テクニカル レポート

ONTAPでの多要素認証

ベストプラクティスと実装ガイド

NetApp
Dan Tulledge / Matt Trudewind
2023年7月| TR-4647

概要

このドキュメントでは、NetApp System Manager、Active IQ® Unified Manager、およびONTAP セキュアシェル（SSH）CLI認証用のNetApp® ONTAP® 9.3ソフトウェアで導入された管理アクセス用の多要素認証機能について説明します。

目次

表一覧

図一覧

強力な管理クレデンシャルの要件

2023年のVerizon Data Breach Investigative Report（VDBIR）によると、データ侵害の49%は、盗まれた認証情報の使用に関連しています。国家のサイバーセキュリティ改善に関するホワイトハウス大統領令やPCIデータセキュリティ基準(PCI DSS)など、米国連邦政府からの新しい要件が浮上しています。これらの要件では、IDに関連付けられたユーザーがそのユーザーであることをユーザーアカウントが証明または検証することが義務付けられています。具体的には、多要素認証（MFA）メカニズムが必要です。MFAを使用すると、攻撃者がユーザー名とパスワードのみを使用してアカウントを侵害することが不可能になります。MFAでは、ユーザを認証するために2つ以上の独立した要素が必要です。二要素認証の例としては、秘密鍵などのユーザが所有するものや、パスワードなどのユーザが知っているものがあります。

NetApp ONTAP 9.3以降では、この要件（NetApp System ManagerおよびActive IQ®Unified ManagerでのWeb認証、NetApp ONTAPでのSSH CLI認証）に対応しています。

表1）MFAの方法

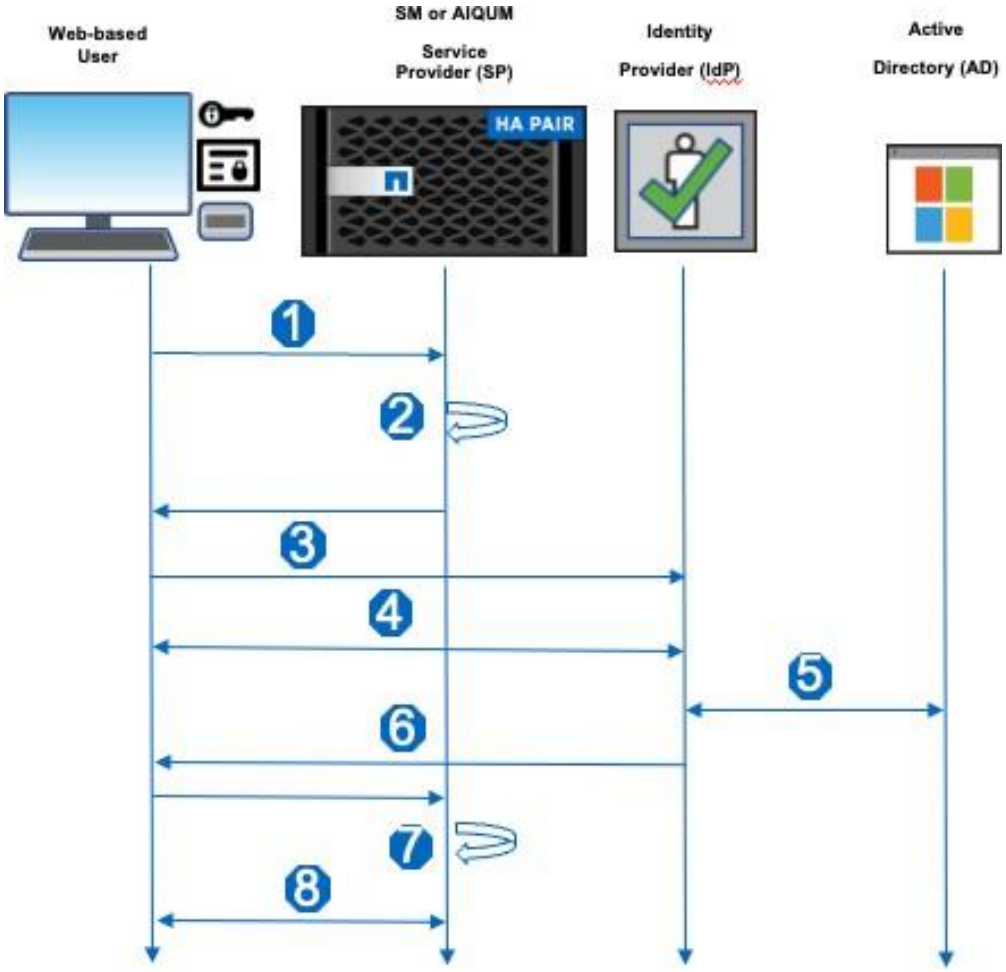
アプリケーション	MFAメソッド
SSH ONTAP CLI	方法1-2要素チェーン認証 ローカルで管理されるONTAPの管理者またはドメインアカウント。プライマリおよびセカンダリの認証方式が、`password` および `publickeynsswitch`、または、およびのチェーンが `publickey`設定されています。タイムベースワンタイムパスワード（TOTP）は、現在の時刻を認証要素の1つとして使用するアルゴリズムによって生成される一時パスコードです。TOTPは、ローカルユーザのセカンダリ認証方式としてのみ使用できます。 方法2-PIVまたはFIDO2認証を使用するYubiKey 公開鍵とYubiKeyデバイスを使用した認証方式を持つONTAPローカル管理者アカウント。Personal Identify Verification（PIV）認証またはFIDO2（Fast Identity Online）認証のいずれかを利用します。 **注：** PIVおよびFIDO2のサポートは、ONTAP 9.12.1以降で利用できます。 **注：** ONTAP 9.13.1では、ドメインアカウント、時間ベースのワンタイムパスワード（TOTP）、および公開鍵の失効がサポートされています。
System Manager ONTAP Webユーザインターフェイスまたは Active IQ Unified Manager Webユーザインターフェイス	Security Assertion Markup Language（SAML）2.0。ONTAP System ManagerまたはActive IQ Unified Managerはサービスプロバイダーロール、Active Directoryフェデレーションサービス（ADFS）、Cisco Duoまたはシボレスはアイデンティティプロバイダー（IdP）ロールです。認証要素はIdPで設定します。 **注：** Cisco Duoのサポートは、ONTAP 9.12.1以降で利用できます。

SAMLベースのWeb対話型ログイン

SAML 2.0は広く採用されている業界標準で、SAMLに準拠したサードパーティのアイデンティティプロバイダ（IdP）が、企業に選択されたIdP固有のメカニズムを使用してシングルサインオン（SSO）のソースとしてMFAを実行できるようにします。

SAML仕様では、プリンシパル、IdP、サービスプロバイダの3つのロールが定義されています。ONTAP環境では、プリンシパルは、System ManagerまたはActive IQ Unified Manager経由でONTAPにアクセスするクラスタ管理者です。IdPは、Microsoft ADFS、Cisco Duo、オープンソースのShibboleth IdPなどの組織が提供するサードパーティ製IdPソフトウェアです。サービスプロバイダは、ONTAPに組み込まれているSAML機能で、System ManagerまたはActive IQ Unified Manager Webアプリケーションで使用されます。

図1）SAMLのワークフロー



管理者は、System ManagerまたはActive IQ Unified Manager Web UIを使用してNetAppノードに接続します。

クラスタに設定されているIdPがSystem ManagerまたはActive IQ Unified Managerで検索されます。

System ManagerまたはActive IQ Unified Managerから、管理者のブラウザがIdPにリダイレクトされます。

IdPで管理者にクレデンシャルを入力するように求められます。

IdPには複数の認証要素があります。

IdPがActive Directoryで管理者のクレデンシャルを検証します。

IdPがSAMLアサーションを発行し、管理者のWebブラウザをSystem ManagerまたはActive IQ Unified Managerにリダイレクトします。

System ManagerまたはActive IQ Unified ManagerがSAMLアサーションを処理し、内部データベースから許可ロールを検索します。

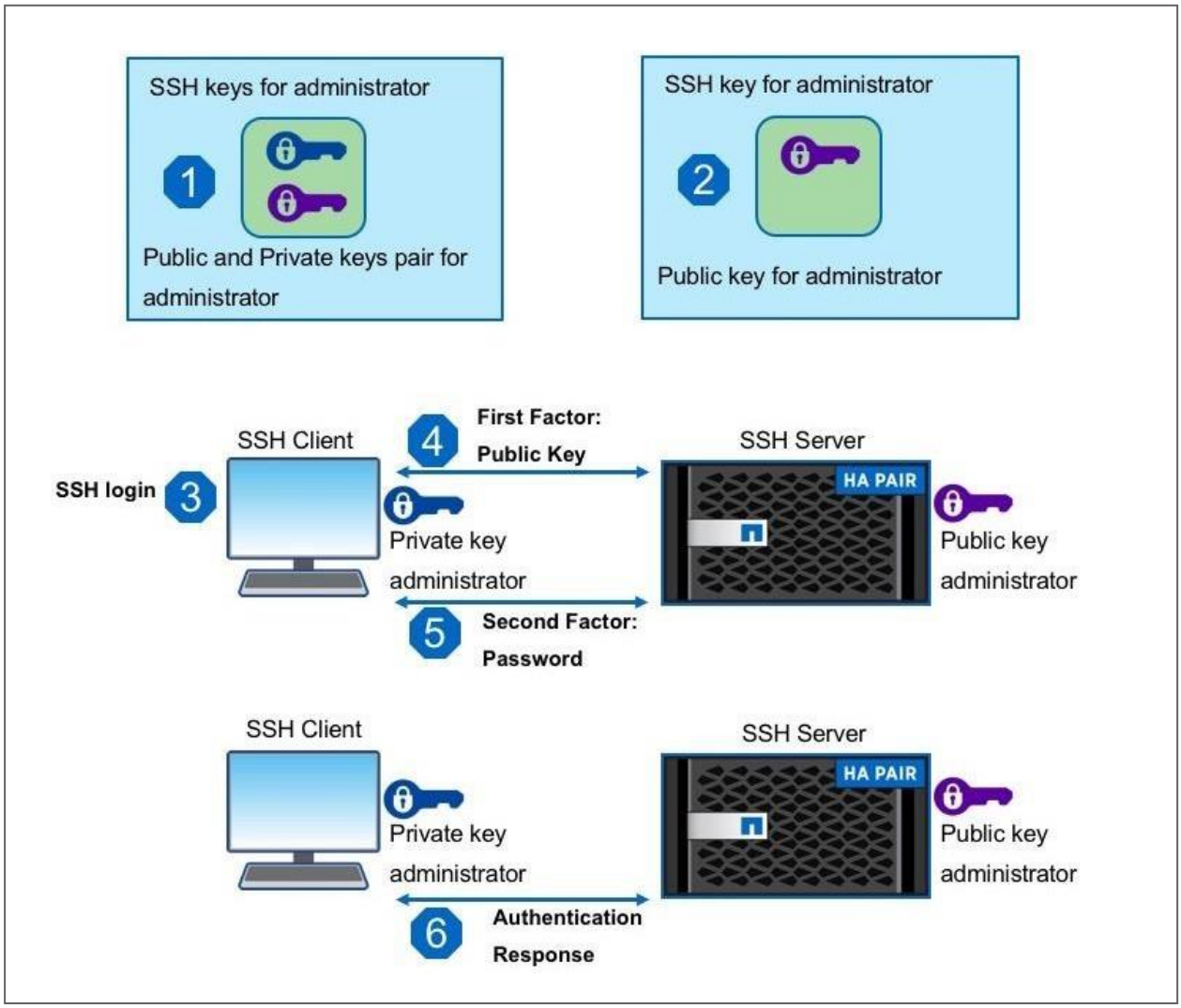
セッションが確立され、System ManagerまたはActive IQ Unified Managerから管理者のWebブラウザにSet-CookieヘッダーでSAMLセッショントークンが返されます。

以降、管理者はセキュアなSAMLトークンを使用してSystem ManagerまたはActive IQ Unified Managerにアクセスできます。

SSH MFAアクセス：2要素チェーン認証を使用したCLIログイン

ONTAP 9.3より前のバージョンONTAPでは、SSHアクセスにはパスワードベースの認証と公開鍵ベースの認証の両方を使用し、それぞれに独立してサポートされていました。ONTAP 9.3では、チェーン認証がサポートされます。公開鍵認証のあとにパスワード認証が続き、2要素認証が提供されます。この機能は、ONTAPローカルアカウントでのみ機能します。ONTAP 9.13.1以降では、Active Directoryドメインアカウントのユーザ IDとパスワードがサポートされます。この機能は、`second-authentication- method security login` コマンドで有効にします。

図2）SSH公開鍵認証とパスワード認証のワークフロー



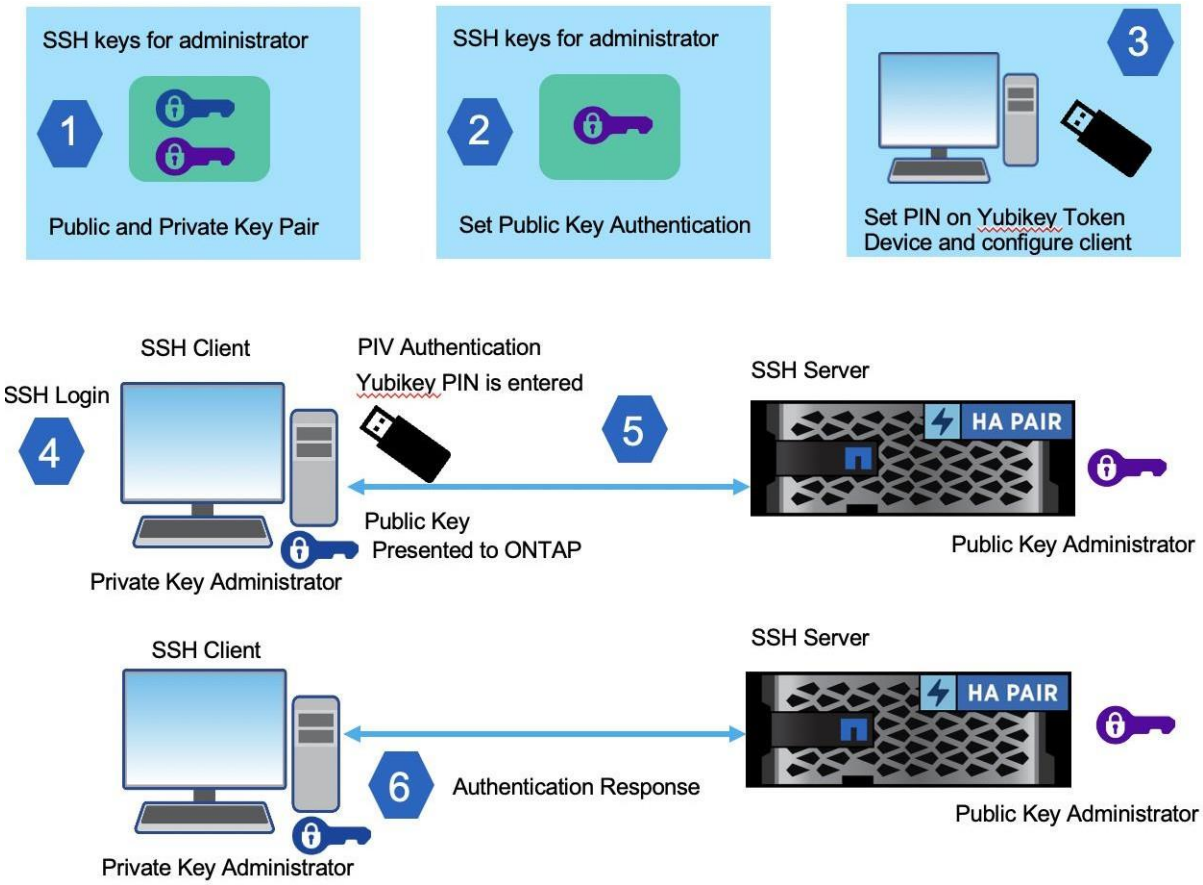
1) 管理者用にSSH公開鍵と秘密鍵のペアが生成されます。

2) 管理者のSSH公開鍵は、ONTAPで2番目の認証方法として設定されます。
   a) ONTAP 9.13.1以降、Time-based-one-time password（TOTP；時間ベースのワンタイムパスワード）は、現在の時刻を認証要素の1つとして使用するアルゴリズムによって生成される一時パスコードです。TOTPは、ローカルユーザのセカンダリ認証方式としてのみ使用できます。詳細については、ONTAPのドキュメントを参照してください。
   b) また、ONTAP 9.13.1では `-x509-certificate security login publickey create`、コマンドを使用してを適用することで公開鍵の失効をサポートしています。
3) 管理者がONTAPへのSSH要求を呼び出します。
4) 部分認証は、管理者の公開鍵を提供して完了します。
5) ONTAPは管理者にパスワードの入力を求め、管理者がパスワードを入力します。
6) 完全認証は2つの要素で成功し、ONTAPはコマンドシェルを提供します。

SSH MFAアクセス：PIVまたはFIDO2認証を使用したYubiKeyによるCLIログイン

ONTAP 9.12.1以降では、PIV認証またはFIDO2認証を使用するYubiKeyハードウェア認証デバイスがサポートされています。YubiKeyハードウェアデバイスはYubicoによって製造され、「強力な2要素、多要素、パスワードレス認証、シームレスなタッチツーサイン」を提供します。PIVは、ONTAP `public-key` 認証とともにYubiKeyデバイスでPIN（Personal Identification Number）を使用する場合、MFAでサポートされます。PINを使用し、ONTAP `public-key` 認証とともにYubiKeyデバイスに物理的にアクセスできる場合、FIDO2はMFAでサポートされます。どちらのソリューションも多要素認証を提供します。この機能は、ONTAPローカルアカウントでのみ機能します。

図3）管理アクセス用のYubiKeyおよびPIVを使用したSSH公開鍵認証



1)管理者用にSSH公開鍵と秘密鍵のペアが生成されます。

管理者のSSH公開鍵は、ONTAPで認証方式として設定されます。

YubiKey PINはハードウェアトークンデバイスで設定され、SSHはクライアントデバイスで設定されます。

管理者がONTAPへのSSH要求を呼び出します。

PINは、ONTAPへの公開鍵認証とともに、PIV認証のために管理者によって入力されます。

完全認証は複数の要素を使用して成功し、ユーザにはONTAPからコマンドシェルが表示されます。

用語

Active Directoryフェデレーションサービス（ADFS）。Microsoftが開発したアイデンティティプロバイダ。Windows Serverオペレーティングシステム上で実行できるため、ユーザーは組織の境界を越えて配置されたシステムやアプリケーションにシングルサインオンでアクセスできます。

クレームルール。要求ルールは、IdPで定義された属性を証明書利用者にマッピングするメカニズムを提供します。これらの属性（ユーザIDや共通名など）は、証明書利用者がIdP認証後に承認をマッピングするために使用されます。

Cisco Duoの略。Cisco Duoは2要素認証解決策で、ユーザIDの検証、デバイスの信頼性の確立、企業のネットワークやアプリケーションへの安全な接続の提供によって、組織のセキュリティを強化します。ONTAPとの統合では、IdPとして機能します。

Kerberos：「チケット」を使用して、セキュアでないネットワークを介して通信するノードが、セキュアな方法で互いのIDを証明できるようにするコンピュータネットワーク認証プロトコル。

Lightweight Directory Access Protocol（LDAP）。インターネットプロトコル（IP）ネットワークを介して分散ディレクトリ情報サービスにアクセスし、管理するための、オープンでベンダーに依存しない業界標準のアプリケーションプロトコルです。

多要素認証（MFA）：コンピュータアクセス制御の方法で、認証メカニズムに複数の別々の証拠を提示した後にのみ、ユーザーにアクセスが許可されます。これらの証拠は、通常、知識(パスワードなど)、所持(スマートカードなど)、遺伝(網膜スキャンなど)のうち少なくとも2つのカテゴリに分類されます。

National Institute of Standards and Technology（NIST；米国標準技術研究所）の略。米国の測定基準研究所および非規制機関商務省。その使命は、イノベーションと産業競争力を促進することです。

Payment Card Industry Data Security Standard（PCI DSS）の略。主要なカードスキームのブランドクレジットカードを扱う組織向けの独自の情報セキュリティ標準。PCI規格はカードブランドによって義務付けられ、Payment Card Industry Security Standards Councilによって管理されています。2018年2月1日より、PCI DSS 3.2は、管理者アクセス権を持つ担当者のカード所有者データ環境(CDE)へのすべての非コンソールアクセスをMFAに義務付け始めました。

証明書利用者。別のシステムエンティティからの情報に基づいてアクションを実行するシステムエンティティ。SAMLの証明書利用者は、証明書利用者（SAML IdP）からプリンシパルまたはユーザに関するアサーションを受信するかどうかに依存します。

SAMLサービスプロバイダ（SAML SP）：MFAをサポートし、認証を外部エンティティ（アイデンティティプロバイダ）にオフロードするすべてのアプリケーション（Active IQ Unified ManagerまたはSystem Manager）。

SAMLアイデンティティプロバイダ（SAML IdP）：SPの認証を処理し、クレデンシャルの検証に成功した場合にSPにリダイレクトする外部のエンティティまたはサービス（MFAまたはそうでない場合）。ADFSとシボレスIdPはSAML IdPの例である。

SAMLメタデータ。2つの通信エンティティ間で構成情報を定義および共有する方法を決定します。たとえば、特定のSAMLバインディング、識別子情報、およびPKI情報に対するエンティティのサポートを定義できます。

Security Assertion Markup Language（SAML）の略。当事者間（特にアイデンティティプロバイダとサービスプロバイダの間）で認証および許可データを交換するためのオープンスタンダード。その名前が示すように、SAMLはXMLベースのマークアップ言語です。

Secure Shell（SSH）：セキュリティ保護されていないネットワーク上でネットワークサービスを安全に運用するためのコマンドライン暗号化ネットワークプロトコル。SSHバージョン2はONTAPで使用されます。

シボレスIdP。Shibbolethはシングルサインオン機能を提供するオープンソースプロジェクトである。これにより、サイトは、プライバシーを保護する方法で、保護されたオンラインリソースへの個々のアクセスについて、情報に基づいた承認決定を下すことができます。

シングルサインオン（SSO）：SAML IdP認証が完了すると、IdPはSAMLアサーションを発行し、管理者のWebブラウザをSystem ManagerまたはActive IQ Unified Managerにリダイレクトします。System ManagerまたはActive IQ Unified ManagerがSAMLアサーションを処理し、内部データベースから許可ロールを検索します。セッションが確立され、System ManagerまたはActive IQ Unified Managerから管理者のWebブラウザにSAMLセッショントークンが返されます。IdPでは、セキュアなSAMLトークンの有効期間がデフォルトで2~8時間に設定されています。寿命は `relying-party- specific` 設定によってオーバーライドできます。管理者はトークンの有効期間中、System ManagerまたはActive IQ Unified Managerへのアクセスを許可されます。

米国公共機関（USPS）2017年12月現在、対象となる防衛情報（CDI）を処理、保存、または送信するUSPS政府の請負業者は、NIST SP 800-171の14の制御ファミリーに準拠するために、DFARS 252.204-7008によって要求されています。DFARSは、「IDおよび認証」制御ファミリーの下で、特権アカウントへのローカルおよびネットワークアクセス、および非特権アカウントへのネットワークアクセスにMFAの使用を指定します。この指令の目的は、CDIを保護するために実施された保障措置が、連邦政府以外の情報システム全体で一貫していることを保証することである。あります。

構成

ONTAP 9.3以降では、MFA構成がサポートされます。ONTAP 9.12.1以降では、FIDO2またはPIVを使用するYubiKeyがサポートされています。SSHを使用してONTAPにCLIアクセスするには、ローカルまたはNetwork Information Service（NIS；ネットワーク情報サービス）およびLightweight Directory Access Protocol（LDAP；ライトウェイトディレクトリアクセスプロトコル）アカウントをONTAPで定義する必要があります。ONTAP 9.13.1以降では、ローカルアカウントまたはNIS/LDAPアカウントに加えて、Active Directoryドメインアカウントも使用できます。

ONTAP SSH 2要素チェーン認証

既存の単一要素認証（1FA）管理者ユーザは、2要素認証（2FA）ログイン方法に変更できます。2つの組み合わせを使用できる3つの方法があります。3つの方法は `password`、、`publickey`および `nsswitch`です。2つの組み合わせは `password`、および `publickeynsswitch`、または `publickey`です。`-authentication-method` またはのいずれかの組み合わせを指定して `-second-authentication-method`、同じ結果を生成できます。

たとえば、管理者は `sam`、`ssh` パスワード認証方式でアプリケーションを使用するように定義されています。2つ目の方法として公開鍵認証を追加するには、次のコマンドを使用します。

```
smrcluster-1::> security login modify -user-or-group-name sam -application ssh -authentication-
method password -second-authentication-method publickey
```

```
Warning: For successful authentication, ensure you create a public key for user "sam" using
"security login publickey create" interface.
```

sam publickey 2番目の認証方法としてを追加する場合は、の公開鍵を入力する必要があることを示す警告メッセージが表示されます。LinuxのOpenSSH/OpenSSLコマンドは ssh-keygen 、のRSA公開鍵と秘密鍵のペアを作成するために使用し samます。Linuxでは、キーは ~/.ssh/id_rsa.pub forに格納され samます。sam SSHにPuTTYクライアントを使用している場合は、 puttygen ユーティリティを使用しての公開鍵と秘密鍵のペアを生成できます sam。ssh-keygen およびの使用方法の詳細 puttygenについては、このドキュメントで後述する「追加情報の検索場所」を参照してください。

sam ssh-keygen Linuxシステムのの出力からIn ONTAPの公開鍵を入力するには、次のコマンドを使用します。

```
smrcluster-1::> security login publickey create -username sam -index 0 -publickey "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDBh8mgwjshX4P3oXw8Qd+s1p2jW8K73mw8ubYhvb+Alx4ZM9T0QmsmYTtFjQQ+bDbp6
ruqjjo
O8hjl+WSVuxUwW5xWRUwYS/rtQmhP/2fudSncwd2cuRxMvMHKSruF8ee2WRTjO7vu7f4a
krCfQL9cOhzh3dEHuFR5qoOgCgr5nq8v3mZpAyoK7C4/uC9Lr8UO3mBctZ6pBfHLnQRCWgxc20FDFI4pM9Lz93fSIQXCCL8xr
pCzi0b
zH+4Dwug1gPJsrfSa7Ki3s1SfNtiAWVqSh78D4iHYT8XjJr1TGVjsvZLg0/UUpwx5nvcR
BWME9EczWi623tPO5fsUSGhQtCPn
smr@cycrh6nbs05.eng.btc.netapp.in" -vserver smrcluster-1
```

これで、sam Chained 2FAを使用して、LinuxシステムからONTAP管理者としてログインできるようになりました。まず、公開鍵認証が実行されます（部分的に成功します）。ONTAPから sam パスワードの入力を求められ、認証が完了します。

```
[sam@centos7 ~]$ ssh ontap9.3.NTAP.LOCAL
Enter passphrase for key '/home/sam/.ssh/id_rsa':
Authenticated with partial success.
Password:
smrcluster-1::>
```

注：この例は sam、の秘密鍵にアクセスするためのパスフレーズのプロンプトを示しています。Linux SSHでは、でパスフレーズが適用された場合にこのプロンプトが生成され ssh-keygenます。の実行中にパスフレーズを入力する必要はありませ ssh-keygenんが、秘密鍵へのアクセスが保護されるため、このパスフレーズを使用することを推奨します。

ONTAPコマンド security login modify -user-or-group-name sam -application ssh -authentication-method password -second-authentication-method publickey では、password がプライマリ認証方式であり、publickey がセカンダリ認証方式であることを指定します。これらの方法は、設定で逆にすることができます。ただし、2FAログインでは、ローカルパスワードファイルまたはNIS/LDAPパスワードのいずれかを使用して、認証の順序は常に公開鍵、パスワードになります。

SSH MFA認証の詳細については、『ONTAP 9セキュリティガイド』の「SSH多要素認証の有効化」を参照してください。

YubiKeyおよびPIVを使用したONTAP SSH MFA認証

既存の単一要素認証（1FA）管理者ユーザは、YubiKeyトークンデバイスとPIVを使用することで、MFAログイン方法をサポートするように変更できます。YubiKeyは、publickey プライマリとして設定する -authentication-method か、publickey -second- authentication-method. IFが -second-authentication-method 指定されている場合に設定することで機能し password、nsswitch プライマリ認証方式として設定する必要があります。

注：ハードウェアベースのSSH MFAの場合、ONTAPで設定される公開鍵に加えて認証要素は次のとおりです。

- PIV
- YubiKeyハードウェアデバイスの所有

Windows向けYubiKey PIVクライアントの設定

ここでは、PIVを使用してONTAPに接続するためのYubiKeyをサポートするようにSSHクライアントを設定する一般的な手順について説明します。Windowsクライアントの手順の概要は次のとおりです。

1) YubiKey Managerをダウンロードしてインストールします。

PIV PINとPUK（PINロック解除コード）を設定して、YubiKeyを初期化します。

ECDSA秘密鍵と証明書を生成またはインポートします。これは、SSH CAPI/PKCS#11クライアントインターフェイスで必要ですが、ONTAPでは使用されません。

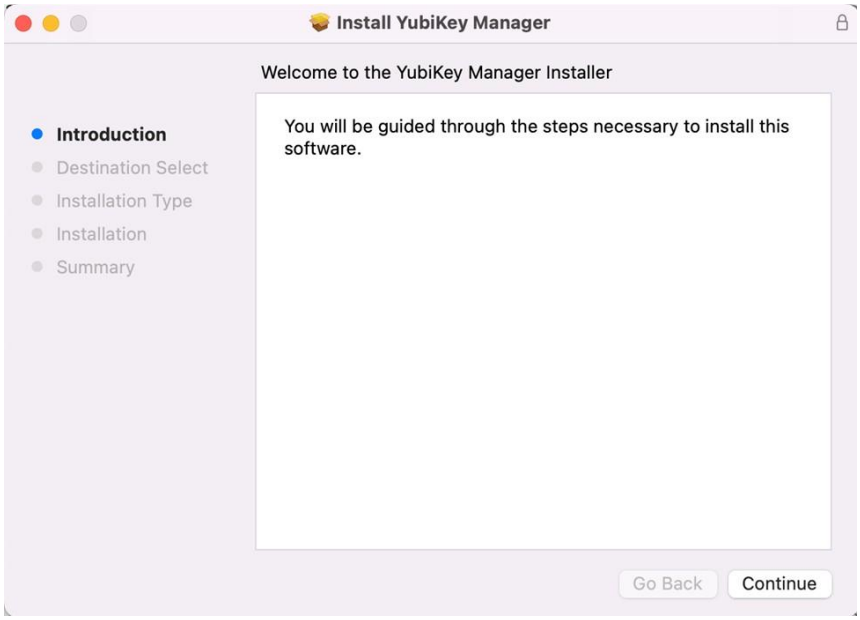
CAPI/PKCS#11インターフェイスを使用するようにSSHクライアントを設定します。

ECDSA証明書または公開鍵をSSH互換の形式に変換します。

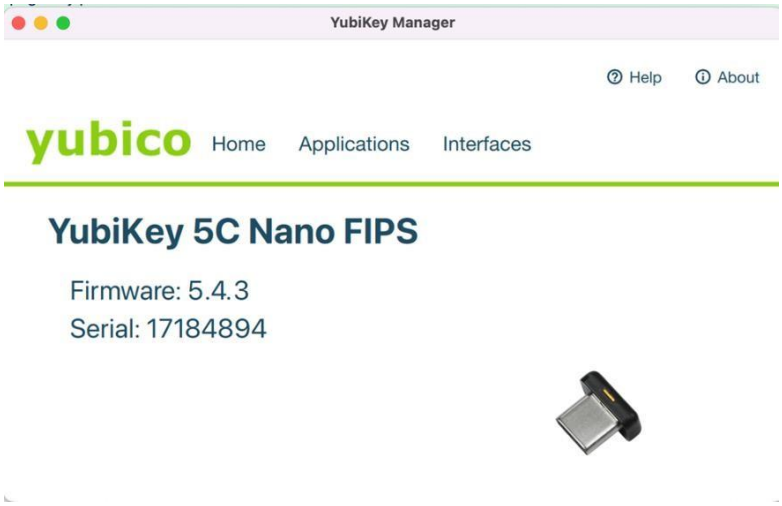
公開ECDSAキーをONTAPにエクスポートします。

YubiKey Managerのダウンロードとインストール

1) YubicoのWebサイトから、お使いのプラットフォームに適したバージョンのYubiKey Managerをダウンロードしてインストールします。[Continue]を選択し、すべてのデフォルトを受け入れます。

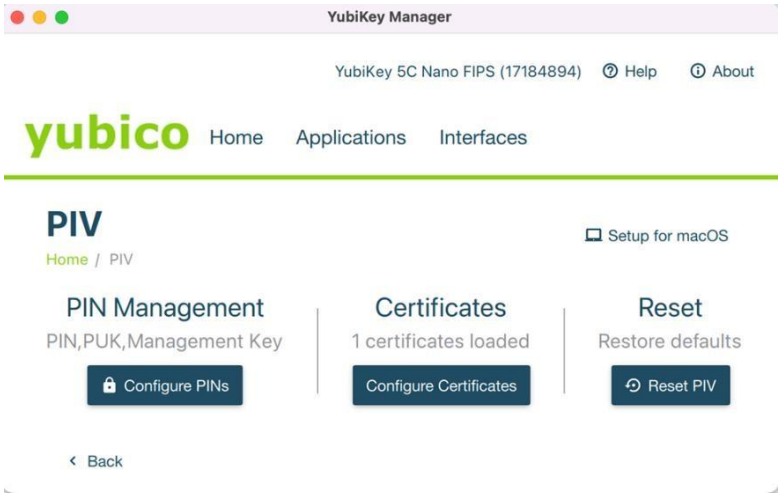


インストールが完了したら、USBスロットにYubiKeyを挿入し、YubiKey Managerを実行します。YubiKeyのモデル、シリアル番号、ファームウェアバージョンが画面に表示されます。

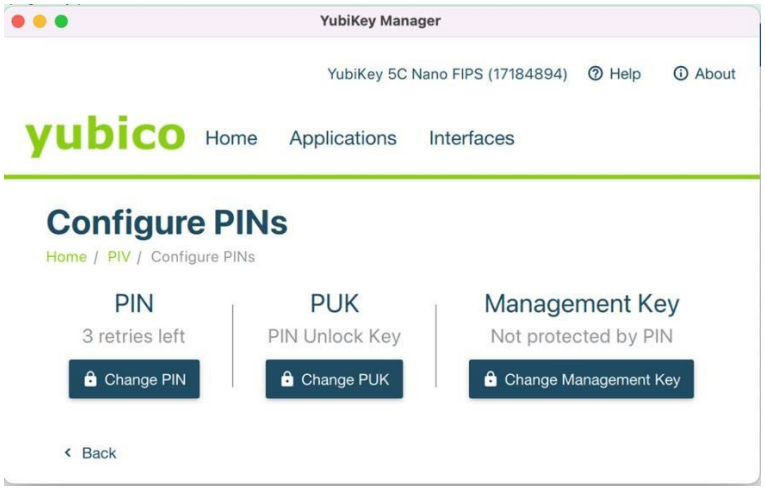


YubiKey PINの初期化

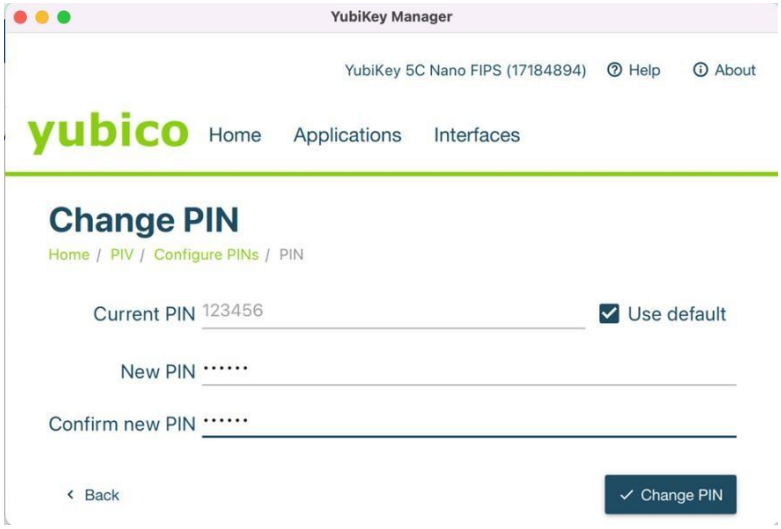
1)アプリケーション> PIVに移動して、PIV設定を構成します。例：



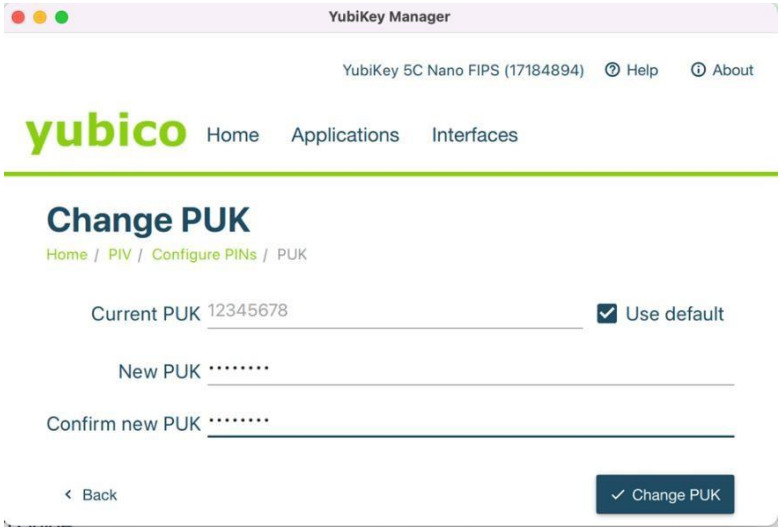
［PIN管理］セクションで［PINの設定］を選択します。例：



［PINの変更］を選択してPINを設定します。4～8文字のPINを選択します。YubiKeyを初めて設定する場合は、[デフォルトを使用]オプションをオンにします。それ以外の場合は、現在のPINを入力します。工場出荷時のデフォルトPINは123456です。新しいPINを2回入力し、[Change PIN]を選択します。



Personal Unblocking Code (PUC)と呼ばれることもあるPUKを設定します。これは、紛失または忘れたPINをリセットするために使用します。6～8文字のPUKを選択します。YubiKeyを初めて設定する場合は、[デフォルトを使用]オプションをオンにします。それ以外の場合は、現在のPUK値を入力します。工場出荷時のデフォルトPUKは12345678です。新しいPUKを2回入力し、[Change PUK]を選択します。

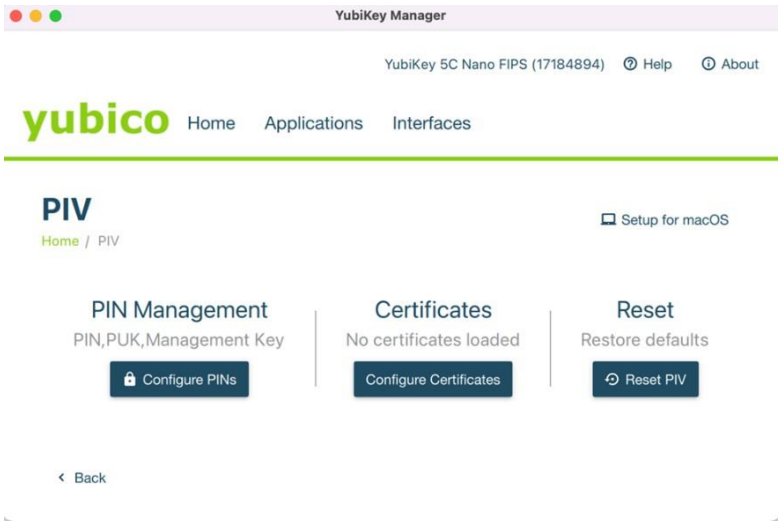


注: 管理キーも変更することをお勧めします。デフォルトの3DES管理キーは010203040505060708010203040506070801020304050607080です。PIN、PUK、および管理キーの詳細については、YubicoのWebサイトを参照してください。

秘密鍵と証明書をインポートまたは生成する

SSH上のPIV認証にYubiKeyを使用するには、プライベートECDSAキーと証明書をインポートまたは生成する必要があります。ONTAP 9.12.1以降では、SSH公開鍵認証にECDSA-256またはECDSA-384キーが使用されます。次の例では、ECDSA-384を使用しています。証明書はONTAP SSHサーバでは使用されず、証明書の公開鍵のみが使用されます。

1) YubiKeyのスロット9aは、PIVキーの保存に使用されます。[証明書の設定]を選択します。

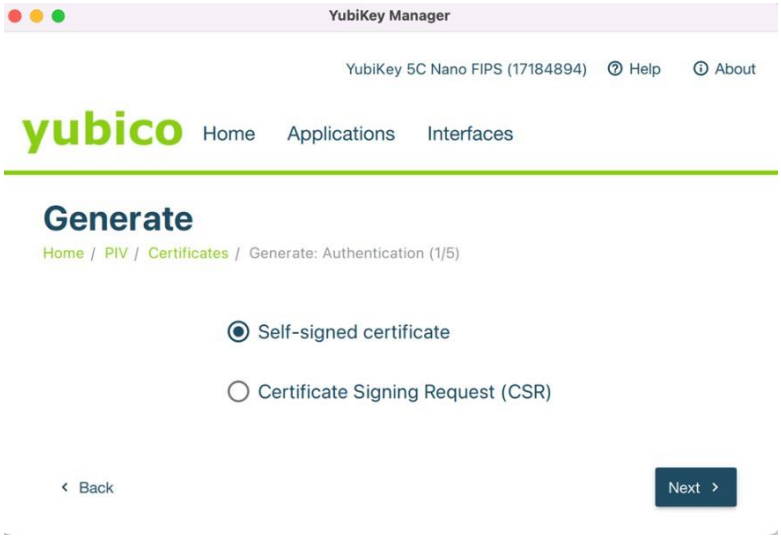


a) [Generate]を選択して続行します。この例では、ECDSAの秘密鍵と公開鍵のペアはP-384曲線を使用して生成されます。

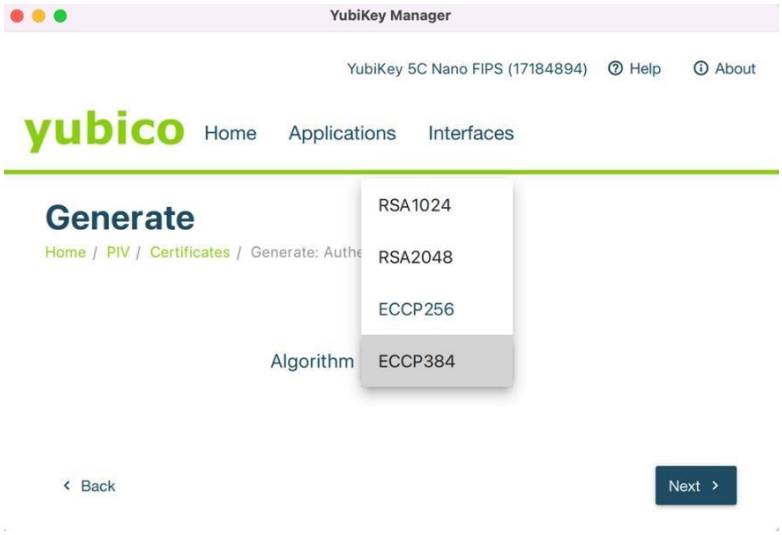
[自己署名証明書]を選択します。この例では、自己署名証明書が生成されます。これは、証明書がONTAPでは使用されず、PKCS#11インターフェイスでのみ必要とされるためです。

注： 導入環境によっては、証明書署名要求（CSR）を事前に生成し、信頼されたCAによる署名を受けてから、署名済み証明書をインポートしなければならない場合があります。

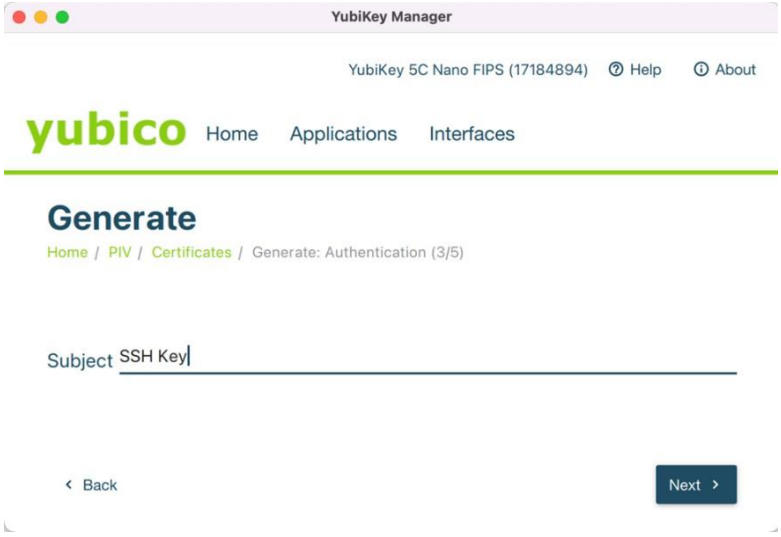
[自己署名証明書]を選択したら、[次へ]を選択します。



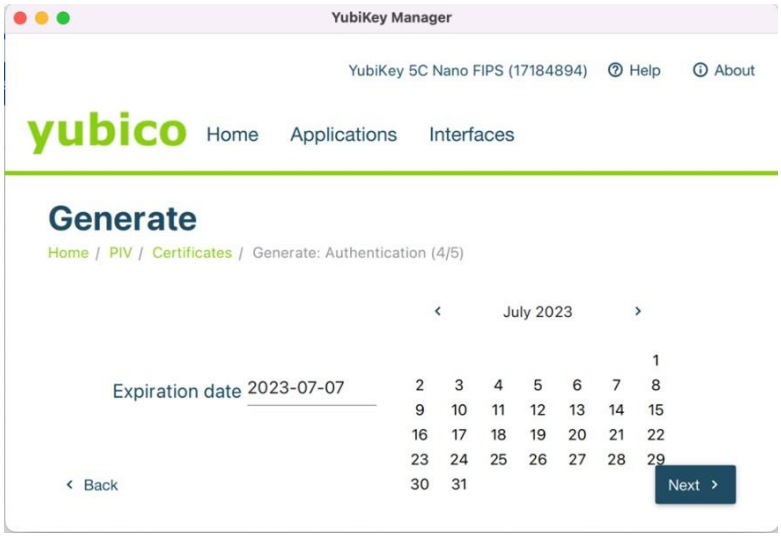
アルゴリズムにECCP-384を選択し、[次へ（Next）]を選択します。



件名（CN）の文字列を入力します。次に、SSHキーに設定する例を示します。



[Next]を選択します。次の画面では、証明書の有効期限を確認するメッセージが表示されます。デフォルトでは1年に設定されています。これはSSHには適用されないため、デフォルトをそのまま使用できます。



最後のダイアログボックスに、選択したオプションが表示されます。[Generate]を選択して、選択内容を確認します。

続行するには、管理キーを入力するように求められます。管理キーが変更されている場合は入力し、工場出荷時のデフォルト設定に設定されている場合は[Use Default]を選択します。

PINの入力を求められます。初期化手順で設定したPINを入力し、[OK]を選択します。

注： 秘密鍵と証明書が生成され、関連する情報が[証明書]セクションに表示されます。

YubiKey PIV認証用のWindows PuTTY-CAC SSHクライアントの設定

YubiKey PIVで公開鍵認証を使用してSSH経由でONTAPに接続する簡単な方法は、PuTTY-CACを使用することです。PuTTY-CACは、スマートカード認証をサポートするオープンソースのSSHクライアントで、特に国防総省共通アクセスカード（CAC）とPIVをPKIトークンとして使用します。これは連邦政府の配備で広く使用されています。

PuTTY-CACはGitHubからダウンロードしてインストールできます。
https://github.com/NoMoreFood/putty-CAC/releases

PuTTY-CACの設定手順の概要は次のとおりです。

1) Yubico PIVツールをインストールします。これには、YubiKeyとやり取りするために必要なPKCS#11ライブラリ(「YKCS11」)のYubicoバージョンが含まれています。

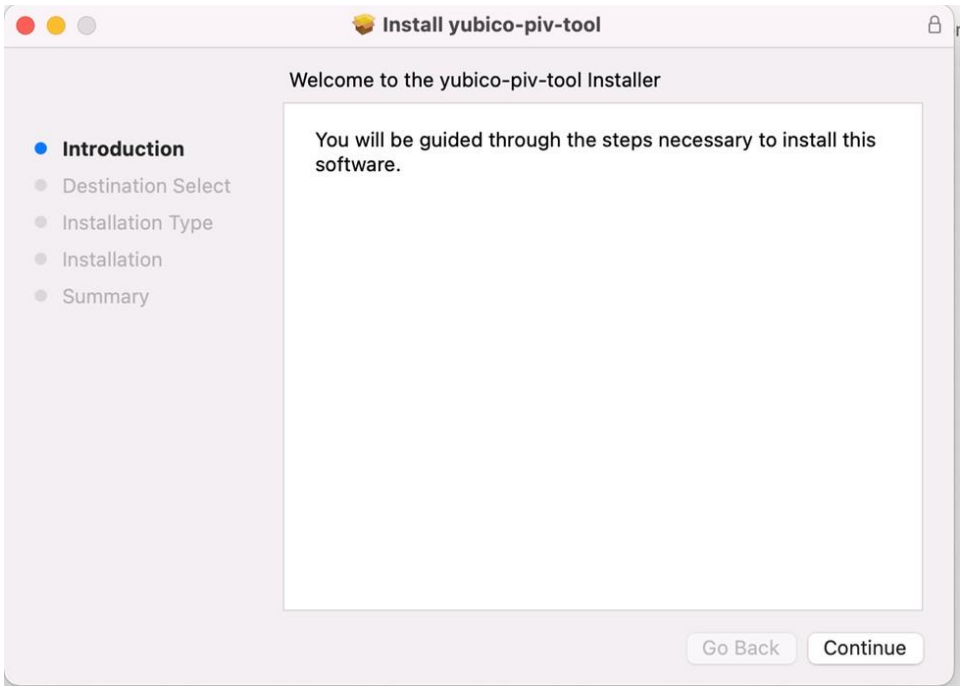
PKCS#11ライブラリを使用して、YubiKeyから証明書を設定します。

SSH互換のECDSAまたはRSA公開鍵をクリップボードにコピーして保存します。

PuTTYセッションホストを設定します。

Yubico PIVツールの取り付け

https://developers.yubico.com/yubico-piv-tool/Releases/から、プラットフォーム用のYubico PIVツールを入手してインストールします。すべてのデフォルトを受け入れます。例：



YubiKeyから取得したPKCS#11証明書の設定

1) PuTTY-CACを起動します。

PuTTY接続ウィンドウで、[Connection]>[SSH]>[Certificate]の順に選択します。

[Set PKCS #11 Cert]を選択します。

Yubico PKCS#11ライブラリを指定します。

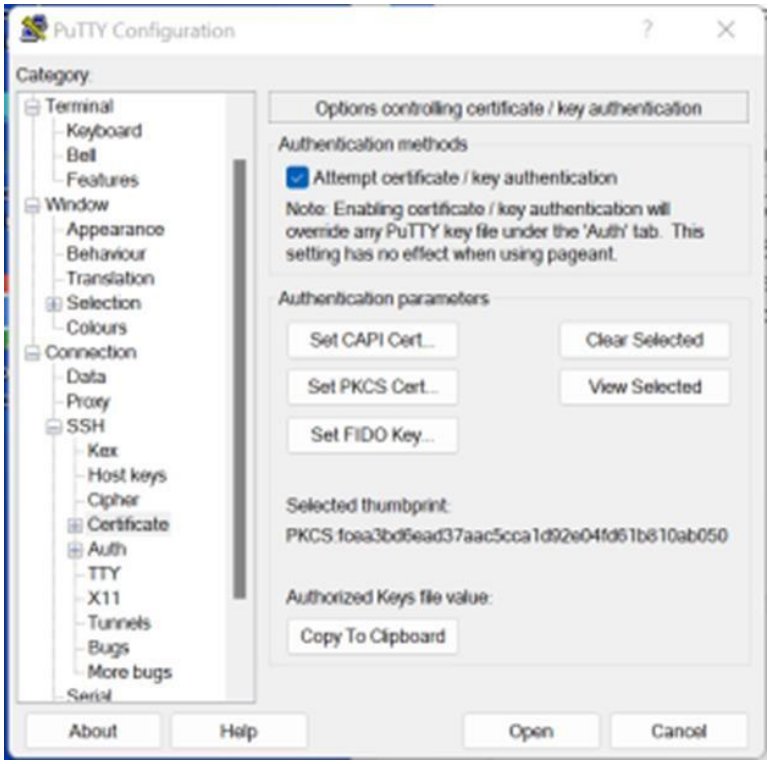
> これがすべてのデフォルトを使用して64ビットのWindows 10/11クライアントにインストールされている場合、このライブラリはにあります。`C:\Program Files\Yubico\Yubico PIV Tool\bin\libykcs11.dll`

ファイルを選択して開きます。

前の手順で示したように、ECDSAキーとYubiKeyの証明書が正常に生成された場合は、その証明書が表示されます。

CNとIssuerをチェックして、以前に生成した証明書であることを確認し、[OK]を選択して続行します。

[Authentication Methods]ダイアログボックスに戻ります。設定に成功すると、選択した証明書のフィンガープリントが表示されます。



SSH互換のECDSA公開鍵をクリップボードにコピーする

1)「クリップボードにコピー」を選択して、SSH互換の公開鍵をクリップボードにコピーします。

次の手順で、この公開鍵を使用してONTAPユーザを設定する必要があります。

PKCS#11ライブラリを介してYubiKeyから取得したSSH互換の公開鍵は、次の形式になります。

```
<key-type> <Base64-encoded public-key> PKCS:<thumbprint><Path-to-YKCS#11 library> CN=<common
name>
```

公開鍵の例：

```
ecdsa-sha2-nistp384
AAAAE2VjZHNhLXNoYTItbmlzdHAzODQAAAAIbmlzdHAzODQAAABhBNsiM3p/oUdcsyeiEFDuvikAFWrMiT7uzp7B9AT++yMbz
kb2oRE
VErfOo+GBPHi3NI1+qrBz/3TlkJG2BQwfD1lcZAiFgp97yhvSJos8GqTY5E6FiTd1rzuLraBxjZxsNg== PKCS:fcea3bd6e
ad37aa
c5cca1d92e04fd61b810ab050=C:\Program Files\Yubico\Yubico PIV Tool\bin\libykcs11.dll
CN=chyelinecc384
```

ONTAPユーザアカウントの公開鍵認証メカニズムを設定します。ONTAPアカウントを設定して公開鍵に関連付けたら、PuttyなどのSSHクライアントを使用してONTAPシステムを管理できます。

次の手順については、「ONTAPでYubiKey PIVの公開鍵認証を構成する」を参照してください。

MAC OSおよびLinux用のYubiKey PIVクライアントの設定

ここでは、PIVを使用してONTAPに接続するためのYubiKeyをサポートするようにSSHクライアントを設定する一般的な手順について説明します。Mac OSおよびLinuxクライアントの手順の概要は次のとおりです。

1) YubiKey Managerをダウンロードしてインストールします。

PIV、PIN、PUKを設定してYubiKeyを初期化します。

ECDSA秘密鍵と証明書を生成またはインポートします。これは、SSH CAPI/PKCS#11クライアントインターフェイスで必要ですが、ONTAPでは使用されません。

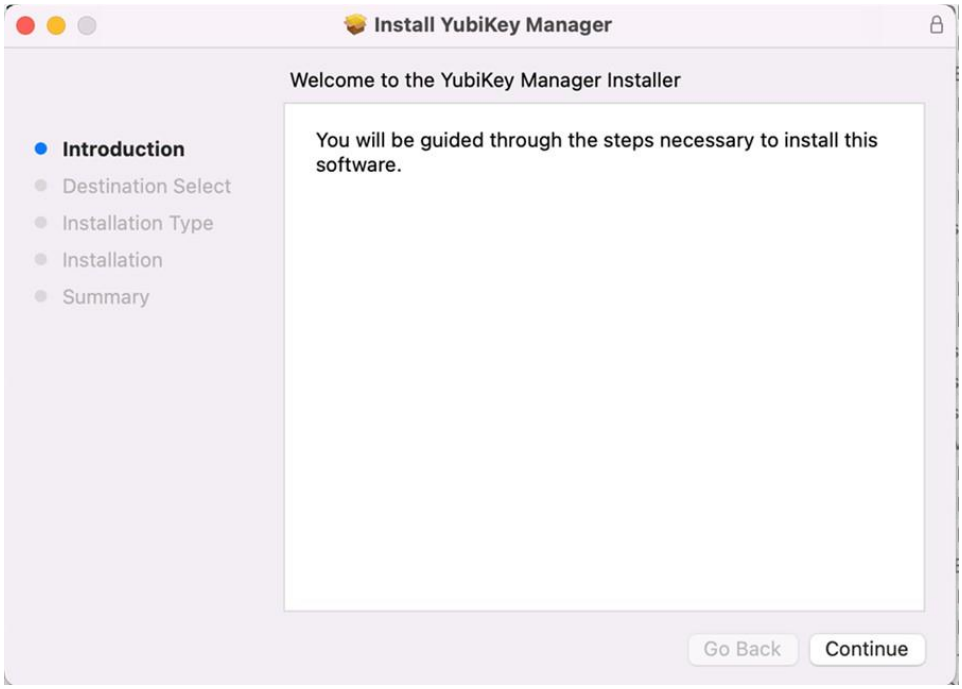
CAPI/PKCS#11インターフェイスを使用するようにSSHクライアントを設定します。

ECDSA証明書または公開鍵をSSH互換の形式に変換します。

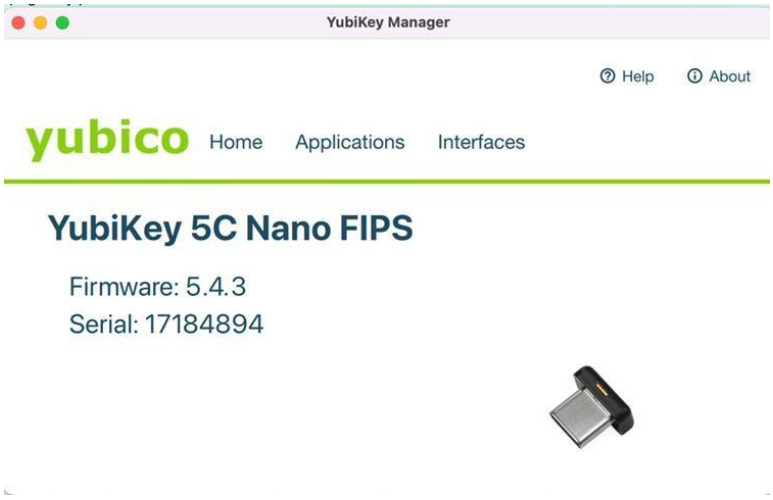
公開ECDSAキーをONTAPにエクスポートします。

YubiKey Managerのダウンロードとインストール

1)YubicoのWebサイトから、お使いのプラットフォームに適したバージョンのYubiKey Managerをダウンロードしてインストールします。[Continue]を選択し、すべてのデフォルトを受け入れます。例：

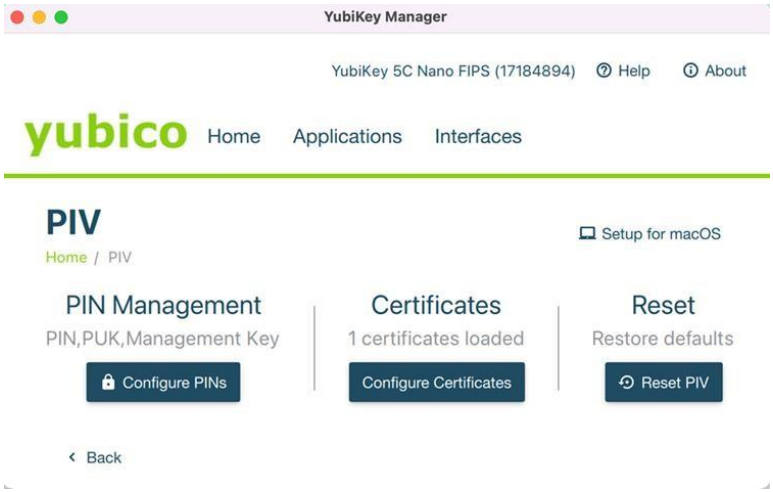


インストールが完了したら、USBスロットにYubiKeyを挿入し、YubiKey Managerを実行します。YubiKeyのモデル、シリアル番号、ファームウェアバージョンが画面に表示されます。

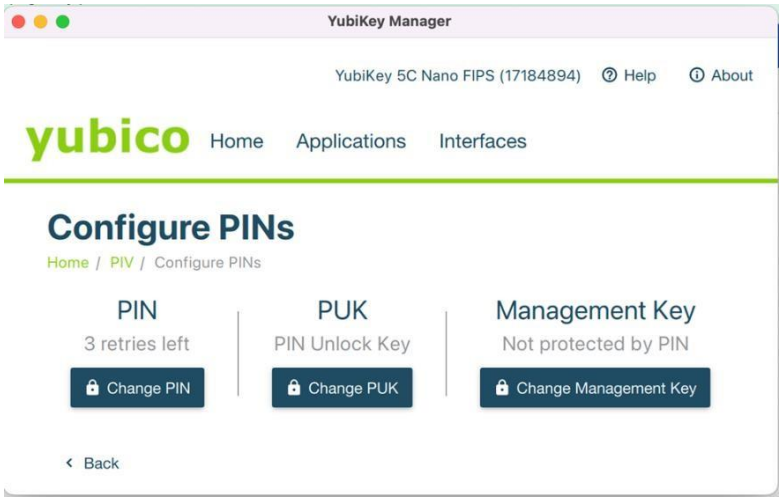


YubiKey PINの初期化

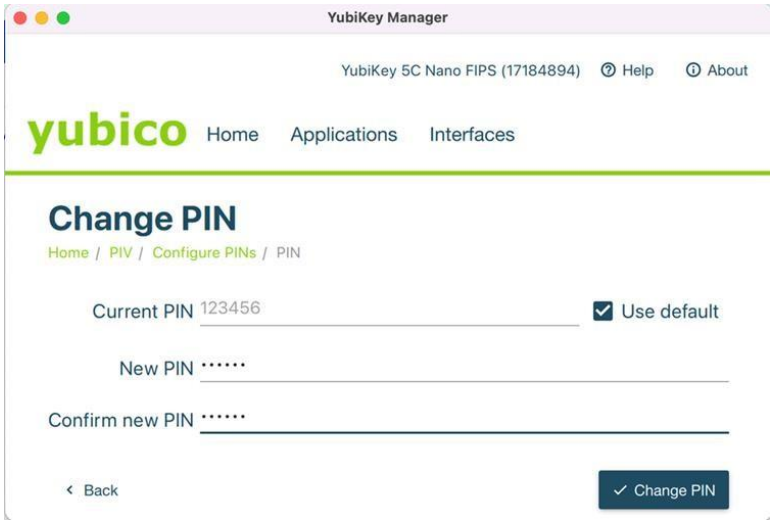
1) Applications > PIVに移動して、PIV設定を構成します。例：



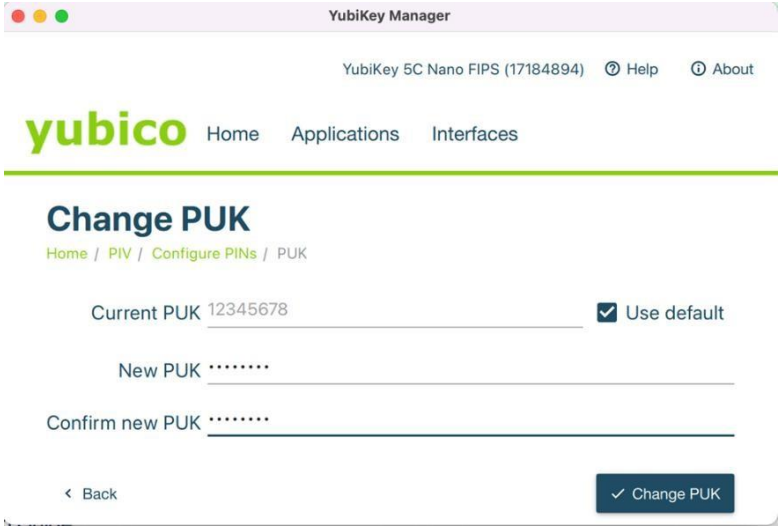
［PIN管理］セクションで［PINの設定］をクリックします。例：



［PINの変更］を選択してPINを設定します。4～8文字のPINを選択します。YubiKeyを初めて設定する場合は、[デフォルトを使用]オプションをオンにします。それ以外の場合は、現在のPINを入力します。工場出荷時のデフォルトPINは123456です。新しいPINを2回入力し、[Change PIN]を選択します。



PUKを設定します。PUCと呼ばれることもあります。これは、紛失または忘れたPINをリセットするために使用します。6～8文字のPUKを選択します。YubiKeyを初めて設定する場合は、[デフォルトを使用]オプションをオンにします。それ以外の場合は、現在のPUK値を入力します。工場出荷時のデフォルトPUKは12345678です。新しいPUKを2回入力し、[Change PUK]を選択します。

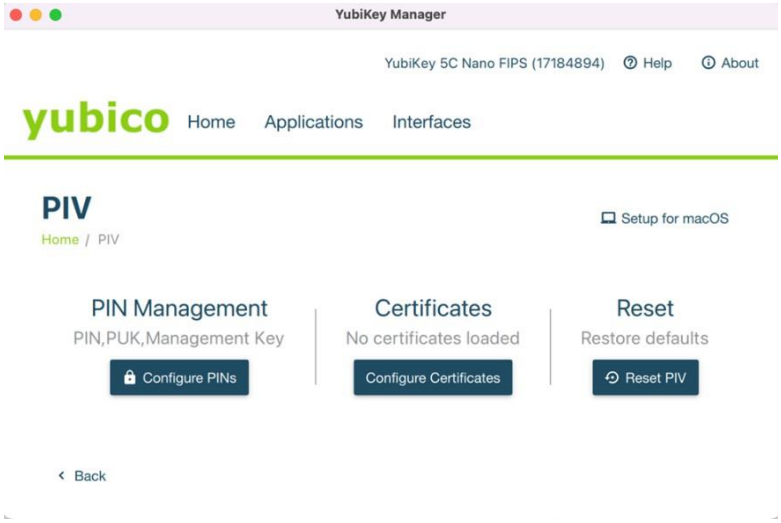


注: 管理キーも変更することをお勧めします。デフォルトの3DES管理キーは010203040505060708010203040506070801020304050607080です。PIN、PUK、および管理キーの詳細については、YubicoのWebサイトを参照してください。

秘密鍵と証明書をインポートまたは生成する

SSH上のPIV認証にYubiKeyを使用するには、プライベートECDSAキーと証明書をインポートまたは生成する必要があります。ONTAP 9.12.1以降では、SSH公開鍵認証にECDSA-256またはECDSA-384キーが使用されます。次の例では、ECDSA-384を使用しています。証明書はONTAP SSHサーバでは使用されず、証明書の公開鍵のみが使用されます。

1) YubiKeyのスロット9aは、PIVキーの保存に使用されます。[証明書の設定]を選択します。

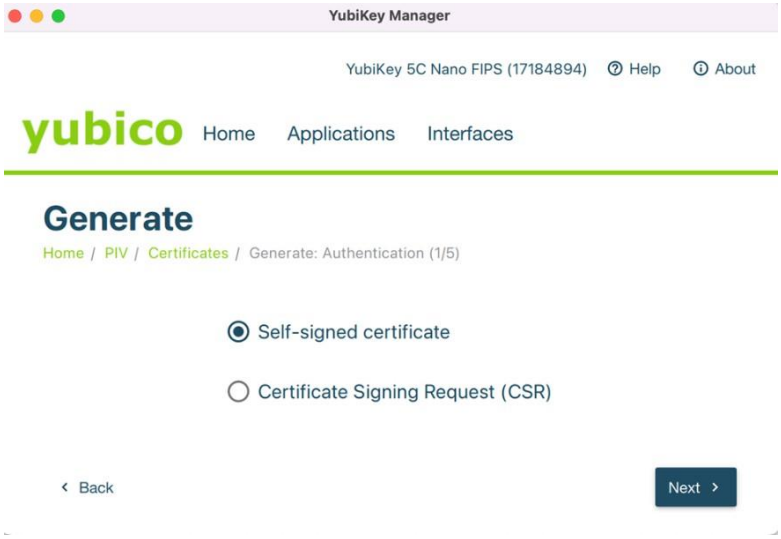


a) [Generate]を選択して続行します。この例では、ECDSAの秘密鍵と公開鍵のペアがP-384曲線を使用して生成されます。

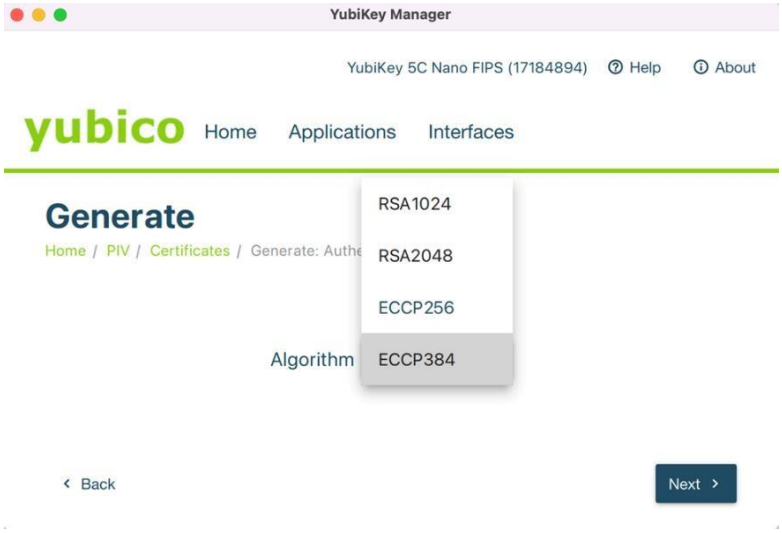
2) [自己署名証明書]を選択します。この例では、自己署名証明書が生成されます。これは、証明書がONTAPでは使用されず、PKCS#11インターフェイスでのみ必要とされるためです。

注： 導入環境によっては、CSRを事前に生成し、信頼されたCAによる署名を受けてから、署名済み証明書をインポートする必要があります。

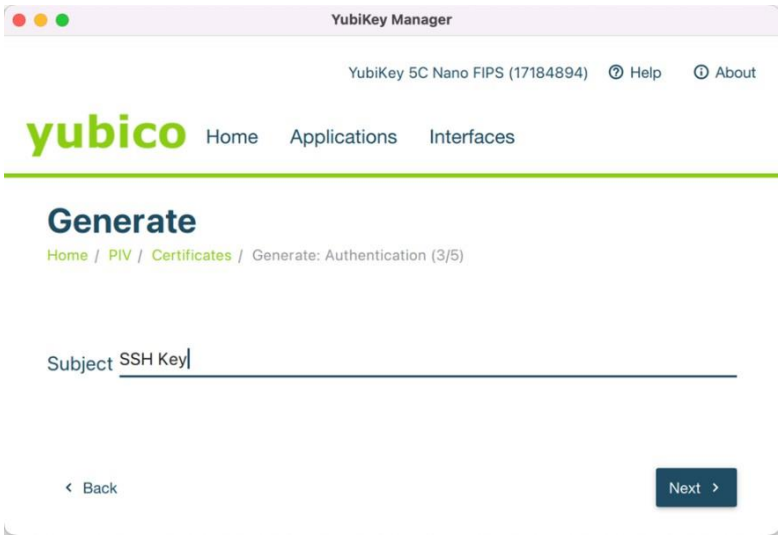
[Self-Signed Certificate]を選択したら、[Next]を選択します。



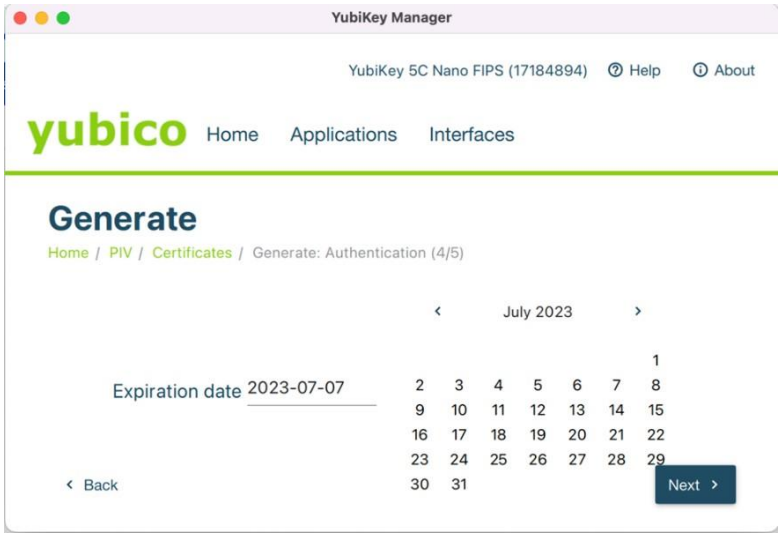
アルゴリズムにECCP-384を選択し、[次へ（Next）]を選択します。



件名（CN）の文字列を入力します。次に、SSHキーに設定する例を示します。



[Next]を選択します。次の画面では、証明書の有効期限を確認するメッセージが表示されます。デフォルトでは1年に設定されています。これはSSHには適用されないため、デフォルトをそのまま使用できます。



最後のダイアログボックスに、選択した選択肢が表示されます。[Generate]を選択して、選択内容を確認します。

続行するには、管理キーを入力するように求められます。管理キーが変更されている場合は入力し、工場出荷時のデフォルト設定に設定されている場合は[Use Default]を選択します。

PINの入力を求められます。初期化手順で設定したPINを入力し、[OK]を選択します。

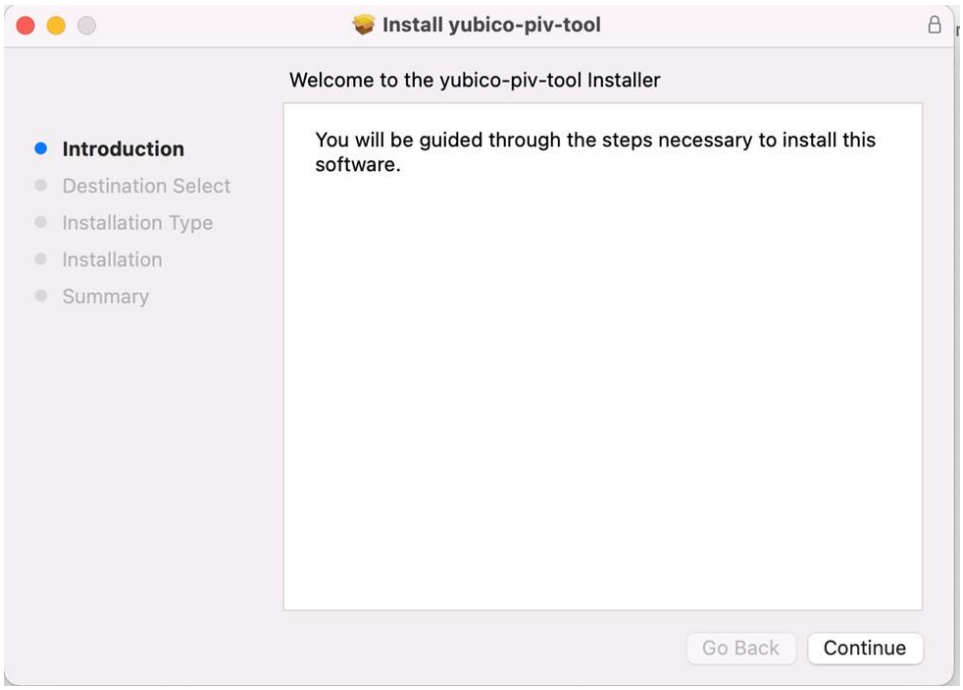
秘密鍵と証明書が生成され、関連する情報が[証明書]セクションに表示されます。

Mac OSまたはLinux SSHクライアントでYubiKey PIV認証を設定する

Yubico PIVツールの取り付け

Yubico PIVツールは、Yubico Smart Card Drivers and Toolsページからダウンロードできます。

1)パッケージファイルをクリックしてインストールします。デフォルトのオプションをすべて受け入れてインストールを完了します。



インストールが完了すると、SSHクライアントに必要なYubico PKCS#11ライブラリが次の場所にあります。`/usr/local/lib/libykcs11.dylib`

ECDSAキーのエクスポート

YubiKey for SSHで生成したRSAまたはECDSAキーを使用するには、SSHで認識される形式に変換する必要があります。

1)これを行うには、`ssh-keygen` Yubico PKCS #11モジュールで使用します `libykcs11.dylib`。

注意: Unixインストールの場合、このライブラリには `.so` 拡張子が付いています。

これを行うには、`ssh-keygen` Yubico PKCS#11ライブラリと `-e` オプションを使用して、ECDSAキーをSSH互換形式にエクスポートします。

出力例：

```
user@user-mac-0 ~ % ssh-keygen -D /usr/local/lib/libykcs11.dylib -e
   ecdsa-sha2-nistp384
AAAAE2VjZHNhLXNoYTItbmlzdHAzODQAAAAIbmlzdHAzODQAAABhBFfz/rELb+Qf51ViOnZQedHZEdG3/ePRz3oo7U0Oa7F+V
xX5jfc
r8sWyuGGNkXNY5GHsFZJw52iykLKjMjmpQCiEoFtUCdbg8Shrvx3YBxEg8B0JXKzAv3+OpvZNL/pjvg==
Public key for PIV Authentication
    ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDgCafjv1ujwNHNPTS42dRpATqWX//mPjh2bTghU88QhQObaCoJ6LCdHtud9Xf5j+yEL
oOs0tb
4BO/Z0s7zjt1G6OZOQVtWUpE4j3hLyJytvzt7WWE+df4i8Jqj0TV9nDrZtZoUtfW3WtVlJXGZu4vmFf1NOLVHrS8/8SAelYkt
9ZhLAG
D61dHpTIYt/oFz5588QDudiQ0HGYWDDt0yoafY3N64BfAnaSitlrQD4py0Y14Zv/7Kgzq1Eb6jGcjuxluvs6wOd6qpt8qNf32
hpqL3Y
meAUFQQuLdqQ6BHCZ2I8pc8W+NrDoRvDuvgOTvsGyB7TqsTyK2tHljdygHQXHvl
Public key for PIV Attestation
```

`ecdsa-sha2-nistp384` 次の概要でタグ付けされたエントリを選択します `Public key for PIV Authentication`。次の手順で、この公開鍵を使用してONTAPユーザを設定する必要があります。

Yubico PKCS#11ライブラリを使用するようにSSHクライアントを設定する

また、Yubico PKCS#11ライブラリを使用するようにSSHクライアントを設定する必要があります。

LinuxおよびMACの場合、これには、 `~/.ssh/config` 指定されたユーザおよびホストのファイルにPKCS11Providerオプションを指定して新しいエントリを作成する必要があります。

次の例では、`newadmin` ONTAPホストのユーザに対してカスタム設定エントリが作成され `vsim1.sim.netapp.com`、SSH newadmin@vsim1.sim.netapp.comを呼び出すと、`/usr/local/lib/libykcs11.dylib` PKCS11Providerオプションで設定されたPKCS#11ライブラリが使用されます。

```
% pwd
 /Users/user/.ssh
% cat config
Host vsim1.sim.netapp.com
HostName vsim1.sim.netapp.com
PKCS11Provider /usr/local/lib/libykcs11.dylib
Port 22
User newadmin
```

次の手順では、ONTAPユーザアカウントに公開鍵認証メカニズムを設定します。ONTAPアカウントを設定して公開鍵に関連付けたら、PuttyなどのSSHクライアントを使用してONTAPシステムを管理できます。

次の手順については、「ONTAPでYubiKey PIVの公開鍵認証を構成する」を参照してください。

ONTAPでのYubiKey PIVの公開鍵認証の設定

この例では、ユーザ名がの新しいadminユーザが `newadmin` SSHを使用して作成され、認証方式がに設定され `publickey`ます。認証方式が標準のSSH公開鍵認証であるかYubiKey PIV認証であるかに関係なく、使用されるコマンドは同じです。

```
smrcluster-1::> security login create -user-or-group-name newadmin -application ssh -
authentication-method publickey -role admin
Warning: To use public-key authentication, you must create a public key for user "newadmin".


Warning: For successful authentication, ensure you create a public key for user "newadmin" using
"security login publickey create" interface.
```

`newadmin publickey` 認証方式としてを追加する場合は、の公開鍵を入力する必要があることを示す警告メッセージが表示されます。この公開鍵は、クライアントでYubiKeyデバイスを設定するときに取得されます。

次に、YubiKey用に設定したPIV公開鍵を設定します。公開鍵は、PuTTY-CAC for PIVの[Copy to Clipboard]機能またはWindowsから取得するか、 `ssh-keygen -e` for PIV for MacOSを使用してSSH互換形式で公開鍵をエクスポートして取得します。

出力例：

```
smrcluster-1::> security login publickey create \
-username newadmin \
-publickey "ecdsa-sha2-nistp384
AAAAE2VjZHNhLXNoYTItbmlzdHAzODQAAAAIbmlzdHAzODQAAABhBFfz/rELb+Qf51ViOnZQedHZEdG3/ePRz3oo7U0Oa7F+V
xX5jfcr8sWyuGGNkXNY5GHsFZJw52iykLKjMjmpQCiEoFtUCdbg8Shrvx3YBxEg8B0JXK
zAv3+OpvZNL/pjvg==
Public key for PIV Authentication"
```

`newadmin` 多要素認証にYubiKeyおよびPIVを使用して、クライアントシステムからONTAP管理者としてログインできるようになりました。

SSH MFA認証の詳細については、『ONTAP 9セキュリティガイド』の「SSH多要素認証の有効化」を参照してください。

YubiKeyおよびFIDO2を使用したONTAP SSH MFA認証

既存の単一要素認証（1FA）管理者ユーザは、YubiKeyトークンデバイスとFIDO2認証を使用してMFAログイン方法をサポートするように変更できます。YubiKeyは、 `publickey` プライマリとして設定する `-authentication-method` か、`publickey - second-authentication-method`. IFが `-second-authentication-method` 指定されている場合に設定することで機能し `password`、`nsswitch` プライマリ認証方式として設定する必要があります。

注： ハードウェアベースのSSH MFAの場合、ONTAPに設定された公開鍵に加えて認証要素は次のとおりです。

- FIDO2ピン
- YubiKeyハードウェアデバイスの所有。FIDO2の場合、認証プロセス中にYubiKeyに物理的に触れることで確認されます。

Windows用のYubiKey FIDO2クライアントの設定

ここでは、FIDO2を使用してONTAPに接続するためのYubiKeyをサポートするようにSSHクライアントを設定するための一般的な手順について説明します。Windowsクライアントの手順の概要は次のとおりです。

1) YubiKey Managerをダウンロードしてインストールし

ます。FIDO2 PINを設定してYubiKeyを初期化します。

`ecdsa-sk edd519-sk` PuTTY-CAC（Windows）または `ssh- keygen`（MAC）を使用して、秘密鍵と公開鍵のペアを生成します。

`ecdsa-sk` または `edd519-sk` 公開鍵を必要に応じてSSH互換の形式に変換します。

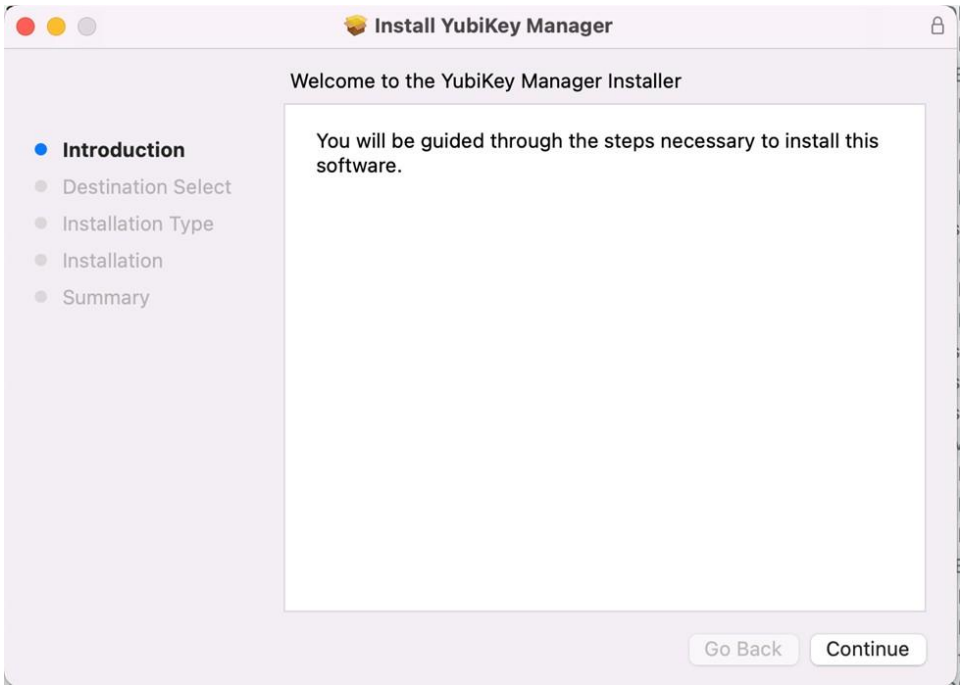
公開鍵認証方式を使用するようにONTAPユーザを設定します。

`ecdsa-sk` または `edd519-sk` 公開鍵をONTAPにエクスポートします。

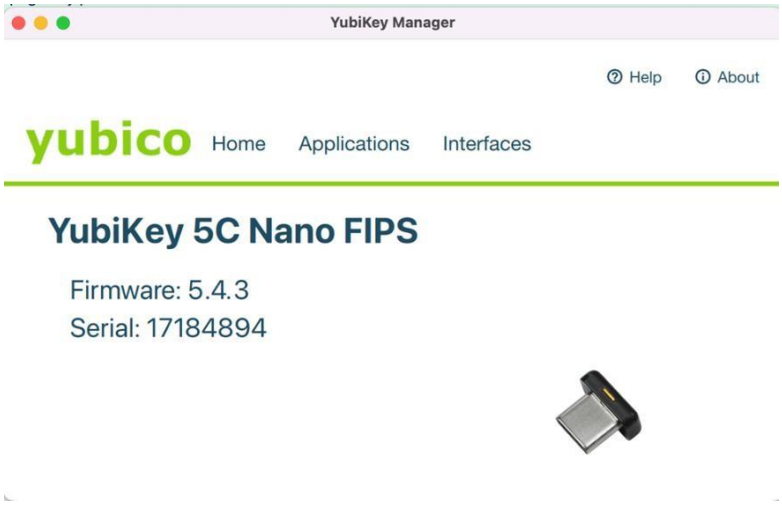
YubiKey Managerのダウンロードとインストール

使用しているプラットフォームに適したバージョンのYubiKey ManagerをYubicoのWebサイトからダウンロードしてインストールします。

1)「続ける」をクリックし、すべてのデフォルト値を受け入れます。例：

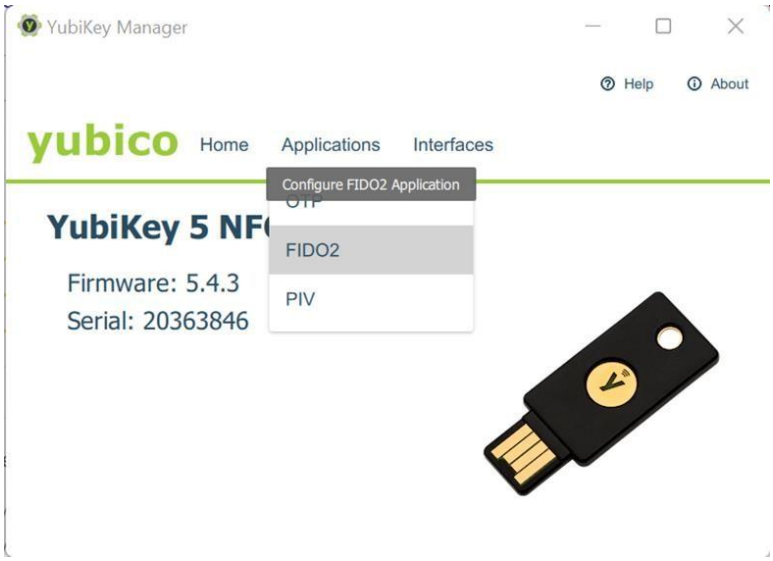


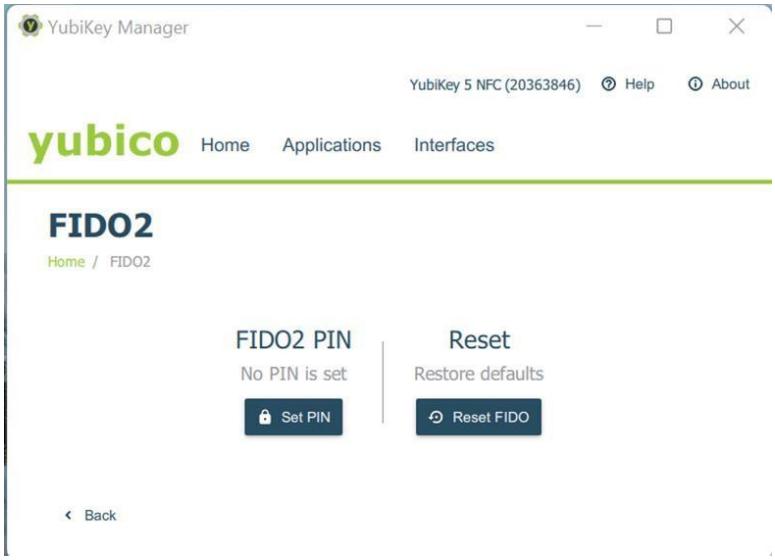
インストールが完了したら、USBスロットにYubiKeyを挿入し、YubiKey Managerを実行します。YubiKeyのモデル、シリアル番号、ファームウェアバージョンが画面に表示されます。



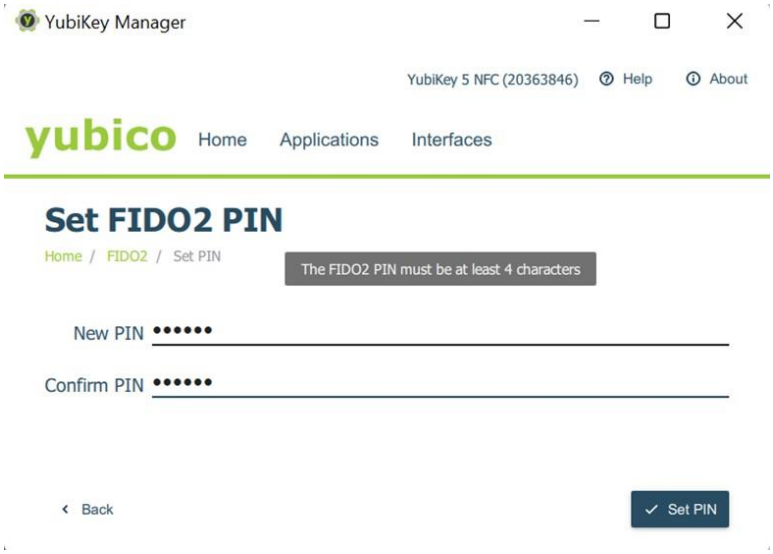
YubiKey PINの初期化

1)「アプリケーション」>「FIDO2」の順に選択して、FIDO2設定を構成します。例：

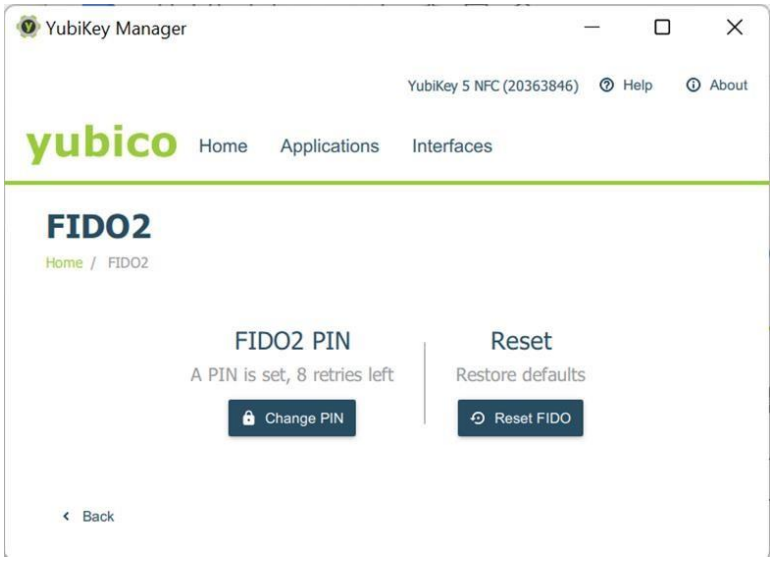




[Set FIDO2 PIN]ダイアログボックスが表示され、FIDO2 PINを設定するように求められます。[New PIN]フィールドに4文字以上のPINを入力します。次に、[Confirm PIN]フィールドに同じPINをもう一度入力します。[Set PIN]を選択して、FIDO2 PINを設定します。



PINが設定されたことを確認するFIDO2ダイアログボックスに戻ります。



YubiKey FIDO2設定の詳細については、YubicoのWebサイトを参照してください。

YubiKey FIDO2認証用のWindows PuTTY-CAC SSHクライアントの設定

SSH上でのFIDO2認証にYubiKeyを使用するには、パブリックとプライベートのECDSAキーペアを生成する必要があります。FIDOデバイスは `ecdsa-sk`、公開鍵タイプと、`ed25519-sk`対応する証明書タイプでサポートされています。

- は `ed25519-sk` `ecdsa-sk` 数学的にはより強力ですが、まだ広くサポートされていません。
- は、`ed25519-sk` ファームウェアバージョン5.2.3以降のYubiKeyでのみサポートされています。
- `ecdsa-sk` キータイプは、互換性のためにサポートされているECDSAを使用します。

ONTAP 9.12.1以降では、SSH公開鍵認証にECDSA-256またはECDSA-384キーを使用します。

YubiKey PIVで公開鍵認証を使用してSSH経由でONTAPに接続する簡単な方法は、 PuTTY-CACを使用することです。PuTTY-CACは、スマートカード認証をサポートするオープンソースのSSHクライアントで、特に国防総省のCACとPIVをPKIトークンとして使用します。これは、連邦政府の導入で広く使用されています。

GitHubから https://github.com/NoMoreFood/putty-cac/releasesからダウンロードできます。

1) PuTY-CACのインストール

WindowsクライアントでPutty-CACを起動します。

> **注:** YubiKeyハードウェアトークンでキーを作成するには、PuTTY-CACをAdministratorとして実行する必要があります。

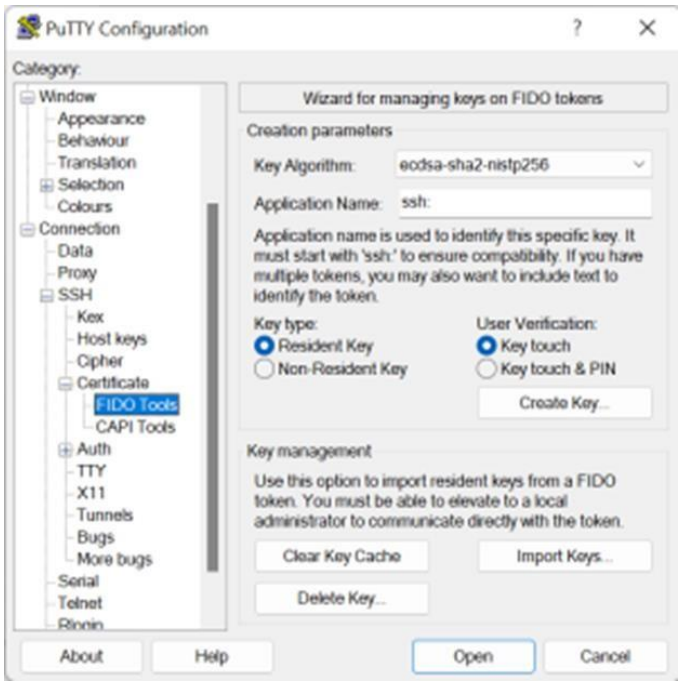
[PuTTY Configuration]ダイアログボックスで、[Connection SSH]>[Certificate]>[FIDO Tools]の順に選択します。[Application Name]と[User Verification]を除くすべてのデフォルト値を受け入れます。

`ecdsa-sha2-nistp256` キーアルゴリズムを使用して、FIDO2の秘密鍵と公開鍵のペアを作成します。

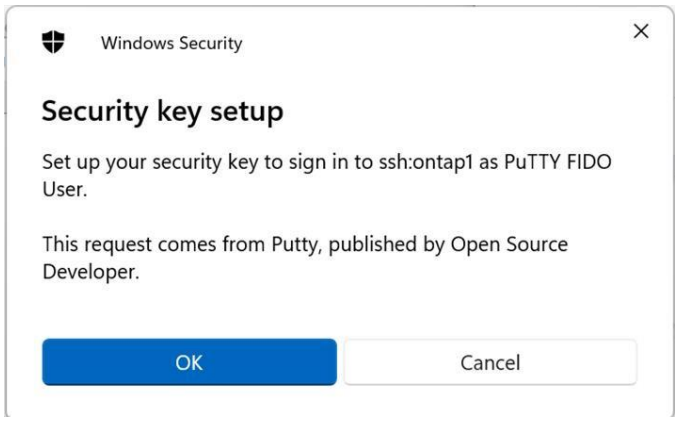
[Application Name]フィールドにssh:の後に文字列を入力して、アプリケーションを識別します。この例ではを使用し `ontap1`ます。

キータイプとして「Resident key」と入力し、YubiKeyデバイスに保存します。

[User Verification]を[Key Touch]から[Key Touch]および[PIN]に変更します。これにより、ユーザはYubiKeyに触れるだけでなくPINを入力する必要があります。

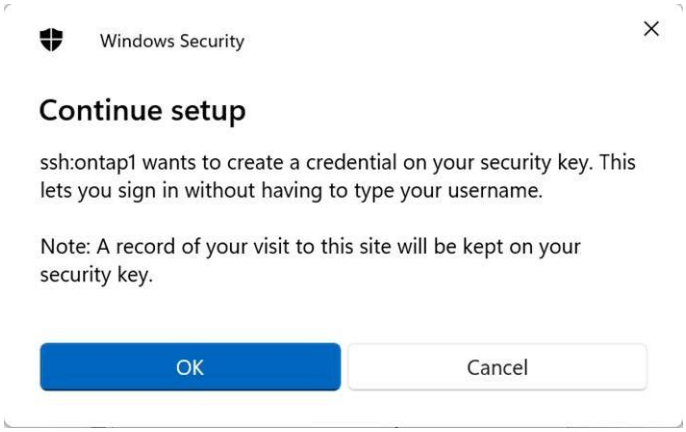


[Create Key]を選択します。[セキュリティキーのセットアップ]ダイアログボックスが表示されます。[OK]を選択します。

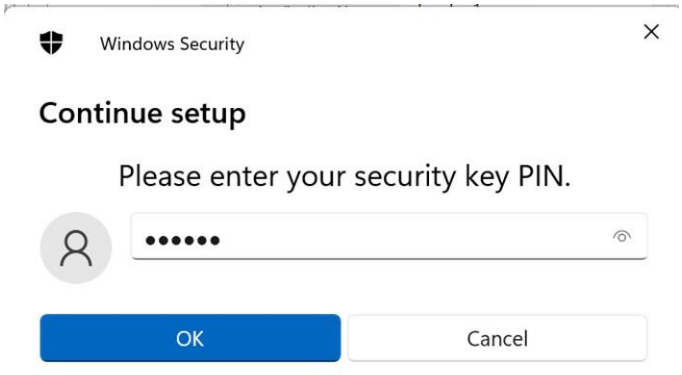


[Continue Setup Confirmation]ダイアログボックスでは、YubiKeyデバイスでクレデンシャルを作成するかどうかの確認を求められます。[OK]を選択します。

Yubico PIVツールの取り付け



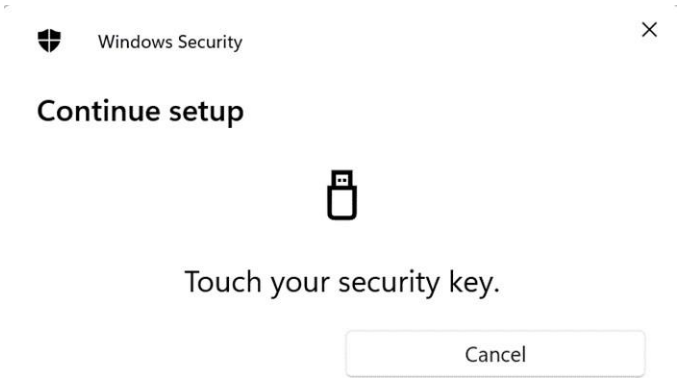
1)設定したFIDO2 PINを入力して、セットアップを続行します。[OK]を選択します。



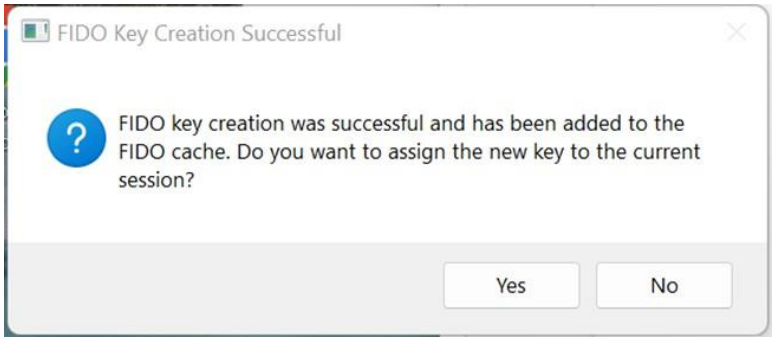
YubiKeyに触れるように求めるダイアログボックスが表示されます。この手順が失敗した場合は、PuTTY-CACがAdministratorではなく通常のユーザアカウントとして実行されている可能性があります。

YubiKeyデバイスが点滅し始めます。

[YubiKey]をタッチします。



キーの作成が成功すると、FIDOキーの作成が成功し、キーがFIDOキャッシュに追加されたことを示すダイアログボックスが表示されます。SSHセッションでキーを使用するには、新しいキーを現在のセッションに割り当てます。[Yes]を選択して続行します。



これで、PuTTY-CACの残りの設定を続行できます。このセッションでONTAPへのSSH接続を設定する場合は、次のセクション「YubiKeyからPuTTY-CACへのFIDO2キーのインポート」をスキップして、「PuTTY-CAC クライアントSSHセッションの設定」に進みます。

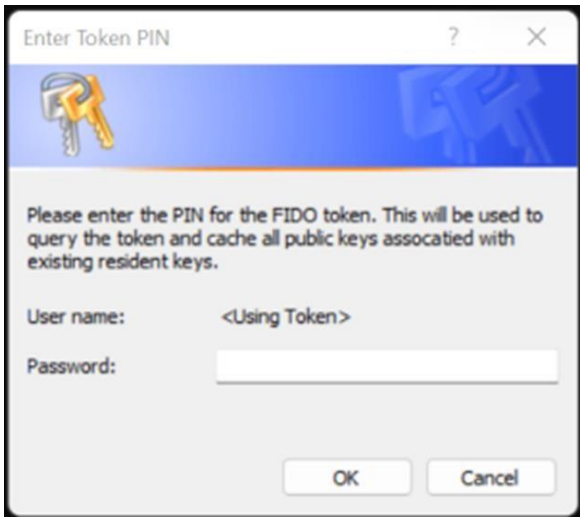
YubiKeyからPuTTY-CACへのFIDO2キーのインポート

YubiKeyでFIDO2キーを作成した直後にセッション設定を続行する準備ができていない場合は、PuTTY-CACキー管理インポート機能を使用して、以降のセッションでFIDO2キーをYubiKeyからPuTTY-CACにインポートできます。

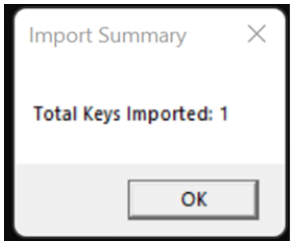
1) PuTTYのメイン設定ダイアログボックスで、[Connection]>[Certificate]>[FIDO Tools]の順に選択し、[Key Management]セクションから[Import Keys]を選択します。

   これにより、PuTTY-CACからputtyimpアプリケーションが起動します。

続行するには、FIDO2 PINの入力を求められます。[Password]フィールドにFIDO2 PINを入力します。



キーのインポートが正常に機能すると、確認メッセージが表示されます。例：



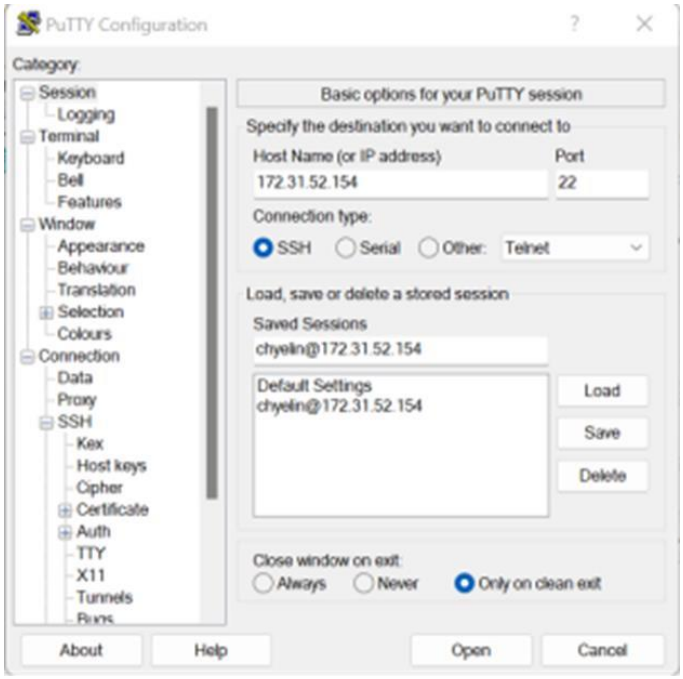
キーをインポートしたら、次のセクション「PuTTY-CACクライアントSSHセッションの設定」に進みます。

PuTTY-CACクライアントSSHセッションの設定

次の手順では、クライアントSSHセッションを設定します。

これは、通常のPuTTYセッションと同じ方法で行います。セッション構成を開始する前に、同じセッションで前述のようにFIDO2の秘密鍵と公開鍵のペアを生成したこと、または「YubiKeyからPuTTY-CACへのFIDO2キーのインポート」の説明に従ってFIDO2をインポートしたことを確認してください。

1)「セッション」タブを選択します。ONTAPサーバのホスト名またはIPアドレスを入力します。[Saved Sessions]ダイアログボックスに名前を入力し、[Save]を選択して設定を保存します。



これで、FIDO2公開鍵をエクスポートして、ONTAP CLIユーザの公開鍵認証を設定できるようになります。

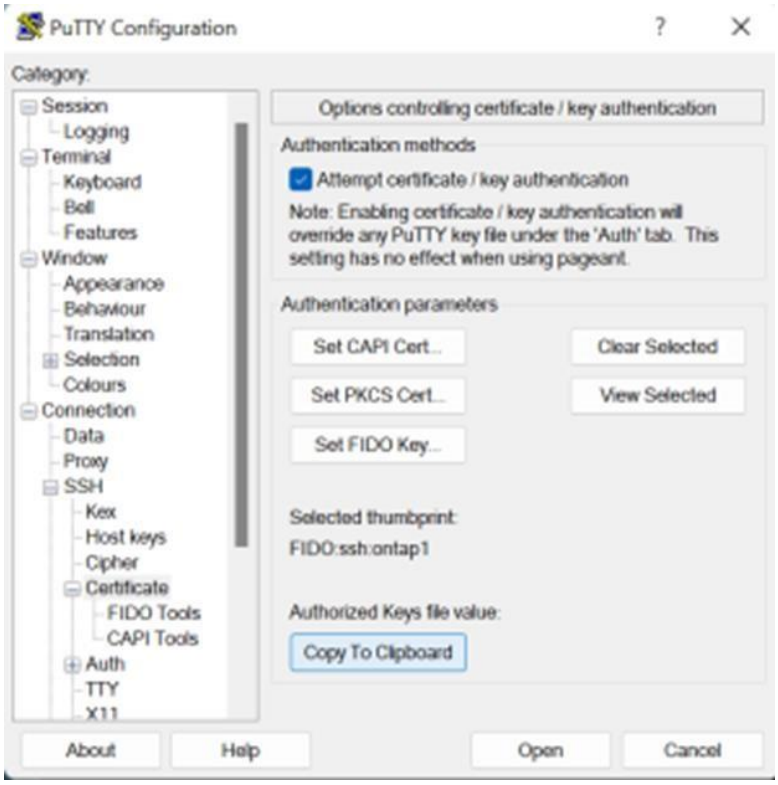
FIDO2公開鍵のエクスポート

ユーザに対してONTAPでFIDO2公開鍵認証を設定するには、公開FIDO2キーが必要です。

1)メインのPuTTY Configurationダイアログボックスに移動し、Certificateオプションを選択します。

[Selected Thumbprint]セクションの文字列が、前の例で設定したアプリケーション名と一致していることを確認します `FIDO:ssh:ontap1`。

メモ： 一致しない場合は、[Set FIDO Key]をクリックして、YubiKeyからFIDO2キーを取得します。次に、[Authorized Keys File Value]で[Copy to Clipboard]を選択します。



次に、FIDO2公開鍵の例を示します。

```
sk-ecdsa-sha2-nistp256@openssh.com
AAAAInNrLWVjZHNhLXNoYTItbmlzdHAyNTZAb3BlbnNzaC5jb20AAAAIbmlzdHAyNTYAAABBBIFMIkbfXsC7J5oiJ6hZmNoG7
CyFTz1
IWKZEt67tRa6yDocKNLu+k0JcnRy1aWfkyvBQqdDPuKO3Lyjl9ITOb0oAAAAKc3NoOm9udGFwMQ== FIDO:ssh:ontap1
ssh:ontap1
```

最後のセクションを確認し、公開キーコメントのアプリケーション名が設定したアプリケーション名と一致することを確認して、これが正しいキーであることを確認します。前の例では、 `ontap1` がアプリケーションであるため、公開鍵アプリケーション名はです `ssh:ontap1`。

ONTAPユーザアカウントの公開鍵認証メカニズムを設定します。ONTAPアカウントを設定して公開鍵に関連付けたら、PuttyなどのSSHクライアントを使用してONTAPシステムを管理できます。

次の手順については、「ONTAPでYubiKey FIDO2の公開鍵認証を設定する」を参照してください。

Mac OSおよびLinux用のYubiKey FIDO2クライアント設定

ここでは、FIDO2を使用してONTAPに接続するためのYubiKeyをサポートするようにSSHクライアントを設定するための一般的な手順について説明します。Mac OSおよびLinuxクライアントの手順の概要は次のとおりです。

1) YubiKey Managerをダウンロードしてインストールします。

FIDO2 PINを設定してYubiKeyを初期化します。

`ecdsa-sk edd519-sk` PuTTY-CAC（Windows）または `ssh- keygen`（Mac）を使用して、秘密鍵と公開鍵のペアを生成します。

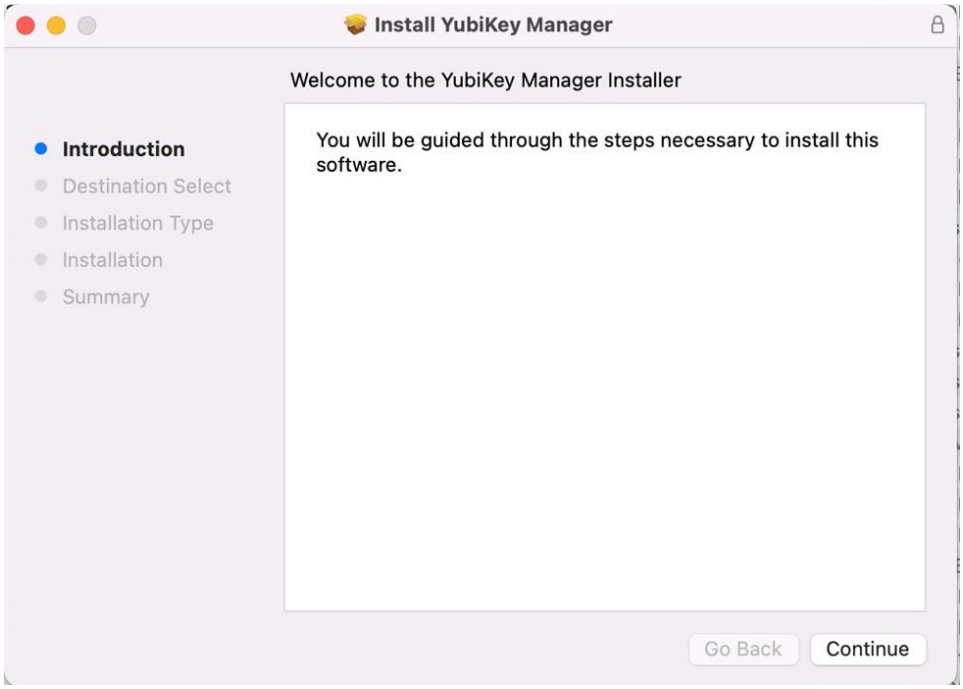
`ecdsa-sk` または `edd519-sk` 公開鍵を必要に応じてSSH互換の形式に変換します。

`publickey` 認証方式を使用するようにONTAPユーザを設定します。

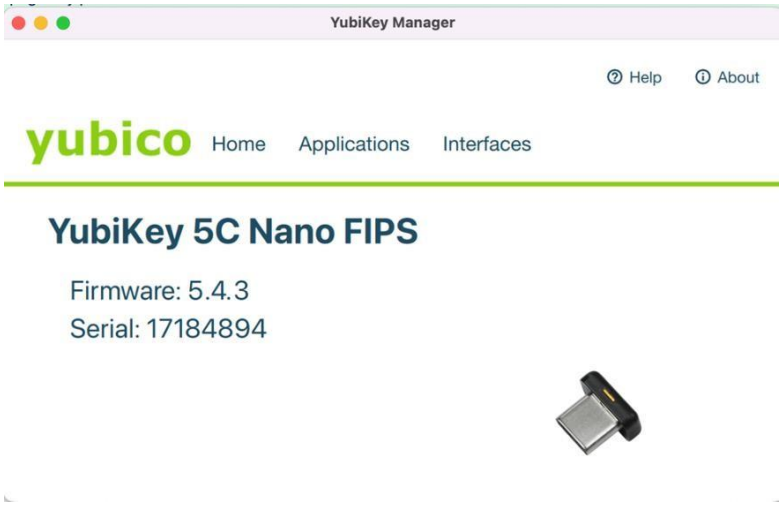
`ecdsa-sk` または `edd519-sk` 公開鍵をONTAPクライアントにエクスポートします。

YubiKey Managerのダウンロードとインストール

1)YubicoのWebサイトから、お使いのプラットフォームに適したバージョンのYubiKey Managerをダウンロードしてインストールします。[Continue]をクリックし、デフォルト値をすべて受け入れます。例：

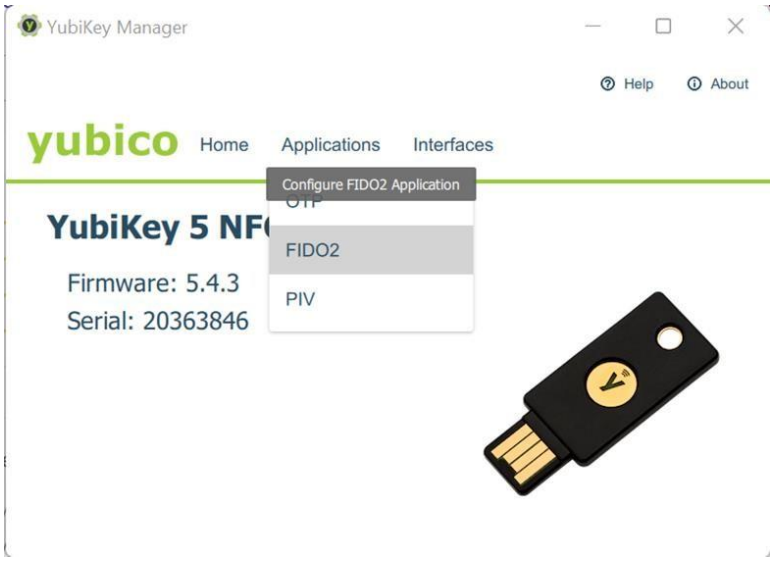


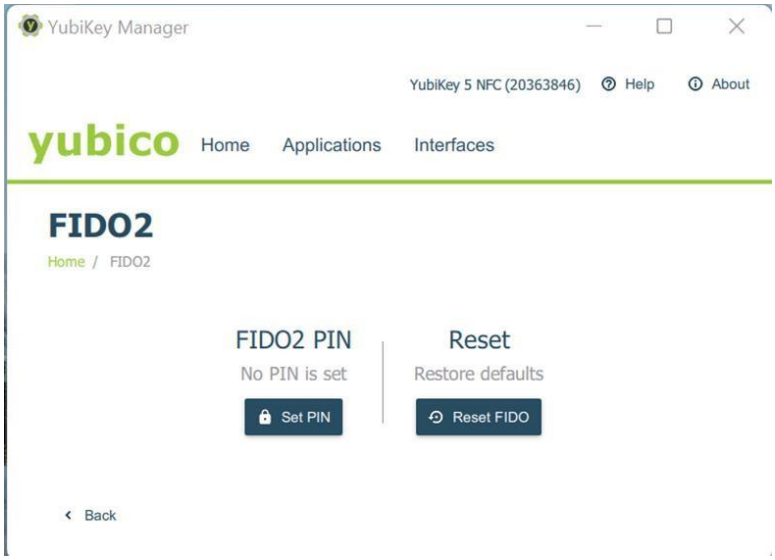
インストールが完了したら、USBスロットにYubiKeyを挿入し、YubiKey Managerを実行します。YubiKeyのモデル、シリアル番号、ファームウェアバージョンが画面に表示されます。



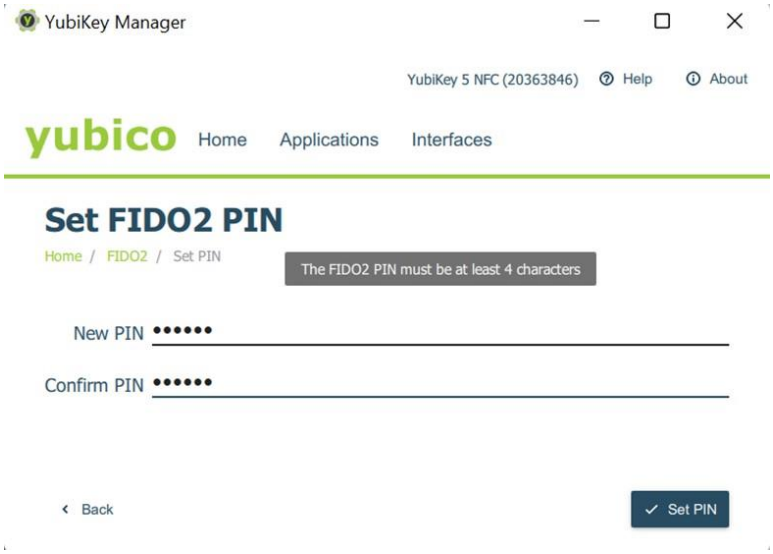
YubiKey PINの初期化

1)「アプリケーション」>「FIDO2」の順に選択して、FIDO2設定を構成します。例：

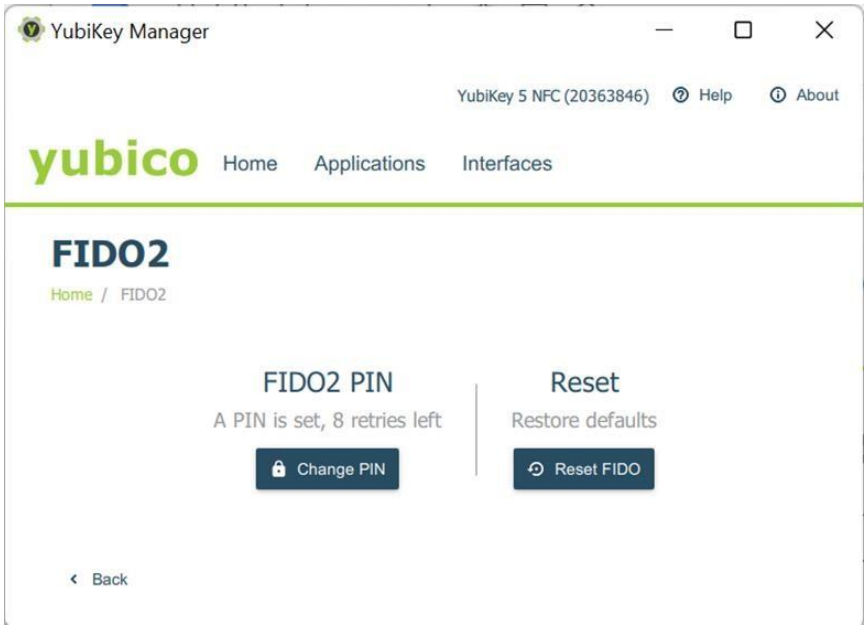




[Set FIDO2 PIN]ダイアログボックスが表示され、FIDO2 PINを設定するように求められます。[New PIN]フィールドに4文字以上のPINを入力します。次に、[Confirm PIN]フィールドに同じPINをもう一度入力します。[Set PIN]を選択して、FIDO2 PINを設定します。



PINが設定されたことを確認するFIDO2ダイアログボックスに戻ります。



YubiKey FIDO2設定の詳細については、YubicoのWebサイトを参照してください。

YubiKey FIDO2認証用のMAC OSまたはLinux SSHクライアントの設定

SSH上でのFIDO2認証にYubiKeyを使用するには、パブリックとプライベートのECDSAキーペアを生成する必要があります。FIDOデバイスは `ecdsa-sk` 、公開鍵タイプと、`ed25519-sk`対応する証明書タイプでサポートされています。

- は `ed25519-sk` `ecdsa-sk` 数学的にはより強力ですが、まだ広くサポートされていません。
- は、 `ed25519-sk` ファームウェアバージョン5.2.3以降のYubiKeyでのみサポートされています。
- `ecdsa-sk` キータイプは、互換性のためにサポートされているECDSAを使用します。

ONTAP 9.12.1以降では `ECDSA-256`、`ECDSA-384` SSH公開鍵認証にORキーが使用されます。

オープンソースOpenSSHの要件

MacOSに付属するOpenSSHのビルトインバージョンは `ecdsa-sk`、`ed25519-sk` FIDO2操作に必要なキータイプとキータイプをサポートしていません。Homebrewを使用してOpenSSHのオープンソースバージョンをインストールする必要があります。例：

```
user@user-mac-0 ~ % brew install openssh
```

OpenSSHのバージョンが8.2以降であることを確認します。デフォルトでは、HomebrewはOpenSSHをにインストールします `/usr/local/opt/openssh`。正しいOpenSSHパッケージを使用していることを確認します。

```
user@user-mac-0 ~ % ssh -V
OpenSSH_9.0p1, OpenSSL 1.1.1p 21 Jun 2022
user@user-mac-0 ~ % which ssh-keygen
/usr/local/opt/openssh/bin/ssh-keygen
user@user-mac-0 ~ % which ssh
/usr/local/opt/openssh/bin/ssh
```

クライアント側のSSH FIDO2キーの生成

次の手順では、FIDO2の秘密鍵と公開鍵のペアを生成します。この例では、`ecdsa-sk` キータイプを使用しています。サポートされているキータイプは `ecdsa-sk`、および `edd25519-sk`です。PINの確認を有効にするには `-O verify-required ssh-keygen`、コマンドに追加のオプションがあります。このオプションを使用しない場合、SSHサーバはユーザにYubiKeyへのタッチを要求するだけで、侵入者がYubiKeyを盗んでONTAPにログインできる可能性があります。

注： この `ssh-keygen` コマンドでは、FIDO2 PIN（認証用のPINを入力）の入力を求められます。また、YubiKeyにタッチしてキーの生成を承認します。

```
user@user-mac-0.ssh % ssh-keygen -t ecdsa-sk -C "$(hostname)-$(date) +'%d-%m-%Y')-yubikey1" -O
verify-required
Generating public/private ecdsa-sk key pair.
You may need to touch your authenticator to authorize key generation.
Enter PIN for authenticator: ******
Enter file in which to save the key (/Users/chyelin/.ssh/id_ecdsa_sk):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/chyelin/.ssh/id_ecdsa_sk
Your public key has been saved in /Users/chyelin/.ssh/id_ecdsa_sk.pub
The key fingerprint is:
SHA256:MO2FeFS3fZY8EB1ypaXX0WEb2Eu1eWsqmUHGySFU93Y chyelin-mac-0-Tue Aug 16 19:40:27 +08 2022
+'%d-%m-%Y')-yubikey1
The key's randomart image is:
+-[ECDSA-SK 256]--+
|         o+oo.==BX|
|        + .+.++BBX|
|       + + .*. =XE|
|        = .o   .==|
|         S .    o |
|              + o |
|           + .    |
|             .    |
|                  |
+----[SHA256]-----+
```

が `ssh-keygen` 正常に完了すると、`~/.ssh` ユーザのディレクトリに2つの新しいキーが表示されます。

`id_ecdsa_sk` ファイルにはFIDO2秘密鍵が含まれています。

には、`id_ecdsa_sk.pub` FIDO2公開鍵が含まれています。これは、ONTAPでユーザの公開鍵認証を設定するために必要なキーです。

例：

```
user@user-mac-0..ssh % pwd
/Users/user/.ssh
user@user-mac-0. .ssh % ls *ecdsa*
id_ecdsa_sk id_ecdsa_sk.pub
user@user-mac-0..ssh % cat id_ecdsa_sk.pub
sk-ecdsa-sha2-nistp256@openssh.com
AAAAInNrLWVjZHNhLXNoYTItbmlzdHAyNTZAb3BlbnNzaC5jb20AAAAIbmlzdHAyNTYAAABBBMW7wI9f5+lHR7Gi/msVe42LU
wIxonh
oWIL2oWzFcjYgKs8UbY60dFD/pjH2RwVkQaCYbvFElkWkIqouuzEhddMAAAAEc3NoOg==
chyelin-mac-0-Tue Aug 16 19:40:27 +08 2022 +'%d-%m-%Y')-yubikey1
```

FIDO2用のSSHクライアントの設定

FIDO2キーペアが生成されたら、次の手順でSSH構成ファイルにエントリを追加し、SSHクライアント接続に使用するFIDO2秘密鍵の場所を指定します。これを行うには、次の情報を含むONTAPのエントリを追加します。

- **Host name**：ユーザがSSHで接続するONTAPのホスト名またはIPアドレス。この例では、次のようになります。`vsim1.sim.netapp.com.`
- **port**：SSHポート。この例では、これがデフォルト値の22です。
- **user**：ユーザ名。これは、ONTAPで設定されているユーザの名前と一致する必要があります。この例では、です `newadmin`。
- **IdentityFile**： FIDO2秘密鍵の場所。この例では、です `~/.ssh/id_ecdsa_sk`。例：

```
user@user-mac-0 .ssh % pwd
/Users/user/.ssh
user@user-mac-0 .ssh % cat config
...
Host vsim1.sim.netapp.com
   HostName vsim1.sim.netapp.com
   Port 22
   User newadmin
   IdentityFile ~/.ssh/id_ecdsa_sk
```

次の手順では、ONTAPユーザアカウントに公開鍵認証メカニズムを設定します。ONTAPアカウントを設定して公開鍵に関連付けたら、PuttyなどのSSHクライアントを使用してONTAPシステムを管理できます。

次の手順については、 「ONTAPでYubiKey FIDO2の公開鍵認証を構成する」セクションを参照してください。

ONTAPでYubiKey FIDO2の公開鍵認証を設定する

この例では、 `newadmin` SSHを使用するユーザ名を持つ新しいadminユーザが作成され、認証方式が公開鍵に設定されます。認証方式が標準のSSH公開鍵認証であるかYubiKey FIDO2認証であるかに関係なく、使用されるコマンドは同じです。

```
smrcluster-1::> security login create -user-or-group-name newadmin -application ssh -
authentication-method publickey -role admin
Warning: To use public-key authentication, you must create a public key for user "newadmin".


Warning: For successful authentication, ensure you create a public key for user "newadmin" using
"security login publickey create" interface.
```

`newadmin publickey` 認証方式としてを追加する場合は、の公開鍵を入力する必要があることを示す警告メッセージが表示されます。この公開鍵は、クライアントでYubiKeyデバイスを設定するときに取得されます。

次に、YubiKey用に設定したFIDO2公開鍵を設定します。公開鍵は、WindowsからPuTTY-CAC for PIVの[クリップボードにコピー]機能、または `ssh-keygen -e` for PIV for MacOSを使用してSSH互換形式で公開鍵をエクスポートして取得します。

注意： MacOSの場合、FIDO2公開鍵は `id_ecdsa_sk.pub`、`id_edd519_sk.pub`ECDSAとEDD519のどちらを使用しているかによって、またはにあります。

出力例（ `sk-key` タイプに注意）：

```
smrcluster-1::> security login publickey create \
-username newadmin \
-publickey "sk-ecdsa-sha2-nistp256@openssh.com
AAAAInNrLWVjZHNhLXNoYTItbmlzdHAyNTZAb3BlbnNzaC5jb20AAAAIbmlzdHAyNTYAAABBBIFMIkbfXsC7J5oiJ6hZmNoG7
CyFTz1
IWKZEt67tRa6yDocKNLu+k0JcnRy1aWfkyvBQqdDPuKO3Lyjl9ITOb0oAAAAKc3NoOm9udGFwMQ== FIDO:ssh:ontap1
ssh:ontap1"
```

これで、`newadmin` YubiKeyとFIDO2を使用して、クライアントシステムからONTAP管理者としてログインできるようになりました。

SSH MFA認証の詳細については、『ONTAP 9セキュリティガイド』の「SSH多要素認証の有効化」を参照してください。

System Manager

System Managerについて

ONTAP管理者がクラスタへのアクセスと管理にCLIではなくグラフィカルインターフェイスを使用する場合は、NetApp System Managerを使用してください。ONTAPにはWebサービスとして搭載されており、デフォルトで有効になっていて、ブラウザからアクセスできます。DNSを使用している場合は、ブラウザでホスト名を指定するか、https://cluster-management-LIF経由でIPv4またはIPv6アドレスを指定します。

自己署名のデジタル証明書がクラスタで使用されている場合、信頼されていない証明書であることを伝える警告がブラウザ画面に表示されることがあります。リスクを承認してアクセスを続行するか、認証局（CA）の署名があるデジタル証明書をクラスタにインストールしてサーバを認証します。

ONTAP 9.3以降では、SAML認証はSystem Managerのオプションです。

System ManagerでのSAML認証の有効化

SSH MFAの設定プロセスとは異なり、System Managerをアクティブ化すると、既存のすべての管理者がSAML IdPを使用して認証する必要があります。クラスタ ユーザ アカウントへの変更は必要ありません。SAML認証を有効にすると、 `saml http` および `ontapi` アプリケーションの管理者ロールを持つ既存のユーザに新しい認証方式が追加されます。

SAML認証を有効にしたあとに、SAML IdPアクセスを必要とする追加のアカウントをONTAPで定義する必要があります `saml http ontapi`。このアカウントには、およびアプリケーション用の管理者ロールと認証方式を指定する必要があります。ある時点でSAML認証が無効になった場合、これらの新しいアカウントでは `http`、および `ontapi` アプリケーションの管理者ロールにパスワード認証方式を定義し、`console` ローカルのONTAP認証に使用するアプリケーションをSystem Managerに追加する必要があります。

SAML IdPを有効にすると、IdPで使用可能な方式（LDAP、Active Directory（AD）、Kerberos、パスワードなど）を使用してSystem Managerへのアクセスの認証が実行されます。など。使用可能な方式はIdPごとに異なります。ONTAPで設定したアカウントのユーザIDがIdPの認証方式に対応していることが重要になります。

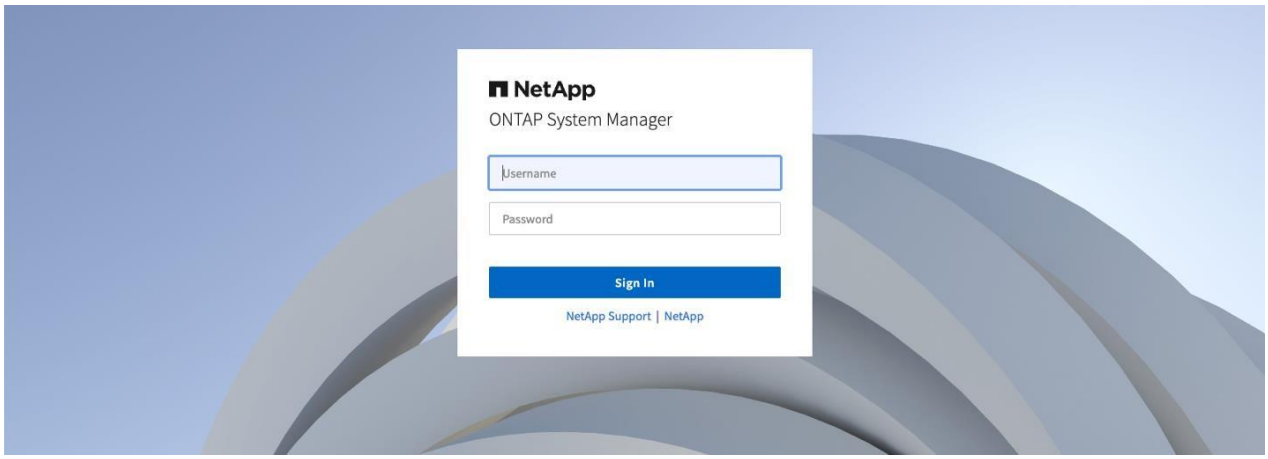
NetAppによって検証されたIdPは、ONTAP 9.3以降向けのMicrosoft ADFSとオープンソースのシボレスIdPです。ONTAP 9.12.1以降では、Cisco Duoもサポートされています。

開始する前に

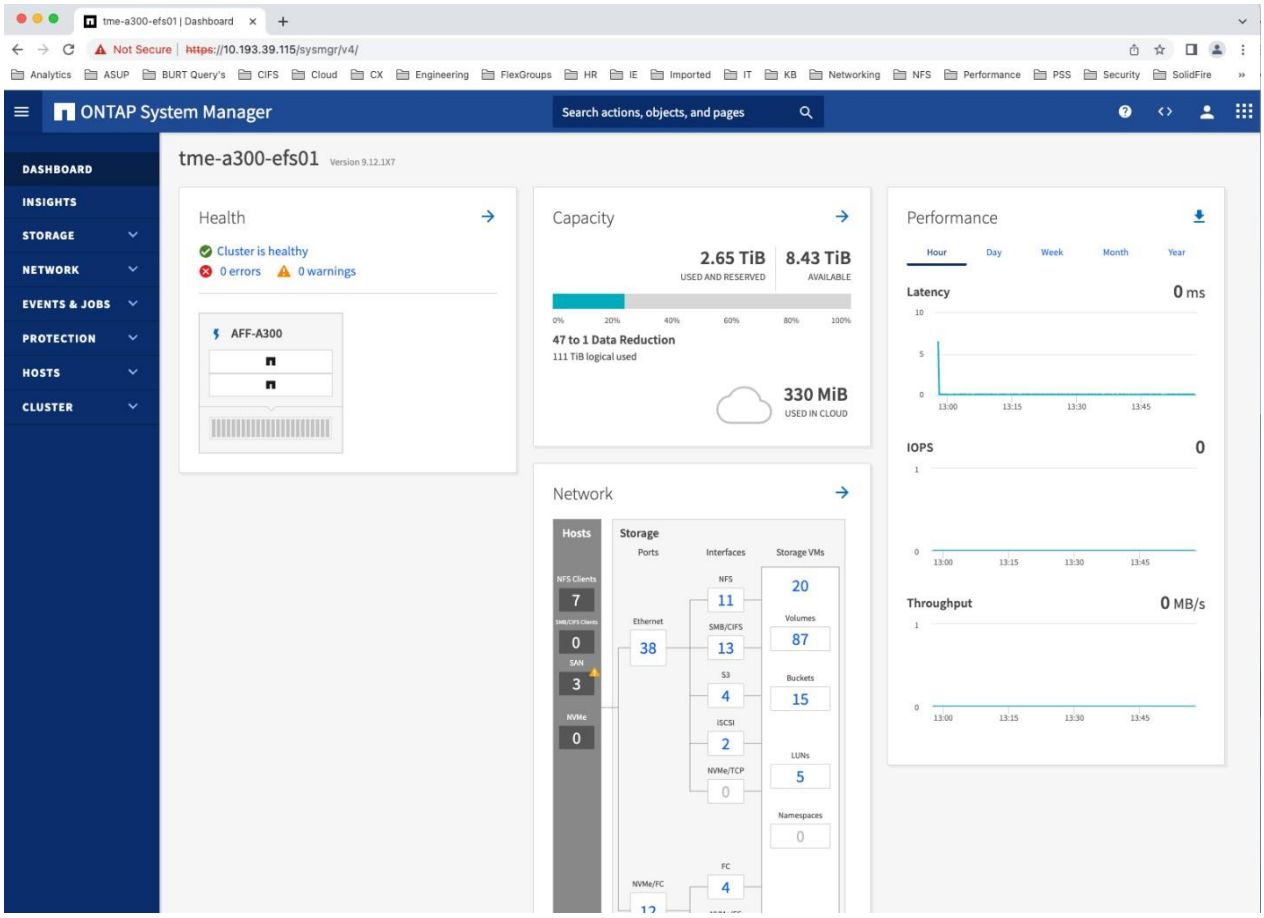
System ManagerでSAML認証を有効にしたあとにIdPの設定が正しくないと、System ManagerのWebインターフェイスにログインできないことがあります。IdPの修正中にSAML認証を無効にするには、ベースボード管理コントローラ（BMC）コンソールにアクセスする必要があります。詳細については、本ドキュメントの「トラブルシューティング」セクションで後述する「System ManagerでSAML認証を有効にしようとしたときにエラーが発生する」を参照してください。

System ManagerのSAML認証を有効にする

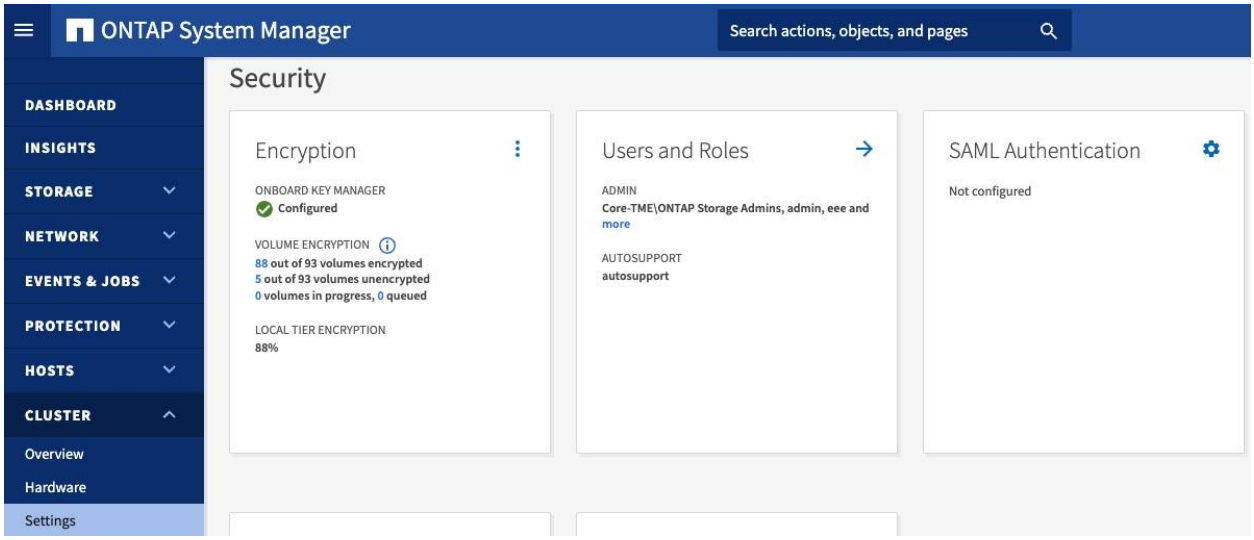
1) クラスタ管理インターフェイス（DNS名またはIPアドレス）を使用してSystem Managerを開きます。
https://cluster-mgmt-LIF



管理者のクレデンシャルで認証



[Cluster]>[Settings]を選択し、[Security]セクションに移動します。

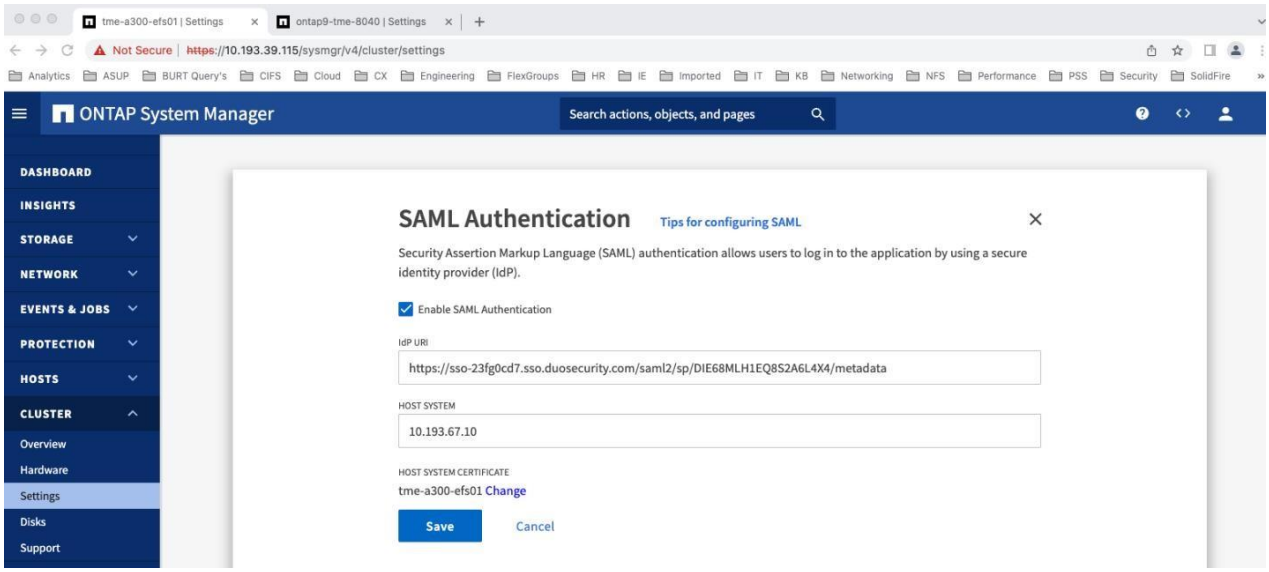


[SAML認証]オプションの横にある歯車アイコンを選択します。

IdP認証を使用するようにSystem Managerを設定します。

a. [SAML認証を有効にする]チェックボックスをオンにします。
b. IdPのURIを入力します。

c. ホストシステムのDNS名またはIPアドレスを入力します。
d. オプション：必要に応じて、ホストシステムの証明書をCA署名証明書に変更します。
e. 保存をクリックします

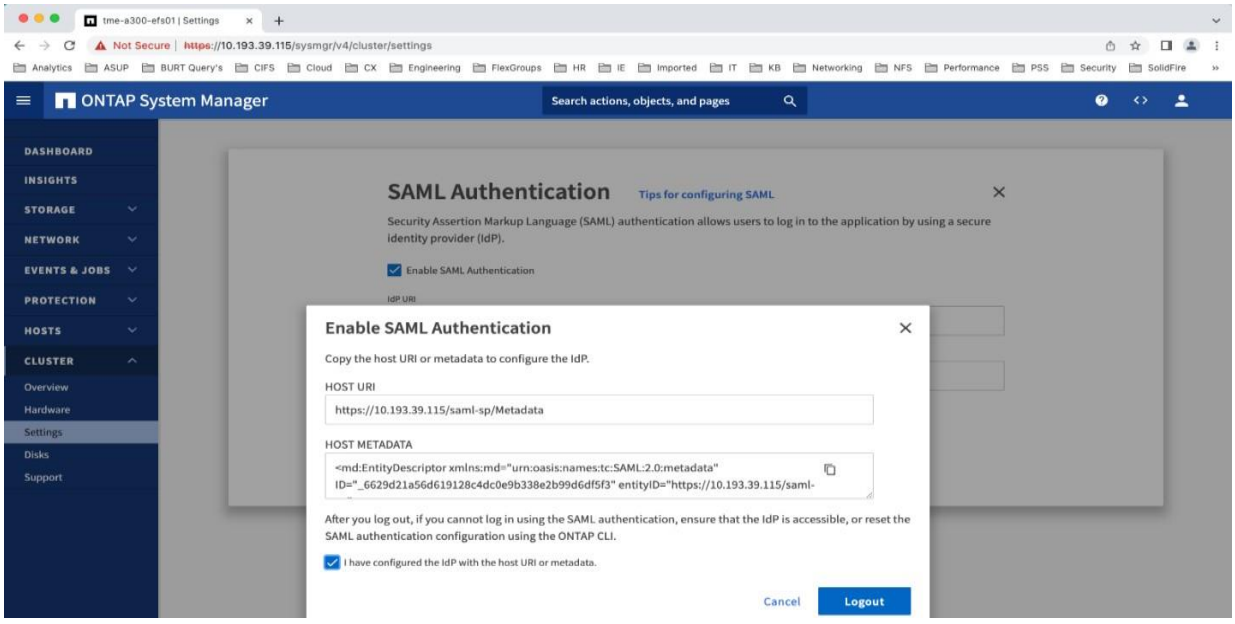


ホストメタデータセクションでコピーアイコンをクリックして、ホストURIとホストメタデータの情報を取得します。

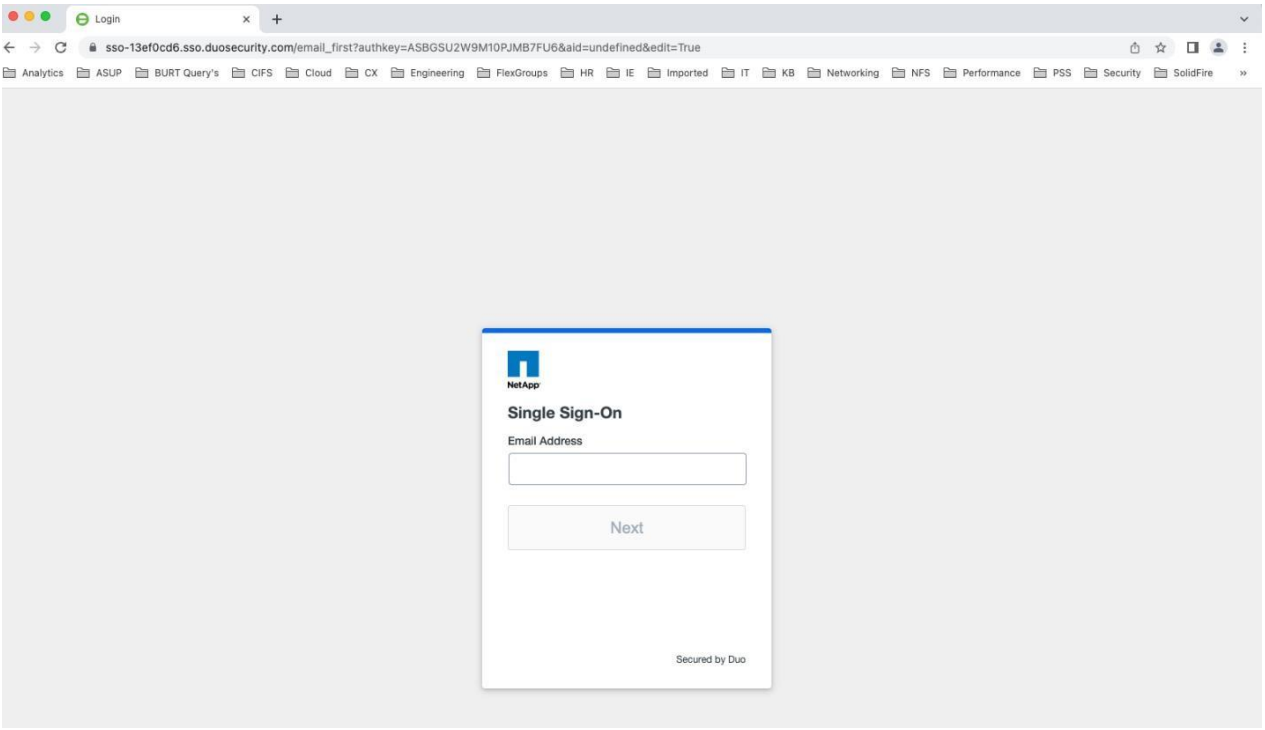
ホストのURIまたはメタデータをIdPにコピーし、IdPサーバで信頼の設定を完了しておきます。（IdPのドキュメントを参照してください）。

IdPサーバの設定が完了したら、[ホストのURIまたはメタデータでIdPを設定しました]ボックスをオンにします。

[ログアウト]をクリックします



IdPログインウィンドウが表示されます。

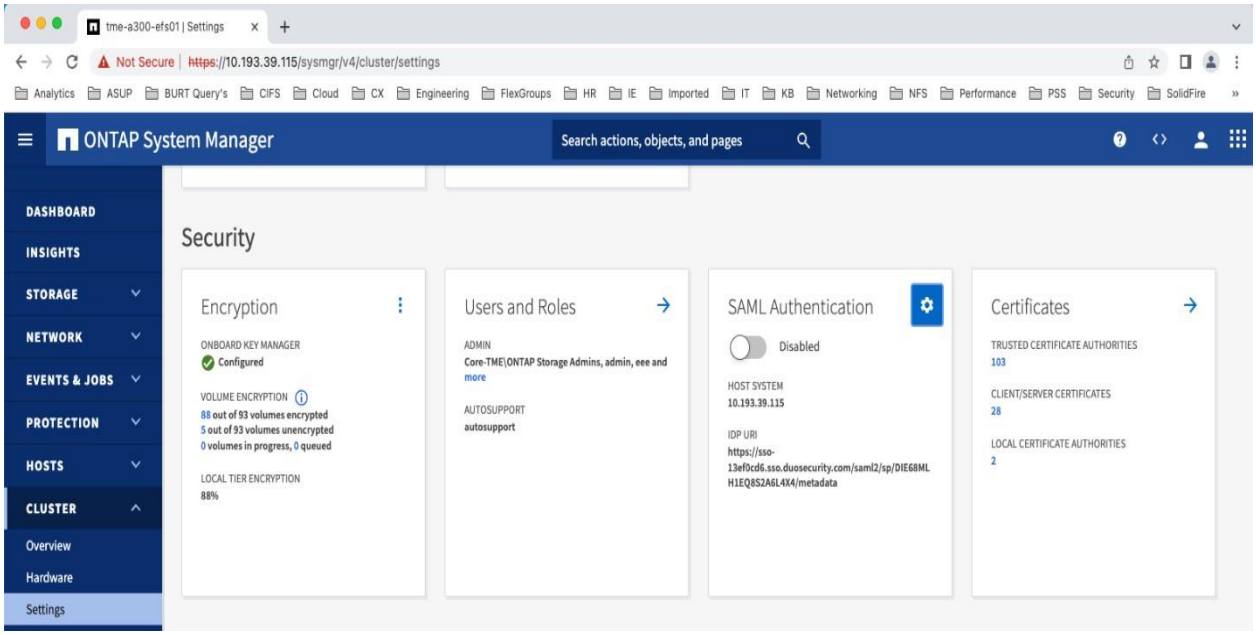


IdPのログインウィンドウを使用してSystem Managerにログインします。（特定の属性をONTAPクラスタと共有しようとしていることを示すプロンプトがIdPに表示される場合があります。ログインに成功するには、共有を許可する必要があります）。

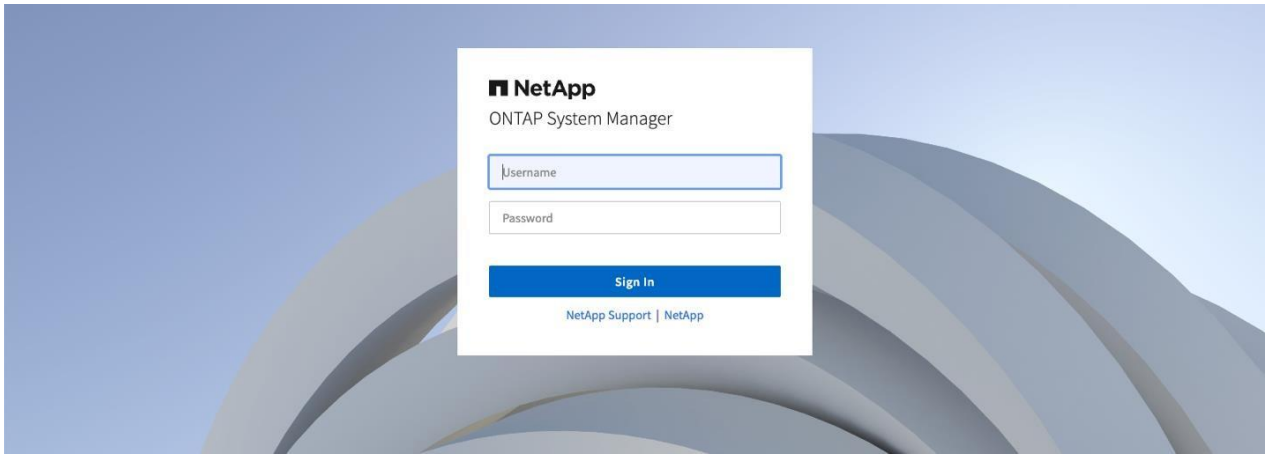
SAML IdP認証に成功すると、セッションの有効期間がIdPに設定されます。同じIdPを使用する他のサービスプロバイダ（SP）の場合、この設定ではセッションのライフタイム内に認証を維持できます。Active IQ Unified Managerが同じIdPを使用するSPサービスプロバイダの1つである場合は、追加の認証なしでActive IQ Unified Managerへのアクセスが許可されます。そのため、SSOが有効になります。

System ManagerでのSAML認証の無効化

1) クラスタ管理インターフェイス（DNS名またはIPアドレス）のhttps://cluster-mgmt-LIFを使用してSystem Managerを開き、IdPで認証します。[Cluster]>[Settings]に戻り、[Security]セクションまでスクロールして、SAML認証のトグルを[Disabled]に変更します。



2) [Save]をクリックし、警告に対して[Yes]と応答します。
System Managerにログインプロンプトが表示されます。



Active IQ Unified Manager

Active IQ Unified Manager のバージョン情報

NetApp ONTAP 9.3以降では、SAML認証はActive IQ Unified Manager 7.3以降のオプションです。

Active IQ Unified ManagerのSAML認証の有効化

SSH MFAの設定プロセス（System Managerの設定プロセスと同様）とは異なり、Active IQ Unified Managerをアクティブ化すると、既存のすべてのリモートユーザにSAML IdPを使用した認証が必要になります。Active IQ Unified Managerリモートユーザアカウントを変更する必要はありません。ローカルユーザとメンテナンスユーザは、SAML認証がアクティブ化されるとアクセスできなくなります。Active IQ Unified Managerメンテナンスコンソールには引き続きアクセスできます。SAML IdPアクセスを必要とする新しいアカウントは、Active IQ Unified Managerでリモートアカウントとして定義する必要があります。Active IQ Unified ManagerでSAML IdPが無効になっている場合、新しいアカウントにはリモート認証システムのクレデンシャル（ADかLDAPか）が必要になります。

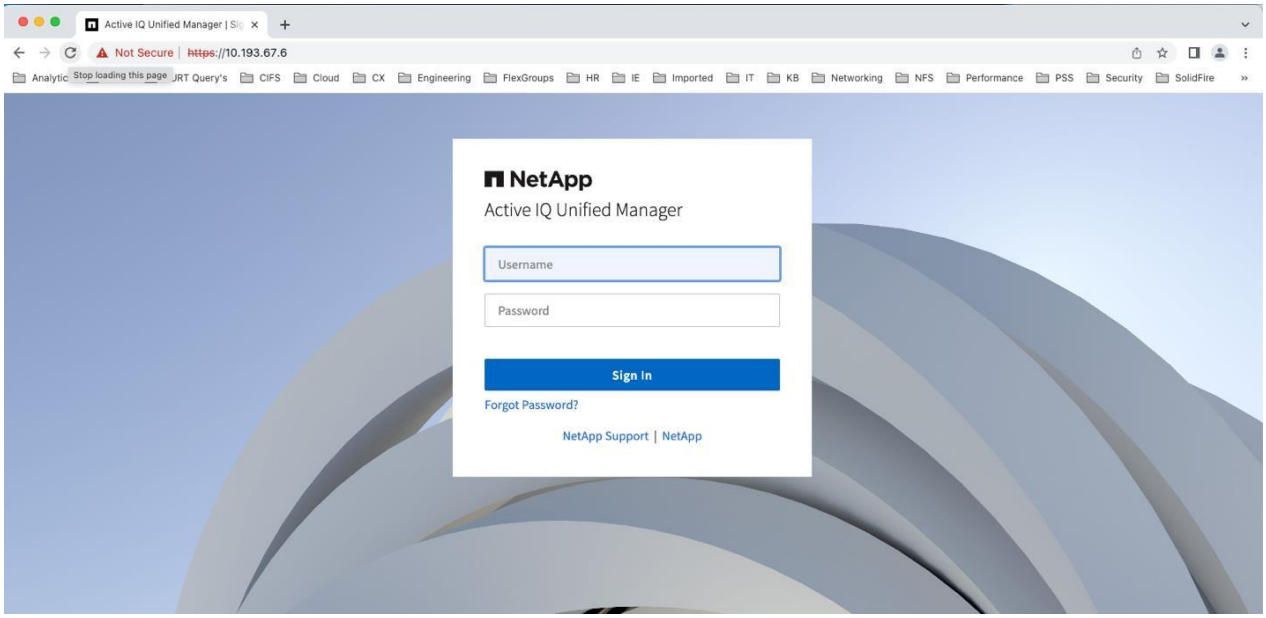
SAML IdPを有効にすると、IdPで使用可能な方式（LDAP、AD、Kerberos、パスワードなど）を使用してActive IQ Unified Managerアクセスの認証が実行されます。 など。使用できるメソッドは導入したIdPに固有です。

開始する前に

Active IQ Unified ManagerでSAML認証を有効にしたあとにIdPの設定が正しくないと、Active IQ Unified ManagerのWebインターフェイスにログインできないことがあります。IdPの修正中にSAML認証を無効にするには、SSHを使用してActive IQ Unified Managerメンテナンスコンソールにアクセスする必要があります。詳細については、本ドキュメントの「トラブルシューティング」セクションで後述する「Active IQ Unified ManagerのSAML認証を有効にしようとしたときに失敗する」を参照してください。

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

1) Active IQ Unified Manager、IdP、およびActive IQ Unified Manager Webクライアントの間にネットワーク接続が確立されていることを確認します。
2) Active IQ Unified Manager Web UIを起動します。

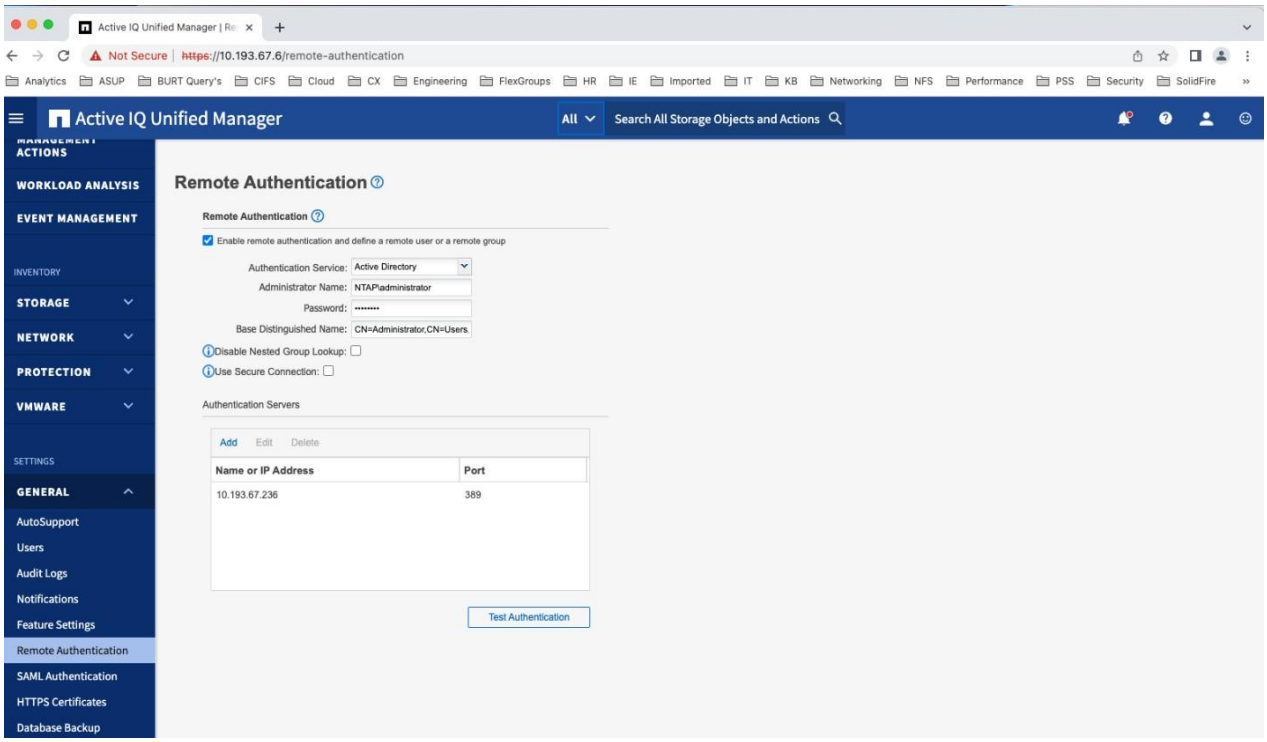


メンテナンスユーザのクレデンシャルを使用して認証します。

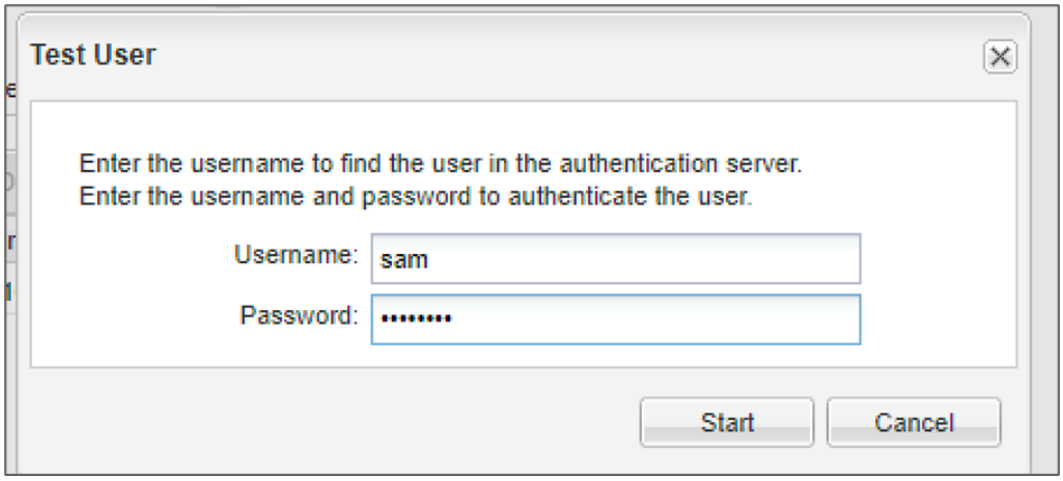
左側の[Settings]で[General]を展開し、[SAML Authentication]をクリックします。

リモート認証を有効にしていない場合は、SAML IdPユーザがActive IQ Unified Managerにアクセスできるように設定する必要があります。

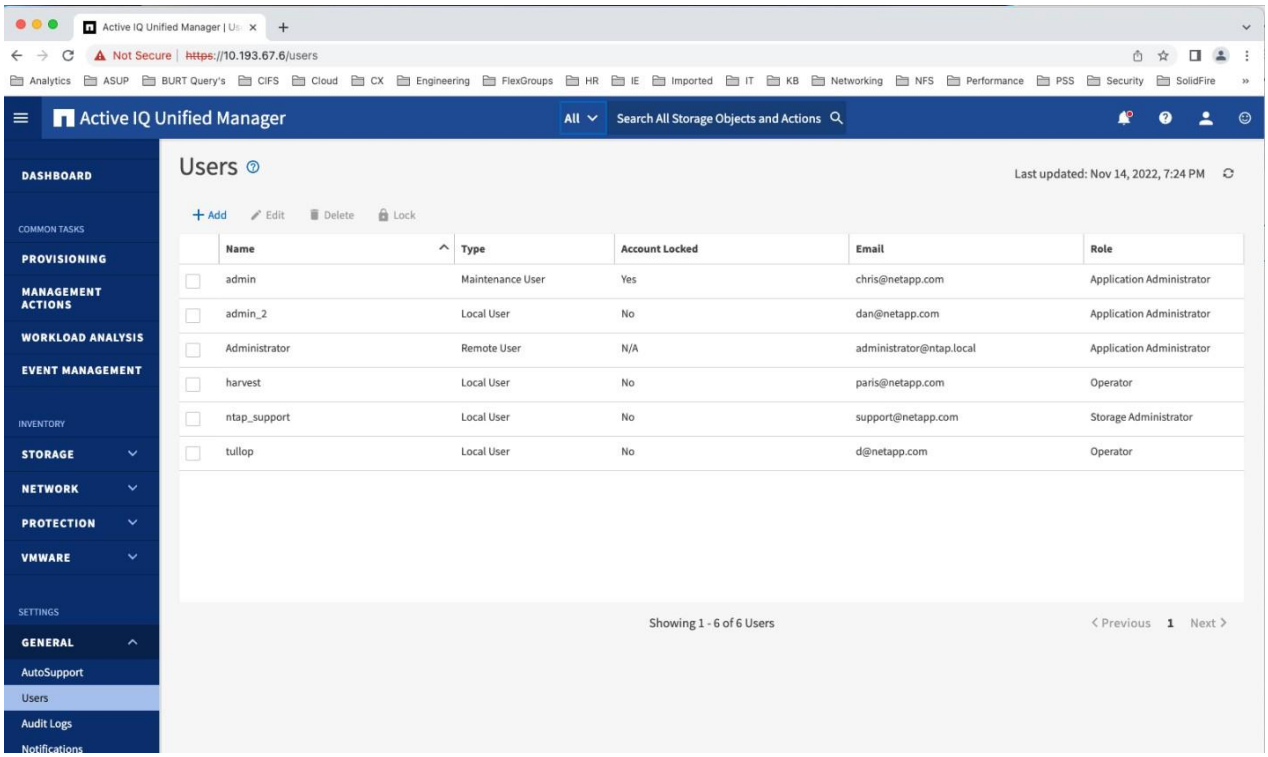
a. [リモート認証を有効にする]チェックボックスを選択します。
b. 認証サービスをActive DirectoryまたはOpenLDAPに設定します（Microsoft Lightweight Directory Servicesはサポートされていません）。
c. 管理者の名前とパスワードを入力します。ADの場合はBase Distinguished Name、LDAPの場合はBind Distinguished Name、Bind Password、およびBase Distinguished Nameを指定します。
d. [Authentication Servers]セクションで、認証サーバのDNS名またはIPアドレスを入力します。



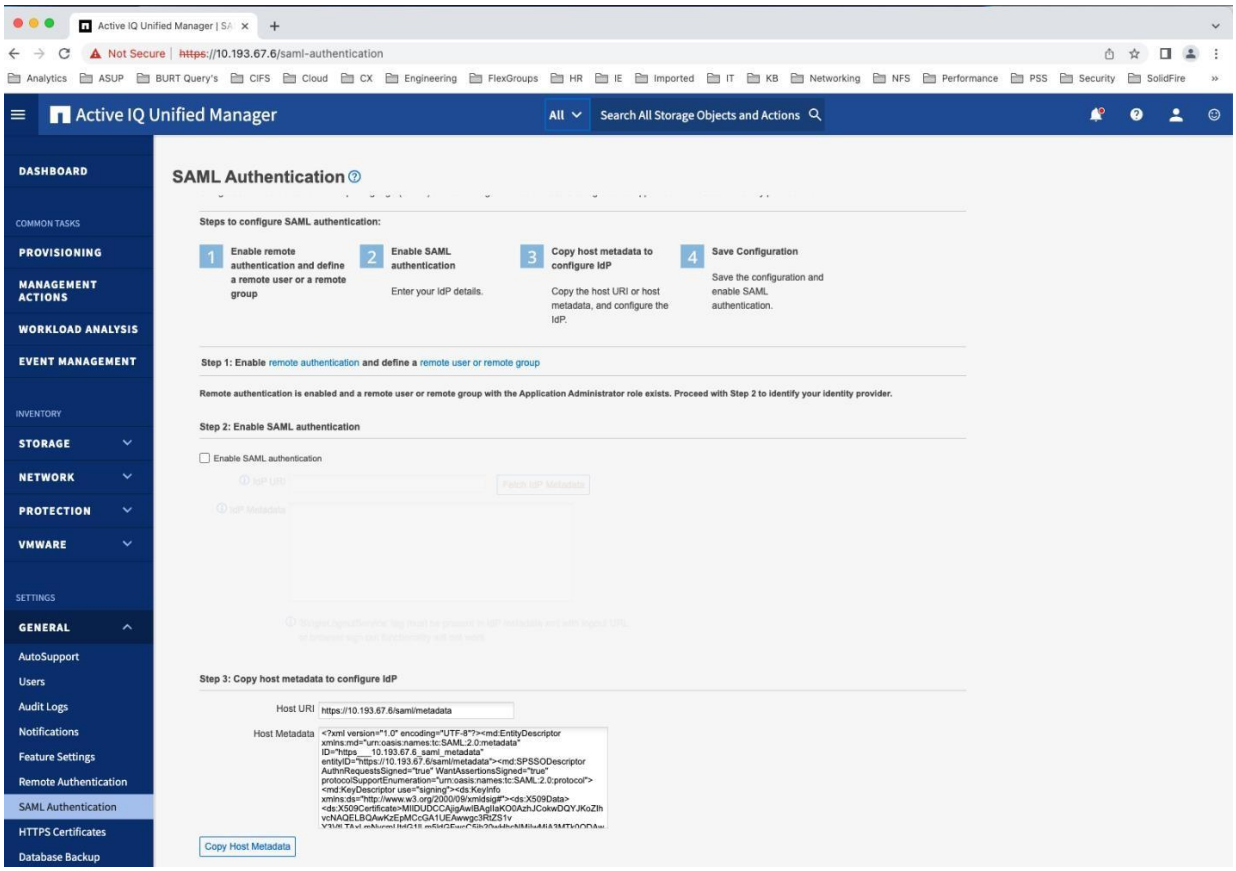
a. [認証のテスト]を使用して、リモート認証設定が動作していることを確認します。



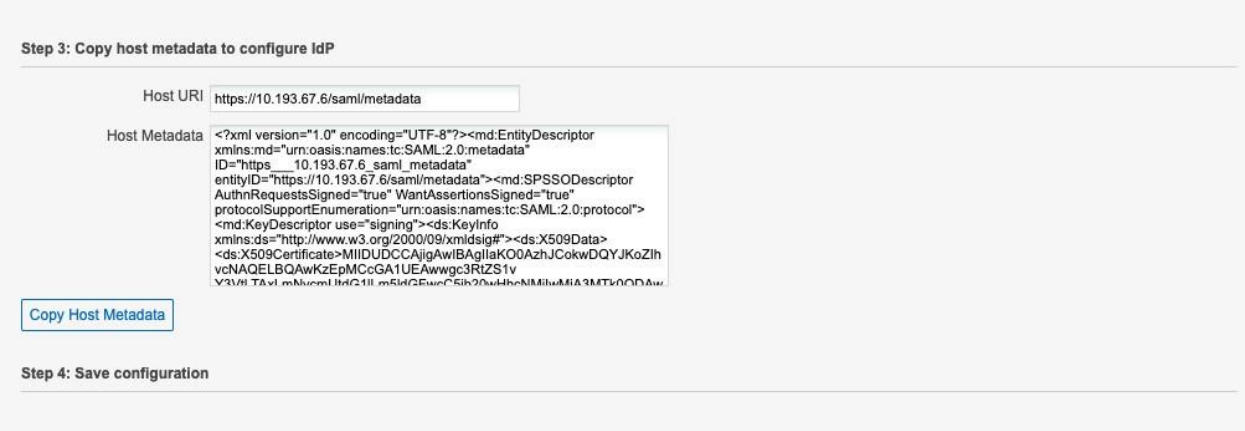
b. [設定]>[全般]>[ユーザ]に移動し、Active IQ Unified Managerアプリケーション管理者ロールが割り当てられたリモートユーザまたはリモートグループのユーザを追加します。



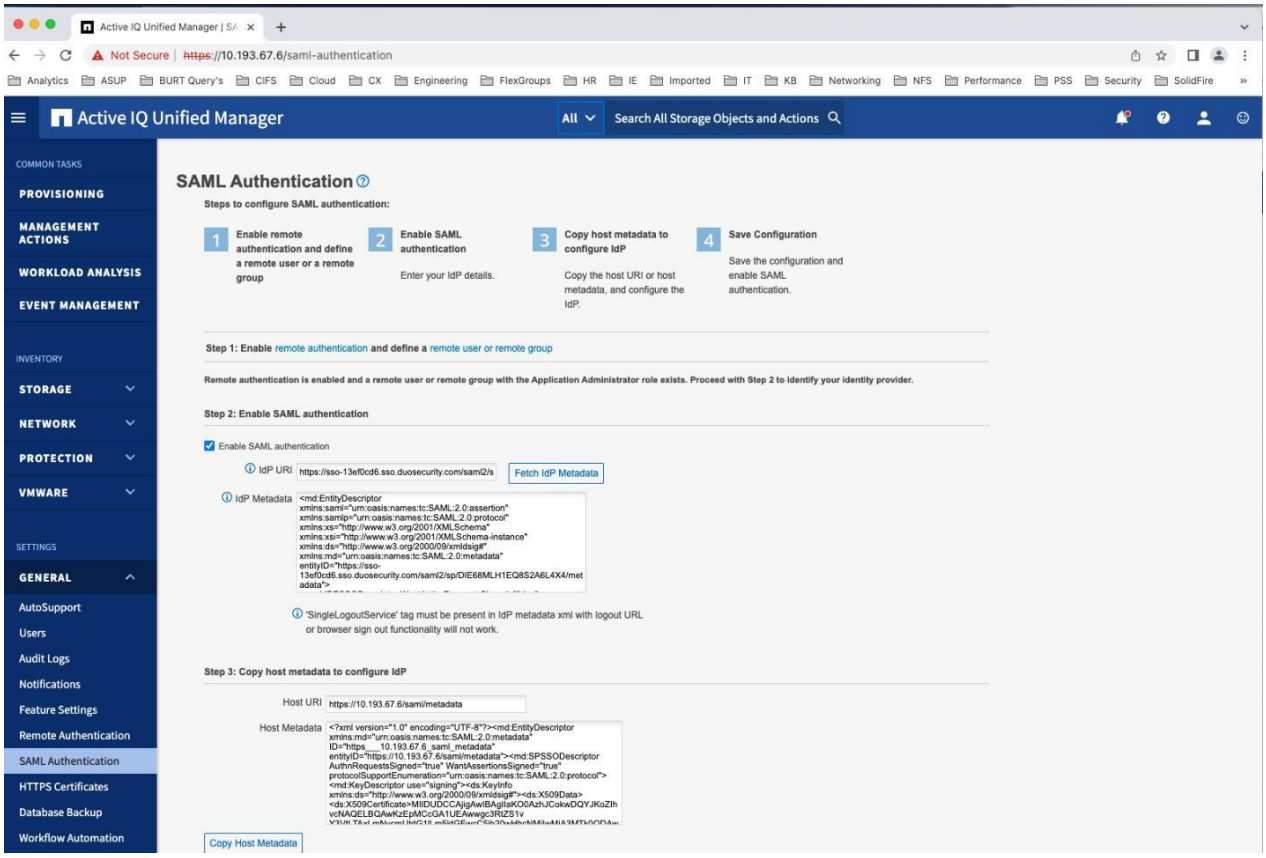
[設定]>[全般]>[SAML認証]ページに移動します。



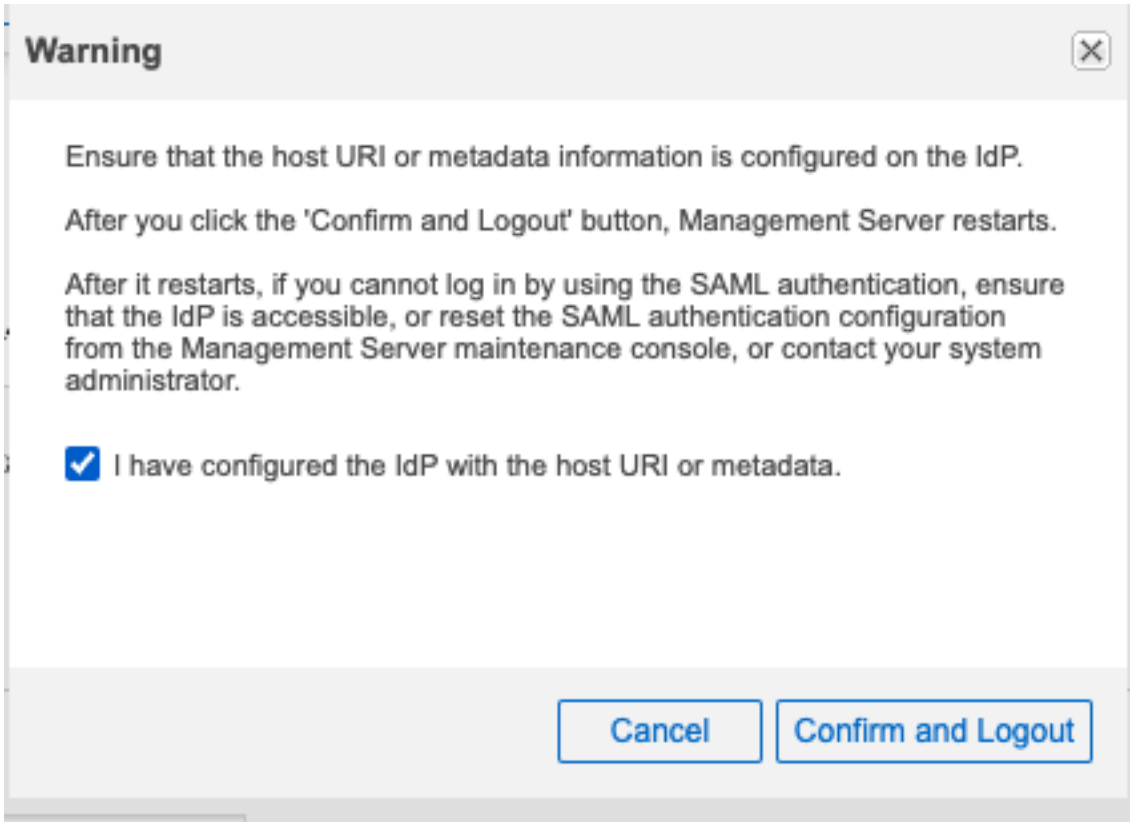
[Copy Host Metadata]をクリックし、メタデータをファイルにコピーして保存します。このファイルは、IdPでActive IQ Unified Managerを設定するときに使用します。



[SAML認証を有効にする]チェックボックスをオンにしてIdPのURLを入力し、[IdPメタデータの取得]をクリックしてActive IQ Unified ManagerにIdPデータを入力します。



[保存]をクリックし、IdPが設定されたことを確認するチェックボックスをオンにし、[Confirm and Logout]をクリックします。



Active IQ Unified Managerサービスが再起動するまで5分待ちます。

IdPを設定します（IdPのドキュメントを参照）。

a. 手順7で取得したActive IQ Unified ManagerメタデータをIdPに入力します。
b. Active IQ Unified Managerを証明書利用者として追加します。
c. 請求ルールを追加します。[名前]をに `urn:oid:0.9.2342.19200300.100.1.1`、[修飾名]をに設定します `urn:oid:1.3.6.1.4.1.5923.1.5.1.1`。

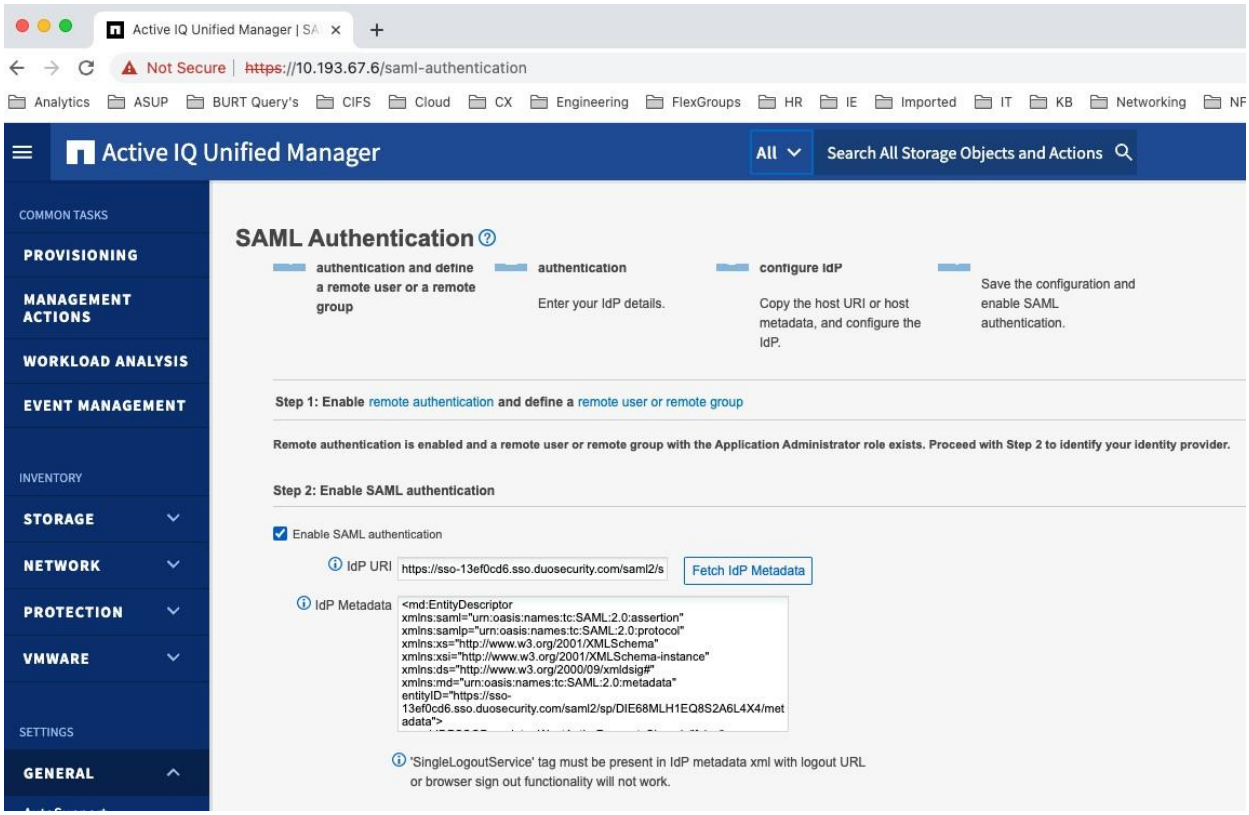
Active IQ Unified Manager Web UIを起動します。

手順5Fで定義したリモートユーザを使用して認証します。

System Managerのセクションと同様に、SAML IdP認証に成功すると、セッションの有効期間がIdPに設定されます。同じIdPを使用する他のSPでは、これにより、セッションのライフタイム期間内に認証が存在できるようになります。System Managerが同じIdPを使用するSPの1つである場合は、Active IQ Unified Manager認証の完了後、追加の認証なしでSystem Managerへのアクセスが許可されます。

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

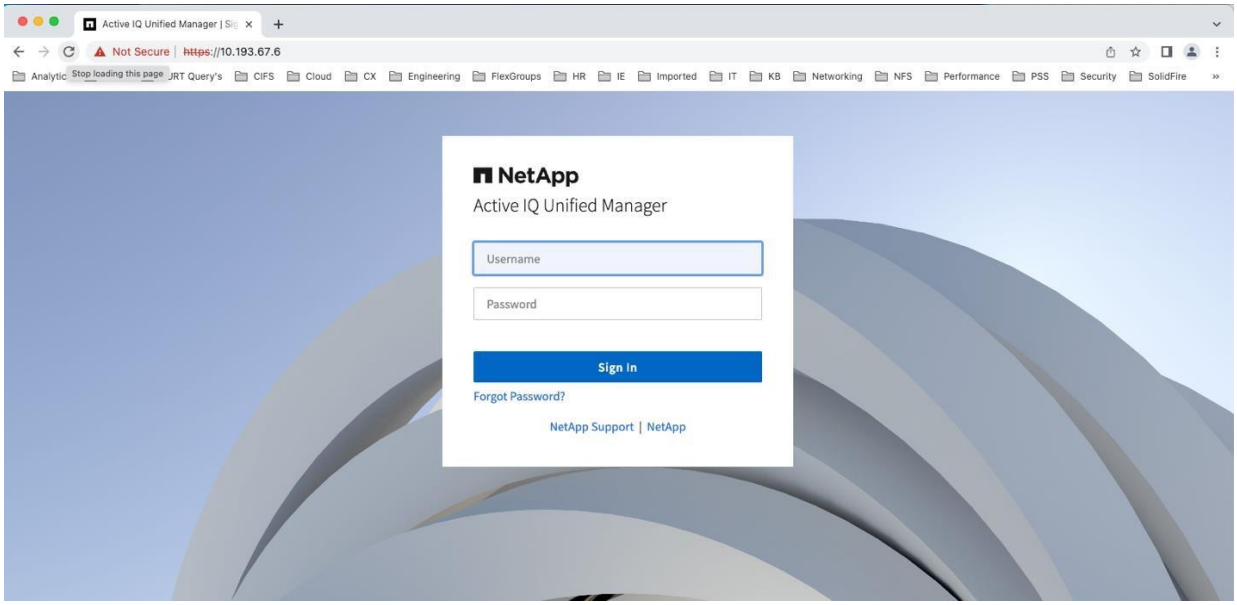
1) Active IQ Unified Manager Web UIを起動し、IdPで認証し、[SAML認証を有効にする]チェックボックスをオフにします。[Save]をクリックします。



[Save]をクリックし、警告に対して[Yes]と応答します。

Active IQ Unified Managerサービスが再起動するまで5分待ちます。

Active IQ Unified Manager Web UIを起動します。



ベストプラクティスと注意事項

ユビキタスMFAの実装

NetApp ONTAP 9.3 SSH MFAでは、ユーザ単位で増分実装を行うことができます。これは段階的な増分導入には便利ですが、MFA導入の最終的な目標は、すべての管理者ユーザが強力な多要素認証でログインクレデンシャルを使用できるようにすることです。

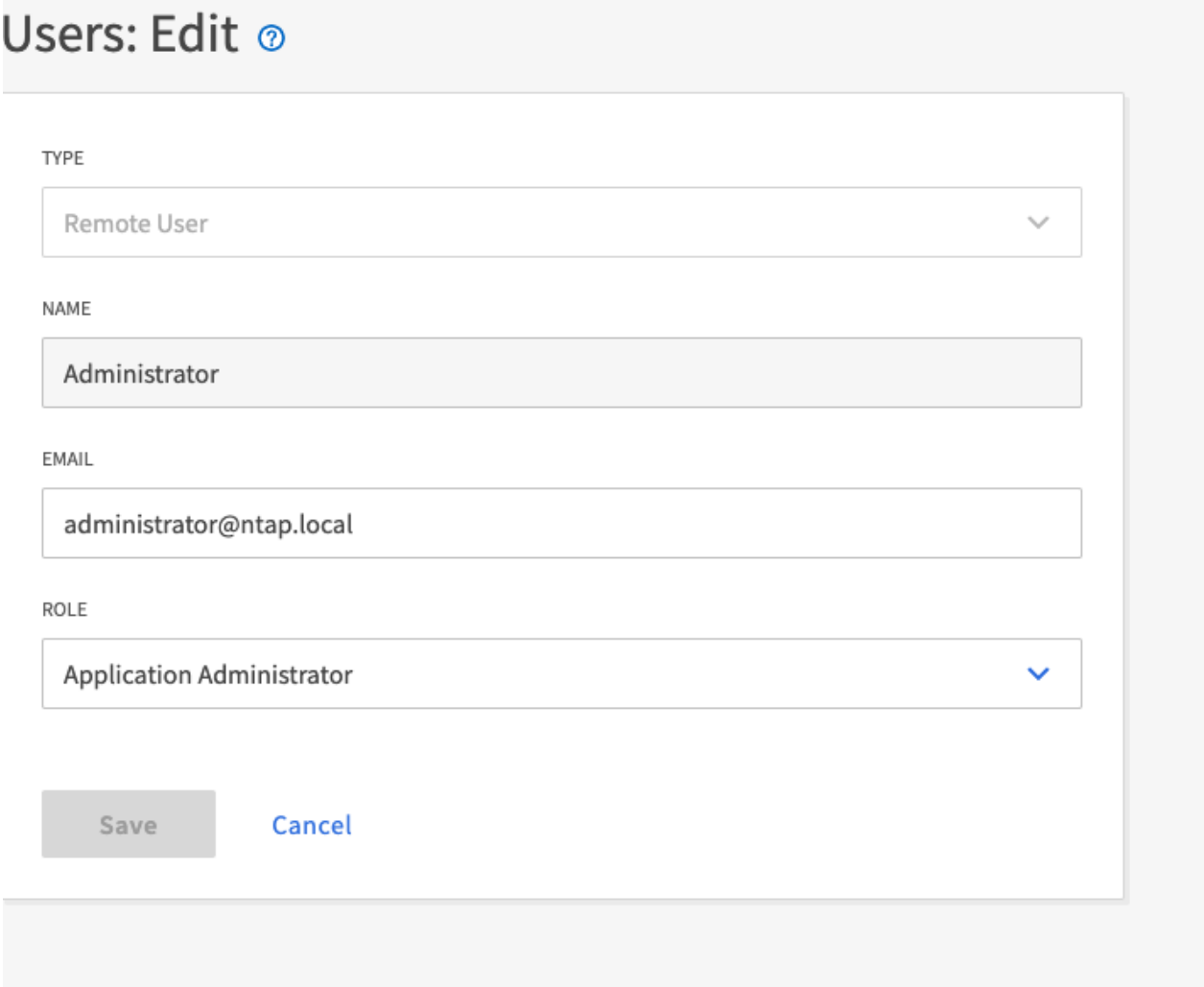
すべてのユーザのMFAログインクレデンシャルに加えて、各管理者のアクセスモードでMFAを使用する必要があります。ONTAPの場合は、System ManagerのHTTPアクセス用にSSH CLIとSAMLを使用します。ユーザの場合は sam、次のログイン設定が必要です。

```
ontap9-tme-8040::*> security login show sam
Vserver: ontap9-tme-8040
                                                                  Second
User/Group                  Authentication                 Acct   Authentication
Name            Application Method         Role Name       Locked Method
--------------- ----------- -------------- --------------- ------ --------------
sam             console     password       admin           no     none
sam             http        password       admin           no     none
sam             http        saml           admin           -      none
sam             ontapi      password       admin           no     none
sam             ontapi      saml           admin           -      none
sam             ssh         password       admin           no     publickey
6 entries were displayed.
```

注： `http` アプリケーションと `ontapi` アプリケーションにSAML認証を設定したら、 `password` 認証方式を設定する必要はありません。外部のサポートツールが単一要素のユーザID /パスワード認証を使用して引き続き管理者アクセスできるように、管理者アカウント用に設定されたままになります。このようなツールでユーザIDとパスワードのアクセスが必要ない場合は `http`、および `ontapi` アプリケーションのすべての管理者アカウントのパスワード認証方式をすべて削除して、最も安全な管理アクセス環境を実現します。

Active IQ Unified Manager SAML認証の場合は、`Administrator` Active IQアプリケーション管理者のロールを持つリモートユーザとして定義する必要があります。

図3）Active IQ Unified Managerリモートユーザの定義



注： Active IQ Unified Manager SAML認証を設定する前に、管理者はADまたはOpenLDAPによって認証されていました。SAML認証を有効にすると、`Administrator` はSAML IdPでのみ認証されます。

単一要素認証からMFA

SSH CLIへの移行

ONTAP管理者アカウントが1つしかない場合は、プライマリアカウントの移行で問題が発生した場合に備えて、少なくとも2つ目のローカル単一要素認証アカウントを作成します。ONTAPログインアカウントの開始状態でローカルSSHパスワードまたは公開鍵認証方式を使用している場合は、コマンドを使用して単一要素認証から2要素認証に移行します `security login modify -user-or-group-name [username] -application ssh -second- authentication-method [password or publickey]`。新しい2つ目の要素がの場合は `publickey`、コマンドを使用して公開鍵をユーザに関連付けます `security login publickey create - vserver [SVM_name] -username [username] -index [index_number] -publickey "[public_key_data]"`。

ONTAPログインアカウントの開始状態がリモートNIS/LDAP `nsswitch` SSH認証方式を使用している場合は、コマンドを使用して単一要素認証から2要素認証に移行します `security login modify -user-or-group-name [username] -application ssh -authentication-method nsswitch -second-authentication-method publickey`。次に、コマンドを使用してユーザに公開鍵を関連付け `security login publickey create -vserver [SVM_name] - username [username] -index [index_number] -publickey "[public_key_data]"`ます。

注： `nsswitch` グループユーザの2要素認証（`security login create ... -is- nsswitch-group=yes`）はサポートされていません。

ONTAP管理者ログインアカウントの開始状態が `domain` （AD）の場合は、アカウントを削除し、ローカルのSSHアカウント `publickey`、`password`または `publickey nsswitch` 認証方式に再度追加する必要があります。リモート `domain` アカウントを削除せずにローカルの2要素認証アカウントを作成した場合、パスワードの競合がローカルおよびリモートのログイン定義と異なると、ログインに失敗することがあります。

ONTAP 9.13.1以降：

- ONTAP管理者ログインアカウントの開始状態が `domain`（AD）の場合は、 `publickey` 2つ目の認証方法としてを追加できます。
- タイムベースワンタイムパスワード（TOTP）は、現在の時刻を2番目の認証方法の認証要素の1つとして使用するアルゴリズムによって生成される一時パスコードです。TOTP認証には、Google Authenticator、Microsoft Authenticator、およびAuthyが含まれます。市場には、TOTP認証に使用できるTOTPアプリが多数あります。
- 公開鍵の失効は、SSH公開鍵と、SSH中に有効期限や失効がチェックされる証明書でサポートされます。

System ManagerとActive IQ Unified Manager SAML認証

System ManagerとActive IQ Unified ManagerでのSAML認証は似ていますが、SAML IdPのアクティブ化と実装は異なります。

System ManagerでSAML認証を有効にすると `saml` `http`、および `ontapi` アプリケーションの管理者ロールを持つ既存のユーザに対して、新しい認証方式のが自動的に追加されます。この時点で、System ManagerのIdPで導入されている認証方式が有効になります。ローカルパスワード、ドメイン、または `nsswitch`（ADまたはLDAP / NIS）の有効期間が長くなります。

Active IQ Unified ManagerでSAML認証を有効にすると、Active IQ Unified Managerで定義されているすべてのリモートユーザが、IdPに導入された方式を使用して認証できるようになります。ADまたはLDAPのリモート認証方式は無効になります。

IdP実装の要因の1つにADまたはLDAPがある可能性があります。他の要素が導入されている場合は、管理者ユーザごとに実装する必要があります。さまざまな要因が存在する可能性があります。最も一般的に使用される要因は、ユーザ名/パスワード、公開鍵、およびグループ、ロール、IPアドレス、Eメールアドレスなど、検証可能なさまざまな属性です。

詳細については、このドキュメントで後述する「Where to Find追加情報」のADFSおよびシボレスIdPのリンクを参照してください。

IdPの可用性に関する考慮事項

ADやLDAPなどのリモート認証メカニズムと同様に、SAML認証を有効にしたあとも、IdPへの接続を継続し、IdP機能の継続的なアップタイムが重要になります。System ManagerとActive IQ Unified Managerの管理アクセスを確保するには、冗長化されたハイアベイラビリティ構成のIdPを設定する必要があります。

ADFSとシボレスはアーキテクチャ上ユニークであるため、高可用性構成を作成するアプローチもユニークです。ADFSでは、SQL Serverを使用してさまざまな場所にあるサーバー間でデータを複製することで、フェデレーションサーバーファームを作成できます。Shibbolethの高可用性に対する推奨アプローチは、ソフトウェアまたはハードウェアのロードバランシングメカニズムを使用して、Shibbolethノード間でステートフルデータを複製するクラスタを作成することです。

詳細については、このドキュメントで後述する「Where to Find追加情報」のADFSおよびシボレスIdPのリンクを参照してください。

MFAから単一要素認証

SSH CLIへの移行

ONTAP SSHローカルアカウントの単一要素認証に戻すには、コマンドを使用して、`security login modify -user-or-group-name [username] -application ssh -second- authentication-method none` 各管理者ユーザの2番目の要素を削除します。2番目の要素がの場合は `publickey`、その管理者ユーザに関連付けられている公開鍵が削除されます。

System ManagerまたはActive IQ Unified Manager SAML認証

System ManagerまたはActive IQ Unified ManagerでMFAを無効にするには、それぞれのSAML認証Webページで[SAML認証を有効にする]の選択を解除します。System ManagerまたはActive IQ Unified ManagerでSAML認証を無効にする方法の詳細については、本ドキュメントで前述した「設定」セクションを参照してください。

System ManagerでSAML認証を無効にすると、ONTAPでこの機能が無効になります。ただし `security login http` 、SAML認証方式は、および `ontapi` アプリケーションの管理者設定のままです。

Active IQ Unified ManagerでSAML認証を無効にすると、リモートユーザはActive IQ Unified Managerリモート認証で設定されているLDAP認証またはAD認証に戻ります。

トラブルシューティング

一般的な問題

System ManagerのSAML認証を有効にしようとすると失敗する

SAML認証を有効にした場合にIdPの設定が正しくないと、管理ユーザはSystem Managerにログインできなくなります。クラスタ管理LIFからSAMLを無効にすることはできません。SAMLはRLMコンソールから無効にする必要があります。

```
ontap9-tme-8040::> security saml-sp show
       Identity Provider URI: https://centos7.ntap2016.local:8443/idp/shibboleth
       Service Provider Host: ontap9-tme-8040.NTAP2016.LOCAL
       Certificate Authority: ontap9-tme-8040
          Certificate Serial: 054D9DDD623882
                 Common Name: ontap9-tme-8040
             Is SAML Enabled: true
ontap9-tme-8040::> security saml-sp modify -is-enabled false

Error: command failed: SAML authentication can only be disabled from the
       "console" application or from a SAML authenticated application.
```

```
login as: admin
admin@10.193.67.15's password:

SP ontap9-tme-8040-01> system console
Type Ctrl-D to exit.
SP-login: admin
Password:
```

```
**************************************************
* This is an SP console session. Output from the    *
* serial console is also mirrored on this session. *
**************************************************
ontap9-tme-8040::> security saml-sp show
       Identity Provider URI: https://centos7.ntap2016.local:8443/idp/shibboleth
       Service Provider Host: ontap9-tme-8040.NTAP2016.LOCAL
       Certificate Authority: ontap9-tme-8040
          Certificate Serial: 054D9DDD623882
                 Common Name: ontap9-tme-8040
             Is SAML Enabled: true

ontap9-tme-8040::> security saml-sp modify -is-enabled false
```

その後、System ManagerにログインしてIdPの問題を修正し、SAML認証を再度有効にできます。

Active IQ Unified ManagerのSAML認証を有効にしようとすると失敗する

SAML認証を有効にした場合にIdPの設定が正しくないと、ローカルユーザまたはリモートユーザとしてActive IQ Unified Managerにログインできなくなります。SSHを使用してメンテナンスユーザのクレデンシャルを使用してActive IQ Unified Managerメンテナンスコンソールにアクセスし、メニュー項目を選択してSAML認証を無効にする必要があります。

```
Active IQUnified Manager Maintenance Console

  Version    : 7.3.N170720.1600
  System ID  : f7755d8a-e703-41dc-a7fb-fd9892e4128c
  Status     : Running

  Discovered interfaces: eth0 (ENABLED)

 Main Menu
 ------------
    1 ) Upgrade (Disabled. Must be run on virtual machine console.)
    2 ) Network Configuration
    3 ) System Configuration
    4 ) Support/Diagnostics
    5 ) Reset Server Certificate
    6 ) External Data Provider
    7 ) Performance Polling Interval Configuration
    8 ) Migrate Data from OnCommand Performance Manager 7.1
    9 ) Disable SAML authentication

    x ) Exit

 Enter your choice:
```

その後、Active IQ Unified ManagerにログインしIdPの問題を修正し、SAML認証を再度有効にします。

ログ

この `shibd.log` ファイルには、IdPの実装に関する問題のデバッグに役立つ情報が記載されています。NetApp ONTAPでは、 `shibd.log` Service Processor Interface（spi；サービスプロセッサインターフェイス）ノード管理ログからアクセスできます。

図4）ONTAP SPIログの選択

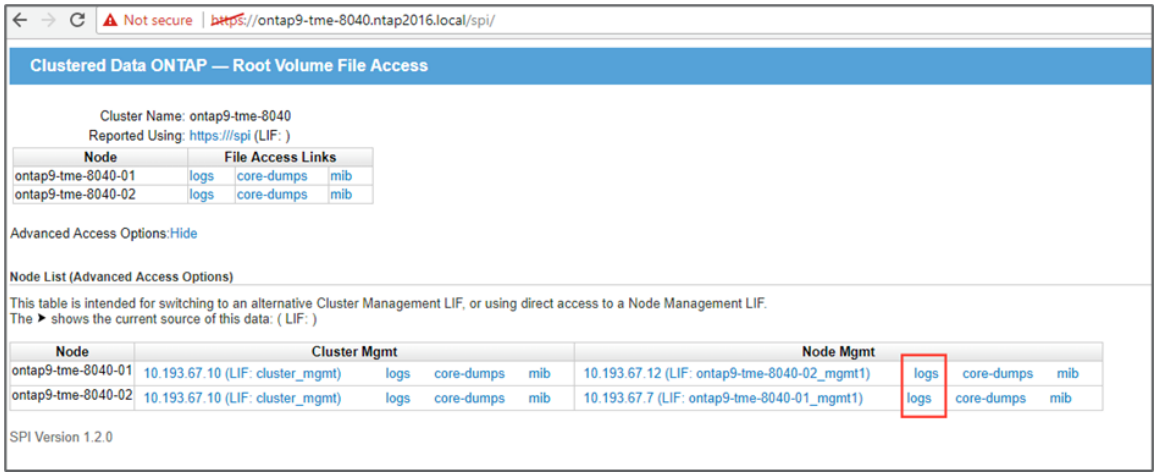
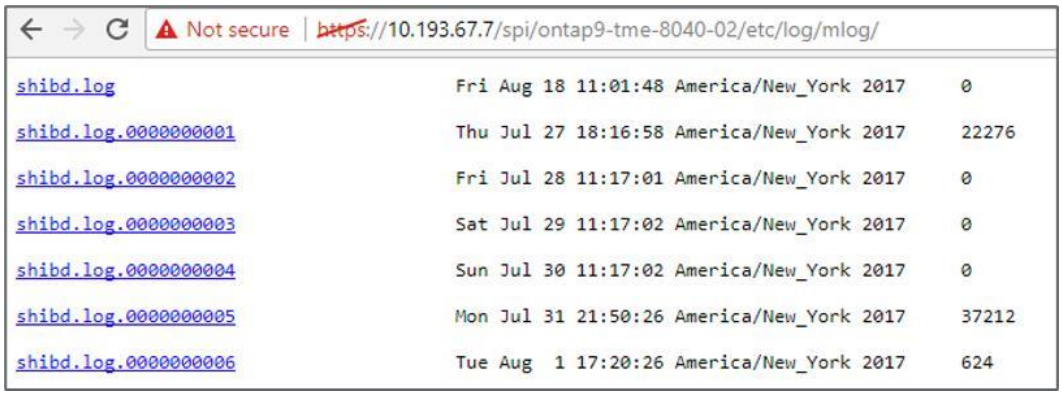


図5）ONTAP SPIファイル `shibd.log`



注: Shibboleth IdPには `/opt/shibboleth-idp/logs/idp- process.log`、似たようなログがあります。

免責事項

NetAppは、本ドキュメントで提供されるいかなる情報または推奨事項の正確性、信頼性、有用性についても、または本ドキュメントで提供されるいかなる情報の使用または推奨事項の順守による結果についても、表明または保証は一切行いません。本ドキュメントの情報は現状のまま提供され、本ドキュメントの情報の使用または推奨内容や手法の実施は、お客様の評価および業務環境への統合能力に基づいて、お客様の責任で行われるものとします。本ドキュメントおよびここに記載の情報は、本ドキュメントに記載のNetApp製品のみに関連して使用できるものとします。

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントやWebサイトを確認してください。

- NIST Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
- PCI DSS 4.0リソースハブ
- ONTAP 9セキュリティガイド
- `ssh-keygen`
- PuTTYgenを使用したSSHによるRSAキーの生成
- Active Directoryフェデレーションサービス（ADFS）
- シボレスIdP
- Verizon 2023データ侵害調査レポート

バージョン履歴

バージョン	日付	ドキュメント バージョン履歴
バージョン1.0	2017年11月	初版：Dan Tulledge
バージョン1.1	2018年3月	Dan Tulledge：9.4アップデート
バージョン2.0	2022年11月	Matt Trudewind 9.12.1アップデート
バージョン2.1	2023年7月	Dan Tulledge 9.13.1アップデート

お問い合わせ

本テクニカル レポートの品質向上について、ご意見をお寄せください。doccomments@netapp.com までお問い合わせください。件名にはテクニカルレポートTR-4647を添えてください。

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報

TR-4647-1122-JP

NetApp