Lumen® Adaptive Network Security

Certificate Management System (CMS) user guide | January 2025

Contents

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.

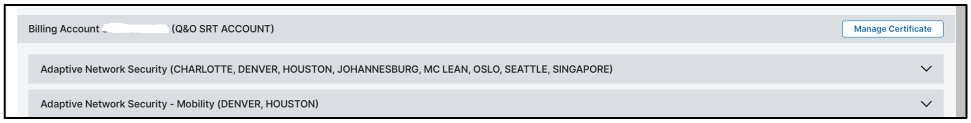
The user needs to have two-factor authentication security solution login for Control Center to access CMS (using the **Admin** tab) and other security features. During initial ANS service provisioning with DPI configuration or ANS Mobility SSL/VPN, an email with the subject 'Successfully Created the 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. Type your Control Center username, then click **NEXT**.
3. Type your password, then click **SIGN IN**.
4. 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.
5. Click Admin, then click Security Certificate Management.



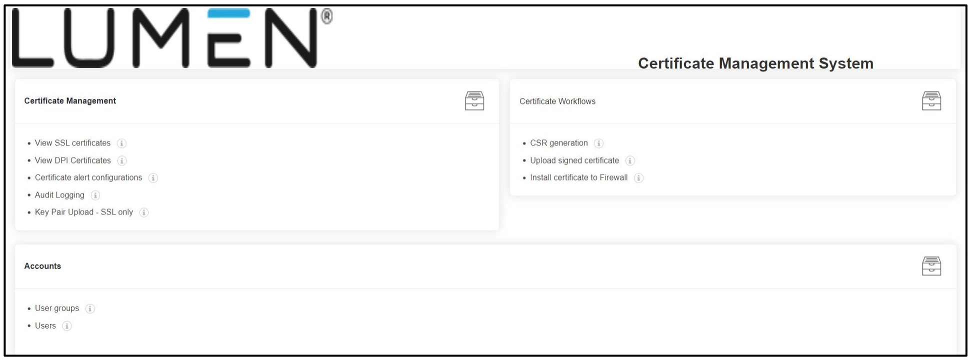
Billing Account [redacted] (Q&O SRT ACCOUNT)

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

Adaptive Network Security - Mobility (DENVER, HOUSTON)

6. 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.



Certificate Management System

Certificate Management

- View SSL certificates
- View DPI Certificates
- Certificate alert configurations
- Audit Logging
- Key Pair Upload - SSL only

Certificate Workflows

- CSR generation
- Upload signed certificate
- Install certificate to Firewall

Accounts

- User groups
- Users

7. 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.

8. 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:

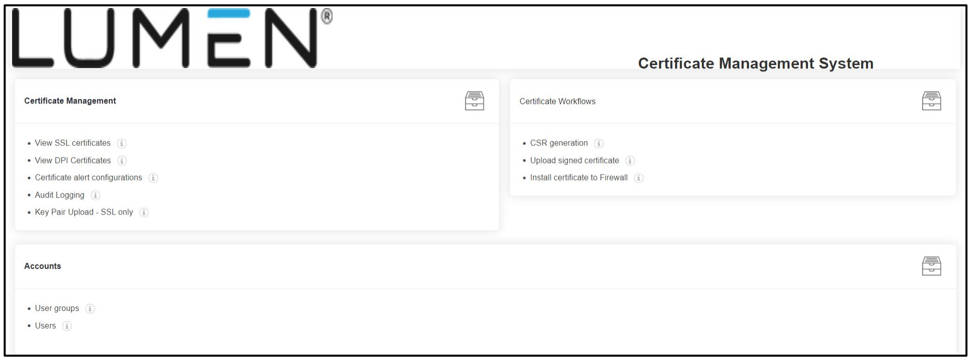
- View the certificate logs and audit logs of all users, along with certificate alerts.
- No access to workflows and Certificates.
- Access to reporting and only view the certificates.
- Cannot modify or delete any user/user groups.

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.

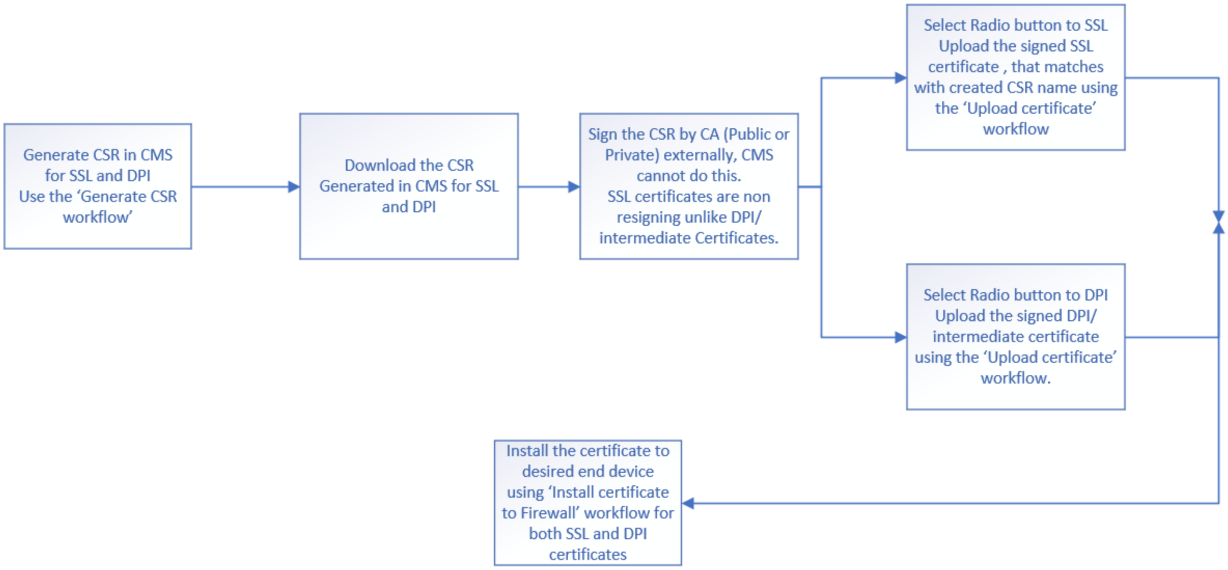
1. Click **Users** (under Accounts section of the page).


LUMEN
Certificate Management System
Certificate Management
View SSL certificates
View DPI Certificates
Certificate alert configurations
Audit Logging
Key Pair Upload - SSL only
Certificate Workflows
CSR generation
Upload signed certificate
Install certificate to Firewall
Accounts
User groups
Users

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

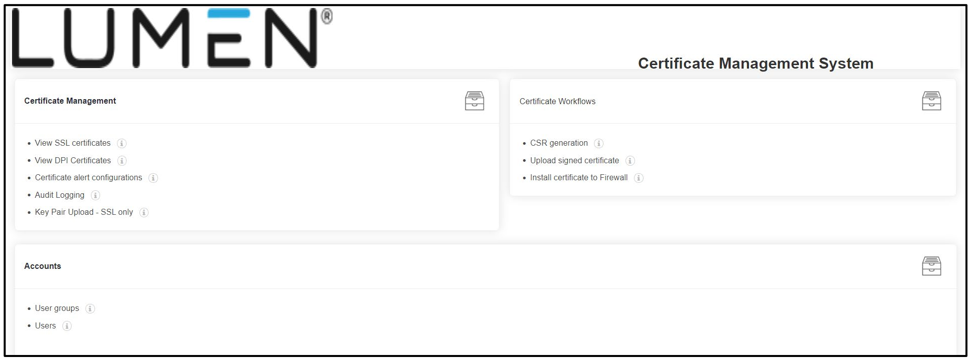

Generate CSR in CMS for SSL and DPI Use the 'Generate CSR workflow'
Download the CSR Generated in CMS for SSL and DPI
Sign the CSR by CA (Public or Private) externally, CMS cannot do this. SSL certificates are non resigning unlike DPI/ intermediate Certificates.
Select Radio button to SSL Upload the signed SSL certificate , that matches with created CSR name using the 'Upload certificate' workflow
Select Radio button to DPI Upload the signed DPI/ intermediate certificate using the 'Upload certificate' workflow.
Install the certificate to desired end device using 'Install certificate to Firewall' workflow for both SSL and DPI certificates

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 appears after you sign in to Control Center.



Certificate Management System

Certificate Management

- View SSL certificates
- View DPI Certificates
- Certificate alert configurations
- Audit Logging
- Key Pair Upload - SSL only

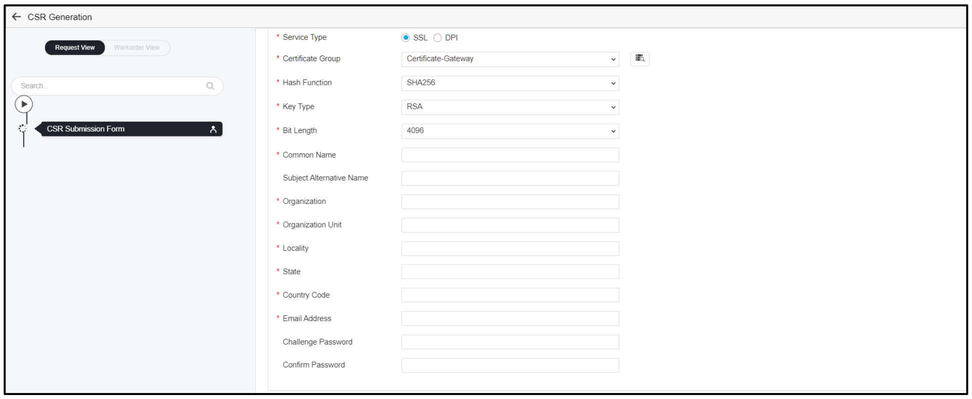
Certificate Workflows

- CSR generation
- Upload signed certificate
- Install certificate to Firewall

Accounts

- User groups
- Users

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



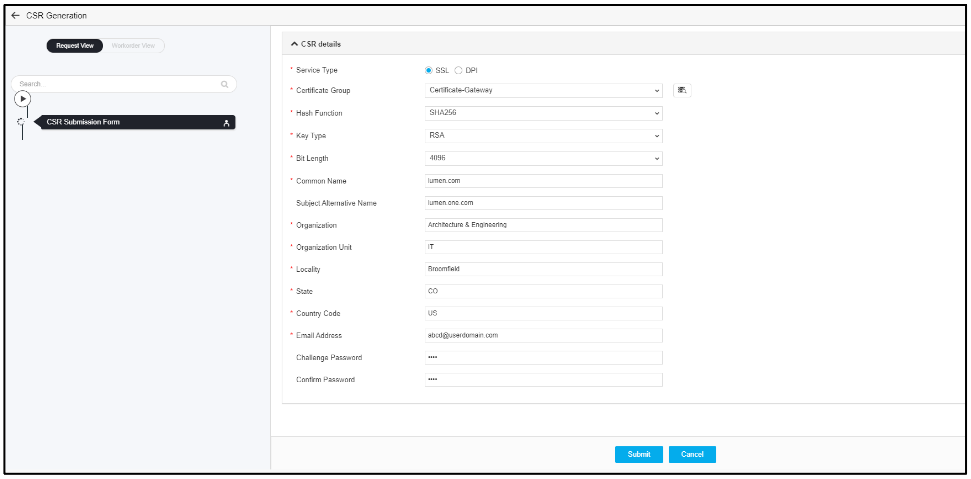
* Service Type	● SSL ○ DPI
* Certificate Group	Certificate-Gateway
* Hash Function	SHA256
* Key Type	RSA
* Bit Length	4096
* Common Name	
Subject Alternative Name	
* Organization	
* Organization Unit	
* Locality	
* State	
* Country Code	
* Email Address	
Challenge Password	
Confirm Password	

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

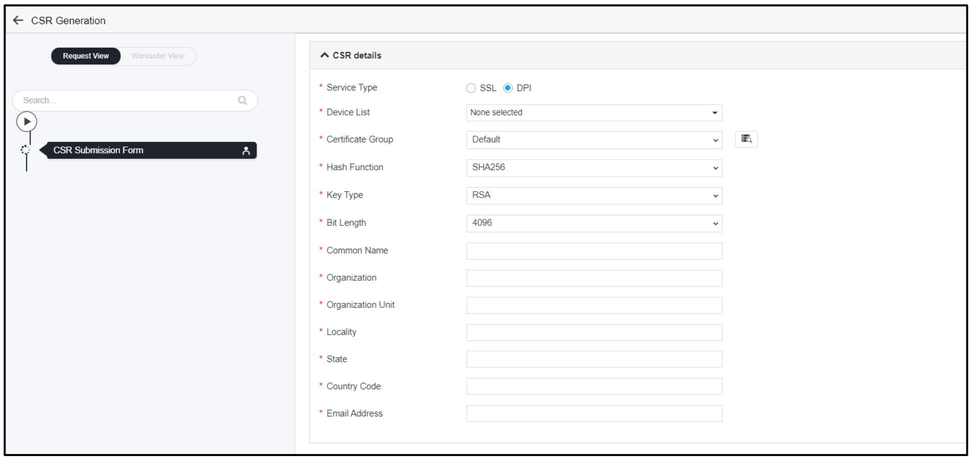
Below is a filled-out CSR generation example for SSL certificates:



* 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	••••

- 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



* Service Type	○ SSL ● DPI
* Device List	None selected
* Certificate Group	Default
* Hash Function	SHA256
* Key Type	RSA
* Bit Length	4096
* Common Name	
* Organization	
* Organization Unit	
* Locality	
* State	
* Country Code	
* Email Address	

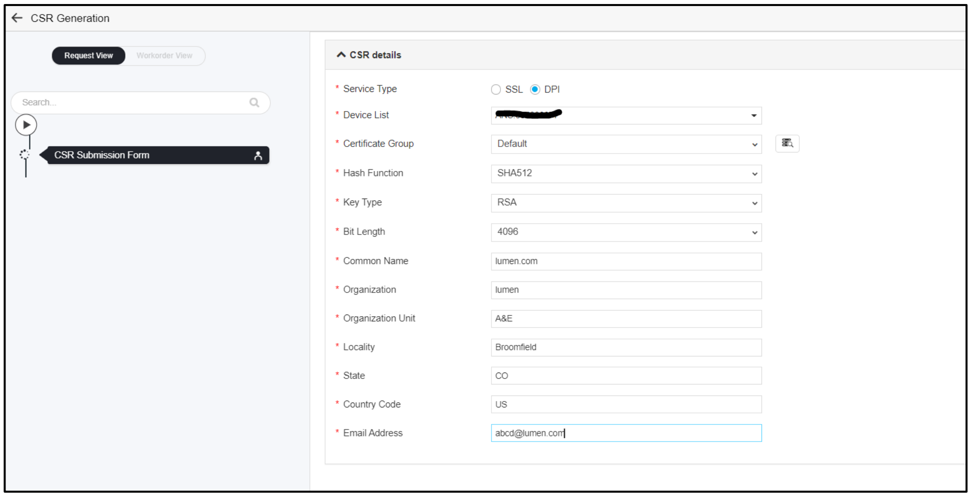
Finding the mapping between VDOM and location's firewall instance

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: 33xxxxxxx". 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**.
3. In the **Network, Security, and Communications** box, click **Adaptive Network Security**.
4. Click the service ID to view details for the service.
5. 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.


CSR Generation

Request View | Workorder View

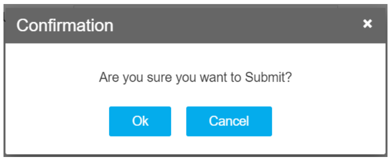
Search...

CSR Submission Form

CSR details

* 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

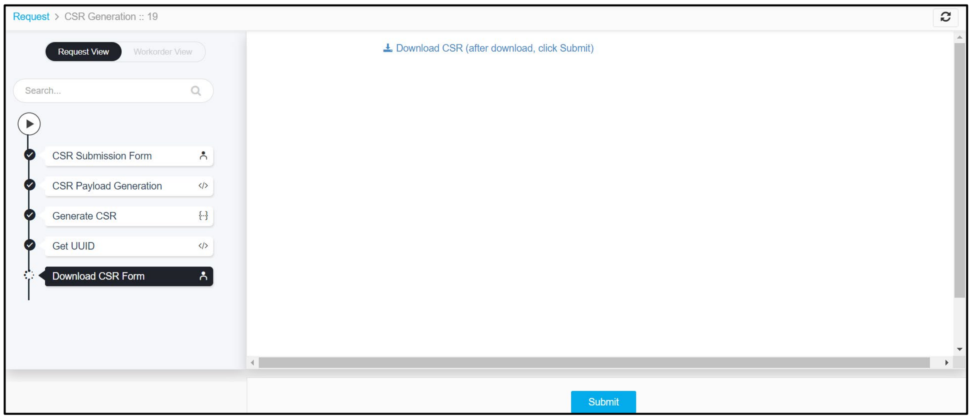
6. Click **Submit** to generate the CSR, then click **Ok** to confirm.


Confirmation ×

Are you sure you want to Submit?

Ok Cancel

7. Click **Download CSR** to download the CSR generated. Then, click **Submit**. (**Note:** Once you click **Submit**, you cannot download the CSR again.)


Request > CSR Generation :: 19

Request View | Workorder View

Search...

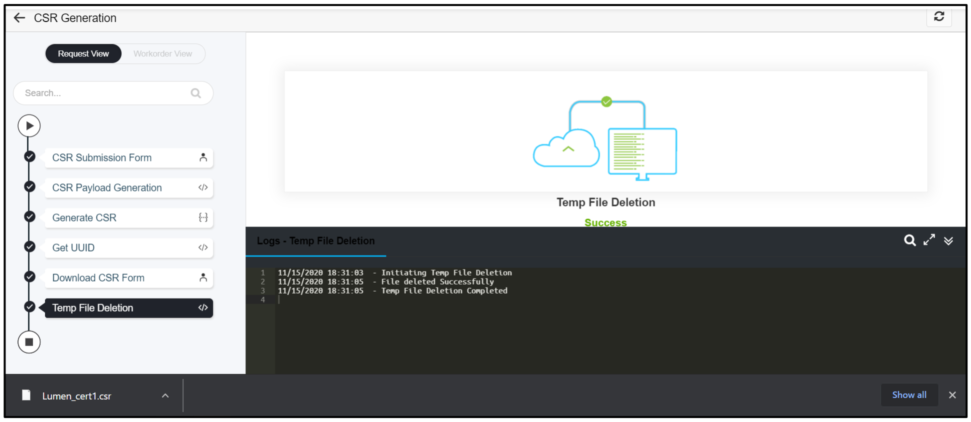
- CSR Submission Form
- CSR Payload Generation
- Generate CSR
- Get UUID
- Download CSR Form

Download CSR (after download, click Submit)

Submit

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

8. 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.



```
11/15/2020 18:31:03  - Initiating Temp File Deletion
11/15/2020 18:31:05  - File deleted Successfully
11/15/2020 18:31:05  - Temp File Deletion Completed
```

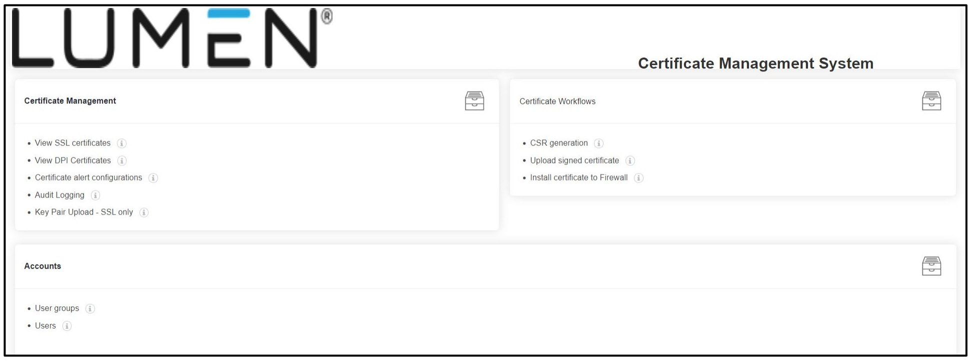
Note: The CSR file for DPI certificates will have the end device number and timestamp added to the beginning to distinguish them and map them to their associated end device at later stage during the process of Installing the certificate to end device.

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.

1. In the **Certificate Workflows** box, click **Upload Certificate**.

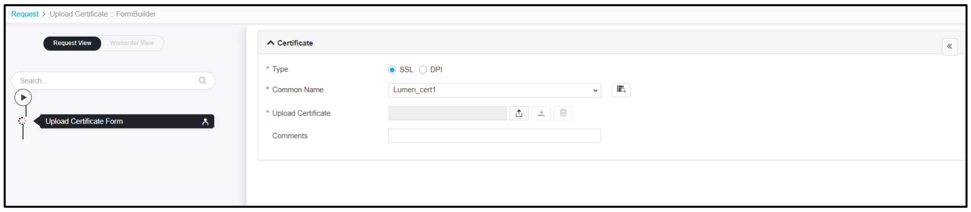

LUMEN®
Certificate Management System
Certificate Management
View SSL certificates
View DPI Certificates
Certificate alert configurations
Audit Logging
Key Pair Upload - SSL only
Certificate Workflows
CSR generation
Upload signed certificate
Install certificate to Firewall
Accounts
User groups
Users

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.

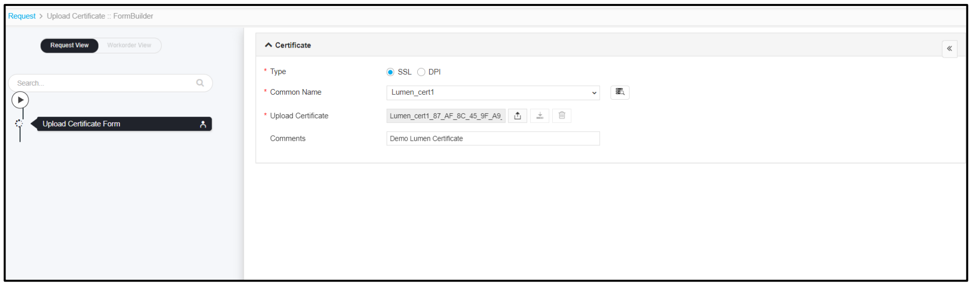
2. Select the **SSL** for type of certificate. Select the 'Common Name' of the Certificate you wish to upload, browse your PC, and upload the signed certificate (SSL or DPI) associated to that common name, expected formats are .crt,.pem,.pfx,.der.

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



* Type: ● SSL ○ DPI
* Common Name: Lumen_cert1
* Upload Certificate:
Comments:

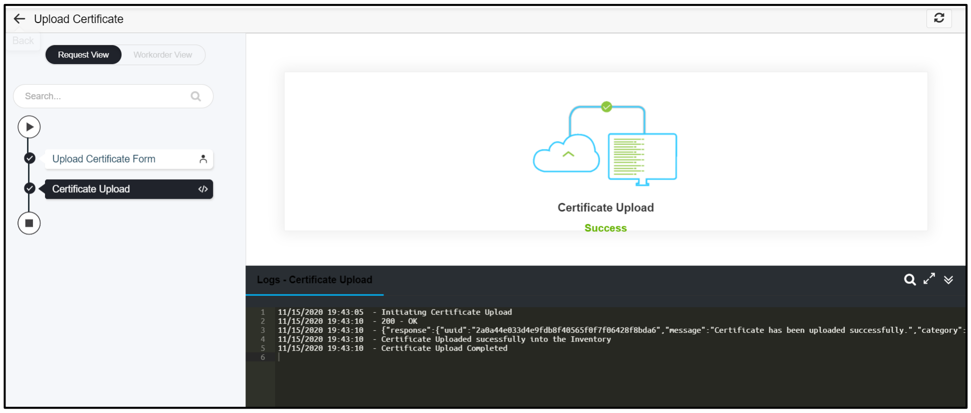
Example:



* Type: ● SSL ○ DPI
* Common Name: Lumen_cert1
* Upload Certificate: Lumen_cert1_87_AF_8C_45_9F_A9_
Comments: Demo Lumen Certificate

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

4. 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.

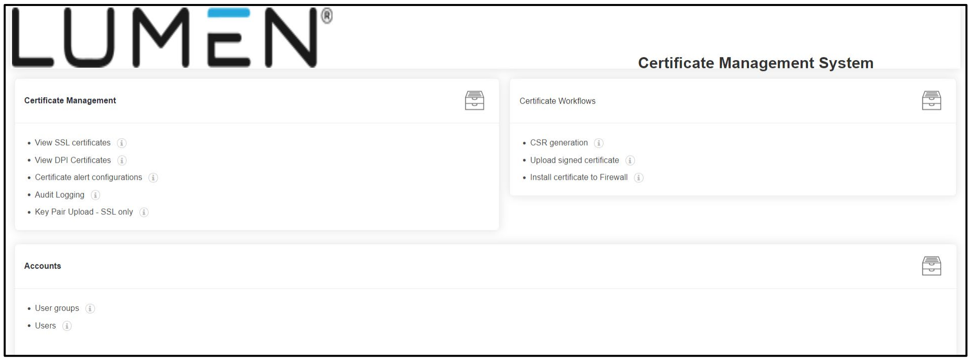


```
11/15/2020 19:43:05  - Initiating Certificate Upload
11/15/2020 19:43:10  - 200 - OK
11/15/2020 19:43:10  - {"response":{"uuid":"2a0a44e033d4e9fdb8f40565f0f7f06428f8bda6","message":"Certificate has been uploaded successfully.","category":
11/15/2020 19:43:10  - Certificate Uploaded sucessfully into the Inventory
11/15/2020 19:43:10  - Certificate Upload Completed
```

Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice.

2. Upload a signed DPI/intermediate certificate.

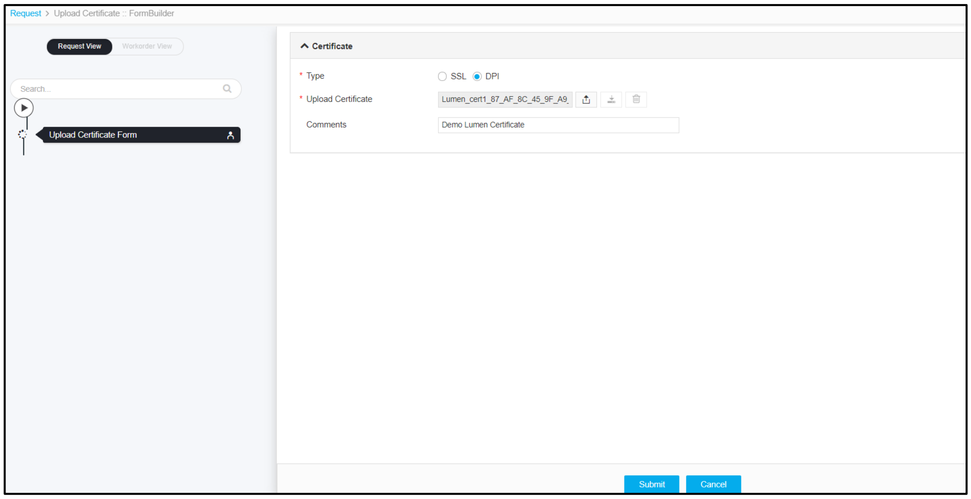
1. In the **Certificate Workflows** box, click **Upload signed certificates**.



2. Select the **DPI** in type of certificate. Click **Upload** 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.



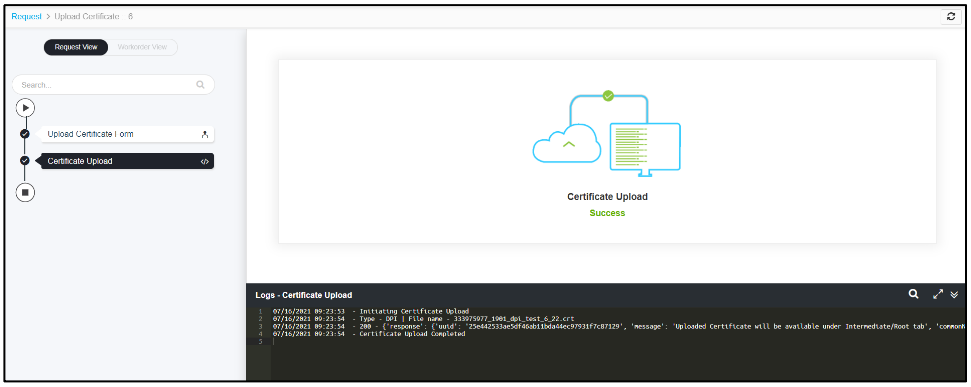
* Type ○ SSL ● DPI

* Upload Certificate Lumen_cert1_87_AF_8C_45_9F_A9_

Comments Demo Lumen Certificate

Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice.

4. Upon successful upload, the screen below appears. To view the uploaded certificate, click **View DPI certificates**.

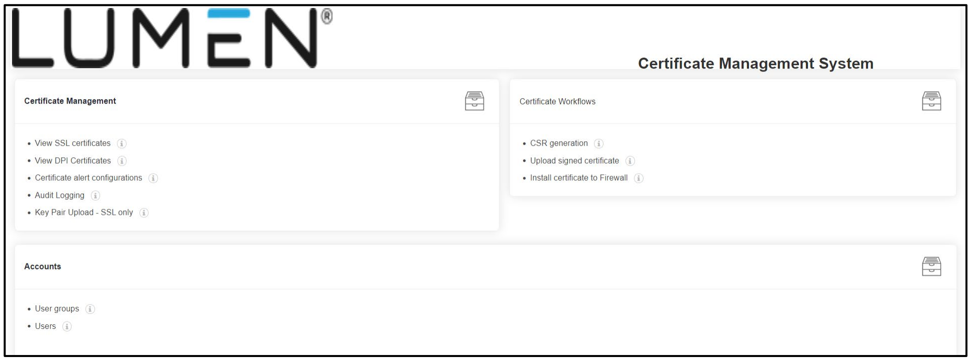


```
07/16/2021 09:23:53  - Initiating Certificate Upload
07/16/2021 09:23:54  - Type - DPI | File name - 333975977_1901_dpi_test_6_22.crt
07/16/2021 09:23:54  - 200 - {'response': {'uuid': '25e442533ae5df46ab11bda44ec97931f7c87129', 'message': 'Uploaded Certificate will be available under Intermediate/Root tab', 'commonN
07/16/2021 09:23:54  - Certificate Upload Completed
```

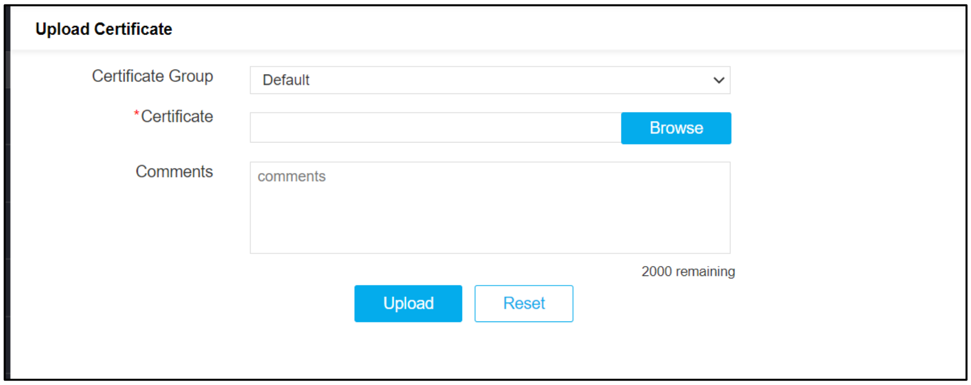
3. Key Pair Upload Option (where CSR was not generated using CMS, only for SSL certificates)

1. In the **Certificate Management** box, click **Key pair upload**.

   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.


Certificate Management System
Certificate Management
View SSL certificates
View DPI Certificates
Certificate alert configurations
Audit Logging
Key Pair Upload - SSL only
Certificate Workflows
CSR generation
Upload signed certificate
Install certificate to Firewall
Accounts
User groups
Users

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.



Upload Certificate

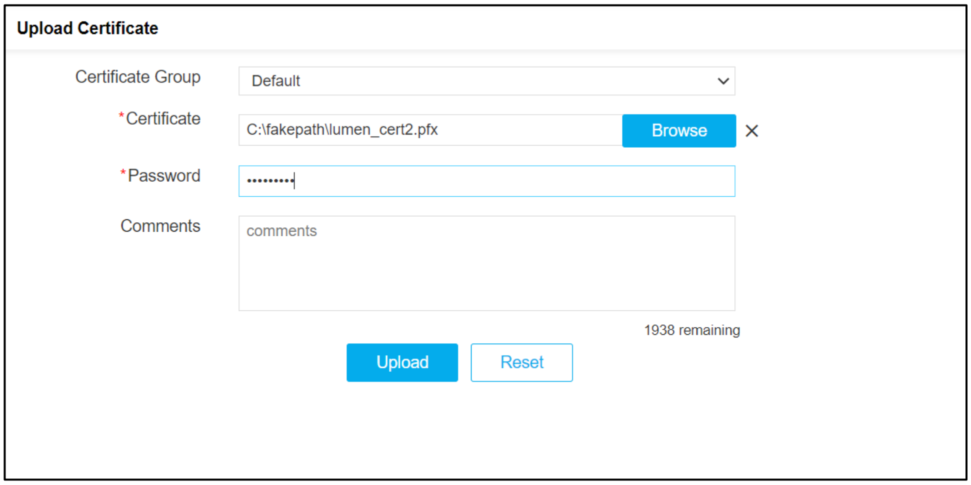
Certificate Group: Default

*Certificate:

Comments: comments

2000 remaining

Example:



Upload Certificate

Certificate Group: Default

*Certificate: C:\fakepath\lumen_cert2.pfx

*Password: •••••••••

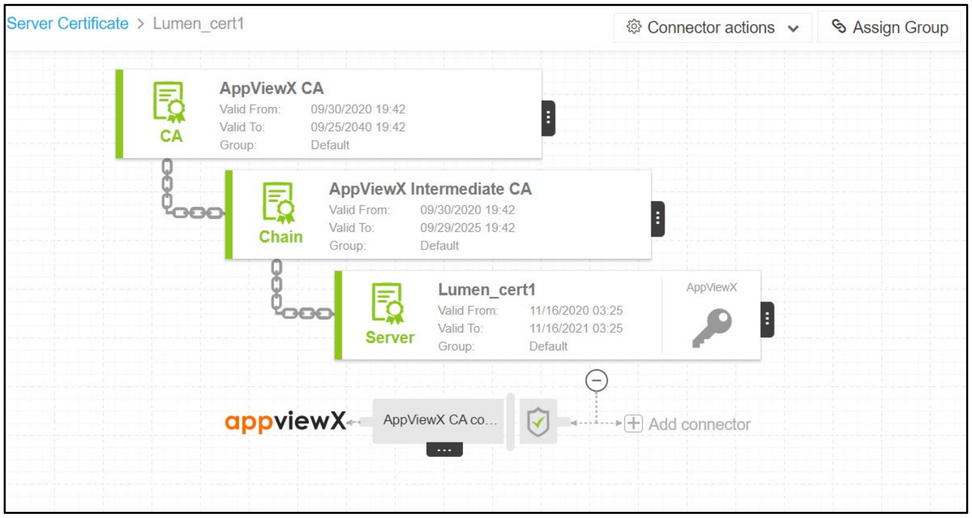
Comments: comments

1938 remaining

3. Click **Upload**.

Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice. ©2025 Lumen Technologies. All Rights Reserved.

4. 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.



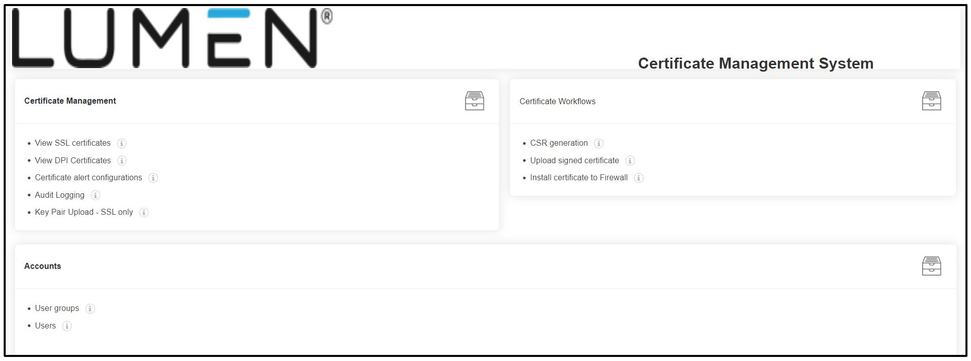
AppViewX CA
Valid From: 09/30/2020 19:42
Valid To: 09/25/2040 19:42
Group: Default

AppViewX Intermediate CA
Valid From: 09/30/2020 19:42
Valid To: 09/29/2025 19:42
Group: Default

Lumen_cert1
Valid From: 11/16/2020 03:25
Valid To: 11/16/2021 03:25
Group: Default

4. Download the SSL Certificate.

1. In the **Certificate Management** box, click **View SSL certificates**. Click **View DPI certificates** for DPI certificates.



Certificate Management System

Certificate Management

- View SSL certificates
- View DPI Certificates
- Certificate alert configurations
- Audit Logging
- Key Pair Upload - SSL only

Certificate Workflows

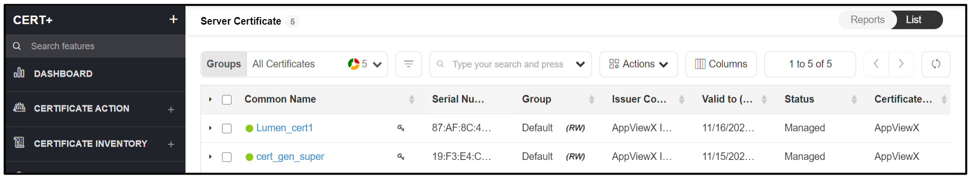
- CSR generation
- Upload signed certificate
- Install certificate to Firewall

Accounts

- User groups
- Users

Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice.

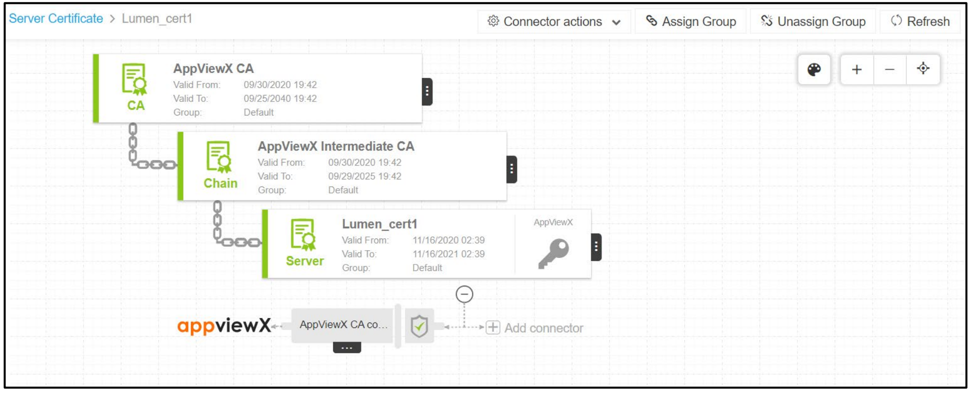
2. The following page will show the inventory of certificates created under your Customer Tenant. Click on the desired Common Name of the certificate you wish to download. The certificates under Common Name column with a green dot to identify a signed certificate and which is available to be pushed to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

3. 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.

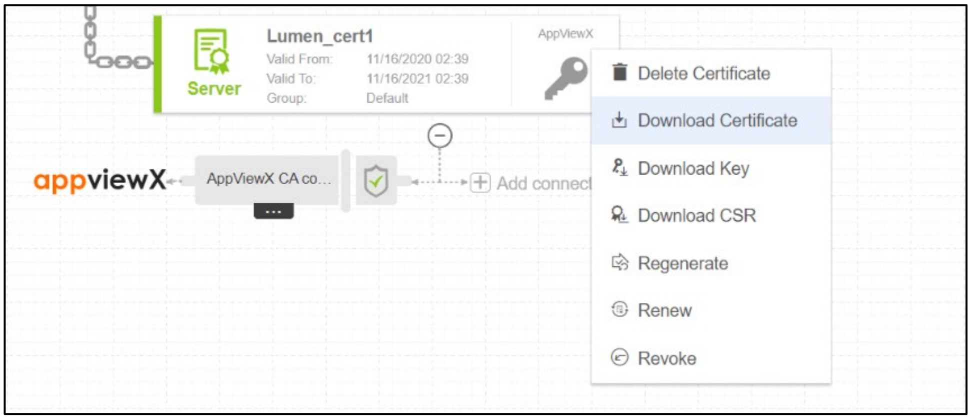


AppViewX CA
Valid From: 09/30/2020 19:42
Valid To: 09/25/2040 19:42
Group: Default

AppViewX Intermediate CA
Valid From: 09/30/2020 19:42
Valid To: 09/29/2025 19:42
Group: Default

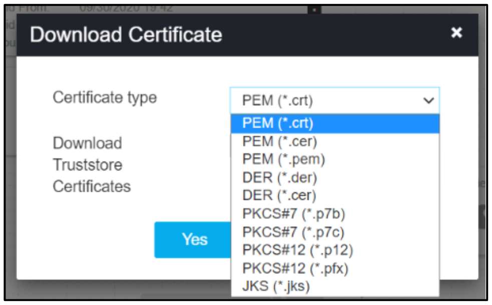
Lumen_cert1
Valid From: 11/16/2020 02:39
Valid To: 11/16/2021 02:39
Group: Default

4. Click **Download Certificate** or **Download CSR** as needed.



Lumen_cert1
Valid From: 11/16/2020 02:39
Valid To: 11/16/2021 02:39
Group: Default

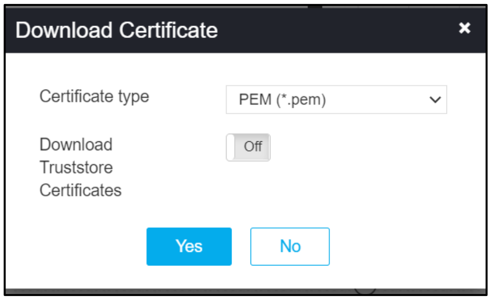
5. Below is a list of the available formats you can download the certificate or CSR in. Select the required format, and if you wish to download a private key for a CSR/certificate, a set password option will prompt you for input, which will be used to encrypt the key.



Download Certificate

Certificate type: PEM (*.crt)

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



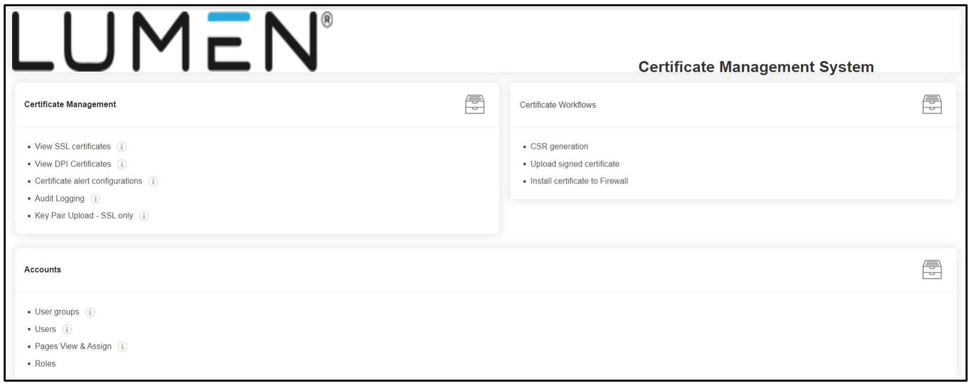
Download Certificate

Certificate type: PEM (*.pem)

Download Truststore Certificates: Off

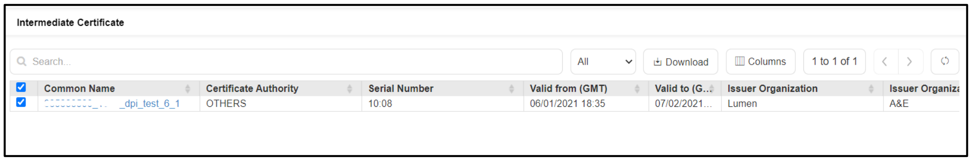
5. Download the DPI certificate.

1. In the **Certificate Management** box, click **View DPI certificates**.



Certificate Management System

2. 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.



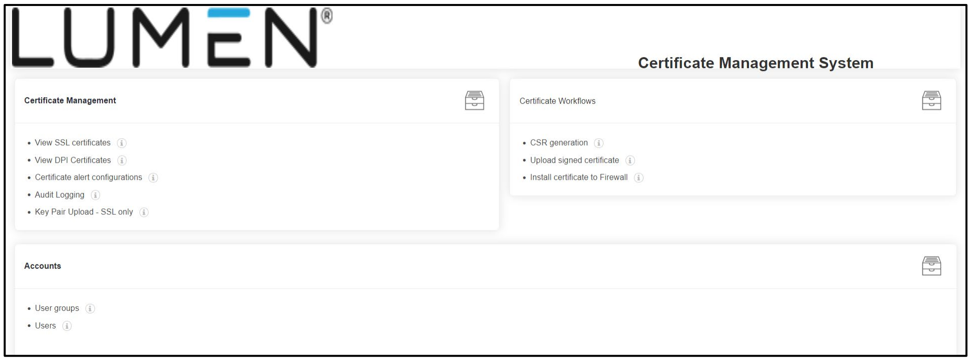
Intermediate Certificate

☑	Common Name	Certificate Authority	Serial Number	Valid from (GMT)	Valid to (G...	Issuer Organization	Issuer Organiza
☑	[redacted]_dpi_test_6_1	OTHERS	10:08	06/01/2021 18:35	07/02/2021...	Lumen	A&E

3. Click **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

1. In the **Certificate Workflows** box, click **Install certificate to Firewall**.



Certificate Management System

Certificate Management

- View SSL certificates
- View DPI Certificates
- Certificate alert configurations
- Audit Logging
- Key Pair Upload - SSL only

Certificate Workflows

- CSR generation
- Upload signed certificate
- Install certificate to Firewall

Accounts

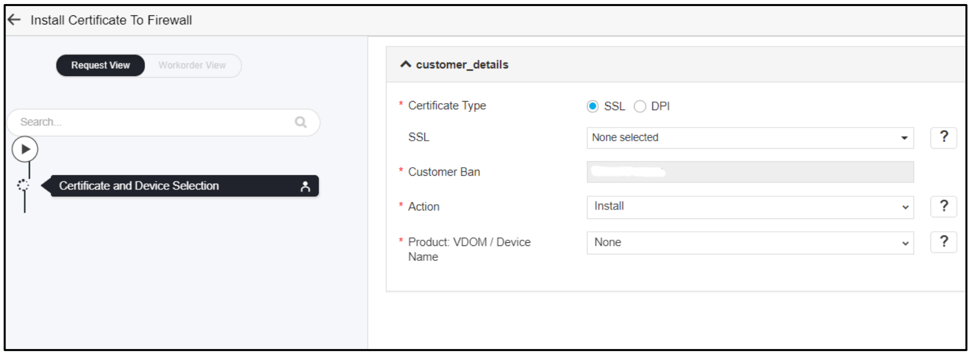
- User groups
- Users

2. 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.



Install Certificate To Firewall

Certificate and Device Selection

customer_details

* Certificate Type ● SSL ○ DPI

SSL: None selected ?

* Customer Ban: [redacted]

* Action: Install ?

* Product: VDOM / Device Name: None ?

3. 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, contact the technical design engineer for your order.

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

4. Sign in to Control Center using 2FA.

5. Click **Services**.

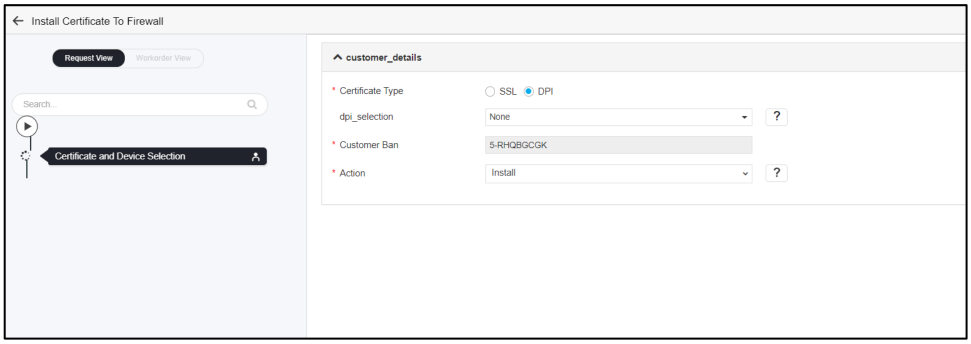
6. In the **Network, Security, and Communications** box, click **Adaptive Network Security** filter for the product.

7. Click the service ID number to expand the details. Association between service ID and SCIDs (VDOM identifier) can be found here. Once the VDOM is identified, revert to the **Install Certificate to Firewall** tab and continue with the next step.

   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.

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

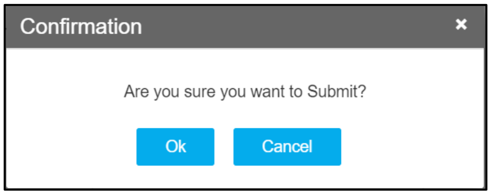


Install Certificate To Firewall

customer_details

- * Certificate Type: ○ SSL ● DPI
- dpi_selection: None
- * Customer Ban: 5-RHQBGCGK
- * Action: Install

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

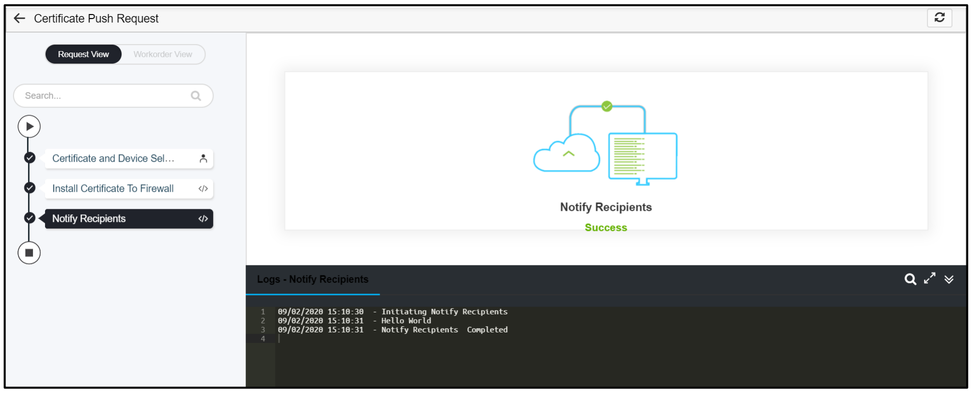


Confirmation

Are you sure you want to Submit?

10. The below page indicates the 'push' workflow was successful. Do not go back mid process. Please wait until the execution is complete. 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.



Notify Recipients

Success

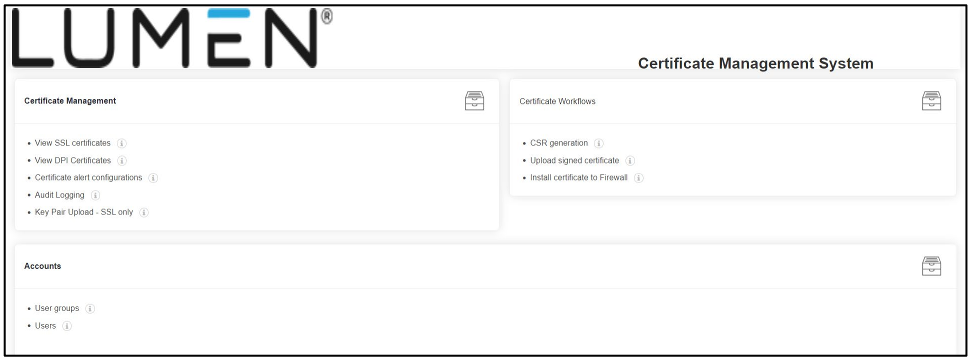
Logs - Notify Recipients

```
09/02/2020 15:10:30  - Initiating Notify Recipients
09/02/2020 15:10:31  - Hello World
09/02/2020 15:10:31  - Notify Recipients  Completed
```

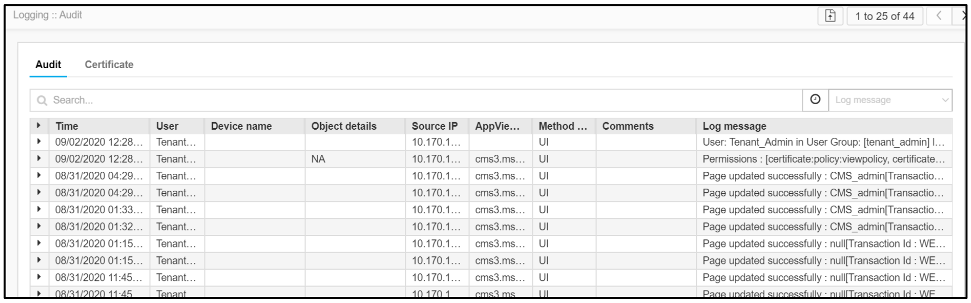
Managing certificates

Viewing the certificate logs

1. In the **Certificate Management** box, click **Audit Logging**.



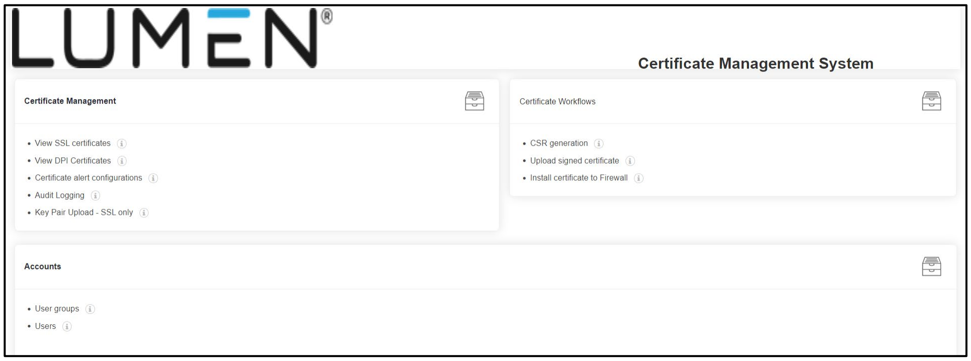
2. You can view the Audit and the certificate logs here:



Time	User	Device name	Object details	Source IP	AppVie…	Method …	Comments	Log message
09/02/2020 12:28…	Tenant…			10.170.1…		UI		User: Tenant_Admin in User Group: [tenant_admin] I…
09/02/2020 12:28…	Tenant…		NA	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

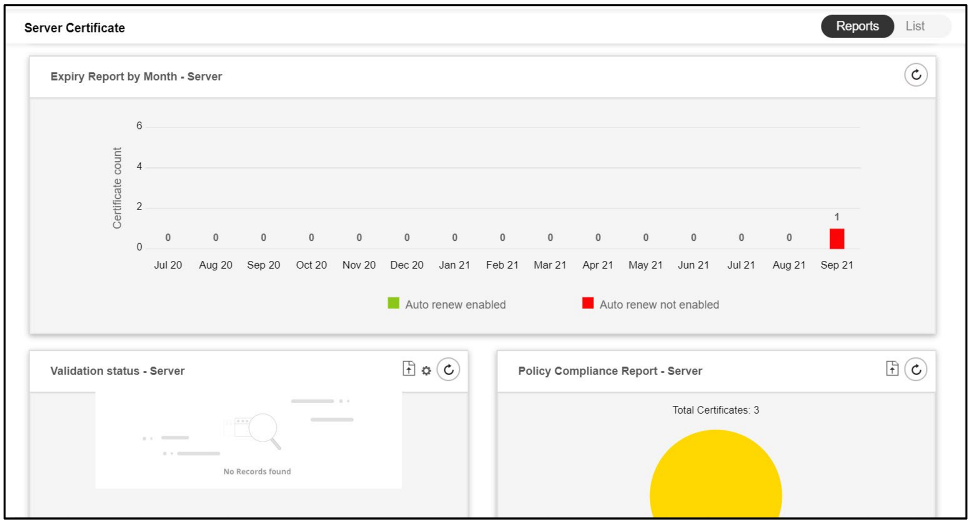
Viewing the SSL certificate inventory using the server dashboard

1. In the **Certificate Management** box, click **View SSL certificates**.



2. In the upper-right corner, click **Reports**.

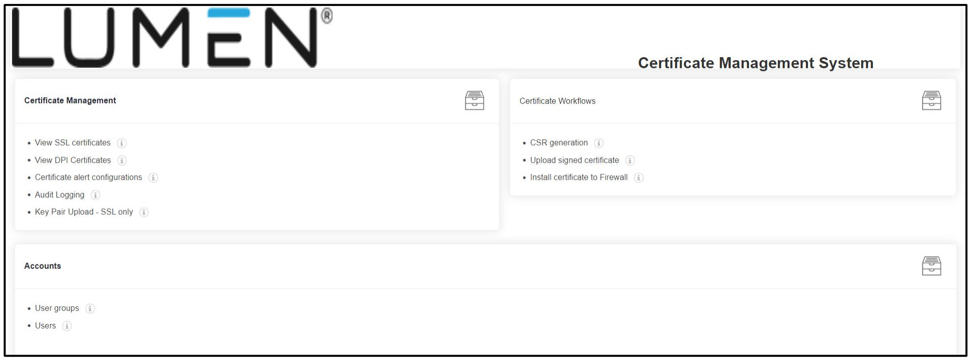
   The page contains details of the certificate: expiry dates, policy compliance, and other details.



.

Setting up certificate alerts

1. In the **Certificate Management** box, click **Certificate alert configuration**.



Certificate Management System

Certificate Management

- View SSL certificates
- View DPI Certificates
- Certificate alert configurations
- Audit Logging
- Key Pair Upload - SSL only

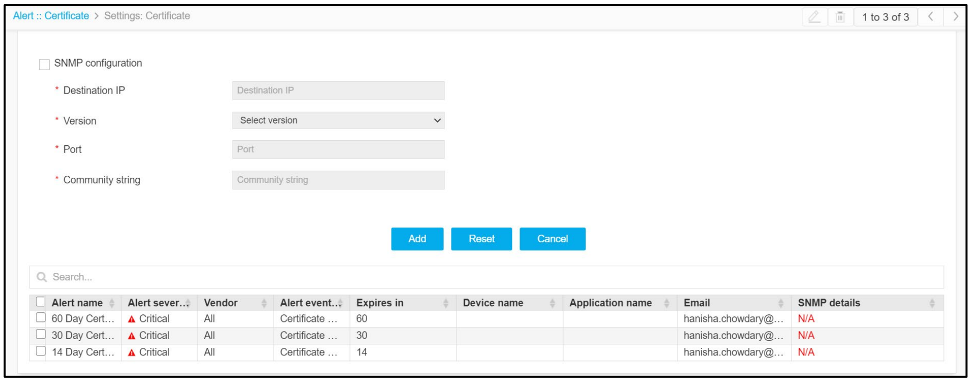
Certificate Workflows

- CSR generation
- Upload signed certificate
- Install certificate to Firewall

Accounts

- User groups
- Users

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.



□ SNMP configuration

* Destination IP — Destination IP

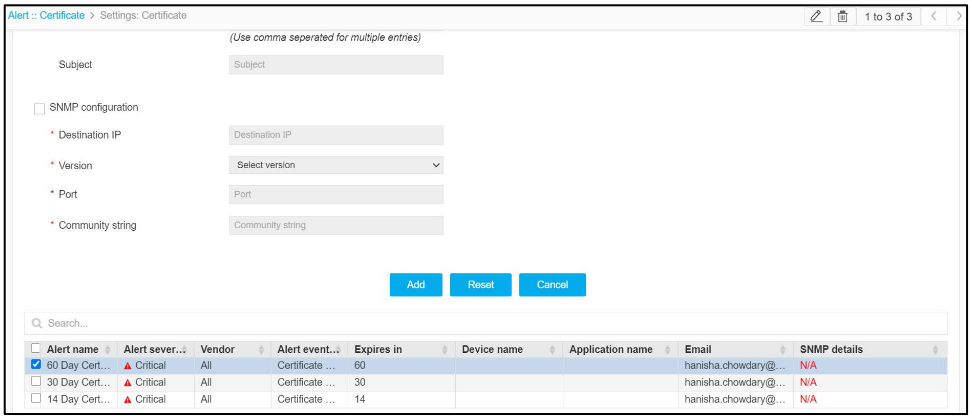
* Version — Select version

* Port — Port

* Community string — Community string

□ Alert name	Alert sever...	Vendor	Alert event...	Expires in	Device name	Application name	Email	SNMP details
□ 60 Day Cert...	▲ Critical	All	Certificate ...	60			hanisha.chowdary@...	N/A
□ 30 Day Cert...	▲ Critical	All	Certificate ...	30			hanisha.chowdary@...	N/A
□ 14 Day Cert...	▲ Critical	All	Certificate ...	14			hanisha.chowdary@...	N/A

3. Select the alert you want to modify, then click the pencil icon (in the upper-right corner) to modify it.



(Use comma seperated for multiple entries)

Subject — Subject

□ SNMP configuration

* Destination IP — Destination IP

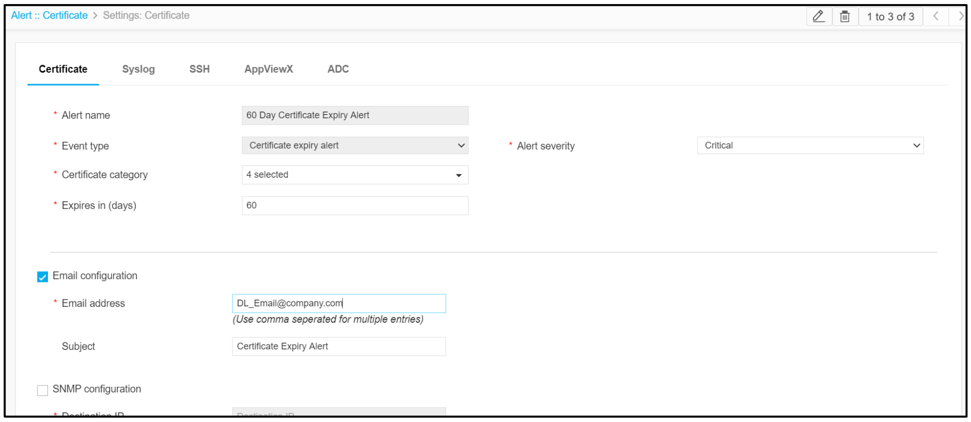
* Version — Select version

* Port — Port

* Community string — Community string

□ Alert name	Alert sever...	Vendor	Alert event...	Expires in	Device name	Application name	Email	SNMP details
☑ 60 Day Cert...	▲ Critical	All	Certificate ...	60			hanisha.chowdary@...	N/A
□ 30 Day Cert...	▲ Critical	All	Certificate ...	30			hanisha.chowdary@...	N/A
□ 14 Day Cert...	▲ Critical	All	Certificate ...	14			hanisha.chowdary@...	N/A

4. In the **Email Configuration** section, change the email address (preferably to a distribution list (DL)).



* Alert name — 60 Day Certificate Expiry Alert

* Event type — Certificate expiry alert

* Alert severity — Critical

* Certificate category — 4 selected

* Expires in (days) — 60

☑ Email configuration

* Email address — DL_Email@company.com

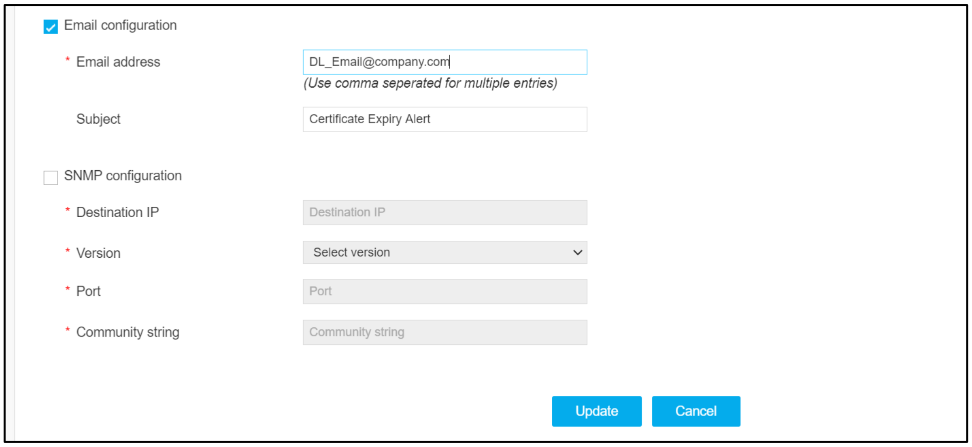
(Use comma seperated for multiple entries)

Subject — Certificate Expiry Alert

□ SNMP configuration

* Destination IP — Destination IP

5. Click **Update**.



☑ Email configuration

* Email address: DL_Email@company.com

(Use comma seperated for multiple entries)

Subject: Certificate Expiry Alert

□ SNMP configuration

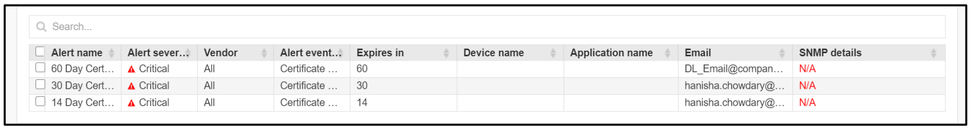
* Destination IP: Destination IP

* Version: Select version

* Port: Port

* Community string: Community string

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

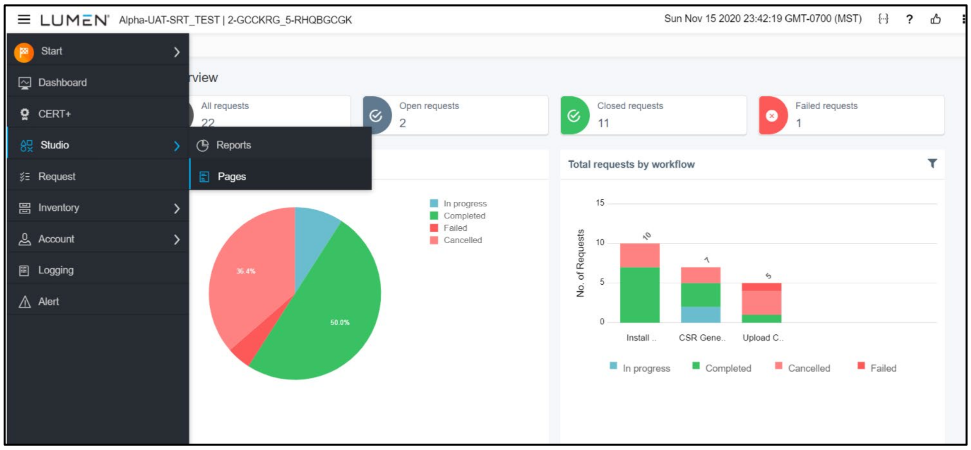


Search...

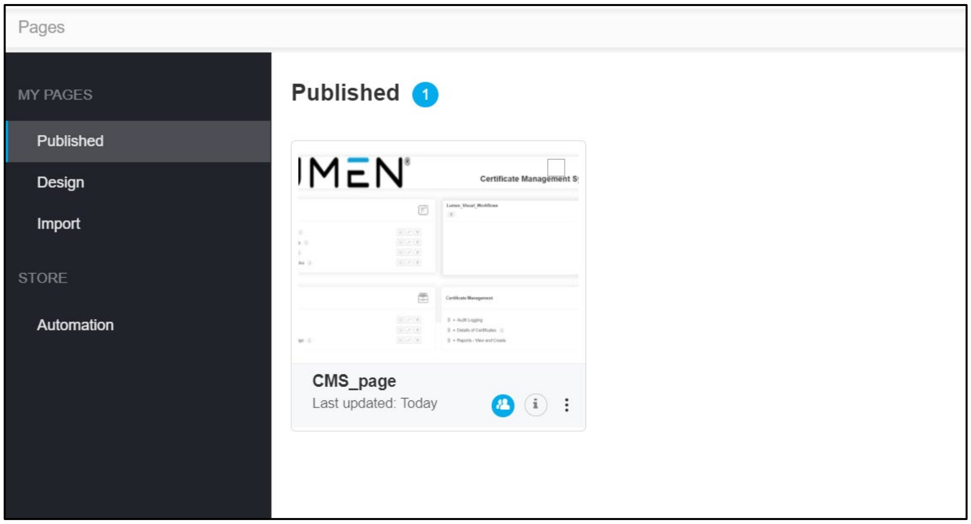
□	Alert name	Alert sever...	Vendor	Alert event...	Expires in	Device name	Application name	Email	SNMP details
□	60 Day Cert...	▲ Critical	All	Certificate ...	60			DL_Email@compan...	N/A
□	30 Day Cert...	▲ Critical	All	Certificate ...	30			hanisha.chowdary@...	N/A
□	14 Day Cert...	▲ Critical	All	Certificate ...	14			hanisha.chowdary@...	N/A

Reverting to Welcome Page section

1. Click the hamburger menu (in the upper-left corner), then click on **Studio → Pages**.



2. Click on the **CMS_page**.



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
- Introduction to DPI certificates
- Difference between root and intermediate certificates
- Certificate terminology
- OpenSSL for SSL CSRs, certificates, and keys