Enabling PKI on Spectre Portal

This page explains how to enable PKI so that users can log in to the Portal and Command Centers with certificates or smart cards instead of passwords. The process assumes that your organization already has the necessary certificates:

For server authentication:
- A server certificate in PKCS12 format containing both public and private keys

For user authentication and authorization in the web UI:
- The public component of the CA that signed your users' certificates in PEM format
- The public component of each Portal or Lumeta user's certificate in PEM format

For user authentication and authorization in the CLI:
- The public component of each Portal or Lumeta user's SSH key

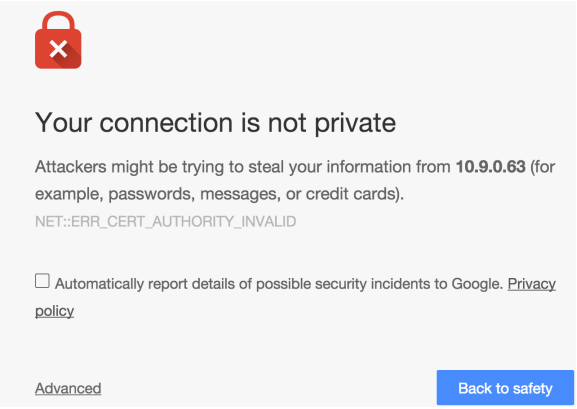
It also assumes that you have completed the following procedures, all of which are external to Lumeta:

- Copied your organization's **Certificate Authority certificate** to your browser's certificate store. (In Windows, for example, use the Certificate Import Wizard)
- Imported the public portion of your **server certificate** corresponding to the Portal or Lumeta system's name, IP address or domain to your browser store. (In Firefox, for example, use Preferences > Advanced > Certificates > View Certificates > Servers > Import.)
- Imported the public portion of your **user certificate** to your browser store. (In Firefox, for example, use Preferences > Advanced > Certificates > View Certificates > Your Certificates > Import.)

When the Public Key Infrastructure (PKI) feature is enabled on Lumeta Portal and Command Center, you will no longer need a password to log into the Lumeta Web UI or CLI. You will use certificates stored on your local system or on a smart card (CAC) to identify yourself to Lumeta. You will still be able to use a password to log in to the system's console.

Setting Up for Server Authentication

The procedures that follow will give your user community a reprieve from disconcerting certificate-related warning messages like this one, from a Chrome browser:



Other browsers display warning messages as well:

- **Firefox:** Your connection is not secure.
- **Internet Explorer:** Your connection is not private.

PKI is supported on the three most recent versions of the following browsers:

- Firefox
- Internet Explorer
- Chrome

The public portion of the server certificate and the CA that signed it should be loaded into the browser or operating system. This procedure is generally outside the scope of this document, though we do provide the Internet Explorer with Windows procedure on the Connecting PKI-Enabled Lumeta Systems with IE page.

The first step is to **load a server certificate**, which enables your supported browser to validate the Portal or Lumeta server. This one-time procedure is performed by the Portal or Lumeta system administrator. Server certificates are used regardless of whether PKI is enabled. When users do not uploaded their own server certificates, the system uses unique self-signed certificates that are delivered with the Portal or Lumeta license.

Although your certificates may use any naming convention, file extension, friendly name, and password (aka secrets), be aware that the Common Name (CN) listed on the server certificate's Subject, must match your Portal or Lumeta system's IP address, host name, or domain.

Before beginning this procedure, procure the following:

- Server Cert in PKCS12 format and generated with the file extension .p12

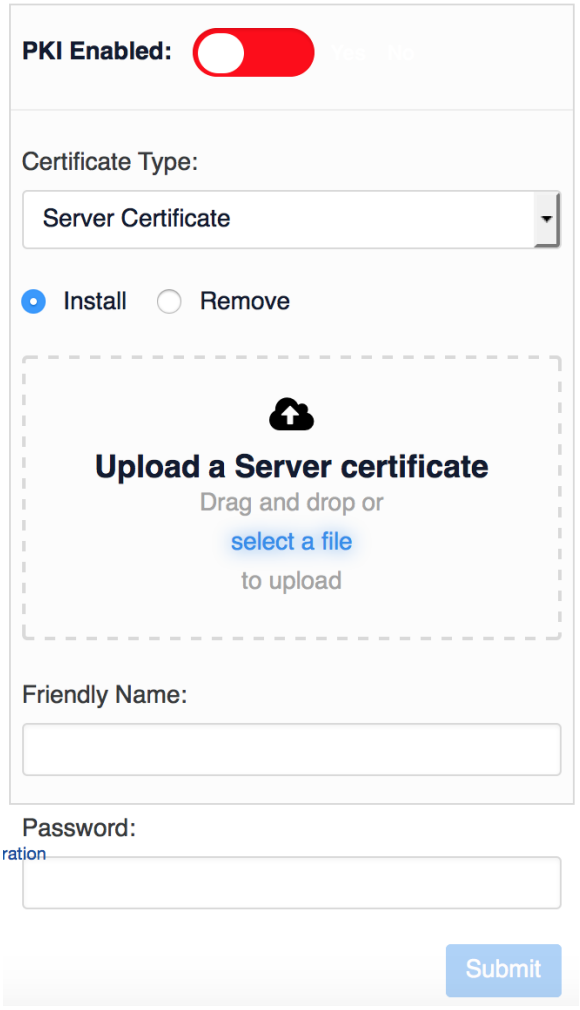
  Portal or Lumeta cannot use the .pfx certificate typically used with Microsoft products. As a work-around, please rename .pfx certificates to .p12 certificates.

  The current workaround is to rename the certificate to use the .p12 extension or generate it as a .p12 in the first place.
- Server Cert Friendly Name
- Server Cert Password

The process for importing a certificate in the Portal or Lumeta UI:
1. Click Settings > Portal or Lumeta Systems
2. Click Manage PKI
3. Select Certificate Type > Server Certificate
4. Drag and Drop or Select Certificate File

Follow this procedure:

1. Log in to Lumeta Portal or Lumeta.
2. Browse to **Settings** > **Lumeta Systems** or **Portal System > Manage PKI**.
3. Select **Server Certificate**.



4. Browse to a Server Certificate stored on your local system. This file is in PKCS12 format and typically has a .p12 or a .pfx extension.

Files with the .pfx extension must be renamed to have a .p12 extension.

5. Input a Friendly Name or **1**, which is often an acceptable alternative.
6. Enter the Password.
7. Click **Submit**.
8. The server certificate is processed; security error messages are eliminated.

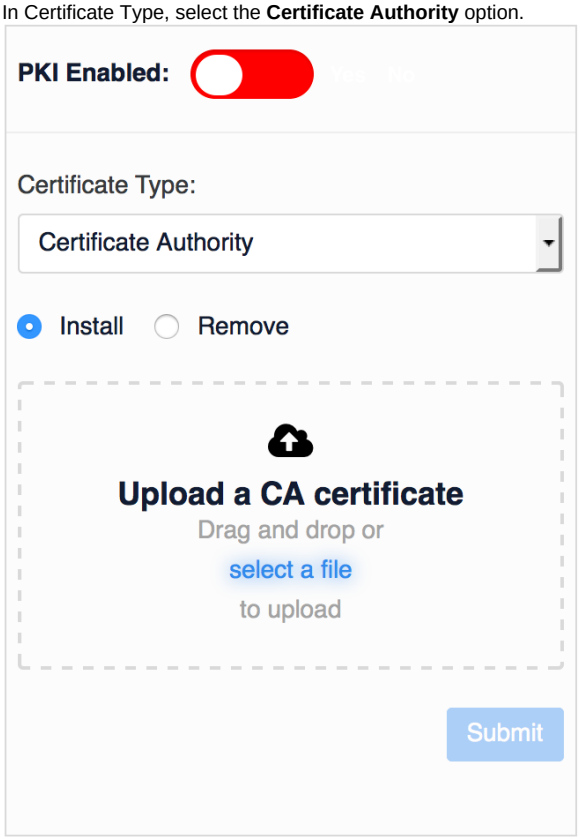
Setting Up for User Authentication & Authorization

The next steps are to load CA certificates, users' certificates, and SSH certificates. The CA file may contain many CAs. It should provide the Lumeta system with all of the CAs that have signed all of your users' certificates.

Load Certification Authority (CA) Certificates to Portal or Lumeta
The next step is to **load a CA certificate**, which will enable the Portal or Lumeta server to validate Portal or Lumeta users. The CA that signed users' certs should be loaded into the browser or operating system of your local system. The procedure is beyond the scope of this document.This is also a one-time procedure performed by the system administrator.

Before beginning, you'll need Certification Authority certificates in PEM format.

1. In Portal or Lumeta, browse to **Settings** > **Portal** or **Lumeta Systems > Manage PKI.**
2. In Certificate Type, select the **Certificate Authority** option.



3. Browse to your locally stored CA file, which is in PEM format. The PEM file may contain many CA certificates. Use the file issued by the CA that signed your users' certificates
4. Click **Submit**.
5. Refresh the browser page.

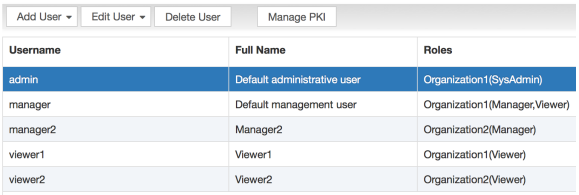
Load Users' Certificates

Load certificates for users so user's can access the web browser interface without needing a password.

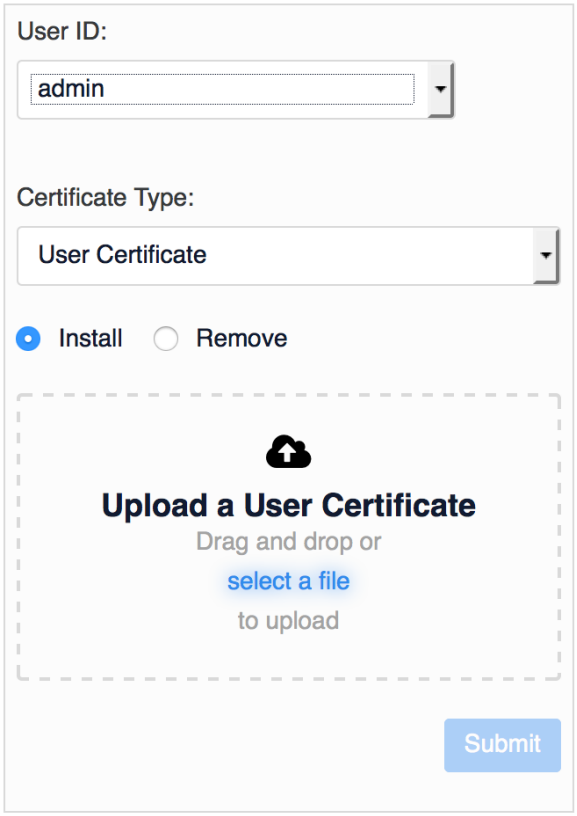
The private portion of a user's certificate may be loaded into the browser or operating system of the local system, or it may rLumetade on a smart card (CAC). A description of loading the certificate into the browser or operating system is beyond the scope of this document.

Before beginning, you'll need the users' public key certificate in PEM format.

1. In Portal or Lumeta, browse to **Settings** > **Users > Manage PKI**.
2. Select a username.



3. Click **Manage PKI**.
   The Manage User PKI page displays with the User ID field populated.
4. In Certificate Type, select **User Certificate**.



5. Upload your locally stored copy of the user's public key certificate which is in PEM format and often has the extension .cer, .crt, or .pem.
6. Click **Submit**.
7. After PKI is enabled, the user will be able to log into Lumeta through the web browser without having to enter a password.
8. Repeat this process, selecting other users from the User ID dropdown menu.

Load Users' SSH Keys

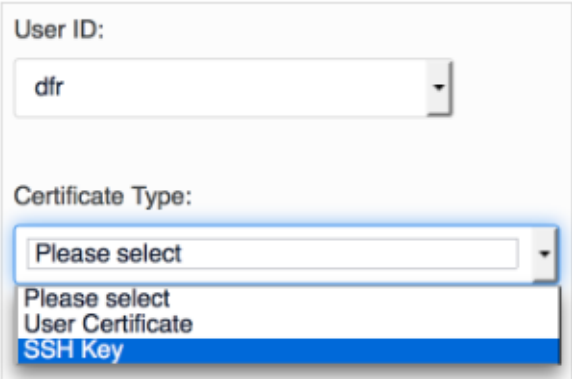
In this procedure, Portal or Lumeta system administrators upload SSH keys to provide their users with access to the CLI. The Portal or Lumeta system administrator repeats this procedure for each Portal or Lumeta user. Users will connect to the CLI using PuTTY-CAC or another SSH client.

Before beginning, you'll need the users' public SSH certificate.

The private portion of a user's SSH key should be either in a file on the local system or on a smart card (CAC). Where to put the private key and how to extract the public key from a smart card is beyond the scope of this document.

1. In Portal or Lumeta, browse to **Settings > Users > Manage PKI**.

2. Select a username.
3. Click **Manage PKI**.
   The Manage User PKI page displays with the User ID populated.
4. In Certificate Type select SSH Key option.

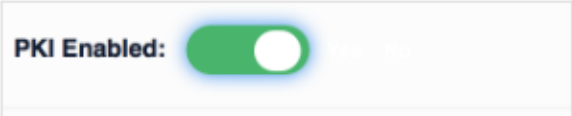


5. Browse to your locally stored SSH public key.
6. Click **Submit**.
7. When PKI is enabled, the user will be able to log into the Portal or Lumeta CLI without being prompted for a password.
8. Repeat this process, selecting other users from the User ID dropdown menu.

Enable PKI

The final step is to enable PKI. This permits Portal or Lumeta users to access the system without having to use a password. You will perform this step once on your Lumetasystem.

1. In Portal or Lumeta, browse to **Settings > Portal** or **Lumeta Systems**, select the command center and click **Manage PKI**.
2. Toggle PKI Enabled to the **Yes** position.



   The HTTP server restarts.
3. Refresh your browser.
   You have successfully enabled PKI. Users can now log in using certificates or smart cards.