# Habilite la autenticación multifactor

## Element Software

NetApp
October 01, 2024

# Tabla de contenidos

Habilite la autenticación multifactor . . . . . 1
Configure la autenticación de múltiples factores . . . . . 1
Información adicional para la autenticación multifactor . . . . . 2

# Habilite la autenticación multifactor

La autenticación multifactor (MFA) utiliza un proveedor de identidades (IDP) de terceros a través del lenguaje de marcado de aserción de seguridad (SAML) para gestionar las sesiones de usuario. La MFA permite a los administradores configurar factores adicionales de autenticación según sea necesario, como la contraseña y los mensajes de texto, y la contraseña y los mensajes de correo electrónico.

## Configure la autenticación de múltiples factores

Es posible usar estos pasos básicos a través de la API de Element para configurar el clúster con el fin de utilizar la autenticación multifactor.

Los detalles de cada método API se pueden encontrar en el "Referencia de la API de Element".

1. Cree una nueva configuración de proveedor de identidades (IdP) de terceros para el clúster llamando al siguiente método API y pasando los metadatos de IdP en formato JSON: `CreateIdpConfiguration`

   Los metadatos de IDP, en formato de texto sin formato, se recuperan del IDP de terceros. Estos metadatos se deben validar para asegurarse de que están formateados correctamente en JSON. Hay numerosas aplicaciones de formateador JSON disponibles que puede utilizar, por ejemplo:https://freeformatter.com/json-escape.html.

2. Recupere los metadatos del clúster, a través de spMetadataUrl, para copiar en el IdP de terceros llamando al siguiente método API: `ListIdpConfigurations`

   SpMetadataUrl es una URL que se utiliza para recuperar metadatos del proveedor de servicios del clúster para el IDP con el fin de establecer una relación de confianza.

3. Configure las afirmaciones SAML en el IDP de terceros para incluir el atributo "'NameID'" para identificar de forma exclusiva a un usuario para el registro de auditorías y para que Single Logout funcione correctamente.
4. Cree una o varias cuentas de usuario administrador de clúster autenticadas por un IdP de terceros para su autorización llamando al siguiente método API:`AddIdpClusterAdmin`

   > El nombre de usuario del administrador del clúster IDP debe coincidir con el mapa de nombre/valor del atributo SAML del efecto deseado, como se muestra en los siguientes ejemplos:

   - Email=bob@company.com — donde el IDP está configurado para liberar una dirección de correo electrónico en los atributos SAML.
   - Group=cluster-Administrator: Donde el IDP está configurado para liberar una propiedad de grupo en la que todos los usuarios deberían tener acceso. Tenga en cuenta que el emparejamiento nombre/valor del atributo SAML distingue mayúsculas y minúsculas por motivos de seguridad.
5. Habilite MFA para el clúster mediante el siguiente método API: `EnableIdpAuthentication`

### Obtenga más información

- "Documentación de SolidFire y el software Element"

- "Plugin de NetApp Element para vCenter Server"

# Información adicional para la autenticación multifactor

Debe conocer las siguientes advertencias en relación con la autenticación de múltiples factores.

- Para actualizar los certificados IdP que ya no son válidos, deberá usar un usuario administrador distinto de IdP para llamar al siguiente método API: `UpdateIdpConfiguration`
- La MFA es incompatible con certificados con una longitud inferior a 2048 bits. De manera predeterminada, se crea un certificado SSL de 2048 bits en el clúster. Debe evitar establecer un certificado de menor tamaño cuando llame al método API: `SetSSLCertificate`

> Si el clúster utiliza un certificado que sea inferior a 2048 bits antes de la actualización, el certificado del clúster debe actualizarse con un certificado de 2048 bits o superior después de la actualización a Element 12.0 o una versión posterior.

- Los usuarios del administrador de IDP no pueden utilizarse para realizar llamadas de API directamente (por ejemplo, mediante SDK o Postman) o para otras integraciones (por ejemplo, OpenStack Cinder o el complemento vCenter). Si necesita crear usuarios que tengan estas capacidades, añada usuarios bien al administrador del clúster LDAP o usuarios de administrador del clúster local.

## Obtenga más información

- "Gestionar el almacenamiento con la API de Element"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

## Información de copyright



## Información de la marca comercial