# QuickStart Guide for Mobile Device Management

**Version 8.5**

| Inventory | Configuration | Security Management | Distribution | |
|-----------|---------------|---------------------|--------------|---|

JAMF software

# How to Use This Guide

Mobile Device Management (MDM) with the Casper Suite is based on four tasks—Inventory, Configuration, Security Management, and Distribution. This guide contains a lesson-based workflow for each task.

You can complete one or all of the workflows in any order that meets your MDM needs.

After completing a workflow, use the advanced options in the "Explore More" section to further customize your framework.

Keep in mind that you only need to complete each lesson once. If you've already completed a lesson (for example, installing the JSS), skip it and move on to the next one in the workflow.

## Using a Print Version of This Guide

1. Locate the task that you want to complete on the Lesson Plan page.

2. Complete each lesson in the workflow.

   You can find additional information about each lesson in the *Casper Suite Administrator's Guide*. A list of relevant sections is provided in the "Administrator's Guide Reference Sections" section of each lesson.

3. After you complete the last lesson in the workflow, refer to the "Explore More" section of this guide for a list of extended options and where to read more about them in the *Casper Suite Administrator's Guide*.

## Using a PDF of This Guide

Use the Bookmarks panel to navigate each workflow.

# QuickStart Guide for MDM Lesson Plan

| Prerequisites | Install the JAMF Software Server (JSS)<br><br>**Page 6** | Specify an SMTP Server *(Optional)*<br><br>**Page 9** | Add an LDAP Server Connection *(Optional)*<br><br>**Page 10** | Configure the Mobile Device Management Framework<br><br>**Page 11** |
|---|---|---|---|---|
| **Inventory** | Prerequisites<br><br>**Pages 6-12** | Enroll Mobile Devices with the JSS<br><br>**Page 14** | View Mobile Device Details<br><br>**Page 16** | |
| **Configuration** | Prerequisites<br><br>**Pages 6-12** | Enroll Mobile Devices with the JSS<br><br>**Page 14** | Create and Distribute an iOS Configuration Profile<br><br>**Page 17** | |
| **Security Management** | Prerequisites<br><br>**Pages 6-12** | Enroll Mobile Devices with the JSS<br><br>**Page 14** | Run a Remote Command for Mobile Devices<br><br>**Page 19** | |
| **Distribution** | Prerequisites<br><br>**Pages 6-12** | Enroll Mobile Devices with the JSS<br><br>**Page 14** | Distribute an App<br><br>**Page 20** | |

# Prerequisites

# Install the JAMF Software Server (JSS)

The JAMF Software Server (JSS) is the MDM server from which you configure and perform over-the-air management tasks.

Follow the steps in this section to install the JSS on Mac OS X Server.

> *Note:* To obtain the JSS Installers for Linux and Windows along with installation instructions, see the introductory email that you received when you purchased the product or contact your JAMF Software Representative.
>
> 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

## Requirements

A Mac computer with:

- A clean installation of Mac OS X Server 10.6 or later
- An Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- Java 1.6
- MySQL Enterprise Edition 5.5 or later (recommended) *or* MySQL Community Server 5.5 or later, available at:
  http://www.mysql.com/downloads/

> *Note:* If you are running Mac OS X Server 10.6, you can use the version of MySQL that is built into the operating system.

- Ports 8443 and 9006 available

## Step 1: Create the jamfsoftware Database

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

- User name: jamfsoftware
- Password: jamfsw03

> *Note:* If you customize the database name, user name, or password, you will be prompted to enter the custom settings on the Database pane 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 Mac OS X 10.7 or later, the default path for MySQL is `/usr/local/mysql/bin/`.

2. Type the password for the MySQL "root" user.

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 user name other than "jamfsoftware," it is recommended that you do not use "root".

# Step 2: Run the JSS Installer

Run the JSS Installer to install Apache Tomcat (the web application server that runs the JSS) and the JSS web application.

**To run the JSS Installer:**

1. Copy the JSS Installer for Mac (`JSS Installer.mpkg`) to the server.

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 disk on which to install the software, and then click **Continue**.

6. If you customized the database name, user name, or password when you created the jamfsoftware database, or MySQL is using a port other than 3306, the Database pane is displayed. Update the information to reflect your custom settings, 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**.

## Administrator's Guide Reference Sections

- "Installing the JSS on Mac OS X Server"
- "Setting Up the JSS"

# Specify an SMTP Server *(Optional)*

To enroll mobile devices by sending an OTA (over-the-air) invitation, the JSS must contain information about your SMTP server.

## Requirements

- The DNS name or IP address (host name) of your SMTP server
- The email address from which OTA invitations will be sent
- Credentials for an administrator account to the SMTP server (Only if the SMTP server requires authentication)

**To specify an SMTP server:**

1. Open the JSS in a web browser.
2. Log in using the account that you created when you set up the JSS.
3. Click the **Settings** tab.
4. Click the **General Settings** link.
5. Click the **SMTP Server** tab, and enter information about the SMTP server.
6. Click **Save**.

## Administrator's Guide Reference Sections

"Enabling Email Notifications"

# Add an LDAP Server Connection *(Optional)*

To require users to log in to initiate the OTA enrollment process, an LDAP server connection must be set up in the JSS.

Requiring user login has the following advantages:

- It ensures that only users with valid accounts can enroll their devices.
- It populates location information for the mobile device in the JSS.

> *Note:* If your organization does not utilize an LDAP directory server but you want to require user login, you can create a JSS user account that has privileges to enroll devices. For more information, see "Managing JSS User Accounts" of the *Casper Suite Administrator's Guide*.

## Requirements

- The DNS name or IP address (host name) of your LDAP server
- Credentials for the LDAP server's service account
- Information about two LDAP user accounts for testing purposes (For example, username, real name, email address, etc.)
- Information about two LDAP user groups for testing purposes (For example, group name, members, etc.)

**To add an LDAP server connection:**

1. Open the JSS in a web browser.

2. Log in using the account that you created when you set up the JSS.

3. Click the **Settings** tab.

4. Click the **LDAP Server Connections** link.

5. Click the **Add LDAP Server Connection** button.

6. Choose the LDAP server you want to integrate with, and then click **Continue**.

7. Follow the onscreen instructions to configure the LDAP server connection.

## Administrator's Guide Reference Sections

"Integrating with LDAP Servers"

# Configure the Mobile Device Management Framework

Before enrolling devices with the JSS, set up the security components that are required for MDM:

- Public key infrastructure (PKI)
- Web server certificate
- Apple Push Notification service (APNs) certificate

## Public Key Infrastructure

To ensure the security of over-the-air tasks, the JSS requires a public key infrastructure (PKI) that supports certificate-based authentication. This includes:

- A certificate authority (CA) with Simple Certificate Enrollment Protocol (SCEP) capabilities
- A signing certificate
- A root CA certificate

If your organization currently uses a CA with SCEP capabilities, you can integrate it with the JSS. If not, the JSS has a built-in CA that is enabled by default. The built-in CA has the signing and root CA certificates uploaded for you.

For instructions on how to integrate with a third-party CA, see "Configuring the Mobile Device Management Framework" in the *Casper Suite Administrator's Guide*.

## Web Server Certificate

MDM requires a valid web server certificate to ensure that managed devices communicate with the JSS and not an imposter server.

If you do not have a valid web server certificate, see "Generating a Web Server Certificate" in the *Casper Suite Administrator's Guide* for more information.

## Apple Push Notification Server Certificate

For the JSS to perform over-the-air management tasks, it must be able to communicate with Apple Push Notification service (APNs). To enable this communication, you must obtain an APNs certificate from Apple and upload it to the JSS.

The JSS guides you through the process of generating an APNs certificate from the Apple Push Certificate Portal. This process requires:

- A valid JAMF Nation account

    To create a JAMF Nation account, go to:

    http://jamfnation.jamfsoftware.com/createAccount.html
- A valid Apple ID

**To generate an APNs certificate:**

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

2. Click the **Settings** tab.

3. Click the **Global Management Framework Settings** link.

4. Click the **Push Notification Certificate** tab.

5. Click the **Create a certificate using the Push Notification Certificate Assistant** link.

6. Choose how you want to obtain the CSR.

   - If the server hosting the JSS has an outbound connection, select **Request Signed CSR Automatically through JAMF Nation**. Enter the user name and password for your JAMF Nation account, and then click **Continue**.

     The JSS connects to JAMF Nation over port 443 and obtains the signed CSR. (You will download the CSR in the next step.)

   - If the server hosting the JSS does not have an outbound connection, select **Download CSR and Request Signing Manually**. Then, follow the onscreen instructions to get the CSR signed.

7. On the Request Cert pane, follow the onscreen instructions to request an APNs certificate from Apple.

   It is recommended that you sign in to the Apple Push Certificate Portal with a corporate Apple ID, since the account will be associated with your corporate APNs certificate.

8. On the Upload Cert pane, click **Choose File.** Select the APNs certificate (.pem) that you want to upload and click **Choose**. Then, click **Continue** in the JSS.

9. Click **Done** to save the certificate.

## Administrator's Guide Reference Sections

- "Configuring the Mobile Device Management Framework"
- "Generating a Web Server Certificate"

# Lessons

# Enroll Mobile Devices with the JSS

After configuring the MDM framework, you can enroll mobile devices with the JSS for management. Enrollment establishes a connection between the devices and the JSS, allowing you to perform over-the-air management tasks without requiring user interaction.

You can initiate the enrollment process over-the-air by:

- Sending an OTA invitation via email or text message (SMS)
- Providing users with an enrollment URL

## Requirements

To send an OTA invitation, you need:

- An SMTP server set up in the JSS
- Mobile devices with access to a wireless network connection (for email invitations) or a valid phone number with SMS capabilities (for SMS-based invitations)
- (For required login only) An LDAP server connection set up in the JSS or a JSS user account with OTA enrollment privileges

To provide an enrollment URL, you need:

- An LDAP server connection set up in the JSS or a JSS user account with OTA enrollment privileges
- Mobile devices with access to a wireless network connection

**To send an OTA invitation:**

1. Open the JSS in a web browser.

2. Log in using the account that you created when you set up the JSS.

3. Click the **Management** tab.

4. Click the **Mobile Device Enrollment** link.

5. Click the **Send OTA Invitations** button.

6. Select whether to send the invitation by email or SMS.

   If you chose to send an SMS invitation, use the pop-up menu that is displayed to specify the network carrier.

7. Enter the email addresses or phone numbers that you want to send the invitation to, and then click **Continue**.

   Make sure to separate each entry with a line break or a comma.

8. Customize the invitation message as needed, and then click **Continue**.

9. Use the pop-up menus to set an expiration data for the invitation.

10. To require users to log in to access the invitation, leave **Required login** selected.

Users must log in with credentials for an LDAP directory account or a JSS user account with OTA enrollment privileges.

11. To allow multiple uses of the invitation, leave **Allow multiple uses of invitations** selected, and then click **Continue**.

12. Verify that the information on the Complete pane is correct, and then click **Send**.

When users receive the invitation, they tap the enrollment URL and follow a series of guided steps to enroll their devices. When the enrollment process is complete, the devices are managed by the JSS.

**To provide an enrollment URL:**

Direct users to the full URL of the JSS followed by /enroll/. For example:

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

Users log in and follow a series of guided steps to enroll their devices. When the enrollment process is complete, the devices are managed by the JSS.

# Administrator's Guide Reference Sections

- "Integrating with LDAP Servers"
- "Managing JSS User Accounts"
- "Enrolling Mobile Devices with the JSS"

# View Mobile Device Details

Once a device is managed by the JSS, you can view the following inventory data for the device:

- Device Information
- Location
- Purchasing
- Apps
- Security
- Network Information

- Certificates
- Profiles
- Provisioning Profiles
- Management History
- Attachments

**To view mobile device details:**

1. Open the JSS in a web browser.

2. Log in using the account that you created when you set up the JSS.

3. Click the **Inventory** tab.

4. Click the **Mobile Devices** link above the search field.

5. Leave the search field blank and click the **Search Mobile Devices** button, or type the **Enter** key. This returns all devices in this JSS.

6. Click the **Details** link across from any device to view detailed inventory data.

## Administrator's Guide Reference Sections

"Searching Mobile Devices"

## Explore More: Inventory

For more information about Inventory, see page 22 of this document.

# Create and Distribute an iOS Configuration Profile

iOS configuration profiles are XML files (.mobileconfig) that define groups of settings for managed mobile devices. The JSS allows you to create configuration profiles using an interface similar to Apple's iPhone Configuration Utility (iPCU) and Profile Manager.

When you are done creating the profile, you can distribute it wirelessly by choosing a distribution method and assigning devices to the scope.

*Note:* Some payloads and settings available in iPCU and Profile Manager cannot be configured with the JSS.

Before creating a configuration profile, you should have basic knowledge of the payloads and settings that you can configure and how they affect devices. For detailed information, see Apple's *iPhone Configuration Utility* document, available at:

http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

This lesson explains how to create a configuration profile that enforces a passcode on devices.

**To create and distribute an iOS configuration profile using the JSS:**

1. Open the JSS in a web browser.

2. Log in using the account that you created when you set up the JSS.

3. Click the **Management** tab.

4. Click the **Mobile Device Profiles** link.

5. Click the **Add Profile** button.

6. Select **Create a Configuration Profile**, and then click **Continue**.

7. Enter a display name and description for the profile.

8. Choose "Deploy Automatically" from the **Deployment** pop-up menu.

9. In the payloads list, select Passcode and click **Configure**.

10. Use the options and fields in the main pane to configure settings for the payload.

11. When you are done, click the **Scope** tab and assign devices to the scope.

12. Click **Save**.

Devices in the scope install the profile the next time they contact the JSS.

# Administrator's Guide Reference Sections

"Creating and Distributing iOS Configuration Profiles"

# Explore More: Configuration

For more information about Configuration, see page 23 of this document.

# Run a Remote Command for Mobile Devices

You can manage the security of a device by running the following remote commands from the JSS:

- **Remote wipe**—Permanently erases all data on the device and deactivates it
- **Remote lock**—Locks the device
- **Remote clear passcode**—Removes the passcode from a device

**To run a remote command:**

1. Open the JSS in a web browser.

2. Log in using the account that you created when you set up the JSS.

3. Click the **Management** tab.

4. Click the **Remote Commands** link.

5. Click the **New Remote Command** button.

6. Select the command that you want to run, and then click **Continue**.

7. Follow the onscreen instructions to assign devices to the scope.

   Devices in the scope run the command the next time they contact the JSS.

## Administrator's Guide Reference Sections

"Running Remote Commands for Mobile Devices"

## Explore More: Security Management

For more information about Security Management, see page 24 of this document.

# Distribute an App

The JSS allows you to distribute in-house and App Store apps to managed mobile devices.

The following instructions explain how to distribute an unmanaged App Store app.

**To distribute an unmanaged App Store app:**

1. Open the JSS in a web browser.

2. Log in using the account that you created when you set up the JSS.

3. Click the **Management** tab.

4. Click the **Mobile Device App Catalog** link.

5. Click the **Add App** button.

6. Select **App Store App**, and then click **Continue**.

7. Enter the name of the app and choose an App Store country. Then, click **Continue**.

8. Click the **Add** link across from the app.

9. Choose "Make Available in Self Service" from the **Deployment** pop-up menu and deselect the **Deploy as managed app (when possible)** checkbox.

10. Click the **Scope** tab and assign devices to the scope.

11. Click **Save**.

Devices in the scope display the app in the Self Service web clip the next time they contact the JSS.

## Administrator's Guide Reference Sections

- "Understanding Unmanaged and Managed Apps"
- "Distributing App Store Apps"

## Explore More: Distribution

For more information about Distribution, see page 25 of this document.

# Explore More

# Explore More: Inventory

- "Performing an Advanced Mobile Device Search," describes your advanced options when searching for managed devices in the JSS.

- "Performing Mass Actions on Mobile Device Search Results," explains how to perform management tasks on one or more managed devices.

- "Editing a Mobile Device Record," explains how to edit device details in the JSS.

- "Deleting a Mobile Device from the JSS," explains how to delete a device from the JSS.

- "Searching Mobile Device Apps," explains how to search mobile device apps in the JSS.

- "Creating Mobile Device Groups," explains how to create organizational components based on a managed device's inventory attributes.

# Explore More: Configuration

- "Distributing iOS Configuration Profiles Created with Apple's Tools," explains how to distribute configuration profiles created with Apple's iPCU or Profile Manager.

- "Updating iOS Configuration Profiles," explains how to update configuration profiles that are installed on managed devices.

- "Removing iOS Configuration Profiles," explains how to remove configuration profiles from managed devices.

- "Deleting an iOS Configuration Profile," explains how to delete a configuration profile from the JSS.

# Explore More: Security Management

- "Running Remote Commands for Mobile Devices," explains how to run a remote command using the JSS.

- "Viewing the Status of Remote Commands for Mobile Devices," explains how to view whether a remote command has run on a managed device.

- "Canceling a Remote Command for Mobile Devices," explains how to cancel a remote command in the pending state.

# Explore More: Distribution

- "Configuring the Mobile Device Management Framework," explains how to add and remove the Self Service web clip from managed devices.

- "Understanding Unmanaged and Managed Apps," explains the difference between a unmanaged and an managed app, and the requirements for managing an app.

- "Understanding App Distribution Methods" explains the different ways that you can distribute an app and how they affect management, installation, updates to, and removal of the app.

- "Provisioning Profiles," explains how to upload and delete provisioning profiles from the JSS.

- "Distributing In-House Apps," explains how to distribute in-house apps.

- "Distributing App Store Apps," explains how to distributed App Store apps.

- "Updating Apps" explains how to distribute updates to in-house and App Store apps.

- "Removing Apps" explains how to remove in-house and App Store apps.

- "Deleting App" explains how to delete in-house and App Store apps from the JSS.

- "eBooks," explains how to distribute in-house eBooks and eBooks available in the iBookstore. It also explains how to edit eBooks and delete them from the JSS.