



多要素認証を有効にする

Element Software

NetApp
November 12, 2025

目次

多要素認証を有効にする	1
多要素認証を設定する	1
詳細情報の参照	1
多要素認証に関する追加情報	2
詳細情報の参照	2

多要素認証を有効にする

多要素認証を設定する

多要素認証 (MFA) は、セキュリティアサーションマークアップ言語 (SAML) を介してサードパーティの ID プロバイダー (IdP) を使用してユーザーセッションを管理します。MFA を使用すると、管理者は必要に応じて、パスワードとテキスト メッセージ、パスワードと電子メール メッセージなどの追加の認証要素を構成できます。

Element API 経由でこれらの基本的な手順を使用して、多要素認証を使用するようにクラスターを設定できます。

各APIメソッドの詳細については、["要素APIリファレンス"](#)。

1. 次の API メソッドを呼び出して、IdP メタデータを JSON 形式で渡すことで、クラスターの新しいサードパーティ ID プロバイダー (IdP) 構成を作成します。 `CreateIdpConfiguration`

IdP メタデータはプレーンテキスト形式でサードパーティの IdP から取得されます。このメタデータは、JSON で正しくフォーマットされていることを確認するために検証する必要があります。使用できるJSONフォーマッターアプリケーションは数多くあります。例えば、次のとおりです。 <https://freeformatter.com/json-escape.html>.

2. 次の API メソッドを呼び出して、`spMetadataUrl` を介してクラスター メタデータを取得し、サードパーティの IdP にコピーします。 `ListIdpConfigurations`

`spMetadataUrl` は、信頼関係を確立するために IdP のクラスターからサービス プロバイダー メタデータを取得するために使用される URL です。

3. 監査ログとシングル ログアウトが適切に機能するために、ユーザーを一意に識別するための “NameID” 属性を含めるようにサードパーティの IdP で SAML アサーションを構成します。
4. 次の API メソッドを呼び出して、承認のためにサードパーティの IdP によって認証された 1 つ以上のクラスター管理者ユーザー アカウントを作成します。 `AddIdpClusterAdmin`



次の例に示すように、目的の効果を得るには、IdP クラスター管理者のユーザー名が SAML 属性の名前/値のマッピングと一致する必要があります。

- `email=bob@company.com` - ここで、IdP は SAML 属性で電子メール アドレスを解放するように構成されています。
- `group=cluster-administrator` - ここで、IdP は、すべてのユーザーがアクセスできるグループ プロパティを解放するように構成されます。セキュリティ上の理由から、SAML 属性の名前と値のペアでは大文字と小文字が区別されることに注意してください。

5. 次の API メソッドを呼び出して、クラスターの MFA を有効にします。 `EnableIdpAuthentication`

詳細情報の参照

- ["SolidFireおよびElementソフトウェアのドキュメント"](#)
- ["vCenter Server 用NetApp Elementプラグイン"](#)

多要素認証に関する追加情報

多要素認証に関しては、次の注意事項に注意する必要があります。

- 有効ではなくなった IdP 証明書を更新するには、IdP 以外の管理者ユーザーを使用して次の API メソッドを呼び出す必要があります。 `UpdateIdpConfiguration`
- MFA は、長さが 2048 ビット未満の証明書とは互換性がありません。デフォルトでは、クラスター上に 2048 ビットの SSL 証明書が作成されます。API メソッドを呼び出すときは、小さいサイズの証明書の設定を避ける必要があります。 `SetSSLCertificate`



アップグレード前にクラスターが 2048 ビット未満の証明書を使用している場合は、Element 12.0 以降にアップグレードした後、クラスター証明書を 2048 ビット以上の証明書に更新する必要があります。

- IdP 管理ユーザーは、API 呼び出しを直接行うために使用することはできません (たとえば、SDK または Postman 経由)。また、他の統合 (たとえば、OpenStack Cinder または vCenter プラグイン) に使用することもできません。これらの権限を持つユーザーを作成する必要がある場合は、LDAP クラスター管理者ユーザーまたはローカル クラスター管理者ユーザーのいずれかを追加します。

詳細情報の参照

- ["Element API によるストレージの管理"](#)
- ["SolidFireおよびElementソフトウェアのドキュメント"](#)
- ["vCenter Server 用NetApp Elementプラグイン"](#)

著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を隨時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5225.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。