



User Guide - CommScope PKIWorks

CableLabs PKI Operations

Version: 3.0

Date: August 25, 2025

Table of Contents

| | | |
|----------|---|-----------|
| 1 | <i>Initial set-up and system access</i> | 2 |
| 1.1 | eToken Minidriver Installation (Option 1) | 2 |
| 1.2 | PKIWorks Client Certificate Installation (Option 2) | 7 |
| 1.3 | PKIWorks Client Software Setup | 10 |
| 1.4 | Login and accept access agreement | 13 |
| 2 | <i>General Navigation</i> | 14 |
| 2.1 | Select Account | 14 |
| 3 | <i>Generating and Downloading New Certificates</i> | 16 |
| 3.1 | Generating Certificates | 16 |
| 3.1.1 | Certificate generation by MAC range | 16 |
| 3.1.2 | Certificate generation with user-generated certificate signing request (CSR or PKCS#10) | 19 |
| 3.1.3 | Certificate generation with an upload file | 21 |
| 3.2 | Accessing Certificates | 23 |
| 3.2.1 | Status Description | 23 |
| 3.2.2 | View Requests and Status | 24 |
| 3.2.3 | Download Output File | 25 |
| 3.2.4 | Confirm File Download | 25 |
| 3.2.5 | Decrypting the batch file PKIWorks Client | 26 |
| 4 | <i>Downloading Root and Intermediate Certificates</i> | 32 |
| 5 | <i>Revoking Certificates</i> | 33 |
| 5.1.1 | Subscriber Revocation request | 33 |

1 Initial set-up and system access

There are two options to authenticate and gain access to the PKI Works portal:

1. **eToken Mini Driver.** This is a secure hardware token that needs to be inserted into the computer where the site is being accessed and certificates issued from.
2. **Client Certificate.** This is a digital certificate installed on the computer where the site is being accessed and certificates issued from.

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 eToken Minidriver Installation (Option 1)

PKIWorks requires a secure hardware token for user authentication. The eToken Minidriver must be installed. If the eToken Minidriver is already installed or if a newer version is installed, skip this section Appendix A and proceed to Appendix B.

1. Use the below URL to download the latest version of Thales Minidriver:

https://supportportal.thalesgroup.com/csm?sys_kb_id=c23ea51137bf7284cc47261953990e62&id=kb_article_view&sysparm_rank=4&sysparm_tsqueryId=e7ac37c5db38105491a9742339961961&sysparm_article=KB0016030

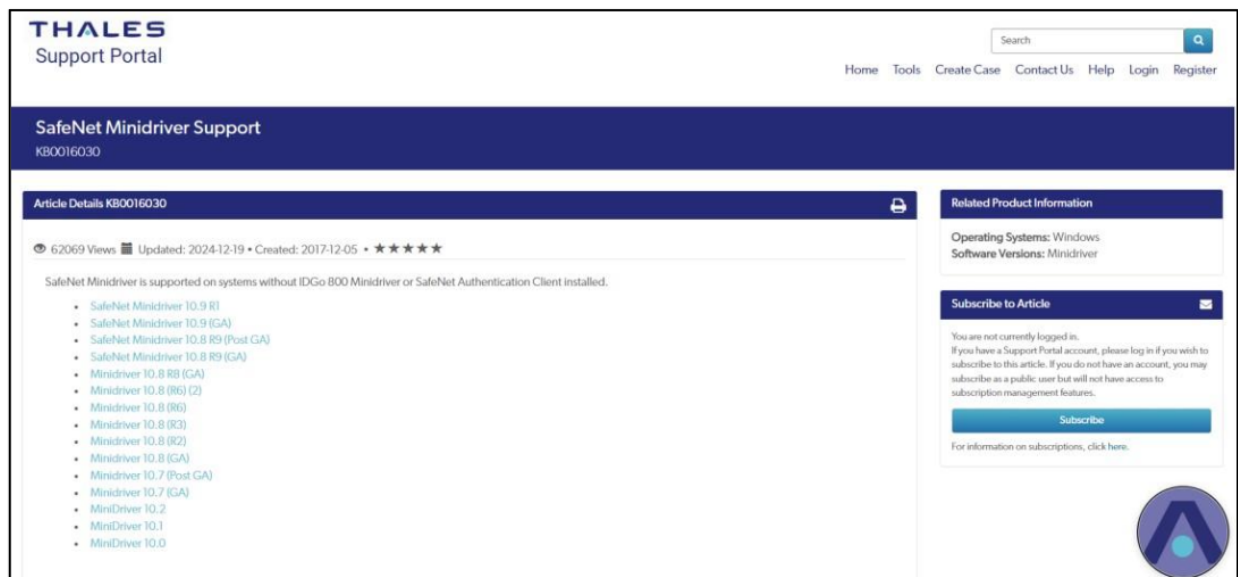


Figure 1 - Available list of eToken Minidrivers

2. Click on the latest minidriver link and DOWNLOAD.

Article Details KB0028458

7138 Views Updated: 2024-09-03 • Created: 2024-04-16

SafeNet Minidriver 10.9

SafeNet Minidriver is a simple alternative to developing a legacy cryptographic service provider (CSP) by encapsulating the complex cryptographic operations from the card Minidriver vendor. SafeNet Minidriver presents a consistent interface between Thales PKI authenticators and Microsoft's Smart Card Base Cryptographic Service Provider (CSP) or Crypto Next Generation (CNG) Key Storage Provider (KSP) and to the Smart Card Management Interface).

Following are the features included in this release:

- SnapDragon CPU support
- External PIN Pad readers through SAC
- Openssl 3.0 upgrade
- Major security enhancements
- SafeNet Minidriver 10.9 also features support for CC cards in Linked Mode.
- Smartcard Minidriver Certification with below mentioned versions.

| Microsoft Certified Minidriver | |
|--------------------------------|---------------------------|
| Intel Minidriver | ARM Minidriver |
| SIS MD 10.9.3120 | SIS MD ARM 10.9.3120 |
| IDPrime MD 10.9.3120 | IDPrime MD ARM 10.9.3120 |
| eToken MD 10.8.82.0 | eToken MD ARM 10.8.2719.0 |

 Click here to download file: [DOW0009693](#)

md5hash: 1773469858038b1cb72cd119795ab10d
 Filename: SafeNet Minidriver 10.9 GA.zip
 File Size: 31.50 MB

Figure 2 - Minidriver download link

3. A zip file is downloaded, and an informational pop-up may be displayed.
4. Go to the downloads folder and unzip the zip file. The unzipped folder contains executables. Depending upon the machine's preference, choose x32 bit or x64 bit file

C:\Downloads\SafeNet Minidriver 10.9 GA\SafeNet Minidriver 10.9 GA\MSI

5. Double click on the .msi file or right click and click INSTALL.
6. Click **NEXT**.



Figure 3 - Installation wizard for Minidriver

7. Accept License Agreement.



Figure 4 - Accept License Agreement

8. eToken minidriver installation is ready to install. Click **INSTALL**.

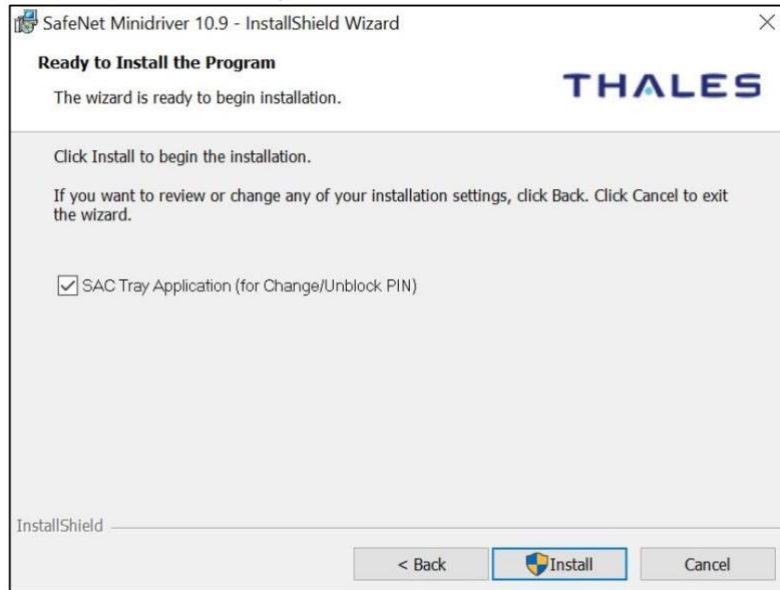
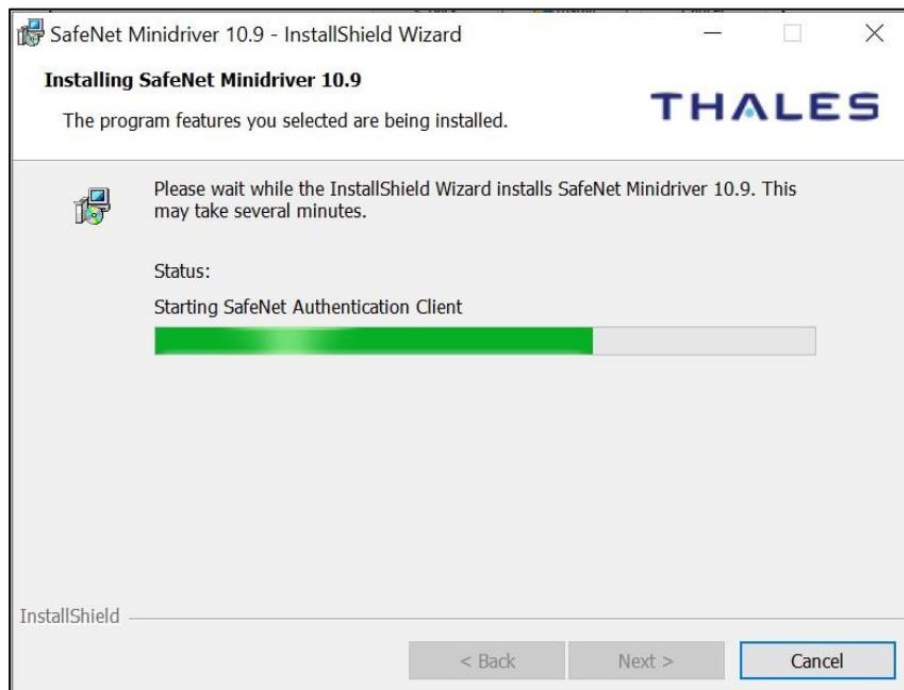


Figure 5 - eToken Installation Ready

9. Wait while the eToken Driver is being installed.



10. Click **Finish** to complete the installation process.

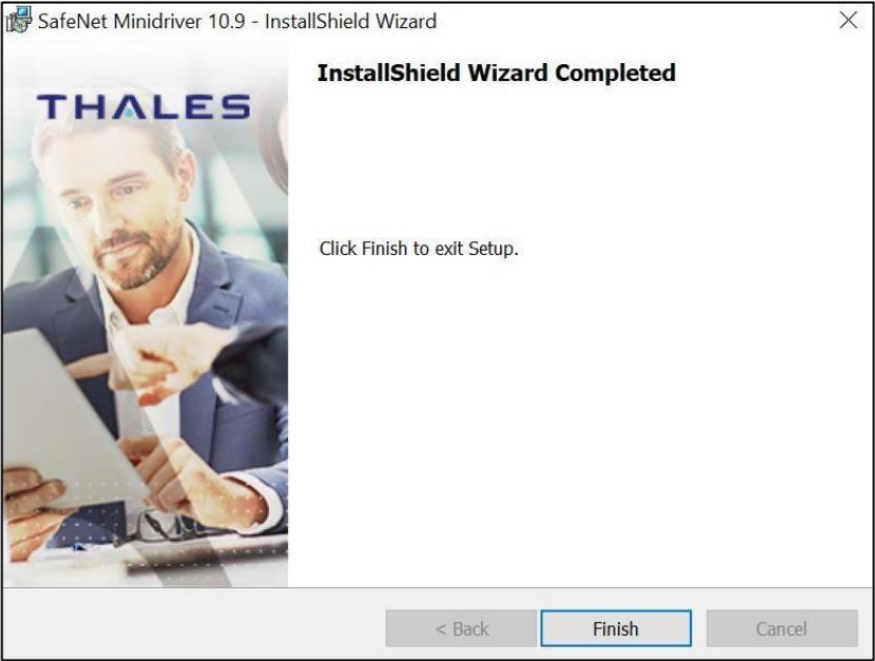


Figure 6 - eToke Installation complete

1.2 PKIWorks Client Certificate Installation (Option 2)

PKIWorks requires the installation of certificates prior to using the web site.

1. From the CommScopePKIWorksClient zip file, double click the ARRIS PKI Center Certificate Setup.exe.
2. The Certificate Installer begins. Click Run at the Security Warning if prompted.

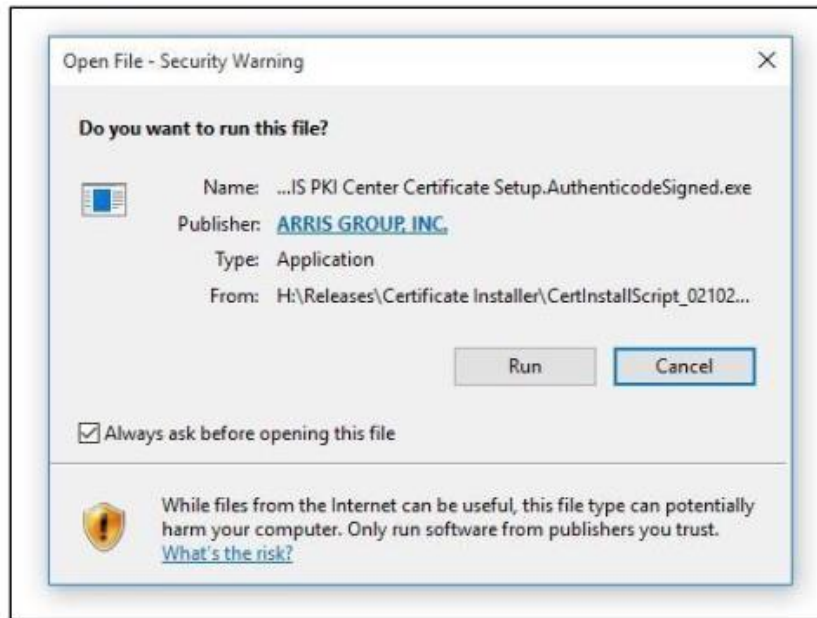


Figure 7 - Open File - Security Warning

3. Click Next at the Welcome window.



Figure 8 - Certificate Installer Welcome

4. To continue the installation, click Install.

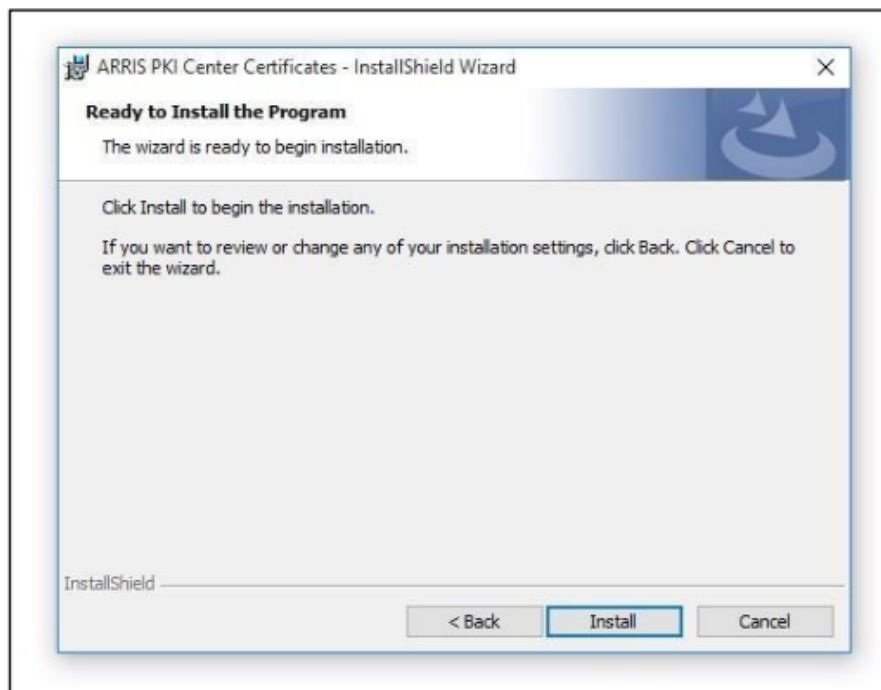


Figure 9 - Ready to Install

5. Click **Finish** to complete the installation process.

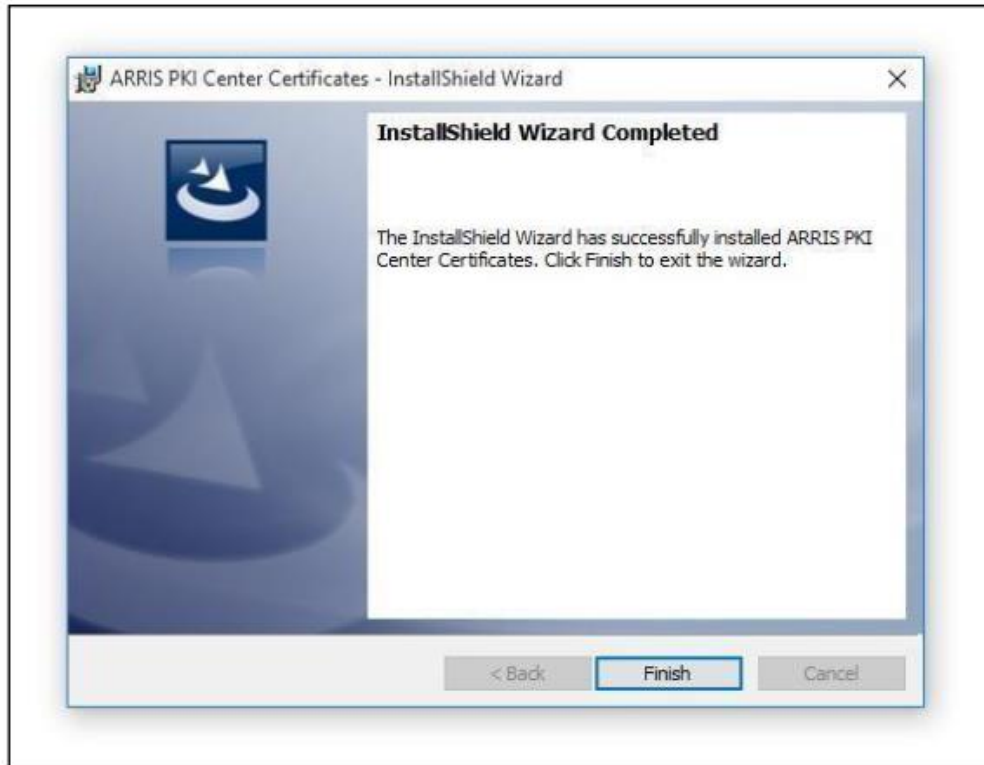


Figure 10 - Certificate Install Completed

Note: If your anti-virus software has a false detection or false positive during certificate installation, configure the anti-virus software to allow the installation to execute.

1.3 PKIWorks Client Software Setup

PKIWorks Client requires a secure hardware token for user authentication. The eToken Driver must be installed. Refer to **eToken Minidriver** above for details.

This section will walk you through the steps needed to install PKIWorks Client.

1. From the CommScopePKIWorksClient zip file, open the PKIWorks Client folder.
2. Double click on PKIWorks Client Setup.exe to begin the installation of PKIWorks Client. *Note: This installation will also install visual c++ redistributables and .net framework 4.8 as part of installation if not already installed.*

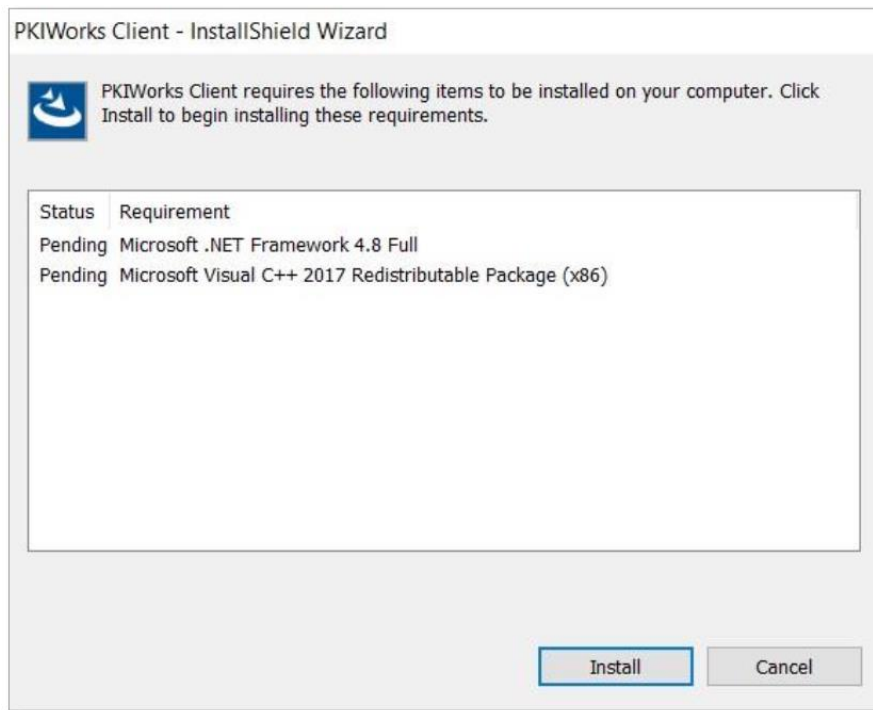


Figure 11 - C++ and .Net prerequisites prior to installation

3. The installer will guide you through the set-up process

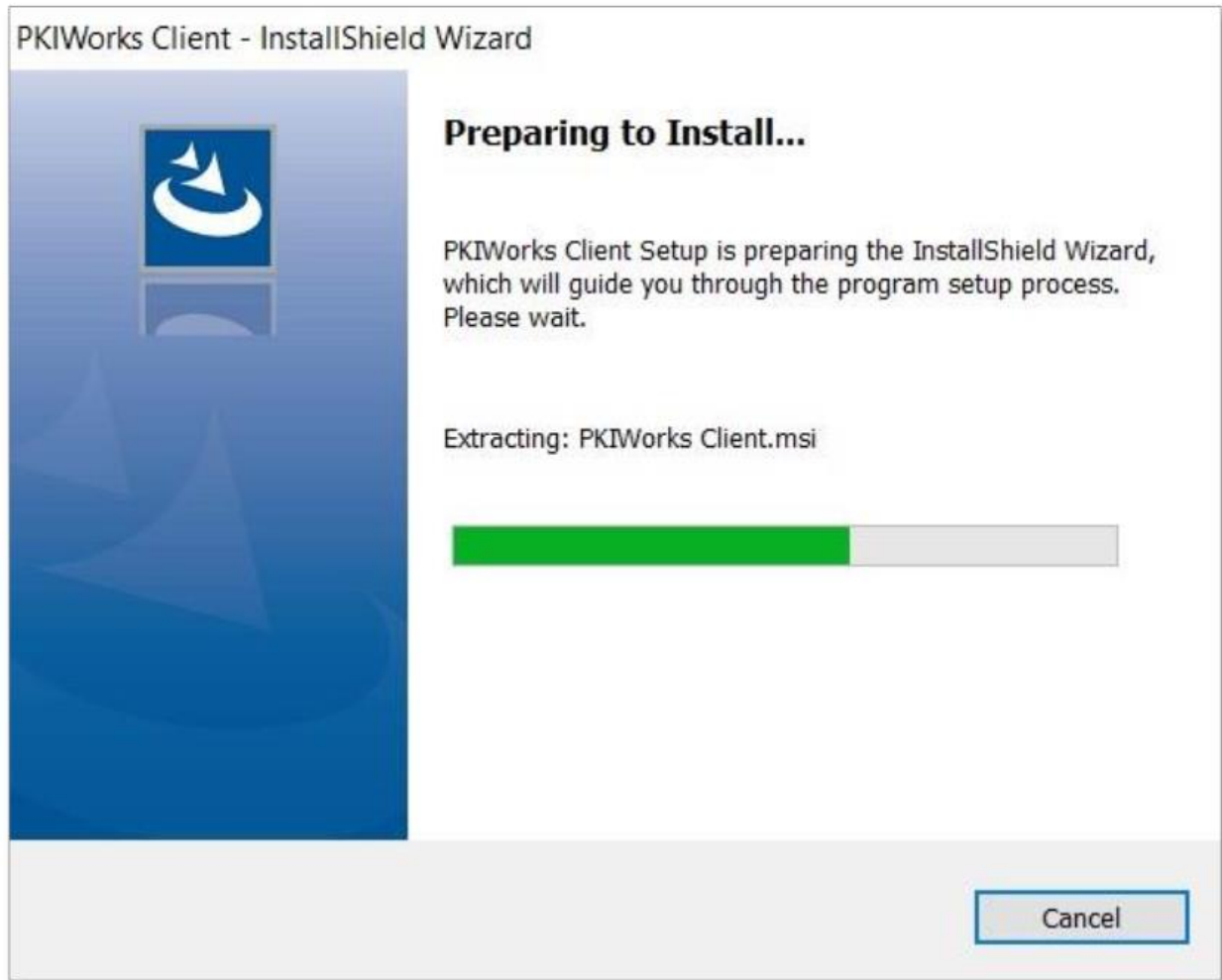


Figure 12 - Prepare to install

4. Accept the terms of the license agreement and click **Next**.

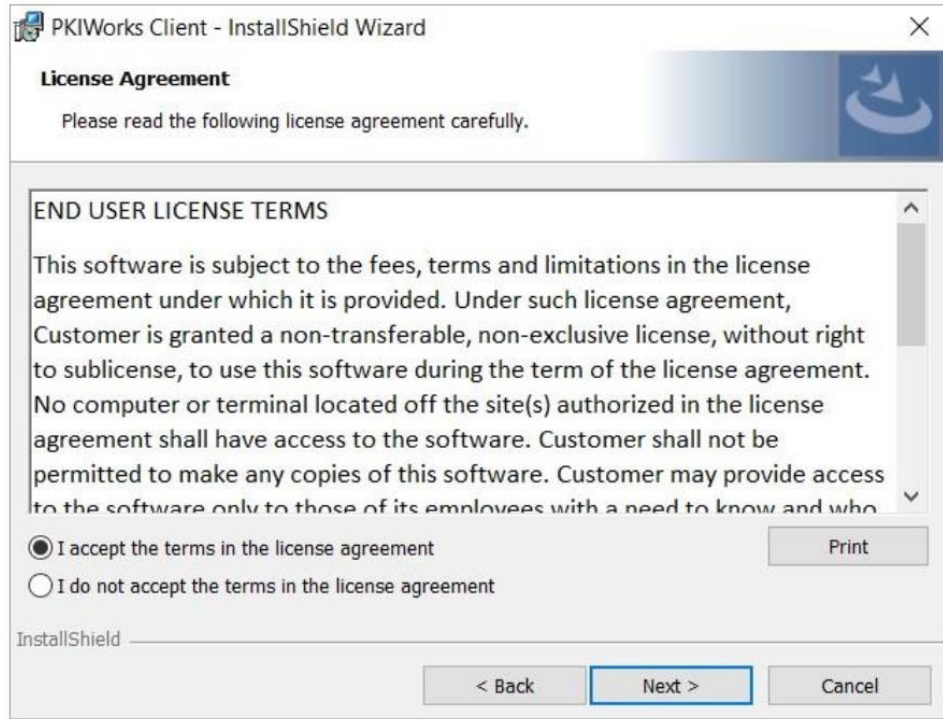


Figure 13 - End user license agreement

5. Click the Install button to start the installation.

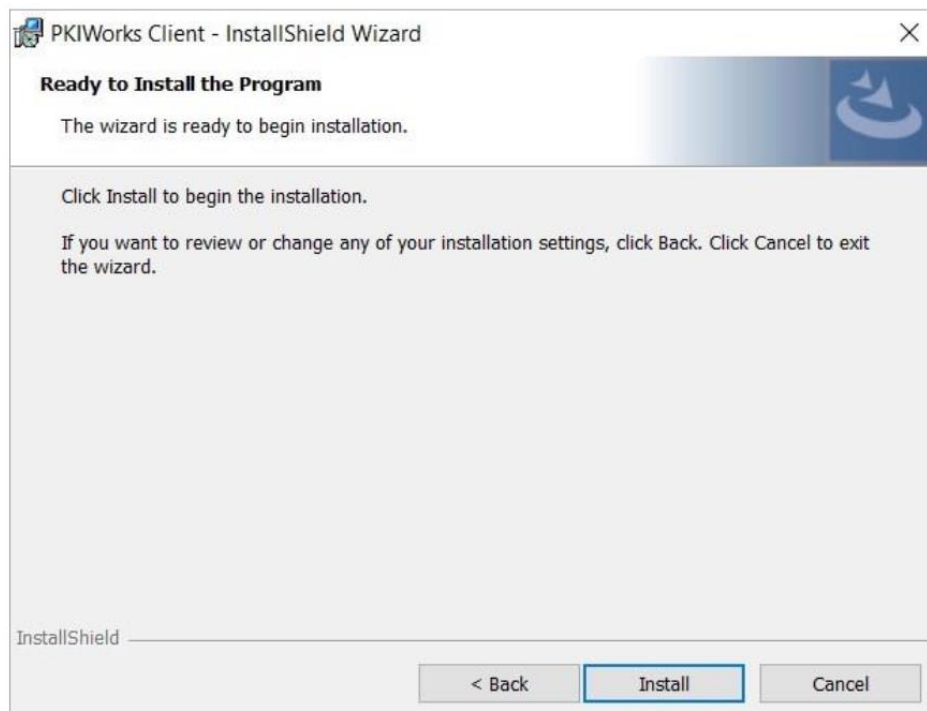


Figure 14 - PKIWorks Client Ready to Install Screen

6. Click Finish to complete the installation process.

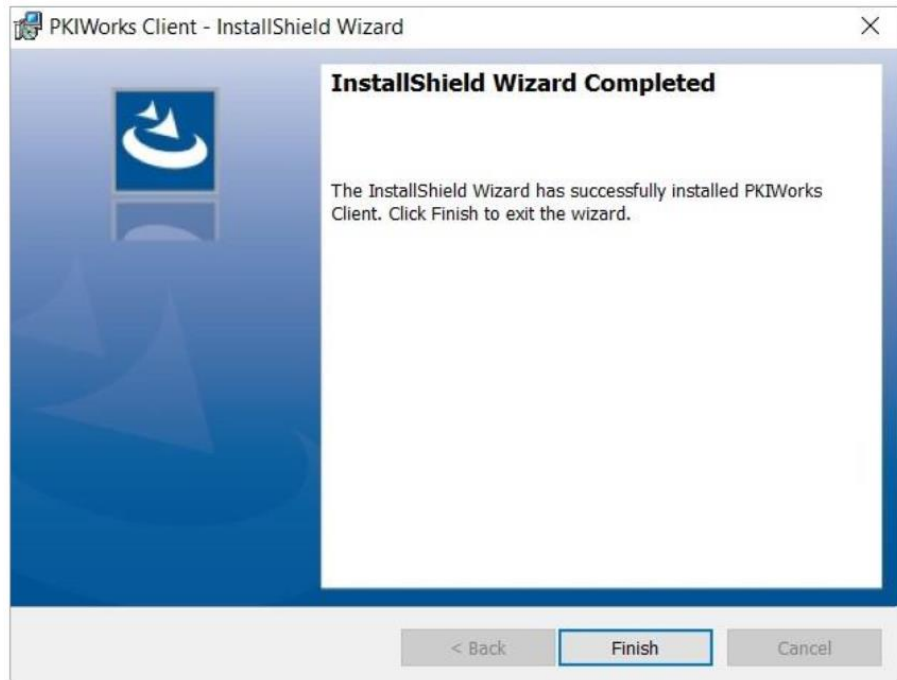


Figure 15 - PKIWorks Client Installation Completed.

1.4 Login and accept access agreement

For token login, login to the PKIWorks Basics portal at <https://cert.pkiworks.com> using the received eToken, and acknowledge the access agreement to begin.

The browsers supported include Microsoft Edge, Google Chrome, and Mozilla Firefox.

2 General Navigation

2.1 Select Account

After logging in and agreeing to the access agreement, a dialog box appears showing the User's authorized accounts along with their expiry dates if applicable. Also shown are the User's Company accounts along with their expiry dates if applicable. The User can select any active account and can perform all actions like submitting, viewing, or downloading requests. If either the User account or the Company account are expired, contact pkiops@cablelabs.com for assistance.

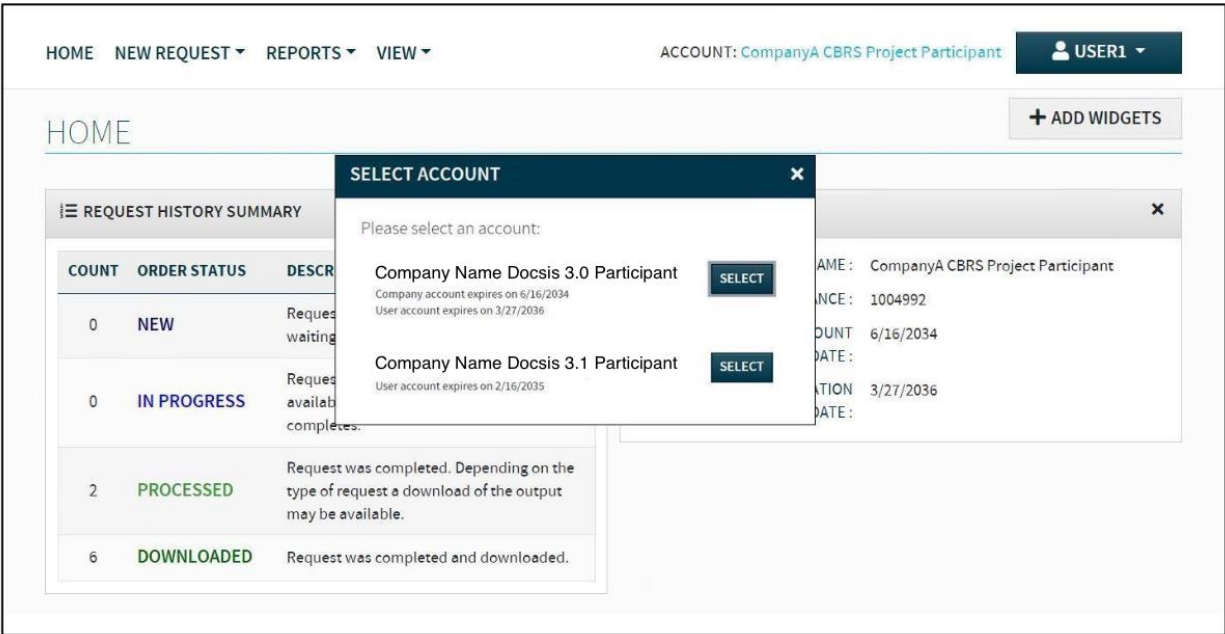


Figure 16 - Select Account

After selecting an account, Home screen of the selected account is displayed. Home screen shows the **Account Summary** and **Request History Summary**. Account Summary section displays the selected Account Name, Remaining Balance, Company Account Expiration Date if specified, and the User Account Expiration Date if specified. Request History Summary shows the number of orders/requests that were submitted for the account, and brief order status description. To view the details of these orders you must be in the specific account in which the order was placed.

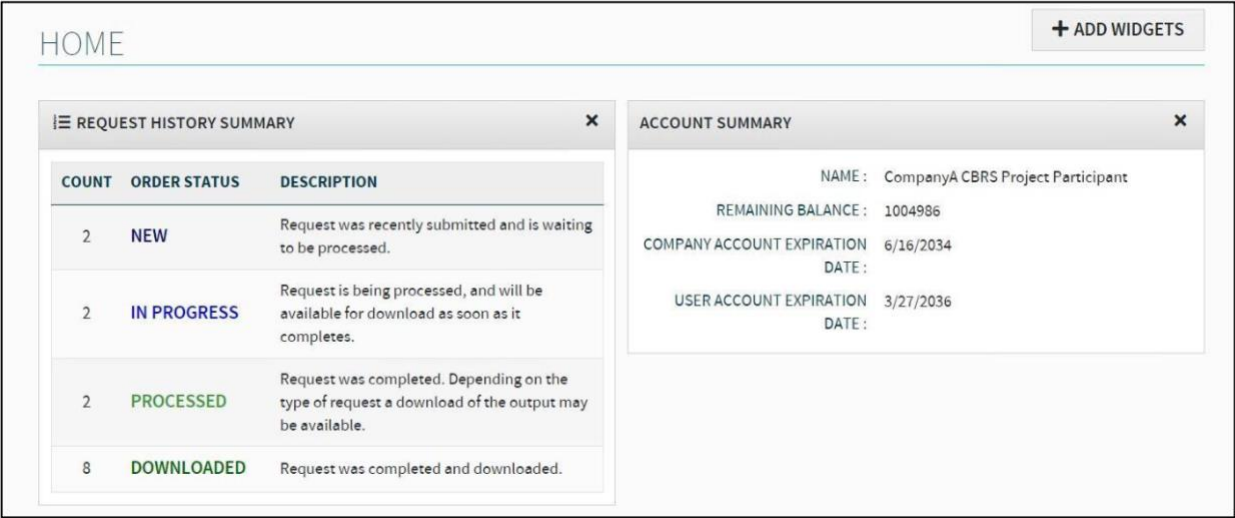


Figure 17 – Home Screen

3 Generating and Downloading New Certificates

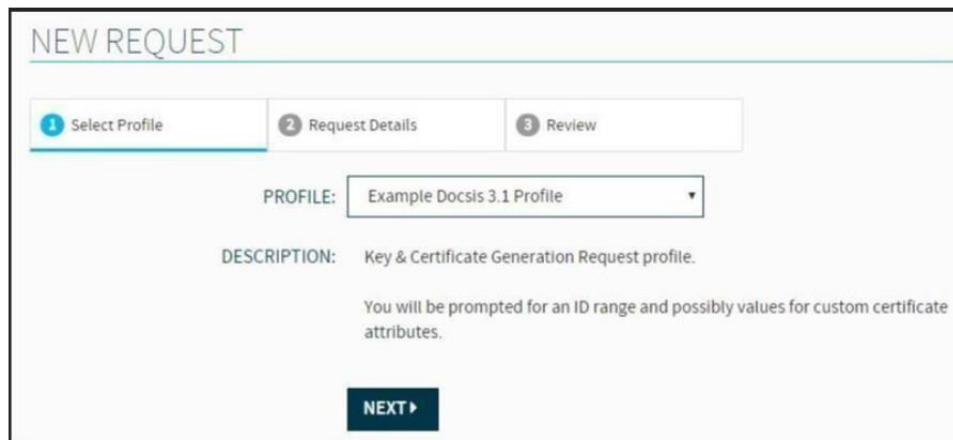
To create a new request, go to the New Request Menu and select +Key and Certificate Generation Request. Next, select a profile. By default, each account is pre-configured with one profile; the profile configuration determines the request type to be submitted, as described below. To request additional profiles, please contact pkioops@cablelabs.com. Depending on the configuration of the profile, refer to the following sections for the next step:

3.1 Generating Certificates

3.1.1 Certificate generation by MAC range

Note: PKIWorks Client software must be installed to decrypt these keys.

This request is used to generate key(s) and certificate(s) for one or more IDs. First, select a profile. When selected, the profile and a brief description are displayed.



NEW REQUEST

1 Select Profile 2 Request Details 3 Review

PROFILE: Example Docsis 3.1 Profile

DESCRIPTION: Key & Certificate Generation Request profile.

You will be prompted for an ID range and possibly values for custom certificate attributes.

NEXT >

Figure 18 – Profile Description

After selecting the appropriate profile, click **Next** to fill in the request details. Complete the following fields, as illustrated in Figure 19.

7. **Description**, this field is an optional description of the request. Enter any desired text.
8. **CA Cert**, this field is prepopulated with the CA cert that matches the selected profile.
9. If the request is for IEEE MAC, select **CLICK TO SHOW RANGES** link to see what ranges are available. This will show a list of MAC address ranges that have been assigned for use by this profile.
 1. **Available** is the remaining balance for the account. If it is lower than the requested amount, please contact pkioops@cablelabs.com for assistance.
 2. **Certificate Quantity**, enter the number of certificates requested. (100,000 is the maximum quantity in one batch)

3. **Start Address** is a required field. Specify the MAC address range for this request by entering a chosen start address or select the Get Next Available button to automatically populate this field.
4. **End Address** will be calculated and displayed automatically. The address must be a 12-digit hex string, e.g., 0000010001B0.
10. **Remaining**, this field shows the account balance after deducting this order's certificate quantity.
11. **Country**, **Organization** and **OU** are the custom variables for this profile. If the selected profile has any variables, they will appear in this section. In this example, all these fields are required, but some may already have pre-populated values that are displayed for information. Fill in any variable fields that do not already have a value specified.

Click on the **Review** button to review the request, then click **NEW ORDER** to submit the request.

NEW REQUEST

1 Select Profile

2 Request Details

3 Review

CURRENT PROFILE:

Example Docsis 3.1 Profile

DESCRIPTION:

CA CERT:

TestDocsisSubCA

ADDRESS TYPE:

MAC

ACCEPTED ADDRESSES:

CLICK TO SHOW RANGES

AVAILABLE:

899489

CERTIFICATE QUANTITY:

150

REMAINING:

899339

START ADDRESS:

10000000C350

GET NEXT AVAILABLE

END ADDRESS:

10000000C3E5

COUNTRY:

ORGANIZATION:

OU:

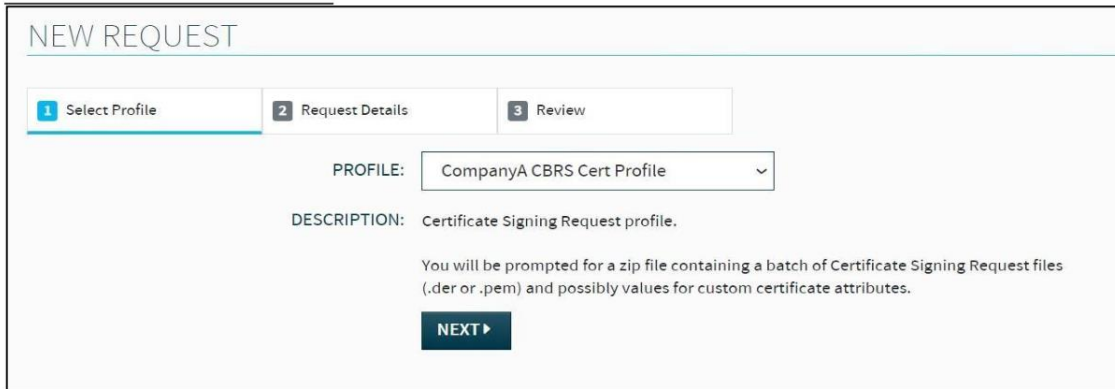
BACK

REVIEW

Figure 19 - Key and Certificate Request Details for MAC, etc.

3.1.2 Certificate generation with user-generated certificate signing request (CSR or PKCS#10)

This request is used to generate one or more certificates based on user-provided certificate signing request(s). First, select a profile. When selected, the profile and a brief description are displayed.



NEW REQUEST

1 Select Profile 2 Request Details 3 Review

PROFILE: CompanyA CBRS Cert Profile

DESCRIPTION: Certificate Signing Request profile.

You will be prompted for a zip file containing a batch of Certificate Signing Request files (.der or .pem) and possibly values for custom certificate attributes.

NEXT ▶

Figure 20 - Profile Description

After selecting the appropriate profile, click **Next** to fill in the request details. Complete the following fields, as illustrated in Figure 21.

1. **Description**, this field is an optional description of the request. Enter any desired text.
2. **CA Cert**, this field is prepopulated with the CA cert that matches the selected profile.
3. If the selected profile has any variables, they will appear in this section. In this case, all the subject fields are pre-populated. Fill in any variable fields that do not already have a value specified.
4. **Request Input**, the user must select the request file. This can be either a zip file with one or more certificate requests or a single certificate request in DER format.

Click on the **Review** button to review the request, then click **“NEW ORDER”** to submit the request.

NEW REQUEST

1 Select Profile

2 Request Details

3 Review

CURRENT PROFILE:

CompanyA CBRS Cert Profile

DESCRIPTION:

Requesting 10 certificates for Company A
CBRS Cert Profile

CA CERT:

Test_CBRS_RSA_Mfr_CA0002

COUNTRY:

US

ORGANIZATION:

ARRIS Group, Inc.

ORGANIZATIONAL UNIT:

WinnForum CBSD Certificate

REQUEST INPUT:

Upload one or more batch files (.zip) or a single CSR file (.csr, .pem, .der, or .p10)

SELECT FILE(S)...

CompanyA CBRS Cert Profile-122213457891011-p10.zip

Successfully uploaded the file

Remove

Cut & paste single PEM request

BACK

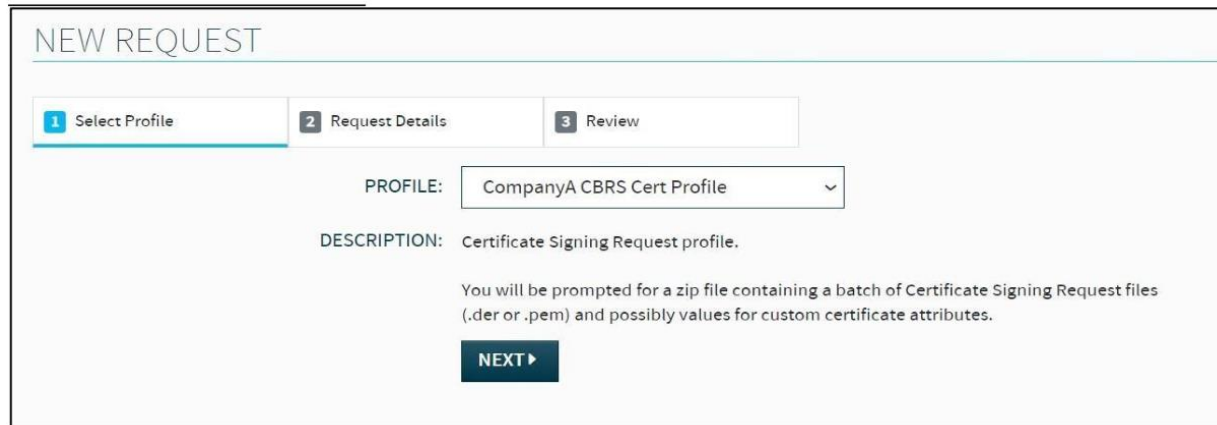
REVIEW

Figure 21 - Certificate Request Details

3.1.3 Certificate generation with an upload file

This request is used to generate PKCS#12 files for one or more IDs provided as a CSV list of MAC addresses or a manual list of MAC addresses.

First, select a PKCS#12 profile. When selected, the profile and a brief description are displayed (See Figure 22)



NEW REQUEST

1 Select Profile 2 Request Details 3 Review

PROFILE: CompanyA CBRS Cert Profile

DESCRIPTION: Certificate Signing Request profile.

You will be prompted for a zip file containing a batch of Certificate Signing Request files (.der or .pem) and possibly values for custom certificate attributes.

NEXT ▶

Figure 22 - Profile Description

After selecting the appropriate profile, click **Next** to fill in the request details. Complete the following fields:

1. **Description**, this field is an optional description of the request. Enter any desired text.
2. **CA Cert**, this field is prepopulated with the CA cert that matches the selected profile.
3. **Request Input**, Submit PKCS#12 requests by uploading a CSV or text file containing up to 100K ID entries (Figure 23), or by entering up to 100 IDs on the form (Figure 24)
4. **Password**, Enter a password for private key encryption. The password must contain:
 1. At least 8 characters in length
 - AND
 2. 1 letter, 1 digit AND 1 special character (@\$!%*#?&)

PKCS#12 files will not be generated if ID is invalid according to validation policy. Note that if multiple PKCS#12 files are generated, the same password applies to all the generated PKCS#12 files.

5. **Country, Organization and OU** are the custom variables for this profile. If the selected profile has any variables, they will appear in this section. In this example, all these fields are already pre-populated values that are displayed for information. Fill in any variable fields that do not already have a value specified.

NEW ORDER

1 Select Profile ✓

2 Request Details

3 Review

CURRENT PROFILE: Example Docsis P12 Profile

DESCRIPTION:

CA CERT: TEST_CABLELABS_MFG_CA_CABLE<

COUNTRY: US

ORGANIZATION: CS

ORGANIZATIONAL UNIT: KGF

REQUEST INPUT: ☒ Upload a file containing up to 100,000 IDs (.csv or .txt)

☐ Enter 1 to 100 IDs

PASSWORD: ⓘ

CONFIRM PASSWORD:

Figure 23 - PKCS#12 File Upload Details

NEW ORDER

1 Select Profile ✓ 2 Request Details 3 Review

CURRENT PROFILE: Example Docsis P12 Profile

DESCRIPTION:

CA CERT: TEST_CABLELABS_MFG_CA_CABLE()

COUNTRY: US

ORGANIZATION: CS

ORGANIZATIONAL UNIT: KGF

REQUEST INPUT: ☐ Upload a file containing up to 100,000 IDs (.csv or .txt)

☒ Enter 1 to 100 IDs

PASSWORD: ⓘ

CONFIRM PASSWORD:

Figure 24 - PKCS#12 Request with List of IDs entered

3.2 Accessing Certificates

PKIWorks Basics sends an email notification after the new request is processed and ready to download.

The PKIWorks Basics website also shows the status of each new request.

3.2.1 Status Description

A request goes through several states over time. Here is an explanation of these states:

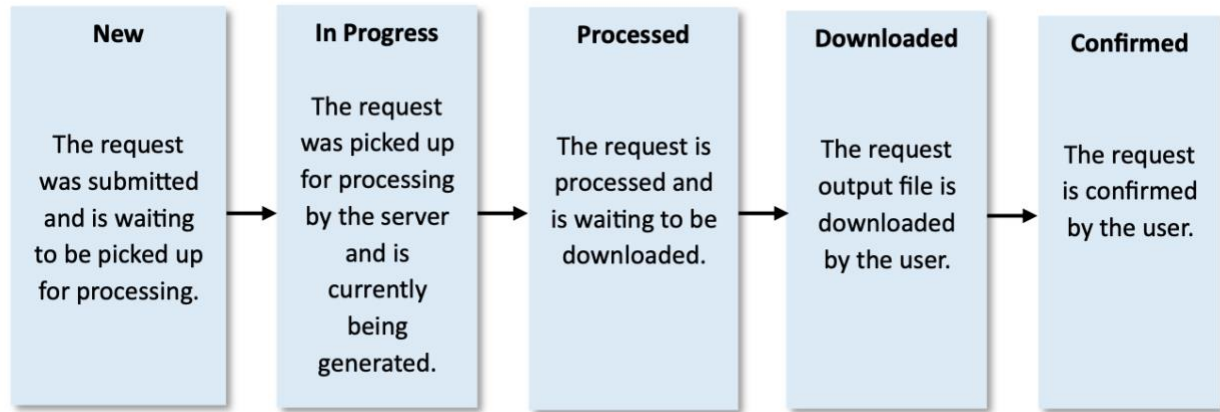


Figure 25 - Certificate Requests Statuses

3.2.2 View Requests and Status

Click on the View Requests tab to monitor the progress of requests, view past requests, view their details, or download them.

To check the updates for new requests, click on the **Refresh Now** button. Alternatively, check the **AutoRefresh** checkbox to automatically refresh the status every minute. Click on the arrow to the left to view the request details.

Depending on the size of the request, it may take a considerable amount of time to process. PKIWorks Basics sends an email notification (or backup email notification if set up for the account) when the request has been processed.

ACTUAL/REQUESTED QTY shows the number of certificates generated vs number of certificates requested. If a request zip file contains invalid CSRs, the certificate generation will be skipped for those invalid CSR files and certificates are generated for the rest of the valid CSR files.

| | REQUEST ID | TYPE | STATUS | ACTUAL/REQUESTED QTY | DATE SUBMITTED (UTC) | ACTIONS |
|---|-----------------|--------------------|-------------|----------------------|-----------------------|--|
| ✓ | 339346144715301 | Cert | NEW | 0/32 | 6/3/2025 9:57:00 PM | |
| ✓ | 339346134854901 | Cert | PROCESSED | 25/25 | 6/3/2025 9:56:00 PM | DOWNLOAD |
| ✓ | 3393461179238 | Cert & Private Key | IN PROGRESS | 0/10000 | 6/3/2025 9:53:00 PM | |
| ✓ | 3393461080898 | P12 | PROCESSED | 11/11 | 6/3/2025 9:51:00 PM | DOWNLOAD |
| ✓ | 3393460681720 | P12 | DOWNLOADED | 4/4 | 6/3/2025 9:47:00 PM | DOWNLOAD CONFIRM |
| ✓ | 3393449347713 | CRL | PROCESSED | 1/1 | 6/3/2025 6:36:00 PM | |
| ✓ | 3393448890798 | CRL | PROCESSED | 1/1 | 6/3/2025 6:28:00 PM | |
| ✓ | 339283645446801 | Cert | CONFIRMED | 5/5 | 5/27/2025 4:21:00 PM | |
| ✓ | 3392256727670 | Cert & Private Key | CONFIRMED | 10/10 | 5/20/2025 11:19:00 PM | |
| ✓ | 3392256297543 | Cert & Private Key | DOWNLOADED | 0/10 ⚠ | 5/20/2025 11:12:00 PM | DOWNLOAD CONFIRM |

Figure 26 - View Requests

3.2.3 Download Output File

Once the request has been processed, if there is a corresponding file to download, a download icon will appear. Click on the download icon to begin downloading.

The browser will prompt to download the file. Download the file to a safe location. If it is a Cert and Private Key request, run the PKIWorks client to decrypt the key(s). Please refer to the PKIWorks Client Installation and User Guide, included in your admin kit, for instructions.

Depending on browser and network security settings, the file download may be initially blocked. If so, after the initial block, click the Download button again. To avoid this, refer to the browser settings to enable file downloads from PKIWorks Basics and make it a trusted site.

In case some of the certificates skipped generation due to invalid CSR files in the request zip file, an error log text file is included in the downloaded output file. The error log file provides details on why the certificates are not generated.


| REQUEST ID | TYPE | STATUS | ACTUAL/REQUESTED QTY | DATE SUBMITTED (UTC) | ACTIONS |
|--------------------|--------------------|--|----------------------|-----------------------|-----------------------|
| 3244704248645 | Cert & Private Key | PROCESSED | 3/3 | 9/16/2020 4:31:00 AM | DOWNLOAD |
| 3244704184457 | Cert & Private Key | <div> <div>Opening pkiworks-3244704184457.zip</div> <div>You have chosen to open:</div> <div>  pkiworks-3244704184457.zip which is: Compressed (zipped) Folder (5.9 KB) from: https://cert.staging.pkiworks.com </div> <div> What should Firefox do with this file? <input checked="" type="radio"/> Open with Windows Explorer (default) <input type="radio"/> Save File </div> <div> <div>OK</div> <div>Cancel</div> </div> </div> | 3/3 | 9/16/2020 4:30:00 AM | DOWNLOAD CONFIRM |
| 3244704052125 | Cert & Private Key | | 3/3 | 9/16/2020 4:28:00 AM | DOWNLOAD |
| 3244695401794 | Cert & Private Key | | 3/3 | 9/16/2020 2:03:00 AM | DOWNLOAD |
| 3244655448619 | Cert & Private Key | | 3/3 | 9/15/2020 2:58:00 PM | DOWNLOAD CONFIRM |
| Bulk-3244596127272 | Cert | | 15/15 | 9/14/2020 10:29:00 PM | BULK DOWNLOAD |
| Bulk-3244595757132 | Cert | | 15/15 | 9/14/2020 10:23:00 PM | BULK DOWNLOAD |
| Bulk-3244595629195 | Cert | | 15/15 | 9/14/2020 10:20:00 PM | BULK DOWNLOAD CONFIRM |
| 3244237189174 | Cert & Private Key | CONFIRMED | 3/3 | 9/10/2020 6:47:00 PM | DOWNLOAD CONFIRM |
| 323983941265201 | Cert | | 15/15 | 7/21/2020 9:10:00 PM | |

Figure 27 - Download output file dialog

3.2.4 Confirm File Download

An action labeled CONFIRM will appear in the ACTIONS column once the file has been downloaded.

| MITTED (UTC) | ACTIONS |
|--------------|--|
| :57:00 PM | |
| :56:00 PM | DOWNLOAD |
| :53:00 PM | |
| :51:00 PM | DOWNLOAD |
| :47:00 PM | DOWNLOAD CONFIRM |
| :36:00 PM | |
| :28:00 PM | |
| 4:21:00 PM | |
| 11:19:00 PM | |
| 11:12:00 PM | DOWNLOAD CONFIRM |

Figure 28 - Confirm Certificates

Clicking this label will confirm that the file was received and verified by the customer and will delete the output file immediately. *If not clicked, the output file will be deleted by default within 90 days (or sooner depending on account configuration).*

Once the request is confirmed, the order status will be changed to “CLOSED” as shown in Figure 26 and “DOWNLOAD” icon will no longer be available.

CONFIRM REQUEST

⚠ WARNING!

Are you sure you want to confirm this request? By doing so you acknowledge you have downloaded and verified your request and grant us permission to dispose of your request's output file for security.

← BACK TO LIST

✓ CONFIRM

REQUEST ID : 337660686365701

TYPE : Cert

DATE SUBMITTED : 11/20/2024 8:08:00 PM

Figure 29 - Confirm request dialog

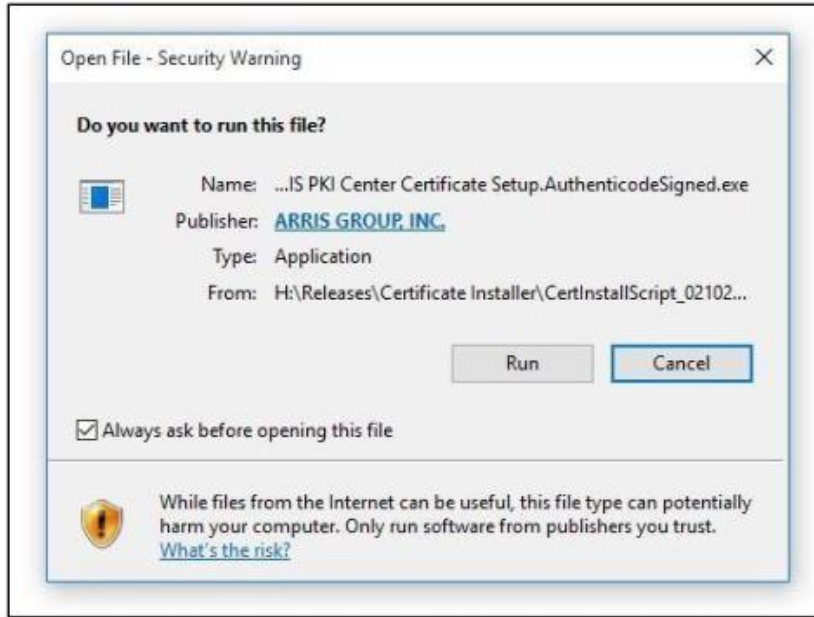
3.2.5 Decrypting the batch file PKIWorks Client

If the output data contains both keys and certificates, you must run the PKIWorks Client application using the eToken issued to the user. PKIWorks Client is used to decrypt information contained in your output data. Details on installation can be found above under **PKIWorks Client Certificate Installation** (Option 2)

PKIWorks requires the installation of certificates prior to using the web site.

From the CommScopePKIWorksClient zip file, double click the ARRIS PKI Center Certificate Setup.exe.

- 6. The Certificate Installer begins. Click Run at the Security Warning if prompted.



- 7.
8. Figure 7 - Open File - Security Warning
9. Click Next at the Welcome window.



- 10.
11. Figure 8 - Certificate Installer Welcome

To continue the installation, click Install.

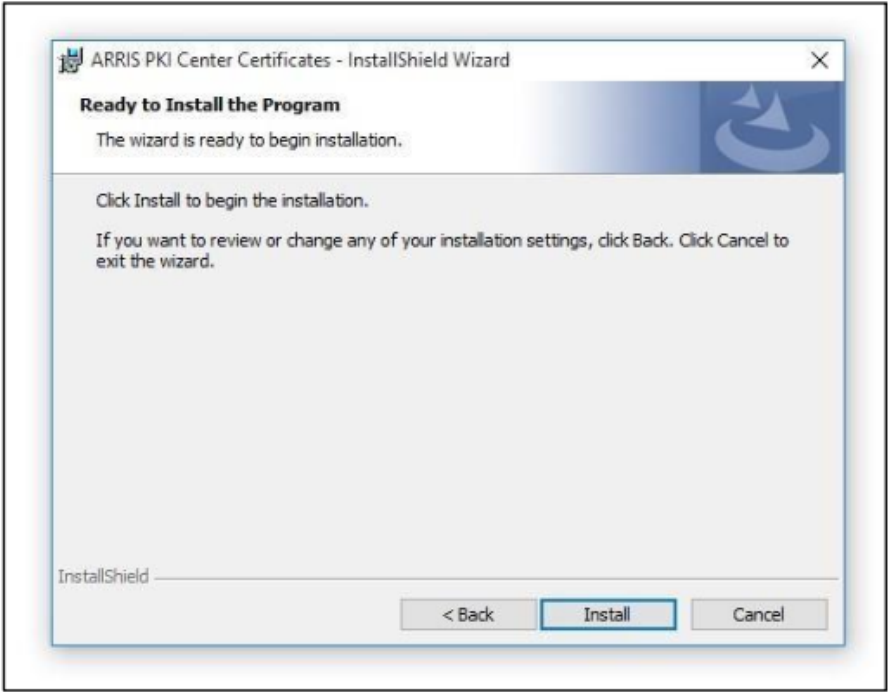
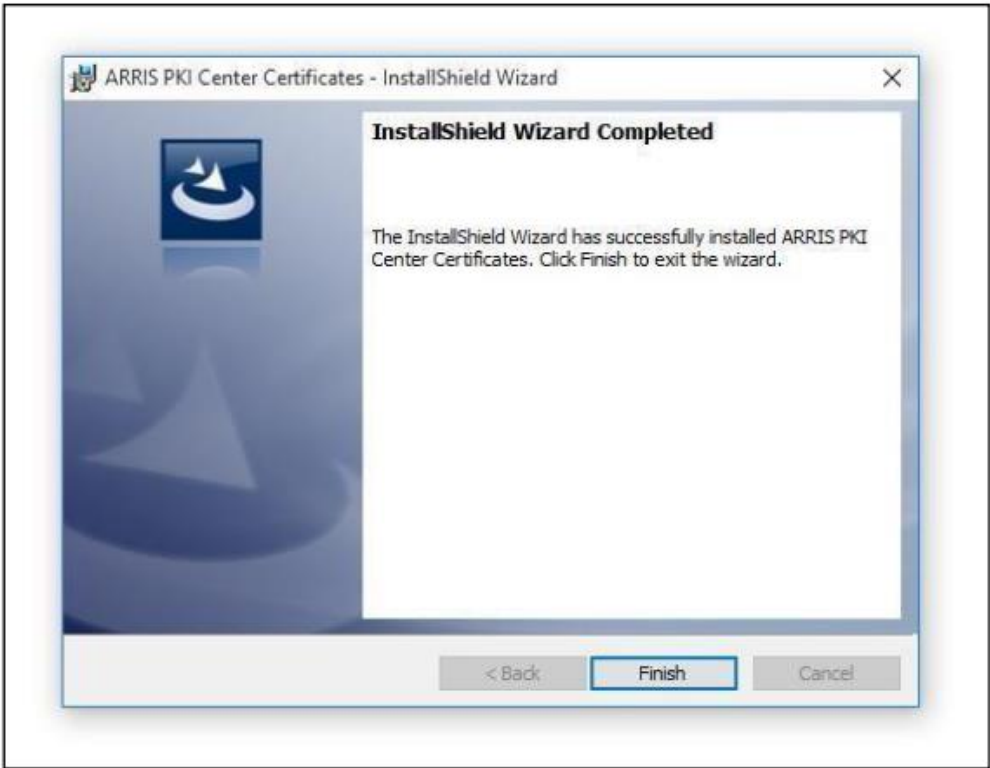


Figure 9 - Ready to Install

Click **Finish** to complete the installation process.



12.

13. Figure 10 - Certificate Install Completed

Note: If your anti-virus software has a false detection or false positive during certificate installation, configure the anti-virus software to allow the installation to execute.

PKIWorks Client Software Setup. Be sure to save your private data in a secure location. Your output can be processed in either DER or PEM formats.

1. In the PKI Works Client application, click the Browse... button to select the PKIWorks file to be processed. The file will load into the application where the manifest information will be displayed including the Request ID, Certificate and Private key quantity, as well as other pertinent information.
2. The File extraction and Clear private key folders have default locations. Browse or enter a different location if desired. The File extraction folder is the location where the files from the output data will be extracted including generated certificates (DER or PEM), the issuing certificates, order logs and all other files, excluding private keys.
3. The Clear private Key folder is the location where the clear private keys will be extracted.
4. In the Output Format section, select either the DER or PEM format.
5. In the Private Key Validation section, choose a validation option to validate the private keys after decryption. The default is 1 percent.
 1. Enable the Validate All Private Keys option for 100 percent validation.
 2. Enable the Validate Percent of All Private Keys option for 1 to 99 percent validation.

PKIWorks Client (Version 4.4.0)

COMMSCOPE® PKIWorks

File to extract:

File extraction folder:

Clear private key folder:

Batch File Manifest:

| Name | Value |
|-------------------|----------------------|
| User Name | User1 |
| Request ID | 3256778105757 |
| Request Completed | 2/2/2021 10:22:46 PM |
| Certificates | 15 |
| Private Keys | 15 |
| Errors | 0 |
| Start Address | 50000000C6AD |
| End Address | 50000000C6BB |

Output Format
☒ DER ☐ PEM

Private Key Validation
☐ Validate All Private Keys (Slow)
☒ Validate Percent of All Private Keys

Status
Progress: Ready for process

Start time :
End time :

Operations

Figure 30 - PKI Works Client with Private Key Validation

- Once you have selected all of your target folders and all other options, click on the Process button to begin processing your data.
- If there are private keys or other encrypted data in your archive, you will be prompted for your eToken user token password. Enter your password and click Login to proceed with the decryption.

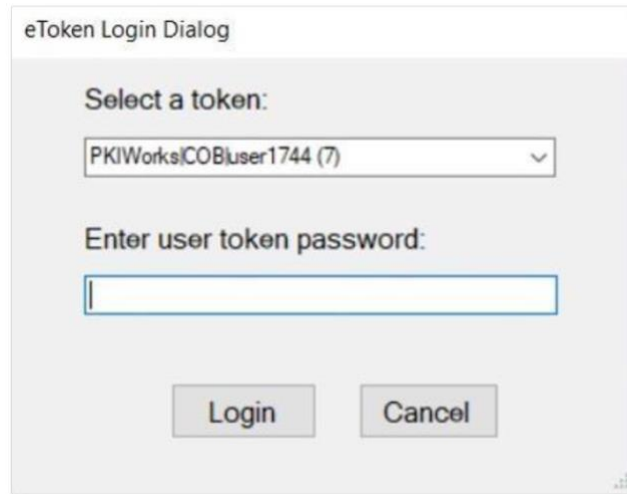


Figure 31 - User authentication password

8. Once the process is complete, a summary will be presented showing the elapsed time, number of processed files and other information about the files that were processed.



Figure 32 - Successful processing of file

9. The specified folder will now contain your data. In the File extraction folder you can see all the files that were extracted from your request, including certificates. You can now open and inspect these certificates. These certificates have values you specified in your request such as the address, model name, and issuing CA. Your private keys will be found in the private key folder. Here you can see all the keys named with the address of the certificate they correspond to.

4 Downloading Root and Intermediate Certificates

Users can view/download the CA certificate chains for generated certificates.

To download the CA certificate chains:

- Go to <https://cert.pkiworks.com>.
- Go to **RESOURCES** → **CA & CRL** (see Figure 33)

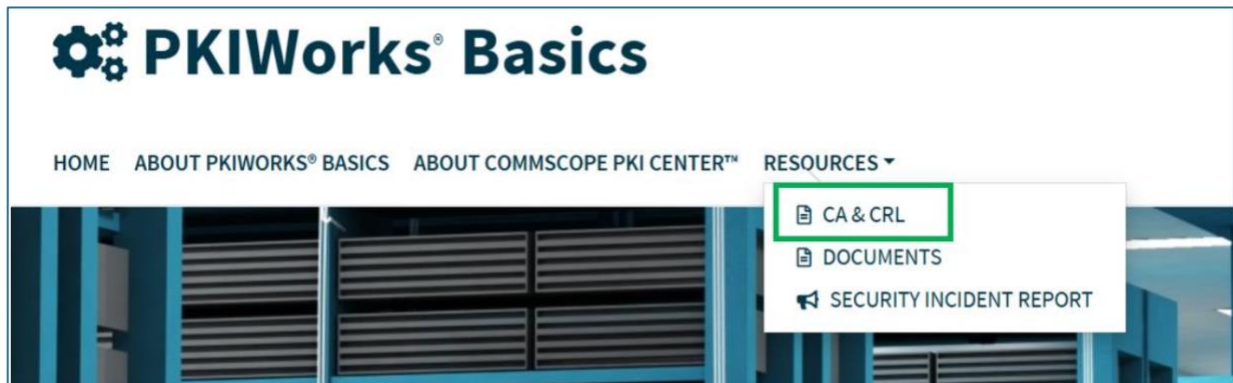


Figure 33 - View CA/CRLs

A list of CA Certificate chains and available CRLs is displayed. Note that the following is a partial example only and does not show all available CA certificates.

5 Revoking Certificates

5.1.1 Subscriber Revocation request

This request is used to revoke active certificates.

NOTE: Revoking certificates does NOT return certificates to your balance. Once certificates are issued and downloaded, they are considered used and cannot be returned to your balance. Revoke should only be used if a certificate has been compromised.

First, select an account as shown in Figure 34.

1. Go to New Request → Certificate Revocation Request

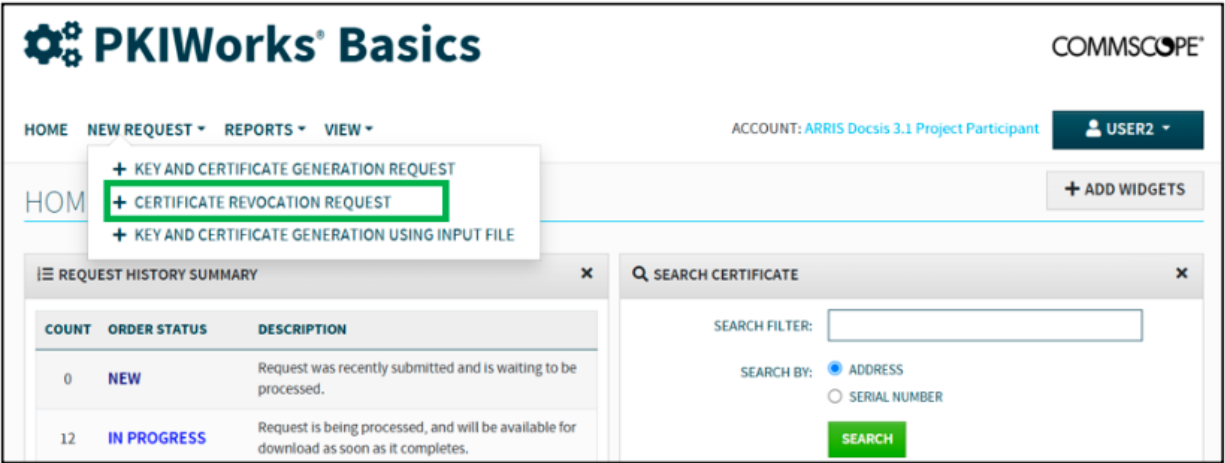


Figure 34 - Certificate Revocation Request

2. New Revocation Request page is displayed. Revocation Reason is set to 'Unspecified' by default.

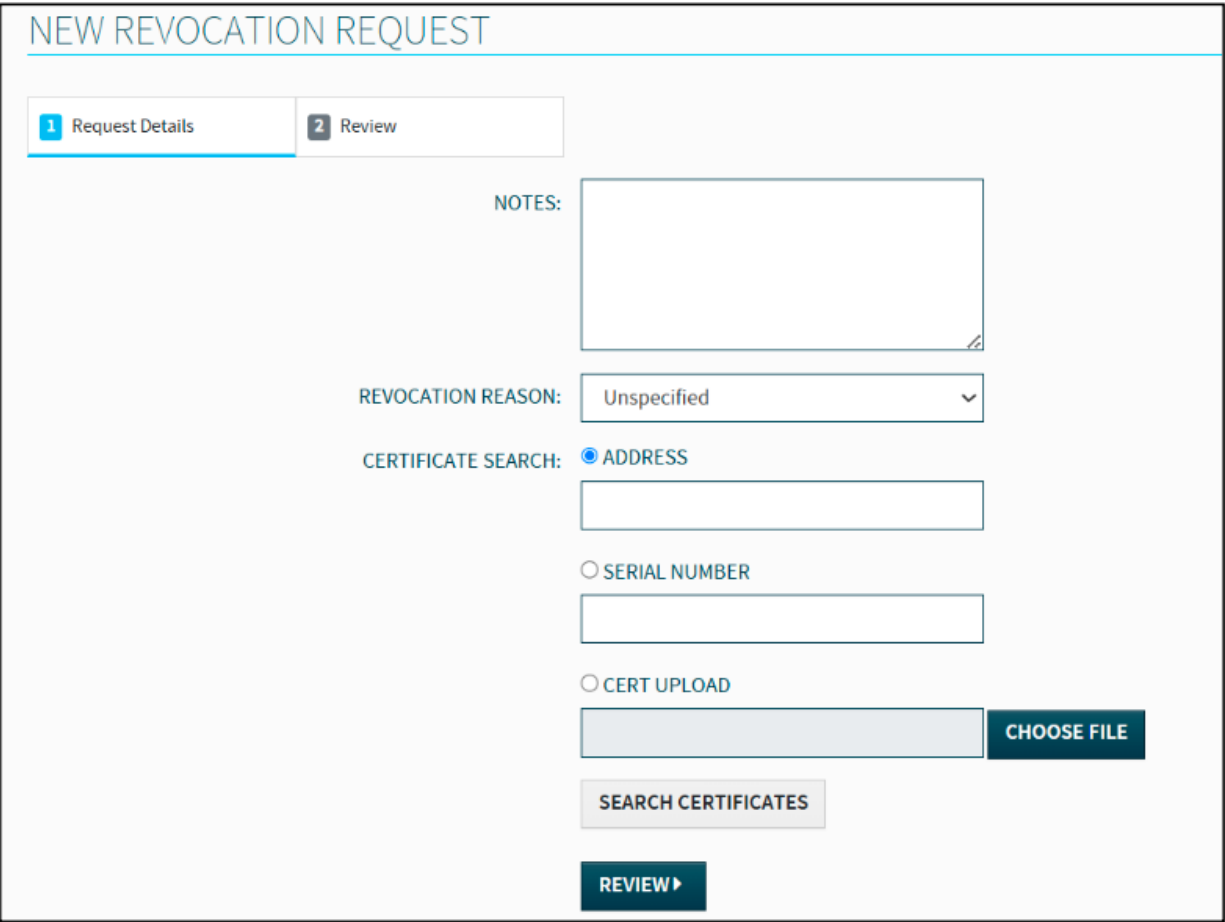


Figure 35 - Certificate Revocation Request Page

3. Subscribers can change the Revocation Reason to other available options.

NEW REVOCATION REQUEST

1 Request Details

2 Review

NOTES:

REVOCATION REASON:

Unspecified

CERTIFICATE SEARCH:

Select...

Affiliation Changed

Superseded

Cessation Of Operation

Unspecified

☐ CERT UPLOAD

CHOOSE FILE

SEARCH CERTIFICATES

REVIEW ▶

Figure 36 - Revocation Reasons

- 4. A confirmation message pops up when selecting Revocation Reason anything other than **Unspecified**. Users can confirm or cancel the change.

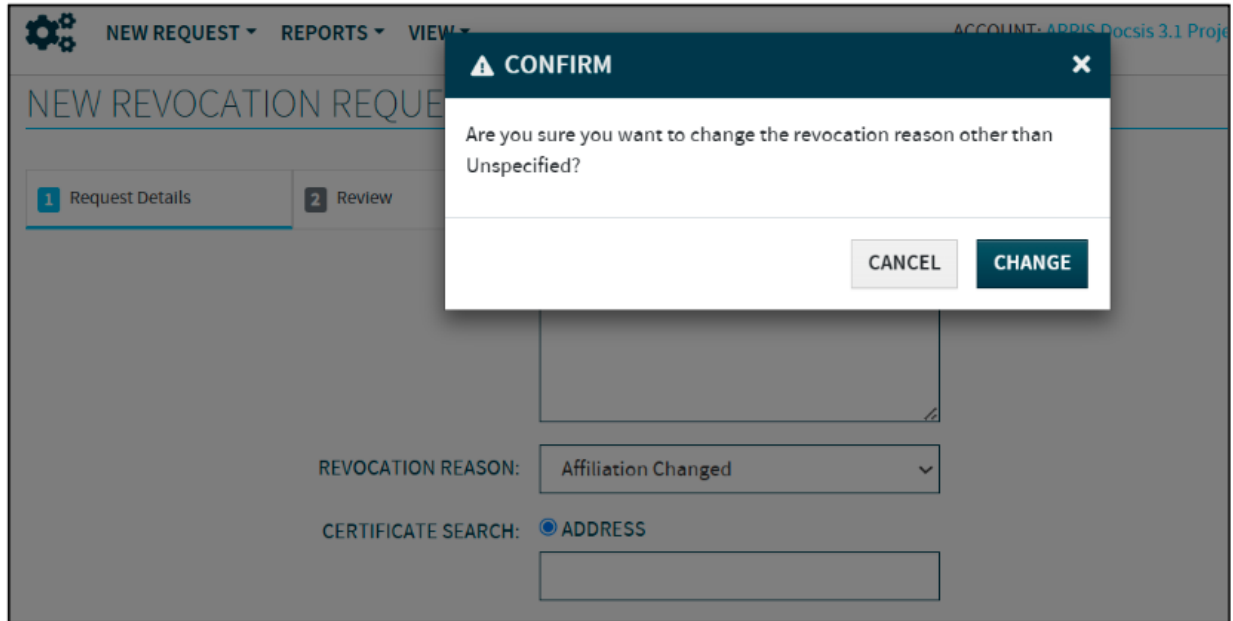


Figure 37 - Revocation Reason Change Confirmation

5. Provide certificate **Address** or **Serial Number** or **upload a certificate** file to search for a certificate to revoke. In the below scenario, we are using certificate **Serial Number** to perform the search.
6. Click on the **SEARCH CERTIFICATES** button.

1 Request Details 2 Review

NOTES:

REVOCATION REASON: Unspecified

CERTIFICATE SEARCH:

☐ ADDRESS

☒ SERIAL NUMBER

6DB16CD6CB1B768ADF7EAEAD6E94C60E

☐ CERT UPLOAD

CHOOSE FILE

SEARCH CERTIFICATES

REVIEW ▶

Figure 38 - Search for Certificate

7. The certificate information is returned. Click on **SELECT CERTIFICATE**.

NEW REVOCATION REQUEST

1 Request Details
2 Review

NOTES:

REVOCATION REASON:
Unspecified

CERTIFICATE SEARCH:
☐ ADDRESS
☒ SERIAL NUMBER

6DB16CD6CB1B768ADF7EAEAD6E94C60E

☐ CERT UPLOAD

CHOOSE FILE

CERTIFICATE(S) FOUND:

SUBJECT: C=US,O=C5,OU=SD,CN=12:33:29:AC:00:0C
ADDRESS: 123329AC000C (MAC)
SERIAL NUMBER: 6DB16CD6CB1B768ADF7EAEAD6E94C60E74DF9F71
STATUS: Active
VALID FROM: 5/20/2025 11:19:06 PM
VALID TO: 5/20/2045 11:19:05 PM

SELECT CERTIFICATE

SEARCH CERTIFICATES

REVIEW

Figure 39 - Select Certificate

8. Click on the **Review** button to review the request,
9. Click **CREATE REQUEST** to submit the request.

NEW REVOCATION REQUEST

1 Request Details

✓

2 Review

DESCRIPTION :

QUANTITY : 1

REVOKING CERT : 123329AC000C (MAC)

SERIAL NUMBER : 6DB16CD6CB1B768ADF7EAEAD6E94C60E74DF9F71

REVOCATION REASON : Unspecified

◀ BACK

✓ CREATE REQUEST

Figure 40 - Create Revocation Request