Jamf Software Server Installation and Configuration Guide for Linux

Version 9.98

Contents

Preface

About This Guide

The Jamf Software Server (JSS) is a web application that functions as the administrative core of the Casper Suite. The JSS allows you to perform inventory and remote management and configuration tasks on managed computers and mobile devices. All other administrative applications in the Casper Suite communicate with the JSS.

This guide provides step-by-step instructions for installing and setting up the JSS on the Linux platform. It also explains how to perform advanced configuration tasks.

Additional Resources

For information on related topics, see the following resources:

- *Casper Suite Administrator's Guide*
  This guide provides information about setting up and managing the JSS after it is installed. It is available at:
  https://www.jamf.com/resources/casper-suite-administrators-guide/

- *Manually Installing the Jamf Software Server*
  This technical paper explains how to manually install the JSS on Linux and Windows platforms. You can download it from:
  https://www.jamf.com/resources/manually-installing-the-jamf-software-server/

Overview of Technologies

Applications and Utilities

This section provides an overview of the applications and utilities that you need to install and maintain the Jamf Software Server (JSS), and Jamf Distribution Server (JDS) instances.

Jamf Software Server

The Jamf Software Server (JSS) is a web application that functions as the administrative core of the Casper Suite. The JSS allows you to perform inventory and remote management and configuration tasks on managed computers and mobile devices. All other administrative applications in the Casper Suite communicate with the JSS.

JSS Installer for Linux

The JSS Installer for Linux is a .run file that allows you to install and upgrade the JSS on supported Linux operating systems.

To obtain the JSS Installer for Linux, log in to Jamf Nation and click **Show alternative downloads** below the Casper Suite DMG on the following page:

https://www.jamf.com/jamf-nation/my/products

JSS Database Utility

The JSS Database Utility allows you to back up and restore the jamfsoftware database. It also allows you to restart Apache Tomcat and MySQL and modify their settings.

The JSS Database Utility is installed automatically when you run the JSS Installer. It is located in:

`/usr/local/jss/bin/JSSDatabaseUtil.jar`

JDS Installers

The JDS Installer for Mac (.pkg) and the JDS Installer for Linux (.run) allow you to install JDS instances on Mac or supported Linux operating systems.

A JDS instance is a distribution point that is managed by the JSS, similar to a computer or mobile device. For more information on JDS instances, see Jamf Distribution Server Instances.

To obtain the JDS Installers, log in to Jamf Nation and go to the following page:

https://www.jamf.com/jamf-nation/my/products

Ports

The following table describes the main ports used to host communication between computers, distribution points, and the Jamf Software Server (JSS):

Port	Used for	Direction
22	The standard port for SSH (known as remote login in macOS). Default port used by Casper Remote and Recon to connect to computers.	Outbound from Casper Remote and Recon, and inbound to computers
80	The standard port for HTTP. When you use HTTP to distribute files from a file share distribution point, they are downloaded on this port.	Inbound to the distribution point, and outbound from computers
443*	The standard port for HTTPS. When you use HTTPS to distribute files from a file share distribution point, they are downloaded on this port. The cloud distribution point and JDS instance also communicates on this port. In addition, this port is used for the following: ■ Connect the JSS to the Jamf Push Proxy. ■ Connect the JSS to the patch server. ■ Required for MDM-capable computers to communicate with Apple Push Notification service (APNs). ■ Connect to Apple's Device Enrollment Program (DEP) and Volume Purchase Program (VPP). **Note:** Apple could change this port without Jamf's knowledge.	Inbound to the distribution point, and outbound from the JSS, computers, and mobile devices
548	The standard port for Apple File Protocol (AFP). If you use an AFP share to distribute files from a file share distribution point, computers mount the AFP share on this port.	Inbound to the share, and outbound from computers
3306	The default port used by the JSS to connect to MySQL.	Outbound from the JSS, and inbound to MySQL
8443	The SSL port for the JSS. Default port used by applications and computers and mobile devices to connect to the JSS.	Inbound to the JSS, and outbound from computers and mobile devices

The following table describes other commonly used ports:

Port	Used for	Direction
25	The standard port for SMTP. The JSS connects to an SMTP server to send email notifications to JSS users.	Outbound from the JSS, and inbound to the SMTP server

Port	Used for	Direction
139	If you use an SMB share to distribute files from a file share distribution point, computers mount the SMB share on this port.	Inbound to the share, and outbound from computers
389	The standard port for LDAP. Any LDAP connections—even those coming from other applications—go through the JSS. This means that only the JSS connects to your LDAP server.	Outbound from the JSS, and inbound to the LDAP server
636	The standard port for LDAPS. Any LDAP connections—even those coming from other applications—go through the JSS. This means that only the JSS connects to your LDAP server.	Outbound from the JSS, and inbound to the LDAP server
445	If you have an SMB client, such as "DAVE", installed on computers, they may mount the SMB share on this port.	Inbound to the share, and outbound from computers
514	The default port used by the JSS to write to Syslog servers.	Outbound from the JSS, and inbound to Syslog servers
2195*	The port used to send messages from the JSS to APNs.	Outbound from the JSS, and inbound to the APNs server
2196*	The port used by the JSS to connect to APNs for feedback.	Outbound from the JSS, and inbound to the APNs server
5223*	The port used to send messages from APNs to the computers and iOS devices in your network.	Outbound from computers and iOS devices, and inbound to the APNs server
5228	The port used to send messages from Google Cloud Messaging (GCM) to the personally owned Android devices in your network.	Outbound from Android devices, and inbound to the GCM server
8080	The HTTP port for the JSS on Linux and Windows platforms. Although it is available, applications do not connect to this port unless the defaults are overridden.	N/A
9006	The HTTP port for the JSS on the Mac platform. Although it is available, applications do not connect to this port unless the defaults are overridden.	N/A
61617	The port used by the JSS to queue and dequeue messages from the message broker.	Outbound from the JSS, and inbound to the message broker

On the Linux platform, the JSS runs on 8443 and 8080 by default. If you decide to change these ports, you must change the port information in Tomcat's `server.xml` file and in the Preferences window for each Casper Suite application.

You cannot change the default ports for SSH or SMB with the Casper Suite.

* Ports 443, 2195, 2196, and 5223 must be open outbound and inbound to the 17.0.0.0/8 address block in order for computers and iOS devices to communicate with APNs.

For detailed information on MDM troubleshooting, see the following documentation from Apple:

- http://support.apple.com/kb/HT6175?viewlocale=en_US
  Learn about TCP and UDP ports used by Apple products.

- http://support.apple.com/kb/TS4264?viewlocale=en_US
  Find out why you are not receiving Apple push notifications.

- https://developer.apple.com/library/ios/technotes/tn2265/_index.html#//apple_ref/doc/uid/DTS40010376-CH1-TNTAG41
  Troubleshoot push notifications.

Installed Files and Folders

The following files and folders are installed when you run the JSS Installer:

JSS web application
The files that make up the JSS web application are stored in the following location:

`/usr/local/jss/tomcat/webapps/ROOT/`

Apache Tomcat
Tomcat is the web application server that runs the JSS web application. A directory named `tomcat` is installed in the following location:

`/usr/local/jss/`

For more information about the version of Tomcat installed by the JSS Installer, see the Apache Tomcat Version Installed by the JSS Installer Knowledge Base article.

jamf.tomcat8
This is the service file for Tomcat. It is installed in the following location:

`/etc/init.d/jamf.tomcat8`

server.xml
The JSS Installer installs a modified copy of Tomcat's `server.xml` file. This file enables SSL, ensures that the JSS appears in the `root` context, and enables database connection pooling. It is installed in the following location:

`/usr/local/jss/tomcat/conf/`

keystore
Tomcat requires a .keystore file to provide connections over SSL. The JSS Installer creates a default .keystore file and stores it in the following location:

`/usr/local/jss/tomcat/`

JSS Database Utility
The JSS Database Utility (`JSSDatabaseUtil.jar`) is installed in the following location:

`/usr/local/jss/bin/`

Database backup location
By default, the JSS Database Utility stores database backups in the following location:

`/usr/local/jss/backups/database/`

Logs
Logs for the installation and for the JSS are stored in the following location:

`/usr/local/jss/logs/`

Requirements

This section lists the requirements for the applications and utilities you need to install and maintain the Jamf Software Server (JSS), and Jamf Distribution Server (JDS) instances.

Jamf Software Server

You can host the JSS on any server that meets the following requirements:

- Java 1.7 or Java 1.8 (Java 1.8 is recommended)
- MySQL 5.6.x or 5.7.x (MySQL 5.7.x is recommended)
- Apache Tomcat 7 or 8.0.x (Tomcat 8.0.x is recommended)

Tested Linux operating systems include:

- Ubuntu 14.04 LTS Server
- Ubuntu 16.04 LTS Server
- Red Hat Enterprise Linux (RHEL) 6.8 and 7.3

Although you can install the JSS on any server that meets the minimum requirements, the JSS Installer for Linux has additional requirements. (For more information, see the next section.)

Tested browsers for the JSS are as follows:

- Safari
- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer 10 or later

JSS Installer for Linux

The JSS Installer for Linux requires a server with:

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- One of the following operating systems:
  - Ubuntu 12.04 LTS Server (64-bit)
  - Ubuntu 14.04 LTS Server (64-bit)
  - Red Hat Enterprise Linux (RHEL) 6.4, 6.5, 6.6, or 7.0
- Open Java Development Kit (OpenJDK) 7 or 8
  For installation instructions, go to http://openjdk.java.net/install/.

- MySQL 5.6.x or 5.7.x (MySQL 5.7.x is recommended)
  You can download MySQL from:
  https://www.mysql.com/downloads/

- Wget utility installed

- Ports 8443 and 8080 available

JSS Database Utility

The JSS Database Utility requires a server with MySQL 5.6.x or 5.7.x (MySQL 5.7.x is recommended) installed.

JDS Installer for Mac

The JDS Installer for Mac requires a computer with:

- An Intel processor

- 2 GB of RAM

- 100 GB of disk space available

- macOS v10.7 or later with macOS Server v1.4.3 or later installed
  Note : If you are hosting a JDS instance on a server with macOS Server v5.0.x installed, you must modify the Apache proxy and websites configuration files before you can use the JDS instance. (For more information, see the Troubleshooting Jamf Distribution Server (JDS) Issues on Computers with macOS Server v5.0.x Installed Knowledge Base article.)

JDS Installer for Linux

The JDS Installer for Linux requires a computer with:

- An Intel processor

- 2 GB of RAM

- 100 GB of disk space available

- One of the following operating systems:

  - Ubuntu 10.04 LTS Server

  - Ubuntu 12.04 LTS Server

  - Red Hat Enterprise Linux (RHEL) 6.4, 6.5, 6.6, or 7.0
    Note: To install a JDS instance on a Linux operating system that is running on a virtual machine, you need a virtualization platform that provides SMBIOS information.

Installation

Installing the JSS

Installing the Jamf Software Server (JSS) involves the following steps:

1. Install the required software (if you haven't already).
2. Create the jamfsoftware database.
3. Run the JSS Installer.

Before you begin, make sure your server meets the JSS Installer requirements. (For more information, see Requirements.)

Note: For instructions on how to manually install the JSS on Linux, see the *Manually Installing the Jamf Software Server* technical paper. You can download it from:

https://www.jamf.com/resources/manually-installing-the-jamf-software-server/

Step 1: Install the Required Software

Java and MySQL must be installed on the server before you can create the jamfsoftware database and run the JSS Installer. For instructions on how to install and configure Java and MySQL, see the following Knowledge Base article:

Installing Java and MySQL

Step 2: Create the jamfsoftware Database

Create a MySQL database in which the JSS can store its data and a MySQL user that can access the database.

A default MySQL database name, username, and password are used throughout the instructions in this section. It is recommended, however, that you use a custom username and password that comply with your organization's security requirements. It is also recommended that you not use "root" as the username. A different database name can also be set if desired.

The default MySQL settings used in the instructions below are:

- Database name: jamfsoftware
- Username: jamfsoftware
- Password: jamfsw03

Note: If you customize any of the MySQL settings, you will be prompted to enter them on the Database pane when you run the JSS Installer.

1. Open a command prompt and access the MySQL command line as "root" by typing something similar to the following:

   ```
   mysql -u root -p
   ```

   If you did not create a root password when installing MySQL, do not type `-p`.
   If MySQL is not in the path or it is installed in a custom location, enter the installation path in place of `mysql`.

2. If prompted, enter the password for the MySQL "root" user.

3. Create a database by executing:

   ```
   CREATE DATABASE jamfsoftware;
   ```

   You can customize the database name by replacing `jamfsoftware` with the desired name as shown in the following example:

   ```
   CREATE DATABASE myDatabaseName;
   ```

4. Create a new MySQL user:

   ```
   CREATE USER 'jamfsoftware'@'localhost' IDENTIFIED BY 'jamfsw03';
   ```

5. Grant access to that user so that it can access the database:

   ```
   GRANT ALL ON jamfsoftware.* TO 'jamfsoftware'@'localhost';
   ```

   You can customize the MySQL username and password by replacing 'jamfsoftware' and 'jamfsw03' with the desired username and password as shown in the following examples:

   ```
   CREATE USER 'customUsername'@'localhost' IDENTIFIED BY 'customPassword';
   ```

   ```
   GRANT ALL ON myDatabaseName.* TO 'customUsername'@'localhost';
   ```

Step 3: Run the JSS Installer

The JSS Installer for Linux installs Apache Tomcat and the JSS web application.

1. Copy the JSS Installer for Linux (`jssinstaller.run`) to the server.
   Note: To obtain the JSS Installer for Linux, log in to Jamf Nation and click **Show alternative downloads** below the Casper Suite DMG on the following page:
   https://www.jamf.com/jamf-nation/my/products

2. Log in to the server as a user with superuser privileges.

3. Initiate the installer by executing a command similar to the following:

```
sudo sh /path/to/jssinstaller.run
```

4. When the requirement check is complete, type "y" to proceed.

5. (RHEL only) When the installation is complete, edit the firewall configuration to allow access to port 8443 by executing:

```
sudo system-config-firewall-tui
```

6. (RHEL only) Choose **Other** or **Customize**, and manually add port 8443 with TCP protocol. The option you choose depends on whether you have a GUI or shell-only interface.

7. Access the JSS by opening a web browser and typing the protocol, IP address or hostname of the server, and port. For example:
https://jss.mycompany.com:8443/

8. If you entered a custom database name, username, or password when you created the jamfsoftware database, or MySQL is using a port other than 3306, the Database Connection Properties pane is displayed. Before you can access the JSS, you must follow the onscreen instructions to create a connection between the JSS and the jamfsoftware database.

Related Information

For related information, see the following section in this guide:

Installed Files and Folders
Learn about the files and folders that are installed by the JSS Installer.

For related information, see the following Knowledge Base article:

Apache Tomcat Version Installed by the JSS Installer
View the Tomcat version that is installed by the JSS Installer.

Upgrading the JSS

This section explains how to upgrade the Jamf Software Server (JSS).

Note: To take full advantage of all new features, bug fixes, and enhancements available in the Casper Suite, it is recommended that you use the latest version of the JSS and the client applications. To upgrade the client applications, simply replace the existing applications with the latest version.

1. Back up the current database using the JSS Database Utility.
   For more information, see [Backing Up the Database](#).

2. Copy the latest version of the JSS Installer for Linux (`jssinstaller.run`) to the server.
   Note: To obtain the JSS Installer for Linux, log in to Jamf Nation and click **Show alternative downloads** below the Casper Suite DMG on the following page:
   https://www.jamf.com/jamf-nation/my/products
   Note: The JSS Installer for Linux cannot be used to upgrade the JSS v8.1 or earlier.

3. Log in to the server as a user with superuser privileges.

4. Initiate the installer by executing:

   ```
   sudo sh /path/to/jssinstaller.run
   ```

5. Follow the onscreen instructions to complete the upgrade.

Setup

Setting Up the JSS

The first time you connect to the Jamf Software Server (JSS), the JSS Setup Assistant guides you through the following setup tasks:

- Accept the license agreement.
- Enter your activation code.
- Create your first JSS user account.
- Enter your JSS URL.
  The JSS URL is the URL that client applications, computers, and mobile devices will connect to when communicating with the JSS.

After you complete the JSS Setup Assistant, you can click the setup tips that are displayed onscreen to start configuring commonly used settings.

You may also want to make changes to the following pre-configured settings to ensure they meet the needs of your organization. These settings are important because over time, they can significantly affect the size of your database and your levels of network traffic:

- **"Update Inventory" policy**—Determines how often computers submit inventory to the JSS.
  For more information, see "Computer Inventory Collection" in the *Casper Suite Administrator's Guide*.
- **Recurring check-in frequency**—Determines the interval at which computers check in with the JSS for available policies.
  For more information, see "Recurring Check-in Frequency" in the *Casper Suite Administrator's Guide*.
- **Mobile device inventory collection frequency**—Determines how often mobile devices submit inventory to the JSS.
  For more information, see "Mobile Device Inventory Collection Settings" in the *Casper Suite Administrator's Guide*.

JSS User Accounts and Groups

The Jamf Software Server (JSS) is a multi-user application. JSS user accounts and groups allow you to grant different privileges and levels of access to each user.

When configuring a JSS user account or group, you can grant access to the full JSS or to a specific site. You can grant privileges by choosing one of the following privilege sets:

- **Administrator**—Grants all privileges.
- **Auditor**—Grants all read privileges.
- **Enrollment Only**—Grants all privileges required to enroll computers and mobile devices.
- **Custom**—Requires you to grant privileges manually.

If there are multiple users that should have the same access level and privileges, you can create a group with the desired access level and privileges and add accounts to it. Members of a group inherit the access level and privileges from the group. Adding an account to multiple groups allows you to grant a user access to multiple sites.

There are two ways to create JSS user accounts and groups: you can create standard accounts or groups, or you can add them from an LDAP directory service.

Important: It is recommended that you have at least one account that is not from an LDAP directory service in case the connection between the JSS and the LDAP server is interrupted.

The JSS User Accounts and Groups settings also allow you to do the following:

- Configure account preferences for each JSS user account.
- Configure the password settings in the Password Policy for all standard JSS user accounts.
- Unlock a JSS user account that is locked.

Requirements

To add accounts or groups from an LDAP directory service, you need an LDAP server set up in the JSS. (For more information, see "Integrating with LDAP Servers" in the *Casper Suite Administrator's Guide*.)

Creating a JSS User Group

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **System Settings**.

4. Click **JSS User Accounts & Groups** .

5. Click **New** .

6. Do one of the following:

- To create a standard JSS user group, select **Create Standard Group** and click **Next**.
- To add a JSS user group from an LDAP directory service, select **Add LDAP Group** and click **Next**. Then follow the onscreen instructions to search for and add the group.

7. Use the Group pane to configure basic settings for the group.

8. If you chose "Custom" from the **Privilege Set** pop-up menu, click the **Privileges** tab and select the checkbox for each privilege that you want to grant the group.

9. Click **Save**.

Creating a JSS User Account

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **System Settings**.

4. Click **JSS User Accounts & Groups** 👤 .

5. Click **New** ➕ .

6. Do one of the following:
   - To create a standard JSS user account, select **Create Standard Account** and click **Next**.
   - To add a JSS user account from an LDAP directory service, select **Add LDAP Account** and click **Next**. Then follow the onscreen instructions to search for and add the account.

7. On the Account pane, enter information about the account as needed.

8. Choose an access level from the **Access Level** pop-up menu:
   - To grant full access to the JSS, choose "Full Access".
   - To grant access to a site, choose "Site Access".
     Note: The "Site Access" option is only displayed if there are sites in the JSS. For more information on adding sites to the JSS, see "Sites" in the *Casper Suite Administrator's Guide*.
   - To add the account to a standard group, choose "Group Access".
     Note: The "Group Access" option is only displayed if there are standard groups in the JSS. For more information on creating groups, see Creating a JSS User Group.

9. Do one of the following:
   - If you granted the account full access or site access, choose a privilege set from the **Privilege Set** pop-up menu. Then, if you chose "Custom", click the **Privileges** tab and select the checkbox for each privilege that you want to grant the account.
   - If you added the account to a group, click the **Group Membership** tab and select the group(s) you want to add the account to.

10. Click **Save**.

Configuring Account Preferences

You can configure Language & Region and Search preferences for each JSS user account. Language & Region preferences allow you to configure settings such as date format and time zone. Search preferences allow you to configure settings for computer, mobile device, and user searches.

1. Log in to the JSS with a web browser.

2. At the top of the page, click the disclosure triangle next to your username and then click **Preferences**.

3. Click the **Language & Region** tab and use the pop-up menus to configure language and region preferences.

4. Click the **Search Preferences** tab and use the pop-up menus to configure search preferences.
   Note: The default search preference is "Exact Match". For most items, the option can be changed to either "Starts with" or "Contains".

5. Click **Save**.

Configuring the Password Policy

The Password Policy in the JSS allows you to configure the password settings. The Password Policy applies to all standard JSS user accounts. You can configure the following password settings:

- Number of login attempts allowed before a JSS user is locked out of the account
- Password length and age
- Password reuse limitations
- Password complexity
- Settings to allow a user to unlock their own account

Note: The settings configured in the Password Policy do not apply to JSS user accounts added from an LDAP directory service.

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **System Settings**.

4. Click **JSS User Accounts & Groups** 👤 .

5. Click **Password Policy** 🔑 .

6. Click **Edit**.

7. Use the settings on the pane to specify the password settings.

8. Click **Save**.

The settings are applied immediately.

Unlocking a JSS User Account

A JSS user could be locked out of their account if they exceed the specified number of allowed login attempts. If the Password Policy is configured to allow the user to unlock their account, the user can reset their password to unlock their account. In this case, an email is immediately sent to the email address associated with the account in the JSS allowing the user to unlock their account by resetting their password. For an email to be sent, an SMTP server must be set up in the JSS. (For more information, see Integrating with an SMTP Server.)

In addition, a JSS user account that is locked can be manually unlocked from the JSS by another JSS user with the Administrator privilege set.

The access status of the account is displayed as "Disabled" in the JSS until the account is unlocked.

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **System Settings**.

4. Click **JSS User Accounts & Groups** 👤 .
   A list of JSS user accounts and groups is displayed.

5. Click the JSS user account that has an access status of "Disabled", which means the account is locked.

6. Click **Edit**.

7. Choose "Enabled" from the **Access Status** pop-up menu to unlock the account.

8. Click **Save**.

   The JSS user account is unlocked immediately.

Related Information

For related information, see the following section in the *Casper Suite Administrator's Guide*:

"Sites"
Learn about sites and how to add them to the JSS.

Activation Code

The Activation Code settings in the Jamf Software Server (JSS) allow you to update the activation code for your license. You can also change the organization name associated with the license and view licensing information.

Updating the Activation Code

Every time you receive a new activation code, it must be updated in the JSS.

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** .

3. Click **System Settings**.

4. Click **Activation Code** .

5. Click **Edit**.

6. Enter the new activation code.

7. Click **Save**.

Integrating with an SMTP Server

Integrating with an SMTP server allows you to do the following:

- Send email notifications to Jamf Software Server (JSS) users when certain events occur. (For more information, see "Email Notifications" in the *Casper Suite Administrator's Guide*.)
- Send enrollment invitations via email.
- Send mass emails to end users.

To integrate with an SMTP server, you need to configure the SMTP Server settings in the JSS.

Configuring the SMTP Server Settings

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **SMTP Server** .
5. Click **Edit**.
6. Configure the settings on the pane.
7. Click **Save**.

Testing the SMTP Server Settings

Once the SMTP Server settings are configured, you can send a test email from the JSS.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **SMTP Server** .
5. Click **Test**.
6. Enter a test email address and click **Test** again.

A message displays, reporting whether or not the email was sent successfully.

Related Information

For related information, see the following sections in the *Casper Suite Administrator's Guide*:

- "Email Notifications"
  Learn about the different email notifications that can be sent JSS users.

- "User-Initiated Enrollment for Computers"
  Find out how to send computer enrollment invitations via email.

- "User-Initiated Enrollment for Mobile Devices"
  Find out how to send mobile device enrollment invitations via email.

- "Performing Mass Actions for Computers"
  Find out how to send a mass email to computer users.

- "Performing Mass Actions for Mobile Devices"
  Find out how send a mass email to mobile device users.

Change Management

Change Management allows you to track the changes that happen in the Jamf Software Server (JSS), such as the creation of a JSS user account. The Change Management settings in the JSS allow you to log those changes to a log file (JAMFChangeManagement.log) on the JSS host server and/or log the changes to a syslog server.

The Change Management logs can also be viewed in the JSS. The information displayed includes:

- Date/time the change took place
- Username of the administrator who made the change
- Object type (such as a JSS user account)
- Object name (such as the username of a JSS user account)
- Action (such as "Created")
- Details about the change

In addition, you can view the changes to a specific object in that object's history. (For more information, see "Viewing the History of a JSS Object" in the *Casper Suite Administrator's Guide*.)

Requirements

To log changes to a log file, the account used to run Tomcat must have write permissions for the directory where the `JAMFChangeManagement.log` file is located.

Configuring the Change Management Settings

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **System Settings**.

4. Click **Change Management** ▦ .

5. Click **Edit**.

6. Configure the settings on the pane.

7. Click **Save**.

Viewing Change Management Logs in the JSS

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **System Settings**.

4. Click **Change Management** ▦ .

5. Click **Logs**.
   The Change Management logs are displayed on the pane.

6. Do one of the following:

   ▪ To view the object associated with a change, click the object in the Object Name column.

   ▪ To view details about the change, click **Details** in the Details column.

Related Information

For related information, see the following Knowledge Base article:

[Change Management with the Casper Suite: macOS Setup Guide](#)
If you are hosting the JSS on a server with macOS Server installed, learn about setting up the syslogd utility so you can log changes to a syslog server.

Integrating with GSX

Integrating with Apple's Global Service Exchange (GSX) allows you to look up and populate the following purchasing information for computers and mobile devices:

- Purchase date
- Warranty expiration date
- Apple Care ID (warranty reference number)

Note: GSX may not always return complete purchasing information. Only the information found in GSX is returned.

To integrate with GSX, you need to configure the GSX Connection settings in the JSS, which involves entering GSX account information and uploading an Apple certificate.

You can also use the JSS to test the connection and upload a renewed Apple certificate when needed.

Requirements

To configure the GSX Connection settings, you need:

- A GSX account with the "Manager" role, access to Web Services, and access to coverage/warranty information
- An Apple certificate (.pem or .p12)

For instructions on creating a GSX account and obtaining an Apple certificate, see the [Integrating with Apple's Global Service Exchange (GSX)](#) Knowledge Base article.

Configuring the GSX Connection Settings

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **Global Management**.

4. Click **GSX Connection** 🌐 .

5. Click **Edit**.

6. Select **Enable Connection to GSX**.
   Note: This and some of the other settings on this pane may already be configured if the JSS was used to generate a CSR.

7. Enter the username and account number for the GSX account.

8. Configure the region and URI settings as needed.

9. Select **Certificate-based Authentication** and click **Upload**.

10. Follow the onscreen instructions to upload the Apple certificate (.pem or .p12).

Testing the GSX Connection

Once the GSX Connection settings are configured, you can test the connection to make sure it works .

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Global Management**.
4. Click **GSX Connection** 🌐 .
5. Click **Test**.
6. Click **Test** again.

A message displays, reporting the success or failure of the connection.

Renewing the Apple Certificate

You can use the JSS to upload a renewed Apple certificate without removing the existing certificate so the connection with GSX is not lost. A notification is displayed 31 days prior to the expiration date of the Apple certificate.

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** ⚙ .
3. Click **Global Management**.
4. Click **GSX Connection** 🌐 .
5. Click **Edit.**
6. Click **Renew**.
7. Follow the onscreen instructions to upload a renewed Apple certificate.

Related Information

For related information, see the following sections in the *Casper Suite Administrator's Guide*:

- "Performing Mass Actions for Computers"
  Find out how to mass look up and populate purchasing information from GSX.

- "Performing Mass Actions for Mobile Devices"
  Find out how to mass look up and populate purchasing information from GSX.

- "Viewing and Editing Inventory Information for a Mobile Device"
  You can look up and populate purchasing information for a single mobile device by editing the device's inventory information in the JSS.

- "Viewing and Editing Inventory Information for a Computer"
  You can look up and populate purchasing information for a single computer by editing the computer's inventory information in the JSS.

- "Local Enrollment Using Recon"
  Find out how to look up and populate purchasing information when enrolling a computer by running Recon locally.

- "Remote Enrollment Using Recon"
  Find out how to look up and populate purchasing information when enrolling a computer by running Recon remotely.

JSS Summary

The JSS Summary is a custom report that allows you to view information about your Jamf Software Server (JSS). The JSS Summary can be useful for troubleshooting JSS issues, and for providing information to Jamf for purposes of support or license renewal.

By default, the JSS Summary includes the following information about the JSS:

- Number of managed and unmanaged computers
- Number of managed mobile devices
- Operating system on the JSS host server
- Path to the JSS web application
- Apache Tomcat version
- Information about the version of Java installed on the JSS host server
- Information about the MySQL connection and configuration

You can also add information to the JSS Summary from the following categories as needed:

- Computers
- Mobile Devices
- Users
- System Settings
- Global Management
- Computer Management
- Computer Management–Server Infrastructure
- Computer Management–Management Framework
- Mobile Device Management
- Network Organization
- Database

You can view the JSS Summary in a browser window or send the JSS Summary to Jamf.

Requirements

To send the JSS Summary to Jamf, you need a valid Jamf Nation account.

To create a Jamf Nation account, go to:
https://www.jamf.com/jamf-nation/users/new

Viewing the JSS Summary

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **JSS Information**.

4. Click **JSS Summary** 📋 .

5. Select the checkboxes next to the items you want to include.

6. Click **Create**.
   The JSS Summary displays in a browser window.

7. Click the **Back** button in the web browser to return to the JSS Summary pane in the JSS.

Sending the JSS Summary to Jamf

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **JSS Information**.

4. Click **JSS Summary** 📋 .

5. Select the checkboxes next to the items you want to include.

6. Click **Send Summary to Jamf**.

7. Enter your Jamf Nation credentials, and then click **Send**.

   The JSS Summary is sent to Jamf via Jamf Nation.

Related Information

For information about Customer Experience Metrics (CEM), see the following Knowledge Base article:

Customer Experience Metrics
Learn about Customer Experience Metrics and how to configure the setting in your JSS environment.

For additional information about Customer Experience Metrics, visit the following webpage:
https://www.jamf.com/products/jamf-pro/customer-experience-metrics/

Server Infrastructure

About Distribution Points

Distribution points are servers used to host files for distribution to computers and mobile devices. The following types of files can be distributed from a distribution point using the Casper Suite:

- Packages
- Scripts
- In-house apps
- In-house eBooks

The Casper Suite supports three types of distribution points:

- File share distribution points
- A cloud distribution point
- Jamf Distribution Server (JDS) instances

You can use any combination of these types of distribution points.

By default, the first distribution point you add to the Jamf Software Server (JSS) is the master distribution point. The master distribution point is used by all other distribution points as the authoritative source for all files during replication. You can change the master distribution point at any time.

When planning your distribution point infrastructure, it is important to understand the differences between each type of distribution point. The following table explains the key differences:

	File Share Distribution Point	Cloud Distribution Point	JDS Instance
Description	Standard server that is configured to be a distribution point	Distribution point that uses one of the following content delivery networks (CDNs) to host files: - Rackspace Cloud Files - Amazon Web Services - Akamai	Distribution point that is managed by the JSS, similar to a computer or mobile device
Maximum Number per JSS	Unlimited	One	Unlimited
Server /Platform Requirements	Any server with an Apple Filing Protocol (AFP) or Server Message Block (SMB) share	None	Mac or Linux

	File Share Distribution Point	Cloud Distribution Point	JDS Instance
Protocol	AFP, SMB, HTTP, or HTTPS	HTTPS	HTTPS
Ports	- AFP: 548 - SMB: 139 - HTTP: 80 - HTTPS: 443	443	443
Authentication Options	- AFP or SMB: - No authentication - Username and password - HTTP or HTTPS: - No authentication - Username and password - Certificate-based authentication	None	- No authentication - Certificate-based authentication
Files that Can Be Hosted	- Packages - Scripts	- Packages - In-house apps - In-house eBooks **Note:** If you use the cloud distribution point, scripts are stored in the jamfsoftware database.	- Packages - In-house apps - In-house eBooks **Note:** If you use one or more JDS instances, scripts are stored in the jamfsoftware database.
Parent-Child Capabilities	No	No	Yes
File Replication Method	Replication to file share distribution points must be initiated from Casper Admin.	Replication to a cloud distribution point must be initiated from Casper Admin.	Replication to root JDS instances must be initiated from Casper Admin. Replication to non-root JDS instances happens automatically and immediately.

	File Share Distribution Point	Cloud Distribution Point	JDS Instance
Selective Replication	Not available when replicating to file share distribution points.	Available when replicating to a cloud distribution point if the master distribution point is a JDS instance or file share distribution point. The files for replication must be specified in the JSS and the replication initiated from Casper Admin.	Not available when replicating to root JDS instances. Available when replicating to non-root JDS instances. The files for replication must be specified in the JSS. The replication from non-root parent to child instances is initiated on check in with the JSS.

Related Information

For related information, see the following sections in this guide:

- File Share Distribution Points
  Find out how to manage file share distribution points in the JSS.

- Cloud Distribution Point
  Find out how to manage the cloud distribution point.

- Jamf Distribution Server Instances
  Find out how to install and manage JDS instances.

File Share Distribution Points

Any server with an AFP or SMB share can be used as a file share distribution point. Before you can use a file share distribution point with the Casper Suite, you must set up the distribution point and add it to the Jamf Software Server (JSS).

For information on setting up a file share distribution point, see the following Knowledge Base article:
Setting Up a File Share Distribution Point

When you add a file share distribution point to the JSS, you can do the following:

- Make it the master distribution point.
- Choose a failover distribution point.
- Configure HTTP downloads.

Adding a File Share Distribution Point

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Server Infrastructure**.
4. Click **File Share Distribution Points** .
5. Click **New** .
6. Use the General pane to configure basic settings for the distribution point.
7. Click the **File Sharing** tab and enter information about the AFP or SMB share.
8. (Optional) Click the **HTTP** tab and configure HTTP downloads.
9. Click **Save**.

Replicating Files to a File Share Distribution Point

During replication, all files on the master distribution point are replicated to the file share distribution point that you choose.

1. Open Casper Admin and authenticate to the JSS.
2. In the sidebar, select the file share distribution point you want to replicate files to.
3. Click **Replicate**.

Related Information

For related information, see the following section in the *Casper Suite Administrator's Guide*:

"Network Segments"
You can use network segments to ensure that computers and mobile devices use the closest distribution point by default.

For related information, see the following Knowledge Base articles:

- [Setting Up a File Share Distribution Point on Linux Using Samba](#)
  Find out how to use Samba to set up a file share distribution point with an SMB share on a Linux server.

- [Using Apache HTTP Server to Enable HTTP Downloads on a Linux File Share Distribution Point](#)
  Find out how to use Apache HTTP Server to enable HTTP downloads on a Linux file share distribution point.

- [Using IIS to Enable HTTP Downloads on a Windows Server 2008 File Share Distribution Point](#)
  Find out how to activate Internet Information Services (IIS) and use it to enable HTTP downloads on a Windows Server 2008 file share distribution point.

Cloud Distribution Point

The cloud distribution point uses a content delivery network (CDN) to host packages, in-house apps, and in-house eBooks. The Jamf Software Server (JSS) supports the following content delivery services:

- Rackspace Cloud Files
- Amazon S3 or Amazon CloudFront
- Akamai NetStorage or Akamai EdgeSuite
- Jamf Cloud Distribution Service (JCDS)

When you configure the cloud distribution point in the JSS, you can choose to make it the master. You can also choose whether to replicate specific files or the entire contents of the master distribution point if the master is a JDS instance or file share distribution point.

The JSS supports the use of signed URLs created with Amazon CloudFront. It also supports Akamai Remote Authentication. For more information about signed URLs created with CloudFront, see the following website:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html

For more information about Akamai Remote Authentication, contact your Akamai Account Manager.

Requirements

If you plan to use Akamai for your cloud distribution point, Akamai must be configured to use File Transfer Protocol (FTP).

Note: If you have upgraded from the Casper Suite v8.x, you must migrate the scripts and packages on your master distribution point before configuring the cloud distribution point. (For more information, see the Migrating Packages and Scripts Knowledge Base article.)

Files that are uploaded to a cloud distribution point cannot have filenames that include the following characters:

/ : ? < > \ * | " [ ] @ ! % ^ #

Configuring the Cloud Distribution Point

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** .

3. Click **Server Infrastructure**.

4. Click **Cloud Distribution Point** .

5. Click **Edit**.

6. Choose a content delivery network from the **Content Delivery Network** pop-up menu.

7. Configure the settings on the pane.

8. Click **Save**.

Testing the Cloud Distribution Point

Once the cloud distribution point is configured, you can test the connection to the content delivery network.

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** .

3. Click **Server Infrastructure**.

4. Click **Cloud Distribution Point** .

5. Click **Test**.

6. Click **Test** again.

   A message displays, reporting the success or failure of the connection.

Replicating Files to the Cloud Distribution Point

During replication, files on the master distribution point are replicated to the cloud distribution point via Casper Admin. The files that are replicated depend on whether the cloud distribution point is configured to replicate specific files or the entire contents of the master.

1. Open Casper Admin and authenticate to the JSS.

2. In the sidebar, select the cloud distribution point you want to replicate files to.

3. Click **Replicate**.

Related Information

For related information, see the following section in the *Casper Suite Administrator's Guide*:

"Network Segments"
You can use network segments to ensure that computers and mobile devices use the closest distribution point by default. For related information, see the following Knowledge Base article:

Information Required to Configure a Cloud Distribution Point in the JSS
Learn about the information that must be obtained from your cloud services provider to configure the cloud distribution point in the JSS.

For more information about content delivery services, visit the following websites:

- Rackspace Cloud Files
  http://www.rackspace.com/cloud/files/
- Amazon S3
  http://aws.amazon.com/s3/
- Amazon CloudFront
  http://aws.amazon.com/cloudfront/
- Akamai NetStorage
  http://www.akamai.com/html/solutions/netstorage.html
- Akamai EdgeSuite
  http://www.akamai.com/en/html/services/edgesuite.html
- Jamf Cloud Distribution Service
  http://www.jamfsoftware.com/products/jamf-cloud/

Jamf Distribution Server Instances

A Jamf Distribution Server (JDS) instance is a distribution point that is managed by the Jamf Software Server (JSS), similar to a computer or mobile device. It can be used to host packages, in-house apps, and in-house eBooks.

Before using a JDS instance, you must install it and configure it. JDS instances can be installed on Mac or Linux. When you install a JDS instance, it is enrolled with the JSS. You can install as many instances as your organization requires.

By default, the first JDS instance you install is the root. The root instance is used by other instances as the authoritative source for all files. The root instance can also be used as the master distribution point. You can make a different instance the root at any time.

You can define parent-child relationships between non-root JDS instances, making selective file replication more manageable.

When you configure a JDS instance, you can do the following:

- Make it the master distribution point.
- Choose a parent JDS instance (non-root JDS instances only).
- Enable certificate-based authentication.
- Limit the rate at which the JDS instance downloads files.
- Specify WebDAV accounts.
- Choose whether to replicate specific files or the entire contents of the parent JDS instance (non-root JDS instances only).

You can also view the progress of file replication and view inventory information for each JDS instance.

Requirements

The JDS Installer for Mac requires a computer with:

- An Intel processor
- 2 GB of RAM
- 100 GB of disk space available
- macOS v10.7 or later with macOS Server v1.4.3 or later installed

The JDS Installer for Linux requires a computer with:

- An Intel processor
- 2 GB of RAM
- 100 GB of disk space available
- One of the following operating systems:
  - Ubuntu 10.04 LTS Server

- Ubuntu 12.04 LTS Server
- Red Hat Enterprise Linux (RHEL) 6.4, 6.5, 6.6, or 7.0
  Note: To install a JDS instance on a Linux operating system that is running on a virtual machine, you need a virtualization platform that provides SMBIOS information.

To manage JDS instances in the JSS, you need a valid SSL certificate on the JSS host server. (For more information, see SSL Certificate.)

Note: If you have upgraded from the Casper Suite v8.x, you must migrate the scripts and packages on your master distribution point before configuring JDS instances. (For more information, see the Migrating Packages and Scripts Knowledge Base article.)

Installing a JDS Instance on Mac

1. Copy the JDS Installer for Mac (`JDS Installer.pkg`) to the server on which you plan to install a JDS instance.
   Note: To obtain the JDS Installer for Mac, log in to Jamf Nation and go to the following page: https://www.jamf.com/jamf-nation/my/products

2. Double-click the installer.

3. Follow the onscreen instructions to complete the installation.

Installing a JDS Instance on Linux

1. Copy the JDS Installer for Linux (`JDS Installer.run`) to the server on which you plan to install a JDS instance.
   Note: To obtain the JDS Installer for Linux, log in to Jamf Nation and go to the following page: https://www.jamf.com/jamf-nation/my/products

2. Log in to the server as a user with superuser privileges.

3. Initiate the installer by executing a command similar to the following:

```
sudo /path/to/JDS Installer.run
```

4. When prompted, enter the JDS hostname. For example, "jds.mycompany.com".

5. When prompted, enter the JSS URL. For example, "https://jss.mycompany.com:8443/".

6. When prompted, enter credentials for a JSS user account with the "JDS" privilege.

7. Follow the onscreen instructions to complete the installation.

Configuring a JDS Instance

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **Server Infrastructure**.

4. Click **JDS Instances** 🔧 .

5. Click the JDS instance you want to configure.

6. Click **Edit.**

7. Use the General pane to configure basic settings for the JDS instance.

8. Click the **Distribution Point** tab and configure distribution settings.

9. Click **Save.**

Replicating Files to the Root JDS Instance

During replication, all files on the master distribution point are replicated to the root JDS instance. Then, files are replicated to child JDS instances from their non-root parent instances on check in with the JSS. The files that are replicated to non-root JDS instances depend on whether each instance is configured to replicate specific files or the entire contents of their parent JDS instance.

1. Open Casper Admin and authenticate to the JSS.

2. In the sidebar, select the root JDS instance.

3. Click **Replicate.**

Viewing the Progress of File Replication

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **Server Infrastructure**.

4. Click **JDS Instances** .

5. Click **Grid View** at the top of the list.

The progress of file replication for each JDS instance is displayed. If your master distribution point is a JDS instance, it is marked with two asterisks (**). If your master distribution point is a different type of distribution point, the root instance is marked with a single asterisk (*).

Viewing Inventory Information for a JDS Instance

The JSS displays the following inventory information for each JDS instance:

- Whether or not it is the master distribution point
- Whether or not it is the root instance
- Hostname
- URL
- Reported IP address
- jamfds binary version
- Operating system
- Operating system version
- Total memory
- Available memory
- Hard drive size
- Hard drive used space

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** .

3. Click **Server Infrastructure**.

4. Click **JDS Instances** .

5. Click the JDS instance you want to view inventory information for.

Related Information

For related information, see the following section in the *Casper Suite Administrator's Guide*:

"Network Segments"
You can use network segments to ensure that computers and mobile devices use the closest distribution point by default.

For related information, see the following Knowledge Base articles:

- Components Installed on JDS Instances
  Find out what items are installed on JDS instances.

- Changing JDS Hierarchy
  Learn about the implications of changing your JDS hierarchy.

- Uninstalling a JDS Instance
  Find out how to uninstall a JDS instance.

Jamf Infrastructure Manager Instances

A Jamf Infrastructure Manager instance is a service that is managed by the Jamf Software Server (JSS). It can be used to host the following:

- **LDAP Proxy**—This allows traffic to pass securely between a JSS and an LDAP directory service. The Infrastructure Manager and the LDAP Proxy typically reside within the DMZ.
  The LDAP Proxy requires integration with an LDAP directory service.
  For more information, see "LDAP Proxy" in the *Casper Suite Administrator's Guide*.

- **Healthcare Listener**—This allows traffic to pass securely from a healthcare management system to a JSS.
  For more information, see "Healthcare Listener" in the *Casper Suite Administrator's Guide*.

When you install an instance of the Infrastructure Manager, the JSS allows you to enable the LDAP Proxy or the Healthcare Listener. Infrastructure Manager instances can be installed on Linux and Windows.

Requirements

The Jamf Infrastructure Manager Installer requires a computer with the following:

- One of the following operating systems:

  - Ubuntu 14.04 LTS Server (64-bit) or Ubuntu 16.04 LTS Server (64-bit)
  - Red Hat Enterprise Linux (RHEL) 7.0, 7.1, or 7.2
  - Windows Server 2008 R2 (64-bit), Windows Server 2012 (64-bit), or Windows Server 2012 R2 (64-bit)

- A 64-bit capable Intel processor

- 2 GB of RAM

- 300 MB of disk space available

- Java 1.8 (For more information, see the [Installing Java and MySQL](#) Knowledge Base article.)

On the JSS, the built-in CA or a trusted third-party CA must be configured.

Installing a Jamf Infrastructure Manager Instance on Ubuntu

1. Copy the Infrastructure Manager Installer for Linux (`jamf-im.deb`) to the computer on which you plan to install it.
   Note: To obtain the Infrastructure Manager Installer for Linux, log in to Jamf Nation and go to the following page:
   https://www.jamf.com/jamf-nation/my/products
   This installer allows you to enable the LDAP Proxy.
   To install an Infrastructure Manager instance that allows you to enable the Healthcare Listener, contact Jamf Support.

2. Log in to the server as a user with superuser privileges.

3. Initiate the installer by executing a command similar to the following:

```
sudo dpkg --install /path/to/jamf-im.deb
```

4. When prompted, enter the JSS URL. For example, "https://jss.mycompany.com:8443/".

5. When prompted, enter credentials for a JSS user account with the "Infrastructure Manager" privilege.

6. When prompted, enter the JSS password.

7. When prompted, enter the hostname of the computer on which the Infrastructure Manager is installed. For example, "computername.mycompany.com".
   Note: The hostname must be entered as a fully qualified domain name.

8. Follow the onscreen instructions to complete the installation.

   When the Infrastructure Manager instance installation is complete, the JSS allows you to enable the LDAP Proxy and/or enable the Healthcare Listener.

Installing a Jamf Infrastructure Manager Instance on Red Hat Enterprise Linux

1. Copy the Infrastructure Manager Installer for Linux (jamf-im.rpm) to the computer on which you plan to install it.
   Note: To obtain the Infrastructure Manager Installer for Linux, log in to Jamf Nation and go to the following page:
   https://www.jamf.com/jamf-nation/my/products
   This installer allows you to enable the LDAP Proxy.
   To install an Infrastructure Manager instance that allows you to enable the Healthcare Listener, contact Jamf Support.

2. Log in to the server as a user with superuser privileges.

3. Initiate the installer by executing a command similar to the following:

```
sudo rpm -i /path/to/jamf-im-1.1.0-1.noarch.rpm
```

4. When prompted, execute the following command:

```
sudo jamf-im enroll
```

5. When prompted, enter the JSS URL. For example, "https://jss.mycompany.com:8443/".

6. When prompted, enter credentials for a JSS user account with the "Infrastructure Manager" privilege.

7. When prompted, enter the JSS password.

8. When prompted, enter the hostname of the computer on which the Infrastructure Manager is installed. For example, "computername.mycompany.com".
   Note: The hostname must be entered as a fully qualified domain name.

9. Follow the onscreen instructions to complete the installation.

When the Infrastructure Manager instance installation is complete, the JSS allows you to enable the LDAP Proxy and/or enable the Healthcare Listener.

Installing a Jamf Infrastructure Manager Instance on Windows

1. Copy the Infrastructure Manager Installer for Windows (Jamf-Infrastructure-Manager-version.msi) to the computer on which you plan to install it.
   Note: "Version" is the version of the Infrastructure Manager you are using. For example, "Jamf-Infrastructure-Manager-1.1.0.msi".
   To obtain the Infrastructure Manager Installer for Windows, log in to Jamf Nation and go to the following page:
   https://www.jamf.com/jamf-nation/my/products
   This installer allows you to enable the LDAP Proxy.
   To install an Infrastructure Manager instance that allows you to enable the Healthcare Listener, contact Jamf Support.

2. Run the installer.
   Note: The installer must be run as an administrator.

3. When prompted, select setup type.

4. When prompted, enter the JSS URL. For example, "https://jss.mycompany.com:8443/".

5. When prompted, enter credentials for a JSS user account with the "Infrastructure Manager" privilege.

6. When prompted, enter the JSS password.

7. When prompted, enter the hostname of the computer on which the Infrastructure Manager is installed. For example, "computername.mycompany.com".
   Note: The hostname must be entered as a fully qualified domain name.

8. Follow the onscreen instructions to complete the installation.

When the Infrastructure Manager instance installation is complete, the JSS allows you to enable the LDAP Proxy and/or enable the Healthcare Listener.

Viewing Inventory Information for a Jamf Infrastructure Manager Instance

The JSS displays the following inventory information for each Infrastructure Manager instance:

- Last Check-in
- IP Address at Last Check-in
- Operating System
- Operating System Version

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **Computer Management.**

4. In the "Computer Management–Server Infrastructure" section, click **Infrastructure Managers** 🔗 .
   A list of Infrastructure Manager instances is displayed along with the services that are installed on each instance.

5. Click the Infrastructure Manager instance you want to view inventory information for.

Further Considerations

- When editing an Infrastructure Manager instance, only the display name and recurring check-in frequency can be changed.
  Note: The default check-in frequency at which the Infrastructure Manager instance checks in with the JSS is 30 seconds.

- An Infrastructure Manager instance cannot be deleted if there are dependencies for the Infrastructure Manager. For example, an Infrastructure Manager cannot be deleted if there is an LDAP Proxy hosted on it. To delete the Infrastructure Manager, you must first disable the LDAP Proxy.

- If a Healthcare Listener is hosted on the Infrastructure Manager, the Healthcare Listener is deleted when the Infrastructure Manager is deleted.

Related Information

For related information, see the following section in the *Casper Suite Administrator's Guide*:

"Email Notifications"
Learn how to enable an email notification in the event that an Infrastructure Manager instance does not check in with the JSS.

Advanced Configuration

SSL Certificate

The Jamf Software Server (JSS) requires a valid SSL certificate to ensure that computers and mobile devices communicate with the JSS and not an imposter server.

The Apache Tomcat settings in the JSS allow you to create an SSL certificate from the CA that is built into the JSS. You can also upload the certificate keystore for an SSL certificate that was obtained from an internal certificate authority (CA) or a trusted third-party vendor.

Note: If your environment is hosted in Jamf Cloud, the Apache Tomcat settings are managed by Jamf Cloud and are not accessible.

Requirements

To create or upload an SSL certificate, the JSS must be installed as the "ROOT" web application, and the user running the Tomcat process must have read/write access to Tomcat's `server.xml` file.

Creating or Uploading an SSL Certificate

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** .

3. Click **System Settings**.

4. Click **Apache Tomcat Settings** .

5. Click **Edit**.

6. Select **Change the SSL certificate used for HTTPS** and click **Next**.

7. Follow the onscreen instructions to upload or create an SSL certificate.

8. Restart Tomcat for the changes to take effect.
   For instructions on how to restart Tomcat, see the following Knowledge Base article:
   Starting and Stopping Tomcat

Related Information

For related information, see the following Knowledge Base article:

Using OpenSSL to Create a Certificate Keystore for Tomcat
Find out how to use OpenSSL to create a certificate keystore that you can upload to the JSS.

Configuring Tomcat to Work with a Load Balancer

When the Jamf Software Server (JSS) is behind a load balancer, you must configure the remote IP valve, proxy port, and scheme in Tomcat's `server.xml` file. The Load Balancing settings in the JSS allow you to configure these settings without having to edit the `server.xml` file manually.

Requirements

To configure Load Balancing settings using the JSS, the JSS must be installed as the "ROOT" web application, and the user running the Tomcat process must have read/write access to Tomcat's `server.xml` file.

Configuring Load Balancing Settings

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** .

3. Click **System Settings**.
   On a smartphone or iPod touch, this option is in the pop-up menu.

4. Click **Apache Tomcat Settings** .

5. Click **Edit**.

6. Select **Configure Tomcat for working behind a load balancer** and click **Next**.

7. Follow the onscreen instructions to configure the Load Balancing settings.

8. Restart Tomcat for the changes to take effect.
   For instructions on how to restart Tomcat, see the following Knowledge Base article:
   [Starting and Stopping Tomcat](#)

Tomcat Thread Pool Settings

Configuring the Tomcat Thread Pool settings using the Jamf Software Server (JSS) allows you to make modifications to Tomcat's `server.xml` file without having to edit it manually.

Requirements

To configure Tomcat Thread Pool settings using the JSS, the JSS must be installed as the "ROOT" web application, and the user running the Tomcat process must have read/write access to Tomcat's `server.xml` file.

Configuring Tomcat Thread Pool Settings

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** .

3. Click **System Settings**.
   On a smartphone or iPod touch, this option is in the pop-up menu.

4. Click **Apache Tomcat Settings** .

5. Click **Edit**.

6. Select **Update the settings for Tomcat's thread pool** and click **Next**.

7. Follow the onscreen instructions to configure the Thread Pool settings.

8. Restart Tomcat for the changes to take effect.
   For instructions on how to restart Tomcat, see the following Knowledge Base article:
   Starting and Stopping Tomcat

JSS Web Application Memory

The Jamf Software Server (JSS) allows you to view the amount of memory being used by the web application. If you need to change the amount of memory allocated to the web application, you can use the JSS Database Utility to do so.

Viewing Memory Usage

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **JSS Information**.
   On a smartphone or iPod touch, this option is in the pop-up menu.

4. Click **Memory Usage** .
   A pie chart of used and available memory is displayed.

Configuring Web Application Memory Using the GUI

1. Open the JSS Database Utility on the JSS host server by executing:

   ```
   sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar
   ```

2. If prompted, enter the password for your account and then press the Return key.

3. If the JSS Database Utility is unable to locate the MySQL binary, you are prompted to enter the path. Click **Continue** and enter the full path to the binary.

4. From the menu bar, choose **Utilities** > **Change Tomcat settings**.

5. Use the Maximum Memory and Minimum Memory sliders to configure the amount of memory allocated to the web application.
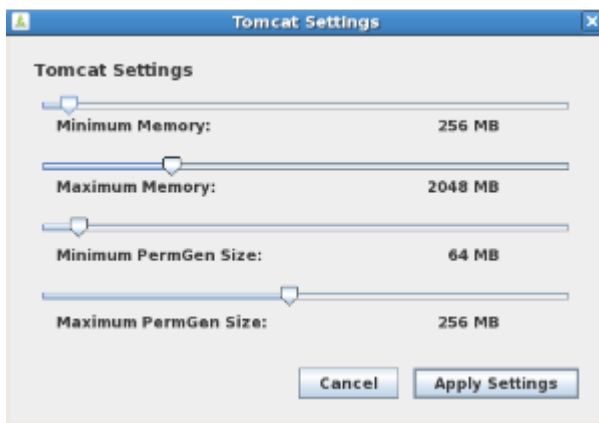
6. Click **Apply Settings**.

7. When prompted to restart Tomcat, click **Yes**.

Configuring Web Application Memory Using the Command Line

1. Open the file that contains the Tomcat memory settings.

   - If you used the JSS Installer to install the JSS, execute:

     ```
     sudo nano /usr/local/jss/tomcat/bin/setenv.sh
     ```

   - If you did not use the JSS Installer to install the JSS, create the `setenv.sh` file in the following location:
     ```
     /usr/local/jss/tomcat/bin/
     ```

2. Append a custom JAVA_OPTS environment variable to the bottom of the `setenv.sh` file to configure the amount of memory allocated to the web application. For example, to allocate 1 GB of RAM, the variable should look something like this:

   ```
   JAVA_OPTS=" -Xmx1024M -XX:MaxPermSize=256M"
   ```

   Note: Custom settings will persist after performing an upgrade.

3. Save and close the file by pressing Control-O, and then Control-X.

4. Restart Tomcat for the change to take effect.
   For instructions on how to restart Tomcat, see the following Knowledge Base article:
   [Starting and Stopping Tomcat](#)

Tomcat PermGen Size

You can use the JSS Database Utility to configure the minimum and maximum PermGen sizes for Tomcat.

Note: When upgrading from Tomcat 7 to Tomcat 8, the minimum and maximum PermGen sizes are automatically reset to 256 MB. When using Java 1.8, PermGen sizes do not need to be set.

Configuring Tomcat PermGen Size Using the GUI

1. Open the JSS Database Utility on the JSS host server by executing:

```
sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar
```

2. If prompted, enter the password for your account and then press the Return key.

3. If the JSS Database Utility is unable to locate the MySQL binary, you are prompted to enter the path. Click **Continue** and enter the full path to the binary.

4. From the menu bar, choose **Utilities** > **Change Tomcat settings**.

5. Use the PermGen Size sliders to configure the minimum and maximum PermGen sizes as needed.
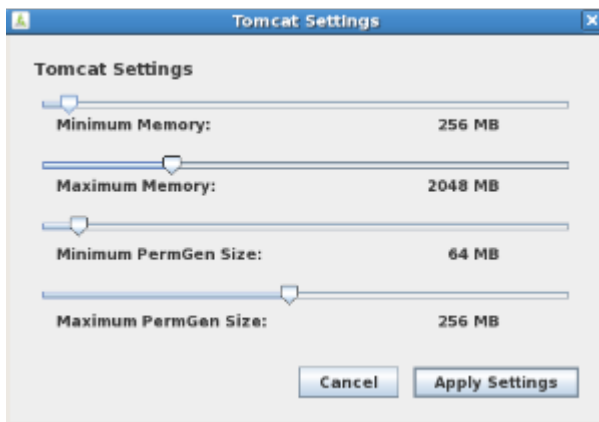
6. Click **Apply Settings**.

7. When prompted to restart Tomcat, click **Yes**.

Configuring Tomcat PermGen Size Using the Command Line

1. Open the file that contains the Tomcat memory settings.

   - If you used the JSS Installer to install the JSS, execute:

```
sudo nano /usr/local/jss/tomcat/bin/setenv.sh
```

- If you did not use the JSS Installer to install the JSS, execute one of the following commands:
  Note: If using the JSS v9.93 or earlier, or if you manually installed Tomcat 7, replace "tomcat8" references with "tomcat7".

  - On Ubuntu, execute:

    ```
    sudo nano /etc/init.d/tomcat8
    ```

  - On RHEL, execute:

    ```
    sudo nano /etc/tomcat8/tomcat8.conf
    ```

2. Locate the `JAVA_OPTS` environment variable that defines memory and uncomment it if it is commented. This variable looks something like this:

   ```
   JAVA_OPTS=" -XmxSizeM -XX:MaxPermSize=256M"
   ```

3. Change the -XX parameter to change the Tomcat PermGen sizes. For example, to use 256 MB as the maximum PerGem size, change the variable to look something like this:

   ```
   JAVA_OPTS=" -Xmx1024M -XX:MaxPermSize=256M"
   ```

4. Save and close the file by pressing Control-O, and then Control-X.

5. Restart Tomcat for the change to take effect.
   For instructions on how to restart Tomcat, see the following Knowledge Base article:
   Starting and Stopping Tomcat

Viewing the Status of Database Tables

MySQL database tables can become corrupt if the database was not shut down properly or if the Jamf Software Server (JSS) host server is too slow to manage the number of computers in your organization. You can view the status of database tables right from the JSS.

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **JSS Information.**
   On a smartphone or iPod touch, this option is in the pop-up menu.

4. Click **Database Table Status** 🗄 .

Clustering

A clustered environment is one that has multiple instances of the Jamf Software Server (JSS) web application pointing to the same database. Clustering is useful in large environments that require multiple web applications, or environments with a web application in the DMZ.

When setting up a clustered environment, it is recommended that you configure the Clustering settings in the JSS using the web application that you plan to make the master, and then install other JSS web applications that point to the same database. However, if you already have multiple JSS web applications installed and pointed to the same database, you can configure the Clustering settings in the JSS after the fact. (For more information on setting up a clustered environment, contact Jamf Support.)

The Clustering settings in the JSS allow you to configure the frequency at which clustered web applications are synced with the database, and specify which web application should function as the master.

The master web application handles tasks such as upgrading the database schema and flushing logs from the database.

The JSS also allows you to view a list of web applications that are pointed to the same database and information about them.

Requirements

To cluster web applications that are not in the DMZ, you need a load balancer with the address of the JSS. For example:

https://jss.mycompany.com:8443/

The load balancer should route traffic to the servers running the web application.

Configuring Clustering Settings

1. Log in to the JSS web application with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **System Settings**.
   On a smartphone or iPod touch, this option is in the pop-up menu.

4. Click **Clustering** 🌐 .

5. Click **Edit**.

6. Configure the settings on the pane.
   To specify which web application should function as the master, select the **Master** option for the web application.

7. Click **Save**.

8. If you already have multiple JSS web applications pointed to the same database, restart Tomcat on any of the web applications for the changes to take effect.
   For instructions on how to restart Tomcat, see the following Knowledge Base article:
   Starting and Stopping Tomcat

Related Information

For related information, see the following Knowledge Base articles:

Caching Configuration
Find out how to configure distributed caching for clustered JSS environments.

Installing a JSS Web Application in the DMZ
Find out how to install a web application in the DMZ, and learn when in the process you should configure the Clustering settings in the JSS.

Limited Access Settings

If you have a clustered environment, the Limited Access settings in the Jamf Software Server (JSS) allow you to disable the JSS interface and limit the types of devices that can communicate with the JSS. This is most commonly used if you have a web application in the DMZ.

For each JSS web application, you can choose one of the following Limited Access settings:

- Full Access
- Computer Access Only
- Mobile Device Access Only
- Computer and Mobile Device Access

Choosing anything other than "Full Access" disables the JSS interface.

Configuring the Limited Access Settings

1. Log in to any of the JSS web applications with a web browser.

2. In the top-right corner of the page, click **Settings** .

3. Click **System Settings**.
   On a smartphone or iPod touch, this option is in the pop-up menu.

4. Click **Limited Access** .

5. Select a setting for each JSS web application as needed.

6. Click **Save**.

Backing Up the Database

You can create database backups as needed, or you can schedule database backups to be created automatically on a schedule. The time it takes to create a backup depends on the size of the database.

When you schedule database backups, you can also automate the deletion of scheduled backups that are older than a certain number of days.

Creating Database Backups Using the GUI

1. Open the JSS Database Utility by executing:

   ```
   sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar
   ```

2. If prompted, enter the password for your account and press the Return key.
3. If the JSS Database Utility is unable to locate the MySQL binary, you are prompted to enter the path. Click **Continue** and enter the full path to the binary.
4. If the Database Connection Setup pane appears, configure the settings to match your database configuration and click **Apply Settings**.
5. Click **Save Backup Now**.
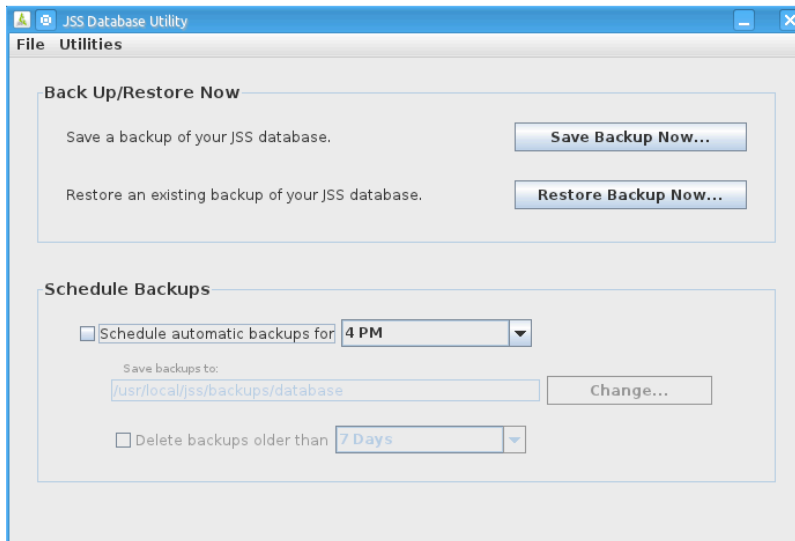
6. Select the location where you want to save the backup and click **Choose**.

   The JSS Database Utility creates the backup and saves it as a .sql.gz file.

Creating Database Backups Using the Command Line

1. Execute the following command:

   ```
   sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar backup -
   saveBackupTo <path>
   ```

   For example:

   ```
   sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar backup -
   saveBackupTo /home/username/backups/
   ```

2. If prompted, enter the password for your account and press the Return key.

3. If prompted, configure the database configuration settings to match your own by executing:

   ```
   sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar backup -
   saveBackupTo <path> -server <database server address> -port
   <database port> -database <database name> -user <database user> -
   pass
   ```

   For example:

   ```
   sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar backup -
   saveBackupTo /home/username/backups/ -server localhost -port 3306 -
   database jamfsoftware -user jss -pass
   ```

   The JSS Database Utility creates the backup and saves it as a .sql.gz file.

   To access command-line help for the backup verb, execute:

   ```
   sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar help backup
   ```
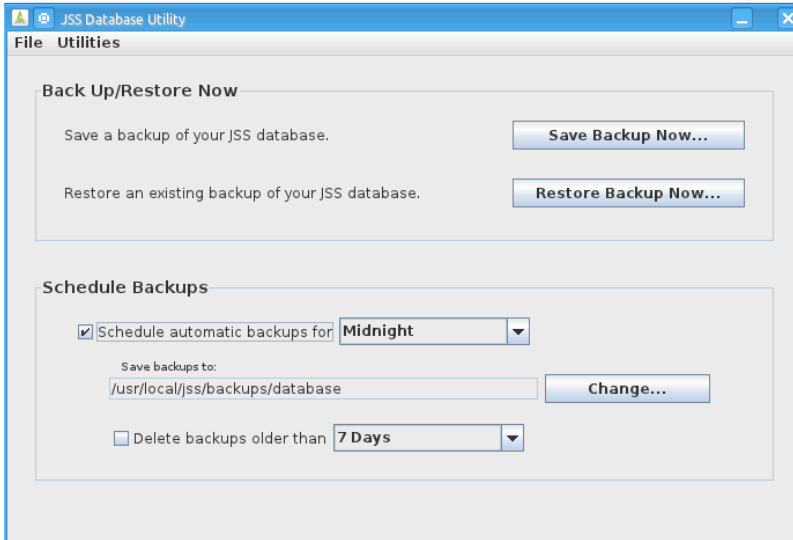
Scheduling Database Backups Using the GUI

1. Open the JSS Database Utility by executing:

   ```
   sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar
   ```

2. If prompted, enter the password for your account and press the Return key.

3. If the JSS Database Utility is unable to locate the MySQL binary, you are prompted to enter the path. Click **Continue** and enter the full path to the binary.

4. If the Database Connection Setup pane appears, configure the settings to match your database configuration and click **Apply Settings**.

5. Select the **Schedule automatic backups for** checkbox and choose the hour of the day that you want backups to occur.

6. To save the backups in a custom location, click the **Change** button and select a new location.

7. To automate the deletion of scheduled backups, select the **Delete backups older than** checkbox, and choose the number of days after which backups should be deleted.

   The JSS Database Utility creates daily backups at the hour you specified. It also deletes scheduled backups older than the number of days you specified.

Scheduling Database Backups Using the Command Line

1. Execute a command similar to the following:

```
sudo java –jar /usr/local/jss/bin/JSSDatabaseUtil.jar schedule –
hour <number between 0 and 23> –scheduledBackupPath <path> –
deleteBackupsOlderThanDays <number greater than 0>
```

   For example:

```
sudo java –jar /usr/local/jss/bin/JSSDatabaseUtil.jar schedule –
hour 3 –scheduledBackupPath /home/username/backups/ –
deleteBackupsOlderThanDays 7
```

2. If prompted, enter the password for your account and press the Return key.

3. If prompted, configure the database configuration settings to match your own by executing a command similar to the following:

```
sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar schedule -
hour <number between 0 and 23> -scheduledBackupPath <path> -
deleteBackupsOlderThanDays <number greater than 0> -server
<database server address> -port <database port> -database <database
name> -user <database user> -pass
```

For example:

```
sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar schedule -
hour 3 -scheduledBackupPath /home/username/backups/ -
deleteBackupsOlderThanDays 7 -server localhost -port 3306 -database
jamfsoftware -user jss -pass
```

The JSS Database Utility creates daily backups at the hour you specified. It also deletes scheduled backups older than the number of days you specified.

To access command-line help for the `schedule` verb, execute:

```
sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar help schedule
```
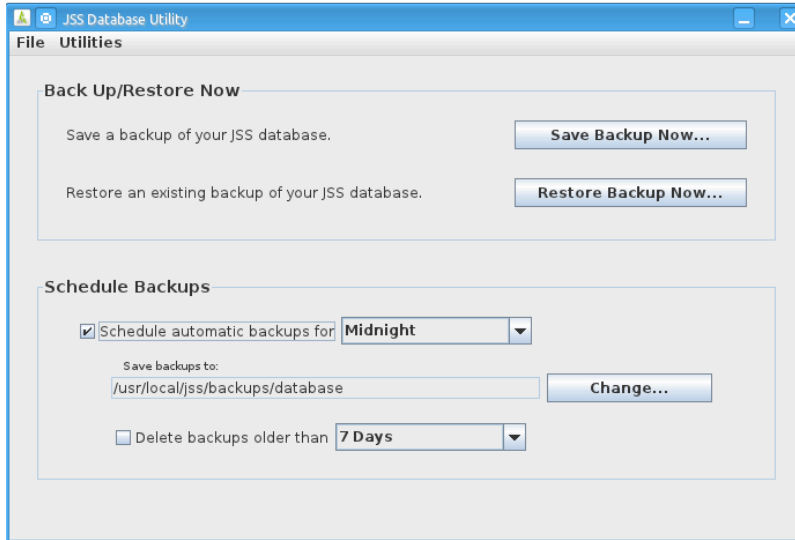
Stopping Scheduled Database Backups Using the GUI

1. Open the JSS Database Utility by executing:

```
sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar
```

2. If prompted, enter the password for your account and press the Return key.

3. If the JSS Database Utility is unable to locate the MySQL binary, you are prompted to enter the path. Click **Continue** and enter the full path to the binary.

4. If the Database Connection Setup pane appears, configure the settings to match your database configuration and click **Apply Settings**.

5. Deselect the **Schedule automatic backups for** checkbox.

The JSS Database Utility stops creating scheduled backups immediately.

Stopping Scheduled Database Backups Using the Command Line

Execute the following command:

```
sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar unschedule
```

The JSS Database Utility stops creating scheduled backups immediately.

To access command-line help for the unschedule verb, execute:

```
sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar help
unschedule
```

Related Information

For related information, see the following section in this guide:

Restoring Database Backups
Find out how to restore database backups.
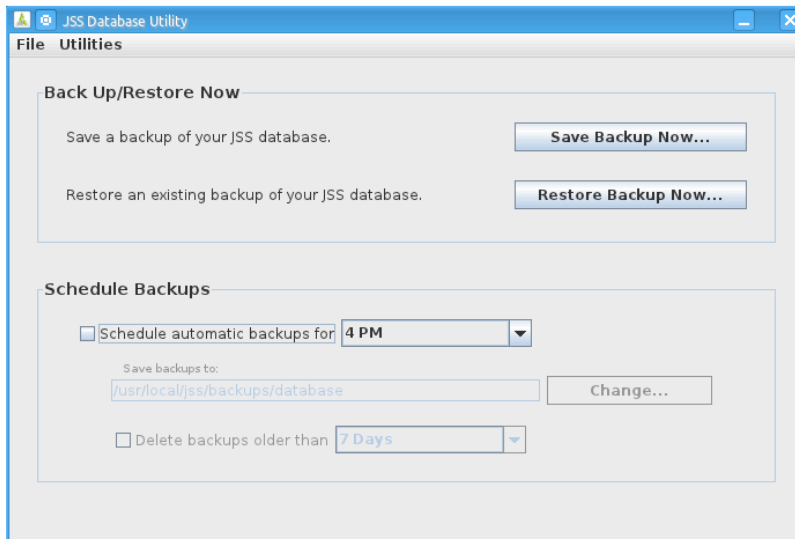
Restoring Database Backups

If you need to revert to an earlier version of your database, you can restore a database backup.

Restoring a Database Backup Using the GUI

1. Open the JSS Database Utility by executing:

```
sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar
```

2. If prompted, enter the password for your account and then press the Return key.

3. If the JSS Database Utility is unable to locate the MySQL binary, you are prompted to enter the path. Click **Continue** and enter the location of the binary.

4. If the Database Connection Setup pane appears, edit the settings to match your database configuration and click **Apply Settings**.

5. Click **Restore Backup Now**.

6. Select the backup that you want to restore (.sql or .sql.gz) and click **Choose**.

7. When prompted to restart Tomcat, click **Yes**.

The JSS Database Utility restarts Tomcat and replaces the current database with the one that you restored.

Restoring a Database Backup Using the Command Line

1. Execute a command similar to the following:

   ```
   sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar restore -file
   <filename>
   ```

   For example:

   ```
   sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar restore -file
   backup.sql.gz
   ```

2. If prompted, enter the password for your account and then press the Return key.

3. If prompted, edit the database configuration settings to match your own by executing a command similar to the following:

   ```
   sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar restore -file
   <filename> -server <database server address> -port <database port> -
   database <database name> -user <database user> -pass
   ```

   For example:

   ```
   sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar restore -file
   backup.sql.gz -server localhost -port 3306 -database jamfsoftware -
   user jss -pass
   ```

4. Restart Tomcat by executing:

   ```
   sudo /etc/init.d/jamf.tomcat7 restart
   ```

   The JSS Database Utility replaces the current database with the one that you restored.

   To access command-line help for the `restore` verb, execute:

   ```
   sudo java -jar /usr/local/jss/bin/JSSDatabaseUtil.jar help restore
   ```

Flushing Logs

Flushing logs reduces the size of the database and can speed up searches. You can flush the following types of logs:

- Application Usage logs
- Computer Usage logs
- Policy logs
- Casper Remote logs
- Screen sharing logs
- Casper Imaging logs
- Computer and mobile device management history
- JDS management history
- Computer inventory reports (computer inventory information from past inventory submissions)
- Mobile device inventory reports (mobile device inventory information from past inventory submissions)
- JSS access logs
- Change Management logs
- Event logs

You can schedule log flushing to take place daily, or you can manually flush logs as needed. You can also choose to flush logs that are older than a certain number of days, weeks, or months.

For information on the types of data flushed with each log and the database tables affected, see the following Knowledge Base article:

[Data and Tables Affected by Log Flushing](#)

Scheduling Log Flushing

1. Log in to the JSS with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **System Settings**.

4. Click **Log Flushing** 📅 .

5. Click **Edit**.

6. Use the pop-up menus to choose the number of days, weeks, or months after which each type of log should be flushed.

7. Choose a time of day from the **Time to Flush Logs Each Day** pop-up menu.

8. Click **Save**.

Manually Flushing Logs

1. Log in to any of the JSS web applications with a web browser.

2. In the top-right corner of the page, click **Settings** ⚙ .

3. Click **System Settings**.

4. Click **Log Flushing** 📅 .

5. Click **Flush Manually**.

6. Select the checkbox for each type of log you want to flush.

7. From the **Flush Logs Older Than** pop-up menu, choose the choose the number of days, weeks, or months after which logs should be flushed.

8. Click **Flush**.

A message displays, reporting the success or failure of the flush.

Related Information

For related information, see the following sections in the *Casper Suite Administrator's Guide*:

- "Viewing and Flushing Policy Logs for a Computer"
  Find out how to view and flush policy logs for a computer.

- "Viewing and Flushing Logs for a Policy"
  Find out how to view and flush logs for a policy.

- "Viewing the History for a Computer"
  Find out how to view the logs and the management history for a computer.

- "Viewing the Management History for a Mobile Device"
  Find out how to view the management history for a mobile device.

Migrating to Another Server

1. Back up the existing jamfsoftware database using the JSS Database Utility.
   For more information, see Backing Up the Database.

2. Ensure that the new server meets the requirements for the JSS Installer, and then follow the instructions in Installing the JSS to install the required software (if needed) and create the jamfsoftware database.

3. Copy the JSS Installer to the new server.

4. Install the JSS by launching the installer and following the onscreen instructions.
   For more information, see Installing the JSS.

5. Copy the database backup to the new server, and then use the JSS Database Utility to restore the backup.
   For more information, see Restoring Database Backups.

6. Re-upload or create the SSL certificate.
   For more information, see SSL Certificate.

7. Update the DNS entry to point to the new server's IP address.
   Note: If you can't change the DNS entry, you must change the JSS URL and re-enroll all mobile devices and computers.