JAMF ADCS Certificate setup Guide

Version: 1.0 March 2018

This is documentation on how to use JAMF to deploy a device or computer based cert for EAP-TLS Cert based Wireless.

Items you'll need:

Certs: in .cer format

Root CA cert

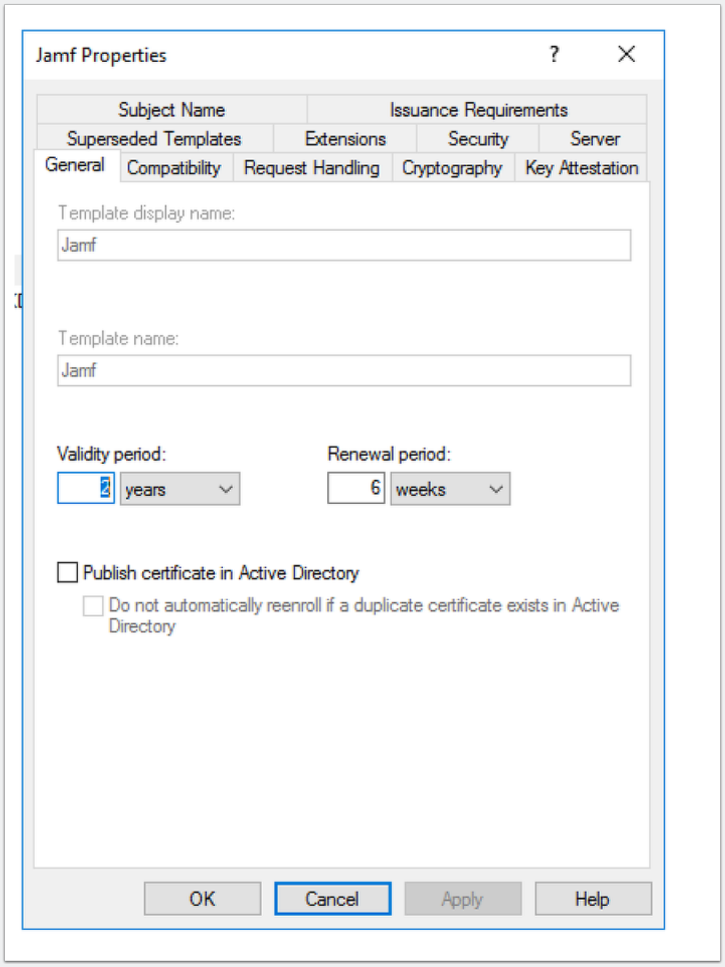
Issuing Cert

Access to the Root CA server to create the certificate template.

Admin access to your Jamf console.

The FQDN name or your radius servers.

Step 1: Create the Certificate Template on the root CA: General



Jamf Properties

Template display name:
Jamf

Template name:
Jamf

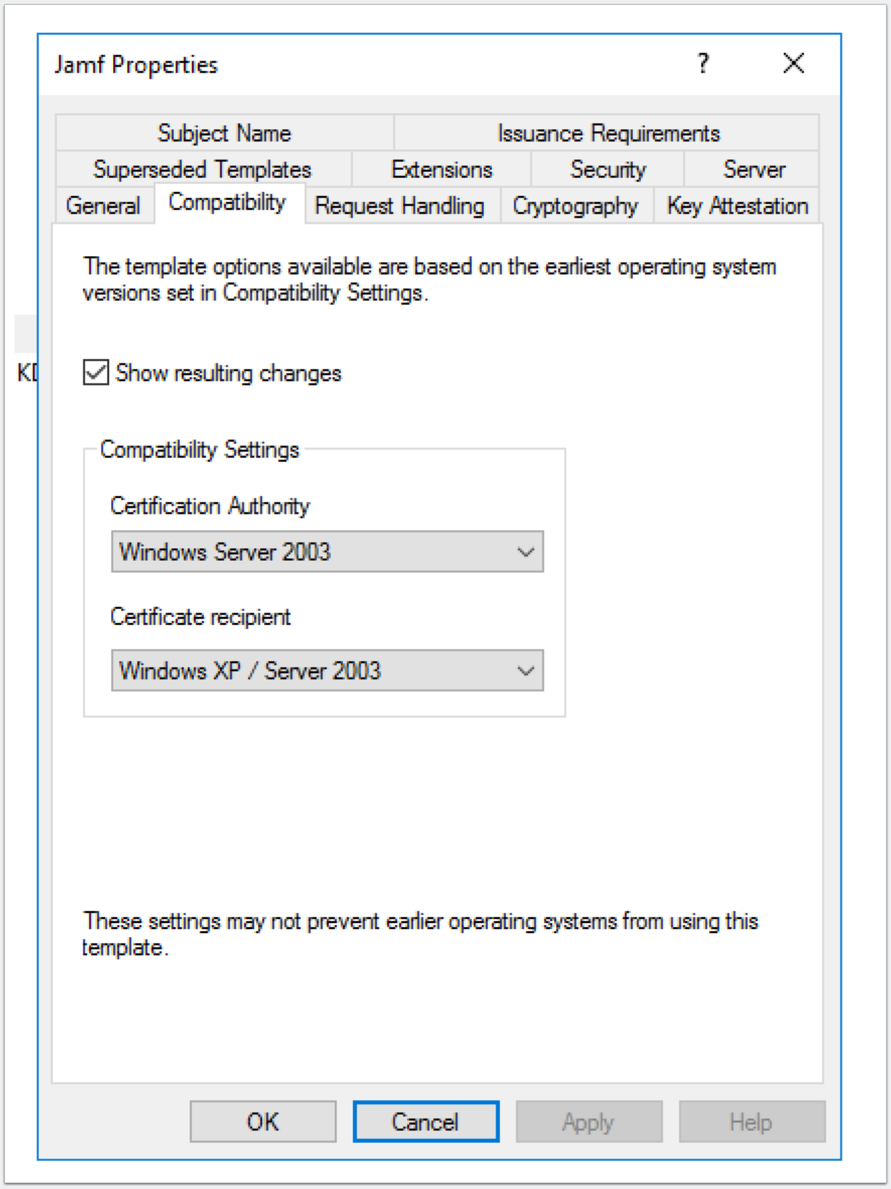
Validity period:
2 years

Renewal period:
6 weeks

☐ Publish certificate in Active Directory

☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

Compatibility



Jamf Properties

The template options available are based on the earliest operating system versions set in Compatibility Settings.

☑ Show resulting changes

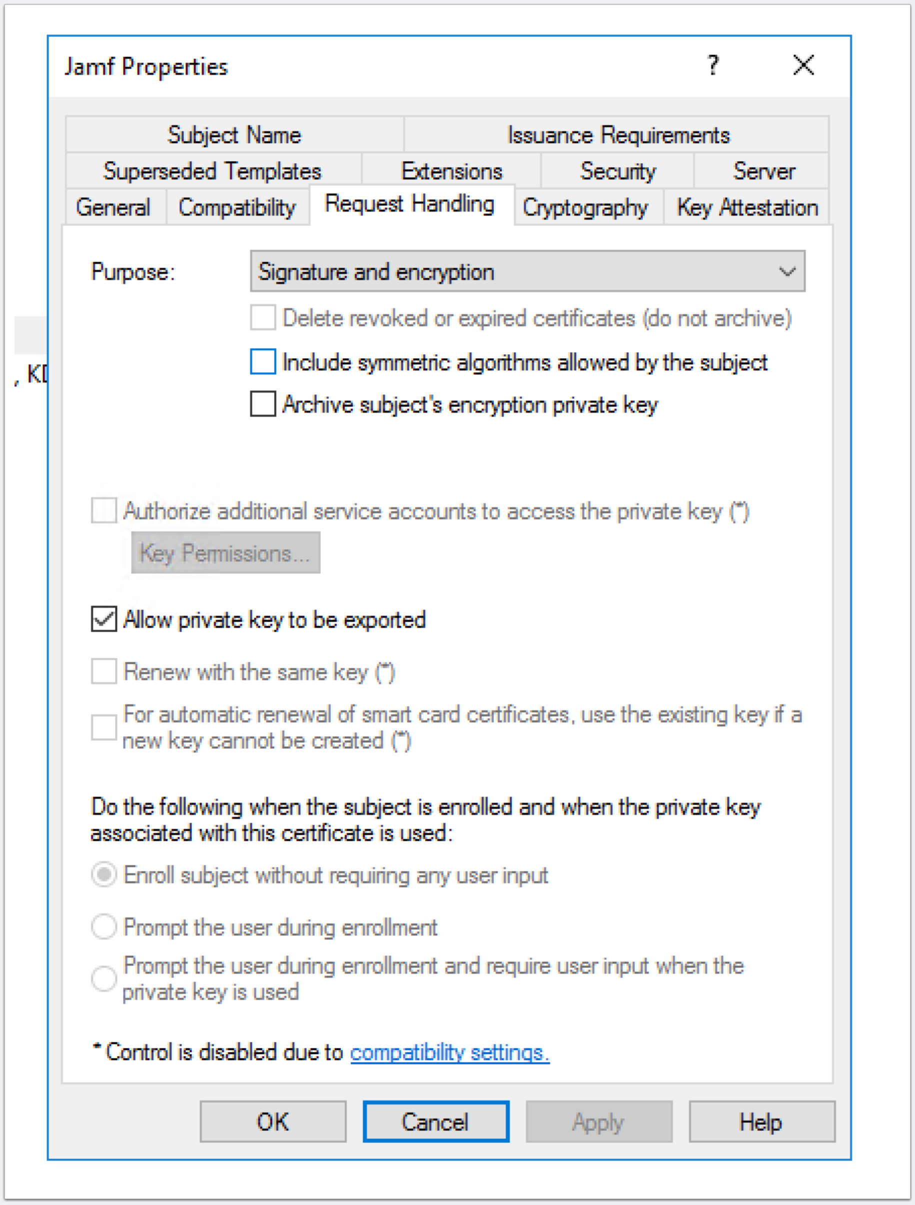
Compatibility Settings

Certification Authority: Windows Server 2003

Certificate recipient: Windows XP / Server 2003

These settings may not prevent earlier operating systems from using this template.

Request Handling



Jamf Properties

Purpose: Signature and encryption

□ Delete revoked or expired certificates (do not archive)

□ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

□ Authorize additional service accounts to access the private key (*)

☑ Allow private key to be exported

□ Renew with the same key (*)

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

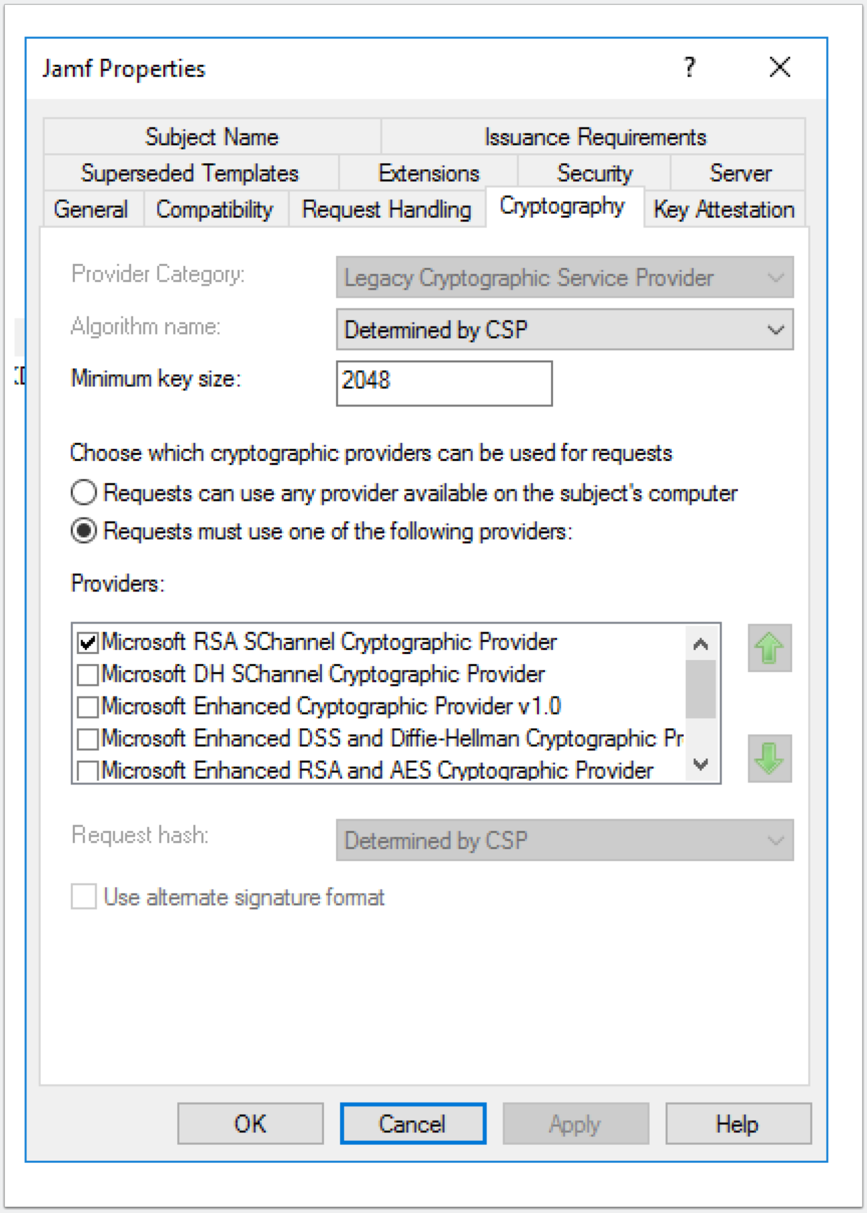
● Enroll subject without requiring any user input

○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

* Control is disabled due to compatibility settings.

Crytography



Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

○ Requests can use any provider available on the subject's computer

● Requests must use one of the following providers:

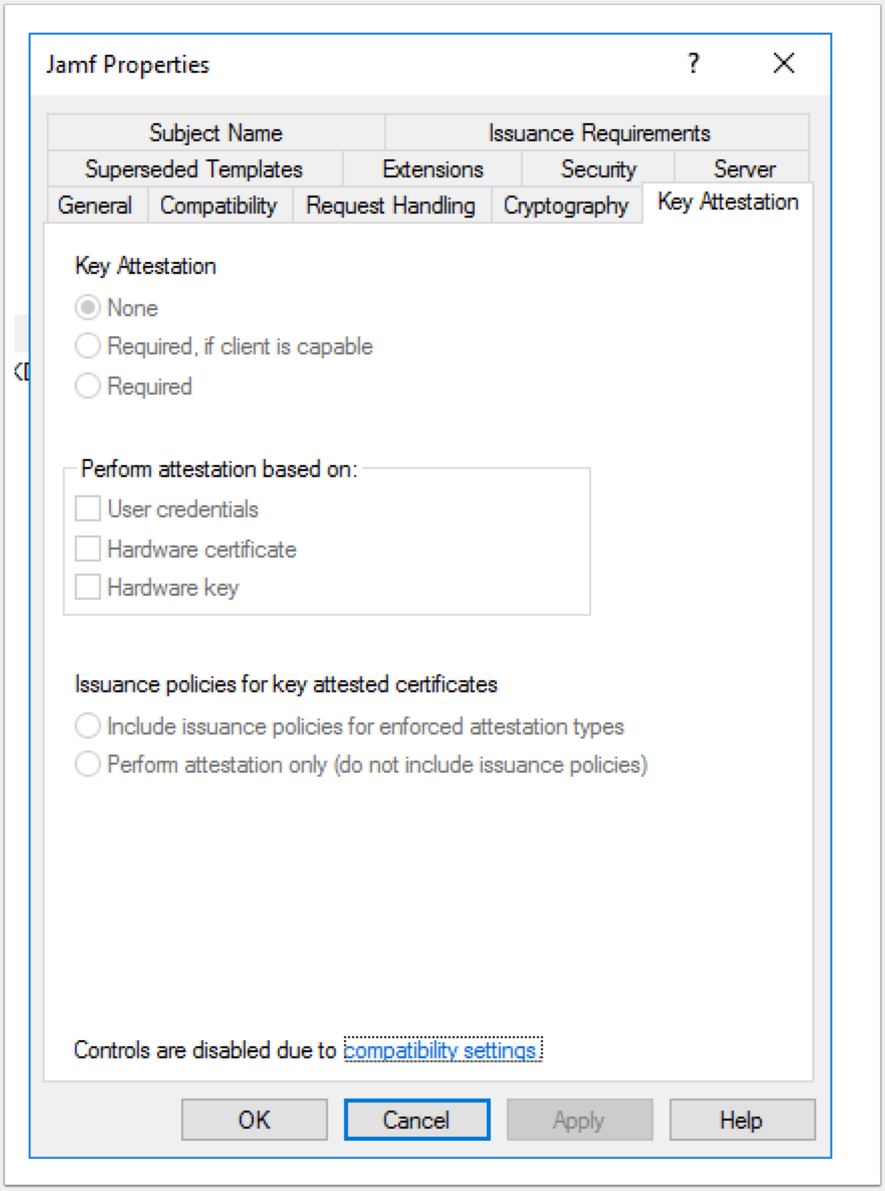
Providers:

☑ Microsoft RSA SChannel Cryptographic Provider
□ Microsoft DH SChannel Cryptographic Provider
□ Microsoft Enhanced Cryptographic Provider v1.0
□ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr
□ Microsoft Enhanced RSA and AES Cryptographic Provider

Request hash: Determined by CSP

□ Use alternate signature format

Key Attestation



Key Attestation

● None

○ Required, if client is capable

○ Required

Perform attestation based on:

□ User credentials

□ Hardware certificate

□ Hardware key

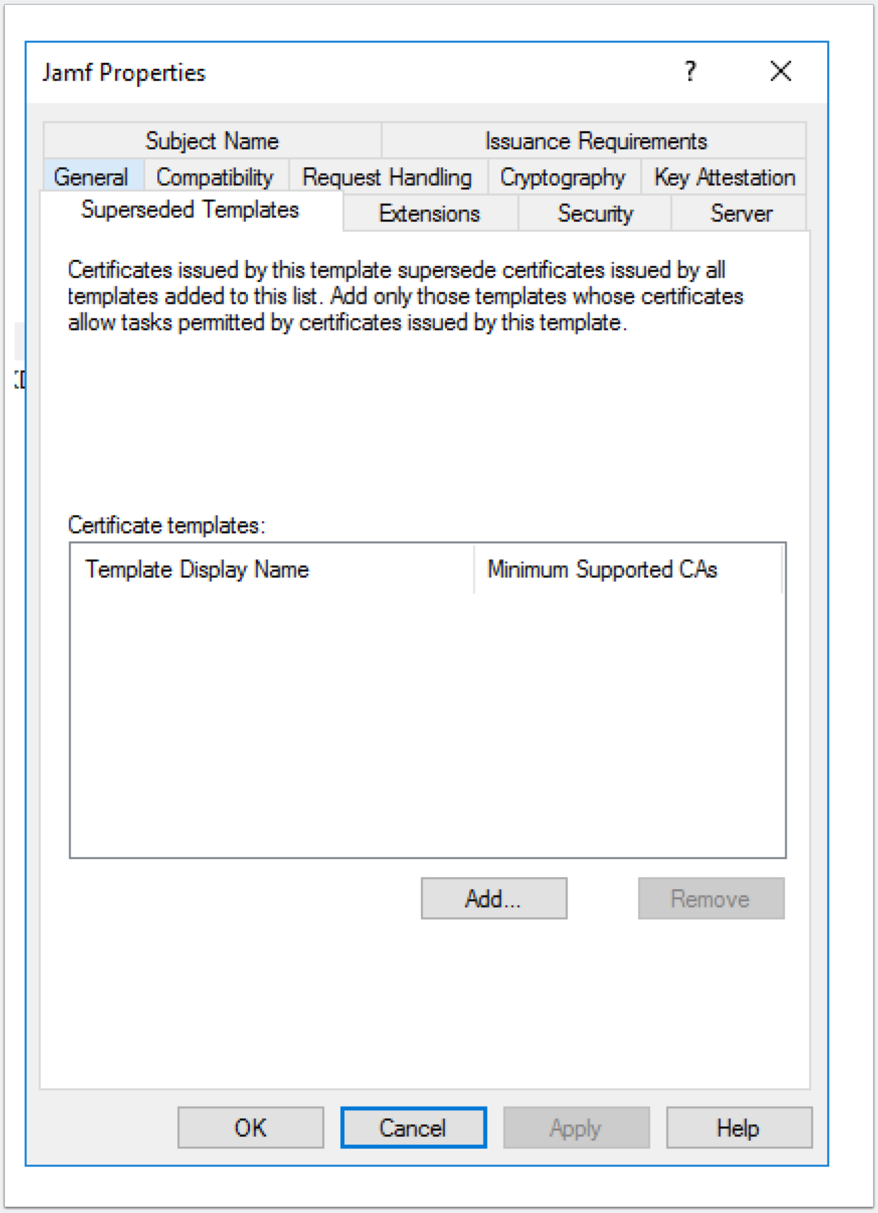
Issuance policies for key attested certificates

○ Include issuance policies for enforced attestation types

○ Perform attestation only (do not include issuance policies)

Controls are disabled due to compatibility settings

Superseded Templates

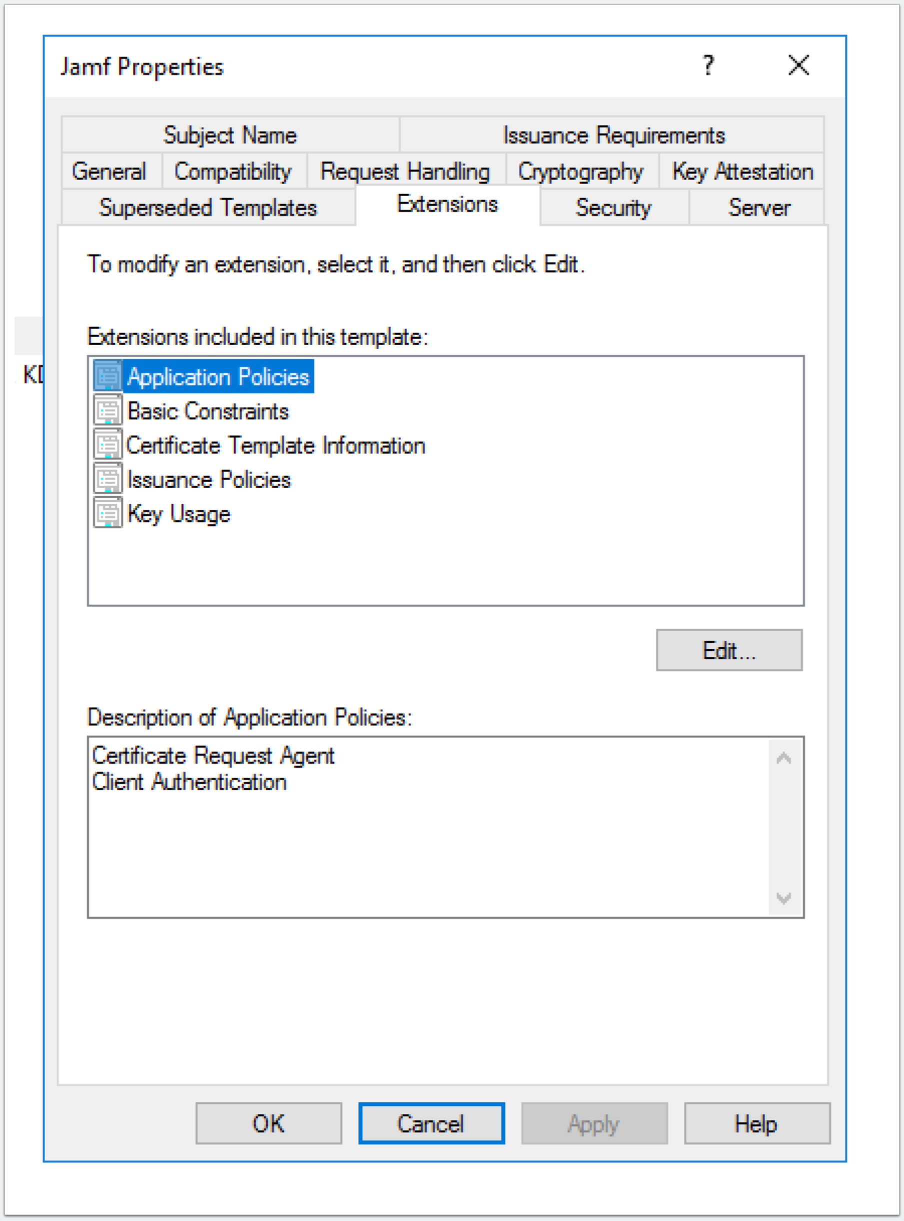


Certificates issued by this template supersede certificates issued by all templates added to this list. Add only those templates whose certificates allow tasks permitted by certificates issued by this template.

Certificate templates:

Template Display Name	Minimum Supported CAs

Extensions: Application Policies



To modify an extension, select it, and then click Edit.

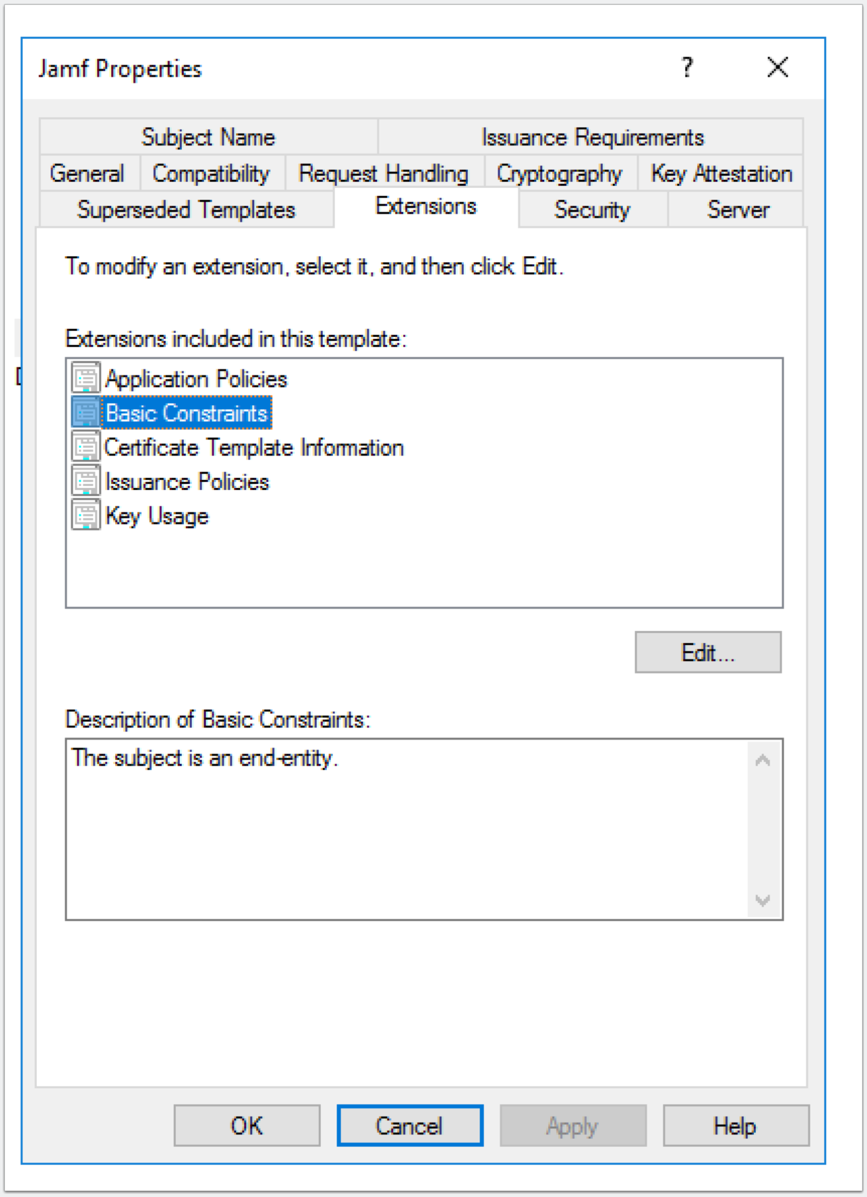
Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Certificate Request Agent
Client Authentication

Extensions: Basic Constraints



To modify an extension, select it, and then click Edit.

Extensions included in this template:

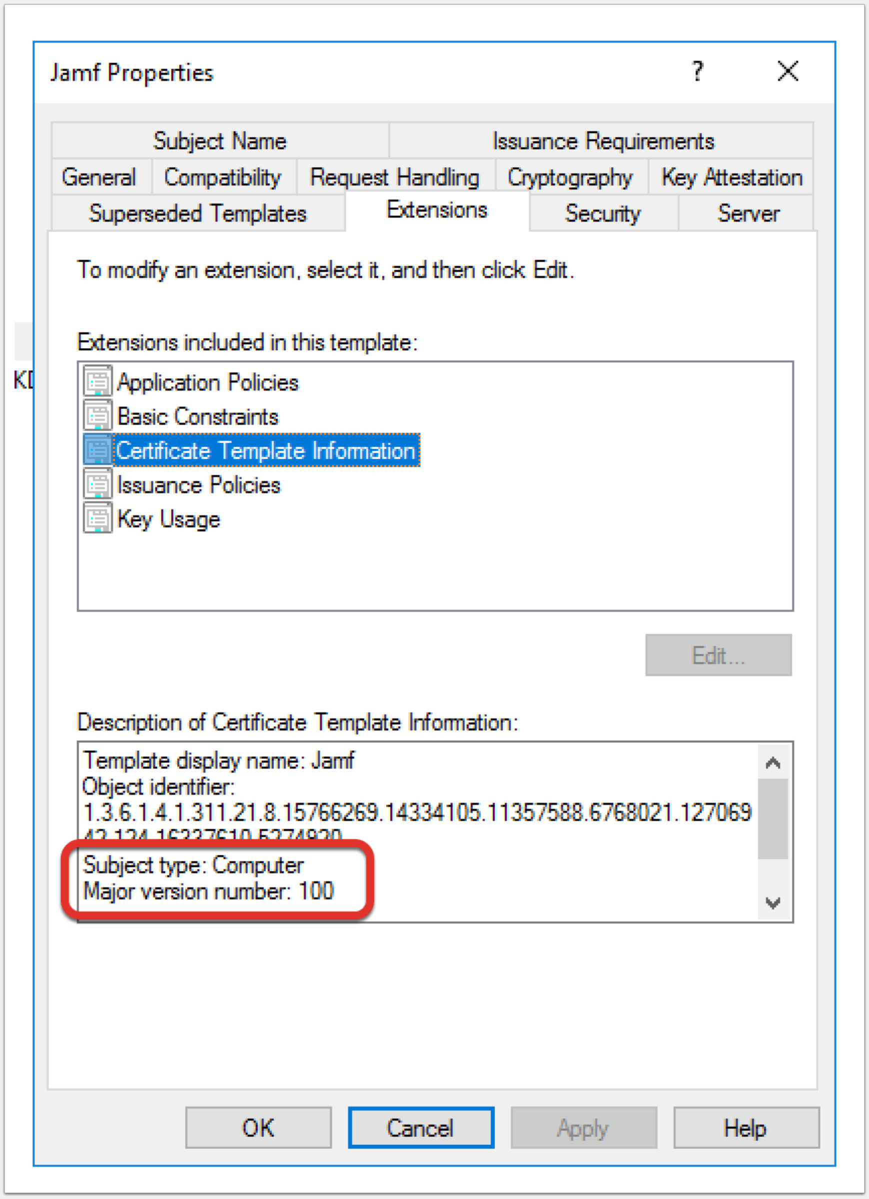
- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Basic Constraints:

The subject is an end-entity.

Extensions: Certificate Template Info

This is a computer template



To modify an extension, select it, and then click Edit.

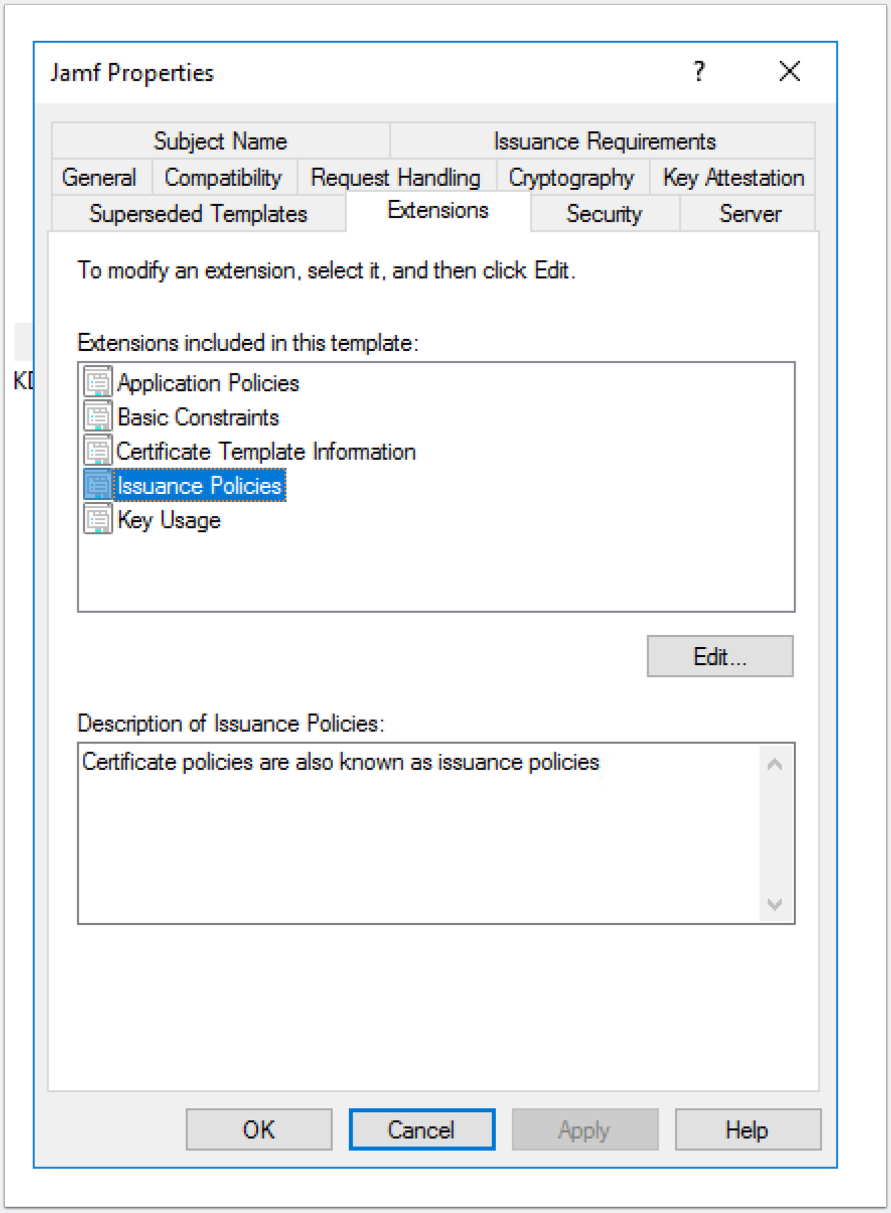
Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Certificate Template Infomation:

Template display name: Jamf
Object identifier:
1.3.6.1.4.1.311.21.8.15766269.14334105.11357588.6768021.127069
42.124.16237610.5274920
Subject type: Computer
Major version number: 100

Extensions: Issuance Policies



To modify an extension, select it, and then click Edit.

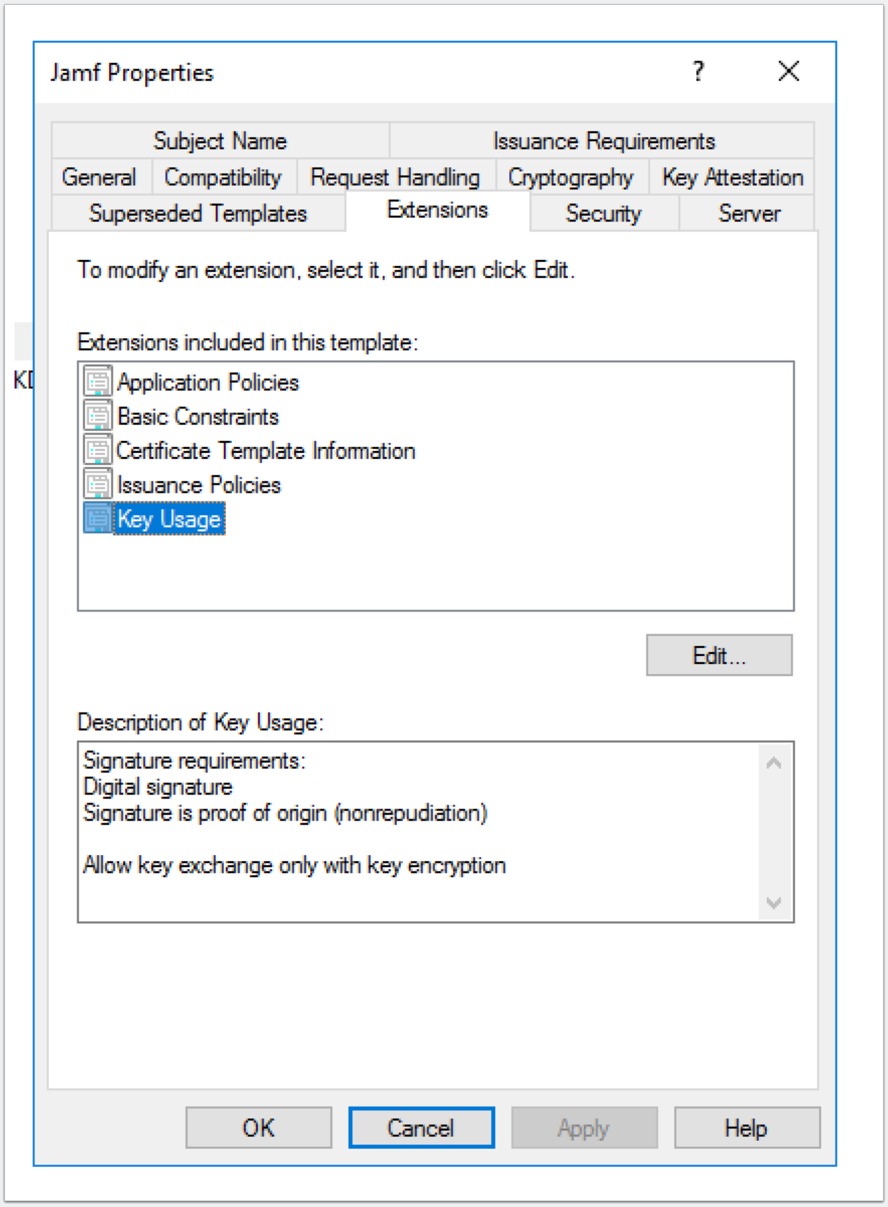
Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Issuance Policies:

Certificate policies are also known as issuance policies

Extensions: Key Usage



To modify an extension, select it, and then click Edit.

Extensions included in this template:

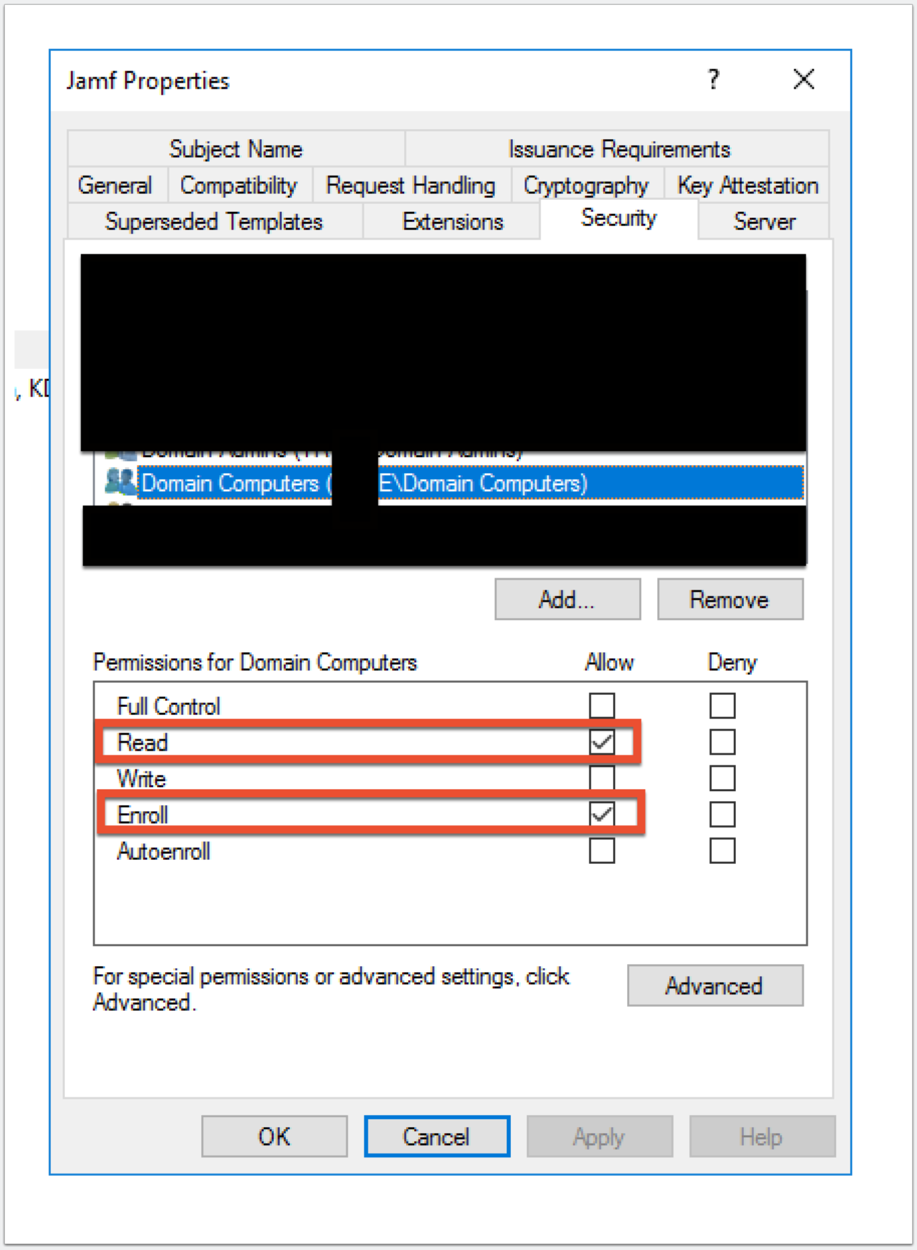
- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Key Usage:

Signature requirements:
Digital signature
Signature is proof of origin (nonrepudiation)

Allow key exchange only with key encryption

Security



Jamf Properties

[redacted]

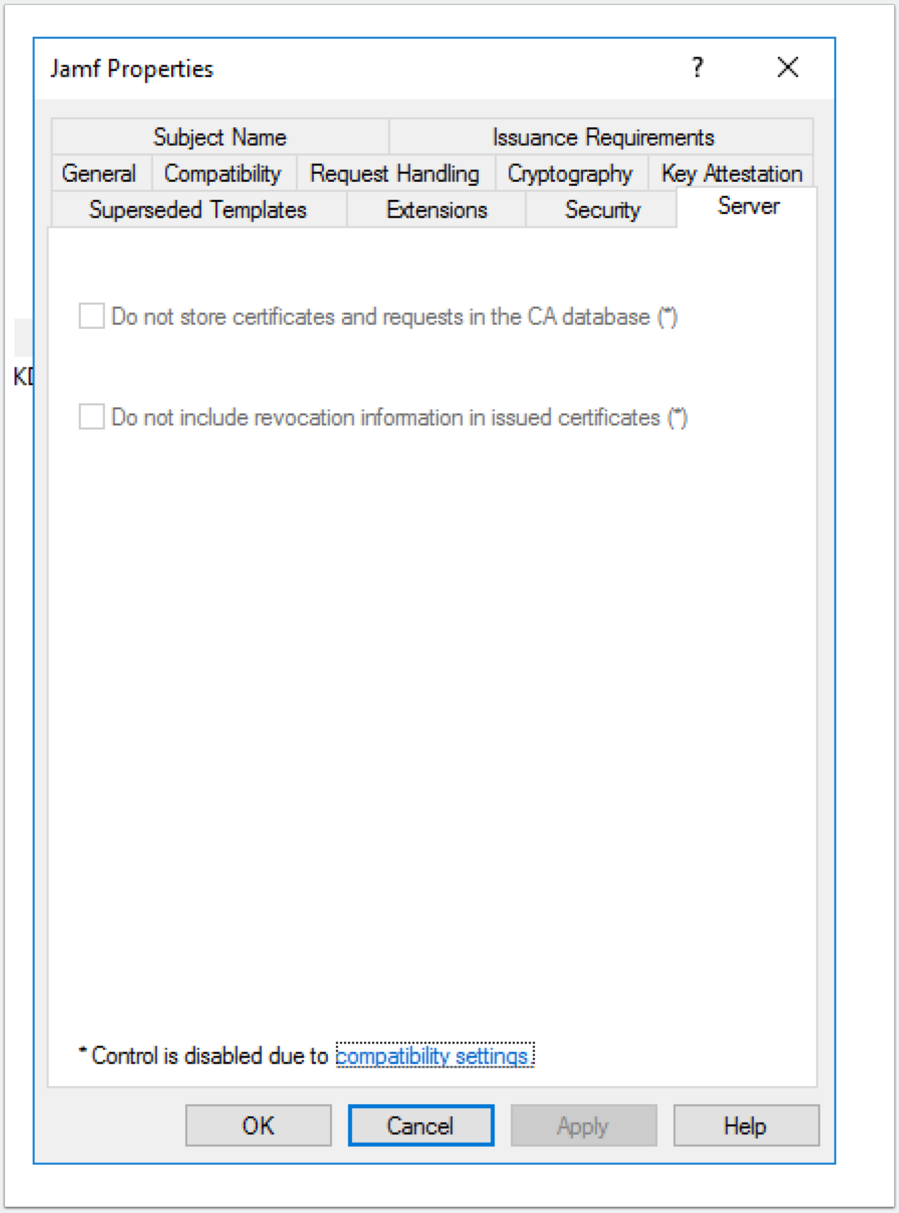
Domain Computers ([redacted]E\Domain Computers)

[redacted]

Permissions for Domain Computers	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□

For special permissions or advanced settings, click Advanced.

Server

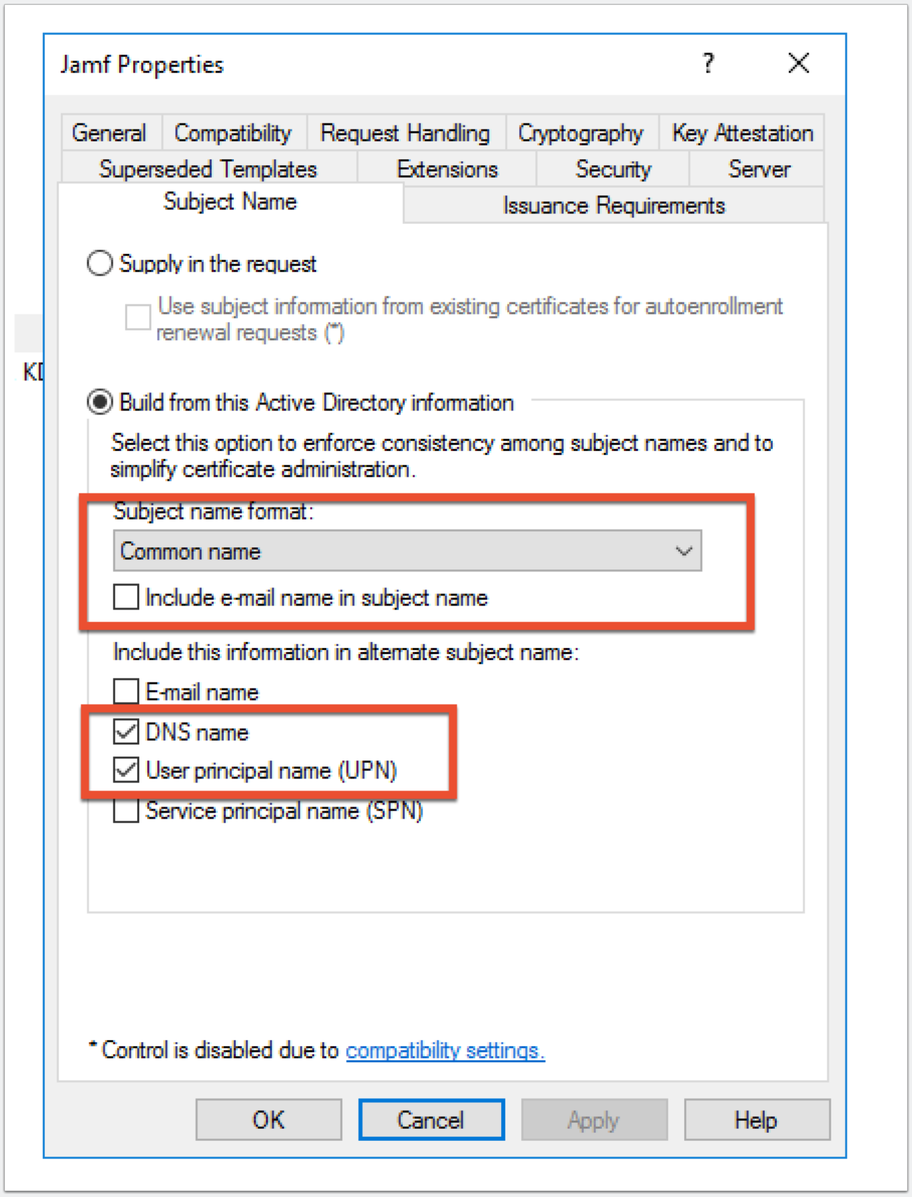


□ Do not store certificates and requests in the CA database (*)

□ Do not include revocation information in issued certificates (*)

* Control is disabled due to compatibility settings

Subject Name



○ Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests (*)

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

Common name

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

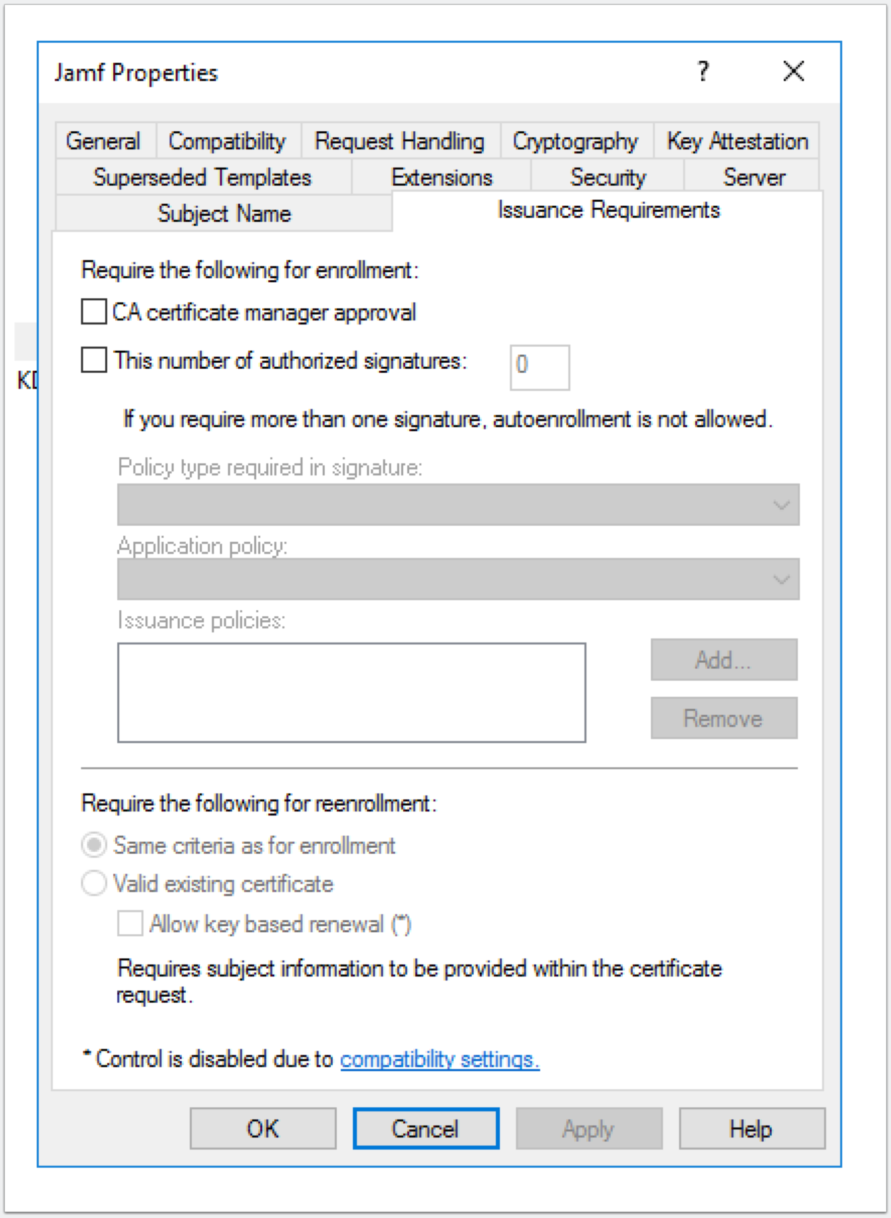
☑ DNS name

☑ User principal name (UPN)

□ Service principal name (SPN)

* Control is disabled due to compatibility settings.

Issuance Requirements



Require the following for enrollment:

□ CA certificate manager approval

□ This number of authorized signatures: 0

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy:

Issuance policies:

Require the following for reenrollment:

● Same criteria as for enrollment

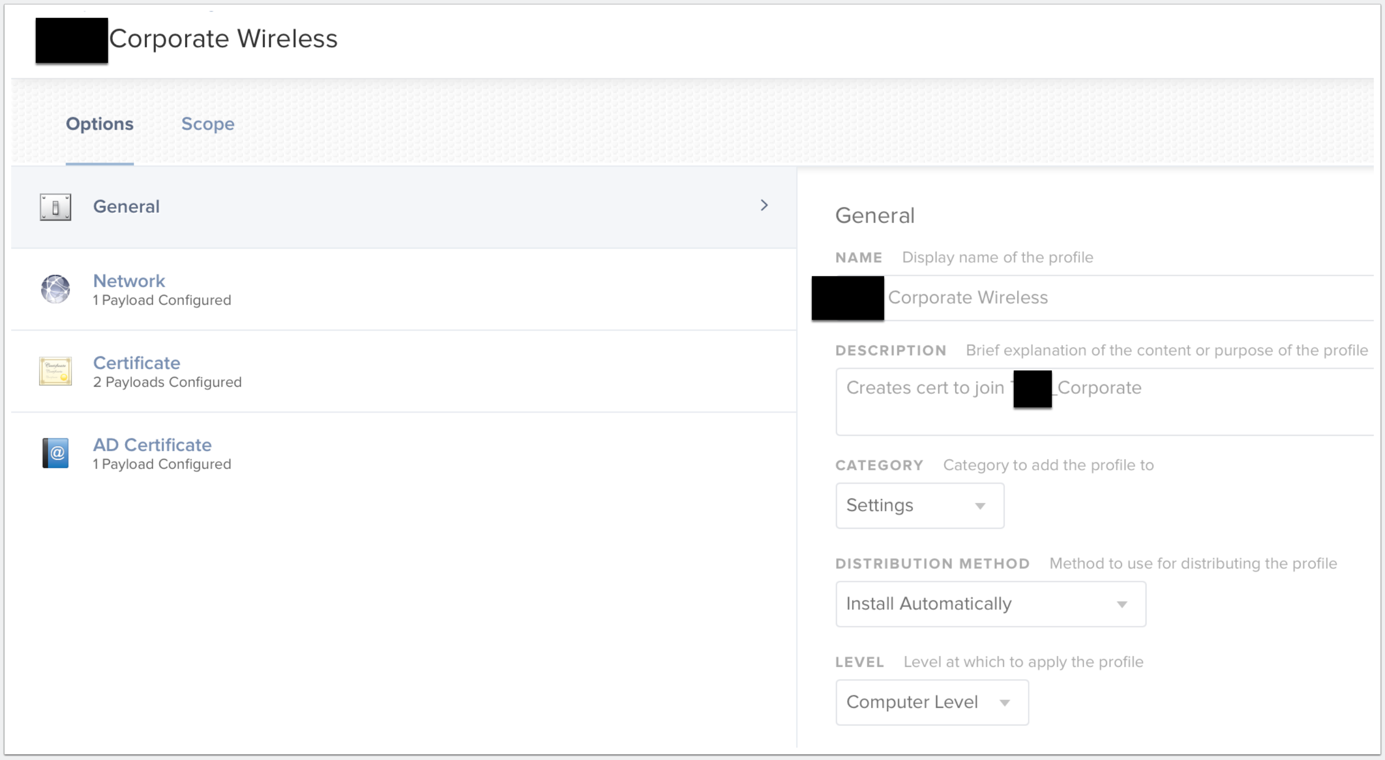
○ Valid existing certificate

□ Allow key based renewal (*)

Requires subject information to be provided within the certificate request.

* Control is disabled due to compatibility settings.

Step 2: JAMF Setup



[redacted] Corporate Wireless

General

NAME Display name of the profile

[redacted] Corporate Wireless

DESCRIPTION Brief explanation of the content or purpose of the profile

Creates cert to join [redacted] Corporate

CATEGORY Category to add the profile to

Settings

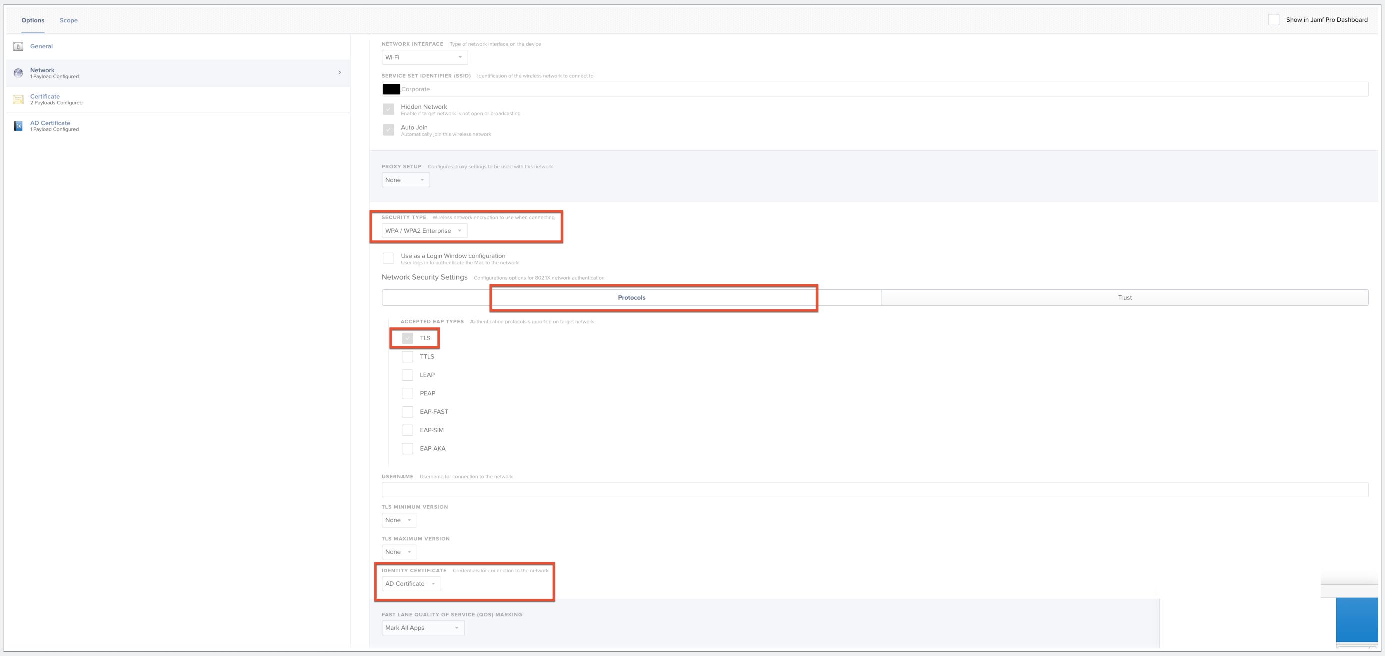
DISTRIBUTION METHOD Method to use for distributing the profile

Install Automatically

LEVEL Level at which to apply the profile

Computer Level

Network: Protocols



NETWORK INTERFACE Type of network interface on the device
Wi-Fi

SERVICE SET IDENTIFIER (SSID) Identification of the wireless network to connect to
[redacted] Corporate

☑ Hidden Network
Enable if target network is not open or broadcasting

☑ Auto Join
Automatically join this wireless network

PROXY SETUP Configures proxy settings to be used with this network
None

SECURITY TYPE Wireless network encryption to use when connecting
WPA / WPA2 Enterprise

□ Use as a Login Window configuration
User logs in to authenticate the Mac to the network

Network Security Settings Configurations options for 802.1X network authentication

Protocols | Trust

ACCEPTED EAP TYPES Authentication protocols supported on target network

- ☑ TLS
- □ TTLS
- □ LEAP
- □ PEAP
- □ EAP-FAST
- □ EAP-SIM
- □ EAP-AKA

USERNAME Username for connection to the network

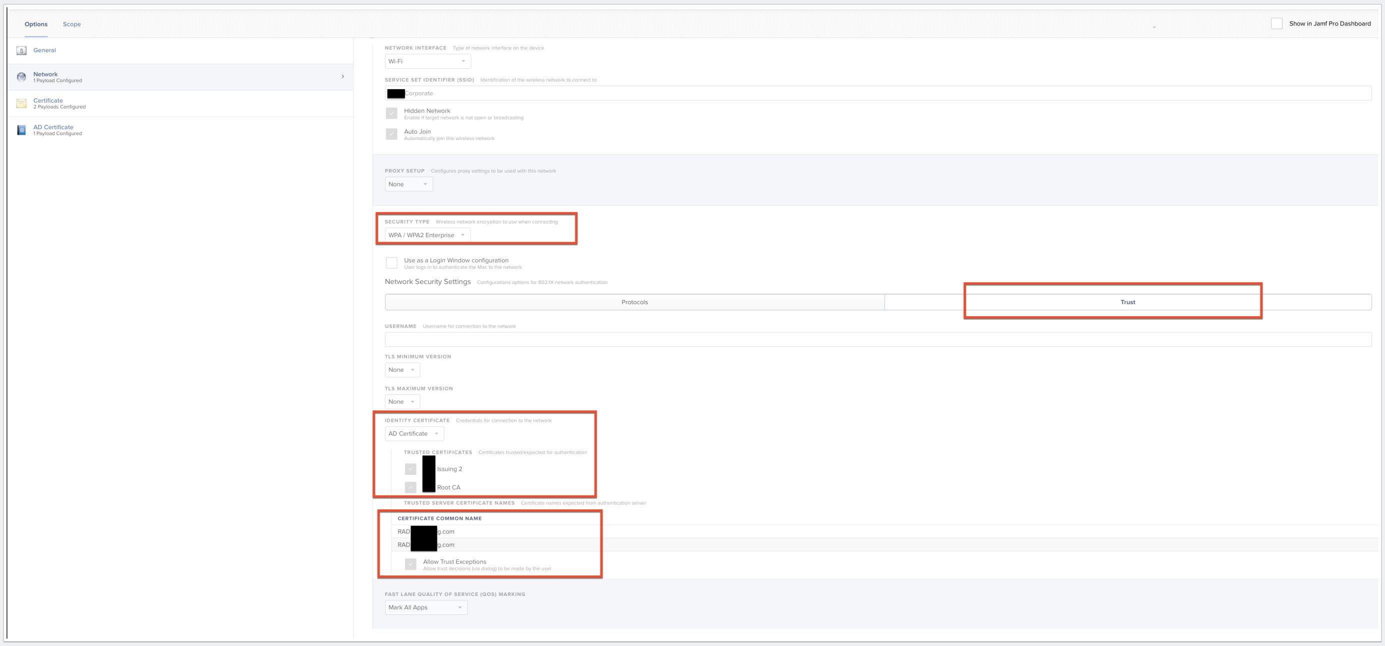
TLS MINIMUM VERSION
None

TLS MAXIMUM VERSION
None

IDENTITY CERTIFICATE Credentials for connection to the network
AD Certificate

FAST LANE QUALITY OF SERVICE (QOS) MARKING
Mark All Apps

Network: Trust



NETWORK INTERFACE Type of network interface on the device
Wi-Fi

SERVICE SET IDENTIFIER (SSID) Identification of the wireless network to connect to
[redacted]Corporate

☑ Hidden Network
Enable if target network is not open or broadcasting

☑ Auto Join
Automatically join this wireless network

PROXY SETUP Configures proxy settings to be used with this network
None

SECURITY TYPE Wireless network encryption to use when connecting
WPA / WPA2 Enterprise

□ Use as a Login Window configuration
User logs in to authenticate the Mac to the network

Network Security Settings Configurations options for 802.1X network authentication

USERNAME Username for connection to the network

TLS MINIMUM VERSION
None

TLS MAXIMUM VERSION
None

IDENTITY CERTIFICATE Credentials for connection to the network
AD Certificate

TRUSTED CERTIFICATES Certificates trusted/expected for authentication
☑ [redacted] Issuing 2
☑ Root CA

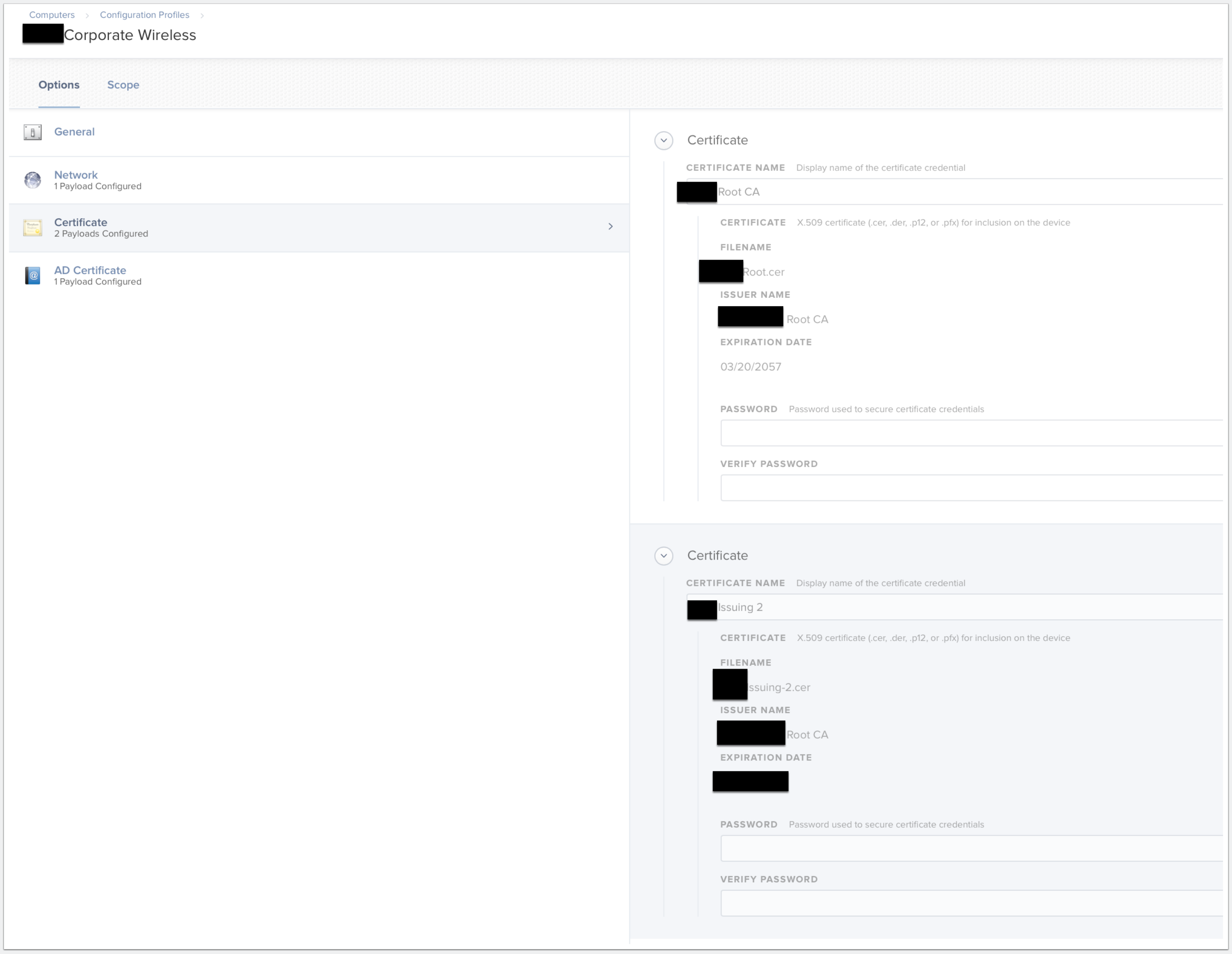
TRUSTED SERVER CERTIFICATE NAMES Certificate names expected from authentication server

CERTIFICATE COMMON NAME
RAD[redacted]g.com
RADg.com

☑ Allow Trust Exceptions
Allow trust decisions (via dialog) to be made by the user

FAST LANE QUALITY OF SERVICE (QOS) MARKING
Mark All Apps

Certificate



[redacted]Corporate Wireless

Certificate

CERTIFICATE NAME Display name of the certificate credential

[redacted]Root CA

CERTIFICATE X.509 certificate (.cer, .der, .p12, or .pfx) for inclusion on the device

FILENAME

[redacted]Root.cer

ISSUER NAME

[redacted] Root CA

EXPIRATION DATE

03/20/2057

PASSWORD Password used to secure certificate credentials

VERIFY PASSWORD

Certificate

CERTIFICATE NAME Display name of the certificate credential

[redacted]Issuing 2

CERTIFICATE X.509 certificate (.cer, .der, .p12, or .pfx) for inclusion on the device

FILENAME

[redacted]ssuing-2.cer

ISSUER NAME

[redacted] Root CA

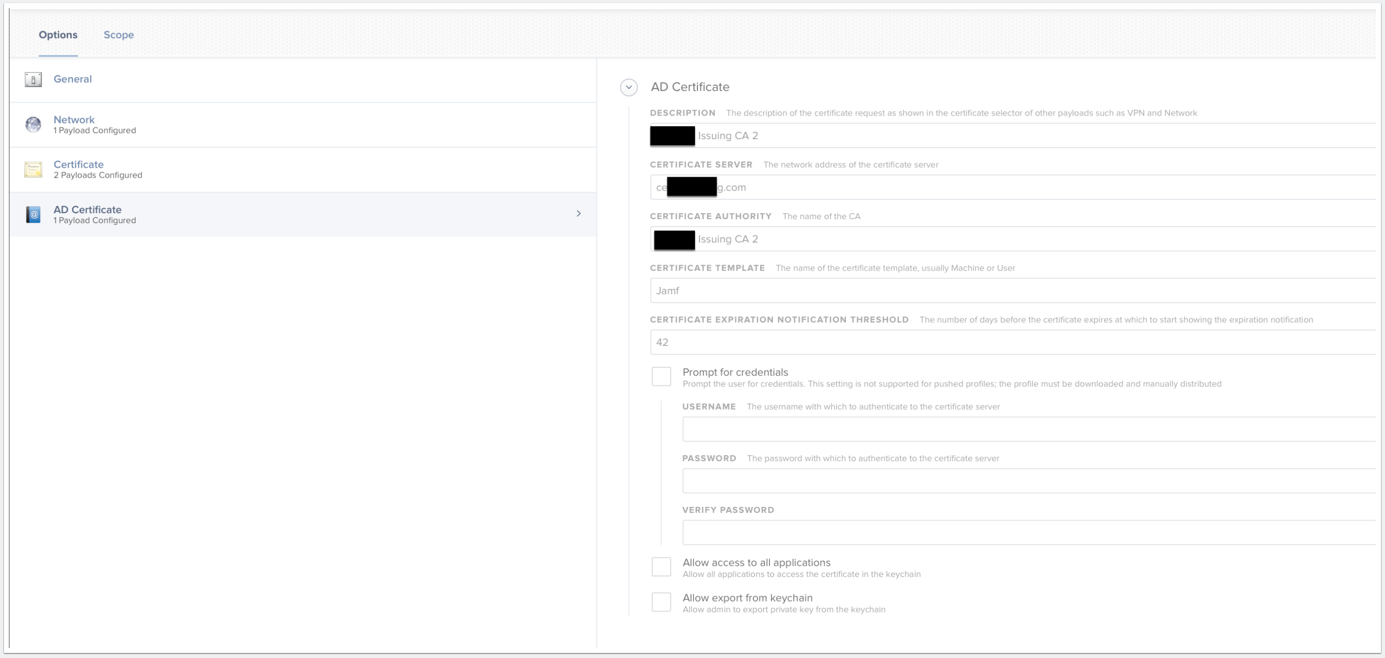
EXPIRATION DATE

[redacted]

PASSWORD Password used to secure certificate credentials

VERIFY PASSWORD

AD Certificate



AD Certificate

DESCRIPTION The description of the certificate request as shown in the certificate selector of other payloads such as VPN and Network

[redacted] Issuing CA 2

CERTIFICATE SERVER The network address of the certificate server

ce[redacted]g.com

CERTIFICATE AUTHORITY The name of the CA

[redacted] Issuing CA 2

CERTIFICATE TEMPLATE The name of the certificate template, usually Machine or User

Jamf

CERTIFICATE EXPIRATION NOTIFICATION THRESHOLD The number of days before the certificate expires at which to start showing the expiration notification

42

☐ Prompt for credentials
Prompt the user for credentials. This setting is not supported for pushed profiles; the profile must be downloaded and manually distributed

USERNAME The username with which to authenticate to the certificate server

PASSWORD The password with which to authenticate to the certificate server

VERIFY PASSWORD

☐ Allow access to all applications
Allow all applications to access the certificate in the keychain

☐ Allow export from keychain
Allow admin to export private key from the keychain