



## 多因素驗證API方法 Element Software

NetApp  
January 15, 2024

# 目錄

多因素驗證API方法	1
如需詳細資訊、請參閱	1
AddIdpClusterAdmin	1
建立IdpConfiguration	3
刪除驗證工作階段	5
刪除驗證sessionsByClusterAdmin	6
刪除驗證使用者名稱	8
刪除Idp組態	10
停用Idp驗證	11
啟用Idp驗證	11
GetIdpAuthenticationState	13
listActiveAuthSessions	13
清單組態	15
更新IdpConfiguration	16

# 多因素驗證API方法

您可以使用多因素驗證（MFA）、透過安全聲明標記語言（SAML）、使用第三方身分識別供應商（IDP）來管理使用者工作階段。

- [AddIdpClusterAdmin](#)
- [建立IdpConfiguration](#)
- [刪除驗證工作階段](#)
- [刪除驗證sessionsByClusterAdmin](#)
- [刪除驗證使用者名稱](#)
- [刪除Idp組態](#)
- [停用Idp驗證](#)
- [啟用Idp驗證](#)
- [GetIdpAuthenticationState](#)
- [listActiveAuthSessions](#)
- [清單組態](#)
- [更新IdpConfiguration](#)

## 如需詳細資訊、請參閱

- ["零件與元件軟體文件SolidFire"](#)
- ["先前版本的NetApp SolidFire 產品及元素產品文件"](#)

## AddIdpClusterAdmin

您可以使用「AddIdpClusterAdmin」方法來新增由協力廠商身分識別供應商（IDP）驗證的叢集管理員使用者。IDP叢集管理帳戶是根據IDP中與使用者相關聯的SAML聲明所提供的SAML屬性值資訊來設定。如果使用者已成功驗證IDP、且SAML聲明中的SAML屬性陳述與多個IDP叢集管理帳戶相符、則使用者將擁有符合IDP叢集管理帳戶的合併存取層級。

### 參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
存取	控制此IDP叢集管理員可以使用的方法。	字串陣列	無	是的

名稱	說明	類型	預設值	必要
接受Eula	接受終端使用者授權合約。設為true可將叢集管理員帳戶新增至系統。如果省略或設為假、則方法呼叫會失敗。	布林值	無	是的
屬性	Json物件格式的名稱-值配對清單。	Json物件	無	否
使用者名稱	對應至IDP叢集管理員的SAML屬性值（例如、email=test@example.com）。您可以使用「NameID」或SAML屬性聲明中的項目（例如「eDuPersonAffection」）、來定義這項功能。	字串	無	是的

## 傳回值

此方法具有下列傳回值：

名稱	說明	類型
叢集管理ID	新建立叢集管理員的唯一識別碼。	整數

## 申請範例

此方法的要求類似於下列範例：

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

## 回應範例

此方法會傳回類似下列範例的回應：

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

## 新的自版本

12.0

## 建立IdpConfiguration

您可以使用「Create IpdConfiguration」（建立IpdConfiguration）方法、為叢集建立可能的信任關係、以便使用協力廠商身分識別供應商（IDP）進行驗證。IDP通訊需要SAML服務供應商憑證。此憑證會視需要產生、並由此API呼叫傳回。

## 參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
idp中繼 資料	要儲存的IDP中繼資料。	字串	無	是的
idpName	用於識別SAML 2.0 單一登入的IDP供應商名稱。	字串	無	是的

## 傳回值

此方法具有下列傳回值：

名稱	說明	類型
idpConfigInfo	第三方身分識別供應商（IDP）組態的相關資訊。	"idpConfigInfo"

## 申請範例

此方法的要求類似於下列範例：

```
{
  "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"
  },
}
```

## 回應範例

此方法會傳回類似下列範例的回應：

```
{
  "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"
    }
  }
}
```

## 新的自版本

12.0

## 刪除驗證工作階段

您可以使用「刪除驗證工作階段」方法刪除個別的使用者驗證工作階段。如果呼叫使用者不在ClusterAdmins / Administrator存取群組中、則只能刪除屬於呼叫使用者的驗證工作階段。

### 參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
工作階段ID	要刪除之驗證工作階段的唯一識別碼。	UUID	無	是的

### 傳回值

此方法具有下列傳回值：

名稱	說明	類型
工作階段	刪除驗證工作階段的工作階段資訊。	" <a href="#">驗證工作階段資訊</a> "

### 申請範例

此方法的要求類似於下列範例：

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

### 回應範例

此方法會傳回類似下列範例的回應：

```
{
  "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"
    }
  }
}
```

## 新的自版本

12.0

## 刪除驗證sessionsByClusterAdmin

您可以使用「刪除驗證資源ByClusterAdmin」方法來刪除與指定「ClusterAdminID」相關的所有驗證工作階段。如果指定的ClusterAdminID對應至一組使用者、則該群組所有成員的所有驗證工作階段都會刪除。若要檢視可刪除的工作階段清單、請使用帶有「ClusterAdminID」參數的ListAuthSessionsByClusterAdmin方法。

### 參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
叢集管理ID	叢集管理員的唯一識別碼。	整數	無	是的

### 傳回值

此方法具有下列傳回值：



名稱	說明	類型
工作階段	已刪除驗證工作階段的工作階段資訊。	" <a href="#">驗證工作階段資訊</a> "

## 申請範例

此方法的要求類似於下列範例：

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

## 回應範例

此方法會傳回類似下列範例的回應：

```
{
  "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"
    }
  ]
}
```

## 新的自版本

12.0

## 刪除驗證使用者名稱

您可以使用「刪除驗證使用者名稱」方法刪除特定使用者的所有驗證工作階段。非存取群組ClusterAdmins /系統管理員的呼叫者只能刪除自己的工作階段。具有ClusterAdmins /系統管理員權限的呼叫者可以刪除屬於任何使用者工作階段。若要查看可刪除的工作階段清單、請使用具有相同參數的「listAuthSessionsByUsername」。若要檢視可能刪除的工作階段清單、請使用具有相同參數的「listAuthSessionsByUsername」方法。

### 參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
驗證方法	要刪除之使用者工作階段的驗證方法。只有ClusterAdmins / Administrator存取群組中的呼叫者可以提供此參數。可能的值包括： <ul style="list-style-type: none"><li>• *authMethod=Cluster*指定ClusterAdmin使用者名稱。</li><li>• *authMethod=LDAP*指定使用者的LDAP DN。</li><li>• *authMethod=IDP *指定使用者的IDP UUID或NameID。如果IDP未設定為傳回任一選項、則會指定建立工作階段時發出的隨機UUID。</li></ul>	驗證方法	無	否
使用者名稱	使用者的唯一識別碼。	字串	無	否

### 傳回值

此方法具有下列傳回值：

名稱	說明	類型
工作階段	已刪除驗證工作階段的工作階段資訊。	" <a href="#">驗證工作階段資訊</a> "

## 申請範例

此方法的要求類似於下列範例：

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

## 回應範例

此方法會傳回類似下列範例的回應：

```
{
  "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"
    }
  ]
}
```

## 新的自版本

12.0

## 刪除Idp組態

您可以使用「刪除IdpConfiguration」方法來刪除叢集現有的協力廠商IDP組態。刪除最後一個IDP組態會從叢集移除SAML服務供應商憑證。

### 參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
idpConfiguration ID	協力廠商IDP組態的UUID。	UUID	無	否
idpName	用於識別及擷取SAML 2.0單一登入的IDP供應商名稱。	字串	無	否

### 傳回值

此方法沒有傳回值。

### 申請範例

此方法的要求類似於下列範例：

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

### 回應範例

此方法會傳回類以下列範例的回應：

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

新的自版本

12.0

## 停用Idp驗證

您可以使用「disableIdpAuthentication」方法、停用叢集使用協力廠商IDP進行驗證的支援。停用後、第三方IDP驗證的使用者將無法再存取叢集、而且任何作用中的驗證工作階段都會失效/中斷連線。LDAP與叢集管理員可透過支援的UI存取叢集。

### 參數

此方法沒有輸入參數。

### 傳回值

此方法沒有傳回值。

### 申請範例

此方法的要求類似於下列範例：

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

### 回應範例

此方法會傳回類以下列範例的回應：

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

新的自版本

12.0

## 啟用Idp驗證

您可以使用「enableIdpAuthentication」方法、為叢集啟用使用協力廠商IDP的驗證支援。啟用IDP驗證之後、LDAP和叢集管理員便無法再透過支援的UI存取叢集、而且任何作用中的驗證工作階段都會失效/中斷連線。只有第三方IDP驗證的使用者才能透過支援的UI存取叢

集。

## 參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
idpConfiguration ID	協力廠商IDP組態的UUID。如果只有一個IDP組態存在、則預設為啟用該組態。如果只有一個IdpConfiguration、則不需要提供idpConfiguration ID參數。	UUID	無	否

## 傳回值

此方法沒有傳回值。

## 申請範例

此方法的要求類似於下列範例：

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

## 回應範例

此方法會傳回類以下列範例的回應：

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

## 新的自版本

12.0

## GetIdpAuthenticationState

您可以使用「GetIdpAuthenticationState」方法、傳回使用第三方IDP進行驗證狀態的相關資訊。

### 參數

此方法沒有輸入參數。

### 傳回值

此方法具有下列傳回值：

名稱	說明	類型
已啟用	指出是否已啟用協力廠商IDP驗證。	布林值

### 申請範例

此方法的要求類似於下列範例：

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

### 回應範例

此方法會傳回類似下列範例的回應：

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

### 新的自版本

12.0

## listActiveAuthSessions

您可以使用「listActiveAuthSessions」方法列出所有作用中的已驗證工作階段。只有擁有系統管理存取權限的使用者才能呼叫此方法。

## 參數

此方法沒有輸入參數。

## 傳回值

此方法具有下列傳回值：

名稱	說明	類型
工作階段	驗證工作階段的工作階段資訊。	<a href="#">"驗證工作階段資訊"</a>

## 申請範例

此方法的要求類似於下列範例：

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

## 回應範例

此方法會傳回類似下列範例的回應：

```
{
  "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"
    }
  ]
}
```



## 新的自版本

12.0

## 清單組態

您可以使用「listIdpConfigurations」方法來列出協力廠商IDP的組態。或者、您可以提供「enabledOnly」旗標來擷取目前啟用的IDP組態、或是IDP中繼資料UUID或IDP名稱、以查詢特定IDP組態的資訊。

### 參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
僅限enabledOnly	篩選結果以傳回目前啟用的IDP組態。	布林值	無	否
idpConfiguration ID	協力廠商IDP組態的UUID。	UUID	無	否
idpName	擷取特定IDP名稱的IDP組態資訊。	字串	無	否

### 傳回值

此方法具有下列傳回值：

名稱	說明	類型
idpConfigInfos	第三方IDP組態的相關資訊。	"idpConfigInfo" 陣列

### 申請範例

此方法的要求類似於下列範例：

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

### 回應範例

此方法會傳回類似下列範例的回應：

```
{
  "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://priver.name.url.com",
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
MI...BHi\n
-----END CERTIFICATE-----\n",
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
    }
  }
}
```

新的自版本

12.0

## 更新IdpConfiguration

您可以使用「更新IdpConfiguration」方法、使用叢集的協力廠商IDP來更新現有組態。

### 參數

此方法具有下列輸入參數：

名稱	說明	類型	預設值	必要
GenerateNewCertificate	如果指定為true、則會產生新的SAML金鑰和憑證、並取代現有配對。附註：更換現有的憑證將會中斷叢集與IDP之間建立的信任關係、直到叢集的服務供應商中繼資料在IDP重新載入為止。如果未提供或設定為假、SAML憑證和金鑰將維持不變。	布林值	無	否
idpConfiguration ID	協力廠商IDP組態的UUID。	UUID	無	否
idp中繼 資料	IDP中繼資料、提供SAML 2.0單一登入的組態與整合詳細資料。	字串	無	否
idpName	用於識別及擷取SAML 2.0單一登入的IDP供應商名稱。	字串	無	否
newIdpName	如果指定、此名稱會取代舊的IDP名稱。	字串	無	否

## 傳回值

此方法具有下列傳回值：

名稱	說明	類型
idpConfigInfo	第三方IDP組態的相關資訊。	"idpConfigInfo"

## 申請範例

此方法的要求類似於下列範例：

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

## 回應範例

此方法會傳回類似下列範例的回應：

```
{
  "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://priver.name.url.com",
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
MI...BHi\n
-----END CERTIFICATE-----\n",
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
    }
  }
}
```

## 新的自版本

12.0

## 版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

## 商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。