jamf | PRO

Security Overview

15 September 2020

jamf

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

Contents

Jamf Pro

Overview

Jamf Pro is an endpoint management solution for institutionally owned Mac, iPhone, iPad, and Apple TV devices, and personally owned iOS devices.

Jamf Pro includes the following components:

- The Jamf Pro server
- Device management framework
- Content distribution
- Jamf Pro apps for Mac computers:
  - **Jamf Admin**—Jamf Admin is a repository that allows you to add and manage packages, scripts, printers, and Dock items. It also allows you to create configurations (images) using these items and replicate files to distribution points.
  - **Jamf Imaging**—Jamf Imaging allows you to image computers by deploying configurations to them.

    Disclaimer: Imaging workflows are no longer recommended. Apple does not recommend or support monolithic system imaging as an installation method because of recent improvements in macOS security, hardware, management, and deployment. Apple encourages IT administrators to convert from device imaging to Automated Device Enrollment (formerly DEP) workflows.

  - **Jamf Remote**—Jamf Remote allows you to immediately perform remote management tasks on computers, such as installing packages, running scripts, and binding to directory services.

    Disclaimer: Using Jamf Remote for remote management workflows is no longer recommended. Because of increased user data protections with macOS 10.14 or later, you cannot enable remote management remotely using the SSH protocol. To enable remote management on computers with macOS 10.14, the user must select the **Screen Sharing** checkbox in System Preferences.

  - **Composer**—Composer allows you to build packages (PKG or DMG) of software, applications, preference files, or documents. Composer also allows you to build a DMG of an operating system.
  - **Recon**—Recon allows you to enroll Mac computers locally or remotely (either single device or using the network scanner), or create a QuickAdd package for enrollment.
- **Jamf Self Service for iOS**—Jamf Self Service for iOS allows you to distribute configuration profiles, apps, and books to iOS devices for users to install.

- **Jamf Pro Server Tools**—Jamf Pro Server Tools allows you to perform, schedule, and restore database backups, as well as manage settings for the database connection, Apache Tomcat, and MySQL. You can also use Jamf Pro Server Tools to convert the MySQL database storage engine from MyISAM to InnoDB. Jamf Pro Server Tools is available as a command-line interface and a GUI. The following components are included:
  - `jamf-pro`—The command-line interface for executing command-based tasks.
  - `server-tools.jar`—The GUI to `jamf-pro`.

For related information, see the Applications and Utilities section in the *Jamf Pro Administrator's Guide*.

Data Collection

Information Collected for Computers

Computers can submit many types of inventory information to Jamf Pro. Basic inventory information—such as hardware, operating system, user and location information, security reporting, storage, and applications—is collected automatically.

The Computer Inventory Collection settings in Jamf Pro allow you to collect the following additional items:

- Local user accounts
- Printers
- Active services
- Last backup date/time for managed mobile devices that are synced to computers
- User and location from an LDAP directory service (only available if an LDAP server is set up in Jamf Pro)
- Package receipts
- Available software updates
- Application Usage information
- Fonts
- Plug-ins

You can also collect FileVault 2 information, including:

- Individual recovery keys (if enabled in Jamf Pro using a disk encryption configuration or redirected to Jamf Pro using a macOS configuration profile)
- List of FileVault 2 enabled users
- Presence of an institutional recovery key
- Individual recovery key validation (validity is checked during every inventory submission)

Information can also be collected using computer extension attributes, which are custom fields that allow for the collection of almost any type of data from a computer.

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

- Computer Inventory Collection Settings
- Computer Extension Attributes
- Computer Inventory Information

Information Collected for Institutionally Owned Mobile Devices

Jamf Pro stores detailed inventory information for each managed mobile device.

You can view the following information for each institutionally owned mobile device:

- Hardware information, including UDID, serial number, MAC address, model, and capacity
- Operating system information
- Installed apps
- Installed configuration profiles.

Information can also be collected using mobile device extension attributes, which are custom fields that allow for the collection of almost any type of data from an institutionally owned mobile device.

Information Collected for Personally Owned Mobile Devices

Jamf Pro stores a limited set of inventory details for each personally owned mobile device.

You can view the following information for each personally owned mobile device:

- Hardware information, including UDID, serial number, MAC address, model, and capacity
- Operating system information
- Managed apps installed by Jamf Pro
- Configuration profiles installed by Jamf Pro

Mobile device extension attributes do not apply to personally owned mobile devices.

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

- Mobile Device Inventory Collection Settings
- Mobile Device Extension Attributes
- Mobile Device Inventory Information

Information Shared with Microsoft Intune

When the connection between Jamf Pro and Microsoft Intune is successfully established, Jamf Pro sends inventory information to Microsoft Intune for each computer that has been registered with Azure AD. You can view Azure Active Directory ID information for a user and a computer in the Local User Account category of a computer's inventory information in Jamf Pro. For detailed information on the inventory attributes sent to Microsoft Intune, see the "Appendix: Inventory Information Shared with Microsoft Intune" section of the Integrating with Microsoft Intune to Enforce Compliance on Macs Managed by Jamf Pro technical paper.

Note: Inventory information is not shared with Microsoft Intune unless the macOS Intune Integration setting is enabled in Jamf Pro.

Network Ports Used by Jamf Pro

The complete list of required ports depends on the specific services and features that are enabled in a particular environment. The following ports are required to support basic functionality in all environments:

Port	Description	Direction
8443	The standard SSL port for the Jamf Pro server. Default port used by applications and computers and mobile devices to connect to the Jamf Pro server.	Inbound to the Jamf Pro server; and outbound from computers and mobile devices
8080	The HTTP port for the Jamf Pro server on Linux and Windows platforms. Although it is available, applications do not connect to this port unless the defaults are overridden. This port is also used in load-balanced environments if SSL is terminated at the load balancer.	N/A
9006	The HTTP port for the Jamf Pro server on the Mac platform. Although it is available, applications do not connect to this port unless the defaults are overridden. This port is also used in load-balanced environments if SSL is terminated at the load balancer.	N/A
3306	The default port used by the Jamf Pro server to connect to MySQL.	Outbound from the Jamf Pro server; and inbound to MySQL

Additional ports may be required depending on specific configurations for:

- Content distribution: AFP, SMB, HTTP, or HTTPS
- LDAP integration for user or group lookups, for scope and inventory, or user authentication using a directory service
- An SMTP server for email notifications
- Computer remote control using Jamf Remote through SSH
- Remote syslog server

Mobile device management of computers and iOS devices (both institutionally owned and personally owned) requires communication with Apple Push Notification service (APNs) on the following ports:

Ports	Description	Direction
443	The default port used by Jamf Pro to communicate with APNs using the HTTP/2 protocol	Outbound from the Jamf Pro server; and inbound to the APNs server

Ports	Description	Direction
2197	The optional port for Jamf Pro on-premise environments used for communication with APNs using the HTTP/2 protocol	Outbound from the Jamf Pro server; and inbound to the APNs server
2195	The port used by the binary protocol to send messages from the Jamf Pro server to APNs	Outbound from the Jamf Pro server; and inbound to the APNs servers
2196	The port used by the Jamf Pro server to connect to APNs for feedback using the binary protocol	Outbound from the Jamf Pro server; and inbound to the APNs server
5223	The port used to send messages from APNs to the Mac computers and iOS devices in your network	Outbound from Mac computers and iOS devices; and inbound to the APNs server

For a complete list of the ports used to host communication among computers and mobile devices and Jamf Pro, see the Network Ports Used by Jamf Pro Knowledge Base article.

Communication Encryption

Communication between Jamf Pro and managed computers and mobile devices is encrypted using standard Transmission Layer Security (TLS). Specific protocols and ciphers that are enabled can be configured using the standard procedures for Apache Tomcat. For more information, see the following website:

The HTTP Connector
http://tomcat.apache.org/tomcat-8.5-doc/config/http.html

Computers can be configured to use certificate-based communication with Jamf Pro and to require SSL certificate verification for the Jamf Pro web app. With certificate-based communication enabled, Jamf Pro verifies a device signature header on all sensitive communication and only responds if the signature matches the device for which resources are being requested. With SSL certificate verification enabled, computers are required to verify the SSL certificate for the Jamf Pro web app and will reject any responses that include an invalid SSL certificate.

For instructions on configuring SSL certificate verification, see the Safely Configuring SSL Certificate Verification Knowledge Base article.

Management of both MDM-capable computers and mobile devices uses standard communication encryption as provided by Apple Push Notification service (APNs).

Jamf Pro as SCEP Proxy

You can enable Jamf Pro to proxy communication between a SCEP server and the computers and mobile devices in your environment. This allows Jamf Pro to communicate directly with a SCEP server to obtain certificates that devices need and install the certificate directly on the device. Devices do not need to access the SCEP server. For more information, see the Enabling Jamf Pro as SCEP Proxy technical paper.

Database Encryption

The full database is not encrypted but specific fields that contain sensitive information are.

Passwords for local Jamf Pro administrator accounts are hashed using the scrypt password-based key derivation function.

All other passwords and sensitive information are encrypted using a standard AES-256 algorithm with a unique key for each Jamf Pro instance that is stored in the database. This includes passwords and information such as the following:

- LDAP integration service account passwords
- Computer local management account passwords
- FileVault 2 individual recovery keys
- Distribution point service account passwords
- SMTP account password
- GSX account password
- Computer directory binding administrator account passwords
- Microsoft SCEP server challenge password

The Jamf Push Proxy

The Jamf Push Proxy enables communication between the Jamf Pro server and devices with Jamf Self Service installed. This communication allows you to send Notification Center notifications to computers and mobile devices with Self Service installed.

> **Note:** Jamf Pro communicates with the Jamf Push Proxy using port 443.

For more information, see the Jamf Push Proxy section in the *Jamf Pro Administrator's Guide*.

For related information, see the Network Ports Used by Jamf Pro Knowledge Base article.

Vulnerability Assessments

Automated penetration testing and vulnerability scans are performed on Jamf Pro prior to each release. In addition, code-assisted penetration testing and vulnerability assessments are performed annually by a third-party security consultant.

Third-Party Audits

Jamf has successfully completed an audit for ISO 27001 covering Jamf Pro and a Service Organization Control 2 (SOC 2) Type 2 audit for its Jamf Pro hosted services. Contact your sales or support representative for more information and to obtain copies of audit documents.

The Jamf Pro Server

Overview

The Jamf Pro server is an Apache Tomcat web application with a MySQL backend 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.

The server used to host Jamf Pro should meet the minimum requirements for operating system, Tomcat version, database configuration, and Java installation. For detailed information on these requirements, see the Jamf Pro System Requirements section in the *Jamf Pro Release Notes*.

Distributed Servers and Jamf Pro Web App Clustering

The Jamf Pro web app and database servers may be co-located on a single server or distributed on separate servers, and the same database server can be used with multiple web application servers.

Disabling the Jamf Pro Web App User Interface

The Jamf Pro web app may be configured in "Limited Access" mode to restrict access to the administrator user interface while still allowing device management capabilities for computers only, mobile devices only, or both.

Jamf Pro Administrator Accounts

Local Jamf Pro administrator account credentials are stored in the database and authenticated by the Jamf Pro server. As of Jamf Pro 9.7, password policy enforcement (for length, complexity, age, history, etc.), account lockout thresholds, and lost password reset functionality are available for local Jamf Pro administrator accounts.

Credentials for Jamf Pro administrator accounts from LDAP integration are not stored in the Jamf Pro server and are passed directly to the LDAP directory service for authentication. Standard password policy enforcement, account lockout thresholds, and lost password reset are provided by the LDAP directory service.

Role-based access with granular CRUD (create, read, update, delete) privileges is available for Jamf Pro objects.

Integrating with Directory Services

Jamf Pro supports integration with the following directory services:

- Apple's Open Directory
- Microsoft's Active Directory
- NetIQ eDirectory

Integrating with an LDAP directory service allows you to do the following:

- Look up and populate user information from the directory service for inventory purposes.
- Add Jamf Pro user accounts or groups from the directory service.
- Require users to log in to Self Service or the enrollment portal using their LDAP directory accounts.
- Require users to log in during mobile device setup using their LDAP directory accounts.
- Base the scope of remote management tasks on users or groups from the directory service.

For related information, see the Integrating with LDAP Directory Services section in the *Jamf Pro Administrator's Guide*.

Multi-Factor or Single Sign-On Authentication

As of Jamf Pro 9.93, Single Sign-On with SAML 2.0 authentication is supported. The Single Sign-On (SSO) feature allows you to integrate with a third-party Identity Provider (IdP) and implement SSO for the Jamf Pro server, User-Initiated Enrollment (macOS and iOS), and Self Service for macOS.

Tested Identity Providers for Jamf Pro are as follows:

- Okta
- Active Directory Federation Services
- Shibboleth Identity Provider
- OneLogin
- Ping Identity PingOne
- Google Apps for Work

For related information, see the Single Sign-On section in the *Jamf Pro Administrator's Guide*.

Server Logs

The following logs are available for logging activity in Jamf Pro:

- `JAMFSoftwareServer.log`
- `JAMFChangeManagement.log`

- `JSSInstaller.log`
- `backupDatabase.log`

As of Jamf Pro 9.7, the `JSSAccess.log` is available for logging activity in the Jamf Pro server.

Access logging can be configured for the Jamf Pro web app by modifying the Apache Tomcat settings. For more information on access logging, visit the following website:

The Valve Component
https://tomcat.apache.org/tomcat-8.5-doc/config/valve.html

Device Management Framework

Computer Enrollment

Enrollment is the process of adding Mac or Windows computers to Jamf Pro. When computers are enrolled, inventory information for the computers is submitted to Jamf Pro. For more information on the different ways to enroll computers with Jamf Pro, see the Computer Enrollment Methods section in the *Jamf Pro Administrator's Guide*.

Mobile Device Enrollment

Enrollment is the process of adding mobile devices to Jamf Pro to establish a connection between the devices and Jamf Pro. This allows you to perform inventory, configuration, security management, and distribution tasks on the device. For more information on the different ways to enroll mobile devices with Jamf Pro, see the Mobile Device Enrollment Methods section in the *Jamf Pro Administrator's Guide*.

Components Installed on Managed Computers

For a list of components that are installed on all computers managed by Jamf Pro, see the Components Installed on Managed Computers section in the *Jamf Pro Administrator's Guide*.

Computer Logs

The following logs are available to track activity on managed computers:

- `jamf.log`—The general jamf binary log.
- Jamf Pro application logs—The logs specific to each application.
- Jamf Pro server logs:
  - Application Usage logs
  - Computer Usage logs
  - Policy logs
  - Hardware and software history
  - User and location history
  - Remote management commands
  - Remote control and screen sharing

Components Installed on Mobile Devices

For a list of components that are installed on all mobile devices managed by Jamf Pro, see the Components Installed on Mobile Devices section in the *Jamf Pro Administrator's Guide*.

Managed Mobile Device Logs

The following logs are available to track activity on managed mobile devices:

- Device console log:
  - Xcode
  - Apple Configurator
- Jamf Pro server logs:
  - Remote management commands
  - User and location history

Remote Management Commands Available on Managed Computers and Mobile Devices

For a list of available remote commands that allow you to remotely perform tasks, see the following sections in the *Jamf Pro Administrator's Guide*:

- Remote Commands for Computers
- Remote Commands for Mobile Devices

Self Service

Jamf Self Service for macOS

The Jamf Self Service for macOS application allows users to browse and install configuration profiles, Mac App Store apps, and books. Users can also run policies and third-party software updates via patch policies, as well as access webpages using bookmarks.

You can make the following items available in Self Service and customize how they are displayed to users:

- Configuration profiles
- Software updates (via patch policies)
- Policies
- Mac App Store apps
- Books

In addition, you can make bookmarks available in Self Service to give users easy access to webpages directly from the application.

Authenticating to Self Service for macOS

To require or allow users to log in using an LDAP directory account, you need an LDAP server set up in Jamf Pro. For more information, see the Integrating with LDAP Directory Services section in the *Jamf Pro Administrator's Guide*.

To require or allow a user to log in using a Jamf Pro user account, you must first create an account for that user. For more information, see the Jamf Pro User Accounts and Groups section in the *Jamf Pro Administrator's Guide*.

To require or allow a user to log in using Single Sign-On, you must enable Single Sign-On for Self Service for macOS. For more information, see the Single Sign-On section in the *Jamf Pro Administrator's Guide*.

Jamf Self Service for iOS

Jamf Self Service for iOS allows you to distribute configuration profiles, apps, and books to iOS devices for users to install. Users tap Self Service to browse and install items using an intuitive interface.

There are two kinds of Self Service for iOS devices: the Jamf Self Service app and the Self Service web clip. The Self Service app can be installed on devices with iOS 7 or later. The latest version of the Self Service app available in the App Store requires devices with iOS 10 or later. By default, Jamf Self Service is installed on all managed mobile devices except Apple TV devices and personally owned devices. For more information on the Self Service levels of compatibility, see the Jamf Self Service for iOS section in the *Jamf Pro Administrator's Guide*.

Jamf Self Service for iOS is available for free from the App Store.

Authenticating to Jamf Self Service for iOS

To require or allow a user to log in using a Jamf Pro user account, you must first create an account for that user. For more information, see the Jamf Pro User Accounts and Groups section in the *Jamf Pro Administrator's Guide*.

To require or allow users to log in to Self Service, you need an LDAP server set up in Jamf Pro. For more information, see the Integrating with LDAP Directory Services section in the *Jamf Pro Administrator's Guide*.

Managing Apps on Mobile Devices

Managed apps allow the administrator to prevent data from being backed up and require the app and associated data to be removed from the device if the MDM profile is removed.

For related information, see the Understanding Managed Apps section in the *Jamf Pro Administrator's Guide*.

Security Settings on Managed Computers

Managing FileVault 2 on Computers

The following options are available for managing FileVault 2 on managed computers:

Configuration:

- Disk encryption configuration
- macOS configuration profile with a Security & Privacy payload

Reporting:

- Advanced inventory searches
- Smart computer group that uses the “FileVault 2 Eligibility” criteria
- Smart computer group that uses the “FileVault 2 Status” criteria

Remediation:

- Policy that contains a package to update an individual recovery key
- Policy that contains a package to update an institutional recovery key
- Policy that adds or removes FileVault 2 enabled users (macOS 10.10–10.12.x only)

System Integrity Protection Options

The following System Integrity Protection options are available for computers managed by Jamf Pro:

Reporting:

- Status for System Integrity Protection when viewing inventory information
- Advanced inventory searches
- Smart group that uses the "System Integrity Protection" criteria

Gatekeeper Options

The following Gatekeeper options are available for computers managed by Jamf Pro:

Configuration:

- Computer configuration profile with a Security & Privacy payload

Reporting:

- Status for Gatekeeper when viewing inventory information
- Advanced inventory searches
- Smart group that uses the "Gatekeeper" criteria

XProtect Definitions Version Options

The following XProtect Definitions Version options are available for computers managed by Jamf Pro:

Reporting:

- Version of XProtect Definitions installed on a computer when viewing inventory information
- Advanced inventory searches
- Smart computer group that uses the "XProtect Definitions Version" criteria

For more information on System Integrity Protection, Gatekeeper and XProtect Definitions Version, see the Jamf Pro Reporting Capabilities for Apple's macOS Security Features Knowledge Base article.

Patch Management Options

The following tools are available for patch management:

Reporting:

Computer inventory reports are available by default and display current configurations (OS version /build, application versions/builds, settings, etc.) as well as available software updates. Additional extension attributes may be configured to track other custom inventory items.

Remediation:

Configure policies to automatically deploy software updates to computers that meet certain reporting criteria or all managed devices.

Settings Management Options

Jamf Pro allows the deployment of configuration profiles that include standard payloads provided by Apple to manage settings on computers and iOS devices.

Applying Randomized Passwords to Management Accounts

User-initiated enrollment invitations for computers are configured to "Randomly generate passwords" for the management account by default, which assigns a random password with the specified number of alphanumeric characters to the enrollment invitation. The management account receives the random password when the invitation is redeemed if the following requirements are met:

- The computer does not already exist in Jamf Pro or, if it does, it does not have an existing management account.
- The specified management account does not already exist on the computer.

If the computer already exists and is already managed (re-enrollment), then the existing management account password will be used instead of the randomized password from the enrollment invitation. Likewise, if the account already exists on the computer, then the password will be stored in Jamf Pro inventory. The password will not be updated on the computer so certain functionality may be affected, like Jamf Remote.

Management account passwords can also be randomized through a policy. In this case, the password is reset by the jamf binary, communicated back to Jamf Pro, and added to the inventory for the computer. Random passwords that are set through a policy may also contain certain symbols in addition to alphanumeric characters.

For related information, see the Administering the Management Account section in the *Jamf Pro Administrator's Guide*.

Mobile Device Management Capabilites

The management capabilities available for a particular device may vary depending on the device ownership type, device type, and OS version. For an overview of management capabilities available with Jamf Pro, see the Mobile Device Management Capabilities section in the *Jamf Pro Administrator's Guide*.

Content Distribution

Distributing Content to Managed Computers and Mobile Devices

Jamf Pro supports two types of distribution points:

- File share distribution points
- A cloud distribution point that uses one of the following content delivery networks (CDNs) to host files:
  - Rackspace Cloud Files
  - Amazon S3 or Amazon CloudFront
  - Akamai NetStorage
  - Jamf Cloud Distribution Service (JCDS)
    Jamf Cloud can be used as a cloud distribution point if your environment supports the use of JCDS.

For related information, see the About Distribution Points section in the *Jamf Pro Administrator's Guide*.

Jamf Cloud Distribution Service

Jamf Pro allows you to distribute content using Jamf Cloud Distribution Service (JCDS) as your cloud distribution point. JCDS can be used to host packages, in-house apps, and in-house books. Files are distributed using HTTPS and stored by Jamf Online Services using Amazon S3. Data is logically separated with controlled access. The checksum is calculated when a package is uploaded to JCDS, and the checksum ensures integrity when the package is downloaded. Clients download content from JCDS using signed URLs for secure content distribution. JCDS is designed for high availability with no downtime.

Note : The Jamf Pro server communicates with JCDS using port 443.

JCDS is only available as a cloud distribution point if Jamf Pro is hosted on Jamf Cloud and if you have the subscription-based option.

For information about configuring a cloud distribution point in Jamf Pro, see the Cloud Distribution Point section the *Jamf Pro Administrator's Guide*.

For related information about JCDS, see the following Knowledge Base articles:

- Jamf Cloud Distribution Service Communication
- Network Ports Used by Jamf Pro

Jamf Cloud Hosting

Overview

Jamf can manage your Jamf Pro server infrastructure through the Jamf Cloud Hosting service. Jamf Cloud instances may include the following components:

- A hosted Jamf Pro environment
- Elastic Load Balancers
- Apache Load Balancers
- Apache Tomcat
- Java Development Kit (OpenJDK compatible)
- MySQL-compatible database(s)
- Linux-based host operating system

In addition, if you have the subscription-based option, you can use Jamf Cloud Distribution Service (JCDS) as your cloud distribution point.

Geographical Regions

Jamf Cloud uses servers in the United States, the United Kingdom, Germany, Japan, and Australia. Data at rest remains in the region that hosts the Jamf Pro instance.

Service Availability

Jamf Cloud uses a clustered Jamf Pro configuration with multiple, load balanced web applications.

Regular maintenance is performed and may include Jamf Pro version upgrades, infrastructure improvements, and security improvements. Customers are notified prior to the start of maintenance.

Database Backups

Databases are continuously replicated to another server in a different data center. A snapshot of each database is taken every 24 hours and may be used to restore data if a critical event occurs.

Recovery

Jamf Cloud uses application and database servers in multiple data centers to provide high availability and recovery in case of service outage.

Communication Encryption

Jamf Cloud uses an external, third-party SSL certificate for the Jamf Pro web app. In addition, Jamf Cloud uses TLS for data sent between a managed endpoint and the Jamf Pro server.

Logical Data Separation

Data is kept logically separate on various layers throughout the Jamf Cloud infrastructure. Only processes and threads such as queries within an authenticated organization's context may access that organization's data. This restriction applies to all data and processes/threads, both in memory and on disk.

Employee Access

Jamf Cloud Operations staff may log in to the servers hosting Jamf Pro to access settings related to a support issue. In rare cases, Jamf Cloud Operations staff may also need to access your database to resolve a support issue. In this event, Jamf Cloud Operations staff will do their best to respect your privacy, and will only access the files and settings needed to perform the required tasks.

Shared Security Model

Each vendor used to support Jamf Cloud must adhere to the same security measures employed by Jamf. Vendors are required to pass a vendor assessment before their products or services are deployed to the Jamf Cloud environment. Each vendor is responsible for the security of the products or services they provide. Jamf is responsible for using the products or services securely.

Physical Security

All physical data centers used for Jamf Cloud are managed by Amazon Web Services. In addition, physical security measures such as biometric access controls, 24/7 armed guards, and video surveillance are used to ensure that no unauthorized access is permitted. For more information, see the following document:

Amazon Web Services: Overview of Security Processes
https://d1.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Vulnerability Assessments

Jamf Cloud is subjected to penetration testing and vulnerability assessments. In addition, Jamf Cloud uses tools for continuous vulnerability monitoring and intrusion detection.

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 the LDAP Proxy section 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 the Healthcare Listener section 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.

Network Communication

When using the LDAP Proxy, the Jamf Infrastructure Manager can be customized for incoming access by any available port 1024 or greater. The port used must be opened, inbound, on your firewall and also on the computer on which the Infrastructure Manager is installed. The recommended port is 8389 for communication between your Jamf Pro server and the Infrastructure Manager.

Note: The Infrastructure Manager does not currently respect network proxy settings configured in the host operating system or in Java. Therefore, the Infrastructure Manager must be enrolled with Jamf Pro and receive its initial configuration on a network that does not require connection via an outbound proxy. Unless a firewall rule is created to allow the Infrastructure Manager to connect to Jamf Pro without using an outbound proxy, the Infrastructure Manager will not receive LDAP configuration updates or be able to notify Jamf Pro that it is operational. It will still be able to receive the inbound LDAP lookup requests from Jamf Pro, however.

For communication between the Infrastructure Manager and an LDAP directory service, your LDAP server's regular incoming port is used. This port is specified in the LDAP server's configuration in Jamf Pro. The most common configurations are port 389 for LDAP and port 636 for LDAPS. This communication occurs between the Infrastructure Manager in the DMZ and an internal LDAP directory service only.

Note: If your environment is hosted in Jamf Cloud and uses Network Address Translation (NAT), you can configure the Jamf Infrastructure Manager to ensure successful communication between the Infrastructure Manager and Jamf Pro. For more information, see the Configuring the Jamf Infrastructure Manager to Use Network Address Translation (NAT) Knowledge Base article.

When using Jamf Pro hosted on Jamf Cloud, the necessary external IP addresses for Jamf Cloud must be allowed inbound to the Infrastructure Manager. For more information, see the Permitting Inbound /Outbound Traffic with Jamf Cloud Knowledge Base article.

> **Note:** Internal domain addresses (for example, .local, .company, or .mybiz) are not supported at this time. The Infrastructure Manager must be resolvable to the external Jamf Pro server.

For more information about network communication and the connections initiated between the Infrastructure Manager and Jamf Pro, see the Network Ports Used by Jamf Pro Knowledge Base article.

Server Logs for the Jamf Infrastructure Manager

Infrastructure Manager instance activities can be tracked in the following locations:

- **Linux:** `/usr/share/jamf-im`
- **Windows:** `C:\Program Files\Infrastructure Manager`