SAML認証設定の管理

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/active-iq-unified-manager-918/config/concept_manage_saml_authentication_settings_um.html on November 13, 2026. Always check docs.netapp.com for the latest.

目次

SAML認証設定の管理 . . . 1
- Active IQ Unified Manager で SAML 認証を有効にする . . . 1
- Active IQ Unified Manager でIDプロバイダーを使用する . . . 1
  - サポートされる暗号化標準 . . . 1
  - 検証済みのアイデンティティ プロバイダ . . . 1
  - ADFSの設定要件 . . . 1
  - その他の設定要件 . . . 2
- Active IQ Unified Manager で SAML 認証を有効にする . . . 2
- Active IQ Unified Manager でSAML認証IDプロバイダーを変更する . . . 3
- Active IQ Unified Manager のセキュリティ証明書変更後に SAML 認証設定を更新する . . . 4
- Active IQ Unified Manager で SAML 認証を無効にする . . . 5
- Active IQ Unified Manager メンテナンスコンソールから SAML 認証を無効にする . . . 6
- Active IQ Unified Manager の SAML 認証ページを使用する . . . 6

SAML認証設定の管理

Active IQ Unified Manager で SAML 認証を有効にする

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。

Active IQ Unified Manager でIDプロバイダーを使用する

Unified ManagerでIDプロバイダー（IdP）を使用してすべてのリモートユーザーのSAML認証を実行するように構成する場合、Unified Managerへの接続を成功させるために必要な構成設定について理解しておく必要があります。

Unified Managerの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）標準において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以下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「`Forms Authentication`」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際にユーザーがエラーを受け取る可能性があります。以下の手順に従ってください。

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 Authentication`」ではなく「`Forms Authentication`」に設定してください。

- Unified Managerのセキュリティ証明書がCAによって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。この問題を解決するには、2つの回避策があります。
  - 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。

    "信頼当事者トラストごとの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ために、CAサーバーをADFSサーバー内に配置してください。

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分を超えてはならず、超えると認証が失敗します。

Active IQ Unified Manager で SAML 認証を有効にする

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、**General** > **SAML Authentication** 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 サーバーに Unified Manager サーバー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。

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 が再起動されます。

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。

IDプロバイダとしてADFSを使用している場合、Unified ManagerのGUIにはADFSのタイムアウトが適用されず、Unified Managerのセッションタイムアウトに達するまで動作し続けます。GUIセッションのタイムアウトを変更するには、一般 > 機能設定 > *非アクティブタイムアウト*をクリックします。

Active IQ Unified Manager でSAML認証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、**General** > **SAML Authentication** 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。

   Unified Manager サーバーから IdP に直接アクセスできる場合は、IdP URL を入力した後、**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. 設定を保存 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。

Active IQ Unified Manager のセキュリティ証明書変更後に 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に変更を加えた場合は、SAML認証構成設定を更新する必要があります。ホストシステムの名前を変更したり、ホストシステムに新しいIPアドレスを割り当てたり、システムのセキュリティ証明書を手動で変更したりすると、証明書が更新されます。

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認証が機能しなくなり、ユーザーはUnified Managerのグラフィカルインターフェースにアクセスできなくなります。ユーザーインターフェー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てください。

   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の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承認してから、メンテナンスユーザーの認証情報を使用してログインします。
4. *設定/認証*ページで、*SAML認証*タブを選択し、IdP接続を設定します。
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 が再起動されます。
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設定を完了してください。

ID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. 更新されたUnified Managerサーバーの `saml_sp_metadata.xml`を使用して、新しい証明書利用者信頼エントリを追加します。 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`および `relying-party.xml`ファイルに更新します。 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。

Active IQ Unified Manager で SAML 認証を無効にする

Unified Manager の Web UI にログインする前に、セキュアな ID プロバイダー（IdP）を介したリモートユーザーの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 認証が無効になっている場合、Active Directory や LDAP などの構成済みのディレクトリサービスプロバイダーがサインオン認証を実行します。

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、**General** > **SAML Authentication** をクリックします。
2. 「SAML認証を有効にする」チェックボックスのチェックを外します。
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 が再起動されます。

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てください。

Active IQ Unified Manager 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てください。

   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が再起動されます。

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。

Active IQ Unified Manager の SAML 認証ページを使用する

[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。以下にURIの例を示します。

  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。

  Unified ManagerサーバーからIdP URLに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。必要に応じてこの値を変更できます。

- 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。

著作権に関する情報

Copyright © 2026 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随時、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 5252.227-19（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。