



NetApp Verified Architecture

Access Management for NetApp E-Series storage systems using Azure Active Directory NVA deployment

Amy Vargas, Mike Penner and Eric Stanton, NetApp
June 2021 | NVA-1161-DEPLOY

Abstract

This document provides deployment information for Access Management of NetApp® E-Series storage systems using Azure Active Directory (AD).

TABLE OF CONTENTS

Program summary	3
NetApp Verified Architecture program	3
Access management for E-Series storage systems	3
Solution overview	4
Solution technology	4
Use case summary	4
Technology requirements	5
Hardware requirements	5
Software requirements	5
Deployment procedures	5
Create the Azure enterprise application	5
Generate the SAML signing certificate	6
Import the IdP metadata through SANtricity System Manager	6
Import the SP metadata to the Azure enterprise application	6
Configure role mappings	6
Test and enable SAML	7
Solution verification	7
Create the Azure enterprise application	7
Generate SAML signing certificate	10
IdP metadata file generation and import	10
SP metadata file generation and import	13
Configure role mappings	18
Test and enable SAML	31
Conclusion	34
Where to find additional information	35
Version history	35

LIST OF TABLES

Table 1) Hardware requirements	5
Table 2) Software requirements.	5
Table 3) Azure AD groups and roles.	25

Program summary

NetApp Verified Architecture program

The NetApp Verified Architecture program offers customers a verified architecture for NetApp solutions. NetApp Verified Architectures provide customers with a NetApp solution architecture that:

- Is thoroughly tested
- Is prescriptive in nature
- Minimizes deployment risks
- Accelerates time to market

This document is for NetApp and partner solutions engineers and customer strategic decision makers. It includes specific configuration and deployment information for this solution as tested.

Access management for E-Series storage systems

Access Management is a method of establishing user authentication for NetApp SANtricity® applications and NetApp E-Series storage systems. Authentication can be configured by using one or more of the following methods:

- **Local user roles (preconfigured).** Authentication is managed through role-based access control (RBAC) capabilities, which include hard-coded user profiles with specific access permissions. Administrators can use these local user roles as the single method of authentication or use them in combination with a directory service.
- **Directory service.** Authentication is managed through an Lightweight Directory Access Protocol (LDAP) server and directory service, such as Microsoft's Active Directory.
- **Multifactor authentication (System Manager only).** Authentication is managed through an Identity Provider (IdP) by using Security Assertion Markup Language (SAML 2.0).

After you configure an Access Management method, SANtricity users log in with their assigned user profiles. They can then perform management tasks according to their assigned roles. For example, one type of user might have access to security functions but not storage management functions. Another type of user might have view-only permissions. For more information, see [TR-4853: Access Management for E-Series Storage Systems](#).

For the purposes of this document, only the directory service option is used for access management.

Multifactor authentication access management

When using multifactor authentication access management, authorization and authentication services are configured on the following:

- **Service Provider (SP).** The system that provides services to a user and needs to be able to authenticate and authorize a user to allow them to have access to those services. For this document, the storage system controllers are the SPs.
- **IdP.** The system that is capable of authenticating a user by determining if the provided credentials are valid for the provided username. For this document, the Azure Enterprise Application is the IdP.

SP

The following information is required by the controllers in order to communicate with the IdP:

- The IdP metadata should include the following information:
 - Entity ID: Identifier for the IdP.
 - Single-sign-on (SSO) service: URL to send authentication requests to the IdP.

- Single logout service: URL to send logout notifications to the IdP.
- Name ID format: Formats used for the user's name.
- Signing certificate: X.509 certificate that contains the public key necessary for the SP to validate the signature for messages received from the IdP.
- Mapping of user attributes provided by the IdP to System Manager roles

IdP

The SP metadata required by the IdP includes the following information:

- Entity ID: Identifier for the SP.
- Authentication requests signed: Indicates that the authentication requests sent from the SP will be signed to verify the origination of the request. This is not supported with Azure.
- Want assertions signed: Indicates that the SP prefers to have the assertions (authentication responses) to be signed to verify the origination of the response.
- Supported protocols: Specifies the protocols that the SP supports. In this case, it is the SAML 2.0 XML namespace.
- Name ID format: Formats requested for this document are e-mail and unspecified.
- Single logout service: URL for the IdP to send logout requests to the SP. Azure supports logout to one controller only because it allows one URL to be specified.
- Assertion Consumer Service – URL for the IdP to send authentication responses to the SP
- Signing Certificate – X.509 certificate that contains the public key necessary for the IdP to validate the signature for messages received from the SP. This is not supported with Azure.
- Encryption Certificate – X.509 certificate that contains the public key necessary for the IdP to encrypt messages sent to the SP. This is not supported with Azure.

Role mapping

When the IdP successfully authenticates a user's credentials, the IdP responds with an assertion message that includes information about the authenticated user. This information allows the SP to determine the permissions that should be granted to the user. Role mapping is used by the SP to associate information returned from the IdP to specific roles on the SP.

Configuration of the role mapping can be challenging since it requires establishing relationships on the SP and IdP. The IdP must include role information in the authentication response and the SP must be able to interpret that information and correlate it with a defined SANtricity System Manager role for the authenticated user.

Solution overview

This document describes how to configure SANtricity System Manager and Azure settings to use Azure Active Directory (AD) for access management. Azure AD is a commonly used directory service that can be configured to work with many applications. It provides a centralized identity platform to allow seamless and secure access to applications from any location.

Solution technology

The solution was validated using one NetApp E5700 storage system and one NetApp E280x storage system.

Use case summary

The primary use case for this solution is to use Azure AD to sign into SANtricity System Manager.

Technology requirements

This section covers the hardware and software used in the validation of this solution. All testing documented in the [Solution Verification](#) section was performed with the hardware and software indicated.

Note: The configuration verified in this document was based on lab equipment availability and not on the requirements or limitations of the hardware tested.

Hardware requirements

Table 1 lists the hardware components that were used to validate this solution. The hardware components that are used in any particular implementation of the solution might vary based on customer requirements.

Table 1) Hardware requirements.

Hardware	Quantity
NetApp E5700	One dual controller system
NetApp E280x	One dual controller system

Software requirements

Table 2 lists the software components that were used to validate this solution. The software components that are used in any particular implementation of the solution might vary based on customer requirements.

Table 2) Software requirements.

Software	Version
SANtricity OS (includes storage system OS, SANtricity System Manager and the Web Services API)	11.70R3

Deployment procedures

This section describes the steps required to deploy Azure AD access management through SANtricity System Manager. At a high level, deploying the solution involves the following tasks:

- Create one or more Azure enterprise applications
- Generate the SAML signing certificate
- Import the IdP metadata through SANtricity System Manager
- Import the SP metadata to the Azure enterprise application
- Configure role mappings through the following:
 - The Azure enterprise application
 - SANtricity System Manager
- Test the connection and enable SAML through SANtricity System Manager

Create the Azure enterprise application

The enterprise application created in Azure can be done in one of the following ways:

- Create one enterprise application for all E-Series storage systems.
- Create one enterprise application for each E-Series storage system.

- Create one enterprise application for each controller in an E-Series storage system.

For this document, a single Azure enterprise application was created that included both E-Series storage systems being tested. This configuration helped reduce the number of steps needed to get things set up. However, there are a few minor drawbacks to this configuration:

- Azure allows for only one logout URL for an enterprise application for IdP-initiated logouts of a user. If all controllers are using the same enterprise application, then logging a user out from Azure will result in that user only being logged out of the controller associated with the logout URL. For all other controllers, that same user will need to be manually logged out through SANtricity System Manager.
- Because the SP metadata for only one controller is imported, the signing and encryption certificates are not used for communications. Any authentication requests sent from the controllers to Azure is signed but Azure does not verify the signature because it does not have the certificate necessary to do the verification. Also, Azure is not able to send encrypted responses to the controllers because it does not have the certificate to do the encryption. However, all communications between the IdP and SP are over an already established Transport Layer Security (TLS) connection, so encryption is not as critical.

Generate the SAML signing certificate

By default, Azure generates a signing certificate for the E-Series enterprise application. This will most likely suffice for most users. A different certificate can be generated and imported through the SAML signing certificate panel for the enterprise application if desired.

Import the IdP metadata through SANtricity System Manager

The IdP metadata file is used to provide information that the SP needs in order to communicate with the IdP. In this case, the E-Series storage system controllers are the SPs and the Azure enterprise application is the IdP.

In order to generate the IdP metadata file, an Azure enterprise application must first be created for the E-Series storage systems. After it is created, the IdP metadata file can be downloaded from the Azure enterprise application and then imported onto the appropriate E-Series storage systems.

Import the SP metadata to the Azure enterprise application

In order for the Azure enterprise application to be able to communicate with the E-Series storage systems, it must have access to the SP information for each of the controllers. This action can be completed by exporting the SP metadata files from all of the controllers and then importing the SP metadata file for one of the controllers to the Azure enterprise application. The SAML configuration then needs to be updated to include information for the other controllers.

Note: Although the SP metadata from just one of the controllers is imported to the Azure enterprise application, the SP metadata must still be exported on all of the controllers that are being configured for access management. If the SP metadata is not exported from a controller, then it is not able to authenticate with the IdP.

Note: When an SP metadata file is imported to the Azure enterprise application, it overwrites any preexisting SP metadata file that might have already been present.

Configure role mappings

To start the role mapping process, the Azure user groups must be created or identified to be reported with the user information and role mappings for a successful authentication. The user attributes configuration will then need to be updated to indicate the appropriate user information to be included with a successful authentication response.

After Azure has been configured to report the group, role and user information, SANtricity System Manager can then be configured on each of the E-Series storage systems to specify the role mapping for the authenticated users.

Test and enable SAML

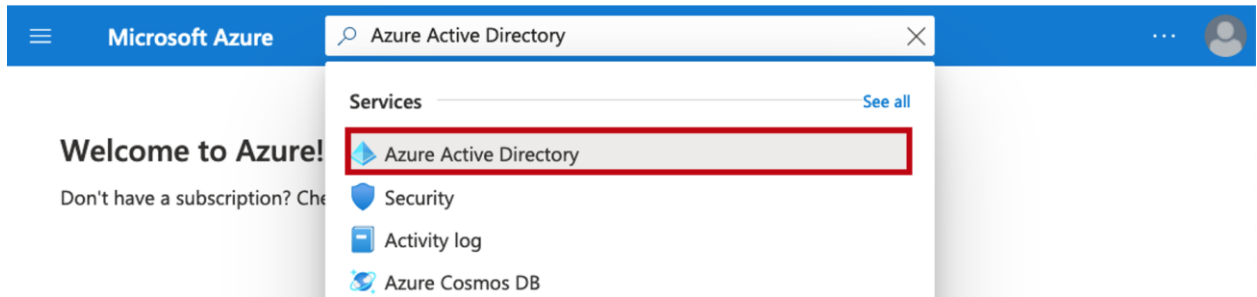
After everything has been configured through both SANtricity System Manager and the Azure application, the connection can then be tested. It is very important to test and resolve any issues before enabling SAML. After SAML is enabled, it cannot be disabled through the user interface.

Solution verification

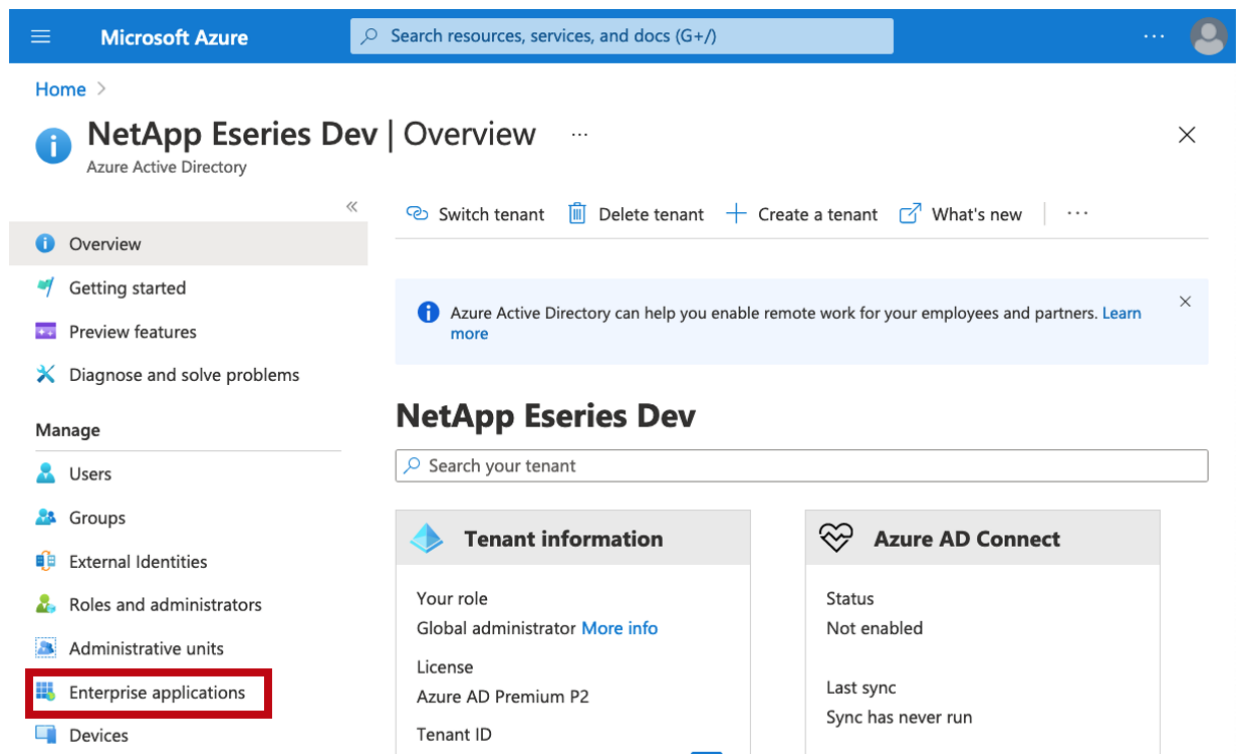
Create the Azure enterprise application

To create the Azure enterprise application, complete the following steps:

1. Open the Azure Portal.
2. In the Search bar, enter Azure Active Directory and select the Azure Active Directory item listed.



3. From the menu on the left, select Enterprise Applications.



4. Click New Application near the top of the page.

Microsoft Azure Search resources, services, and docs (G+/)

Home > NetApp Eseries Dev > Enterprise applications

Enterprise applications | All applications

NetApp Eseries Dev - Azure Active Directory

« **+ New application** Columns Preview features Got feedback?

Try out the new Enterprise Apps search preview! Click to enable the preview. →

Overview

- Overview
- Diagnose and solve problems

Manage



- All applications**
- Application proxy
- User settings
- Collections

Security

Application type: Enterprise Applications Applications status: Any **Apply**

Application visibility: Any **Reset**

First 50 shown, to search all of your applications, enter a display name or the application ID.

Name	Homepage URL	Object ID	Application ID
 eseries-array		b424af80-4fbe-4377...	722b1972-5447-4fa3...
 my-eseries-test-1		23e8ace3-e9b2-4c37...	f73d514e-619f-4859...

5. On the page displayed, click Create Your Own application near the top of the page.

Microsoft Azure Search resources, services, and docs (G+/)

Home > NetApp Eseries Dev > Enterprise applications >

Browse Azure AD Gallery

+ Create your own application Request new gallery app Got feedback?


You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience. →

Search application


Single Sign-on : **All** User Account Management : **All** Categories : **All**

Cloud platforms

Amazon Web Services (AWS)



Google Cloud Platform



6. In the Create your Own dialog box, enter a name for the application, select the Integrate Any Other Application you Don't Find in the Gallery (Non-gallery) option, and click Create.

Create your own application

What's the name of your app?

What are you looking to do with your application?

☐ Configure Application Proxy for secure remote access to an on-premises application
☐ Register an application to integrate with Azure AD (App you're developing)
☒ Integrate any other application you don't find in the gallery (Non-gallery)

We found the following applications that may match your entry
 We recommend using gallery applications when possible.

Dev SAML

Create

7. Wait for the application to be created and for the application Overview page to be displayed.

Microsoft Azure

Search resources, services, and docs (G+)

[Home](#) > [NetApp Eseries Dev](#) > [Enterprise applications](#) > [Browse Azure AD Gallery](#) >

E-Series SAML | Overview

Enterprise Application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Properties

Name ⓘ
E-Series SAML

Application ID ⓘ
b3a39afb-9286-4207-8606-5 ...

Object ID ⓘ
e236d96a-7e65-40c8-8986-9 ...

Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

[Assign users and groups](#)

9

Access Management for NetApp E-Series storage systems
using Azure Active Directory

© 2021 NetApp, Inc. All rights reserved.

Generate SAML signing certificate

For this validation, the default Azure certificate and signing options were used for the application. If needed, changes to the default settings can be made as follows:

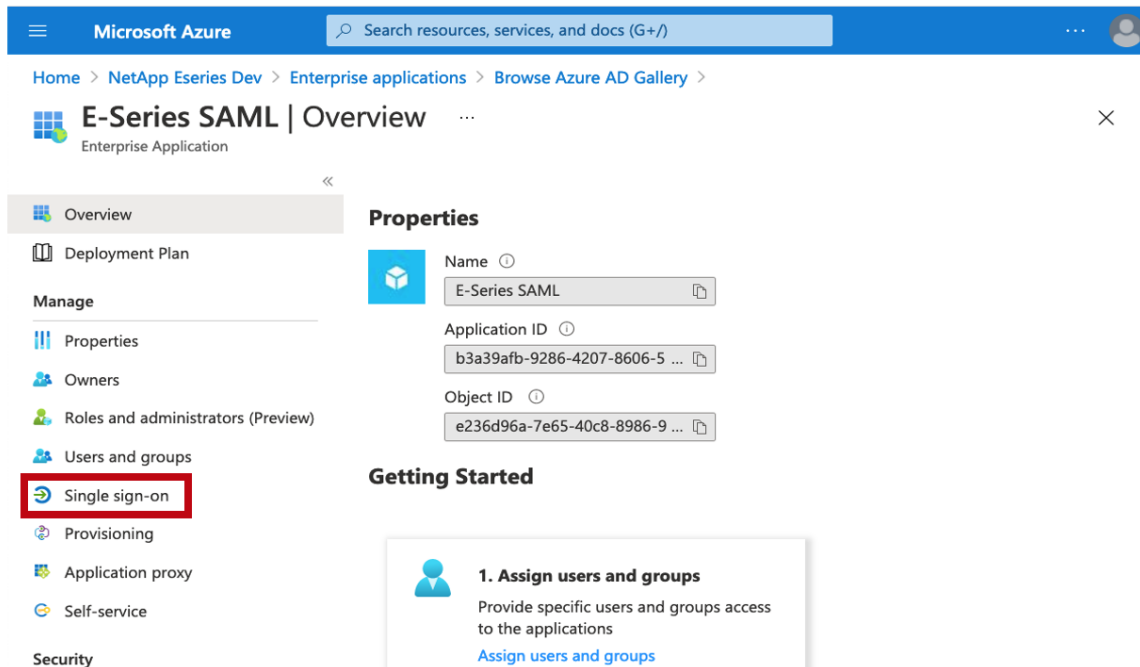
Note: During the validation, it was observed that Azure did not seem to have an option to allow the storage array's signing certificate to be used to authenticate incoming communications to Azure. There was also not an option to provide SAML-enabled encrypted communications between the IdP and the SP.

1. Open the E-Series application through the Azure portal.
2. From the menu on the left, select Single Sign-On.
3. In the SAML Signing Certificate section, select Edit.
4. To generate a new certificate, click New Certificate.
5. To import a certificate, click Import Certificate, select the certificate, and then click Add.
6. From the dialog box, use the drop-down menus to update Signing Option and/or Signing Algorithm.
7. After all the changes are complete, click Save.

IdP metadata file generation and import

To generate and import the IdP metadata file, complete the following steps:

1. On the enterprise application Overview page, from the menu on the left, click Single Sign-On.



2. On the Single Sign-On page, click the SAML panel.

Microsoft Azure Search resources, services, and docs (G+/)

Home > NetApp Eseries Dev > Enterprise applications > Browse Azure AD Gallery > E-Series SAML

E-Series SAML | Single sign-on

Enterprise Application

Select a single sign-on method [Help me decide](#)

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators (Preview)
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service

- On the SAML-Based Sign-On page, scroll down to the SAML Signing Certificate section and click the Download link for Federation Metadata XML to save the file locally.

Note: It can take a minute or two to retrieve the file from Azure before the actual download dialog box is displayed.

Microsoft Azure Search resources, services, and docs (G+/)

Home > NetApp Eseries Dev > Enterprise applications > Browse Azure AD Gallery > E-Series SAML

E-Series SAML | SAML-based Sign-on

Enterprise Application

Upload metadata file Change single sign-on mode Test this application

3 SAML Signing Certificate [Edit](#)

Status	Active
Thumbprint	9CEA37643ACE0D710AD63296857B251D1F CA5C48
Expiration	12/20/2025, 2:50:17 PM
Notification Email	amyv@netapp.com
App Federation Metadata Url	https://login.microsoftonline.com/f4...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up E-Series SAML

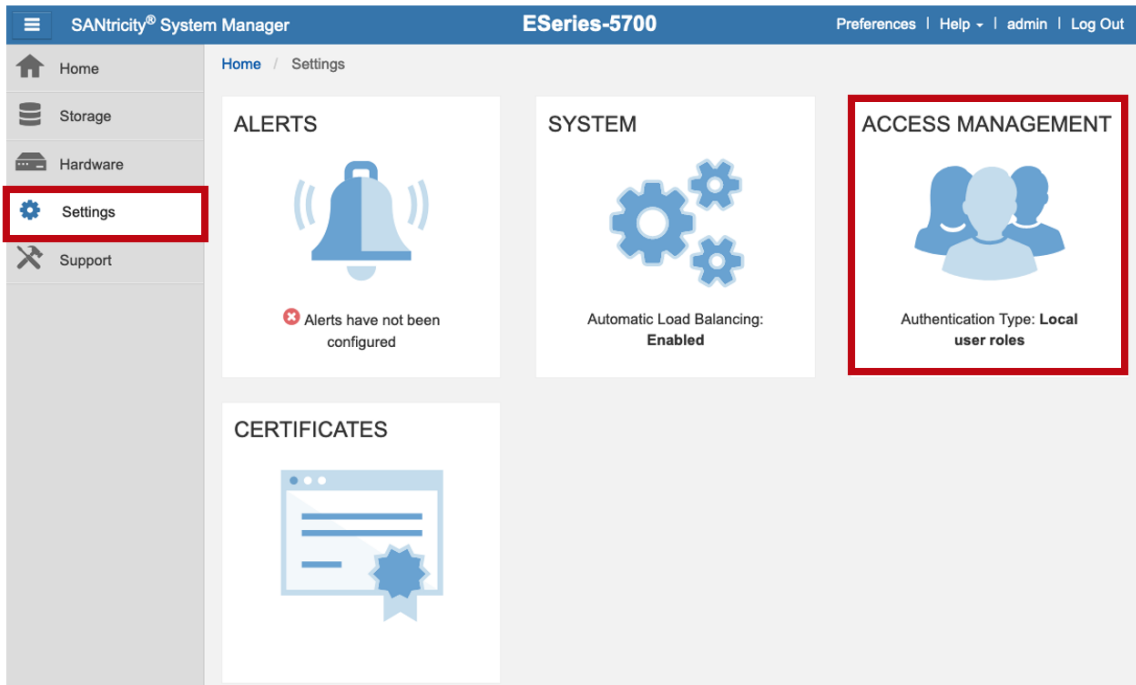
You'll need to configure the application to link with Azure AD.

Login URL <https://login.microsoftonline.com/f4...>

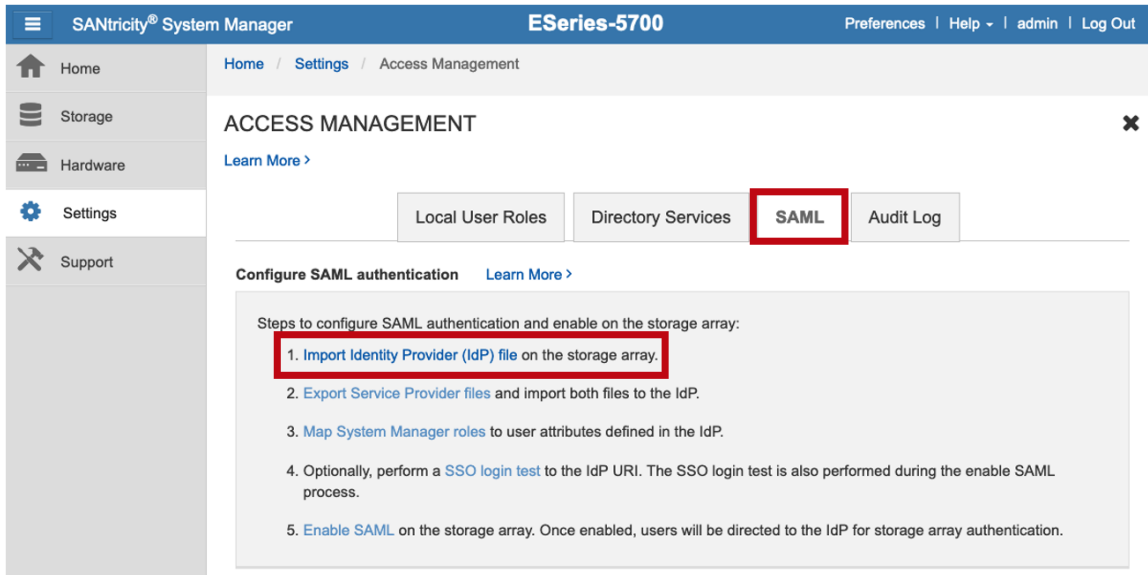
Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators (Preview)
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Security

- For each E-Series storage system being used, perform the following steps:

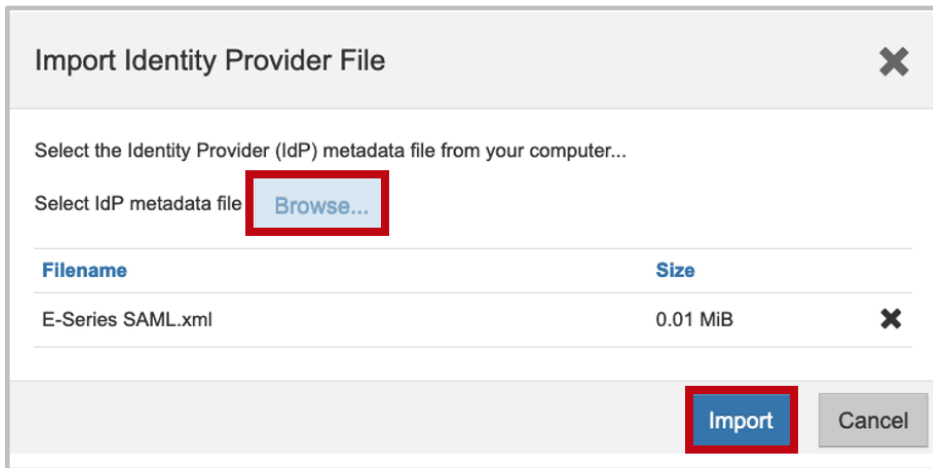
- a. Using one of the controllers, open SANtricity System Manager.
- b. From the left menu, select Settings and then select the Access Management tile.



- c. Select the SAML tab and then click Import Identity Provider (IdP) file.



- d. in the dialog box, click Browse and then browse to and select the Metadata XML file that was saved from Azure. Click Import.



- e. After the file is imported, verify that the IdP entity ID was updated under the SAML tab.

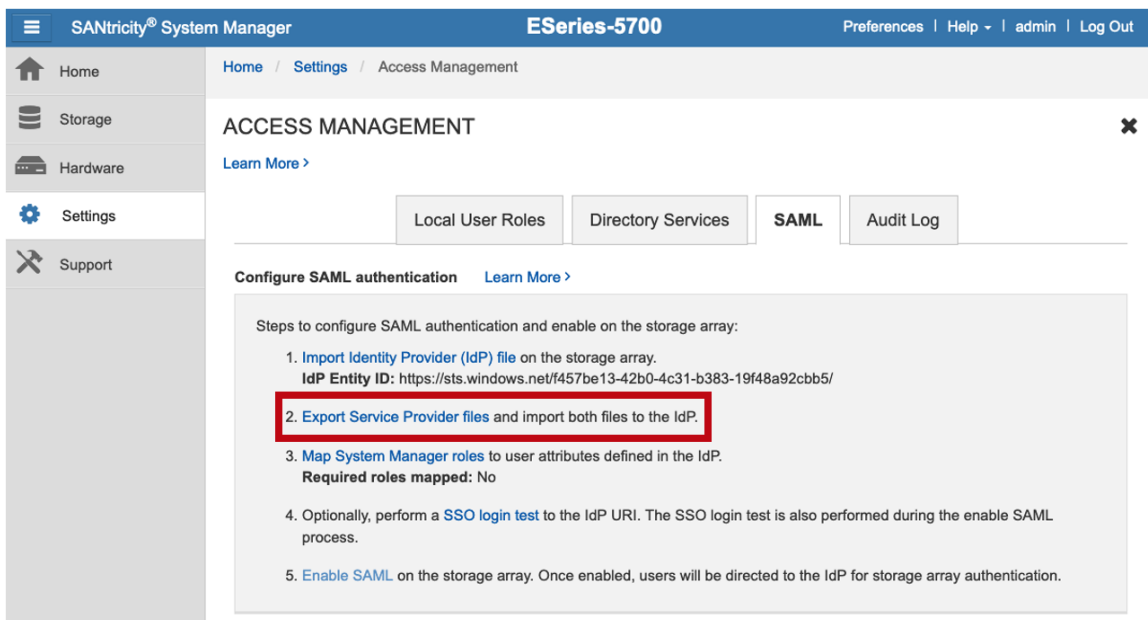
SP metadata file generation and import

Export the SP metadata files from each of the E-Series controllers and then import them to the Azure enterprise application using the following steps:

1. For each of the E-Series storage systems, perform the following steps to export the SP metadata files from all of the controllers:

Note: Although the SP metadata from just one of the controllers will be imported to the Azure enterprise application, the SP metadata must still be exported on all of the controllers that are being configured for access management. If the SP metadata is not exported from a controller, then it will not be able to authenticate with the IdP.

- a. Using one of the controllers, open SANtricity System Manager.
- b. From the menu on the left, select Settings and then select the Access Management tile.
- c. From the SAML tab of SANtricity System Manager, click Export Service Provider files.



- d. Enter the appropriate domain names or IP addresses for both Controller A and Controller B.

Export Service Provider Files

Export the Service Provider metadata files (one per controller)...

Controller A

Domain name ?

10.113.1.101

Export Service Provider metadata file for Controller A

Export

Controller B

Domain name ?

10.113.1.102

Export Service Provider metadata file for Controller B

Export

Close

- e. Click Export for each of the controllers to save off the SP file for each of the controllers and then click Close.

Export Service Provider Files

Export the Service Provider metadata files (one per controller)...

Controller A

Domain name ?

10.113.1.101

Export Service Provider metadata file for Controller A

Export

Controller B

Domain name ?

10.113.1.102

Export Service Provider metadata file for Controller B

Export

Close

2. With this testing, a total of four files were saved off at this point:
 - Metadata for Controller A on the E5700
 - Metadata for Controller B on the E5700
 - Metadata for Controller A on the E280x
 - Metadata for Controller B on the E280x
3. If it is not already, open the Azure portal.
4. Search for and open Azure Active Directory.
5. From the left menu, click the Enterprise Applications.
6. Click the application for the E-Series storage systems.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the path: Home > NetApp Eseries Dev > Enterprise applications. The main heading is 'Enterprise applications | All applications'. Below this, there are filters for 'Application type' (Enterprise Applications) and 'Applications status' (Any), along with an 'Apply' button. There is also a filter for 'Application visibility' (Any) with a 'Reset' button. A search bar prompts the user to enter a display name or application ID. The table below lists the applications:

Name	Homepage URL	Object ID	Application ID
E-Series SAML		e236d96a-7e65-40c...	b3a39afb-9286-4207...
eseries-array		b424af80-4fbe-4377...	722b1972-5447-4fa3...
my-eseries-test-i		23e8ace3-e9b2-4c37...	f73d514e-619f-4859...

7. From the menu on the left, select Single Sign-On.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > NetApp Eseries Dev > Enterprise applications > Browse Azure AD Gallery >

E-Series SAML | Overview

Enterprise Application

- Overview
- Deployment Plan
- Manage
 - Properties
 - Owners
 - Roles and administrators (Preview)
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Application proxy
 - Self-service
- Security

Properties

Name ⓘ
E-Series SAML

Application ID ⓘ
b3a39afb-9286-4207-8606-5 ...

Object ID ⓘ
e236d96a-7e65-40c8-8986-9 ...

Getting Started

- Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)

8. On the SAML-Based Sign-On page, from the top menu, click Upload Metadata File.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > NetApp Eseries Dev > Enterprise applications > Browse Azure AD Gallery > E-Series SAML >

E-Series SAML | SAML-based Sign-on

Enterprise Application

« **Upload metadata file** > Change single sign-on mode Test this application ...

- SAML Signing Certificate** [Edit](#)

Status	Active
Thumbprint	9CEA37643ACE0D710AD63296857B251D1F CA5C48
Expiration	12/20/2025, 2:50:17 PM
Notification Email	amyv@netapp.com
App Federation Metadata Url	https://login.microsoftonline.com/f4...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download
- Set up E-Series SAML**


You'll need to configure the application to link with Azure AD.

Login URL <https://loain.microsoftonline.com/f4...>

9. Browse for and select the SP metadata file for controller A on the E5700 and then click Add.

Upload metadata file.

Values for the fields below are provided by E-Series SAML. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by E-Series SAML.




- In the dialog box, add the information for the remaining controllers to the Identifier (Entity ID) and Reply URL (Assertion Consumer Service URL) sections.

Basic SAML Configuration ×

 Save





Identifier (Entity ID) * ⓘ

The default identifier will be the audience of the SAML response for IDP-initiated SSO

	Default
10.113.1.90	<input type="checkbox"/> ⓘ 
10.113.1.59	<input type="checkbox"/> ⓘ 
10.113.1.102	<input type="checkbox"/> ⓘ 
10.113.1.101	<input checked="" type="checkbox"/> ⓘ 
<input type="text"/>	

Reply URL (Assertion Consumer Service URL) * ⓘ

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

	Default
https://10.113.1.90/devmgr/v2/saml/assertion	<input type="checkbox"/> ⓘ 
https://10.113.1.59/devmgr/v2/saml/assertion	<input type="checkbox"/> ⓘ 
https://10.113.1.102/devmgr/v2/saml/assertion	<input type="checkbox"/> ⓘ 
https://10.113.1.101/devmgr/v2/saml/assertion	<input checked="" type="checkbox"/> ⓘ 
<input type="text"/>	

- Leave all the remaining sections set to their default values and click Save.

Basic SAML Configuration



Save

<https://10.113.1.101/devmgr/v2/saml/assertion>

Sign on URL ⓘ

Relay State ⓘ

Logout Url ⓘ

Configure role mappings

Configure role mappings for both the Azure enterprise application and SANtricity System Manager by using the following steps:

Note: Only certain Azure accounts can be used to create roles and groups. For this testing, an Azure login with the Privileged Authentication Administrator role was used to create the roles and assign them to groups.

Note: Only certain SANtricity System Manager accounts can be used to create roles. For this testing, a SANtricity System Manager role that had full privileges was used to create the new role mappings.

There are multiple steps involved in this process. They are grouped as follows:

1. Azure AD: Create the application role
2. Azure AD: Create the application group
3. Azure AD: Assign the application group
4. Azure AD: Add users to groups
5. Azure AD: Configure user attributes and claims
6. SANtricity System Manager: Configure Role mapping

Azure AD: Create the application role

To create the necessary groups in Azure AD, complete the following steps:

1. If it is not already, open the Azure portal.
2. Search for and open Azure Active Directory.
3. From the menu on the left, click App Registrations and then click the E-Series enterprise application.

Microsoft Azure

Search resources, services, and docs (G+)

Home > NetApp Eseries Dev

NetApp Eseries Dev | App registrations

Azure Active Directory

Users Groups External Identities Roles and administrators Administrative units Enterprise applications Devices **App registrations** Identity Governance Application proxy Licenses

New registration Endpoints Troubleshooting Download

All applications **Owned applications** Deleted applications (Preview)

Start typing a name or Application ID to filter these results

Display name	Application (client) ID	Created on	Certificates & secrets
ES E-Series SAML	b3a39afb-9286-4207-...	5/12/2021	-

4. From the menu on the left, click App Roles and then click Create App Role.

Microsoft Azure

Search resources, services, and docs (G+)

Home > NetApp Eseries Dev > E-Series SAML

E-Series SAML | App roles

Search (Cmd+/) Create app role Got feedback?

Authentication Certificates & secrets Token configuration API permissions Expose an API **App roles** Owners Roles and administrators | Preview Manifest

App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

[How do I assign App roles](#)

Display name	Description	Allowed member ty...	Value
User	User	Users/Groups	
msiam_access	msiam_access	Users/Groups	

5. On the dialog displayed, perform the following steps:
 - a. In the Display Name field and in the Value field, enter GlobalAdminUser (no spaces).
 - b. From the Allowed Member Types options, select Users/Groups.
 - c. In the Description field, enter SANtricity Global Admin User role.

Click Apply.

Create app role

Display name * ⓘ

Allowed member types * ⓘ ☒ Users/Groups ☐ Applications ☐ Both (Users/Groups + Applications)

Value * ⓘ

Description * ⓘ

Apply Cancel

6. To create each of the remaining roles, repeat steps 4 and 5:
 - MonitorUsers
 - SecurityAdminUser
 - StorageAdminUser
7. Verify that the newly added roles are present and have the correct values.

E-Series SAML | App roles

App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

How do I assign App roles

Display name	Description	Allowed me...	Value
User	User	Users/Groups	
msiam_access	msiam_access	Users/Groups	
GlobalAdminUser	SANtricity Global Admin User role	Users/Groups	GlobalAdminUser
MonitorUser	SANtricity Monitor User role	Users/Groups	MonitorUser
SecurityAdminUser	SANtricity Security Admin User role	Users/Groups	SecurityAdminUser
StorageAdminUser	SANtricity Storage Admin User role	Users/Groups	StorageAdminUser

Azure AD: Create the application group

To add the necessary application groups, complete the following steps:

1. Search for and open Azure Active Directory.
2. From the menu on the left, select Groups.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header with the 'Microsoft Azure' logo and a search bar. Below the header, the breadcrumb trail reads 'Home >'. The main title is 'NetApp Eseries Dev | Overview (Preview)' with a close button. The left-hand navigation pane is expanded, showing various options. The 'Groups' option, represented by a group of people icon, is highlighted with a red rectangular box. Other options in the pane include 'Overview (Preview)', 'Preview features', 'Diagnose and solve problems', 'Manage' (with sub-items like Users, External Identities, Roles and administrators, Administrative units, Enterprise applications, and Devices), and 'Users'.

3. On the All Groups page, click New Group.

The screenshot shows the 'Groups | All groups' page in the Microsoft Azure portal. The breadcrumb trail is 'Home > NetApp Eseries Dev >'. The main title is 'Groups | All groups' with a close button. The left-hand navigation pane is expanded, showing 'All groups', 'Deleted groups', 'Diagnose and solve problems', 'Settings' (with sub-items like General, Expiration, and Naming policy), and 'Activity' (with sub-items like Privileged access groups (Preview), Access reviews, and Audit logs). The top action bar contains several buttons: '+ New group' (highlighted with a red rectangle), 'Download groups', 'Delete', 'Refresh', 'Columns', and a menu icon. Below the action bar, there's a search bar labeled 'Search groups' and an 'Add filters' button. A table of groups is displayed below the search bar. The table has columns for 'Name', 'Object Id', 'Group Type', and 'Membership Ty...'. One group is listed with the name 'hello', Object Id '9dec8571-dc2a-4aa2...', Group Type 'Security', and Membership Type 'Assigned'.

Name	Object Id	Group Type	Membership Ty...
<input type="checkbox"/> HE hello	9dec8571-dc2a-4aa2...	Security	Assigned

4. In the New Group dialog box, complete the following steps:
 - a. In the name field, enter SANtricity Global Admin User.

- b. Set the Azure AD Roles Can Be Assigned to the Group value to Yes.
- c. Click Create.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > NetApp Eseries Dev > Groups >

New Group

Group type * ⓘ
Security

Group name * ⓘ
SANtricity Global Admin User

Group description ⓘ
Enter a description for the group

Azure AD roles can be assigned to the group (Preview) ⓘ
☒ Yes ☐ No

Membership type ⓘ
Assigned

Create

5. In the New Group confirmation dialog box, select Yes.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > NetApp Eseries Dev > Groups >

New Group

Creating a group to which Azure AD roles can be assigned is a setting that cannot be changed later. Are you sure you want to add this capability? [Learn More.](#)

☒ Yes ☐ No

6. To create the remaining groups, repeat steps 3 through 5:
 - SANtricity Monitor Users
 - SANtricity Security Admin Users
 - SANtricity Storage Admin Users
7. Verify that the groups are displayed correctly.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > NetApp Eseries Dev >

Groups | All groups

NetApp Eseries Dev - Azure Active Directory

+ New group | Download groups | Delete | Refresh | Columns | ...

This page includes previews available for your evaluation. View previews →

Search groups | Add filters

	Name	Group Type	Membership Ty...	Email
<input type="checkbox"/>	SS SANtricity Storage Admin Users	Security	Assigned	
<input type="checkbox"/>	SS SANtricity Security Admin Users	Security	Assigned	
<input type="checkbox"/>	SM SANtricity Monitor Users	Security	Assigned	
<input type="checkbox"/>	SG SANtricity Global Admin User	Security	Assigned	
<input type="checkbox"/>	HE hello	Security	Assigned	

Settings

- General
- Expiration
- Naming policy

Activity

- Privileged access groups (Preview)
- Access reviews

Azure AD: Assign the application group

To assign the groups to the E-Series application, complete the following steps:

1. Search for and open Azure Active Directory.
2. From the menu on the left, select Enterprise Applications.
3. Select the E-Series enterprise application.
4. From the menu on the left, click Users and Groups and then click Add User/Group.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > NetApp Eseries Dev > Enterprise applications > E-Series SAML

E-Series SAML | Users and groups

Enterprise Application

+ Add user/group | Edit | Remove | Update Credentials | Columns | ...

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

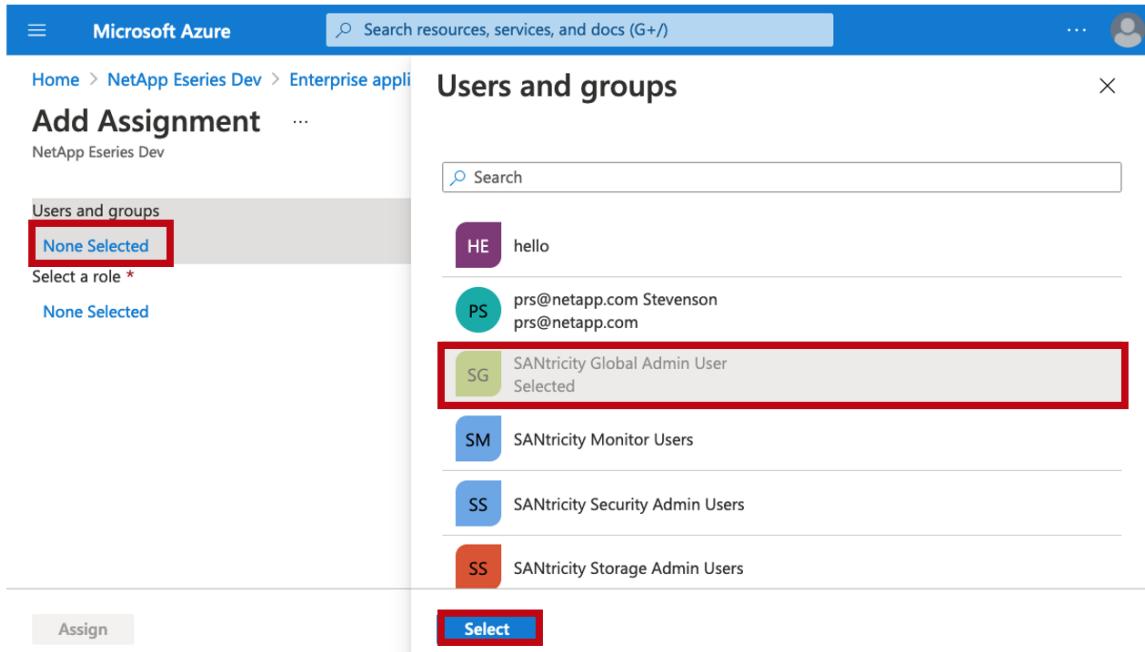
First 100 shown, to search all users & groups, enter a display name.

Display Name	Role assigned
No application assignments found	

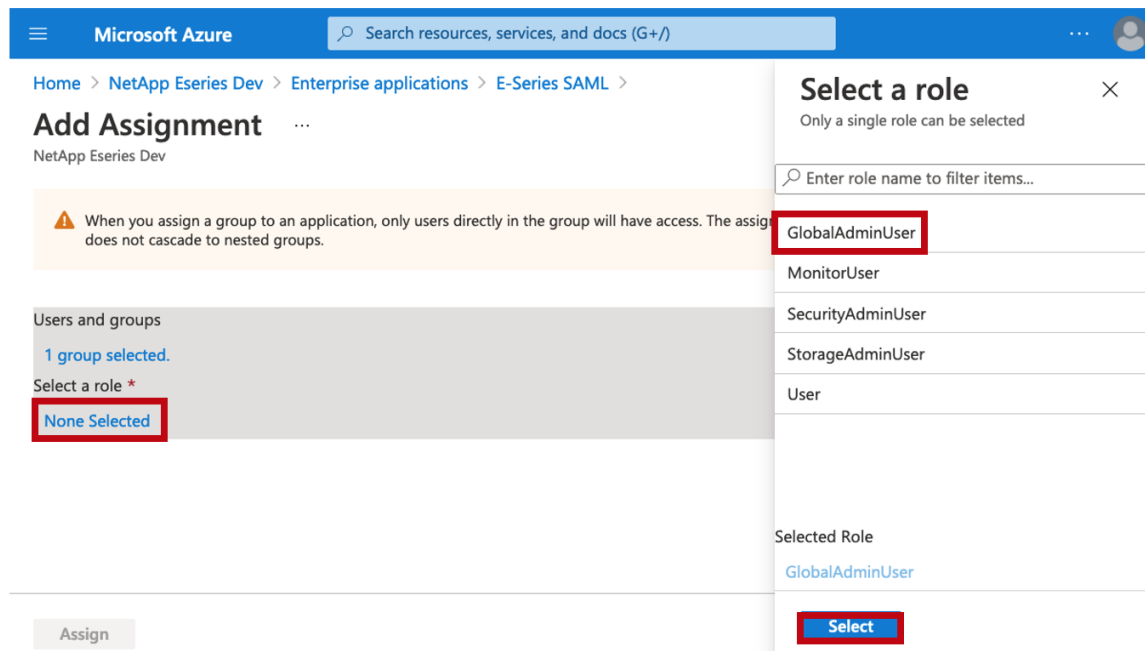
Manage

- Properties
- Owners
- Roles and administrators (Preview)
- Users and groups**
- Single sign-on

5. On the Add Assignments page, complete the following steps to add the appropriate group:
 - a. Under Users and Groups, click None Selected.
 - b. In the Users and Groups dialog box, click SANtricity Global Admin User and then click Select.



6. On the same page, perform the following steps to add the appropriate role:
 - a. Under Users and Groups, click None Selected.
 - b. In the Select a Role dialog box, click GlobalAdminUser.
 - c. Click Select.



7. On the Add Assignment page, click Assign.

Microsoft Azure Search resources, services, and docs (G+/)

Home > NetApp Eseries Dev > Enterprise applications > E-Series SAML >

Add Assignment

NetApp Eseries Dev

⚠ When you assign a group to an application, only users directly in the group will have access. The assignment does not cascade to nested groups.

Users and groups

1 group selected.

Select a role *

GlobalAdminUser

Assign

8. To add the remaining groups and assign the specified roles, repeat steps 4 through 7. Table 3 lists all the groups (and their assigned roles) that should be created.

Table 3) Azure AD groups and roles.

Group	Role
NetApp SANtricity System Global Admin Users	GlobalAdminUser
NetApp SANtricity System Monitor Users	MonitorUser
NetApp SANtricity System Security Admin Users	SecurityAdminUser
NetApp SANtricity System Storage Admin Users	StorageAdminUser

9. Verify that all groups and their assigned roles are correct.

Microsoft Azure Search resources, services, and docs (G+/)

Home > NetApp Eseries Dev > Enterprise applications > E-Series SAML

E-Series SAML | Users and groups

Enterprise Application

« + Add user/group Edit Remove Update Credentials Columns ...

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.

First 100 shown, to search all users & groups, enter a display name.

Display Name	Role assigned
<input type="checkbox"/> SG SANtricity Global Admin User	GlobalAdminUser
<input type="checkbox"/> SM SANtricity Monitor Users	MonitorUser
<input type="checkbox"/> SS SANtricity Security Admin Users	SecurityAdminUser
<input type="checkbox"/> SS SANtricity Storage Admin Users	StorageAdminUser

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

Azure AD: Add users to groups

To assign users to each of the groups, complete the following steps:

1. Search for and open Azure Active Directory.
2. From the menu on the left, click Groups and then click on the group to which you would like to add users. In this example, we added a user to SANtricity Global Admin Users, so we selected that group.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo and a search bar. The left sidebar contains navigation options: Home, NetApp Eseries Dev, Groups, and All groups. The main content area displays the 'All groups' page for 'NetApp Eseries Dev - Azure Active Directory'. A table lists several groups, with the 'SANtricity Global Admin User' group highlighted by a red box. The table columns are Name, Group Type, Membership Ty..., and Email.

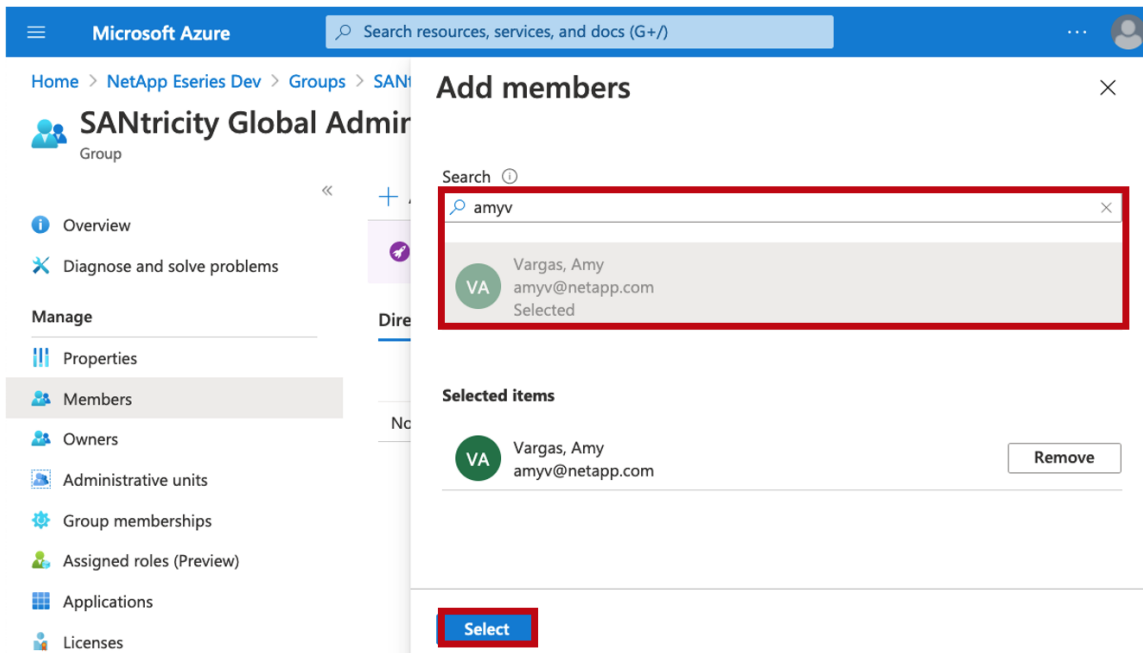
Name	Group Type	Membership Ty...	Email
HE hello	Security	Assigned	
SG SANtricity Global Admin User	Security	Assigned	
SM SANtricity Monitor Users	Security	Assigned	
SS SANtricity Security Admin Users	Security	Assigned	
SS SANtricity Storage Admin Users	Security	Assigned	

3. From the menu on the left, click Members and then click Add Members.

The screenshot shows the Microsoft Azure portal interface for the 'SANtricity Global Admin User | Members' page. The left sidebar contains navigation options: Overview, Diagnose and solve problems, Manage, Properties, Members, Owners, Administrative units, Group memberships, Assigned roles (Preview), and Applications. The 'Members' link is highlighted with a red box. The main content area displays the 'Add members' button, which is also highlighted with a red box. Below the button, there is a section for 'Direct members' with a table showing no members found.

Name	Type	Email	User type
No members have been found			

4. In the dialog box, complete the following steps:
 - a. Search for and select each user that should be added as a member.
 - b. After all members have been selected, click Select.



5. To assign the appropriate members to all the remaining groups, repeat steps 2 through 4.

Azure AD: Configure user attributes and claims

To configure the user attributes and claims, complete the following steps:

1. Search for and open Azure Active Directory.
2. From the menu on the left, click Enterprise Applications.
3. Click the E-Series application.
4. From the menu on the left, click Single Sign-On.
5. On the SAML-Based Sign-On page, scroll down to the User Attributes & Claims section and click Edit.

Microsoft Azure

Search resources, services, and docs (G+)

Home > NetApp Eseries Dev > Enterprise applications > E-Series SAML >

E-Series SAML | SAML-based Sign-on

Enterprise Application

Upload metadata file Change single sign-on mode Test this application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

2 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate

Status	Active
Thumbprint	6321A03372B8B304D87A7A33A814C4801D3884EE
Expiration	5/12/2024, 11:43:11 AM

6. Click on the value for the Unique User Identifier (Name ID) to change it.

Note: The Unique User Identifier is used to specify the field from the user database that will be reported as the name of the user. When a user is successfully authenticated, this name is displayed in SANtricity System Manager as the current user. In the following example, we want to use a value of `user.mail` instead of `user.principalname`.

Microsoft Azure

Search resources, services, and docs (G+)

Home > NetApp Eseries Dev > Enterprise applications > E-Series SAML > SAML-based Sign-on >

User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ***]

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ***

7. On the Manage Claim page, complete the following steps:
 - a. From the Source Attribute drop-down menu, select `user.mail`.
 - b. Click Save.

Microsoft Azure Search resources, services, and docs (G+)

Enterprise applications > E-Series SAML > SAML-based Sign-on > User Attributes & Claims

Manage claim

Save Discard changes

Name nameidentifier

Namespace http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

Name identifier format * Email address

Source * ☒ Attribute ☐ Transformation

Source attribute * user.mail

Claim conditions

8. After the update to the Unique User Identifier completes, click Add New Claim.

Microsoft Azure Search resources, services, and docs (G+)

Home > NetApp Eseries Dev > Enterprise applications > E-Series SAML > SAML-based Sign-on

User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.mail [nameid-format:emailAddr... ***

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ***

9. On the page displayed, perform the following steps:
- In the Name field, enter Role.
 - For the Source Attribute option, select user.assignedroles.
 - Click Save.

Microsoft Azure Search resources, services, and docs (G+)

Enterprise applications > E-Series SAML > SAML-based Sign-on > User Attributes & Claims >

Manage claim

Save Discard changes

Name * **role** ✓

Namespace Enter a namespace URI ✓

Source * ☒ Attribute ☐ Transformation

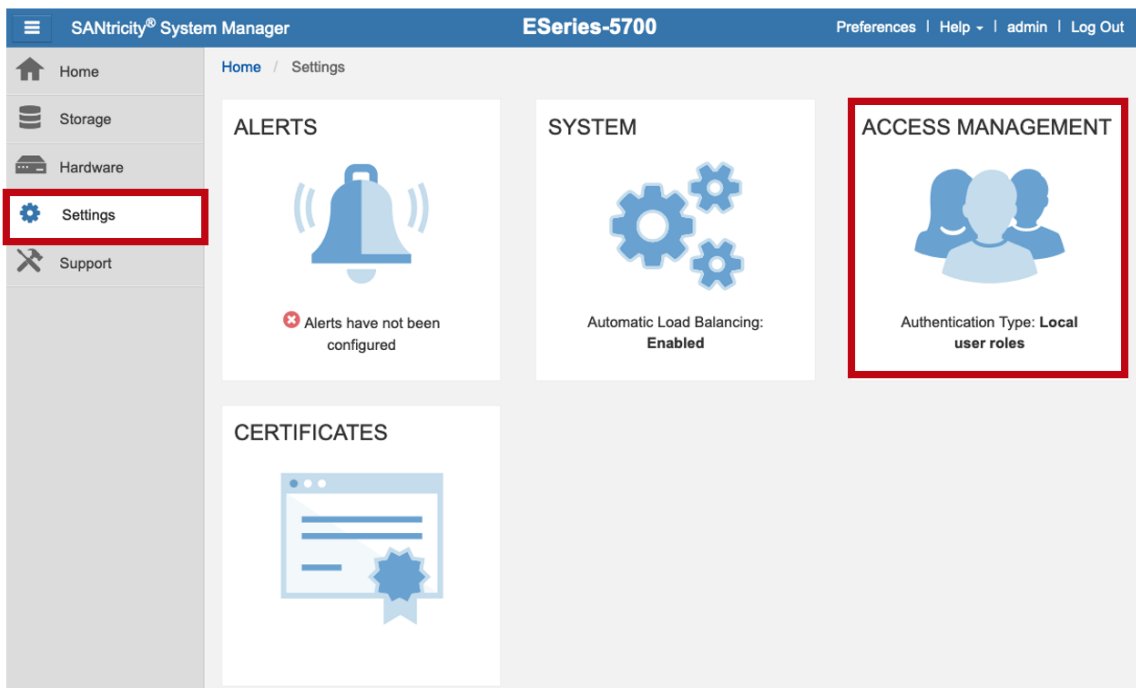
Source attribute * **user.assignedroles** ✓

Claim conditions

SANtricity System Manager: Role mapping configuration

To configure SANtricity System Manager role mapping, complete the following steps:

1. For each E-Series storage system, complete the following steps:
 - a. Using either controller, open SANtricity System Manager for the E-Series storage system.
 - b. From the menu on the left, select Settings and the select the Access Management tile.



- c. Select the SAML tab and then click Map System Manager Roles.

SANtricity® System Manager
ESeries-5700
Preferences | Help | admin | Log Out

Home
Storage
Hardware
Settings
Support

Home / Settings / Access Management
ACCESS MANAGEMENT
Learn More >

Local User Roles
Directory Services
SAML
Audit Log

Configure SAML authentication
Learn More >

Steps to configure SAML authentication and enable on the storage array:

1. [Import Identity Provider \(IdP\) file](#) on the storage array.
IdP Entity ID: <https://sts.windows.net/f457be13-42b0-4c31-b383-19f48a92cbb5/>
2. [Export Service Provider files](#) and import both files to the IdP.
3. [Map System Manager roles](#) to user attributes defined in the IdP.
Required roles mapped: No
4. Optionally, perform a [SSO login test](#) to the IdP URI. The SSO login test is also performed during the enable SAML process.
5. [Enable SAML](#) on the storage array. Once enabled, users will be directed to the IdP for storage array authentication.

d. Add the appropriate role mappings and then click Save.

Mappings

User Attribute	Attribute Value	Roles
role	monitoruser	<div> <div>Monitor</div> <div>Click to choose</div> </div>
role	securityadminuser	<div> <div>Monitor</div> <div>Security admin</div> <div>Click to choose</div> </div>
role	globaladminuser	<div> <div>Monitor</div> <div>Support admin</div> <div>Storage admin</div> <div>Security admin</div> <div>Click to choose</div> </div>
role	storageadminuser	<div> <div>Monitor</div> <div>Storage admin</div> <div>Click to choose</div> </div>

+ Add another mapping

Test and enable SAML

To verify the connection and enable SAML, complete the following steps:

1. On each of the E-Series storage systems, perform the following steps:
 - a. Using either controller, open SANtricity System Manager for the E-Series storage system.
 - b. From the menu on the left, select Settings.

- c. On the Access Management page, select the Access Management tile.
- d. Select the SAML tab.
- e. Click SSO Login Test.

Home / Settings / Access Management

ACCESS MANAGEMENT

[Learn More >](#)

Local User Roles Directory Services **SAML** Audit Log

Configure SAML authentication [Learn More >](#)

Steps to configure SAML authentication and enable on the storage array:

1. [Import Identity Provider \(IdP\) file](#) on the storage array.
IdP Entity ID: <https://sts.windows.net/f457be13-42b0-4c31-b383-19f48a92cbb5/>
2. [Export Service Provider files](#) and import both files to the IdP.
3. [Map System Manager roles](#) to user attributes defined in the IdP.
Required roles mapped: No
4. Optionally, perform a [SSO login test](#) to the IdP URI. The SSO login test is also performed during the enable SAML process.
5. [Enable SAML](#) on the storage array. Once enabled, users will be directed to the IdP for storage array authentication.

- f. In the dialog box, enter the log-in credentials for a user with both Security Admin and Monitor permissions. If needed, enable pop-up dialogs through the browser for each of the controllers in the E-Series storage system. Failure to do so could cause the test to run indefinitely or even fail.
- g. Verify that a message is displayed indicating the test is successful. Before proceeding to the next step, it should be noted that after SAML is enabled, it cannot be disabled through the user interface. Therefore, it is imperative that the SSO Login test passes successfully before enabling SAML.
- h. After the SSO Login test passes successfully, click Enable SAML..

Home / Settings / Access Management

ACCESS MANAGEMENT

[Learn More >](#)

Local User Roles Directory Services **SAML** Audit Log

Configure SAML authentication [Learn More >](#)

Steps to configure SAML authentication and enable on the storage array:

1. [Import Identity Provider \(IdP\) file](#) on the storage array.
IdP Entity ID: <https://sts.windows.net/f457be13-42b0-4c31-b383-19f48a92cbb5/>
2. [Export Service Provider files](#) and import both files to the IdP.
3. [Map System Manager roles](#) to user attributes defined in the IdP.
Required roles mapped: No
4. Optionally, perform a [SSO login test](#) to the IdP URI. The SSO login test is also performed during the enable SAML process.
5. [Enable SAML](#) on the storage array. Once enabled, users will be directed to the IdP for storage array authentication.

- i. In the confirmation dialog box, enter Enable and then click Enable.

Note: After SAML is enabled, all other authentication methods such as local users and LDAP are disabled.

Confirm Enable SAML

SAML Authentication Will Be Enabled on the Storage Array

Once enabled, users will be authenticated via the configured Identity Provider. Directory services and local user role access to the storage array will be prohibited.

Note: SAML cannot be disabled using System Manager. Physical access to the serial port on the controller is required.

[Which external management tools may be affected by this change?](#)

Type ENABLE to confirm that you want to perform this operation.

ENABLE

Enable

Cancel

- j. From the SAML tab, verify that the new IdP Entity ID is displayed.

SANtricity® System Manager

ESeries-5700

Preferences | Help | admin | Log Out

Home

Storage

Hardware

Settings

Support

Home / Settings / Access Management

ACCESS MANAGEMENT

Learn More >

Local User Roles | Directory Services | SAML | Audit Log

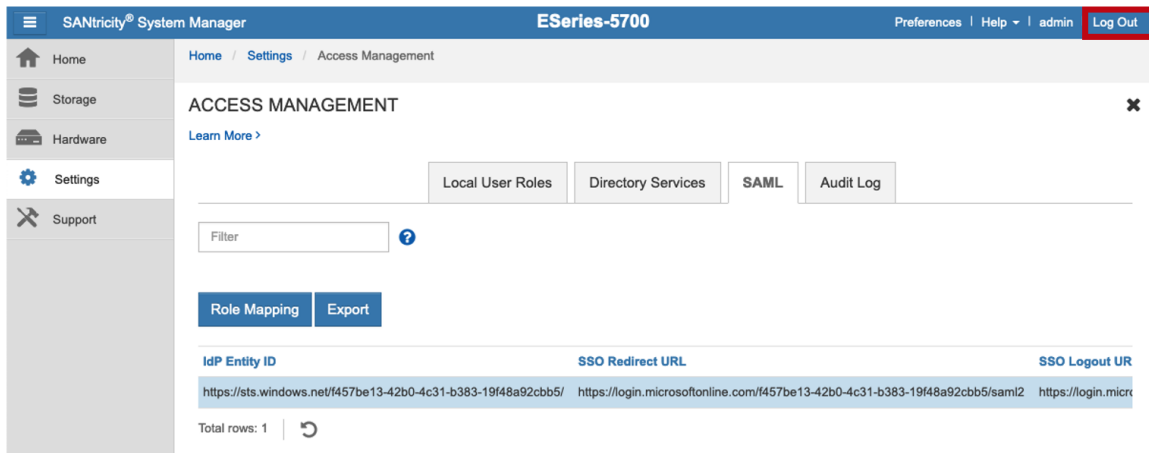
Filter ?

Role Mapping | Export

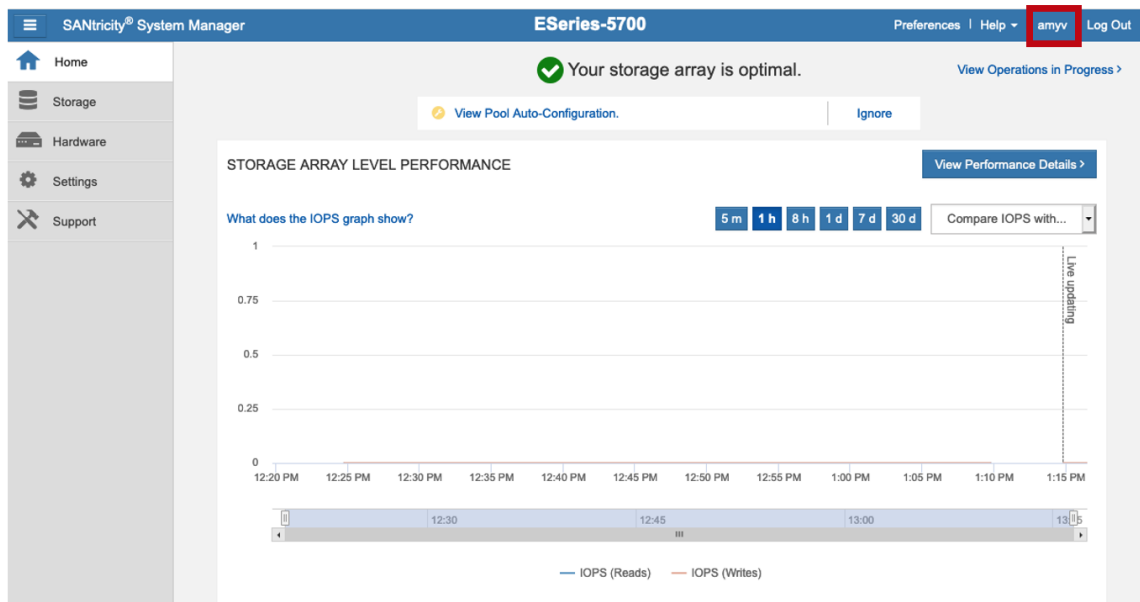
IdP Entity ID	SSO Redirect URL	SSO Logout UR
https://sts.windows.net/f457be13-42b0-4c31-b383-19f48a92cbb5/	https://login.microsoftonline.com/f457be13-42b0-4c31-b383-19f48a92cbb5/saml2	https://login.micr

Total rows: 1

2. On each of the E-Series storage system controllers that are currently logged in, complete the following steps:
 - a. In the upper-right corner, click Log Out.



- b. When the page is displayed showing that the log out was successful, complete the following steps. On shared systems, these steps should always be performed to ensure the user is properly logged out of SANtricity before the next user logs in.
 - i. Close the browser window.
 - ii. Clear the browser history.
 - iii. Reopen the browser window for the controller.
 - iv. Enter the appropriate username and password when prompted.
- c. Verify that the Azure AD user is now displayed in the upper-right corner.



Conclusion

In this document, it was verified that SANtricity System Manager can be successfully configured to use Azure AD for access management. After they are properly configured, users and administrators can

benefit from having a centralized identity platform that allows for seamless and secure access to SANtricity System Manager.

Where to find additional information

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

- Access Management for E-Series Storage Systems Technical Report
<https://www.netapp.com/media/19404-tr-4853.pdf>
- NetApp Product Documentation
<https://www.netapp.com/support-and-training/documentation/>

Version history

Version	Date	Document version history
Version 1.0	June 2021	Initial release.

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

Copyright © 2021 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

NVA-1161-DEPLOY-0621