

User Guide – DigiCert ONE

CableLabs PKI Operations Version: 1.0 Date: October 4, 2024

Table of Contents

User Profile Set-up	2
Password and Authenticator Set-up	2
Authentication Certificate Set-up	4
To use the existing Admin Certificate	4
To create a new authentication certificate	5
General Navigation	6
Check Balances	7
Generating and Downloading New Certificates	8
Downloading Root and Intermediate Certificates	
Revoking Certificates	

User Profile Set-up

Password and Authenticator Set-up

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

- 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

Set up authentication app	
Open the authentication app and scan this barco	de:
Scan not working? Get a setup key	
3	
Enter setup OTP	
Enter the one-time passcode (OTP) provided by t authentication app.	he
One-time passcode (OTP)	

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



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. If desired, you can use your existing Admin Certificate from the Magnum MPKI8 platform or create a new one.

To use the existing Admin Certificate

 \sim

- Scroll down to the Authentication Certificates
- Click on Upload client authentication certificate

Authentication certificates	
Create authentication certificate	Upload client authentication certificate
Filter certificates by	
Valid	~

Figure 4 - Upload authentication certificate

- On the new page enter a nickname for the cert (e.g. John Doe Auth Cert 1)
- Drag the certificate file from your locale computer to the Upload area and click **Upload client authentication certificate**.
- The certificate will show up in your list

Create authentication certificate	Upload client authenticat	tion certific
ter certificates by		
/alid	\checkmark	
John Doe Auth Cert 2 Status Valid	Source DigiCert ONE (internal	
John Doe Auth Cert 2 Status Valid Start date 03-Oct-2024	Source DigiCert ONE (internal CA) End date 01-Oct-2027	
John Doe Auth Cert 2 Status Valid Start date 03-Oct-2024 Serial number	Source DigiCert ONE (internal CA) End date 01-Oct-2027 Intermediate CA	

Figure 5 - List of Authentication Certificates

To create a new authentication certificate

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

Nickname	
End date	
Encryption	
AES (recommended)	~
Signature hash algorithm	
SHA-256 (recommended)	~
Cancel Generate certificate	

Figure 6 - 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. You will need to use this password to open certificate your download.
- Install the certificate in your local key store using the password above.
- The certificate will show up in your list of available certificates to use:

Create authentication certificate	Upload client authenticati	ion certific
Filter certificates by		
Valid	~	
John Doe Auth Cert 2	Source	
John Doe Auth Cert 2 Status Valid	Source DigiCert ONE (internal CA)	
John Doe Auth Cert 2 Status Valid Start date	Source DigiCert ONE (internal CA) End date	
John Doe Auth Cert 2 Status Valid Start date 03-0ct-2024	Source DigiCert ONE (internal CA) End date 01-Oct-2027	
John Doe Auth Cert 2 Status Valid Start date 03-Oct-2024 Serial number	Source DigiCert ONE (internal CA) End date 01-Oct-2027 Intermediate CA	

Figure 7 - List of Authentication Certificates

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.

		0
	My DigiCert ONE Managers	
n@	loT Trust	

Figure 8 - 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**.

dmin Profil	e		
ogout			
	dmin Profil ogout	dmin Profile	dmin Profile

Figure 9 - 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





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 11 - Access IoT Trust Manager

- Click in **Certificates** in the left navigation bar
- To initiate a new batch, select Start batch certificate request

All certificates Default 🗸 🔇	Certificate mar	nagement
	All certificates Defa	ult 🗸
Request certificate Start batch certificate request	Request certificate	Start batch certificate request

Figure 12 - 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 20248

Start batch certificate request
Nickname (optional)
DOCSIS 3.1 - 2024-09-01 - Batch 1
Description (optional)
Enrollment profile
Only enrollment profiles configured to allow batch enrollment are shown.
CableLabs - DOCSIS 3.1 - RSA 2048

Figure 13 - 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)
 - o 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)
O Binary .CER (SMPB)
Batch results log format The log file includes the results of each certificate request in the batch.
O CSV
O 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 14 - Download options

 Select the appropriate authentication certificate to encrypt the certificate package that was set-up under you 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 pro 	ofile
Only eligible certificates are shown in this list	t
PKI Ops Auth Cert 1	~
O Upload certificate or PGP key	
Figure 15 - 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 I will upload CSV with re Generate requests for N	generated? equest info AAC addresses
Starting MAC address	
BD:12:46:DE:42:39	
Number of requests (500,000 maximum)	Increment each address by
10000	1
Cancel Start requ	lest

Figure 16 - 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.

Certificate value \diamondsuit \bigtriangledown	Certificate type $\ensuremath{\bigtriangledown}$	Device 🖓	Device profile \bigtriangledown	Enrollment \bigtriangledown method	Certificate policies	\bigtriangledown	Status 🖓	s
86:6C:A0:BC:52:2B	End entity certificate	86:6C:A0:BC:52:2B	Basic device profile	BATCH			Issued	2

Figure 17 - Certificate Manager screen

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 \diamondsuit \bigtriangledown	Date started \diamondsuit \bigtriangledown	Status 🔷 🖓	Results	Actions
DOCSIS <u>3.1 -</u> 2024-09-01 - Batch <u>1</u>	17-Sep-2024	Completed	10 / 10 records successful	÷

Figure 18 - 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 D Completed 1	Pate started 7-Sep-2024 12:20:03	Date finished 17-Sep-2024 12:20:06	Type Batch key gen MAC	Requestor pkiops@cablelabs.com	
 General information Certificates issued 	Total requests in	ıbatch		⊻ Ø : On this page	
10 Enrollment profile CableLabs - DOCSIS 3.1 - RSA 2	10 File size 2048 0			General information Batch management Download history	

Figure 19 - Batch details screen

• Open the batch file using your preferred method depending on the download options selected.

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.

		0
	My DigiCert ONE Managers	
n@	loT Trust	

Figure 20 - Access IoT Trust Manager

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



Figure 21 - 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.

Download certificate		
Combined certificate files		
ile type		
Individual .crts (zipped)	✓ Download	
ndividual certificate files		
Certificate	Intermediate certificate	Root certificate
d:12:46:de:42:41.crt	CableLabs Device Certification 💙	CableLabs Root Certification Authority.crt
Download	Download	Download
BEGIN CERTIFICATE MIID/TCCAmWgAvIBAgIULAbHdXLwDy3XZKrJ0 y9%ob25Im@wDQYJKoZIhvcNAQEL BQAwajELMAKGAIUEBhMCVVMxEjAQBgNVBAoTC UNHYmx1TGFiczEUMBIGAIUECxHL RGV2aMNIENNBMCEVMTAvBgNVBAMTKENNYmx1T GFicyBEZXZpY2Ug02VydGlmahNH dGlvbiBBdXRob32pdHkwHhcNHjQwOTE3MTgyM QC2WhCNDQwOTE3MTgyMDA2WjBS MQswCQYDQQQEwJVUZESMBAGAIUECHMJQ2Fib GVMYNJ2MRwEQYDVQQDExFIZDoxMjo@NjpkZ T0MMjoMTCA5ILWQYJKoZIhvcN AQEBBQADqeEADC2AOcGBALpxkCxJiEWOM	BEGIN CERTIFICATE MIIFZzCCA0-gAwIBAgIQcB92BVkoNYasmw4mZ LYvD JANBgkqhkiG9w0BAQsFADBm MQswCQYDvQ0GEwJVUZESMBAGAIUEChMJQ2Fib GVMYMJ2MRLWEAYDVQLEwLSb290 IENNMDEXL2AtBqNVBAMTJMHYmxlTGFicyBSb 290IENLcnRpZmljYXRb24gQXV0 aG9yaXRSMB4XDTEGWTAy0DAMDAMHFoXDTQH TAyHZIZMTK10VmajELMAkGALUE BhMCV/MxEjAQBgNVBAOTCLNHYmxlTGFiczEUM BIGAIUECxHRCV2aMtICNMMPX BIGAIUECxHRCV2aMtICNMMPX MTAvBgNVBAMTKENHYmxlTGFicyBEZXZpY2UgQ 2VydGLmaMMhdGVbiBB0XR0b32p	BEGIN CERTIFICATE MIIFWTCCA6mgAwIBAgIQZyAJXdlnKvzySC3px th+ojANBgkqhkiG9wBAQSFADBm MQswCQTDVQQGEwJVU2ESMBAGA1UECHMJQ2Fib GVYMYJ2MRIwEATDVQQLEwISb29 IENBMGEXL2AtBgNVBAMTJNNYmxlTGFicyBSb 290IENIcnRpZnljYXRpb24gQXV0 aG99xXRSMB4XDTEWTAyDDawHF0xDTQSM [TI2MTI2MTk10V0wZjELMAkGA1UE BhMCVVMzEjADBgNVBA0TCUNHYmxlTGFiczESM BAGA1UCCxMJUm9vGCBDTAxHSSw LQYDVQQDEyZDYWJSZUxHYnMgUm9vdCBDZXJ0a wZpYZF0aW01EF1G6hvcmI0eTCC

Figure 22 - 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 23 - 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).

4e:2f:16:b4:9e:e7	CH Download as .crts (zipped)
2F:C8:0E:E6:CE:88	More download options
2f:c8:0e:e6:ce:89	Revoke
2F:C8:0E:E6:CE:87	: сн

Figure 24 - 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**.

9	Certificate revocation Certificate revocation was successful	×
	Certificate revocation was successful	