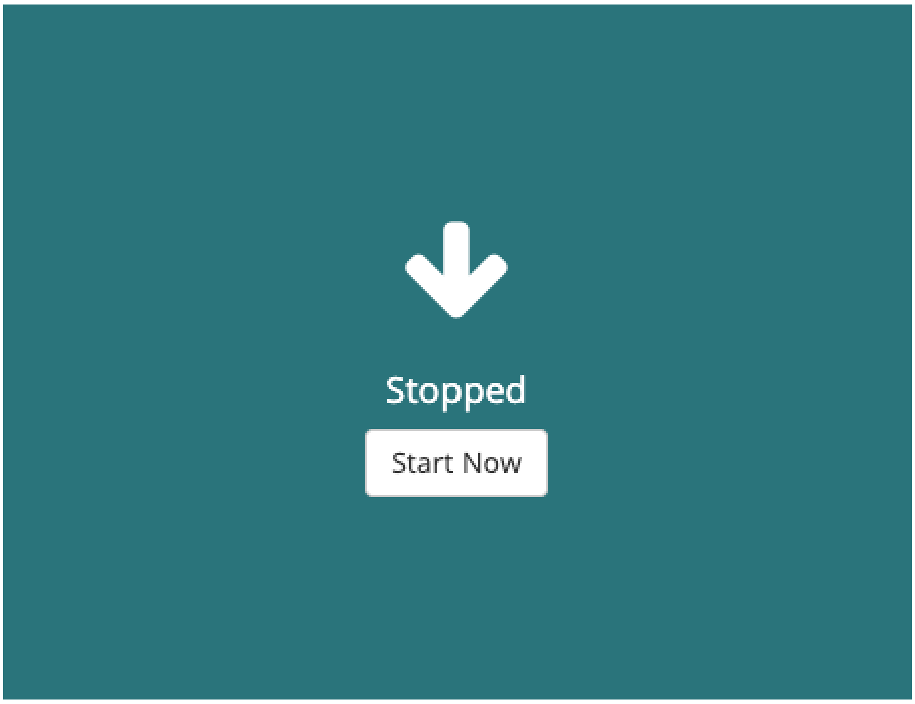
Stop and restart Jama Connect services (traditional)

Some tasks require that you stop and restart the Jama Connect services. For example, when you make changes to the application, they don’t take effect until you restart Jama Connect.

1. In the Admin Console, select **Stop Now**.



2. Wait until the screen shows "Stopped", then complete your tasks.



3. Select **Start Now** to restart Jama Connect services.
4. Wait for the components that make up Jama Connect to be started and initialized.

The dashboard displays the status in this order: **Starting**, **Queued**, then **Started**.

Monitoring memory usage (traditional)

Make sure you have allocated an appropriate amount of memory for your organization's usage. Check and adjust usage regularly to keep your environment running for best performance.

Several factors affect the amount of memory that Jama Connect requires, including:

- Size of your dataset

- Number of concurrent users
- Users' common workflows

If any of the containers' memory consumption is close to the maximum available memory, you can adjust those values. These containers in order require the most memory:

- jamacore
- elasticsearch
- searchservice

Make sure that you don't over-allocate the total memory of the application server. Also, leave approximately 5 GB of available memory (headroom) for system processes. For help in estimating your application server size, use the tables in Resource sizing for your application server.

Use one of these methods to monitor usage, then adjust your memory settings [10] as needed.

- Log in to Jama Connect as the root user.
- Select the **License management** tab to view usage by license type.
- Use the Admin Console monitoring graphs.
- Use any Java application monitoring tool that supports JMS.
- Use JavaMelody, which comes preconfigured with the Jama Connect application. To access JavaMelody, log in to Jama Connect as the root user [15] and navigate to **[your.jama.url]/javamelody**.

Maintaining your Jama Connect database

Follow these recommendations to maintain your Jama Connect database, which includes having a data backup plan and ensuring the appropriate memory is allocated to the database server.

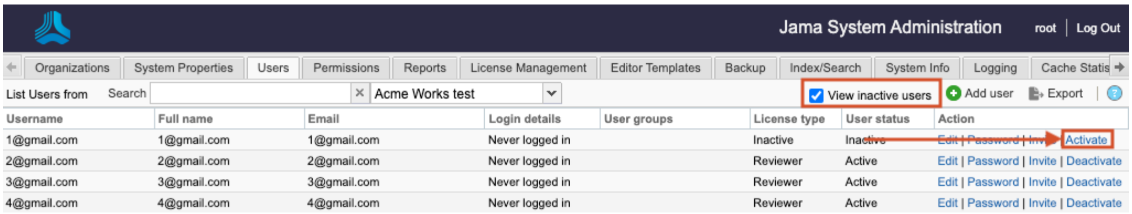
1. **Create a data backup plan** — Back up your database server at least daily and implement backup strategies as needed.
2. **Allocate appropriate memory to the database server** — Have your Database Administrator monitor memory usage and allocate memory in advance to prevent running out of memory.
3. **Configure system variables and server properties based on usage** — For details, see the documentation for MySQL or SQL Server.
4. **Check or analyze databases and tables every 6 months** — We recommend that you review or analyze your databases at least every 6 months, or after you write, change, or delete a substantial amount of data. Pay extra attention to table or index size because Jama Connect is a write-heavy application. If a table has grown out of size or the index is too large, it might need to be rebuilt.
   Use these resources to determine if an index or table must be rebuilt:
   - Leverage MySQL and SQL Server statistic gathering to detect the need to repair or analyze databases or tables.
   - Run mysqlcheck to check, repair, optimize, or analyze tables in MySQL. For details, see mysqlcheck — A Table Maintenance Program.
   - Use the Maintenance Plan Wizard tool to manage backups, data integrity checks, and statistic gathering in SQL Server. For details, see Use the Maintenance Plan Wizard.

Deactivate and reactivate users (traditional)

Users can't be deleted from Jama Connect, but you can deactivate users if they are no longer active members of the team. When you deactivate a user, their account becomes inactive and their named license is freed up for another user. You can also reactivate the user as needed.

> **IMPORTANT**
>
> You must have organization or system administrator permissions to deactivate and reactivate a user.

1. Log in to Jama Connect as the root user [15].
2. Select the **Users** tab.
3. To deactivate a user, select **Deactivate** in the Action column next to the user you want to deactivate.
   Deactivated users disappear from the list.
4. To reactivate a deactivated user:
   1. Select **View inactive users** to view all users, then select **Activate** in the Action column next to the user you want to reactivate.



List Users from Search Acme Works test ☑ View inactive users

Username	Full name	Email	Login details	User groups	License type	User status	Action
1@gmail.com	1@gmail.com	1@gmail.com	Never logged in		Inactive	Inactive	Edit | Password | Inv Activate
2@gmail.com	2@gmail.com	2@gmail.com	Never logged in		Reviewer	Active	Edit | Password | Invite | Deactivate
3@gmail.com	3@gmail.com	3@gmail.com	Never logged in		Reviewer	Active	Edit | Password | Invite | Deactivate
4@gmail.com	4@gmail.com	4@gmail.com	Never logged in		Reviewer	Active	Edit | Password | Invite | Deactivate

   2. In the User license type window, select a license type and select **Save**.

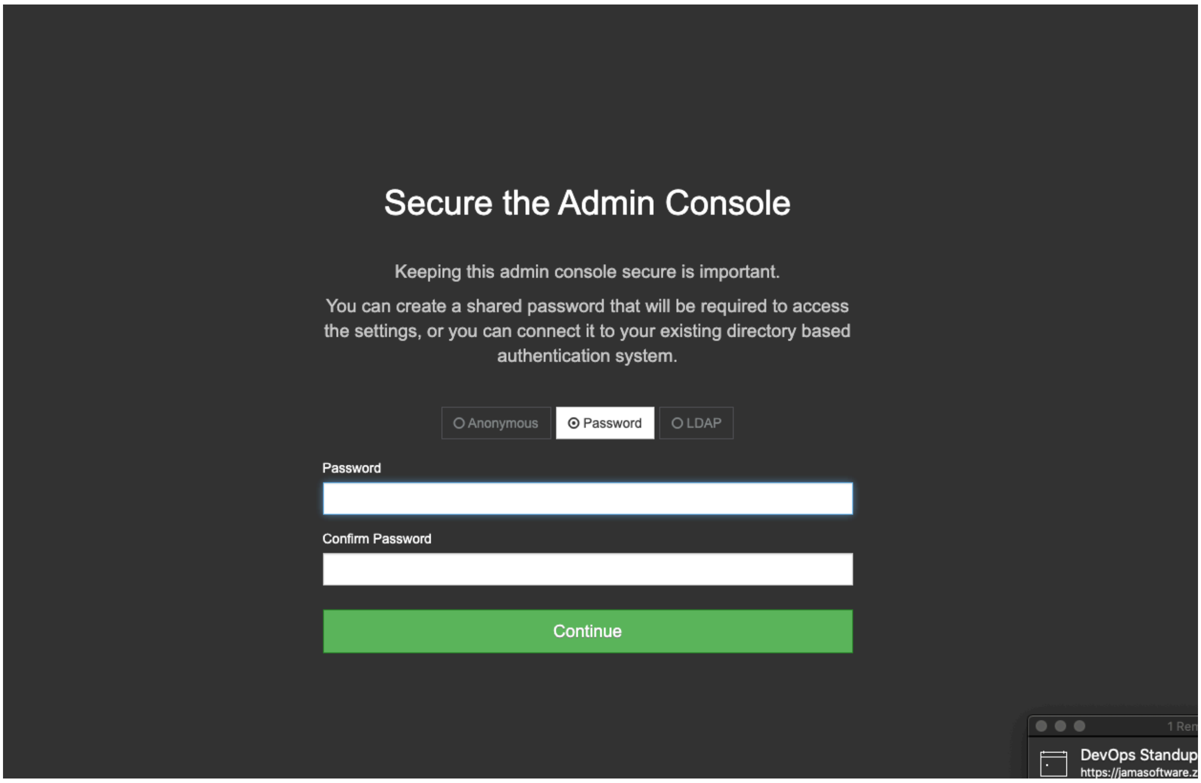
Reset Admin Console password (traditional)

You can reset the password for the Admin Console if, for example, the administrator forgot it.

1. To remove the current password, run this command on the application server:

```
replicated auth reset
```

2. To create a new password, enter this URL in a browser:
   https://[your.admin.console.ip]:8800/create-password



Secure the Admin Console

Keeping this admin console secure is important.

You can create a shared password that will be required to access the settings, or you can connect it to your existing directory based authentication system.

3. Select **Password**, then type a new, secure password for access to the Admin Console.

The new password takes effect immediately.

Update the license (internet, traditional)

When you renew your license or change the number of available seats, you must update your license. You receive a single key for your organization, called a *license key*, which specifies the type and number of licenses you have.

Your application server must be able to access the internet (except for airgap [53]customers).

TIP

Schedule a license update during a maintenance window because the process involves an interruption to the Jama Connect application.

To sync your license:

1. In the header of the Admin Console, select the **gear icon > View License**.
2. Select **Sync License**.
3. Stop and restart Jama Connect [49] for changes to take effect.

Update the license (airgap, traditional)

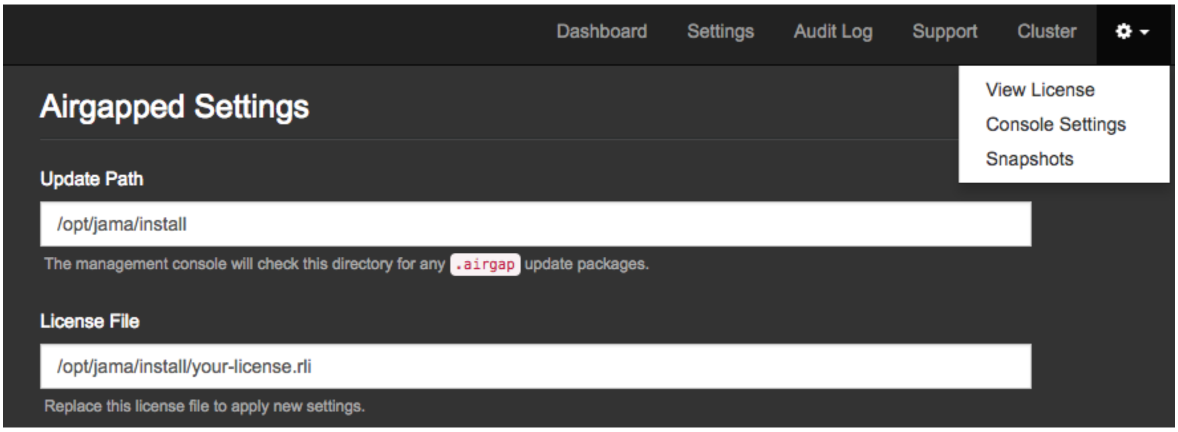
When you renew your license or change the number of available seats, you must update your license. You can ask your account manager for a new .rli license file, which Jama Software sends you via email.

TIP

Schedule a license update during a maintenance window because the process involves an interruption to the Jama Connect application.

To sync your license:

1. Open the email from Jama Software with the new .rli license file.
2. In the header of the Admin Console, select the **gear icon > Console Settings** and verify the location of the current license (for example, /data/install). Place your new license in that same location.



Airgapped Settings

Update Path

/opt/jama/install

The management console will check this directory for any .airgap update packages.

License File

/opt/jama/install/your-license.rli

Replace this license file to apply new settings.

3. If the name of the new .rli file differs from the original, update the name in the **License File** field. Don't use spaces in the filename.
4. In the header of the Admin Console, select the **gear icon > View License**, then select **Sync License** at the bottom of the page.
5. Scroll to the bottom of the page and select **Save**.
6. Stop and restart Jama Connect [49] for changes to take effect.

TIP

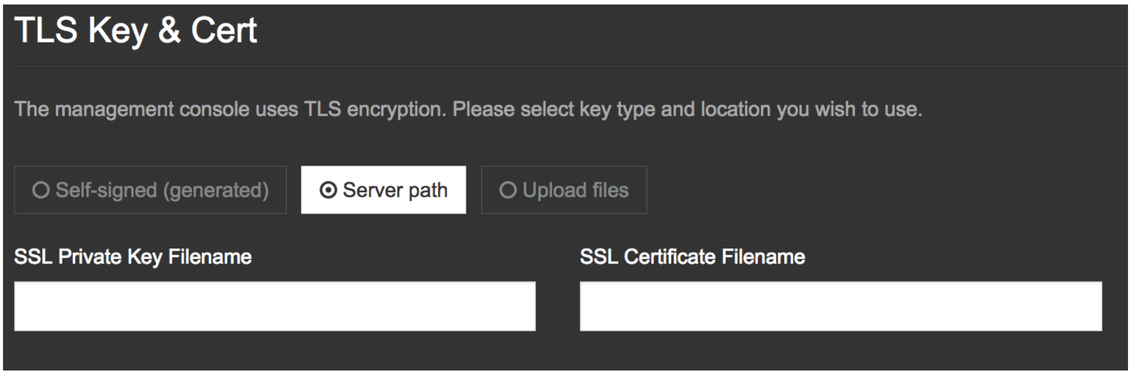
You can also sync a new license with this command:

```
curl -o jama_8-#-#.airgap -O
```

Update the certificate (traditional)

If a certificate expires, it becomes invalid and must be replaced.

1. In the header of the Admin Console, select the **gear icon > Console Settings**.
2. Under **TLS Key & Cert**, select the location of the SSL private key and certificate.
   - If the SSL key and certificate are on the application server, select **Server path**, then enter the file locations.



TLS Key & Cert

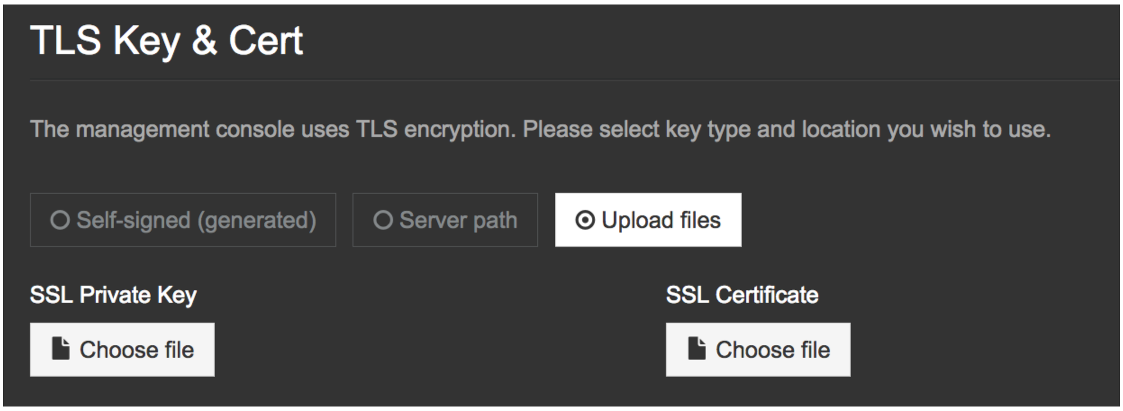
The management console uses TLS encryption. Please select key type and location you wish to use.

○ Self-signed (generated) ● Server path ○ Upload files

SSL Private Key Filename

SSL Certificate Filename

   - If the SSL key and certificate are on the computer you use to access the Admin Console, select **Upload files** to upload the key and certificate files, then select **Choose file** for SSL Private Key and SSL Certificate.



TLS Key & Cert

The management console uses TLS encryption. Please select key type and location you wish to use.

○ Self-signed (generated) ○ Server path ● Upload files

SSL Private Key

SSL Certificate

3. Scroll to the bottom of the page and select **Save**. A message confirms that your settings were saved.
4. To apply settings, you must restart the application:
   - **Immediately** — Select **Restart now**.
   - **Later** — Select **Cancel** and **Restart later**.

Update the IP address for the application server (traditional)

If you need to update the IP address or hostname of your application server, you must also edit the Replicated configuration files to reflect this change.

If you previously used an IP address, continue using an IP address. If you previously used a hostname, continue using a hostname.

NOTE

If you are using DNS and the hostname for this server isn't changing (just the underlying IP), you don't need to edit any files.

1. Make the IP/hostname changes in your network and on the server.
2. Stop the Jama Connect services [49].
3. Stop Replicated (Admin Console):
   - **CentOS, RHEL 7+, and Fedora**

     ```
     sudo systemctl stop replicated replicated-ui replicated-operator
     ```
   - **Debian, Ubuntu, and thers**

     ```
     sudo service replicated stop
     sudo service replicated-ui stop
     sudo service replicated-operator stop
     ```
4. Edit the Replicated configuration files to replace all occurrences of the old IP address or hostname with the new IP address or hostname.
   - **Fedora/CentOS/RHEL**
     /etc/sysconfig/replicated and **/etc/sysconfig/replicated-operator**
   - **Debian/Ubuntu**
     /etc/default/replicated and **/etc/default/replicated-operator**
   - **Others**
     Contact support at support@jamasoftware.com if you can't locate the Replicated configuration files.
5. If you have a firewall in place or use a proxy and configured no_proxy settings in Docker, update these settings with the new IP address.
6. Restart Docker.
   - **Fedora/CentOS/RHEL 7+**

     ```
     sudo systemctl restart docker
     ```
   - **Debian/Ubuntu and Others**

     ```
     sudo service docker restart
     ```
7. Start the Replicated service (Admin Console).
   - **Fedora/CentOS/RHEL 7+**

     ```
     sudo systemctl start replicated replicated-ui replicated-operator
     ```
   - **Debian/Ubuntu and Others**

     ```
     sudo service replicated start
     sudo service replicated-ui start
     sudo service replicated-operator start
     ```
8. Once the Replicated containers are up, navigate to https://{new_ip_address}:8800, then enter the new IP address or hostname under **Settings > Hostname**.
9. Log in to Jama Connect as the root user [15].
10. Change the URL [55] to reflect the new IP address.
11. Run Fix URL references [56] to change any existing references in the text of items that were already created.

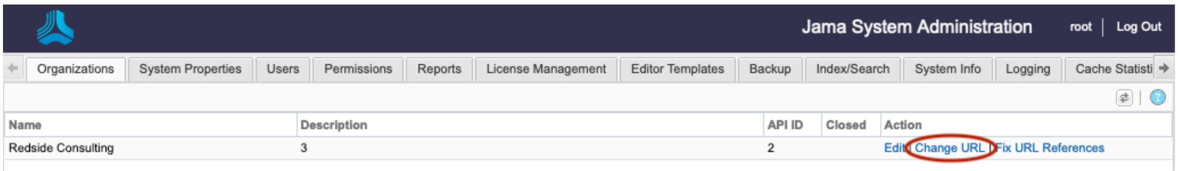
Change URL (traditional)

The Base URL is the first part of all web addresses that Jama Connect installations use, beginning with http and ending with a slash (/).

You might want to change your Base URL if a company changes its name or if you need to create a test instance.

To change your Base URL:

1. Log in to Jama Connect as the root user [15].
2. Select the **Organizations** tab.
3. Select **Change URL** from the Action column.



Name	Description	API ID	Closed	Action
Redside Consulting	3	2		Edit | Change URL | Fix URL References

4. Enter the new URL in the **New Base URL** text box.
5. Select **Change URL**.
6. Update all URL references [56] in the application to the new value.
   If this step isn't completed, the application still contains old URL references, which can result in unpredictable behavior such as images not being displayed in exports.
7. If you're using SAML authentication, disable and re-enable SAML settings to update the base URL in our SAML services.

The new URL is updated and active.

Update URL references after changing URL (traditional)

The option **Fix URL References** updates all URL references in the application to reflect a new URL. After you change a URL [55], always run this function.

IMPORTANT

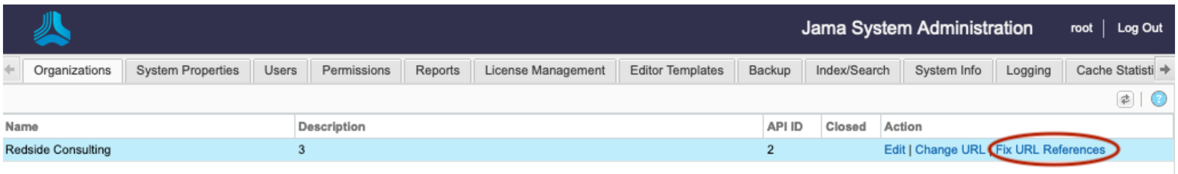
The **Fix URL References** option doesn't modify items in archived projects. It also doesn't change the URL used to connect the application server to your database server; that URL is stored in your database.properties file. The Base URL (baseurl field) is only updated in the database organization table by the Change URL [55] option.

Use the **Fix URL References** option if:

- You notice images are not being displayed in exports.
- A login prompt appears after URL redirection.
- An error message is displayed when you run exports.

To update all URL references in the application:

1. Log in to Jama Connect as the root user [15].
2. Select **Organizations > Fix URL References**.
3. Select **Fix URL References** from the Action column.



Name	Description	API ID	Closed	Action
Redside Consulting	3	2		Edit | Change URL | Fix URL References

4. Enter the new URL in the text box, **To this URL**.

5. Select **Fix URL References**.
6. When prompted, select **Yes** to finish.

Delete an organization (traditional)

Deleting an organization is an activity that is done only when more than one organization exists.

> **NOTE**
>
> Before version 4.3, users had the option to add multiple organizations. However, this option was removed in the spring of 2014. As of release 8.10, if you have multiple organizations, delete all but your production organization.

Overall system performance might be affected during the delete process depending on the size of the organization to be deleted. Schedule the deletion during off-peak hours.

Deleting an organization completely removes all data about the organization including projects, settings, and users. Deleted organizations can’t be recovered. If you need to preserve the non-production organizations, contact your account representative.

1. Back up your data [46].
2. Log in to Jama Connect as the root user [15].
3. Enable maintenance mode [24] under the **System properties** tab. If maintenance mode isn't enabled, the option to delete organizations isn't available.
4. Under the **Organizations** tab, select the **Delete** action in the row of the organization to be deleted.
5. When prompted, select **Yes** to confirm you are deleting the organization.

Remove old Docker images (traditional)

Old Docker images from previous versions of Jama Connect use up storage space and might cause indexing to fail. To avoid this, periodically remove old Docker images from your system to keep it running smoothly.

You also want to remove *dangling volumes*, which are volumes associated with a container that no longer exists. Jama Connect creates new containers and volumes when you restart the application. These volumes can fill up your disk space.

> **IMPORTANT**
>
> Make sure Jama Connect is running so that only images not in use are deleted. These commands clean only images and volumes loaded with the Docker storage driver in use. Files that were written with other storage drivers remain on the volume until separate commands are run for that storage driver.

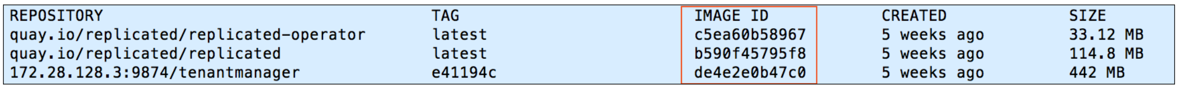
Use these commands to clean up your volumes:

1. Identify how much space is being used on your server:

   ```
   sudo docker system df
   ```
2. List out all Docker images on your server:

```
sudo docker images
```

Images are displayed on the screen, listed by their ID in the IMAGE ID column.



```
REPOSITORY                               TAG               IMAGE ID        CREATED         SIZE
quay.io/replicated/replicated-operator   latest            c5ea60b58967    5 weeks ago     33.12 MB
quay.io/replicated/replicated            latest            b590f45795f8    5 weeks ago     114.8 MB
172.28.128.3:9874/tenantmanager          e41194c           de4e2e0b47c0    5 weeks ago     442 MB
```

3. Remove an image by its ID:

   ```
   sudo docker rmi IMAGE_ID
   ```
4. Remove any dangling volumes from the Docker data root directory:

   ```
   docker volume rm $(docker volume ls -qf dangling=true)
   ```
5. Identify the volumes being removed:

   ```
   docker volume ls -qf dangling=true
   ```

NOTE

When you run the commands above to remove an image that is currently in use, you will get an error. For self-hosted customers with internet access, any missing images download again when you restart Jama Connect. For airgap customers, you'll need to manually load the images.

View scheduled jobs (traditional)

Some jobs can impact performance. When you view scheduled jobs, you can identify which jobs are currently running, when jobs are scheduled to run, and how much memory they require. Knowing this information helps you prepare for any performance hit.

1. Log in to Jama Connect as the root user [15].
2. In the Jama System Administration panel, select **Scheduled jobs** to view jobs, their group, class, and firing time.

View applied patches (traditional)

You might need to check which patches have been installed on your application server. For example, you can see if any patches were missed, or you might need to let support know about your current environment.

1. Log in to Jama Connect as the root user [15].
2. In the Jama System Administration panel, select **Applied Patches** to view the unique ID, run date, and status.

Clear cache (traditional)

If you notice latency or slow performance of Jama Connect, you can free up disk space and memory by clearing the cache.

1. Log in to Jama Connect as the root user [15].
2. In the Jama System Administration panel, select **Cache statistics**.
3. Clear items from the cache:
   - **All items** — Select **Clear all cache** to clear all cache items from the cache.
   - **Specific item** — Select **Clear Cache** on a specific cache item to clear it from the cache.

Reindex all search items (traditional)

Search indexes get out of sync with the database due to large batch updates, API updates, or database updates. During a full index, all search indexes are rewritten to the current values in the database.

> **NOTE**
>
> You must have system administrator permissions to complete this task while logged in as root. While organization admins and project admins can index project items, they can't index all search items.

Important considerations

- Files over 25 MB aren't indexed, so their content isn't searchable.
- Filetypes that can be indexed: PDF, DOC, DOCX, PPT, PPTX, TXT, RTF.
- Filetypes that can't be indexed: XLSX, XLS, XML, HTML, HTM.
- During the index process, the application automatically enters maintenance mode [24]. Users can’t log in during this time and users who are already logged in receive a message about the maintenance.

To sync your search indexes:

1. Notify users before initiating an index.
2. Disable all integrations including legacy connectors and the Jama/Tasktop Integration Hub.
   DWR, SOAP, and REST API calls are automatically blocked during the reindex.

   > **NOTE**
   >
   > The system administrator doesn't have access to disable integrations. Work with an organization admin or integrations admin to disable those services.

3. Log in to Jama Connect as the root user [15].
4. Select the **Index/Search** tab and select **Index items**.
   The system displays a count of items in the application and the estimated time to complete the index.
5. Select **Yes** to continue.

You see an alert when indexing is complete and maintenance mode is automatically disabled.

Folder locations (traditional)

You can use an exported filesystem, such as NFS, for mounting the following directories, provided the path remains the same.

The following two directories are on the application server:

- **/data**
  Stores physical artifacts, like attachments, reports, avatars, diagrams, and metrics. Exported file systems, like NFS, are supported for use with the /data directory.
- **/logs**
  Contains all log files of the Jama Connect components such as the following:
  - **/logs/tomcat**
    Apache Tomcat log files, logs all activities in the application

- **/logs/tomcat/contour**
  Core Jama Connect log files
- **/logs/elasticsearch**
  Elasticsearch log files
- **/logs/search**
  Search service log files
- **/logs/nginx**
  Nginx log files (note that currently only error logging is provided for Nginx)

NOTE

You cannot change the location where log files are written to, however, you can change the appenders and logging levels for different components of the Jama Connect application. The core Jama Connect application log configuration can be updated in:

```
/data/log4jconfig/log4j.properties
```

The log configuration for Elasticsearch and search service can also be found in

```
/data/config
```

Changes to these configuration files persist when you restart Jama Connect and are applied in a few seconds.

IMPORTANT

Replicated snapshots are stored in the following location by default:

```
/var/lib/replicated/snapshots
```

However, if you change the path to include /data it will be easier to include these snapshots in your regular backups of Jama Connect data at /data/directory, as such:

```
/var/lib/replicated/data/snapshots
```

Note that /snapshots should have three times the space allocated as the rest of /data.

Migrating your data (traditional)

To use Jama Connect 8.x, your application server must be running on a Linux platform; Windows server is no longer supported. Also, because Oracle database is no longer supported, you must migrate to either Microsoft SQL Server or MySQL before upgrading to version 8.x.

You must also migrate your existing data when you upgrade the platform (physical or virtual) for your database server or application server.

NOTE

This information applies to self-hosted environments only.

Migrate Jama Connect data when you:

- Upgrade Jama Connect from pre-8.0 version
- Upgrade from Oracle database on pre-8.0 Jama Connect
- Migrate the application to a new server [62]
- Migrate the database to a new server [63]
- Set up or update a test server [63]

Migrating...	Details
From Oracle database	Jama Connect 8.x no longer supports Oracle database. You must migrate to a supported database before upgrading to 8.x.
From Windows server	Jama Connect 8.x no longer supports Windows platform. You must migrate to a supported Linux operating system, then migrate your application and data.

IMPORTANT

If you restore data from an XML or .jama file, your image file automatically references the new server's name or location. But if you use any other method to restore data (such as proprietary tools for MySQL or Microsoft SQL Server), you must run the **Fix URL** option to update references manually [56].

Migration overview (traditional)

The basic process for migrating your application and data involves creating a backup of your /data directory, then creating a snapshot of your Replicated Admin Console settings. Once that is done, you install Jama Connect on a new server and migrate the /data directory backup to the new server. When the new server is online and functioning, you then remove Jama Connect from the original system.

Depending on your current environment, you might also need to:

- Upgrade to Jama Connect 8.x if you’re running a pre-8.x version.
- Migrate to a supported Linux system if you’re running on a Windows server.
- Migrate to a supported database (MySQL or SQL Server) if you’re running an Oracle database.

Migration process

1. Make a backup of your current Jama Connect installation using one of these methods:
   - Jama Connect backup (.jama file or XML file)
   - Proprietary database backup for SQL Server or MySQL
2. Make sure you are running:
   - Jama Connect 8.x or later on a supported Linux system
   - A supported database, SQL Server or MySQL
3. Migrate existing data, using .jama file, XML file, or proprietary SQL database file.
4. Remove previous installation of Jama Connect.

Migrate existing directories (traditional)

If you created your backup with a Jama Connect XML file or with SQL proprietary database software, you must manually migrate certain directories (folders).

A .jama backup file includes the database plus all necessary directories. However, an XML backup file or a proprietary database backup includes only the database.

1. In the **/data** directory, delete these directories:
   - **tenant**
   - **ActiveMQData**
   - **elasticsearch**

   These directories are restored when you restart Jama Connect on the new server.
2. Migrate these directories accordingly:

Directories	Details
/attachments/**	Move to the new application server at /data/contour/attachments/**
/avatars/**	Move to the new application server at /data/contour/avatars/**
/diagrams/**	Move to the new application server at /data/contour/diagrams/**
/metrics/**	Move to the new application server at /data/contour/metrics/**
/reports/**	Move to the new application server at /data/contour/reports/**

   ** All directories and files below the given folder
3. On the new application server, set permissions and ownership for all directories with these commands:

   ```
   chown -R 91:91 /data/contour
   chmod -R u+rwX /data/contour
   ```

Migrate the application to a new server (traditional)

If you have a new server (physical or virtual) for your existing Jama Connect 8.x installation, you must first create a backup and snapshot on the original server, then migrate data and restore the snapshot on the new server.

> **IMPORTANT**
>
> The snapshot contains the license from the original server. Only use a production server snapshot on a new production server, and a test server snapshot on a new test server.

1. Log in to Jama Connect as the root user [15].
2. Enable maintenance mode [24]:
   1. Select the **System properties** tab in the Jama System Administration panel, then select **Edit** in the top right corner.
   2. Scroll to the bottom of the page and select **Yes** for maintenance mode.
3. On the original server:
   1. Create a Replicated snapshot [3] from the Admin Console.
   2. Create a backup (.jama file, XML file, or proprietary SQL backup) and download it from the root menu. Move to the new server under /data/restore.
4. On the new server:
   1. Migrate the existing data [62], including the /data directory and its contents from the old server to the new server, preserving the structure and permissions of the contents.

2. Move the snapshot from the original server to the same directory on the new server.
3. Restore the snapshot [4]. When prompted for the license, select **Restore from a snapshot**.
4. If the IP address of the two servers are different, update the IP address of your application server [54].

Migrate existing database to a new server (traditional)

If you have a new server (physical or virtual) for your existing database, you must create a backup of the original database, then migrate and restore it on the new database server.

Important considerations

- If migrating from the same database type, such as MySQL to MySQL, perform a proprietary backup and restore [49], to avoid converting the data.
- If migrating between different database types, such as MySQL to SQL Server, generate a backup [46] of your database using your current installation of Jama Connect.
- If migrating from a pre-8.0 version of Jama Connect, generate a backup [46] of your database using your current installation of Jama Connect. You must use an XML file for the backup.
- If migrating from an 8.x version of Jama Connect, use a .jama file for the backup.

To migrate your database to a new server:

1. Generate a backup on your application server, using a .jama file (recommended), XML file, or a proprietary database backup.
2. If using a .jama file or XML file:
   a. Wait for the backup file to be written to the /data/contour/backup directory on the application server.
   b. Move the backup file to the /data/restore directory on the destination application server.
3. Create a new database following the instructions appropriate for MySQL or SQL Server.
4. Delete filesystem assets on the destination server:

   ```
   rm -rf /data/{activeMQData,| config, contour, elasticsearch, tenant}
   ```
5. On the respective destination servers, configure the Admin Console, and when prompted, select **Restore from backup file**.
6. Save the settings and restart Jama Connect.

Setting up a test server (traditional)

If configuring a test server, you must disable the following features before you create the backup on the original server. Disabling these features prevents duplicate information from being sent out from both your test and production environments.

Make sure to disable these features:

- Legacy connectors such as the JIRA, TFS, and Rally connectors
- SMTP or IMAP

Troubleshooting (traditional)

NOTE

This information applies to self-hosted environments only.

You can avoid troubleshooting by following regular maintenance practices [49], but if you run into problems here are some resources that might help:

- For issues with installation, log in to the Jama Connect as root user [15] and select the **System Info** tab to see a quick overview of your installation.
- View log and profile [65]
- Clear cache [58]
- View scheduled jobs [58]
- Index all items [59]
- Remove old Docker images [57]
- Reconnect to the Wiris server [67]
- Generate a support bundle [64] and contact

Generate a support bundle (traditional)

A Support Bundle contains information about the application server and the Jama Connect installation. The bundle, which includes support troubleshoot issues in your environment, includes thread dumps [64], log files from the Admin Console, and the components that make up Jama Connect.

1. Generate a Support Bundle from the UI or command line of the application server.
   - **From the UI** — In the header of the Admin Console, select **Support**, then select **Download Support Bundle**.
   - **From the command line:**

     ```
     replicated apps
     replicated support-bundle <app_id>
     ```

     <app id> is the ID of your application taken from the output of the first command.
2. Upload the Support Bundle to Jama Support: support@jamasoftware.com

For more information, see the community article: Jama Support Bundle: How do I get it, what's in it, and which logs should I care about?

Thread dump

A thread dump is a snapshot of the state of your Jama Connect processes at a point in time.

Jama Support might request a thread dump for troubleshooting performance issues.

Any time you generate a Support Bundle [64], the bundle includes three thread dumps taken at 5-second intervals.

TIP

Take multiple thread dumps over an interval of time. A single thread dump on its own doesn't provide complete information about an issue.

You can create a thread dump from the command line or the from the Logging Configuration window.

Manually (command line)	Logging configuration window [65]
`jamacli jamacore-thread-dump`	Select **Logging > Configuration**

NOTE
You can create thread dumps only for containers that are the core Jama Connect application.

View and configure logging (traditional)

Log files record information from the application and can help with troubleshooting. Information is captured in the contour.log file.

Entries in the log file are noted by the [jama.AccessLog] package and include this information:

- Date of request
- Server processing time to handle the request
- The user who submitted the request
- The organization ID of the user who submitted the request
- The user session ID of the user who made the request
- The server address that the request was made to

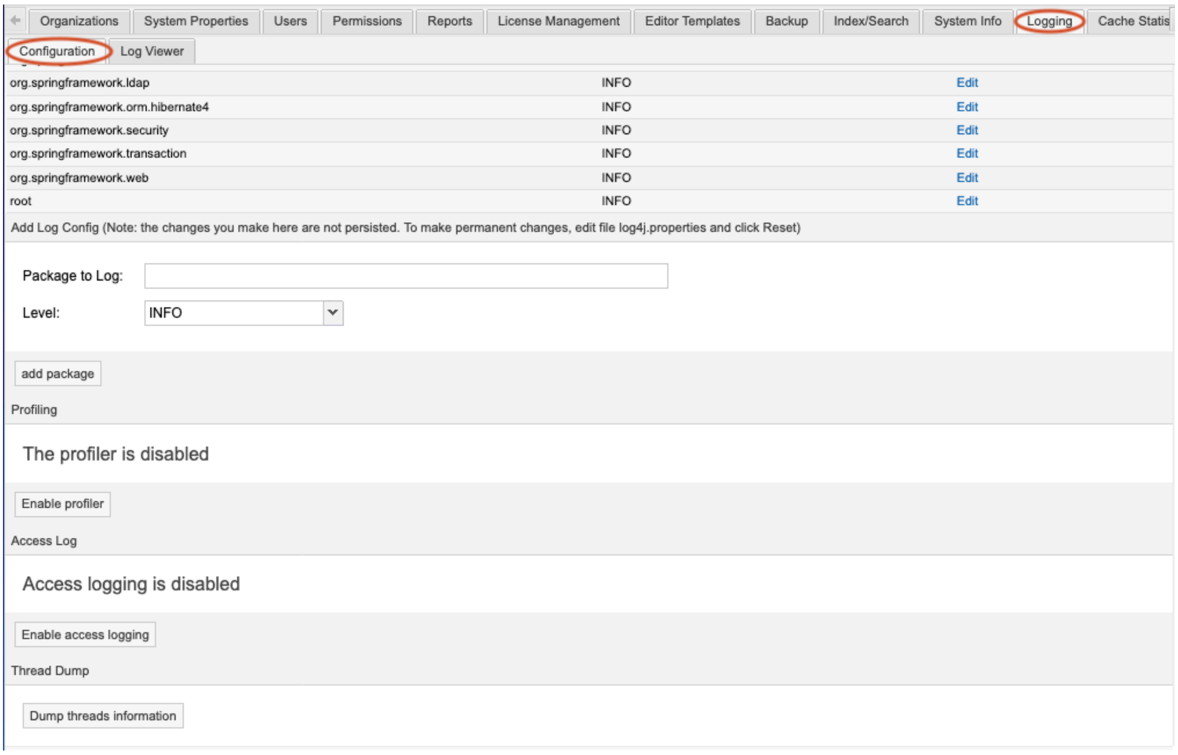
Enabling the profiler logging enhances logging in Jama Connect. However, profiler logging might require additional resources to generate this content. For best performance, use the profiler for troubleshooting purposes.

The profiler prints out the following information:

- The user who submitted the call
- The organization the user belongs to
- The java thread ID of the call
- A stack trace of the call that includes processing time and memory usage of each trace

To view the log and configure logging:

1. Log in to Jama Connect as the root user.
2. Select **Logging > Log Viewer** to view the log. As needed, select **Refresh** at the top right to refresh the log.
3. Select **Logging > Configuration**.



org.springframework.ldap	INFO	Edit
org.springframework.orm.hibernate4	INFO	Edit
org.springframework.security	INFO	Edit
org.springframework.transaction	INFO	Edit
org.springframework.web	INFO	Edit
root	INFO	Edit

Add Log Config (Note: the changes you make here are not persisted. To make permanent changes, edit file log4j.properties and click Reset)

Package to Log:

Level: INFO

Profiling

The profiler is disabled

Access Log

Access logging is disabled

Thread Dump

TIP

By default all logging levels are set to info and will reset to that default when the application is restarted [49].

To permanently change the logging level and appenders, edit the file:

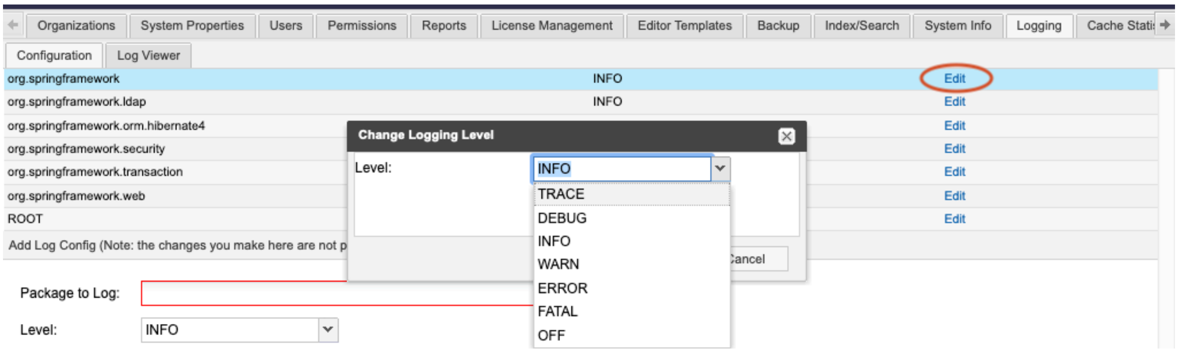
```
/data/config/log4j.properties
```

The log configuration for Elasticsearch and search service can also be found in:

```
 /data/config
```

You cannot change the location to where log files are written. Changes to these configuration files are applied within a few seconds and are persisted across restarts the application.

4. To change the logging level from the default setting of Info, select **Edit**.



org.springframework	INFO	Edit
org.springframework.ldap	INFO	Edit
org.springframework.orm.hibernate4		Edit
org.springframework.security		Edit
org.springframework.transaction		Edit
org.springframework.web		Edit
ROOT		Edit

Add Log Config (Note: the changes you make here are not p

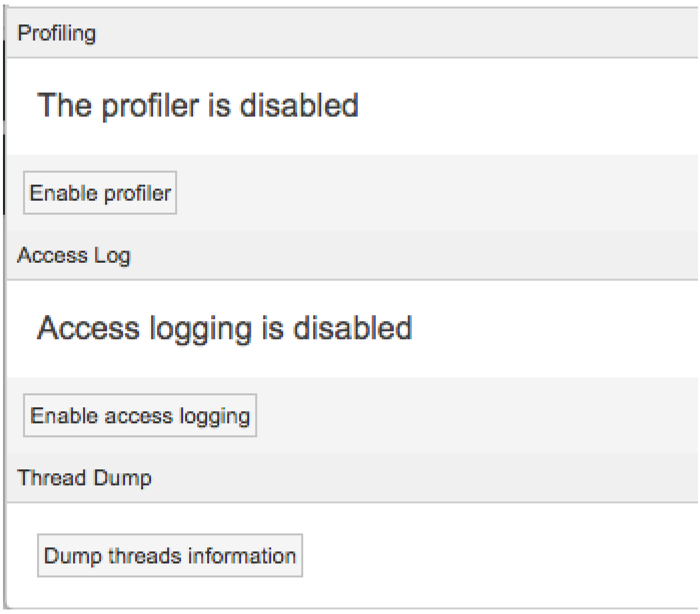
Change Logging Level

Level: INFO

Package to Log:

Level: INFO

5. To log additional content for every log entry in the contour.log file, scroll to the bottom of the page and select **Enable profiler** under Profiling.



Profiling

The profiler is disabled

Access Log

Access logging is disabled

Thread Dump

Profiling is indicated in the log file as the [jama.Profiler] package.

Here is a sample log entry:

```
2011-04-28 09:37:19,865 INFO [org.directwebremoting.impl.DefaultRemoter]
- Exec: projectSvc.getExtTreeNodeForProject()
2011-04-28 09:37:19,869 INFO [jama.Profiler] - user:admin org:2
thread:96 start:2011-04-28 09:37:19,866
[3ms] [+88K/-88K 837755K/254041K]-
com.jamasoftware.Jama.dwr.impl.DwrProjectServiceImpl.getExtTreeNodeForPro
ject
[3ms] [+88K/-88K 837755K/254041K]-
com.jamasoftware.contour.service.impl.ProjectServiceImpl.getExtTreeNodeFo
rProject
[2ms] [+88K/-88K 837755K/254041K]-
com.jamasoftware.contour.service.impl.DocumentTypeServiceImpl.getAvailabl
eDocumentTypesForProject
```

6. To capture information for all user requests and all locked-out users in Jama Connect, select **Access log**, then select **Enable access logging**.

   Information is captured in the contour.log file. Here is a sample log entry:

   ```
   2014-08-29 16:24:59,370 INFO http-bio-8080-exec-17 [jama.AccessLog]
   - [3 ms] PRBDIJN9 1 - 083BBE5B1E8C481033DA7AFBBEF023A5 160 http://
   localhost:8080/contour/
   ```

7. To capture a one-time dump of the current running java threads being executed, select **Dump threads information** under Thread dump.

   Information is captured in contour-threaddump.log.

   This information is useful for identifying long running processes. If Jama Connect seems to hang, run a thread dump and send the log file to .

Reconnect to the Wiris server (traditional)

If your connection to the Wiris server is interrupted, you can fix the issue by modifying the Wiris settings, restarting your system, then returning the settings to their original values.

1. Modify the Wiris settings:
   a. In the Admin Console, select **Settings > WIRIS Connection Settings**.
   b. Select **Use custom Wiris connection**.
   c. Make the following changes:

    - **Wiris Host** — Add “xx” to the end of the string
    - **Wiris Path** — Add “xx” to the end of the string
    - **Wiris Port** – Change to 44311

   d. Select **Save** and restart your system.

2. **Test the connection**. Use Jama Connect in a field that calls the Wiris MathType Editor:
   a. In Jama Connect, select **Projects**, and select the item you want to modify.
   b. From the Add drop-down menu, select **New item > Text**.
   c. In the Add item window, select the Math Editor icon.
   d. Add an equation using the equation editor. As expected, this action fails.
3. In the Admin Console, reset the modified Wiris setting to the original values.
4. Select **Save** and restart your system.
5. **Test the connection**. Use Jama Connect in a field that calls the Wiris MathType Editor:
   a. In Jama Connect, select the item you want to modify.
   b. From the Add drop-down menu, select **New item > Text**.
   c. In the Add item window, select the Math Editor icon.
   d. Add an equation using the equation editor. This action now succeeds