User Guide – DigiCert ONE Device Trust Manager (DTM)

CableLabs PKI Operations

Version: 5.0

Date: June 5, 2026

Table of Contents

NOTE: This document is intended for the users of Device Trust Manager (DTM) in the DigiCert ONE platform. Users of the IoT Trust platform, should refer to the latest user guide for IoT Trust which can be found on the Security Document Library at cablelabs.com

1 Initial set-up and system access

There are two options to authenticate and gain access to the DigiCert One portal:

1. **Google Authenticator**. This uses the Google Authenticator app and is explicitly tied to a user login. The user must have a mobile device to download and use the Authenticator app
2. **Client Authentication Certificate**. This is a digital certificate installed on the computer where the site is being accessed and certificates issued from. Note: this may be different from the client certificate used to encrypt certificate orders.

You will need to select one of these options prior to the initial set-up. The sections below detail the set-up process for each.

1.1 Password and Authenticator Set-up (Option 1)

When your user account is initially set-up, you will receive an email from 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.

- 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)

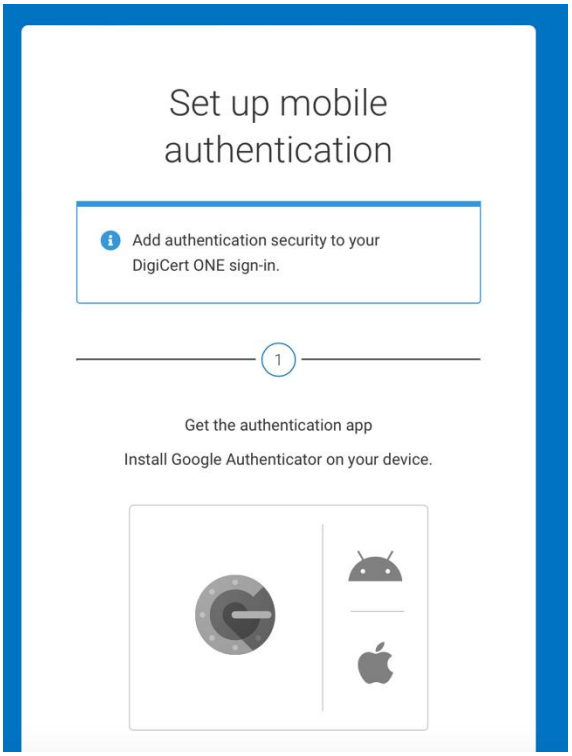


Figure 1 - Connect account with Authenticator App

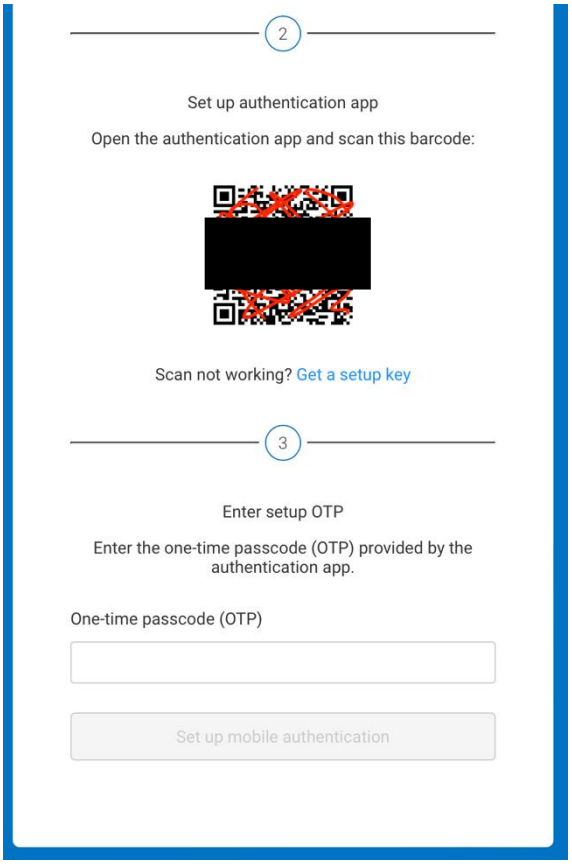


Figure 2 - Complete set-up of Authenticator App

- 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.

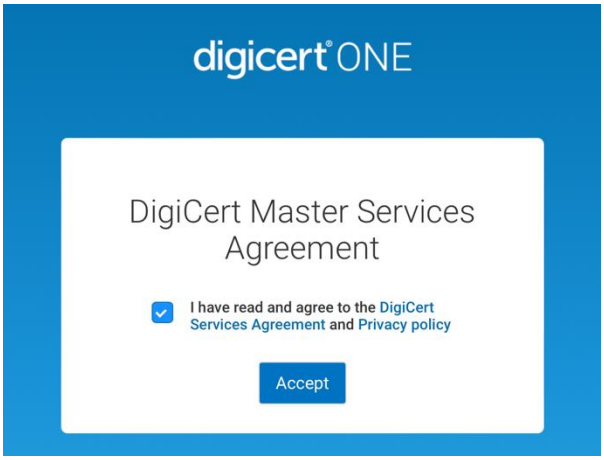


Figure 3 - Accept Terms and Conditions

1.2 Authentication Certificate Set-up (Option 2)

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: Administrative certificates from the MPKI8/Magnum platform cannot be used on the DigiCert ONE platform, as they will be disabled when access to MPKI8/Magnum is disabled.

1.2.1 Create a new authentication certificate

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

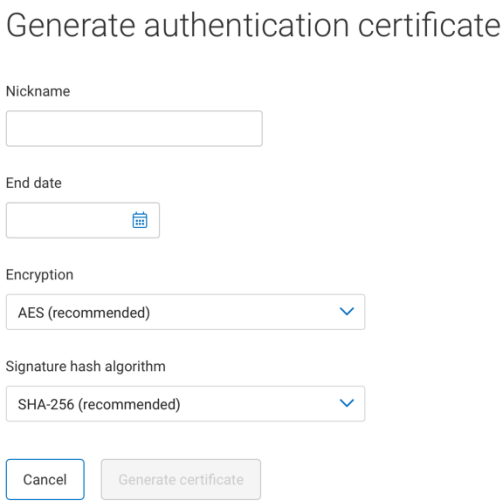


Figure 4 - Generate new authentication certificate

- 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:

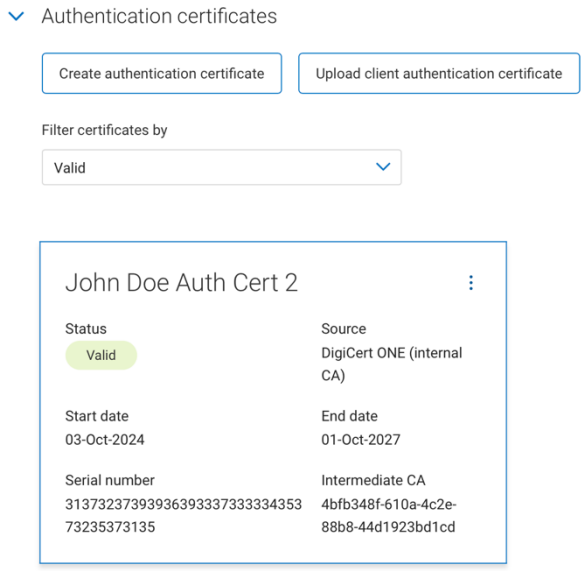
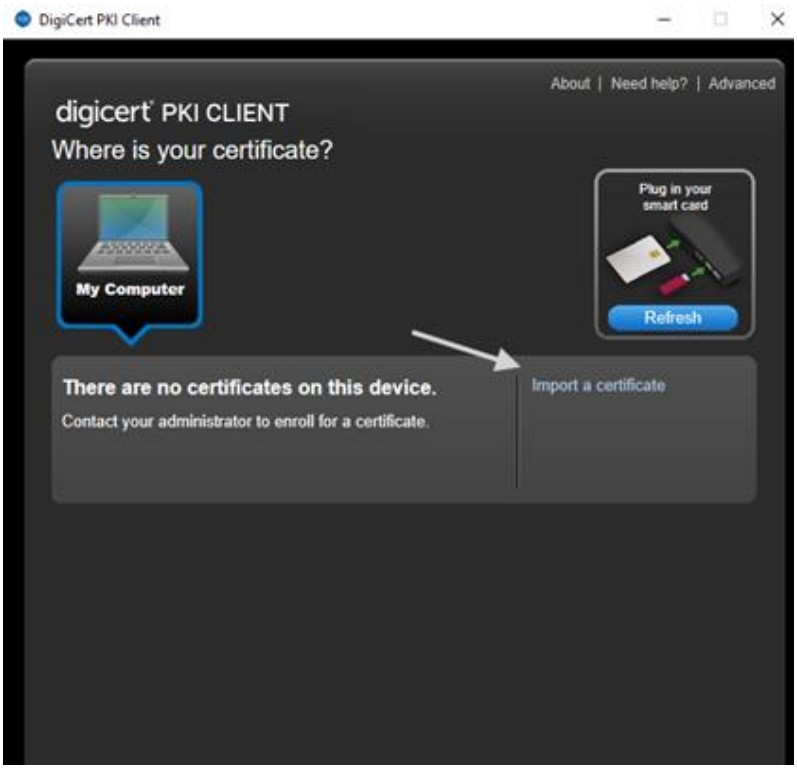


Figure 5 - List of Authentication Certificates

1.2.2 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.*

2 General Navigation

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

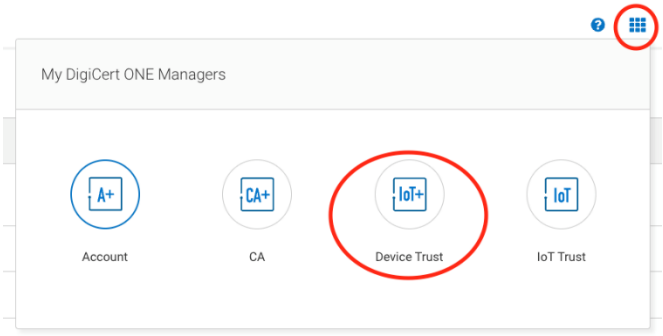


Figure 6 - Access Device Trust Module

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

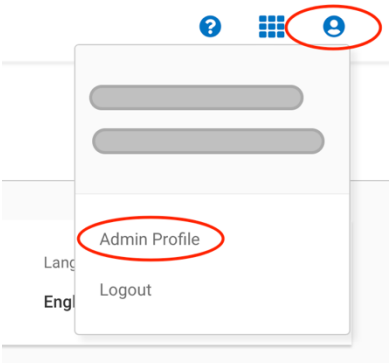


Figure 7 - Access user profile details

3 Check Balances

On the Dashboard page for Device Trust Manager, you will see a listing of available Licenses under the **Plans and Licenses** tab:

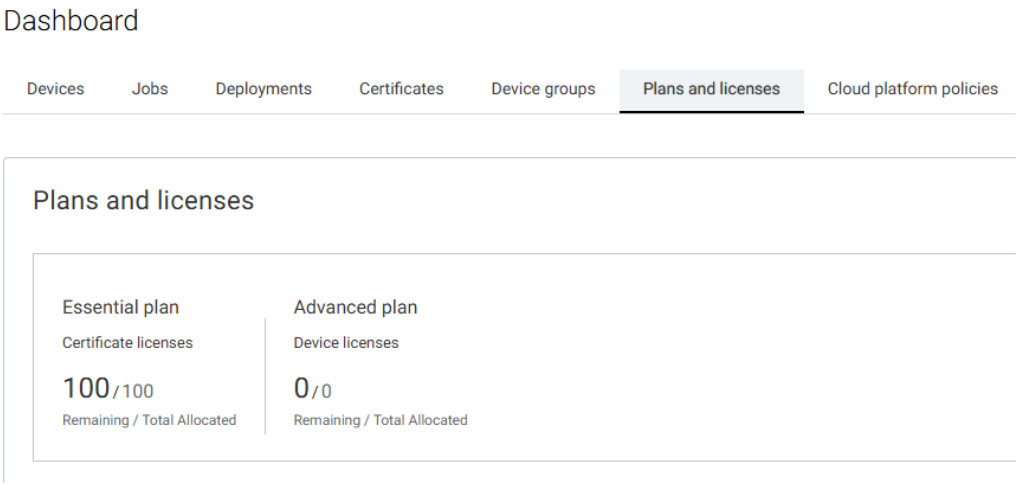


Figure 8 - License Overview

The **Essential plan** certificates are the ones supplied for your devices (cable modems, RPD). The **Advanced plan** licenses are not applicable here, and the balance should be 0.

*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 to 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.

4 Generating and Downloading New Certificates

4.1 Generating Certificates

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

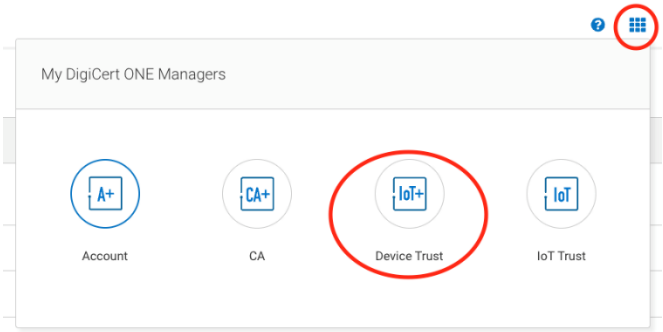
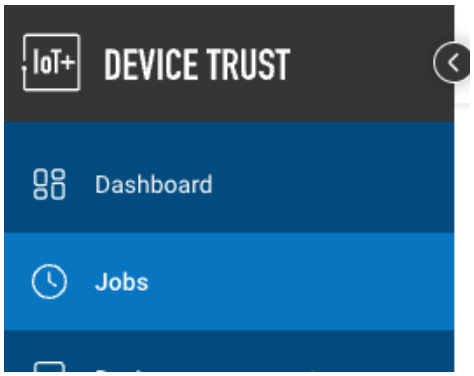


Figure 9 - Access Device Trust Manager

- Click in **Jobs** in the left navigation bar:



- To initiate a new batch, select **New Job** and then select **Batch certificate request**. *Do not select "Batch certificate request for devices".*

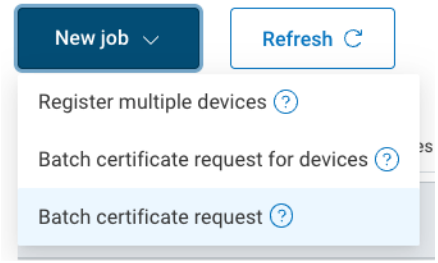


Figure 10 - Start new batch request

- In the new screen, name the batch something unique that can be referenced later e.g. DOCSIS 3.1 – 2024-09-01 – Batch 1.
- Enter a description (optional)
- Click **Next**

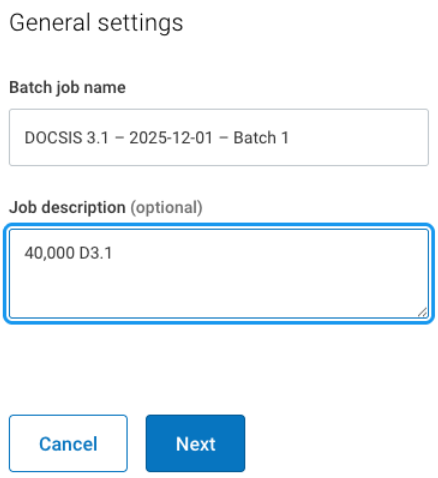


Figure 11 - Batch name and description

- Select the certificate type under **Certificate management policy**. This associates with the type of certificate to be issued (e.g. D3.0, D.3.1, Remote PHY) e.g. *Customer* – DOCSIS 3.1 –RSA 20248. If you want to view the details associated with this profile, click on the *Show Details* link.

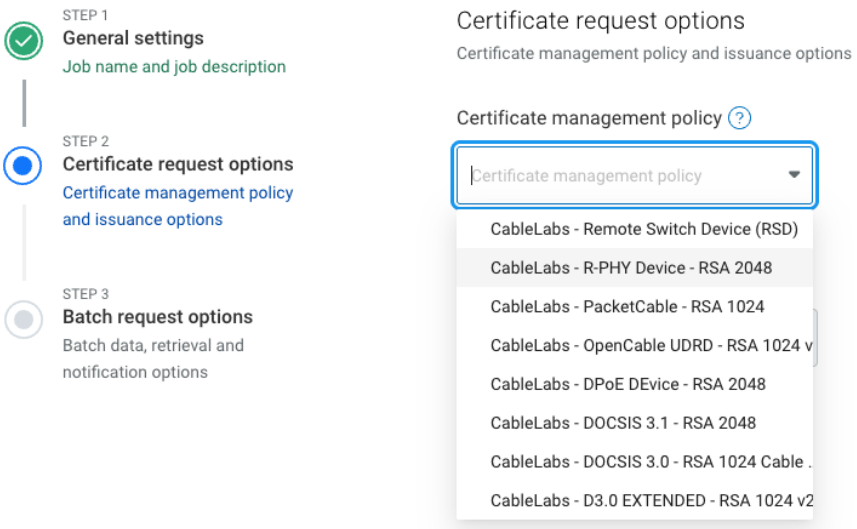


Figure 12 - Batch certificate management policy selection

- Select the certificate to be used to encrypt the certificates for download. Click **Next**.

4.1.1 For customers which generate certificates with an initial MAC address,

- Enter the number of certificates needed, the increment counter and the starting MAC address.

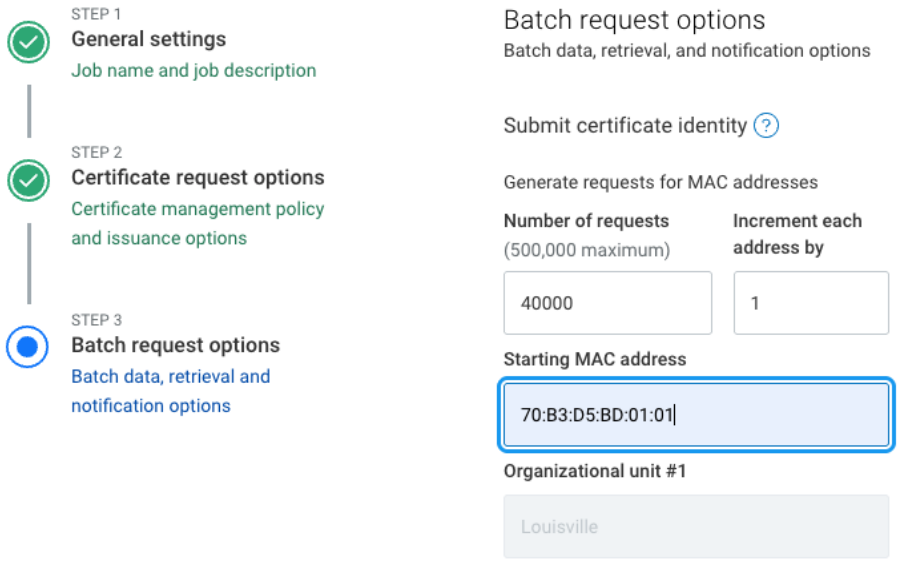


Figure 13 - Batch request options for MAC addresses

- Confirm the email to receive a notification once the certificate generation is complete. You can add (or remove) addresses as necessary. If you want someone without a DigiCert ONE login to be able to download the certificates, check *Allow users without a login to this portal to download the batch file*.
- Click **Submit batch job request**. You will return to the main Certificate management screen, where the status on the batch request will be displayed.

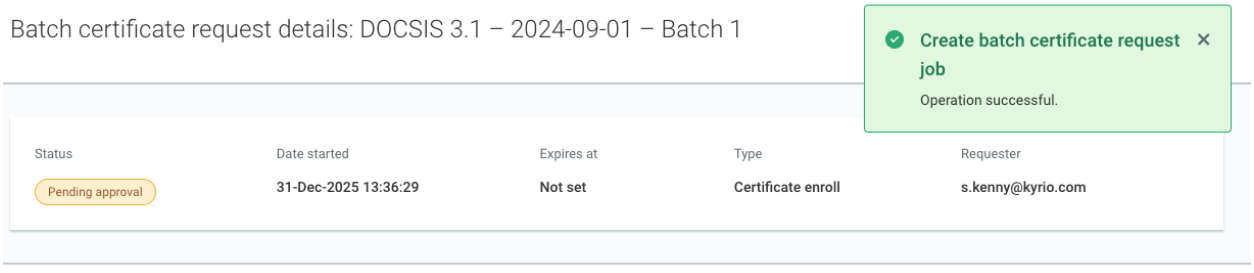


Figure 14 – Batch job request confirm

4.1.2 For customer which generate certificates with a list of certificate details

- Upload the commas separated value (CSV) file with the necessary details for batch generation by either dragging the file to the target area on the page or click **Browse files**. If you need a template with the correct format, click on the **Download CSV template** below the file upload option.

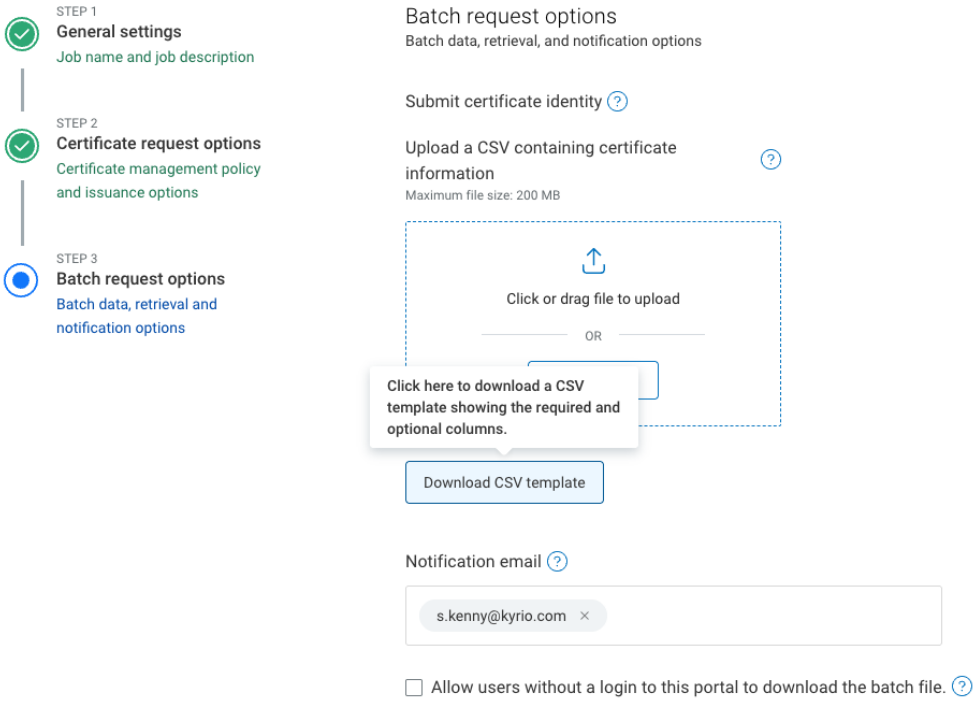


Figure 15 - Batch request options for file uploads

- Confirm the email address where you would like to receive a notification when the certificate generation is complete. You can add (or remove) addresses as necessary. If you want someone without a DigiCert ONE login to be able to download the certificates, check *Allow users without a login to this portal to download the batch file*.
- Click **Submit batch job request**. You will return to the main Certificate management screen, where the status on the batch request will display.

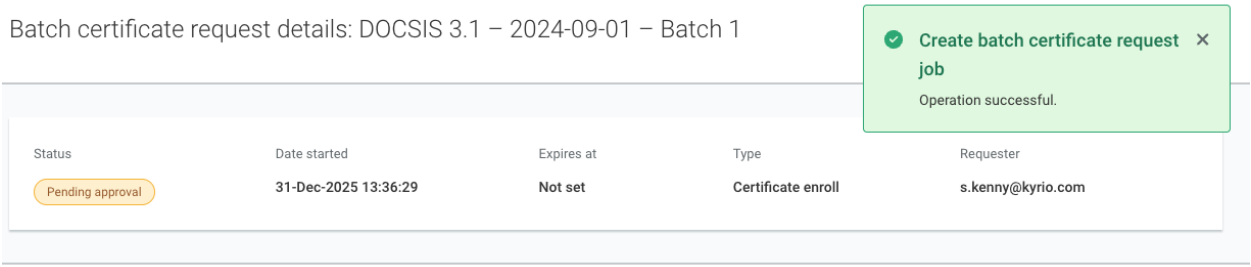


Figure 16 – Batch job request confirm

4.2 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 pkiops@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** 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.

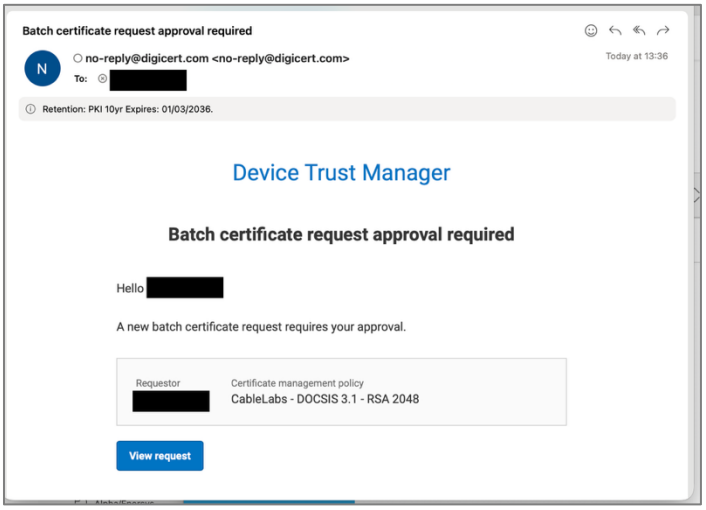


Figure 17 - Email requesting approval for batch

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

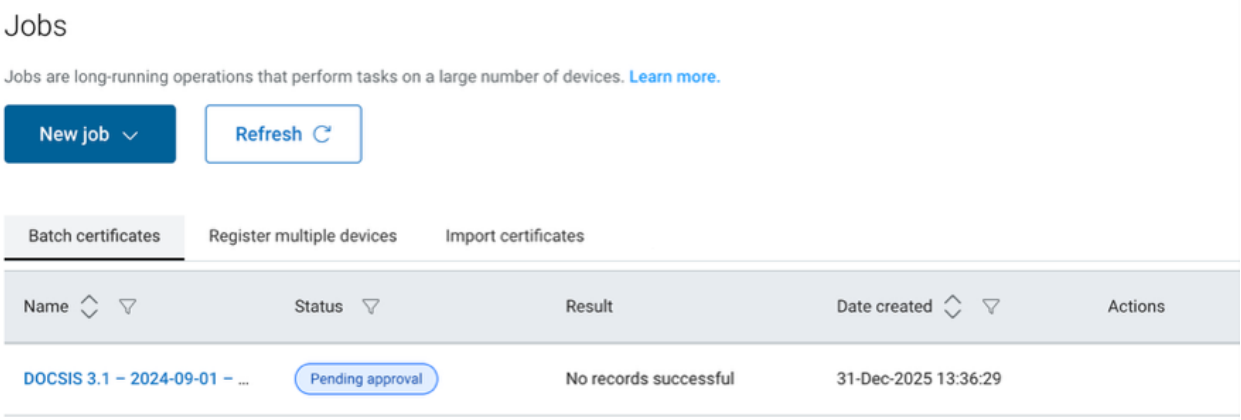


Figure 18 - Batch jobs pending approval

- 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).

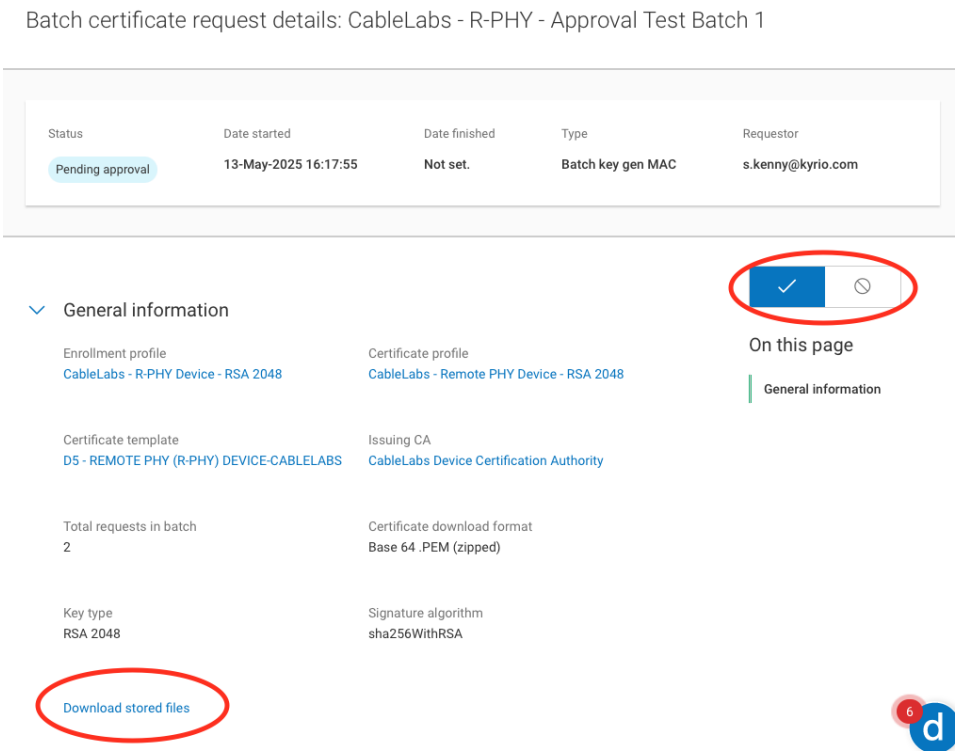


Figure 19 - Batch detail page with Download details and Accept/Reject options

- If the batch is acceptable, you can click on the checkmark icon to approve the batch.

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** (or **Failed** if there was an issue) on the Jobs screen. If cancelled, it will show as **Rejected**

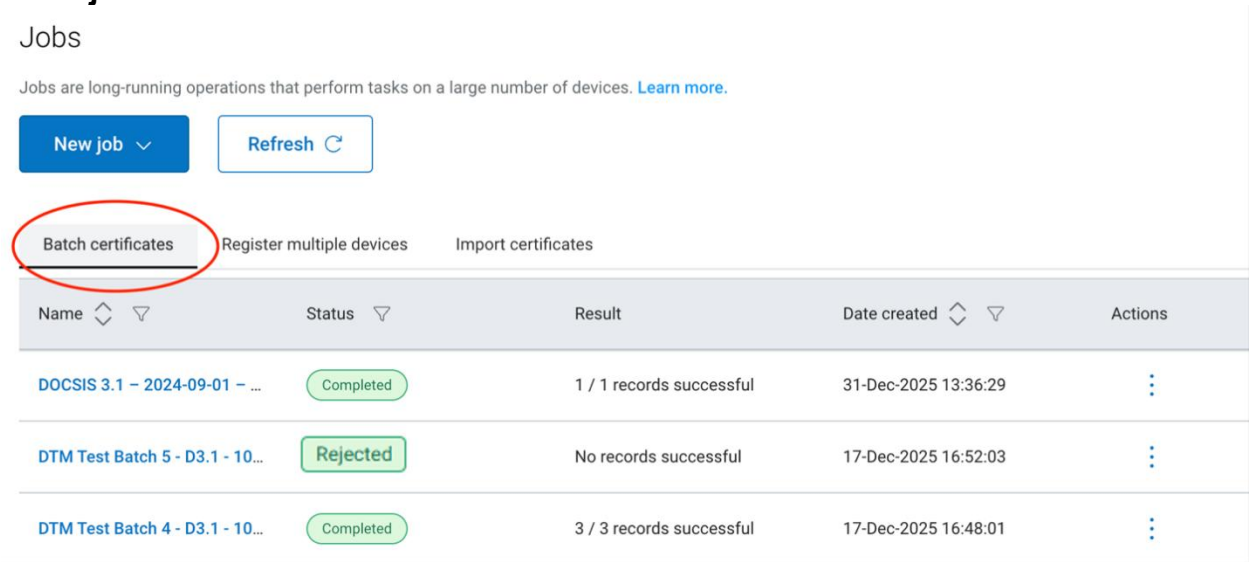


Figure 22 - Batch job status with Approved jobs

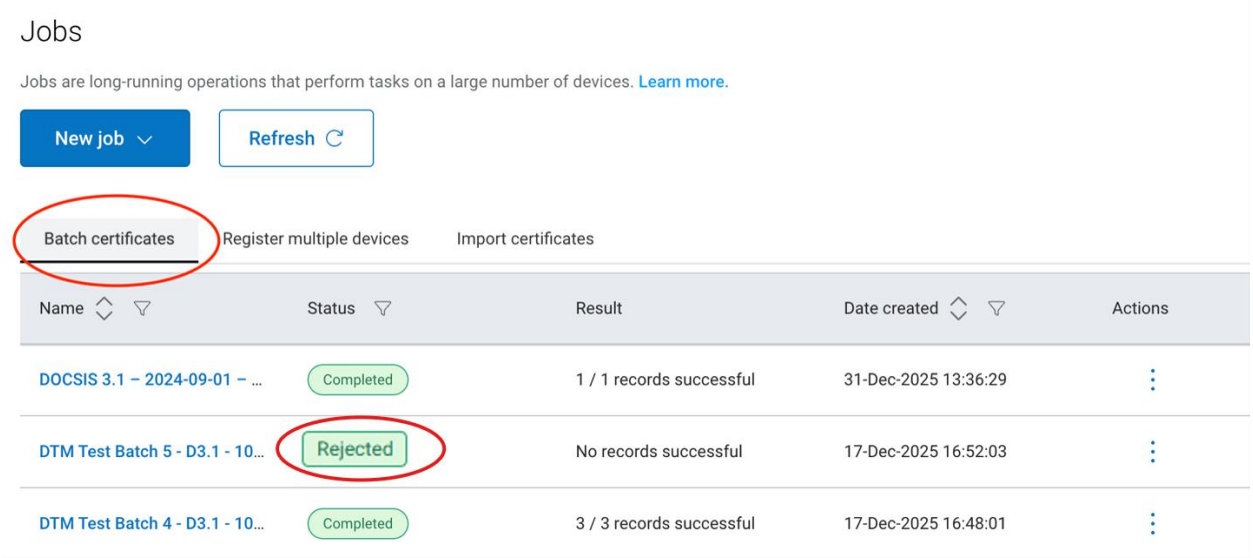


Figure 23 - Batch job status with Rejected jobs

4.3 Downloading Certificates

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

- Click on **Jobs** on the left navigation.
- Click on the batch job you would like to download.
- Click on the download icon (downward blue arrow)
  Note: Once certificates have been Downloaded, they are considered valid and used. Revoking the certificates will not be added back to your balance of available certificates.

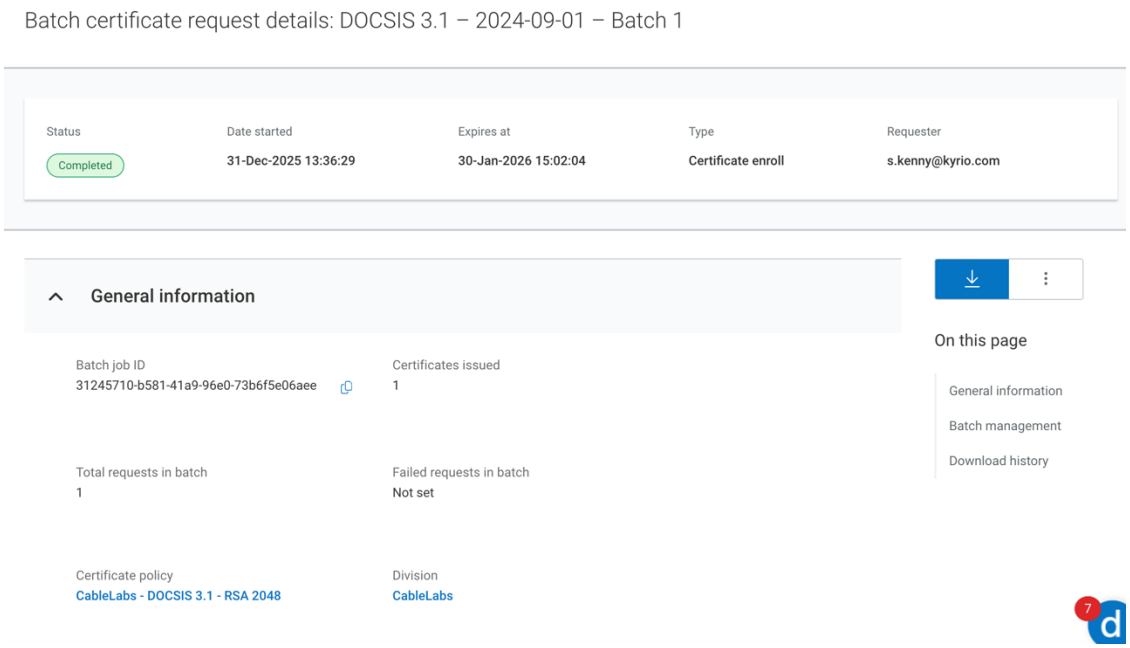


Figure 24 - Batch details screen

- You will be prompted to confirm the download of the certificates (or **Reject** batch). If you want to see the details of the certificates generated to ensure the proper details have been used (e.g. MAC addresses, etc.), click on **Download and view batch report** to see those details *before* completing the download. *Note: Once certificates have been Downloaded, they are considered valid and used. Revoking the certificates will not add them back to your balance of available certificates.*

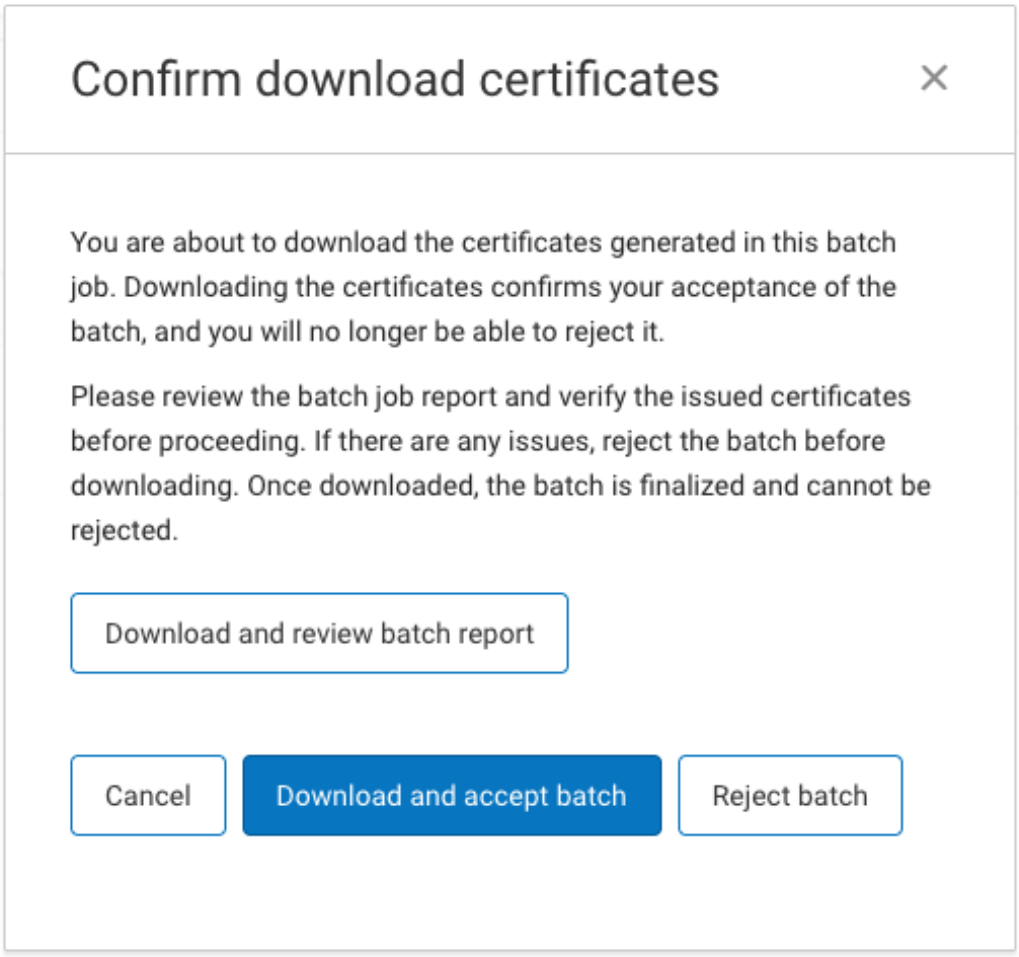


Figure 25 - Batch Download Confirmation.

- The file will be saved to your local machine in the default location for file downloads.
- Open the batch file using your preferred method depending on the download options selected. If you specifically have **SMPB** as the file output format, use the next step to open the file with the PKI Client.

4.3.1 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 26 - Decryption via PKI Client application).

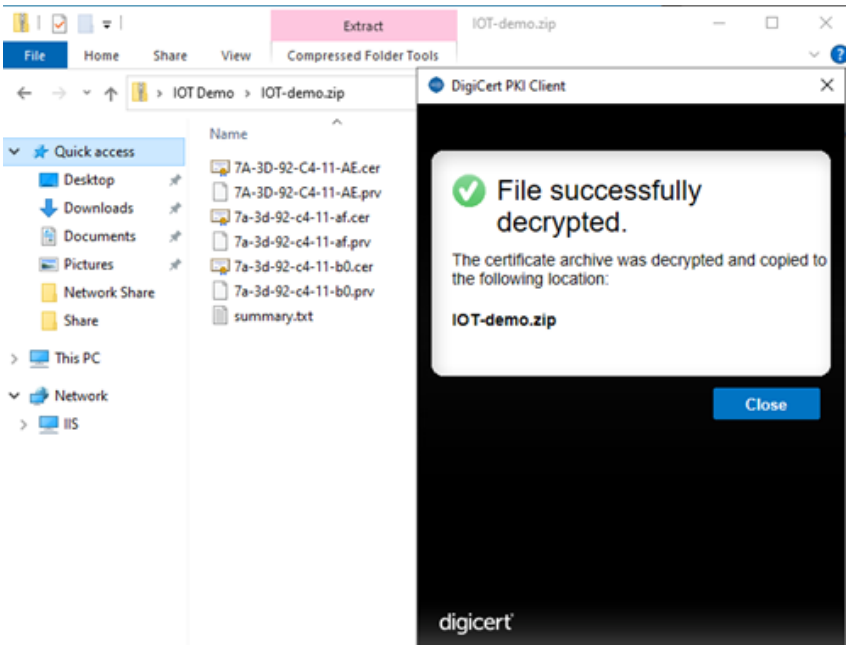


Figure 26 - Decryption via PKI Client application

5 Downloading Root and Intermediate Certificates

The Root and Intermediate (Issuing) CAs are the same as the previous 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 Device Trust Manager (if not already there by default) using the squares menu in the top right of the web page.

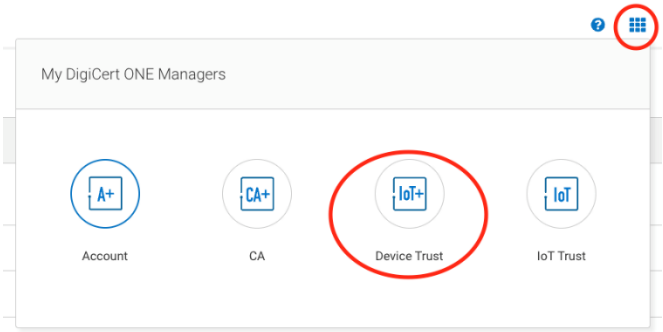


Figure 27 - Access Device Trust Manager

- Click in **Certificate Management** in the left navigation bar
- Click on **Certificates** in the left navigation bar

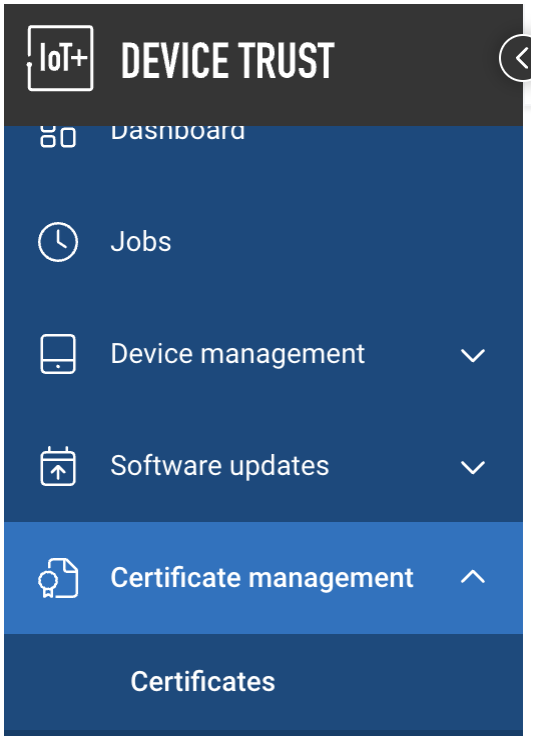


Figure 28 - Left navigation for Certificates

- Click on a link for the **Certificate Value** in the Certificates summary screen

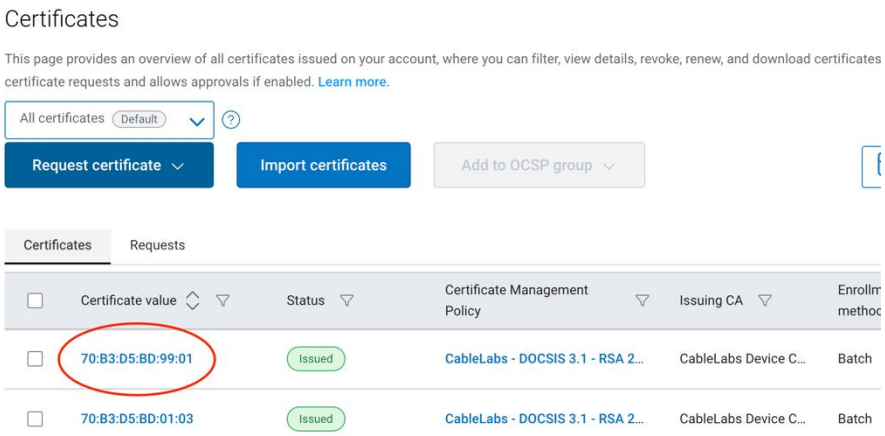
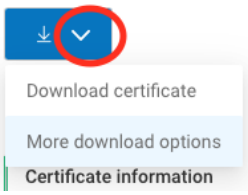


Figure 29 - Click to get details on certificate

- On the certificate details page, click on the downward carat (∨) 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.

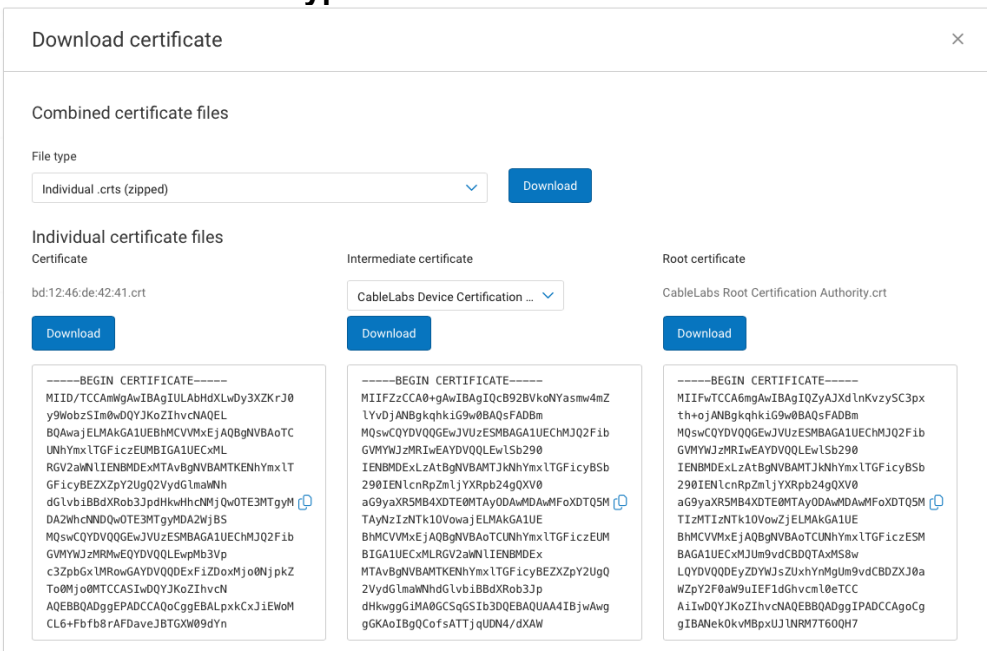


Figure 30 - Certificate Download Options

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

6 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 Device Trust Manager (if not already there by default) using the squares menu in the top right of the web page.

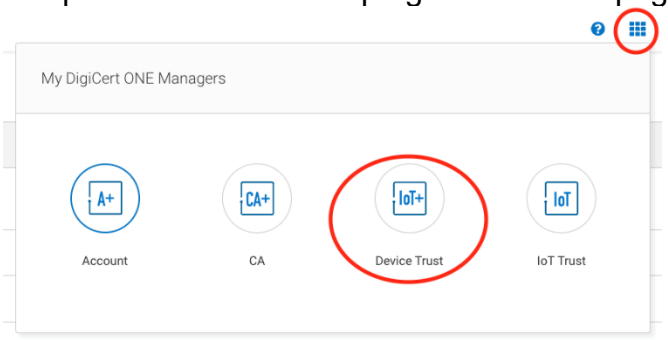


Figure 31 - Access Device Trust Manager

- Click on **Certificate Management** in the left navigation bar
- Click on **Certificates** in the left navigation bar.

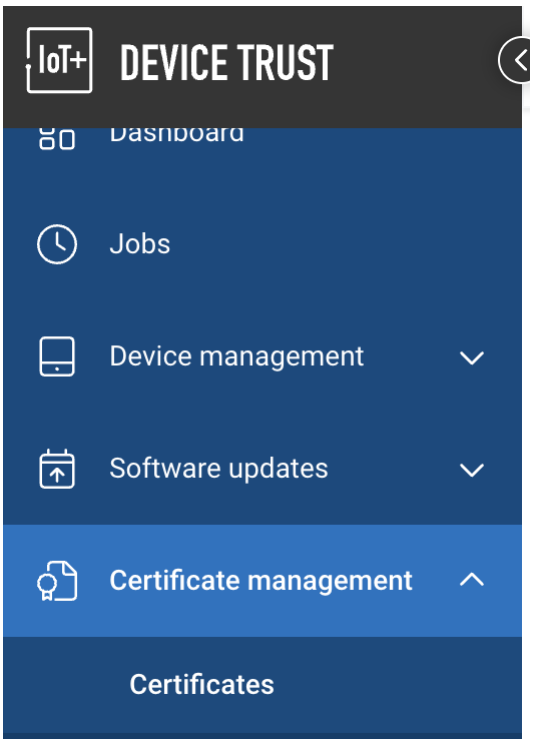


Figure 32 - Left navigation for Certificates

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

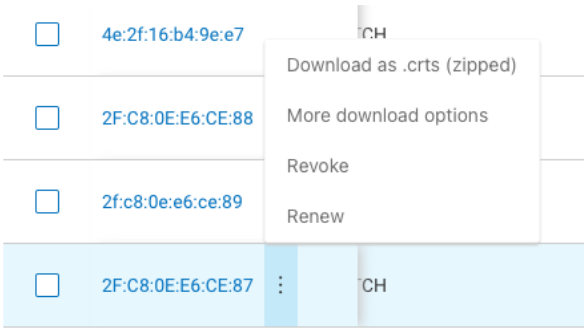


Figure 33 - Individual Certificate Options

- 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**.

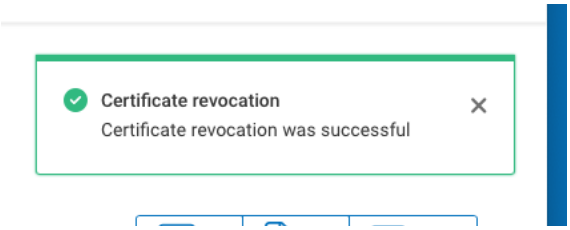


Figure 34 - Cert revocation confirmation message