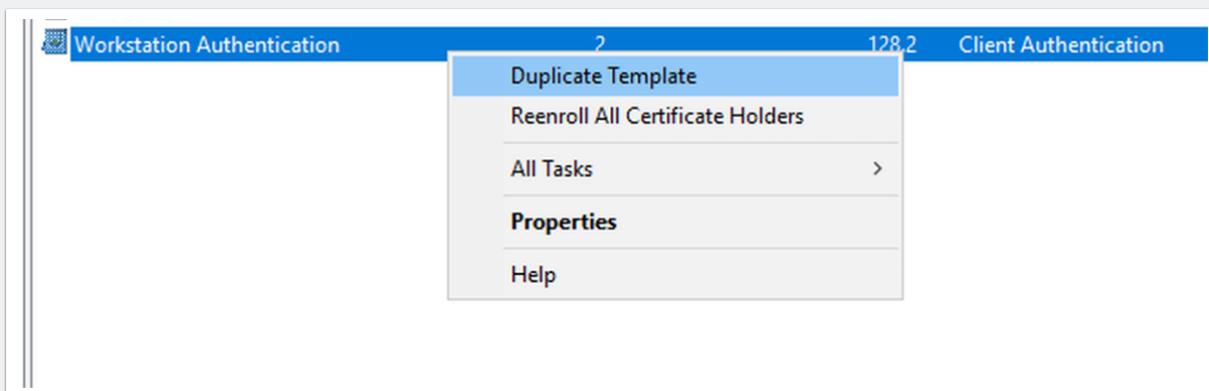


# JAMF PRO ADCS Full Setup Ver. 1.0

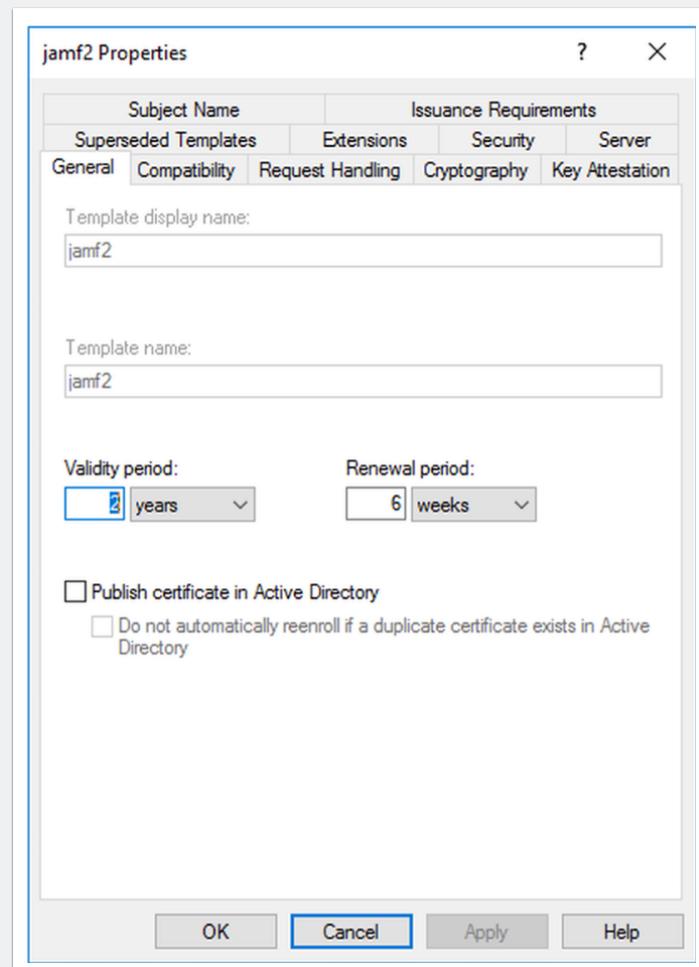
Created by: Kyle Ericson

## Internal CA



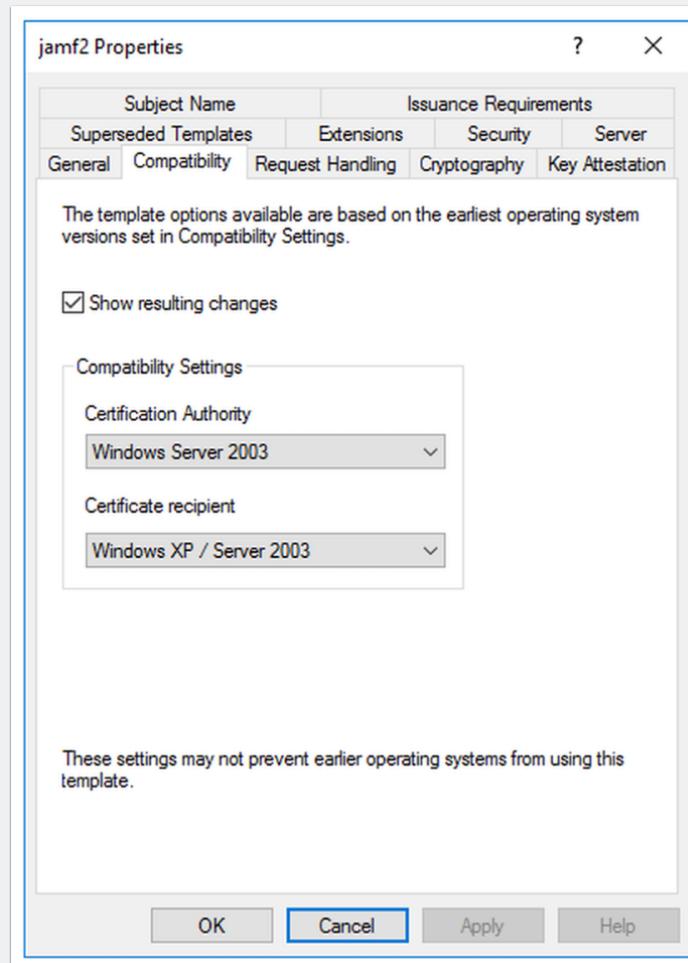
# JAMF PRO ADCS Full Setup Ver. 1.0

## General



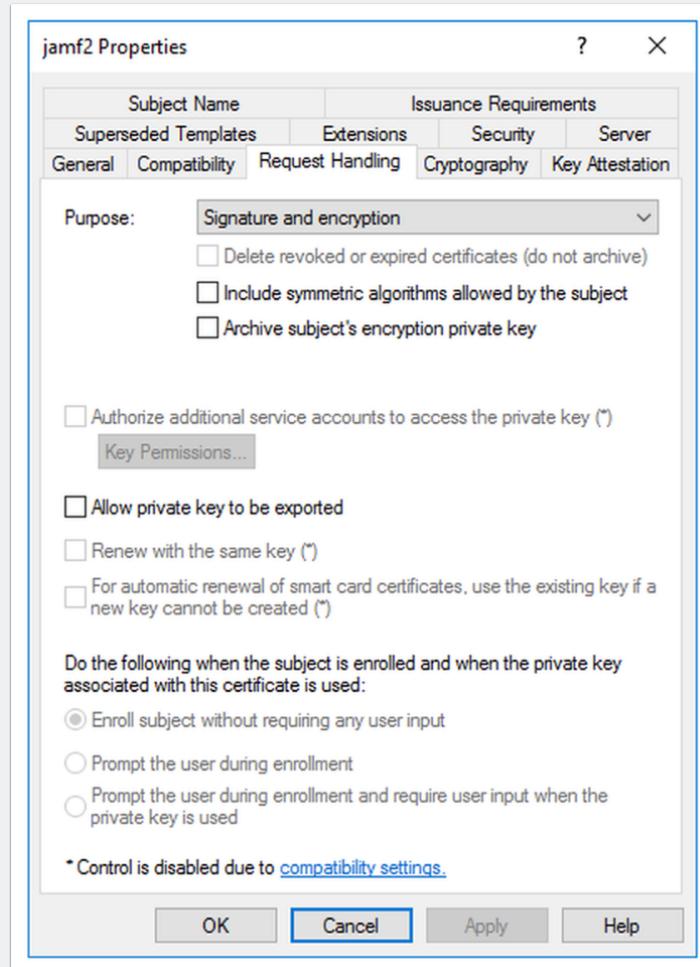
# JAMF PRO ADCS Full Setup Ver. 1.0

## Compatibility



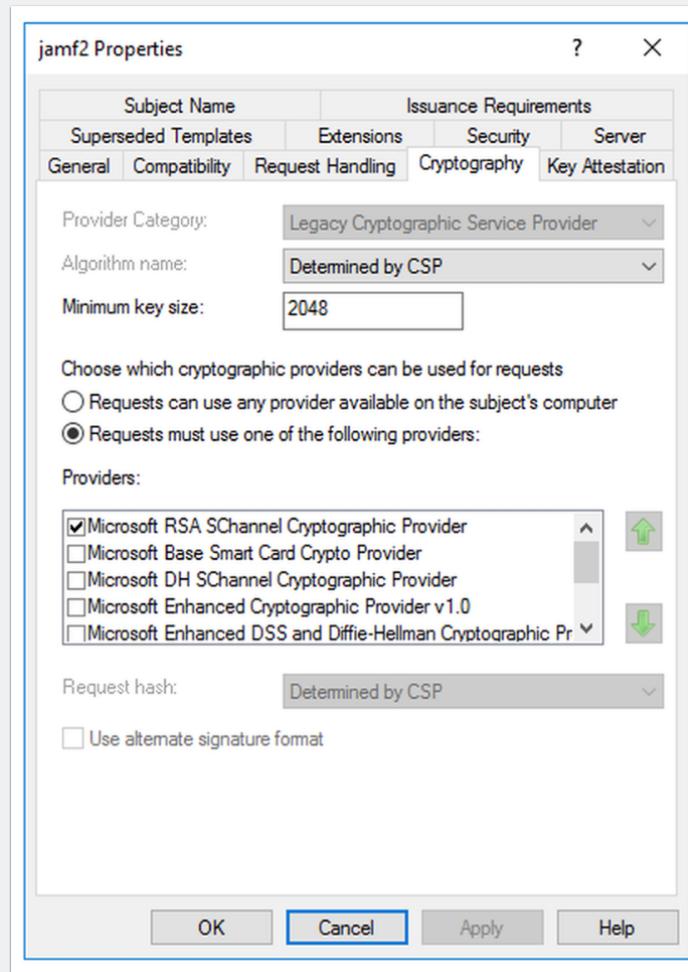
# JAMF PRO ADCS Full Setup Ver. 1.0

## Request Handling



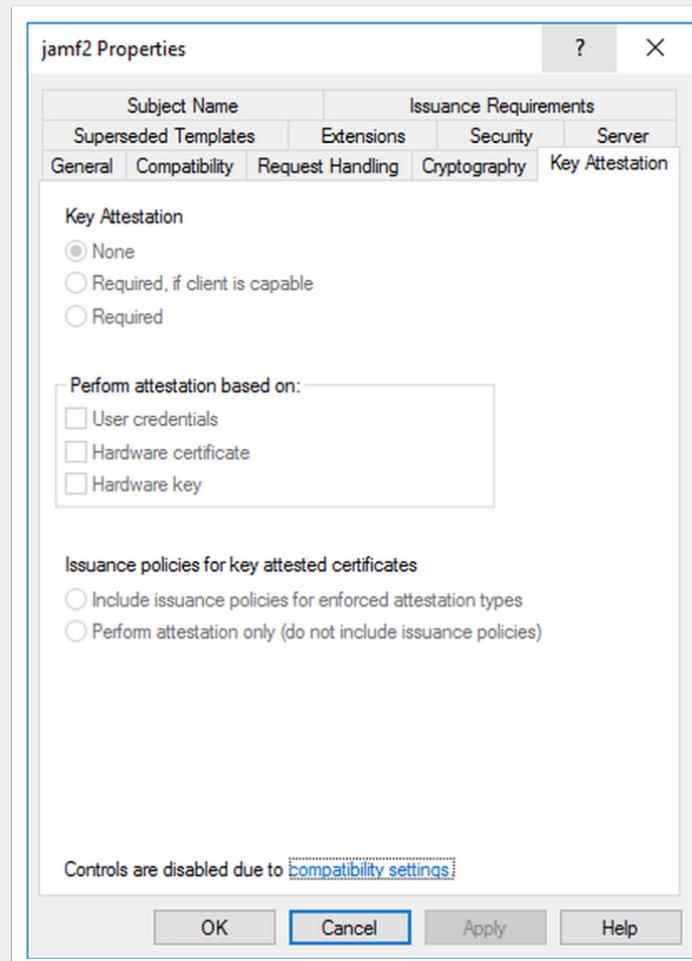
# JAMF PRO ADCS Full Setup Ver. 1.0

## Cryptography



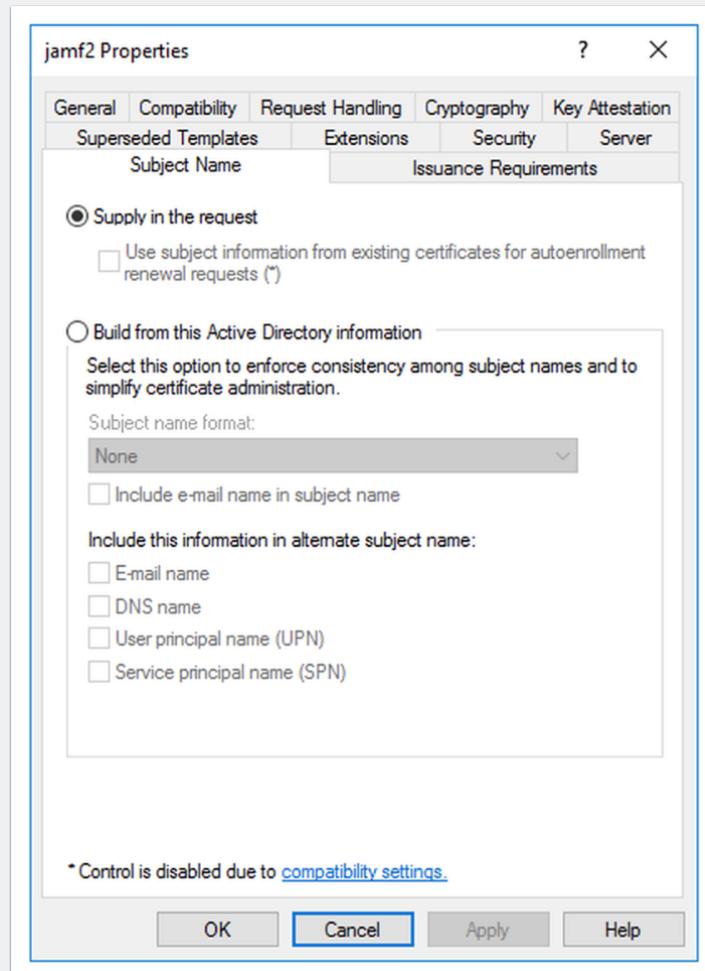
# JAMF PRO ADCS Full Setup Ver. 1.0

## Key Attestation



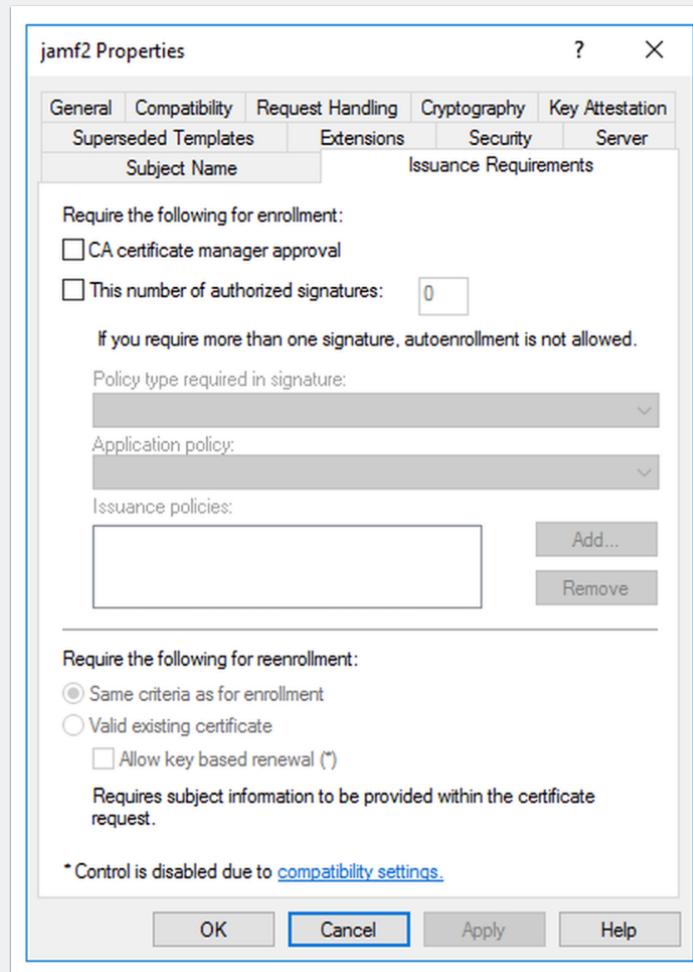
# JAMF PRO ADCS Full Setup Ver. 1.0

## Subject Name



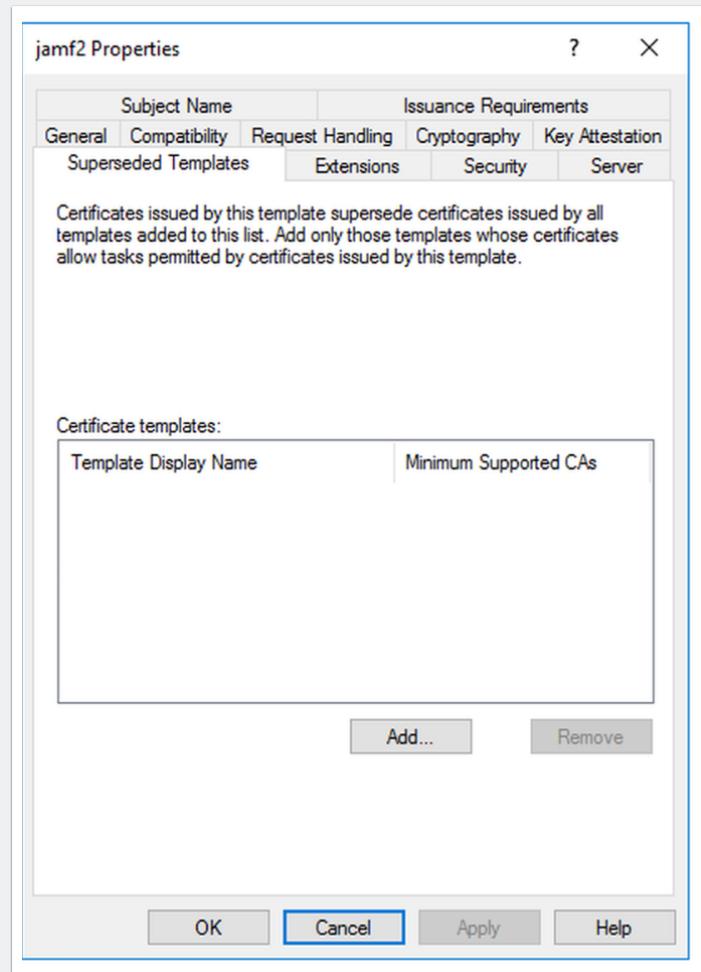
# JAMF PRO ADCS Full Setup Ver. 1.0

## Issuance Requirements



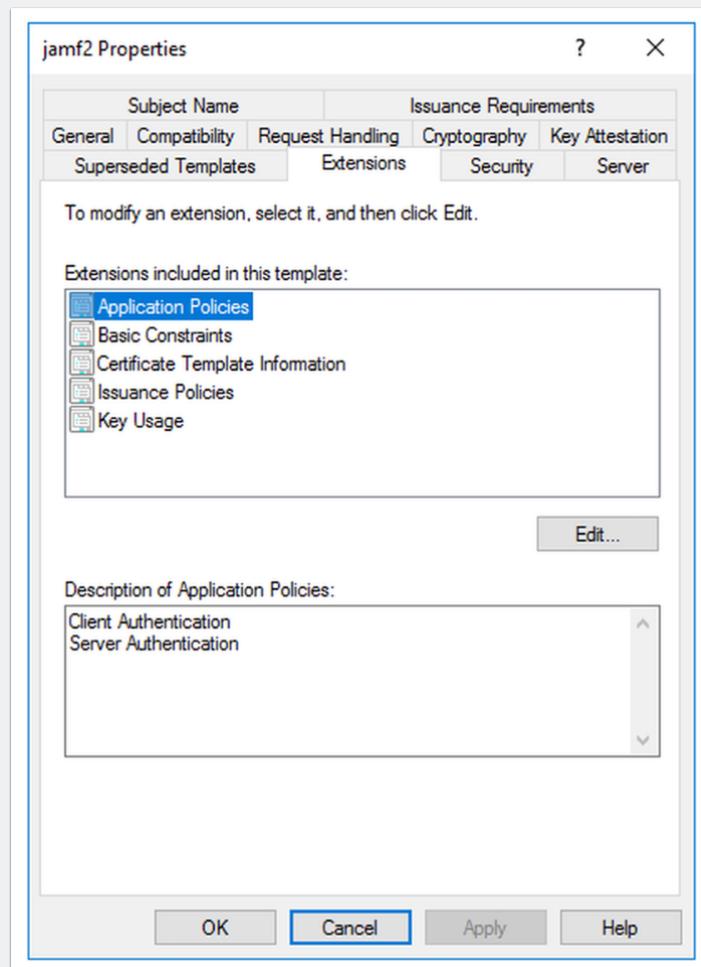
# JAMF PRO ADCS Full Setup Ver. 1.0

## Superseded Templates



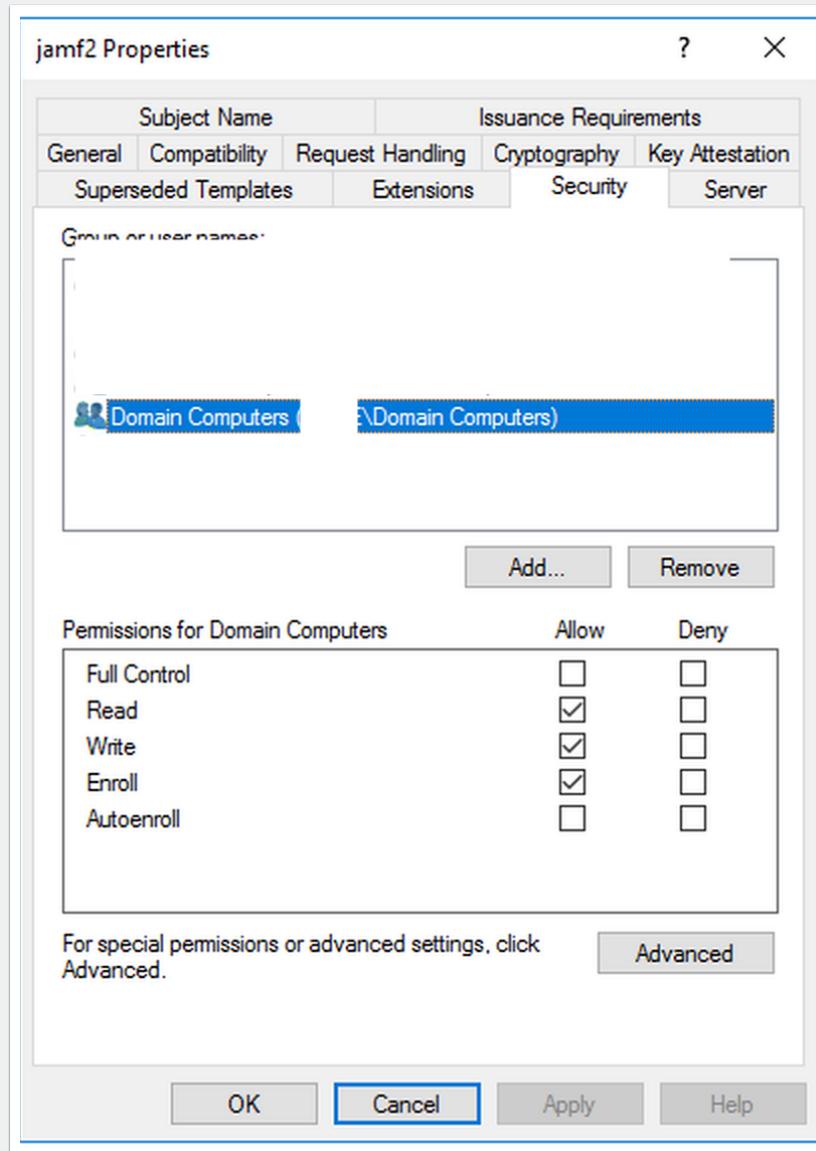
# JAMF PRO ADCS Full Setup Ver. 1.0

## Extensions



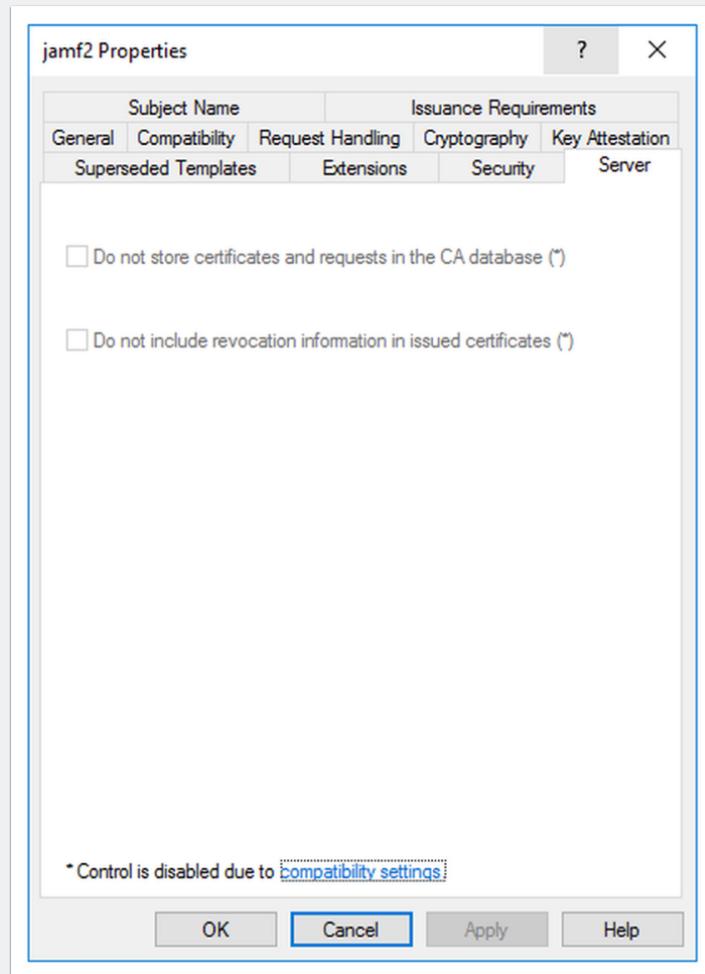
# JAMF PRO ADCS Full Setup Ver. 1.0

## Security



# JAMF PRO ADCS Full Setup Ver. 1.0

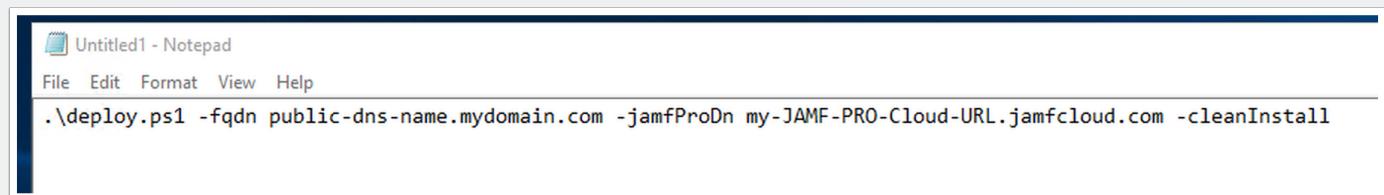
## Server



# JAMF PRO ADCS Full Setup Ver. 1.0

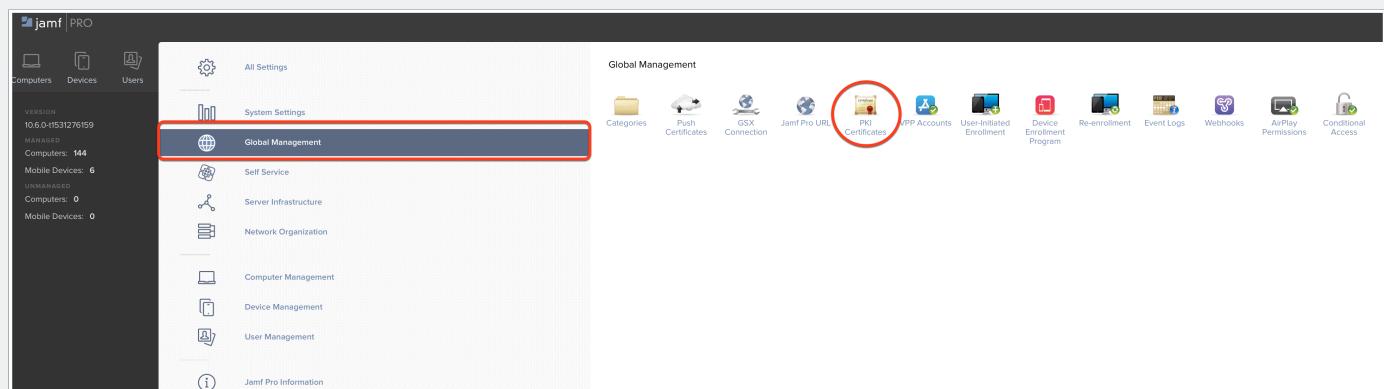
## Install ADCS Connector

On the server where you will install the ADCS connector use this info. I have JAMF in the Cloud so I have a server with a public DNS name.



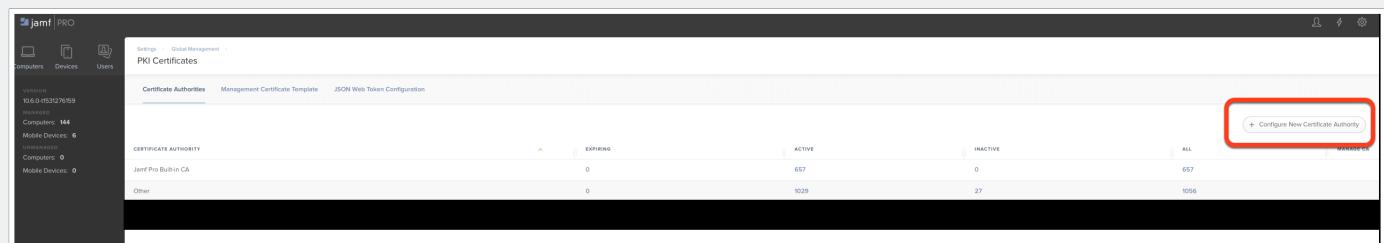
```
Untitled1 - Notepad
File Edit Format View Help
.\deploy.ps1 -fqdn public-dns-name.mydomain.com -jamfProDn my-JAMF-PRO-Cloud-URL.jamfcloud.com -cleanInstall
```

## JAMF PKI Setup



The screenshot shows the JAMF PRO Global Management interface. The left sidebar lists various management categories: Computers, Devices, Users, System Settings, Global Management (which is selected and highlighted with a red box), Self Service, Server Infrastructure, Network Organization, Computer Management, Device Management, User Management, and Jamf Pro Information. The right side of the screen displays the Global Management settings, including sections for Categories, Push Certificates, GSX Connection, Jamf Pro URL, and PKI Certificates. The PKI Certificates icon is circled in red.

## Configure new cert auth

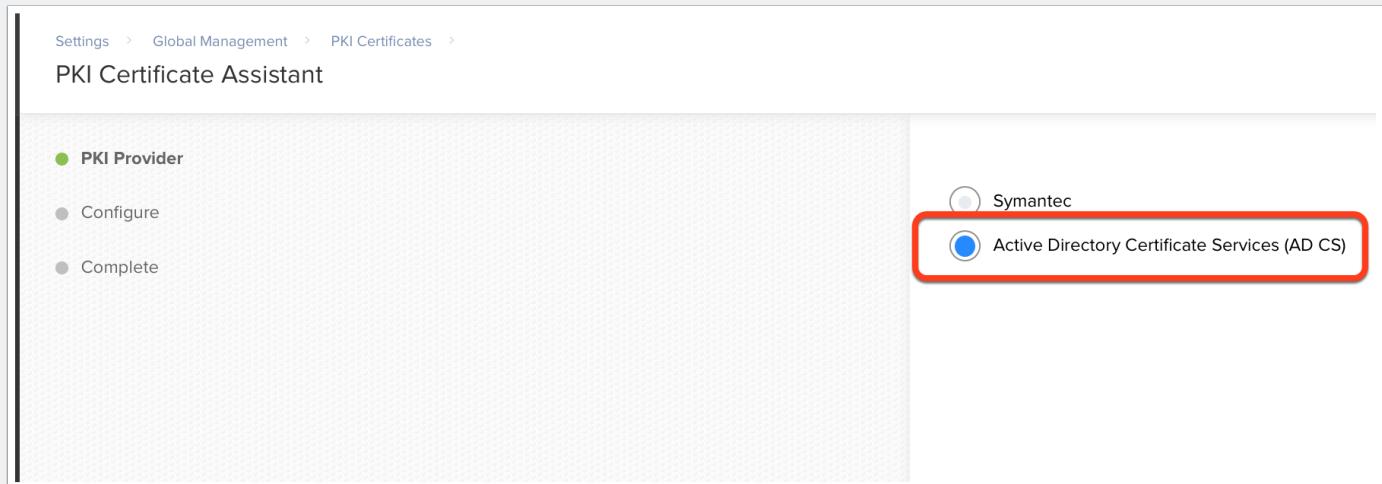


The screenshot shows the JAMF PRO PKI Certificates configuration page. The top navigation bar includes Settings, Global Management, and PKI Certificates. Below this, there are tabs for Certificate Authorities, Management Certificate Template, and JSON Web Token Configuration. A prominent red box highlights the '+ Configure New Certificate Authority' button in the top right corner of the main content area. The main table lists certificate authorities, showing columns for Certificate Authority, Expiring, Active, Inactive, and counts for All and Managed.

CERTIFICATE AUTHORITY	EXPIRING	ACTIVE	INACTIVE	ALL	MANAGED
Jamf Pro Built-in CA	0	657	0	657	657
Other	0	9029	27	1056	1056

# JAMF PRO ADCS Full Setup Ver. 1.0

## AD CS



# JAMF PRO ADCS Full Setup Ver. 1.0

## AD CS Server Intergration

Add in your Issuing CA info:

FQDN of CA: cert40.mydomain.com

CA Name: Issuing CA 5.mydomain.com

URL or IP Address of ADCS Server (Public DNS name): romandog.mydomain.com

Upload the certs that JAMF ADCS connector gives you with the password.

The screenshot shows the 'AD CS Server Integration' configuration screen. It is divided into two main sections: 'AD CS Server Integration' and 'Jamf AD CS Connector'.

**AD CS Server Integration** (Settings to integrate Jamf Pro with Active Directory Certificate Service)

- FULLY QUALIFIED DOMAIN NAME**: Fully qualified domain name of the certificate authority server  
[Required]
- CA NAME**: Name of the certificate authority  
[Required]

**Jamf AD CS Connector** (Settings for Jamf Pro to request a certificate from Active Directory Certificate Service via the Jamf AD CS Connector)

- URL OR IP ADDRESS**: URL or IP address of the Jamf AD CS Connector  
[Required]
- SERVER CERTIFICATE**: Certificate required for Jamf Pro to verify identity of the Jamf AD CS Connector (.pem, .cer)  
Upload button
- CLIENT CERTIFICATE**: Certificate required for Jamf Pro to authenticate with the Jamf AD CS Connector (.pfx, .p12)  
Upload button

# JAMF PRO ADCS Full Setup Ver. 1.0

## JAMF Profile

The screenshot shows the JAMF Pro ADCS Full Setup interface for creating a new configuration profile named "Corporate". The "Network" tab is selected. The configuration includes:

- WIFI:** Service Set Identifier (SSID) is "Corporate".
  - Hidden Network: The network is not open or broadcasting.
  - Auto Join: Automatically joins this wireless network.
- PROXY SETUP:** Configures proxy settings to be used with this network. Set to "None".
- SECURITY TYPE:** wireless network encryption to use when connecting. Set to "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:** Accepted EAP Types: TLS, TTLS, LEAP, PEAP, EAP-FAST, EAP-SIM, EAP-AKA.
  - Trust:** None.
- USERNAME:** Username for connection to the network.
- TLS MINIMUM VERSION:** None.
- TLS MAXIMUM VERSION:** None.
- IDENTITY CERTIFICATE:** Credentials for connection to the network. Issuing CA: 2.
- FAST LANE QUALITY OF SERVICE (QOS) MARKING:** Mark All Apps.

# JAMF PRO ADCS Full Setup Ver. 1.0

## Network: Protocols

The screenshot shows the 'Network: Protocols' configuration page in JAMF Pro ADCS. The left sidebar lists 'General', 'Network (Phylos Configured)', and 'Certificate (Phylos Configured)'. The main area is titled 'Wi-Fi' and contains the following sections:

- SERVICE SET IDENTIFIER (SSID):** Identification of the wireless network to connect to. Options include 'Corporate' (selected), 'Hidden Network' (disabled), and 'Auto Join' (disabled).
- PROXY SETUP:** Configures proxy settings to be used with this network. Set to 'None'.
- SECURITY TYPE:** Wireless network encryption to use when connecting. Set to 'WPA Enterprise'.
- Use as a Logon Window configuration:** A checkbox that, when checked, enables the Mac to use the network for logon.
- ACCEPTED EAP TYPES:** Authentication protocols supported on target devices. Options include TLS, TTLS, LEAP, PEAP, EAP-FAST, EAP-SIM, and EAP-AKA. 'TLS' is selected.
- USERNAME:** Username for connection to the network.
- TLS MINIMUM VERSION:** Set to 'None'.
- TLS MAXIMUM VERSION:** Set to 'None'.
- IDENTITY CERTIFICATE:** Certificate for connection to the network. Set to 'Issuing CA 2'.
- FAST LANE QUALITY OF SERVICE (QOS) MARKING:** Set to 'Mark All Apps'.

# JAMF PRO ADCS Full Setup Ver. 1.0

## Network: Trust

The screenshot shows the 'Corporate' configuration profile in JAMF Pro. The left sidebar lists 'General', 'Options', 'Scope', 'Network' (selected), and 'Certificate'. The main pane shows 'Network' settings:

- GENERAL**: Includes sections for 'Network' (selected), 'Proxy Setup', 'Security Type' (WPA2 Enterprise), and 'Network Security Settings'.
- PROTOCOLS**: Shows a 'Trust' section with a red box around it.
- IDENTITY CERTIFICATE**: Shows a 'Using CA 2' section with a red box around it. It includes 'TRUSTED CERTIFICATES' (listing 'Root CA' and 'Root CA') and 'TRUSTED SERVER CERTIFICATE NAMES' (listing 'RAD539.com' and 'RAD549.com').
- PARTICLE MARKING**: Includes 'Mark All Apps'.

# JAMF PRO ADCS Full Setup Ver. 1.0

## Certificate

The screenshot displays three stacked certificate configuration panels within the JAMF PRO ADCS Full Setup interface.

**Panel 1: Certificate (Issuing CA 2)**

- CERTIFICATE NAME:** Display name of the certificate credential  
Issuing CA 2
- CERTIFICATE SUBJECT:** Representation of a X.500 name (e.g. O=CompanyName, CN=FOO)  
CN=\$USERNAME@ti.com
- SUBJECT ALTERNATIVE NAME TYPE:** The type of a subject alternative name  
None
- TEMPLATE NAME:** The name of the certificate template, usually Machine or User  
jamf2

**Panel 2: Certificate (Issuing Cert)**

- CERTIFICATE:**
  - FILENAME:** Issuing-2.cer
  - ISSUER NAME:** CN=Tri Root CA
  - EXPIRATION DATE:** 03/20/2037
- PASSWORD:** Password used to secure certificate credentials  
[Redacted]
- VERIFY PASSWORD:**  
[Redacted]

**Panel 3: Certificate (Root CA)**

- CERTIFICATE:**
  - FILENAME:** Root.cer
  - ISSUER NAME:** CN=Tri Root CA
  - EXPIRATION DATE:** 03/20/2057