MATRIX42
SMARTER WORKSPACE – BETTER LIFE

Matrix42 Silverback

Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

Version 1.6

February 26, 2016

Copyright © 2000 - 2014 Matrix42 AG

This documentation is copyright protected. All rights are reserved by Matrix42 AG.

Any other use, in particular the disclosure to third parties, storage in a data system, dissemination, processing, presentation, performance and demonstration are prohibited. This applies to the entire document, as well as parts thereof.

Subject to change. Reprint, also in excerpts, is permitted only with the written consent of Matrix42 AG.

The software described in this document is subject to a permanent development due to which there may be differences in the documentation and the actual software. This documentation is not entitled to the actual functionality of the software.

Apple and **Mac OS X** are registered trademarks of Apple Inc.
Citrix® software or **Citrix® server** are Trademarks and Registered Trademarks of Citrix Systems, Inc. in the United States and other countries.
cygwin is copyrighted by Red Hat Inc. 1996-2003.
expat is copyrighted by Thai Open Source Software Center Ltd.
gSOAP is copyrighted by Robert A. van Engelen, Genivia, Inc. All rights reserved.
Iconv is copyrighted by 1999-2003 Free Software Foundation, Inc.
Iperf is copyrighted by the University of Illinois, except for the gnu_getopt.c, gnu_getopt_long.c, gnu_getopt.h files, and inet_aton.c, which are under the GNU General Public License.
Libmspack (C) 2003-2004 by Stuart Caie <kyzer@4u.net>.
OpenSSL This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.
PuTTY is copyrighted by Simon Tatham. Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, and CORE SDI S.A.
RSA Data Security, Inc. MD5 Message-Digest Algorithm is copyrighted by RSA Data Security Inc. Created 1991. All rights reserved.
rsync is an open source utility that provides fast incremental file transfer. rsync is freely available under the GNU General Public License version 2.
runcontrol The Initial Developer of the Original Code is James Clark. Portions created by James Clark are Copyright (c) 1998 James Clark. All rights reserved.
SNMP++ Copyright (c) 1996 Hewlett-Packard Company.
VMware, the **VMware "boxes" logo and design, Virtual SMP, VMotion vSphere, vSphere Hypervisor (ESXi), ESX, View, ThinApp, vCenter** and **vCloud** are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.
Windows, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, and **Windows Server 2012** are registered trademarks of Microsoft Corporation.

Others, at this point not explicitly listed, company, brand and product names are trademarks or registered trademarks of their respective owners and are subject to trademark protection.

Contents

1. Introduction 4
2. Prerequisites 5
3. Certificate Authority Configuration 6
3.1. Creating the necessary Certificate Template 6
3.2. Publishing the Certificate Template 13
4. Configuring Silverback 14
4.1. Certificates for Exchange ActiveSync / VPN 14
4.1. Certificates for Enterprise Wi-Fi (RADIUS) 15
5. Publishing User Certificates in Active Directory for Enterprise Wi-Fi 16
5.1. Basic Overall Concept 16
5.2. Creating the necessary Certificate Template 16
5.2.1. Creating the Certificate Request Agent Template 17
5.2.2. Creating the Silverback Enterprise WiFi Template 21
5.3. Publishing the Newly Created Certificate Templates 24
5.4. Creating the Certificate Request Agent Certificate 25
5.5. Importing the Certificate Request Agent Certificate 28
5.6. Silverback Configuration 30
5.6.1. Silverback Web Settings Configuration 30
5.6.2. Silverback Device Profile Settings 31
5.1. Confirming That It Works! 32
5.1.1. Certificate Authority Requests 32
5.1.2. User Active Directory Object 32

Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

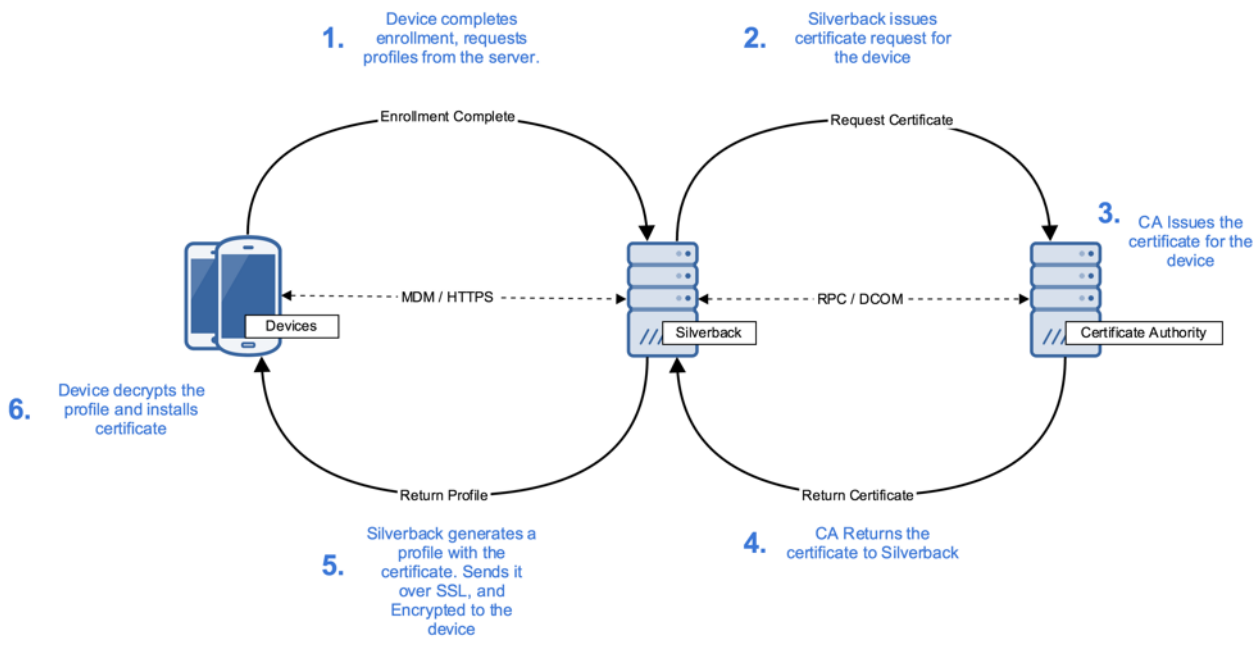
1. Introduction

This document will include the information necessary to integrate Silverback with a Microsoft Active Directory Certificate Authority, which can then be used to distribute User-Based Identity Certificates to users as they enroll into Silverback.

These devices can then be configured to authenticate themselves with this certificate across a range of technologies, such as:

- Exchange ActiveSync.
- Enterprise Wi-Fi Access Points (RADIUS Authentication)
- SharePoint Servers
- VPN Endpoint Appliances (check for current supported device list).

The following picture describes the topology of the Matrix42 solution approach:



2. Prerequisites

To properly integrate Silverback with your Microsoft Active Directory Certificate Authority you will need to ensure that all the following conditions are met:

- The Silverback Server is joined to the same Active Directory Domain as the Certificate Authority.
  - If using a Cloud Connector to connect to a Cloud Based Environment, then it is the Cloud Connector Object that needs to be Domain Joined.
- Dedicated 'Certificate Request' Active Directory Service Account (only required for Section 5 – Publishing Certificates in Active Directory)
- The Silverback Computer Object is added to the necessary Active Directory Groups outlined in the On Premise Solution Design Brief (Section 1.3) and copied below for your convenience:

Name: Silverback Mobile Device Manager
Type: Global Group
Members: $SilverbackComputerAccount

Name: Silverback Enterprise Device Management
Type: Universal Group
Members: Silverback Mobile Device Manager

NOTE: It is the Silverback Enterprise Device Management Group that we will be giving access to certain templates on the Certificate Authority.

Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

3. Certificate Authority Configuration

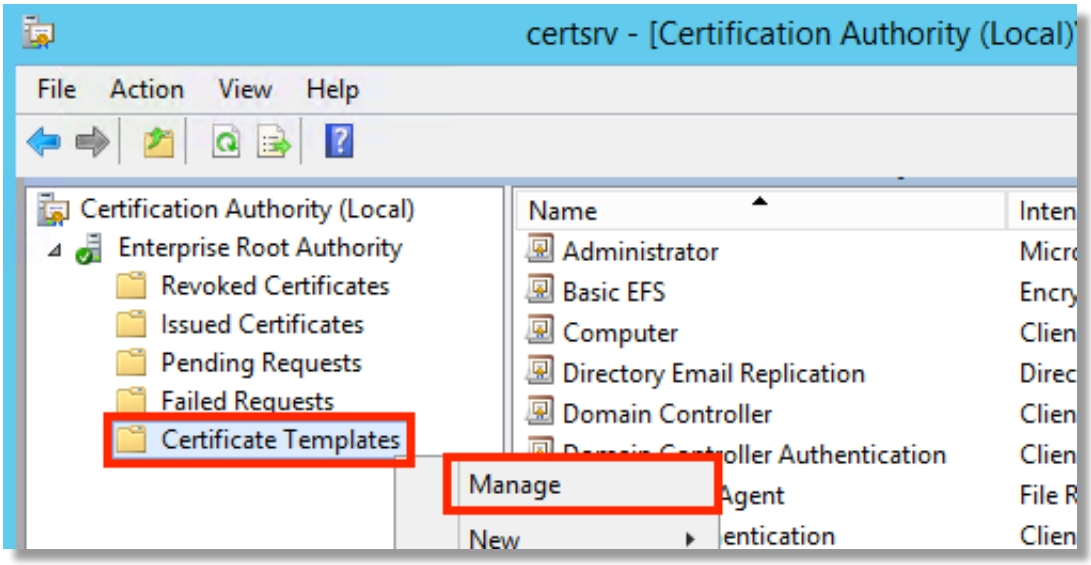
As Silverback will be requesting User-Based Certificates from your Certificate Authority it is necessary to configure the appropriate permissions so that these requests are successful and certificate are issued to devices.

3.1. Creating the necessary Certificate Template

First a dedicated template is created for Silverback to target for the Certificate Requests, to do this please use the following steps:

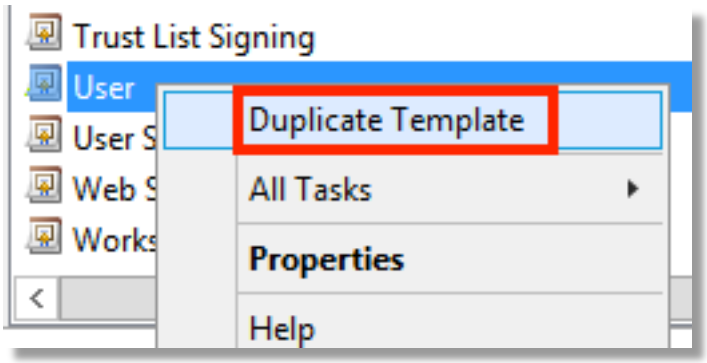
Log into your Certificate Authority, and open the Certificate Authority MMC snap-in.

Expand the Configuration Tree on the Right until the Certificate Templates section is visible.



Right-Click on Certificate Templates and click the Manage option to bring up the Certificate Template Console.

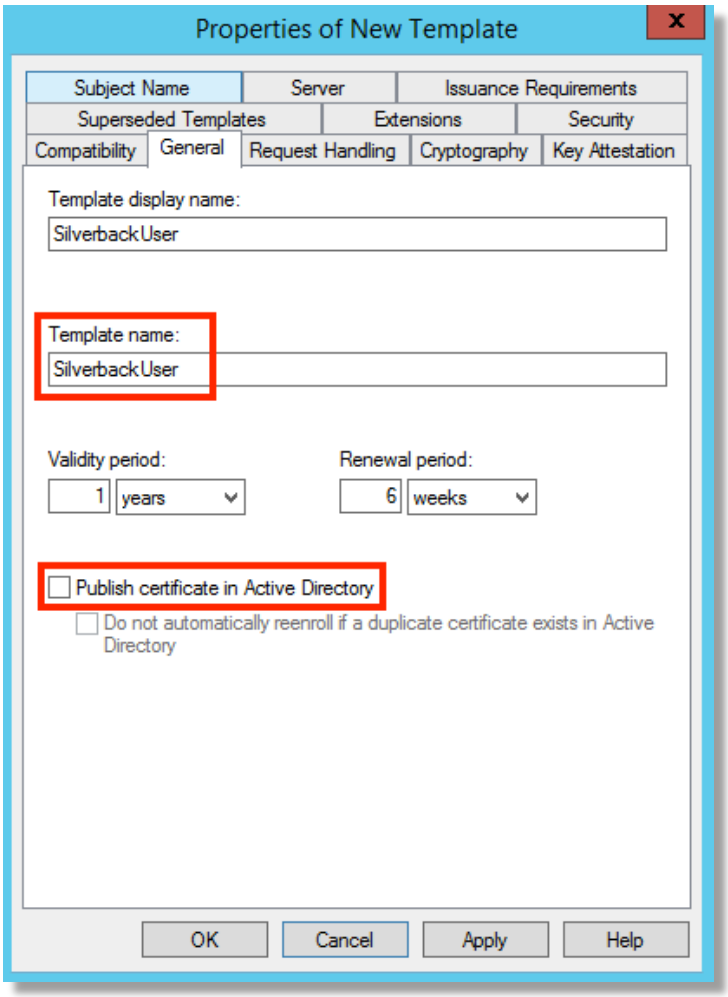
Find the 'User' template, Right-Click and select Duplicate Template.



Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

General Properties of the New Template

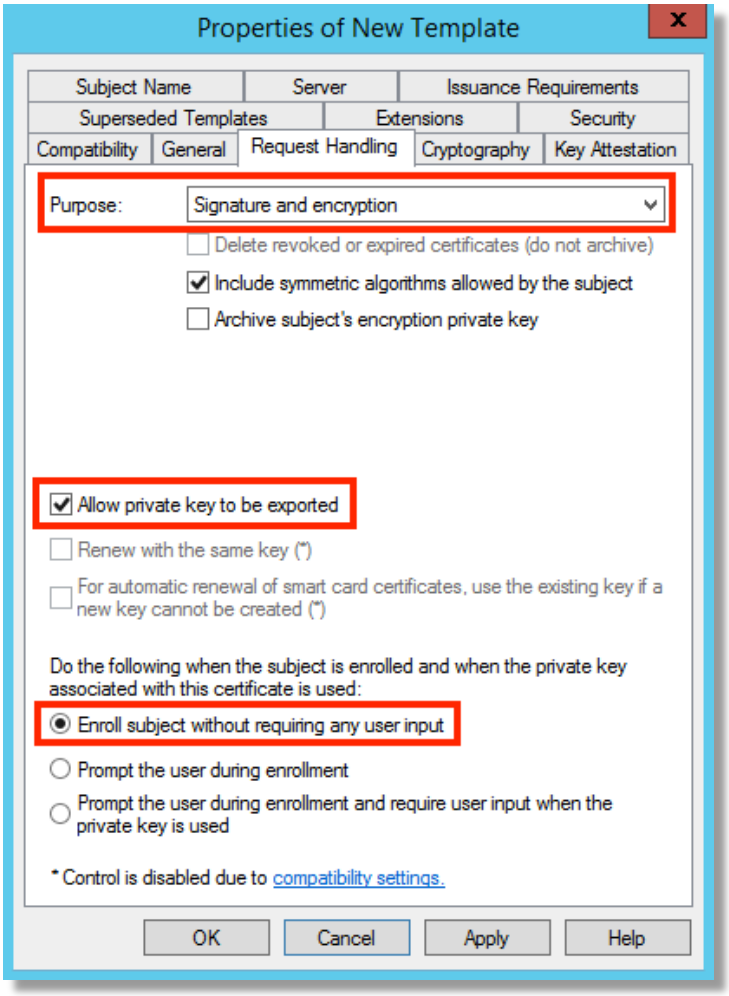
- Name the new Template ‘SilverbackUser’
- Ensure that ‘Publish Certificate in Active Directory is Unchecked.



Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

Request Handling Properties of the New Template

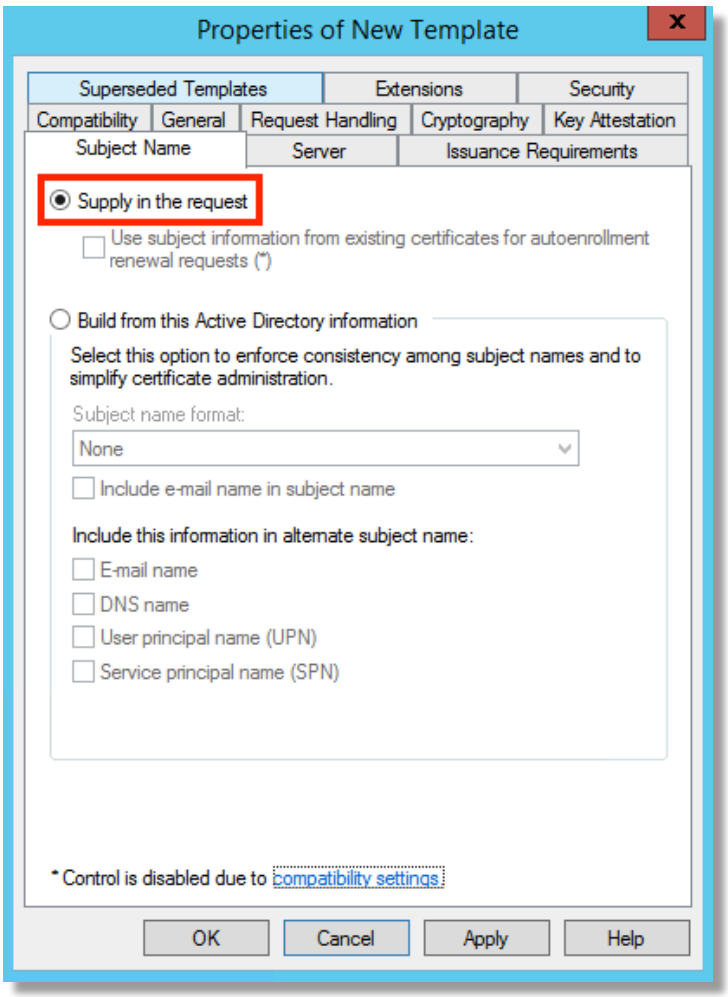
- Purpose: Signature and Encryption
- Allow Private Key to be Exported is Checked.
- Enroll the Subject without requiring any user input.



Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

Subject Name Properties of the New Template

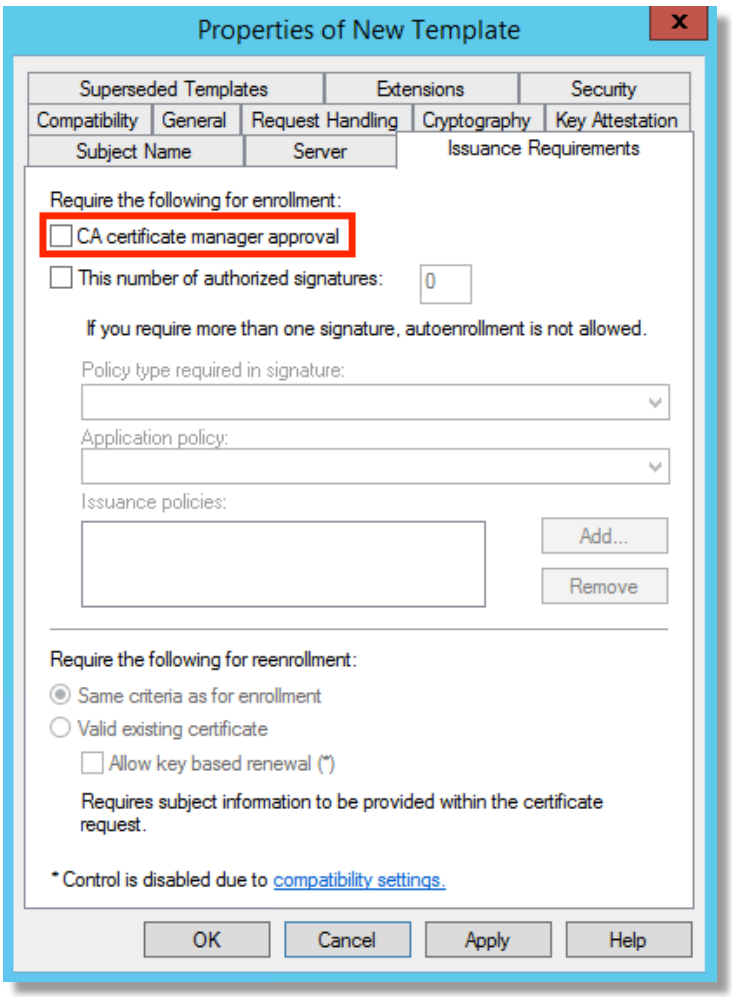
- Ensure this is set to Supply in the Request.



Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

Issuance Requirements Properties of the New Template

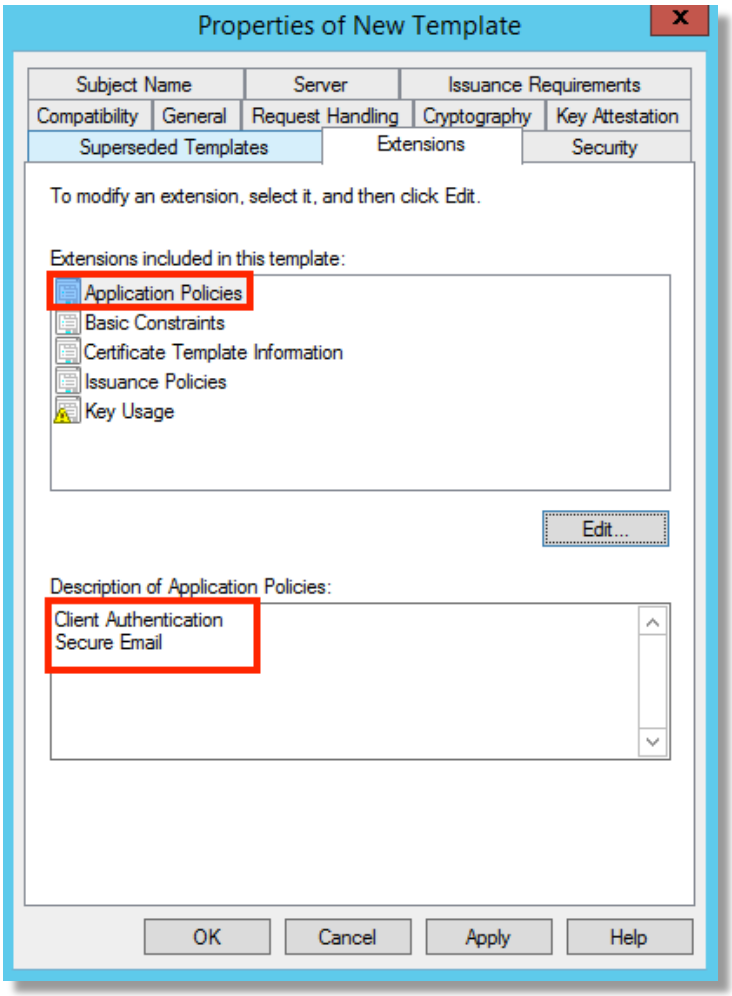
- Ensure that CA Certificate Manager Approval is Unchecked.



Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

Extensions Properties of the New Template

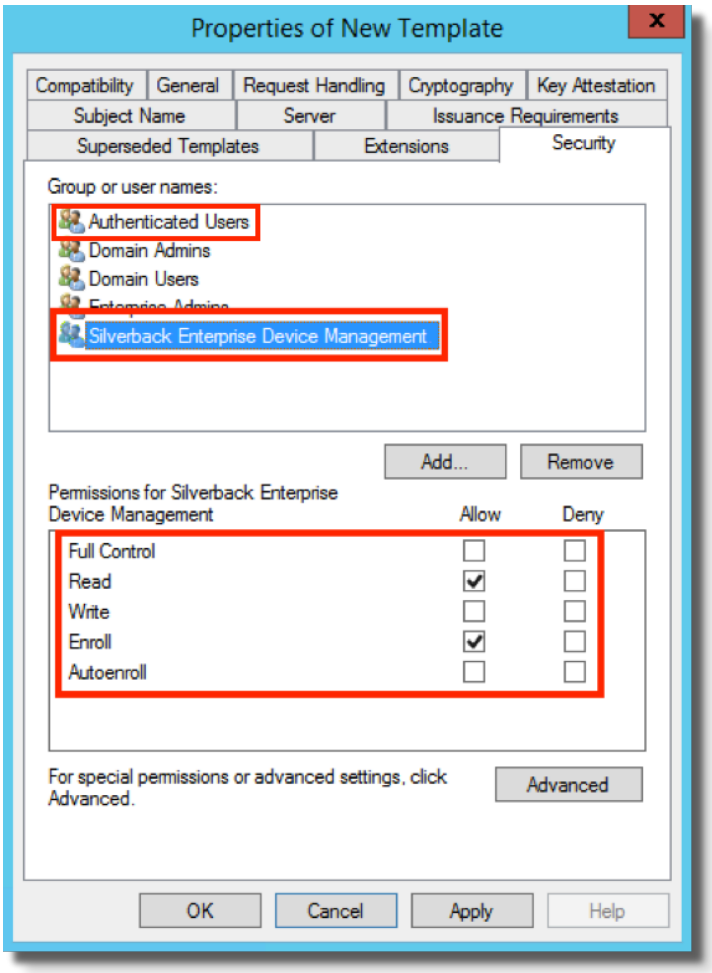
- The Certificate Template must be applying the Client Authentication & Secure Email Extensions to the Issued Certificates.



Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

Security Properties of the New Template

- The Silverback Enterprise Device Management Active Directory Group must have the READ and ENROLL Permission on the Certificate Template.
- The Authenticated Users Active Directory Group must have the READ and ENROLL Permission on the Certificate Template.



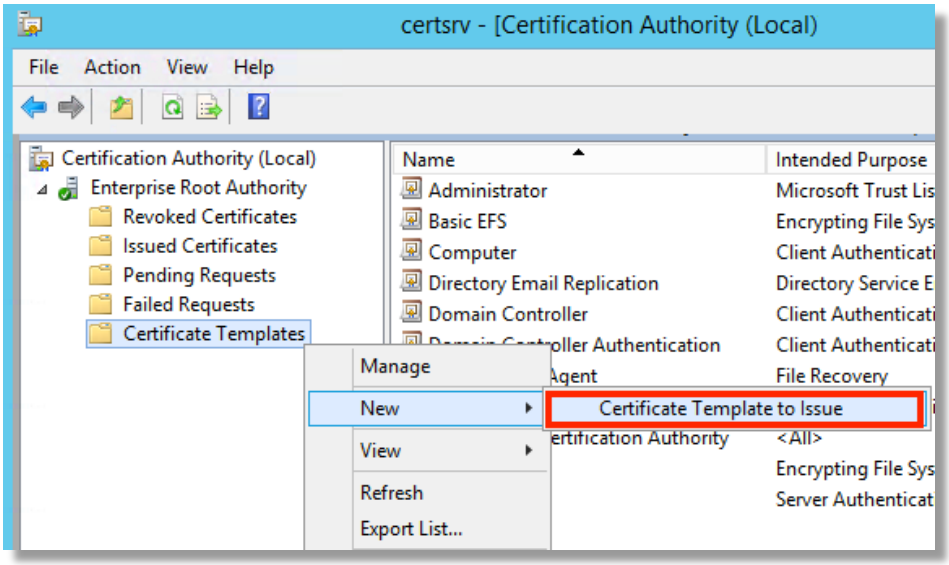
- Click OK to finish creating the Template.

Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

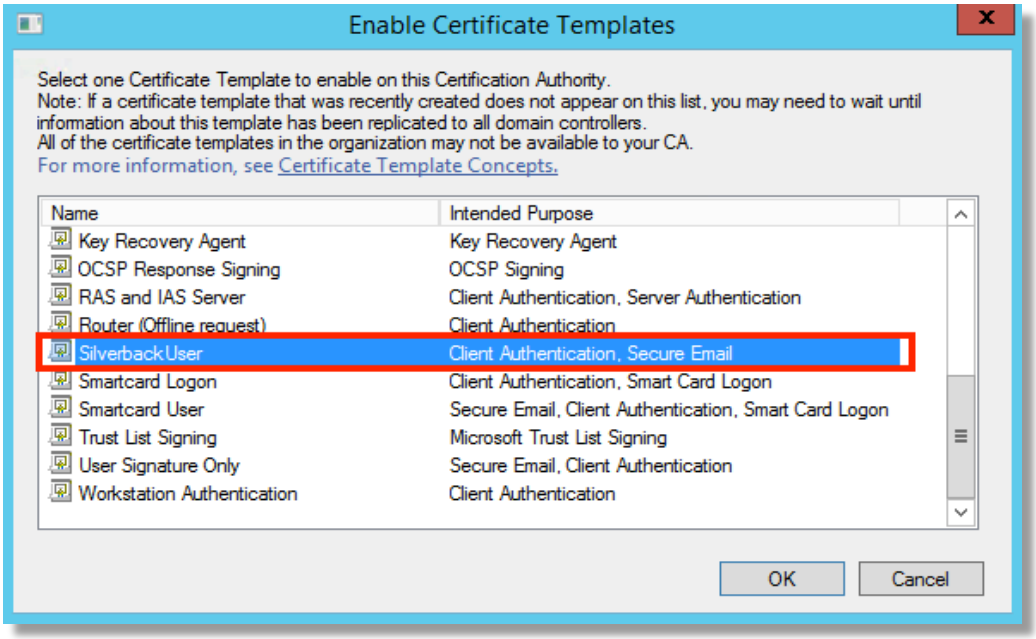
3.2. Publishing the Certificate Template

Next, we will need to publish the Certificate Template that we just created so that it is visible to the Silverback Computer Object.

- Log into your Certificate Authority, and open the Certificate Authority MMC snap-in.
- Expand the Configuration Tree on the Right until the Certificate Templates section is visible.



- Right-Click on Certificate Templates and navigate to the New > Certificate Template to Issue option.
- In the Enable Certificate Template popup box, select the 'SilverbackUser' template created earlier and click OK to finish publishing the Certificate.



4. Configuring Silverback

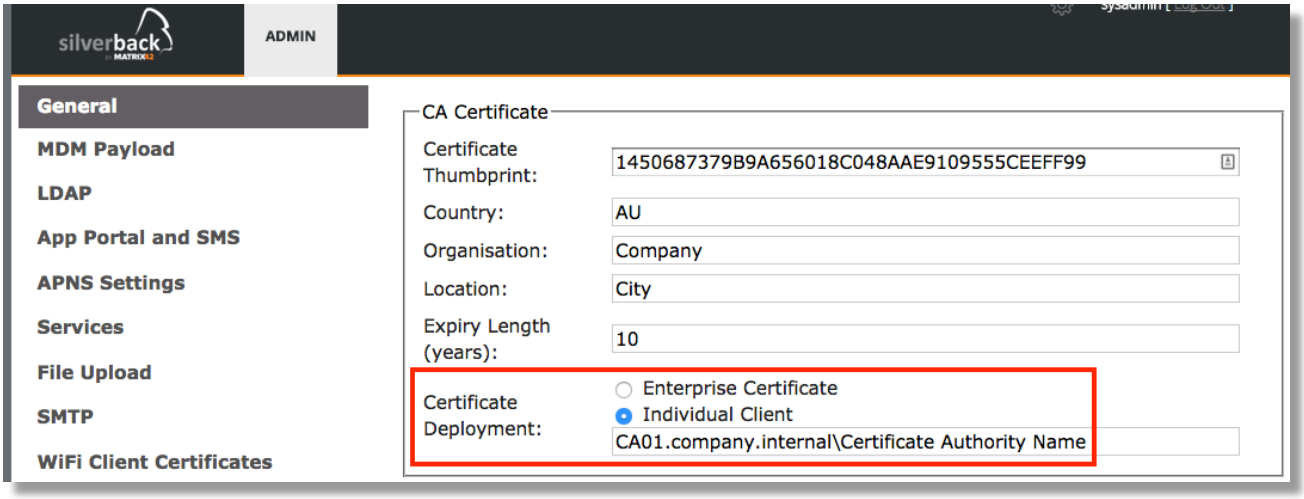
Once your Certificate Authority has been given the appropriate permissions on the newly configured Certificate Templates, it is time to configure Silverback to use them.

This configuration is done via the Silverback Web Interface, in the System Settings section.

4.1. Certificates for Exchange ActiveSync / VPN

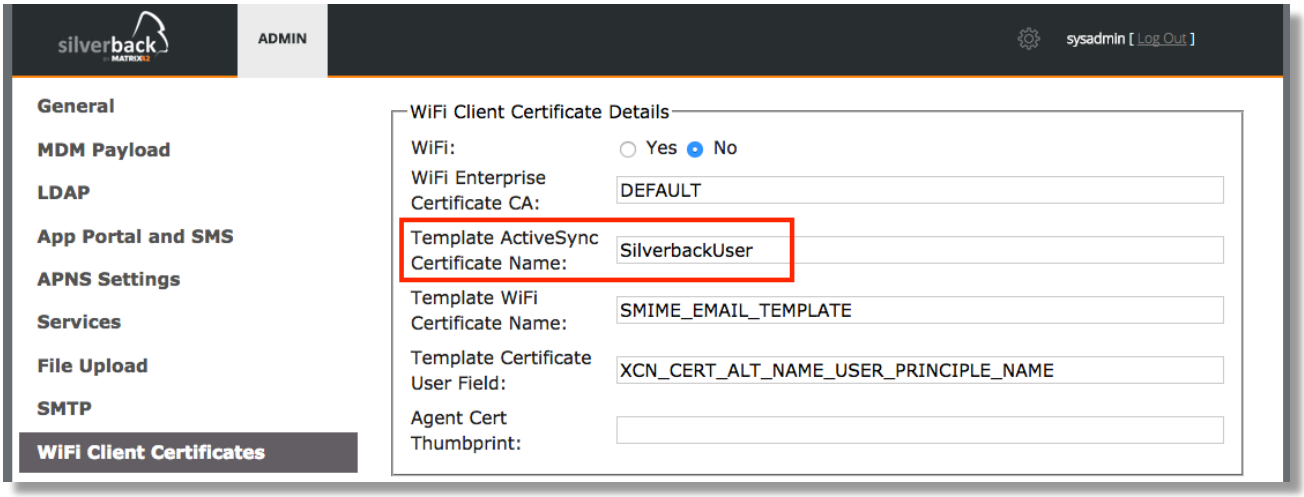
Log into the Silverback Web Console as a System Settings user so we can manipulate some of the finer settings of Silverback.

Under the General Section change the Certificate Deployment Option from Enterprise Certificate to Individual Client, and change the name from DEFAULT to be your Certificate Authority Address:



NOTE: The correct format for the CA Address is “FQDN \ Certificate Authority Name”.

Next, go to the WiFi Client Certificates section and populate the Template ActiveSync Certificate Name with the name of the Certificate Template created earlier.



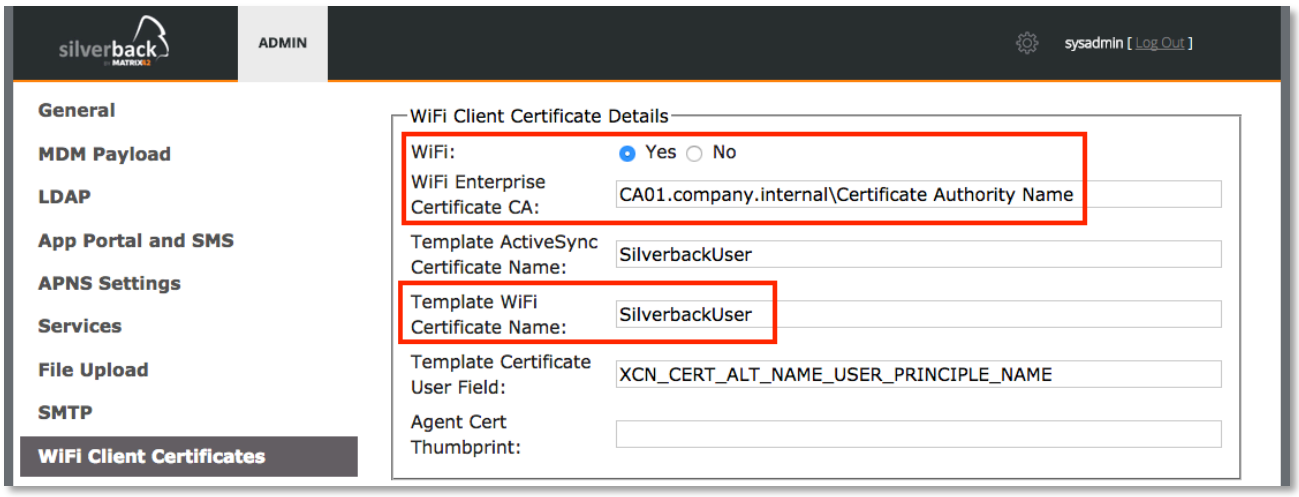
NOTE: If these settings are not correct, and Silverback is not able to request Certificate from the Certificate Authority – a device will not be able to leave the Blocked Container within Silverback, due to the fact that it is unable to complete moving into Managed without an Exchange Profile.

4.1. Certificates for Enterprise Wi-Fi (RADIUS)

Log into the Silverback Web Console as a System Settings user so we can manipulate some of the finer settings of Silverback.

Under the WiFi Client Certificates section, ensure this is switched to YES, and that the WiFi Enterprise Certificate CA is the Correct Address

Change the Template WiFi Certificate Name to match the Certificate Template created earlier.



5. Publishing User Certificates in Active Directory for Enterprise Wi-Fi

In some cases it is necessary for Silverback to publish a User Certificate into the enrolling user's Active Directory Object for authentication. The following is a guide that illustrates how this is achieved with Silverback.

5.1. Basic Overall Concept

In the previous sections of this document we have covered Silverback's Integration with your Internal Certificate authority to allow it to request Certificates for your enrolling users. This means that it is the Silverback Computer Object that is performing the requests.

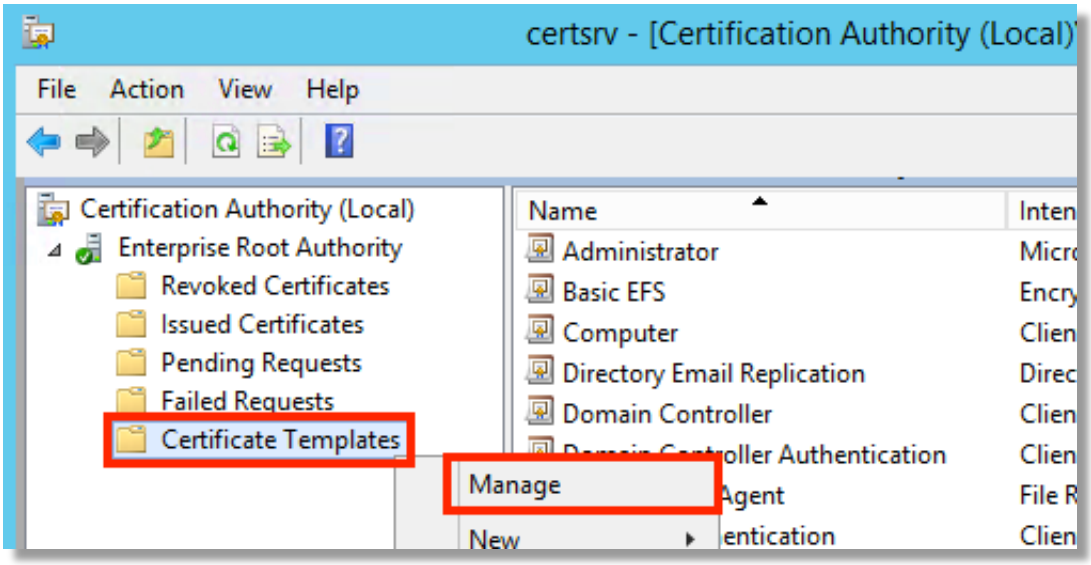
Silverback now needs to be configured to 'impersonate' these users so that the Certificate Authority publishes the generated certificates into the User's Active Directory Object, not the Silverback Computer Account Object.

5.2. Creating the necessary Certificate Template

This type of deployment requires two additional Certificate Templates to be configured and published on your Certificate Authority.

Log into your Certificate Authority, and open the Certificate Authority MMC snap-in.

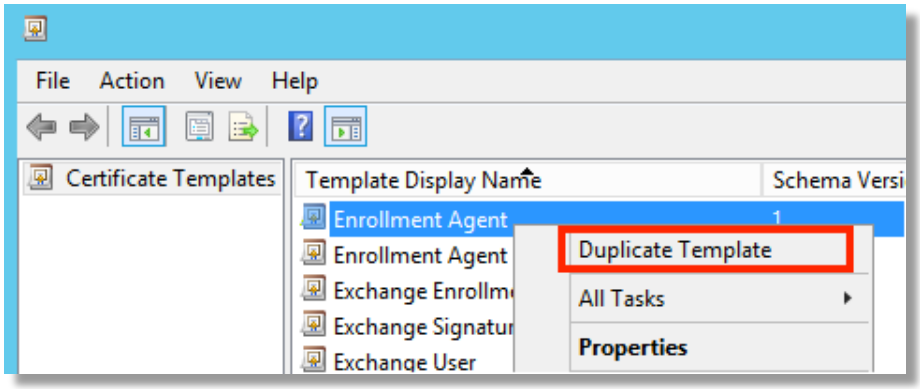
Expand the Configuration Tree on the Right until the Certificate Templates section is visible.



5.2.1. Creating the Certificate Request Agent Template

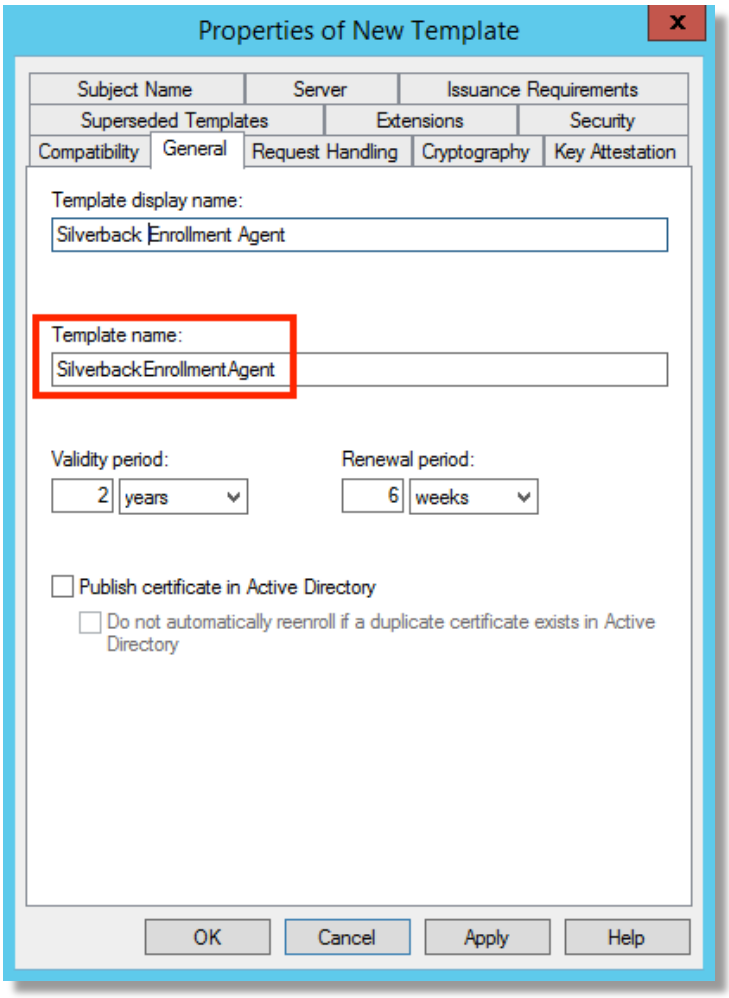
The First Template we will create is the Certificate Request Agent Certificate, which will allow Silverback to send requests to the Certificate Authority on behalf of the enrolling user.

From the Certificate Templates Console opened in Section 5.2, find the 'Enrollment Agent' template and Right-Click -> Duplicate the template.



General Properties of the New Template

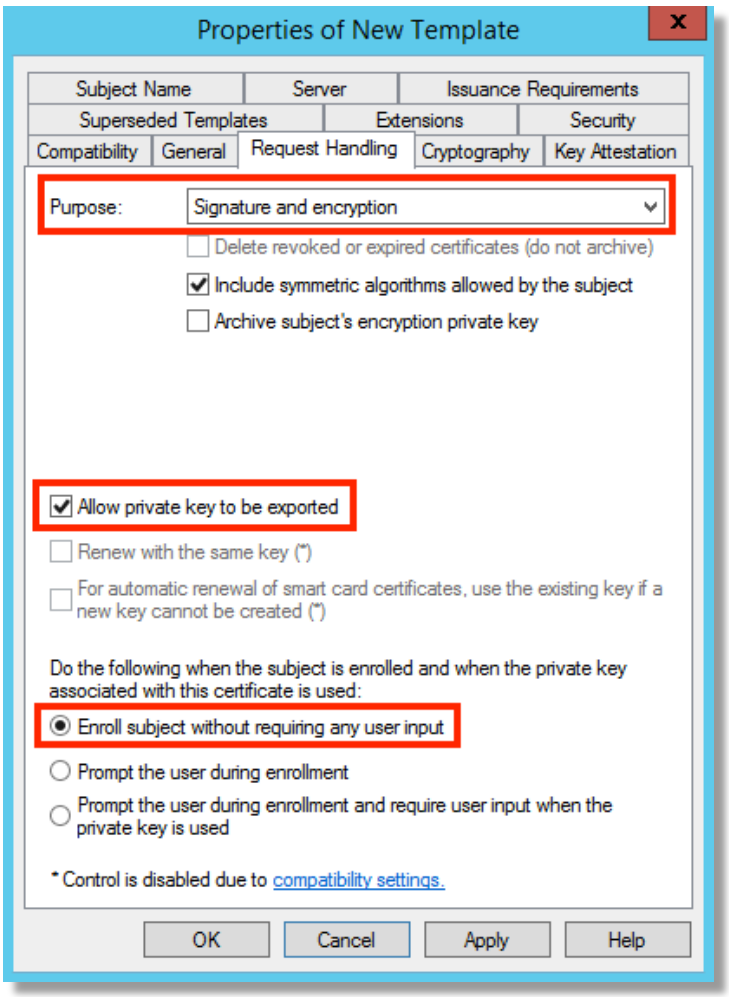
- Name the new Template 'SilverbackEnrollmentAgent'
- Ensure that 'Publish Certificate in Active Directory is Unchecked.



Request Handling Properties of the New Template

Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

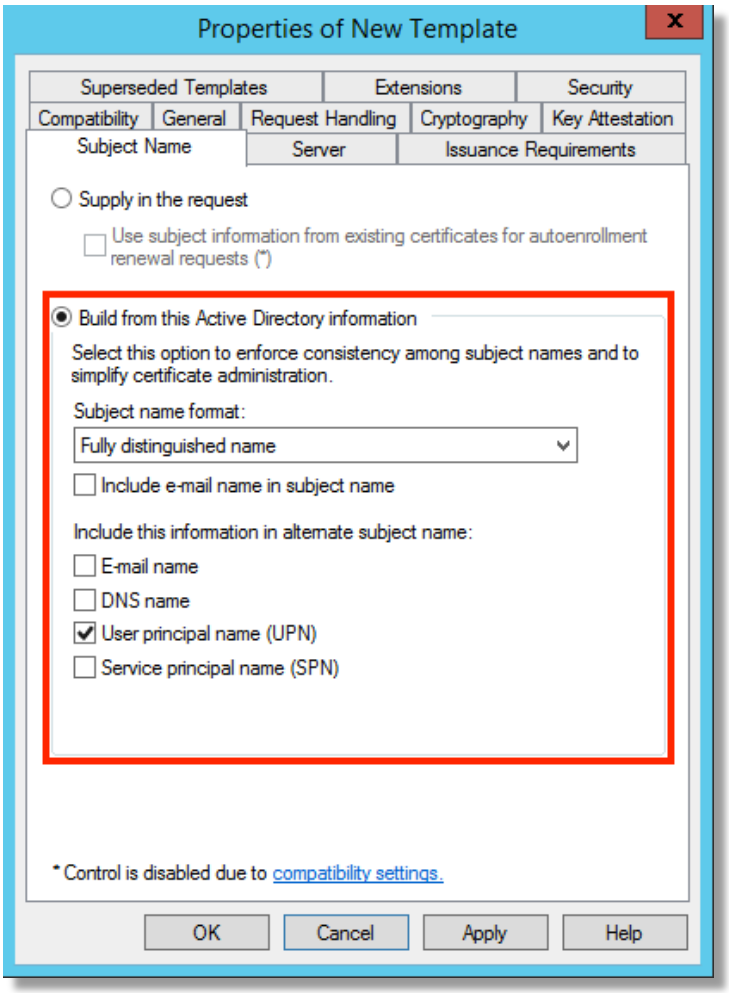
- Purpose: Signature and Encryption
- Allow Private Key to be Exported is Checked.
- Enroll the Subject without requiring any user input.



Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

Subject Name Properties of the New Template

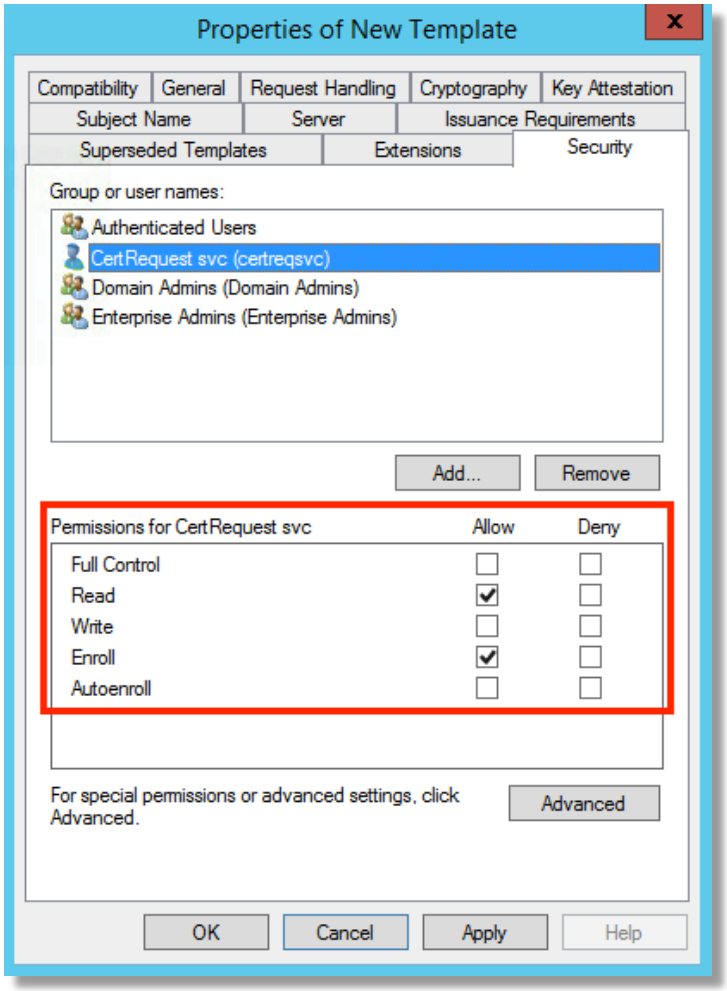
- Build from this Active Directory Information.
  - Fully distinguished name
  - User Principal Name (UPN)



Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

Security Properties of the New Template

- Assign the Service Account Mentioned in Section 2 the READ and ENROLL Permission



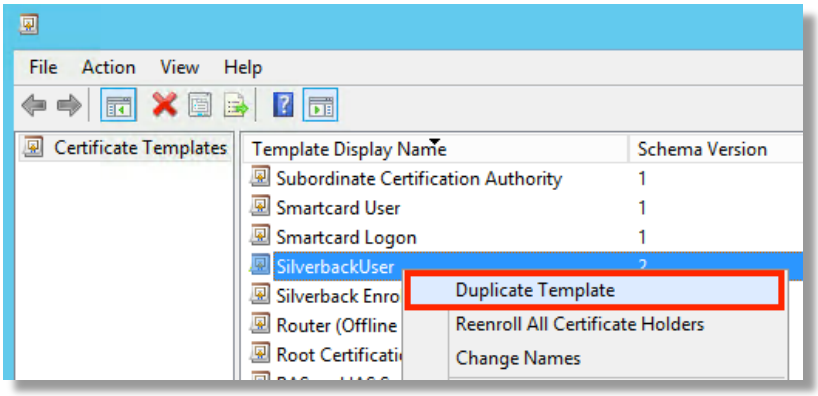
NOTE: It is advised that regular users NOT be able to access this template.

- Click OK to finish creating the Template.

5.2.2. Creating the Silverback Enterprise WiFi Template

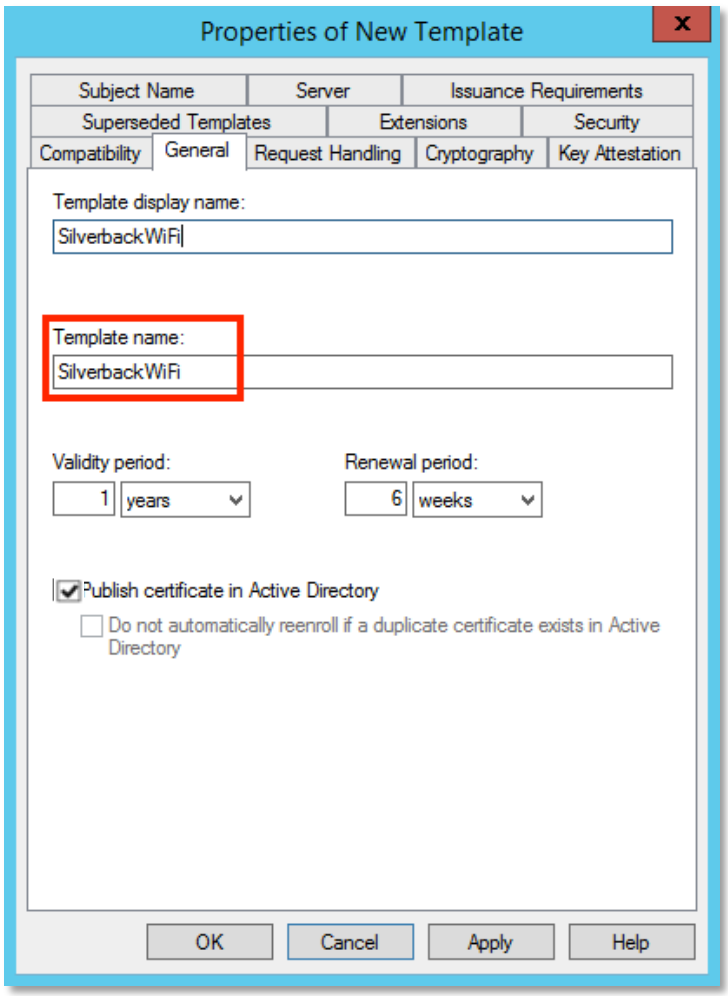
The next certificate we will create is the Enterprise WiFi certificate. For this certificate we will be using the same settings as the Silverback User certificate template created before.

To do this, from the Certificate Templates list, right click on SilverbackUser and select Duplicate Template:

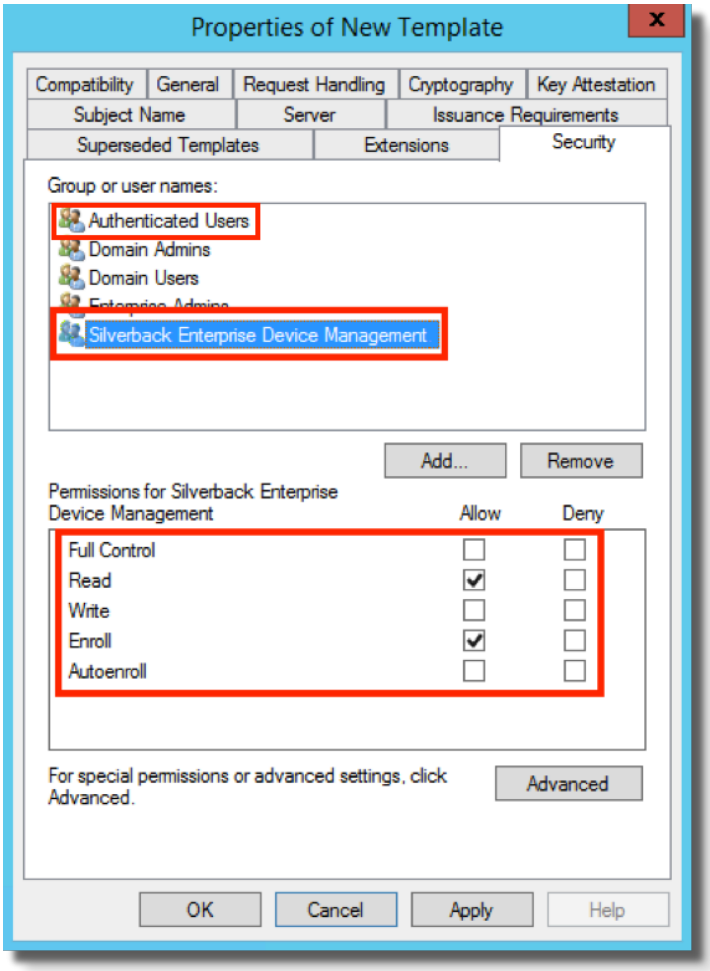


General Properties of the New Template

- Name the new Template 'SilverbackWiFi'
- Ensure that 'Publish Certificate in Active Directory is Checked.



Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

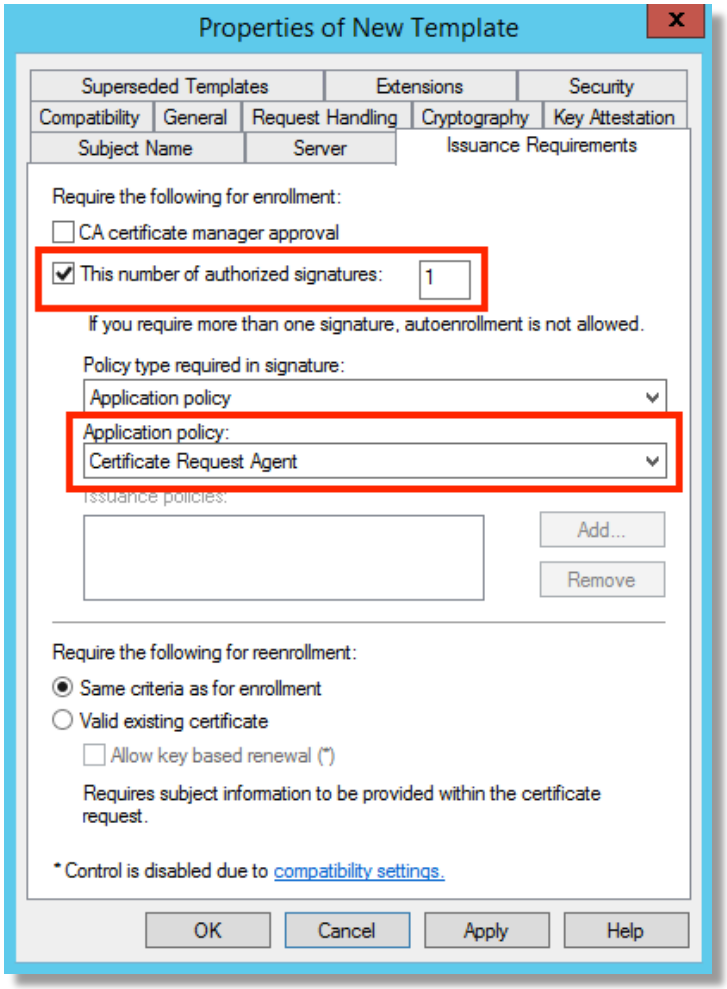


Author: Matrix42 Cloud & Mobile Management

Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

Issuance Requirements Properties of the New Template

- Enable the 'This number of authorized signature' option and set this to 1.
  - Ensure the Application Policy is set to Certificate Request Agent.

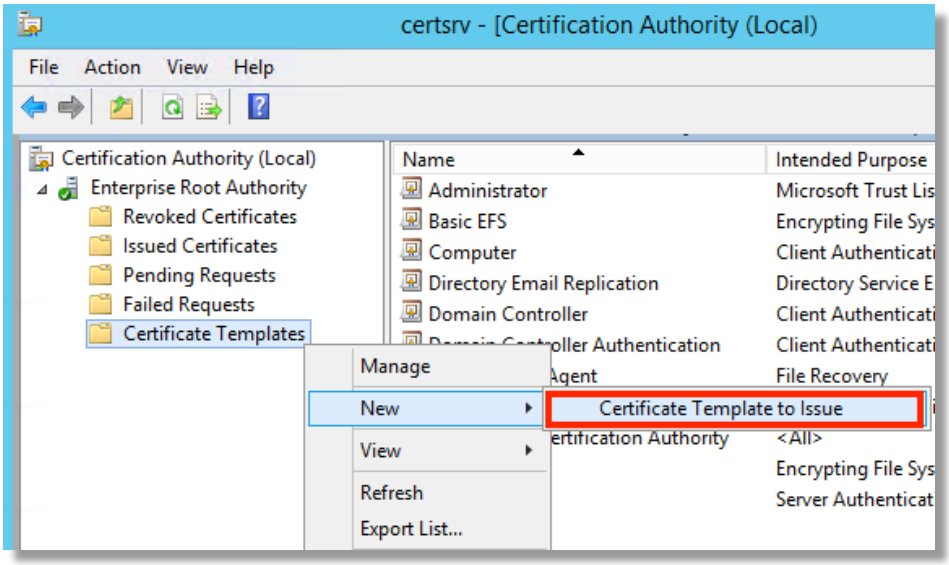


- Click OK to finish creating the Template.

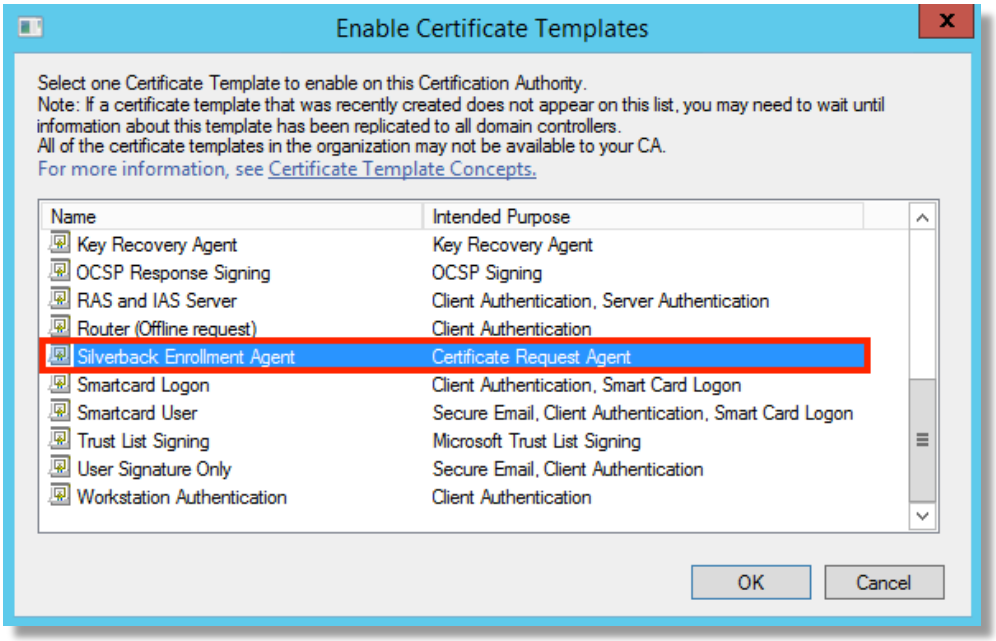
5.3. Publishing the Newly Created Certificate Templates

As we did in Section 3.2, we will need to publish the Certificate Templates just created so they are visible to both Silverback and the Service Account that will create the Certificate Request Agent Certificate..

- Log into your Certificate Authority, and open the Certificate Authority MMC snap-in.
- Expand the Configuration Tree on the Right until the Certificate Templates section is visible.



- Right-Click on Certificate Templates and navigate to the New > Certificate Template to Issue option.
- In the Enable Certificate Template popup box, select the 'SilverbackEnrollmentAgent' template created earlier and click OK to finish publishing the Certificate.



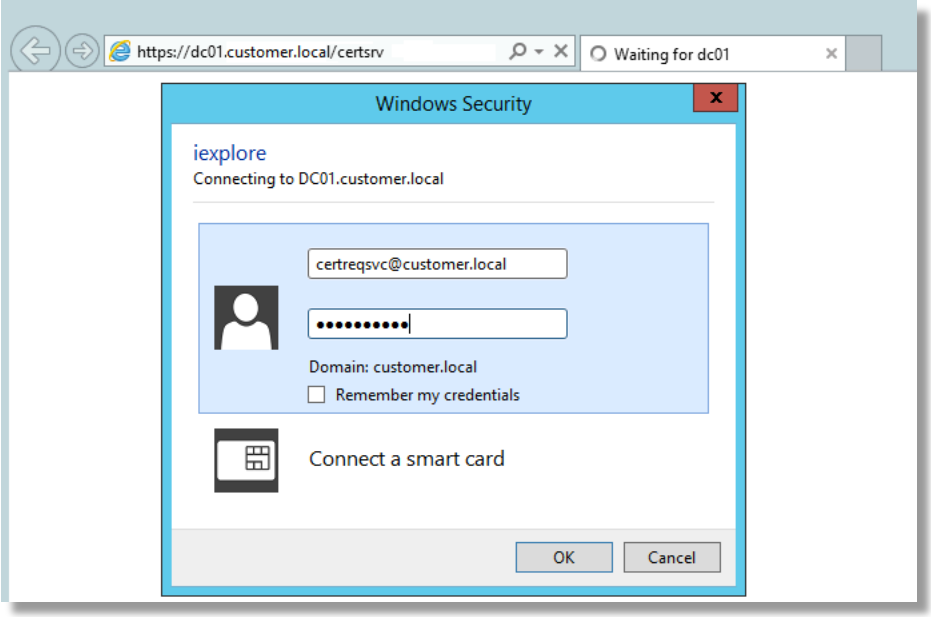
- Repeat this Process for the 'SilverbackWiFi' Template.

Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

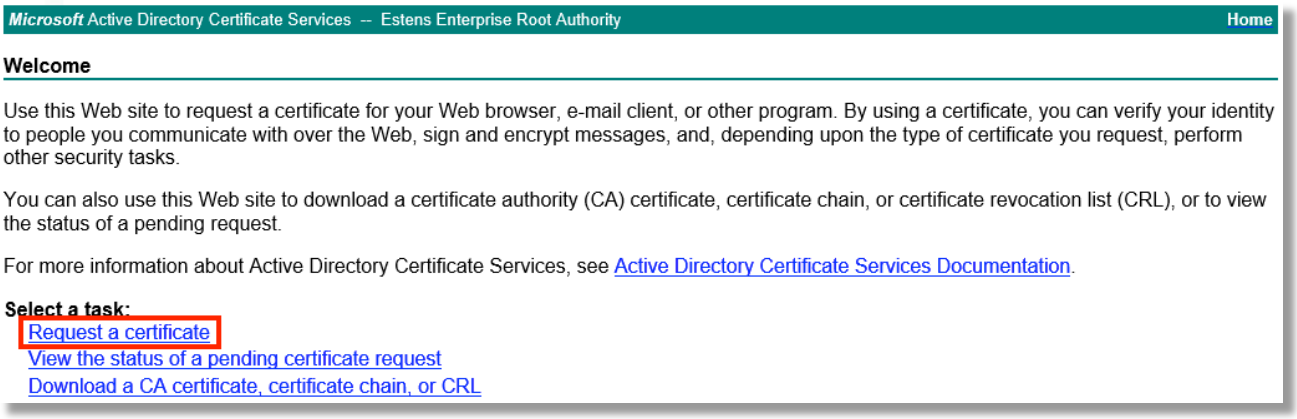
5.4. Creating the Certificate Request Agent Certificate

Next, from the Silverback Computer (or Cloud Connector) Server, we will perform the following steps to create the User Certificate Request Agent.

- Remote Desktop to the Silverback Server (or Cloud Connector) using a Local Administrative Account (that is not affiliated with the domain).
- Open Internet Explorer and visit the Certificate Authority 'CertSrv' website: https://ca01.company.internal/certsrv/
- Log-in use the Dedicated Service Account mentioned in Section 2. (If you do not see a prompt to log-in you are probably using a Domain Account – which will not work).

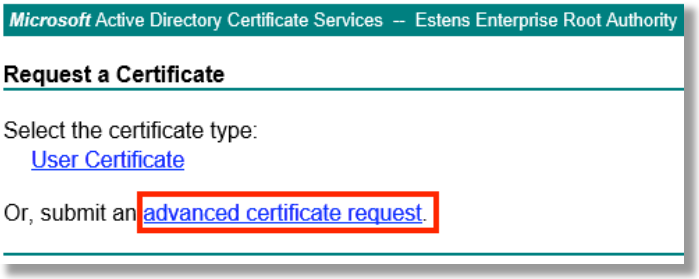


- Click the 'Request a Certificate' option.

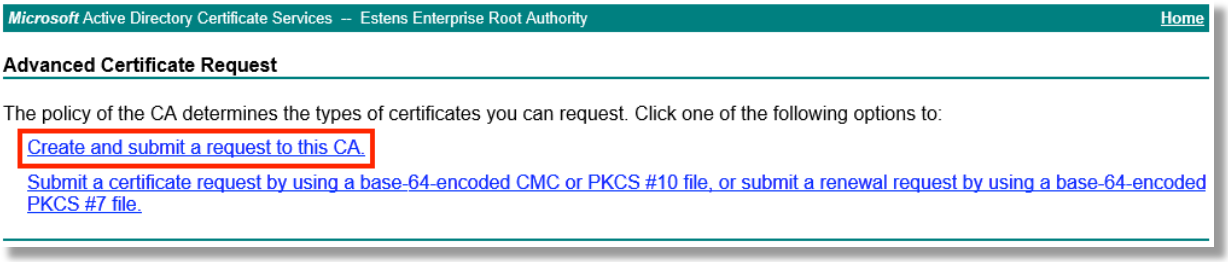


Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

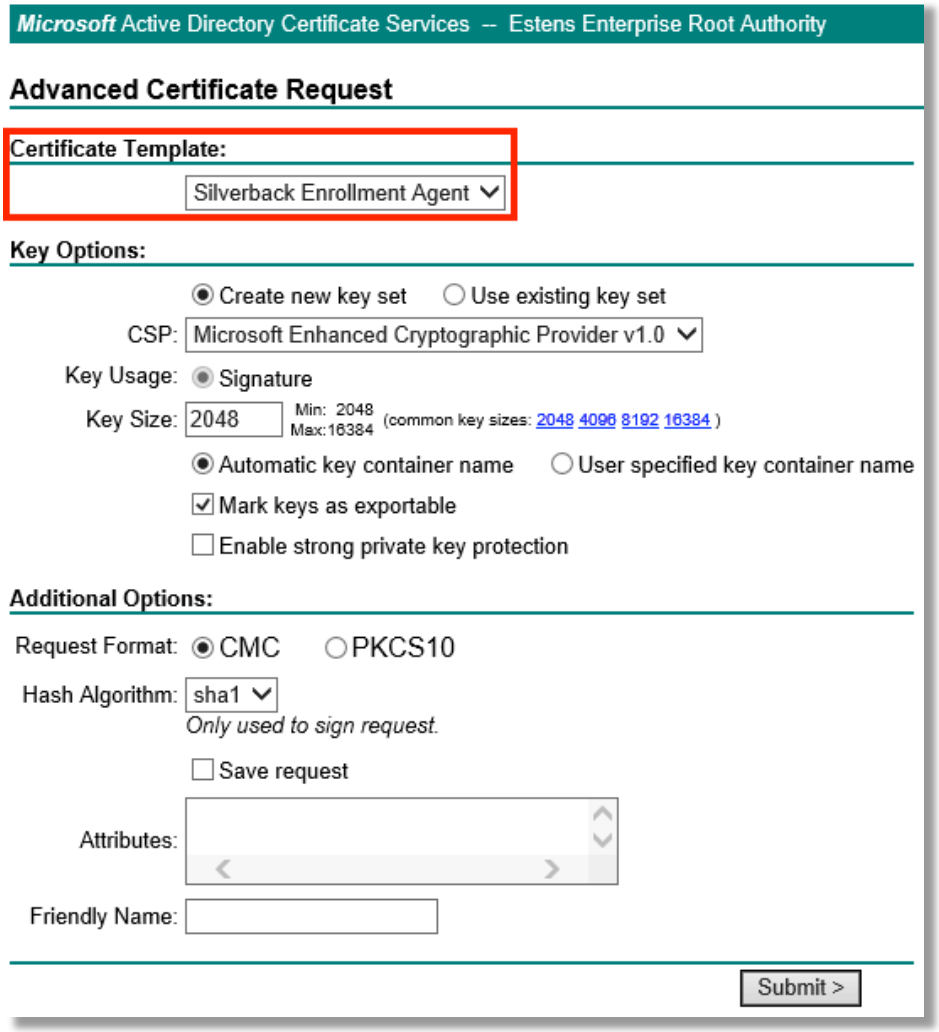
- Click the 'Advanced Certificate Request' option.



- Click the 'Create and Submit a Request to this CA'.

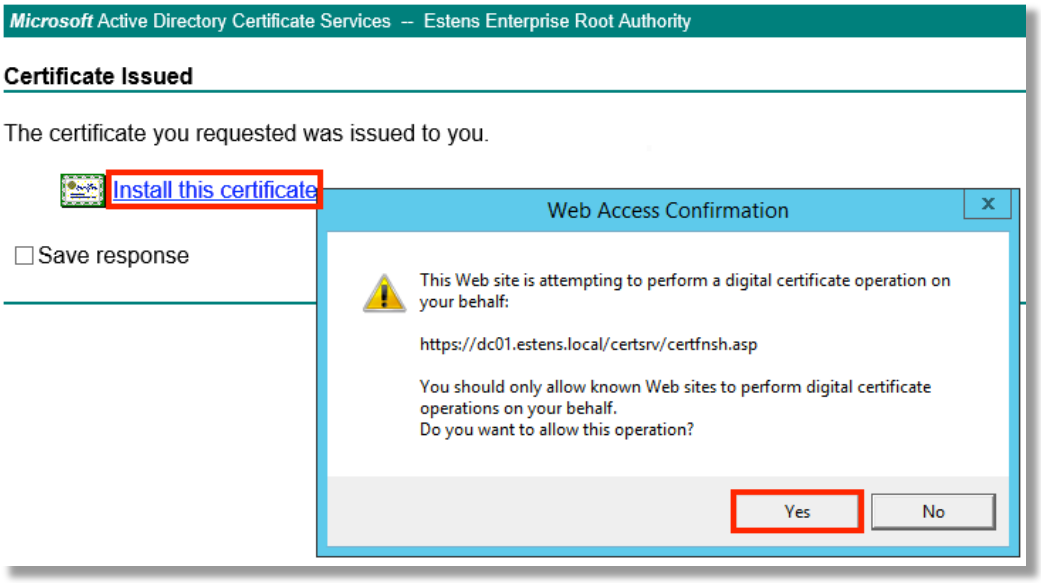


- Change the Template to the 'Silverback Enrollment Agent' template created in Section 5.2.1.

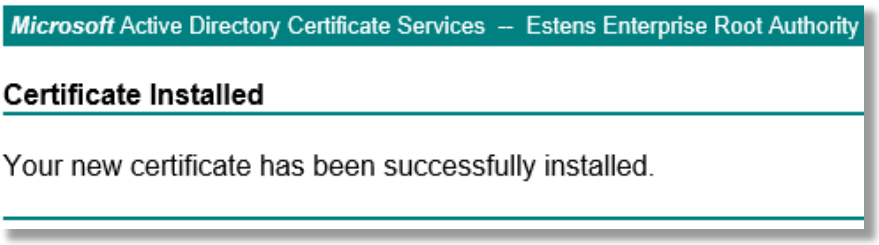


Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

- Click the 'Install this Certificate' link, and if prompted Accept the Web Access Confirmation Prompt.

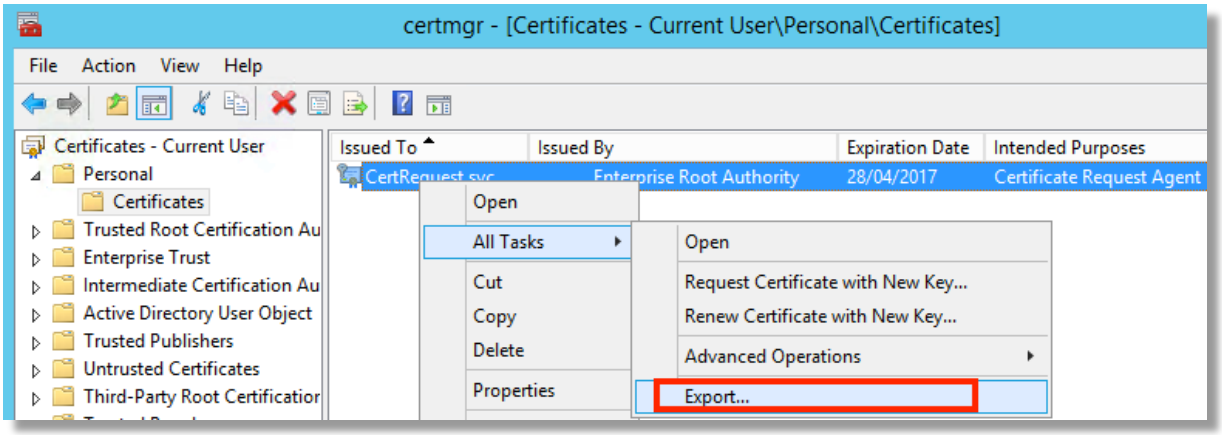


- Once the Certificate has been Generated you will see the following message.



Finally, we log into the Local User Certificate Store to Export the Certificate

- From a RUN Command type 'certmgr.msc' to open the User Certificate Store.
- Expand the Personal Certificate Store, Right Click on the Certificate Request Agent Certificate and Export it.

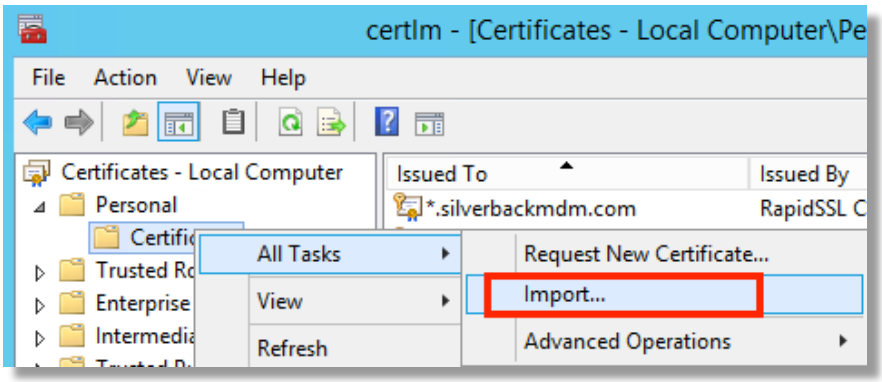


5.5. Importing the Certificate Request Agent Certificate

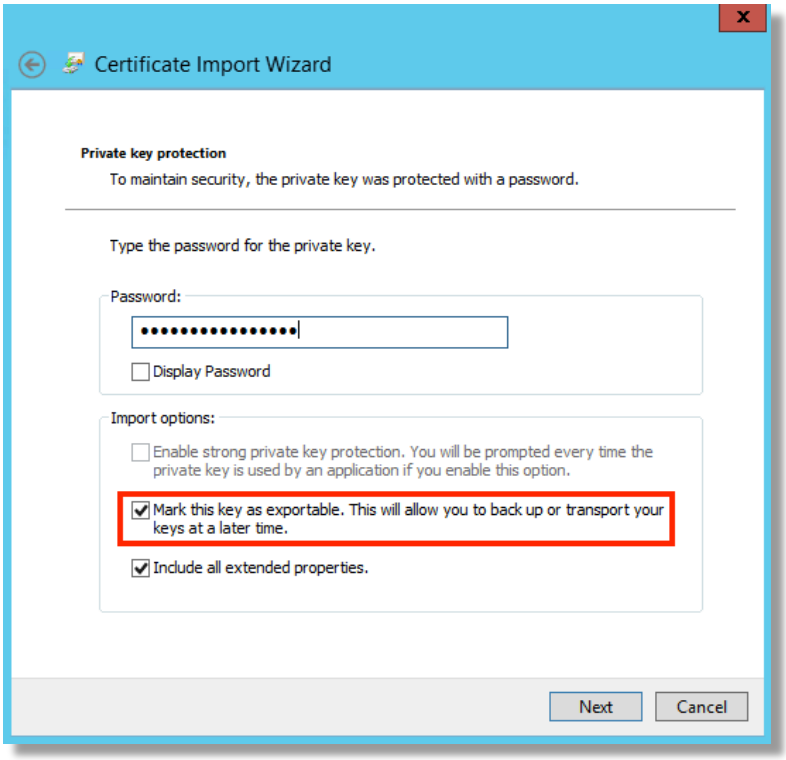
Now the Certificate Request Agent Certificate needs to be imported so Silverback can utilize its abilities to request certificates on behalf of users.

To do this please use the following steps:

- On the Silverback Server (or Cloud Connector), type 'certlm.msc' to open the Local Computer Certificate Store.
- Right-Click the Personal Certificate Store and go to All Tasks > Import…

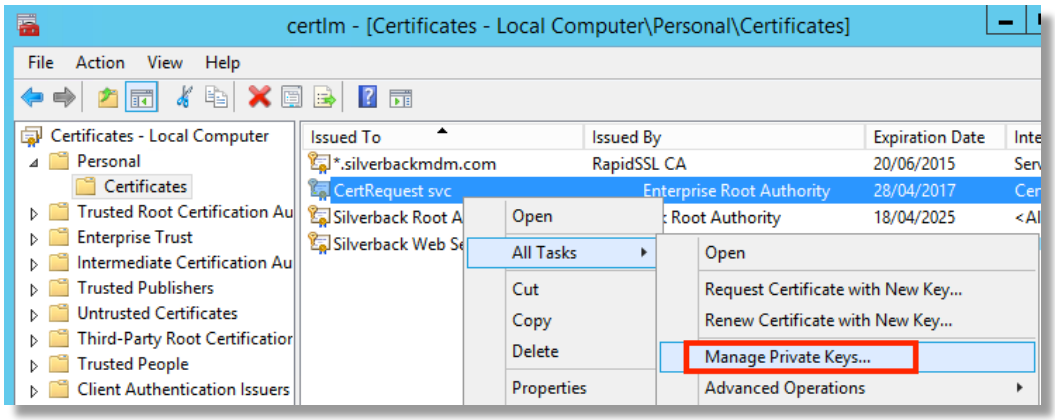


- Be sure to mark the Certificate as Exportable.

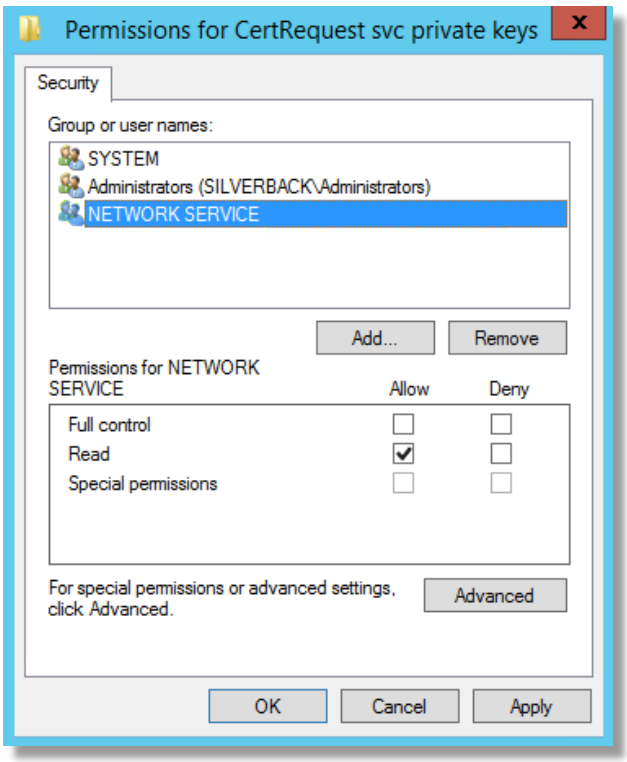


Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Android & iOS Devices.

- Once the Certificate has been imported right-click the Certificate and go to All Tasks > Manage Private Keys.



- Ensure that the Network Service has the READ Permission on the Private Key.

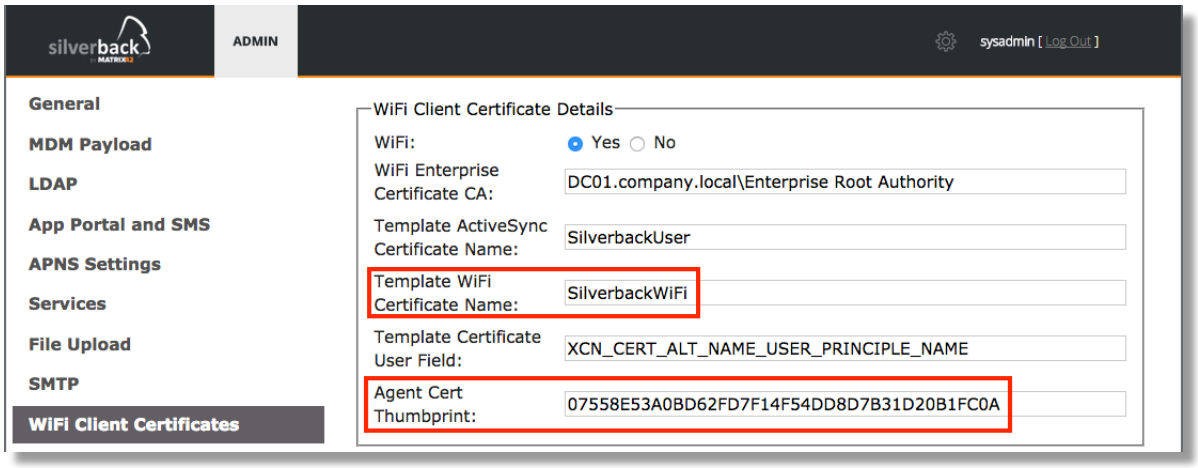


5.6. Silverback Configuration

Once all the Certificate and Certificate Templates have been configured Silverback receives the following configuration settings to populate User-Certificates into Active Directory.

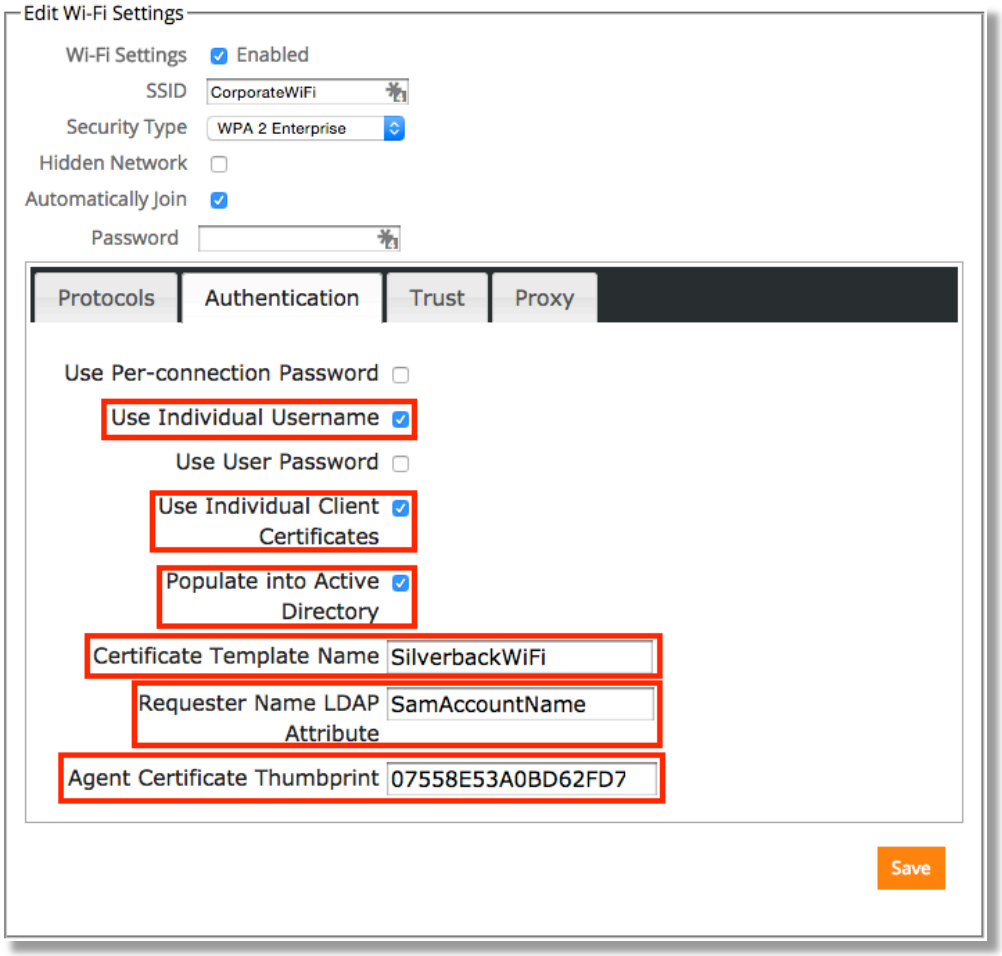
5.6.1. Silverback Web Settings Configuration

- Log into the Silverback Web Settings Administration Site and navigate to the WiFi Client Certificates section.
  - Ensure that the WiFi Template Name matches the Certificate Template created in Section 5.2.2.
  - Ensure that the Agent Cert Thumbprint matches the Certificate Thumbprint of the Certificate Request Agent Certificate created in Section 5.4.



5.6.2. Silverback Device Profile Settings

Log into the Silverback Admin Console and navigate to the configuration profile you are building for your Target Device and your Authentication Settings match the settings outlined below.



- Use Individual Username – Checked.
- Use Individual Client Certificates – Checked.
- Populate into Active Directory – Checked.
- Certificate Template Name – Matches the Certificate Template created in Section 5.5.2.
- Requester Name LDAP Attribute – The Active Directory Attribute you want populated in the User Certificate.
- Agent Certificate Thumbprint – Matches the Certificate created in Section 5.4.

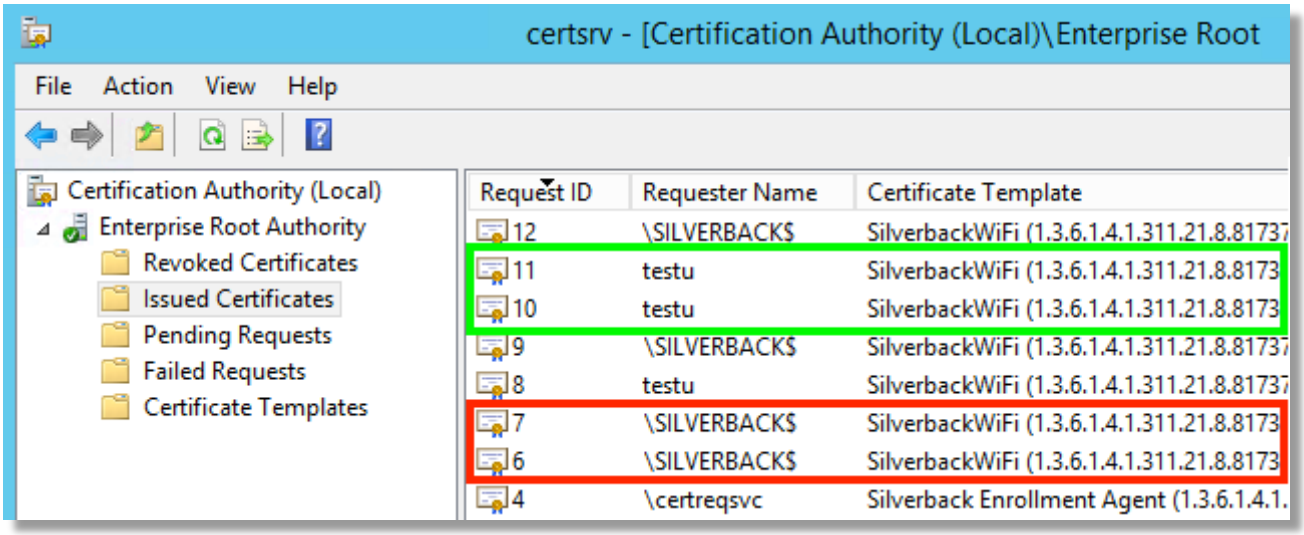
5.1. Confirming That It Works!

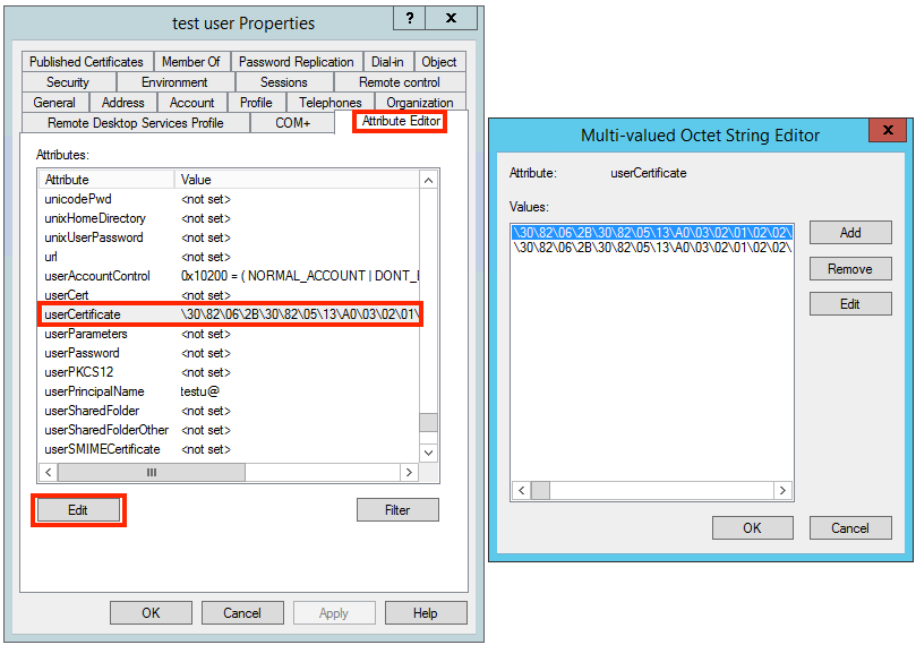
5.1.1. Certificate Authority Requests

If you view the Issued Certificates on your Certificate Authority you should see the requests coming from the users as they enroll into Silverback – not the Silverback Object.

The Requests highlighted in Green were successful.

The Requests highlighted in Red worked, but the Certificate will be in the Computer Object, not the User Object.



5.1.2. User Active Directory Object

Viewing the User Certificates in Active Directory Users and Computers is possible – but they are in a Binary Format: