Contents

5 Overview of Technologies
5 Applications and Utilities
8 Security
10 Ports
11 Requirements
13 Installing and Managing the JSS
13 Required Components
14 Installing the JSS on Mac OS X Server
17 Allocating Additional Memory to Tomcat
19 Setting Up the JSS
21 Upgrading the JSS
22 Changing the Activation Code
23 Backing Up the Database
26 Restoring Database Backups
27 Deleting Logs from the Database
29 Migrating to Another Server
30 Managing Distribution Points
34 Enabling Email Notifications
36 Enabling Change Management
38 Generating a Web Server Certificate
39 Enabling Clustering
41 Configuring Tomcat to Work with a Load Balancer
42 Changing the Limited Access Setting
44 Frequently Asked Questions
46 Troubleshooting the JSS
49 Building Your Framework
49 Integrating with LDAP Servers
57 Managing JSS User Accounts
62 Managing Network Segments
64 Managing Packages
81 Managing Scripts
88 Managing Printers
93 Creating Directory Bindings
98 Managing Removable MAC Addresses
100 Imaging
100 Overview of the Imaging Process
Managing Configurations
Imaging Drives
Customizing the Imaging Process
Managing Autorun Preferences
Using the Autorun Feature
PreStage Imaging
Target Mode Imaging
Overview of Technologies

Applications and Utilities

This section describes the applications and utilities that make up the Imaging Suite.

JSS Installers

JSS Installers provide a quick, easy way to install and upgrade the JAMF Software Server (JSS). JSS Installers are available for the following platforms:

- Mac
- Linux
- Windows

JSS Installer for Mac

The JSS Installer for Mac is an installation package that allows you to install and upgrade the JSS on Mac OS X Server. It also allows you to create your initial distribution point during a fresh installation.

Note: The JSS Installer for Mac included in the product DMG (JSS Installer.mpkg) is unsigned. To obtain a signed version of the JSS Installer for Mac (JSS Installer.pkg), contact JAMF Software Support. The signed version allows you to install or upgrade the JSS when Apple's Gatekeeper feature is set to only allow applications downloaded from the Mac App Store and identified developers.

JSS Installers for Linux and Windows

The JSS Installers for Linux and Windows allow you to install and upgrade the JSS on supported Linux and Windows operating systems.

To obtain these installers and their documentation, see the introductory email that you received from JAMF Software or contact your JAMF Software Representative.
Mac OS X Applications

Casper Admin

The Casper Admin application is a repository for packages, scripts, and printers. Casper Admin allows you to create and maintain configurations (similar to images) using these items and manually replicate distribution points.

The JSS also has an implementation of Casper Admin that is almost identical to the application with a few exceptions. The JSS implementation of Casper Admin does not allow you to perform the following actions:

- Copy packages to distribution points.
- Delete files from distribution points.
- Replicate distribution points or FireWire drives.
- Add new printers.
- Identify Adobe Installers and Adobe Updaters.

Casper Imaging

The Casper Imaging application is used to image local drives. It provides two options for automating the imaging process: Autorun and PreStage imaging.

Casper Imaging can also be used to run scripts, map printers, create local user accounts, bind to Active Directory, and automate other common postfix tasks.

JAMF Software Server

The JSS is a web application that serves as the administrative core of the Imaging Suite. All other JAMF Software administrative applications communicate with the JSS.

Utilities

JAMF Helper

The JAMF Helper displays messages to end users. It is stored in the following location on client computers:

/Library/Application Support/JAMF/bin/

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.
Most tasks in the Imaging Suite are executed using the “jamf” command-line application (also known as the jamf binary). Although you are free to use this application at will, the Imaging Suite automatically installs, updates, and runs it.
Security

This section explains the primary security measures in the Imaging Suite:
- Passwords
- Communication protocols
- Signed applications

Passwords

The Imaging Suite allows you to store individual accounts for client computers and reset the passwords if necessary.

Passwords stored in the database are encrypted using a standard 128-bit RSA encryption with a 1024-bit key.

Communication Protocols

The Imaging Suite has security built into its design. Connections between the JAMF Software Server (JSS) and the other applications in the Imaging Suite take place over Secure Sockets Layer (SSL).

Secure Shell (SSH)

SSH is a network security protocol built into Mac OS X. For more information, go to:

http://openssh.org/

Secure Sockets Layer (SSL)

SSL is a security protocol for Internet communication. For more information, go to:

https://www.openssl.org/

Signed Applications

The following applications are signed by JAMF Software:
- Casper Admin
- Casper Imaging
- JAMF Helper
- JSS Installer for Windows (JSS Installer.msi)
- /usr/sbin/jamf (jamf binary)

A signed version of the JSS Installer for Mac (JSS Installer.pkg) is also available. You can obtain it by contacting JAMF Software Support.
## Ports

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>The standard port for SSH (known as remote login in Mac OS X).</td>
</tr>
<tr>
<td>548</td>
<td>The standard port for Apple File Protocol (AFP). If you use an AFP share to deploy packages or scripts, clients mount the AFP share on this port.</td>
</tr>
<tr>
<td>3306</td>
<td>The default port for MySQL.</td>
</tr>
<tr>
<td>8443</td>
<td>The SSL port for the JSS. Default port used by applications and computers to connect to the JSS.</td>
</tr>
</tbody>
</table>

The following table describes other commonly used ports:

<table>
<thead>
<tr>
<th>Port</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>The standard port for SMTP. The JSS connects to an SMTP server to send email notifications to administrators.</td>
</tr>
<tr>
<td>139</td>
<td>If you use an SMB share to deploy packages or scripts, clients mount the SMB share on this port.</td>
</tr>
<tr>
<td>389</td>
<td>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.</td>
</tr>
<tr>
<td>445</td>
<td>If you have an SMB client, such as “DAVE”, installed on your client computers, they may mount the SMB share on this port.</td>
</tr>
<tr>
<td>514</td>
<td>The default port for Syslog servers.</td>
</tr>
<tr>
<td>8080</td>
<td>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.</td>
</tr>
<tr>
<td>9006</td>
<td>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.</td>
</tr>
</tbody>
</table>

On the Mac platform, the JSS runs on ports 8443 and 9006 by default. On Linux and Windows platforms, 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 Imaging Suite application.

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

This section lists the requirements for the following components and functions of the Imaging Suite:
- JAMF Software Server
- JSS Installers
- JSS Database Utility
- Imaging

JAMF Software Server

You can host the JAMF Software Server (JSS) on any server that meets the following minimum requirements:
- Java 1.6
- MySQL 5.1 or later
- Apache Tomcat 6.0 or later

Tested operating systems include:
- OS X Server v10.6
- OS X Server v10.7
- OS X Server v10.8
- Ubuntu 10.04 LTS Server
- Ubuntu 12.04 LTS Server
- Red Hat Enterprise Linux (RHEL) 6
- Windows Server 2008 R2

Although you can install the JSS on any server that meets the minimum requirements, the JSS Installers for Mac, Linux, and Windows have additional requirements. (See the “JSS Installers” section for detailed information.)

JSS Installers

JSS Installer for Mac

The JSS Installer for Mac requires a Mac computer with:
- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- OS X Server v10.6 or later
- Java 1.6
• MySQL Enterprise Edition 5.5 or later (recommended) or MySQL Community Server 5.5 or later, available at:
  https://www.mysql.com/downloads/
• Ports 8443 and 9006 available

**JSS Installers for Linux and Windows**

Requirements for the JSS Installers for Linux and Windows are available in the JAMF Software Server installation guides for Linux and Windows. To obtain the JSS Installer for Linux or Windows along with its installation guide, contact your JAMF Software Representative, or visit the following website and log in with a valid JAMF Nation account:

https://jamfnation.jamfsoftware.com/myAssets.html

**JSS Database Utility**

The JSS Database Utility requires a server with MySQL Server 5.1 or later.

**Imaging**

Casper Imaging can image computers with OS X v10.5.x, OS X v10.6.x, OS X v10.7.x, or OS X v10.8.x that do not have PowerPC processors.
Installing and Managing the JSS

Required Components

This section describes the components that run the JSS.

Java

Java 1.6 is required to start the Tomcat web application server that runs the JSS.

MySQL

The JSS stores information in a MySQL database. For more information about MySQL, go to:

https://www.mysql.com/

Apache Tomcat

The JSS runs on Tomcat, a web application server similar to Microsoft's Internet Information Server (IIS). For more information about Tomcat, go to:

https://tomcat.apache.org/
Installing the JSS on Mac OS X Server

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.

This section includes details for each step.

Before you begin, review the “Requirements” section and make sure that your server meets the JSS Installer requirements.

**Note:** The instructions in this guide are for the Mac platform only. To obtain the JSS Installer for Windows or Linux along with its installation guide, contact your JAMF Software Representative, or visit the following website and log in with a valid JAMF Nation account:

https://jamfnation.jamfsoftware.com/myAssets.html

For instructions on how to manually install the JSS on Linux and Windows, download the "Manually Installing the JAMF Software Server" technical paper from:

http://jamfsoftware.com/libraries/pdf/white_papers/Manually_Installing_the_JAMF_Software_Server.pdf

**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:

https://jamfnation.jamfsoftware.com/article.html?id=28

**Step 2: Create the jamfsoftware Database**

Create a MySQL database in which the JSS can store its data, and a MySQL user can access it. Name the database “jamfsoftware” and give the MySQL user the following credentials:

- Username: jamfsoftware
- Password: jamfsw03

**Note:** If you customize the database name, username, or password, you will be prompted to enter the custom settings when you run the JSS Installer.
To create the jamfsoftware database:

1. Open Terminal and access the MySQL command line as "root" by typing:

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

   If MySQL is not in the path or it is installed in a custom location, access the MySQL command line by updating the path or by typing:

   ```
   /path/to/mysql -u root -p
   ```

   **Note:** On OS X v10.7 or later, the default path for MySQL is `/usr/local/mysql/bin/`.

2. When prompted, enter the password for the MySQL “root” user.
   If you did not create a root password, press the Return key.

3. Create a database named "jamfsoftware" by executing:

   ```
   CREATE DATABASE jamfsoftware;
   ```

4. Grant permissions to a MySQL user named "jamfsoftware" so that it can access the new database:

   ```
   GRANT ALL ON jamfsoftware.* TO 'jamfsoftware'@localhost IDENTIFIED BY 'jamfsw03';
   ```

   **Note:** If you choose to enter a username other than "jamfsoftware", it is recommended that you do not use "root".

Step 3: Run the JSS Installer

Run the JSS Installer to install Apache Tomcat and the JSS web application, and create your initial distribution point.

To run the JSS Installer:

1. Copy the JSS Installer for Mac to the server.

   **Note:** The JSS Installer for Mac included in the product DMG (JSS Installer.mpkg) is unsigned. To obtain a signed version of the JSS Installer for Mac (JSS Installer.pkg), contact JAMF Software Support. The signed version allows you to install or upgrade the JSS when Apple's Gatekeeper feature is set to only allow applications downloaded from the Mac App Store and identified developers.

2. Double-click the installer and click **Continue** to proceed.

3. When the Introduction pane appears, click **Continue**.

4. Read the information on the Read Me pane, and then click **Continue**.
5. Select a drive on which to install the software, and then click **Continue**.

6. Modify the information on the Database pane to reflect any custom settings if needed, and then click **Continue**.

7. Click **Install**.

8. Enter your administrator password when prompted, and then click **OK** or **Install Software**.

9. When the installation is complete, follow the instructions on the Summary pane to access the JSS. Then, click **Close**.
Allocating Additional Memory to Tomcat

This section explains how to:
- View the amount of memory being used by the web application
- Allocate additional memory to Tomcat

To view web application memory usage:
1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the Database/Web Application Health link.
4. Click the Web App Memory link.

To allocate additional memory to Tomcat using the JSS Database Utility:
1. Open the JSS Database Utility on the server running the JSS.
   The JSS Database Utility is located in:
   /Library/JSS/bin/JSSDatabaseUtil.jar
2. Enter the username and password for an administrator account to the server, and then click OK.
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. From the menu bar, choose Utilities > Change Tomcat settings.
5. Modify the minimum and maximum memory and PermGen sizes as needed.

![Tomcat Settings](image)
6. Click **Apply Settings**.

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

![Question dialog box]

*Would you like the JSS Database Utility to restart Tomcat?*

- [No]
- [Yes]
Setting Up the JSS

The first time you connect to the JAMF Software Server (JSS), the JSS Setup Assistant guides you through creating your first account and configuring the basic computer management framework.

To set up the JSS:

1. Connect to the JSS with a web browser.
2. Read the License Agreement and click Agree.
3. Enter the name of your organization and the activation code you received from your JAMF Software Representative, and then click Continue.
   If you did not receive an activation code, send an email to sales@jamfsoftware.com.
4. Enter a username and password for your first administrator account in the JSS.
5. Enter the password again to verify it, and then click the Continue button.
6. Verify that the settings are configured correctly and click the **Save** button. If you need to make changes, click the **Back** button or make changes in the JSS after you’re finished using the JSS Setup Assistant.

7. Click the **Go to the JSS** button to start using the JSS immediately, or use the links to configure additional settings in a separate browser window.
Upgrading the JSS

This section explains how to upgrade the JAMF Software Server (JSS) on Mac OS X Server.

To upgrade the JSS:

1. Back up the current database using the JSS Database Utility. (See “Backing Up the Database” for complete instructions.)
2. Back up custom reports.
   - If you used the JSS Installer to install the JSS on Mac OS X Server, custom reports are located in `/Library/JSS/Tomcat/webapps/ROOT/WEB-INF/reporting/`.
   - If you did not use the JSS Installer to install the JSS on Mac OS X Server, custom reports are located in `/Library/Tomcat/webapps/ROOT/WEB-INF/reporting/`.
3. Copy the most current version of the JSS Installer for Mac to the server.

   **Note:** The JSS Installer for Mac included in the product DMG (`JSS Installer.mpkg`) is unsigned. To obtain a signed version of the JSS Installer for Mac (`JSS Installer.pkg`), contact JAMF Software Support. The signed version allows you to install or upgrade the JSS when Apple’s Gatekeeper feature is set to only allow applications downloaded from the Mac App Store and identified developers.

4. Double-click the installer and click **Continue**.
5. When the Introduction pane appears, click **Continue**.
6. Read the information on the Read Me pane, and then click **Continue**.
7. Select a drive on which to install the software, and then click **Continue**.
8. If the Database pane appears, enter information about your MySQL database. Then, click **Continue**.
   - The JSS Installer uses this information to connect to the existing database.

   **Note:** This pane is only displayed if the `database.xml` file is in a custom location or contains invalid information.

9. Click **Install**.
10. Enter your administrator password when prompted, and then click **OK**.
11. When the upgrade is complete, follow the instructions on the Summary pane to access the JSS. Then, click **Close**.
Changing the Activation Code

Every time you receive a new activation code, it must be updated in the JAMF Software Server (JSS).

When you update the activation code, you can also update your company name and view the following licensing information:

- **Product**—Product you are licensed for
- **Licenses**—Current number of licenses
- **License Renewal Date**—Date the maintenance contract expires
- **License Type**—Commercial, education, trial, etc.

To change the activation code:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **General Settings** link.
4. Enter the new activation code in the **Activation Code** field and click **Save**.
Backing Up the Database

The JSS Database Utility allows you to create backups of the jamfsoftware database, schedule database backups, and stop scheduled database backups.

Creating Database Backups

Use the JSS Database Utility to create a backup of the jamfsoftware database. The time it takes to create the backup depends on the size of the database.

To create a database backup:

1. Open the JSS Database Utility, located in:
   /Library/JSS/bin/JSSDatabaseUtil.jar
2. Enter the username and password for an administrator account to the server, and then click OK.
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 Save Backup Now.
6. Select the location where you want to save the backup, and then click Choose.

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

Use the JSS Database Utility to schedule daily backups of the jamfsoftware database. You can also automate the deletion of scheduled backups that are older than a certain number of days.

To schedule database backups:

1. Open the JSS Database Utility, located in:
   /Library/JSS/bin/JSSDatabaseUtil.jar
2. Enter the username and password for an administrator account to the server, and then click OK.
3. If the JSS Database Utility is unable to locate the MySQL binary, you are prompted to specify the path. Click Continue and specify 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. Select the Schedule automatic backups for checkbox and choose the hour of the day that you want backups to occur.
6. To change the location where backups are saved, click the Change button and select a new location.
7. To automate the deletion of scheduled backups, select the Delete backups older than checkbox. Then, choose the number of days after which backups should be deleted.

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

Stopping Scheduled Database Backups

Use the JSS Database Utility to stop scheduled backups of the jamfsoftware database.
To stop scheduled database backups:

1. Open the JSS Database Utility, located in:
   /Library/JSS/bin/JSSDatabaseUtil.jar

2. Enter the username and password for an administrator account to the server, and then click OK.

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. Deselect the Schedule automatic backups for checkbox.

The JSS Database Utility stops scheduled backups immediately.
Restoring Database Backups

If you need to revert to an earlier version of your database, you can use the JSS Database Utility to restore a database backup.

To restore a database backup:

1. Open the JSS Database Utility, located in:
   /Library/JSS/bin/JSSDatabaseUtil.jar
2. Enter the username and password for an administrator account to the server, and then click OK.
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.

   ![JSS Database Utility](image)

6. Select the backup that you want to restore (.sql or .sql.gz), and then click Choose.
7. When prompted to restart Tomcat, click Yes.

   ![JSS Database Utility](image)

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

Over time, the JAMF Software Server (JSS) accumulates a large number of logs. Deleting these logs can reduce the size of the database and can speed up searches.

You can schedule log deletion to take place automatically or manually delete logs as needed.

To schedule automatic log deletion:
1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Flush Database Logs** link.
4. Use the pop-up menus to specify the period of time after which logs will be deleted. For example, to delete Policy logs that are six months old or older, choose “Six Months” from the pop-up menu next to **Policy Logs**. To stop deleting a type of log, choose “Do not delete” from the pop-up menu next to it.
5. Use the **Time of Day** pop-up menu to schedule a time for the deletion. For example, to delete logs every morning at 2 a.m., choose “2 AM” from the pop-up menu.
6. Click **Save**.
7. Click **Continue** to confirm the schedule.

To delete logs manually:
1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Flush Database Logs** link.
4. Click the **Flush Manually** button.

5. Select the types of logs you want to delete.

6. Use the **Older than** pop-up menu to specify the period of time after which logs will be deleted. For example, to delete logs that are six months old or older, choose “Six Months” from the pop-up menu.

7. Click **Delete**.

8. Click **Continue** to confirm the results.
Migrating to Another Server

The instructions in this section explain how to migrate the JAMF Software Server (JSS) to another server.

To migrate the JSS:

1. Back up the existing jamfsoftware database using the JSS Database Utility. (See “Backing Up the Database” for detailed instructions.)

2. Ensure that the new server meets the requirements for the JSS Installer. 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. (See “Installing the JSS” for detailed instructions.)

5. Copy the database backup to the new server, and then use the JSS Database Utility to restore the backup. (See “Restoring a Database Backup” for detailed instructions.)

6. Regenerate the web server certificate. (See “Generating a Web Server Certificate” for detailed instructions.)

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.
Managing Distribution Points

A key feature of the Imaging Suite is the ability to deploy packages from multiple distribution points. This allows you to deploy packages to computers in other locations using servers that are geographically close to each destination. It reduces the need for bandwidth between locations and allows you to deploy packages across a widespread network.

Distribution points can share files over Apple Filing Protocol (AFP) or Server Message Block (SMB).

This section explains how to:
- Add distribution points
- Replicate distribution points
- Replicate FireWire or USB drives

Adding Distribution Points

Servers running any platform can function as distribution points.

Adding a distribution point involves the following steps:

1. Set up the distribution point.
2. Add a record of the distribution point to the JAMF Software Server (JSS).

Step 1: Set Up a New Distribution Point

3. Create a share point (AFP or SMB) on the server you want to utilize as the distribution point.
4. Create an account that has read-only access to the share.
5. Create an account that has read/write access to the share.
6. Make sure “Everyone” has read-only access to the share.
7. (Optional) Enable HTTP or HTTPS on the share point.

Step 2: Add a Record of the Distribution Point to the JSS

1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the Servers link.
4. Click the Add Server button in the toolbar.
5. Select the Distribution Point option and click Continue.
6. Enter a display name for the server.
7. Enter the DNS name or IP address for the server.
8. To use this server as the default distribution point, select the **Use this server as the Master** option.

9. To assign a backup distribution point, choose a server from the **Failover Distribution Point** pop-up menu.

10. Click the **File Sharing** tab and enter information about the AFP or SMB share point. Casper Imaging uses the read-only account to mount the share. Casper Admin uses the read/write account.

11. (Optional) Configure the distribution point to use HTTP downloads. This requires that HTTP or HTTPS access is enabled on the server for the distribution point.
   a. Click the **HTTP** tab.
b. Select the **HTTP Downloads are enabled for this Distribution Point** checkbox.

c. Choose “HTTP” or “HTTPS” from the **Protocol** pop-up menu.

d. Enter the port in the **Port** field.

e. In the **Context** field, enter the path to the share point (following the DNS name or port) that exists in the URL. For example, you would type “CasperShare” if the share is accessible at: 

   http://192.168.10.10/CasperShare/

f. If the share requires a username and password to access files, select the **Username & Password Authentication is Required** option.

  g. Enter the username and password, and then enter the password again to verify it.

h. If the share requires a certificate, select **Certificate Authentication is Required** and click the **Choose File** link to upload the certificate.

  The certificate that you upload must be trusted.

12. Click the **Save** button.

---

### Replicating Distribution Points

You can replicate distribution points that are running on any platform.

To ensure distribution points have the same deployable items, synchronize them manually using the Casper Admin application.

**To replicate distribution points:**

1. Open Casper Admin.

2. Select the distribution point(s) you want to replicate and click the **Replicate** button.

---

### Replicating FireWire or USB Drives

To make packages, scripts, printers, and configurations available for Casper Imaging offline, replicate to an external drive and place a copy of Casper Imaging at the root of the drive.

Replicating a FireWire or USB drive involves the following steps:

1. Replicate to an external drive.

2. Use the replicated drive offline.

**Step 1: Replicate to an External Drive**

1. Open Casper Admin.

2. Drag the hard drive icon from the Finder to the sidebar in Casper Admin.

3. If the external drive is already under the Local Drives heading in the sidebar, it is already replicated and is mounted automatically when you open Casper Admin.
4. Select the drive in the sidebar and click the Replicate button.

**Step 2: Use the Replicated Drive Offline**

1. Make a copy of the Casper Imaging application.
2. Put the copy at the root of the replicated drive at the same level as the Packages, Scripts, and Casper Data folders.
3. Open Casper Imaging.
Enabling Email Notifications

In order for the JAMF Software Server (JSS) to send email notifications, you must specify the SMTP server from which the notifications will be sent.

Email notifications can be sent when the following events occur:
- A computer is acquired using a PreStage.
- An error occurs during the imaging or Autorun process.
- There is a JSS service restart.
- A database is backed up successfully.
- A database backup fails.

This section explains how to set up and modify an SMTP server.

To set up or modify an SMTP Server:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **General Settings** link.
4. Click the **SMTP Server** tab.
5. Enter the DNS name or IP address for the SMTP server in the **SMTP Host Address** field.
6. Use the **Encryption Method** pop-up menu to specify the protocol used for data encryption.
7. In the **Port** field, enter the port over which the connection is made. The default port is 25.
8. Enter the number of seconds you want to wait before the connection times out. By default, this is 5 seconds.

9. Enter the email address from which notifications will be sent.

10. If the SMTP server requires authentication, select the Requires Authentication checkbox and enter credentials for a valid account to the server.

11. If you want to send a test message, click the Send Test message to <email address> link. The JSS sends this message to the email address for the account currently logged in to the JSS.

12. Click Save.
Enabling Change Management

Change management logs allow you to track the following information:
- Changes made to the client computers on your network
- Computers from which the changes were made
- Accounts that initiated the changes

You can choose to write these logs to a local log on the server running the JAMF Software Server (JSS) or a Syslog server.

The header for each logged event includes the following information:
- Timestamp (when the event took place)
- Username of the account that initiated the change
- IP address of the client computer that triggered the event
- JSS identifier (com.jamfsoftware.jss)

This section explains how to set up and modify change management to a log file and a Syslog server.

To set up or modify change management to a log file:
1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the General Settings link.
4. Click the Change Management tab.
5. Select the Enable Change Management checkbox if it is not already selected, and enter a directory location for the log file.
6. Click Save.

Change Management logs are written to the file specified in the Log Directory field. They have the filename jamfChangeManagement.log and can be viewed using the Console application.

To set up or modify change management to a Syslog server:
1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the General Settings link.
4. Click the Change Management tab.
5. Select the Enable Change Management checkbox.
6. In the Hostname field, enter the DNS name or IP address for the Syslog server.
7. Enter the UDP port that the Syslog server is using.
   The port is entered as 514 by default.

8. Click Save.
Generating a Web Server Certificate

The JAMF Software Server (JSS) requires a valid web server certificate to ensure that computers communicate with the JSS and not an imposter server.

If you already have a web server certificate from an internal certificate authority (CA) or a trusted third-party vendor, follow the vendor's instructions for using the certificate with Tomcat.

If you do not have a valid web server certificate, you can generate one from the CA that is built into the JSS. To do this, 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.

To generate a web server certificate from the built-in CA:

1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the General Settings link.
4. Click the Server Configuration tab.
5. Click the Replace with certificate from the JSS’s built-in CA link.
6. Click Save.
7. Restart Tomcat to begin utilizing the certificate.
   For instructions on how to restart Tomcat, see the Knowledge Base article at: https://jamfnation.jamfsoftware.com/article.html?id=117
Enabling Clustering

Clustering allows you to point multiple instances of the JAMF Software Server (JSS) web application to the same database. This requires 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.

The web application that functions as the master handles the following tasks:
- Upgrading the database schema
- Flushing database logs

For more information on setting up a clustered environment, contact your JAMF Software Representative.

To enable clustering:
1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the Generals Settings link.
4. Click the Server Configuration tab.
5. Click the Clustering tab.
6. Select the Enable Clustering checkbox.

7. To add web applications to the cluster, click the Add To Cluster links.
8. To make a web application the master, click the Master link.
9. Click Save.
10. Restart Tomcat for the changes to take effect.
For instructions on how to restart Tomcat, see the Knowledge Base article at:
https://jamfnation.jamfsoftware.com/article.html?id=117
Configuring Tomcat to Work with a Load Balancer

When working with a load balancer, you may need to enable a few attributes in Tomcat’s server.xml file to ensure that Tomcat and the load balancer communicate properly.

The JAMF Software Server (JSS) allows you to enable the following attributes without requiring you to access the server.xml file manually:

- Remote IP valve
- Proxy port
- Proxy scheme

To enable these attributes, 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.

To configure Tomcat to work with a load balancer:

1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the General Settings link.
4. Click the Server Configuration tab.
5. Click the Tomcat Configuration tab.
6. Click the Configure link across from an attribute to enable it.
7. Click Save.
8. Restart Tomcat for the changes to take effect.

For instructions on how to restart Tomcat, see the Knowledge Base article at:
https://jamfnation.jamfsoftware.com/article.html?id=117
Changing the Limited Access Setting

When working in a clustered environment, you may have a JAMF Software Server (JSS) that computers can access from outside of the network. If you have a second JSS web application that resides in your DMZ, you can make the administrative interface unavailable by changing the Limited Access setting.

The Limited Access setting has four options:

- **Full JSS**—This is the default option for every JSS. It makes the JSS interface available from anywhere.
- **Computer and Mobile Device Management**—This option is not applicable to the Imaging Suite.
- **Computer Management Only**—This option disables the JSS interface.
- **Mobile Device Management Only**—This option is not applicable to the Imaging Suite.

**Warning:** Do not change the Limited Access setting while connecting through a load balancer. Connect directly to the instance of Tomcat that is inside of your DMZ.

After you change the Limited Access setting, the JSS interface is inaccessible. To make additional changes, you need to manually modify the `web.xml` file. If you need to revert the JSS to the default setting (Full JSS), delete the `web.xml` file in `/Library/JSS/Tomcat/webapps/ROOT/WEB-INF/` and rename the `web.xml.original` file to `web.xml`.

**Note:** If you upgraded from v8.1 or earlier, the `web.xml` and `web.xml.original` files are located in `/Library/Tomcat/webapps/ROOT/WEB-INF/`.

Upgrading the JSS automatically resets the Limited Access setting to Full JSS. You will need to change this setting every time you upgrade.

**To change the Limited Access setting:**

1. Use a web browser to log in to the desired instance of the JSS.
2. Click the **Settings** tab.
3. Click the **General Settings** link.
4. Click the **Server Configuration** tab.
5. Click the **Limited Access JSS** tab.
6. Select a limited access option.

7. Click **Save**.

8. Restart the JSS for any changes to take effect.
Frequently Asked Questions

Q. What is installed on Mac OS X Server when I install the JSS?

A. The following files and folders are installed on Mac OS X Server:

Apache Tomcat
Tomcat is the web application server that runs the JSS web application. A directory named Tomcat is installed in:
/Library/JSS/Tomcat/

CasperShare
The distribution point created by default for a fresh installation. The JSS Installer creates a directory named CasperShare in:
/Shared Items/CasperShare/

com.jamfsoftware.tomcat.plist
This is the launchd item that controls Tomcat. It is installed and loaded in the following location:
/Library/LaunchDaemons/com.jamfsoftware.tomcat.plist

Database backup location
The JSS Database Utility stores database backups in the following location by default:
/Library/JSS/Backups/Database/

JSS Database Utility
The JSS Database Utility is installed in the following location:
/Library/JSS/bin/JSSDatabaseUtil.jar

JSS web application
The JSS is a web application that runs on Tomcat. A directory named ROOT is installed in:
/Library/JSS/Tomcat/webapps/ROOT/

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:
/Library/JSS/Tomcat/.keystore

Logs
Logs for the installation and for the JSS are stored in the following directory:
/Library/JSS/Logs/
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:
/Library/JSS/Tomcat/conf/server.xml

**Note:** The locations of these files and folders are different if you upgraded from v8.1 or earlier and your JSS is installed on OS X Server v10.6. Apache Tomcat and its related files are stored in /Library/Tomcat/ and the JSS web application (previously known as the jamf web application) is stored in /Library/Tomcat/webapps/ROOT/.

**Q. Can I install the JSS on other platforms?**

A. Yes. You can install the JSS on any platform that supports the following software:
- Java 1.6
- MySQL 5.1 or later
- Apache Tomcat 6.0 or later

Tested operating systems include:
- OS X Server v10.8
- OS X Server v10.7
- OS X Server v10.6
- Ubuntu 10.04 LTS Server
- Red Hat Enterprise Linux (RHEL) 6
- Windows Server 2008

Although you can install the JSS on any server that meets the minimum requirements, JSS Installers are only available for Mac, Linux, and Windows.

To obtain the JSS Installers for Linux and Windows and their documentation, see the introductory email that you received from JAMF Software or contact your JAMF Software Representative.
Troubleshooting the JSS

Most issues with the JSS have to do with the configuration of Apache Tomcat or MySQL. The JSS Database Utility allows you to troubleshoot most of the issues that you encounter.

This section explains how to troubleshoot the following issues:

- Connection issues
- Memory issues
- Database issues

Connection Issues

If applications are not connecting to the JAMF Software Server (JSS), you can use a web browser to troubleshoot the issue. If you are able to connect to the JSS, the applications should be able to connect as well.

To troubleshoot connection issues:

1. Open a web browser and try connecting to the JSS on port 8443.
   For example, if the DNS name of the JSS is "jss.mycompany.com", try connecting to:
   https://jss.mycompany.com:8443/

2. If you are prompted to verify a certificate, accept the certificate.

3. If you are able to connect to the JSS, make sure that the application is pointing at the correct IP address.
   a. Quit the application.
   b. Hold down the Option key and re-open the application to bring up the Preferences pane.
   c. On the Preferences pane, enter the DNS name or IP address for the JSS and then click Save.
   d. Enter the username and password for an administrator account to the server, and then click OK.

4. If the application still fails to connect, restart Tomcat.
   For instructions on how to restart Tomcat, see the Knowledge Base article at:
   https://jamfnation.jamfsoftware.com/article.html?id=117
Memory Issues

If there is a large amount of data in the JSS, you may need to allocate additional memory to Tomcat. Tomcat displays the following error page if more memory is required:

![HTTP Status 500 - Exception report](image)

For instructions on viewing the amount of memory being used by the web application and allocating additional memory to Tomcat, see “Allocating Additional Memory to Tomcat”.

Database Issues

MySQL database tables can become corrupt if the JSS is running on a very slow computer to which many clients are connected, or if the server running the JSS crashed and the database was not shut down properly.

When errors occur in the MySQL database, the JSS displays an alert similar to the following:

Got error 127 from table handler

This section explains how to:

- View the status of database tables
- Repair database tables
- Optimize database tables

Viewing the Status of Database Tables

To view the status of database tables:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Database/Web Application Health** link.
4. Click the **Database Table Status** link.

**Repairing Database Tables**

If you have a large database, it may take longer to verify the status of your database tables. Once the status of each table is returned, you may want to repair the tables that do not return an “OK” status.

**To repair database tables:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Database/Web Application Health** link.
4. Click the **Repair Database Tables** link.

**Optimizing Database Tables**

Optimizing database tables allows you to ensure that each table's index is up to date so that you can perform database lookups as quickly as possible.

**To optimize database tables:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Database/Web Application Health** link.
4. Click the **Optimize Database Tables** link.
Building Your Framework

Integrating with LDAP Servers

If you utilize one or more directory services to store information about the users in your organization, you can integrate the JAMF Software Server (JSS) with the directory service(s) to:

- Look up and populate user information for inventory purposes
- Authenticate users to the Imaging Suite

*Note:* Integrating with Open Directory allows the JSS to access both user and computer list information. For details on accessing computer list information from Open Directory, see the “Adding LDAP Server Connections Manually” section.

This section explains how to:

- Add LDAP server connections using the LDAP Server Connection Assistant or manually
- Test LDAP server connections
- Edit and delete LDAP server connections
- Troubleshoot LDAP server connections

Using the LDAP Server Connection Assistant

The LDAP Server Connection Assistant walks you through the process of adding an LDAP server connection to the JSS.

The assistant allows you to integrate with the following directory services:

- Apple's Open Directory
- Microsoft’s Active Directory
- Novell’s eDirectory

*Note:* To integrate with other directory services or access computer list information from Open Directory, you must configure the connection manually.

To use the LDAP Server Connection Assistant:

1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the LDAP Server Connection link.
4. Click the Add LDAP Server Connection button.
5. Choose the LDAP server you want to integrate with and click the Continue button.
6. Enter the host name (DNS name or IP address) for the LDAP server and click Continue.
7. Enter credentials for the LDAP service account and click Continue.
8. For testing purposes, enter the usernames for two different accounts in the LDAP server and click Continue.
9. Verify the returned attribute mappings are correct. If the attribute mappings are correct, click Continue and skip to step 11.

10. If an attribute mapping is incorrect, change the mapping appropriately.
   a. Click the Ellipsis button across from the mapping.
   b. Choose the correct value for the attribute from one of the pop-up menus.
   c. Click the Return to Attribute Mappings button.
   d. Verify the changes are correct and click the Continue button.
11. For testing purposes, enter the names of two different user groups in the LDAP server and click Continue.
12. Verify the group membership status of each test user is correct and click Continue.

13. Click Save to save the LDAP server connection and continue using the JSS.
    If you want to make changes before you save the connection, click the Edit Manually button, make the
    necessary changes, and then click the Save button.

Adding LDAP Server Connections Manually

Before adding an LDAP server connection manually, it is important that you are familiar with search bases,
object classes, and attributes. If you are not familiar with these concepts, use the LDAP Server Connection
Assistant to ensure attributes are mapped correctly.

Adding the connection manually allows you to:

- Integrate with directory services other than Open Directory, Active Directory, and Novell eDirectory
- Access computer list information from Open Directory

After adding the connection, test it to make sure it’s working properly. See the “Testing LDAP Server
Connections” section for testing instructions.

This section provides an overview of the Connection and Mappings panes you’ll use to add the connection
and step-by-step instructions on how to do so.
Connection Pane

This pane allows you to configure how the JSS connects to an LDAP server.

Display name
This field allows you to enter a display name for the LDAP server.

Host name
This field allows you to enter the DNS name or IP address for the LDAP server.

Encrypt Using SSL
You must select this checkbox if you want to connect to the LDAP server over SSL.

Note: For this to work, the LDAP server must have SSL enabled.

Use custom port
If the LDAP server is not running on the standard port, you must select this checkbox and enter the port on which it is running.

Use for
This pop-up menu allows you to specify the type of information you want to access from the LDAP server.

Create Mappings Based On
This pop-up menu allows you to select the LDAP server you want to connect to.

Domain
This field allows you to enter the domain for the LDAP server.
Authentication Type
If the LDAP server requires authentication, specify the authentication type using this pop-up menu. After choosing an authentication type, two additional fields appear in which you can enter credentials for the LDAP service account.

Most LDAP servers require simple authentication.

Open/Close times out in ____ seconds
This field allows you to enter the maximum number of seconds you want to wait for the server to open or close a connection before it times out.

Connection times out in ____ seconds
This field allows you to enter the maximum number of seconds you want to wait for the server to return results before the connection times out.

Referrals
This pop-up menu allows you to choose whether to ignore, follow, or utilize default LDAP referrals to locate information.

Use wildcards when searching for objects
Select this checkbox if you want the JSS to return partial matches when searching the LDAP server for information.

Mappings Pane
This pane allows you to map attributes and specify object class and search base data.

If you're not familiar with these concepts, use the LDAP Server Connection Assistant to add the connection.
To configure an LDAP server connection manually:

1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the LDAP Server Connection link.
4. Click the Add LDAP Server Connection button.
5. Select the Configure manually option and click the Continue button.
6. Configure the connection using the information on the Connection and Mappings panes.
7. Click the Save button.

Testing LDAP Server Connections

Before using an LDAP server connection as part of your framework, test the connection by looking up user (or computer list) information. If the results are returned correctly, the connection is working.

This section explains how to look up user and computer list information.

To look up user information from an LDAP server:

1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the LDAP Server Connection link.
4. Click the Test Connection link across from the connection you want to test.
5. Click the User Lookup, User Group Lookup, or User Group Membership Lookup tab.
6. Enter information in the field(s) provided.
7. Click the **Test** button.

   **To look up computer list information from Open Directory:**

   1. Log in to the JSS with a web browser.
   2. Click the **Settings** tab.
   3. Click the **LDAP Servers Connection** link.
   4. Click the **Test** link across from the Open Directory connection you want to test.
   5. Click the **Computer Lookup**, **Computer Group Lookup**, or **Computer Group Membership Lookup** tab.
   6. Enter information in the field(s) provided.
   7. Click the **Test** button.

### Editing LDAP Server Connections

**To edit an LDAP server connection:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **LDAP Servers Connection** link.
4. Click the **Edit** link across from the connection you want to edit and make changes manually. For more information about the Connection and Mappings panes, see the “Adding LDAP Server Connections Manually” section.
5. Click the **Save** button.

### Deleting LDAP Server Connections

**To delete an LDAP server connection from the JSS:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **LDAP Servers Connection** link.
4. Click the **Delete** link across from the connection you want to delete.

5. Click the **Delete** button to confirm.

**Tools for Troubleshooting LDAP Server Connections**

This section describes two tools you can use to troubleshoot the connection between the JSS and an LDAP server.

**Apache Directory LDAP Studio**

The Apache Directory LDAP Studio allows you to connect to an LDAP server to pinpoint initial connections and find search bases and mappings. You can download Apache Directory LDAP Studio at:

[https://directory.apache.org/studio/](https://directory.apache.org/studio/)

**Workgroup Manager**

Apple's Workgroup Manager allows you to view detailed information for individual LDAP server accounts.

**To view LDAP information using Workgroup Manager:**

1. Open Workgroup Manager.

2. Connect to your server.

3. From the menu bar, choose **Workgroup Manager > Preferences**.

4. Select the **Show “All Records” tab and inspector** checkbox, and then click **OK**.

5. Click the **All Records** tab (target icon) displayed in the sidebar to view the records.
Managing JSS User Accounts

The JAMF Software Server (JSS) is a multi-user application. You can grant different levels of access to each user by setting up JSS user accounts and assigning different privileges to each one.

Individual JSS user accounts can be created manually or—if you have an LDAP server connection set up—added from a directory service. You can also grant access to groups from an LDAP server.

This section explains how to:
- Create a new user account in the JSS
- Add a user account from an LDAP server
- Upgrade the Distinguished Name (DN) from an LDAP account
- Grant access to a group from an LDAP server

**Note:** JSS users added from an LDAP server receive the privileges assigned to their individual user accounts. LDAP members that don’t have individual accounts in the JSS, but are members of one or more groups with access, receive the privileges assigned to each group.

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

To create a new user account in the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Accounts** link.
4. Click the **Create New Account** button.
5. Enter user information on the Account pane.

6. Click the Privileges tab and select the checkbox next to each privilege you want to grant the user.

7. Click the API Privileges tab and select the API privileges you want to grant the user.
8. Click the **Notifications** tab and select the checkbox next to each event you want the user to receive a notification about.

   **Note:** A valid email address must be entered on the Account pane for notifications to be sent.

   ![Notifications tab](image)

9. Click **Save**.

   **To add a user account from an LDAP server:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Accounts** link.
4. Click the **Add Account from LDAP** button.
   If you don’t see this button, you need to set up an LDAP server connection before completing these steps. (For more information, see the “Integrating with LDAP Servers” section.)

   ![Accounts and Groups](image)

5. Enter the username for the account you want to add and click **Next**.

   ![Add User From LDAP Server](image)

6. When the JSS returns the results, click the **Add <username>** link next to the user you want to add.

   ![Add User Link](image)
7. Configure accounts settings on the Privileges, API Privileges, and Notifications panes.
8. Click Save.

To update the Distinguished Name (DN) for an LDAP account:
1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the Accounts link.
4. Click the Edit Account link next to the account you want to modify.
5. Click the Update DN button.
6. Enter the new Distinguished Name and click Save.

To grant access to an LDAP group:
1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the Accounts link.
4. Click the **Add Group from LDAP** button in the toolbar.

   If you don’t see this button, you need to set up an LDAP server connection before completing these steps. (For more information, see the “Integrating with LDAP Servers” section.)

5. Enter the name of the group you want to add and click **Next**.

6. When the JSS returns the results, click the **Add <group name>** link next to the group you want to add.

7. Set privileges for the group on the Privileges pane and click **Save**.
Managing Network Segments

A network segment is a range of IP addresses that can be used to perform the following actions:
- Assign client computers to the closest distribution point.
- Limit a PreStage’s scope to image only client computers within the specified IP range.

Network segments can be class B or class C subnets, or any IP range therein.

This section explains how to create, edit, and delete a network segment in the JAMF Software Server (JSS).

To create a network segment:
1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the Network Segments link.
4. Click the Create New Network Segment button in the toolbar.
5. Enter a display name for the network segment.
6. Specify an IP range for the network segment by entering starting and ending IP addresses.
7. If you want to assign a distribution point to the network segment, make your selection from the Default Distribution Point pop-up menu.
8. Click the Save button.

To edit a network segment:
1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the Network Segments link.
4. Click the **Edit Network Segment** link across from the network segment that you want to edit and make the necessary changes.

5. Click **Save**.

**To delete a network segment:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Network Segments** link.
4. Click the **Delete Network Segment** link across from the network setting you want to delete.
5. Click **Delete** to confirm.
Managing Packages

This section explains how to:
- Add new packages
- Change package attributes
- Add DMGs of Adobe Installer DVDs
- Add DMGs of Adobe Updaters
- Add DMGs of Mac OS X Installer DVDs
- Delete packages

Adding New Packages

Before you deploy a package, you must add it to the JAMF Software Server (JSS) using Casper Admin and assign it to one or more distribution points.

There are two ways to add a new package to Casper Admin:
- Drag a package into Casper Admin
- Copy the package directly to a distribution point

Dragging Packages into Casper Admin

When you drag a package into Casper Admin, it is copied to the master distribution point and displayed in blue text in the Unknown category until you assign it to a software category.

To add a package to Casper Admin:
1. Open Casper Admin and authenticate to the JSS.
2. Drag the package from the Finder to the Package pane in Casper Admin.

Copying Packages Directly to the Distribution Point

This method copies the package to the Packages folder at the root of the file share. You can enter information about the package into the JSS manually.

If you open Casper Admin after adding the package, the name of the package is displayed in blue text in the Unknown category in the sidebar.

To add a package manually:
1. Copy the package to the Packages folder on your distribution point.
2. Log in to the JSS with a web browser.
3. Click the Settings tab.
4. Click the Casper Admin link.

5. Click the New Package button and enter information about the package on the Info pane.

   Note: The information entered in File Name field must match the name of the file exactly.

6. Click Save.

Changing Package Attributes

You can change the attributes that determine how a package is installed.

This section explains:
- How to modify package attributes using Casper Admin or the JSS
- The attributes listed on the Summary, Info, and Options panes

To change package attributes using Casper Admin:
1. Open Casper Admin.
2. Select the package that you want to change.
3. Click the Info button in the toolbar.
4. Make changes to the information on the Info and Options panes, and then click OK.

To change package attributes using the JSS:
1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.

3. Click the **Casper Admin** link and click the package name.

4. Make changes on the Info and Options panes, and then click **Save**.

**Summary Pane**

This pane displays an overview of the package. The **Reveal in Finder** button displays the package in a Finder window.

*Note:* The Summary pane exists in the Casper Admin application only. It is not included in the web version of Casper Admin.
Info Pane

This pane allows you to modify basic information about a package.

![Info Pane](image)

The following attributes are displayed on this pane:

**Display Name**
This is the customizable name that identifies a package when it is displayed in a list of packages or policies. The display name does not have to match the name of the package.

**File Name**
This is the name of the package. If you change a filename using the web version of Casper Admin, you must manually update the filename on each distribution point. If you change a filename using the Casper Admin application, this information is automatically updated for you.

**Category**
This identifies the organizational category to which a package belongs.

**Info**
The information displayed to the administrator when a package is being deployed.

**Notes**
Notes are only displayed in Casper Admin. They are helpful when tracking information about a package, such as who created it and when it was built.
Options Pane

This pane allows you to specify deployment information and set criteria that limits whether a client computer can install or uninstall a package.

Setting these limitations prevents packages from being deployed to client computers that should not receive them.

The following attributes are displayed on this pane:

**Priority**
This determines the order in which packages are installed. For example, an OS package should have a priority of 1 to ensure that it is installed first. An updater or a package that needs to overwrite files that may exist in another package should have a priority of 20.

**Fill User Templates**
The default settings for a new user’s home directory are located in the User Template folder. When you select this option, the files and folders in the first home directory located in /Users/ are copied to the User Template directories in:

/System/Library/User Template/

Selecting this option allows you to distribute preferences or documents and provide a default work environment to any new user on a client computer.

*Note:* This option is only available for DMG packages.
Fill Existing User Home Directories
Selecting this option copies the files and folders in the first home directory located in /Users/ to every existing home directory on the client computer.

Note: This option is only available for DMG packages.

This package must be installed to the boot volume at imaging time
If this option is selected, Casper Imaging installs the package with the first run script.

Stage
You can limit how a package is used and deployed by choosing one of the following options from the Stage pop-up menu:

- Testing—The package can only be deployed using Casper Remote (not a policy), and can only be pushed to five computers at a time.
- Non-Deployable—The package cannot be deployed. This setting is useful if the package needs to be taken out of production temporarily for licensing or other reasons.
- Deleted—The package has been deleted from Casper Admin.

Install Only if Processor Is [PowerPC/x86]
Some packages are built only for a single architecture. You can specify this information by selecting this option and choosing PowerPC or X86 from the pop-up menu.

To install an alternate package when a non-compliant architecture is encountered, choose an alternate package from the If the target computer’s processor is not there pop-up menu.

Adding DMGs of Adobe Installer DVDs
Adobe CS3 and CS4 products can be deployed without repackaging by adding a DMG of the Adobe Installer DVD to Casper Admin and identifying it as an Adobe Installer Image.

If you download installer media directly from Adobe, it is already in DMG format. If you have installer media on DVD, you must first create the DMG using Disk Utility.

Since the Adobe Installer Image, itself, is not a deployable object, you must use Casper Admin or the JSS to create the Adobe installations that install and configure Adobe products.

Creating an Adobe installation involves the following steps:

1. Create the DMG.
2. Add the Adobe Installer DMG.
3. Create a new Adobe installation using Casper Admin or the JSS.

Step 1: Create the DMG
1. Insert the installer DVD into a computer with Mac OS X.
2. Open Disk Utility from the Utilities folder.
3. Click the DVD button in the sidebar.

4. From the menu bar, choose File > New > New Image From <name of the DVD>.

5. Save as a compressed DMG.

**Step 2: Add the Adobe Installer DMG**

1. Open Casper Admin.

2. Drag the DMG of the Adobe Installer DVD into Casper Admin. This copies the DMG directly to the master distribution point.

   After Casper Admin copies the DMG, the Info pane is displayed. If it does not appear, click the Info button in the toolbar.

3. Click the Info tab and select the This file is a disk image containing an installer (Mac OS X or an Adobe Installer/Updater) option.

   It can take Casper Admin up to 30 seconds to analyze the contents of the DMG. When this process is complete, the Options pane appears and a list of payloads available with the installer is displayed.

4. Click OK and select Adobe Installer Images in the View Type list to see the listing for the DMG.

**Step 3: Create a New Adobe Installation Using Casper Admin**

1. Open Casper Admin.

2. Click the New Adobe Install button in the toolbar.
3. If you have multiple Adobe Installer Images, choose the one on which you want to base your installation from the **Installer Image** pop-up menu.

![Installer Image](image1)

4. Enter a display name for the installation.

![Display Name](image2)

5. Click the **Options** tab and set the installation options.

![Installation Options](image3)
6. Click OK.

**Step 3: Create a New Adobe Installation Using the JSS**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **New Adobe Install** button in the toolbar.
5. If you have more than one Adobe Installer Image, choose the image on which you want base your installation from the **Installer Image** pop-up menu.

6. Click **Save**.

7. Enter a display name for the installation on the Info pane.
8. Click the **Options** tab and set the installation options. For more information about these options, see the “Options for an Adobe Install” section.

![Image of Options pane](image)

9. Click **Save**.

### Options for Adobe Installations

The Options pane allows you to specify the following information for an Adobe installation:

**Priority**

Setting the priority determines the order in which packages are installed.

**Serial Number**

Providing this information identifies the serial number of products you are installing.

**Suppress Installer Dock Button**

Adobe Installer’s icon will appear in the Dock of any logged-in user even if the installer is deployed in “silent” mode. Selecting this option ensures that the icon does not appear in the Dock.

**Ignore Conflicting Processes**

Adobe’s Installer will fail if conflicting processes are found. Common conflicts include Safari, Firefox, and Microsoft Office applications. Selecting this option prompts the installer to ignore these conflicts.

As a result, any plug-ins installed for applications that are running during the installation will not be available until the applications are re-opened.

**List of Available Payloads**

This provides a list of payloads available in the Adobe Installer Image.

You can use a single Adobe Installer Image to create multiple distributions of Adobe products that may contain different sets of the payloads.

**Suppress EULA**

Ensures that users are not prompted with an End User License Agreement (EULA) when opening Adobe products.
**Suppress Registration**
Ensures that users not prompted to register Adobe products.

**Suppress Updates**
Ensures that users are not prompted with available Adobe updates when using Adobe applications.

**Stage**
You can set limitations on the use or deployment of a package by choosing one of the following options from the **Stage** pop-up menu:

- **Testing**—The package can only be deployed using Casper Remote (not a policy) and can only be pushed to five computers at a time.
- **Non-Deployable**—The package cannot be deployed. This setting is useful if the package needs to be taken out of production temporarily for licensing or other reasons.
- **Deleted**—This setting indicated that the package has been deleted in Casper Admin.

**Adding DMGs of Adobe Updaters**

Most Adobe updates are available for download on Adobe's support website are already in DMG format.

Updaters that support silent installation can be installed without repackaging. If you add the DMG to Casper Admin and it is not recognized as an Adobe Updater, it is possible that the updater does not support silent installation.

**To add an Adobe Updater DMG:**

1. Open Casper Admin.
2. Drag the DMG of the Adobe Updater into Casper Admin.
   This copies the DMG directly to the master distribution point.
   After Casper Admin copies the DMG, the Info pane is displayed. If it does not appear, click the **Info** button in the toolbar.
3. Click the **Info** tab, and select the **This file is a disk image containing an installer (Mac OS X or an Adobe Installer/Updater)** option.
   It can take Casper Admin up to 30 seconds to analyze the contents of the DMG. When this process is complete, the Options pane appears and a list of payloads available with the updater is displayed.

**Adding DMGs of Mac OS X Installer DVDs**

Installing your operating system using a DMG of the Mac OS X Installer DVD ensures that client computers receive a clean operating system without requiring you to build a separate OS package.

You create a Mac OS X installation by adding a DMG of the Mac OS X Installer DVD to Casper Admin and identifying it as a Mac OS X Installer Image.
If you download installer media directly from Apple, it is already in DMG format. If you have installer media on DVD, you must first create the DMG using Disk Utility.

You can use a single image to create multiple installations, each with custom software and language settings.

Creating a Mac OS X installation involves the following steps:

1. Create the DMG.
2. Add the Mac OS X Installer DVD.
3. Customize a Mac OS X installation using Casper Admin or the JSS.

**Step 1: Create the DMG**

1. Insert the installer DVD into a computer with Mac OS X.
2. Open Disk Utility from your Utilities folder.
3. Click the DVD button in the sidebar.
4. From the menu bar, choose File > New > New Image From <name of the DVD>.
5. Save as a compressed DMG.

**Step 2: Add the Mac OS X Installer DMG**

1. Open Casper Admin.
2. Drag the DMG of the Mac OS X Installer into Casper Admin. This copies the DMG directly to the master distribution point.
   After Casper Admin copies the DMG, the Info pane is displayed. If it does not appear, click the Info button in the toolbar.
3. Click the Info tab and select the This file is a disk image containing an installer (Mac OS X or an Adobe Installer/Updater) option.
   It can take Casper Admin up to 30 seconds to analyze the contents of the DMG.
4. When this process is complete, choose a default language for the installation from the **Language** pop-up menu.

**Note:** The initial Mac OS X Installer image cannot be customized beyond the language. For more information on customizing the installation, see the step entitled “Customize a Mac OS X Installation Using Casper Admin/the JSS”.

5. Click **OK**.

**Step 3: Customize a Mac OS X Installation Using Casper Admin**

1. Open Casper Admin.
2. Select the Mac OS X installation on which you want to base your new installation.
3. Click the **Info** button in the toolbar.
4. Click the **Options** tab and click the **Create Custom OS Install** button.
5. Enter a display name for the installation on the Info pane.

6. Click the **Options** tab again and select the checkbox next to each package you want to install.

7. Click **OK**.

**Step 3: Customize a Mac OS X Installation Using the JSS**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the Casper Admin link.

4. Click the link for the Mac OS X installation on which you want to base the new installation.

5. Click the Options tab and click the Create Custom OS Install button.

6. Enter a display name for the installation on the Info pane.
7. Click the **Options** tab and select the checkbox next to each package you want to install.

![Package Options](image)

8. Click **Save**.

**Deleting Packages**

If you no longer need a package, you can delete it using Casper Admin or the JSS.

When you delete a package, it is moved from the Packages folder to the Deleted Packages folder that is located in the Casper Data folder. To permanently delete the package, empty the trash after the package has been deleted.

After a package is deleted, change the stage to “Deleted” so it cannot be used.

This section explains how to:
- Delete a package using Casper Admin or the JSS
- Empty the trash using Casper Admin or the JSS

**To delete a package using Casper Admin:**

1. Open Casper Admin, and make sure the **Repository** list is highlighted in the sidebar.
2. Select the packages that you want to delete.
3. Click the **Delete** button in the toolbar.
4. Click **OK** to confirm the deletion.
To delete a package using the JSS:
1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click **Casper Admin** link.
4. In the list of packages, click the link for package that you want to delete.
5. Click the **Options** tab and choose “Deleted” from the **Stage** pop-up menu.
6. Click **Save**.

To empty the trash using Casper Admin:
1. Open Casper Admin.
2. Click the **Empty Trash** button in the toolbar.
3. Click **OK** to confirm the deletion.

To empty the trash using the JSS:
1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **Deleted Items** button in the toolbar and click **Empty Trash**.
Managing Scripts

This section explains how to:

- Add new scripts
- Change script attributes
- Delete scripts

Adding New Scripts

Before you deploy a script, you must add it to the JAMF Software Server (JSS) using Casper Admin and assign it to one or more distribution points.

There are two ways to add a new script to Casper Admin:

- Drag the script into Casper Admin.
- Copy the script directly to a distribution point.

Dragging Scripts into Casper Admin

When you drag a script into Casper Admin, it is copied to the master distribution point and displayed in blue text in the Unknown category until you assign it to a software category.

To add a script using Casper Admin:

1. Open Casper Admin and authenticate to the JSS.
2. Drag the script from the Finder into the Package pane in Casper Admin.

Copying Scripts to the Distribution Point

This method copies the script to the Scripts folder at the root of the file share. You can enter information about the script into the JSS manually.

If you open Casper Admin after adding the script, the name of the script is displayed in blue text in the Unknown category in the sidebar.

To add a script manually:

1. Add the script to the Scripts folder on your distribution point.
2. Log in to the JSS with a web browser.
3. Click the Settings tab.
4. Click the Casper Admin link.
5. Click the **New Script** button and enter information about the script on the Info pane.

   **Note:** The information entered in the **File Name** field must match the name of the file exactly.

6. Click **Save**.

### Changing Script Attributes

You can change the attributes that determine how a script is run.

This section explains:

- How to change script attributes using either Casper Admin or the JSS
- The attributes listed on the Summary, Info, and Options panes

**To change script attributes using Casper Admin:**

1. Open Casper Admin.
2. Select the script that you want to change.
3. Click the **Info** button in the toolbar.
4. Make changes to the information on the Info and Options panes, and then click **OK**.

**To change script attributes using the JSS:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link and click the name of the script.
4. Make changes on the Info and Options panes, and then click **Save**.
Summary Pane

This pane displays an overview of the script. The **Reveal in Finder** button displays the script in a Finder window.

*Note:* The Summary pane exists in the Casper Admin application only. It is not included in the web version of Casper Admin.
**Info Pane**

This pane allows you to modify basic information about a script.

![Info Pane Screenshot](image)

The following attributes are displayed on this pane:

**Display Name**
This is the customizable name that identifies a script when it is displayed in a list of scripts or policies. The display name does not have to match the name of the script file.

**File Name**
This is the name of the script file. If you change a filename using the web version of Casper Admin, you must manually update the filename on each distribution point. If you change a filename using the Casper Admin application, this information is automatically updated for you.

**Category**
This identifies the organizational category to which a script belongs.

**Info**
The information displayed to the administrator when a script is being deployed.

**Notes**
Notes are only displayed in Casper Admin. They are helpful when tracking information about a script, such as who created it and when it was created.
Options Pane

This pane allows you to specify deployment information and limit the operating systems on which a script can be run.

The following attributes are displayed on this pane:

Priority
This determines the order in which scripts will run. For example, you can choose whether a script should run before the imaging process, after the imaging process, or the first time the computer boots after imaging.

Parameter Labels
Three parameters are predefined for every script by default, but you can assign up to eight additional parameters.

You can enter names for these additional parameters in the Parameter Labels fields. If you do not enter a name, the script will be displayed as “Parameter x” in deployment interfaces.

Stage
You can limit how a script is used and deployed by choosing one of the following options from the Stage pop-up menu:

- **Testing**—The script can only be deployed using Casper Remote (not a policy), and can only be pushed to five client computers at a time.
- **Non-Deployable**—The script cannot be deployed. This setting is useful if the script needs to be taken out of production temporarily.
- **Deleted**—The script has been deleted from Casper Admin.
Deleting Scripts

If you no longer need a script, you can delete it using Casper Admin or the JSS.

When you delete a script, the script file is moved from the Scripts folder to the Deleted Scripts folder that is located in the Casper Data folder. To permanently delete a script, empty the trash after the script has been deleted.

After a script is deleted, change the stage to “Deleted” so it can’t be used.

This section explains how to:
- Delete a script using Casper Admin or the JSS
- Empty the trash using Casper Admin or the JSS

To delete a script using Casper Admin:
1. Open Casper Admin, and make sure the Repository list is highlighted in the sidebar.
2. Select the scripts that you want to delete.
3. Click the Delete button in the toolbar.
4. Click OK to confirm the deletion.

To delete a script using the JSS:
1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click Casper Admin link.
4. In the list of scripts, click the link for the script that you want to delete.
5. Click the Options tab and choose Deleted from the Stage pop-up menu.
6. Click Save.

To empty the trash using Casper Admin:
1. Open Casper Admin.
2. Click the Empty Trash button in the toolbar.
3. Click OK to confirm the deletion.

To empty the trash using the JSS:
1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the Casper Admin link.

4. Click the Deleted Items button in the toolbar and click Empty Trash.
Managing Printers

This section explains how to:
- Add new printers
- Change printer attributes
- Delete printers

Adding New Printers

Before you deploy a printer, you must add it to the JAMF Software Server (JSS) using Casper Admin as a deployable object.

To add a printer using Casper Admin:
1. Open Casper Admin and authenticate to the JSS.
2. Click the Add Printers button in the toolbar.
3. Authenticate locally if prompted.
4. Select the checkbox next to each printer you want to add.
5. Using the Category pop-up menu, choose the category to which the printers should be added, and then click the Add button.

Changing Printer Attributes

Printers, like packages and scripts, have attributes that determine how they are organized and deployed.

This section explains:
- How to change printer attributes using Casper Admin or the JSS
- The attributes listed on the Summary, Info, and Options panes
To change printer attributes using Casper Admin:
1. Open Casper Admin.
2. Select the printer.
3. Click the **Info** button in the toolbar.
4. Make changes to the information on the Info and Options panes, and then click **OK**.

To change printer attributes using the JSS:
1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link and click the printer name.
4. Make changes on the Info and Options panes, and then click **Save**.

**Summary Pane**
This pane displays an overview of the printer.

*Note:* The Summary pane exists in the Casper Admin application only. It is not included in the web version of Casper Admin.
**Info Pane**

This pane allows you to modify basic information about a printer.

The following attributes are displayed on this pane:

**Display Name**
This is the customizable name that identifies a printer when it is displayed in Casper Imaging, Casper Remote, or policies.

This name can differ from the name of the Postscript Printer Description file (PPD).

**File Name**
This is the name of the Postscript Printer Description file (PPD).

**Category**
This identifies the organizational category to which a printer belongs.

**Info**
The information displayed to the administrator when a printer is being deployed.

**Notes**
Notes are only displayed in Casper Admin. They are helpful when tracking information about a printer or package, such as who created it and when it was built.
Options Pane

This pane allows you to specify deployment information and limit the operating systems to which a printer can be mapped.

The following attributes are displayed on this pane:

Stage
You can limit how a printer is used and deployed by choosing one of the following options from the Stage pop-up menu:

- **Non-Deployable**—The printer cannot be deployed. This setting is useful if the package needs to be taken out of production temporarily for licensing or other reasons.
- **Deleted**—The printer has been deleted from Casper Admin.

Deleting Printers

If you no longer need a printer, you can delete it using Casper Admin.

After a printer is deleted, change the stage to “Deleted” so it cannot be used.

This section explains how to:

- Delete a printer using Casper Admin or the JSS
- Empty the trash using Casper Admin or the JSS

To delete a printer using Casper Admin:

1. Open Casper Admin and make sure the Repository list is highlighted in the sidebar.
2. Select the printers that you want to delete.
3. Click the **Delete** button in the toolbar.
4. Click **OK** to confirm the deletion.

**To delete a printer using the JSS:**
1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. In the list of printers, click the link for printer that you want to delete.
5. Click the **Options** tab and choose “Deleted” from the **Stage** pop-up menu.
6. Click **Save**.

**To empty the trash using Casper Admin:**
1. Open Casper Admin.
2. Click the **Empty Trash** button in the toolbar.
3. Click **OK** to confirm the deletion.

**To empty the trash using the JSS:**
1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **Deleted Items** button in the toolbar and click **Empty Trash**.
Creating Directory Bindings

Directory bindings bind client computers to directory services. You can create the following directory bindings:

- Active Directory (using Apple's built-in tools)
- Open Directory (using Apple's built-in tools)
- Active Directory using Likewise
- Active Directory using ADmitMac
- Active Directory using Centrify

This section explains how to create each directory binding in the JAMF Software Server (JSS).

To create an Active Directory binding:

1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the Casper Admin link.
4. Click the New Directory Binding button in the toolbar.
5. Select the Active Directory Binding (built into Mac OS X) option and click the Continue button.
6. Enter a display name for the binding. This is an arbitrary name that allows you to choose the correct binding if more than one exists.
7. Enter the Active Directory domain.
8. Enter the username and password for an Active Directory account that has permissions to add computers, and enter the password again to verify it.
9. In the Computer OU field, enter the OU in which the computer object should be placed.

![Edit Directory Bindings: New AD Binding](image)
10. If you are binding client computers with more than one directory binding, use the **Priority** pop-up menu to specify the order in which the bindings should be applied.

11. Enter any additional information on the User Experience, AD Mappings, and Administrative panes. The information specified on these panes is the same information entered when using Apple’s Directory Utility application.

12. Click **Save**.

**To create an Open Directory binding:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **New Directory Binding** button in the toolbar.
5. Select the **Open Directory Binding (built into Mac OS X)** option and click the **Continue** button.
6. Enter a display name for the binding. This is an arbitrary name that allows you to choose the correct binding if more than one exists.
7. Enter the DNS name or IP address for the server hosting the Open Directory service.
8. If you use SSL to bind to the Open Directory service, select the **Encrypt Using SSL** checkbox.
9. If you want to allow users from Open Directory to log in to other bound clients, select the **Use For Authentication** option.
10. If you want users from Open Directory to be listed as contacts on other client computers, select the **Use For Contacts** option.
11. If you want to bind to Open Directory securely, select the **Perform Secure Bind** checkbox and enter the username and password for the directory account.
12. If you are binding client computers with more than one directory binding, use the Priority pop-up menu to specify the order in which the bindings should be applied.

13. Click Save.

**To create a Likewise Active Directory binding:**

1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the Casper Admin link.
4. Click the New Directory Bindings button in the toolbar.
5. Select the Likewise Binding option and click the Continue button.
6. Enter a display name for the binding.
   This is an arbitrary name that allows you to choose the correct binding if more than one exists.
7. Enter the domain to which you are binding.
8. Enter the username and password for an administrator account and enter the password again to verify it.
9. In the Computer OU field, enter the OU in which the computer object should be placed.

10. If you are binding client computers with more than one directory binding, use the Priority pop-up menu to specify the order in which the bindings will be applied.

11. Click Save.

**To create an ADmitMac Active Directory binding:**

1. Log in to the JSS with a web browser.
2. Click the Settings tab.
3. Click the Casper Admin link.
4. Click the **New Directory Bindings** button in the toolbar.

5. Select the **ADmitMAC Binding** option and click the **Continue** button.

6. Enter a display name for the binding.
   This is an arbitrary name that allows you to choose the correct binding if more than one exists.

7. Enter the DNS name or IP address for the server to which you are binding.

8. Enter the username and password for an administrator account and enter the password again to verify it.

9. In the **Computer OU** field, enter the OU in which the computer object should be placed.

10. If you are binding client computers with more than one directory binding, use the **Priority** pop-up menu to specify the order in which the bindings will be applied.

11. Enter any additional information on the Home Folders, Login Policy, Admin, OUs, and Mappings panes.
    The information specified on these panes is the same information entered when using Thursby’s ADmitMac interface.

12. Click **Save**.

**To create a Centrify Active Directory binding:**

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

2. Click the **Settings** tab.

3. Click the **Casper Admin** link.

4. Click the **New Directory Bindings** button in the toolbar.

5. Select the **Centrify Binding** option and click the **Continue** button.

6. Enter a display name for the binding.
   This is an arbitrary name that allows you to choose the correct binding if more than one exists.

7. Enter the domain to which you are binding.
8. Enter the username and password for an administrator account and enter the password again to verify it.

9. In the Container DN field, enter the DN in which the client computers should be placed.

10. If you are binding client computers with more than one directory binding, use the Priority pop-up menu to specify the order in which the bindings will be applied.

11. Enter any additional information on the Centrify Options pane. The information specified on this pane is the same information entered when using the Centrify interface.

12. Click Save.
Managing Removable MAC Addresses

Computers are identified by their MAC addresses during the imaging process. This makes utilizing USB Ethernet dongles during imaging problematic, since the JAMF Software Server (JSS) assumes that each computer with a specific dongle is connected to the same computer.

To work around this issue, you can enter a list of MAC addresses that the JSS should ignore when identifying a computer.

This section explains how to add, edit, and delete a removable MAC address.

**To add a removable MAC address:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Removable MAC Addresses** link.
5. Click the **Add Address** button.
6. Enter the MAC address you want the JSS to ignore in the **MAC Address** field.
7. Click the **Save** button.

**To edit a removable MAC address:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Removable MAC Addresses** link.
5. Click the **Edit MAC Address** link across from the MAC address you want to edit and update the address.

6. Click **Save**.

**To delete a removable MAC address:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Inventory Options** link.
4. Click the **Removable MAC Addresses** link.
5. Click the **Delete MAC Address** link across from the MAC address you want to delete.

6. Click **Delete** to confirm.
Overview of the Imaging Process

This section provides information about each component of the imaging process.

Configurations

Configurations are sets of packages, scripts, printers, and directory bindings that make up an image. Configurations allow you to quickly specify what needs to be installed on a computer and make updates without rebuilding an entire image.

Smart Configurations

Smart configurations give you the ability to create similar configurations quickly by creating configurations that inherit the components of other configurations. You can then assign additional packages, scripts, printers, and directory bindings as needed.

Compiled Configurations

Compiled configurations speed up the imaging process by building a single DMG that includes each component in a configuration.

Partitioning

In addition to packages, scripts, printers, and directory bindings, configurations can contain partitioning information.

Secondary partitions can be dynamically sized based on the target drive and can receive the following payloads:

- A configuration
- A Restore partition (Casper Imaging automatically converts an OS package to a Restore partition.)
- A Winclone image
- Nothing
As a safety mechanism, drives that contain multiple pre-configured partitions are not repartitioned; however, secondary partitions can be set up to re-image the partition if it already exists.

**Restore Partitions**

Restore partitions are hidden partitions that allow you to re-image a computer using less network overhead. These partitions function as an alternative to NetBoot or USB/FireWire drives.

In lab environments, Restore partitions allow for fully automated re-imaging of computers. They can also cache packages and scripts locally to reduce the stress on your distribution points.
Managing Configurations

This section explains how to:
- Create configurations
- Create smart configurations
- Compile configurations
- Delete configurations

Creating Configurations

This section explains how to use Casper Admin or the JAMF Software Server (JSS) to:
- Create a configuration
- Set up partitioning

To create a configuration using Casper Admin:

1. Open Casper Admin.
2. Click the New Config button in the toolbar.
3. Enter a name for the configuration.
4. (Optional) Enter a description of the configuration.
5. If you want to set a default homepage for the clients:
   a. Click the Homepage tab.
   b. Enter the web address for the homepage.
6. To add packages, scripts, printers, and directory bindings, drag them from the list in the main pane to the configuration in the sidebar.

To create a configuration using the JSS:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **New Config** button in the toolbar.
5. Enter a name for the configuration.
6. (Optional) Enter a description of the configuration.
7. Click the **Contents** tab and use the **Packages, Scripts, Printers, and Directory Bindings** tabs to locate the items you want to add to the configuration. To add an item, select the checkbox next to it.

![Edit Configuration: My Configuration](image)

8. If you want to set a default homepage for the clients:
   a. Click the **Homepage** tab.
   b. Enter the web address for the homepage in the **Homepage** field.

![Edit Configuration: My Configuration](image)

9. Click the **Save** button.

![Edit Configuration: My Configuration](image)

**To set up partitioning for a configuration using Casper Admin:**

1. Open Casper Admin.
2. Create or edit the configuration to partition.
   - To create a new configuration, click the **New Config** button in the toolbar.
   - To edit an existing configuration, select the configuration in the sidebar.
3. Click the **Additional Partitions** tab.
4. Click the **Add (+)** button.
5. Enter a name for the partition in the **Partition Name** field.
6. Enter the size you want the partition to be in the **Size** field.
7. Enter the maximum percentage of space that the partition should take up on the target drive.
8. If you want to deploy a configuration to the partition:
   a. Choose "Journaled HFS+" from the **Format** pop-up menu.
   b. Choose the configuration that you want to install from the **Install the Configuration** pop-up menu.
   c. If you want this partition to be re-imaged on subsequent images of the primary partition, select the **Re-image this partition if it already exists** option.
   d. To append a string to the computer name from the primary partition, enter the computer name in the **Append to Computer Name** field.
   e. Click **OK**.

   ![Partition Configuration Dialog Box]

9. If you want to deploy a Restore partition to the partition:
   a. Choose "Journaled HFS+" from the **Format** pop-up menu.
   b. Select the **This is a Restore Partition** checkbox.
   c. Choose an OS package from which to create the Restore partition.
   d. To append a string to the computer name from the primary partition, enter the computer name in the **Append to Computer Name** field.
   e. Click **OK**.

   ![Restore Partition Configuration Dialog Box]

   **Note:** Casper Admin identifies any package that has a priority of 1 as an OS package.

10. If you want to deploy a Winclone image to the partition:
    a. Choose "NTFS" from the **Format** pop-up menu.
    b. Choose the image that you want to install.
    c. Select the **Re-image this partition if it already exists** option if you want the partition to be re-imaged on subsequent images of the primary partition.
d. Click OK.

11. Repeat steps 2 through 10 for each additional partition.

**To set up partitioning for a configuration using the JSS:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Create or edit the configuration to partition.
   - To create a new configuration, click the **New Config** button in the toolbar.
   - To edit an existing configuration, select the configuration in the sidebar.
5. Click the **Additional Partitions** tab.
6. Click the **Add New Partition** link.
7. Enter a name for the partition, and then enter the size that you want it to be.
8. Enter the maximum percentage space that the partition should take up on the target drive.
9. If you want to deploy a configuration to the partition:
   a. Choose "Journaled HFS+" from the **Format** pop-up menu.
   b. Choose the configuration that you want to install.
   c. If you want this partition to be re-imaged on subsequent images of the primary partition, select the **Re-image this partition if it already exists** option.
   d. To append a string to the computer name from the primary partition, enter the computer name in the **Append to Computer Name** field.
e. Click OK.

10. If you want to deploy a Restore partition to the partition:
   a. Choose "Journaled HFS+" from the Format pop-up menu.
   b. Select the This is a Restore Partition checkbox.
   c. Choose the OS package from which the Restore partition should be created.
   d. To append a string to the computer name from the primary partition, enter the computer name in the Append to Computer Name field.
   e. Click OK.

11. If you want to deploy a Winclone image to the partition:
   a. Choose "NTFS" from the Format pop-up menu.
   b. Choose the image that you want to install.
c. If you want the partition to be re-imaged on subsequent images of the primary partition, select the **Re-image this partition if it already exists** option.

d. Click **OK**.

![Partition configuration settings](image)

12. Repeat steps 4 through 11 for each additional partition.

13. Click the **Save** button.

## Creating Smart Configurations

Smart configurations are based on other configurations. When you create a smart configuration, the configuration it is based on is called the standard configuration.

Smart configurations inherit the following components from their standard configuration:

- Packages
- Scripts
- Printers
- Directory bindings
- Homepage
- Partitions

Making changes to a standard configuration automatically updates the smart configuration to reflect the changes.

This section explains how to create a smart configuration using Casper Admin or the JSS.

**To create a smart configuration using Casper Admin:**

1. Open Casper Admin.

2. Click the **New Config** button in the toolbar.
3. Enter a name for the configuration.
4. (Optional) Enter a description of the configuration.
5. Select the **Smart Configuration** button.
6. Choose the configuration on which you want to base the smart configuration, and then click **OK**.
7. Add packages, scripts, printers, and directory bindings to the configuration, if necessary.

**Note:** To display only items unique to the smart configuration (the items you added in step 7), click the **Hide Items from Parent Configuration** button. To turn off this feature, click the **Hide Items from Parent Configuration** button again to depress it.

**To create a smart configuration using the JSS:**
1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. Click the **New Config** button in the toolbar.
5. Enter a name for the configuration.
6. (Optional) Enter a description of the configuration.
7. Select the **Smart Configuration** button.
8. Choose the configuration on which you want to base the smart configuration, and then click **OK**.
9. Click the **Contents** tab and add packages, scripts, printers, and directory bindings to the configuration if necessary.
10. Click **Save**.

**Compiling Configurations**

The compilation process installs the contents of a configuration to a single DMG, and then makes a block copy of the configuration. You can choose to make the DMG a compressed or an uncompressed file.

The time it takes to complete the compilation process varies with the amount of data in the configuration. For the fastest results, use a wired connection.

**To compile a configuration using Casper Admin:**
1. Open **Casper** Admin.
2. In the sidebar, select a configuration and click the **Compile** button.
3. Choose to create a compressed or an uncompressed DMG.
4. Enter credentials for the local administrator account.
5. Click OK.

**Note:** You may be prompted to authenticate multiple times during this process.

### Deleting Configurations

If there are clients using Autorun with a configuration you need to delete, it is recommended that you delete the entire configuration from the JSS. This gives you the option to update the Autorun data using a new configuration.

This section explains how to delete a configuration using Casper Admin or the JSS.

**To delete a configuration using Casper Admin:**

1. Open Casper Admin.
2. In the sidebar, select the configuration that you want to delete and click the **Delete** button in the toolbar.
3. Click **OK** to confirm.

**To delete a configuration using the JSS:**

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Casper Admin** link.
4. In the sidebar, select the configuration that you want to delete and click the **Delete the Configuration** link.
5. To assign a new configuration that should be used for Autorun data, choose the configuration from the **Replace for Autorun with** pop-up menu.
6. Click the **Delete Configuration** button.
Imaging Drives

Before imaging a drive, you must boot to a startup disk other than the target drive. Some of the most common options for booting to a different startup disk are:

- NetBoot/NetInstall67
- A USB or FireWire drive
- A Restore partition

The JAMF Software Resource Kit includes a utility called the Casper NetInstall Creator. This utility creates a NetInstall image that has Casper Imaging automatically configured for you.

A Restore partition is a hidden partition configured to open Casper Imaging and automatically re-image a computer without intervention.

Imaging a drive for the first time automatically acquires the computer.

This section explains how to:

- Image a drive
- View imaging logs using the JSS

To image a drive:

1. Boot to a startup disk other than the target drive.
2. Open Casper Imaging.
3. Choose the drive that you want to image from the Target Drive pop-up menu.
4. Select the Erase <target drive> checkbox.
   
   Warning: Selecting this option will cause all data on the target drive to be lost.
5. Enter a name for the computer in the Computer Name field.
6. Choose a configuration from the Install Configuration pop-up menu.
7. Select the Reboot to <target drive> checkbox.
8. Choose a distribution point from the Use Distribution Point pop-up menu.
   
   To use a local drive, choose "Choose Local Drive" and then choose the local drive.
   The local drive must be an external drive that is replicated in Casper Admin. (For more information, see the "Replicating FireWire or USB Drives" section in "Managing Distribution Points".)
9. Click **Install**.

   ![Casper Imaging Install](image)

   **To view Imaging logs using the JSS:**

   1. Log in to the JSS using a web browser.
   2. Click the **Logs** tab.
   3. Click the **Casper Imaging Logs** link.
   4. Click the **View Log** link across from the log that you want to view.
Customizing the Imaging Process

The imaging process is made up of the following components:
- Packages
- Scripts
- Printers
- A local account
- Directory bindings
- An Open Firmware/EFI password
- Network settings

Although configurations already contain most of these components, you can fully customize the imaging process by modifying each component as needed.

This section explains how to:
- Change the selected packages
- Change the selected scripts
- Change the selected printers
- Create a new local account
- Change the selected directory bindings
- Set an Open Firmware/EFI password

To change the selected packages:
1. Open Casper Imaging.
2. Click the Custom Install button in the toolbar.
3. Click the Packages tab.
4. In the list of packages, locate the packages you want to add or remove and select the checkbox next to each one.

![Image of package selection](image1.png)

**To change the selected scripts:**
1. Open Casper Imaging.
2. Click the **Custom Install** button in the toolbar.
3. Click the **Scripts** tab.
4. In the list of scripts, locate the scripts you want to add or remove and select the checkbox next to each one.

![Image of script selection](image2.png)

5. Enter custom parameters and select a priority for each script using the **Before**, **After**, and **At Reboot** options.

**To change the selected printers:**
1. Open Casper Imaging.

![Image of printer selection](image3.png)
2. Click the **Custom Install** button in the toolbar.

3. Click the **Printers** tab.

4. In the list of printers, locate the printers you want to add or remove and select the checkbox next to each one.

   ![Image of Casper Imaging interface](image)

   **To create a new local account:**

   1. Open Casper Imaging.
   2. Click the **Custom Install** button in the toolbar.
   3. Click the **Accounts** tab.
   4. Click the **Add (+)** button below the list of new local accounts.
   5. Enter the new account information in the dialog that appears and click **OK**.

   **To change the selected directory bindings:**

   1. Open Casper Imaging.
   2. Click the **Custom Install** button in the toolbar.
   3. Click the **Accounts** tab.
4. In the list of directory bindings, select the checkbox next to each binding you want to add or remove.

To set the Open Firmware/EFI password:

1. Open Casper Imaging.
2. Click the Custom Install button in the toolbar.
3. Click the Accounts tab.
4. Select the Set Open Firmware/EFI Password checkbox.
5. Choose "Command" from the Mode pop-up menu.
6. Enter and verify the password for your account.
Computer-Specific Network Settings

In order to change the network settings for a computer, Casper Imaging must be able to locate a network configuration that has the same settings (for instance, manually, using DHCP with a manual IP address, using DHCP, or using BootP) as the computer.

For example, if a computer requires a manually entered IP address, the configuration must require the same.

If only a few computers require a certain network configuration (or your OS package does not have one of the network configuration types listed in Casper Imaging), you can build a package that contains the following file:

/Library/Preferences/SystemConfiguration/preferences.plist

You should take this file from a computer that has the network configuration type you are looking for, such as manually or using DHCP with a manual IP address.

This section explains how to:

- Change the network settings
- Set the Apple Remote Desktop info fields
- Reset or fix permissions after imaging
- Display the Mac OS X Setup Assistant on the first boot

To change the network settings:

1. Open Casper Imaging.
2. Click the Custom Install button in the toolbar.
3. Click the Network tab.
4. Choose “Ethernet” or “Airport” from the Show pop-up menu.
5. Choose the network configuration type from the **Configure IPv4** pop-up menu, and then make the necessary changes.

**Note:** Any fields left blank will not be modified when Casper Imaging updates the settings.

To set the Apple Remote Desktop info fields:

1. Open Casper Imaging.
2. Click the **Custom Install** button in the toolbar.
3. Click the **Advanced** tab and specify any relevant information.

To reset or fix permissions after imaging:

1. Open Casper Imaging.
2. Click the **Custom Install** button in the toolbar.
3. Click the **Advanced** tab and select the **Fix Permissions** checkbox.

   ![Casper Imaging Advanced Tab](image)

   **To display the Mac OS X Setup Assistant on the first boot:**

   1. Open Casper Imaging.
   2. Click the **Custom Install** button in the toolbar.
   3. Click the **Advanced** tab and select the **Show Setup Assistant After Reboot** checkbox.

   **Note:** If you do not select the **Show Setup Assistant After Reboot** checkbox, Casper Imaging will make sure the file exists in:

   /private/var/db/.AppleSetupDone
Managing Autorun Preferences

Autorun preferences allow you to control delay, load balancing, and caching settings the Autorun feature in Casper Imaging. The following list explains each preference setting:

- **Delay**—The minimum number of seconds that Casper Imaging waits before automatically imaging a computer.
  During this delay, a pane is displayed that allows you to cancel reformatting of the drive if necessary.

- **Random additional delay**—The number of seconds added to the delay.
  Setting an additional delay can relieve stress from the distribution point when a large deployment is staggered over a period of time.

- **Enable Load Balancing for distribution points**—Randomly assigns distribution points for each computer if the distribution point has a backup.
  This does not guarantee distribution points will balance perfectly as the balancing is done client-side.

- **Leave this much space available when caching packages**—Caches packages locally until the specified amount of space remains on the client.
  This only takes place if Casper Imaging is configured to cache packages during the Autorun process. See the “Using the Autorun Feature” section for more information.

- **Compare Cached Packages using**—Specifies whether file size, modification date, or checksum is used to ensure the latest copy of a package.
  This only takes place if Casper Imaging is configured to cache packages during the Autorun process. See the “Using the Autorun Feature” section for more information.

To set Autorun preferences:

1. Log in to the JSS with a web browser.
2. Click the **Settings** tab.
3. Click the **Autorun Preferences** link.
4. On the pane that is displayed, set Autorun preferences as needed.
5. Click the **Save** button.
Using the Autorun Feature

The Autorun feature allows you to automatically re-image computers according to a schedule. This reduces the amount of time and interaction required to prepare a lab or classroom for use.

The Autorun preferences allow you to configure delay, load balancing, and caching options for the Autorun feature. See the section entitled “Managing Autorun Preferences” for more information.

This section explains how to:
- Store Autorun data for an individual computer
- Create Autorun data for an individual computer
- Bypass the Autorun feature
- Edit Autorun data for an individual computer
- Delete Autorun data for an individual computer
- Mass edit and mass delete Autorun data

To store Autorun data for an individual computer:
1. Open Casper Imaging on the computer you want to store Autorun data for.
2. Configure imaging options for the computer, and then select the **Store all imaging information for this computer in the JSS** checkbox.
3. Enter the password for the local account if prompted and click **OK**.
4. To automatically re-image the computer the next time Casper Imaging is launched, select the **Automatically image this computer the next time Casper Imaging is launched** checkbox.
5. To reduce network traffic during subsequent re-images, select the **Cache a copy of every package and script for re-imaging** checkbox.
   This prompts Casper Imaging to keep a copy of each package and script.
6. To bypass the delay that takes place before the imaging process begins, select the **Skip the 60–120 Second delay before Casper Imaging automatically images** checkbox.

   **Note:** Once Autorun data is stored for the computer, the computer is imaged automatically when Casper Imaging is launched.

To create Autorun data for an individual computer:
1. Log in to the JSS with a web browser.
2. Click the **Inventory** tab.
3. Perform a simple search for the computer.
4. Click **Autorun** across from the computer record.
5. On the Install pane, specify installation information and set imaging options.
6. Use the six remaining tabs (**Packages**, **Scripts**, **Printers**, **Accounts**, **Network**, and **Advanced**) to specify any additional information as needed.

7. Click the **Save** button.

**To bypass the Autorun feature:**

To temporarily bypass the Autorun feature, hold down the **Shift** key when you open Casper Imaging.

**To edit Autorun data for an individual computer:**

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

2. Click the **Inventory** tab.

3. Perform a simple search for the computer.

4. Click **Autorun** across from the computer record.

5. On the Install pane, add or modify the information as needed.

6. Use the six remaining tabs (**Packages**, **Scripts**, **Printers**, **Accounts**, **Network**, and **Advanced**) to specify any additional information as needed.

7. Click the **Save** button.
To delete Autorun data for an individual computer:

1. Log in to the JSS with a web browser.
2. Click the Inventory tab.
3. Perform a simple search for the computer.
4. Click Autorun across from the computer record.
5. Click the Remove Autorun Data for this Computer button.
6. Click the Delete Permanently button to confirm.

To mass edit or mass delete Autorun data:

1. Log in to the JSS with a web browser.
2. Click the Inventory tab.
3. Perform a simple search for the computers.
4. Choose “Edit Autorun Data” from the Take Action on Results pop-up menu. Then, click Go. The Edit Autorun Data pane is displayed at its default settings.
5. If you want to edit the Autorun data, configure new settings as needed and click the **Apply Changes** button.

If you want to delete the Autorun data, click the **Delete Autorun Data for these Computers** button and click **OK** when prompted.

6. Click **Continue** to confirm the changes.
PreStage Imaging

PreStage imaging allows you to image computers or groups of computers automatically as you add them to your network. When you create a PreStage, you pre-configure the imaging process to include information that you want to use to image the computers.

Using a PreStage automatically acquires newly imaged computers.

This section explains how to create, view logs for, edit, and delete a PreStage.

To create a PreStage:

1. Log in to the JSS with a web browser.
2. Click the Management tab.
3. Click the PreStage Imaging link.
4. Click the Create PreStage button in the toolbar.
5. Enter a display name for the PreStage.
6. Set the date and time you want the PreStage to become active using the Make active after pop-up menus.
7. Set the date and time you want the PreStage to expire using the Disable after pop-up menus.
   If you don’t want the PreStage to expire, set a date far ahead in the future, such as “12/30/2020”.
8. Choose how you want the PreStage to assign names to the computers:
   - If you select the List of Names option, you can provide a list of computer names from which names are assigned.
   - If you select the Using MAC Addresses option, names are assigned according to each computer’s MAC address.
   - If you select the Using Serial Number option, names are assigned according to each computer’s serial number.
9. Choose whether to limit the scope of the PreStage to computers in certain network segments, with specific MAC addresses, or with certain serial numbers.
10. If you want Casper Imaging to automatically image the computer during the initial imaging, select the Run Automatically During Initial Imaging checkbox.

![Image of the 'Run Automatically During Initial Imaging' checkbox]

11. To receive an email notification when a new computer is imaged using the PreStage, select the Send Email Notification on Initial Contact from New Computer checkbox.

12. Click the Scope tab.

13. Based on how you chose to limit the scope in step 9, select the network segments to which the PreStage should be made available or enter the MAC addresses or serial numbers for the computers.

![Image of the 'Network Segments' section]

14. Click the Computer Names tab.

15. If you chose to assign names to the computers using a list of names in step 8, do one of the following:
   - Manually enter a list of computer names in the blank field provided.
   - If the names are in numerical order, perform the following steps to have the JSS populate the list for you:
     a. Click the Computer Name Assistant button.
b. Enter a prefix, starting number, ending number, and suffix in the fields provided.

c. A sample entry is displayed for your reference.

d. Click the **Add Names** button.

16. If you chose to assign names to the computers using MAC addresses in step 8, enter a prefix and suffix for the MAC addresses and enter the maximum number of computers the PreStage should be used for. If there is no definite number, enter a large number, such as “99999”.

17. Use the Install, Scripts, Printers, Accounts, Network, and Advanced panes to enter any additional imaging information.

To make this information available for the computers in the future, click the **Install** tab and select the **Store all imaging information for this computer in the JSS** checkbox.

18. Click **Save**.

**To view logs for a PreStage:**

1. Log in to the JSS with a web browser.
2. Click the **Management** tab.
3. Click the **PreStage Imaging** link.
4. Click the **View Status** link across from the PreStage.
5. Click the **View Log** link across from the log that you want to view.
To edit a PreStage:
1. Log in to the JSS with a web browser.
2. Click the Management tab.
3. Click the PreStage Imaging link.
4. Click the Edit link across from the PreStage you want to modify and make the necessary changes.
5. Click Save.

To delete a PreStage:
1. Log in to the JSS with a web browser.
2. Click the Management tab.
3. Click the PreStage Imaging link.
4. Click the Delete link across from the PreStage that you want to delete.
5. Click Delete to confirm.
Target Mode Imaging

Target Mode Imaging (TMI) is an alternative method for imaging large quantities of computers when using the network is not optimal. For example, MacBook Airs that do not have built-in ethernet but come with high-speed Thunderbolt ports can be imaged in mass using TMI. This method of imaging is faster than using USB Ethernet dongles, especially when using Thunderbolt.

Instead of running Casper Imaging on every computer by booting to a NetBoot image or an external drive, you can run Casper Imaging on a host computer and connect other computers that are booted to target disk mode.

TMI automatically acquires newly imaged computers.

TMI requires a host computer with a FireWire or Thunderbolt port and target computers that support target disk mode.

To use TMI:

1. On the host computer, open Casper Imaging.
2. Choose "Target Mode Imaging" from the Target Drive pop-up menu.
3. To erase the target drives, select the Erase hard drives attached to this computer checkbox.

   **Warning:** Selecting this option will cause all data on the target drives to be lost.

4. Specify how you want to name target computers by choosing an option from the Computer Name pop-up menu.

   Choosing "Numerical order", "Use MAC Address", or "Use serial number" prompts you to enter a prefix and suffix. For "Numerical order", you must also enter a start number.

   Choosing "Upload CSV file" prompts you to choose a CSV file. The CSV file must meet the following specifications:
- The first column contains the target computers' serial numbers or MAC addresses. Acceptable delimiters for MAC addresses are a period, a colon, or no delimiter.
- The second column contains the target computers' names.

5. Choose a configuration from the Install Configuration pop-up menu.

6. Choose a distribution point from the Use Distribution Point pop-up menu.
   To use a local drive, choose "Choose Local Drive" and then choose the local drive.
   The local drive must be an external drive that is replicated in Casper Admin. (For more information, see the "Replicating FireWire or USB Drives" section in "Managing Distribution Points").

7. If target computers will not be started up to contact the JSS immediately after imaging, specify an approximate contact time by choosing an option from the Computers Will Contact JSS pop-up menu.

8. To automatically image subsequent drives when they are connected to the host computer, choose "Image automatically without prompting" from the When a new device is detected pop-up menu.
   By default, Casper Imaging displays a prompt before imaging each drive.

9. Click Start.
10. Boot a target computer to target disk mode.
   To do this, turn on the computer and immediately press and hold down the T key.

11. Use a FireWire or Thunderbolt cable to connect the target computer to the host computer, and then click OK if prompted.
   Casper Imaging immediately starts imaging the drive.

12. When the imaging process is complete, disconnect the target computer.

13. Repeat steps 10-12 for each target computer.