Technical Report

Multifactor authentication in ONTAP

Best practices and implementation guide

Dan Tulledge and Matt Trudewind, NetApp

July 2023 | TR-4647

Abstract

This document covers multifactor authentication capability for administrative access introduced in NetApp® ONTAP® 9.3 software for NetApp System Manager, Active IQ® Unified Manager and ONTAP Secure Shell (SSH) CLI authentication.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

The requirement for strong administrative credentials

According to the 2023 Verizon Data Breach Investigative Report (VDBIR) 49% of data breaches involved use of stolen credentials. New requirements from the United States federal government are emerging, such as the White House Executive Order on Improving the Nation's Cybersecurity and the Payment Card Industry Data Security Standard (PCI DSS). These requirements mandate that user accounts prove or verify that the user associated with the identity is who the user claims to be. Specifically, multifactor authentication (MFA) mechanisms are required. MFA makes it impossible for an attacker to compromise an account using only a username and password. MFA requires two or more independent factors to authenticate a user. An example of two-factor authentication is something a user possesses, such as a private key, and something a user knows, such as a password.

Beginning with NetApp ONTAP 9.3, NetApp is addressing this requirement for web authentication in NetApp System Manager and Active IQ® Unified Manager, and for SSH CLI authentication in ONTAP.

Table 1) MFA methods.

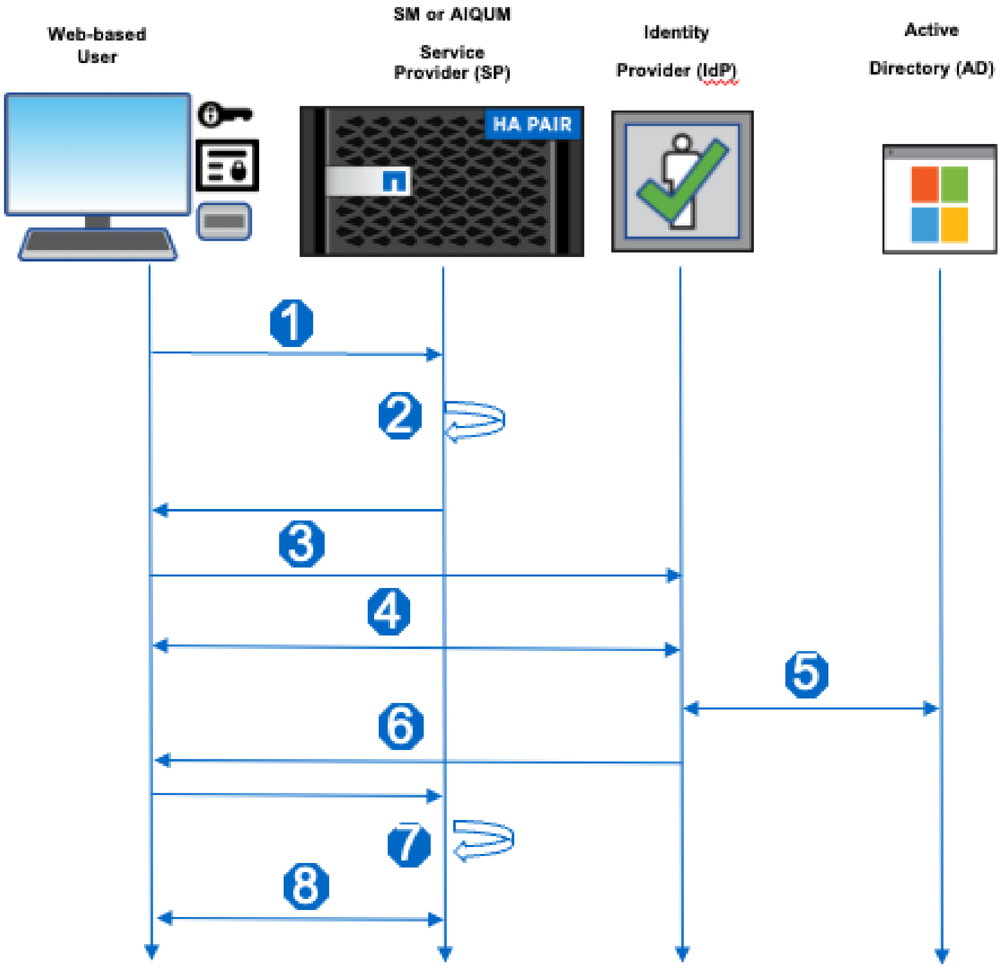
Application	MFA method
SSH ONTAP CLI	Method 1 – Two Factor Chained Authentication An ONTAP locally administered administrator or domain account with chained primary and secondary authentication methods of `password` and `publickey`, or `nsswitch` and `publickey`. Time-based-one-time password (TOTP) is a temporary passcode generated by an algorithm that uses the current time of day as one of its authentication factors. TOTP can only be used as secondary authentication method for local users. Method 2 –YubiKey Using PIV or FIDO2 Authentication An ONTAP locally administered administrator account with an authentication method using a public key along with a YubiKey device leveraging either Personal Identify Verification (PIV) authentication or FIDO2 (Fast Identity Online) authentication. **Note:** PIV and FIDO2 support is available starting in ONTAP 9.12.1 **Note:** Domain accounts, time-based-one-time password (TOTP), and public key revocation are supported in ONTAP 9.13.1.
System Manager ONTAP web user interface or Active IQ Unified Manager web user interface	Security Assertion Markup Language (SAML) 2.0, where ONTAP System Manager or Active IQ Unified Manager is the service provider role and Active Directory Federation Service (ADFS), Cisco DUO or Shibboleth as the identity provider (IdP) role. The authentication factors are configured in the IdP. **Note:** Cisco DUO support is available starting in ONTAP 9.12.1

SAML-based web interactive login

SAML 2.0 is a widely adopted industry standard that allows any third-party SAML-compliant identity provider (IdP) to perform MFA using mechanisms that are unique to the chosen IdP for the enterprise and as a source of single sign-on (SSO).

There are three roles defined in the SAML specification: the principal, the IdP, and the service provider. In the ONTAP implementation, a principal is the cluster administrator gaining access to ONTAP through System Manager or Active IQ Unified Manager. The IdP is third-party IdP software from an organization such as Microsoft ADFS, Cisco DUO, or the open-source Shibboleth IdP. The service provider is the SAML capability built into ONTAP that is used by System Manager or the Active IQ Unified Manager web application.

Figure 1) SAML workflow.



The administrator connects to a NetApp node using either the System Manager or the Active IQ Unified Manager web UI.

System Manager or Active IQ Unified Manager looks up the configured IdP for the cluster.

System Manager or Active IQ Unified Manager redirects the administrator’s browser to the IdP.

The IdP prompts the administrator for credentials.

The IdP is responsible for multiple authentication factors.

The IdP verifies the administrator’s credentials in the Active Directory.

The IdP issues a SAML assertion and redirects the administrator’s web browser back to System Manager or Active IQ Unified Manager.

System Manager or Active IQ Unified Manager processes the SAML assertion, and then searches for the authorization role from its internal database.

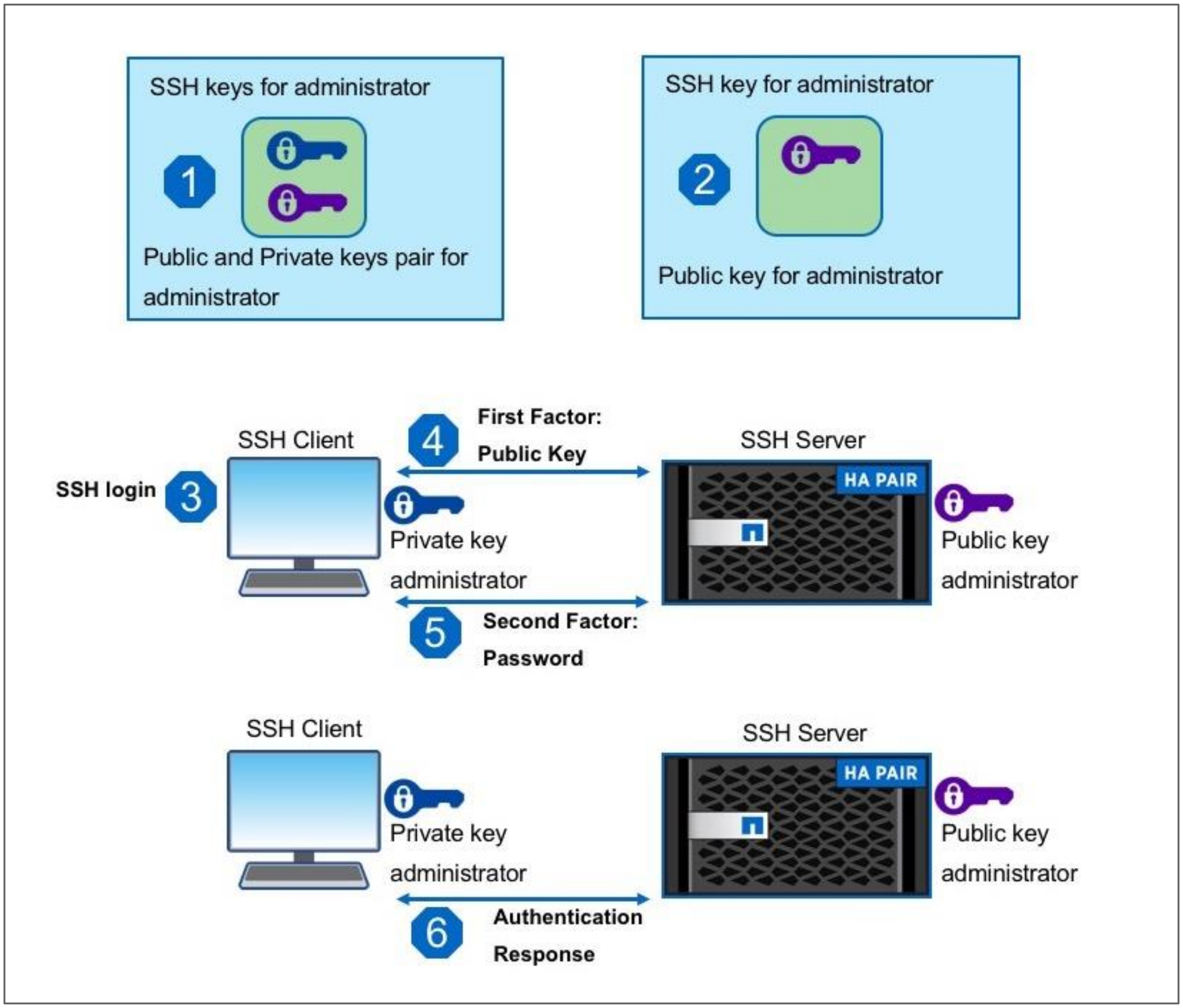
The session is established, and System Manager or Active IQ Unified Manager returns a SAML session token to the administrator's web browser in the Set-Cookie header.

From this point on, the administrator is allowed access to System Manager or Active IQ Unified Manager using a secure SAML token.

SSH MFA Access: CLI login with two-factor chained authentication

Before ONTAP 9.3, ONTAP supported SSH access using both password-based and public-key-based authentication independent of each other. With ONTAP 9.3, chained authentication is supported: a public-key authentication is followed by password authentication, providing two-factor authentication. This capability works only with ONTAP local accounts. Beginning in ONTAP 9.13.1, Active Directory domain accounts userid and passwords are supported The capability is enabled by `second-authentication-method` in the `security login` command.

Figure 2) SSH public-key authentication followed by password authentication workflow.



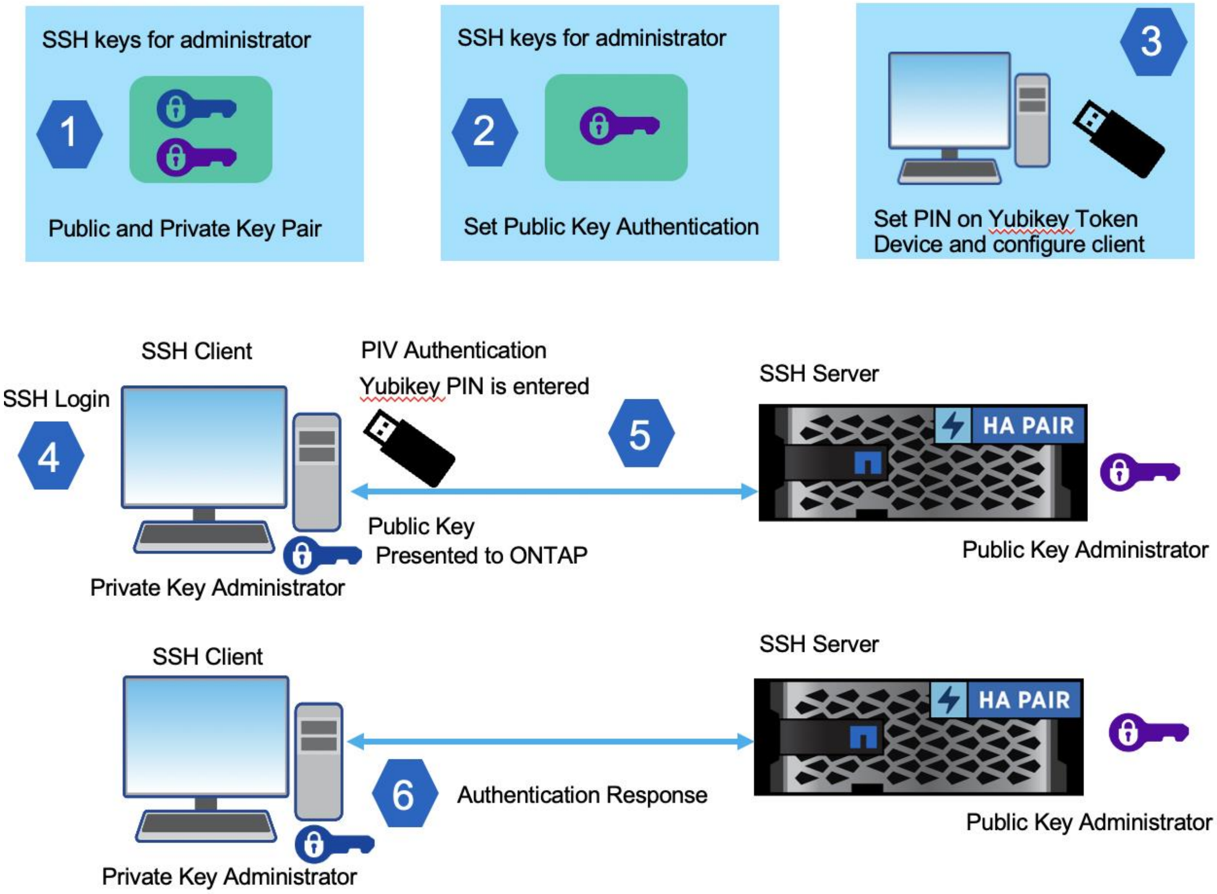
1) An SSH public/private key pair is generated for the administrator.

2) An SSH public key for the administrator is configured in ONTAP as a second authentication method.
   a) Beginning in ONTAP 9.13.1, Time-based-one-time password (TOTP) is a temporary passcode generated by an algorithm that uses the current time of day as one of its authentication factors. TOTP can only be used as secondary authentication method for local users. For more information see the ONTAP documentation.
   b) Also in ONTAP 9.13.1, public key revocation is supported by applying an `-x509-certificate` with the `security login publickey create` command.
3) The administrator invokes an SSH request to ONTAP.
4) Partial authentication is completed with presentation of the administrator public key.
5) ONTAP prompts the administrator for a password, and the administrator provides the password.
6) Full authentication is successful with two factors, and ONTAP presents a command shell.

SSH MFA Access: CLI login with YubiKey using PIV or FIDO2 authentication

Beginning with ONTAP 9.12.1, YubiKey hardware authentication devices that utilize PIV authentication or FIDO2 authentication are supported. The YubiKey hardware device is manufactured by Yubico and provides “strong two-factor, multi-factor and passwordless authentication, and seamless touch-to-sign.” PIV is supported for MFA when using a Personal Identification Number (PIN) on the YubiKey device along with ONTAP `public-key` authentication. FIDO2 is supported for MFA when you use a PIN and have physical access to touch the YubiKey device along with ONTAP `public-key` authentication. Both solutions provide multifactor authentication. This capability works only with ONTAP local accounts.

Figure 3) SSH public-key authentication with YubiKey and PIV for administrative access.



1) The SSH public/private key pair is generated for the administrator.

The SSH public key for the administrator is configured in ONTAP as the authentication method.

The YubiKey PIN is set on a hardware token device and SSH is configured on the client device.

The administrator invokes an SSH request to ONTAP.

The PIN is entered by the administrator for PIV authentication, along with public key authentication to ONTAP.

Full authentication is successful with multiple factors and the user is presented with a command shell from ONTAP.

Terminology

Active Directory Federation Service (ADFS). An identity provider developed by Microsoft. It can run on Windows Server operating systems to give users single sign-on access to systems and applications located across organizational boundaries.

Claim rules. Claim rules provide a mechanism for mapping IdP-defined attributes to a relying party. These attributes—such as a user ID or common name—are used by the relying party to map authorizations after IdP authentication.

Cisco Duo. Cisco Duo is a two-factor authentication solution that helps organizations boost security by verifying user identity, establishing device trust, and providing a secure connection to company networks and applications. For ONTAP integration purposes it functions as an IdP.

Kerberos. A computer network authentication protocol that uses “tickets” to allow nodes communicating over a nonsecure network to prove their identity to one another in a secure manner.

Lightweight Directory Access Protocol (LDAP). An open, vendor-neutral, industry-standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

Multifactor authentication (MFA). A method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism. These pieces of evidence are typically at least two of the following categories: knowledge (something they know—for example, password), possession (something they have—for example, smart card), and inherence (something they are—for example, retinal scan).

National Institute of Standards and Technology (NIST). A measurement standards laboratory and a nonregulatory agency of the U.S. Department of Commerce. Its mission is to promote innovation and industrial competitiveness.

Payment Card Industry Data Security Standard (PCI DSS). A proprietary information security standard for organizations that handle branded credit cards from the major card schemes. The PCI standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. As of February 1, 2018, PCI DSS 3.2 started mandating MFA for all non-console access into the cardholder data environment (CDE) for personnel with administrative access.

Relying party. A system entity that bases an action on information from another system entity. A SAML relying party depends on receiving assertions from an asserting party (a SAML IdP) about a principal or user.

SAML service provider (SAML SP). Any application (either Active IQ Unified Manager or System Manager) that wants to support MFA and offloads the authentication to an external entity (the identity provider).

SAML identity provider (SAML IdP). The external entity or service that handles authentication for the SP and redirects back to the SP on successful verification of the credentials (MFA or not). ADFS and Shibboleth IdP are examples of SAML IdPs.

SAML metadata. Determines how configuration information is defined and shared between two communicating entities. For instance, an entity's support for given SAML bindings, identifier information, and PKI information can be defined.

Security Assertion Markup Language (SAML). An open standard for exchanging authentication and authorization data between parties—in particular, between an identity provider and a service provider. As its name implies, SAML is an XML-based markup language.

Secure Shell (SSH). A command-line cryptographic network protocol for operating network services securely over an unsecured network. SSH version 2 is used with ONTAP.

Shibboleth IdP. Shibboleth is an open-source project that provides single sign-on capabilities. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

Single sign-on (SSO). After a SAML IdP authentication, the IdP issues a SAML assertion, and redirects the administrator's web browser back to System Manager or Active IQ Unified Manager. System Manager or Active IQ Unified Manager processes the SAML assertion, and then looks up the authorization role from its internal database. The session is established, and System Manager or Active IQ Unified Manager returns a SAML session token to the administrator's web browser. The IdP is configured with a default lifetime of 2–8 hours for the secure SAML token. The lifetime is overridable by the relying-party-specific setting. The administrator is allowed access to System Manager or Active IQ Unified Manager for the lifetime of the token.

United States public sector (USPS). As of December 2017, USPS government contractors who process, store, or transmit covered defense information (CDI) are required by Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7008 to comply with the 14 control families of the NIST SP 800-171. Under the "identification and authentication" control family, DFARS specifies use of MFA for local and network access to privileged accounts and for network access to nonprivileged accounts. The intention of the directive is to ensure that the safeguards implemented to protect CDI are consistent across nonfederal information systems as they relate to work contracted by the U.S. government.

Configuration

Beginning in ONTAP 9.3, support is available for MFA configuration. Beginning in ONTAP 9.12.1, support is available for YubiKey utilizing FIDO2 or PIV. For CLI access through SSH to ONTAP, local or Network Information Service (NIS) and Lightweight Directory Access Protocol (LDAP) accounts must be defined in ONTAP. Beginning in ONTAP 9.13.1, Active Directory domain accounts can be used in addition to local or NIS/LDAP accounts.

ONTAP SSH two-factor chained authentication

Existing single-factor authentication (1FA) administrator users can be modified to a two-factor authentication (2FA) login method. There are three methods with two combinations available. The three methods are password, publickey, and nsswitch. The two combinations are password and publickey, or nsswitch and publickey. You can specify either combination for –authentication-method or –second-authentication-method and produce the same result.

As an example, the administrator sam is defined to use the ssh application with the password authentication method. To add public-key authentication as a second method, you use the following command:

```
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.
```

The warning message says that you must enter a public key for `sam` when adding `publickey` as the second authentication method. The Linux OpenSSH/OpenSSL command `ssh-keygen` is used to create an RSA public/private key pair for `sam`. In Linux, the key is stored in `~/.ssh/id_rsa.pub` for `sam`. If `sam` is using the PuTTY client for SSH, you can use the `puttygen` utility to generate a public/private key pair for `sam`. For details on using `ssh-keygen` and `puttygen`, see “Where to find additional information,” later in this document.

To enter the public key for `sam` in ONTAP from the output of `ssh-keygen` from a Linux system, use the following command:

```
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
```

Now `sam` can log in from his Linux system as an ONTAP administrator using chained 2FA. First, public-key authentication is performed (partial success). Then ONTAP prompts `sam` for a password, and the authentication is complete:

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

Note: This example shows a passphrase prompt for access to `sam`’s private key. Linux SSH produces this prompt if a passphrase was applied during `ssh-keygen`. Although it is not necessary to enter a passphrase during `ssh-keygen`, it is a best practice, because it protects access to the private key.

The ONTAP command `security login modify -user-or-group-name sam -application ssh -authentication-method password -second-authentication-method publickey` specifies that `password` is the primary authentication method and `publickey` is the secondary authentication method. These methods can be reversed in the configuration. However, in a 2FA login, the order of authentication is always public key, then password, by means of either local password files or NIS/LDAP passwords.

For more details about SSH MFA authentication, see “Enabling SSH Multifactor Authentication” in the ONTAP 9 Security Guide.

ONTAP SSH MFA authentication with YubiKey And PIV

Existing single-factor authentication (1FA) administrator users can be modified to support MFA login methods by utilizing a YubiKey token device and PIV. YubiKey works by setting `publickey` as either the primary `-authentication-method` or by setting `publickey` as the `-second-authentication-method.` If `-second-authentication-method` is specified, then `password` and `nsswitch` must be set as the primary authentication method.

Note: For hardware-based SSH MFA, the authentication factors in addition to the public key configured in ONTAP are as follows:

- The PIV
- Possession of the YubiKey hardware device

YubiKey PIV Client configuration for Windows

The section describes the general steps to configure the SSH client to support YubiKey for connecting to ONTAP using PIV. The high-level steps for Windows clients are as follows:

1) Download and install the YubiKey Manager.

Initialize the YubiKey by setting the PIV PIN and PUK (PIN Unlock Code).

Generate or import the ECDSA private key and certificate. This is required by the SSH CAPI/PKCS#11 client interface but is not used by ONTAP.

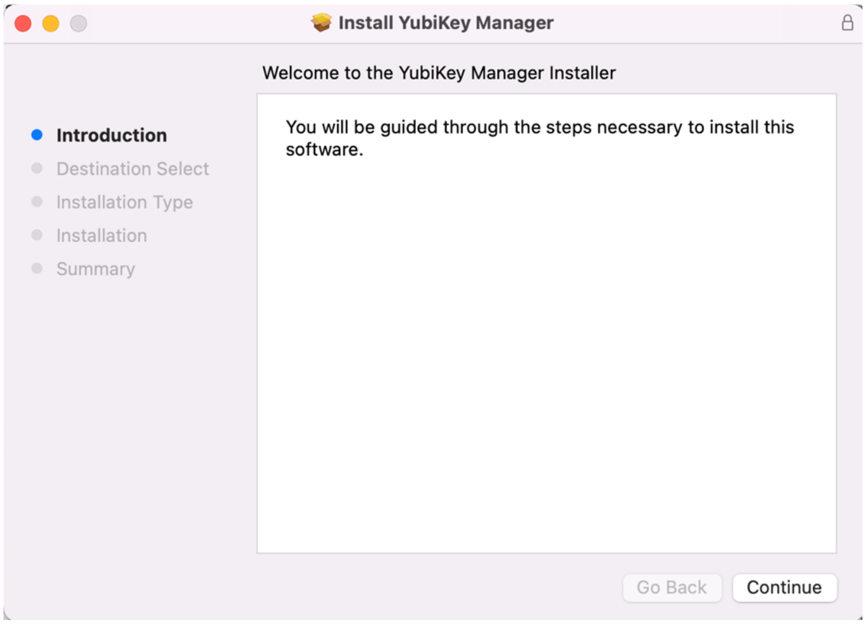
Configure the SSH client to use the CAPI/PKCS#11 interface.

Convert the ECDSA certificate or public key to the SSH-compatible format.

Export the public ECDSA key to ONTAP.

Download and install the YubiKey Manager

1) Download and install the correct version of the YubiKey Manager for your platform from the Yubico website. Select Continue and accept all the defaults:

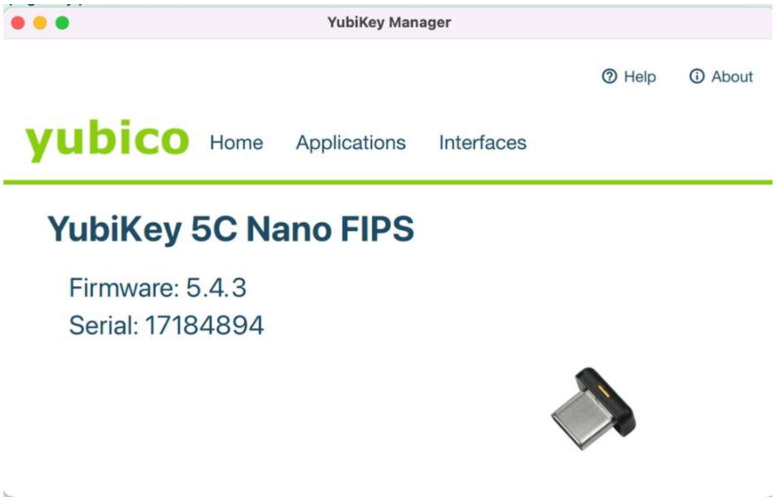


Install YubiKey Manager

Welcome to the YubiKey Manager Installer

You will be guided through the steps necessary to install this software.

After your installation is complete, insert your YubiKey into the USB slot and run the YubiKey Manager. The model, serial number, and firmware version of your YubiKey is displayed on the screen:

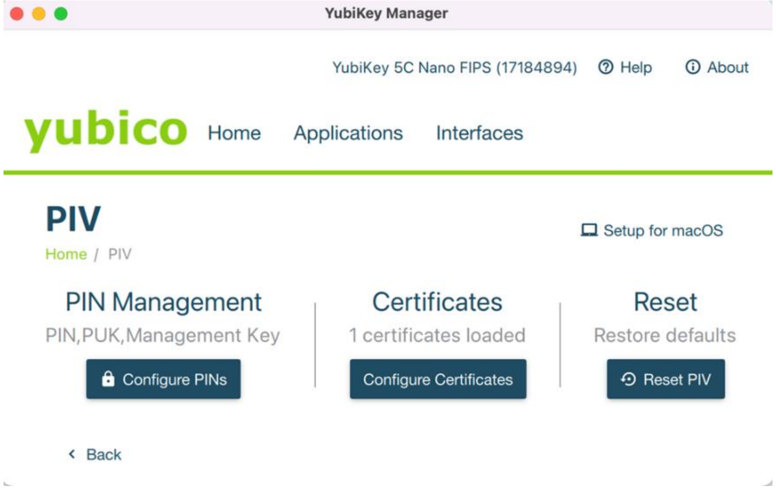


YubiKey 5C Nano FIPS

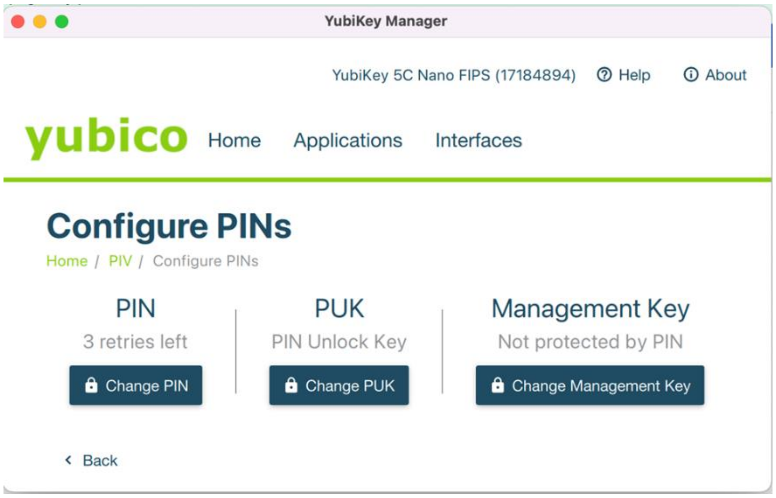
Firmware: 5.4.3
Serial: 17184894

Initialize the YubiKey PIN

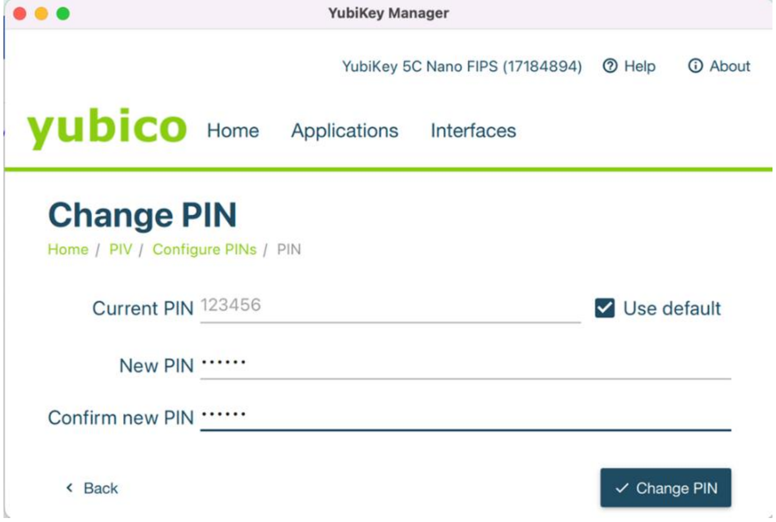
1) Navigate to Applications > PIV to configure the PIV settings. For example:



Select Configure PINs in the PIN Management section. For example:



Select Change PIN to set your PIN. Choose a PIN between 4 to 8 characters long. If you are configuring your YubiKey for the first time, check the Use Default option, otherwise, enter the current PIN. The factory default PIN is 123456. Enter the new PIN twice, then select Change PIN.



Change PIN

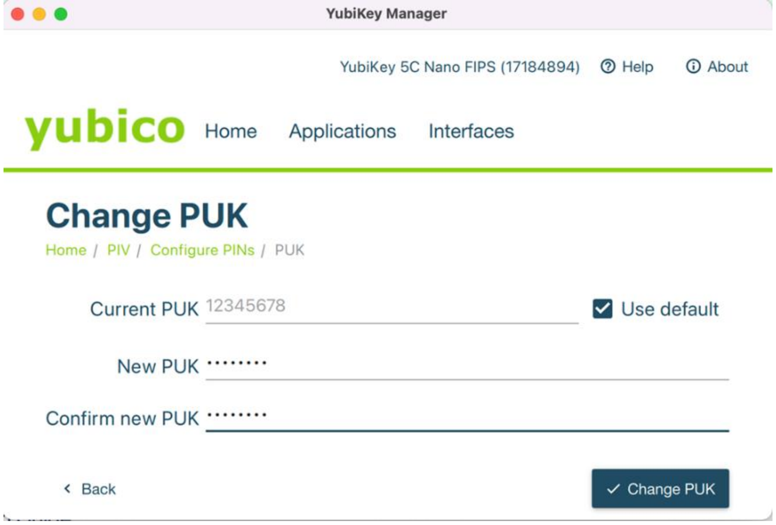
Home / PIV / Configure PINs / PIN

Current PIN 123456 ☑ Use default

New PIN ••••••

Confirm new PIN ••••••

Set the PUK, sometimes called a Personal Unblocking Code (PUC). This is used to reset a PIN that has been lost or forgotten. Choose a PUK between 6 to 8 characters long. If you are configuring your YubiKey for the first time, check the Use Default option, otherwise, enter the current PUK value. The factory default PUK is 12345678. Enter the new PUK twice, then select Change PUK.



Change PUK

Home / PIV / Configure PINs / PUK

Current PUK 12345678 ☑ Use default

New PUK ••••••••

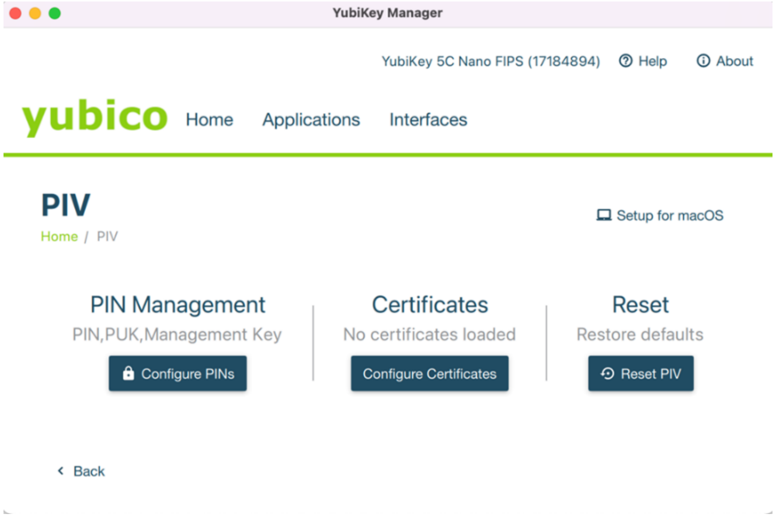
Confirm new PUK ••••••••

Note: It is also recommended to change your Management Key. The default 3DES management key is 010203040506070801020304050607080102030405060708. More information about the PIN, PUK and Management Key can be found on the Yubico website.

Import or generate the private key and certificate

To use the YubiKey for PIV authentication over SSH, you must either import or generate a private ECDSA key and certificate. ONTAP 9.12.1 and later uses ECDSA-256 or ECDSA-384 keys for SSH public key authentication. The following example uses ECDSA-384. The certificate is not used by the ONTAP SSH server, only the public key in the certificate is used.

1) Slot 9a in the YubiKey is used to store the PIV key. Select Configure Certificates:

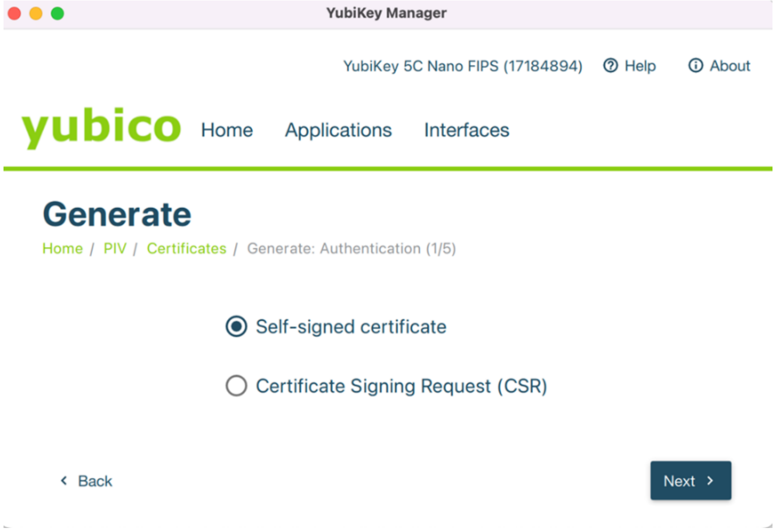


a) Select Generate to proceed. In this example, the ECDSA private/public key pair is generated using the P-384 curve.

Select Self-signed Certificate. In this example, a self-signed certificate is generated because the certificate is not used by ONTAP and only required by the PKCS#11 interface.

Note: Depending on your deployment, you might need to generate a certificate signing request (CSR) ahead of time, have it signed by your trusted CA, and then import the signed certificate.

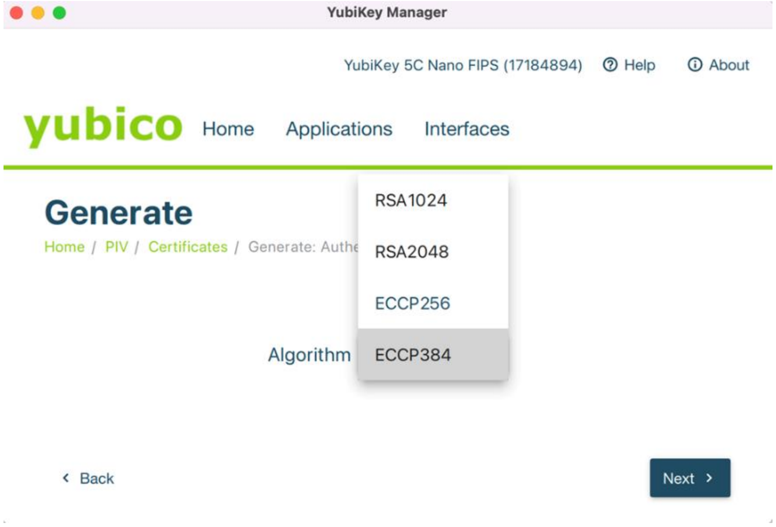
After you have selected Self-signed Certificate, select Next:


YubiKey Manager
YubiKey 5C Nano FIPS (17184894)
Help
About
yubico
Home
Applications
Interfaces
Generate
Home / PIV / Certificates / Generate: Authentication (1/5)
Back
Next

● Self-signed certificate

○ Certificate Signing Request (CSR)

Select ECCP-384 for the algorithm and then select Next:

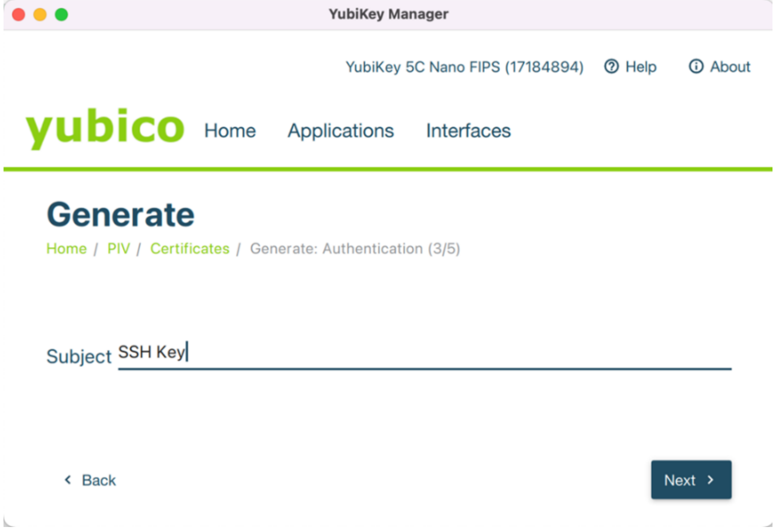


Generate

Home / PIV / Certificates / Generate: Authe

Algorithm ECCP384

Enter a string for the Subject (CN). This example sets it to SSH Key:

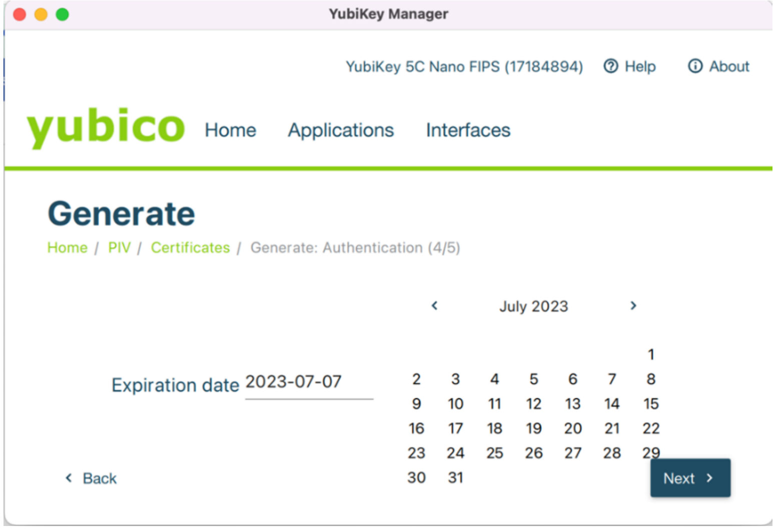


Generate

Home / PIV / Certificates / Generate: Authentication (3/5)

Subject SSH Key

Select Next. The next screen asks for the expiration date of the certificate, which is set to one year by default. This does not apply to SSH, so you can accept the default:



Expiration date 2023-07-07

The last dialog box displays the options you have chosen. Select Generate to confirm your choices.

You are asked for the management key to proceed. Enter the management key if it has changed, select Use Default if it is still set to the factory default setting.

You are asked for the PIN. Enter the PIN you configured in the initialization step, and select OK:

> **Note:** Your private key and certificate are generated, and the relevant information is displayed in the Certificates section

Configure the Windows PuTTY-CAC SSH Client for YubiKey PIV Authentication

A simple way to connect to ONTAP over SSH using public key authentication with YubiKey PIV is to use PuTTY-CAC. PuTTY-CAC is an open source SSH client that supports smart card authentication, particularly using the Department of Defense Common Access Card (CAC) and PIV as a PKI token. It is widely used in federal deployments.

You can download and install PuTTY-CAC from GitHub: https://github.com/NoMoreFood/putty-cac/releases

The high-level PuTTY-CAC configuration steps are as follows:

1) Install the Yubico PIV Tool. This contains Yubico’s version of the PKCS#11 library ("YKCS11") that is needed to interact with the YubiKey.

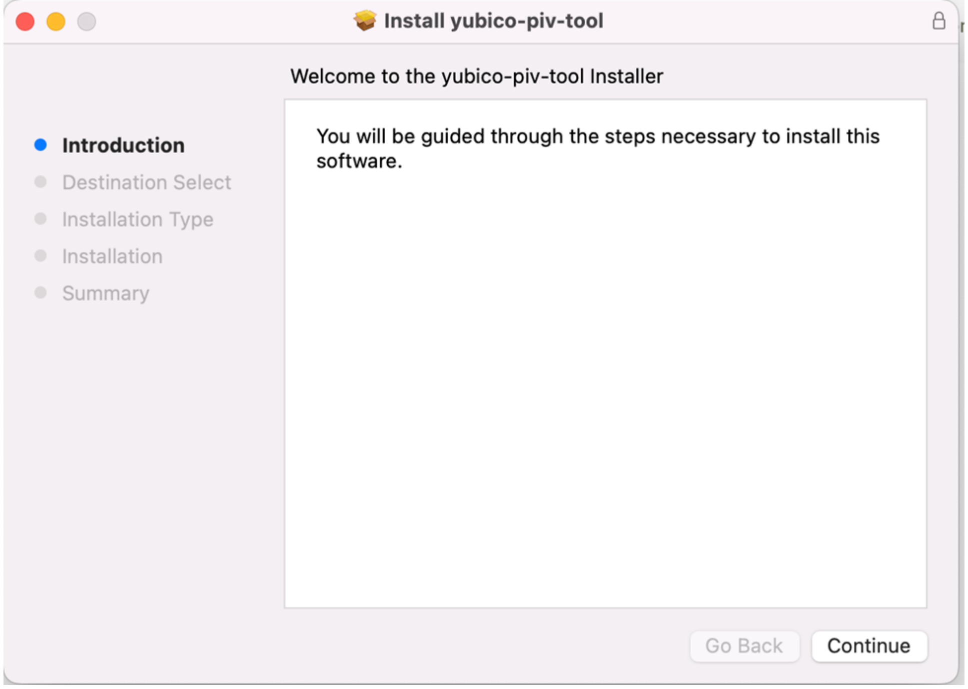
Configure the certificate from the YubiKey using the PKCS#11 library.

Copy the SSH-compatible ECDSA or RSA public key to the clipboard and save it.

Configure the PuTTY session host.

Install the Yubico PIV Tool

Obtain and install the Yubico PIV-tool for your platform from https://developers.yubico.com/yubico-piv-tool/Releases/. Accept all the defaults. For example:



Install yubico-piv-tool

Welcome to the yubico-piv-tool Installer

You will be guided through the steps necessary to install this software.

Configure the PKCS#11 Certificate that came from your YubiKey

1) Start PuTTY-CAC.

At the PuTTY connection window, navigate to Connection > SSH > Certificate.

Select Set PKCS#11 Cert

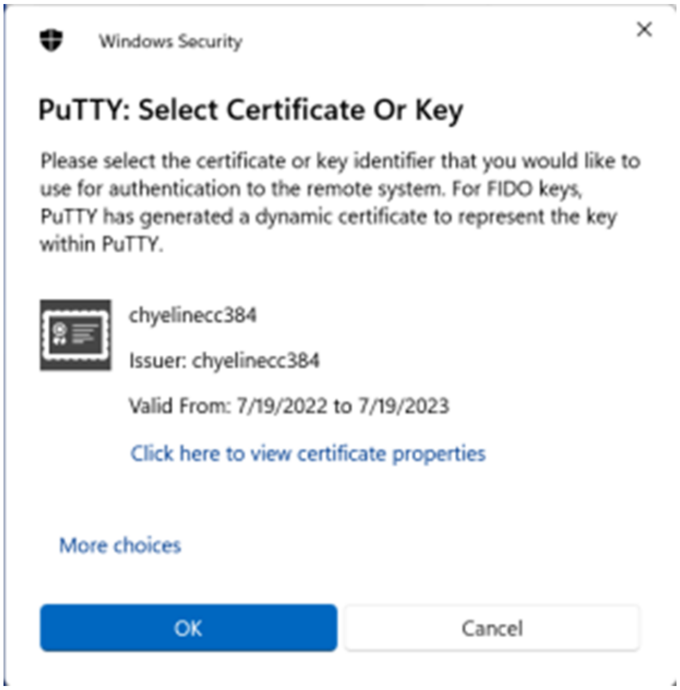
Specify your Yubico PKCS#11 library.

If this is installed on a 64-bit Windows 10/11 client using all the defaults, this library is located in: `C:\Program Files\Yubico\Yubico PIV Tool\bin\libykcs11.dll`.

Select and open the file.

If you have successfully generated your ECDSA key and the certificate for your YubiKey as indicated in the previous step, that certificate is displayed.

Check the CN and Issuer to make sure that this is the certificate you previously generated and select OK to continue.



PuTTY: Select Certificate Or Key

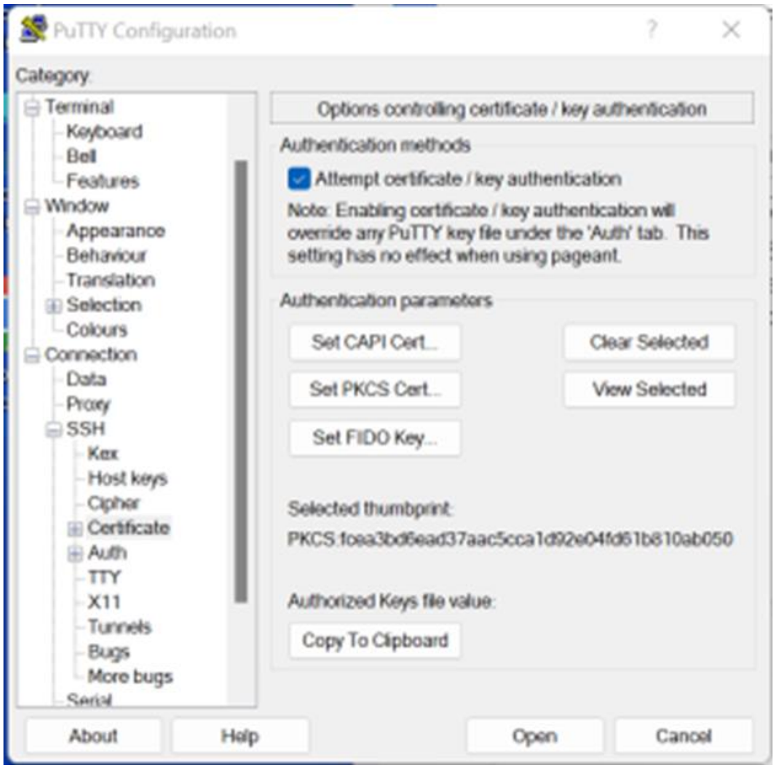
Please select the certificate or key identifier that you would like to use for authentication to the remote system. For FIDO keys, PuTTY has generated a dynamic certificate to represent the key within PuTTY.

chyelinecc384

Issuer: chyelinecc384

Valid From: 7/19/2022 to 7/19/2023

You are brought back to the Authentication methods dialog box. If the configuration is successful, you see the fingerprint of the selected certificate.



☑ Attempt certificate / key authentication

Note: Enabling certificate / key authentication will override any PuTTY key file under the 'Auth' tab. This setting has no effect when using pageant.

Selected thumbprint:
PKCS:foea3bd6ead37aac5cca1d92e04fd61b810ab050

Copy the SSH compatible ECDSA public key to the clipboard

1) Select Copy to Clipboard to copy the SSH-compatible public key to your clipboard.

   You must configure your ONTAP user with this public key in the next step.

The SSH-compatible public key retrieved from the YubiKey via the PKCS#11 library is in the following format:

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

Example of a public key:

```
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
```

Set the public key authentication mechanism for the ONTAP user account. After the ONTAP account is configured and associated with the public key you can use an SSH client such as Putty to manage the ONTAP system.

See the section “Configure public key authentication for YubiKey PIV in ONTAP” for the next steps.

YubiKey PIV client configuration For MAC OS and Linux

This section describes the general steps to configure the SSH client to support YubiKey for connecting to ONTAP using PIV. The high-level steps for Mac OS and Linux clients are as follows:

1) Download and install the YubiKey Manager.

Initialize the YubiKey by setting the PIV, PIN and PUK

Generate or import the ECDSA private key and certificate. This is required by the SSH CAPI/PKCS#11 client interface but is not used by ONTAP.

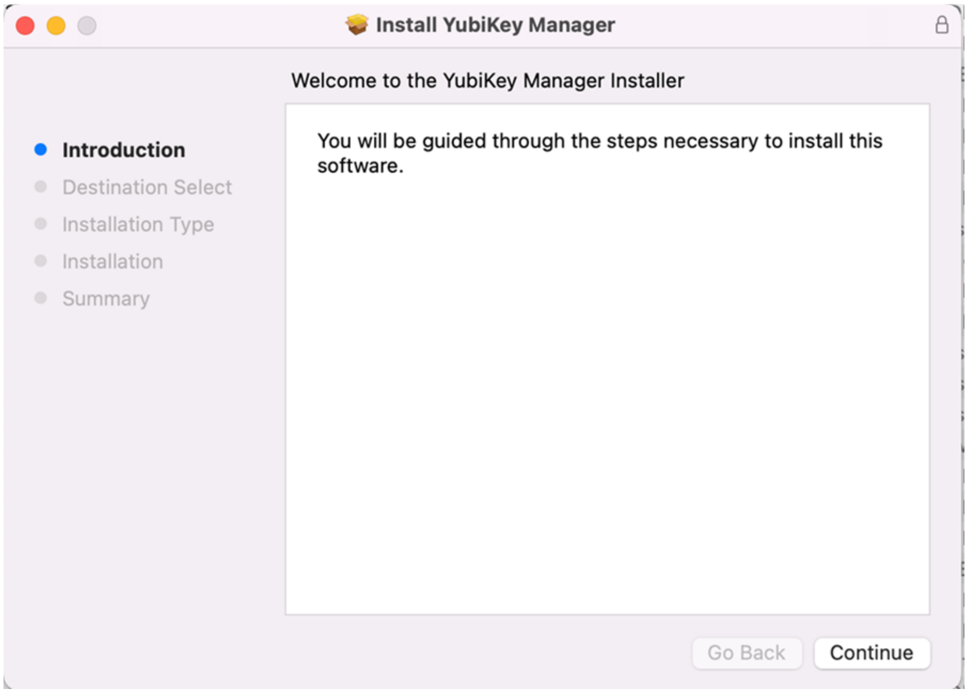
Configure the SSH client to use the CAPI/PKCS#11 interface.

Convert the ECDSA certificate or public key to the SSH-compatible format.

Export the public ECDSA key to ONTAP.

Download and install the YubiKey Manager

1) Download and install the correct version of the YubiKey Manager for your platform from the Yubico website. Select Continue and accept all the defaults. For example:

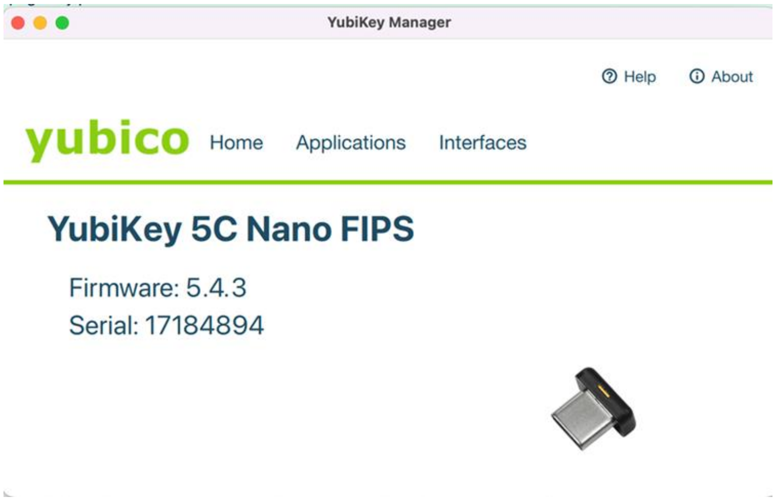


Install YubiKey Manager

Welcome to the YubiKey Manager Installer

You will be guided through the steps necessary to install this software.

After your installation is complete, insert your YubiKey into the USB slot, then run the YubiKey Manager. The model, serial number, and firmware version of your YubiKey is displayed on the screen:



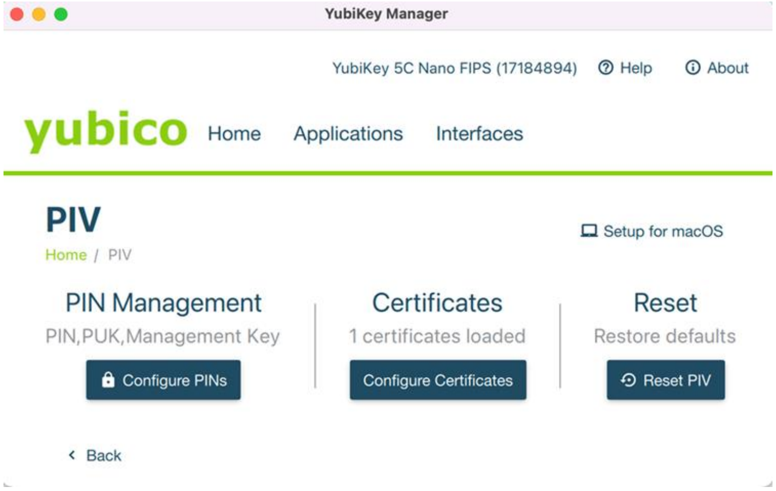
YubiKey 5C Nano FIPS

Firmware: 5.4.3

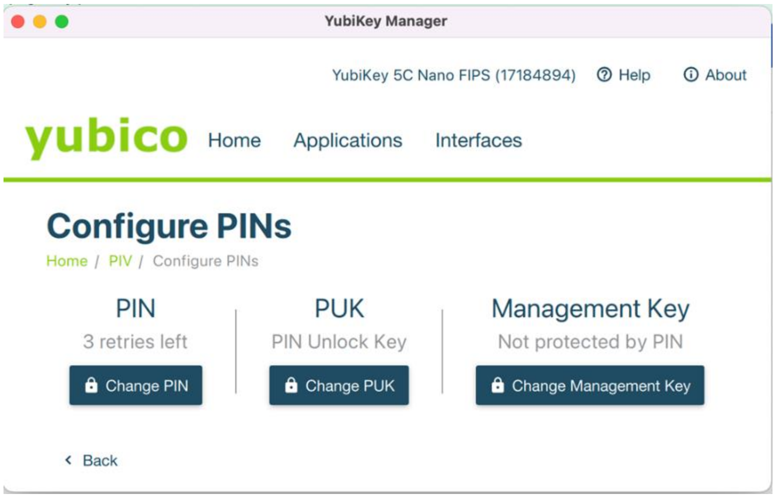
Serial: 17184894

Initialize the YubiKey PIN

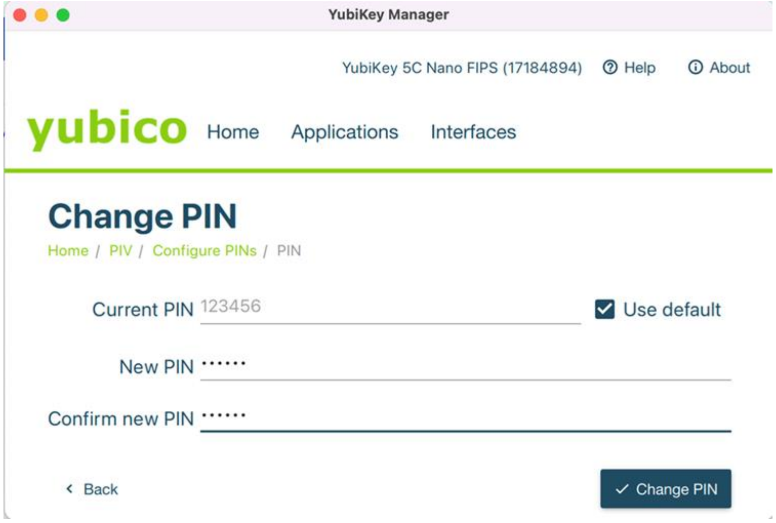
1) Go to Applications > PIV to configure the PIV settings. For example:



Click Configure PINs in the PIN Management section. For example:



Select Change PIN to set your PIN. Choose a PIN between 4 to 8 characters long. If you are configuring your YubiKey for the first time, check the Use Default option, otherwise, enter the current PIN. The factory default PIN is 123456. Enter the new PIN twice and select Change PIN.

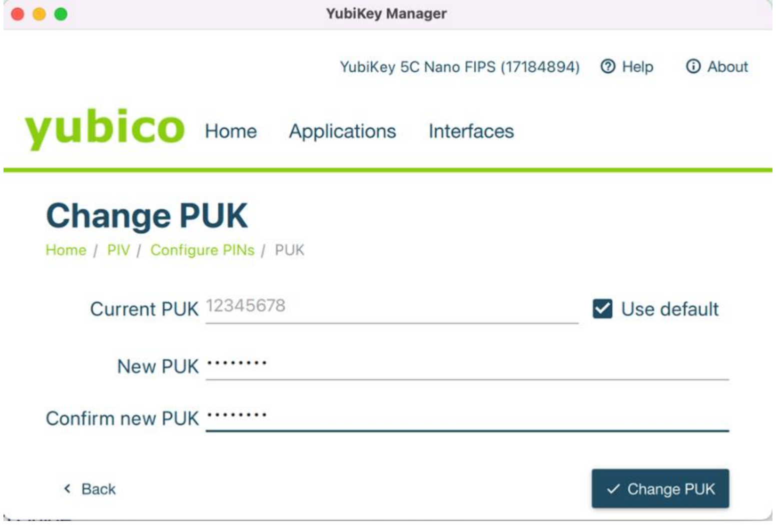


Current PIN 123456 ☑ Use default

New PIN ••••••

Confirm new PIN ••••••

Set the PUK, sometimes called a PUC. This is used to reset a PIN that has been lost or forgotten. Choose a PUK between 6 to 8 characters long. If you are configuring your YubiKey for the first time, check the Use Default option, otherwise, enter the current PUK value. The factory default PUK is 12345678. Enter the new PUK twice and select Change PUK.



Current PUK 12345678 ☑ Use default

New PUK ••••••••

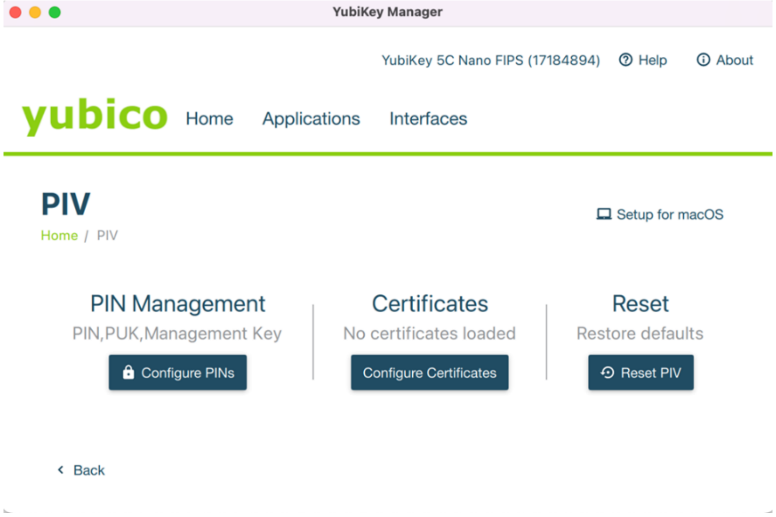
Confirm new PUK ••••••••

Note: It is also recommended to change your Management Key. The default 3DES management key is 010203040506070801020304050607080102030405060708. More information about the PIN, the PUK and Management Key can be found on the Yubico website.

Import or generate the private key and certificate

To use the YubiKey for PIV authentication over SSH, you must either import or generate a private ECDSA key and certificate. ONTAP 9.12.1 and later uses ECDSA-256 or ECDSA-384 keys for SSH public key authentication. The following example uses ECDSA-384. The certificate is not used by the ONTAP SSH server, only the public key in the certificate is used.

1) Slot 9a in the YubiKey is used to store the PIV key. Select Configure Certificates:



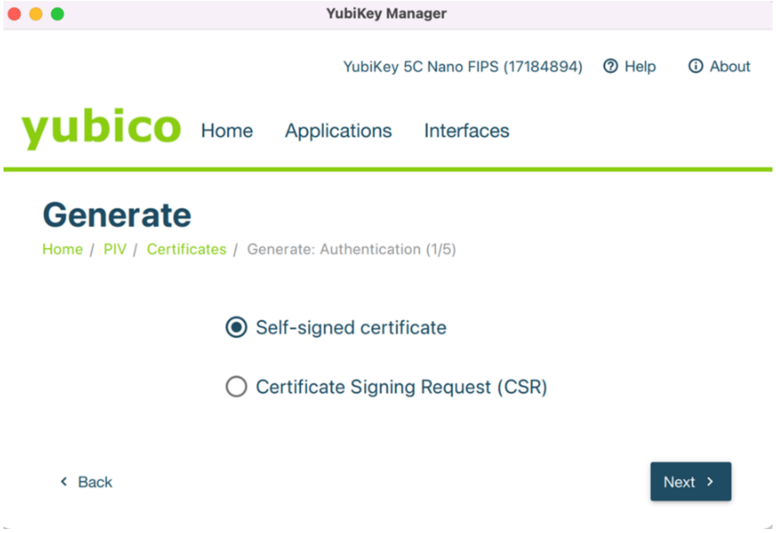
No certificates loaded

a) Select Generate to proceed. In this example the ECDSA private/public key pair is generated using the P-384 curve.

2) Select Self-signed certificate. In this example, a self-signed certificate is generated because the certificate is not used by ONTAP and only required by the PKCS#11 interface.

Note: Depending on your deployment, you might need to generate a CSR ahead of time, have it signed by your trusted CA, and then import the signed certificate.

After the Self-signed Certificate is selected, select Next:



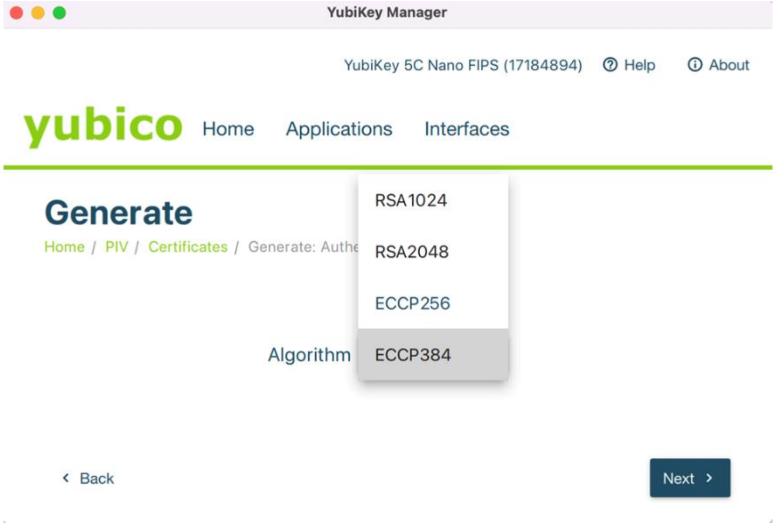
Generate

Home / PIV / Certificates / Generate: Authentication (1/5)

● Self-signed certificate

○ Certificate Signing Request (CSR)

Select ECCP-384 for the algorithm and then select Next:

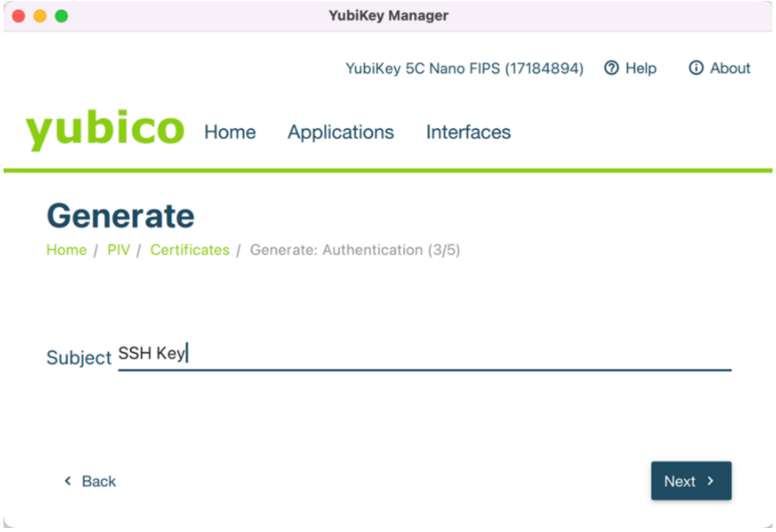


Generate

Home / PIV / Certificates / Generate: Authe

Algorithm ECCP384

Enter a string for the Subject (CN). This example sets it to SSH Key:

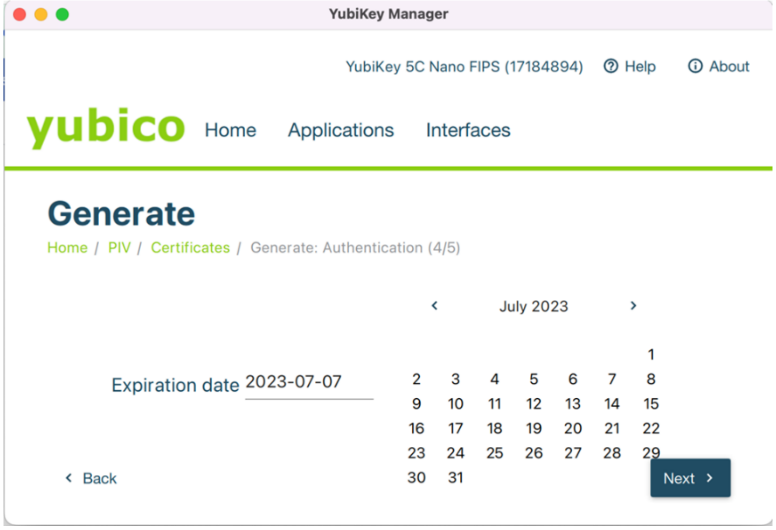


Generate

Home / PIV / Certificates / Generate: Authentication (3/5)

Subject: SSH Key

Select Next. The next screen asks for the expiration date of the certificate, which is set to one year by default. This does not apply to SSH, so you can accept the default:



Generate

Home / PIV / Certificates / Generate: Authentication (4/5)

Expiration date: 2023-07-07

The last dialog box displays the choices you selected. Select Generate to confirm your choices.

You are asked for the management key to proceed. Enter the management key if it has changed, select Use Default if it is still set to the factory default setting.

You are asked for the PIN. Enter the PIN you configured in the initialization step and select OK.

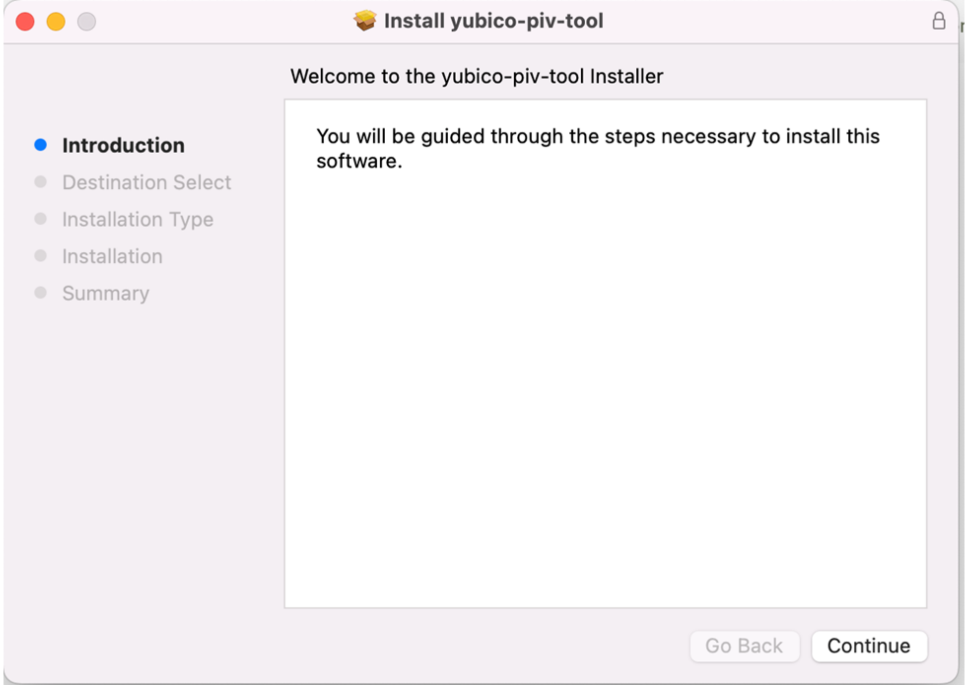
Your private key and certificate are generated, and the relevant information is displayed in the Certificates section.

Configure the Mac OS or Linux SSH Client for YubiKey PIV authentication

Install the Yubico PIV Tool

You can download the Yubico PIV Tool from the Yubico Smart Card Drivers and Tools page.

1) Click the package file to install it. Accept all the default options to complete the installation:


Install yubico-piv-tool
Welcome to the yubico-piv-tool Installer
Introduction
Destination Select
Installation Type
Installation
Summary
You will be guided through the steps necessary to install this software.
Go Back
Continue

After successful installation, the Yubico PKCS#11 library required for the SSH client can be found in the following location: `/usr/local/lib/libykcs11.dylib`.

Export the ECDSA key

To use the RSA or ECDSA key you generated in your YubiKey for SSH, you must convert it to a format recognized by SSH.

1) To do this, use `ssh-keygen` with the Yubico PKCS#11 module, `libykcs11.dylib`.

   Note: For Unix installations, this library has the `.so` extension.

   To do this, use `ssh-keygen` with the Yubico PKCS#11 library and the `-e` option to export the ECDSA key to an SSH-compatible format.

   Example output:

```
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
```

Choose the entry tagged `ecdsa-sha2-nistp384` with the following description: `Public key for PIV Authentication`. You must configure your ONTAP user with this public key in the next step.

Configure the SSH client to use the Yubico PKCS#11 library

You must also configure the SSH client to use the Yubico PKCS#11 library.

For Linux and MAC, this involves creating a new entry with the PKCS11Provider option in file `~/.ssh/config` for the given user and host.

In the following example, a custom configuration entry is created for the user `newadmin` for the ONTAP host `vsim1.sim.netapp.com`, so that invoking SSH newadmin@vsim1.sim.netapp.com will use the PKCS#11 library `/usr/local/lib/libykcs11.dylib` configured in the PKCS11Provider option.

```
% 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
```

The next step is to set the public key authentication mechanism for the ONTAP user account. After the ONTAP account is configured and associated with the public key you can use an SSH client such as Putty to manage the ONTAP system.

For next steps, see the section Configure public key authentication for YubiKey PIV in ONTAP".

Configure public key authentication for YubiKey PIV in ONTAP

In this example, a new admin user with the username `newadmin` is created using SSH, with the authentication method being set to `publickey`. The command used is the same whether the authentication method is the standard SSH public key authentication or YubiKey PIV authentication.

```
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.
```

The warning message says that you must enter a public key for `newadmin` when adding `publickey` as the authentication method. This public key is obtained when you configure the YubiKey device on the client.

Next, set the PIV public key you configured for your YubiKey. The public key is obtained from the Copy to Clipboard function for PuTTY-CAC for PIV, from Windows, or from exporting the public key in an SSH-compatible format using `ssh-keygen -e` for PIV for MacOS.

Example output:

```
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"
```

Now `newadmin` can log in from the client system as an ONTAP administrator using YubiKey and PIV for multifactor authentication.

For more details on SSH MFA authentication, see "Enabling SSH Multifactor Authentication" in the ONTAP 9 Security Guide.

ONTAP SSH MFA authentication with YubiKey and FIDO2

Existing single-factor authentication (1FA) administrator users can be modified to support MFA login methods utilizing a YubiKey token device and FIDO2 authentication. YubiKey works by setting `publickey` as either the primary `-authentication-method` or by setting `publickey` as the `–second-authentication-method`. If `-second-authentication-method` is specified, then `password` and `nsswitch` must be set as the primary authentication method.

Note: For hardware-based SSH MFA, the authentication factors in addition to the public key configured on the ONTAP are as follows:

- FIDO2 PIN
- Possession of the YubiKey hardware device. For FIDO2, this is confirmed by physically touching the YubiKey during the authentication process.

YubiKey FIDO2 client configuration for Windows

This section describes the general steps to configure the SSH client to support YubiKey for connecting to the ONTAP using FIDO2. The high-level steps for Windows clients are as follows:

1) Download and install the YubiKey Manager.

Initialize the YubiKey by setting the FIDO2 PIN.

Generate the private/public `ecdsa-sk` or `edd519-sk` key pair using PuTTY-CAC (Windows) or `ssh-keygen` (MAC).

Convert the `ecdsa-sk` or `edd519-sk` public key to the SSH-compatible format if necessary.

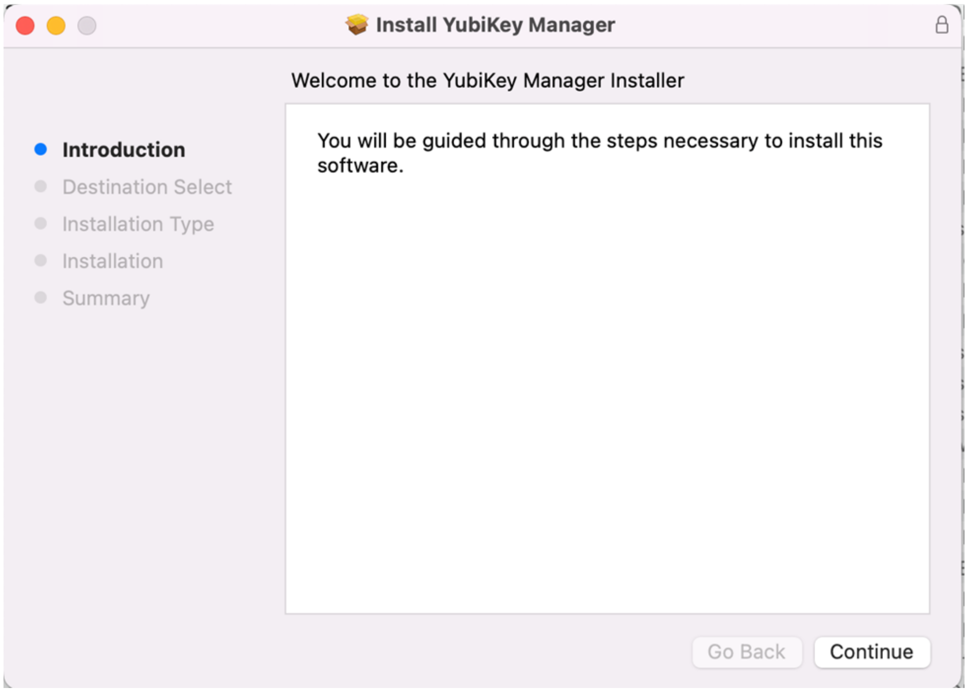
Configure the ONTAP user to use the public key authentication method.

Export the `ecdsa-sk` or `edd519-sk` public key to the ONTAP.

Download and install the YubiKey Manager

Download and install the correct version of the YubiKey Manager for your platform from the Yubico website.

1) Click Continue and accept all the default values. For example:

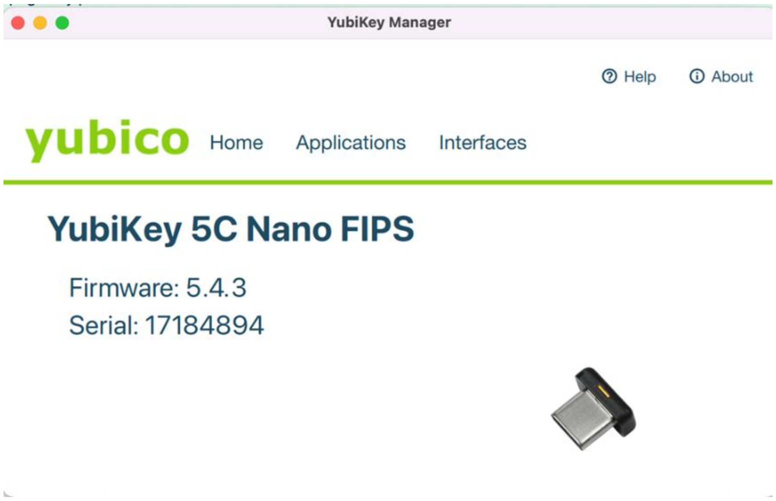


Welcome to the YubiKey Manager Installer

- Introduction
- Destination Select
- Installation Type
- Installation
- Summary

You will be guided through the steps necessary to install this software.

After your installation is complete, insert your YubiKey into the USB slot, then run the YubiKey Manager. The model, serial number, and the firmware version of your YubiKey is displayed on the screen:



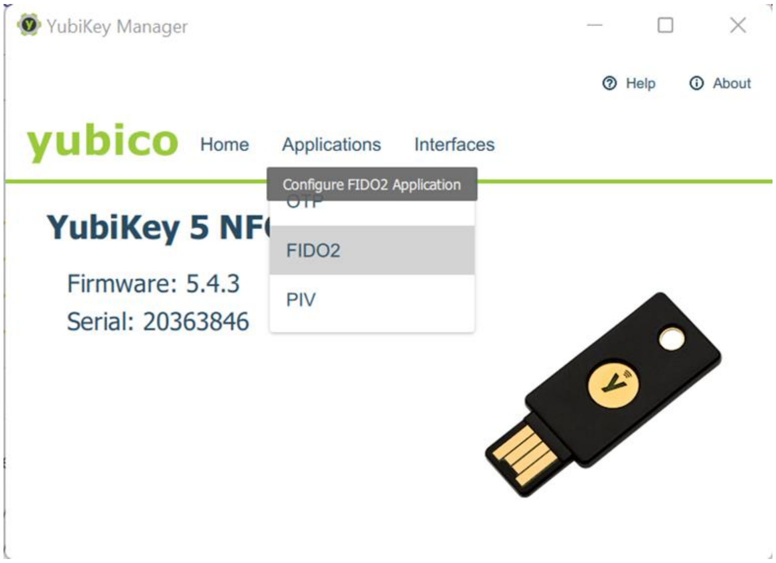
YubiKey 5C Nano FIPS

Firmware: 5.4.3

Serial: 17184894

Initialize the YubiKey PIN

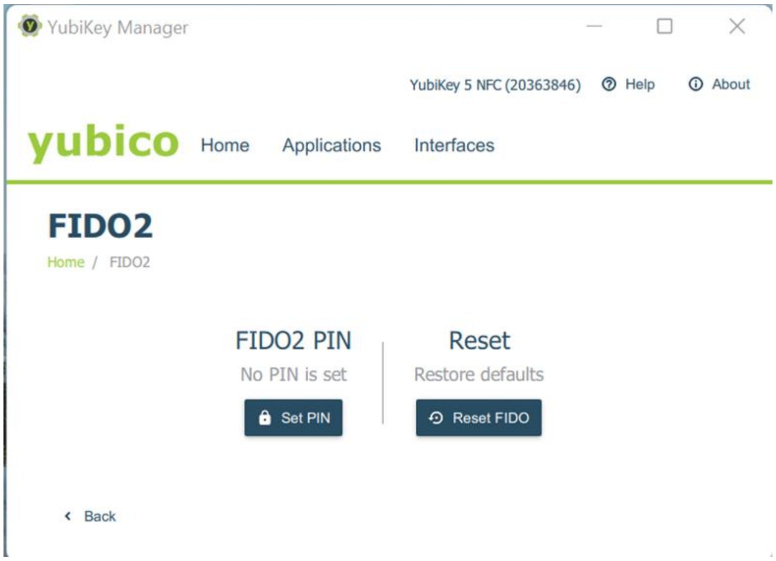
1) Go to Applications > FIDO2 to configure the FIDO2 settings. For example:



YubiKey 5 NFC

Firmware: 5.4.3

Serial: 20363846



FIDO2

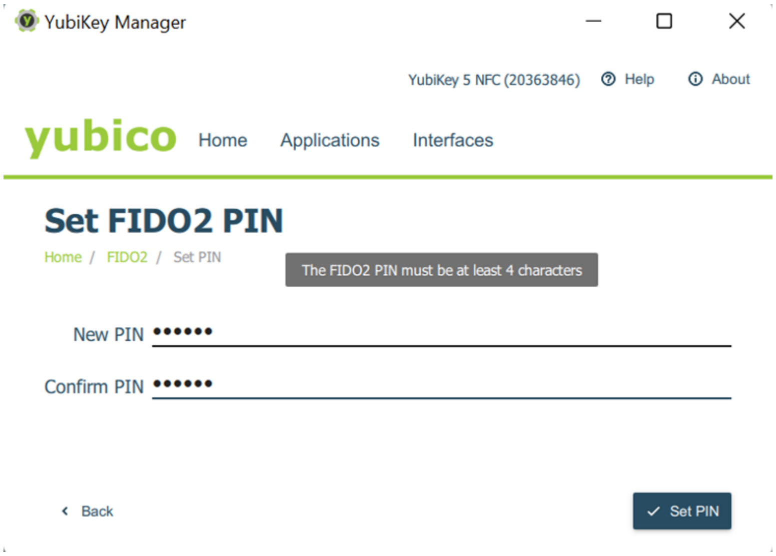
FIDO2 PIN

No PIN is set

Reset

Restore defaults

The Set FIDO2 PIN dialog box appears and asks you to set the FIDO2 PIN. Enter a PIN of at least 4 characters in the New PIN field. Then enter the same PIN again in the Confirm PIN field. Select Set PIN to set the FIDO2 PIN:



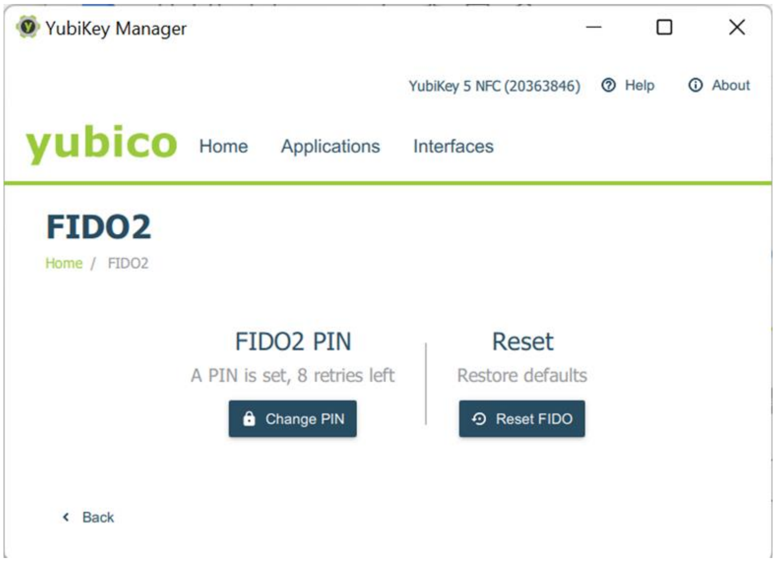
Set FIDO2 PIN

The FIDO2 PIN must be at least 4 characters

New PIN ••••••

Confirm PIN ••••••

You are brought back to the FIDO2 dialog box confirming that your PIN has been set.



FIDO2

FIDO2 PIN

A PIN is set, 8 retries left

Reset

Restore defaults

For more information about the YubiKey FIDO2 configuration, see the Yubico website.

Configure the Windows PuTTY-CAC SSH client for YubiKey FIDO2 authentication

To use the YubiKey for FIDO2 authentication over SSH, you must generate a public/private ECDSA key pair. FIDO devices are supported by the public key types `ecdsa-sk` and `ed25519-sk`, along with corresponding certificate types:

- The `ed25519-sk` is stronger than `ecdsa-sk` mathematically but is not widely supported yet.
- The `ed25519-sk` is only supported by YubiKey with firmware versions 5.2.3 or later.
- The `ecdsa-sk` key type uses ECDSA which is supported for compatibility purposes.

For ONTAP 9.12.1 and later, use ECDSA-256 or ECDSA-384 keys for SSH public key authentication.

A simple way to connect to ONTAP over SSH using public key authentication with YubiKey PIV is to use PuTTY-CAC. PuTTY-CAC is an open source SSH client that supports smart card authentication, particularly using the Department of Defense CAC and PIV as a PKI token—it is widely used in federal deployments.

You can download it from GitHub here: https://github.com/NoMoreFood/putty-cac/releases.

1) Install PuTTY-CAC

Start your Putty-CAC on your Windows client.

Note: To create keys on the YubiKey hardware token, the PuTTY-CAC must be run as Administrator.

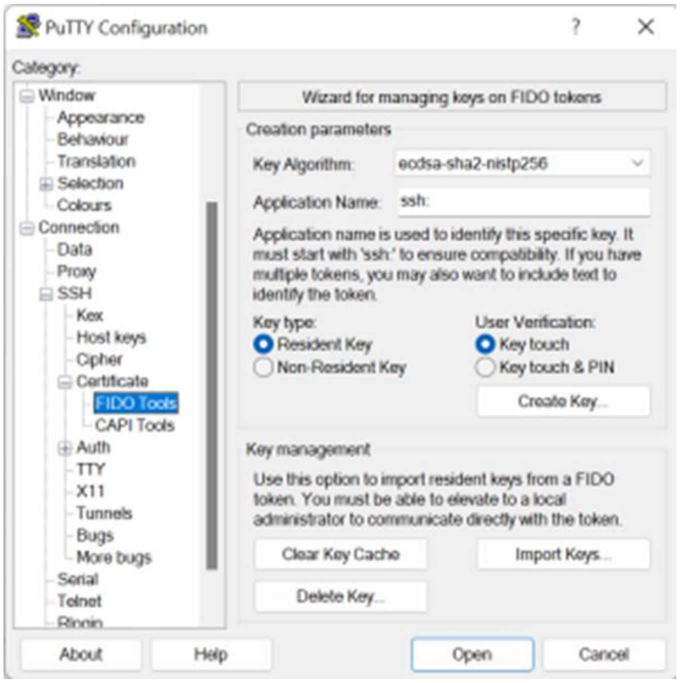
In the PuTTY Configuration dialog box, go to Connection SSH > Certificate > FIDO Tools. Accept all the default values except for the Application Name and User Verification.

Create the FIDO2 private/public key pair using the `ecdsa-sha2-nistp256` key algorithm.

Enter a string after the ssh: in the Application Name field to identify the application. This example uses `ontap1`.

Enter the key type as Resident key to store it on the YubiKey device.

Change the User Verification from Key touch to Key touch and PIN, so that the user will need to enter the PIN in addition to touching the YubiKey.



PuTTY Configuration

Wizard for managing keys on FIDO tokens

Creation parameters

Key Algorithm: ecdsa-sha2-nistp256

Application Name: ssh:

Application name is used to identify this specific key. It must start with 'ssh:' to ensure compatibility. If you have multiple tokens, you may also want to include text to identify the token.

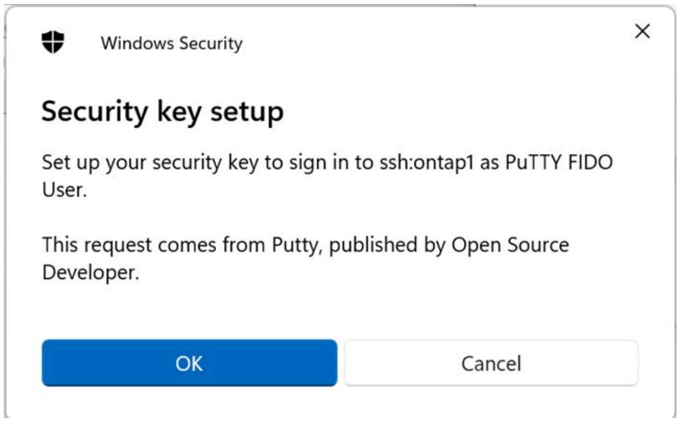
Key type: ● Resident Key ○ Non-Resident Key

User Verification: ● Key touch ○ Key touch & PIN

Key management

Use this option to import resident keys from a FIDO token. You must be able to elevate to a local administrator to communicate directly with the token.

Select Create Key. The Security Key Setup dialog box is displayed. Select OK:


Windows Security

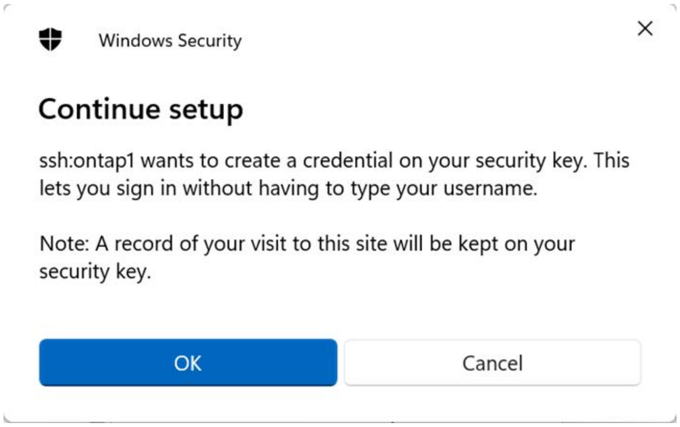
Security key setup

Set up your security key to sign in to ssh:ontap1 as PuTTY FIDO User.

This request comes from Putty, published by Open Source Developer.

The Continue Setup Confirmation dialog box asks you to confirm whether you want to create a credential on your YubiKey device. Select OK.

Install the Yubico PIV Tool

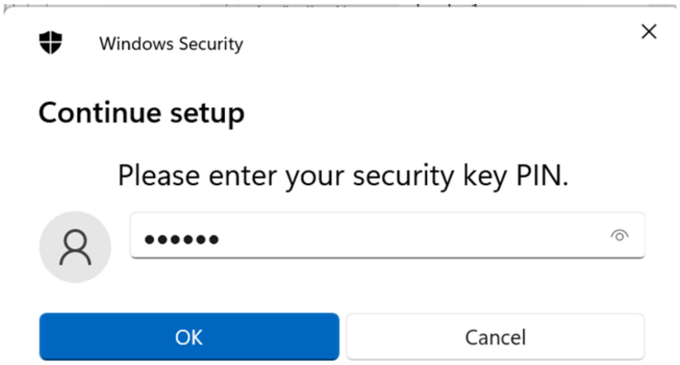

Windows Security

Continue setup

ssh:ontap1 wants to create a credential on your security key. This lets you sign in without having to type your username.

Note: A record of your visit to this site will be kept on your security key.

1) Enter the FIDO2 PIN you previously configured to continue setup. Select OK.


Windows Security

Continue setup

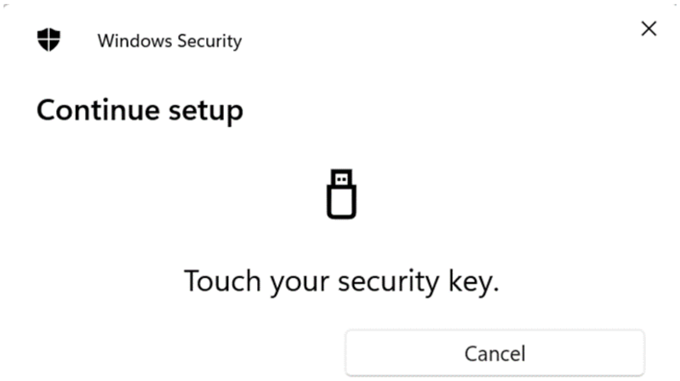
Please enter your security key PIN.

••••••

You see a dialog box asking you to touch your YubiKey. If this step fails, it is most likely that your PuTTY-CAC was run as a regular user account instead of as Administrator.

The YubiKey device starts flashing.

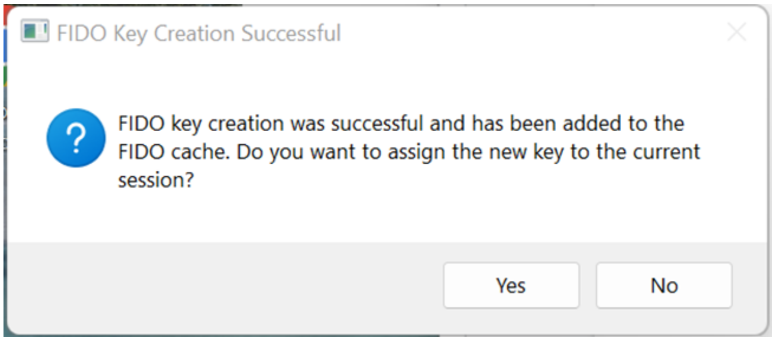
Touch the YubiKey:



Continue setup

Touch your security key.

If the key creation is successful, you see a dialog box indicating that the FIDO key creation is successful and that the key has been added to the FIDO cache. To use the key for your SSH session, assign the new key to the current session. Select Yes to proceed.



FIDO key creation was successful and has been added to the FIDO cache. Do you want to assign the new key to the current session?

You can now continue with the rest of the PuTTY-CAC configuration. If you plan to configure the SSH connection to ONTAP in this session, you can skip the next section Import FIDO2 Keys from YubiKey to PuTTY-CAC and proceed to the Configure the PuTTY-CAC Client SSH session section.

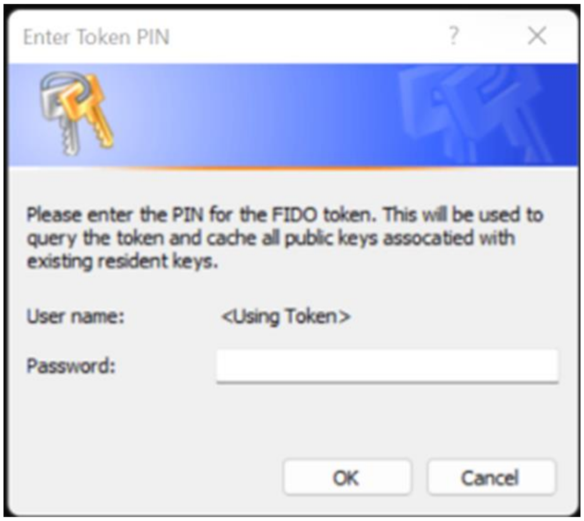
Import FIDO2 Keys from YubiKey to PuTTY-CAC

If you are not yet ready to continue with the session configuration immediately after creating the FIDO2 key on your YubiKey, you can use the PuTTY-CAC key management import feature to import the FIDO2 keys from the YubiKey to PuTTY-CAC in subsequent sessions.

1) From the main PuTTY configuration dialog box, navigate to Connection > Certificate > FIDO Tools and select Import Keys from the Key Management section.

   This invokes the puttyimp application from PuTTY-CAC.

You are asked to enter your FIDO2 PIN to proceed. Enter your FIDO2 PIN into the Password field.

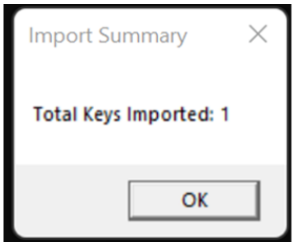

Enter Token PIN

Please enter the PIN for the FIDO token. This will be used to query the token and cache all public keys assocatied with existing resident keys.

User name: <Using Token>

Password:

If the key import works successfully, you receive a confirmation message. For example:


Import Summary

Total Keys Imported: 1

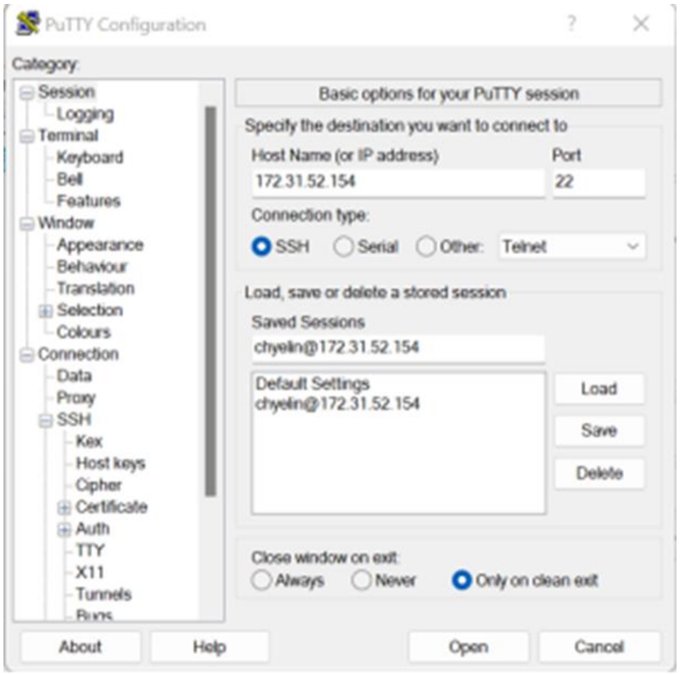
After importing the key, proceed to the next section Configure the PuTTY-CAC Client SSH session.

Configure the PuTTY-CAC Client SSH session

The next step is to configure the client SSH session.

You do this in the same way as you do for a regular PuTTY session. Before starting the session configuration, make sure that you have either generated your FIDO2 private/public key pair as described above in the same session, or that you have imported your FIDO2 as described in Import FIDO2 Keys from YubiKey to PuTTY-CAC.

1) Select the Session tab. Enter the host name or IP Address of your ONTAP server. Enter a name in the Saved Sessions dialog box and select Save to save your configuration:



Specify the destination you want to connect to

Host Name (or IP address): 172.31.52.154

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions: chyelin@172.31.52.154

Default Settings
chyelin@172.31.52.154

Close window on exit: ○ Always ○ Never ● Only on clean exit

You are now ready to export the FIDO2 public key so that you can use it to configure public key authentication for the ONTAP CLI User.

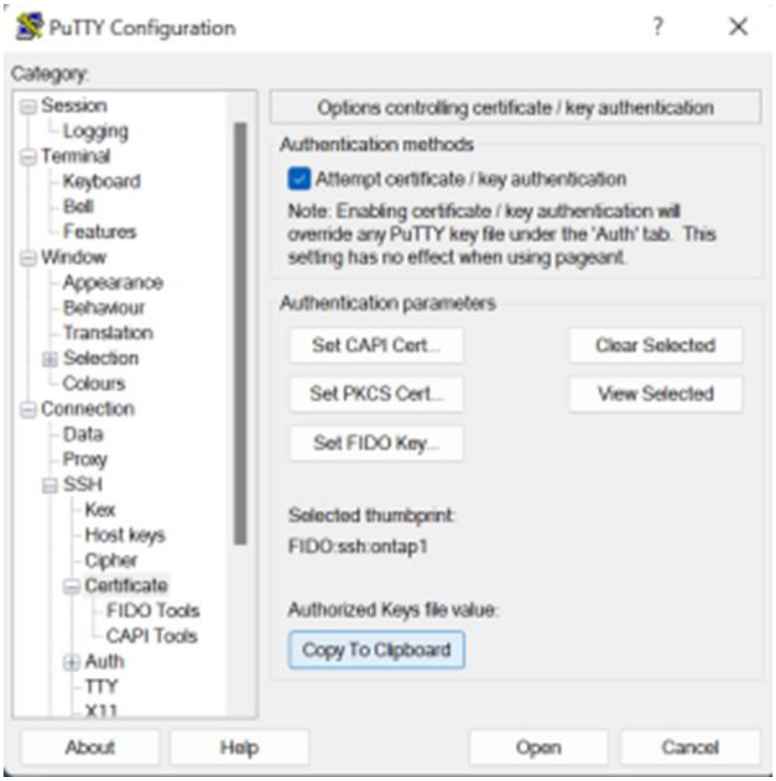
Export the FIDO2 public key

To configure FIDO2 public key authentication in ONTAP for the user, you need the public FIDO2 key.

1) Go to the main PuTTY Configuration dialog box and select the Certificate option.

Confirm that the string in the Selected Thumbprint section matches the application name you configured in the previous example: `FIDO:ssh:ontap1`.

Note: If it does not match, click Set FIDO Key to retrieve the FIDO2 key from the YubiKey. Then select Copy to Clipboard under Authorized Keys File Value.



☑ Attempt certificate / key authentication

Note: Enabling certificate / key authentication will override any PuTTY key file under the 'Auth' tab. This setting has no effect when using pageant.

Selected thumbprint:
FIDO:ssh:ontap1

Authorized Keys file value:

The following is an example of the FIDO2 public key:

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

Verify that this is the correct key by looking at the last section and checking that the application name in the public key comments matches the application name you configured. In the previous example, `ontap1` is the application, so the public key application name is `ssh:ontap1`.

Set the public key authentication mechanism for the ONTAP user account. After the ONTAP account is configured and associated with the public key, you can use an SSH client such as Putty to manage the ONTAP system.

See the Configure public key authentication for YubiKey FIDO2 In ONTAP” section for the next steps.

YubiKey FIDO2 client configuration For Mac OS and Linux

This section describes the general steps to configure the SSH client to support YubiKey for connecting to the ONTAP using FIDO2. The high-level steps for Mac OS and Linux clients are as follows:

1) Download and install the YubiKey Manager.

Initialize the YubiKey by setting the FIDO2 PIN.

Generate the private/public `ecdsa-sk` or `edd519-sk` key pair using PuTTY-CAC (Windows) or `ssh-keygen` (Mac).

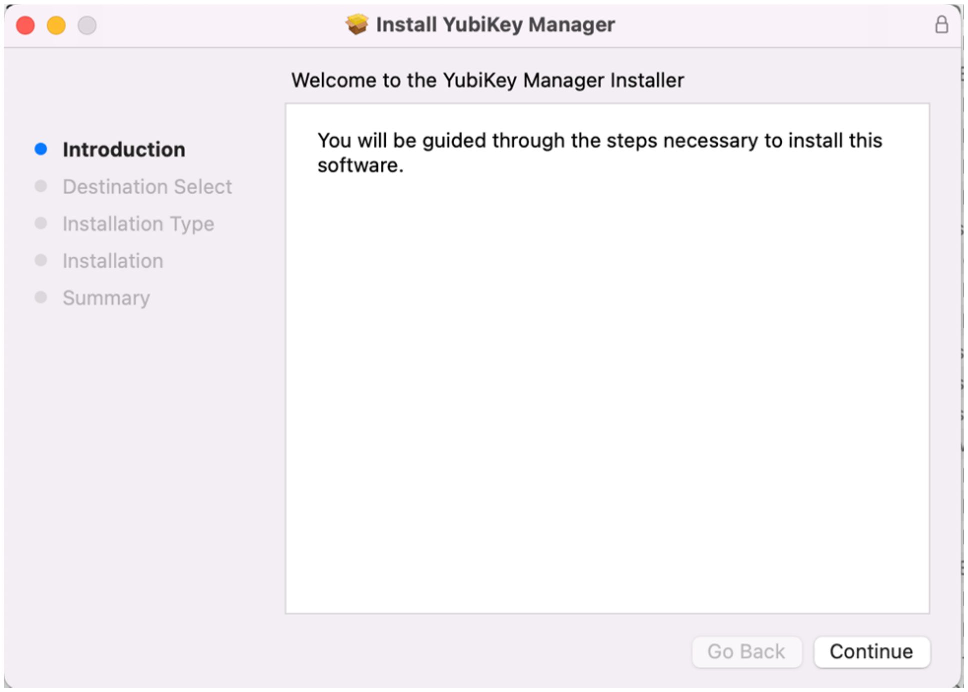
Convert the `ecdsa-sk` or `edd519-sk` public key to the SSH-compatible format if necessary.

Configure the ONTAP user to use the `publickey` authentication method.

Export the `ecdsa-sk` or `edd519-sk` public key to the ONTAP client.

Download and install the YubiKey Manager

1) Download and install the correct version of the YubiKey Manager for your platform from the Yubico website. Click Continue and accept all the default values. For example:

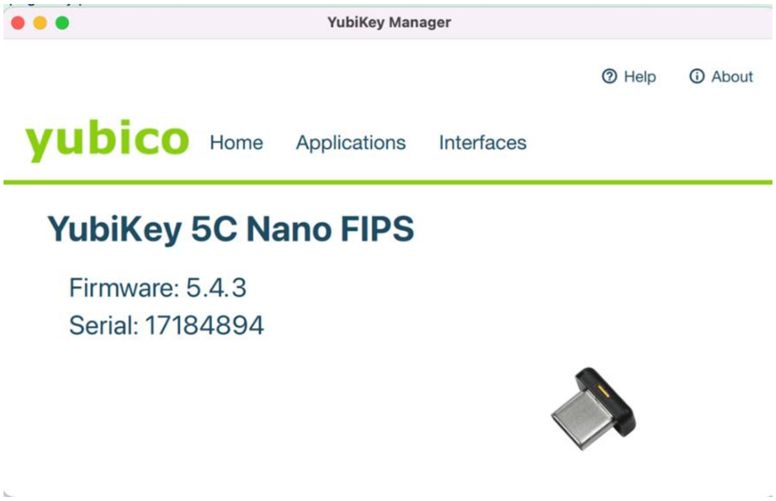


Install YubiKey Manager

Welcome to the YubiKey Manager Installer

You will be guided through the steps necessary to install this software.

After your installation is complete, insert your YubiKey into the USB slot, then run the YubiKey Manager. The model, serial number, and the firmware version of your YubiKey is displayed on the screen:



YubiKey Manager

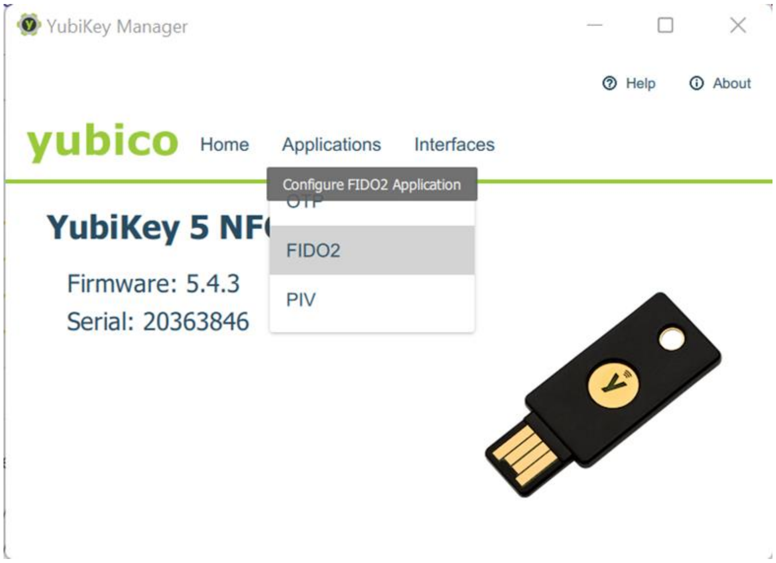
YubiKey 5C Nano FIPS

Firmware: 5.4.3

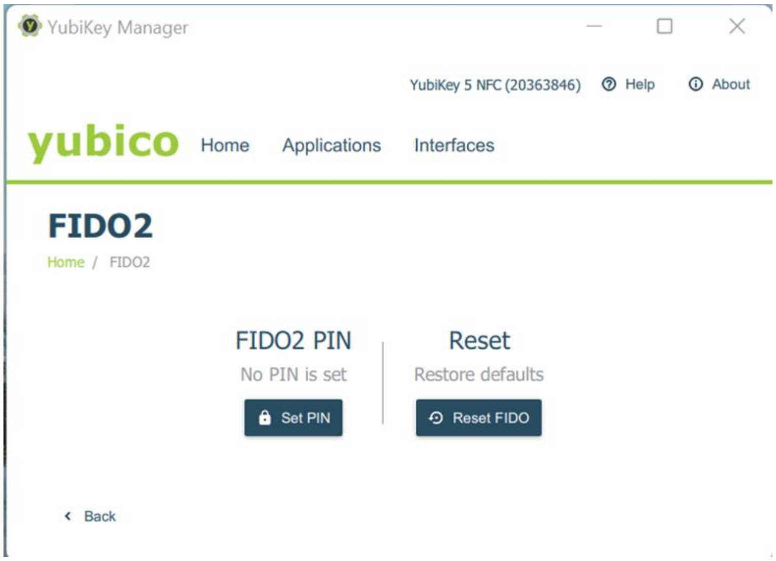
Serial: 17184894

Initialize the YubiKey PIN

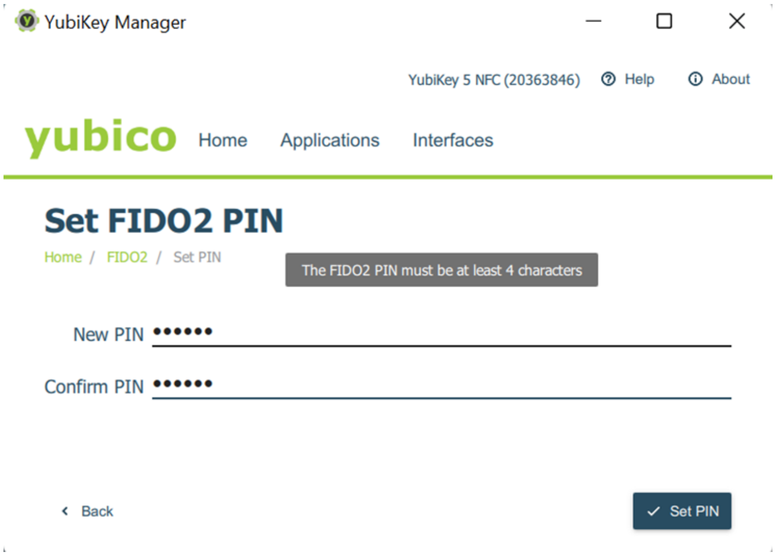
1) Go to Applications > FIDO2 to configure the FIDO2 settings. For example:



Firmware: 5.4.3
Serial: 20363846



The Set FIDO2 PIN dialog box appears and asks you to set the FIDO2 PIN. Enter a PIN of at least 4 characters in the New PIN field. Then enter the same PIN again in the Confirm PIN field. Select Set PIN to set the FIDO2 PIN:



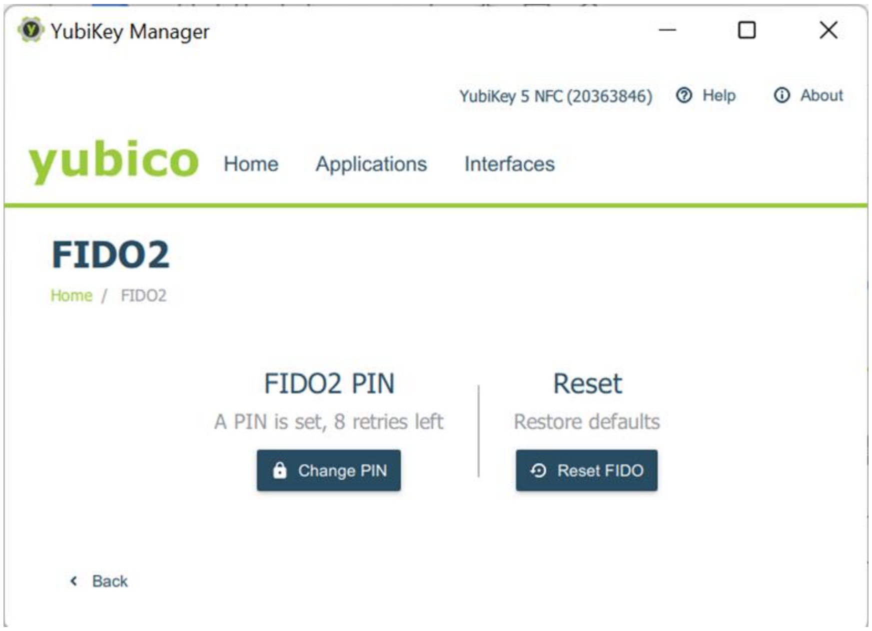
Set FIDO2 PIN

The FIDO2 PIN must be at least 4 characters

New PIN ••••••

Confirm PIN ••••••

You are brought back to the FIDO2 dialog box confirming that your PIN has been set:



FIDO2

FIDO2 PIN

A PIN is set, 8 retries left

Reset

Restore defaults

For more information about the YubiKey FIDO2 configuration, see the Yubico website.

Configure the MAC OS or Linux SSH client for YubiKey FIDO2 authentication

To use the YubiKey for FIDO2 authentication over SSH, you must generate a public/private ECDSA key pair. FIDO devices are supported by the public key types `ecdsa-sk` and `ed25519-sk`, along with corresponding certificate types:

- The `ed25519-sk` is stronger than `ecdsa-sk` mathematically but is not widely supported yet.
- The `ed25519-sk` is only supported by YubiKey with firmware versions 5.2.3 or later.
- The `ecdsa-sk` key type uses ECDSA which is supported for compatibility purposes.

ONTAP 9.12.1 and later uses `ECDSA-256` or `ECDSA-384` keys for SSH public key authentication.

Open source OpenSSH requirement

The built-in version of OpenSSH that comes with the MacOS does not support the `ecdsa-sk` and `ed25519-sk` key types required for FIDO2 operation. You must install the open-source version of OpenSSH using Homebrew. For example:

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

Confirm that the OpenSSH version is 8.2 or later. By default, Homebrew install OpenSSH in `/usr/local/opt/openssh`. Make sure that you are using the correct OpenSSH package:

```
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
```

Generate the client-side SSH FIDO2 key

The next step is to generate the FIDO2 private/public key pair. This example uses the `ecdsa-sk` key type. Supported key types are `ecdsa-sk` and `edd25519-sk`. To enable PIN verification, you have the additional option `-O verify-required` in the `ssh-keygen` command. Without this option, the SSH server only requests the user to touch the YubiKey, leaving open the possibility that an intruder can steal the YubiKey to log in to ONTAP.

Note: The `ssh-keygen` command prompts the user to enter the FIDO2 PIN (enter PIN for authenticator) and also touch the YubiKey to authorize the key generation.

```
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]-----+
```

If the `ssh-keygen` completes successfully, you now see two new keys in the `~/.ssh` directory for the user.

The `id_ecdsa_sk` file contains the FIDO2 private key.

The `id_ecdsa_sk.pub` contains the FIDO2 public key. This is the key you need to configure public key authentication for the user on the ONTAP.

For example:

```
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
```

Configure the SSH client for FIDO2

After the FIDO2 key pair is generated, the next step is to add an entry to the SSH configuration file to specify the location of the FIDO2 private key to use for the SSH client connection. To do this, add the following entry for ONTAP with the following information:

- **Host name:** The host name or IP address of the ONTAP where the user will SSH into. In this example, this is `vsim1.sim.netapp.com`.
- **Port:** The SSH port. In this example, this is the default value of 22.
- **User:** The username. This must match the name of the user configured on the ONTAP. In this example, this is `newadmin`.
- **IdentityFile:** The location of the FIDO2 private key. In this example, this is `~/.ssh/id_ecdsa_sk`.

For example:

```
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
```

The next step is to set the public key authentication mechanism for the ONTAP user account. After the ONTAP account is configured and associated with the public key you can use an SSH client such as Putty to manage the ONTAP system.

For next steps, see the section Configure public key authentication for YubiKey FIDO2 In ONTAP.

Configure public key authentication for YubiKey FIDO2 In ONTAP

In this example, a new admin user with the username `newadmin` using SSH is created, with the authentication method set to public key. The command used is the same whether the authentication method is the standard SSH public key authentication or YubiKey FIDO2 authentication.

```
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.
```

The warning message says that you must enter a public key for `newadmin` when adding `publickey` as the authentication method. This public key is obtained when you configure the YubiKey device on the client.

Next, set the FIDO2 public key that you configured for your YubiKey. The public key is obtained from the Copy to Clipboard function for PuTTY-CAC for PIV from Windows or from exporting the public key in an SSH-compatible format using `ssh-keygen -e` for PIV for MacOS.

Note: For MacOS the FIDO2 public key is in the `id_ecdsa_sk.pub` or `id_edd519_sk.pub`, depending on whether you are using ECDSA or EDD519.

Example output (note the `sk-key` type):

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

Now `newadmin` can log in from his client system as an ONTAP administrator using YubiKey and FIDO2 for multifactor authentication.

For more information about SSH MFA authentication, see “Enabling SSH Multifactor Authentication” in the ONTAP 9 Security Guide.

System Manager

About System Manager

If an ONTAP administrator prefers to use a graphical interface instead of the CLI for accessing and managing a cluster, use NetApp System Manager, which is included with ONTAP as a web service, enabled by default, and accessible by using a browser. Point the browser to the host name if using DNS or the IPv4 or IPv6 address through https://cluster-management-LIF.

If the cluster uses a self-signed digital certificate, the browser might display a warning indicating that the certificate is not trusted. You can either acknowledge the risk to continue the access or install a certificate authority (CA) signed digital certificate on the cluster for server authentication.

Starting with ONTAP 9.3, SAML authentication is an option for System Manager.

Enabling SAML authentication for System Manager

Unlike the SSH MFA configuration process, once activated, System Manager requires all existing administrators to authenticate through the SAML IdP. No changes are required to the cluster user accounts. When SAML authentication is enabled, a new authentication method of `saml` is added to existing users with administrator roles for `http` and `ontapi` applications.

After SAML authentication is enabled, additional new accounts requiring SAML IdP access should be defined in ONTAP with the administrator role, and the `saml` authentication method for `http` and `ontapi` applications. If SAML authentication is disabled at some point, these new accounts will require the password authentication method to be defined with the administrator role for `http` and `ontapi` applications and addition of the `console` application for local ONTAP authentication to System Manager.

After the SAML IdP is enabled, the IdP performs authentication for System Manager access by using methods available to the IdP, such as LDAP, Active Directory (AD), Kerberos, password, and so on. The methods available are unique to the IdP. It is important that the accounts configured in ONTAP have user IDs that map to the IdP authentication methods.

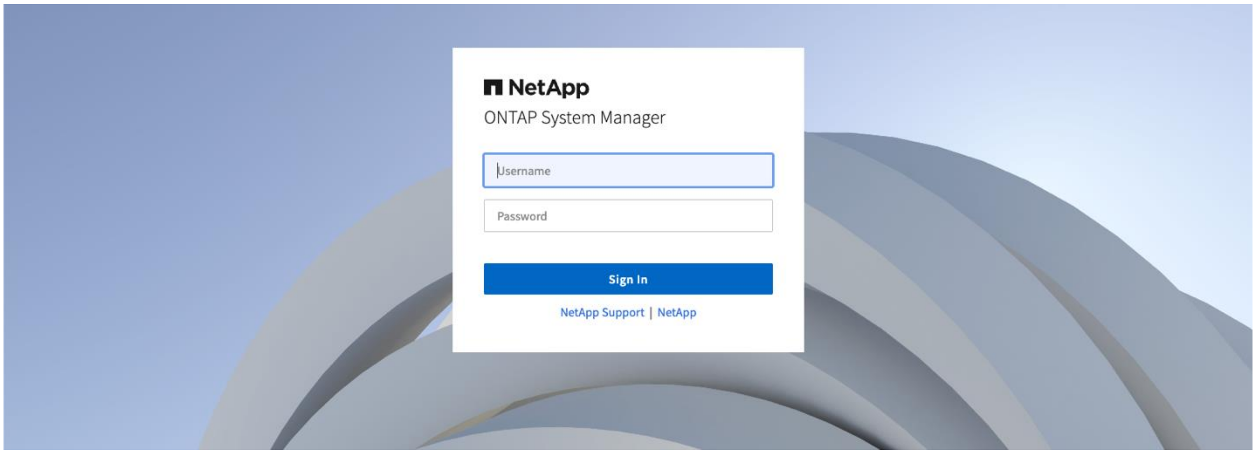
IdPs that have been validated by NetApp are Microsoft ADFS and open-source Shibboleth IdP for ONTAP 9.3 and later. Starting in ONTAP 9.12.1 Cisco DUO is also a supported IdP.

Before you start

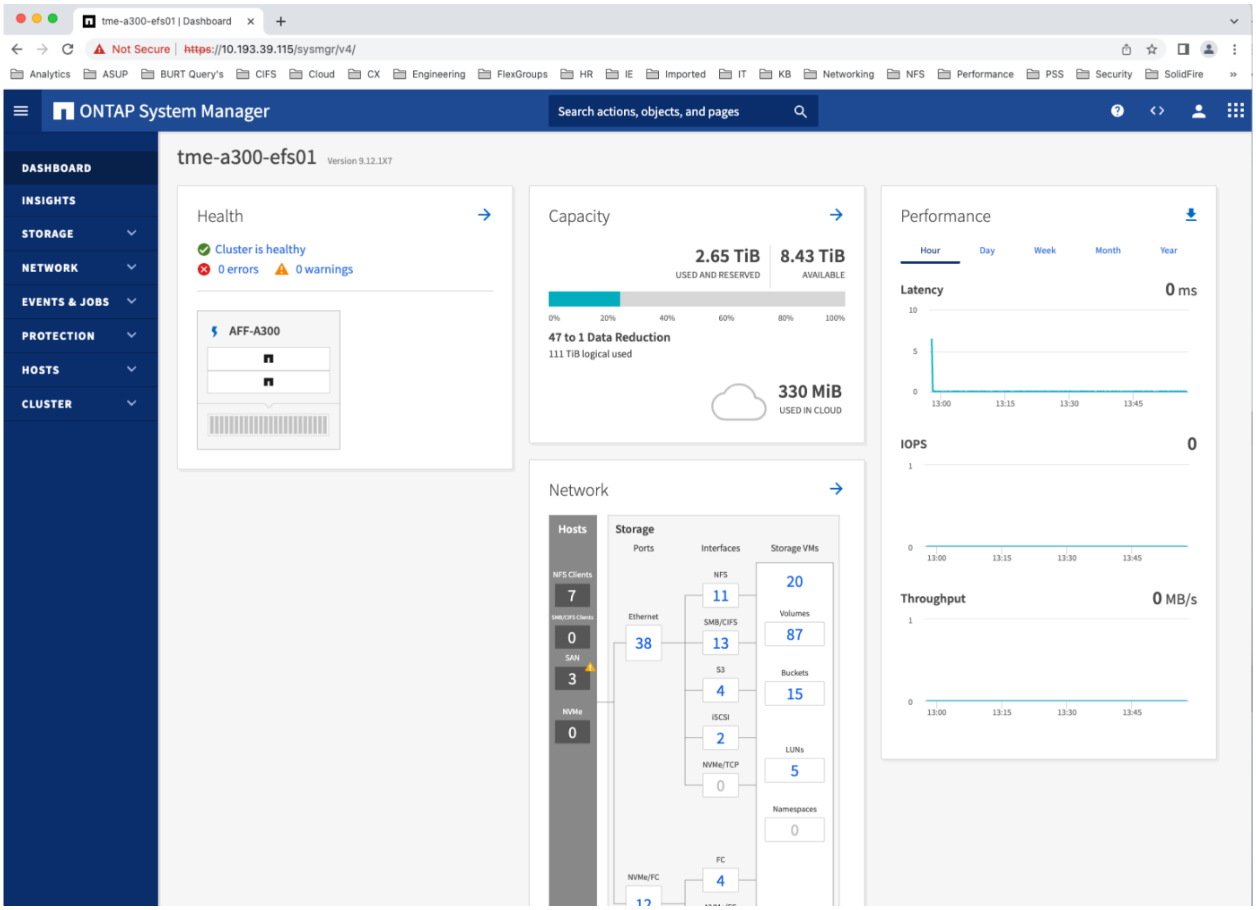
If your IdP is misconfigured after you enable SAML authentication in System Manager, you might not be able to log in to the System Manager web interface. To disable SAML authentication while remediating the IdP, you must access the Baseboard Management Controller (BMC) console. For details, see “Failure When Attempting to Enable SAML Authentication for System Manager” later in this document, in the “Troubleshooting” section.

Enable SAML authentication for System Manager

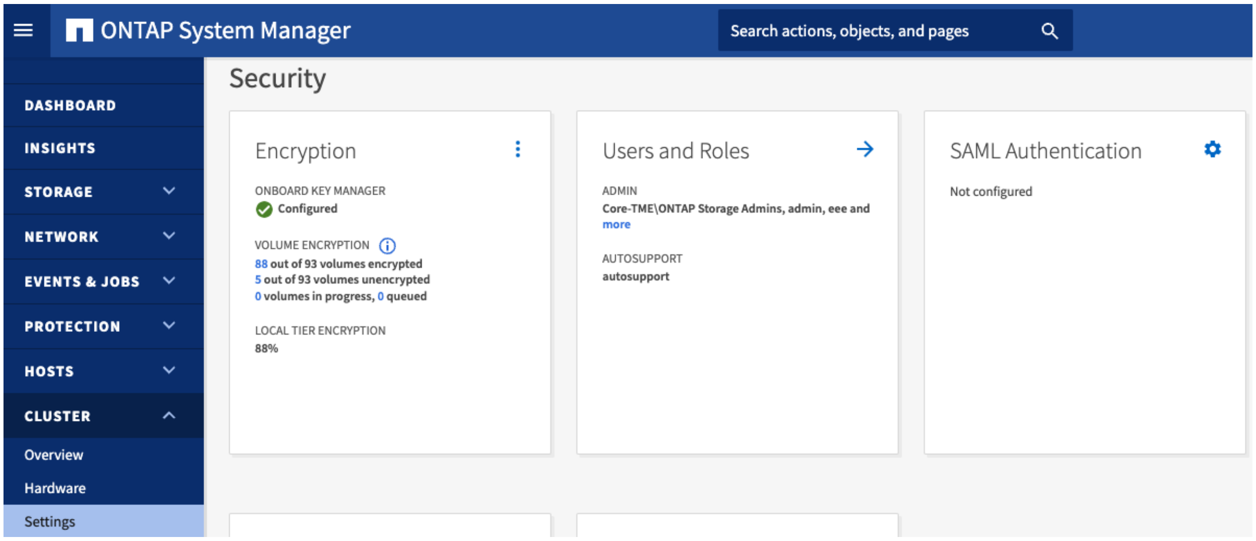
1) Open System Manager using the cluster management interface (DNS name or IP address).
   https://cluster-mgmt-LIF



Authenticate using administrator credentials.



Select Cluster > Settings and navigate to the Security section



Select the gear icon beside the SAML Authentication option.

Configure System Manager to use IdP authentication:

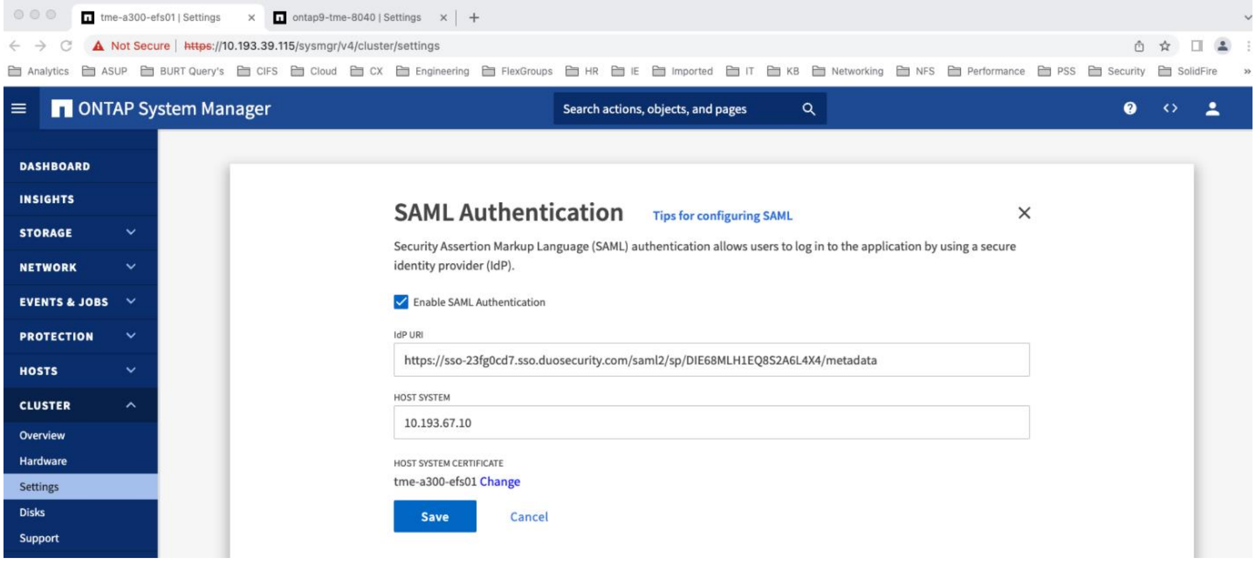
a. Check the box to Enable SAML Authentication

b. Enter the URI of the IdP.

c. Enter the DNS name or IP address of the host system.

d. Optional: If required, change the host system certificate to a CA-signed certificate.

e. Click Save



SAML Authentication — Tips for configuring SAML

Security Assertion Markup Language (SAML) authentication allows users to log in to the application by using a secure identity provider (IdP).

☑ Enable SAML Authentication

IdP URI: https://sso-23fg0cd7.sso.duosecurity.com/saml2/sp/DIE68MLH1EQ8S2A6L4X4/metadata

HOST SYSTEM: 10.193.67.10

HOST SYSTEM CERTIFICATE: tme-a300-efs01 Change

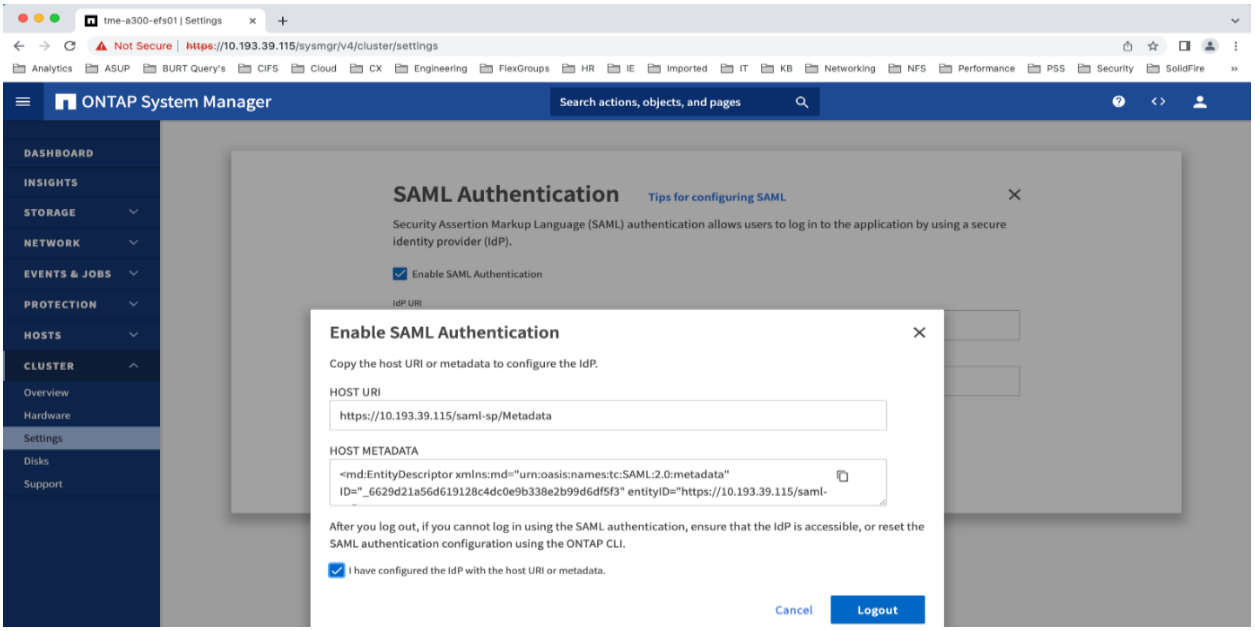
Save Cancel

Click the copy icon in the HOST METADATA section to retrieve the host URI and host metadata information.

Make sure that you have copied the host URI or metadata to the IdP and done the trust configuration on the IdP server. (Refer to your IdP documentation.)

Once the IdP server has been configured, check the “I have configured the IdP with the host URI or metadata” box

Click Logout


tme-a300-efs01 | Settings
Not Secure
https://10.193.39.115/sysmgr/v4/cluster/settings
Analytics
ASUP
BURT Query's
CIFS
Cloud
CX
Engineering
FlexGroups
HR
IE
Imported
IT
KB
Networking
NFS
Performance
PSS
Security
SolidFire
ONTAP System Manager
Search actions, objects, and pages
DASHBOARD
INSIGHTS
STORAGE
NETWORK
EVENTS & JOBS
PROTECTION
HOSTS
CLUSTER
Overview
Hardware
Settings
Disks
Support
SAML Authentication
Tips for configuring SAML
Security Assertion Markup Language (SAML) authentication allows users to log in to the application by using a secure identity provider (IdP).
Enable SAML Authentication
IdP URI

Enable SAML Authentication

Copy the host URI or metadata to configure the IdP.

HOST URI: https://10.193.39.115/saml-sp/Metadata

HOST METADATA:

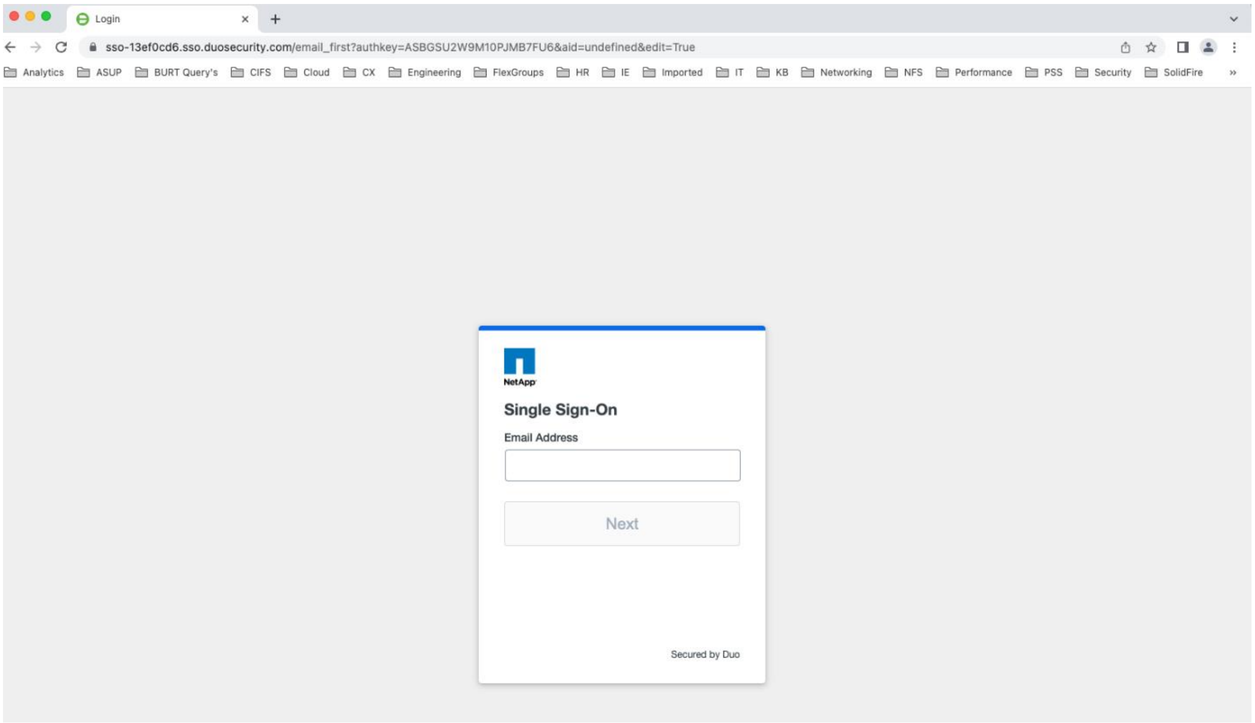
```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="_6629d21a56d619128c4dc0e9b338e2b99d6df5f3" entityID="https://10.193.39.115/saml-
```

After you log out, if you cannot log in using the SAML authentication, ensure that the IdP is accessible, or reset the SAML authentication configuration using the ONTAP CLI.

☑ I have configured the IdP with the host URI or metadata.

Cancel Logout

The IdP login window is displayed.

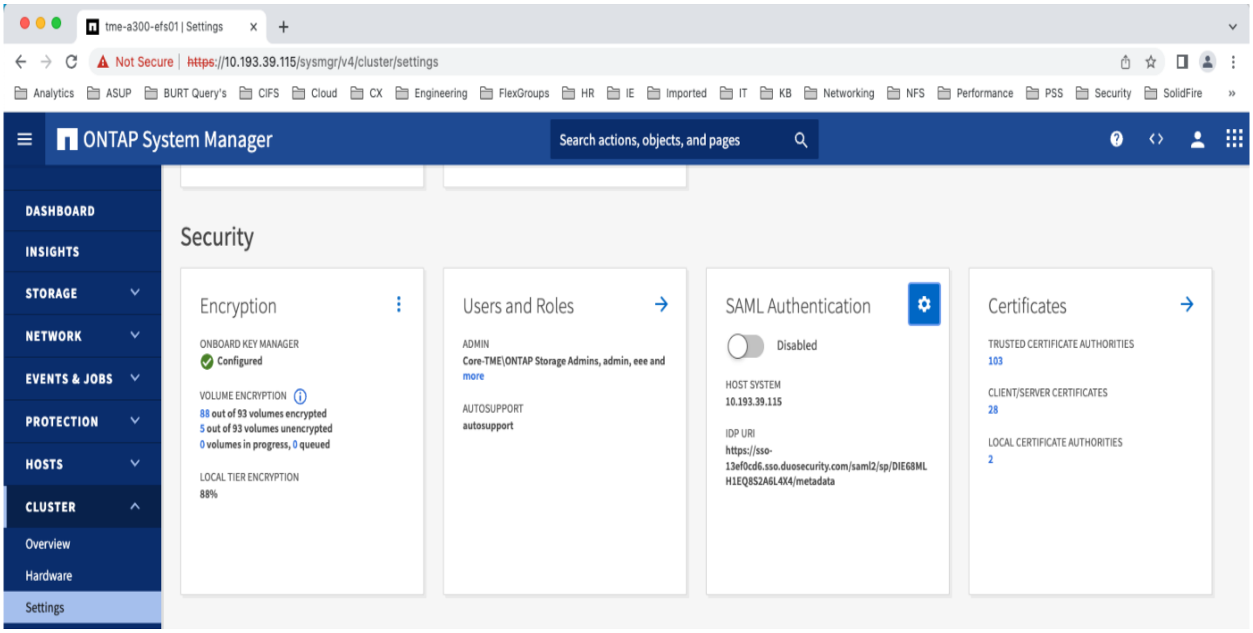


Log in to System Manager by using the IdP login window. (You might see a prompt from the IdP stating that you are about to share specific attributes with the ONTAP cluster. For successful login, you must allow sharing.)

After the SAML IdP authentication succeeds, the session has a lifetime configured in the IdP. For other service providers (SPs) that use the same IdP, this configuration allows the authentication to exist within the session lifetime period. If Active IQ Unified Manager is one of the SPs service providers that uses the same IdP, access to Active IQ Unified Manager is allowed without an additional authentication. Thus, SSO is enabled.

Disable SAML Authentication for System Manager

1) Open System Manager using the cluster management interface (DNS name or IP address) https://cluster-mgmt-LIF, authenticate through the IdP, navigate back to Cluster > Settings and scroll to the Security section then change the toggle to “Disabled” for SAML Authentication.



Security

Encryption

ONBOARD KEY MANAGER
✓ Configured

VOLUME ENCRYPTION
88 out of 93 volumes encrypted
5 out of 93 volumes unencrypted
0 volumes in progress, 0 queued

LOCAL TIER ENCRYPTION
88%

Users and Roles

ADMIN
Core-TME\ONTAP Storage Admins, admin, eee and more

AUTOSUPPORT
autosupport

SAML Authentication

○ Disabled

HOST SYSTEM
10.193.39.115

IDP URI
https://sso-13ef0cd6.sso.duosecurity.com/saml2/sp/DIE68MLH1EQ8S2A6L4X4/metadata

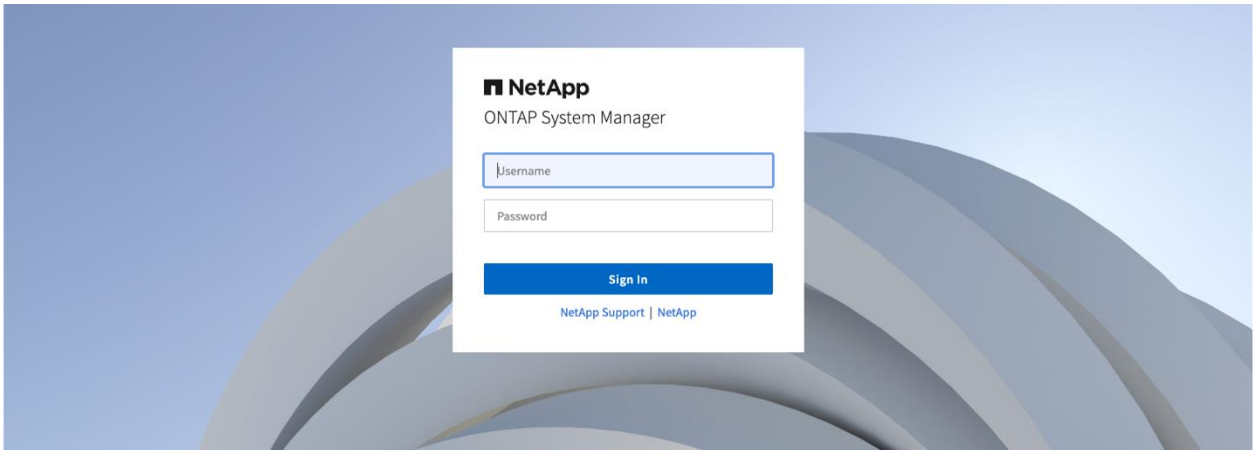
Certificates

TRUSTED CERTIFICATE AUTHORITIES
103

CLIENT/SERVER CERTIFICATES
28

LOCAL CERTIFICATE AUTHORITIES
2

2) Click Save and respond Yes to the warning.
System Manager displays the login prompt.



Active IQ Unified Manager

About Active IQ Unified Manager

Starting with NetApp ONTAP 9.3, SAML authentication is an option for Active IQ Unified Manager 7.3 and later.

Enabling SAML Authentication for Active IQ Unified Manager

Unlike the SSH MFA configuration process (but like the System Manager configuration process), once activated, Active IQ Unified Manager requires all existing remote users to authenticate through the SAML IdP. No changes are required to the Active IQ Unified Manager remote user accounts. Local and maintenance users lose access when SAML authentication is activated. The Active IQ Unified Manager maintenance console remains accessible. New accounts requiring SAML IdP access should be defined in Active IQ Unified Manager as remote accounts. If the SAML IdP is disabled in Active IQ Unified Manager, these new accounts require the credentials on the remote authentication system whether it is AD or LDAP.

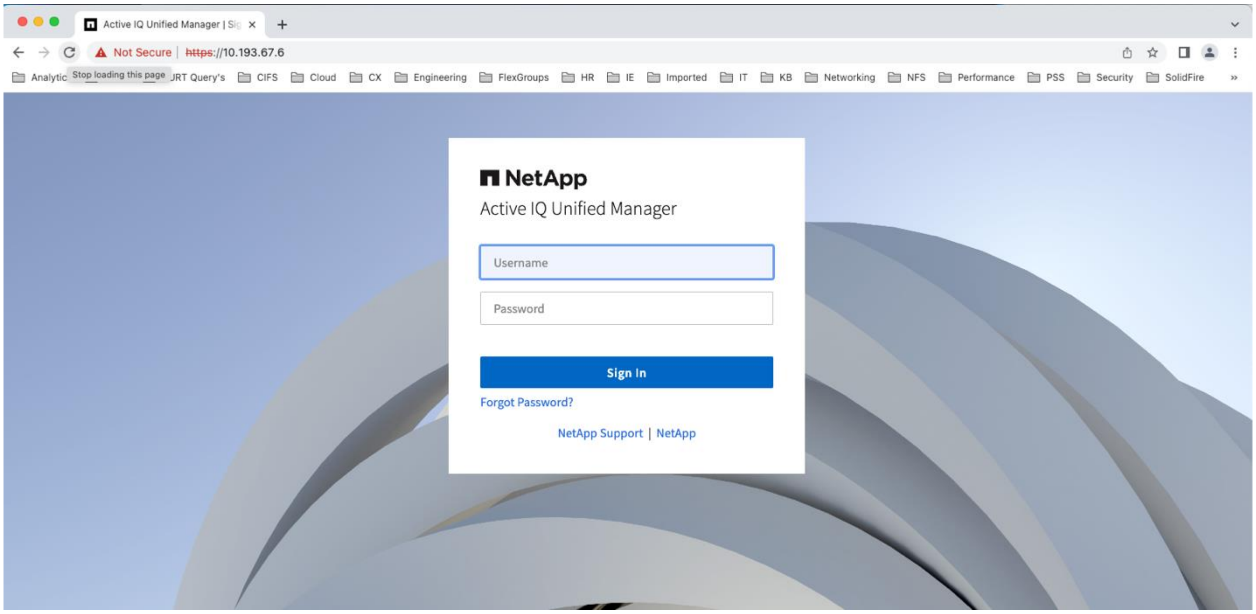
After enabling the SAML IdP, the IdP performs authentication for Active IQ Unified Manager access by using methods available to the IdP, such as LDAP, AD, Kerberos, password, and so on. The methods available are unique to the IdP deployed.

Before you start

If your IdP is misconfigured after you enable SAML authentication in Active IQ Unified Manager, you might not be able to log in to the Active IQ Unified Manager web interface. To disable SAML authentication while remediating the IdP, you must access the Active IQ Unified Manager maintenance console by using SSH. For details, refer to the “Failure When Attempting to Enable SAML Authentication for Active IQ Unified Manager” section later in this document, in the “Troubleshooting” section.

Enable SAML authentication for Active IQ Unified Manager

1) Ensure that you have network connectivity between Active IQ Unified Manager, the IdP, and Active IQ Unified Manager web clients.
2) Launch the Active IQ Unified Manager web UI.

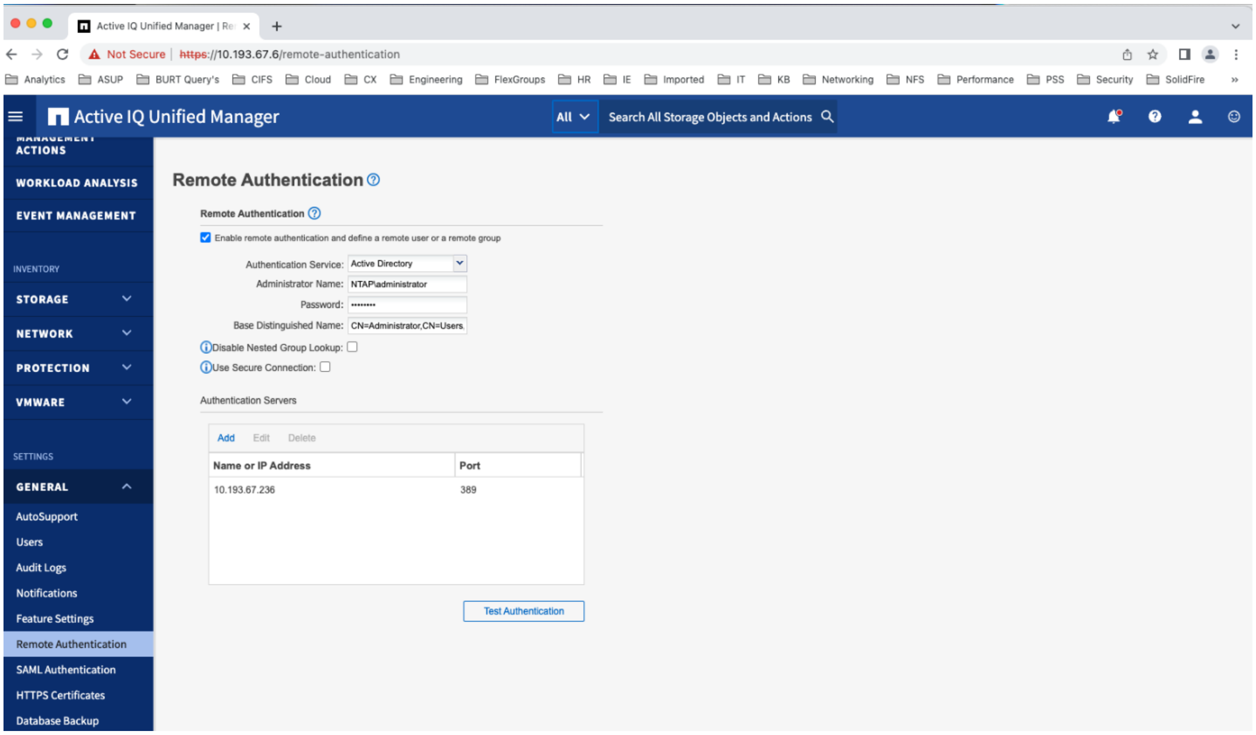


Authenticate by using the maintenance user credentials.

On the lefthand side under Settings expand General and click SAML Authentication

If you haven’t enabled remote authentication, you must do so for SAML IdP users to have access to Active IQ Unified Manager:

a. Select the Enable Remote Authentication checkbox.
b. Set the authentication service to Active Directory or OpenLDAP (Microsoft Lightweight Directory Services is not supported).
c. Enter the administrator name and password. For AD, specify Base Distinguished Name; for LDAP, specify Bind Distinguished Name, Bind Password, and Base Distinguished Name.
d. In the Authentication Servers section, enter the authentication server’s DNS name or IP address.



https://10.193.67.6/remote-authentication

Remote Authentication

Remote Authentication

☑ Enable remote authentication and define a remote user or a remote group

Authentication Service: Active Directory
Administrator Name: NTAP\administrator
Password: ••••••••
Base Distinguished Name: CN=Administrator,CN=Users,
Disable Nested Group Lookup: □
Use Secure Connection: □

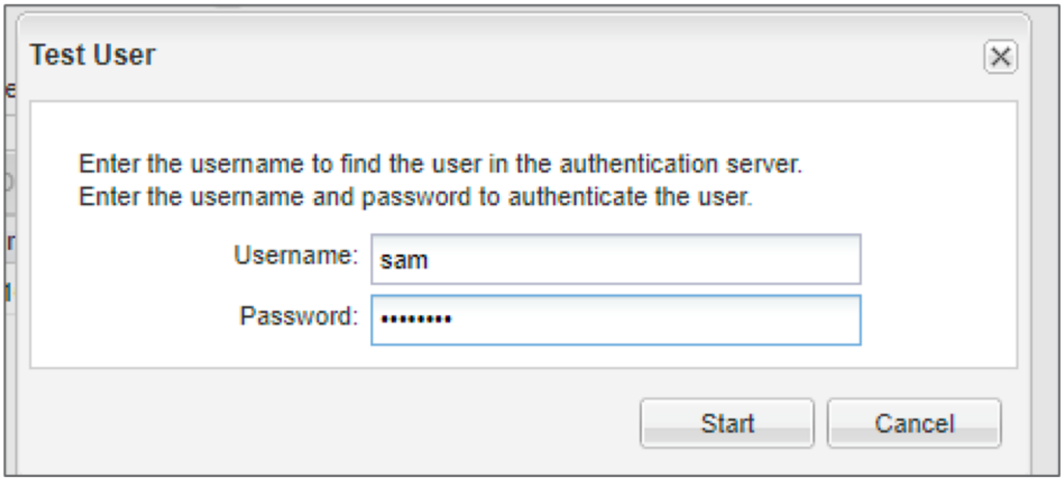
Authentication Servers

Add Edit Delete

Name or IP Address	Port
10.193.67.236	389

Test Authentication

a. Use Test Authentication to ensure that Remote Authentication Settings are operational.

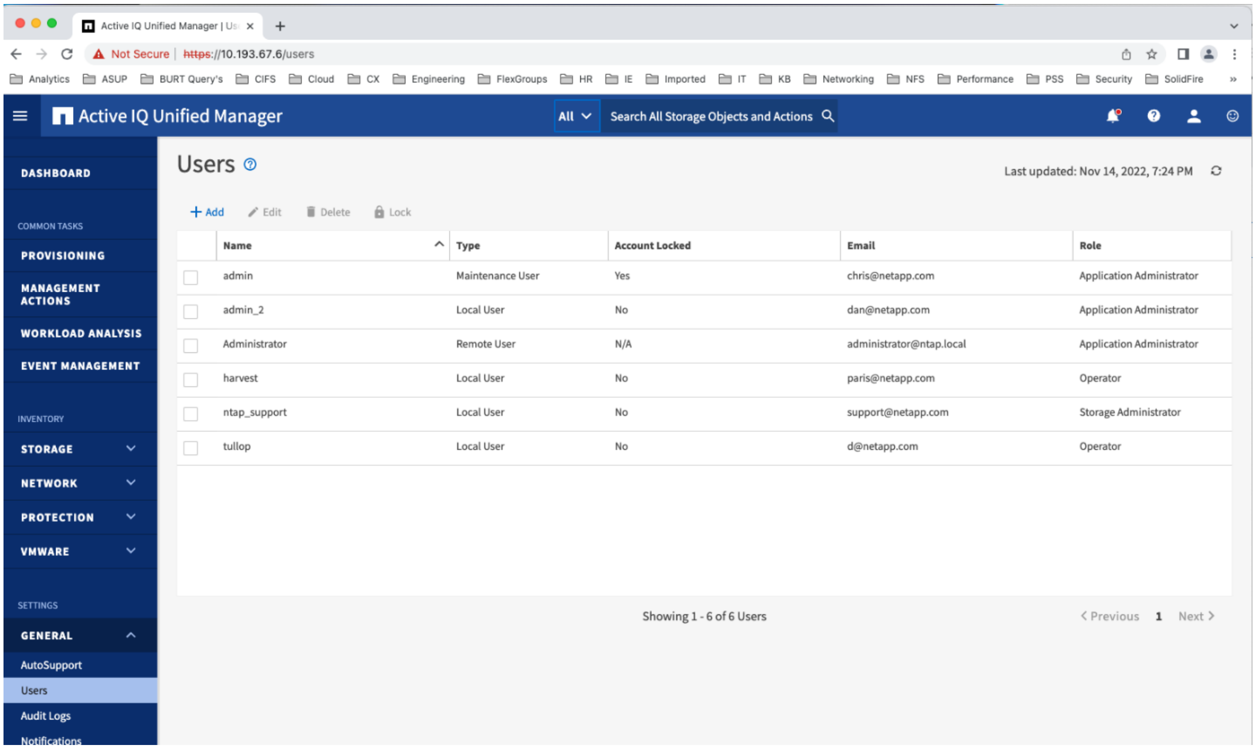


Test User

Enter the username to find the user in the authentication server.
Enter the username and password to authenticate the user.

Username: sam
Password: •••••••••

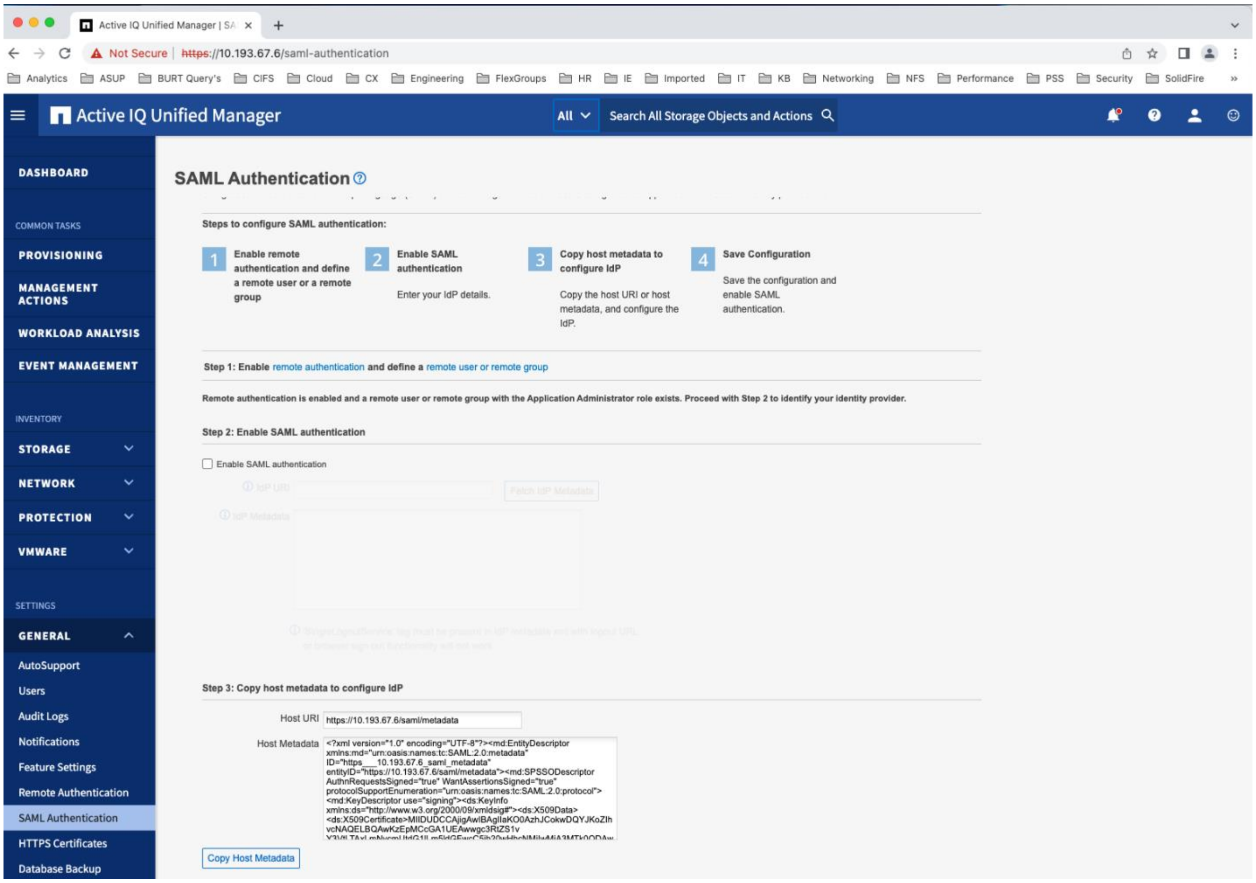
b. Navigate to the Settings > General > Users and add users of type remote user or remote group with the Active IQ Unified Manager Application Administrator role.



	Name	Type	Account Locked	Email	Role
□	admin	Maintenance User	Yes	chris@netapp.com	Application Administrator
□	admin_2	Local User	No	dan@netapp.com	Application Administrator
□	Administrator	Remote User	N/A	administrator@ntap.local	Application Administrator
□	harvest	Local User	No	paris@netapp.com	Operator
□	ntap_support	Local User	No	support@netapp.com	Storage Administrator
□	tullop	Local User	No	d@netapp.com	Operator

Showing 1 - 6 of 6 Users

Navigate to Settings > General > SAML Authentication Page.



SAML Authentication

Steps to configure SAML authentication:

1 Enable remote authentication and define a remote user or a remote group

2 Enable SAML authentication

Enter your IdP details.

3 Copy host metadata to configure IdP

Copy the host URI or host metadata, and configure the IdP.

4 Save Configuration

Save the configuration and enable SAML authentication.

Step 1: Enable remote authentication and define a remote user or remote group

Remote authentication is enabled and a remote user or remote group with the Application Administrator role exists. Proceed with Step 2 to identify your identity provider.

Step 2: Enable SAML authentication

□ Enable SAML authentication

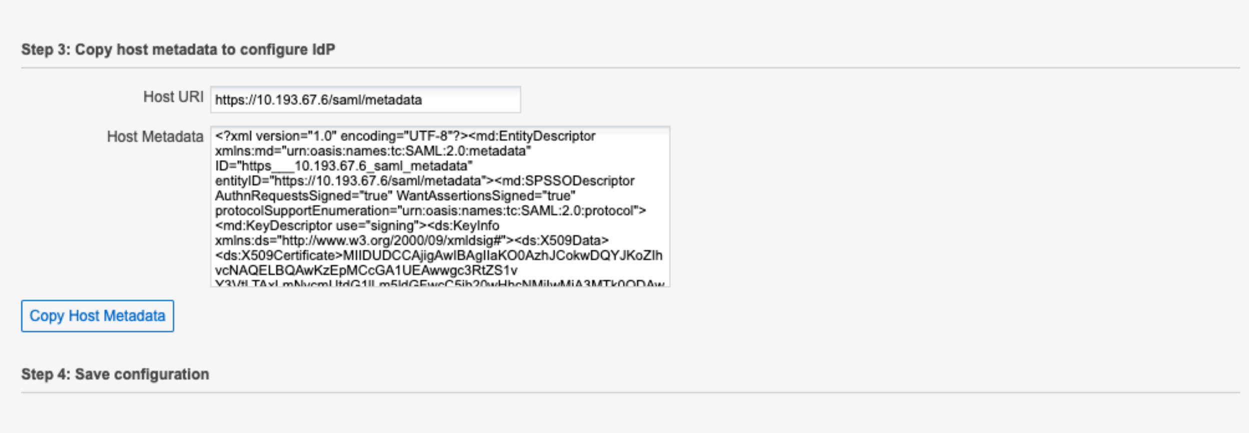
Step 3: Copy host metadata to configure IdP

Host URI: https://10.193.67.6/saml/metadata

Host Metadata:

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="https___10.193.67.6_saml_metadata"
entityID="https://10.193.67.6/saml/metadata"><md:SPSSODescriptor
AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing"><ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data>
<ds:X509Certificate>MIIDUDCCAjigAwIBAgIIaKO0AzhJCokwDQYJKoZIh
vcNAQELBQAwKzEpMCcGA1UEAwwgc3RtZS1v
```

Click > Copy Host Metadata, copy the metadata into a file, and save it. This file will be used to configure Active IQ Unified Manager in the IdP.



Step 3: Copy host metadata to configure IdP

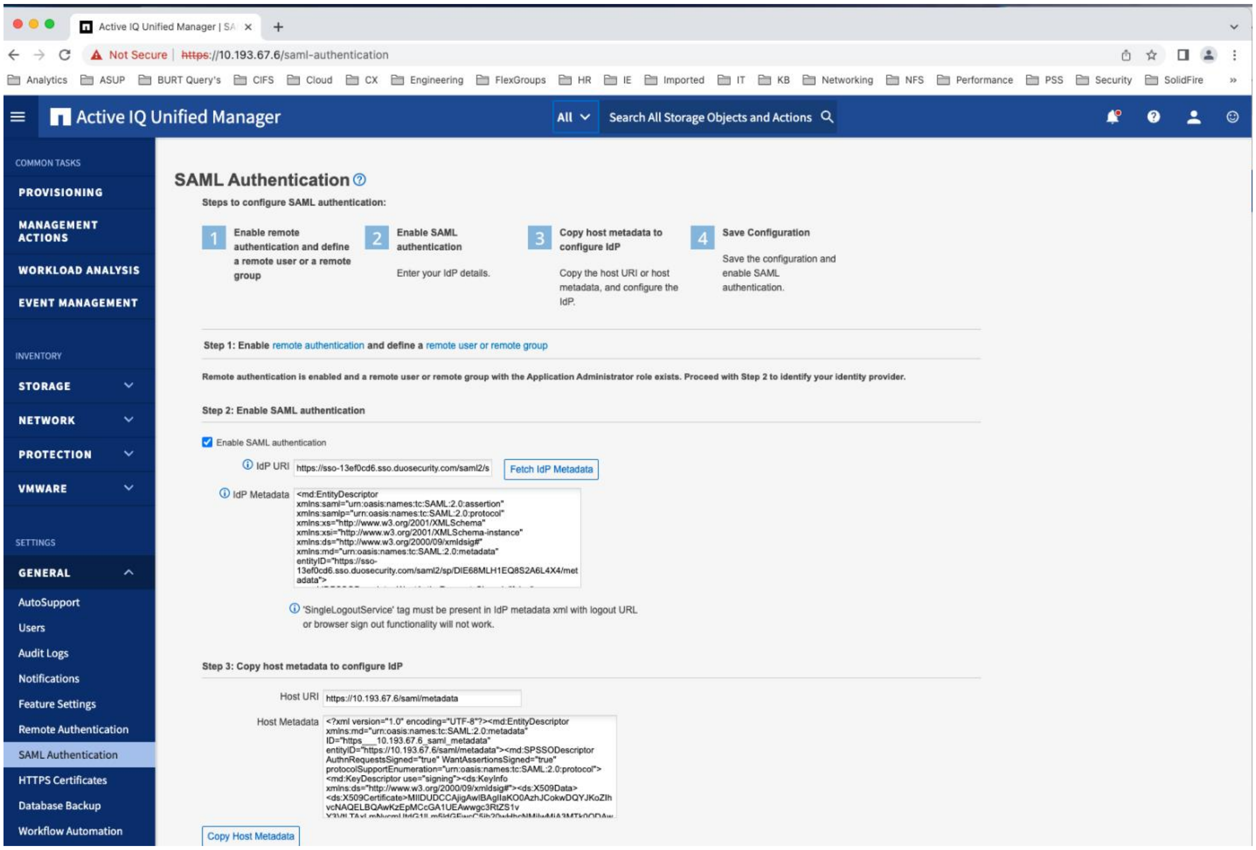
Host URI: https://10.193.67.6/saml/metadata

Host Metadata:

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="https___10.193.67.6_saml_metadata"
entityID="https://10.193.67.6/saml/metadata"><md:SPSSODescriptor
AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing"><ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data>
<ds:X509Certificate>MIIDUDCCAjigAwIBAgIIaKO0AzhJCokwDQYJKoZIh
vcNAQELBQAwKzEpMCcGA1UEAwwgc3RtZS1v
```

Step 4: Save configuration

Select the Enable SAML Authentication checkbox, enter the IdP URL, and click Fetch IdP Metadata to populate Active IQ Unified Manager with the IdP data.



SAML Authentication

Steps to configure SAML authentication:

1. Enable remote authentication and define a remote user or a remote group
2. Enable SAML authentication. Enter your IdP details.
3. Copy host metadata to configure IdP. Copy the host URI or host metadata, and configure the IdP.
4. Save Configuration. Save the configuration and enable SAML authentication.

Step 1: Enable remote authentication and define a remote user or remote group

Remote authentication is enabled and a remote user or remote group with the Application Administrator role exists. Proceed with Step 2 to identify your identity provider.

Step 2: Enable SAML authentication

☑ Enable SAML authentication

IdP URI: https://sso-13ef0cd6.sso.duosecurity.com/saml2/s

IdP Metadata:

```
<md:EntityDescriptor
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://sso-
13ef0cd6.sso.duosecurity.com/saml2/sp/DIE68MLH1EQ8S2A6L4X4/met
adata">
```

'SingleLogoutService' tag must be present in IdP metadata xml with logout URL or browser sign out functionality will not work.

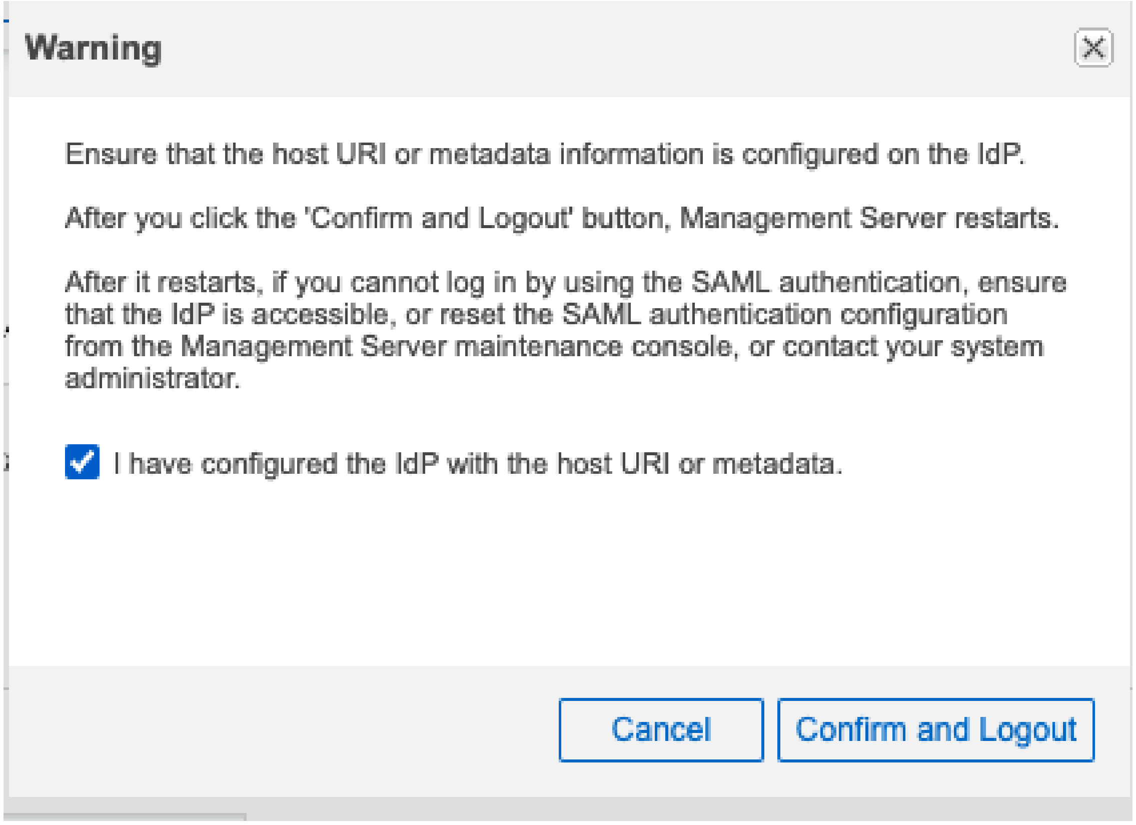
Step 3: Copy host metadata to configure IdP

Host URI: https://10.193.67.6/saml/metadata

Host Metadata:

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="https___10.193.67.6_saml_metadata"
entityID="https://10.193.67.6/saml/metadata"><md:SPSSODescriptor
AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing"><ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data>
<ds:X509Certificate>MIIDUDCCAjigAwIBAgIIaKO0AzhJCokwDQYJKoZIh
vcNAQELBQAwKzEpMCcGA1UEAwwgc3RtZS1v
```

Click Save, check the box to confirm you have configured the IdP, the click > Confirm and Logout



Ensure that the host URI or metadata information is configured on the IdP.

After you click the 'Confirm and Logout' button, Management Server restarts.

After it restarts, if you cannot log in by using the SAML authentication, ensure that the IdP is accessible, or reset the SAML authentication configuration from the Management Server maintenance console, or contact your system administrator.

☑ I have configured the IdP with the host URI or metadata.

Wait 5 minutes for the Active IQ Unified Manager services to restart.

Configure the IdP (refer to your IdP documentation).

a. Populate the IdP with the Active IQ Unified Manager metadata from step 7.
b. Add Active IQ Unified Manager as a Relying Party.
c. Add claim rules. Set Name to `urn:oid:0.9.2342.19200300.100.1.1` and Unqualified Name to `urn:oid:1.3.6.1.4.1.5923.1.5.1.1`.

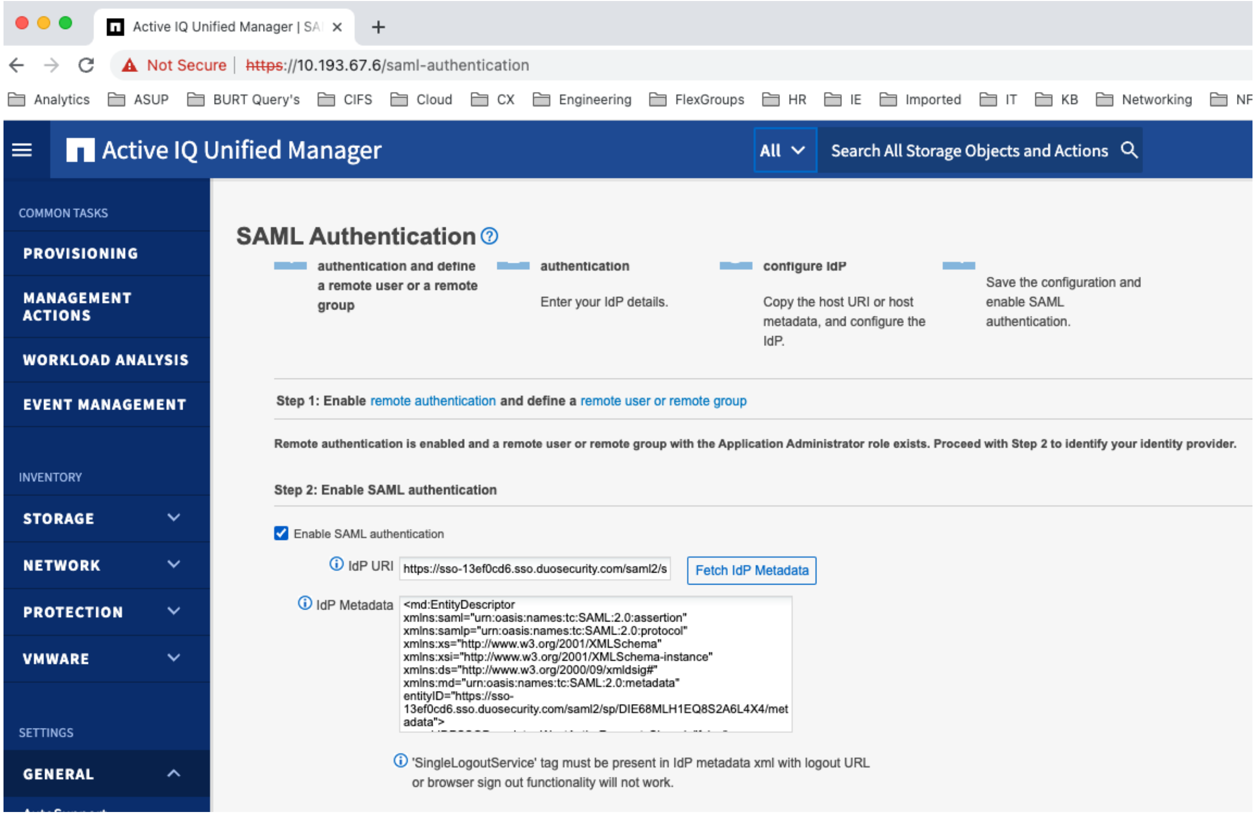
Launch the Active IQ Unified Manager web UI.

Authenticate using a remote user defined in step 5f.

As in the System Manager section, after the SAML IdP authentication succeeds, the session has a lifetime configured in the IdP. For other SPs that use the same IdP, this allows the authentication to exist within the session lifetime period. If System Manager is one of the SPs that uses the same IdP, access to System Manager is allowed without an additional authentication after a successful Active IQ Unified Manager authentication.

Disable SAML authentication for Active IQ Unified Manager

1) Launch the Active IQ Unified Manager web UI, authenticate through the IdP, and deselect the Enable SAML Authentication checkbox. Click Save.



SAML Authentication

authentication and define a remote user or a remote group

authentication
Enter your IdP details.

configure IdP
Copy the host URI or host metadata, and configure the IdP.

Save the configuration and enable SAML authentication.

Step 1: Enable remote authentication and define a remote user or remote group

Remote authentication is enabled and a remote user or remote group with the Application Administrator role exists. Proceed with Step 2 to identify your identity provider.

Step 2: Enable SAML authentication

☑ Enable SAML authentication

IdP URI: https://sso-13ef0cd6.sso.duosecurity.com/saml2/s

IdP Metadata:

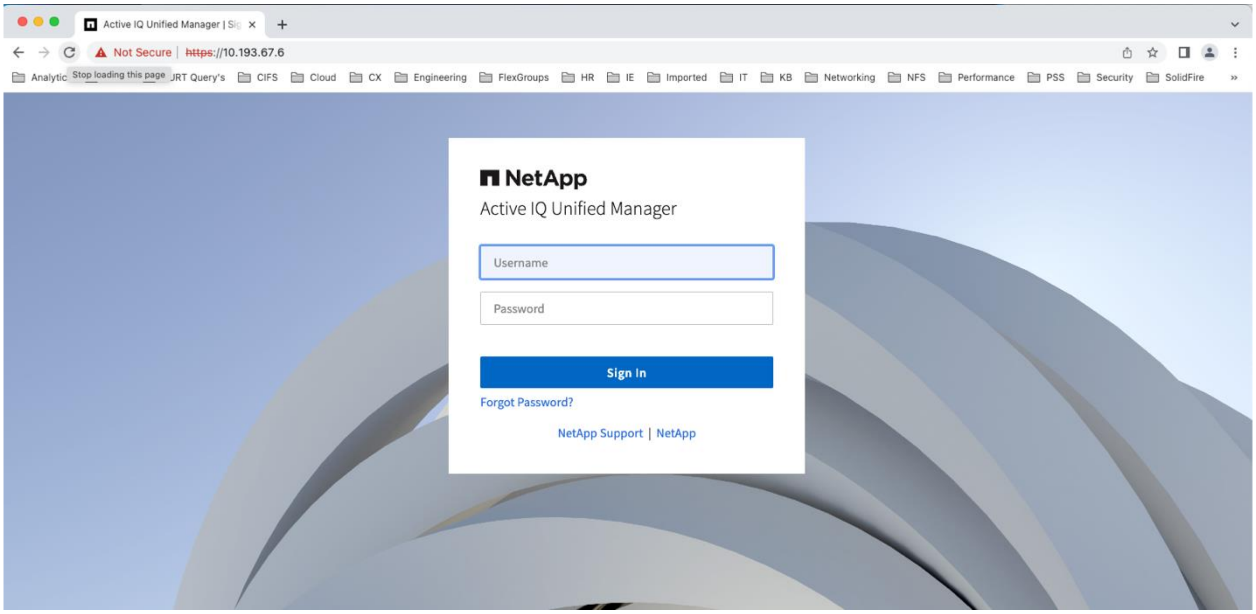
```
<md:EntityDescriptor
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://sso-
13ef0cd6.sso.duosecurity.com/saml2/sp/DIE68MLH1EQ8S2A6L4X4/met
adata">
```

'SingleLogoutService' tag must be present in IdP metadata xml with logout URL or browser sign out functionality will not work.

Click Save and respond Yes to the warning.

Wait five minutes for the Active IQ Unified Manager services to restart.

Launch the Active IQ Unified Manager web UI.



Best practices and caveats

Ubiquitous MFA implementation

NetApp ONTAP 9.3 SSH MFA allows user-by-user incremental implementation. Although this is useful for a gradual incremental deployment, the end goal of an MFA deployment **must be** for all administrative users to use login credentials with strong multifactor authentication.

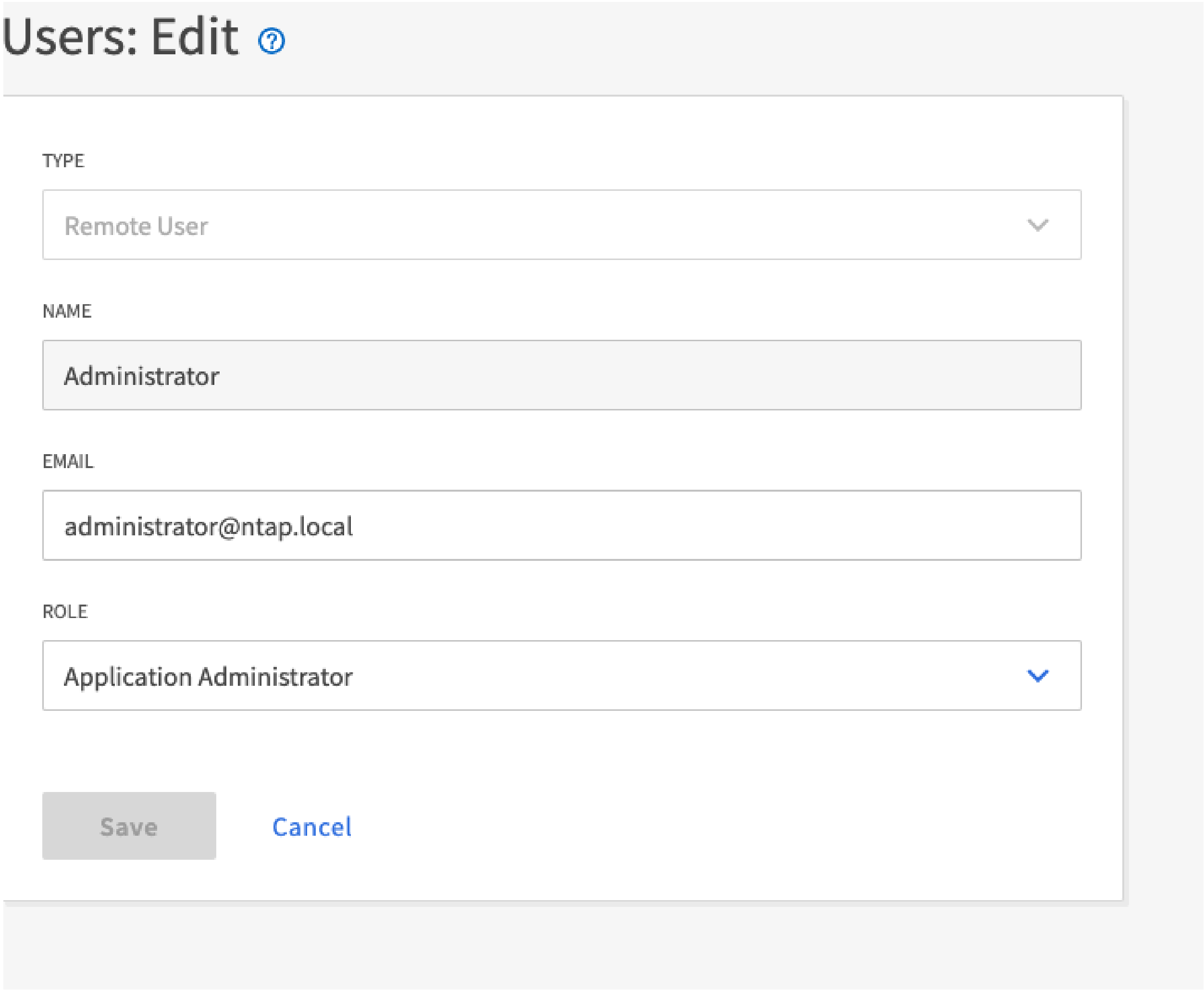
In addition to having MFA login credentials for all users, each administrator’s mode of access should use MFA. For ONTAP, this implies SSH CLI and SAML for System Manager HTTP access. For a user `sam`, the following login configuration would need to be in place:

```
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.
```

Note: After SAML authentication is configured for the `http` and `ontapi` applications, the `password` authentication method does not need to be configured. They remain configured for administrator accounts to enable external supportability tools to continue administrator access with single-factor user ID/password authentication. If no such tools require user ID/password access, delete all password authentication methods for all administrator accounts for `http` and `ontapi` applications to provide the most secure administrative access environment.

For Active IQ Unified Manager SAML authentication, `Administrator` would need to be defined as a remote user with a role of Active IQ application administrator.

Figure 3) Active IQ Unified Manager remote user definition.



Users: Edit

TYPE

Remote User

NAME

Administrator

EMAIL

administrator@ntap.local

ROLE

Application Administrator

Note: Before Active IQ Unified Manager SAML authentication configuration, Administrator would have been authenticated by either AD or OpenLDAP. After SAML authentication is enabled, `Administrator` is authenticated only by the SAML IdP.

Migration from single-factor authentication to MFA

SSH CLI

If there is only one ONTAP administrator account, create at least a second local single-factor authentication account in case something goes wrong with the migration of your primary account. If the starting state of ONTAP login accounts uses local SSH password or public-key authentication methods, migrate from single-factor to two-factor authentication by using the command `security login modify -user-or-group-name [username] -application ssh -second-authentication-method [password or publickey]`. If the new second factor is `publickey`, associate a public key with the user by using the command `security login publickey create -vserver [SVM_name] -username [username] -index [index_number] -publickey "[public_key_data]"`.

If the starting state of ONTAP login accounts uses the remote NIS/LDAP `nsswitch` SSH authentication method, migrate from single-factor to two-factor authentication by using the command `security login` modify -user-or-group-name [username] -application ssh -authentication-method nsswitch -second-authentication-method publickey. Then associate a public key with the user by using the command security login publickey create -vserver [SVM_name] -username [username] -index [index_number] -publickey "[public_key_data]".

Note: Two-factor authentication for nsswitch group users (security login create ... -is-nsswitch-group=yes) is not supported.

If the starting states of ONTAP administrator login accounts are domain (AD), the accounts must be deleted and re-added to local SSH account publickey and password, or publickey and nsswitch authentication methods. If you don't delete remote domain accounts and create a local two-factor authentication account, logins can fail because of password conflicts if they are different from the local and remote login definitions.

In ONTAP 9.13.1 and later:

- If the starting states of ONTAP administrator login accounts are domain (AD), you can add publickey as a second authentication method.
- Time-based-one-time password (totp) is a temporary passcode generated by an algorithm that uses the current time of day as one of its authentication factors for the second authentication method. TOTP authenticators include Google Authenticator, Microsoft Authenticator, and Authy. There are many TOTP apps in the market that can be used for TOTP authentication.
- Public key revocation is supported with SSH publickeys as well as certificates which will be checked for expiration/revocation during SSH.

System Manager and Active IQ Unified Manager SAML authentication

Although SAML authentication in System Manager and Active IQ Unified Manager is similar, the activation and implementation of the SAML IdP is different.

Enabling SAML authentication on System Manager automatically adds a new authentication method of saml for existing users with administrator roles for http and ontapi applications. At that point, the authentication methods deployed by the IdP for System Manager are in effect. The local password, domain, or nsswitch (AD or LDAP/NIS) is longer in effect.

Enabling SAML authentication on Active IQ Unified Manager automatically enables all remote users defined in Active IQ Unified Manager to authenticate by using methods deployed in the IdP. Remote authentication methods of AD or LDAP will no longer be in effect.

It is possible that AD or LDAP is one of the factors in the IdP implementation. If other factors are deployed, they should be implemented for each administrator user. There can be a broad range of factors. The most commonly used factors are username/password, public key, and a variety of attributes that can be verified, such as group, role, IP address, and email address.

For more details, refer to the ADFS and Shibboleth IdP links in "Where to Find Additional Information," later in this document.

IdP availability considerations

As with remote authentication mechanisms such as AD or LDAP, after enabling SAML authentication, continuation of connectivity to the IdP and continuous uptime of the IdP function become critical. Configuration of redundant, highly available IdP configurations is necessary to ensure availability to administrative access for System Manager and Active IQ Unified Manager.

Since ADFS and Shibboleth are architecturally unique, the approaches to creating high-availability configurations are also unique. ADFS can create a federation server farm by using SQL Server to replicate data between servers in diverse locations. Shibboleth's recommended approach for high availability is to create a cluster that replicates stateful data between Shibboleth nodes by using either software or hardware load-balancing mechanisms.

For more details, refer to the ADFS and Shibboleth IdP links in “Where to Find Additional Information,” later in this document.

Migration from MFA to single-factor authentication

SSH CLI

To revert to single-factor authentication for ONTAP SSH local accounts, use the command `security login modify -user-or-group-name [username] -application ssh -second-authentication-method none` to remove the second factor for each administrator user. If the second factor was `publickey`, the public key associated with that administrator user is deleted.

System Manager or Active IQ Unified Manager SAML authentication

To disable MFA for System Manager or Active IQ Unified Manager, deselect Enable SAML Authentication on the respective SAML Authentication webpage. For details on disabling SAML authentication for System Manager or Active IQ Unified Manager, refer to the “Configuration” section, earlier in this document.

After disabling SAML authentication on System Manager, the function is disabled in ONTAP. However, SAML authentication methods remain in `security login` administrator configurations for `http` and `ontapi` applications.

Disabling SAML authentication on Active IQ Unified Manager reverts remote users back to either LDAP or AD authentication as configured in the Active IQ Unified Manager remote authentication.

Troubleshooting

Common problems

Failure when attempting to enable SAML authentication for System Manager

If you enable SAML authentication and the IdP is misconfigured, administrative users will not be able to log in to System Manager. You will not be able to disable SAML from the cluster management LIF; you must disable SAML from the RLM console.

```
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
```

You can then log in to System Manager, remediate IdP issues, and reenable SAML authentication.

Failure when attempting to enable SAML authentication for Active IQ Unified Manager

If you enable SAML authentication and the IdP is misconfigured, you will not be able to log in to Active IQ Unified Manager as a local or remote user. You must use SSH to access the Active IQ Unified Manager maintenance console with the maintenance user’s credentials and select the menu item to disable SAML authentication.

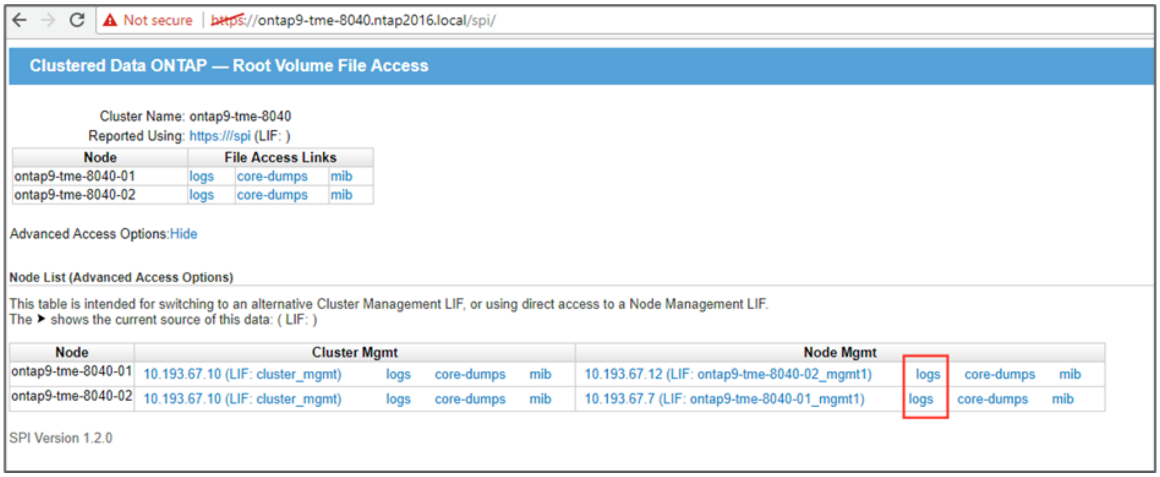
```
Active IQUnified Manager Maintenance Console

  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:
```

You can then log in to Active IQ Unified Manager, remediate IdP issues, and reenable SAML authentication.

Logs

The `shibd.log` file provides valuable information for debugging IdP implementation issues. In NetApp ONTAP, `shibd.log` is accessible through the service processor interface (SPI) node management logs.

Figure 4) ONTAP SPI log selection.



~~https~~://ontap9-tme-8040.ntap2016.local/spi/

Clustered Data ONTAP — Root Volume File Access

Cluster Name: ontap9-tme-8040
Reported Using: https:///spi (LIF:)

Node	File Access Links		
ontap9-tme-8040-01	logs	core-dumps	mib
ontap9-tme-8040-02	logs	core-dumps	mib

Advanced Access Options:Hide

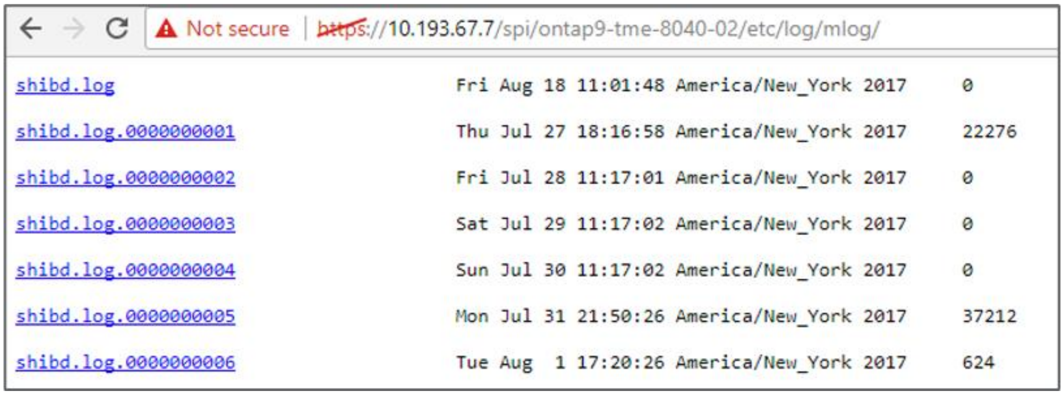
Node List (Advanced Access Options)

This table is intended for switching to an alternative Cluster Management LIF, or using direct access to a Node Management LIF.
The ➤ shows the current source of this data: (LIF:)

Node	Cluster Mgmt				Node Mgmt			
ontap9-tme-8040-01	10.193.67.10 (LIF: cluster_mgmt)	logs	core-dumps	mib	10.193.67.12 (LIF: ontap9-tme-8040-02_mgmt1)	logs	core-dumps	mib
ontap9-tme-8040-02	10.193.67.10 (LIF: cluster_mgmt)	logs	core-dumps	mib	10.193.67.7 (LIF: ontap9-tme-8040-01_mgmt1)	logs	core-dumps	mib

SPI Version 1.2.0

Figure 5) ONTAP SPI `shibd.log` files.



~~https~~://10.193.67.7/spi/ontap9-tme-8040-02/etc/log/mlog/

```
shibd.log                        Fri Aug 18 11:01:48 America/New_York 2017    0
shibd.log.0000000001             Thu Jul 27 18:16:58 America/New_York 2017    22276
shibd.log.0000000002             Fri Jul 28 11:17:01 America/New_York 2017    0
shibd.log.0000000003             Sat Jul 29 11:17:02 America/New_York 2017    0
shibd.log.0000000004             Sun Jul 30 11:17:02 America/New_York 2017    0
shibd.log.0000000005             Mon Jul 31 21:50:26 America/New_York 2017    37212
shibd.log.0000000006             Tue Aug  1 17:20:26 America/New_York 2017    624
```

Note: In the Shibboleth IdP, there is an analogous log: `/opt/shibboleth-idp/logs/idp-process.log`.

Disclaimer

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- NIST Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
- PCI DSS 4.0 Resource Hub
- ONTAP 9 Security Guide
- `ssh-keygen`
- Generate RSA Keys with SSH by Using PuTTYgen
- Active Directory Federation Services (ADFS)
- Shibboleth IdP
- Verizon 2023 data breach investigations report

Version history

Version	Date	Document Version History
Version 1.0	November 2017	Initial Release: Dan Tulledge
Version 1.1	March 2018	Dan Tulledge: 9.4 update
Version 2.0	November 2022	Matt Trudewind 9.12.1 update
Version 2.1	July 2023	Dan Tulledge 9.13.1 update

Contact us

Let us know how we can improve this technical report. Contact us at doccomments@netapp.com:

Include TECHNICAL REPORT TR-4647 in the subject line.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright information

Trademark information

TR-4647-1122