



# **User Guide – DigiCert ONE**

CableLabs PKI Operations

Version: 2.0

Date: May 13, 2025

Table of Contents

**User Profile Set-up.....2**

**Password and Authenticator Set-up .....2**

**Authentication Certificate Set-up.....4**

        Create a new authentication certificate.....4

        Install PKI Client and administrative certificate. ....5

**General Navigation ..... 6**

**Check Balances..... 6**

**Generating and Downloading New Certificates ..... 7**

    Batch Review and Approval (optional) ..... 10

    Downloading Certificates ..... 13

    Decrypting the SMPB batch ..... 14

**Downloading Root and Intermediate Certificates ..... 14**

**Revoking Certificates..... 16**

## User Profile Set-up

### Password and Authenticator Set-up

When your user account is initially set-up, you will receive an email from [no-reply@digicert.com](mailto:no-reply@digicert.com) and the Subject: **Welcome to DigiCert ONE**. If you did not receive an email (after checking SPAM and junk folders), please contact [pkiops@cablelabs.com](mailto:pkiops@cablelabs.com).

- Click on the **Set your password** link in the email.
- Enter your desired password and confirm it. This password requirements are:
  - Minimum of 12 characters
  - Maximum of 125 characters
  - At least one of the following
    - 1 lower case character
    - 1 upper case character
    - 1 symbol (@#\$%^&\*)
    - 1 number
- Click **Submit**.
- Enter your username and password to login.
- You will be prompted to connect your account with Google Authenticator. Follow the steps to connect with Authenticator app (this will be used in place of your administrative cert to login to the portal)

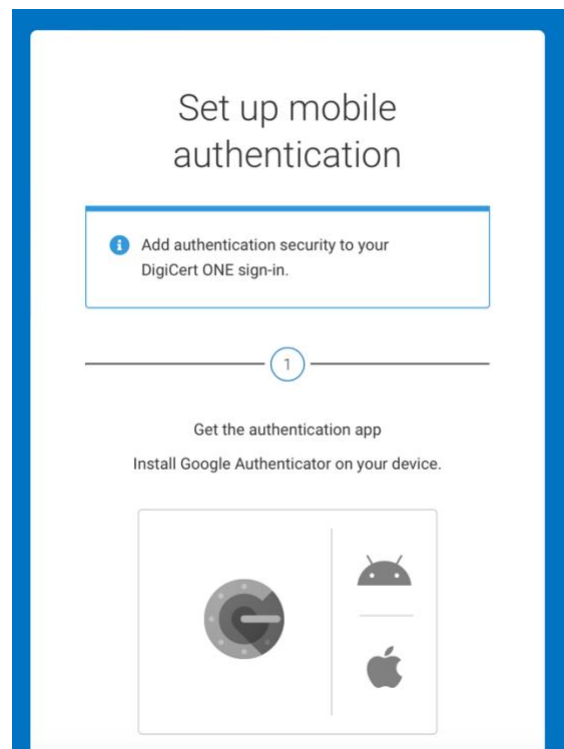



Figure 1 - Connect account with Authenticator App

2

Set up authentication app

Open the authentication app and scan this barcode:



Scan not working? [Get a setup key](#)

3

Enter setup OTP

Enter the one-time passcode (OTP) provided by the authentication app.

One-time passcode (OTP)

Set up mobile authentication

Figure 2 - Complete set-up of Authenticator App

- Once you've connected with the Authenticator app and entered the passcode from the app, you'll be prompted to accept the terms and conditions. Check the box and click **Accept**. You will be taken to your profile page.

digicert® ONE

DigiCert Master Services Agreement

☒ I have read and agree to the DigiCert Services Agreement and Privacy policy

Accept

Figure 3 - Accept Terms and Conditions

## Authentication Certificate Set-up

From the Profile page, you will be able to set up your Authentication Certificate, which will be used to encrypt the certificates for download and storage.

*Note: The current administrative certificate from the MPKI8/Magnum platform cannot be used on the DigiCert ONE platform as it will be disabled when access to MPKI8/Magnum is disabled.*

### Create a new authentication certificate

- Scroll down to the **Authentication Certificates**
- Click on **Create authentication certificate**

#### Generate authentication certificate

Nickname

End date

Encryption

Signature hash algorithm

Cancel Generate certificate

Figure 4 - Generate new authentication certificate

- On the new page enter a nickname for the cert (e.g. John Doe Auth Cert 1)
- Enter an end date for the certificate (e.g. 2-5 years out)
- Keep the recommended selections (AES, SHA-256)
- Click on Generate certificate
- In the new window, copy the password. *Note: You will need to use this password to open certificate your download. Copy it to a local file on your machine (e.g. a text file or Word document) temporarily.*
- Install the certificate in your local key store using the password above. Installation will vary depending on your operating system.
- The certificate will show up in your list of available certificates to use:

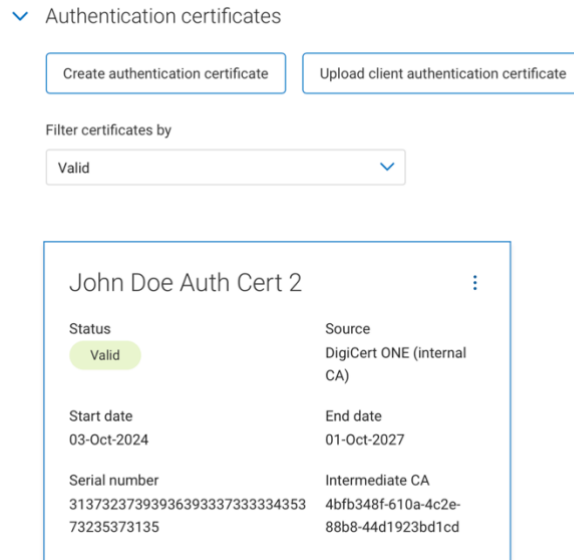
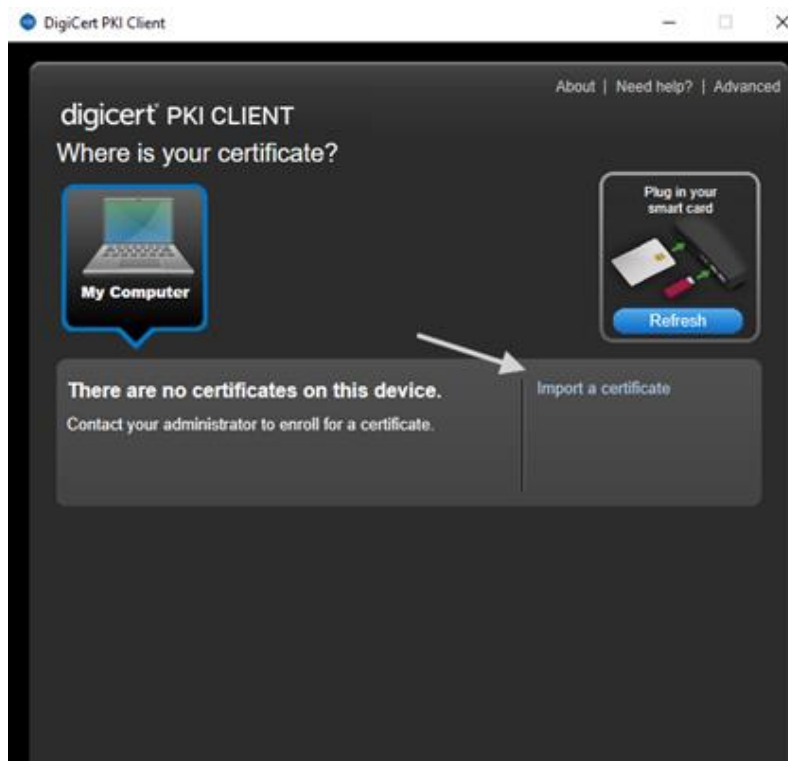


Figure 5 - List of Authentication Certificates

## Install PKI Client and administrative certificate.

- Download the [PKI Client](#) and install it with local Admin permissions.
- Search “**PKI Client**” from the Windows search.
- After the Client launches and initializes, select “**My Computer**” and then “**Import a certificate.**”



- Browse for your previously downloaded Client Auth certificate created in the previous step.
- You will be presented with a prompt asking if you want to protect your certificate with a PIN. It is advisable to do so as this will protect your certificate from unauthorized access.

**Please Note:** If this PIN is lost, a new certificate will need to be generated as resetting the PIN without the previous PIN is a destructive act on the PKI Client cert store.

## General Navigation

The key functionality of the portal can be found under the IoT Trust section of the site. To access the IoT Trust section, click on the squares menu in the top right of the web page.

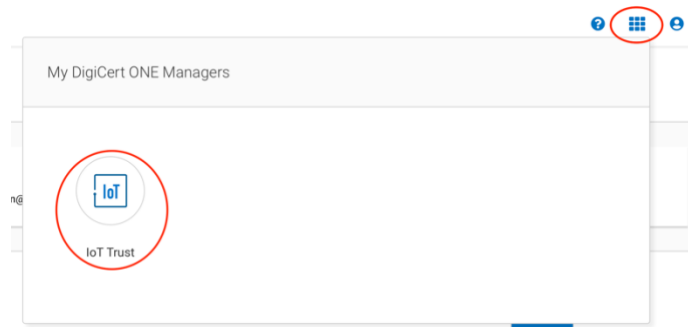


Figure 6 - Access IoT Trust Module

To access your user profile, click on the Person icon in the top right of the page and select **Admin Profile**.

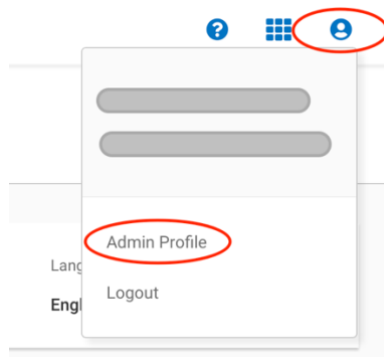


Figure 7 - Access user profile details

## Check Balances

On the Dashboard page for IoT Trust Manager, you will see a listing of available Licenses at the top:

## IoT Trust Manager Dashboard

Licenses			
Devices	Certificates	Devices with ICA	Issuing CA
100/132	100/133	0/0	0/0
Remaining / Allocated	Remaining / Allocated	Remaining / Allocated	Remaining / Allocated

Figure 8 - License Overview

The **Devices** and **Certificates** numbers should be the same as certificates are connected to devices on a one-to-one basis.

*Note: The License values shown are cumulative across all account types in the DigiCert ONE system. E.g. If you purchased 100,000 D3.0 certificates, 100,000 D3.1 certificates and 25,000 PacketCable certificates, the license value will show as 225,000. These licenses can be used for **any** certificate type and will not be limited based on the purchase (e.g. in the example above, you can use the 25,000 PacketCable certs for D3.0 or D3.1 certs and vice versa).*

The **Allocated** number is an indication of **all** the certificates allocated over the entire history of the account. This number will continue grow over time from order to order.

The **Remaining** number is an indication of the certificates remaining in the account and available for issuance.

*Note: On the DigiCert ONE platform, you can have a negative balance. CableLabs will perform monthly reporting and present an invoice for any negative balances. Extended periods in negative balances may result in suspension of the account until the balance is positive.*

## Generating and Downloading New Certificates

- Login to your account and go to IoT Trust Manager (if not already there by default) using the squares menu in the top right of the web page.

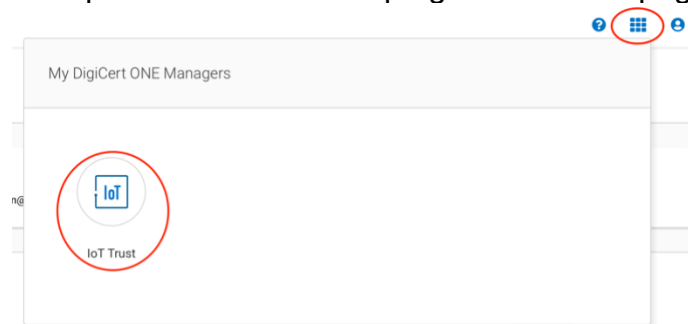


Figure 9 - Access IoT Trust Manager

- Click in **Certificates** in the left navigation bar



- To initiate a new batch, select **Start batch certificate request**

## Certificate management

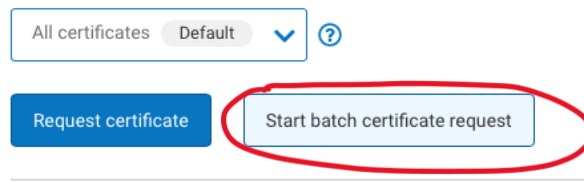


Figure 10 - Start new batch request

- Name the batch something unique that can be referenced later e.g. Cert Type - Date DOCSIS 3.1 – 2024-09-01 – Batch 1.
- Enter a description (optional)
- Select the certificate type under **Enrollment Profile** e.g. *Customer* – DOCSIS 3.1 –RSA 2048

## Start batch certificate request

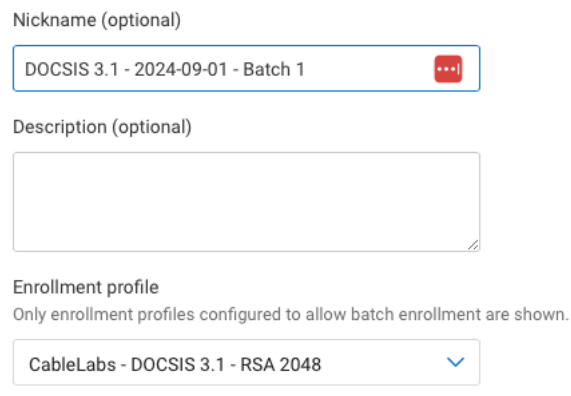


Figure 11 - Batch Reference Details

- Select the desired download format. **Note:** For customers wanting to retain the same download format as the MPKI8/Magnum platform, select **Binary .CER (SMPB)**. The format options include:
  - Base 64 .PEM (zipped) –
  - Base 64 .PEM (JSON) – Certificate is in a JSON format and can be downloaded and inserted into a database directly (still encrypted)
  - Binary .DER (zipped) -
  - Binary .CER (SMPB) – Proprietary format that includes zip file + text file within a zip file. This is the same format used in the MPKI8/Magnum platform (in combination with the MPKI8 PKI Client).

Certificate download format

☐ Base 64 .PEM (zipped)

☐ Base 64 .PEM (JSON)

☐ Binary .DER (zipped)

☒ Binary .CER (SMPB)

Batch results log format

The log file includes the results of each certificate request in the batch.

☒ CSV

☐ JSON

Certificate chain options

☒ Include root and intermediate certificates only as separate files in the download package.

☐ Also package intermediate certificates with each end entity certificate.

☐ Also package root and intermediate certificates with each end entity certificate.

Figure 12 - Download options

- Select the options as to how you want the keys generated for the certificates (either from your own CSRs or having DigiCert generate the certificate plus key pairs). *Note: Most companies will have the platform generate the keys, which is how the MPKI8/Magnum system worked.*

☒ I have the keypairs and will provide the CSRs or public keys in the request

☒ I will upload zipped archive with CSRs

Upload file

Supported file formats: Zipped CSRs

Maximum file size: 200 MB

Click or drag file to upload

☐ I will upload CSV with request info

☒ DigiCert ONE generates the keypairs and returns encrypted

When keys cannot be provided during enrollment.

Figure 13 - Select how certificate/key pairs are generated

- If **DigiCert ONE generates the keypairs and returns encrypted** is selected, the following options will appear. Select the appropriate authentication certificate to encrypt the certificate package that was set-up under your profile (see above) or upload a local certificate or PGP key.  
**Note:** If you have an existing authentication certificate for MPKI8/Magnum platform and you want to use the MPKI8 PKI Client app to decrypt the certificate package after download, ensure you are using the same authentication certificate as the PKI Client app.

How will the certificates be encrypted?

☒ Use authentication certificate from my profile

Only eligible certificates are shown in this list

PKI Ops Auth Cert 1

☐ Upload certificate or PGP key

Figure 14 - Select encryption certificate

- Select how you want to assign value for the certificates CN (common name) value. This will almost always be **Generate requests for MAC addresses**.
- Enter the starting MAC address, the number of certificates to generate (max ??) and the increment value.

How will the certificates be generated?

☐ I will upload CSV with request info

☒ Generate requests for MAC addresses

Starting MAC address

BD:12:46:DE:42:39

Number of requests (500,000 maximum)

10000

Increment each address by

1

Cancel Start request

Figure 15 - Select starting MAC, quantity and increment values

- Click **Start Request**. You will return to the main Certificate management screen, where the status on the batch request will display.

<input type="checkbox"/>	Certificate value	Certificate type	Device	Device profile	Enrollment method	Certificate policies	Status
<input type="checkbox"/>	86:6C:A0:BC:52:2B	End entity certificate	86:6C:A0:BC:52:2B	Basic device profile	BATCH		Issued

Figure 16 - Certificate Manager screen

### Batch Review and Approval (optional)

If you have configured your account to require approval of the order request before download, you will need to have an administrative user approve the request. This is an optional feature to verify the batch information (e.g. MAC address range). If there are errors with the batch, it can be cancelled and the balance of certificates return to your account. Contact [pkioptions@cablelabs.com](mailto:pkioptions@cablelabs.com) if you have questions about Batch approval and/or whether you want to enable or disable it on your account.

**Note: Once certificates have been issued, they are considered valid and used. Revoked certificates cannot be added back to your balance of available certificates.**

- Depending on how the account has been configured, users from your organization may receive an email indicating that there is a batch ready for approval. It will be from the address [no-reply@digicert.com](mailto:no-reply@digicert.com) and have the subject **Batch certificate request approval required**. If necessary, add this address to your trusted list of senders and/or check your junk email folder to see if it is located there. Click on **View request** to access the specific request.

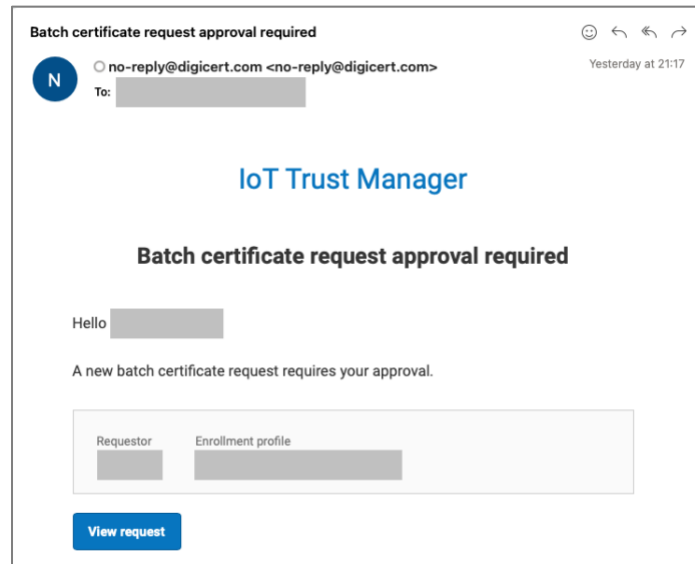


Figure 17 - Email requesting approval for batch

- Alternatively, you can access the approval request directly from the IoT Manager by logging into DigiCert ONE (<https://one.digicert.com>), go to **IoT Manager** and select **Certificates** from the side navigation. Select **Batch jobs** to see the list of available batch requests and click on the **Nickname** link for the batch that needs to be approved (See Figure 18 - Batch jobs pending approval).

Batch jobs

Start batch certificate request		Import new certificate		⋮	
Nickname	Date started	Status	Results	Actions	
CableLabs - R-PHY - Approval Test Batch 1	13-May-2025	Pending approval		⋮	

Figure 18 - Batch jobs pending approval

- Once in the batch detail page (through either the email link or the website link), you can review the details of the batch by clicking **Download stored files** at the bottom of the page (See Figure 19).

Batch certificate request details: CableLabs - R-PHY - Approval Test Batch 1

Status

Date started

Date finished

Type

Requestor

Pending approval

13-May-2025 16:17:55

Not set.

Batch key gen MAC

s.kenny@kyrio.com

General information

Enrollment profile

CableLabs - R-PHY Device - RSA 2048

Certificate template

D5 - REMOTE PHY (R-PHY) DEVICE-CABLELABS

Total requests in batch

2

Key type

RSA 2048

Certificate profile

CableLabs - Remote PHY Device - RSA 2048

Issuing CA

CableLabs Device Certification Authority

Certificate download format

Base 64 .PEM (zipped)

Signature algorithm

sha256WithRSA

On this page

General information

Download stored files

Figure 19 - Batch detail page with Download details and Accept/Reject options

- If the batch is acceptable, you can click on the checkmark icon to approve the batch. *Note: Once certificates have been Approved, they are considered valid and used. Revoking the certificates will not be added back to your balance of available certificates.*



Figure 20 - Approve batch order

- Alternatively, if there are issues with the batch, you can reject it by clicking the cancel icon. You will be prompted to provide a reason for the cancellation.



Figure 21 - Cancel batch order

- If the batch is approved, it will complete the process and show **Completed** on the Batch jobs screen. If cancelled, it will show as **Rejected** on the Batch jobs screen

Batch jobs

Start batch certificate request

Import new certificate

Nickname	Date started	Status	Results	Actions
CableLabs - R-PHY - Approval Test Batch 1	13-May-2025	Rejected	No records successful	
CableLabs - OpenCable UDRD - Test Batch 3	08-May-2025	Completed	2 / 2 records successful	

Figure 22 - Batch job status with Approved and Rejected jobs

Downloading Certificates

Once the certificates have been generated, you can download the certificates

- Click on **Batch Jobs** under **Certificates** on the left navigation.
- Click on the batch job you would like to download.

Nickname	Date started	Status	Results	Actions
DOCSIS 3.1 - 2024-09-01 - Batch 1	17-Sep-2024	Completed	10 / 10 records successful	

Figure 23 - Certificate Batch status

- Click on the download icon (downward blue arrow) to start the download. The file will be saved to your local machine in the default location for file downloads.

Batch certificate request details: DOCSIS 3.1 - 2024-09-01 - Batch 1

Status	Date started	Date finished	Type	Requestor
Completed	17-Sep-2024 12:20:03	17-Sep-2024 12:20:06	Batch key gen MAC	pkiops@cablelabs.com

General information

Certificates issued

10

Total requests in batch

10

Enrollment profile

CableLabs - DOCSIS 3.1 - RSA 2048

File size

0

Download icon

Edit icon

More icon

On this page

General information

Batch management

Download history

Figure 24 - Batch details screen

- Open the batch file using your preferred method depending on the download options selected. If you specifically chose **SMPB** as the file output format, use the next step to open the file with the PKI Client.

## Decrypting the SMPB batch

- To decrypt the batch on a system with the Client Authentication certificate imported to the PKI Client, simply double click the downloaded SMPB file.
- You will be presented with a window asking for a File location to save the decrypted zip file. Selecting "Continue" will present you with the PIN you set earlier when importing the Client Authentication certificate.
- After successfully decrypting the file, you can now open the new zip file with Windows Explorer to view the contents (See Figure 25 - Decryption via PKI Client application).

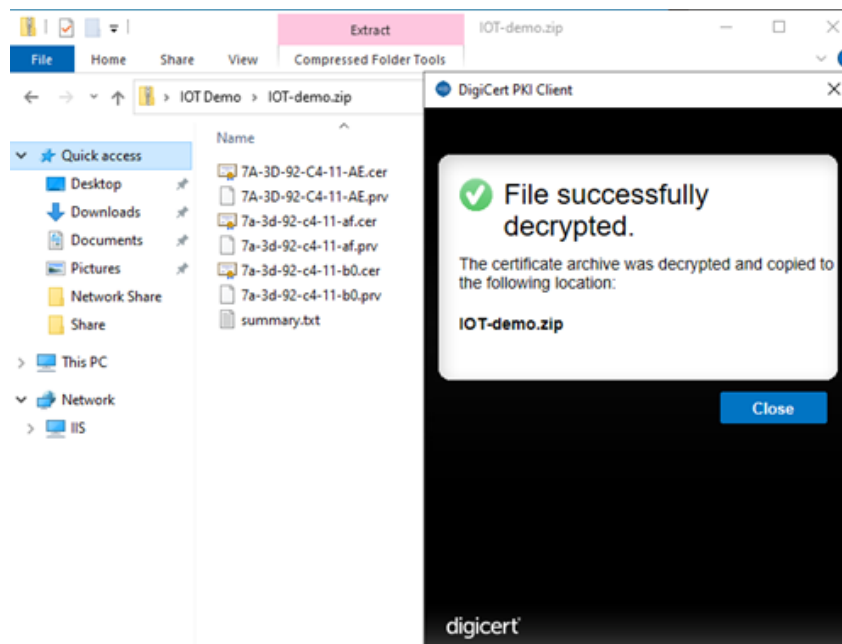


Figure 25 - Decryption via PKI Client application

## Downloading Root and Intermediate Certificates

The Root and Intermediate (Issuing) CAs are the same as the current Magnum/MPKI8 platform. If you have already downloaded these certificates, you do not need to re-download them.

If you need to download either certificate from the platform, perform the following steps:

- Login to your account and go to IoT Trust Manager (if not already there by default) using the squares menu in the top right of the web page.

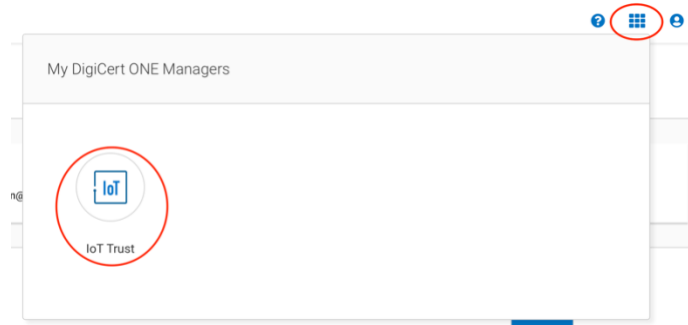


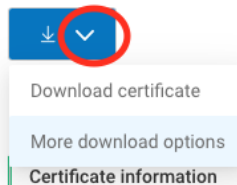
Figure 26 - Access IoT Trust Manager

- Click in **Certificates** in the left navigation bar
- Click on a link for the **Certificate Value**

<input type="checkbox"/>	Certificate value	Certificate type	Device
<input type="checkbox"/>	<a href="#">bd:12:46:de:42:41</a>	End entity certificate	bd:12:46:de:42:41

Figure 27 - Click to get details on certificate

- On the certificate details page, click on the downward carat (v) and select **More download options**.



- On the download options page, you can select to download either the Intermediate certificate or Root certificate. You also have additional options to



download the device certificate as well as a bundle of the certs in different options under the **File Type** selection.

The screenshot shows a 'Download certificate' window with a close button (X) in the top right. It contains three main sections:

- Combined certificate files:** A dropdown menu for 'File type' set to 'Individual .crts (zipped)' and a 'Download' button.
- Individual certificate files:** A section with a 'Certificate' dropdown set to 'CableLabs Device Certification ...' and a 'Download' button.
- Root certificate:** A section with a 'Root certificate' dropdown set to 'CableLabs Root Certification Authority.crt' and a 'Download' button.

Below these sections are three text boxes containing certificate data, each with a 'Download' button. The first box is labeled 'bd:12:46:de:42:41:cr1' and the others are labeled 'CableLabs Device Certification ...' and 'CableLabs Root Certification Authority.crt'.

Figure 28 - Certificate Download Options

- Once downloaded, click the **X** in the top right of the window to close the download options screen.

## Revoking Certificates

Certificates may be revoked if the certificate has been compromised or the certificate was generated in error (e.g. wrong MAC addresses).

*Note: Once certificates have been issued, they are considered valid and used. Revoked certificates cannot be added back to your balance of available certificates.*

To revoke a certificate (or multiple certificates), perform the following steps:

- Login to your account and go to IoT Trust Manager (if not already there by default) using the squares menu in the top right of the web page.

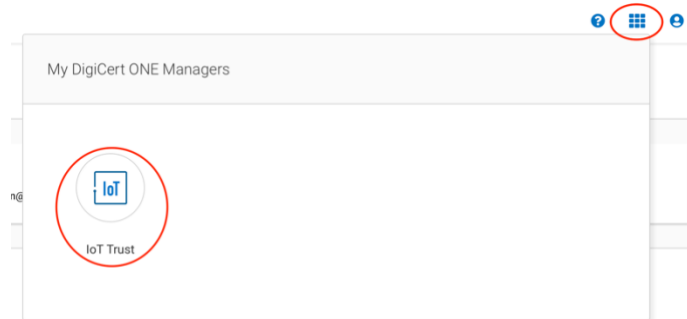


Figure 29 - Access IoT Trust Manager

- Click in **Certificates** in the left navigation bar

- Find the certificate you need to revoke and click on the three dots next to the **Certificate value** (MAC address).

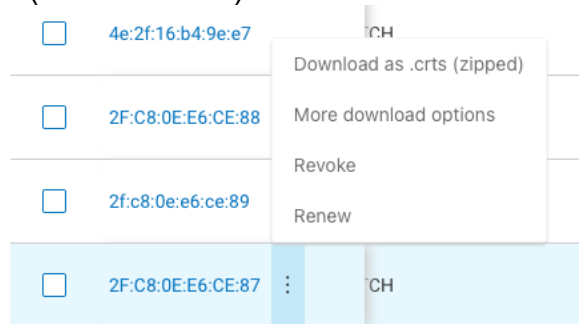


Figure 30 - Individual Certificate Options

- Select **Revoke** from the list of options.
- In the new window, select a reason for the revocation and add a description. Click **Revoke certificate** to complete the process.
- You will receive a confirmation that the certificate has been revoked and the status in the certificate list will show **Revoked**.

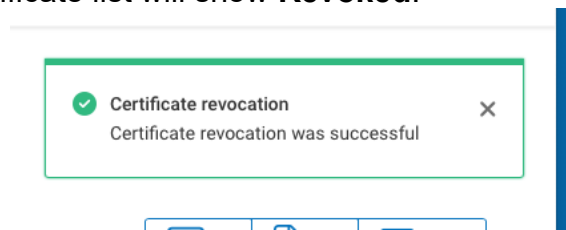


Figure 31 - Cert revocation confirmation message