



QuickStart Guide for Managing Mobile Devices

Version 9.7

JAMF Software, LLC
© 2015 JAMF Software, LLC. All rights reserved.

JAMF Software has made all efforts to ensure that this guide is accurate.

JAMF Software
301 4th Ave S Suite 1075
Minneapolis, MN 55415-1039
(612) 605-6625

Under the copyright laws, this publication may not be copied, in whole or in part, without the written consent of JAMF Software, LLC.

Apache Tomcat and Tomcat are trademarks of the Apache Software Foundation.

Apple, the Apple logo, Finder, iPhone, and Mac OS X Server are trademarks of Apple Inc.

App Store is a service mark of Apple Inc., registered in the U.S. and other countries.

The CASPER SUITE, COMPOSER®, the COMPOSER Logo®, JAMF SOFTWARE®, the JAMF SOFTWARE Logo®, RECON®, and the RECON Logo® are registered or common law trademarks of JAMF SOFTWARE, LLC in the U.S. and other countries.

iOS is a trademark or registered trademark of Cisco in the U.S. and other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Red Hat and Red Hat Enterprise Linux are trademarks of Red Hat, Inc., registered in the United States and other countries.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

All other product and service names mentioned are the trademarks of their respective companies.



How to Use This Guide

Managing mobile devices with the Casper Suite is based on four tenets—Inventory, Configuration, Security Management, and Distribution. This guide contains a lesson-based workflow for each tenet.

To use this guide, use the “Lesson Plan” section or the Bookmarks panel to navigate each workflow. You can complete one or all of the workflows in any order that meets your organization’s needs.

After completing a workflow, see the appropriate “Explore More” section in this guide. Each “Explore More” section includes a list of extended options and related sections in the *Casper Suite Administrator’s Guide*.

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.



QuickStart Guide for Managing Mobile Devices Lesson Plan

Prerequisites	Install the JAMF Software Server	Integrate with an SMTP Server <i>(Optional)</i>	Integrate with an LDAP Directory Service <i>(Optional)</i>	Set Up Security Components
Inventory	Prerequisites	Enroll Mobile Devices	View Inventory Information	
Configuration	Prerequisites	Enroll Mobile Devices	Create an iOS Configuration Profile	
Security Management	Prerequisites	Enroll Mobile Devices	Send a Remote Command to a Mobile Device	
Distribution	Prerequisites	Enroll Mobile Devices	Distribute an App	



Prerequisites

Install the JAMF Software Server

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

Installing the 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.

You can install the JSS on the following platforms:

- Mac (For more information, see [Install the JSS on OS X.](#))
- Linux (For more information, see [Install the JSS on Linux.](#))
- Windows (For more information, see [Install the JSS on Windows.](#))

Install the JSS on OS X

Requirements

Installing the JSS on OS X requires a Mac computer with:

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- OS X v10.7 or later
- OS X Server (recommended)
- Java SE Development Kit (JDK) 1.6 or 1.7 for Mac OS X

You can download the JDK from:

<http://www.oracle.com/technetwork/java/javase/downloads/jdk7-downloads-1880260.html>

- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.6 or 1.7 (must be the same version as Java)

You can download the JCE from:

<http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>

- 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

Step 1: Install the Required Software

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

[Installing Java and MySQL](#)

Step 2: Create the jamfsoftware Database

Create a MySQL database in which the JSS can store its data and a MySQL user that can access 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 on the Database pane when you run the JSS Installer.

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: 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 privileges 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

The JSS Installer for Mac installs Apache Tomcat and the JSS web application. It also creates your initial distribution point.

To run the JSS Installer for Mac, copy it to the server. Then open the installer and follow the onscreen instructions.

Install the JSS on Linux

Requirements

Installing the JSS on Linux requires a server with:

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- One of the following operating systems:
 - Ubuntu 12.04 LTS Server (64-bit)
 - Ubuntu 14.04 LTS Server (64-bit)
 - Red Hat Enterprise Linux (RHEL) 6.4 or later
- Open Java Development Kit (OpenJDK) 6 or 7
For more information, go to <http://openjdk.java.net/>.
- 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 8080 available

Step 1: Install the Required Software

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

[Installing Java and MySQL](#)

Step 2: Create the jamfsoftware Database

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

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

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

If you did not create a root password when installing MySQL, do not type -p.

If MySQL is not in the path or it is installed in a custom location, enter the installation path in place of mysql.

2. If prompted, enter the password for the MySQL “root” user.
3. Create a database named “jamfsoftware” by executing:

```
CREATE DATABASE jamfsoftware;
```

4. Grant privileges 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

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

1. Copy the JSS Installer for Linux (jssinstaller.run) to the server.

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

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

2. Log in to the server as a user with superuser privileges.
3. Initiate the installer by executing a command similar to the following:

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

4. When the requirement check is complete, type “y” to proceed.
5. (RHEL only) When the installation is complete, edit the firewall configuration to allow access to port 8443 by executing:

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

6. (RHEL only) Choose **Other** or **Customize**, and manually add port 8443 with TCP protocol. The option you choose depends on whether you have a GUI or shell-only interface.
7. Access the JSS from an enrolled computer by opening a web browser and typing the protocol, IP address or DNS name of the server, and port. For example:
`https://jss.mycompany.com:8443/`
8. If you entered a custom database name, username, or password when you created the jamfsoftware database, or MySQL is using a port other than 3306, the Database Connection Properties pane is displayed. Before you can access the JSS, you must follow the onscreen instructions to create a connection between the JSS and the jamfsoftware database.

Install the JSS on Windows

Requirements

Installing the JSS on Windows requires a server with:

- A 64-bit capable Intel processor
- 2 GB of RAM
- 400 MB of disk space available
- Windows Server 2008 R2 (64-bit) or Windows Server 2012 (64-bit)
- Java SE Development Kit (JDK) 1.6 or 1.7 for Windows x64.

You can download the JDK from:

<http://www.oracle.com/technetwork/java/javase/downloads/jdk7-downloads-1880260.html>

- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.6 or 1.7 (must be the same version as the JDK)

You can download the JCE from:

<http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>

- 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 8080 available

Step 1: Install the Required Software

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

[Installing Java and MySQL](#)

Step 2: Create the jamfsoftware Database

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

1. Open the MySQL Command Line Client.
2. When prompted, enter the password for the MySQL “root” user.
3. Create a database named “jamfsoftware” by executing:

```
CREATE DATABASE jamfsoftware;
```

4. Grant privileges 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

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

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

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

To run the JSS Installer for Windows, copy it to the server. Then open the installer and follow the onscreen instructions.

Note: The installer must be run as an administrator.

Integrate with an SMTP Server (*Optional*)

To send an enrollment invitation via email, you need to integrate with an SMTP server by configuring the SMTP Server settings in the JSS.

Configuring the SMTP Server Settings

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **SMTP Server** .
5. Click **Edit**.
6. Configure the settings on the pane.
7. Click **Save**.

Administrator's Guide Reference Sections

"Integrating with an SMTP Server"

Integrate with an LDAP Directory Service *(Optional)*

To require users to log in using an LDAP directory account during enrollment, you need to integrate with an LDAP directory service by adding an LDAP server to the JSS. This allows you to collect user and location information during enrollment.

Adding an LDAP Server

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **LDAP Servers** .
5. Click **New** .
6. Follow the onscreen instructions to add the LDAP server.

Administrator's Guide Reference Sections

"Integrating with LDAP Directory Services"

Set Up Security Components

Before enrolling mobile devices, use the JAMF Software Server (JSS) to set up the security components that are required for managing mobile devices:

- Public key infrastructure (PKI)
- SSL certificate
- Push certificate

PKI

To ensure secure communication with the Apple Push Notification service (APNs), the JSS requires a public key infrastructure (PKI) that supports certificate-based authentication. The PKI must include the following components:

- A certificate authority (CA) that supports Simple Certificate Enrollment Protocol (SCEP)
- A signing certificate
- A CA certificate

The JSS includes a preconfigured PKI that uses a built-in CA with support for SCEP. There is no configuration necessary to use the built-in CA—the signing and CA certificates are created and stored for you. The built-in CA is used by default to issue certificates to both computers and mobile devices.

You can also configure your own PKI if you have access to an external CA that supports SCEP. The external CA can be a CA hosted by your organization or by a trusted third-party vendor. If you integrate an external CA with the JSS, this CA will be used to issue certificates to mobile devices.

For instructions on integrating with an external CA, see the “Public Key Infrastructure” section in the *Casper Suite Administrator’s Guide*.

SSL Certificate

The JSS requires a valid SSL certificate to ensure that mobile devices communicate with the JSS and not an imposter server.

For instructions on creating or uploading an SSL certificate, see the “SSL Certificate” section in the *Casper Suite Administrator’s Guide*.

Push Certificate

The JSS requires a valid push certificate to communicate with Apple Push Notification service (APNs). This communication is required to enroll and manage mobile devices.

An assistant in the JSS guides you through the following steps to create a new push certificate (.pem) and upload it to the JSS:

1. Obtain a signed certificate request (CSR) from JAMF Nation.
2. Create the push certificate in Apple's Push Certificates Portal by logging into the portal, uploading the signed CSR obtained from JAMF nation, and downloading the resulting push certificate.
3. Upload the push certificate to the JSS.

Requirements

To create a push certificate, you need:

- A valid JAMF Nation account
To create a JAMF Nation account, go to:
<https://jamfnation.jamfsoftware.com/createAccount.html>
- A valid Apple ID (A corporate Apple ID is recommended.)
- If you are renewing a push certificate that was originally obtained from Apple's iOS Developer Program (iDEP), you must use the Apple ID for the iDEP Agent account used to obtain the certificate.

Creating a Push Certificate

1. Log in to the JSS with a web browser.
2. In the top-right corner of the page, click **Settings** .
3. Click **Global Management**.
On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **Push Certificates** .
5. Click **New**  and do one of the following:
 - If the server hosting the JSS has an outbound connection, select **Download signed CSR from JAMF Nation**.
The JSS connects to JAMF Nation over port 443 and obtains the signed CSR.
 - If the server hosting the JSS does not have an outbound connection, select **Download CSR and sign later using JAMF Nation**.
6. Follow the onscreen instructions to create and upload the push certificate (.pem).

Administrator's Guide Reference Sections

- "Public Key Infrastructure"
- "SSL Certificate"
- "Push Certificates"



Lessons

Enroll Mobile Devices

Enrollment is the process of adding mobile devices to the JAMF Software Server (JSS) to establish a connection between the devices and the JSS. When mobile devices are enrolled, inventory information for the devices is submitted to the JSS, and the devices become managed. This allows you to perform inventory, configuration, security management, and distribution tasks on the devices.

You can allow users to enroll their own mobile devices by having them log in to an enrollment portal where they are prompted to install the necessary profile and certificates.

To direct users to the enrollment portal, you need to provide them with the enrollment URL. This is the full URL for the JAMF Software Server (JSS) followed by `/enroll`. For example:

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

You can provide this URL by sending it in an email or SMS invitation from the JSS. If you have an LDAP server set up in the JSS, users can log in to the enrollment portal using an LDAP directory account. This allows you to collect user and location information during enrollment.

Requirements

To send a mobile device enrollment invitation via email, you need an SMTP server set up in the JSS. (For more information, see [Integrate with an SMTP Server](#).)

For users to log in to the enrollment portal with their LDAP directory account, you need an LDAP server set up in the JSS. (For more information, see [Integrate with an LDAP Directory Service](#).)

Sending an Enrollment Invitation

You can send an enrollment invitation by email or SMS message.

Before you configure the invitation, make sure you have the email addresses or phone numbers of the users you want to send the invitation to.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Enrollment Invitations**.

On a smartphone or iPod touch, this option is in the pop-up menu.

4. Click **New** .
5. Follow the onscreen instructions to send the enrollment invitation.

An enrollment invitation is immediately sent to email addresses or phone numbers you specified.

When users receive the invitation, they tap the enrollment URL and follow a series of guided steps to enroll their mobile devices.

Administrator's Guide Reference Sections

- "User-Initiated Enrollment for Mobile Devices"
- "User-Initiated Enrollment Experience for Mobile Devices"

View Inventory Information

The JAMF Software Server (JSS) stores detailed inventory information for each mobile device. You can view and edit the following information in the JSS:

- General
- Hardware
- User and Location
- Purchasing
- Security
- Apps
- Managed eBooks
- Network
- Certificates
- Profiles
- Provisioning Profiles
- Attachments

Viewing Inventory Information for a Mobile Device

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Search Inventory**.
On a smartphone or iPod touch, this option is in the pop-up menu.
4. Choose “Mobile Devices” from the **Search** pop-up menu.
5. Leave the search field blank and press the Enter key.
6. Click the mobile device you want to view information for.
The mobile device’s inventory information is displayed.
7. Use the categories to view information for the mobile device.

Administrator’s Guide Reference Sections

“Viewing and Editing Inventory Information for a Mobile Device”

Explore More

For more information on Inventory functions, see [Explore More: Inventory](#).

Create an iOS Configuration Profile

iOS configuration profiles are XML files (.mobileconfig) that provide an easy way to define settings and restrictions for mobile devices. You can use the JAMF Software Server (JSS) to create iOS configuration profiles and specify the mobile devices and users to which the profile should be applied (called “scope”).

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

Creating an iOS Configuration Profile

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Configuration Profiles**.
On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **New**  .
5. In the General payload, enter a display name for the profile.
6. Select the Passcode payload and click **Configure**.
7. Configure the settings on the pane.
8. Click the **Scope** tab and configure the scope of the profile.
9. Click **Save**.

The profile is installed the next time mobile devices in the scope contact the JSS.

Administrator’s Guide Reference Sections

“iOS Configuration Profiles”

Send a Remote Command to a Mobile Device

The remote commands available in the JAMF Software Server (JSS) allow you to remotely perform the following tasks on a mobile device:

- Update inventory.
- Lock a device.
- Clear the passcode on a device.
- Clear the restrictions on a device (only for supervised devices).
- Unmanage a device.
- Wipe a device.
Note: You also have the option to clear the Activation Lock on a device when wiping the device.
- Send a blank push notification.
- Manage settings for voice or data roaming (only for devices with cellular capability).
- For a personally owned device, wipe institutional data and unmanage the device.

You can send a remote command to a single mobile device.

Note: The remote commands available for a particular device vary depending on the device ownership type, device platform, device type, and iOS version.

Sending a Remote Command

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Search Inventory**.
On a smartphone or iPod touch, this option is in the pop-up menu.
4. Choose "Mobile Devices" from the **Search** pop-up menu.
5. Leave the search field blank and press the Enter key.
6. Click the mobile device you want to send the remote command to.
7. Click the **Management** tab, and then click the button for the remote command that you want to send.

The remote command runs on the mobile device the next time the device contacts the JSS.

Administrator's Guide Reference Sections

"Remote Commands for Mobile Devices"

Distribute an App

When you distribute an app, you configure settings for the app and specify the users and mobile devices that should receive it (called “scope”).

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Apps**.
On a smartphone or iPod touch, this option is in the pop-up menu.
4. Click **New**  .
5. Select **App Store app** and click **Next**.
6. Enter the name of the app, choose an App Store country, and click **Next**.
7. Click **Add** for the app you want to add.
8. Verify the settings on the General pane.
9. Click the **Scope** tab and configure the scope of the app.
10. Click **Save**.

The app is distributed the next time mobile devices in the scope contact the JSS.

Administrator’s Guide Reference Sections

“App Store Apps”

Explore More

For more information on Distribution functions, see [Explore More: Distribution](#).



Explore More

Explore More: Inventory

- “Mobile Device Inventory Collection Settings”—Learn how to configure the frequency at which inventory is collected from mobile devices.
- “Mobile Device Inventory Display Settings”—Find out how to change the attribute fields displayed in the results of a simple mobile device search.
- “Simple Mobile Device Searches”—Learn how to quickly search the items in your inventory for a general range of results.
- “Advanced Mobile Device Searches”—Learn how to use detailed search criteria to search the mobile devices in your inventory.
- “Mobile Device Reports”—Learn how to change the attribute fields displayed in the results of a simple mobile device search.
- “Performing Mass Actions for Mobile Devices”—Find out how to perform potentially tedious tasks for multiple mobile devices at the same time.
- “Viewing and Editing Inventory Information for a Mobile Device”—Learn about the types of inventory information that you can view and edit for a mobile device.
- “Viewing Management Information for a Mobile Device”—Learn how to view management information, such as iOS configuration profiles and apps, for a mobile device.
- “Viewing the History for a Mobile Device”— Learn how to view management history, user and location history, and app installation history for a mobile device.
- “Deleting a Mobile Device from the JSS”—Find out how to delete a mobile device from the JAMF Software Server (JSS).
- “User Assignments”—Find out how to assign users to mobile devices.
- “Simple User Searches”—Learn how to quickly search the users in your inventory for a general range of results.
- “Viewing and Editing Inventory Information for a User”—Find out how to view and edit inventory information for a user.

Explore More: Distribution

- “Understanding Managed Apps”—Learn about the differences between unmanaged apps and managed apps, and find out which mobile devices support managed apps.
- “Understanding App Distribution Methods”—Learn about the different app distribution methods.
- “Provisioning Profiles”—Learn how to upload provisioning profiles that authorize in-house apps.
- “In-House Apps”—Find out how to distribute in-house apps and their provisioning profiles.
- “App Store Apps”—Find out how to distribute App Store apps.
- “In-House eBooks”—Find out how to distribute in-house eBooks.
- “eBooks Available in the iBookstore”—Find out how to distribute eBooks that are available in the iBookstore.
- “Integrating with VPP”—Find out how to integrate with Apple’s Volume Purchase Program (VPP) so that you can utilize VPP-managed distribution.
- “VPP Registration”—Find out how to register users with VPP so that you can assign content to users for VPP-managed distribution.
- “VPP Assignments”—Find out how to assign content to users for VPP-managed distribution.