Enable multi-factor authentication

Element Software

NetApp
June 11, 2021

Table of Contents

Enable multi-factor authentication

Multi-factor authentication (MFA) uses a third-party Identity Provider (IdP) via the Security Assertion Markup Language (SAML) to manage user sessions. MFA enables administrators to configure additional factors of authentication as required, such as password and text message, and password and email message.

Set up multi-factor authentication

You can use these basic steps via the Element API to set up your cluster to use multi-factor authentication.

Details of each API method can be found in the Element API Reference.

1. Create a new third-party Identity Provider (IdP) configuration for the cluster by calling the following API method and passing the IdP metadata in JSON format: `CreateIdpConfiguration`

   IdP metadata, in plain text format, is retrieved from the third-party IdP. This metadata needs to be validated to ensure that it is correctly formatted in JSON. There are numerous JSON formatter applications available that you can use, for example:https://freeformatter.com/json-escape.html.

2. Retrieve cluster metadata, via spMetadataUrl, to copy to the third-party IdP by calling the following API method: `ListIdpConfigurations`

   spMetadataUrl is a URL used to retrieve service provider metadata from the cluster for the IdP in order to establish a trust relationship.

3. Configure SAML assertions on the third-party IdP to include the “NameID” attribute to uniquely identify a user for audit logging and for Single Logout to function properly.
4. Create one or more cluster administrator user accounts authenticated by a third-party IdP for authorization by calling the following API method:`AddIdpClusterAdmin`

   The username for the IdP cluster Administrator should match the SAML attribute Name/Value mapping for the desired effect, as shown in the following examples:

   - email=bob@company.com — where the IdP is configured to release an email address in the SAML attributes.
   - group=cluster-administrator - where the IdP is configured to release a group property in which all users should have access. Note that the SAML attribute Name/Value pairing is case-sensitive for security purposes.

5. Enable MFA for the cluster by calling the following API method: `EnableIdpAuthentication`

Find more information

- SolidFire and Element Resources page
- NetApp Element Plug-in for vCenter Server

Additional information for multi-factor authentication

You should be aware of the following caveats in relation to multi-factor authentication.

- In order to refresh IdP certificates that are no longer valid, you will need to use a non-IdP admin user to call the following API method: `UpdateIdpConfiguration`
- MFA is incompatible with certificates that are less than 2048 bits in length. By default, a 2048-bit SSL certificate is created on the cluster. You should avoid setting a smaller sized certificate when calling the API method: `SetSSLCertificate`

> If the cluster is using a certificate that is less than 2048 bits pre-upgrade, the cluster certificate must be updated with a 2048-bit or greater certificate after upgrade to Element 12.0 or later.

- IdP admin users cannot be used to make API calls directly (for example, via SDKs or Postman) or used for other integrations (for example, OpenStack Cinder or vCenter Plug-in). Add either LDAP cluster admin users or local cluster admin users if you need to create users that have these abilities.

Find more information

- Managing storage with the Element API
- SolidFire and Element Resources page
- NetApp Element Plug-in for vCenter Server