MATRIX42
SMARTER WORKSPACE – BETTER LIFE

Matrix42 Silverback

Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Windows 8.1 Devices.

Version 0.0.1

23. June 2015

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 & Overview 4
2. Prerequisites 5
2.1. Account Requirements 5
2.2. Additional Requirements 5
3. Certificate Authority Configuration 6
3.1. Certificate Template Permissions 6
3.2. Publishing Certificate Templates 8
4. Generating the Registration Authority Certificates 9
4.1. Generating the Certificates 9
4.2. Configuring Certificate Permissions 10
4.3. Certificates for Cloud Connector Install (Cloud Connector Only) 11
4.3.1. Exporting the Certificates from the Cloud Connector Server 11
4.3.2. Importing the Certificates on the Silverback Server 12
4.3.3. Completing the Certificate Chain 12
5. Silverback Configuration 13
5.1.1. Silverback Web Settings Configuration 13
5.1.2. Silverback Payload Settings 14
6. Appendix 15
6.1. Exchange Enrollment Agent Request Template 15
6.1. CEP Encryption Request Template 15

Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Windows 8.1 Devices.

1. Introduction & Overview

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 Windows 8.1 Devices 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).

Windows Phone 8.1 Certificate Delivery requires a special delivery system similar to that of Microsoft's NDES (Network Devices Enrollment Service), but is not required for Silverback's Implementation.

Silverback replaces the need for the NDES requirement within your Internal Network acting as the Registration Authority itself, allowing devices to send Certificate Requests to the Certificate Authority *through* Silverback.

2. Prerequisites

This document assumes that you have followed the 'Silverback Microsoft CA Integration for Android & iOS' guide as it builds on concepts outlined within this document and also uses the same Certificate Templates created for Exchange ActiveSync & Enterprise Wi-Fi (Section 3).

2.1. Account Requirements

To Complete the necessary work, the following additional requirements will be necessary:

- Administrative Access to the Certificate Authority Silverback is sending requests too.
  - Account must be able to Create/Publish Certificate Templates.
- Administrative Access to Silverback Application Server (and Cloud Connector if applicable).
  - Both Remote Desktop and Silverback Console Access.
  - Remote Desktop Account must be a Domain Member.

2.2. Additional Requirements

- A copy of the complete certificate chain for the Internal Certificate Authority (Public Key's Only).

3. Certificate Authority Configuration

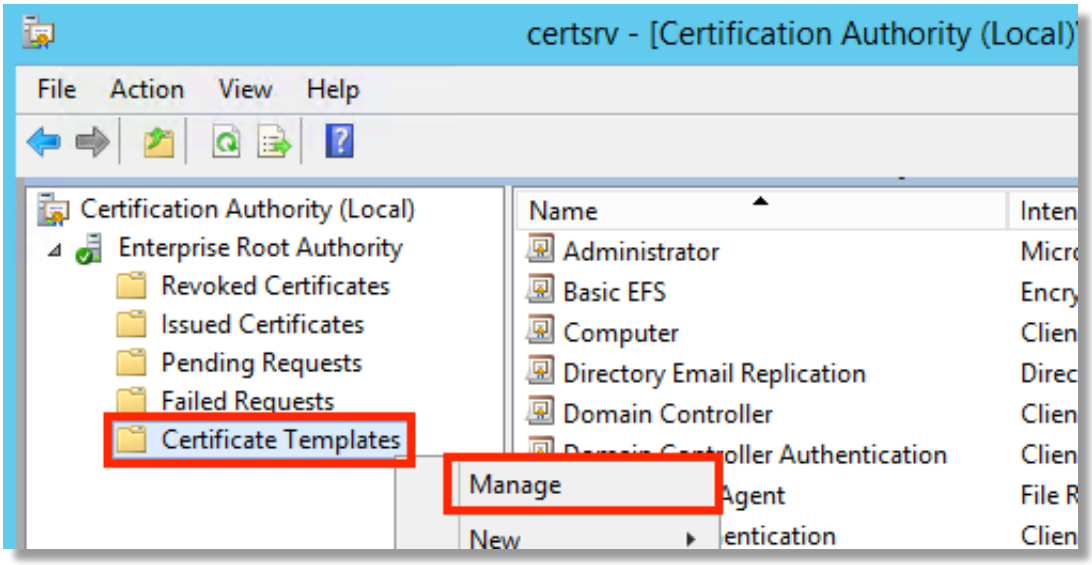
As Silverback will be acting as a Registration Authority by allowing Windows 8.1 Family devices to send Certificate Requests to the Certificate Authority through itself without the need for an NDES Server (Network Device Enrollment Service) we need to have some very specific certificates installed for Silverback to use.

These are the:

- CEP Encryption, &
- Exchange Enrollment Agent (Offline Request)

3.1. Certificate Template Permissions

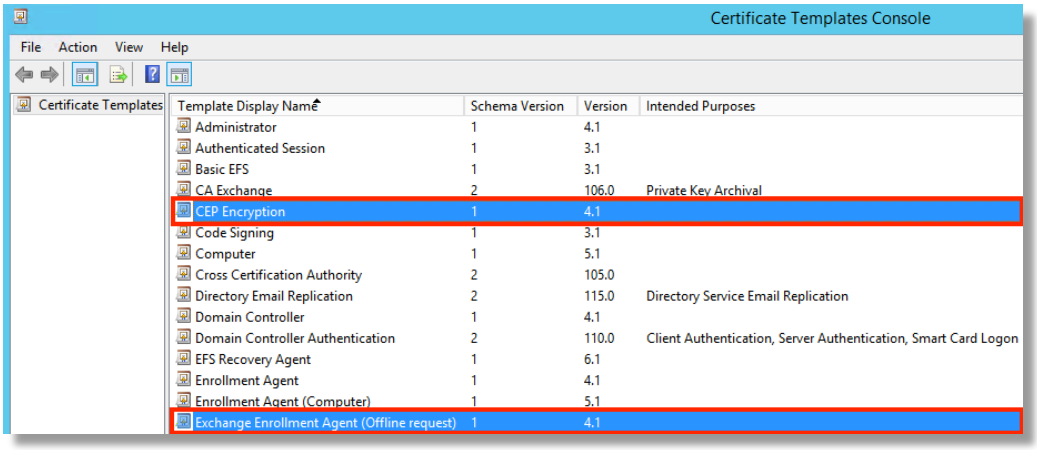
- Log into your Certificate Authority, and open the Certificate Authority MMC snap-in.
- Expand the Configuration Tree on the Right until the Certificate Templates section is visible.



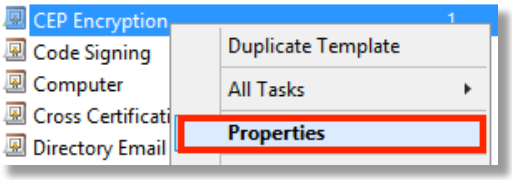
- Right-Click on Certificate Templates and click the Manage option to bring up the Certificate Template Console.

Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Windows 8.1 Devices.

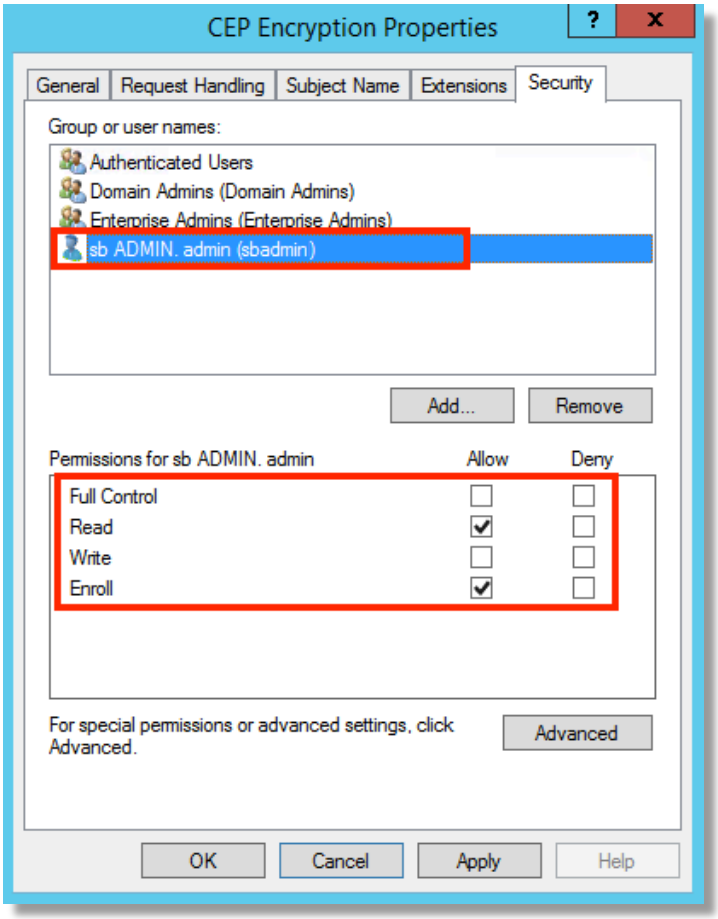
- Identify both the 'CEP Encryption' and 'Exchange Enrollment Agent (Offline Request)' Templates.



- Right Click on each of these templates in turn, and click Properties.



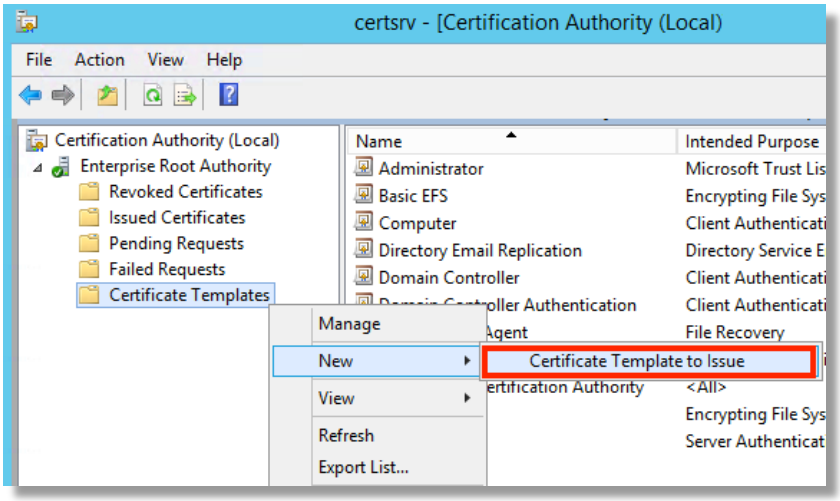
- Change to the Security Tab and give the Domain Admin Account the READ & Enroll Permission



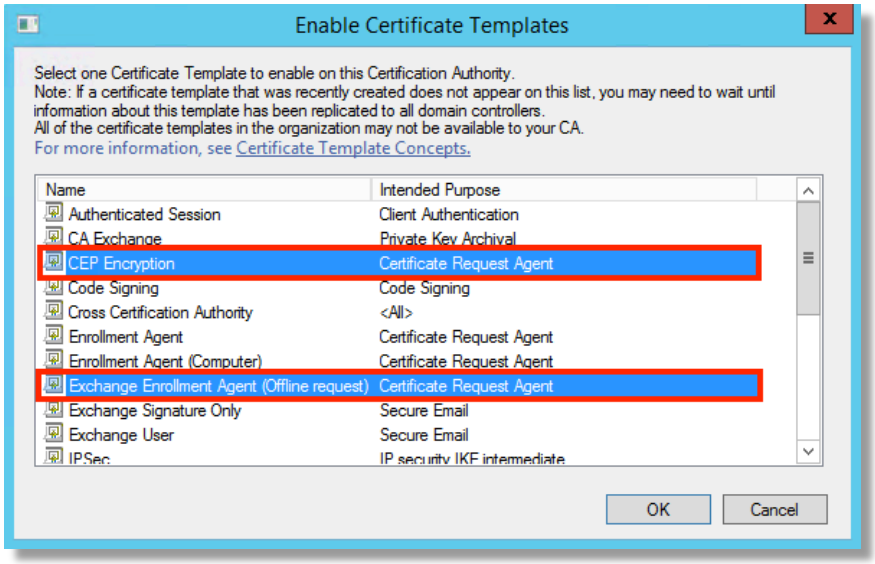
3.2. Publishing Certificate Templates

Once the correct permissions have been applied to the Certificate Templates, they need to be published so the Silverback Administrative Account can see and request certificates from them.

- 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 both the 'CEP Encryption' and 'Exchange Enrollment Agent (Offline Request) template's and click OK to finish publishing them.



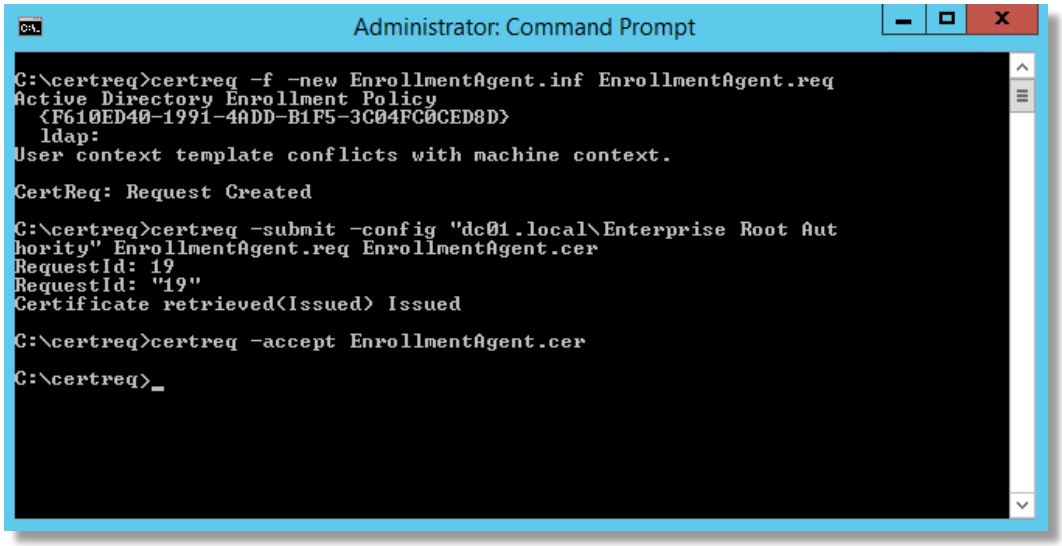
4. Generating the Registration Authority Certificates

Registration Authority Certificates will allow Silverback to channel Certificate Requests direct from the Windows Device through to the Certificate Authority with no interaction from the user or administrator.

4.1. Generating the Certificates

The following process can be completed from any Domain Joined Computer that can contact the Certificate Authority, but for best results it is best to be done on the Silverback Server (or Cloud Connector) itself.

- Log onto the Silverback (or Cloud Connector) Server, and open an Administrative Prompt.
- Using the Request Templates in Appendix 6 execute the following series of commands to complete the Certificates:
  - Create the Certificate Request File:
    certreq –f -new EnrollmentAgent.inf EnrollmentAgent.req
  - Send the Certificate Request File to the Certificate Authority:
    certreq –submit -config "dc01.local\Enterprise Root Authority" EnrollmentAgent.req EnrollmentAgent.cer
  - Accept the returned Certificate and combine it with the Private Key:
    certreq –accept EnrollmentAgent.cer



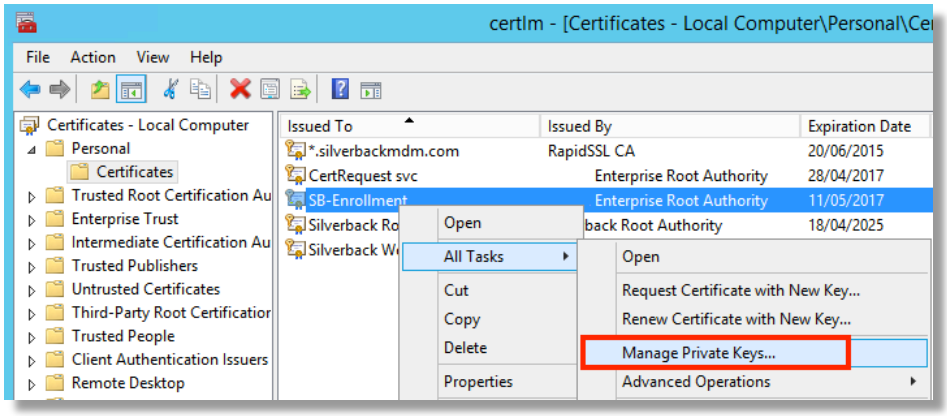
- Repeat this process for both the CEP Encryption & Exchange Enrollment Agent Certificate Templates.

The Certificate will be in the Local Computer -> Personal Certificate Store upon completion of this process.

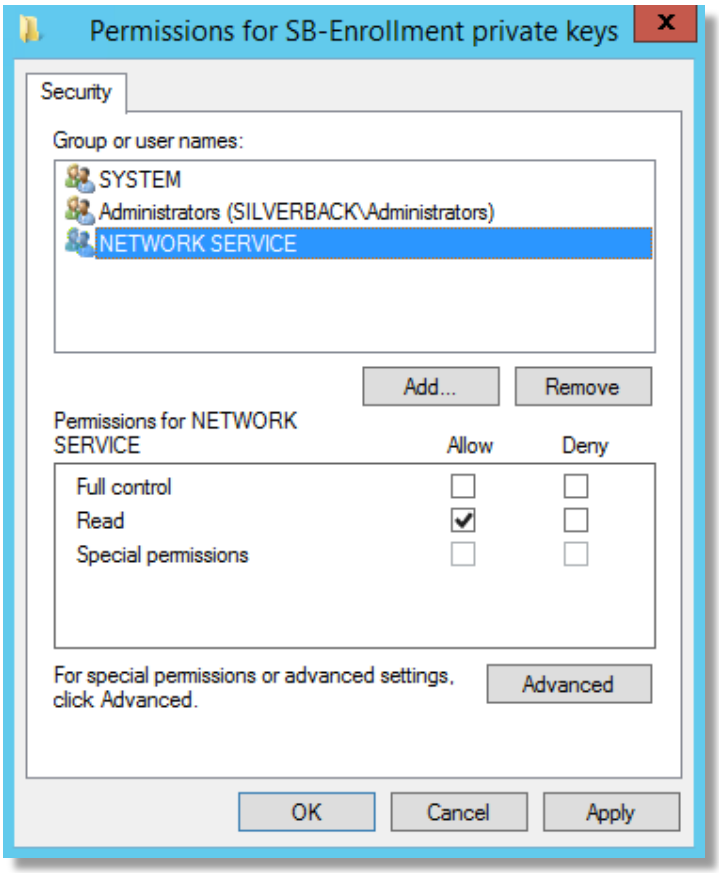
4.2. Configuring Certificate Permissions

As the majority of Silverback runs as the Network Service we will need to assign the appropriate permissions on the Private Key of the newly created certificates.

- Log onto the Silverback (or Cloud Connector) Server, open a RUN dialog box and type 'certlm.msc' to open the Local Computer Certificate Store
- Right-Click the Exchange Enrollment Agent and select All Tasks -> Manage Private Keys



- Give the Network Service the READ Permission on the Private Key and click OK.



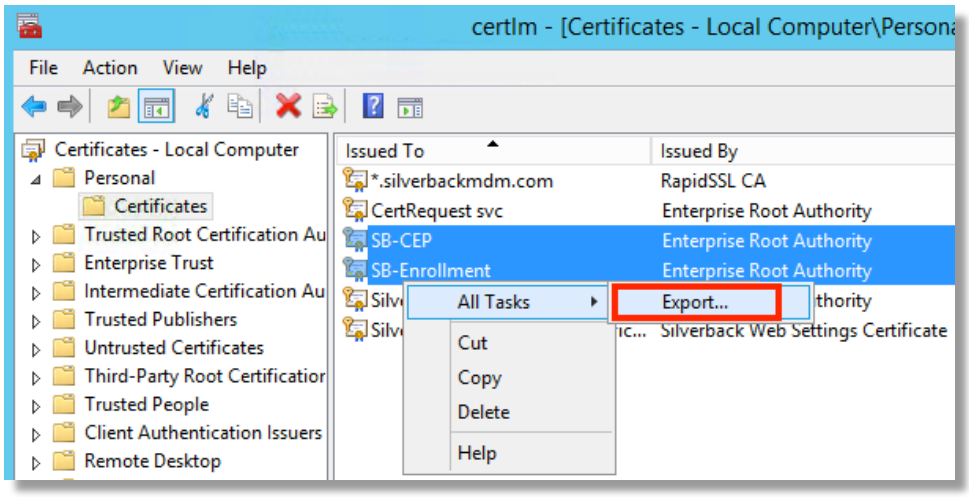
- Repeat this process for the CEP Encryption Certificate.

4.3. Certificates for Cloud Connector Install (Cloud Connector Only)

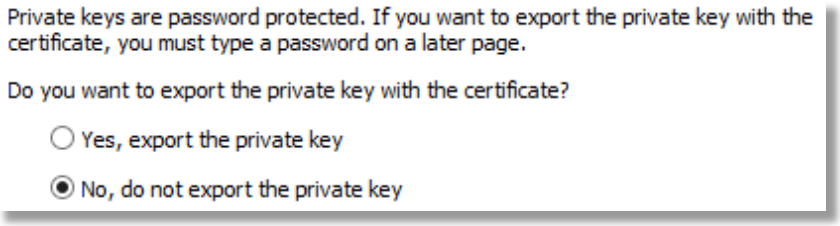
To better maintain the Security Integrity of your Internal Certificate Authority, only the Public Key Certificates are required on the Silverback Server itself, with the Cloud Connector Server having both the Public & Private Key Installed.

4.3.1. Exporting the Certificates from the Cloud Connector Server

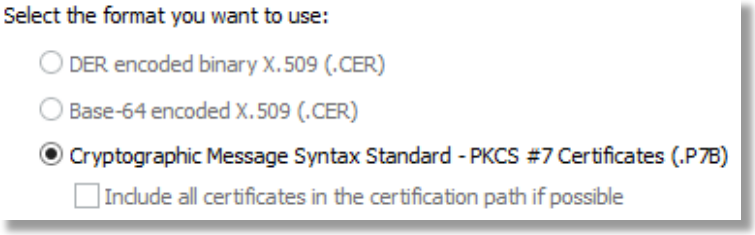
- Log onto the Silverback Cloud Connector Server, open a RUN dialog box and type 'certlm.msc' to open the Local Computer Certificate Store.
- Right-Click the Exchange Enrollment Agent and CEP Encryption Certificates, Right Click and select All Tasks -> Export



- Do NOT Export the Private Key.



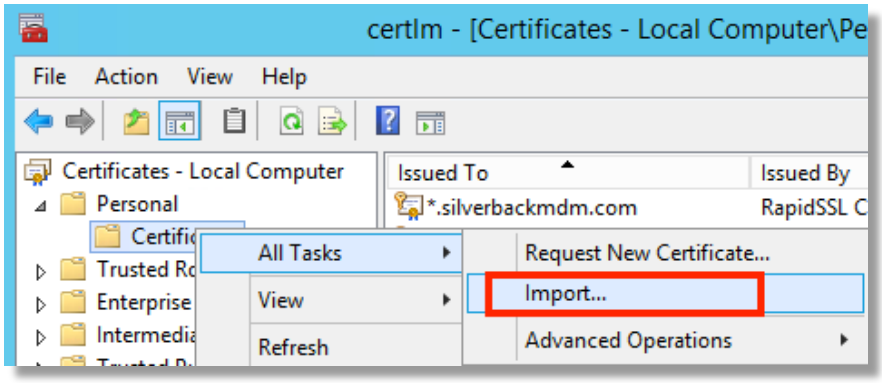
- Export the Certificates using the P7B Format for easier transport.



- Now copy the P7B File to the Silverback Cloud Based Server for Installation.

4.3.2. Importing the Certificates on the Silverback Server

- Log onto the Silverback Cloud Connector Server, open a RUN dialog box and type 'certlm.msc' to open the Local Computer Certificate Store.
- Right-Click the Personal Certificate Store and go to All Tasks > Import…

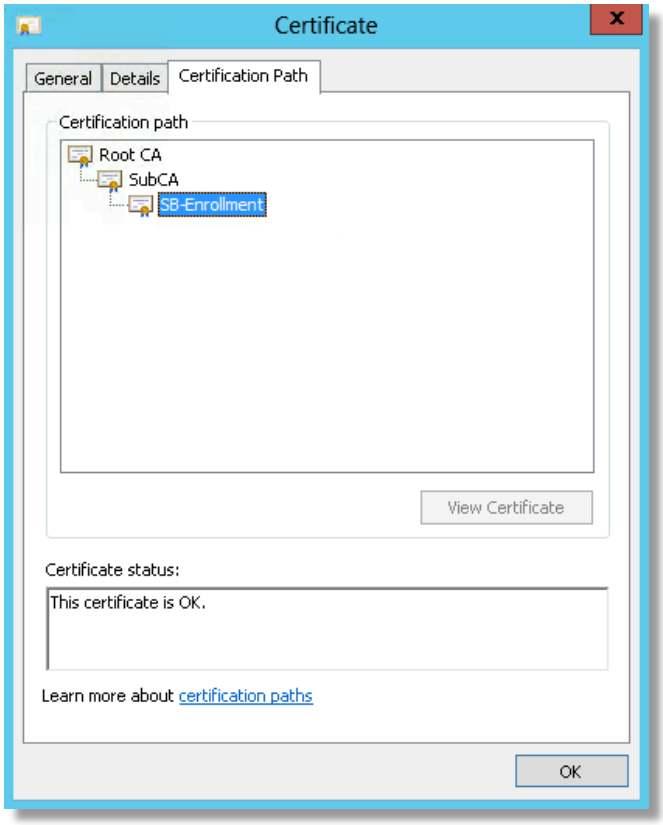


- Import the P7B file that was exported in Section 4.3.1.

The Private Keys should now be visible for Silverback to reference before sending the request to the Cloud Connector for in the Corporate Environment of the Customer.

4.3.3. Completing the Certificate Chain

- Install any Root/Intermediate Certificate necessary to complete the Certificate Chain for the CEP Encryption & Exchange Enrollment Agent Certificates. Silverback must trust them.



5. Silverback Configuration

Once the Certificate have been configured and installed correctly Silverback needs to be configured to use them. This configuration is done via the Silverback Web Settings Configuration Page.

5.1.1. Silverback Web Settings Configuration

- Log into the Silverback Web Settings Administration Site and navigate to the WP Settings section.
  - Under the Windows 8.1 Family Device Settings section populate the following fields:
    - Enrollment Issuing CA Thumbprint

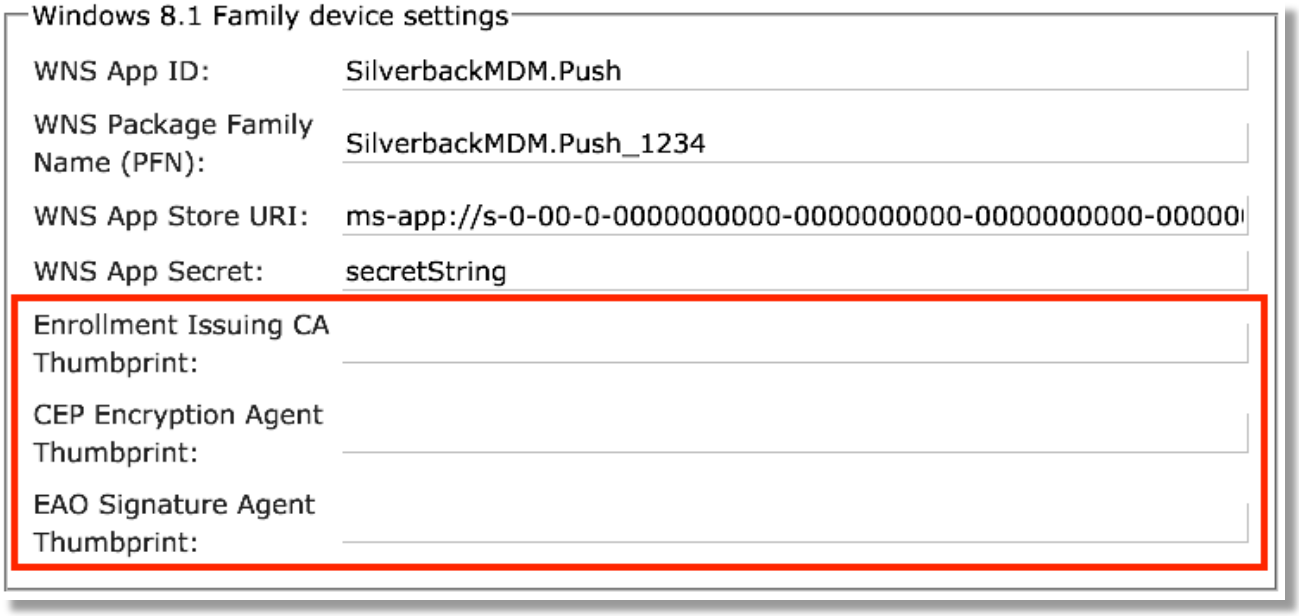
      Thumbprint for the Certificate Authority Silverback is targeting for requests.

    - CEP Encryption Agent Thumbprint

      Thumbprint for the Certificate Authority Silverback is targeting for requests.

    - EAO Signature Agent Thumbprint

      Thumbprint for the Certificate Authority Silverback is targeting for requests.

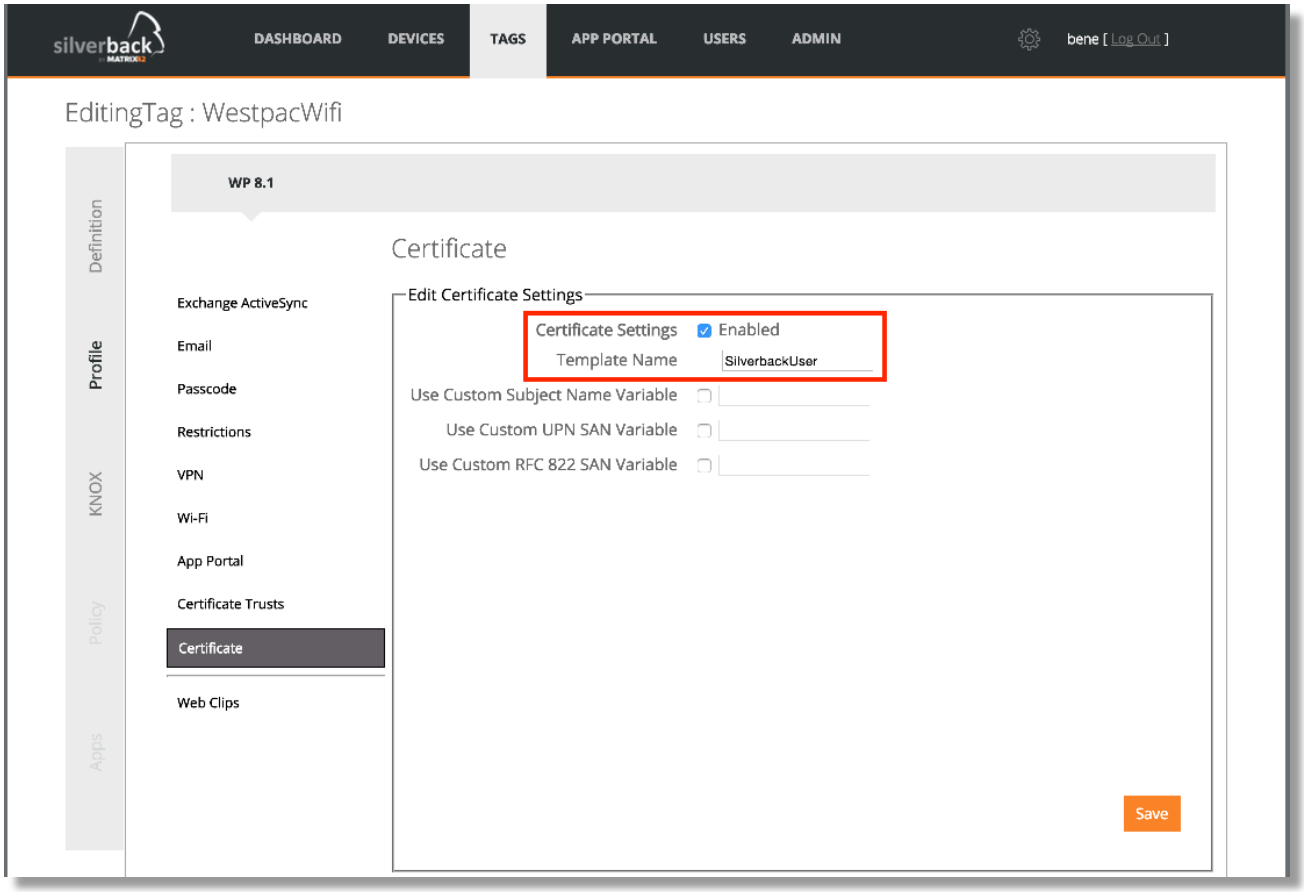


Silverback Integration with Microsoft Active Directory Enterprise Certificate Services for Windows 8.1 Devices.

5.1.2. Silverback Payload Settings

Unlike iOS & Android the Certificate Template for Windows Devices is located within the Silverback Admin Console, and is configureable as part of the configuration settings that are delivered to the device.

- Log into the Silverback Admin Console and navigate to the Tag that will be delivering the settings that require a certificate (Exchange ActiveSync / Wi-Fi / VPN / etc).
- Ensure Certificate Delivery is enabled and specify the Certificate Template Name.



6. Appendix

6.1. Exchange Enrollment Agent Request Template

```
[NewRequest]
Subject = "CN=SB-Enrollment"
Exportable = TRUE
KeyLength = 2048
KeySpec = 2
KeyUsage = 0x80
MachineKeySet = TRUE
ProviderName = "Microsoft Enhanced Cryptographic Provider v1.0"
ProviderType = 1
[EnhancedKeyUsageExtension]
OID = 1.3.6.1.4.1.311.20.2.1
[RequestAttributes]
CertificateTemplate = EnrollmentAgentOffline
```

6.1. CEP Encryption Request Template

```
[NewRequest]
Subject = "CN=SB-CEP"
Exportable = TRUE
KeyLength = 2048
KeySpec = 1
KeyUsage = 0x20
MachineKeySet = TRUE
ProviderName = "Microsoft RSA Schannel Cryptographic Provider"
ProviderType = 12
[EnhancedKeyUsageExtension]
OID = 1.3.6.1.4.1.311.20.2.1
[RequestAttributes]
CertificateTemplate = CEPEncryption
```