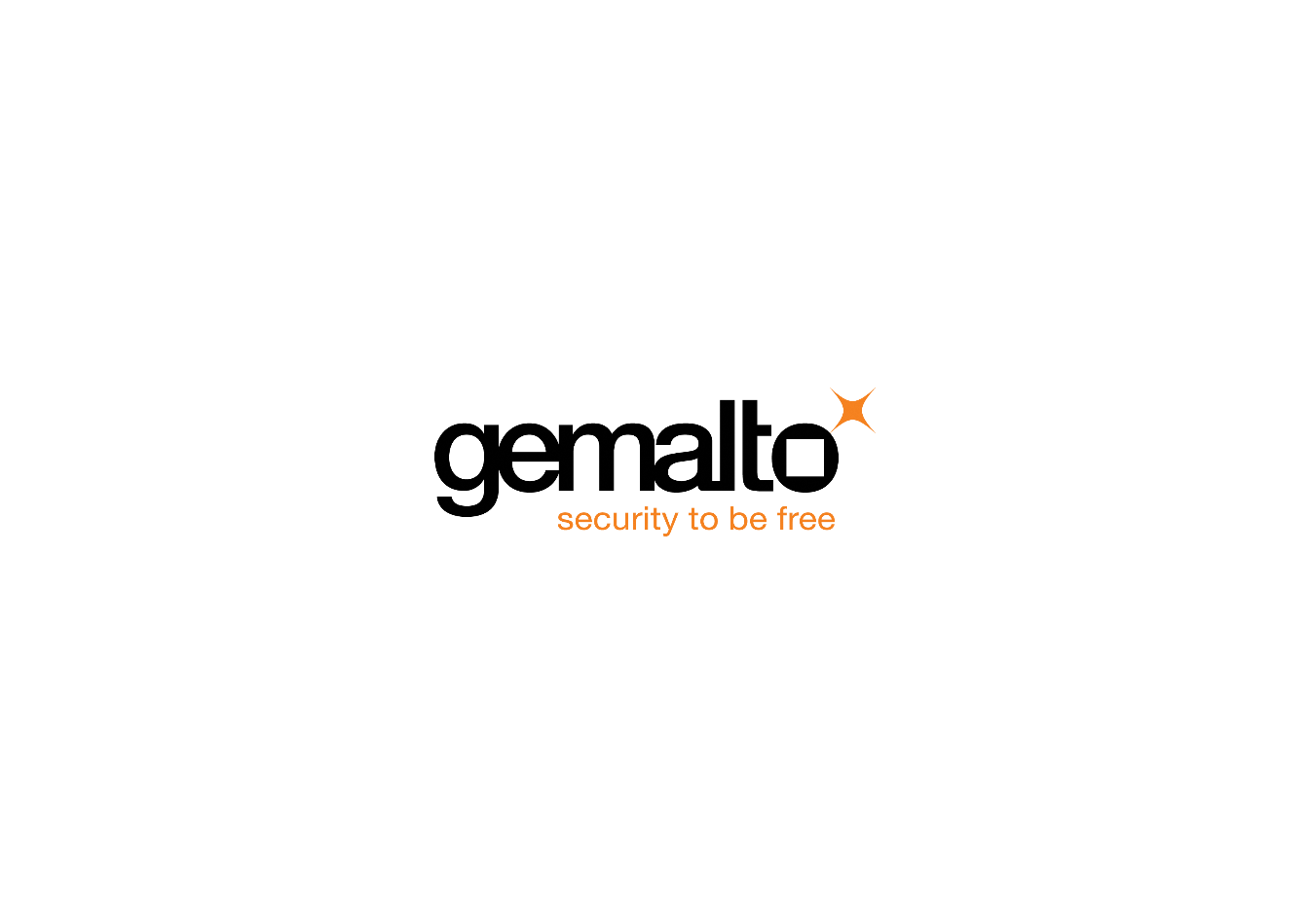
HSE Keyfactor Interoperability

Integration Guide



All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

* The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
* This document shall not be posted on any publicly accessible network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

**Document Number:** xxx-xxxxxx-xxx, Rev. A

**Release Date:** March 2019

Contents

[Preface 4](#_Toc4513091)

[Scope 4](#_Toc4513092)

[Document Conventions 4](#_Toc4513093)

[Command Syntax and Typeface Conventions 5](#_Toc4513094)

[Support Contacts 6](#_Toc4513095)

1. [Introduction 7](#_Toc4513096)

[Overview 7](#_Toc4513097)

[3rd Party Application Details 7](#_Toc4513098)

[Supported Platforms 7](#_Toc4513099)

[Prerequisites 7](#_Toc4513100)

[SafeNet HSE Setup 7](#_Toc4513101)

1. [Signing an HSE Certificate Request with Keyfactor 8](#_Toc4513102)

[Generate the CSR for the HSE from CM7 8](#_Toc4513103)

[Keyfactor Signing 10](#_Toc4513104)

Preface

This document is intended to guide security administrators through the steps for the Keyfactor CA Integration with SafeNet HSE, and also covers the necessary information to generate a CSR and have it signed by the Keyfactor CA and install the signed certificate on the HSE.

## Scope

This document outlines the steps to sign an HSE CSR with the Keyfactor CA

## Document Conventions

This section provides information on the conventions used in this template.

#### Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

|  |  |
| --- | --- |
| **note** | **NOTE:** Take note. Contains important or helpful information. |

#### Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

|  |  |
| --- | --- |
| **caution** | **CAUTION:** Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss. |

#### Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

|  |  |
| --- | --- |
| warning | **WARNING:** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury*.* |

### Command Syntax and Typeface Conventions

| Convention | Description |
| --- | --- |
| bold | The bold attribute is used to indicate the following:   * Command-line commands and options (Type **dir /p**.) * Button names (Click **Save As**.) * Check box and radio button names (Select the **Print Duplex** check box.) * Window titles (On the **Protect Document** window, click **Yes**.) * Field names (**User Name:** Enter the name of the user.) * Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) * User input (In the **Date** box, type **April 1**.) |
| *italic* | The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.) |
| Consolas | Denotes syntax, prompts, and code examples. |

### Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

|  |  |  |
| --- | --- | --- |
| Contact Method | Contact Information | |
| Address | Gemalto  4690 Millennium Drive  Belcamp, Maryland 21017, USA | |
| Phone | US | 1-800-545-6608 |
| International | 1-410-931-7520 |
| Technical Support Customer Portal | <https://serviceportal.safenet-inc.com>  Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base. | |



# Introduction

## Overview

This document is intended to guide security administrators through the steps to generate a CSR from an HSE and have it signed by the Keyfactor CA.

### 3rd Party Application Details

* Keyfactor CA

### Supported Platforms

The following platforms are tested with the Keyfactor CA:

| Platforms Tested | HSE SW Version |
| --- | --- |
| CN4010 | 3.0.2 |

## Prerequisites

### SafeNet HSE Setup

Refer to the SafeNet HSE documentation for installation steps and details regarding the configuration and initial setup of the HSE. Before you get started ensure the following:

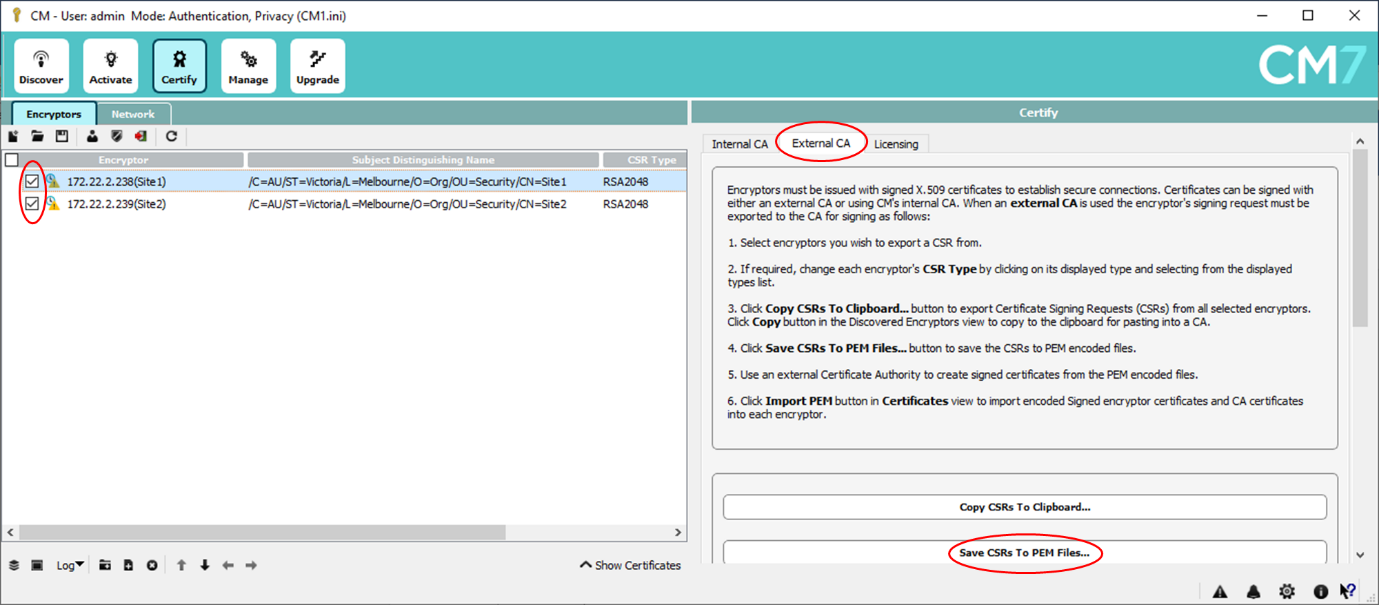
* Install the CM7 management application on the Management computer.
* Assign an ip address to the HSE via the serial interface.
* Discover and Activate the HSE in CM7.

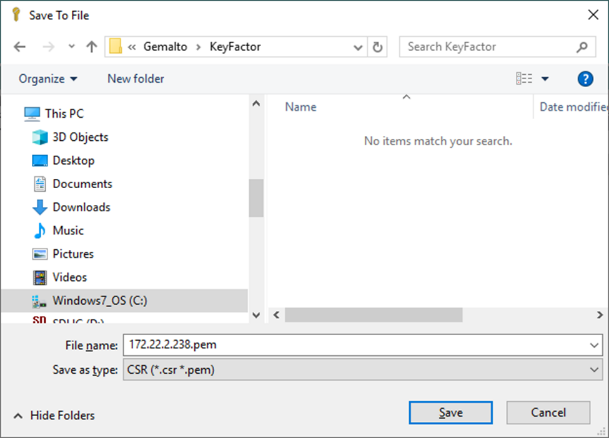
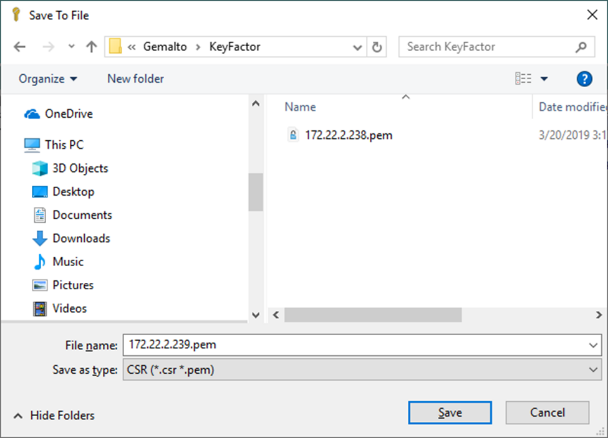
# Signing an HSE Certificate Request with Keyfactor

## Generate the CSR for the HSE from CM7

Generate a Certificate Signing Request (CSR) using CM7 following the steps below:

* Launch CM7 and login and them select the Certify button at the top of the CM7 window. Select the HSEs in the list (select each checkbox).
  + On the right of CM7 windows, select the “External CA” tab.
  + Next, click on “Save CSRs To PEM Files…”.

Browse to where you want to save the files – you will get a pop-up windows for each HSE selected:

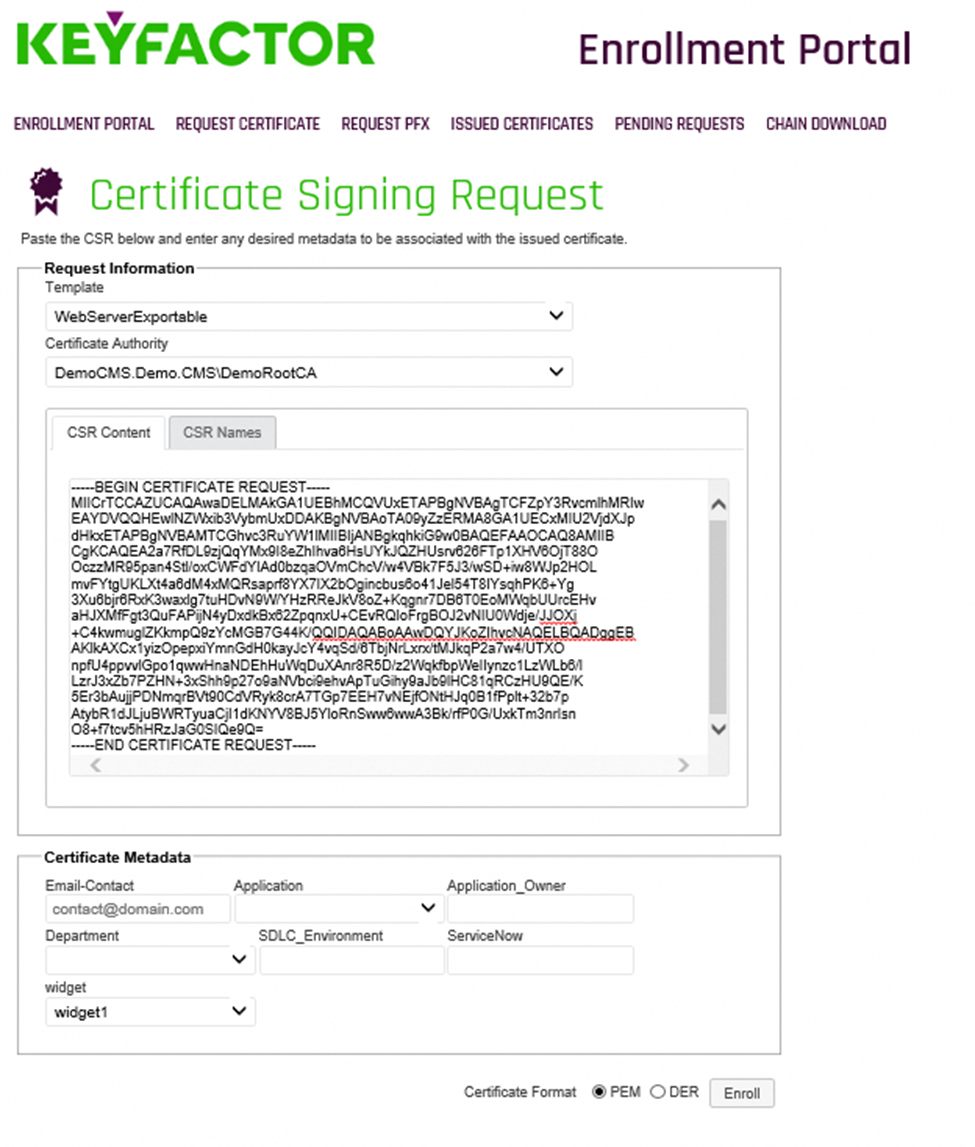
 

* This is the PEM file for one of the devices:  
  
* Send the PEM files to the Keyfactor administrator for them to be signed.

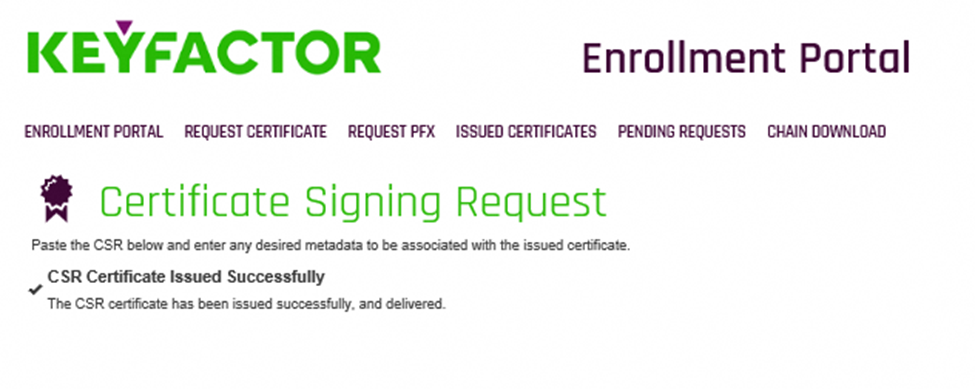
### Keyfactor Signing

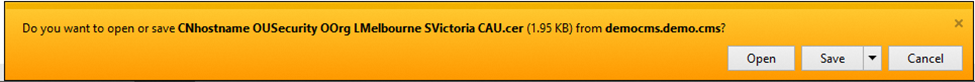
Step 1:

Paste the CSR into Keyfactor COMMAND platform & click Enroll



Step 2: Once the certificate is generated, please download certificate along with the certificate chain

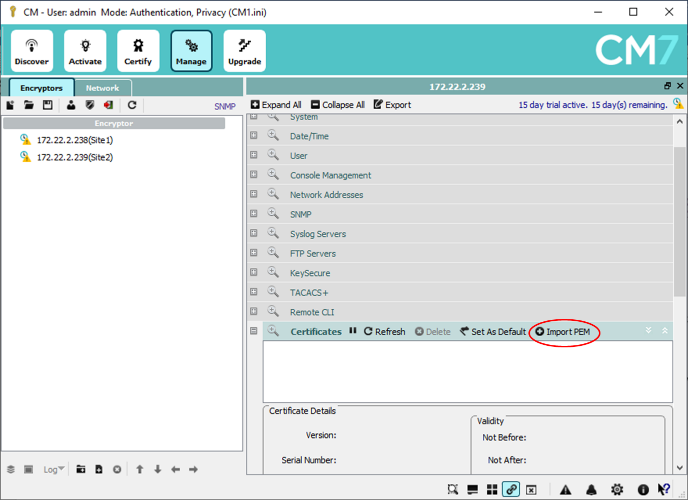
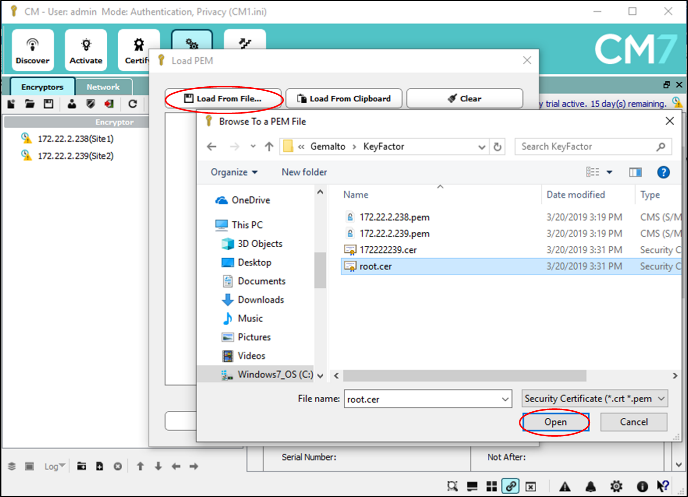
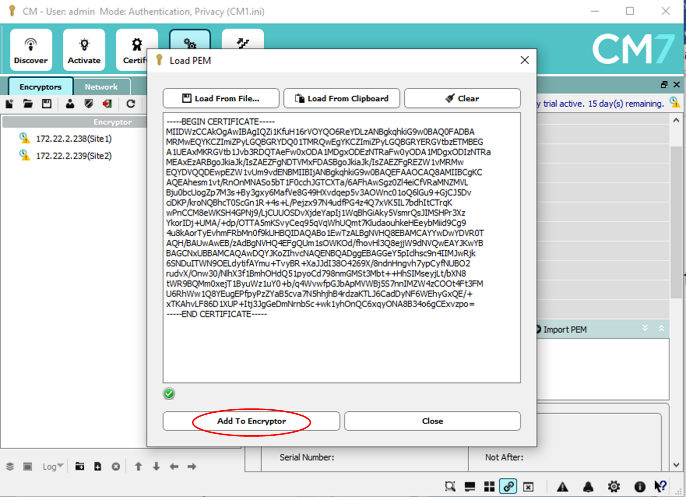


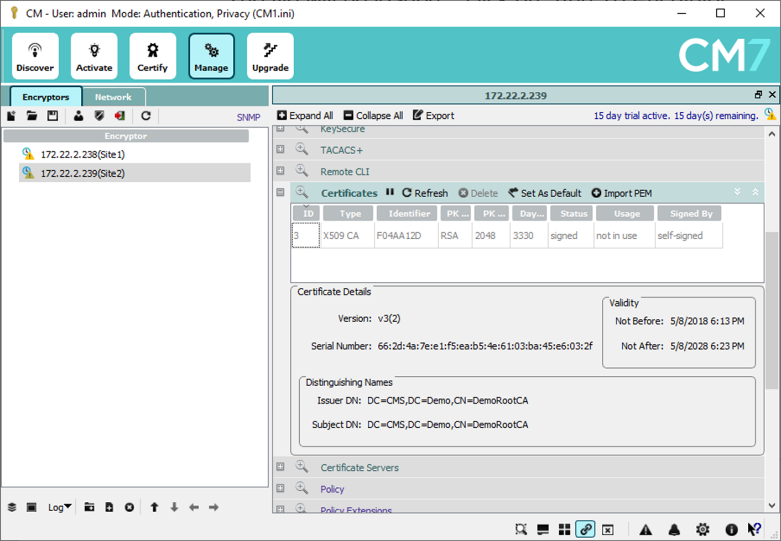


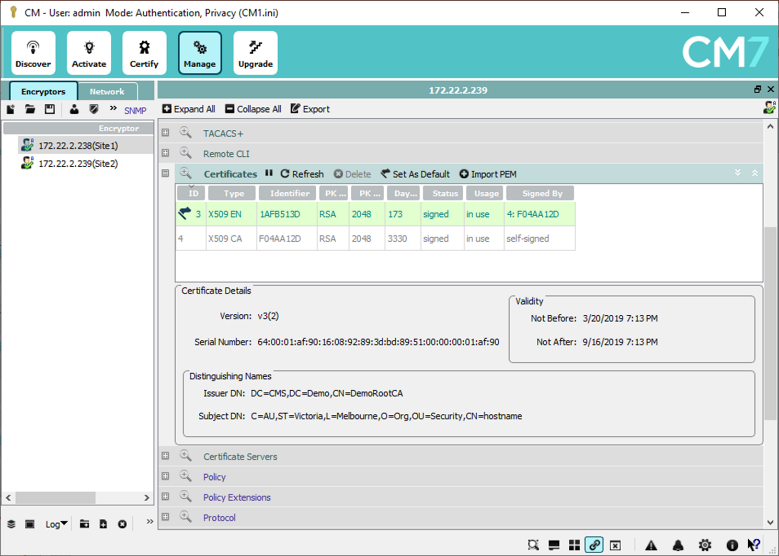
Step 3: Send the root certificate and the signed certificate to the CM7 administrator.

#### Install the Signed Certificate on the HSEs

Once you have received the signed certificate from the Keyfactor administrator, follow the instructions below to install both the root certificate and the signed certificate on the HSE:

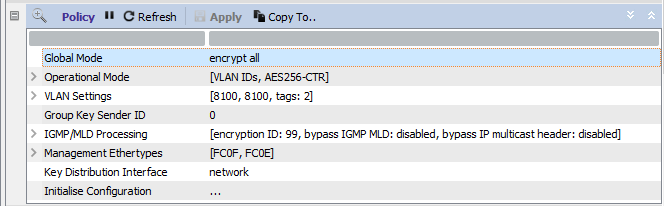
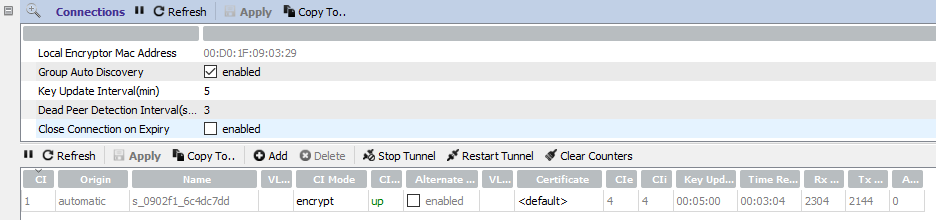
* Launch CM7 and login and select the “Manage” option at the top of the window.
* Expand the “Certificates” section of the HSE and click on Import PEM. Select the root certificate  
  
* Select “Load from File…” and browse to the location of the root certificate and select it and click on Open.  
  
* The file will be loaded – click on “Add To Encryptor”.  
  
* The root certificate is now installed on the HSE.



* Now click on “Import PEM” and repeat the process for the signed certificate for the HSE.  
  

Now both the root certificate and signed device certificate is installed on the HSE. This process should be repeated for all HSEs in the network.

Next step is to enable an encryption policy and send traffic.

* Expand the “Policy” section and enable encryption on the HSEs.  
  
* Now send traffic and validate the connection is up and traffic is passing.   
  (Note: there are pings running through the HSEs – this is what the traffic counts show.)  
    
    
  The screenshot above shows that the connection is up and the traffic counts are non-zero indicating encrypted traffic. Also notice that the Key update interval is 5 minutes. The key renewals will increment the CIe and CIi fields.   
    
  Note: The connection would not have been established if the certificates signed by Keyfactor were incompatible. As the connection came up and as will be seen in the screenshot below, the key renewals also work means that the Keyfactor certificates successfully worked to establish the connection.  
    
  After 20+ minutes of the connection being established, below is an updated screenshot of the connection:  
    
  As can be seen above, the CIe and CIi fields have a value of 4 which means there have been 4 successful key renewals. The Rx and Tx counters have also increased in value indicating that encrypted traffic continued during the key renewals.