

Lumen® Adaptive Network Security

**Certificate Management System (CMS)
User guide | February 2022**

Contents

Overview	3
How certificates work with Lumen CMS	3
Login process	3
User groups and access	5
Deleting a user in CMS	6
Certificate deployment process	7
Create a certificate signing request (CSR)	8
Finding the mapping between VDOM and location's firewall instance	11
Uploading/downloading a signed certificate	14
1. 1. Upload the signed SSL certificate to Existing CSR. 14	
2. 2. Upload a signed DPI/intermediate certificate. 16	
3. 3. Key Pair Upload Option (where CSR was not generated using CMS, only for SSL certificates) 18	
4. 4. Download the SSL Certificate. 20	
5. 5. Download the DPI certificate. 23	
Pushing Lumen firewall instances	24
Managing certificates	28
Viewing the certificate logs	28
Viewing the SSL certificate inventory using the server dashboard	29
Setting up certificate alerts	30
Reverting to Welcome Page section	32
Additional references	34

Overview

The Lumen® Certificate Management System (CMS) platform is an automated, systematic, and secure way for you to apply or change digital certificates with Lumen security services platform.

The CMS is currently enabled as part of the set up with Adaptive Network Security (ANS) Mobility security services. The CMS provides auditable security around the handling and storage of all digital key material, per customer. This allows each one of our customers to maintain the advantages of having a per customer public key infrastructure (PKI) system without the need for Lumen personnel interaction.

The CMS is enabled as part of the set up with Lumen® Adaptive Network Security (ANS) Mobility security service and ANS with Deep Packet Inspection (DPI). Certificates for DPI are used as intermediate signing certificates on the ANS firewall instance. Certificates for ANS Mobility are used for user remote access SSL/VPN encryption on the ANS firewall instance.

How certificates work with Lumen CMS

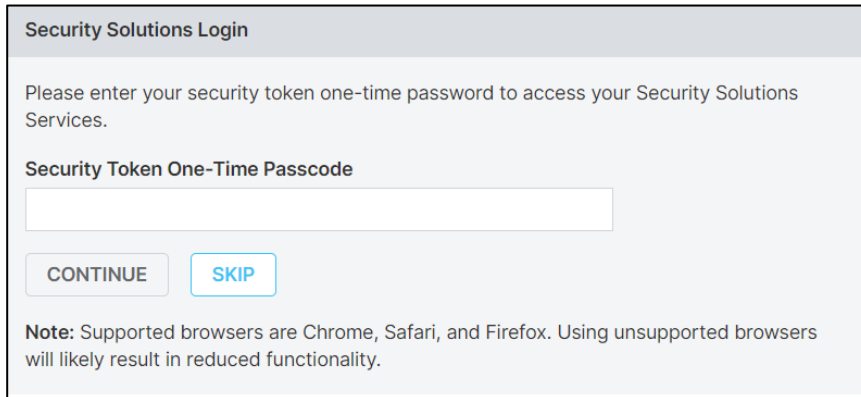
You generate the digital key and certificate signing request (CSR) within the CMS. You can export the CSR, have it signed by your trusted certificate authority (CA), and return it to the CMS for distribution on the Lumen security firewall devices. Once the certificate is available to the CMS, you can initiate a process to automatically move the certificate (and matching key) to a Lumen security firewall instance you select. The CMS also provides information around their certificates, like compliance of encryption standards for the certificate and expiry dates associated to their certificates.

The user needs to have two-factor authentication security solution login for Control Center to access CMS (using the **Admin** tab) and other security features. During initial ANS service provisioning with DPI configuration or ANS Mobility SSL/VPN, an email with the subject 'Successfully Created the Tenant' will be sent to the user indicating the account in CMS has been built for them and can proceed to access it using Control Center.

Login process

You can access the CMS from Control Center.

1. Go to <https://www.lumen.com/login>.
2. Click **CONTINUE**.
3. Type your Control Center username, then click **NEXT**.
4. Type your password, then click **SIGN IN**.



Security Solutions Login

Please enter your security token one-time password to access your Security Solutions Services.

Security Token One-Time Passcode

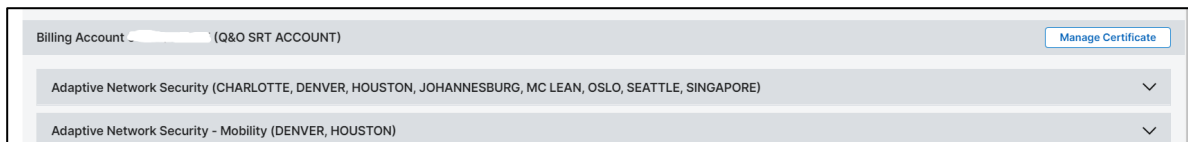
[CONTINUE](#) [SKIP](#)

Note: Supported browsers are Chrome, Safari, and Firefox. Using unsupported browsers will likely result in reduced functionality.

5. Type your security token one-time passcode, then click **CONTINUE**. Two-factor authentication with a security soft token is required to access security capabilities on Control Center like CMS, which cannot be accessed if skipped.

Please see Security Tokens Control Center support if you need a two-factor security token on Control Center.

6. Click Admin, then click Security Certificate Management.



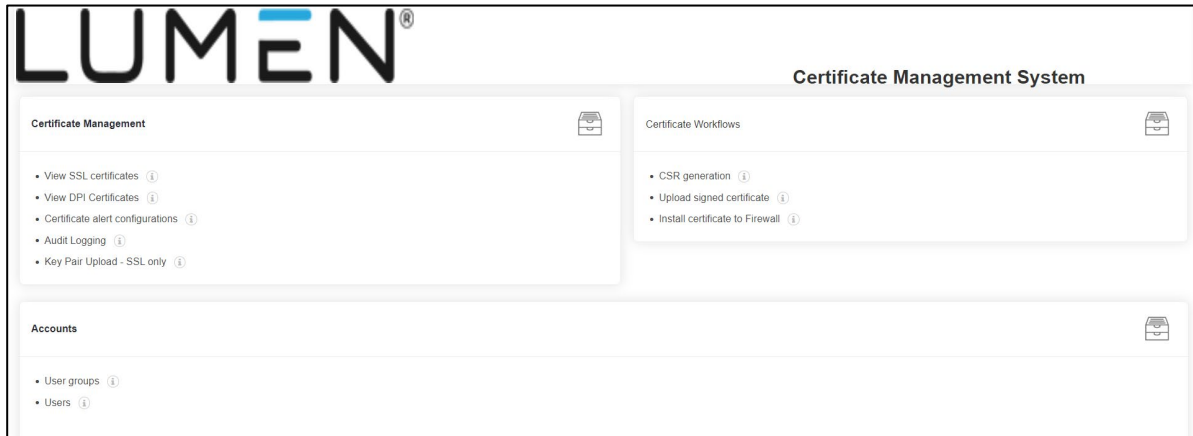
Billing Account [redacted] (Q&O SRT ACCOUNT) [Manage Certificate](#)

Adaptive Network Security (CHARLOTTE, DENVER, HOUSTON, JOHANNESBURG, MC LEAN, OSLO, SEATTLE, SINGAPORE) ▾

Adaptive Network Security - Mobility (DENVER, HOUSTON) ▾

7. Click **Manage Certificate** associated to your ANS product billing account number (BAN). It will redirect to CMS.

The following page will display. All options on the page are in the form of separate links. Each of these links opens in a new tab. Once you are finished with the task or running the workflow, we recommend the user close the tab.



8. Follow the instructions under Certificate Identification section of this document to create a CSR, download the CSR, upload the signed certificate, and install certificate to firewall. If you have an already signed certificate to install certificate to firewall, then proceed with the **upload key pair** option (for SSL only) from the page.
9. Please make any modifications to email addresses used for system notifications under Alerts, explained in the Certificate Management section of this document.

User groups and access

You choose the user group assigned to users of CMS within your tenant in the provisioning phase. By default, the cert-mgr-admin role is assigned.

CMS has 4 user groups: Cert-mgr-admin, cert-mgr-role1, cert-mgr-role2 and cert-mgr-role3.

Use **cert-mgr-admin** as the default admin user group of CMS.

Cert-mgr-admin has admin (highest) level of user group access which has following capabilities:

- Upload, download CSR, private key, and certificates.
- View the certificate and audit logs of all users, along with certificate alerts.
- Run the workflows but cannot edit them.
- View the certificates.
- Can delete a user but cannot modify any other user groups or users

Cert-mgr-role1 user group has following capabilities:

- Upload, download CSR, private key, and certificates.
- View the certificate logs and audit logs of all users, along with certificate alerts.
- Can run the workflows but cannot edit them.

- View the certificates.
- Cannot modify or delete any user/user groups.

Cert-mgr-role2 user group has following capabilities:

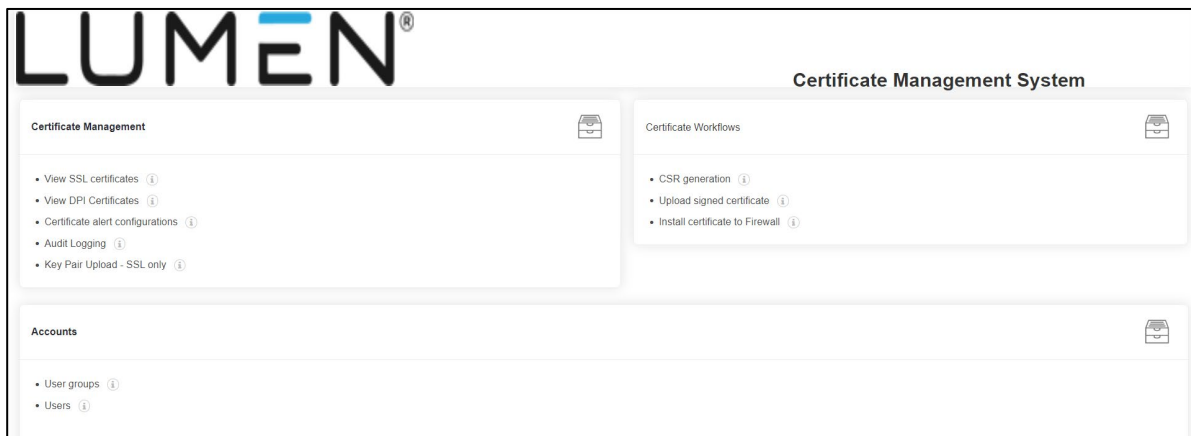
- View the certificate logs and audit logs of all users, along with certificate alerts.
- No access to workflows and Certificates.
- Access to reporting and only view the certificates.
- Cannot modify or delete any user/user groups.

Cert-mgr-role3 user group is defined for future purpose but not assigned any access, ignore any warning signs shown associated to this role.

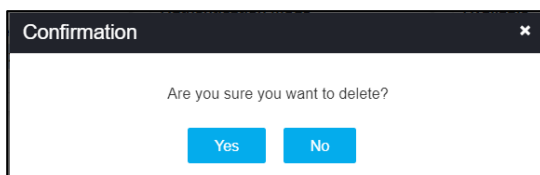
Deleting a user in CMS

To delete a user, cert-mgr-admin level of permissions are required, so ensure you are using an account/user assigned to the cert-mgr-admin role.

1. Click **Users** (under Accounts section of the page).



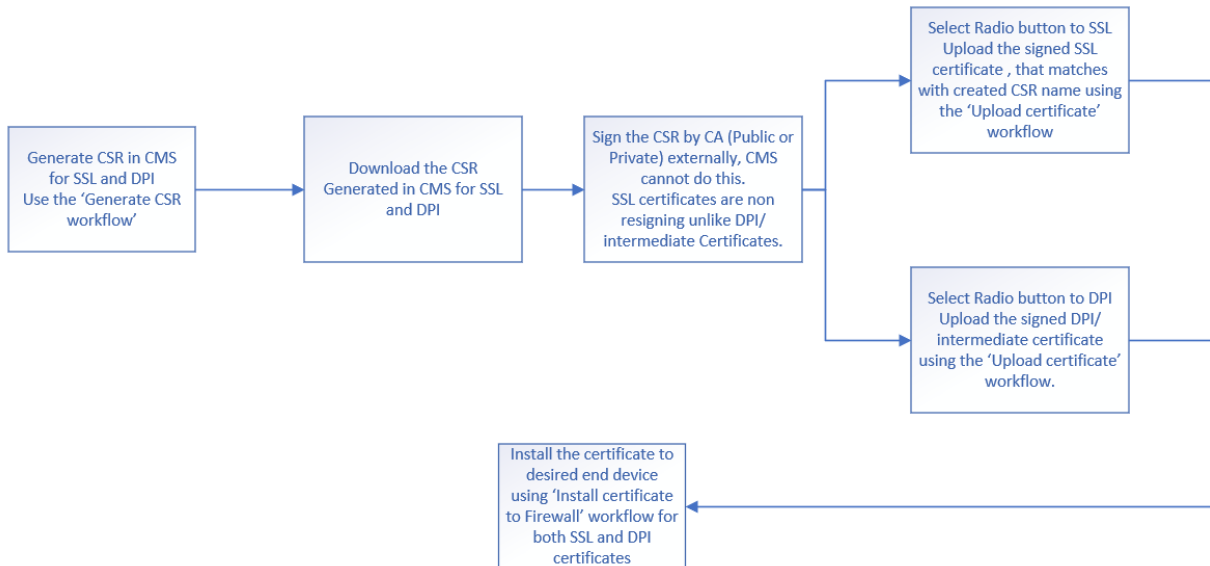
2. Select the checkbox on the row for the user, then click the **Delete** icon.



3. Click **Yes** to confirm deleting the selected user. Close the tab after task is completed.

Certificate deployment process

CERTIFICATE DEPLOYMENT FLOW

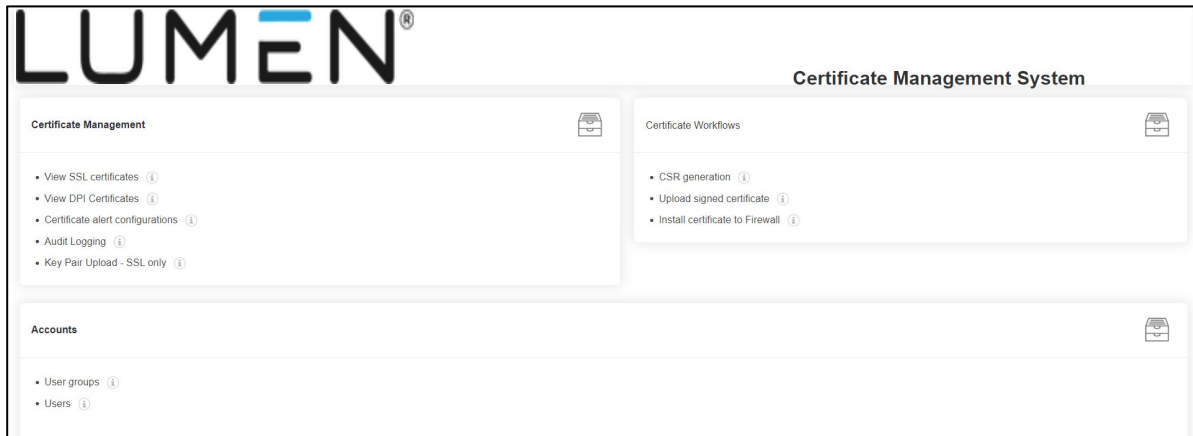


This module provides instructions for

- Create a CSR.
- Upload the signed certificate to existing CSR.
- Download the certificate or CSR. (Optional, informative step, not a required step).
- Key pair upload option (in a case where the SSL/identity certificate's CSR was not generated using CMS).
- Push certificate to the Lumen firewall instance device.

Create a certificate signing request (CSR)

1. A page like the one below will be displayed post login to Control Center.



2. Click on the **CSR Generation** below the **Lumen Workflows**.

3. This page is used to generate CSR for SSL and DPI certificates. Select the **SSL** button to generate a CSR for an identity certificate and **DPI** button to generate CSR for intermediate/resigning certificate. Below are filled out examples for both.
 - Group indicates the group CSR belongs and group **Default** can be used for generic purposes.
 - CSR details for **SSL** can be filled out as needed, all fields are except SANS are required.
 - Service Type: SSL
 - Certificate Group: Default or Certificate-Gateway

- Hash Function: Any above SHA224
- Key Type: DSA or RSA (preferred)
- Bit Length: Choose any above 2048 (preferred – 4096)
- Common Name
- Subject Alternative Name (SANS)
- Organization
- Organization Unit
- Locality
- State
- Country Code: Should be a 2-character code (e.g., *US* for United States or *CA* for Canada)
- Email Address
- Challenge password
- Confirm password

Below is a filled-out CSR generation example for SSL certificates:

The screenshot displays the 'CSR Generation' interface. On the left, there is a sidebar with a search bar and a 'Request View' button. The main area is titled 'CSR details' and contains the following fields:

- Service Type: SSL DPI
- Certificate Group: Certificate-Gateway
- Hash Function: SHA256
- Key Type: RSA
- Bit Length: 4096
- Common Name: lumen.com
- Subject Alternative Name: lumen.one.com
- Organization: Architecture & Engineering
- Organization Unit: IT
- Locality: Broomfield
- State: CO
- Country Code: US
- Email Address: abcd@userdomain.com
- Challenge Password: ****
- Confirm Password: ****

At the bottom right, there are 'Submit' and 'Cancel' buttons.

- CSR details for **DPI** can be filled out as needed and all fields are required.
 - Service Type: DPI
 - Device List: Select the VDOM(s) or end device (FortiGate Firewall) you wish to use DPI certificate. The end device you wish to push certificate. If you are unsure of which VDOM associates to which location's firewall instance, refer the steps below to find the mapping.
 - Certificate Group: Default or Certificate-Gateway

- Hash Function: Any above SHA224
- Key Type: DSA or RSA (preferred)
- Bit Length: Choose any above 2048 (preferred – 4096)
- Common Name
- Organization
- Organization Unit
- Locality
- State
- Country Code: Should be a 2-character code (Ex: US for United States, CA for Canada)
- Email Address

The screenshot displays the 'CSR Generation' interface. On the left, there is a sidebar with a search bar and a 'CSR Submission Form' button. The main area is titled 'CSR details' and contains the following fields:

- * Service Type: SSL DPI
- * Device List: None selected
- * Certificate Group: Default
- * Hash Function: SHA256
- * Key Type: RSA
- * Bit Length: 4096
- * Common Name: [Text Input]
- * Organization: [Text Input]
- * Organization Unit: [Text Input]
- * Locality: [Text Input]
- * State: [Text Input]
- * Country Code: [Text Input]
- * Email Address: [Text Input]

Finding the mapping between VDOM and location's firewall instance

If no VDOMs or desired VDOM are not displayed, reach out to your technical design engineer related to your order.

As shown above the VDOM identifier is in the format “ANS: 33xxxxxx”. This maps to the service component (SCID) for Adaptive Network Security associated with the order number service ID (“44xxxxxx”) on Control Center **Inventory** tab.

1. Sign in to Control Center using 2FA.
2. Click Services, then click Network, Security, and Communications.

Inventory - MyLevel3 ?

Customer Number: All | Billing Account Number: All | Service Type: All | Product: Adaptive Network Security

Customer Number: All | Billing Account Number: All | Service Type: All | Product: Adaptive Network Security

Service Inventory | Network Map

10 Services

Service ID	Site Name	Status	Product	Serial ID	Service Location	Product Identifier	Billing Account Number	A Location Address	Z Location Address
441510320		Active	Adaptive Network Security		6 BRAHAM ST, LONDON, LN, E1 8EE, UNITED KINGDOM	441510320	1-ATIDXB	6 BRAHAM ST, LONDON, LN, E1 8EE, UNITED KINGDOM	

Service Details

Product Identifier (PID): 441510320

Service Components (SCIDs): 334789658 (Adaptive Network Security)

Serial ID:

Service Location: 6 BRAHAM ST, LONDON, LN, E1 8EE, UNITED KINGDOM

VPN ID: 2005986416

Activity History (last 6 months):

Created	Activity	Status	Updated	ID
No tickets, requests, or orders in the last 6 months.				

Create New Ticket

3. Once the VDOM is identified, revert to the **CSR generation** tab and proceed with the below steps.

Below is a filled-out CSR generation example for DPI certificates.

The screenshot shows the 'CSR Generation' interface. On the left, there is a sidebar with a search bar and a 'CSR Submission Form' button. The main area displays the 'CSR details' form with the following fields:

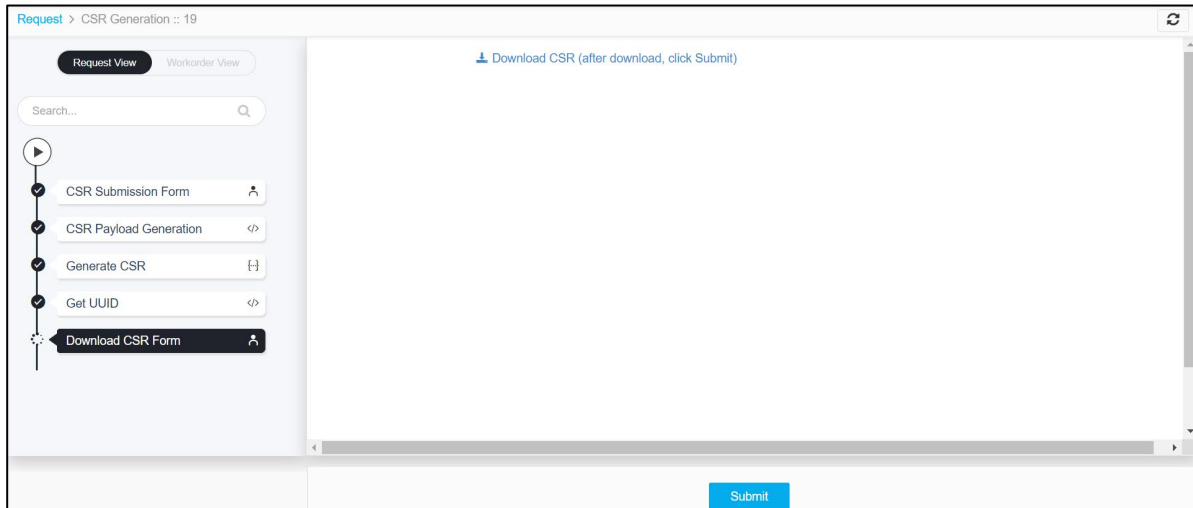
- Service Type: SSL DPI
- Device List: [Redacted]
- Certificate Group: Default
- Hash Function: SHA512
- Key Type: RSA
- Bit Length: 4096
- Common Name: lumen.com
- Organization: lumen
- Organization Unit: A&E
- Locality: Broomfield
- State: CO
- Country Code: US
- Email Address: abcd@lumen.com

- Click **Submit** to generate the CSR, then click **Ok** to confirm.

A confirmation dialog box titled 'Confirmation' with a close button (X) in the top right corner. The text inside the dialog asks: 'Are you sure you want to Submit?'. Below the text are two buttons: 'Ok' and 'Cancel'.

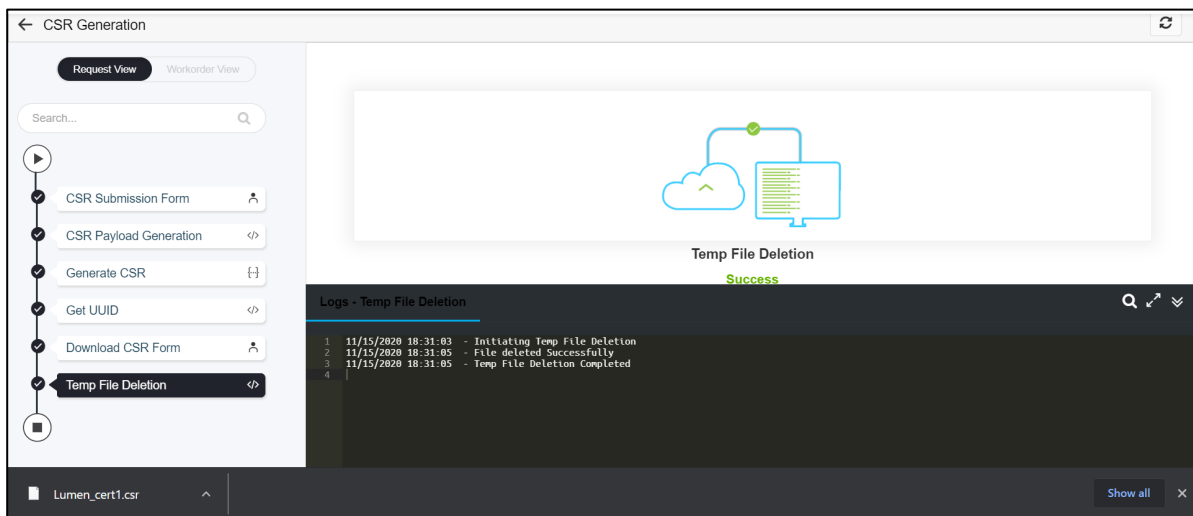
- Click on the 'Download CSR (after download, click Submit)', this will download the CSR generated. Click on 'Submit' after downloading the CSR.

Note: Once you click Submit as shown in bottom of the page below, you cannot download the CSR again.



A zip file containing the CSR will be downloaded, unzip it for the contents.

- Below indicates the completed execution of the workflow. Click on the back arrow at the top-left corner, to go back to the page view or close the tab.



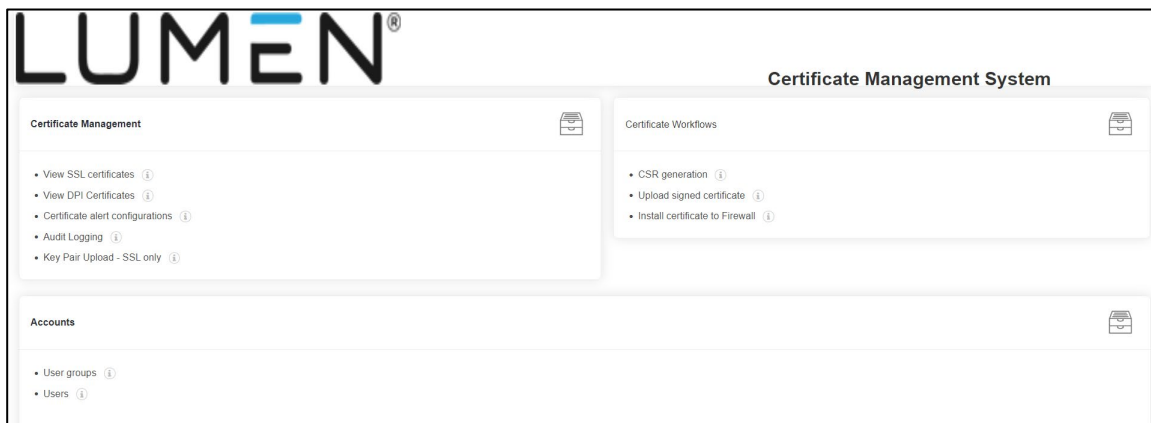
Note: The CSR file for DPI certificates will have the end device number and timestamp added to the beginning to distinguish them and map them to their associated end device at later stage during the process of Installing the certificate to end device.

Uploading/downloading a signed certificate

1. Upload a signed SSL/identity certificate.
2. Upload a signed DPI/intermediate certificate.
3. Key pair upload option for SSL
4. Download the SSL Certificate.
5. Download the DPI Certificate.

1. Upload the signed SSL certificate to Existing CSR.

4. Click on the **Upload Certificate** from upper-right **Certificate Workflows** box on this page displayed upon Login to CMS.



Note: If the CSR or private key was generated in the CMS, then follow this option but if you wish to upload a certificate with both private and public key (where private key was not generated in CMS) go to 'key pair upload' option. The 'Key pair upload' option cannot be utilized for DPI certificates, in case of DPI/intermediate certificates, the CSR must be generated using the CMS.

5. Select the **SSL** for type of certificate. Select the 'Common Name' of the Certificate you wish to upload, browse your PC, and upload the signed certificate (SSL or DPI) associated to that common name, expected formats are .crt,.pem,.pfx,.der.

Note: Upload only the certificate with same name as above generated CSR, do not upload the root CA certificates or any other certificates.

Request > Upload Certificate - FormBuilder

Request View | Workorder View

Search...

Upload Certificate Form

^ Certificate

Type: SSL DPI

Common Name: Lumen_cert1

Upload Certificate: [Upload] [Download] [Delete]

Comments:

Example:

Request > Upload Certificate - FormBuilder

Request View | Workorder View

Search...

Upload Certificate Form

^ Certificate

Type: SSL DPI

Common Name: Lumen_cert1

Upload Certificate: Lumen_cert1_87_AF_8C_45_9F_A9 [Upload] [Download] [Delete]

Comments: Demo Lumen Certificate

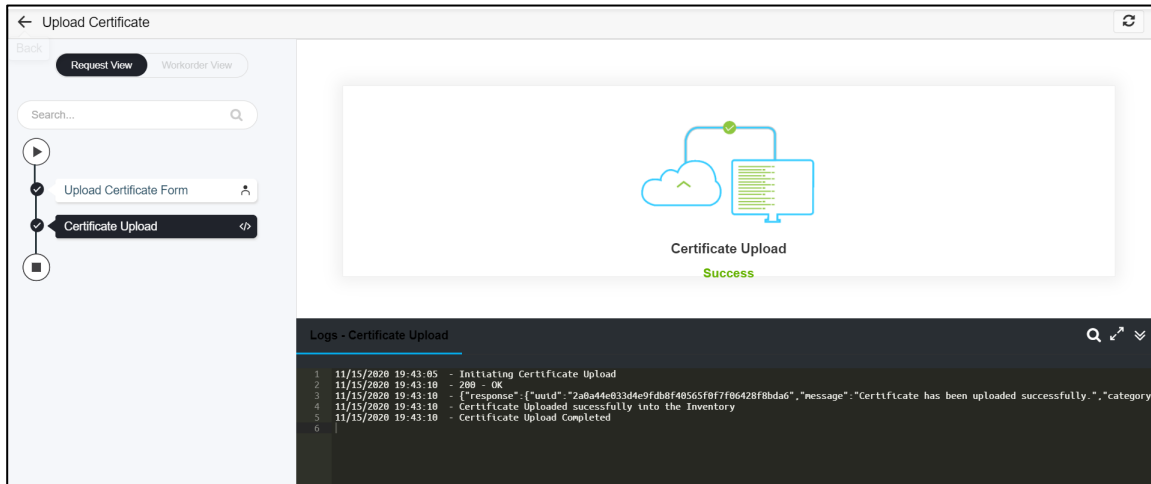
6. Click **Submit**, then click **Ok** if you are sure of your selections.

Confirmation

Are you sure you want to Submit?

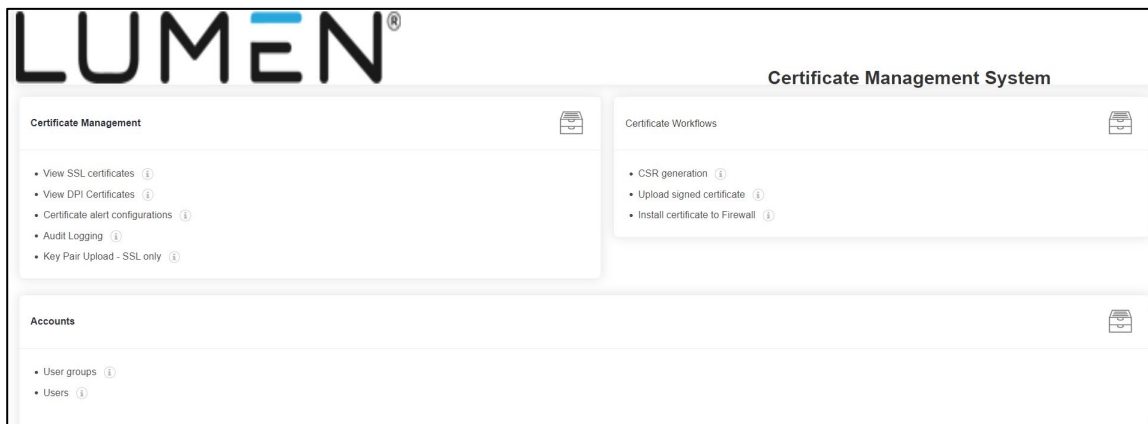
Ok Cancel

7. The below screen indicates completion of the workflow, click on the back arrow located top left of the screen to return to the welcome page that is displayed on login.



2. Upload a signed DPI/intermediate certificate.

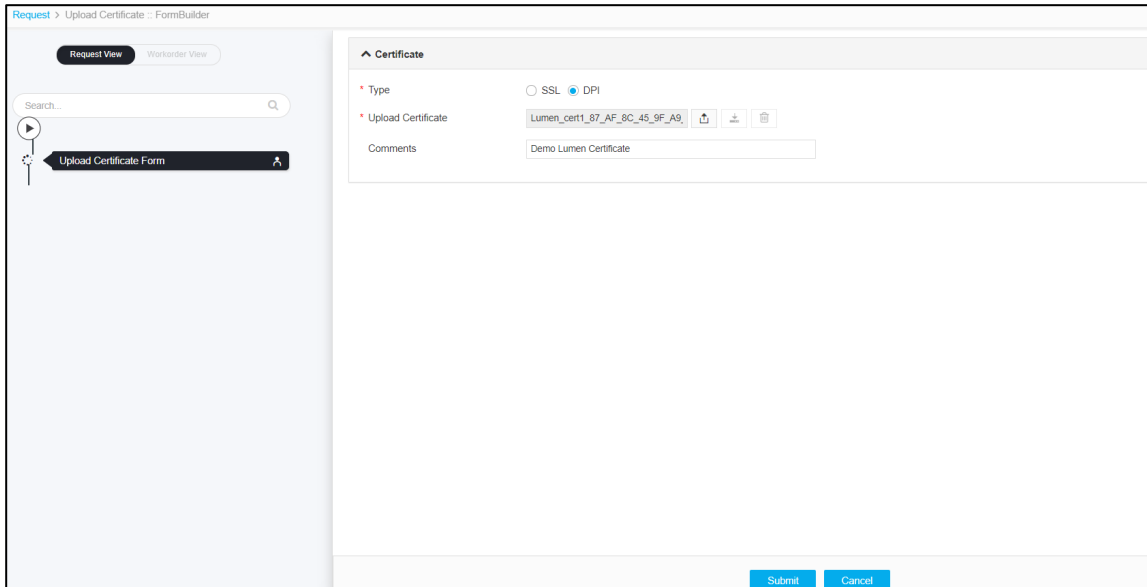
1. Click on the 'Upload signed certificates' link in the section of Certificate Upload from the user page, this link will open in a new tab.



2. Select the **DPI** in type of certificate. Click on upload button as indicated in below picture and then select the DPI/intermediate certificate associated to the CSR previously created in CMS. Add comments if desired.

3. Click on **Submit**.

Note: The CSR for DPI certificates must be generated on CMS, do not upload a certificate with CSR generated elsewhere.

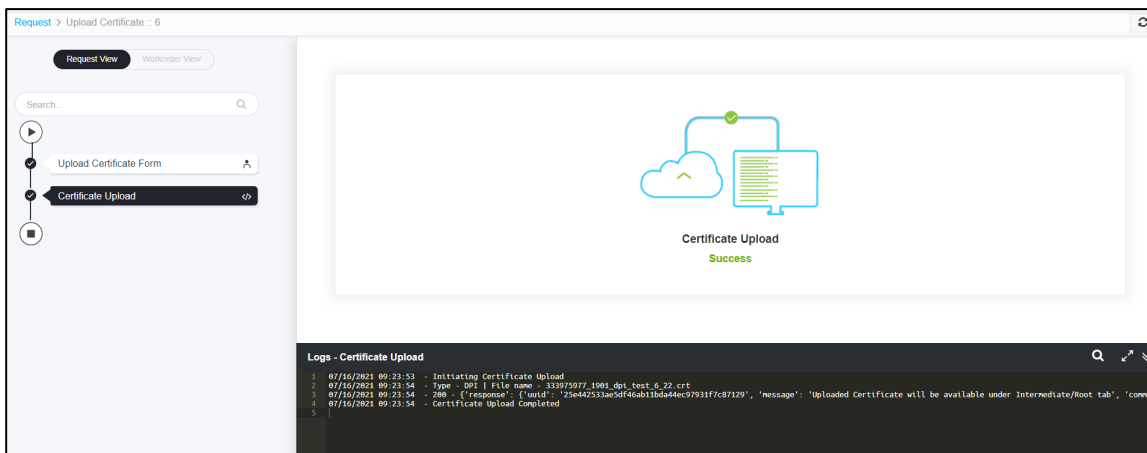


The screenshot shows the 'Upload Certificate' form in the Lumen CMS interface. The form is titled 'Request > Upload Certificate - FormBuilder'. It has two tabs: 'Request View' (selected) and 'Workorder View'. The form contains the following fields:

- Type:** Radio buttons for 'SSL' and 'DPI' (selected).
- Upload Certificate:** A text input field containing 'Lumen_cert1_67_AF_6C_45_9F_A9', with a file upload icon and a trash icon.
- Comments:** A text input field containing 'Demo Lumen Certificate'.

At the bottom right of the form, there are two buttons: 'Submit' and 'Cancel'.

4. Upon successful upload, below screen will be displayed. The uploaded certificate can be viewed using the '**View DPI certificates**' link on the page.



The screenshot shows the 'Certificate Upload' success screen in the Lumen CMS interface. The page is titled 'Request > Upload Certificate - 6'. It has two tabs: 'Request View' (selected) and 'Workorder View'. The page contains the following elements:

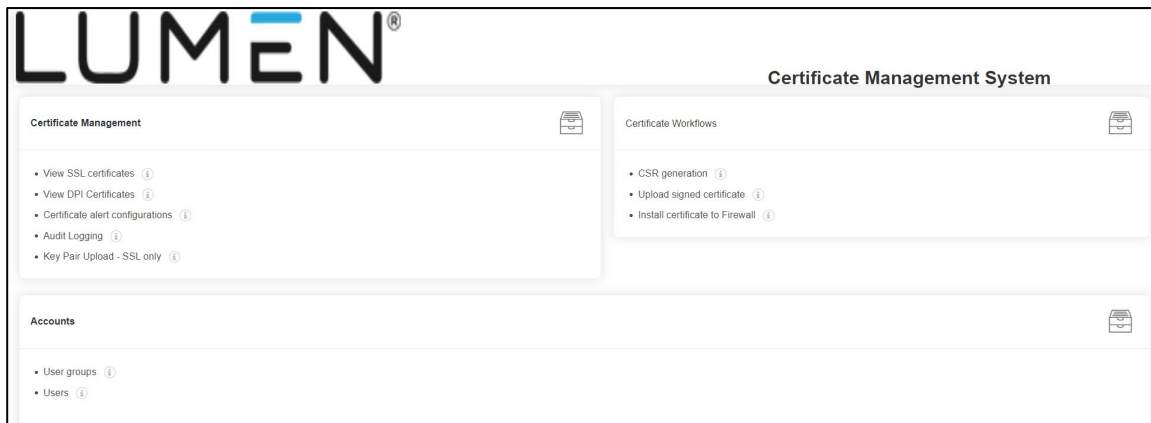
- Navigation:** A sidebar with a search bar and a list of items: 'Upload Certificate Form' and 'Certificate Upload' (selected).
- Success Message:** A large green checkmark icon with the text 'Certificate Upload Success' below it.
- Logs:** A log viewer at the bottom showing the following entries:

```
1 07/16/2021 09:23:53 - Initiating Certificate Upload
2 07/16/2021 09:23:54 - type - DPI | file name - 33293577_1981_dpi_test_6_22.crt
3 07/16/2021 09:23:54 - 200 - {"response": [{"uid": "256442533ae5df46ab1bd44ec97931fc87129"}, {"message": "Uploaded Certificate will be available under Intermediate/Root tab"}]}
4 07/16/2021 09:23:54 - Certificate Upload Completed
5
```

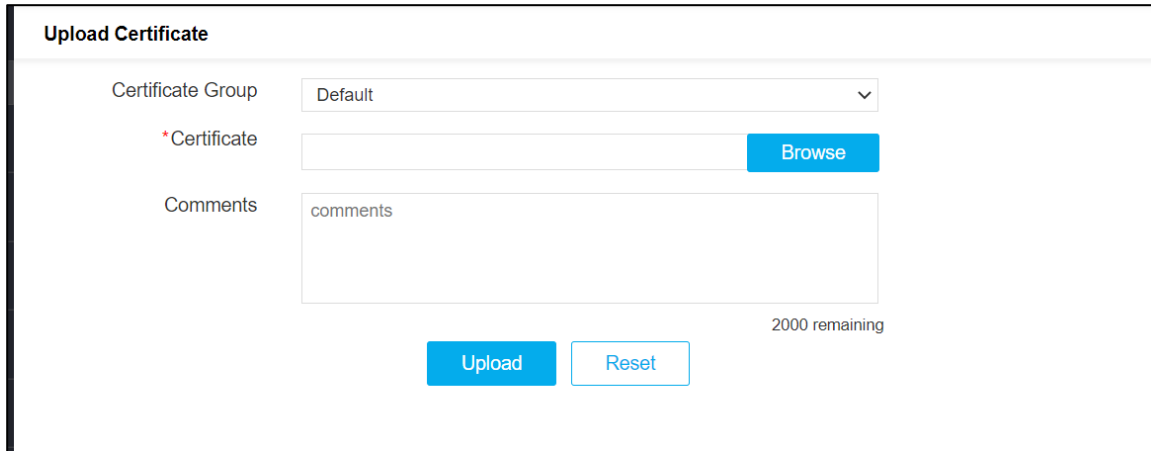
3. Key Pair Upload Option (where CSR was not generated using CMS, only for SSL certificates)

1. Click on the 'Key pair upload' option under the **Certificates** section of the page. The Link opens in new tab, and this welcome page will exist in the current tab.

Note: This option is to be used only for SSL certificates, cannot work with DPI certificates. Must upload both private and public key/certificate for successful installation on to the end device.



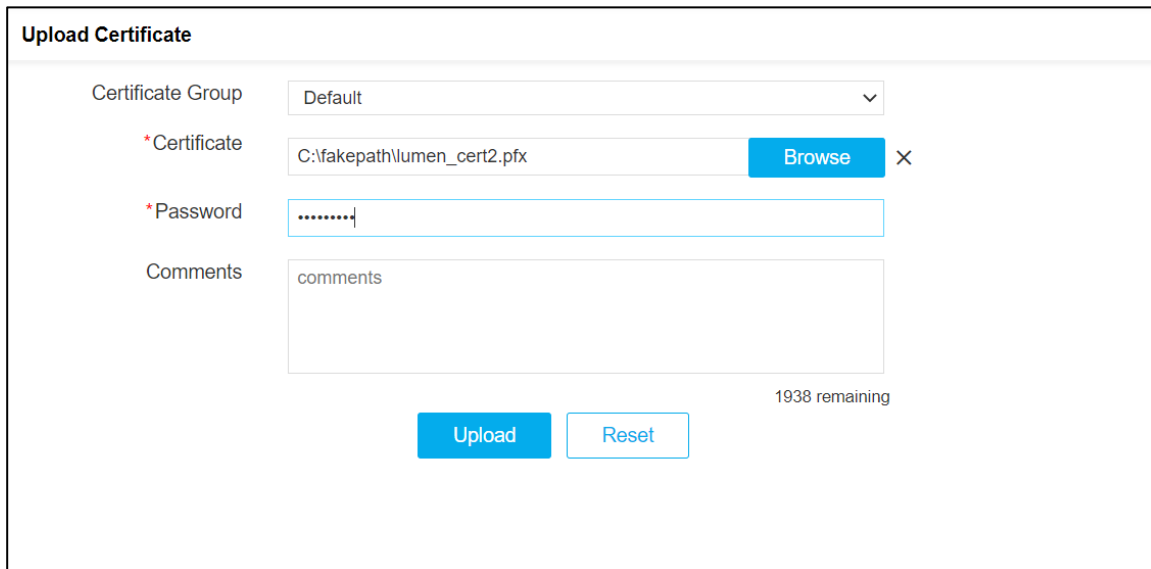
2. Select the Certificate Group as **Default**, browse the certificate you wish to upload (Ensure a private and public certificate pair is uploaded for it to be successfully pushed to the Firewalls). If you set a password for the private key, it will be prompted as shown in the example below and enter the password for successful upload.



The screenshot shows the 'Upload Certificate' form with the following fields and controls:

- Certificate Group:** A dropdown menu set to 'Default'.
- *Certificate:** An empty text input field with a blue 'Browse' button to its right.
- Comments:** A text area containing the placeholder text 'comments'.
- Character Count:** '2000 remaining' is displayed at the bottom right of the form.
- Buttons:** 'Upload' and 'Reset' buttons are located at the bottom center.

Example:



The screenshot shows the 'Upload Certificate' form with the following fields and controls:

- Certificate Group:** A dropdown menu set to 'Default'.
- *Certificate:** A text input field containing the path 'C:\fakepath\lumen_cert2.pfx' with a blue 'Browse' button and a close icon (X) to its right.
- *Password:** A text input field with masked characters '.....|'.
- Comments:** A text area containing the placeholder text 'comments'.
- Character Count:** '1938 remaining' is displayed at the bottom right of the form.
- Buttons:** 'Upload' and 'Reset' buttons are located at the bottom center.

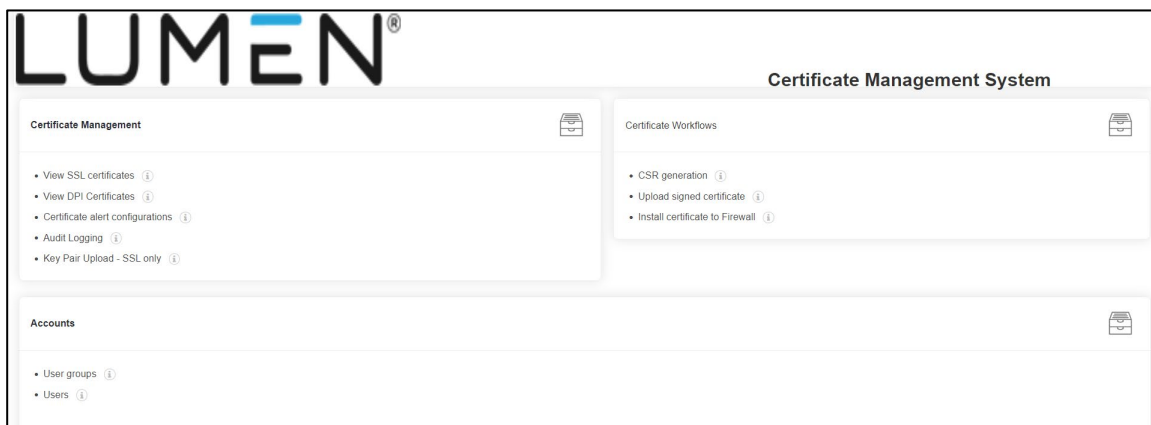
3. Click **Upload**.

- Upon a successful upload, a certificate chain will be shown as below. To revert to the welcome page, follow the **How to revert to Welcome Page** section or use the previous tab as the link from this page is opened in new tab.



4. Download the SSL Certificate.

- Click on the **View SSL certificates** option under the **Certificate Management** section of the page for SSL certificates. click on **View DPI certificates** option for DPI certificates.

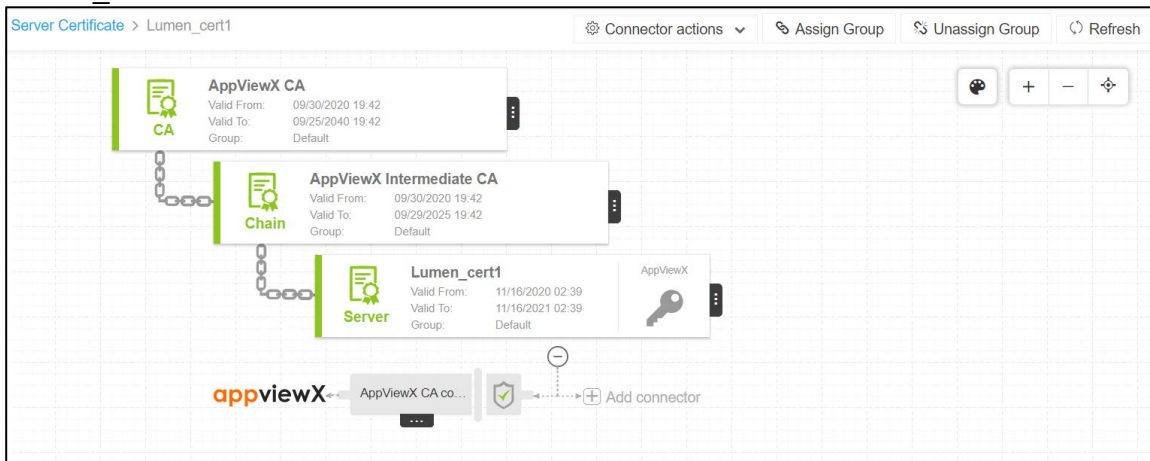


- The following page will show the inventory of certificates created under your Customer Tenant. Click on the desired Common Name of the certificate you wish to download. The certificates under Common Name column with a green dot to identify a signed certificate and which is available to be pushed to the Lumen firewall instance.

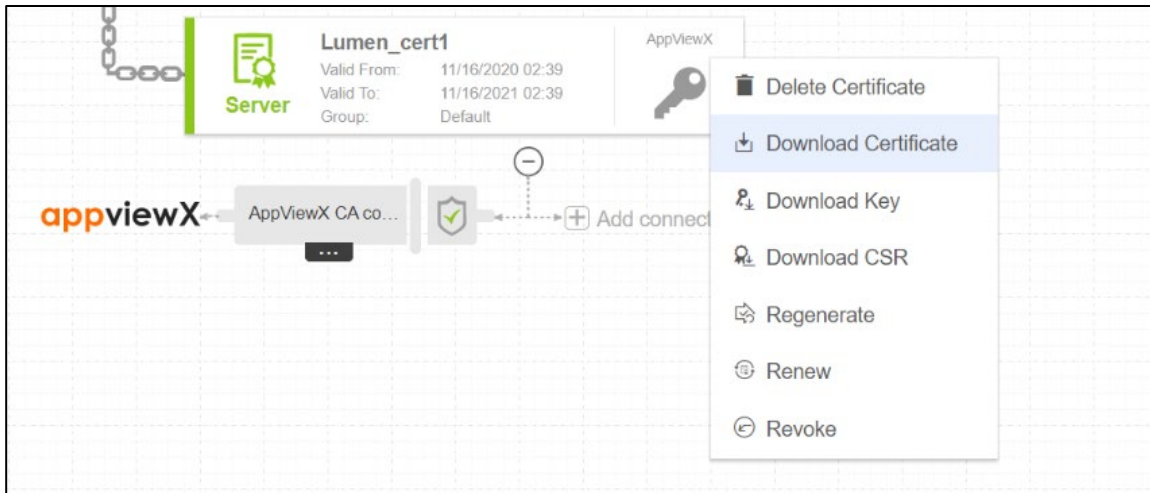
Common Name	Serial Nu...	Group	Issuer Co...	Valid to (...	Status	Certificate...
Lumen_cert1	87-AF:8C:4...	Default (RW)	AppViewX I...	11/16/202...	Managed	AppViewX
cert_gen_super	19:F3:E4:C...	Default (RW)	AppViewX I...	11/15/202...	Managed	AppViewX

Note: If the screen view is not as shown below, click on the 'List' on the top right corner for this screen.

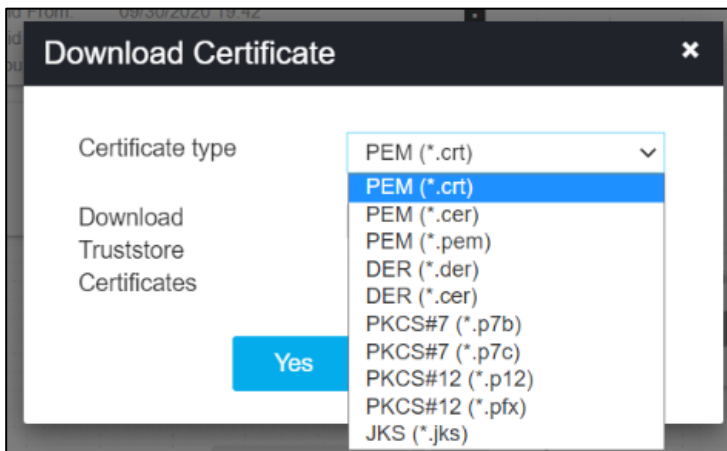
- The following page will display the common name of certificate selected. **Lumen_Cert1** is shown below as the Signed Certificate for demo purposes. Click on the 3 sequential dots by the Lumen_cert1 block.



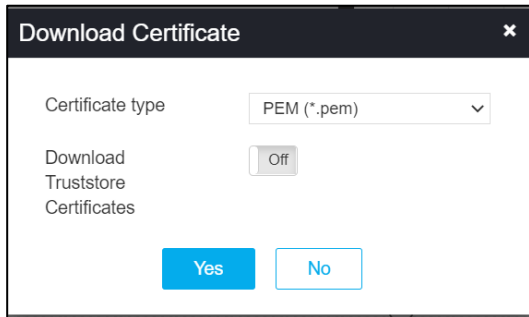
- Click on **Download Certificate** or **Download CSR** as desired.



- Below is a list of the available formats you can download the certificate or CSR in. Select the required format, and if you wish to download a private key for a CSR/certificate, a set password option will prompt you for input, which will be used to encrypt the key.

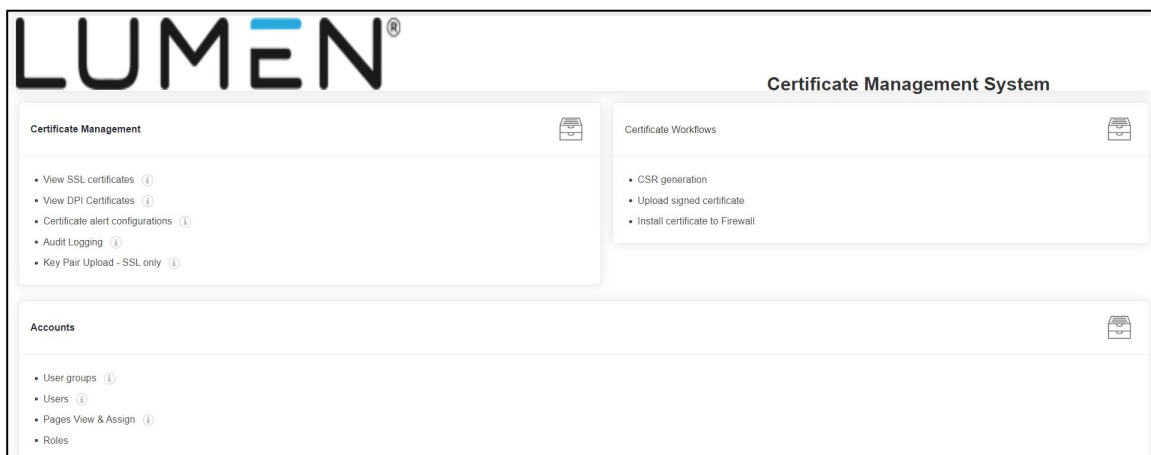


- Click **Yes** after the desired format is selected and the file will be available in downloads section of your PC.



5. Download the DPI certificate.

- Click on the **View DPI certificates** option under the **Certificate Management** section of the page for SSL certificates.



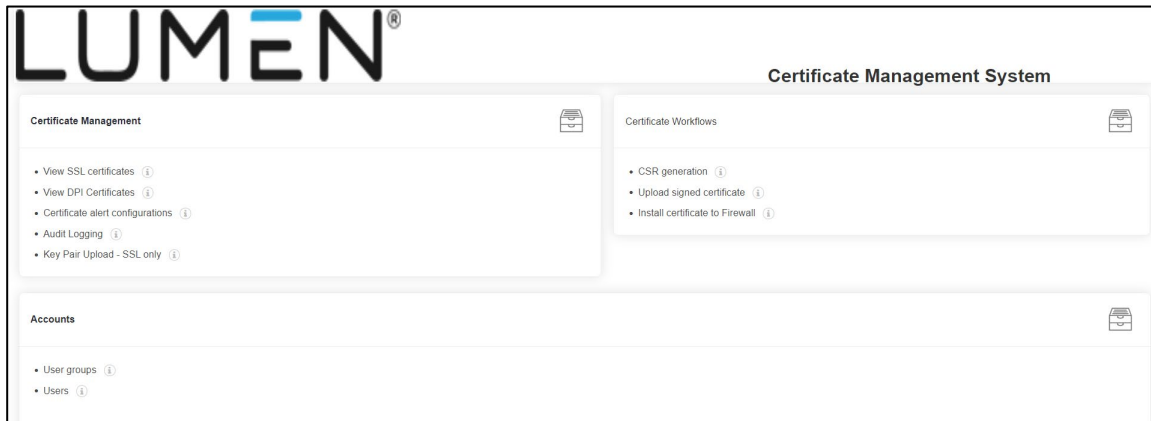
- The following page will show the inventory of DPI certificates under your Customer Tenant. Select the desired Common Name of the certificate you wish to download. Only the certificates can be downloaded for DPI, not the keys.

Common Name	Certificate Authority	Serial Number	Valid from (GMT)	Valid to (G...)	Issuer Organization	Issuer Organiz
....._dpi_test_6_1	OTHERS	10.08	06/01/2021 18.35	07/02/2021...	Lumen	A&E

- Click on **Download**. The file should be available in your PC in the format of a .zip, please unzip it for the certificate.

Pushing Lumen firewall instances

- Click Install Certificate to Firewall in the upper-right Certificate Workflows box.



- Select **SSL** or **DPI** Certificate Type, identity certificates are used for SSL and intermediate certificates used for DPI.

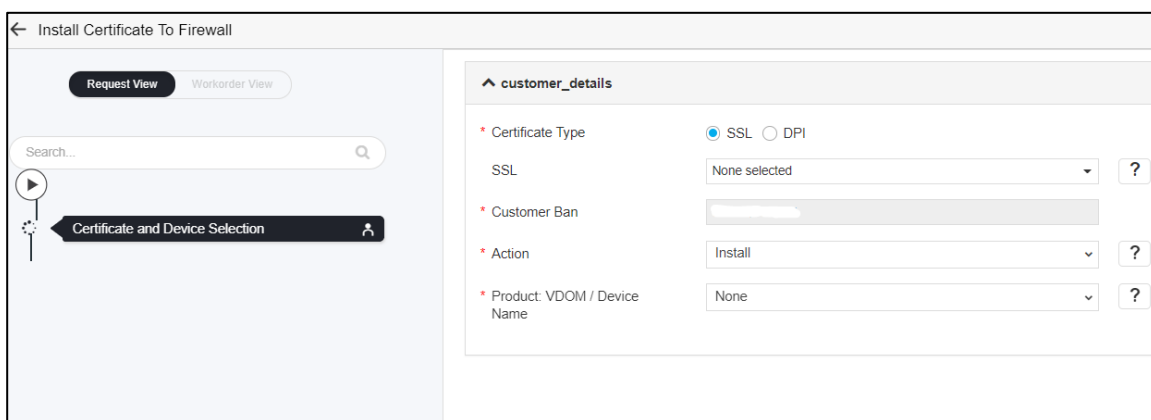
The customer BAN (Billing Account Number) and the list of Virtual Domains (VDOM) / firewall instances available for the associated BAN are auto populated.

3 operations can be performed on the product VDOM for **SSL and DPI Certificates**, they are install certificate, update certificate, and delete certificate.

Action : Install → Used for initial install of the certificate(s) to VDOMs

Action : Update → Used to replace a certificate already on the VDOM

Action : Delete → Delete the Certificate on the VDOM.



10. Above page is relevant for Installing SSL certificates to Firewalls. Choose the certificate type: **SSL** for identity certificates and **DPI** for intermediate/resigning certificates.

SSL: Identity certificates that are complete (signed by the CA after CSR generation) appear in this list.

Customer Ban: Auto populated.

Action: As discussed in above step 2, choose one of the three options available. (Use **Install** if this is the first time this certificate is being deployed onto product VDOM).

Product VDOM / Device Name: The end device you wish to push certificate. If you are unsure of which VDOM associates to which location’s firewall instance, refer the steps below to find the mapping.

If no VDOMs or desired VDOM are not displayed, reach out to Technical Design Engineer related to your order.

As shown above the VDOM identifier is in the format “ANS: 33xxxxxx”. This maps to the Service Component (SCID) for Adaptive Network Security associated with the Order Number Service ID (“44xxxxxx”) on Control Center Inventory tab.

11. Sign in to Control Center using 2FA.

12. Click Services, then click Network, Security, and Communiexions.

The screenshot shows the LUMEN Control Center interface. The top navigation bar includes the LUMEN logo, 'Control Center', and user information (EID 11170076, milenac). A sidebar on the left contains navigation options: Home, Admin, Inventory (selected), Orders, Service Mgmt, Reports, Billing, and Shop. The main content area displays an 'Inventory - MyLevel3' view with filters for Billing Account Number, Service Type, and Product, all set to 'All'. Below the filters is a table with the following data:

Site Name	Status	Product	Serial ID	Service Location	Product Identifier	Billing Account Number	A Location Address	Z Locatio
LEEDS 2	Active	Unprotected Private Line		MCCRHOUSE, LEEDS, WY, LS11, BHA, UNITED KINGDOM	FRC2005565493	0205205691	MCCRHOUSE, LEEDS, WY, LS11, BHA, UNITED KINGDOM	CORRIANDE AVENUE FT TFFS, LOW E14 2AA, U KINGDOM
	Pending	Fiber+ Internet		1710 CHASE RIDGE LN, LAWRENCEVILLE, GA		5-RGCVR3SG	12365 PIATA TRACE PKWY, AUSTIN, TX, 78727-6418, USA	
	Active	IP VPN		101 E 2ND ST, TULSA, OK, 74103-3203, USA	29718128	5-RHQBGCGK	101 E 2ND ST, TULSA, OK, 74103-3203, USA	

13. Select the **Adaptive Network Security** filter for the product.

Inventory - MyLevel3 ?

Customer Number: All | Billing Account Number: All | Service Type: All | Product: Adaptive Network Security

14. Click on the [+] by the service ID number to expand the details. Association between service ID and SCIDs (VDOM identifier) can be found here.

Customer Number: All | Billing Account Number: All | Service Type: All | Product: Adaptive Network Security

Service Inventory | Network Map

10 Services

Service ID	Site Name	Status	Product	Serial ID	Service Location	Product Identifier	Billing Account Number	A Location Address	Z Location Address
441510320		Active	Adaptive Network Security		6 BRAHAM ST, LONDON, LN, E1 8EE, UNITED KINGDOM	441510320	1-ATIDXB	6 BRAHAM ST, LONDON, LN, E1 8EE, UNITED KINGDOM	

Service Details

Product Identifier (PID) **441510320**

Service Components (SCIDs) **334789658** Adaptive Network Security

Serial ID:

Service Location: 6 BRAHAM ST, LONDON, LN, E1 8EE, UNITED KINGDOM

VPN ID **2005986416**

Activity History (last 6 months)

Created	Activity	Status	Updated	ID
No tickets, requests, or orders in the last 6 months				

Create New Ticket

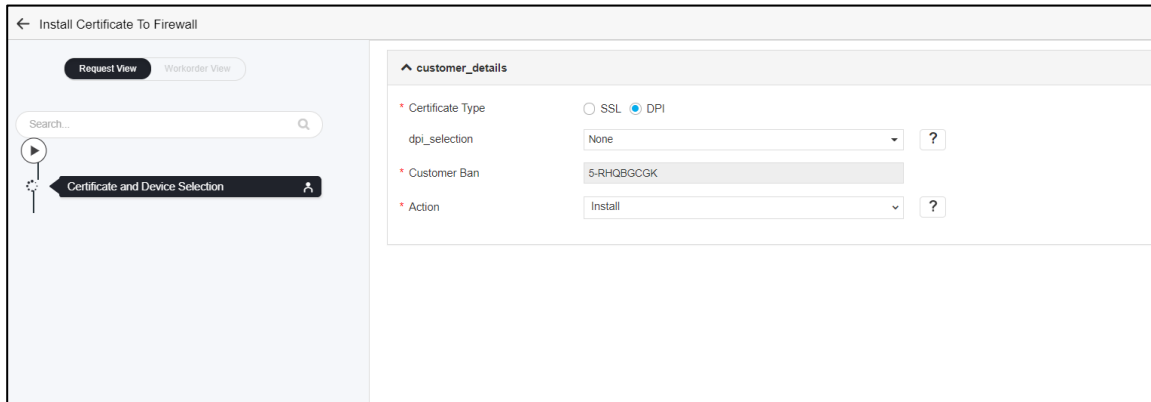
Once the VDOM is identified, revert to the **Install Certificate to Firewall** tab and proceed with step 5 below.

Below Page is for Installing DPI certificates to Firewalls

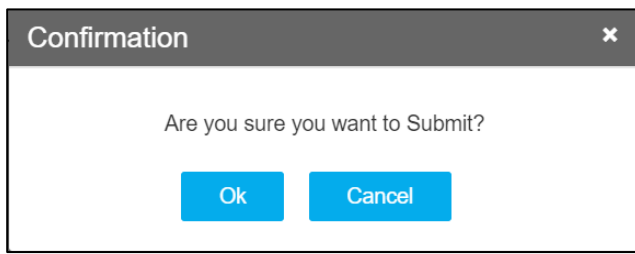
DPI: Intermediate/resigning certificates that are complete (signed by the CA) will be available in this list.

Customer BAN and Action are as described above.

15. The certificate will be installed on the VDOM CSR was created.

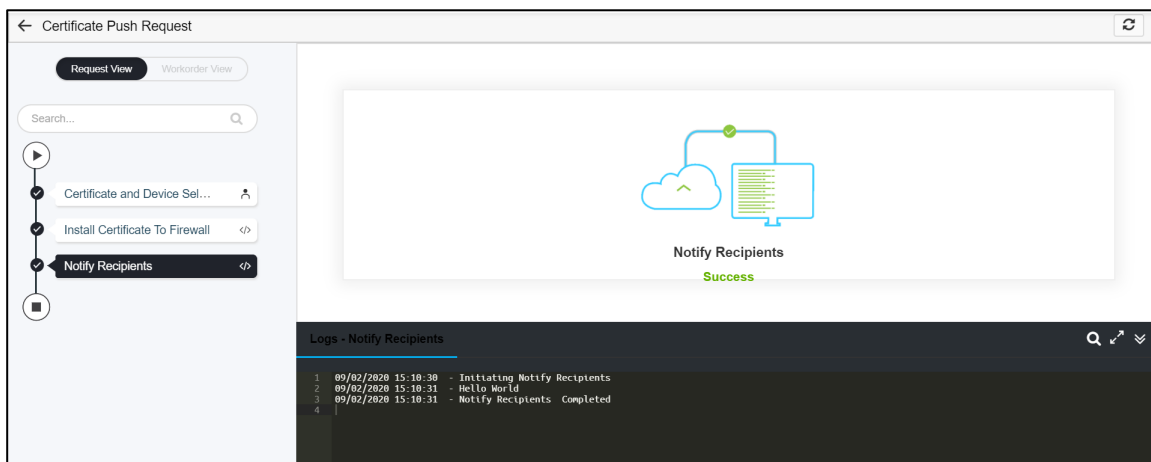


16. Click **Ok** if you are sure of your certificate and VDOM choice.



17. The below page indicates the 'push' workflow was successful. Do not go back mid process. Please wait until the execution completes. The Notify recipients refers to internal email that is sent to Lumen provisioning team.

Click on the back arrow located top left of the screen to return to the welcome page displayed on login or close the tab as each tab opens in new window.



Managing certificates

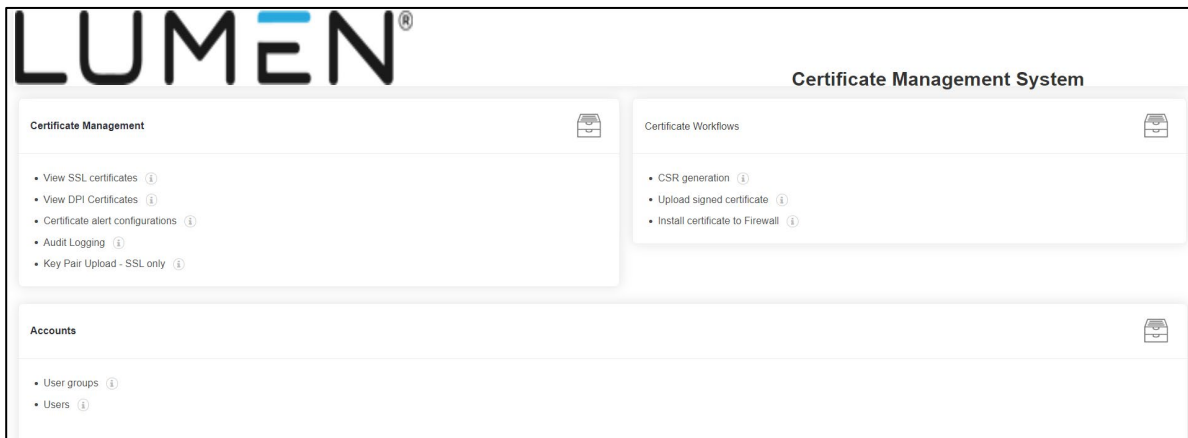
This section provides instructions to

- view the certificate logs
- view the certificate inventory using the server dashboard

Viewing the certificate logs

1. Click on the **Audit logging** from the lower right **Certificate Management** box.

This page is displayed upon CMS Login. The link opens in new tab, and this welcome page will exist in the current tab.



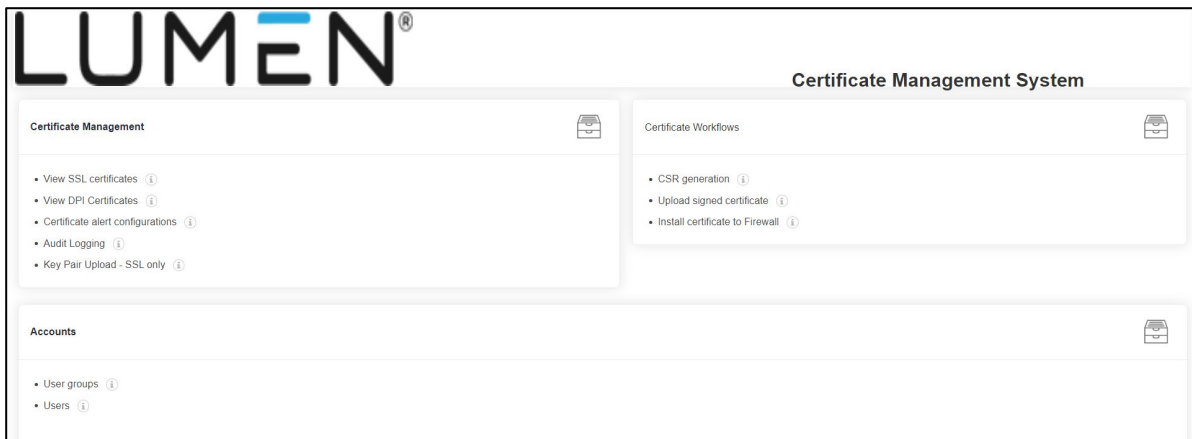
2. You can view the Audit and the certificate logs here:

Time	User	Device name	Object details	Source IP	AppView...	Method ...	Comments	Log message
09/02/2020 12:28...	Tenant...		NA	10.170.1...	cms3.ms...	UI		User: Tenant_Admin in User Group: [tenant_admin] I...
09/02/2020 12:28...	Tenant...			10.170.1...	cms3.ms...	UI		Permissions : [certificate.policy:viewpolicy, certificate...
08/31/2020 04:29...	Tenant...			10.170.1...	cms3.ms...	UI		Page updated successfully : CMS_admin[Transactio...
08/31/2020 04:29...	Tenant...			10.170.1...	cms3.ms...	UI		Page updated successfully : CMS_admin[Transactio...
08/31/2020 01:33...	Tenant...			10.170.1...	cms3.ms...	UI		Page updated successfully : CMS_admin[Transactio...
08/31/2020 01:32...	Tenant...			10.170.1...	cms3.ms...	UI		Page updated successfully : CMS_admin[Transactio...
08/31/2020 01:15...	Tenant...			10.170.1...	cms3.ms...	UI		Page updated successfully : null[Transaction Id : WE...
08/31/2020 01:15...	Tenant...			10.170.1...	cms3.ms...	UI		Page updated successfully : null[Transaction Id : WE...
08/31/2020 11:45...	Tenant...			10.170.1...	cms3.ms...	UI		Page updated successfully : null[Transaction Id : WE...
08/31/2020 11:45...	Tenant...			10.170.1...	cms3.ms...	UI		Page updated successfully : null[Transaction Id : WE...

Viewing the SSL certificate inventory using the server dashboard

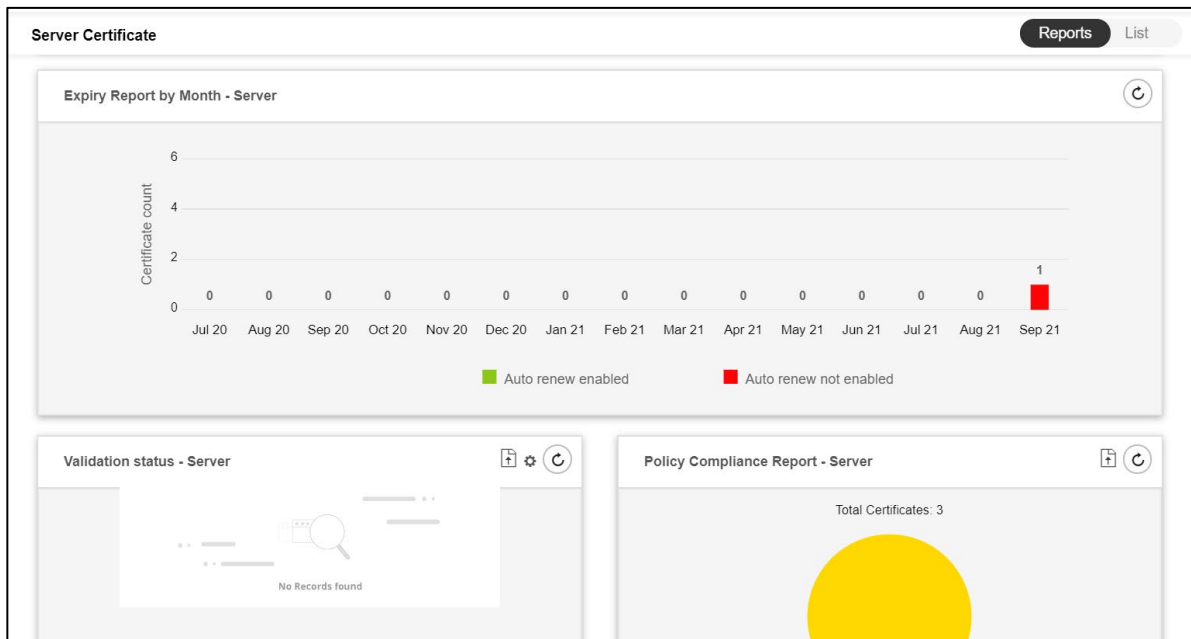
1. Click the **View SSL certificates** in the lower-right **Certificate Management** box.

The link opens in new tab; close it after task is finished.



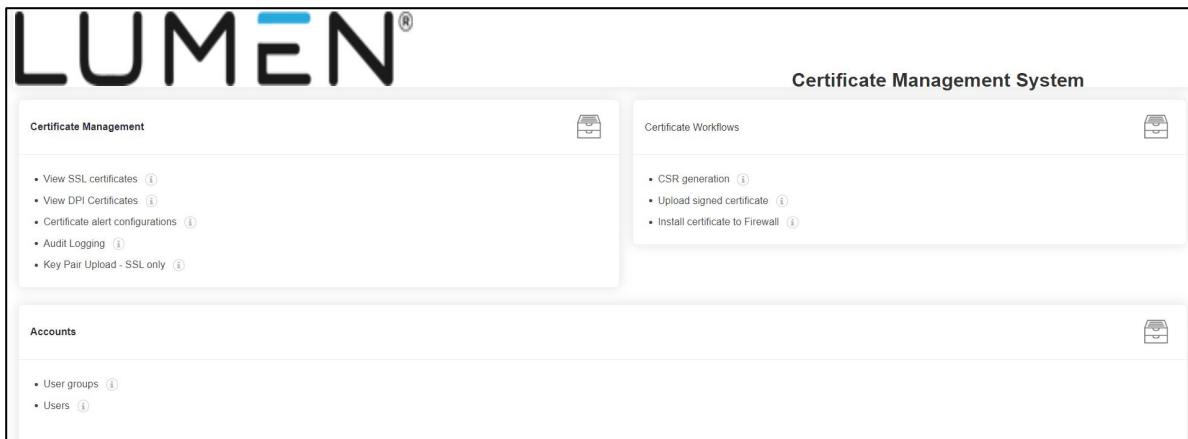
2. Click **Reports** in top-right corner of the page.

The page contains details of certificate. Expiry dates, policy compliance and other details

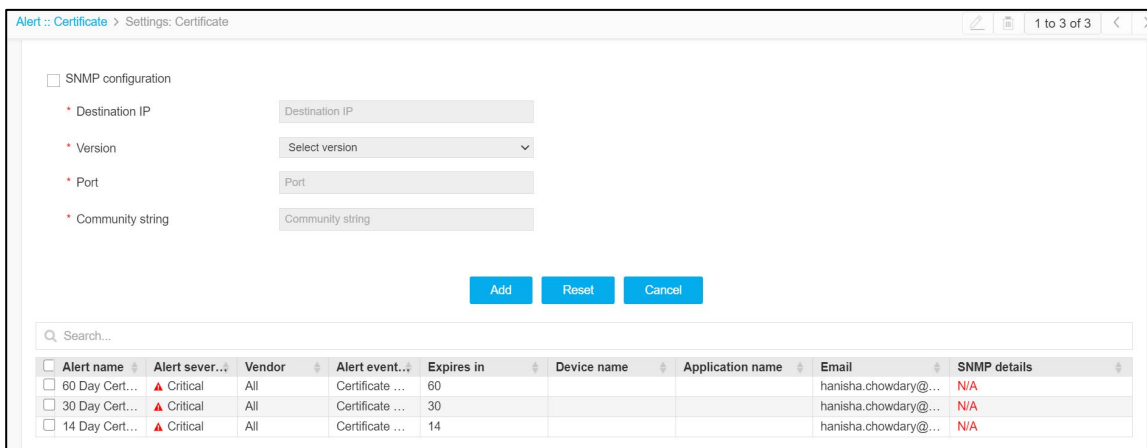


Setting up certificate alerts

1. Click on the **Certificate alert configuration** from the lower-right **Certificate Management** box. This page is displayed upon CMS login. The Link opens in new tab, and this welcome page will exist in the current tab.



2. Scroll down to the end of page, here you can find the alerts, as shown below. The alerts are set by default for 60, 30 and 14 days, also the alert email will be sent to email given in the tenant creation, that is email of the customer admin.



We suggest you edit this email to the DL email list associated to your team.

3. Select the alert you want to modify, and then click on the top right pencil icon to modify it.

Alert :: Certificate > Settings: Certificate 1 to 3 of 3

(Use comma separated for multiple entries)

Subject:

SNMP configuration

* Destination IP:

* Version:

* Port:

* Community string:

Search...

<input type="checkbox"/>	Alert name	Alert sever...	Vendor	Alert event...	Expires in	Device name	Application name	Email	SNMP details
<input checked="" type="checkbox"/>	60 Day Cert...	▲ Critical	All	Certificate ...	60			hanisha.chowdary@...	N/A
<input type="checkbox"/>	30 Day Cert...	▲ Critical	All	Certificate ...	30			hanisha.chowdary@...	N/A
<input type="checkbox"/>	14 Day Cert...	▲ Critical	All	Certificate ...	14			hanisha.chowdary@...	N/A

4. Change the email address in the **Email Configuration** section to a DL mailing list preferably.

Alert :: Certificate > Settings: Certificate 1 to 3 of 3

Certificate | Syslog | SSH | AppViewX | ADC

* Alert name:

* Event type: * Alert severity:

* Certificate category:

* Expires in (days):

Email configuration

* Email address:
(Use comma separated for multiple entries)

Subject:

SNMP configuration

5. Click **Update**.

Email configuration

* Email address
(Use comma seperated for multiple entries)

Subject

SNMP configuration

* Destination IP

* Version

* Port

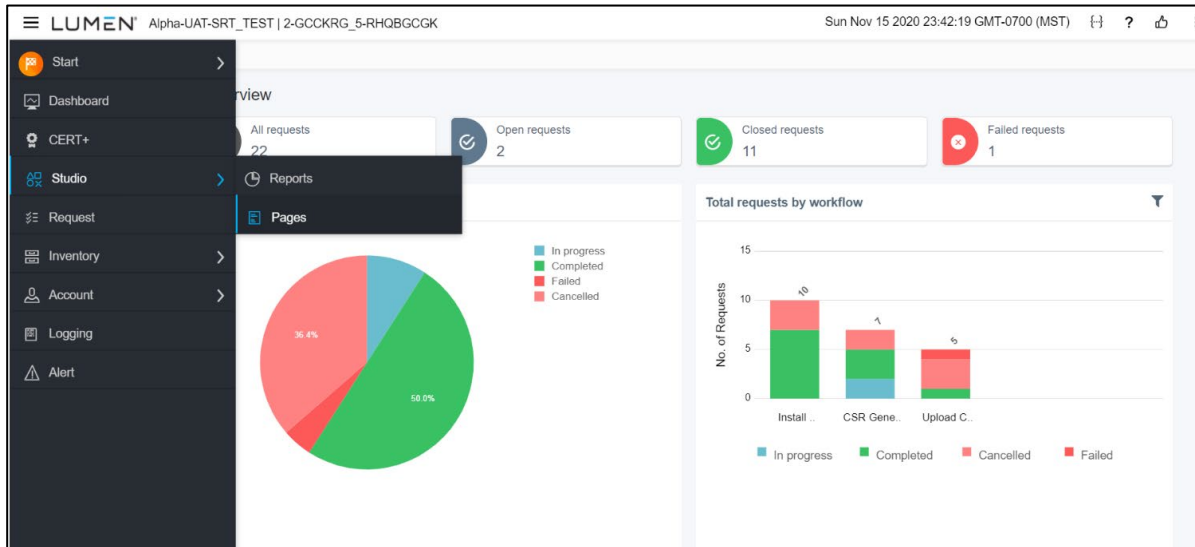
* Community string

6. The email has changed to email updated in above step.

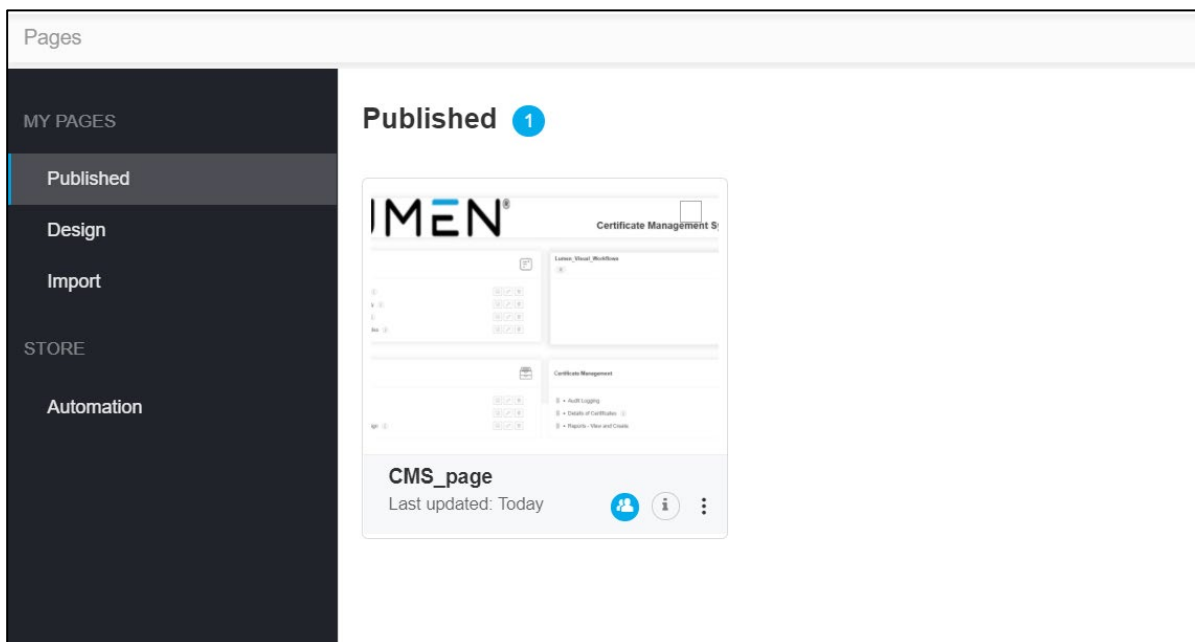
Alert name	Alert sever...	Vendor	Alert event..	Expires in	Device name	Application name	Email	SNMP details
<input type="checkbox"/> 60 Day Cert...	▲ Critical	All	Certificate ...	60			DL_Email@compan...	N/A
<input type="checkbox"/> 30 Day Cert...	▲ Critical	All	Certificate ...	30			hanisha.chowdary@...	N/A
<input type="checkbox"/> 14 Day Cert...	▲ Critical	All	Certificate ...	14			hanisha.chowdary@...	N/A

Reverting to Welcome Page section

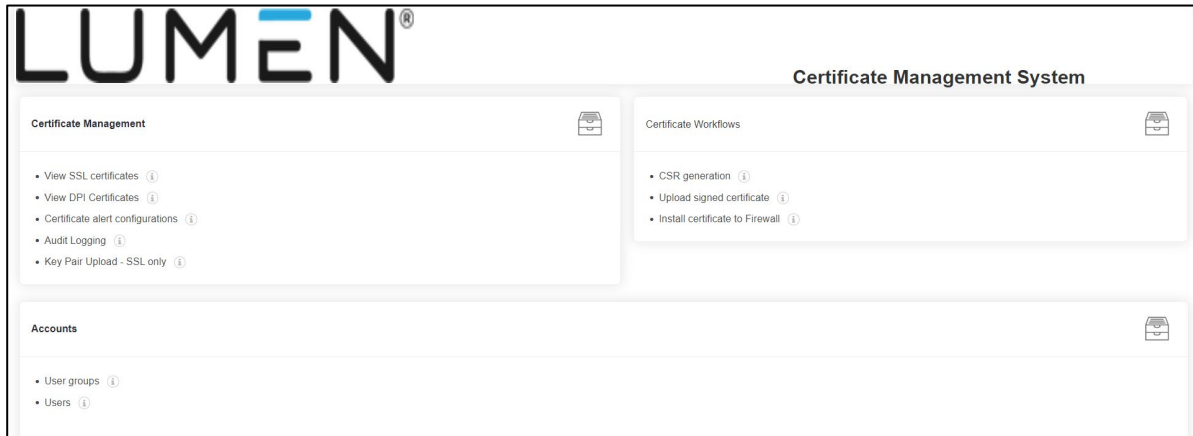
18. Click on the hamburger on the top left, click on **Studio → Pages**.



19. Click on the **CMS_page**.



20. The page will be displayed as below.



For additional assistance on Control Center, go to:

- [Control Center Admin support](#). This includes [Security Tokens Control Center support](#) if you need two-factor security token on Control Center.
- [Security Support Contacts](#) if you need further Control Center Portal Support Center assistance.

Additional references

- Guide to using Microsoft CA for DPI, to sign the intermediate certificates with internal/customer's CA:
<https://docs.fortinet.com/document/fortigate/6.2.9/cookbook/680736/microsoft-ca-deep-packet-inspection>
- Users who don't have an internal CA could follow the instructions in the below link to sign the intermediate certificate CSR generated on CMS for DPI:
<https://dadhacks.org/2017/12/27/building-a-root-ca-and-an-intermediate-ca-using-openssl-and-debian-stretch/>
- Introduction to SSL certificates:
<https://www.digicert.com/resources/beginners-guide-to-tls-ssl-certificates-whitepaper-en-2019.pdf>
- Introduction to DPI certificates:
<https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more>
- Difference between Root and intermediate certificates:
<https://www.encryptionconsulting.com/root-vs-intermediate-certificates/>
- Certificate Terminology:
<https://wiki.mozilla.org/CA/Terminology>
- Openssl for SSL CSRs, certificates, and keys:
<https://www.digitalocean.com/community/tutorials/openssl-essentials-working-with-ssl-certificates-private-keys-and-csrs>