SAML認証設定を管理する

Active IQ Unified Manager

NetApp
October 15, 2025

目次

SAML認証設定を管理する

リモート認証を設定したあと、Security Assertion Markup Language（SAML）認証を有効にして、Unified ManagerのWeb UIにアクセスするリモート ユーザをセキュアなアイデンティティ プロバイダ（IdP）で認証するように設定できます。

SAML認証を有効にした場合、Unified Managerのグラフィカル ユーザ インターフェイスにアクセスできるのはリモート ユーザのみです。ローカル ユーザとメンテナンス ユーザはUIにアクセスできません。この設定は、メンテナンス コンソールにアクセスするユーザには影響しません。

アイデンティティ プロバイダの要件

すべてのリモート ユーザに対して SAML 認証を実行するために ID プロバイダ (IdP) を使用するように Unified Manager を構成する場合は、Unified Manager への接続が成功するために必要な構成設定に注意する必要があります。

Unified Manager URI とメタデータを IdP サーバーに入力する必要があります。この情報は、Unified Manager の[SAML 認証]ページからコピーできます。 Unified Manager は、Security Assertion Markup Language (SAML) 標準のサービス プロバイダー (SP) と見なされます。

サポートされる暗号化標準

- Advanced Encryption Standard（AES）：AES-128およびAES-256
- Secure Hash Algorithm（SHA）：SHA-1およびSHA-256

検証済みのアイデンティティ プロバイダ

- Shibboleth
- Active Directoryフェデレーション サービス（ADFS）

ADFSの設定要件

- Unified Manager がこの証明書利用者信頼エントリの ADFS SAML 応答を解析するために必要な 3 つのクレーム ルールを次の順序で定義する必要があります。

要求規則	**Value**
SAM-account-name	Name ID
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Token groups – Unqualified Name	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- 認証方法を「フォーム認証」に設定する必要があります。そうしないと、Unified Manager からログアウトするときにエラーが発生する可能性があります。次の手順を実行します。
  a. ADFS管理コンソールを開きます。

b. 左側のツリー ビューで[認証ポリシー]フォルダをクリックします。

c. 右側の[操作]で、[グローバル プライマリ認証ポリシーの編集]をクリックします。

d. イントラネット認証方法を、デフォルトの「Windows 認証」ではなく「フォーム認証」に設定します。

- Unified Manager セキュリティ証明書が CA 署名されている場合、IdP 経由のログインが拒否されることがあります。この問題の対処方法は2つあります。
  - 次のリンクの手順に従って、CA証明書チェーンの関連する証明書利用者についてのADFSサーバでの失効確認を無効にします。

    "証明書利用者信頼ごとに失効チェックを無効にする"

  - Unified Manager サーバーの証明書要求に署名するには、CA サーバーを ADFS サーバー内に配置します。

その他の設定要件

- Unified Manager のクロック スキューは 5 分に設定されているため、IdP サーバーと Unified Manager サーバー間の時間差は 5 分を超えることはできません。5 分を超えると認証が失敗します。

SAML認証の有効化

Security Assertion Markup Language（SAML）認証を有効にして、Unified ManagerのWeb UIにアクセスするリモート ユーザをセキュアなアイデンティティ プロバイダ（IdP）で認証するように設定できます。

開始する前に

- リモート認証を設定し、正常に動作することを確認しておく必要があります。
- アプリケーション管理者ロールが割り当てられたリモート ユーザまたはリモート グループを少なくとも1つ作成しておく必要があります。
- アイデンティティ プロバイダ（IdP）がUnified Managerでサポートされ、設定が完了している必要があります。
- IdPのURLとメタデータが必要です。
- IdPサーバへのアクセスが必要です。

Unified ManagerでSAML認証を有効にしたあと、Unified Managerサーバのホスト情報を使用してIdPを設定するまでは、ユーザはグラフィカル ユーザ インターフェイスにアクセスできません。そのため、設定プロセスを開始する前に、両方で接続の準備を完了しておく必要があります。IdPの設定は、Unified Managerの設定前にも設定後にも実行できます。

SAML認証を有効にしたあとでUnified Managerのグラフィカル ユーザ インターフェイスにアクセスできるのはリモート ユーザのみです。ローカル ユーザとメンテナンス ユーザはUIにアクセスできません。この設定は、メンテナンス コンソール、Unified Managerコマンド、ZAPIにアクセスするユーザには影響しません。

このページでSAMLの設定を完了すると、Unified Managerが自動的に再起動されます。

手順

1. 左側のナビゲーション ペインで、[全般] > [**SAML** 認証] をクリックします。
2. **SAML** 認証を有効にする チェックボックスを選択します。

   IdPの接続の設定に必要なフィールドが表示されます。

3. IdPのURIとUnified ManagerサーバをIdPに接続するために必要なIdPメタデータを入力します。

   IdP サーバが Unified Manager サーバから直接アクセスできる場合は、IdP URI を入力した後に [**IdP** メタデータの取得] ボタンをクリックして、IdP メタデータ フィールドに自動的に入力することができます。

4. Unified ManagerのホストメタデータURIをコピーするか、ホスト メタデータをXMLテキスト ファイルに保存します。

   この情報を使用してIdPサーバを設定できます。

5. *保存*をクリックします。

   設定を完了してUnified Managerを再起動するかどうかの確認を求めるメッセージ ボックスが表示されます。

6. *確認してログアウト*をクリックすると、Unified Manager が再起動します。

許可されたリモート ユーザがUnified Managerのグラフィカル インターフェイスにアクセスする際にクレデンシャルを入力するページが、次回からUnified Managerのログイン ページではなくIdPのログイン ページに変わります。

まだ完了していない場合は、IdPにアクセスし、Unified ManagerサーバのURIとメタデータを入力して設定を完了します。

> アイデンティティ プロバイダにADFSを使用している場合は、Unified Manager GUIでADFSのタイムアウトが考慮されず、Unified Managerのセッション タイムアウトに達するまでセッションが続行されます。一般 > 機能設定 > 非アクティブ タイムアウト をクリックすると、GUI セッション タイムアウトを変更できます。

SAML認証に使用するIDプロバイダーを変更する

Unified Managerでリモート ユーザの認証に使用するアイデンティティ プロバイダ（IdP）を変更することができます。

開始する前に

- IdPのURLとメタデータが必要です。
- IdPへのアクセスが必要です。

新しいIdPの設定は、Unified Managerの設定前にも設定後にも実行できます。

手順

1. 左側のナビゲーション ペインで、[全般] > [**SAML** 認証] をクリックします。
2. 新しいIdPのURIとUnified ManagerサーバをIdPに接続するために必要なIdPメタデータを入力します。

IdP が Unified Manager サーバーから直接アクセスできる場合は、IdP URL を入力した後に **IdP** メタデータの取得 ボタンをクリックすると、IdP メタデータ フィールドに自動的に入力されます。

3. Unified ManagerのメタデータURIをコピーするか、メタデータをXMLテキスト ファイルに保存します。
4. *[構成を保存]*をクリックします。

   設定を変更するかどうかの確認を求めるメッセージ ボックスが表示されます。

5. [OK]をクリックします。

新しいIdPにアクセスし、Unified ManagerサーバのURIとメタデータを入力して設定を完了します。

許可されたリモート ユーザがUnified Managerのグラフィカル インターフェイスにアクセスする際にクレデンシャルを入力するページが、次回から古いIdPのログイン ページではなく新しいIdPのログイン ページに変わります。

Unified Manager のセキュリティ証明書の変更後に SAML 認証設定を更新する

Unified Manager サーバーにインストールされている HTTPS セキュリティ証明書を変更する場合は、SAML 認証構成設定を更新する必要があります。証明書が更新されるのは、ホスト システムの名前を変更した場合、ホスト システムに新しいIPアドレスを割り当てた場合、システムのセキュリティ証明書を手動で変更した場合です。

セキュリティ証明書が変更され、Unified Manager サーバーが再起動されると、SAML 認証は機能しなくなり、ユーザーは Unified Manager グラフィカル インターフェイスにアクセスできなくなります。ユーザー インターフェイスへのアクセスを再度有効にするには、IdP サーバーと Unified Manager サーバーの両方で SAML 認証設定を更新する必要があります。

手順

1. メンテナンス コンソールにログインします。
2. メイン メニュー*で、***SAML** 認証を無効にする オプションの番号を入力します。

   SAML認証を無効にしてUnified Managerを再起動することの確認を求めるメッセージが表示されます。

3. 更新された FQDN または IP アドレスを使用して Unified Manager ユーザー インターフェイスを起動し、更新されたサーバー証明書をブラウザで受け入れ、メンテナンス ユーザーの資格情報を使用してログインします。
4. *セットアップ/認証*ページで、*SAML 認証*タブを選択し、IdP 接続を構成します。
5. Unified Managerのホスト メタデータURIをコピーするか、ホスト メタデータをXMLテキスト ファイルに保存します。
6. *保存*をクリックします。

   設定を完了してUnified Managerを再起動するかどうかの確認を求めるメッセージ ボックスが表示されます。

7. *確認してログアウト*をクリックすると、Unified Manager が再起動します。

8. IdP サーバーにアクセスし、Unified Manager サーバーの URI とメタデータを入力して構成を完了します。

アイデンティティプロバイダー	設定手順
ADFS	a. ADFS管理GUIで、既存の証明書利用者信頼エントリを削除します。 b. 新しい証明書利用者信頼エントリを追加するには、 `saml_sp_metadata.xml`更新された Unified Manager サーバーから。 c. Unified Manager がこの証明書利用者信頼エントリの ADFS SAML 応答を解析するために必要な 3 つのクレーム ルールを定義します。 d. ADFS Windowsサービスを再開します。
Shibboleth	a. Unified Managerサーバーの新しいFQDNを `attribute-filter.xml`そして `relying-party.xml`ファイル。 b. Apache Tomcat Webサーバを再起動し、ポート8005がオンラインになるまで待ちます。

9. Unified Managerにログインし、IdP経由のSAML認証が想定どおりに機能することを確認します。

SAML認証を無効にする

リモート ユーザーが Unified Manager Web UI にログインする前に、セキュア ID プロバイダー (IdP) を介した認証を停止する場合は、SAML 認証を無効にすることができます。SAML認証が無効な場合は、Active DirectoryやLDAPなどの設定済みのディレクトリ サービス プロバイダによるサインオン認証が行われます。

SAML認証を無効にすると、設定されているリモート ユーザに加え、ローカル ユーザとメンテナンス ユーザもグラフィカル ユーザ インターフェイスにアクセスできるようになります。

グラフィカル ユーザ インターフェイスにアクセスできない場合、SAML認証はUnified Managerメンテナンス コンソールからも無効にすることができます。

SAML認証を無効にしたあと、Unified Managerが自動的に再起動されます。

手順

1. 左側のナビゲーション ペインで、[全般] > [**SAML** 認証] をクリックします。
2. **SAML** 認証を有効にする チェックボックスをオフにします。
3. *保存*をクリックします。

   設定を完了してUnified Managerを再起動するかどうかの確認を求めるメッセージ ボックスが表示されます。

4. *確認してログアウト*をクリックすると、Unified Manager が再起動します。

リモート ユーザがUnified Managerのグラフィカル インターフェイスにアクセスする際にクレデンシャルを入力するページが、次回からIdPのログイン ページではなくUnified Managerのログイン ページに変わります。

IdP にアクセスし、Unified Manager サーバーの URI とメタデータを削除します。

メンテナンスコンソールから**SAML**認証を無効にする

Unified Manager GUIにアクセスできない場合は、必要に応じてメンテナンス コンソールからSAML認証を無効にすることができます。この状況は、設定に誤りがある場合やIdPにアクセスできない場合に発生します。

開始する前に

メンテナンス コンソールにメンテナンス ユーザとしてアクセスできる必要があります。

SAML認証が無効な場合は、Active DirectoryやLDAPなどの設定済みのディレクトリ サービス プロバイダによるサインオン認証が行われます。設定されているリモート ユーザに加え、ローカル ユーザとメンテナンス ユーザもグラフィカル ユーザ インターフェイスにアクセスできるようになります。

SAML認証は、UIの[セットアップ / 認証]ページからも無効にできます。

SAML認証を無効にしたあと、Unified Managerが自動的に再起動されます。

手順

1. メンテナンス コンソールにログインします。
2. メイン メニュー*で、***SAML** 認証を無効にする オプションの番号を入力します。

   SAML認証を無効にしてUnified Managerを再起動することの確認を求めるメッセージが表示されます。

3. **y** と入力して Enter キーを押すと、Unified Manager が再起動します。

リモート ユーザがUnified Managerのグラフィカル インターフェイスにアクセスする際にクレデンシャルを入力するページが、次回からIdPのログイン ページではなくUnified Managerのログイン ページに変わります。

必要に応じて、IdPにアクセスしてUnified ManagerサーバのURIとメタデータを削除します。

[SAML認証]ページ

[SAML 認証]ページでは、Unified ManagerのWeb UIにログインするリモート ユーザを、セキュアなアイデンティティ プロバイダ（IdP）経由でSAMLを使用して認証するようにUnified Managerを設定することができます。

- SAML設定を作成または変更するには、アプリケーション管理者ロールが必要です。
- リモート認証を設定しておく必要があります。
- リモート ユーザまたはリモート グループを少なくとも1つ設定しておく必要があります。

リモート認証とリモート ユーザの設定後、[SAML認証を有効にする]チェックボックスを選択し、セキュアなアイデンティティ プロバイダを使用した認証を有効にすることができます。

- **IdP URI**

  Unified Manager サーバーから IdP にアクセスするための URI。URIの例を次に示します。

  ADFSのURIの例：

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  ShibbolethのURIの例：

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **IdP**メタデータ

  XML形式のIdPメタデータ。

  IdP URL が Unified Manager サーバーからアクセスできる場合は、[**IdP** メタデータの取得] ボタンをクリックしてこのフィールドに入力できます。

- ホストシステム **(FQDN)**

  インストール時に定義された Unified Manager ホスト システムの FQDN。この値は必要に応じて変更できます。

- ホスト**URI**

  IdP から Unified Manager ホスト システムにアクセスするための URI。

- ホストメタデータ

  XML 形式のホスト システム メタデータ。