DIGICERT

Integration Guide

Applicable Devices:

KMES Series 3

TABLE OF CONTENTS

[1] OVERVIEW OF THE KMES SERIES 3 / DIGICERT INTEGRATION

[1.1] ABOUT DIGICERT

DigiCert is one of the world's leading providers of scalable TLS/SSL, IoT and PKI solutions for identity and encryption. Many of the most innovative companies, including 89% of the Fortune 500 and 97 of the 100 top global banks, choose DigiCert for its expertise in identity and encryption for web servers and Internet of Things devices. DigiCert supports TLS and other digital certificates for PKI deployments at any scale through its certificate lifecycle management solution, CertCentral®.

[1.2] PURPOSE OF THE INTEGRATION

This integration gives users the ability to orchestrate the issuing of certificates, signed by the DigiCert CA, using the KMES Series 3. Another way to put that is it incorporates DigiCert signing of keys into the Futurex Registration Authority process.

What is a Registration Authority (RA)?

Registration Authorities (RAs) approve and deny requests for certificates, also known as certificate signing requests (CSRs). The RA presides over and assists the Certificate Authorities (CAs) by informing them of which certificates can be issued (**NOTE:** DigiCert acts as an external CA for this use-case). Upon approving a CSR, the RA has validated the identity and registration information of the user, and permitted the CA to issue a certificate.

[1.3] KEY BENEFITS OF THE INTEGRATION

The KMES Series 3 / DigiCert integration gives you the ability to:

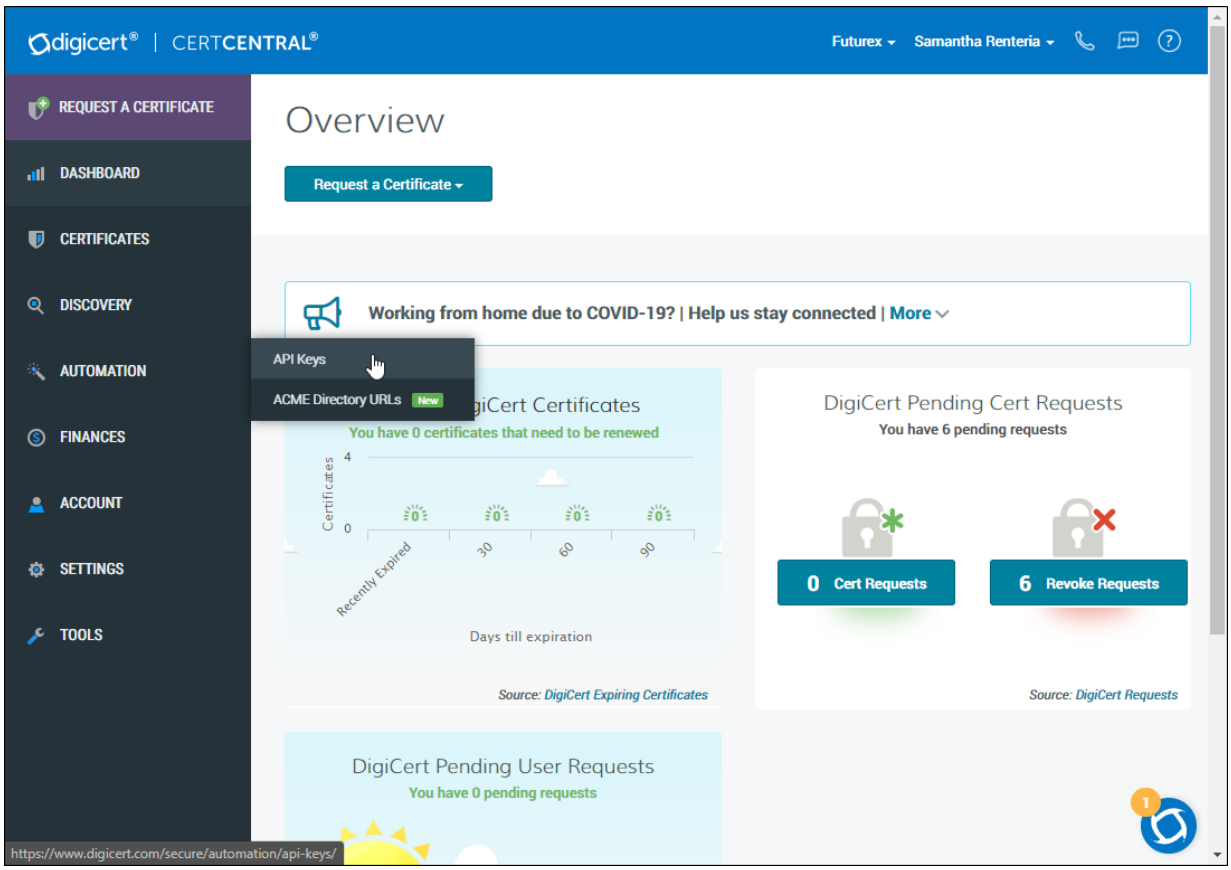
- Automatically download successfully signed requests submitted by the RA
- Utilize Futurex approval requirements
- Revoke signed requests from the RA
- Resign requests from the RA
- Cancel pending orders
- Utilize rate limiting mechanisms

[2] CONFIGURATION ON DIGICERT

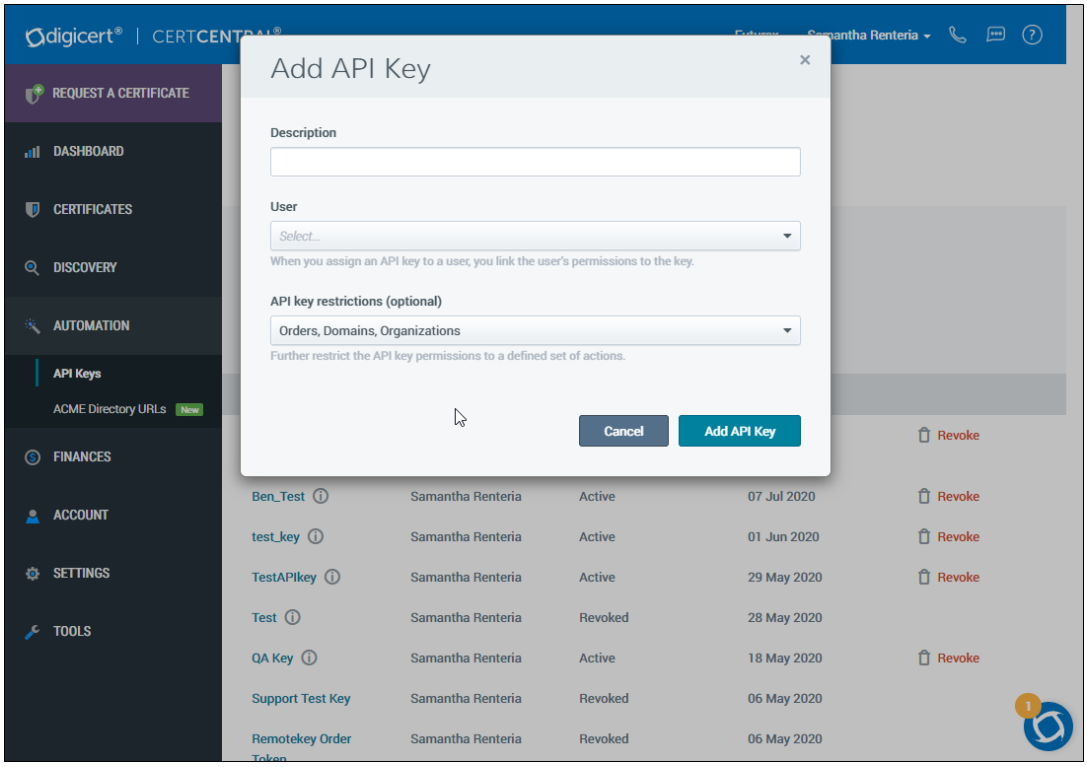
For DigiCert to authenticate the KMES Series 3 device that will be sending CSRs to the DigiCert CA, it is necessary to first generate an API Key in the DigiCert dashboard (CertCentral®), which will be imported into the KMES Series 3 in the next section.

[2.1] GENERATE A NEW API KEY

While logged in to the DigiCert dashboard (CertCentral®) hover over *Automation* on the left-hand menu, then click *API Keys*.

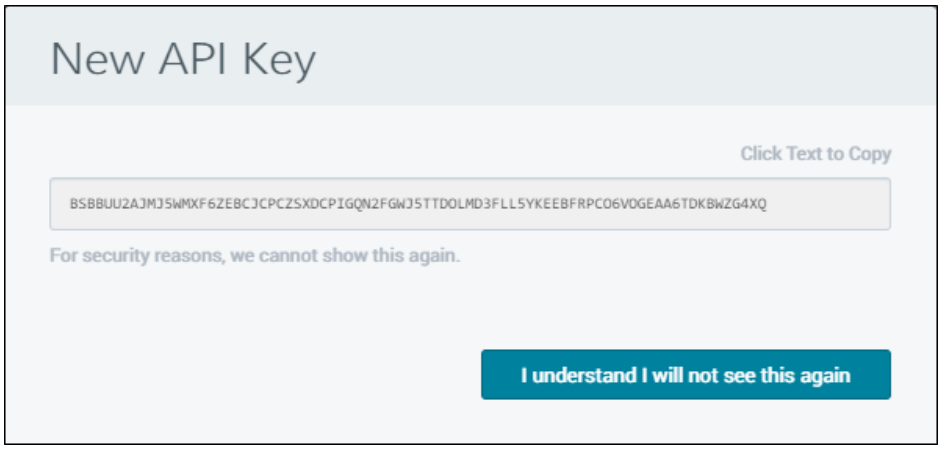


Click the *Add API Key* button and fill in the required fields.



NOTE: When adding an API Key in the DigiCert dashboard it must have the "Orders, Domains, Organizations" permissions.

Once you click *Add API Key* it will create and show you the clear API Key/Token that was generated. Click the text to copy the API Key to your clipboard, then acknowledge that the DigiCert dashboard will not show you the API Key again.



[2.2] CREATE A NEW FILE WITH THE .CSV EXTENSION THAT CONTAINS YOUR API KEY/TOKEN

In a text editor, create a new file and type "api token" in the first line of the file, then hit *Enter* to go to the next line, and paste in the API Key. It should look similar to this:

```
api token
BTIMAQBS2XZAVTIF7BKJDJ6DON5AHWFU4DV3WJWWJCWSREE5UAUFY5QUZ4SIR7MDHTJBCVX5ANRTPENUO
```

Save the file with an extension of .csv. This is necessary in order to import it into the KMES Series 3.

[3] CONFIGURATION ON THE KMES SERIES 3

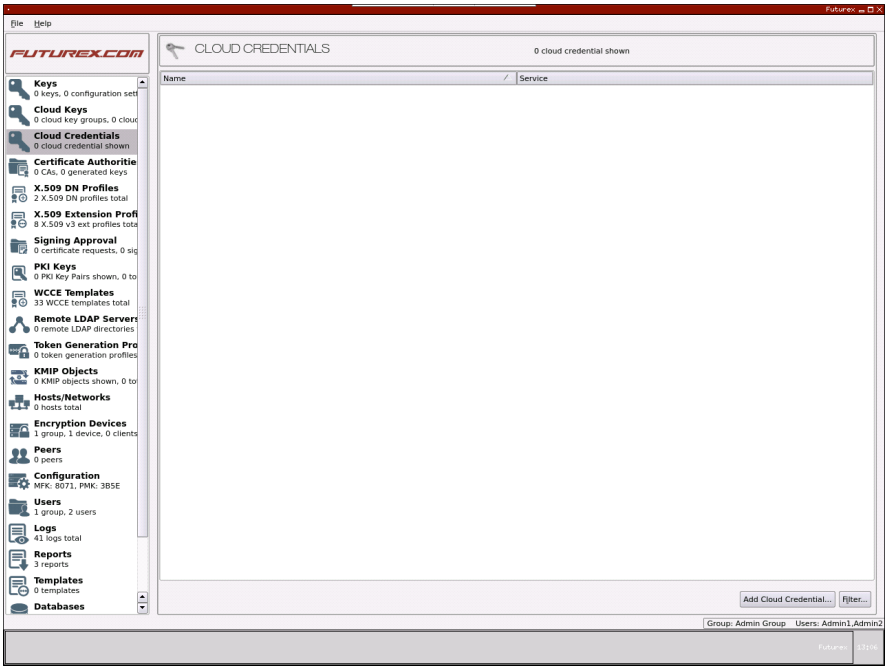
In this section, we will create a CA group container on the KMES Series 3 that will hold a representation of the issuing CA housed at DigiCert. This is done by performing the following actions:

- Creating a CA group container and defining it as "External DigiCert X.509"
- Specifying which DigiCert signing/issuing CA that you want to use to issue certificates
- Defining an Issuance Policy for the CA group container

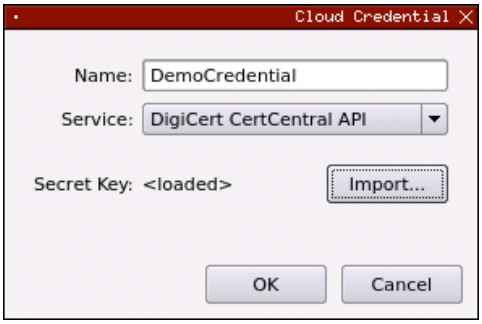
[3.1] SETTING CLOUD CREDENTIALS

Cloud Credentials are used to allow the KMES Series 3 device to interface with 3rd party services, such as DigiCert. The *Cloud Credentials* menu is where the API Key generated in section 3.1 will be imported. The full list of steps for importing the API Key are provided below:

1. Log into the key management device and select *Cloud Credentials* from the menu on the left.



2. At the bottom right of the window, click the *Add Cloud Credential* button. This will open a *Cloud Credential* window.



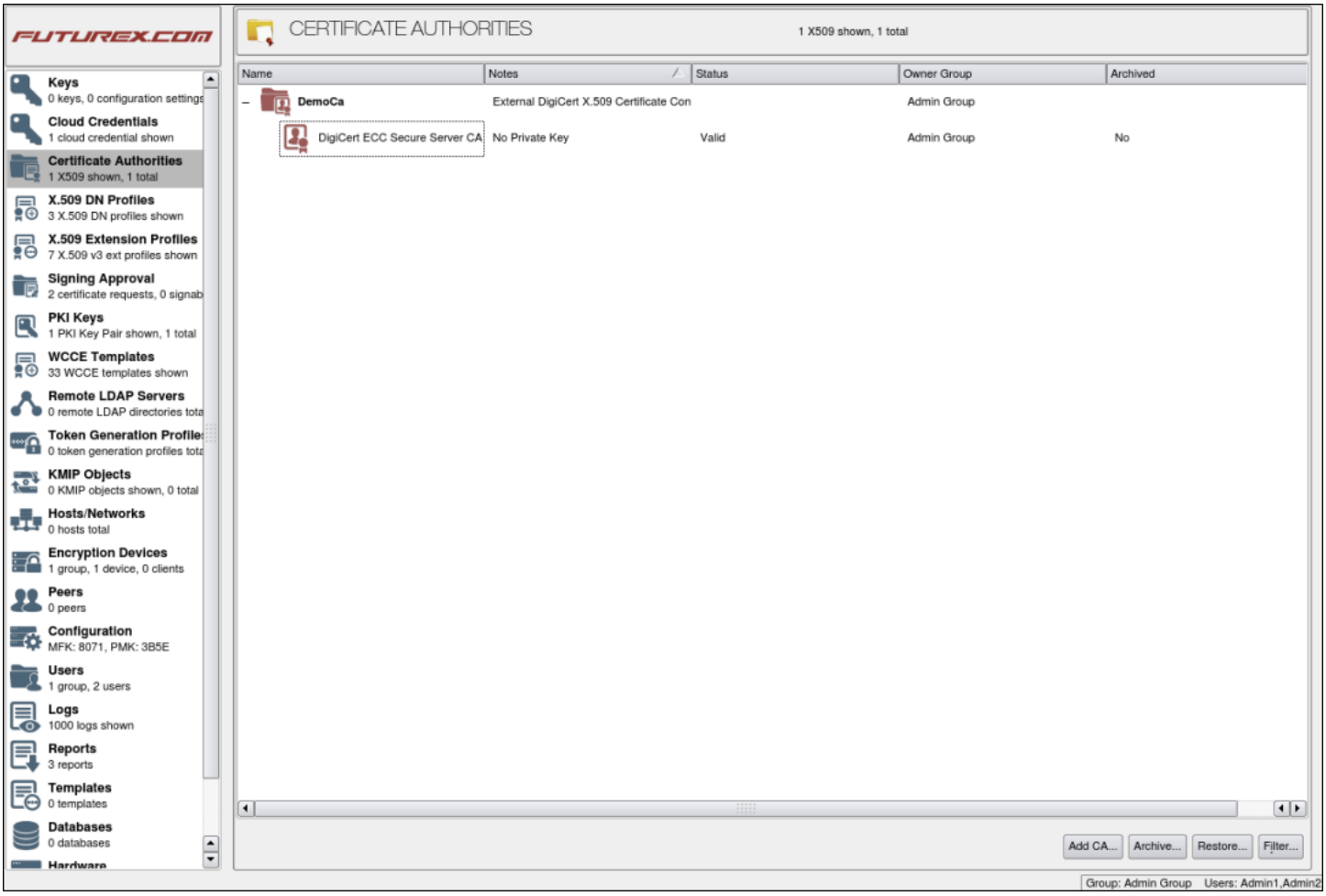
3. Fill in the following information:
    - **Name**: This is what will be used to identify the credentials on the KMES Series 3. DigiCert does not use this; this is used to identify the cloud credential on the KMES Series 3.
    - **Service**: Select *DigiCert CertCentral API*.
    - **Secret Key**: Click the *Import* button, then select the CSV file that was created in section 3.2.
4. Click **OK** to save the cloud credential.

If necessary, you can select a credential and click the Edit button, or right click on it and select *Edit*, thus allowing you to change its settings as required. You can also delete a credential via right clicking and selecting *Delete*, or by using the *Delete* button.

In addition, you can view and change the credential's permissions on the device by right clicking it and selecting *Permissions*.

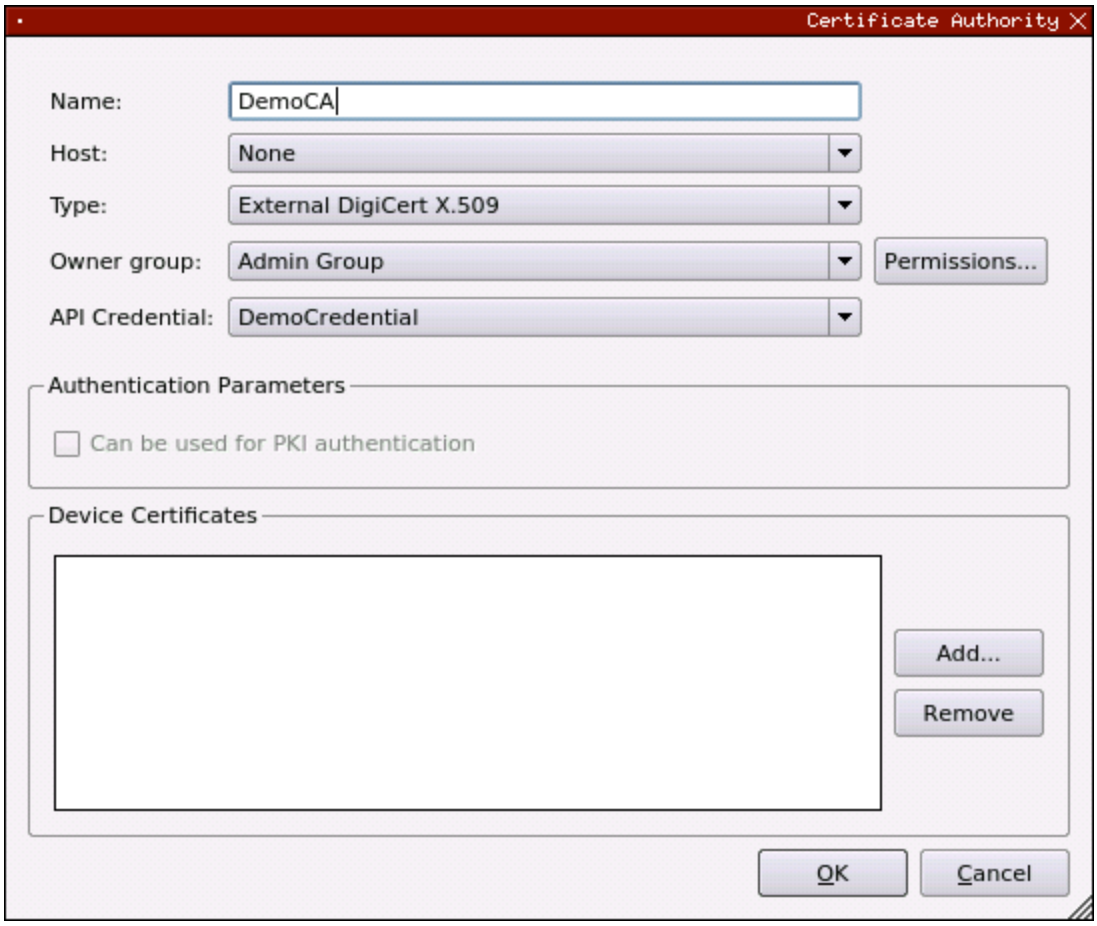
[3.2] MANAGING CERTIFICATE AUTHORITIES

Certificate Authorities are managed through the *Certificate Authorities* screen.



Adding a CA Group Container

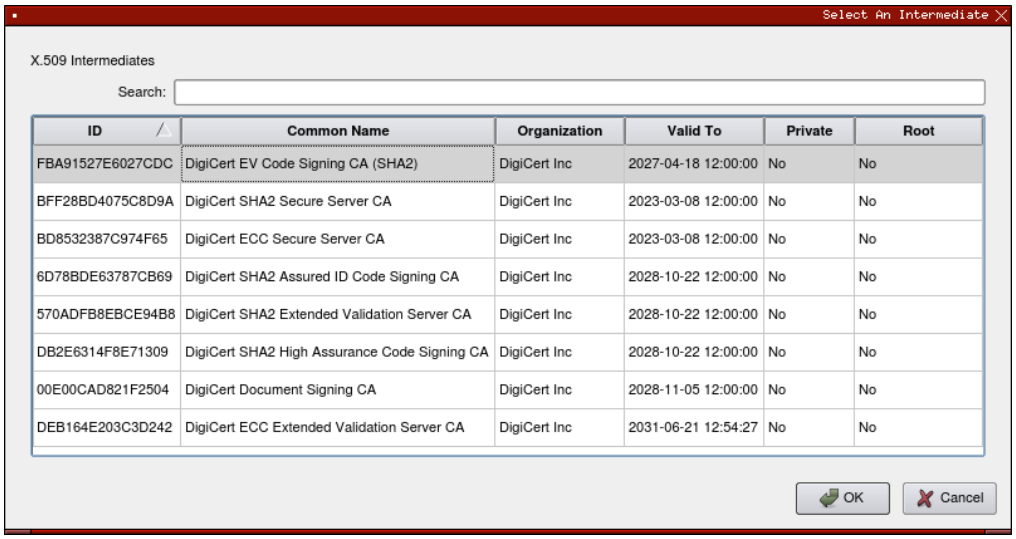
1. Navigate to the *Certificate Authorities* tab by selecting the menu item on the left.
2. Right-click on the window and select *Add CA...* to create a new CA group container.
    - The CA group container holds all certificates in the certificate tree.



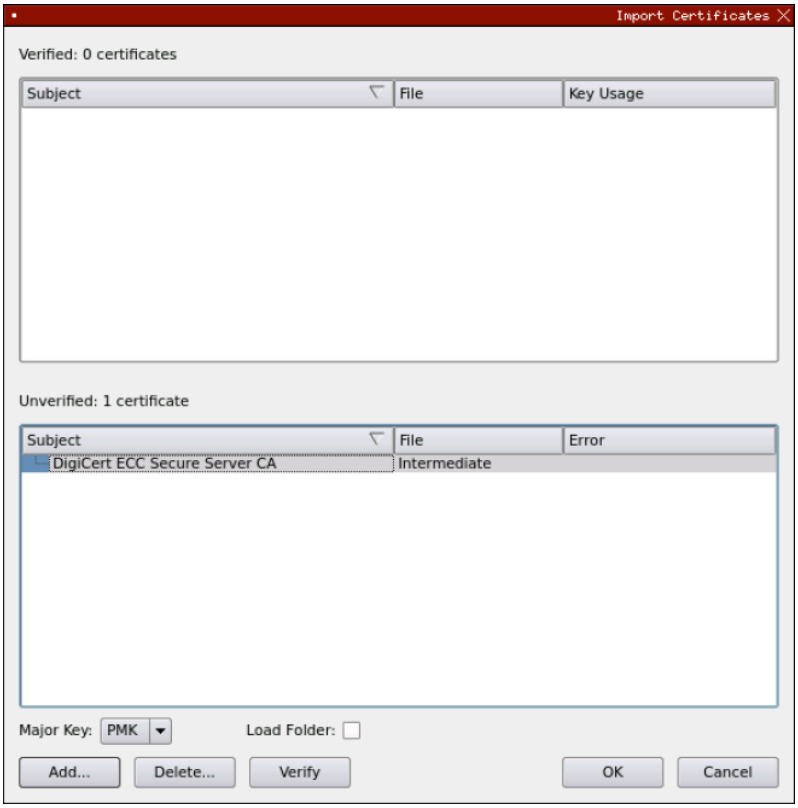
3. Specify the following information in the Certificate Authority window:
    - Name: a short text description of the CA group object, used for referencing on the device.
    - Host: Specification of a key encryption key to securely transport sensitive data, such as RSA private keys, to an external system; this is optional.
    - Type: This specifies the CA type; in this case, you must select External DigiCert X.509.
    - Owner Group: (optional) designation of the KMES Series 3 user group that will have full ownership permissions to this CA container object.
    - API Credential: Choose one of the DigiCert cloud credentials created. This will allow the CA to connect to DigiCert.
4. Click OK to create the CA group container.

Adding External Certificates

1. Right click on a CA group container, and select *Import -> External Certificate(s)*.



2. The *Select An Intermediate* window will populate with a list of intermediate certificates pulled from DigiCert. Highlight the intermediate you wish to use, then click OK to add it.
    - If necessary, it is possible to quickly locate a intermediate certificate via the Search bar at the top of the window.

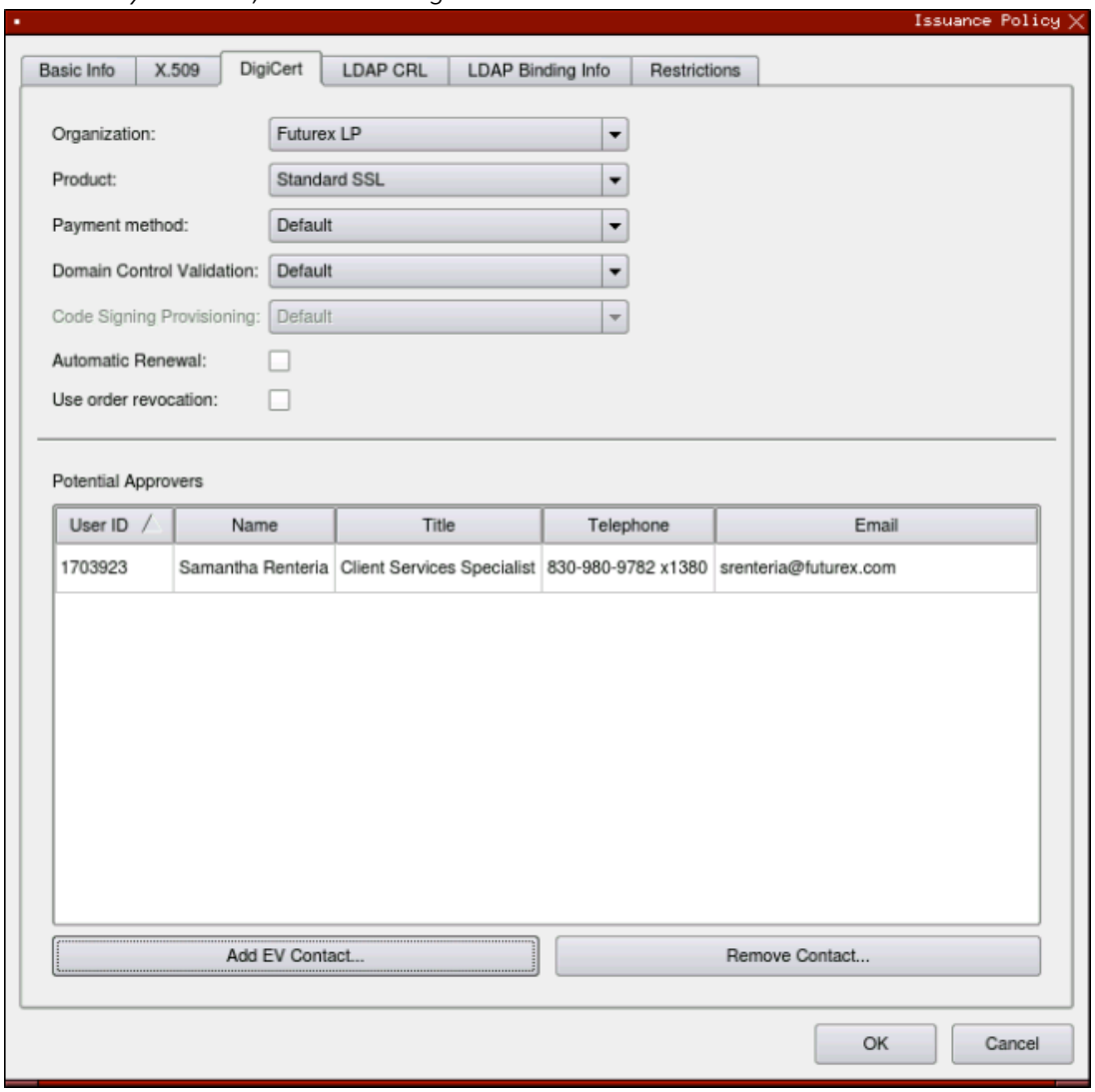


3. An Import Certificates window will open. Verified certificates will appear in the Verified panel, and unverified will appear in the Unverified panel.
    - Choose the major key that will be used to verify the certificate.
    - Once chosen, click the Verify button at the bottom of the window to verify the certificate. If verified, it will appear in the Verified panel.
4. Click OK to add the certificate.

Adding an Issuance Policy

An Issuance Policy allows users to define the workflow of how certificates are deployed, who can deploy them, and what type of certificates can be deployed.

1. Expand the CA group container, right click on a certificate, and select Issuance *Policy -> Add*.
2. In the *Issuance Policy* window, select the *DigiCert* tab.



3. Fill in the following information as required:
    - **Organization**: Select the correct organization name from the list.
    - **Product**: Select the correct SSL certificate type (e.g. Standard, Multi-Domain, WildCard, EV, Code Signing, etc.). (**NOTE**: This field must match the type of certificate that was imported. If it does not match it will create an "Invalid" certificate.)
    - **Payment method**: The three payment methods are Default, Account Balance, and Profile.
    - **Domain Control Validation**: The Domain Control Validation field may or may not be editable, depending on the Product type that was selected. Essentially, this setting determines whether the CA verifies that the person making the request is in fact authorized to use the domain related to that request, before issuing an SSL.
    - **Code Signing Provisioning**: If the Product type is Code Signing this field will be editable. If the Product type is Standard SSL, for example, the Code Signing Provisioning field will be grayed out.
    - **Potential Approvers**: If using an extended validation (EV) certificate, an approver is required. Select Add EV Contact to add an approver to the list.
4. Click OK to save the settings.

NOTE: Currently it is not possible to change the **Organization** or **Product** fields without deleting and recreating the Issuance Policy. All of the other fields can be changed.

NOTE: If any type of Extended Validation (EV) certificate is selected for the Product type, then an EV contact must be added. Right now only "Approver" users can be added as an EV contact.

NOTE: If you want to associate additional domain names with a certificate, there must be an *X.509 Extension Profile* attached to the certificate that supports Subject Alternate Names. For more information about how to configure an X.509 Extension Profile that supports Subject Alternate Names, please see the relevant Administrative guide.

APPENDIX A: XCEPTIONAL SUPPORT

In today's high-paced environment, we know you are looking for timely and effective resolutions for your mission-critical needs. That is why our Xceptional Support Team will help do whatever it takes to ensure you have the best experience and support possible. Every time. Guaranteed.

- 24x7x365 mission critical support
- Level 1 to level 3 support
- Extremely knowledgeable subject matter experts

At Futurex, we strive to supply you with the latest data encryption innovations as well as our best-in-class support services. Our Xceptional Support Team goes above and beyond to meet your needs and provide you with exclusive services that cannot be found anywhere else in the industry.

- Technical Services
- Onsite Training
- Virtual Training
- Customized Consulting
- Customized Software Solutions
- Secure Key Generation, Printing, and Mailing
- Remote Key Injection
- Certificate Authority Services

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com

ENGINEERING CAMPUS

864 Old Boerne Road

Bulverde, Texas, USA 78163

Phone: +1 830-980-9782

+1 830-438-8782

E-mail: info@futurex.com

XCEPTIONAL SUPPORT

24x7x365

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com

SOLUTIONS ARCHITECT

E-mail: solutions@futurex.com