NetApp Knowledge Base

What are the requirements around setting custom SSL certificates in Element Software?

https://kb-stage.netapp.com/on-prem/solidfire/Element_OS_Kbs/What_are_the_requirements_around_…
Updated: Wed, 24 Jun 2026 07:24:35 GMT

Applies to

- Element Software versions 12.2 and above
- Element Management Node (mNode)

Answer

By default, Element Software and its associated management node (mNode) are packaged with certificates meeting the requirements below as of version 12.2.

Certificate Requirements

- A unique SSL certificate made for the storage cluster
- The cert commonName field must be the cluster name or short name from the FQDN
- The Subject Alternative Name must contain the FQDN of the MVIP
- It can not contain additional FQDN's of other systems.
  - nslookup [MVIP] must return the FQDN
  - nslookup [FQDN]must return the MVIP
- PEM encoding (x509)
- ExtendedKeyUsage (EKU) is set (x509v3)
- Certificate length of 2048 bits or more (this is a requirement for using for Multifactor Authentication (MFA))

The default certificates are self-signed. Custom certificates (for example, certificates signed by a third party Certificate Authority (CA)) can be installed on Element storage clusters and their accompanying mNodes provided they meet the above requirements.

Environmental Requirement

Ensure that the certificate being installed is allowed by any firewalls in the network path.

To check the certificate policy's URL to be allowed/added to the firewall's exception list:

- in a web broswer, review the certificate in the Cluster UI
- click on the lock icon in web browser and select Certificate > Certification Path > Organization's certificate
- in the window that pops up, select Details > Certificate Policy
- The URL for this certificate policy should be at the bottom -- this URL needs to be allowed by the firewall
- Enable FW rule on port http (80) from all storage node's MIP to the CA server

Setting the Custom Certificate

Once obtained, custom certificates can be then be set via various API-driven methods on both the Element cluster and mNode. See, for instance:

- Changing the Element software default SSL certificate
- What are the API methods for setting custom SSL certificates on the Element mNode?

Additional Information

Troubleshooting

If any of the above requirements are not in place, the SetSSLCertificate (Element) or SetNodeSSLCertificate (mNode) API will fail with an error message. See, for instance:

- "Missing ExtendedKeyUsage (EKU) extension" error when setting a custom SSL certificate in Element Software
- "Invalid private key" error when setting a custom SSL certificate in Element Software
- "Key size" error when setting a custom SSL certificate in Element Software

Related Topics

For information on using MFA with Element Software, see Where is the Element Multi-factor Authentication guide located?

For information on using FIPS with Element Software, see Enabling FIPS 140-2 for HTTPS on your cluster.

For information on Ciphers in the context of SSL on Element, see the 'TLS and SSL' section of the guide linked from Where is the HCI Hardening guide located?