Lumen® Adaptive Network Security

Certificate Management System (CMS)
Quick start guide | October 2021

The Lumen Certificate Management system (CMS) platform is an automated, systematic, and secure way for you to apply or change SSL certificates with Lumen Security Services platform. You can access CMS from Control Center using your two-factor authentication security login.

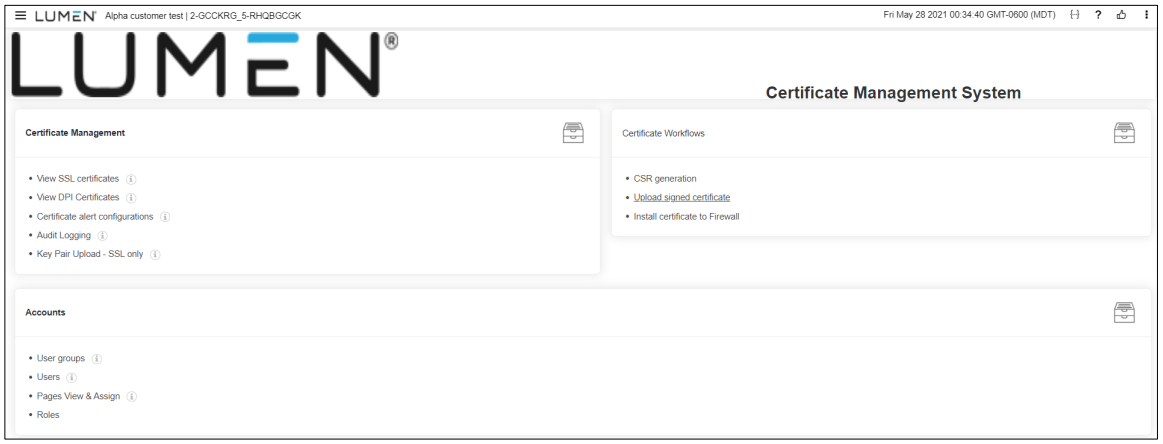
1. Sign in to Control Center using your two-factor authentication. (Two-factor authentication is required to access security capabilities in Control Center, like CMS, which cannot be accessed if skipped.)

2. Click **Admin**, then click **Security Certificate Management**. (Must have a role assigned in Control Center to view this product. The default role is cert-mgr-admin.)

3. Click **Manage Certificate** associated to your Adaptive Network Security billing account number (BAN).

   You will be redirected to CMS.

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



5. If you already have an SSL signed certificate with a key that you wish to deploy on the Lumen firewall instance aka Virtual Domain (VDOM), skip steps 6–10. Instead, follow the 'upload key pair' option from the CMS user guide under Adaptive Network Security, and proceed with step 11. Please note, this is only for SSL certificates, for DPI certificates proceed with Step 6.

6. Select **SSL** radio button for SSL certificates and **DPI** radio button for intermediate/DPI certificates

7. Select **Generate a CSR** (certificate signing request) under the **Workflows** section on the welcome page. If you need help generating a CSR, refer to the CMS Customer Guide under Adaptive Network Security. If creating a DPI CSR, the customer is required to choose a VDOM. VDOM number maps to the SCID (Service component) for ANS associated with the order number/service ID on the control center inventory tab, for further details on how to find the VDOM number associated with the firewall, please refer to the complete CMS user guide.

8. Download CSR as part of the workflow. DPI CSRs cannot be accessed later, so please be sure to download it.

9. Sign the CSR by your private or public certificate authority (CA) outside of CMS.

   Note: CMS does not currently provide a certificate authority to sign the CSR.

10. Upload only the signed certificate with matching common name (not any root certificate) for SSL certificates and signed intermediate certificates for DPI.

11. Click **Install certificate to Firewall** workflow from the page to install SSL and DPI certificate to Lumen firewall instance (known as VDOM).

12. Click on **Get VDOM details** in the workflow, pick the **SSL** radio button for SSL certificates and DPI radio button for DPI certificates. For SSL certificates, VDOM number maps to the SCID (Service component) for ANS associated with the order number/service ID on the control center inventory tab, for further details on how to find the VDOM number associated with the firewall, please refer to the complete CMS user guide.

13. Choose the VDOM and certificate you wish to deploy on the VDOM along with the action to be performed (Install, Update or delete. Refer to the customer guide for details on each of the options.) and click **Submit** to complete the installation.

14. Basic alerting is configured at startup, sending alerts to the admin email used to initiate the onboarding process. For best practice, we recommend editing the destination in those default alerts, to include a distribution list vs a single email. You can also configure specific alerting, through the **Alerts- View and Create** link of the welcome page, refer to the documentation on alerts if further assistance is required.

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 Information Links

- Guide to utilizing 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