Multi-factor authentication API methods

Element Software

NetApp
October 01, 2024

Table of Contents

Multi-factor authentication API methods

You can use multi-factor authentication (MFA) to manage user sessions using a third-party Identity Provider (IdP) via the Security Assertion Markup Language (SAML).

- AddIdpClusterAdmin
- CreateIdpConfiguration
- DeleteAuthSession
- DeleteAuthSessionsByClusterAdmin
- DeleteAuthSessionsByUsername
- DeleteIdpConfiguration
- DisableIdpAuthentication
- EnableIdpAuthentication
- GetIdpAuthenticationState
- ListActiveAuthSessions
- ListIdpConfigurations
- UpdateIdpConfiguration

Find more information

- SolidFire and Element Software Documentation
- Documentation for earlier versions of NetApp SolidFire and Element products

AddIdpClusterAdmin

You can use the `AddIpdClusterAdmin` method to add a cluster administrator user authenticated by a third-party Identity Provider (IdP). IdP cluster admin accounts are configured based on SAML attribute-value information provided within the IdP's SAML assertion associated with the user. If a user successfully authenticates with the IdP and has SAML attribute statements within the SAML assertion matching multiple IdP cluster admin accounts, the user will have the combined access level of those matching IdP cluster admin accounts.

Parameters

This method has the following input parameters:

Name	Description	Type	Default value	Required
access	Controls which methods this IdP cluster admin can use.	string array	None	Yes

Name	Description	Type	Default value	Required
acceptEula	Accept the End User License Agreement. Set to true to add a cluster administrator account to the system. If omitted or set to false, the method call fails.	boolean	None	Yes
attributes	List of name-value pairs in JSON object format.	JSON object	None	No
username	A SAML attribute-value mapping to an IdP cluster admin (for example, email=test@example.com). This can be defined using a specific SAML subject using `NameID` or as an entry in the SAML attribute statement, such as `eduPersonAffiliation`.	string	None	Yes

Return values

This method has the following return value:

Name	Description	Type
clusterAdminID	Unique identifier for the newly created cluster admin.	integer

Request example

Requests for this method are similar to the following example:

```
{
    "method": "AddIdpClusterAdmin",
    "params": {
        "username": "email=test@example.com",
        "acceptEula": true,
        "access": ["administrator"]
    }
}
```

Response example

This method returns a response similar to the following example:

```
{
    "result": {
        "clusterAdminID": 13
    }
}
```

New since version

12.0

CreateIdpConfiguration

You can use the `CreateIpdConfiguration` method to create a potential trust relationship for authentication using a third-party Identity Provider (IdP) for the cluster. A SAML Service Provider certificate is required for IdP communication. This certificate is generated as required, and returned by this API call.

Parameters

This method has the following input parameters:

Name	Description	Type	Default value	Required
idpMetadata	IdP metadata to store.	string	None	Yes
idpName	Name used to identify an IdP provider for SAML 2.0 single sign-on.	string	None	Yes

Return values

This method has the following return value:

Name	Description	Type
idpConfigInfo	Information about the third-party Identity Provider (IdP) configuration.	idpConfigInfo

Request example

Requests for this method are similar to the following example:

```
{
    "method": "CreateIdpConfiguration",
    "params": {
        "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>
             <EntityDescriptor
               xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"
               xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"
               xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"
               xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"
               ...</Organization>
             </EntityDescriptor>",
        "idpName": "https://provider.name.url.com"
    },
}
```

Response example

This method returns a response similar to the following example:

```
{
    "result": {
        "idpConfigInfo": {
        "enabled": false,
        "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
        "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n
        <EntityDescriptor
xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"\r\n
        xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"\r\n
        xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"\r\n
        xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"\r\n
        ... </Organization>\r\n
        </EntityDescriptor>",
        "idpName": "https://privider.name.url.com",
        "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
        MIID...SlBHi\n
        -----END CERTIFICATE-----\n",
        "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
        }
    }
}
```


New since version

12.0

DeleteAuthSession

You can use the `DeleteAuthSession` method to delete an individual user authentication session. If the calling user is not in the ClusterAdmins / Administrator AccessGroup, only the authentication session belonging to the calling user can be deleted.

Parameters

This method has the following input parameter:

Name	Description	Type	Default value	Required
sessionID	Unique identifier for the auth session to be deleted.	UUID	None	Yes

Return values

This method has the following return value:

Name	Description	Type
session	Session information for the delete auth session.	authSessionInfo

Request example

Requests for this method are similar to the following example:

```
{
    "method": "DeleteAuthSession",
    "params": {
        "sessionID": "a862a8bb-2c5b-4774-a592-2148e2304713"
    },
    "id": 1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id": 1,
    "result": {
        "session": {
            "accessGroupList": [
                "administrator"
            ],
            "authMethod": "Cluster",
            "clusterAdminIDs": [
                1
            ],
            "finalTimeout": "2020-04-09T17:51:30Z",
            "idpConfigVersion": 0,
            "lastAccessTimeout": "2020-04-06T18:21:33Z",
            "sessionCreationTime": "2020-04-06T17:51:30Z",
            "sessionID": "a862a8bb-2c5b-4774-a592-2148e2304713",
            "username": "admin"
        }
    }
}
```

New since version

12.0

DeleteAuthSessionsByClusterAdmin

You can use the `DeleteAuthSessionsByClusterAdmin` method to delete all authentication sessions associated with the specified `ClusterAdminID`. If the specified ClusterAdminID maps to a group of users, all authentication sessions for all members of that group will be deleted. To view a list of sessions for possible deletion, use the ListAuthSessionsByClusterAdmin method with the `ClusterAdminID` parameter.

Parameters

This method has the following input parameter:

Name	Description	Type	Default value	Required
clusterAdminID	Unique identifier for the cluster admin.	integer	None	Yes

Return values

This method has the following return value:

Name	Description	Type
sessions	Session information for the deleted authentication sessions.	authSessionInfo

Request example

Requests for this method are similar to the following example:

```
{
  "method": "DeleteAuthSessionsByClusterAdmin",
  "params": {
    "clusterAdminID": 1
  }
}
```

Response example

This method returns a response similar to the following example:

```
{
"sessions": [
      {
        "accessGroupList": [
          "administrator"
        ],
        "authMethod": "Cluster",
        "clusterAdminIDs": [
          1
        ],
        "finalTimeout": "2020-03-14T19:21:24Z",
        "idpConfigVersion": 0,
        "lastAccessTimeout": "2020-03-11T19:51:24Z",
        "sessionCreationTime": "2020-03-11T19:21:24Z",
        "sessionID": "b12bfc64-f233-44df-8b9f-6fb6c011abf7",
        "username": "admin"
      }
    ]
}
```


New since version

12.0

DeleteAuthSessionsByUsername

You can use the `DeleteAuthSessionsByUsername` method to delete all authentication sessions for a given user(s). A caller not in AccessGroup ClusterAdmins/Administrator can only delete their own sessions. A caller with ClusterAdmins/Administrator privileges can delete sessions belonging to any user. To see the list of sessions that could be deleted, use `ListAuthSessionsByUsername` with the same parameters. To view a list of sessions for possible deletion, use the `ListAuthSessionsByUsername` method with the same parameter.

Parameters

This method has the following input parameters:

Name	Description	Type	Default value	Required
authMethod	Authentication method of the user sessions to be deleted. Only a caller in the ClusterAdmins/Administrator AccessGroup can provide this parameter. Possible values are: • **authMethod=Cluster** specifies the ClusterAdmin username. • **authMethod=Ldap** specifies the user's LDAP DN. • **authMethod=Idp** specifies either the user's IdP UUID or NameID. If the IdP is not configured to return either option, this specifies a random UUID issued when the session was created.	authMethod	None	No
username	Unique identifier for the user.	string	None	No

Return values

This method has the following return value:

Name	Description	Type
sessions	Session information for the deleted authentication sessions.	authSessionInfo

Request example

Requests for this method are similar to the following example:

```
{
  "method": "DeleteAuthSessionsByUsername",
  "params": {
    "authMethod": "Cluster",
    "username": "admin"
  }
}
```

Response example

This method returns a response similar to the following example:

```
{
"sessions": [
      {
        "accessGroupList": [
          "administrator"
        ],
        "authMethod": "Cluster",
        "clusterAdminIDs": [
          1
        ],
        "finalTimeout": "2020-03-14T19:21:24Z",
        "idpConfigVersion": 0,
        "lastAccessTimeout": "2020-03-11T19:51:24Z",
        "sessionCreationTime": "2020-03-11T19:21:24Z",
        "sessionID": "b12bfc64-f233-44df-8b9f-6fb6c011abf7",
        "username": "admin"
      }
    ]
}
```

New since version

12.0

DeleteIdpConfiguration

You can use the `DeleteIdpConfiguration` method to delete an existing configuration of a third-party IdP for the cluster. Deleting the last IdP configuration removes the SAML Service Provider certificate from the cluster.

Parameters

This method has the following input parameters:

Name	Description	Type	Default value	Required
idpConfigurationID	UUID for the third-party IdP configuration.	UUID	None	No
idpName	Name used to identify and retrieve an IdP provider for SAML 2.0 single sign-on.	string	None	No

Return values

This method has no return values.

Request example

Requests for this method are similar to the following example:

```
{
  "method": "DeleteIdpConfiguration",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
    "idpName": "https://provider.name.url.com"
  }
}
```

Response example

This method returns a response similar to the following example:

```
{
  "result":{}
}
```

New since version

12.0

DisableIdpAuthentication

You can use the `DisableIdpAuthentication` method to disable support for authentication using third-party IdPs for the cluster. Once disabled, users authenticated by third party IdPs are no longer able to access the cluster and any active authenticated sessions are invalidated/disconnected. LDAP and cluster admins are able to access the cluster via supported UIs.

Parameters

This method has no input parameters.

Return values

This method has no return values.

Request example

Requests for this method are similar to the following example:

```
{
  "method": "DisableIdpAuthentication",
  "params": {}
}
```

Response example

This method returns a response similar to the following example:

```
{
"result": {}
}
```

New since version

12.0

EnableIdpAuthentication

You can use the `EnableIdpAuthentication` method to enable support for authentication using third-party IdPs for the cluster. Once IdP authentication is enabled, LDAP and cluster admins are no longer able to access the cluster via supported UIs and any active authenticated sessions are invalidated/disconnected. Only users authenticated by third party IdPs are able to access the cluster via supported UIs.

Parameters

This method has the following input parameter:

Name	Description	Type	Default value	Required
idpConfigurationID	UUID for the third-party IdP configuration. If only one IdP configuration exists, then the default is to enable that configuration. If you have only a single IdpConfiguration, you need not provide the idpConfigurationID parameter.	UUID	None	No

Return values

This method has no return values.

Request example

Requests for this method are similar to the following example:

```
{
  "method": "EnableIdpAuthentication",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
  }
}
```

Response example

This method returns a response similar to the following example:

```
{
"result": {}
}
```

New since version

12.0

GetIdpAuthenticationState

You can use the `GetIdpAuthenticationState` method to return information regarding the state of authentication using third-party IdPs.

Parameters

This method has no input parameters.

Return values

This method has the following return value:

Name	Description	Type
enabled	Indicates whether third-party IdP authentication is enabled.	boolean

Request example

Requests for this method are similar to the following example:

```
{
  "method": "GetIdpAuthenticationState"
}
```

Response example

This method returns a response similar to the following example:

```
{
  "result": {"enabled": true}
}
```

New since version

12.0

ListActiveAuthSessions

You can use the `ListActiveAuthSessions` method to list all of the active authenticated sessions. Only users with Administrative access rights can call this method.

Parameters

This method has no input parameters.

Return values

This method has the following return value:

Name	Description	Type
sessions	Session information for the authentication sessions.	authSessionInfo

Request example

Requests for this method are similar to the following example:

```
{
  "method": "ListActiveAuthSessions"
}
```

Response example

This method returns a response similar to the following example:

```
{
"sessions": [
      {
        "accessGroupList": [
          "administrator"
        ],
        "authMethod": "Cluster",
        "clusterAdminIDs": [
          1
        ],
        "finalTimeout": "2020-03-14T19:21:24Z",
        "idpConfigVersion": 0,
        "lastAccessTimeout": "2020-03-11T19:51:24Z",
        "sessionCreationTime": "2020-03-11T19:21:24Z",
        "sessionID": "b12bfc64-f233-44df-8b9f-6fb6c011abf7",
        "username": "admin"
      }
    ]
}
```

New since version

12.0

ListIdpConfigurations

You can use the `ListIdpConfigurations` method to list configurations for third-party IdPs. Optionally, you can provide either the `enabledOnly` flag to retrieve the currently enabled IdP configuration or an IdP metadata UUID or IdP name to query information for a specific IdP configuration.

Parameters

This method has the following input parameters:

Name	Description	Type	Default value	Required
enabledOnly	Filters the result to return the currently enabled IdP configuration.	boolean	None	No
idpConfigurationID	UUID for the third-party IdP configuration.	UUID	None	No
idpName	Retrieves IdP configuration information for a specific IdP name.	string	None	No

Return values

This method has the following return value:

Name	Description	Type
idpConfigInfos	Information on the third-party IdP configuration(s).	idpConfigInfo array

Request example

Requests for this method are similar to the following example:

```
{
  "method": "ListIdpConfigurations",
  "params": {}
}
```

Response example

This method returns a response similar to the following example:

```
{
    "result": {
        "idpConfigInfo": {
        "enabled": true,
        "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
        "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n
        <EntityDescriptor
xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"\r\n
        xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"\r\n
        xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"\r\n
        xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"\r\n
        ...</Organization>\r\n
        </EntityDescriptor>",
        "idpName": "https://privider.name.url.com",
        "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
        MI...BHi\n
        -----END CERTIFICATE-----\n",
        "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
        }
    }
}
```

New since version

12.0

UpdateIdpConfiguration

You can use the `UpdateIdpConfiguration` method to update an existing configuration with a third-party IdP for the cluster.

Parameters

This method has the following input parameters:

Name	Description	Type	Default value	Required
generateNewCertificate	When specified as true, a new SAML key and certificate is generated and replaces the existing pair. Note: Replacing the existing certificate will disrupt the established trust between the cluster and the IdP until the cluster's Service Provider metadata is reloaded at the IdP. If not provided or set to false, the SAML certificate and key remains unchanged.	boolean	None	No
idpConfigurationID	UUID for the third-party IdP configuration.	UUID	None	No
idpMetadata	IdP metadata for configuration and integration details for SAML 2.0 single sign-on.	string	None	No
idpName	Name used to identify and retrieve an IdP provider for SAML 2.0 single sign-on.	string	None	No
newIdpName	If specified, this name replaces the old IdP name.	string	None	No

Return values

This method has the following return value:

Name	Description	Type
idpConfigInfo	Information around the third-party IdP configuration.	idpConfigInfo

Request example

Requests for this method are similar to the following example:

```
{
"method": "UpdateIdpConfiguration",
"params": {
        "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
        "generateNewCertificate": true
    }
}
```

Response example

This method returns a response similar to the following example:

```
{
    "result": {
        "idpConfigInfo": {
        "enabled": true,
        "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
        "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n
        <EntityDescriptor
xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"\r\n
        xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"\r\n
        xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"\r\n
        xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"\r\n
        ...</Organization>\r\n
        </EntityDescriptor>",
        "idpName": "https://privider.name.url.com",
        "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
        MI...BHi\n
        -----END CERTIFICATE-----\n",
        "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
        }
    }
}
```

New since version

12.0

Copyright information

Trademark information