Integration Guide

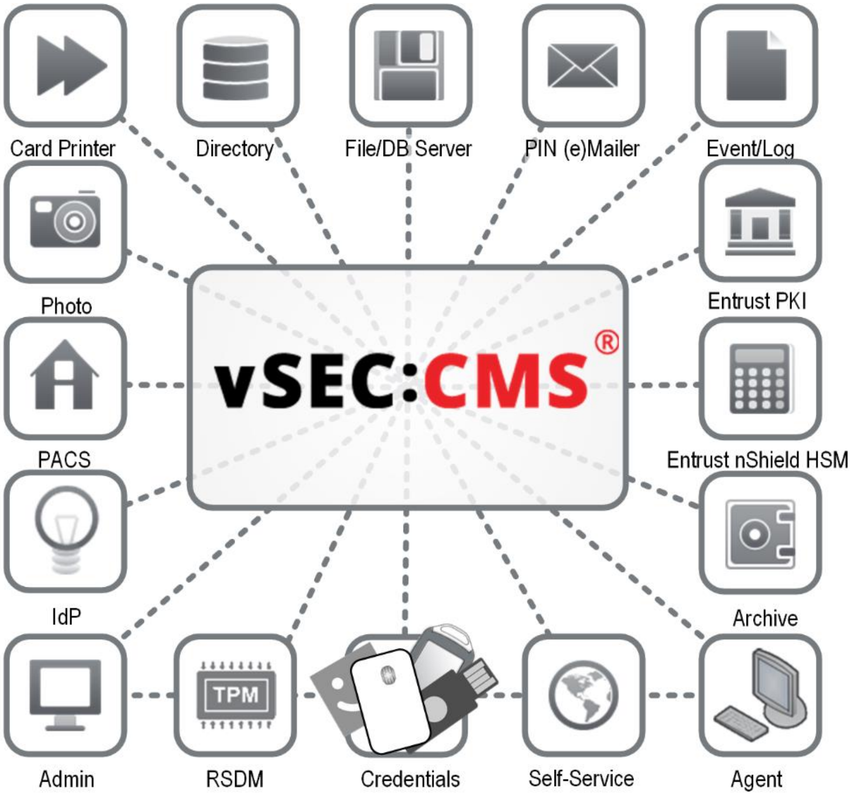
Entrust CA Gateway and Versasec vSEC:CMS

Document issue: 1.0
Date of Issue: June 2021
Date of Review: November 2021

Contents

Introduction

vSEC:CMS will change your views on how to manage the lifecycle of physical and virtual credentials. It is an innovative, easily integrated and cost-effective Credential Management System that will help you deploy and manage secure authentication devices within your organization. vSEC:CMS is a client-server system that integrates deeply with the ecosystem that surrounds and interacts with the security credential.



Versasec vSEC:CMS is integrated with Entrust Certificate Authority (CA) Gateway; PKIaaS; Entrust nShield HSMs and Entrust Datacard printers SR300 and CR805.

vSEC:CMS streamlines all aspects of a credential management system by connecting to enterprise directories, certificate authorities, smart card printers, physical access control systems, email servers, log servers, PIN mailers... the list goes on. With vSEC:CMS, organisations can issue PKI devices and credentials to employees, personalize them with authentication credentials and manage their lifecycle directly from the off-the-shelf system.

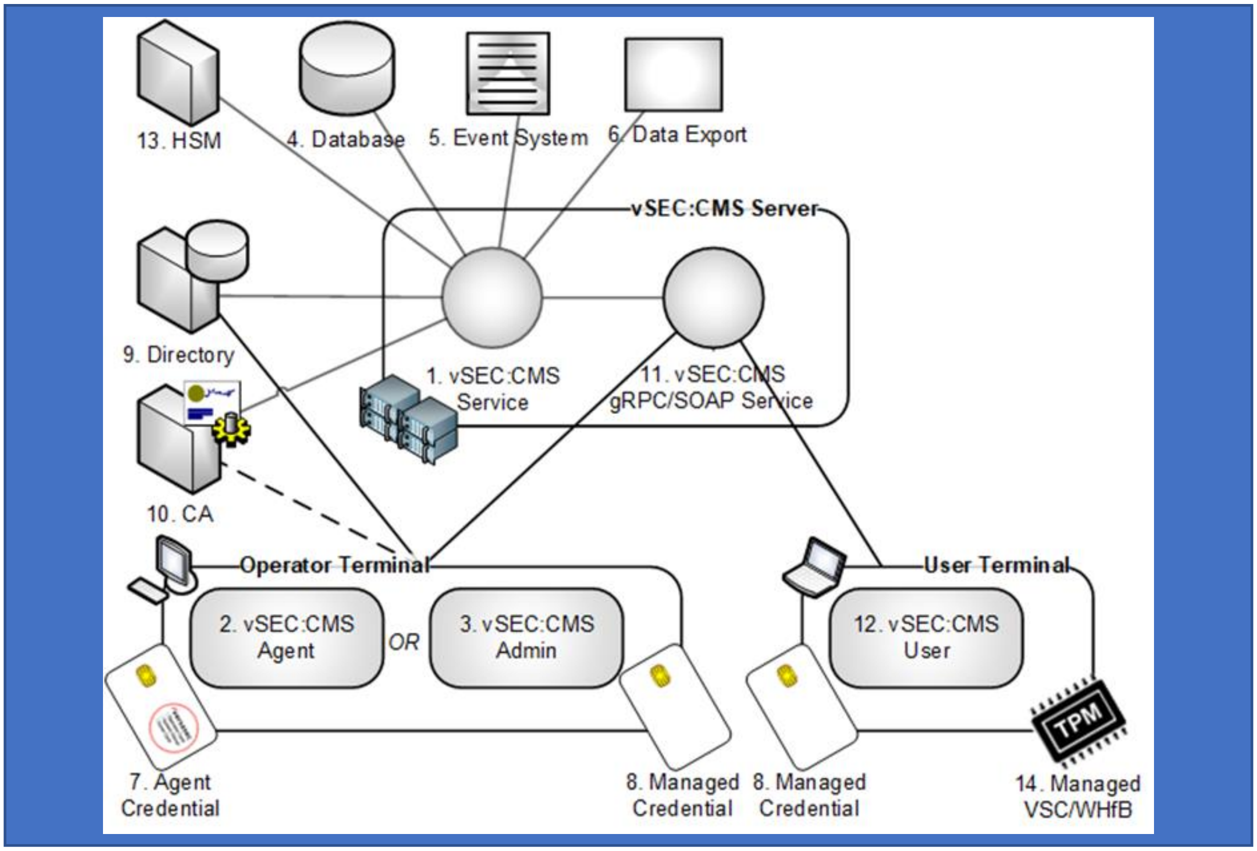
Enterprises can implement the feature-rich credential management system offering a variety of key benefits:

- Fast implementation that takes minutes, rather than weeks or months;
- Smooth and fast integration with other systems;
- Intuitive user interface that improves operational efficiency;
- No hidden costs and low total cost of ownership;
- Consistently high security level without exception;
- Large scale capabilities, available from day one.

Architecture

A full architecture involves a number of components, as well as a number of external components. The architectural diagram below illustrates a complete deployment with all optional components included.

Figure 1



vSEC:CMS is client-server-based software system with four main components:

- A MS Windows service, named vSEC:CMS Service in the architecture drawing above, it performs all the key computations and manages all the connections.
- A MS Windows service, named vSEC:CMS SOAP/gRPC Service in the architecture drawing above, which communicates with the vSEC:CMS Service and is the interface for the vSEC:CMS Admin/Agent/User applications.
- The vSEC:CMS Admin and vSEC:CMS Agent applications, which is run by operators in the user's context and provides both the management and the administration interface to the vSEC:CMS system.
- The vSEC:CMS User which is run on an end user's workstation from where users can perform self-service operations.

The communication channel between the vSEC:CMS Server Service and the vSEC:CMS Admin/Agent/User applications are secured using AES128 encryption.

The vSEC:CMS Admin and vSEC:CMS User application construct requests (gRPC or SOAP XML using Windows Web Services API (WWSAPI)). The requests are sent using HTTP/HTTPS to the vSEC:CMS Comm Service. The vSEC:CMS Comm Service is a .NET WWSAPI service running as a Windows service.

The vSEC:CMS Comm Service performs as follows:

- Sends the request as received from the vSEC:CMS Admin/Agent/User applications to the vSEC:CMS Windows service through encrypted shared memory;
- Receives back the response from the vSEC:CMS Windows service through encrypted shared memory;
- Constructs the response;
- Returns the response to the vSEC:CMS Admin/Agent/User applications.

vSEC:CMS Service

The vSEC:CMS Service is managing the Database connection. If the vSEC:CMS internal DB is used, its data files (SQLite) are stored in the [DAT] folder which sits beside the service executables. For production use of vSEC:CMS Versasec recommends using a SQL database.

By default the security keys used by vSEC:CMS are stored in a software key store in the vSEC:CMS Service (stored encrypted on file system, loaded obfuscated in non-pageable memory of the service process). Alternatively the keys can be stored/protected by an on-premise or cloud-based HSM.

The credentials to access the CA (Enrollment Agent in case of Microsoft CA) are normally stored in the vSEC:CMS Service and used for the whole system. Alternatively “personalized” credentials stored on each Operator token are supported..

If configured, the vSEC:CMS Service will send status information to the MS Windows Event System.

vSEC:CMS Comm Service

The vSEC:CMS Comm Service communicates with the vSEC:CMS Service over an encrypted direct data channel. The vSEC:CMS Comm Service is the Server that the Clients communicate with. The Clients are the vSEC:CMS Admin, vSEC:CMS Agent and the vSEC:CMS User applications. The communication is using gRPC or alternatively for backward compatibility SOAP, both over HTTPS. The vSEC:CMS Comm Service has three separate Windows services named vSEC:CMS - Operator Console Service for vSEC:CMS Admin and vSEC:CMS Agent applications, vSEC:CMS - User Self-Service for the vSEC:CMS User application and the vSEC:CMS RSDM service for managing virtual credentials on remote computers.

vSEC:CMS Admin

vSEC:CMS Admin is started for each operator in the context of the currently logged on user. It provides the application interface to the operator. The operator needs to logon to the application using a valid operator token (hardware credential), thereby providing two-factor authentication.

vSEC:CMS Agent

vSEC:CMS Agent has all the day-to-day capabilities of vSEC:CMS Admin but in a more lightweight format. The operator needs to logon to the application using a valid operator token (hardware credential), thereby providing two-factor authentication.

vSEC:CMS User

The vSEC:CMS User application is started for each user on their workstation. It provides the UI to the user to perform user self-service operations on their credential. All communication is performed through the vSEC:CMS Comm Service. The connection and the port is configurable through the vSEC:CMS Admin interface.

System Operators and Roles

An operator is any person who is in possession, and has knowledge of the passcode, of an Operator credential and can therefore perform operations with vSEC:CMS.

There are two types of operator tokens:

1. The System Owner – one required per system. Used for administrative purposes, but not recommended for normal operator use. This token is assigned when loading the production license for a new vSEC:CMS installation. Any vSEC:CMS supported physical credential can be used (one license count will be consumed). Once the system has been initialized and setup it is recommended that the System Owner credential is stored safely, for example in a safe;
2. The Authentication Only Operator. Any supported vSEC:CMS physical credential can be used and consumes one license count per operator token.

Operators have different roles, each of which has different levels in regards to what operations they can perform. The default roles are defined as:

- System Administrator: an operator that can perform all operations
- Elevated: an operator that can perform license upgrade and configuration changes
- Normal: an operator that can perform credential management workflows
- Restricted: an operator that can perform credential unblock workflows;
- Key recovery: an operator that can perform key recovery workflows.

Role management for operators is fully customisable. The default roles can be customised fully as needed, or if you need to add more roles, new ones can be created as well.

Capabilities

A number of capabilities are offered around such topics as:

- Mobile device support
- PIV and PIV-D container support
- Onboarding and maintenance of PIV and PIV-D credentials
- Smartcard logon to Microsoft Windows and Apple Mac desktops

This table identifies the features supported by the Versasec

1. Entrust CAGW:

Which features from CAGW that vSEC:CMS can/should support?

#	CAGW Features	vSEC:CMS Support
1.	CA Key archive, support recovery all keys from CA.	×
2.	Support key generate in smartcard/token (OBKG)	√
3.	Support multi-CA in backend: Entrust SM, Windows CA.	√
4.	Certificate renew	×
5.	Certificate reissue	√
6.	Certificate revocation (revoke, suspend/resume)	√

2. About CMS in general:

#	Features	vSEC:CMS Support?
<hardware: smart card, token,…>		
1.	PIV	√
2.	Onboarding and maintenance of PIV and PIV-D credentials	√
3.	Standard Minidriver(40 card types supported).	√
<software: not really hardware….>		
4.	Mobile device support	X
5.	VSC	√
6.	Windows Hello for Business (WHfB)	√
<usage purpose>		
7.	Smartcard logon to Microsoft Windows and Apple Mac desktops	√

8.	Email singning & Encryption	√
<CMS special features>		
9.	Device management	√
10.	Multi-role	√
11.	PIN Management	√
12.	Administrator Key Management	√
13.	Support API for 3rd products integration.	√

Preparing Your Certificate Authority

Services can be configured to communicate with either the Entrust Authority Security Manager CA or Microsoft's CA. Please refer to your CA's documentation to determine how to administer it.

For the purposes of this integration, your organization must configure digital IDs which support the following types of key-pairs and certificates.

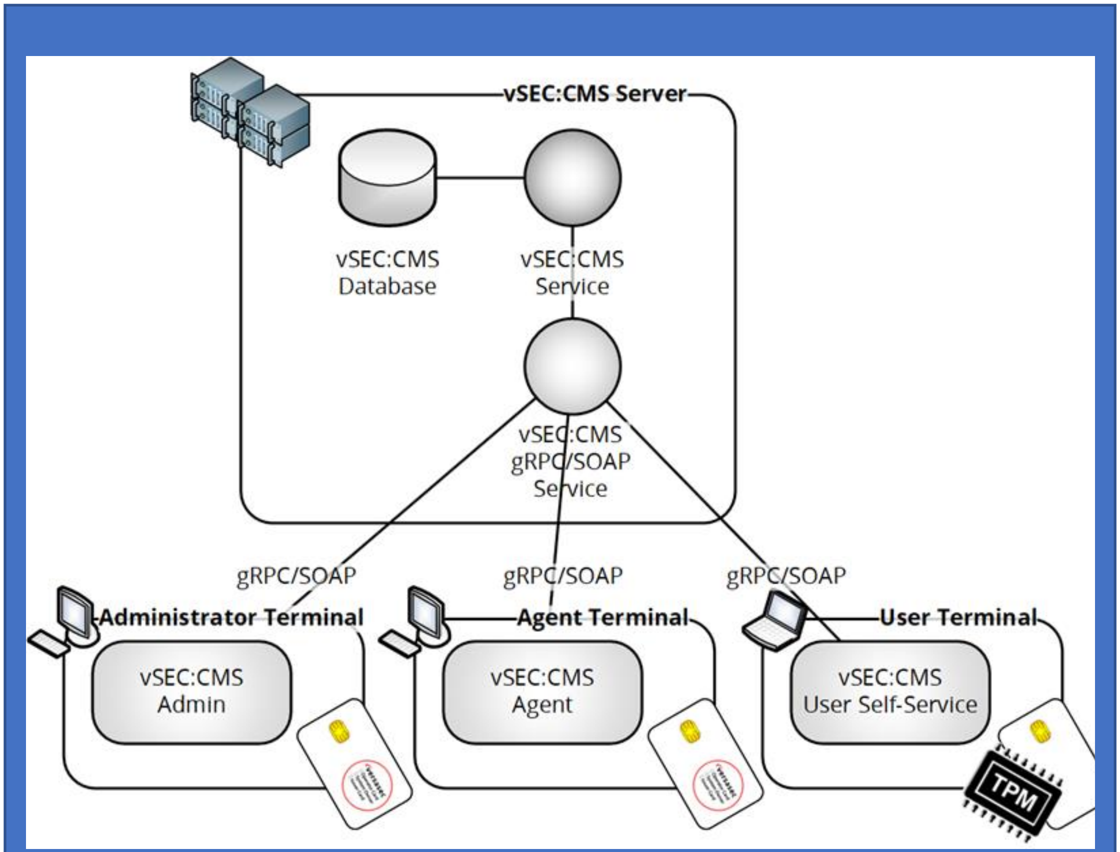
- 1 key-pair, ex. when you require PIV Authentication certificates
- 2 key-pair, ex. when you require PIV Authentication and Digital Signature certificates
- 3 key-pair, ex. when you require PIV Authentication, Digital Signature certificates, and PIV Key Management (encryption) certificates

Integration Guidelines

Overview

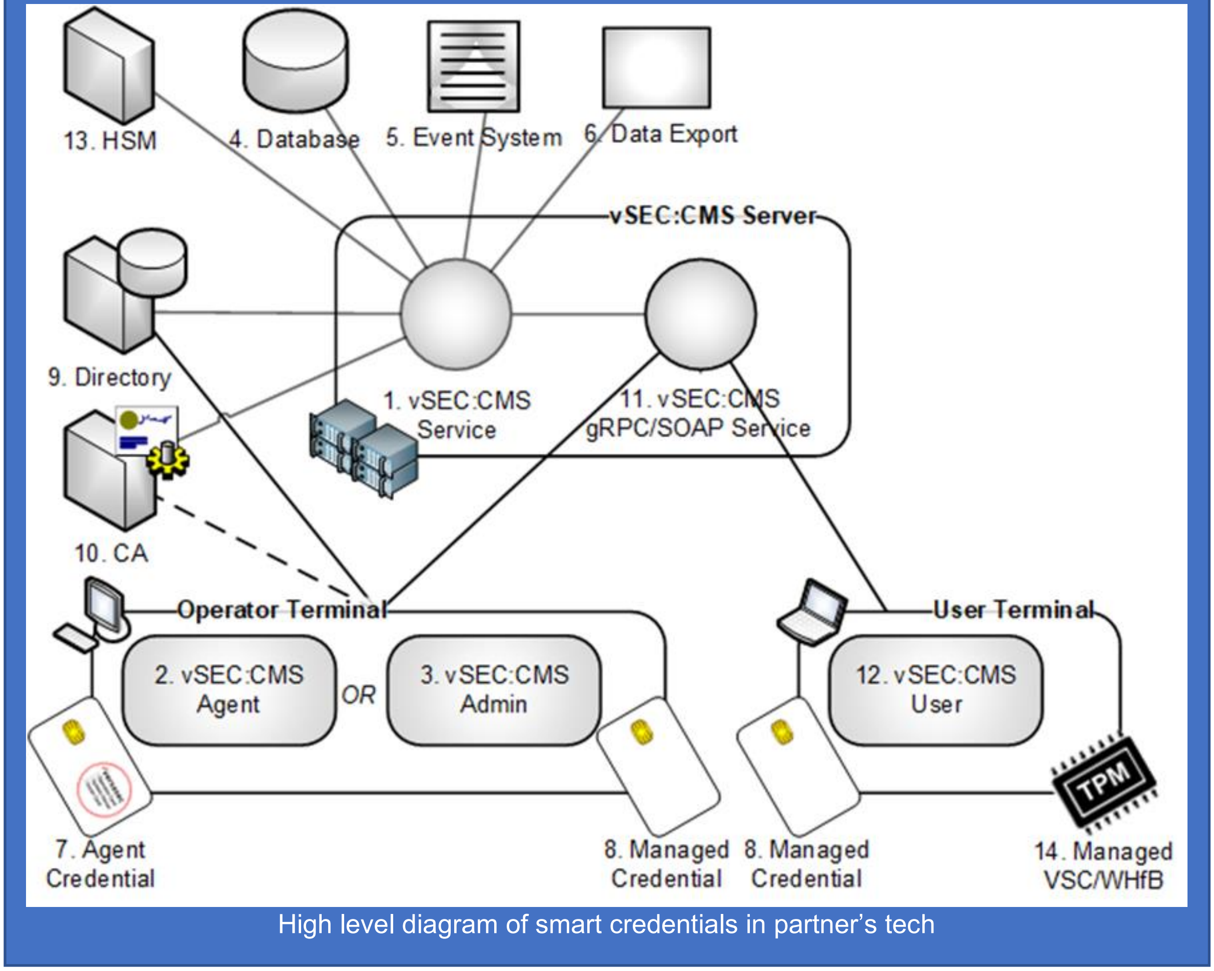
Introduction to Integration Partner's Technology

1. https://versasec.zendesk.com/hc/en-us/articles/360021224540-Using-Entrust-Gateway-CA
2. High level architecture diagram. For more detailed architecture information, please refer to the documentation at this link



High level architecture diagram

3. High level diagram of Entrust Smart Credentials in integration partner's technology



High level diagram of smart credentials in partner's tech

The following Entrust Technologies are integrated with Versasec vSEC:CMS:

- Entrust Datacard printers SR300, CR805 with (2) vSEC:CMS Agent and (3) vSEC:CMS Admin
- Entrust CA Gateway, Entrust PKIaaS with (10) CA
- Entrust nShield HSMs with (13) HSM

Requirements

From vSEC:CMS S-Series version 6.0 it is possible to configure connection to Entrust CA Gateway to manage certificate lifecycle with any credential that is supported by vSEC:CMS. The Entrust CA Gateway API is a RESTful Web service API that provides a range of certificate issuance and management functions.

Hardware Requirements
vSEC:CMS can be installed on following server platforms:

a. Microsoft Windows 2008 Server;
b. Microsoft Windows 2008 R2 Server;
c. Microsoft Windows 2012 Server;
d. Microsoft Windows 2012 R2 Server;
e. Microsoft Windows 2016 Server;
f. Microsoft Windows 2019 Server.
g. Virtual servers are supported

The server minimum hardware requirement:

h. At minimum 2 Processor with 2 GHz or faster;
i. Memory 2 GB RAM or greater;
j. Available disk space on server of 40 GB or greater for the operating system plus 2GB or greater for the vSEC:CMS database.

Server recommended hardware requirement where the vSEC:CMS is installed:

k. At minimum 2 Intel Xeon processors with 2 GHz or faster;
l. Memory 8 GB or greater;
m. Available disk space on server of 40 GB or greater for the operating system plus 2GB or greater for the vSEC:CMS database;
n. Gigabit-LAN (1.000 Mbit/s).

Client recommended hardware requirements for any workstation that vSEC:CMS operator console is installed on:

o. At minimum 2 Intel i7 processors with 3.6 GHz or faster;
p. Memory 8 GB or greater;
q. Gigabit-LAN (1.000 Mbit/s).

Software Requirements
Depending on the credential that you are using it will be necessary to have the appropriate credential drivers installed on your host. Check with the credential provider that you have the correct credential drivers installed.

Additionally, for versions prior to 6.0 Microsoft .NET Framework 4.7.2 should be installed on any host where vSEC:CMS components are installed. From version 6.0 and above Microsoft .NET Framework 4.8 should be installed.

Tip: You can validate what version of Microsoft .NET Framework is installed on your host by running the Powershell command so see the Full version information:

r. Get-ChildItem 'HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP' -Recurse | Get-ItemProperty -Name version -EA 0 | Where { $_.PSChildName -Match '^(?!S)\p{L}'} | Select PSChildName, version

The complete list of supported credentials https://versasec.com/products/supported-smart-cards

Configuration

To use the Entrust Derived Credentials feature in vSEC:CMS, the customer needs the following:

1. Entrust CA Gateway Account and credentials
2. Installation and Configuration of vSEC:CMS
    - Setup vSEC:CMS
    - First Time StartUp
    - Create of System Owner Hardware Credential
    - AD Configuration
3. Entrust CA Gateway Connection
    - Configure Connection
4. vSEC:CMS Agent Application (from version 6.1)

Entrust CA Gateway Account

Use of CA Gateway requires a purchase from Entrust and a credential in order to connect. Contact Entrust account team for more information info@entrust.com

Installation & Configuration of vSEC:CMS

Install the version of vSEC:CMS https://versasec.com/products/product-registration

Setup vSEC:CMS

- RDP to the server where vSEC:CMS is to be installed and start the installer vSECCMS_Setup_X.X.X.exe and select **I Agree** to consent to the license agreement, where X.X.X is the specific version you are deploying;

- Select Server: Installation of the Server component (including Operator Console) to install the server component and click Next;

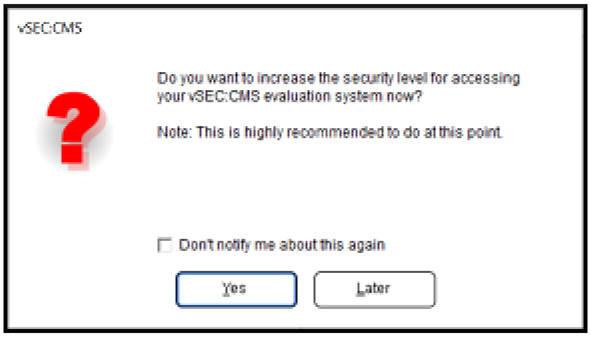
- Accept the default location for the installation or change this if required and click Install;

- Once complete click **Close** to finish.

- We now have a fully installed version of vSEC:CMS and we can start the Operator Console (OC) from the shortcut icon on the desktop.

First Time Startup

- On starting the OC for the first time you will receive a message dialog prompting you to create a passcode as no passcode has been set.



vSEC:CMS

Do you want to increase the security level for accessing your vSEC:CMS evaluation system now?

Note: This is highly recommended to do at this point.

□ Don't notify me about this again

- It is important to set one up at this stage to protect access even in this evaluation phase. Select Yes and create a passcode that will be used to log onto the OC.

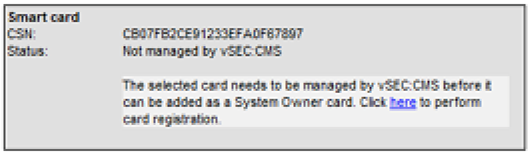
Creation of System Owner Hardware Credential

It is not mandatory for the evaluation version to create a System Owner (SO) credential. **We strongly recommend creating the System Owner credential since it will be a mandatory step to migrate to the Production license version.** Any of the vSEC:CMS supported hardware credentials can be used for this step.

Important: Depending on the credential that you are testing with it will be necessary to have the appropriate credential drivers installed on your host. Please check with the credential provider that you have the correct credential drivers installed.
Important: It will be required that USB redirection is allowed on the server where vSEC:CMS is installed such that the locally connected smart card that is to be used as SO is available to the server.

Important: Once you create the SO credential, and presuming it is used when upgrading to a production system, it will only be possible to reset the credential to its factory settings if the credential vendor provides tools to reset their credential. Some credential vendors do not provide such tools, therefore in that case once the SO credential is created it will not be possible to reset it to its default factory state. However, if you are still in evaluation mode and you wish to start from scratch, then you can restore the SO credential to its default state. Navigate to Options - Operators and select the System Owner in the table and click the Delete button to restore it to its default factory state.
Important: Ensure that a credential configuration exists for the credential that you are going to use here. See the article Add Credential Configuration before starting below.

- From the **File** menu select **Add System Owner Card**. With a supported credential connected to your host you should select the credential from the reader list. **Note:** If you are using a PIV supported credential then it will be necessary to register the credential before it can be issued as an SO credential. You need to click the link to register the credential as in the example below before you can complete the other steps described below.



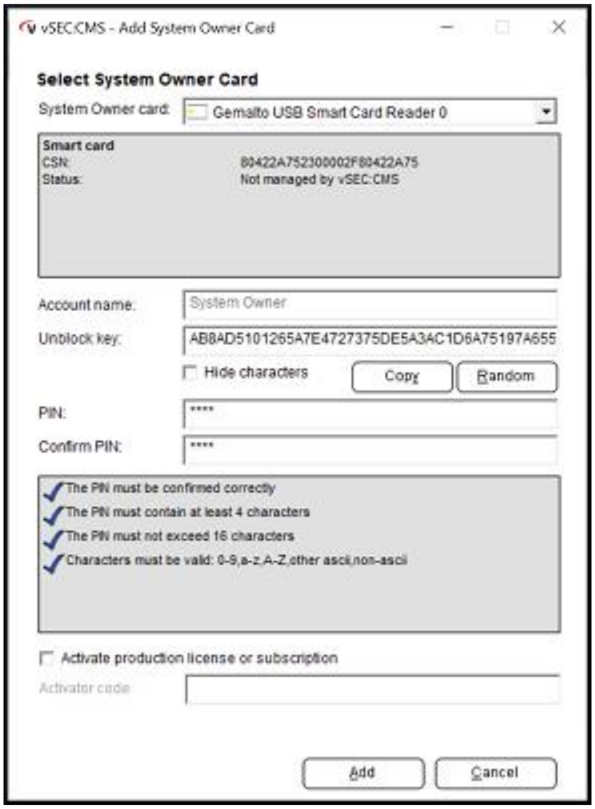
Smart card
CSN: CB07FB2CE91233EFA0F67897
Status: Not managed by vSEC:CMS

The selected card needs to be managed by vSEC:CMS before it can be added as a System Owner card. Click here to perform card registration.

- Click the **Random** button to allow vSEC:CMS to generate a random unblock key and click the **Copy** button. You should save this information to a secure location as this may be needed in the future if you need to unblock the credential. Enter a PIN and confirm. Uncheck the **Activate production license or subscription** checkbox as you are still using the evaluation version and click the **Add** button.

Below is an example of how the setting would look.

- Once complete a summary dialog will appear describing what steps were performed. The credential will then be managed by vSEC:CMS. If you wish to revert back to use passcode only to access the vSEC:CMS then from the **Options - Operators** select the **System Owner** in the table and click the **Delete** button to revert back to passcode only.



Select System Owner Card

System Owner card: Gemalto USB Smart Card Reader 0

Smart card
CSN: 80422A752300002F80422A75
Status: Not managed by vSEC:CMS

Account name: System Owner
Unblock key: AB8AD5101265A7E4727375DE5A3AC1D6A75197A655
□ Hide characters
PIN: ****
Confirm PIN: ****

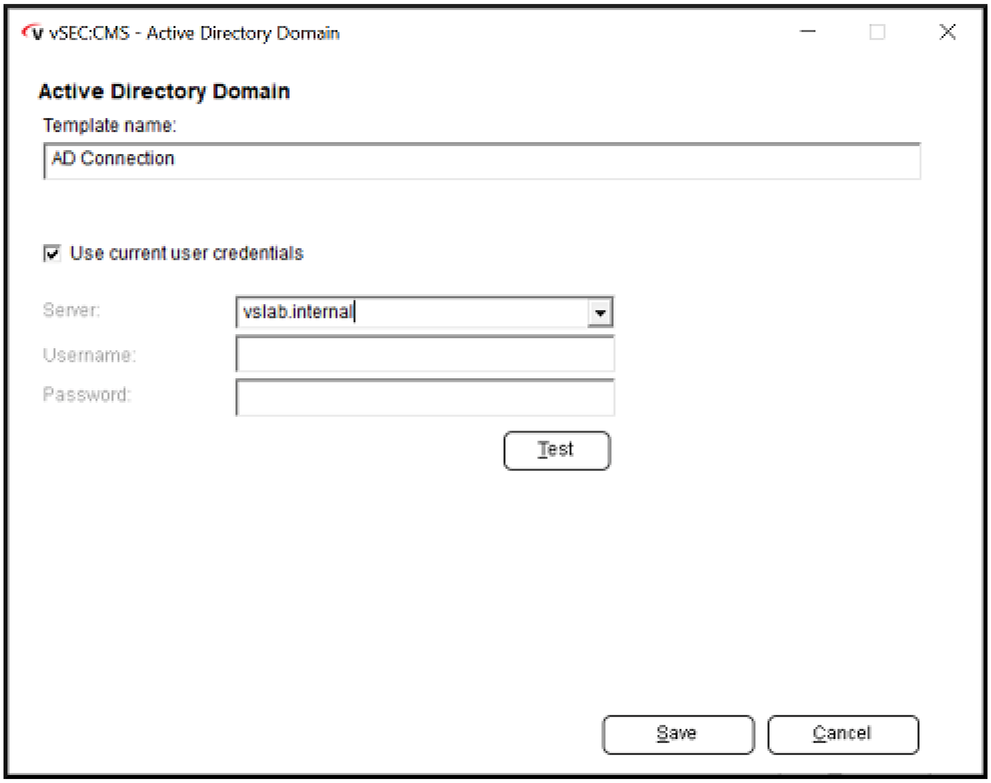
✓ The PIN must be confirmed correctly
✓ The PIN must contain at least 4 characters
✓ The PIN must not exceed 16 characters
✓ Characters must be valid: 0-9,a-z,A-Z,other ascii,non-ascii

□ Activate production license or subscription
Activator code

AD Configuration

- From **Options - Connections** click **Add** and **select Active Directory** and click **Ok.**

- **Enter a template name** and presuming that vSEC:CMS is on a server that can access the AD it is recommended to select Use current user credentials. In the Server drop-down list **select the AD** you wish to use and **click the Test button** to verify that you can connect to and find a user in your AD.



Template name: AD Connection

☑ Use current user credentials

Server: vslab.internal

Username:

Password:

Note: vSEC:CMS only performs reads from AD.

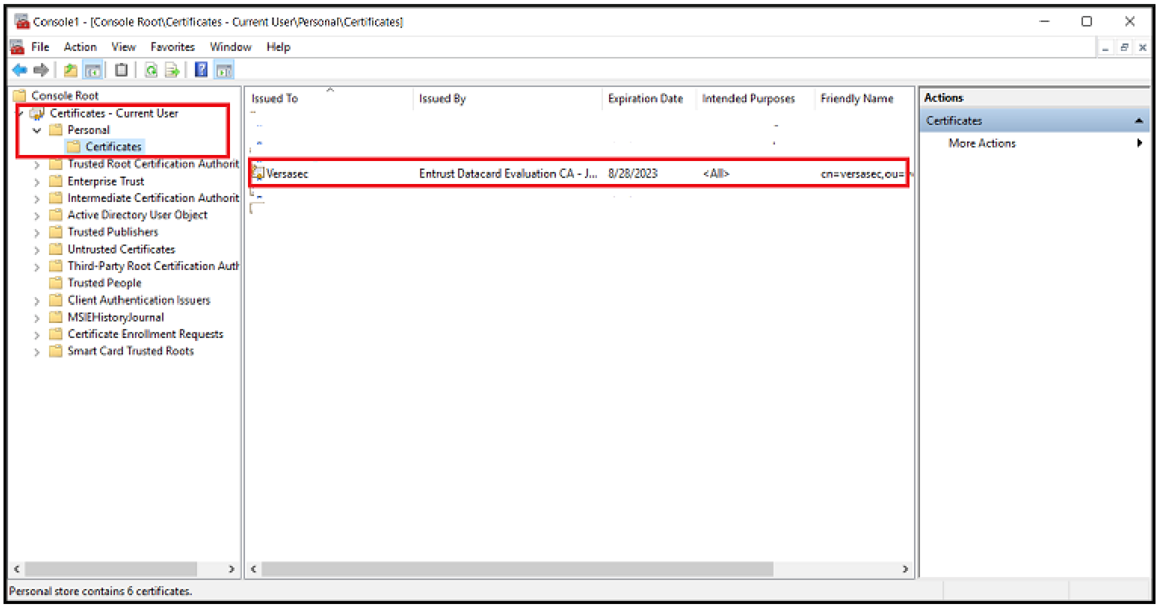
- If you are not connected to AD then you can uncheck **Use current user credentials** and manually enter an AD hostname/IP address and user and password to connect with.
- Click **Save** to save and close the configuration.

Entrust CA Gateway Connection

Configure Connection

- The first requirement is to set up a connection to your Entrust CA Gateway. Navigate to **Options - Connections - Certificate Authorities** and click **Add**. Enter a template name and in the drop-down field select **Entrust Gateway**. In the **Entrust Gateway Server URL** enter the appropriate connection URL for your setup. You will need to have a client certificate for the connection. This can be installed in the local Microsoft certificate store for the Windows account that vSEC:CMS service is running under.

Important: It is recommended that the client certificate used here is installed into the local Microsoft certificate store before configuring the connection. For example, in this example the certificate is stored as below where the Current User is the Windows user that vSEC:CMS service is running under.



Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

- Console Root
  - Certificates - Current User
    - Personal
      - Certificates
    - Trusted Root Certification Authorit
    - Enterprise Trust
    - Intermediate Certification Authorit
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Auth
    - Trusted People
    - Client Authentication Issuers
    - MSIEHistoryJournal
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots

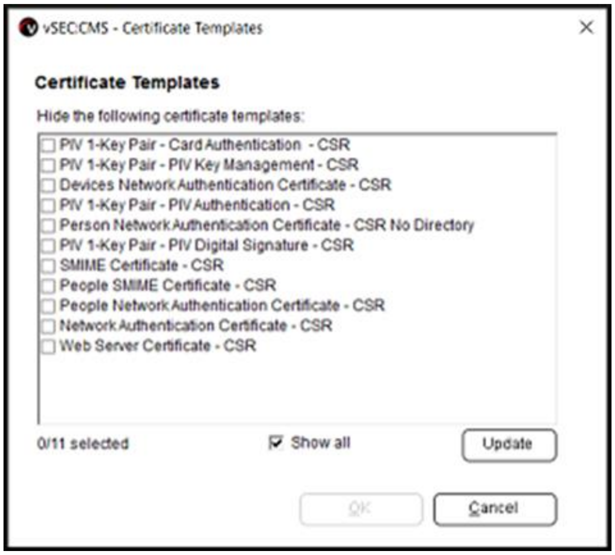
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
Versasec	Entrust Datacard Evaluation CA - J...	8/28/2023	<All>	cn=versasec,ou=

Personal store contains 6 certificates.

- Click the **Test** button to test that the details are correct and that you can connect ok. If all the details are correct you should get a success dialog.

- Click the **Get Instances** which will retrieve all available CAs. Select the CA that you wish to use from the available ones in the drop-down field.

- Click the **Templates** button. Select **Show all** and click **Update**. You should see a list of all the available templates. Click **Ok** to close out.



vSEC:CMS - Certificate Templates

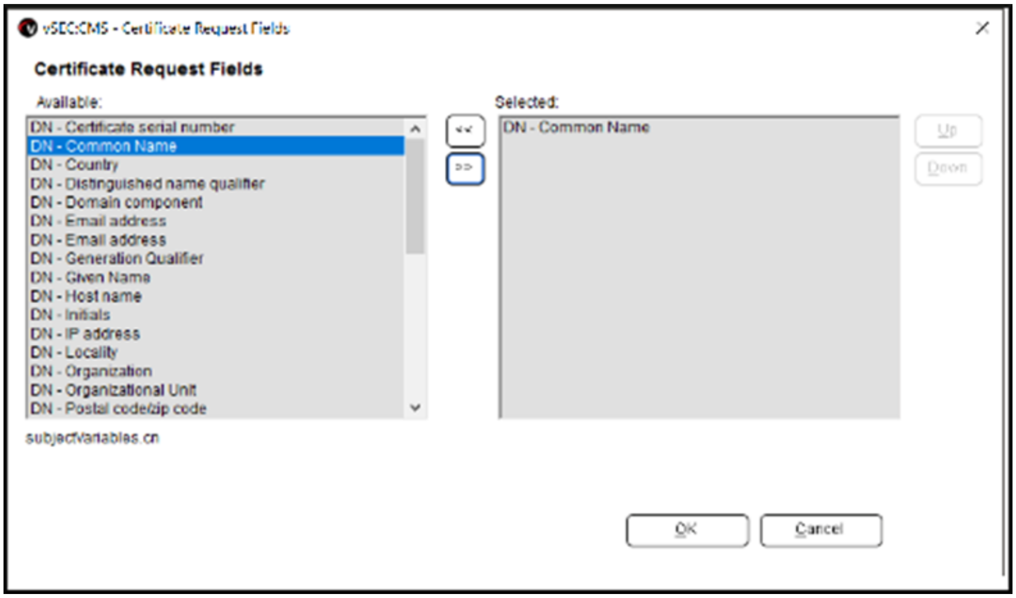
Certificate Templates

Hide the following certificate templates:

- □ PIV 1-Key Pair - Card Authentication - CSR
- □ PIV 1-Key Pair - PIV Key Management - CSR
- □ Devices Network Authentication Certificate - CSR
- □ PIV 1-Key Pair - PIV Authentication - CSR
- □ Person Network Authentication Certificate - CSR No Directory
- □ PIV 1-Key Pair - PIV Digital Signature - CSR
- □ SMIME Certificate - CSR
- □ People SMIME Certificate - CSR
- □ People Network Authentication Certificate - CSR
- □ Network Authentication Certificate - CSR
- □ Web Server Certificate - CSR

0/11 selected ☑ Show all

- Click the **Request fields** button. Here you configure how the certificate request fields will be populated depending on what you need to be set in the certificate request fields.
- Click the **Fields** button and from the **Available** list select the certificate request fields that you wish to use. In this example we will use **DN - Common Name** and add this to the **Selected** list on the right hand side and click **Ok**.



vSEC:CMS - Certificate Request Fields

Certificate Request Fields

Available:

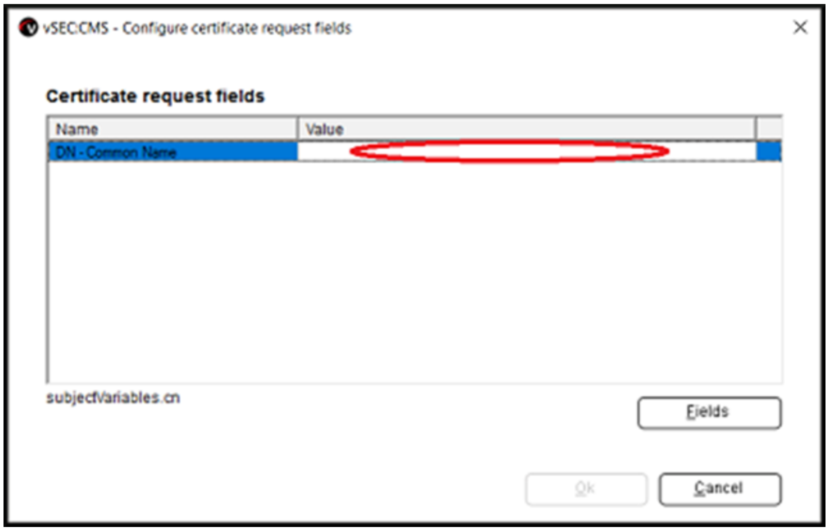
DN - Certificate serial number
DN - Common Name
DN - Country
DN - Distinguished name qualifier
DN - Domain component
DN - Email address
DN - Email address
DN - Generation Qualifier
DN - Given Name
DN - Host name
DN - Initials
DN - IP address
DN - Locality
DN - Organization
DN - Organizational Unit
DN - Postal code/zip code

Selected:

DN - Common Name

subjectVariables.cn

- We need to configure how the certificate request field gets populated with data. Click the **Value** field in the area as shown below.



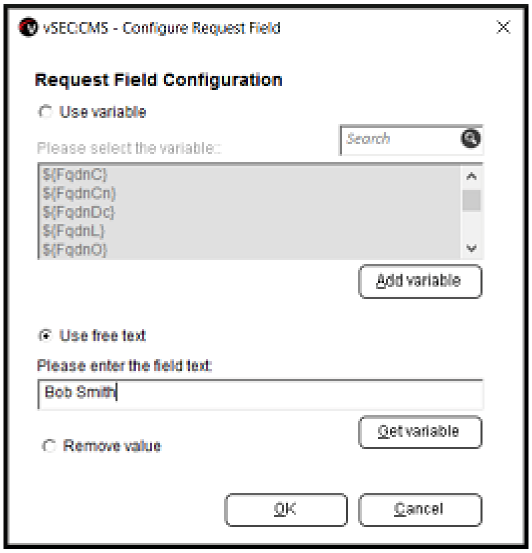
vSEC:CMS - Configure certificate request fields

Certificate request fields

Name	Value
DN - Common Name	

subjectVariables.cn

- This will popup a dialog like below. There are 2 ways that you can populate data into the request field. If you have vSEC:CMS variables already configured to map to Active Directory attributes then you can select **Use variable** and select the variable that you want to use or add one by clicking **Add variable**. Alternatively, select **Use free text** and enter the static data, Bob Smith in this example and select **Ok** to save and close



vSEC:CMS - Configure Request Field

Request Field Configuration

○ Use variable

Please select the variable:

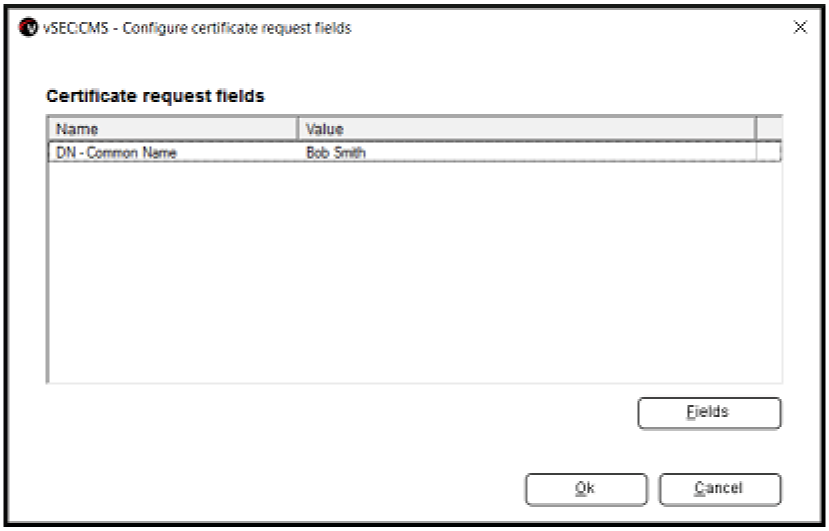
${FqdnC}
${FqdnCn}
${FqdnDc}
${FqdnL}
${FqdnO}

● Use free text

Please enter the field text: Bob Smith

○ Remove value

- Click **Ok** to save and close.

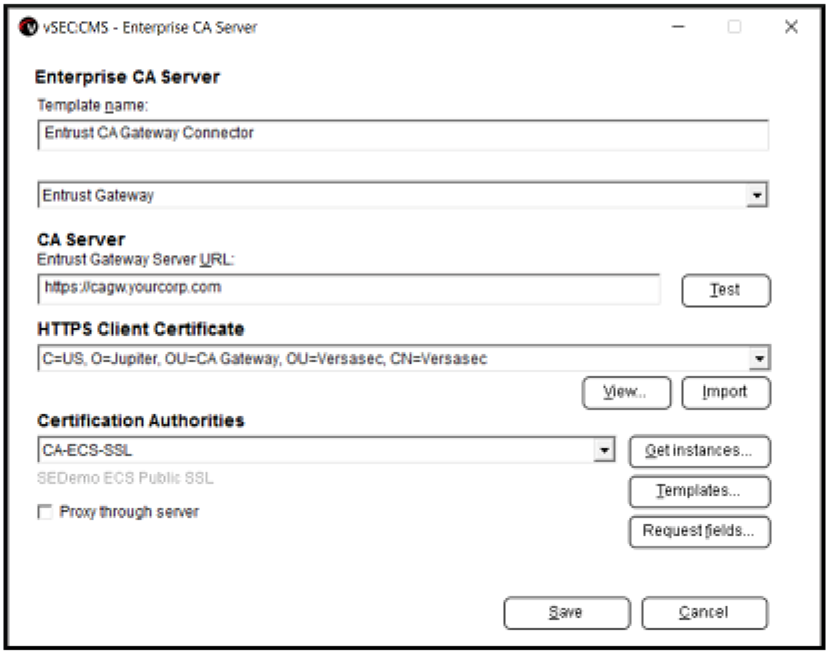


vSEC:CMS - Configure certificate request fields

Certificate request fields

Name	Value
DN - Common Name	Bob Smith

- You can enable the Proxy through server **(recommended)** if you plan to issue credentials through self-service or client operator consoles. Click Save to save and close the connection settings.



vSEC:CMS - Enterprise CA Server

Enterprise CA Server

Template name: Entrust CA Gateway Connector

Entrust Gateway

CA Server

Entrust Gateway Server URL: https://cagw.yourcorp.com

HTTPS Client Certificate

C=US, O=Jupiter, OU=CA Gateway, OU=Versasec, CN=Versasec

Certification Authorities

CA-ECS-SSL

SEDemo ECS Public SSL

□ Proxy through server

vSEC:CMS Agent Application

From version 6.1 vSEC:CMS can be installed on a host as a client Agent application. This is a lite version of vSEC:CMS Admin application which will allow an operator to perform the following tasks:

- Life cycle operations;

- PIN unblock flows, both online and offline;
- Certificate flows;
- View credential information.

Follow the installation instructions on Versasec Zendesk https://versasec.zendesk.com/hc/en-us/articles/4404055576850-Install-Agent-Application

Application Management

User Enrollment and Lifecycle Management

Enrolling Users

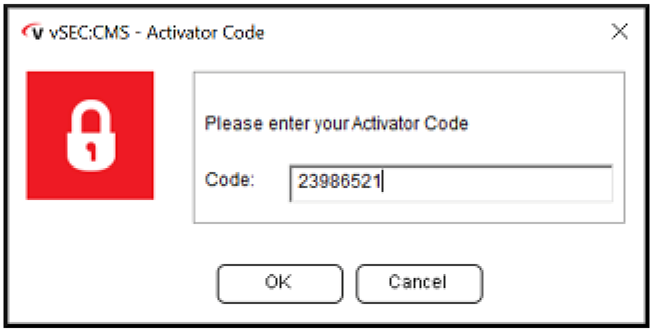
1. Migrate from Evaluation version to Production
   Setup Production Licenses
   Admin Action
2. The issuance workflow of credential can be performed via:
   - vSEC:CMS Admin (Admin Action)
   - vSEC:CMS User (User Action)

Migrate from Evaluation version to Production

Setup Production Licenses

You, as the end customer, receive an **Activation Code** from your provider and then you issue the production license using this.

- Log onto the vSEC:CMS console with your System Owner (SO) credential and navigate to Options - License and click the Activate button. Note: The SO credential used can be any credential that is supported by vSEC:CMS.
- You will be prompted to enter an activation code. You should have received the activation code from your provider already. Enter the code and click Ok.



Please enter your Activator Code

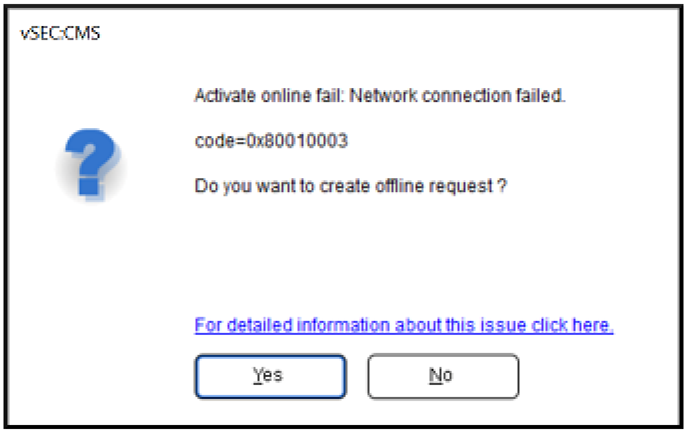
Code: 23986521

- Depending on whether the vSEC:CMS console session that you are logged into has an internet connection that can reach Versasec's licensing service or not, different options are available.

- If your host can connect to Versasec's licensing service, the console application will securely send the activation code to Versasec's license issuance service to validate the request and provide back the activation resulting in the system license becoming a production licensed system.

Important: During this process a new secure master key will be generated. It is important to update any credentials that may have been issued when vSEC:CMS was in the evaluation version.

- If your host cannot connect to Versasec's licensing service when you click the Ok button for the Activator Code dialog you will receive an error dialog like below.



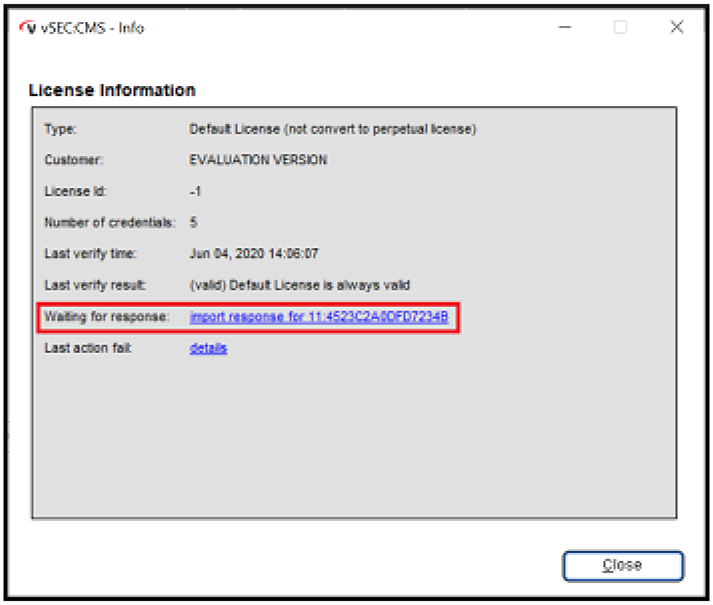
vSEC:CMS

Activate online fail: Network connection failed.

code=0x80010003

Do you want to create offline request ?

- Click **Yes** and save the license request file. Then, from a host that can connect to Versasec's licensing service, open a browser and navigate to https://versasec.com/license/validation. Upload the license request file and upon successful validation by Versasec's licensing service the browser will redirect you to a page where you can download the activation license file. Download the activation license file and copy it to your server. Log onto the console and from **Options - License click the View License button**. You should see something similar to below with a link from Waiting for response.



vSEC:CMS - Info

License Information

Type: Default License (not convert to perpetual license)

Customer: EVALUATION VERSION

License Id: -1

Number of credentials: 5

Last verify time: Jun 04, 2020 14:06:07

Last verify result: (valid) Default License is always valid

Waiting for response: import response for 11:4523C2A0DFD7234B

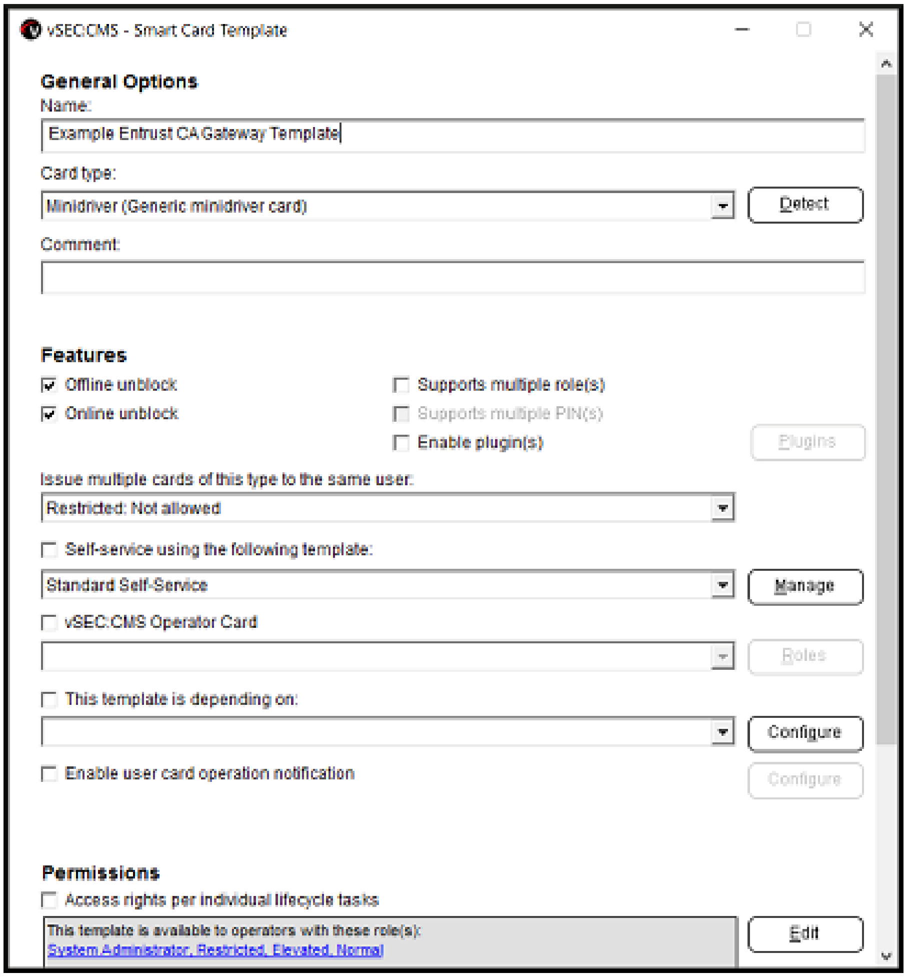
Last action fail: details

- Click the link and you will be prompted to select the activation license file. You should then see a success message indicating that the license has been activated. **Note:** If for some reason the server on which the vSEC:CMS has internet connectivity but cannot reach Versasec's issuance server you can set up a temporary firewall rule (for program) on the server and block outbound for the vSEC:CMS Service (CmsService.exe). This will allow you to create an offline license activation request in this case.

Important: Once the production license has been applied it will be necessary to issue at least one additional Operator Token (OT) that has a full administrator role in the system. See the article Configure Operator Credential for details on this.

Admin Actions:

- **Navigate to Template -** Card Templates and click **Add**. Select General[Edit]. Enter a template name and for Card type select Minidriver (Generic minidriver card). Leave all other settings as default and scroll to the bottom of the dialog and **select Ok** to save and close.



vSEC:CMS - Smart Card Template

General Options

Name:
Example Entrust CA Gateway Template

Card type:
Minidriver (Generic minidriver card)

Comment:

Features

☑ Offline unblock
☑ Online unblock
☐ Supports multiple role(s)
☐ Supports multiple PIN(s)
☐ Enable plugin(s)

Issue multiple cards of this type to the same user:
Restricted: Not allowed

☐ Self-service using the following template:
Standard Self-Service

☐ vSEC:CMS Operator Card

☐ This template is depending on:

☐ Enable user card operation notification

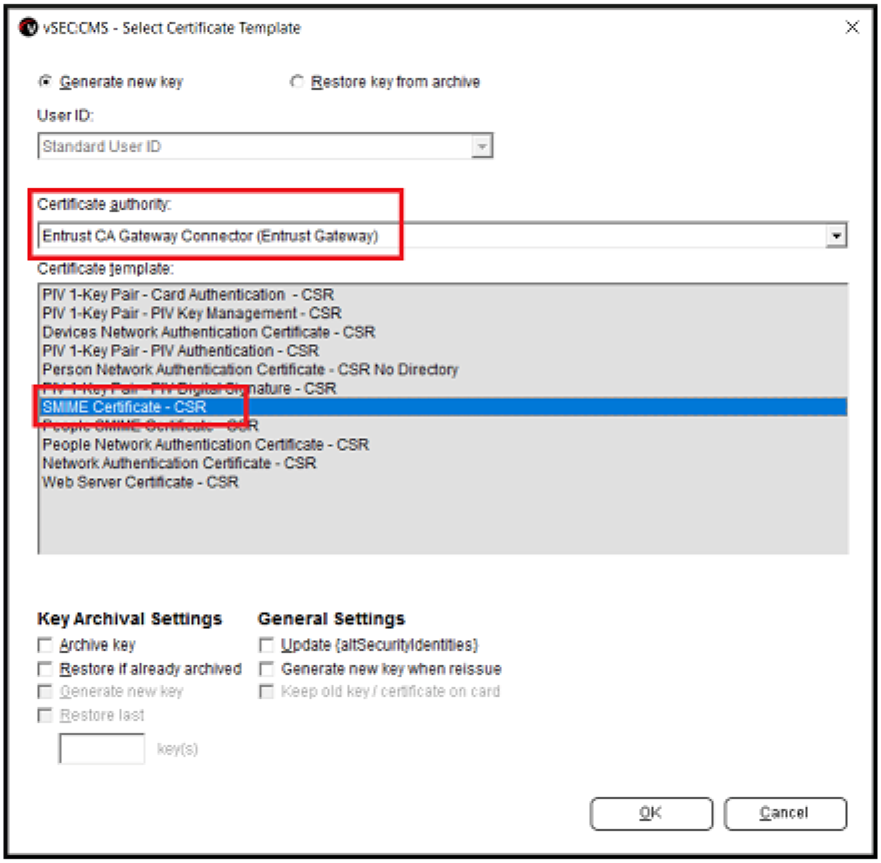
Permissions

☐ Access rights per individual lifecycle tasks

This template is available to operators with these role(s):
System Administrator, Restricted, Elevated, Normal

- **Select Issue Card [Edit].** Presuming that a connection is already in place to connect to a directory (Active Directory) in the User ID Options section select **Assign user ID** and select the **AD connection** from the drop-down list.

- In the **Enroll Certificate Options** section enable **Enrol certificate(s)** and click **Add**. Select the CA from **Certificate Authority** drop-down field and select the certificate that we will issue during the card issuance. Click **Ok** to save and close.



vSEC:CMS - Select Certificate Template

● Generate new key ○ Restore key from archive

User ID:

Standard User ID

Certificate authority:

Entrust CA Gateway Connector (Entrust Gateway)

Certificate template:

PIV 1-Key Pair - Card Authentication - CSR
PIV 1-Key Pair - PIV Key Management - CSR
Devices Network Authentication Certificate - CSR
PIV 1-Key Pair - PIV Authentication - CSR
Person Network Authentication Certificate - CSR No Directory
PIV 1-Key Pair - PIV Digital Signature - CSR
SMIME Certificate - CSR
People SMIME Certificate - CSR
People Network Authentication Certificate - CSR
Network Authentication Certificate - CSR
Web Server Certificate - CSR

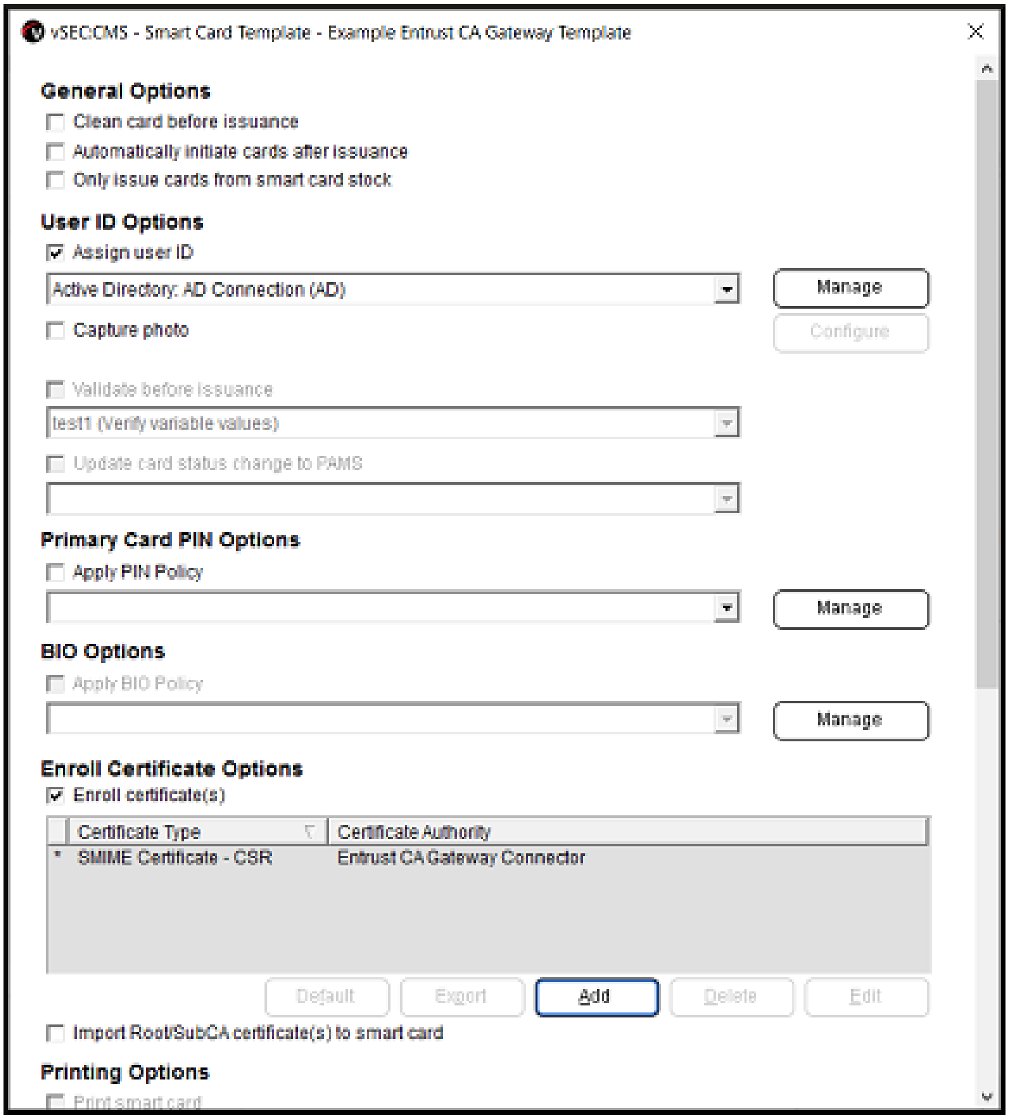
Key Archival Settings

☐ Archive key
☐ Restore if already archived
☐ Generate new key
☐ Restore last key(s)

General Settings

☐ Update (altSecurityIdentities)
☐ Generate new key when reissue
☐ Keep old key / certificate on card

- Leave all other settings as is.



vSEC:CMS - Smart Card Template - Example Entrust CA Gateway Template

General Options

□ Clean card before issuance

□ Automatically initiate cards after issuance

□ Only issue cards from smart card stock

User ID Options

☑ Assign user ID

Active Directory: AD Connection (AD)

□ Capture photo

□ Validate before issuance

test1 (Verify variable values)

□ Update card status change to PAMS

Primary Card PIN Options

□ Apply PIN Policy

BIO Options

□ Apply BIO Policy

Enroll Certificate Options

☑ Enroll certificate(s)

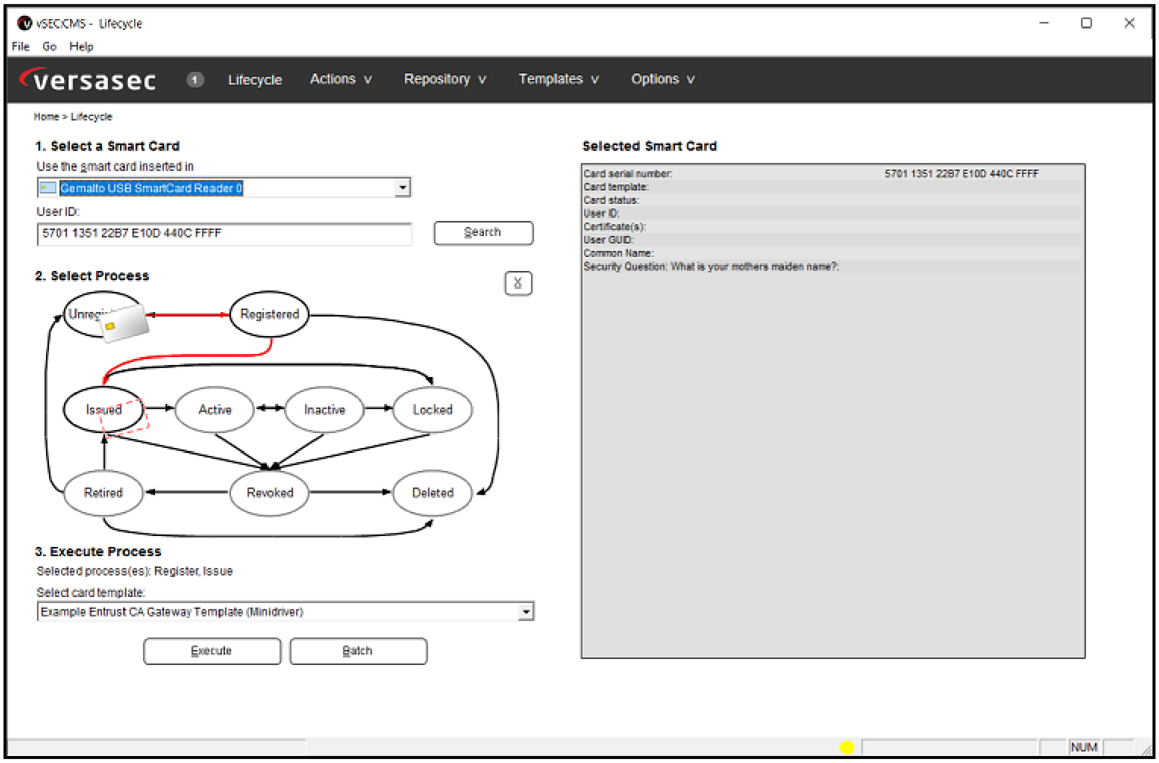
Certificate Type	Certificate Authority
SMIME Certificate - CSR	Entrust CA Gateway Connector

□ Import Root/SubCA certificate(s) to smart card

Printing Options

□ Print smart card

- Scroll down to the bottom of the dialog and click **Ok**.
- Click **Ok** to save and close the template configuration.
- Navigate to the **Lifecycle** page. Attach a blank credential and click the **Issue** oval. Select the template from the drop-down field and click **Execute.**



1. Select a Smart Card

Use the smart card inserted in: Gemalto USB SmartCard Reader 0

User ID: 5701 1351 22B7 E10D 440C FFFF

2. Select Process

3. Execute Process

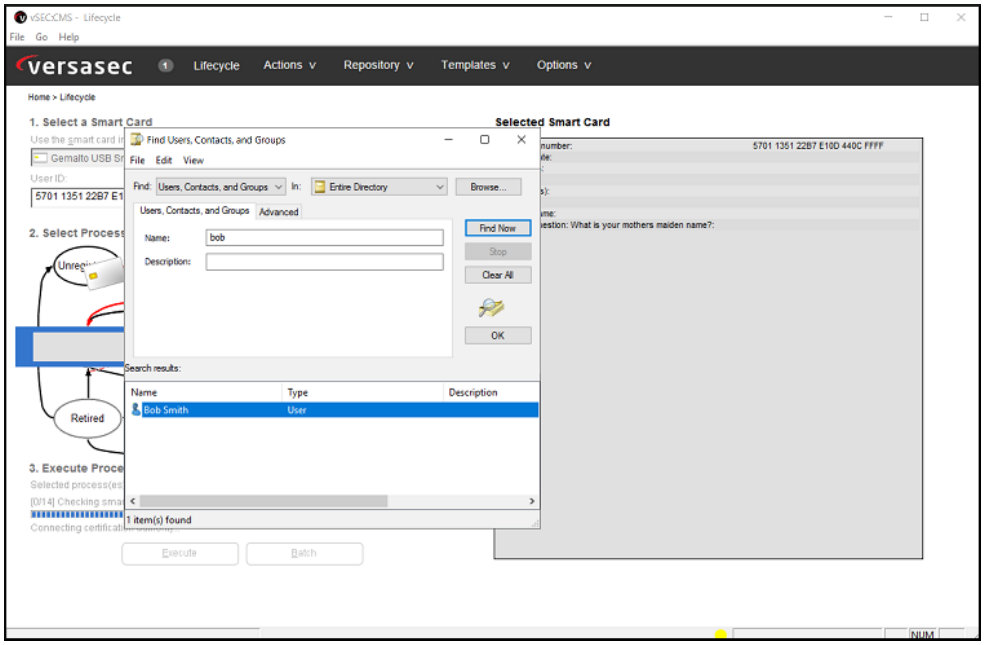
Selected process(es): Register, Issue

Select card template: Example Entrust CA Gateway Template (Minidriver)

Selected Smart Card

Card serial number:	5701 1351 22B7 E10D 440C FFFF
Card template:	
Card status:	
User ID:	
Certificate(s):	
User GUID:	
Common Name:	
Security Question: What is your mothers maiden name?:	

- This will start the issuance flow. You will be prompted to select the user from AD that the credential will be issued to. In this case we will select a user Bob Smith from our example AD. This user's CN will match the static value we entered when setting up the CA connection earlier.



Find: Users, Contacts, and Groups In: Entire Directory

Name: bob

Description:

Search results:

Name	Type	Description
Bob Smith	User	

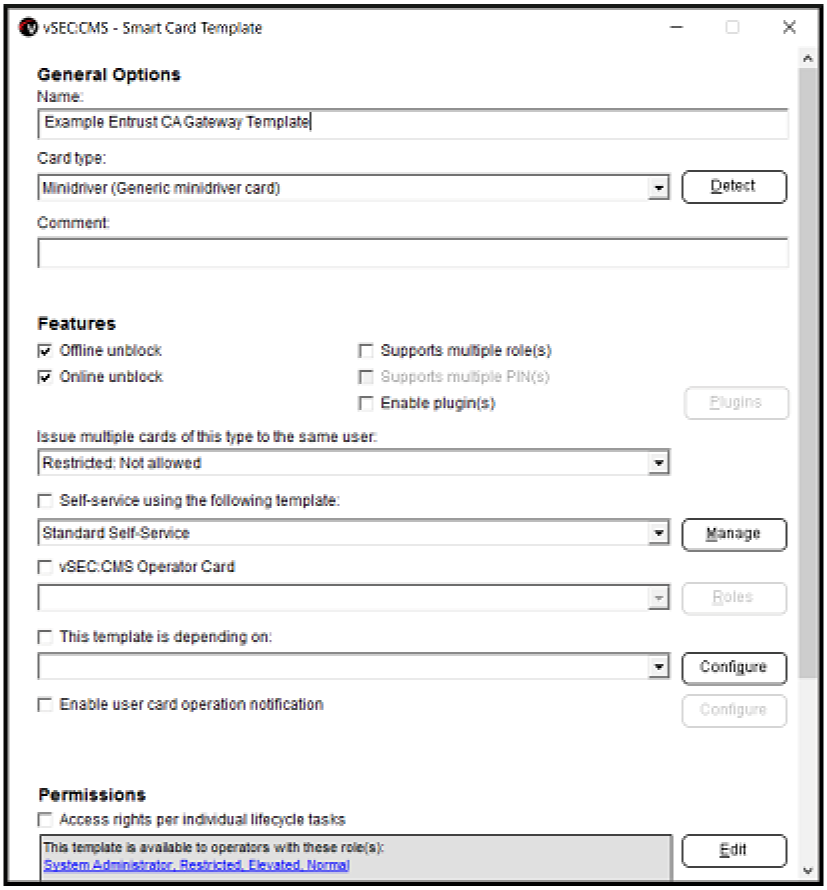
1 item(s) found

- The keys will be generated on the credential and the certificate request will be created and sent to the CA for verification and issuance. Once issued by the CA it will send back to the credential and store it there. A short summary will be provided on completing the issuance.

- Assign to user credential profile to users and user groups. The credential PIN by default will be blocked. You will need to set a PIN before you can use the certificate on the credential. Click the Active oval followed by the Execute button. You will be prompted to authenticate again and then set a PIN that meets the policy supported on the credential. Once the certificate can be accessed and used as needed.

Enrolling Users via vSEC:CMS Admin (Admin Action)

- Navigate to **Template - Card Templates** and click **Add**. Select **General [Edit]**. Enter a template name and for **Card type** select **Minidriver (Generic minidriver card)**. Leave all other settings as default and scroll to the bottom of the dialog and select **Ok** to save and close.



vSEC:CMS - Smart Card Template

General Options

Name: Example Entrust CA Gateway Template

Card type: Minidriver (Generic minidriver card)

Comment:

Features

☑ Offline unblock

☑ Online unblock

☐ Supports multiple role(s)

☐ Supports multiple PIN(s)

☐ Enable plugin(s)

Issue multiple cards of this type to the same user: Restricted: Not allowed

☐ Self-service using the following template: Standard Self-Service

☐ vSEC:CMS Operator Card

☐ This template is depending on:

☐ Enable user card operation notification

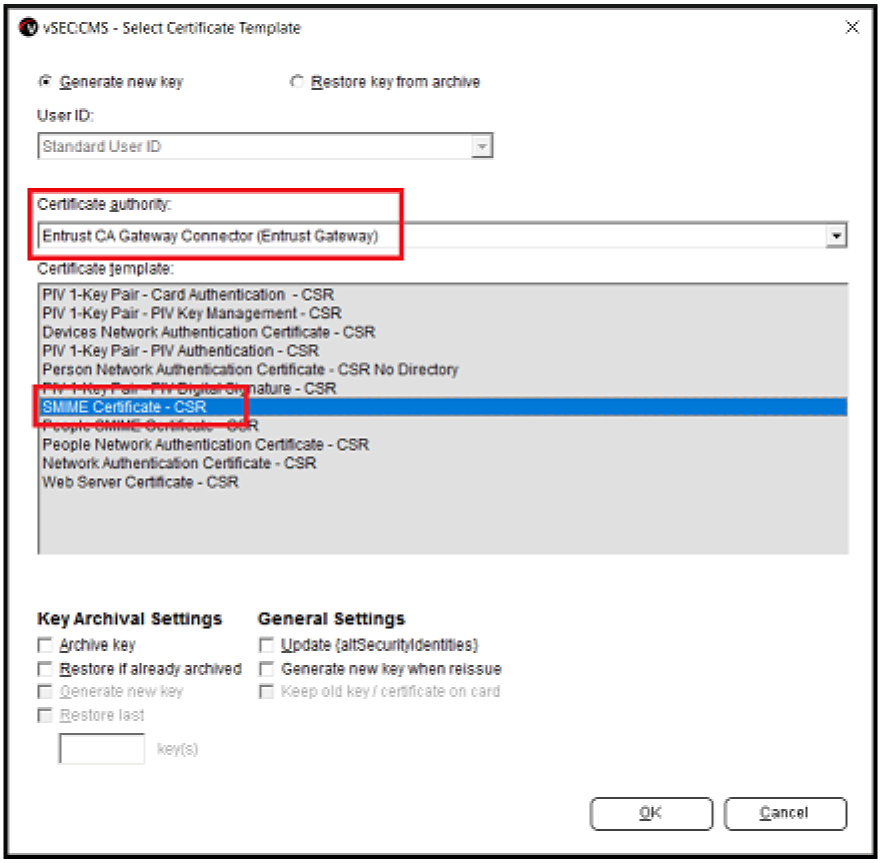
Permissions

☐ Access rights per individual lifecycle tasks

This template is available to operators with these role(s): System Administrator, Restricted, Elevated, Normal

- Select **Issue Card [Edit]**. Presuming that a connection is already in place to connect to a directory (Active Directory) in the **User ID Options** section select **Assign user ID** and select the AD connection from the drop-down list.

- In the **Enroll Certificate Options** section enable **Enrol certificate(s)** and click **Add**. Select the CA from **Certificate Authority** drop-down field and select the certificate that we will issue during the card issuance. Click **Ok** to save and close.



vSEC:CMS - Select Certificate Template

● Generate new key ○ Restore key from archive

User ID: Standard User ID

Certificate authority: Entrust CA Gateway Connector (Entrust Gateway)

Certificate template:

PIV 1-Key Pair - Card Authentication - CSR
PIV 1-Key Pair - PIV Key Management - CSR
Devices Network Authentication Certificate - CSR
PIV 1-Key Pair - PIV Authentication - CSR
Person Network Authentication Certificate - CSR No Directory
PIV 1-Key Pair - PIV Digital Signature - CSR
SMIME Certificate - CSR
People SMIME Certificate - CSR
People Network Authentication Certificate - CSR
Network Authentication Certificate - CSR
Web Server Certificate - CSR

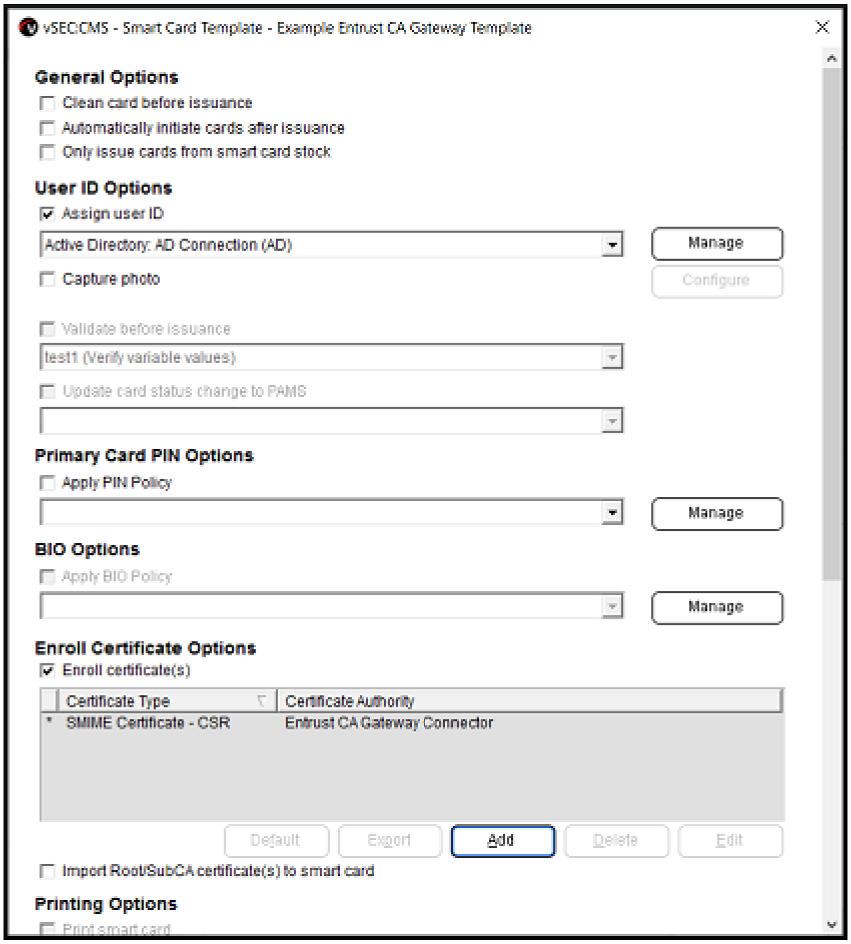
Key Archival Settings

□ Archive key
□ Restore if already archived
□ Generate new key
□ Restore last key(s)

General Settings

□ Update (altSecurityIdentities)
□ Generate new key when reissue
□ Keep old key / certificate on card

- Leave all other settings as is.



vSEC:CMS - Smart Card Template - Example Entrust CA Gateway Template

General Options

☐ Clean card before issuance
☐ Automatically initiate cards after issuance
☐ Only issue cards from smart card stock

User ID Options

☑ Assign user ID
Active Directory: AD Connection (AD)
☐ Capture photo
☐ Validate before issuance
test1 (Verify variable values)
☐ Update card status change to PAMS

Primary Card PIN Options

☐ Apply PIN Policy

BIO Options

☐ Apply BIO Policy

Enroll Certificate Options

☑ Enroll certificate(s)

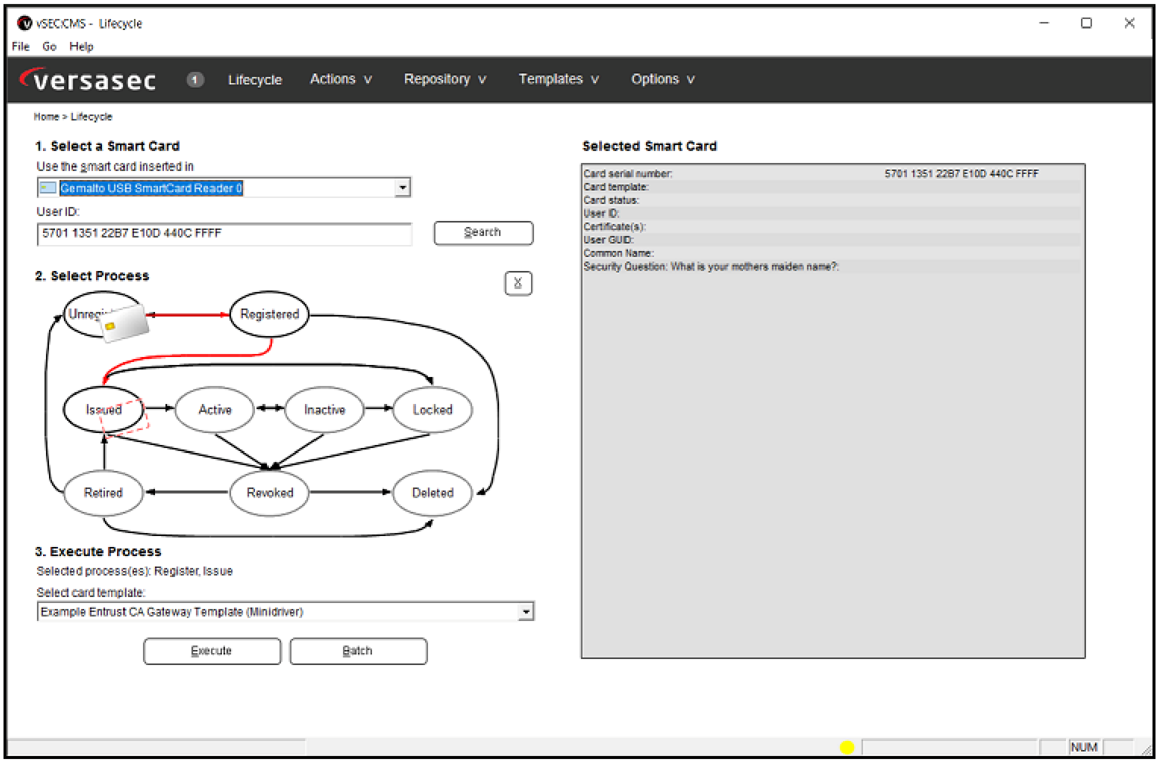
Certificate Type	Certificate Authority
SMIME Certificate - CSR	Entrust CA Gateway Connector

☐ Import Root/SubCA certificate(s) to smart card

Printing Options

☐ Print smart card

- Scroll down to the bottom of the dialog and click **Ok**.
- Click **Ok** to save and close the template configuration.
- Navigate to the **Lifecycle** page. Attach a blank credential and click the **Issue** oval. Select the template from the drop-down field and click **Execute**.



vSEC:CMS - Lifecycle

Home > Lifecycle

1. Select a Smart Card

Use the smart card inserted in: Gemalto USB SmartCard Reader 0

User ID: 5701 1351 22B7 E10D 440C FFFF

2. Select Process

3. Execute Process

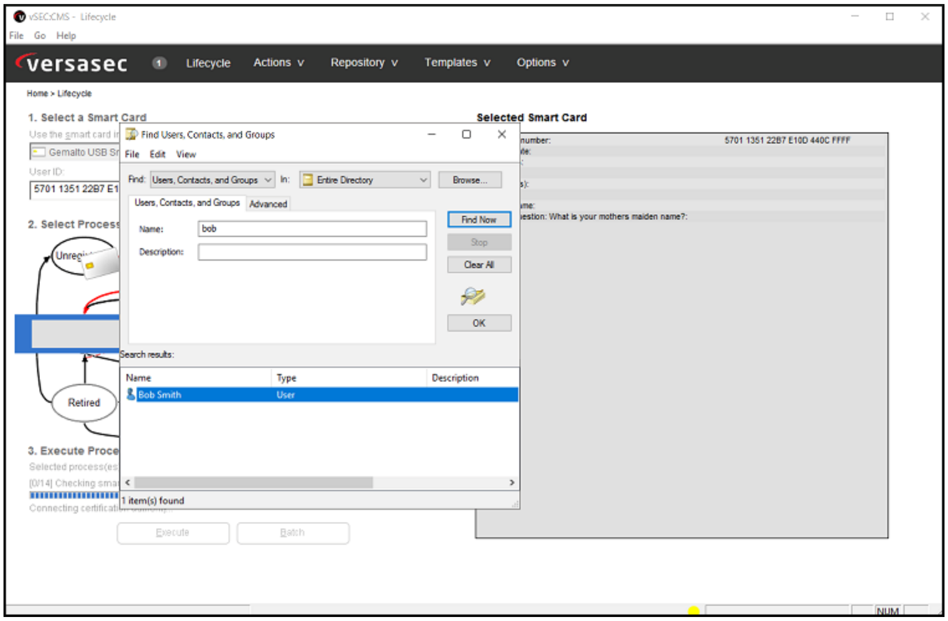
Selected process(es): Register, Issue

Select card template: Example Entrust CA Gateway Template (Minidriver)

Selected Smart Card

Card serial number:	5701 1351 22B7 E10D 440C FFFF
Card template:	
Card status:	
User ID:	
Certificate(s):	
User GUID:	
Common Name:	
Security Question: What is your mothers maiden name?:	

- This will start the issuance flow. You will be prompted to select the user from AD that the credential will be issued to. In this case we will select a user Bob Smith from our example AD. This user's CN will match the static value we entered when setting up the CA connection earlier.



Find Users, Contacts, and Groups

Find: Users, Contacts, and Groups In: Entire Directory

Name: bob

Description:

Search results:

Name	Type	Description
Bob Smith	User	

1 item(s) found

[0/14] Checking smart card...

Connecting certification authority...

- The keys will be generated on the credential and the certificate request will be created and sent to the CA for verification and issuance. Once issued by the CA it will send back to the credential and store it there. A short summary will be provided on completing the issuance.

- Assign to user credential profile to users and user groups. The credential PIN by default will be blocked. You will need to set a PIN before you can use the certificate on the credential. Click the Active oval followed by the Execute button. You will be prompted to authenticate again and then set a PIN that meets the policy supported on the credential. Once the certificate can be accessed and used as needed.

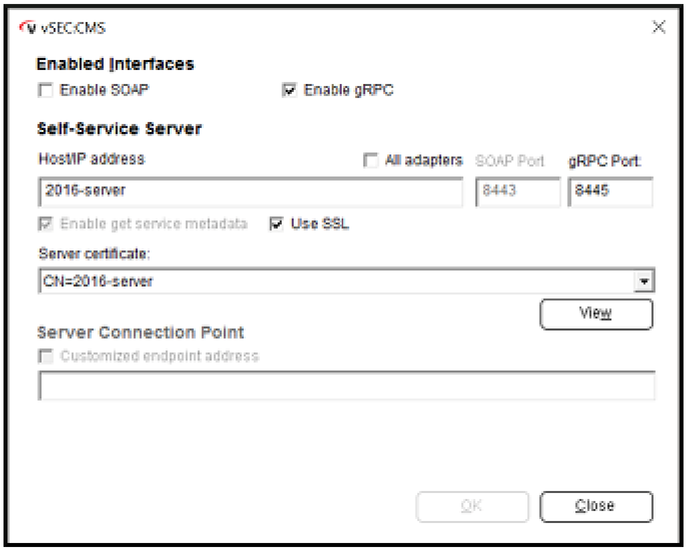
Enrolling Users via vSEC:CMS User Application (USS)

End User actions:

- If you don't have a connection for self-service already set up then from Options - Connections click the Add button and select User Self-Service and click Ok. Enable the Enable gRPC checkbox as we will use gRPC for this case.

IMPORTANT: Please ensure that you have read through the article vSEC:CMS Client-Server Communication which gives more details on vSEC:CMS client-server architecture.

- Depending on your environment settings enter a hostname and port to listen on. You can also setup support for SSL if you wish to use HTTPS for secure communication between the client and server. If you use SSL it is important that the HostIP address field is entered with the name of the server as it appears in the SSL certificate. The SSL certificate should be a machine certificate available on the vSEC:CMS server.



vSEC:CMS

Enabled Interfaces

☐ Enable SOAP ☑ Enable gRPC

Self-Service Server

Host/IP address: 2016-server

☐ All adapters

SOAP Port: 8443

gRPC Port: 8445

☑ Enable get service metadata

☑ Use SSL

Server certificate: CN=2016-server

Server Connection Point

☐ Customized endpoint address

- Make sure that the vSEC:CMS - User Self-Service service is running after you configure this in Windows services.
  Important: Ensure that a credential configuration exists for the credential that you are going to use here. See the article Add Credential Configuration before starting below.

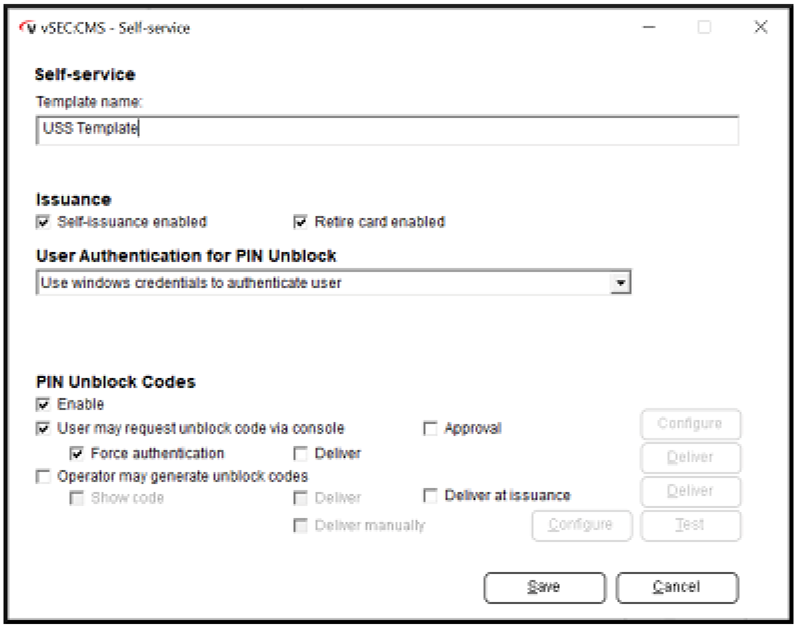
- From **Templates -** Card Templates click the **Add button.**

- Click the **Edit link** beside **General. Enter** a template name. Presuming that you are using one of the minidriver credentials that is supported by vSEC:CMS select Minidriver (Generic minidriver card) for Card type.

- **Click** the **Manage button** beside Self-service using the following template. **Click the Add button**. **Enter a template name** and **enable Self-issuance enabled and Retire card enabled checkboxes.**

- From the User Authentication for PIN Unblock drop-down list **select Use windows credentials** to authenticate user.

- Leave **all other settings as** is and **click** the Save button to save and close.



vSEC:CMS - Self-service

Self-service

Template name:

USS Template

Issuance

☑ Self-issuance enabled ☑ Retire card enabled

User Authentication for PIN Unblock

Use windows credentials to authenticate user

PIN Unblock Codes

☑ Enable

☑ User may request unblock code via console □ Approval

☑ Force authentication □ Deliver

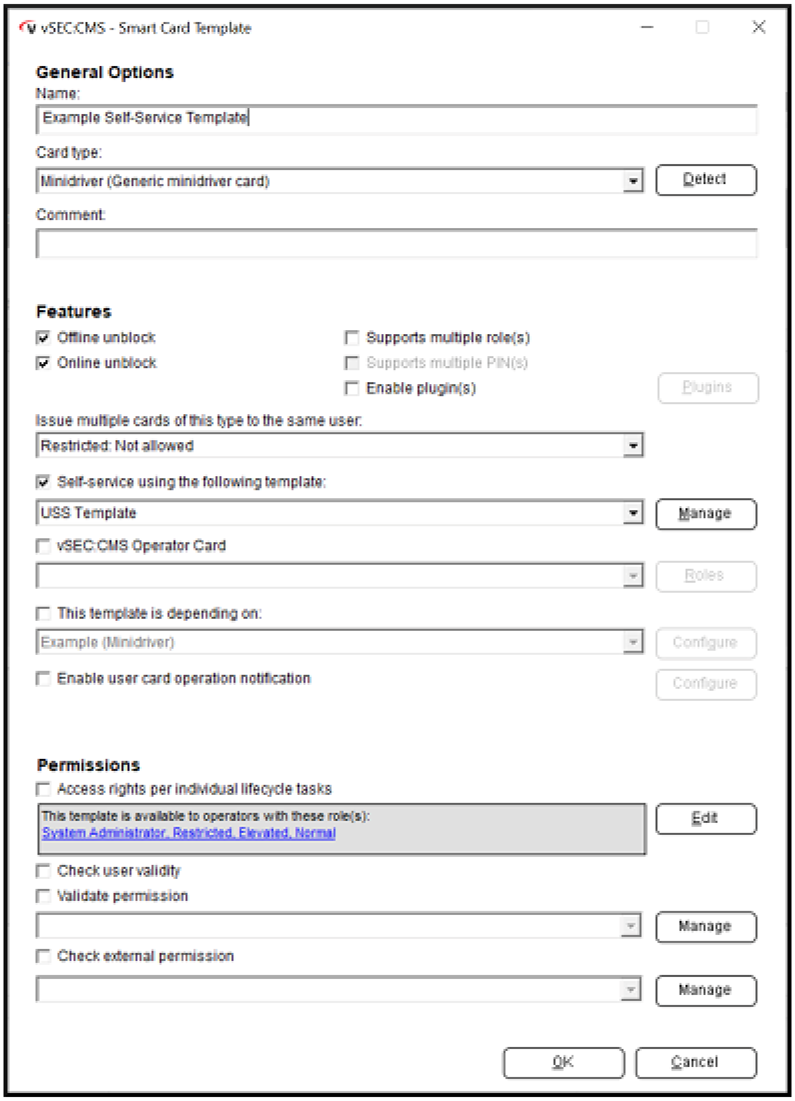
□ Operator may generate unblock codes □ Deliver at issuance

□ Show code □ Deliver

□ Deliver manually

- **Click Close** and from the main **General dialog** enable Self-service using the following template and from the drop-down list **select the template just created.**

- Leave all other settings as is and click **Ok** to save and close the dialog.



General Options

Name: Example Self-Service Template

Card type: Minidriver (Generic minidriver card)

Comment:

Features

☑ Offline unblock
☑ Online unblock
☐ Supports multiple role(s)
☐ Supports multiple PIN(s)
☐ Enable plugin(s)

Issue multiple cards of this type to the same user: Restricted: Not allowed

☑ Self-service using the following template: USS Template

☐ vSEC:CMS Operator Card

☐ This template is depending on: Example (Minidriver)

☐ Enable user card operation notification

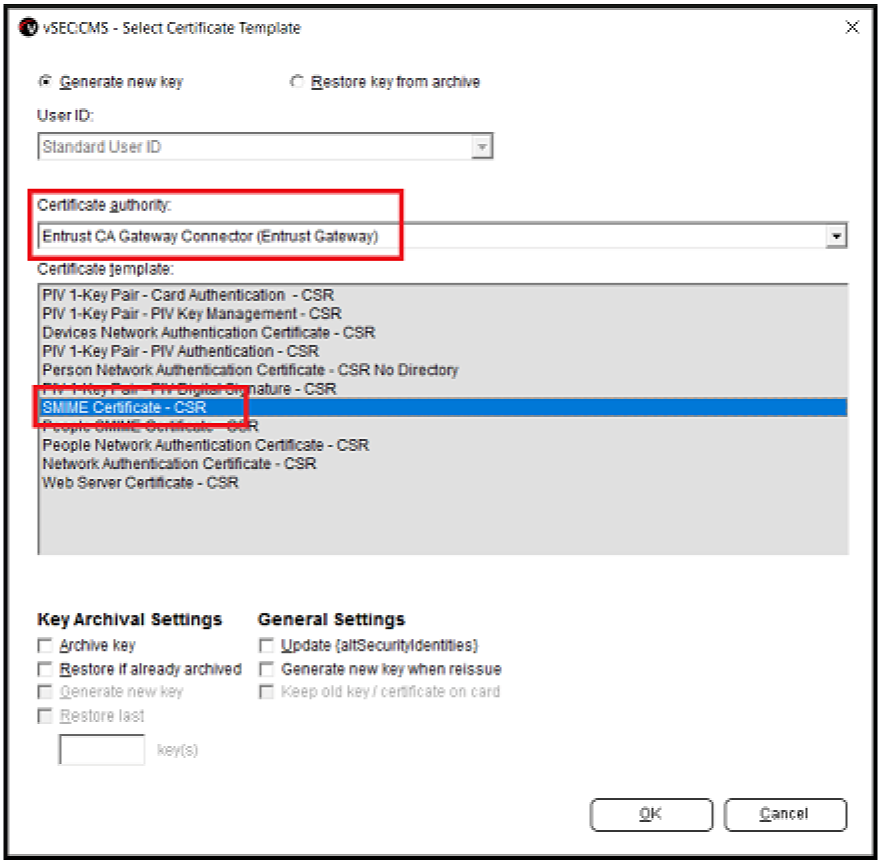
Permissions

☐ Access rights per individual lifecycle tasks

This template is available to operators with these role(s):
System Administrator, Restricted, Elevated, Normal

☐ Check user validity
☐ Validate permission
☐ Check external permission

- In the Enroll Certificate Options section **enable Enroll certificate(s) and click Add.**
- **Select the CA from Certificate Authority** drop-down field and **select** the certificate that we will issue during the card issuance.
- **Click Ok** to save and close.



vSEC:CMS - Select Certificate Template

● Generate new key ○ Restore key from archive

User ID:

Standard User ID

Certificate authority:

Entrust CA Gateway Connector (Entrust Gateway)

Certificate template:

PIV 1-Key Pair - Card Authentication - CSR
PIV 1-Key Pair - PIV Key Management - CSR
Devices Network Authentication Certificate - CSR
PIV 1-Key Pair - PIV Authentication - CSR
Person Network Authentication Certificate - CSR No Directory
PIV 1-Key Pair - PIV Digital Signature - CSR
SMIME Certificate - CSR
People SMIME Certificate - CSR
People Network Authentication Certificate - CSR
Network Authentication Certificate - CSR
Web Server Certificate - CSR

Key Archival Settings

□ Archive key
□ Restore if already archived
□ Generate new key
□ Restore last key(s)

General Settings

□ Update (altSecurityIdentities)
□ Generate new key when reissue
□ Keep old key / certificate on card

- Leave all other settings as is.
- Scroll down to the bottom of the dialog and **click Ok.**
- **Click Ok** to save and close the template configuration.

On a client machine **it will be necessary to install the USS application.** Use the vSEC:CMS Client MSI to install this component. It is recommended to install the USS silently as it is possible to pass in the URL link to the backend vSEC:CMS server that the USS needs to communicate with. This will remove the requirement to manually configure the USS to communicate with the backend in this case.

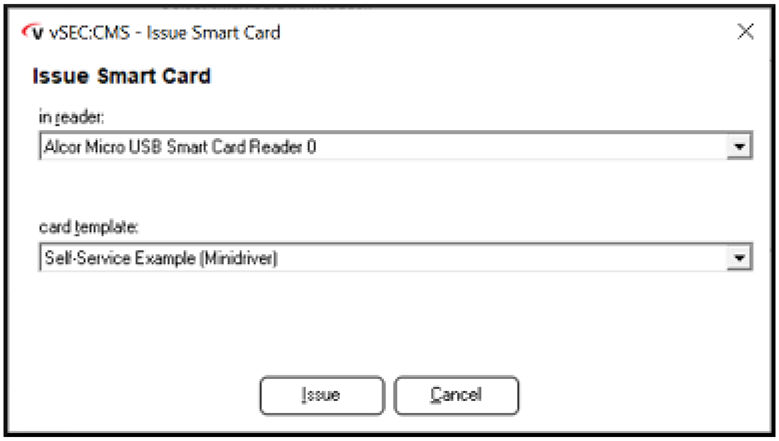
- Open a command Window as administrator and change to the location where the MSI installer is located. Run the command similar to below
  msiexec /i "vSEC_CMS Client 64bit.msi" /quiet ADDLOCAL=USS USSGRPC="https://2016-server:8445" USSPCL=4

Where USSGRPC points to the backend gPRC service where vSEC:CMS is installed and USSPCL=4 configures the USS client to use gRPC.

Important: The client host will automatically reboot when running the above command so make sure you have saved any material you may be working on when performing this task.

Important: Depending on the credential that you are testing with it will be necessary to have the appropriate credential drivers installed on your host. Please check with the credential provider that you have the correct credential drivers installed.

- **Start the My Smartcard** from the shortcut icon on the client desktop.
- **Go to the My Profile page**. With the credential attached that is to be issued click the Issue button.



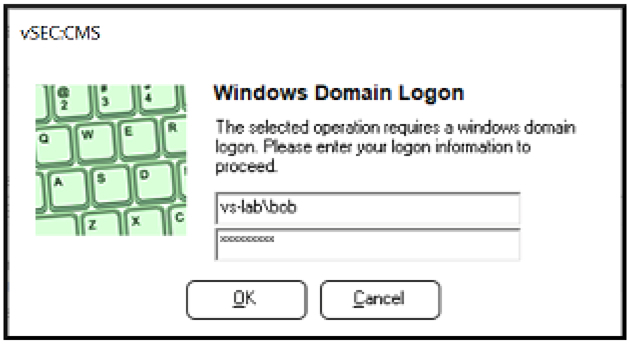
vSEC:CMS - Issue Smart Card

Issue Smart Card

in reader: Alcor Micro USB Smart Card Reader 0

card template: Self-Service Example (Minidriver)

- Enter the domain credentials of the user to authenticate.



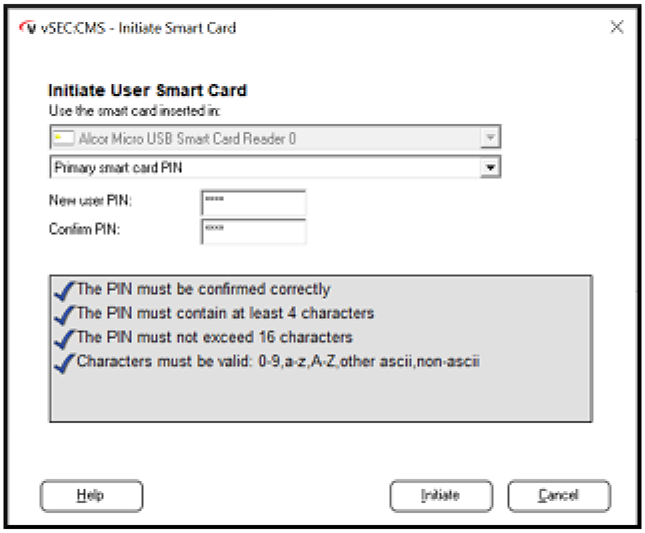
vSEC:CMS

Windows Domain Logon

The selected operation requires a windows domain logon. Please enter your logon information to proceed.

vs-lab\bob

xxxxxxxxxx



vSEC:CMS - Initiate Smart Card

Initiate User Smart Card

Use the smart card inserted in:

Alcor Micro USB Smart Card Reader 0

Primary smart card PIN

New user PIN: ****

Confirm PIN: ****

✓ The PIN must be confirmed correctly
✓ The PIN must contain at least 4 characters
✓ The PIN must not exceed 16 characters
✓ Characters must be valid: 0-9,a-z,A-Z,other ascii,non-ascii

- Once you complete this the certificate credential can be used for whatever use cases are required.

Updating and Renewing Users

Renew Certificate withing vSEC:CMS https://versasec.zendesk.com/hc/en-us/articles/360015002600-Renew-Certificates

Reporting Lost or Compromised Identities

Refer backlife processes, delete option https://versasec.zendesk.com/hc/en-us/articles/360014299039-Life-Cycle-Processes

Encryption Key History Escrow and Recovery

Zendesk article https://versasec.zendesk.com/hc/en-us/articles/360014298939-Configure-Key-Archival-and-Key-Recovery

External Documentation

1. Versasec Support Portal https://versasec.zendesk.com/hc/en-us