

UNCLASSIFIED



JAMF PRO v10.x EMM SUPPLEMENTAL PROCEDURES

Version 3, Release 1

24 July 2024

Developed by Jamf and DISA for the DOD

UNCLASSIFIED

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. JAMF PRO EMM SOFTWARE SECURITY AND CONFIGURATION INFORMATION	1
1.1 Jamf Pro EMM Architecture	1
1.2 Jamf Pro EMM Software Components	1
1.3 Jamf Pro Required Firewall Ports	1
1.4 PKI Considerations	2
1.5 Provisioning Derived Credentials	2
1.5.1 Apple iOS	2

LIST OF TABLES

	Page
Table 1-1: Jamf Pro EMM Components.....	1
Table 1-2: Required Ports and Services.....	1

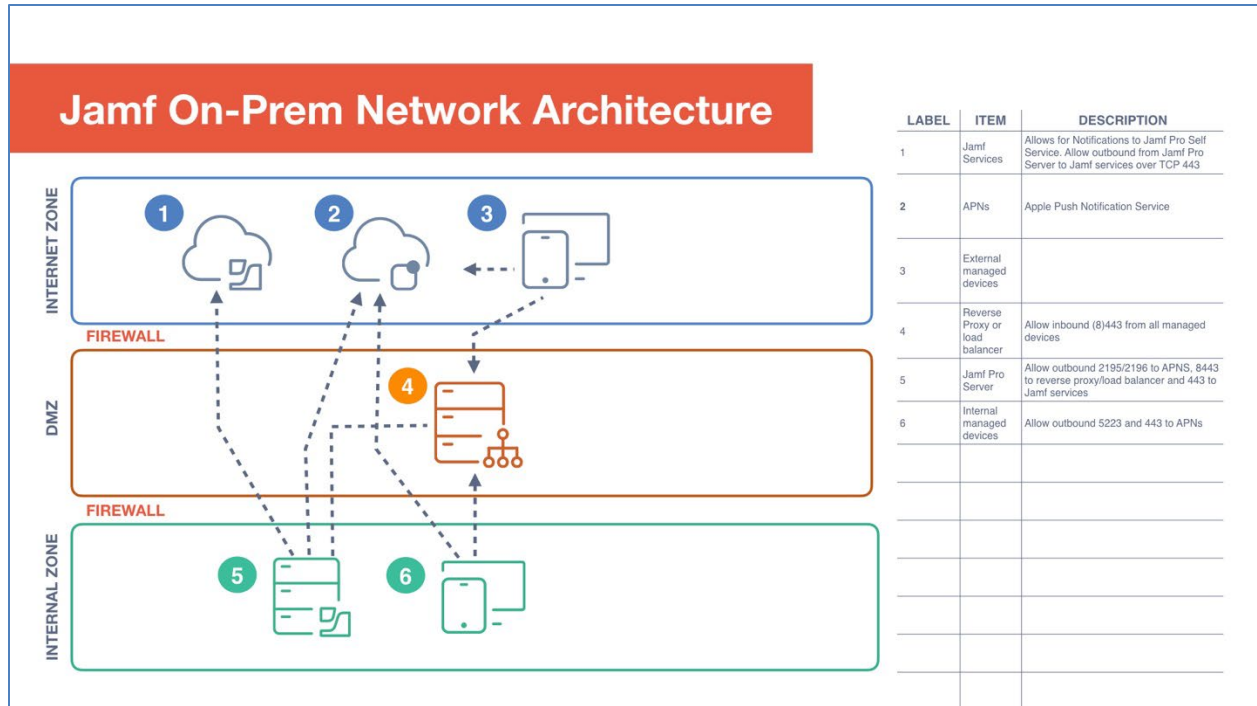
LIST OF FIGURES

	Page
Figure 1-1: Jamf Pro EMM Architecture	1

1. JAMF PRO EMM SOFTWARE SECURITY AND CONFIGURATION INFORMATION

1.1 Jamf Pro EMM Architecture

Figure 1-1: Jamf Pro EMM Architecture



1.2 Jamf Pro EMM Software Components

Table 1-1: Jamf Pro EMM Components

Component	Description
Jamf Self Service	Jamf Pro iOS app
Jamf Pro Server	Jamf Pro MDM Server

1.3 Jamf Pro Required Firewall Ports

Table 1-2: Required Ports and Services

From	To	Port (TCP)	Description
Administrators	MDM Server	22	SSH
Mobile Devices	MDM Server	80	HTTP (for CRLs)
Mobile Devices	MDM Server	443	HTTPS
Administrators	MDM Server	8443	HTTPS-alt
Mobile Devices	Apple Push Notification Services	5223	HTTPS
MDM Server	Apple Push Notification Services	2195/2195	

1.4 PKI Considerations

To implement over-the-air (OTA) provisioning of a DOD mobile device, an authenticated and encrypted tunnel can be set up between the mobile device and the mobile device management (MDM) server. The mobile device and MDM server must support the same root certificate authority to set up a mutually authenticated trusted tunnel between both endpoints.

For the mobile device to support the current DOD root Certificate Authority (CA), DOD Root CA 3, the mobile device needs to natively, out-of-the-box, trust the current DOD root Certificate Authority, or the certificate will need to be side-loaded on the mobile device, which is not scalable in an Enterprise environment. Unfortunately, few, if any, mobile devices natively trust this root CA. Alternately, since there is a path of trust between DOD Root CA 3 and the Federal Common Policy Certificate Authority (FCPCA), a mobile device that natively trusts the FCPCA can authenticate the MDM if either the MDM server or web service used by the MDM (for example IIS, Apache) pushes down a path to the FCPCA to the mobile device during the TLS handshake.

The Jamf Pro MDM's web service is provided by Apache Tomcat. A Local Admin on the MDM can manage these certificates through the Web UI's System Manager by navigating to "Devices" and selecting "Configuration Profiles". They can then use the payload "Certificate" to upload a PKCS12 file containing the server's certificate and all CA certificates in the path from the DOD PKI Issuing CA (e.g., DOD ID SW CA 37) to Federal Common Policy.

1.5 Provisioning Derived Credentials

The need to provision derived credentials benefits from some MDM features that are not required to support other functionality. This section describes these features for iOS.

1.5.1 Apple iOS

On iOS, to enable third-party apps to use derived credentials, the key sharing interface of the Purebred application should be leveraged. The key sharing interface is a use of Apple's document provider extensions to share PKCS 12 objects between a key management application and an application desired to use keys. Sample code is available at <https://github.com/purebred>.

For iOS 13, depending on the MDM vendor and the use of the iOS-provided mail client for work email, a managed Exchange payload with the following settings set to "True" could be leveraged to allow users to select Purebred-issued credentials for signed and encrypted email:

```
SMIMESigningUserOverrideable;  
SMIMESigningCertificateUUIDUserOverrideable;  
SMIMEEncryptByDefaultUserOverrideable;
```

All are configurable within Jamf Pro for distribution to managed iOS devices.