



Jamf Pro Installation and Configuration Guide for Windows

Version 10.26.0



© copyright 2002-2020 Jamf. All rights reserved.

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

Jamf
100 Washington Ave S Suite 1100
Minneapolis, MN 55401-2155
(612) 605-6625

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

Amazon and Amazon RDS are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries.

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

Apple, Mac, macOS, OS X, and Safari are trademarks of Apple, Inc. registered in the U.S. and other countries.

The CASPER SUITE, COMPOSER®, the COMPOSER Logo®, Jamf, the Jamf 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.

Chrome and Google are trademarks or registered trademarks of Google Inc.

Intel is a registered trademark of the Intel Corporation in the U.S. and other countries.

Firefox is a registered trademark of the Mozilla Foundation.

Linux is a registered trademark of Linus Torvalds in the United States and other countries.

Microsoft, Microsoft Edge, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

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

Ubuntu is a registered trademark of Canonical Ltd.

All other product and service names mentioned herein are either registered trademarks or trademarks of their respective companies.

Contents

4 Preface

5 About This Guide

6 Additional Resources

8 Overview of Technologies

9 Applications and Utilities

10 Jamf Pro System Requirements

11 Installation

12 Installing Jamf Pro Using the Installer

16 Upgrading Jamf Pro Using the Installer

18 Manually Installing Jamf Pro

26 Setup

27 Setting Up Jamf Pro

28 Jamf Pro User Accounts and Groups

33 Activation Code

34 Integrating with an SMTP Server

36 Change Management

38 GSX Connection

41 Jamf Pro Summary

44 Database Management

45 Backing Up the Database

49 Restoring Database Backups

51 Viewing the Status of Database Tables

52 Server Infrastructure

53 About Distribution Points

56 File Share Distribution Points

58 Cloud Distribution Point

61 Jamf Infrastructure Manager Instances

63 Advanced Configuration

64 SSL Certificate

65 Configuring Tomcat to Work with a Load Balancer

66 Tomcat Thread Pool Settings

67 Jamf Pro Web App Memory

69 Clustering

71 Limited Access Settings

72 Flushing Logs

74 Migrating to Another Server

jamf | PRO

Preface

About This Guide

The Jamf Pro server is a web app that functions as the administrative core of Jamf Pro. The Jamf Pro server allows you to perform inventory and remote management and configuration tasks on managed computers and mobile devices. All other administrative applications in Jamf Pro communicate with the Jamf Pro server.

This guide provides step-by-step instructions for installing and configuring Jamf Pro on the Windows platform using the Jamf Pro Installer for Windows. It also includes instructions for performing a manual installation on Windows and explains how to perform advanced configuration tasks.

Additional Resources

Jamf Nation

<https://www.jamf.com/jamf-nation/>

The Jamf Nation website allows you to communicate with other Jamf Pro administrators via discussions, submit feature requests, and access several different types of resources related to Jamf Pro.

Knowledge Base

<https://www.jamf.com/jamf-nation/articles>

The Knowledge Base contains hundreds of articles that address frequently asked questions and common issues.

Product Documentation

To access the following product documentation for a specific Jamf Pro version, log in to Jamf Nation and go to:

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

- *Jamf Pro Release Notes*
The release notes include information on new features and enhancements, system requirements, functionality changes, and bug fixes.
- *Jamf Pro Administrator's Guide*
This guide contains overviews of features and instructions for performing administrative tasks using Jamf Pro.

In addition, you can search Jamf Nation to find best practice workflows, technical papers, and documentation for other Jamf Pro apps.

Other Resources

For access to other Jamf Pro-related resources, visit the following webpages:

- [Resources on jamf.com](#)
The Resources area on the Jamf website gives you access to product documentation, best practice workflows, technical papers, and more.
- [Jamf 100 Course](#)
The Jamf 100 Course offers a self-paced introduction to Jamf Pro and an enterprise-focused foundation of the macOS, iOS, and tvOS platforms.
- [Jamf Online Training Catalog](#)
The Jamf Online Training catalog provides self-paced modules to help you learn Apple device management with Jamf Pro. This resource is available for free to all Jamf customers.

- [Jamf Knowledge Base Videos](#)

The Jamf YouTube channel features Knowledge Base videos and troubleshooting tips on managing computers and mobile devices with Jamf Pro.

- [Jamf Marketplace](#)

The Jamf Marketplace is a central location for you to find, learn about, and utilize valuable tools to integrate with and extend the Jamf platform.

jamf | PRO

Overview of Technologies

Applications and Utilities

This section provides an overview of the applications and utilities that you need to install and maintain Jamf Pro.

Jamf Pro Server

The Jamf Pro server is a web app that functions as the administrative core of Jamf Pro. The Jamf Pro server allows you to perform inventory and remote management and configuration tasks on managed computers and mobile devices. All other administrative applications in Jamf Pro communicate with the Jamf Pro server.

Jamf Pro Installer for Windows

The Jamf Pro Installer for Windows is a standard .msi installation package that allows you to install and upgrade Jamf Pro on supported Windows operating systems. It is signed by Jamf.

To obtain the Jamf Pro Installer for Windows, log in to Jamf Nation, click **Show alternative downloads**, and then click the **Download** button under "Jamf Pro Installer for Windows" on the following page:

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

Jamf Pro Server Tools

Jamf Pro Server Tools allows you to back up and restore the Jamf Pro database. It also allows you to restart Apache Tomcat and MySQL and modify their settings.

Jamf Pro Server Tools is installed automatically when you run the Jamf Pro Installer. It is located at:

```
C:\Program Files\JSS\bin\server-tools-gui.jar
```

Jamf Pro Server Tools also has a command-line interface (CLI). It is located at:

```
C:\Program Files\JSS\bin\jamf-pro.exe
```

Jamf Pro System Requirements

For system requirements information, see "Jamf Pro System Requirements" in the [Jamf Pro Release Notes](#) for your version of Jamf Pro.

jamf | PRO

Installation

Installing Jamf Pro Using the Installer

Installing Jamf Pro using the installer involves the following steps:

1. Install the required software (if you haven't already).
2. Run the Jamf Pro Installer.
3. Create the Jamf Pro database.
4. Connect to the Jamf Pro Server.

Note: It is recommended that Jamf Pro be installed before the Jamf Pro database is created. The advantage is that the Jamf Pro Server Tools CLI is installed with the Jamf Pro installer. The CLI simplifies the process of creating the database as opposed to creating the database manually. In addition, while the Jamf Pro database can be created and configured before Jamf Pro is installed, the Jamf Pro-to-MySQL connection information cannot be configured until after Jamf Pro is installed.

Requirements

The server used to host Jamf Pro should meet the minimum requirements for operating system, Tomcat version, database configuration, and Java installation. For additional information on these Jamf Pro Server Environment requirements, see "Jamf Pro System Requirements" in the [Jamf Pro Release Notes](#) for your version of Jamf Pro.

In addition, the following resources are recommended as the minimum allocation for a typical installation of Jamf Pro:

Windows

- A 64-bit capable Intel processor
- 8 GB of RAM
- 150 GB of disk space available
- Ports 8443 and 8080 available

Note: The Jamf Pro Installer for Windows automatically creates a firewall exception for port 8443. If you are using a third-party firewall, or if you are using a port other than 8443, you will need to manually add a firewall exception.

In environments where the double-byte character set encoding is required, use English as the system language for the server used to host Jamf Pro to avoid potential display issues.

Full local administrator privileges are required to install Jamf Pro on Windows Server. If you are unable to install Jamf Pro, Group Policy Object restrictions may be the cause. Check the GPO settings or contact someone in your organization who can ensure that GPO restrictions allow you full administrator privileges.

Note: Each installation of Jamf Pro and its required services is unique, and requirements, such as Jamf Pro web app memory, may vary depending on your implementation. For information about allocating additional memory to the Jamf Pro web app, see [Jamf Pro Web App Memory](#).

If you have questions regarding scaling your environment's resources beyond the typical recommendations, contact [Jamf Support](#).

Step 1: Install the Required Software

Java and MySQL must be installed on the server before you can create the Jamf Pro database and run the Jamf Pro Installer. For instructions, see the [Installing Java and MySQL for Jamf Pro 10.14.0 or Later](#) Knowledge Base article.

Step 2: Run the Jamf Pro Installer

The Jamf Pro Installer for Windows installs Apache Tomcat, the Jamf Pro web app, and Jamf Pro Server Tools.

Note: To obtain the Jamf Pro Installer for Windows, log in to Jamf Nation, click **Show alternative downloads**, and then click the **Download** button under "Jamf Pro Installer for Windows" on the following page:

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

To run the Jamf Pro 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.

Step 3: Create the Jamf Pro Database

You must create a MySQL database before you can use Jamf Pro. For instructions, see the [Creating the Jamf Pro Database Using the Jamf Pro Server Tools Command-Line Interface](#) Knowledge Base article.

Step 4: Connect to the Jamf Pro Server

1. Configure the database connection settings using Jamf Pro Server Tools GUI or CLI. For instructions, see the [Editing the Database Connection Using Jamf Pro Server Tools](#) Knowledge Base article.

2. Access Jamf Pro by opening a web browser and typing the protocol, IP address or hostname of the server, and port. For example: `https://jamf.mycompany.com:8443/`

Note: Some web browsers may initially prevent access to Jamf Pro on port 8443 and may produce an "invalid certificate" error. If this error occurs, do the following:

- a. Enter your Jamf Pro server URL in the web browser's address bar using "http" and port 8080 (e.g., "http://jamf.mycompany.com:8080").
- b. When prompted by the Jamf Pro setup assistant for the Jamf Pro URL, enter your Jamf Pro server URL using "https" and port 8443 (e.g., `https://jamf.mycompany.com:8443`).

You can begin using your Jamf Pro server URL to access Jamf Pro after you have uploaded a valid certificate and restarted Tomcat. For more information, see [SSL Certificate](#) in the *Jamf Pro Administrator's Guide*.

Step 5: Secure Your Jamf Pro Server

Secure your Jamf Pro server by following the recommendations in the [Jamf Pro Security Recommendations](#) Knowledge Base article.

Installed Files and Folders

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

Jamf Pro web app

The files that make up the Jamf Pro web app (formerly the JSS web app) are stored in the following location:

```
C:\Program Files\JSS\Tomcat\webapps\ROOT\
```

Apache Tomcat

Tomcat is the web application server that runs the Jamf Pro web app. A directory named Tomcat is installed in the following location:

```
C:\Program Files\JSS\
```

For more information about the version of Tomcat installed by the Jamf Pro Installer, see the [Apache Tomcat Versions Installed by the Jamf Pro Installer](#) Knowledge Base article.

server.xml

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

```
C:\Program Files\JSS\Tomcat\conf\
```

keystore

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

```
C:\Program Files\JSS\Tomcat\certs\
```

Jamf Pro Server Tools

Jamf Pro Server Tools, filename `server-tools-gui.jar`, is installed in the following location:

```
C:\Program Files\JSS\bin\
```

Jamf Pro Server Tools also has a command-line interface (CLI), filename `jamf-pro.exe`, that is installed in the same location.

Database backup location

By default, Jamf Pro Server Tools stores database backups in the following location:

```
C:\Program Files\JSS\Backups\Database\
```

Logs

Logs for the installation and for the Jamf Pro server (formerly the Jamf Software Server) are stored in the following location:

```
C:\Program Files\JSS\Logs\
```

Upgrading Jamf Pro Using the Installer

Upgrading Jamf Pro involves the following steps:

1. Prepare to upgrade.
2. Run the Jamf Pro Installer.

Note: The Jamf Pro Installer cannot be used to upgrade Jamf Pro 8.1 or earlier.

3. Finalize the upgrade and revert server settings.

Step 1: Prepare to Upgrade

1. Review the following Knowledge Base articles:
 - [Preparing to Upgrade Jamf Pro](#)
 - [Incremental Upgrade Scenarios for Jamf Pro 10.0.0 or Later](#)
2. Ensure that you have backed up the current database.
For more information, see [Backing Up the Database](#).
3. On Windows, ensure the following:
 - You are logged in as a local administrator, not as a domain administrator.

Note: Full local administrator privileges are required to install Jamf Pro on Windows Server. If you are unable to install Jamf Pro, Group Policy Object restrictions may be the cause. Check the GPO settings or contact someone in your organization who can ensure that GPO restrictions allow you full administrator privileges.

- Apache Tomcat is stopped.
For instructions, see the following Knowledge Base article:
[Starting and Stopping Tomcat](#)
4. If you are upgrading from Jamf Pro 10.15.0 or earlier and currently have MySQL 5.7.7 or earlier installed, follow the instructions in the [Upgrading to MySQL 8.0](#) Knowledge Base article to upgrade to MySQL 8.0.
 5. If you are upgrading from Jamf Pro 10.13.0 or earlier, follow the instructions in the [Migrating to Java 11](#) Knowledge Base article to migrate from Java 8 to Java 11.

Step 2: Run the Jamf Pro Installer

Important: If an upgrade fails, do not click **OK**. Contact your Jamf account representative immediately.

1. Copy the most current version of the Jamf Pro Installer for Windows (`Jamf Pro Installer.msi`) to the server.
2. To obtain the Jamf Pro Installer for Windows, log in to Jamf Nation and click **Show alternative downloads** below the Jamf Pro DMG on the following page:
<https://www.jamf.com/jamf-nation/my/products>
3. Double-click the installer and follow the onscreen instructions to complete the upgrade.

Important: If you are upgrading to Jamf Pro 10.6.0 or later, you must make a one-time change to the MySQL configuration to avoid performance issues. See "Step 2. Configure MySQL" in the [Creating the Jamf Pro Database Using the Jamf Pro Server Tools Command-Line Interface](#) Knowledge Base article for instructions.

Step 3: Verify Server Settings

1. Verify that the `Connector` settings for port 8443 in the `server.xml` file match the settings listed in the [Configuring Supported Ciphers for Tomcat HTTPS Connections](#) Knowledge Base article, and modify them if needed.
2. If you modified the `server.xml` file, restart Tomcat.

Step 4: Complete the Upgrade

Log in to Jamf Pro and verify devices are checking in as expected.

Note: Due to a display issue that occurs with Internet Explorer, it is recommended that you use Firefox, Chrome, or Safari.

Related Information

For related information, see the following Knowledge Base article:
[Manually Upgrading Jamf Pro on Windows](#)

Use the `ROOT.war` file to upgrade Jamf Pro instead of using the installer.

Manually Installing Jamf Pro

This section provides a basic set of steps for manually installing and configuring Jamf Pro on Windows Server.

Note: The supporting scripts and configuration used for manual installation differ from an installation using the Jamf Pro Installer for Windows. If you do not want to manually install Jamf Pro, you can use the Jamf Pro Installer for Windows. For information about obtaining the installer and installation instructions, see [Installing Jamf Pro Using the Installer](#).

Note: If you are upgrading to Tomcat 8.5, you will need to manually modify the `server.xml` file to make it compatible with Tomcat 8.5. For more information, see the [Server.xml Changes for Tomcat 8.5](#) Knowledge Base article. For instructions on manually upgrading Jamf Pro on Windows, see the [Manually Upgrading Jamf Pro on Windows](#) Knowledge Base article.

Requirements

The server used to host Jamf Pro should meet the minimum requirements for operating system, Tomcat version, database configuration, and Java installation. For additional information on these Jamf Pro Server Environment requirements, see "Jamf Pro System Requirements" in the [Jamf Pro Release Notes](#) for your version of Jamf Pro.

In addition, the following resources are recommended as the minimum allocation for a typical installation of Jamf Pro:

Windows

- A 64-bit capable Intel processor
- 8 GB of RAM
- 150 GB of disk space available
- Ports 8443 and 8080 available

In environments where the double-byte character set encoding is required, use English as the system language for the server used to host Jamf Pro to avoid potential display issues.

Full local administrator privileges are required to install Jamf Pro on Windows Server. If you are unable to install Jamf Pro, Group Policy Object restrictions may be the cause. Check the GPO settings or contact someone in your organization who can ensure that GPO restrictions allow you full administrator privileges.

Note: You will need to manually add a firewall exception for port 8443.

You must also obtain the following to manually install Jamf Pro:

- Jamf Pro web app (ROOT.war)—To obtain this item in the Jamf Pro manual installation archive, log in to Jamf Nation, click **Show alternative downloads**, then click the **Download** button below "Jamf Pro Manual Installation" on the following page:
<https://www.jamf.com/jamf-nation/my/products>
- Jamf Pro Server Tools Command-Line Interface (CLI)—Instructions for obtaining this item are provided below.

Note: Each installation of Jamf Pro and its required services is unique, and requirements, such as Jamf Pro web app memory, may vary depending on your implementation. For information about allocating additional memory to the Jamf Pro web app, see [Jamf Pro Web App Memory](#).

If you have questions regarding scaling your environment's resources beyond the typical recommendations, contact [Jamf Support](#).

Installation and Configuration

Follow the step-by-step instructions in this section to install and configure Jamf Pro on Windows Server.

Step 1: Install Java and MySQL

Java and MySQL must be installed on the server before you can create the Jamf Pro database and install Jamf Pro. For instructions, see the [Installing Java and MySQL for Jamf Pro 10.14.0 or Later](#) Knowledge Base article.

Step 2: Install Tomcat

Apache Tomcat is the web application server that runs Jamf Pro.

Jamf tests each version of Jamf Pro with the corresponding version of Tomcat listed in the [Apache Tomcat Versions Installed by the Jamf Pro Installer](#) Knowledge Base article. You are highly encouraged to install the version of Tomcat associated with the version of Jamf Pro you are installing.

The following instructions explain how to manually configure Tomcat to use a self-signed SSL certificate on port 8443.

1. In a web browser, open the Tomcat 8 download page:
<https://tomcat.apache.org/download-80.cgi>
2. If you need the latest version of Tomcat:
 - a. On the Tomcat 8 download page, navigate to **Tomcat 8.5.x > Binary Distributions > Core**.
 - b. Click the "32-bit/64-bit Windows Service Installer" link to download the installer.
3. If you need a previous version of Tomcat:
 - a. On the Tomcat 8 download page, navigate to the **Quick Navigation** section and click **Archives**.
 - b. Click the folder for the version of Tomcat that you want.
 - c. Click the `bin/` folder.

- d. Click the "apache-tomcat-8.5.x.exe" link to download the installer.
4. Launch the Apache Tomcat 8.5.x Windows Service Installer.
5. Follow the onscreen instructions, and choose "Minimum" from the **Select the type of install** pop-up menu.
6. Expand the option for **Tomcat** and select the **Service Startup** option to customize the install.

Note: Selecting the **Service Startup** option automatically starts Tomcat when the computer starts.

7. Click **Next** and use the default settings to configure the rest of the installation.

Step 3: Install the Jamf Pro Server Tools CLI

1. Download the Jamf Pro Server Tools CLI. For instructions, see the following Knowledge Base article: [Using the Jamf Pro Server Tools Command-Line Interface](#)
2. Open Command Prompt.
3. Configure the Tomcat directory by executing a command similar to the following:

```
jamf-pro config set --tomcat-dir "C:\Program Files\Apache Software Foundation\Tomcat 8.5"
```

4. Configure the Tomcat service by executing a command similar to the following:

```
jamf-pro config set --tomcat-service Tomcat8
```

It is highly recommended that you regularly create backups as you work toward a fully configured and operational Jamf Pro. For instructions, see [Backing Up the Database](#).

Note: You can also download the Jamf Pro Server Tools GUI by clicking the following link: <https://archive.services.jamfcloud.com/jamf-pro-server-tools/release/latest/gui/server-tools.jar>
For more information, see the [Jamf Pro Server Tools Overview](#) Knowledge Base article.

Step 4: Allocate Additional Memory to Tomcat

You can allocate additional memory to Tomcat by using one of the following methods:

- **Method 1:** Allocating Additional Memory to Tomcat Using the Jamf Pro Server Tools CLI

- a. Open Command Prompt.
- b. Set the minimum Tomcat memory by executing the following command:

```
jamf-pro server config set --min-memory 256M
```

- c. Set the maximum Tomcat memory by executing the following command:

```
jamf-pro server config set --max-memory 512M
```

- **Method 2:** Manually Allocating Additional Memory to Tomcat

The default Java Maximum Memory Pool for Tomcat on Windows is set to 256 MB. This should be increased to at least 512 MB. To accommodate a large number of computers in Jamf Pro, you will have to allocate additional Java Virtual Machine (JVM) memory to Tomcat. If other services are running on your server, make sure to leave enough memory to accommodate them.

- a. Open the Tomcat8w.exe application found in the "C:\Program Files\Apache Software Foundation\Tomcat 8.5\bin" path.
- b. Click the **Java** tab.
- c. Enter the amount of memory you want to allocate in the **Maximum Memory Pool** field.
- d. Click **Apply**.
- e. Open Command Prompt and start Tomcat by executing:

```
net start Tomcat8
```

The Tomcat service should be running and will automatically unpack the `ROOT.war` file into a `ROOT` directory in the `webapps` directory.

Step 5: Create the Jamf Pro Database

A MySQL database must be created before you can install Jamf Pro.

You can create the Jamf Pro database using one of the following methods:

- **Method 1:** Creating the Jamf Pro Database Using the Jamf Pro Server Tools CLI
Follow the instructions in the [Creating the Jamf Pro Database Using the Jamf Pro Server Tools Command-Line Interface](#) Knowledge Base article.
- **Method 2:** Manually Creating the Jamf Pro Database
Follow the instructions in the [Manually Creating the Jamf Pro Database](#) Knowledge Base article.

Step 6: Install Jamf Pro

1. (Optional) Create a `C:\temp\jamf` directory in which to temporarily store downloads, tools, and scripts for Jamf Pro by executing:

```
mkdir C:\temp\jamf
```

2. (Optional) Copy the `ROOT.war` file from the Jamf Pro manual download archive to the `C:\temp\jamf` directory that you just created.
3. Open Command Prompt.

4. Stop Tomcat by executing:

```
net stop Tomcat8
```

5. Rename the ROOT web app directory to something like TOMCAT in Windows Explorer or at the Command Prompt by executing a command similar to the following:

```
move "C:\Program Files\Apache Software Foundation\Tomcat 8.5\
webapps\ROOT" "C:\Program Files\Apache Software Foundation\
Tomcat 8.5\webapps\TOMCAT"
```

6. Copy the Jamf Pro ROOT.war web app to the Tomcat webapps directory in Explorer or at the Command Prompt by executing a command similar to the following:

```
copy C:\temp\jamf\ROOT.war "C:\Program Files\Apache
Software Foundation\Tomcat 8.5\webapps\"
```

7. Generate a keystore to enable SSL for Tomcat by executing a command similar to the following:

```
"C:\Program Files\Amazon Corretto\jdk11.0.3_7\bin\keytool.exe" -
genkey -alias tomcat -keyalg RSA -keypass "changeit" -storepass
"changeit" -dname "CN=jamf.mycompany.com, OU=Jamf IT, O=Jamf,
L=Minneapolis, ST=MN, C=US" -keystore "C:\Program Files\Apache
Software Foundation\Tomcat 8.5\keystore" -validity <numdays>
```

Make sure to change the following attributes as appropriate to your site:

| Attribute | Value | Example |
|-----------|---|--------------------|
| CN= | Fully qualified domain name of the server | jamf.mycompany.com |
| OU= | Organizational unit | Jamf IT |
| O= | Organization | Jamf |
| L= | Location (city or office) | Minneapolis |
| ST= | State, province, or county | MN |
| C= | Country or region | US |

8. Back up the Tomcat server.xml configuration file by executing a command similar to the following:

```
copy "C:\Program Files\Apache Software Foundation\Tomcat 8.5\conf\server.
xml" "C:\Program Files\Apache Software Foundation\Tomcat 8.5\conf\server.
xml.bak"
```

9. Open the `server.xml` configuration file.

Note: You can do this with Wordpad, as long as the file is saved as a plain text document named `server.xml`.

10. Locate the following comment section in the file (note that this is the Connector on port 8443 not the Connector on port 8443 with HTTP/2 section):

```
<!-- Define a SSL/TLS HTTP/1.1 Connector on port 8443
      This connector uses the NIO implementation.
      ...
-->
```

11. Replace the commented out (initial `<!--` and trailing `-->`) Connector tag immediately following the comment (shown in "a" below) with the Connector tag text shown in "b" below:

a.

```
<!-- Define a SSL/TLS HTTP/1.1 Connector on port 8443
      ...
-->
<!--
<Connector port="8443" ...
      ...
/>
-->
```

b.

```
<!-- Define a SSL/TLS HTTP/1.1 Connector on port 8443
      This connector uses the NIO implementation that requires the
      JSSE style configuration. When using the APR/native
      implementation, the OpenSSL style configuration is required
      as described in the APR/native documentation -->
<Connector URIEncoding="UTF-8"
  server="Apache Tomcat"
  port="8443"
  executor="tomcatThreadPool"
  SSLEnabled="true"
  maxPostSize="-1"
  scheme="https"
  protocol="org.apache.coyote.http11.Http11Nio2Protocol"
  sslImplementationName="org.apache.tomcat.util.net.jsse.
JSSEImplementation"
  secure="true">
  <SSLHostConfig sslProtocol="TLS"
    protocols="TLSv1.2"
    honorCipherOrder="true"
    certificateVerification="none"
    ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
      TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
      TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,
      TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
      TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
      TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,
      TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
      TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
      TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,
      TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,
      TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,
      TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,
      TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
      TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
      TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,
      TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,
      TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,
      TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,
      TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA" >
    <Certificate type="RSA"
      certificateKeystoreFile="C:\Program Files\Apache Software
Foundation\Tomcat 8.5\keystore"
      certificateKeystorePassword="changeit" />
  </SSLHostConfig>
</Connector>
```


12. Go back to Command Prompt, and add a rule to the `firewall` configuration to allow access to port 8443 by executing:

```
netsh advfirewall firewall add rule name=Jamf_Secure dir=in  
action=allow protocol=TCP localport=8443
```

13. Start Tomcat by executing the following command:

```
net start Tomcat8
```

Step 7: Connect to the Jamf Pro Server

1. Configure the database connection settings using Jamf Pro Server Tools GUI or CLI. For instructions, see the [Editing the Database Connection Using Jamf Pro Server Tools](#) Knowledge Base article.
2. Access Jamf Pro by opening a web browser and typing the protocol, IP address or hostname of the server, and port. For example: `https://jamf.mycompany.com:8443/`

Note: Some web browsers may initially prevent access to Jamf Pro on port 8443 and may produce an "invalid certificate" error. If this error occurs, do the following:

- a. Enter your Jamf Pro server URL in the web browser's address bar using "http" and port 8080 (e.g., "http://jamf.mycompany.com:8080").
- b. When prompted by the Jamf Pro setup assistant for the Jamf Pro URL, enter your Jamf Pro server URL using "https" and port 8443 (e.g., `https://jamf.mycompany.com:8443`).

You can begin using your Jamf Pro server URL to access Jamf Pro after you have uploaded a valid certificate and restarted Tomcat. For more information, see [SSL Certificate](#) in the *Jamf Pro Administrator's Guide*.

Step 8: Secure Your Jamf Pro Server

Secure your Jamf Pro server by following the recommendations in the [Jamf Pro Security Recommendations](#) Knowledge Base article.

jamf | PRO

Setup

Setting Up Jamf Pro

The first time you connect to the Jamf Pro server, the Jamf Pro Setup Assistant guides you through the following setup tasks:

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

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

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

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

Related Information

For related information, see the following Knowledge Base article:

[Network Ports Used by Jamf Pro](#)

Learn about the network ports that you may need to configure when setting up Jamf Pro.

Jamf Pro User Accounts and Groups

Jamf Pro is a multi-user application. Jamf Pro user accounts and groups allow you to grant different privileges and levels of access to each user.

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

- **Administrator**—Grants all privileges.
- **Auditor**—Grants all read privileges.
- **Enrollment Only**—Grants all privileges required to enroll computers and mobile devices.

Note: This includes privileges to do the following:

- Log in to the Jamf Pro interface
- Read, create, and delete enrollment invitations
- Read and delete computer and mobile device records via the Jamf Pro API

- **Custom**—Requires you to grant privileges manually. For a Custom user account or group to have access to a particular function, privileges may need to be granted for multiple objects. For example, to create a mobile device configuration profile, the user needs privileges for both “Mobile Devices” and “Mobile Device Configuration Profiles”.

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

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

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





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

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




General Requirements

To add accounts or groups from an LDAP directory service, you need an LDAP server set up in Jamf Pro. For more information, see “Integrating with LDAP Servers” in the *Jamf Pro Administrator’s Guide*.

Creating a Jamf Pro User Group

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **Jamf Pro User Accounts & Groups** .
5. Click **New** .
6. Do one of the following:
 - To create a standard Jamf Pro user group, select **Create Standard Group** and click **Next**.
 - To add a Jamf Pro user group from an LDAP directory service, select **Add LDAP Group** and click **Next**. Then follow the onscreen instructions to search for and add the group.
7. Use the Group pane to configure basic settings for the group.
8. If you chose "Custom" from the **Privilege Set** pop-up menu, click the **Privileges** tab and select the checkbox for each privilege that you want to grant the group.
9. Click **Save** .

Creating a Jamf Pro User Account

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **Jamf Pro User Accounts & Groups** .
5. Click **New** .
6. Do one of the following:
 - To create a standard Jamf Pro user account, select **Create Standard Account** and click **Next**.
 - To add a Jamf Pro user account from an LDAP directory service, select **Add LDAP Account** and click **Next**. Then follow the onscreen instructions to search for and add the account.
7. On the Account pane, enter information about the account as needed.

8. Choose an access level from the **Access Level** pop-up menu:

- To grant full access to Jamf Pro, choose "Full Access".
- To grant access to a site, choose "Site Access".

Note: The "Site Access" option is only displayed if there are sites in Jamf Pro. For more information on adding sites to Jamf Pro, see "Sites" in the *Jamf Pro Administrator's Guide*.

- To add the account to a standard group, choose "Group Access".

Note: The "Group Access" option is only displayed if there are standard groups in Jamf Pro. For more information on creating groups, see [Creating a Jamf Pro User Group](#).

9. Do one of the following:

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

10. Click **Save** .

Configuring Account Preferences

You can configure language & region, search, and interface preferences for each Jamf Pro user account. Language & region preferences allow you to configure settings such as date format and time zone. Search preferences allow you to configure settings for computer, mobile device, and user searches. Interface preferences allow you to configure whether or not Jamf Pro alerts you when navigating away from unsaved changes.

1. Log in to Jamf Pro.

2. At the top of the page, click the account settings  icon and then click **Account Preferences**.

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

4. Click the **Search Preferences** tab and use the pop-up menus to configure search preferences.

Note: The default search preference is "Exact Match". For most items, the option can be changed to either "Starts with" or "Contains".

5. Click the **Interface Preferences** tab and use the checkbox to configure the unsaved changes alert preference.





6. Click **Save** .

Configuring the Password Policy

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

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

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

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **Jamf Pro User Accounts & Groups** .
5. Click **Password Policy**.
6. Click **Edit** .
7. Use the settings on the pane to specify the password settings.
8. Click **Save** .

The settings are applied immediately.





Unlocking a Jamf Pro User Account

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

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

The access status of the account is displayed as “Disabled” in Jamf Pro until the account is unlocked.

1. Log in to Jamf Pro.

2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **Jamf Pro User Accounts & Groups** .
- A list of Jamf Pro user accounts and groups is displayed.
5. Click the Jamf Pro user account that has an access status of “Disabled”, which means the account is locked.
6. Click **Edit** .
7. Choose “Enabled” from the **Access Status** pop-up menu to unlock the account.
8. Click **Save** .

The Jamf Pro user account is unlocked immediately.

Related Information

For related information, see the following section in the *Jamf Pro Administrator's Guide*:

"Sites"





Learn about sites and how to add them to Jamf Pro.

Activation Code

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

Updating the Activation Code

Every time you receive a new activation code, it must be updated in Jamf Pro.

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **Activation Code** .
5. Click **Edit** .
6. Enter the new activation code.
7. Click **Save** .





Integrating with an SMTP Server

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

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




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

Configuring the SMTP Server Settings

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

Testing the SMTP Server Settings

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

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

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

Related Information

For related information, see the following sections in the *Jamf Pro Administrator's Guide*:

- "Email Notifications"
Learn about the different email notifications that can be sent to Jamf Pro users.
- "User-Initiated Enrollment for Computers"
Find out how to send computer enrollment invitations via email.
- "User-Initiated Enrollment for Mobile Devices"
Find out how to send mobile device enrollment invitations via email.
- "Performing Mass Actions for Computers"
Find out how to send a mass email to computer users.
- "Performing Mass Actions for Mobile Devices"
Find out how send a mass email to mobile device users.

Change Management

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

The Change Management logs can also be viewed in Jamf Pro. The information displayed includes:

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

In addition, you can view the changes to a specific object in that object's history.

Note: The option to log changes to a log file or a syslog server is only available for on-premise environments. If your environment is hosted in Jamf Cloud, changes are automatically displayed in the Change Management settings and cannot be exported.



For more information, see "Viewing the History of a Jamf Pro Object" in the *Jamf Pro Administrator's Guide*.



General Requirements

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



Configuring the Change Management Settings for On-Premise Environments

The option to configure the Change Management settings is only available for on-premise environments. If your environment is hosted in Jamf Cloud, changes are automatically displayed in the Change Management settings.

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **Change Management** .

5. Click **Edit** .
6. Configure the settings on the pane.
7. Click **Save** .

Viewing Change Management Logs in Jamf Pro

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **Change Management** .
The Change Management logs are displayed on the pane.
5. Do one of the following:
 - To view the object associated with a change, click the object in the Object Name column.
 - To view details about the change, click **Details** in the Details column.

GSX Connection

The GSX Connection settings allow you to integrate Jamf Pro with Apple's Global Service Exchange (GSX) to look up and populate the following purchasing information for computers and mobile devices:

- Purchase date
- Warranty expiration date

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

To integrate Jamf Pro with GSX, you must first create a GSX account and obtain a certificate from Apple. Then you can configure the GSX Connection settings in Jamf Pro, which involves entering GSX account information, retrieving an API token from Apple, and uploading the Apple certificate.

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

Configuring the GSX Connection Settings




Requirements

To configure the GSX Connection settings, you need:

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

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


Procedure

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **Global Management**.
4. Click **GSX Connection** .
5. Click **Edit** .
6. Select **Enable Connection to GSX**.

Note: This setting and others on this pane may already be configured if Jamf Pro was used to generate a CSR.




7. Enter the username and account number, including the leading zeros, for the GSX account.
8. Provide your API token in the **API Token** field by doing the following:
 - a. Click the “Log in to your Apple GSX account” link below the **API Token** field.
 - b. Log in to your Apple GSX account.
 - c. Click **Copy to clipboard** to copy your API Token.
 - d. In Jamf Pro, paste your API Token into the **API Token** field.

Note: The API token is not displayed after you finish configuring the GSX connection or when you edit an existing GSX connection. This is because the API token changes with every request and will always be different.

9. In the Certificate-based Authentication section, click **Upload**.
10. The **URI** field will be populated automatically.
11. Follow the onscreen instructions to upload the Apple certificate (.pem or .p12).
12. Click **Save** .

Testing the GSX Connection

After the GSX Connection settings are configured, you can test the connection to verify it works.

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **Global Management**.
4. Click **GSX Connection** .
5. Click **Test** .
6. Click **Test** again.




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

A successful connection will display information similar to the following:

```
[Accept: application/json, Content-Type: application/json, X-Apple-SoldTo: 0000000000, X-Apple-ShipTo: 0000000000] GET https://partner-connect.apple.com/gsx/api/authenticate/check HTTP/1.1  
Response: OK
```

Renewing the Apple Certificate

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

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

Related Information

For related information, see the following sections in the *Jamf Pro Administrator's Guide*:

- "Performing Mass Actions for Computers"
Find out how to mass look up and populate purchasing information from GSX.
- "Performing Mass Actions for Mobile Devices"
Find out how to mass look up and populate purchasing information from GSX.
- "Mobile Device Inventory Information"
You can look up and populate purchasing information for a single mobile device by editing the device's inventory information in Jamf Pro.
- "Computer Inventory Information"
You can look up and populate purchasing information for a single computer by editing the computer's inventory information in Jamf Pro.
- "Local Enrollment Using Recon"
Find out how to look up and populate purchasing information when enrolling a computer by running Recon locally.
- "Remote Enrollment Using Recon"
Find out how to look up and populate purchasing information when enrolling a computer by running Recon remotely.

Jamf Pro Summary

The Jamf Pro Summary is a custom report that can be useful for troubleshooting Jamf Pro issues, and for providing information to Jamf for purposes of support or license renewal.

By default, the Jamf Pro Summary includes the following information:



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

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

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

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

Viewing the Jamf Pro Summary

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **Jamf Pro Information**.
4. Click **Jamf Pro Summary** .
5. Select the checkboxes next to the items you want to include.
6. Click **Create**.
The Jamf Pro Summary displays in a browser window.
7. Click the **Back** button in the web browser to return to the Jamf Pro Summary pane.



Sending the Jamf Pro Summary to Jamf

Requirements

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

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

Procedure

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **Jamf Pro Information**.
4. Click **Jamf Pro Summary** .
5. Select the checkboxes next to the items you want to include.
6. Click **Send Summary to Jamf**.
7. Enter your Jamf Nation credentials, and then click **Send**.

The Jamf Pro Summary is sent to Jamf via Jamf Nation.

Related Information

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

[Customer Experience Metrics](#)

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

For related information about Customer Experience Metrics, visit the following webpage:

<https://www.jamf.com/products/jamf-pro/customer-experience-metrics/>

jamf | PRO

Database Management

Backing Up the Database

You can create database backups as needed or schedule automated database backups using Jamf Pro Server Tools.

Note: The time it takes to create a backup depends on the size of the database.

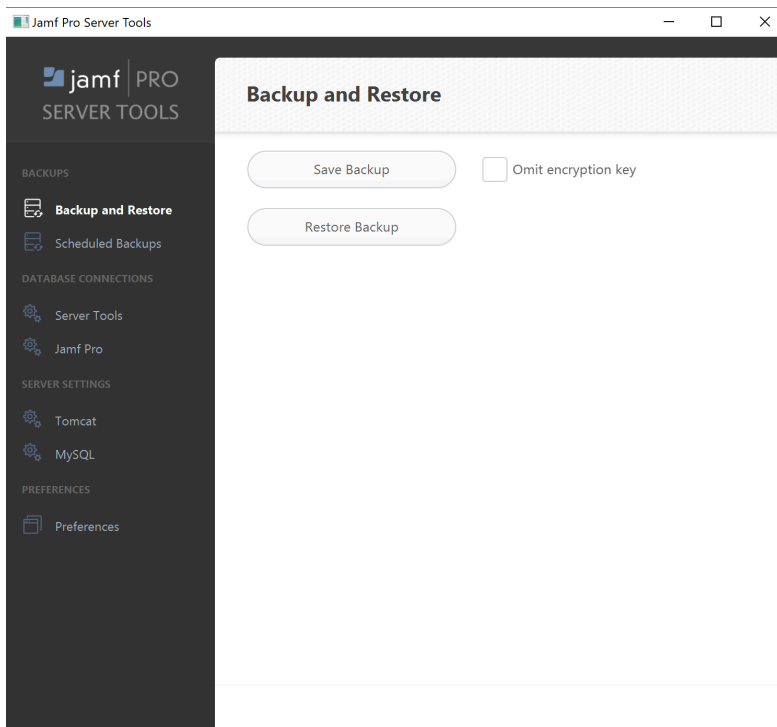
Creating a Database Backup

1. Open the Jamf Pro Server Tools GUI by performing the following steps:
 - a. Open a command terminal and enter the following but do not press Enter:

```
java -jar
```

- b. Drag the Jamf Pro Server Tools .jar file into the window. This will add the .jar file path to the `java -jar` command.
 - c. Press Enter.
2. Click **Database Connection** in the sidebar.
3. Configure the settings to match your database configuration, and then click **Test Connection**.
 - If successful, the message "Successfully Connected" appears. Continue with Step 4 below.
 - If the connection is not successful, an error message will appear.
4. Click **Backup and Restore** in the sidebar.

5. Click **Save Backup**.



6. Choose a location to save the backup and click **Open**.

Jamf Pro Server Tools saves the backup as a `.sql.gz` file.

Scheduling Database Backups

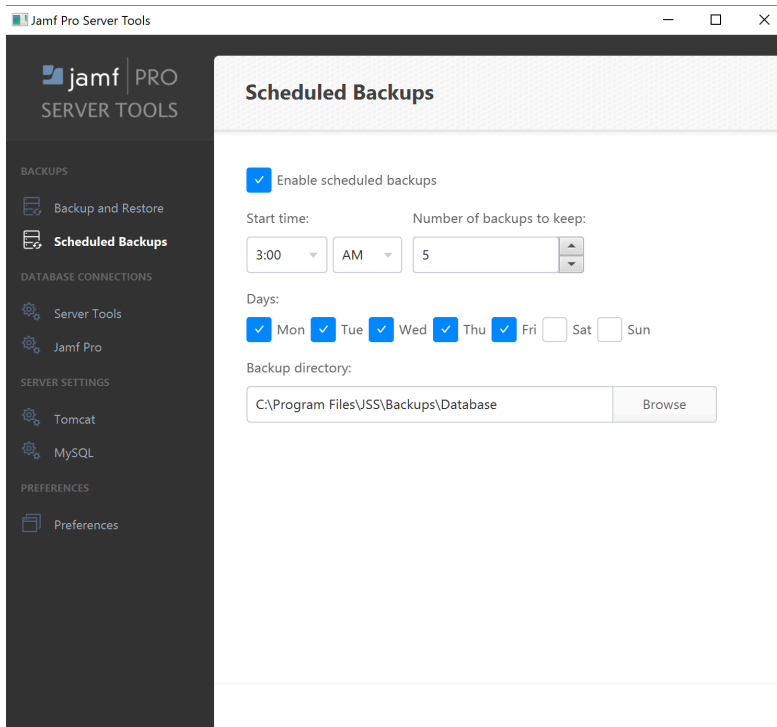
You can schedule database backups to occur on an ongoing basis. You can also automate the deletion of scheduled backup files that are older than a specified number of days.

1. Open the Jamf Pro Server Tools GUI by performing the following steps:
 - a. Open a command terminal and enter the following but do not press Enter:

```
java -jar
```

- b. Drag the Jamf Pro Server Tools `.jar` file into the window. This will add the `.jar` file path to the `java -jar` command.
 - c. Press Enter.
2. Click **Scheduled Backups** in the sidebar.
 3. Select the **Enable scheduled backups** checkbox.
 4. If prompted, enter your Jamf Pro Server Tools configuration password.
 5. Choose the hour and the days that you want backups to occur.

- To automatically delete old backups, enter the number of most-recent backups that you want to keep in the **Backups limit** field. All older backup files will be deleted when the scheduled backups run. To retain all backups, enter "0".
- To save the backups in a custom location, click **Browse** and select a new location. It is recommended that you store the backups on a separate drive.

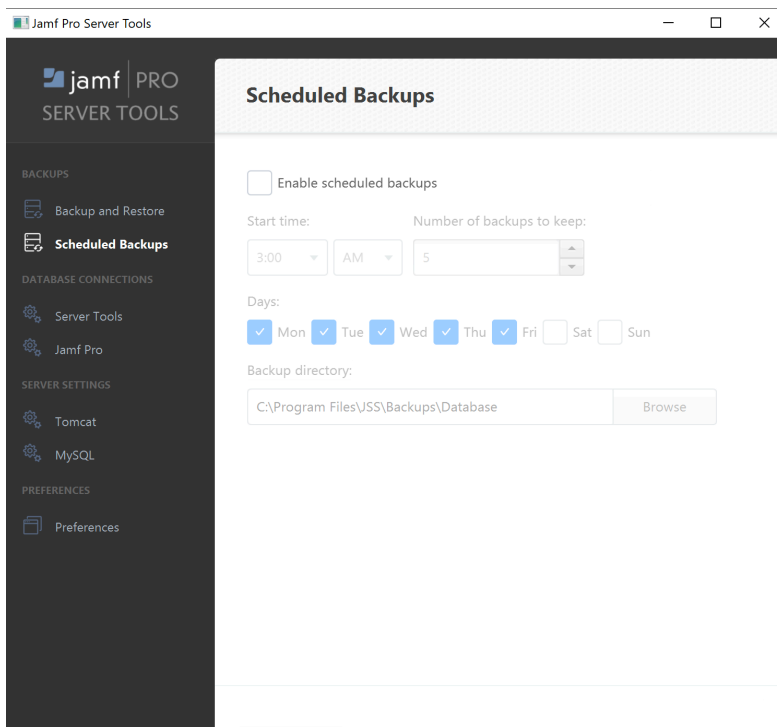


Stopping Scheduled Database Backups

1. Open the Jamf Pro Server Tools GUI by performing the following steps:
 - a. Open a command terminal and enter the following but do not press Enter:

```
java -jar
```

- b. Drag the Jamf Pro Server Tools .jar file into the window. This will add the .jar file path to the `java -jar` command.
 - c. Press Enter.
2. Click **Scheduled Backups** in the sidebar.
 3. Deselect the **Enable scheduled backups** checkbox.



Jamf Pro Server Tools immediately stops creating scheduled backups.

Related Information

For related information, see the following Knowledge Base articles:

- [Jamf Pro Server Tools Overview](#)
- [Backing Up and Restoring the Database Using the Jamf Pro Server Tools Command-Line Interface](#)

Restoring Database Backups

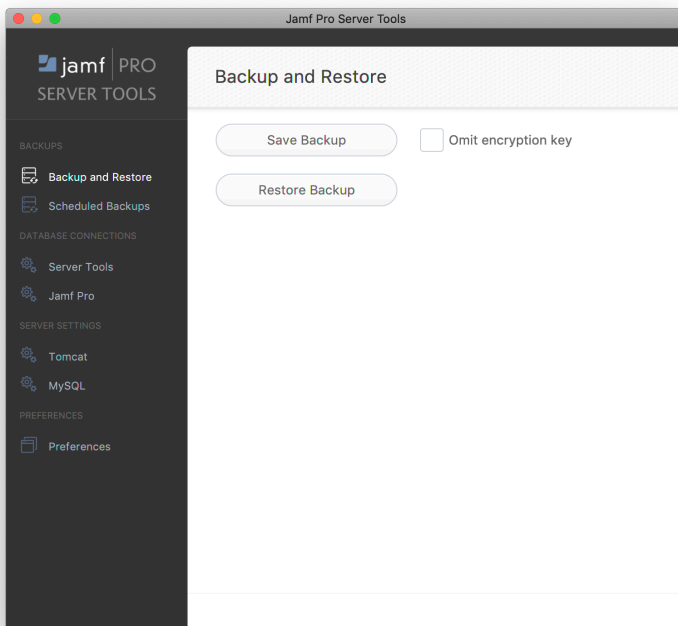
If you need to revert to an earlier version of your database, you can restore a database backup using Jamf Pro Server Tools.

Note: You must stop Tomcat before you restore a database backup.

1. Open the Jamf Pro Server Tools GUI by performing the following steps:
 - a. Open a command terminal and enter the following but do not press Enter:

```
java -jar
```

- b. Drag the Jamf Pro Server Tools .jar file into the window. This will add the .jar file path to the `java -jar` command.
 - c. Press Enter.
2. Click **Tomcat Settings** in the sidebar.
 3. Click **Stop Tomcat**.
 4. Click **Backup and Restore** in the sidebar.
 5. Click **Restore Backup Now**.



6. Select the backup file that you want to restore, and click **Open**.
7. Click **Tomcat Settings** in the sidebar.

8. Click **Start Tomcat**.

The existing database is replaced with the database backup that you selected.



Related Information

For related information, see the following Knowledge Base articles:

- [Jamf Pro Server Tools Overview](#)
- [Backing Up and Restoring the Database Using the Jamf Pro Server Tools Command-Line Interface](#)

Viewing the Status of Database Tables

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

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **Jamf Pro Information**.
4. Click **Database Table Summary** .

jamf | PRO

Server Infrastructure

About Distribution Points

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

- Packages
- Scripts
- In-house apps
- In-house books

Jamf Pro supports two types of distribution points:

- File share distribution points
- A cloud distribution point

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

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

Note: On computers with macOS 10.15 or later that do not have an MDM profile, you must use an HTTP, HTTPS, or cloud distribution point to install packages.

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

| | File Share Distribution Point | Cloud Distribution Point |
|---|---|--|
| Description | Standard server that is configured to be a distribution point | Distribution point that uses one of the following content delivery networks (CDNs) to host files: <ul style="list-style-type: none">▪ Rackspace Cloud Files▪ Amazon Web Services▪ Akamai |
| Maximum Number per Jamf Pro Instance | Unlimited | One |

| | File Share Distribution Point | Cloud Distribution Point |
|--------------------------------------|---|--|
| Server /Platform Requirements | Any server with an Apple Filing Protocol (AFP) or Server Message Block (SMB) share Note: File share distribution points cannot be mounted and hosted on the same server. | None |
| Protocol | AFP, SMB, HTTP, or HTTPS | HTTPS |
| Ports | <ul style="list-style-type: none"> ▪ AFP: 548 ▪ SMB: 139 ▪ HTTP: 80 ▪ HTTPS: 443 | 443 |
| Authentication Options | <ul style="list-style-type: none"> ▪ AFP or SMB: <ul style="list-style-type: none"> ▪ No authentication ▪ Username and password ▪ HTTP or HTTPS: <ul style="list-style-type: none"> ▪ No authentication ▪ Username and password | None |
| Files that Can Be Hosted | Packages | <ul style="list-style-type: none"> ▪ Packages ▪ In-house apps ▪ In-house books |
| Parent-Child Capabilities | No | No |
| File Replication Method | Replication to file share distribution points must be initiated from Jamf Admin. | Replication to a cloud distribution point must be initiated from Jamf Admin. |
| Selective Replication | Not available when replicating to file share distribution points. | Available when replicating to a cloud distribution point if the principal distribution point is a file share distribution point. The files for replication must be specified in Jamf Pro and the replication initiated from Jamf Admin. |

Related Information

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

- [File Share Distribution Points](#)
Find out how to manage file share distribution points in Jamf Pro.
- [Cloud Distribution Point](#)
Find out how to manage the cloud distribution point.

File Share Distribution Points

A server with an AFP or SMB share can be used as a file share distribution point. Before you can use a file share distribution point with Jamf Pro, you must set up the distribution point and add it to Jamf Pro.

Note: A server with an AFP share cannot share files on the Apple File System (APFS), which is the default file system for computers with macOS 10.13 or later. Computers with macOS 10.13 or later that are HFS+ formatted can still support AFP. If you need a file share distribution point for APFS formatted computers, SMB is an option.





For more information on APFS and SMB, see Apple's [Deployment Reference for Mac](#).

For information on setting up a file share distribution point, see the [Setting Up a File Share Distribution Point](#) Knowledge Base article.

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

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

Adding a File Share Distribution Point

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

Replicating Files to a File Share Distribution Point

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

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

Related Information

For related information, see the following section in the *Jamf Pro Administrator's Guide*:

“Network Segments”

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

For related information, see the following Knowledge Base articles:

- [Setting Up a File Share Distribution Point on Linux Using Samba](#)
Find out how to use Samba to set up a file share distribution point with an SMB share on a Linux server.
- [Using Apache HTTP Server to Enable HTTP Downloads on a Linux File Share Distribution Point](#)
Find out how to use Apache HTTP Server to enable HTTP downloads on a Linux file share distribution point.
- [Using IIS to Enable HTTPS Downloads on a Windows Server 2016 or 2019 File Share Distribution Point](#)
Find out how to activate Internet Information Services (IIS) and use it to enable HTTPS downloads on a Windows Server 2016 or 2019 file share distribution point.

Cloud Distribution Point

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

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

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

Note: If you plan to use the JCDS for your cloud distribution point, it is recommended that you do not attempt to upload files larger than 20 GB. Due to the file size download limit set by Amazon CloudFront, files larger than 20 GB may not download successfully. For more information, see the following website:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cloudfront-limits.html>

Jamf Pro supports the use of signed URLs created with Amazon CloudFront. It also supports Akamai Remote Authentication. For more information about signed URLs created with CloudFront, see the following website:

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html>

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

General Requirements





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

Note: If you have upgraded from Jamf Pro 8.x, you must migrate the scripts and packages on your principal distribution point before configuring the cloud distribution point. For more information, see the [Migrating Packages and Scripts](#) Knowledge Base article.

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




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

Configuring the Cloud Distribution Point

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **Server Infrastructure**.
4. Click **Cloud Distribution Point** .
5. Click **Edit** .
6. Choose a content delivery network from the **Content Delivery Network** pop-up menu.
7. Configure the settings on the pane.
8. Click **Save** .

Testing the Cloud Distribution Point

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

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **Server Infrastructure**.
4. Click **Cloud Distribution Point** .
5. Click **Test** .
6. Click **Test** again.

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

Replicating Files to the Cloud Distribution Point

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

1. Open Jamf Admin and authenticate to the Jamf Pro server.
2. In the sidebar, select the cloud distribution point you want to replicate files to.
3. Click **Replicate**.

Related Information

For related information, see the following section in the *Jamf Pro Administrator's Guide*:

“Network Segments”

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

[Information Required to Configure a Cloud Distribution Point in Jamf Pro](#)

Learn about the information that must be obtained from your cloud services provider to configure the cloud distribution point in Jamf Pro.

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

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

Jamf Infrastructure Manager Instances

A Jamf Infrastructure Manager instance is a service that is managed by Jamf Pro. It can be used to host the following:

- **LDAP Proxy**—This allows traffic to pass securely between Jamf Pro and an LDAP directory service. The Infrastructure Manager and the LDAP Proxy typically reside within the DMZ. The LDAP Proxy requires integration with an LDAP directory service. For more information, see "LDAP Proxy" in the *Jamf Pro Administrator's Guide*.
- **Healthcare Listener**—This allows traffic to pass securely from a healthcare management system to Jamf Pro. For more information, see "Healthcare Listener" in the *Jamf Pro Administrator's Guide*.

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

For more information, see the [Jamf Infrastructure Manager Installation Guide](#).



Managing a Jamf Infrastructure Manager Instance

You can use Jamf Pro to edit or delete an Infrastructure Manager instance. When editing an Infrastructure Manager instance, only the display name and recurring check-in frequency can be changed.

Note: The default check-in frequency at which the Infrastructure Manager instance checks in with Jamf Pro is 30 seconds.

Jamf Pro also displays the following inventory information for each Infrastructure Manager instance:

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

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **Server Infrastructure**.
4. Click **Infrastructure Managers**  .
A list of Infrastructure Manager instances is displayed along with the services that are installed on each instance.
5. Click the Infrastructure Manager instance you want to manage.

Notes:

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

Related Information

For related information, see the following section in the *Jamf Pro Administrator's Guide*:

"Email Notifications"

Learn how to enable an email notification in the event that an Infrastructure Manager instance does not check in with Jamf Pro.

jamf | PRO

Advanced Configuration

SSL Certificate

Jamf Pro requires a valid SSL certificate to ensure that computers and mobile devices communicate with the Jamf Pro server and not an imposter server.

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




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

Creating or Uploading an SSL Certificate

Requirements

To create or upload an SSL certificate, Jamf Pro must be installed as the “ROOT” web app, and the user running the Tomcat process must have read/write access to Tomcat’s `server.xml` file.

Procedure

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **Apache Tomcat Settings** .
5. Click **Edit** .
6. Select **Change the SSL certificate used for HTTPS** and click **Next**.
7. Follow the onscreen instructions to upload or create an SSL certificate.
8. Restart Tomcat for the changes to take effect.
For instructions, see the [Starting and Stopping Tomcat](#) Knowledge Base article.

Related Information

For related information, see the following Knowledge Base article:

[Using OpenSSL to Create a Certificate Keystore for Tomcat](#)

Find out how to use OpenSSL to create a certificate keystore that you can upload to Jamf Pro.



Configuring Tomcat to Work with a Load Balancer

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

Requirements

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

Configuring Load Balancing Settings

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **Apache Tomcat Settings** .
5. Click **Edit**.
6. Select **Configure Tomcat for working behind a load balancer** and click **Next**.
7. Follow the onscreen instructions to configure the Load Balancing settings.
8. Restart Tomcat for the changes to take effect.
For instructions on how to restart Tomcat, see the following Knowledge Base article: [Starting and Stopping Tomcat](#)



Tomcat Thread Pool Settings

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

Requirements

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

Configuring Tomcat Thread Pool Settings

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **Apache Tomcat Settings** .
5. Click **Edit**.
6. Select **Update the settings for Tomcat's thread pool** and click **Next**.
7. Follow the onscreen instructions to configure the Thread Pool settings.
8. Restart Tomcat for the changes to take effect.
For instructions on how to restart Tomcat, see the following Knowledge Base article: [Starting and Stopping Tomcat](#)



Jamf Pro Web App Memory

Jamf Pro allows you to view the amount of memory being used by the web app. If you need to change the amount of memory allocated to the web app, you can use Jamf Pro Server Tools.

Note: To improve the user experience, or if your Tomcat server is experiencing problems with instability, you may want to increase the memory allocated to Tomcat. Depending on your environment and Jamf Pro configuration (such as the number of managed devices, check-in frequency, or actions performed by the server), you may need to increase the amount of memory assigned to Tomcat. Each environment is different. Consult your system administrator for monitoring and scaling your environment.

If you decide to allocate more memory to Tomcat, ensure that enough memory remains available for the operating system to perform normally. If other services, such as MySQL, are running on the same hardware as Tomcat, ensure enough memory is available to operate all running services, or consider moving those services to a separate dedicated server.

Viewing Memory Usage

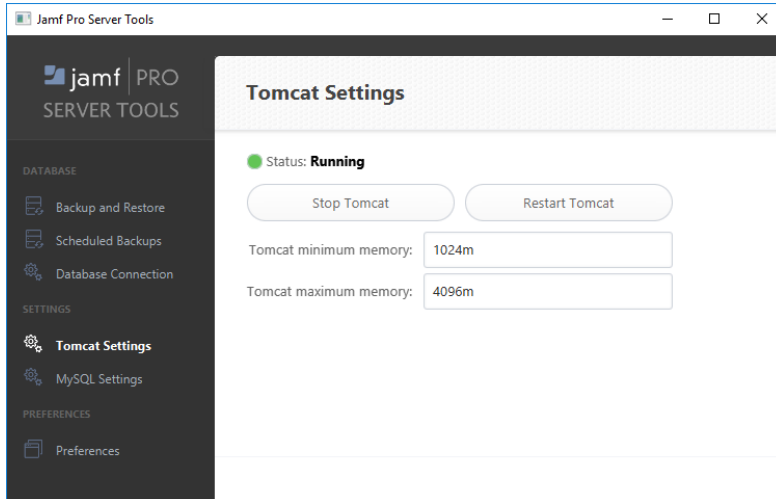
1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **Jamf Pro Information**.
4. Click **Memory Usage** .
Current free and used memory values are displayed.

Configuring Web App Memory Using Jamf Pro Server Tools

1. Open Jamf Pro Server Tools on the Jamf Pro host server. Jamf Pro Server Tools is located in:
`C:\Program Files\JSS\bin\server-tools-gui.jar`
2. Select **Tomcat Settings**.

3. Enter values in the **Tomcat minimum memory** and **Tomcat maximum memory** fields to configure the amount of memory allocated to the web app.

Note: Type an "m" after the memory value to specify megabytes, e.g., "256m".



4. Restart Tomcat. The changes will take effect after Tomcat restarts.

Configuring Web App Memory Using the Tomcat Monitor Application

1. Open the Tomcat monitor application, located at: C:\Program Files\JSS\Tomcat\bin\tomcat8w.exe
2. In the Apache Tomcat 8.5 Properties window, click the **Java** tab.
3. In the **Maximum memory pool** field, enter the amount of memory you want to allocate to Tomcat, and then click **Apply**.
4. Click the **General** tab, and then click the **Stop** and **Start** buttons to restart Tomcat and apply the changes.

Clustering

A clustered environment is one that has multiple instances of the Jamf Pro web app pointing to the same database. Clustering is useful in large environments that require multiple web apps, or environments with a web app in the DMZ.

When setting up a clustered environment, it is recommended that you configure the Clustering settings in Jamf Pro using the web app that you plan to make the primary, and then install other Jamf Pro web apps that point to the same database. However, if you already have multiple Jamf Pro web apps installed and pointed to the same database, you can configure the Clustering settings in Jamf Pro after the fact. For more information on setting up a clustered environment, contact your Jamf account representative.

The Clustering settings in Jamf Pro allow you to configure the frequency at which clustered web apps are synced with the database, and specify which web app should function as the primary.

The primary web app handles tasks such as upgrading the database schema and flushing logs from the database.

Jamf Pro also allows you to view a list of web apps that are pointed to the same database and information about them.




Requirements


To cluster web apps that are not in the DMZ, you need a load balancer with the address of the Jamf Pro server (formerly the Jamf Software Server). For example:

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

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

Configuring Clustering Settings

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **Clustering** .
5. Click **Edit** .
6. Configure the settings on the pane.
To specify which web app should function as the primary, select the **Primary** option for the web app.

7. Click **Save** .
8. If you already have multiple Jamf Pro web apps pointed to the same database, restart Tomcat on any of the web apps for the changes to take effect.
For instructions on how to restart Tomcat, see the [Starting and Stopping Tomcat](#) Knowledge Base article.

Related Information

For related information, see the following Knowledge Base articles:

[Caching Configuration](#)

Find out how to configure distributed caching for clustered Jamf Pro environments.

[Installing a Jamf Pro Web App in the DMZ](#)

Find out how to install a web app in the DMZ, and learn when in the process you should configure the Clustering settings in Jamf Pro.




Limited Access Settings

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

For each Jamf Pro web app, you can choose one of the following Limited Access settings:

- Full Access
- Computer and Mobile Device Access
This setting disables the Jamf Pro interface.

Configuring the Limited Access Settings

1. Log in to any of the Jamf Pro web apps.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **Limited Access** .
5. Select a setting for each Jamf Pro web app as needed.
6. Click **Save** .

Flushing Logs





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

- Application Usage logs
- Computer Usage logs
- Policy logs
- Jamf Remote logs
- Screen sharing logs
- Jamf Imaging logs
- Computer and mobile device management history
- Computer inventory reports (computer inventory information from past inventory submissions)
- Mobile device inventory reports (mobile device inventory information from past inventory submissions)
- Jamf Pro access logs
- Change Management logs
- Event logs
- User and Location History
- User Reports





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

For information on the types of data flushed with each log and the database tables affected, see the [Data and Tables Affected by Log Flushing](#) Knowledge Base article.

Scheduling Log Flushing

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **Log Flushing** .
5. Click **Edit** .
6. Use the pop-up menus to choose the number of days, weeks, or months after which each type of log should be flushed.
7. Choose a time of day from the **Time to Flush Logs Each Day** pop-up menu.
8. Click **Save** .

Manually Flushing Logs

1. Log in to any of the Jamf Pro web apps.
2. In the top-right corner of the page, click **Settings** .
3. Click **System Settings**.
4. Click **Log Flushing** .
5. Click **Flush** .
6. Select the checkbox for each type of log you want to flush.
7. From the **Flush Logs Older Than** pop-up menu, choose the number of days, weeks, or months after which logs should be flushed.
8. Click **Flush** .

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

Related Information

For related information, see the following sections in the *Jamf Pro Administrator's Guide*:

- "Computer History Information"
Find out how to view the logs and the management history for a computer.
- "Policy Management"
Find out how to view and flush policy logs for a computer.
- "Mobile Device History Information"
Find out how to view the management history for a mobile device.

Migrating to Another Server

Instructions on how to migrate Jamf Pro to a new host server are now provided in the [Migrating to Another Server](#) Knowledge Base article.