

NexLog
Advanced Recording Solutions



Authentication & Active Directory
Implementation Guide
Version 2025.1[6258]

Copyright 2025 Eventide Communications LLC

P/N: #141341 Version 2025.1[6258]

Every effort has been made to make this guide as complete and accurate as possible, but Eventide Communications LLC DISCLAIMS ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. The information provided is on an "as-is" basis and is subject to change without notice or obligation. Eventide Communications LLC has neither liability nor responsibility to any person or entity with respect to loss or damages arising from the information contained in this guide.

Notice: This computer program and its documentation are protected by copyright law and international treaties. Any unauthorized copying or distribution of this program, its documentation, or any portion thereof may result in severe civil and criminal penalties.

The software installed in accordance with this documentation is copyrighted and licensed by Eventide Communications LLC under separate license agreement. The software may only be used pursuant to the terms and conditions of such license agreement. Any other use may be a violation of law.

NexLog, and Speech Factor are registered trademarks of Eventide Communications LLC.

Eventide is a registered trademark of Eventide Inc.

Eventide Communications is a trademark of Eventide Communications LLC.

All other trademarks contained herein are the property of their respective owners.

Eventide Communications LLC

One Alsan Way

Little Ferry, NJ 07643

201-641-1200

www.eventidecommunications.com

Table Of Contents

1. Introduction

1.1. Welcome	7
1.2. Customer Support Information	7
1.2.1. Identifying NexLog DX-Series Model and Version	7

2. Authentication Modes

2.1. Choosing the Right Mode	12
2.2. Setting the Authentication Mode	13

3. Local Authentication

4. SMB Authentication

4.1. How It Works	17
4.2. Prerequisites	18
4.3. Create the File Share	18
4.4. Configure SMB Authentication	19
4.5. Create SMB Users	19
4.5.1. SMB Usernames	19
4.5.2. SMB Passwords	20

5. LDAP Authentication

5.1. How It Works	17
5.2. Prerequisites	18
5.3. Create the LDAP Bind Account	22
5.4. Configure LDAP Authentication	23
5.4.1. LDAP Configuration	23
5.4.2. LDAPS Configuration	26

6. Active Directory Authentication

6.1. How It Works	17
6.2. Prerequisites	18
6.3. Configure Time Sync	33
6.4. Configure Hostname	34
6.5. Configure TLS	34
6.6. Configure AD Authentication	35
6.6.1. Create AD User	35
6.6.2. Set Service Principals	36
6.6.3. Create Keytab	38
6.6.4. Deploy AD Configuration	39
6.6.5. Joining the Domain	44
6.6.6. Single Sign-On	44

7. SAML Authentication

7.1. How It Works	17
7.2. Prerequisites & Considerations	53
7.3. Identity Provider Implementation Guides	54
7.3.1. ADFS Configuration	54
7.3.2. Duo Configuration	72
7.3.3. Entra ID Configuration	79
7.3.4. Okta Configuration	88
7.4. Configuring the recorder	95
7.4.1. Recorder SAML Configuration	95

8. Users and Groups

8.1. Local Users with LDAP	101
8.2. Domain Users with LDAP Group Mapping	101
8.2.1. Enable LDAP Group Mapping	102
8.2.2. Export Recorder Groups to LDAP	103
8.3. Domain Users without LDAP Group Mapping	104
8.4. Passwords	104

9. NexLog Access Bridge	
9.1. NAB with Active Directory	105
9.1.1. NAB with Single Sign-On	105
9.2. NAB with SMB	106
9.3. NAB Base Database Exemption	106

A. Troubleshooting

B. AD Powershell Script

1. INTRODUCTION

1.1. Welcome

Welcome and congratulations on your purchase of the Active Directory software option for use with an Eventide NexLog DX-Series and Eventide MediaWorks DX software.

This guide will help you maximize the use of your product. It includes:

- Explanation of the NexLog DX-Series authentication modes.
- Step-by-step instructions on how to configure the available authentication modes.
- Troubleshooting steps for common issues.

1.2. Customer Support Information

Eventide is committed to your satisfaction. If, after using this manual, you still have questions about the operation of your recorder, contact the Eventide Service department

Web: service.eventidecommunications.com

Email: service@eventidecommunications.com

Phone: +1 (201) 641-1200, option 6, option 2

The Eventide website has additional information that may be helpful. Go to www.eventidecommunications.com.

1.2.1. Identifying NexLog DX-Series Model and Version

You may need to identify the software version and serial number for the following products/components:

- NexLog DX-Series Recorder Software: On the touch screen Front Panel or with a monitor and mouse attached (while the recorder is running), do the following to display the version information:

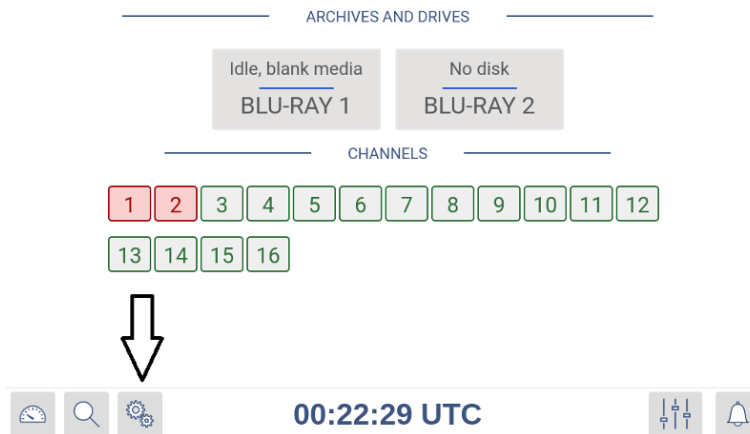


Fig. 1.1 Front Panel Replay Screen (with arrow pointing to Setup button)

- Select the third icon on the lower left featuring two gears.
- The Recorder Serial Number and Current Firmware Version should be displayed.

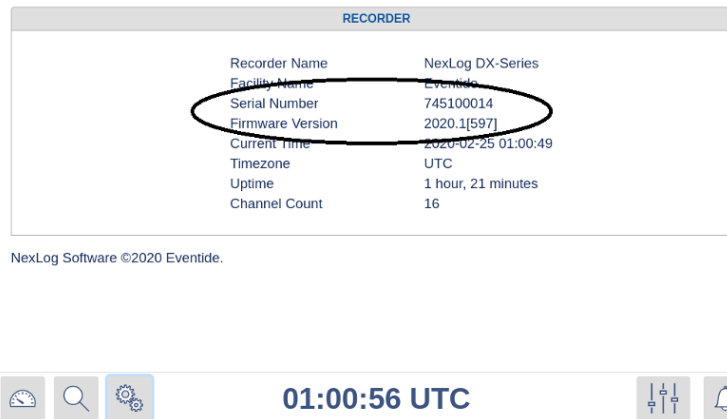


Fig. 1.2 Front Panel Setup Screen (with serial and software version circled)

Alternatively, you can get the version and serial number remotely via the Web-based NexLog DX-Series Configuration Manager:

- Navigate to the recorder's address (example: <http://192.168.2.100>) with a web browser.



Fig. 1.3 MediaWorks DX Login Screen (with arrow pointing to Setup Gear)

- Click the Configuration Manager gear icon in the bottom right corner.
- Log into the recorder here. Note that the default logon credentials for the recorder (before they are changed by the administrator) are User Name: *Eventide* Password: *<serial number>*. The Serial number of the recorder can be found on a sticker on the recorder.
- The system's Serial Number and current Firmware Version should be displayed.



Fig. 1.4 Configuration Manager Home Screen (with Serial and Firmware circled)

- **MediaWorks DX:** On the **Help** menu, select **About** to display the version information.

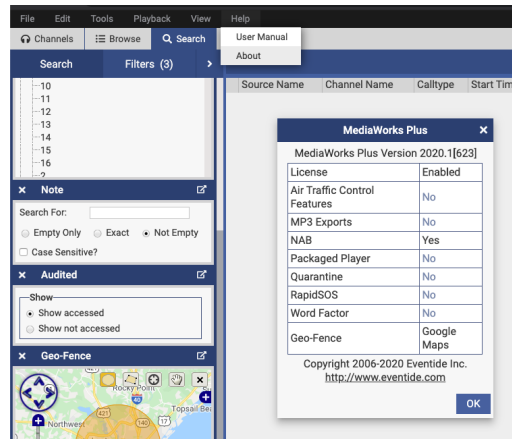


Fig. 1.5 MediaWorks DX About Pop Up

2. AUTHENTICATION MODES

NexLog DX-Series has four authentication modes available for configuration.

- Local Recorder Authentication
- Network File Share (SMB)
- Lightweight Directory Access Protocol (LDAP)
- Microsoft Active Directory

Table 2.1: Authentication Mode Comparison lists each mode and the notable differences between them.

Table 2.1 **Authentication Mode Comparison**

	Local	SMB	LDAP	Active Directory	SAML
AD Password		•	•	•	•
AD Groups			•	•	•
Single Sign-On				•	•
Change Password	•				
Password Expiration	•				•
Secure Transmission	•		•	•	•
Account Expirations	•	•	•	•	•
Account Deactivation	•	•	•	•	•
Automatic User Creation			•	•	•
License Required			•	•	•

Local Recorder Authentication

This authentication mode is the default on any new NexLog DX-Series installation. Users and groups are managed directly on the NexLog DX-Series recorder.

Network File Share

This mode requires that users and groups be manually created using the NexLog DX-Series web configuration manager. When a user logs in, their credentials are tested against the network share for read access. If the user can read the contents of the network share, they will be authenticated.

Lightweight Directory Access Protocol

This mode interfaces with a Microsoft Windows Active Directory or OpenLDAP server. Groups created on the NexLog DX-Series must be mapped to a group on the LDAP server. Users are added to the LDAP group. When a user logs in, the recorder validates their login credentials and queries LDAP for their group memberships.

Active Directory

This mode functions the same as LDAP, but only works with Microsoft Windows Active Directory. The primary difference is that this mode allows automatic login by Single Sign-On (SSO).

2.1. Choosing the Right Mode

Selecting the correct authentication mode required for a NexLog DX-Series installation can reduce unnecessary setup and deployment time. The right mode can only be determined by a system administrator who is familiar with the users and operating environment.

Reference Table 2.1: Authentication Mode Comparison for a simple feature comparison of each mode.

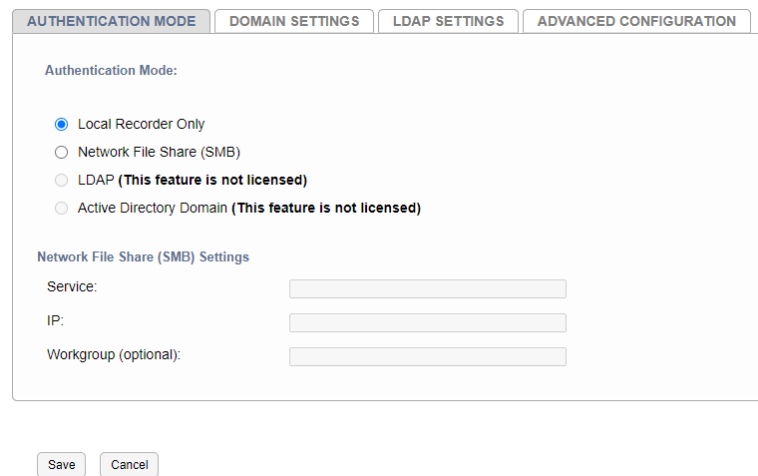
If the NexLog DX-Series recorder is installed on a network without directory services, or you do not wish to sync users or passwords to an external source, Local Recorder Authentication should be used.

If the desire is for users to use the same password as other systems, and user creation and permissions can be done on the recorder, Network File Share (SMB) Authentication should be used.

If user accounts and their passwords should be maintained in a central directory, LDAP Authentication should be used.

If the central directory uses advanced authentication methods, like smart cards, and automatic login via Single Sign-On is desired, Active Directory Authentication must be used.

2.2. Setting the Authentication Mode



The screenshot shows a web configuration window titled "Authentication Mode Selection - Unlicensed". It has four tabs: "AUTHENTICATION MODE", "DOMAIN SETTINGS", "LDAP SETTINGS", and "ADVANCED CONFIGURATION". The "AUTHENTICATION MODE" tab is active. Under the heading "Authentication Mode:", there are four radio button options: "Local Recorder Only" (which is selected), "Network File Share (SMB)", "LDAP (This feature is not licensed)", and "Active Directory Domain (This feature is not licensed)". Below these options is a section titled "Network File Share (SMB) Settings" containing three input fields: "Service:", "IP:", and "Workgroup (optional):". At the bottom of the window are "Save" and "Cancel" buttons.

Fig. 2.1 **Authentication Mode Selection - Unlicensed**

The authentication mode can be set by logging into the web configuration manager, and navigating to Users and Security → Active Directory.

For details on accessing the web configuration manager, consult the NexLog DX-Series system User Manual.

As seen in Figure 2.1, LDAP and Active Directory authentication require a license to enable.

3. LOCAL AUTHENTICATION

Local Authentication is the native, out of the box, authentication method for NexLog DX-Series recorders.

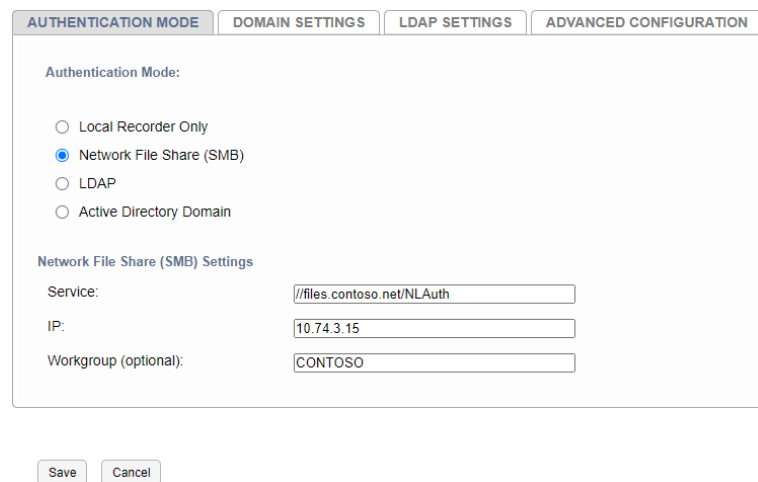
Users, passwords, MFA, groups, and account expirations are all handled directly within the web configuration manager.

Consult the NexLog DX-Series system User Manual for configuration information.

4. SMB AUTHENTICATION

Network File Share or SMB Authentication allows a user to use their existing network password for recorder authentication.

All other user attributes (name, email, permissions, groups, etc) are managed via the recorder's Local Authentication configuration.



The screenshot shows a configuration window with four tabs: AUTHENTICATION MODE, DOMAIN SETTINGS, LDAP SETTINGS, and ADVANCED CONFIGURATION. The AUTHENTICATION MODE tab is active. It contains a section titled 'Authentication Mode:' with four radio button options: 'Local Recorder Only', 'Network File Share (SMB)' (which is selected), 'LDAP', and 'Active Directory Domain'. Below this is a section titled 'Network File Share (SMB) Settings' with three text input fields: 'Service:' containing '//files.contoso.net/NLAuth', 'IP:' containing '10.74.3.15', and 'Workgroup (optional):' containing 'CONTOSO'. At the bottom of the window are 'Save' and 'Cancel' buttons.

Fig. 4.1 SMB Authentication Configuration

4.1. How It Works

When a user logs in to the NexLog DX-Series recorder, the credentials entered are tested against the recorder's local authentication database.

If the credentials do not match, they are transmitted to the configured network file share.

If the supplied credentials work against the network file share, the user is considered authenticated and the login will be processed. The user's permissions for the file share are not considered, only their authentication to it.

If the network file share does authenticate with the supplied credentials, the login is rejected.

4.2. Prerequisites

To setup SMB Authentication you must have:

- An SMB or CIFS network file share
 - It must be accessible from the recorder.
 - Login users must be able to authenticate to this share, even if read access is denied.
- The IP address of the server hosting the network file share
- The domain name, if any, associated with the login users
- List of users with recorder access

4.3. Create the File Share

Create a shared folder on a server or computer that is accesible from the NexLog DX-Series recorder.

If there is a firewall in place between the server and recorder, ensure that the firewall is allowing the traffic listed below between the two servers.

- Microsoft SMB TCP | tcp/135 through tcp/139
- Microsoft SMB UDP | udp/135 through udp/139
- NetBIOS TCP | tcp/445
- NetBIOS UDP | udp/445

Caution

SMB file shares can be created without encrypted communication. This means that if an insecure SMB protocol is used, a network monitor may be able to see the login credentials in plain-text. For this reason, SMB 1.0 should not be used.

Optional: Create a new text file in the shared folder called `DO NOT DELETE` . Edit the new text file to add a message for what the share is used for. This may help accidental deletion by a future system administrator.

4.4. Configure SMB Authentication

Once the file share has been created and user access has been tested, you can proceed with configuring the NexLog DX-Series recorder.

Login to the web configuration manager and navigate to Users and Security → Active Directory. Reference Figure 4.1 for an input example.

Select the radio button for Network File Share (SMB).

In the Service field, enter the full location of the network file share. The location must be entered in linux samba format using forward-slash `/` instead of the Windows format using backslash `\`. The full location is the `//hostname/share name`

If the file share is accessed on a Windows PC using `\\files.contoso.net\NLAuth`, then you would enter `//files.contoso.net/NLAuth`.

In the IP field, enter the IP address of the server hosting the network file share.

In the Workgroup field, enter the NetBIOS domain or workgroup name of users logging in with SMB Authentication. If your domain name is `contoso.net`, this would likely be `CONTOSO`.

Save your changes when finished.

4.5. Create SMB Users

When creating a local user account, that will be used with SMB, it follows the same principles as Local Authentication with two exceptions.

4.5.1. SMB Usernames

The username on the recorder must match the username as it appears on the file share server.

If the username on the server (or Active Directory) is `JohnSmith852`, it must be entered on the recorder as `JohnSmith852`.

The following would all be **invalid** usernames for `JohnSmith852`, and may prevent the user from being able to log in:

- `johnsmith852`
- `johnSmith852`
- `Johnsmith852`
- `JOHNSMITH852`

4.5.2. SMB Passwords

When creating a new locally authenticated user, a password must be provided. SMB Authentication is no exception to this, since SMB credentials are tested *after* local credentials.

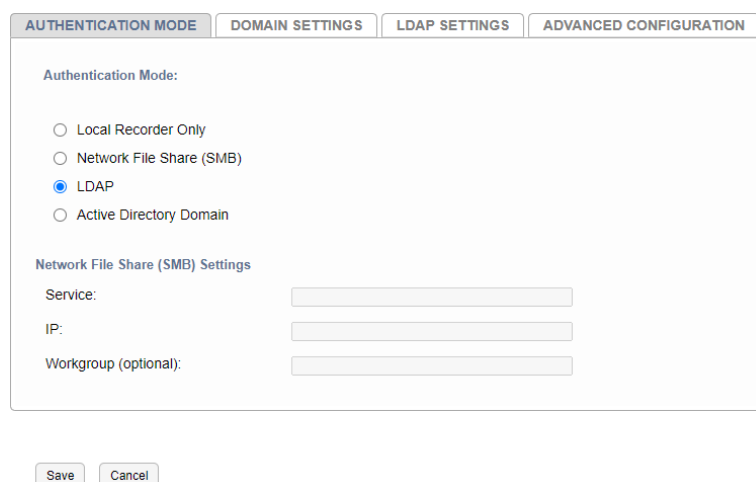
When creating the user, create a secure long password. This password **does not** need to be provided to the user.

5. LDAP AUTHENTICATION

License Required

This feature must be licensed to be used. Contact your Eventide Communications Dealer for assistance.

Lightweight Directory Access Protocol (LDAP) allows users, passwords, and group memberships to be managed via a pre-existing central directory database.



The screenshot shows a configuration window with four tabs: AUTHENTICATION MODE, DOMAIN SETTINGS, LDAP SETTINGS, and ADVANCED CONFIGURATION. The AUTHENTICATION MODE tab is active. Under 'Authentication Mode:', there are four radio buttons: 'Local Recorder Only', 'Network File Share (SMB)', 'LDAP' (which is selected), and 'Active Directory Domain'. Below this, under 'Network File Share (SMB) Settings', there are three text input fields labeled 'Service:', 'IP:', and 'Workgroup (optional):'. At the bottom of the window are 'Save' and 'Cancel' buttons.

Fig. 5.1 **Authentication Mode - LDAP**

This authentication mode can be use along with Local Authentication. It is recommended that a local account be created to serve as a “break glass” account in the event that the recorder is no longer able to talk to the directory service.

5.1. How It Works

When a user logs in to the NexLog DX-Series recorder, their username is evaluated to see if it exists, or is already associated with the directory service.

If the user does not exist, or is associated with the directory service, the credentials entered are tested against the directory server.

If the supplied credentials work, the user is considered authenticated and the login will be processed. If the user does not already exist on the recorder, their recorder account will be created.

If the supplied credentials do not work for the directory service, the login is rejected.

Upon successful login, the recorder will query the directory service for the user's group memberships. If the user is a member of the recorder's paired groups, that group's permissions will be given to the user.

5.2. Prerequisites

To setup LDAP Authentication you must know the following:

- LDAP protocol in use, LDAP or LDAPS (TLS/SSL)
- LDAP server hostname
- LDAP server port number
- Base user search path or organizational unit (OU)
- Base group search path or organizational unit (OU)
- Username for the recorder's LDAP account
- Password for the recorder's LDAP account
- Domain for the recorder's LDAP account

5.3. Create the LDAP Bind Account

In the LDAP service's administration manager, create a service account for the NexLog DX-Series recorder to use.

This account is used for user and group lookups to validate the access that a user should have on the recorder.

The account must have read access to the OU where users and groups are stored, as well as the ability to read the attributes of recorder users.

5.4. Configure LDAP Authentication

Once the service account user been created in the directory service, you can proceed with configuring the NexLog DX-Series recorder.

Login to the web configuration manager and navigate to Users and Security → Active Directory.

Under Authentication Mode, select the radio button for LDAP (Reference Figure 5.1).

Next, select the LDAP Settings tab.

Select the protocol that will be used to communicate with the directory service.

Refer to Section 5.4.1 - LDAP Configuration or Section 5.4.2 - LDAPS Configuration of this document for the options specific to your protocol selection.

When finished, click Save to enable your settings.

A reboot may be required to complete the configuration.

5.4.1. LDAP Configuration

Note

This section details the configuration options for the unencrypted **LDAP** protocol selection. If your connection should be encrypted, refer to Section 5.4.2 - LDAPS Configuration for configuration information.

LDAP Settings

☐ Use LDAP User Group Settings

Protocol: LDAP

Server Hostname: dc1.contoso.net

Server Port Number: 389

Base DN for User Search: OU=Users,OU=HQ,DC=contoso,DC=net

LDAP Bind Username: NLRecorder

LDAP Bind User Password:

LDAP Bind User Realm: CONTOSO

SSL Validation: Ignore

Fetch CA Certificate

Display CA Certificate details

Note: LDAP Server CA Certificates can also be uploaded [here](#).

Fig. 5.2 LDAP Settings Example

Below is a list of each LDAP Settings field, detailing what information should be entered.

Use LDAP User Group Settings

Optional, refer to Section 8.2.1 - Enable LDAP Group Mapping

Protocol

LDAP

Server Hostname

This is the fully qualified domain name of the LDAP server or domain controller the recorder will use to authenticate users to.

Example: `dc1.contoso.net`

Server Port Number

This is the LDAP port that the recorder will use to communicate with the LDAP server.

If all recorder users exist in the same domain as the recorder’s bind account, the default **LDAP** port would be used. If users exist in the parent and child domains, the **LDAP Global Catalog (GC)** port would be used.

Table 5.1 LDAP Server Port Numbers

	Protocol	Port
LDAP	TCP/UDP	389
LDAP GC	TCP	3268

Base DN for User Search

This field should contain the root path containing all recorder users. It should be entered using LDAP syntax.

Example: **OU=Users,OU=HQ,DC=contoso,DC=net**

 Important

The recorder’s LDAP Bind user should also be located within this path.

Table 5.2 LDAP DIT Path Syntax

Key	Description
DC	Domain Component
CN	Common Name
OU	Organizational Unit

LDAP Bind Username

This is the username of the service account created for the recorder. This should be the username only.

Example: `NLRecorder`

LDAP Bind Password

This is the password of the service account created for the recorder.

LDAP Bind Realm

This is the NetBIOS domain name of the service account created for the recorder. This is commonly the first domain component (`DC`) of the Base DN when read from left to right.

5.4.2. LDAPS Configuration

Note

This section details the configuration options for the encrypted **LDAPS** protocol selection. If your connection should be unencrypted, refer to Section 5.4.1 - LDAP Configuration for configuration information.

Below is a list of each LDAP Settings field, detailing what information should be entered.

LDAP Settings

☐ Use LDAP User Group Settings

Protocol: LDAPS ▾

Server Hostname:

Server Port Number:

Base DN for User Search:

LDAP Bind Username:

LDAP Bind User Password:

LDAP Bind User Realm:

SSL Validation: Require ▾

Note: LDAP Server CA Certificates can also be uploaded [here](#).

Fig. 5.3 LDAPS Settings Example

Use LDAP User Group Settings

Optional, refer to Section 8.2.1 - Enable LDAP Group Mapping

Protocol

LDAPS

Server Hostname

This is the fully qualified domain name of the LDAP server or domain controller the recorder will use to authenticate users to.

Example: `dc1.contoso.net`

Server Port Number

This is the LDAPS port that the recorder will use to communicate with the LDAP server.

If all recorder users exist in the same domain as the recorder's bind account, the default **LDAPS** port would be used. If users exist in the parent and child domains, the **LDAPS Global Catalog (GC)** port would be used.

Table 5.3 LDAPS Server Port Numbers

	Protocol	Port
LDAP	TCP	636
LDAP GC	TCP	3269

Base DN for User Search

This field should contain the root path containing all recorder users. It should be entered using LDAP syntax.

Example: `OU=Users,OU=HQ,DC=contoso,DC=net`

Important

The recorder's LDAP Bind user should also be located within this path.

Table 5.4 LDAPS DIT Path Syntax

Key	Description
DC	Domain Component
CN	Common Name
OU	Organizational Unit

LDAP Bind Username

This is the username of the service account created for the recorder. This should be the username only.

Example: `NLRecorder`

LDAP Bind Password

This is the password of the service account created for the recorder.

LDAP Bind Realm

This is the NetBIOS domain name of the service account created for the recorder. This is commonly the first domain component (`DC`) of the Base DN when read from left to right.

SSL Validation

Ignore

This is the default setting when enabling LDAPS. When the recorder makes a connection to the directory service, it will not request or validate the server's TLS/SSL certificate. This option should not be used in a production environment!

Attempt

When the recorder makes a connection to the directory service, it will request its TLS/SSL certificate. If no certificate is provided, the session proceeds normally. If a bad certificate is provided, the session is immediately terminated.

Require

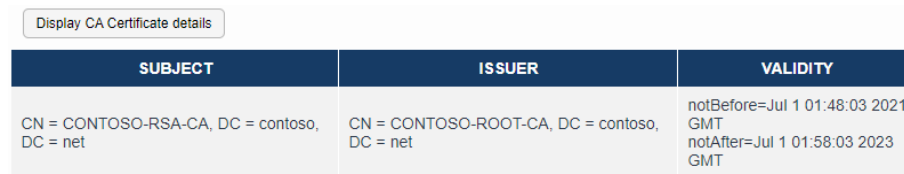
When the recorder makes a connection to the directory service, it will request its TLS/SSL certificate. If no certificate is provided, or a bad certificate is provided, the session is immediately terminated. This is the recommended option for production environments.

Fetch CA Certificate

When using LDAPS, the recorder must trust the CA certificate that signed the LDAP server's TLS certificate. This is especially important when using the recommend `Require` option.

Display CA Certificate

This button can be used to validate that the correct issuing CA certificate was obtained.



The screenshot shows a web interface with a button labeled "Display CA Certificate details" at the top. Below the button is a table with three columns: SUBJECT, ISSUER, and VALIDITY. The SUBJECT column contains "CN = CONTOSO-RSA-CA, DC = contoso, DC = net". The ISSUER column contains "CN = CONTOSO-ROOT-CA, DC = contoso, DC = net". The VALIDITY column contains "notBefore=Jul 1 01:48:03 2021 GMT" and "notAfter=Jul 1 01:58:03 2023 GMT".

SUBJECT	ISSUER	VALIDITY
CN = CONTOSO-RSA-CA, DC = contoso, DC = net	CN = CONTOSO-ROOT-CA, DC = contoso, DC = net	notBefore=Jul 1 01:48:03 2021 GMT notAfter=Jul 1 01:58:03 2023 GMT

Fig. 5.4 LDAPS Server CA Certificate Trust

6. ACTIVE DIRECTORY AUTHENTICATION

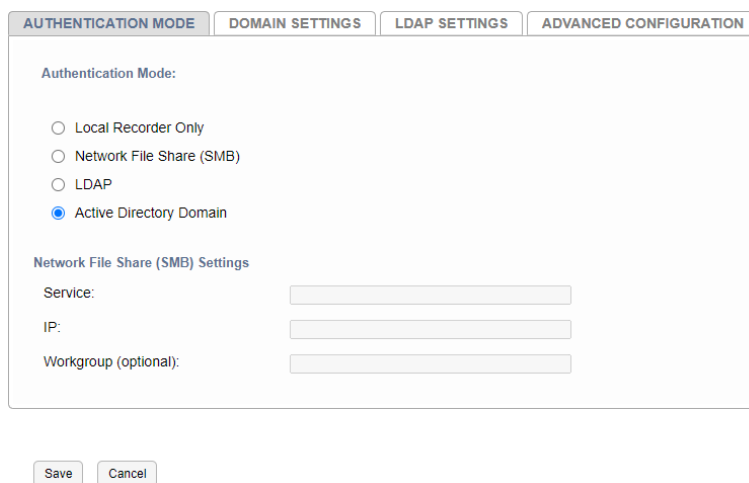
License Required

This feature must be licensed to be used. Contact your Eventide Communications Dealer for assistance.

Active Directory (AD) authentication works in the same manner as LDAP Authentication authentication, allowing users, passwords, and group memberships to be managed via a pre-existing central directory database. The differentiating feature is that AD authentication allows for Single Sign-On (SSO) from a domain joined client PC.

This authentication mode will join the recorder to the network domain.

Since the only advantage of using AD authentication instead of LDAP is SSO, this section will guide you through configuring Active Directory authentication specifically to use Single Sign-On. If SSO is not desired, it is recommended that you use LDAP instead, since this method requires an advanced knowledge level of Active Directory.



The screenshot shows a configuration window with four tabs: AUTHENTICATION MODE, DOMAIN SETTINGS, LDAP SETTINGS, and ADVANCED CONFIGURATION. The AUTHENTICATION MODE tab is active. It contains a section titled 'Authentication Mode:' with four radio button options: 'Local Recorder Only', 'Network File Share (SMB)', 'LDAP', and 'Active Directory Domain'. The 'Active Directory Domain' option is selected. Below this is a section titled 'Network File Share (SMB) Settings' with three input fields: 'Service:', 'IP:', and 'Workgroup (optional):'. At the bottom of the window are 'Save' and 'Cancel' buttons.

Fig. 6.1 Authentication Mode - Active Directory

This authentication mode can be use along with Local Authentication. It is recommended that a local account be created to serve as a “break glass” account in the event that the recorder is no longer able to talk to the directory service.

6.1. How It Works

When a user logs in to the NexLog DX-Series recorder, their username is evaluated to see if it exists, or is already associated with the directory service.

If the user does not exists, or is associated with the directory service, the credentials entered are tested against the directory server.

If the supplied credentials work, the user is considered authenticated and the login will be processed. If the user does not already exist on the recorder, their recorder account will be created.

If the supplied credentials do not work for the directory service, the login is rejected.

Upon successful login, the recorder will query the directory service for the user’s group memberships. If the user is a member of the recorder’s paired groups, that group’s permissions will be given to the user.

6.2. Prerequisites

Before configuring AD authentication, the recorder must be setup with the following:

- Time Sync
- Hostname with valid DNS records
- TLS/SSL Certificate

Setting up this authentication mode will make use of commands that require a domain administrator permission level. Ensure that a domain administrator is available to assist.

To setup AD Authentication you must know the following:

- The full domain name, realm and workgroup for user accounts
- The FQDN of the AD Password Server
- The FQDN of the AD Kerberos Key Distribution Center Server (KDC)
- The FQDN of the AD Admin Server
- LDAP protocol in use, LDAP or LDAPS (TLS/SSL)
- LDAP server hostname

- LDAP server port number
- Base user search path or organizational unit (OU)
- Base group search path or organizational unit (OU)
- Username for the recorder's AD account
- Password for the recorder's AD account
- Domain for the recorder's AD account

6.3. Configure Time Sync

The NexLog DX-Series recorder must be time synced to the same source as the domain server, otherwise authentication will fail because the times are incorrect. To configure the time sync settings, login to the web configuration manager and navigate to System → Date and Time.

Note

In this example, we use NTP Time Sync, however other Time Sync sources are also valid.

In the Time Sync dropdown, select NTP (Network Time Protocol). Enter one or more domain controller addresses into the fields provided, then press Save and Force Sync.

The image shows two stacked web configuration panels. The top panel, titled "RECORDER TIME SETTINGS", contains checkboxes for "Time" and "Timezone", both of which are checked. To the right of these checkboxes is a date and time selector showing "2021-07-19" and "19:10:01". Below the checkboxes is a "Timezone" dropdown menu set to "America/New_York" and a "Time Sync" dropdown menu set to "NTP (Network Time Protocol)". At the bottom of this panel are "Save" and "Cancel" buttons. The bottom panel, titled "NTP SETTINGS", contains four text input fields for "Server 1 Address", "Server 2 Address", "Server 3 Address", and "Server 4 Address". The first three fields contain the values "dc1.contoso.net", "dc2.contoso.net", and "dc3.contoso.net" respectively. The fourth field is empty. At the bottom of this panel is a "Save and Force Sync" button.

Fig. 6.2 Date and Time - NTP Settings

Consult the NexLog DX-Series system manual for additional information.

6.4. Configure Hostname

The hostname of the recorder must be configured in Networking → System Identification. The hostname will be used repeatedly in the domain administration steps, so it is important to have agreement on what the hostname should be to fit in with current domain policy.

For example, if the desired fully qualified domain name for the system is

`https://NLRecorder.contoso.net`, then `NLRecorder` is the hostname.

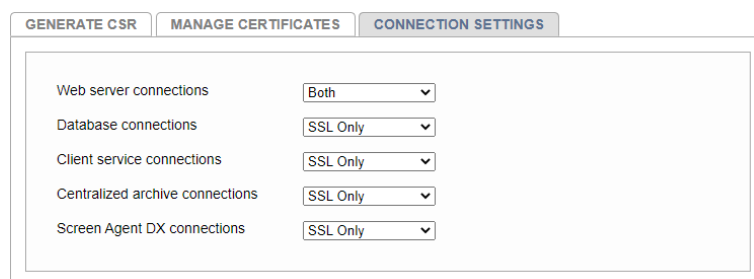
The DNS server used by the recorder must be configured on this same page. Enter the IP address of the DNS server(s) and Save.

Ensure that the DNS server has a valid `A Record` with a matching `PTR Record` pointing to the recorder.

6.5. Configure TLS

The NexLog DX-Series recorder must have a valid TLS/SSL certificate that is trusted by the end client PCs. The certificate can be issued by `Microsoft Certificate Services`, a public CA, or a private CA who's root CA is trusted by the network. SSO will not function without a valid certificate. To configure TLS, consult the NexLog DX-Series system manual. The certificate's `Common Name` would typically be the fully qualified domain name used in the hostname setup.

After configuring TLS, navigate to Users and Security → SSL → Connection Settings and set Database connections to Both or SSL Only.



CONNECTION SETTINGS	
Web server connections	Both
Database connections	SSL Only
Client service connections	SSL Only
Centralized archive connections	SSL Only
Screen Agent DX connections	SSL Only

Fig. 6.3 TLS/SSL Connection Settings

6.6. Configure AD Authentication

Once the recorder's prerequisites have been satisfied, you can begin configuring the domain settings and then apply the configuration to the recorder.

It is important that each section below is followed in order. All domain configuration and command examples should be performed on a PC using a domain administrator account or equivalent.

6.6.1. Create AD User

On the domain controller or `Active Directory Users & Computers`, create a service account for the NexLog DX-Series recorder to use.

This account is used for user and group lookups to validate the access that a user should have on the recorder. The account must have read access to the OU where users and groups are stored, as well as the ability to read the attributes of recorder users.

The account name should be the same as the recorder's hostname.

! Important

If you would like to use Single-Sign On (SSO), the recorder's AD `sAMAccountName` **MUST** be the same as the recorder's hostname.

After creating the account, open its properties and navigate to the `Account` tab. In the `Account options` section, enable the option

`This account supports Kerberos AES 256 bit encryption`

Below is an example powershell command that enables all of the required options. If using this example, be sure to set the correct `Path`, `UserPrincipalName`, and `Account Password`.

PowerShell Example

```
New-ADUser -Name "NexLog Recorder" `
  -GivenName "NexLog" `
  -Surname "Recorder" `
  -sAMAccountName "NLRecorder" `
  -UserPrincipalName "NLRecorder@contoso.net" `
  -Path "CN=Users,DC=contoso,DC=net" `
  -Enabled $true `
  -KerberosEncryptionType "AES256" `
  -TrustedForDelegation $true `
  -ChangePasswordAtLogon $false `
  -PasswordNeverExpires $true `
  -AccountPassword (ConvertTo-SecureString "1qazXSW2!@" -
AsPlainText -force) `
  -PassThru
```

6.6.2. Set Service Principals

The Service Principal Names (SPN) are alias accounts associated with recorder's active directory user account. They allow for kerberos authentication of the web service (HTTP) and database (POSTGRES).

The SPNs can be set from the [Active Directory Users & Computers](#) GUI, by enabling the [Advanced Features](#) view and navigating to the user's [Attributes](#) tab. However, this method is more complicated and it is recommended to set the SPNs from PowerShell.

Open an elevated PowerShell and execute the script below. Replace the two variables with the values for your environment.

This command is case-sensitive. The below script will change the FQDN to lowercase, and the Kerberos Realm to uppercase.

PowerShell

```
# Replace these variables
$recorderUser = "NLRecorder"
$fullDomain = "contoso.net"

# DO NOT edit these variables
```

```

$recorderFQDN = "$($recorderUser.ToLower()).$
($fullDomain.ToLower())"
$kerberosRealm = "$($fullDomain.ToUpper())"

Set-ADUser -Identity $recorderUser -PassThru -ServicePrincipalNames
@{Add=`
    "HTTP/$recorderFQDN@$kerberosRealm",
    "POSTGRES/$recorderFQDN@$kerberosRealm"} `
-TrustedForDelegation $true

```

For NexLog Access Bridge to work with Active Directory authentication, you must also enable Delegation. This can be done by navigating to the **Delegation** tab, then enabling **Trust this user for delegation to any service (Kerberos only)**.

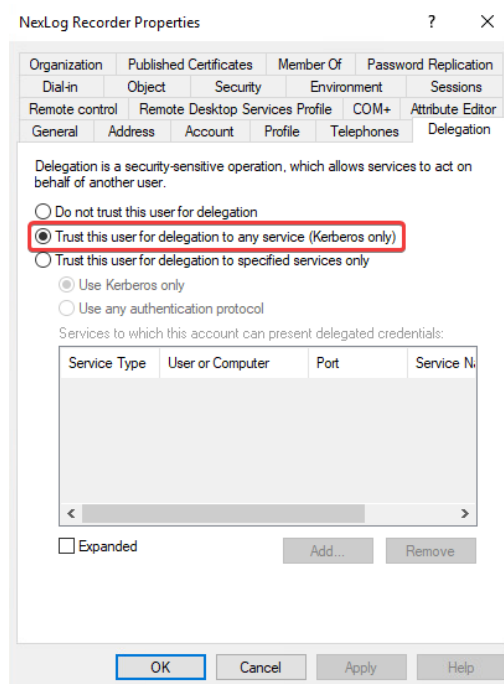


Fig. 6.4 AD Users and Computer - Delegation

 Warning

Consistency Checks

Running consistency checks on Microsoft Active Directory will affect the recorder's service account name which includes a forward slash (/). Microsoft tools such as `LDIF`, or `LdFix` may want to normalize the names by removing the forward slash, resulting in a domain authentication failure when using the web configuration page or client software. Always ignore it if a consistency check suggests modifying the service accounts configured for the recorder.

6.6.3. Create Keytab

 Important

If a recorder is already configured with a keytab, generating a new keytab for the same recorder will invalidate the previous one and cause all Active Directory logins to fail until the newly generated keytab is imported and the recorder is restarted.

The keytab is used to authenticate the HTTP and POSTGRES service accounts with the active directory domain.

The keytab file must typically be generated on domain controller, and then will be imported to the recorder.

Open an elevated PowerShell and execute the script below. Replace the four variables with the values for your environment.

This command is case-sensitive. The below script will change the FQDN to lowercase, and the Kerberos Realm to uppercase.

PowerShell

```
# Replace these variables
$recorderUser = "NLRecorder"
$recorderPassword = "1qazXSW2!@"
$fullDomain = "contoso.net"
$outputLocation = "C:\" # An existing directory path ending with "\"

# DO NOT edit these variables
$recorderFQDN = "$($recorderUser.ToLower()).$
($fullDomain.ToLower())"
$kerberosRealm = "$($fullDomain.ToUpper())"

# Creates the initial keytab for the HTTP SPN
Ktpass -out "$($outputLocation)NexLog_initial.keytab" `
    -princ HTTP/$recorderFQDN@$kerberosRealm `
    -mapUser "$($fullDomain.Split(".",2)[0])\$recorderUser" `
    -mapOp set `
    -pass $recorderPassword `
    -crypto AES256-SHA1 `
    -pType KRB5_NT_PRINCIPAL

# Adds the POSTGRES SPN to the HTTP keytab
Ktpass -in "$($outputLocation)NexLog_initial.keytab" `
    -out "$($outputLocation)NexLog_final.keytab" `
    -princ POSTGRES/$recorderFQDN@$kerberosRealm `
    -mapUser "$($fullDomain.Split(".",2)[0])\$recorderUser" `
    -mapOp add `
    -setUpn `
    -setPass `
    -pass $recorderPassword `
    -crypto AES256-SHA1 `
    -pType KRB5_NT_PRINCIPAL
```

This should create two keytab files. The important one is the second one (named `NexLog_final.keytab` in the script); this second one is the one that will be uploaded to the recorder.

6.6.4. Deploy AD Configuration

After all of the previous sections have been completed, you can proceed with deploying the Active Directory authentication configuration to the recorder.

Insure that you have completed the prerequisite tasks, and gathered the prerequisite information.

Prerequisite Tasks

- ☐ Time Sync configured and syncing with a domain controller
- ☐ Hostname set and validated with DNS
- ☐ TLS certificate has been applied and tested
- ☐ The recorder's AD User has been created
- ☐ Service Principal Names have been set
- ☐ NexLog_final.keytab has been created

Prerequisite Information

- ☐ Domain Administator login credentials
- ☐ The full domain name, realm and workgroup for user accounts
- ☐ The FQDN of the AD Password Server
- ☐ The FQDN of the AD Kerberos Key Distribution Center Server (KDC)
- ☐ The FQDN of the AD Admin Server
- ☐ LDAP protocol in use, LDAP or LDAPS (TLS/SSL)
- ☐ LDAP server hostname
- ☐ LDAP server port number
- ☐ Base user search path or organizational unit (OU)
- ☐ Base group search path or organizational unit (OU)
- ☐ Username for the recorder's AD account
- ☐ Domain for the recorder's AD account

6.6.4.1. Install the Keytab

The final keytab file, `NexLog_final.keytab`, must be imported to the recorder.

Login to the web configuration manager and navigate to Users and Security → Active Directory.

Under Authentication Mode, select the radio button for Active Directory Domain (Reference Figure 6.1).

Next, select the Domain Settings tab.

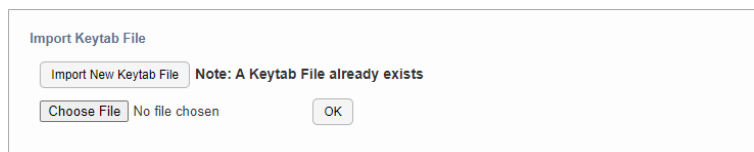


Fig. 6.5 Domain Settings - Import Keytab File

Scroll to the Import Keytab File section and press Import New Keytab File. If a Keytab is already uploaded, the page will say **Note: A Keytab File already exists.**

Press Choose File and select the keytab named **NexLog_final.keytab**. Press the OK button to begin the upload.

! Important

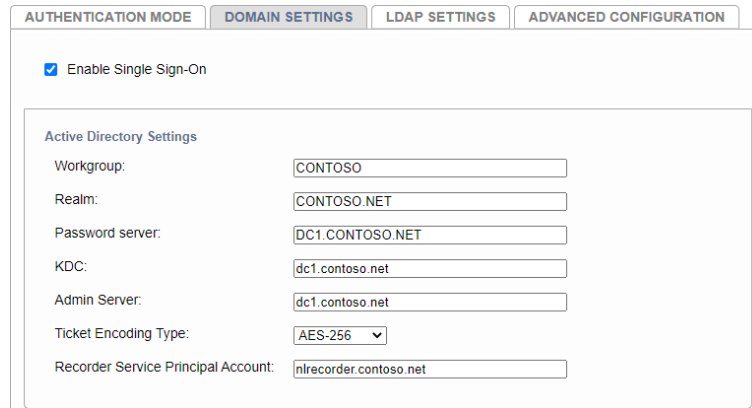
It is not necessary for the initial setup, but if the keytab is ever replaced, you must reboot the recorder for it to be applied.

6.6.4.2. Configure Domain Settings

In the web configuration manager and navigate to Users and Security → Active Directory.

Under Authentication Mode, select the radio button for Active Directory Domain (Reference Figure 6.1).

Next, select the Domain Settings tab, then enable the Enable Single Sign-On check box.



AUTHENTICATION MODE DOMAIN SETTINGS LDAP SETTINGS ADVANCED CONFIGURATION

☒ Enable Single Sign-On

Active Directory Settings

Workgroup: CONTOSO

Realm: CONTOSO.NET

Password server: DC1.CONTOSO.NET

KDC: dc1.contoso.net

Admin Server: dc1.contoso.net

Ticket Encoding Type: AES-256

Recorder Service Principal Account: nlrecorder.contoso.net

Fig. 6.6 Domain Settings - Active Directory Settings

In the Active Directory Settings section, complete all fields. Some of these fields must be in UPPERCASE and others must be in lowercase, but you don't have to worry about that because when you save, the form will automatically set the case correctly for fields where it matters.

Workgroup

(UPPERCASE) The NetBIOS workgroup name for login users

Example: CONTOSO

Realm

(UPPERCASE) The domain's kerberos realm

Example: CONTOSO.NET

Password Server

(UPPERCASE) The password server the recorder should use to authenticate user credentials. This is typically a domain controller.

Example: DC1.CONTOSO.NET

KDC

(lowercase) The Kerberos Key Distribution Center server the recorder should use kerberos authentication. This is typically a domain controller.

Example: `dc1.contoso.net`

Admin Server

(lowercase) The server that should be used for group membership queries. This is typically a domain controller.

Example: `dc1.contoso.net`

Ticket Encoding Type

The kerberos encryption type the account should use. This must be the same as what was used to generate the keytab. **Options:**

AES-128

AES-256 (default)

RC4-HMAC

Recorder Service Principal Account

(lowercase) The primary service principal account name for the recorder. This is typically the same as the recorder's FQDN.

Example: `nlrecorder.contoso.net`

Once all fields have been completed in Active Directory Settings, switch to the LDAP Settings tab and complete all fields.

Select the protocol that will be used to communicate with the directory service.

Refer to Section 5.4.1 - LDAP Configuration or Section 5.4.2 - LDAPS Configuration of this document for the options specific to your protocol selection. The `LDAP Bind` fields will be disabled when using Active Directory authentication.

When finished, click Save to enable your settings.

A reboot is required to complete the configuration. Once the recorder is back after the reboot, you can join it to the domain.

6.6.5. Joining the Domain

For Active Directory authentication to work, the recorder must be joined to the domain by a domain administrator. Once joined (and rebooted), you can try logging into either Configuration Manager or MediaWorks DX with any domain user; depending on your configuration, you'll likely get a warning that the user exists but does not have any client permissions. See Section 8: Users and Groups for more details on permission groups.

Login to the web configuration manager and navigate to Users and Security → Active Directory.

Next, select the Domain Settings tab.

Scroll to the Domain Membership section where it will indicate the recorder's domain membership status.

If the recorder is not already joined to the domain, enter the credentials of a domain administrator in the fields provided, then press Join Domain.



The screenshot shows a web interface for 'Domain Membership'. It contains two input fields: 'User Account' with the text 'contosoadmin' and 'Password' with masked characters. Below these fields, a status message reads 'The recorder is joined to the domain'. At the bottom left, there is a button labeled 'Leave Domain'.

Fig. 6.7 Domain Settings - Join domain

If the recorder was joined to the domain successfully, the status will change to

The recorder is joined to the domain and the button text will change to Leave Domain .

A reboot is required to complete the operation. Once the recorder is back after the reboot, you can attempt logging in with domain credentials.

6.6.6. Single Sign-On

Single Sign-On (SSO) is an additional feature of Active Directory that allows users to log in to Windows once, and then login to MediaWorks DX directly from a URL or by checking a box on the login prompt. The recorder will check with the domain for authentication and log the current Windows user into the system.

For users to log in with SSO, it must be enabled on the recorder. Enabling or disabling SSO will require a recorder reboot to take effect.

To use SSO the recorder must have a fully qualified domain name (FQDN), such as `NLRecorder.contoso.net` because Active Directory authenticates against the FQDN and not an IP address.

! Important

The recorder's AD `sAMAccountName` **MUST** be the same as the recorder's hostname for SSO to work.

If `NLRecorder.contoso.net` is the URL used to access the recorder, `NLRecorder` **MUST** be the recorder service account's username.

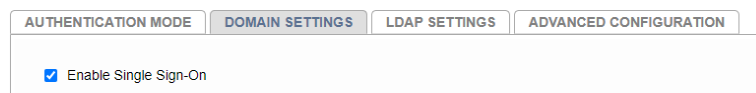


Fig. 6.8 Domain Settings - Single Sign-On

To enable SSO, navigate to Users and Security → Active Directory → Domain Settings then check the Enable Single Sign-On checkbox and reboot the recorder. To disable, uncheck the box and reboot.

Single Sign-On support is browser dependent and each browser may have different security configurations to support it. Included in the next sections are configuration options for the most common web browsers.

Note

SSO will also require that the recorder's FQDN is added to your group policy's Trusted Sites List.

Go to your Group Policy's Site to Zone Assignment List and enable the policy setting. Then add your FQDN as a zone assignment. Read the numbered values on the Group Policy Editor to determine which value will work for you.

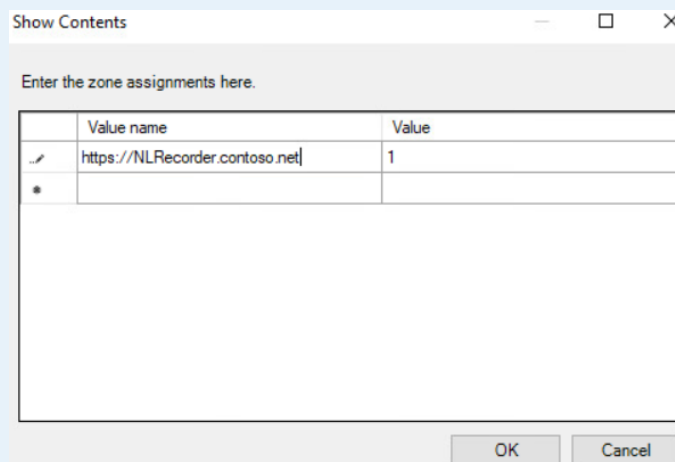


Fig. 6.9 Site to Zone Assignment List Example

6.6.6.1. Brave Browser

The Brave browser can be configured by editing the registry directly on a PC, or by deploying the registry change to multiple workstations via Group Policy.

Use HKLM to apply the setting to all users of the PC, or HKCU for specific users. For the value, you can separate multiple server names with commas. Wildcards (*) are allowed.

Table 6.1 Brave Browser Registry Settings -
AuthNegotiateDelegateAllowlist

Registry	HKEY_LOCAL_MACHINE or
Hive	HKEY_CURRENT_USER

Registry Path	Software\Policies\BraveSoftware\Brave
Value Name	AuthNegotiateDelegateAllowlist
Value Type	REG_SZ
Example Value	NLRecorder.contoso.net, recorder.contoso.net

Table 6.2 Brave Browser Registry Settings - AuthServerAllowlist

Registry Hive	HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER
Registry Path	Software\Policies\BraveSoftware\Brave
Value Name	AuthServerAllowlist
Value Type	REG_SZ
Example Value	NLRecorder.contoso.net, recorder.contoso.net

6.6.6.2. Google Chrome

Google Chrome can be configured by editing the registry directly on a PC, or by deploying the registry change to multiple workstations via Group Policy.

Use HKLM to apply the setting to all users of the PC, or HKCU for specific users. For the value, you can separate multiple server names with commas. Wildcards (*) are allowed.

Table 6.3 Google Chrome Registry Settings - AuthNegotiateDelegateAllowlist

Registry Hive	HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER
---------------	---

Registry Path	Software\Policies\Google\Chrome
Value Name	AuthNegotiateDelegateAllowlist
Value Type	REG_SZ
Example Value	NLRecorder.contoso.net, recorder.contoso.net

Table 6.4 Google Chrome Registry Settings - AuthServerAllowlist

Registry Hive	HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER
Registry Path	Software\Policies\Google\Chrome
Value Name	AuthServerAllowlist
Value Type	REG_SZ
Example Value	NLRecorder.contoso.net, recorder.contoso.net

6.6.6.3. Microsoft Edge (Chromium)

The Chromium based Microsoft Edge browser can be configured by editing the registry directly on a PC, or by deploying the registry change to multiple workstations via Group Policy.

Use HKLM to apply the setting to all users of the PC, or HKCU for specific users. For the value, you can separate multiple server names with commas. Wildcards (*) are allowed.

Table 6.5 Microsoft Edge Browser Registry Settings - AuthNegotiateDelegateAllowlist

Registry Hive	HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER
---------------	---

Registry Path	Software\Policies\Microsoft\Edge
Value Name	AuthNegotiateDelegateAllowlist
Value Type	REG_SZ
Example Value	NLRecorder.contoso.net, recorder.contoso.net

Table 6.6 Microsoft Edge Browser Registry Settings - AuthServerAllowlist

Registry Hive	HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER
Registry Path	Software\Policies\Microsoft\Edge
Value Name	AuthServerAllowlist
Value Type	REG_SZ
Example Value	NLRecorder.contoso.net, recorder.contoso.net

6.6.6.4. Mozilla Firefox

The Mozilla Firefox browser can be configured by editing the registry directly on a PC, deploying the registry change or Firefox template to multiple workstations via Group Policy, or directly within the Firefox interface.

Firefox Interface

1. Open Mozilla Firefox and navigate to the URL: `about:config`.
2. If a warning page appears with the message: `Proceed with Caution`, click `Accept the Risk and Continue`.

3. Locate and double-click on the `network.automatic-ntlm-auth.trusted-uris`.
4. In the value field, enter the URL address used to access the recorder (ex. `NLRecorder.contoso.net`). For the value, you can separate multiple server names with commas.
5. Click ☐.
6. Locate and double-click on the `network.negotiate-auth.trusted-uris`.
7. In the value field, enter the URL address used to access the recorder (ex. `NLRecorder.contoso.net`). For the value, you can separate multiple server names with commas.
8. Click ☐.
9. Exit and reopen Firefox.

Firefox Registry

Configuring Firefox via the Windows registry requires an addition to two paths.

Table 6.7 **Mozilla Firefox Browser Registry Settings - NTLM**

Registry Hive	HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER
Registry Path	Software\Policies\Mozilla\Firefox\Authentication\NTLM
Value Name	1 (increase number for each entry)
Value Type	REG_SZ
Example Value	<code>NLRecorder.contoso.net</code>

Table 6.8 **Mozilla Firefox Browser Registry Settings - SPNEGO**

Registry Hive	HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER
Registry Path	Software\Policies\Mozilla\Firefox\Authentication\SPNEGO
Value Name	1 (increase number for each entry)

Value
Type REG_SZ

Example
Value NLRecorder.contoso.net

7. SAML AUTHENTICATION

License Required

This feature must be licensed to be used. Contact your Eventide Communications Dealer for assistance.

7.1. How It Works

When a user logs in to the NexLog DX-Series recorder, the SAML attribute mapped to recorder usernames is evaluated to see if that user already exists. Access to the recorder is controlled by groups and permissions set within the SAML Identity Provider.

Groups must be included in the assertion and the mapping of groups to permissions must be configured on the recorder.

If the user **does not** exist, the user is created and permissions are set based on the mapping of groups in the assertion to permissions.

If the user **does** exist, permissions are updated on each login.

7.2. Prerequisites & Considerations

1. A TLS certificate must be configured and enabled on the recorder and the FQDN, matching the certificate, must be known. For the purposed of this document the value, **sp.nexlog.host**, will be used throughout.
2. All users are created just-in-time. Users created before configuring SAML authentication where the username matches what is in the assertion will still be able to use local authentication.
3. The claim passed and mapped to the username on the recorder will extract the string before the @ (if included in the value, e.g. `user1@domain.com --> user1`).
4. Permissions should be mapped to groups and are reapplied at each login. Any changes made locally on the recorder will be overwritten.

7.3. Identity Provider Implementation Guides

7.3.1. ADFS Configuration

7.3.1.1. Prerequisites

Microsoft ADFS Server

The ADFS server is a Windows Server role that provides users with single sign-on access to systems and applications located across organizational boundaries. It authenticates users to multiple applications, including Office 365, and provides seamless access to resources.

TLS Certificate

A valid TLS certificate must be installed and enabled on the recorder.

Entity ID

The entity ID is a unique identifier for the service provider (SP) and the identity provider (IdP). The entity ID for the SP must be provided, and the entity ID for the IdP is programmatically pulled from its metadata file.

Metadata File

The metadata file is an XML document that contains information about the IdP. It includes the IdP's entity ID, public key, and other relevant information. The metadata file is used to configure the SP to trust the IdP.

User Groups

User groups must be correctly set up in the recorder and Active Directory. The groups in the recorder must align with those in Active Directory to ensure proper group mapping for SAML authentication.

Configuration Manager

Access to Configuration Manager is required to configure the SAML authentication provider on the recorder. The Configuration Manager login icon will not be available in the lower righthand corner when accessing Configuration Manager. You will need to log in by going to **<host>/admin**.

MediaWorks Replay

After successfully configuring ADFS, log in to MediaWorks by navigating to the recorder and logging in.

7.3.1.1.1. Configuration Steps

We'll start with a clean slate on the ADFS server. The graphic below shows the ADFS management tool on the server itself.

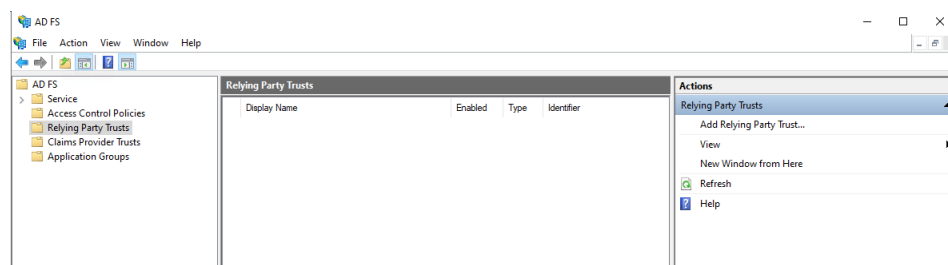


Fig. 7.1 Relying Party Trusts

We need to ensure that the ADFS server has a few items in its properties for its Metadata to be used later in this configuration process. Right click the **Service** folder, and choose **Edit Federation Service Properties**

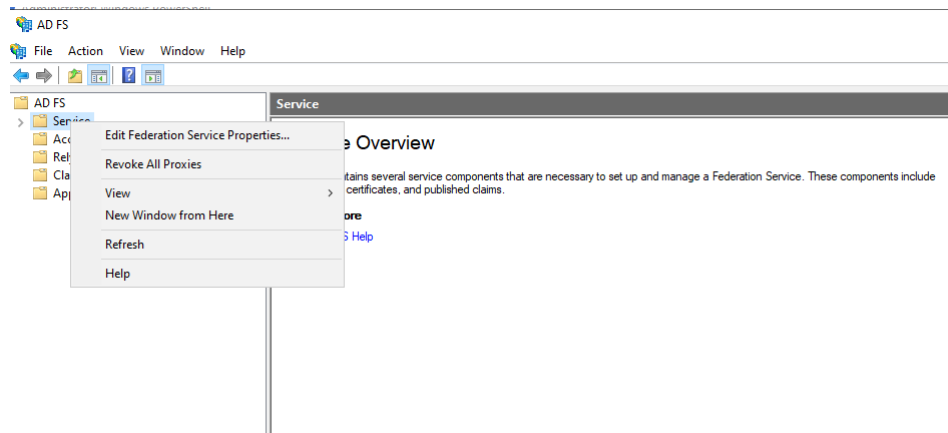
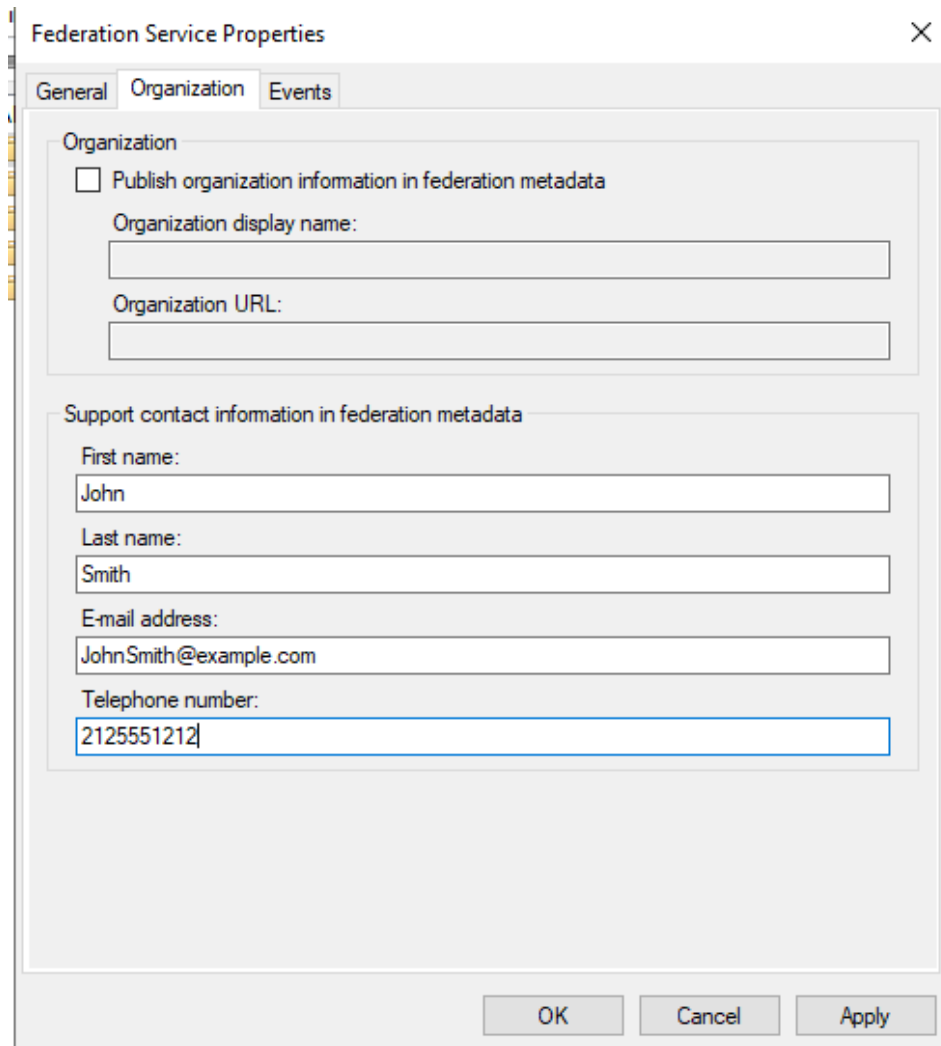


Fig. 7.2 Edit Federation Service Properties

Once the properties dialog box is visible, click on the **Organization** tab.



The image shows a Windows-style dialog box titled "Federation Service Properties". It has three tabs: "General", "Organization" (which is selected), and "Events". The "Organization" tab contains two main sections. The first section, titled "Organization", has a checkbox labeled "Publish organization information in federation metadata" which is currently unchecked. Below this checkbox are two text input fields: "Organization display name:" and "Organization URL:". The second section, titled "Support contact information in federation metadata", contains five text input fields: "First name:" (with the value "John"), "Last name:" (with the value "Smith"), "E-mail address:" (with the value "JohnSmith@example.com"), and "Telephone number:" (with the value "2125551212"). At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Apply".

Fig. 7.3 Organization Tab

If the Support contact information is not populated, you will need to populate with some information for the Metadata to be imported.

The next step is to either right click the **Relying Party Trusts** folder and choose **Add Relying Party Trust**, or on the right side of the ADFS management window, click **Add Relying Party Trust**.

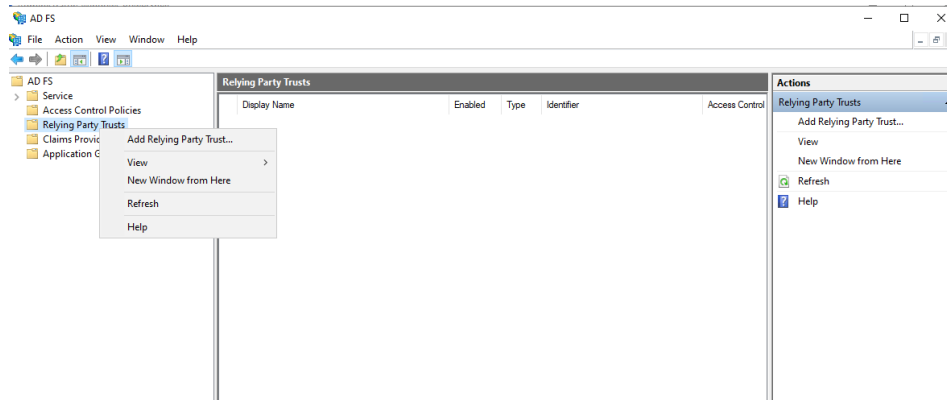


Fig. 7.4 Add Relying Party Trust

This will bring up the **Add Relying Party Trust Wizard**, which will default to the **Claims aware** selection.

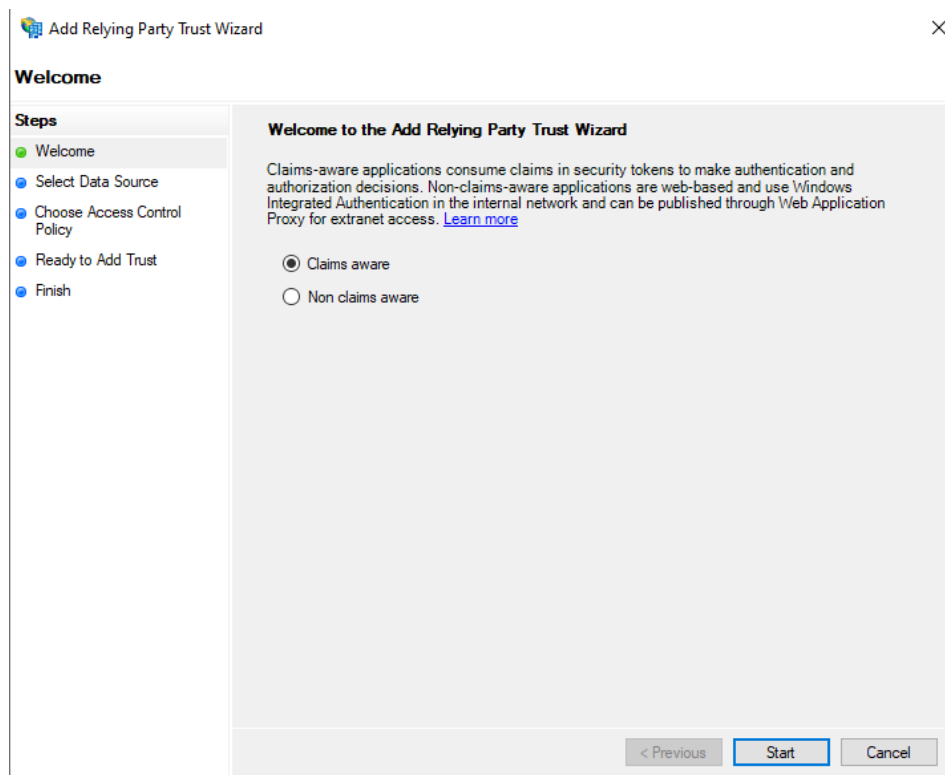


Fig. 7.5 Add Relying Party Trust Wizard

Click **Next** to continue.

Choose the third option, **Enter data about the relying party manually**

Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

☐ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

☐ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

☒ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

< Previous **Next >** Cancel

Fig. 7.6 Enter Data Relying Party Manually

Click **Next** to continue

Give the new relying party a name. This is simply used for display purposes in the ADFS server itself. Additionally, you may add notes here as well.

The screenshot shows the 'Add Relying Party Trust Wizard' window, specifically the 'Specify Display Name' step. The window has a title bar with a close button (X). On the left, a 'Steps' pane lists the following steps: Welcome (green dot), Select Data Source (green dot), Specify Display Name (green dot and highlighted), Configure Certificate (blue dot), Configure URL (blue dot), Configure Identifiers (blue dot), Choose Access Control Policy (blue dot), Ready to Add Trust (blue dot), and Finish (blue dot). The main area of the wizard is titled 'Specify Display Name' and contains the instruction 'Enter the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' label followed by a text box containing 'NexlogDX FIPS SAML'. Below the text box is a 'Notes:' label followed by a larger text area containing the text 'This relying party is used for SAML authentication.' At the bottom right of the wizard, there are three buttons: '< Previous' (disabled), 'Next >' (active/highlighted), and 'Cancel' (disabled).

Fig. 7.7 Give Relying Party Name

Click **Next** to continue.

On the **Configure Certificate** page, click **Next** to continue the wizard.

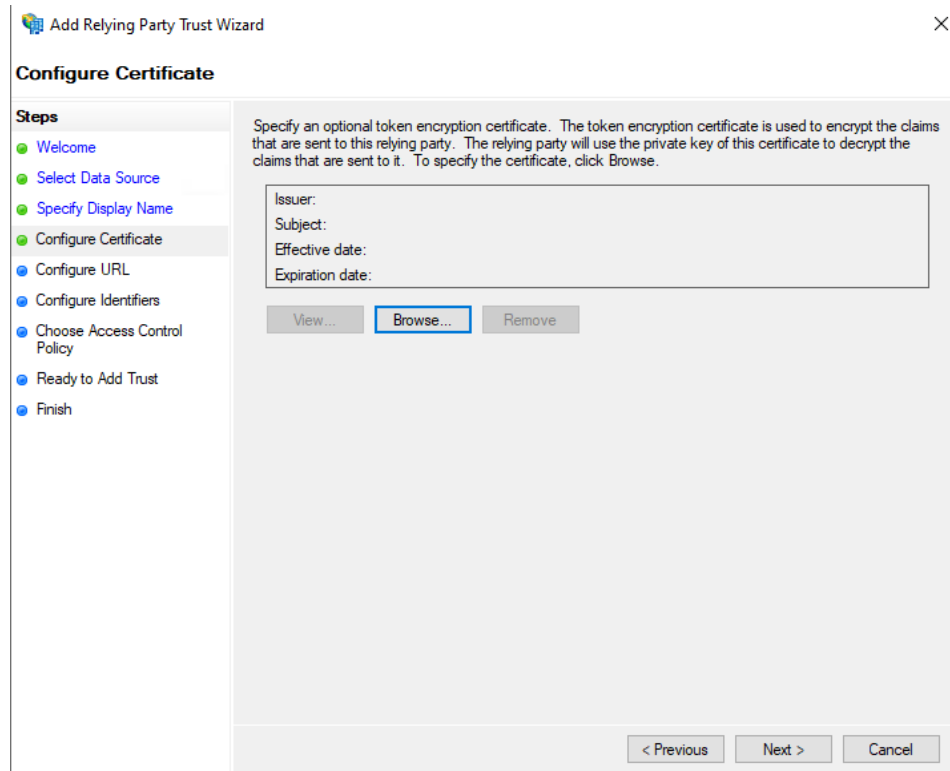


Fig. 7.8 Configure Certificate

Click **Next** to continue

Once on the **Configure URL** page, you will need to select the second option, **Enable support for the SAML 2.0 WebSSO protocol**. In the box for the Relying party, we will construct the URL using the FQDN referenced in the beginning of this document, **sp.nexlog.host**. You will need to provide the FQDN that you have provisioned, but the rest of the URL should be as shown below.

Add Relying Party Trust Wizard

Configure URL

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL**
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

☐ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☒ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

Example: https://www.contoso.com/adfs/ls/

< Previous **Next >** Cancel

Click **Next** to continue to the **Configure Identifiers** dialog.

Though ADFS doesn't make reference to it in this dialog, the information that it is looking for is the entityID of the Service Provider(SP). This can be any value if it is unique within the ADFS server. Standard practice is to make this a URL, though the URL does not have to point to anything, nor does it need to resolve. It's simply used as a unique identifier. For this document, we will use the value, **https://sp.nexlog.host/relyingidentifier**. Make note of this value, as it will be used later to configure the recorder side of SAML. Enter the value in the text box, then click the **Add** button to add in the bottom text box.

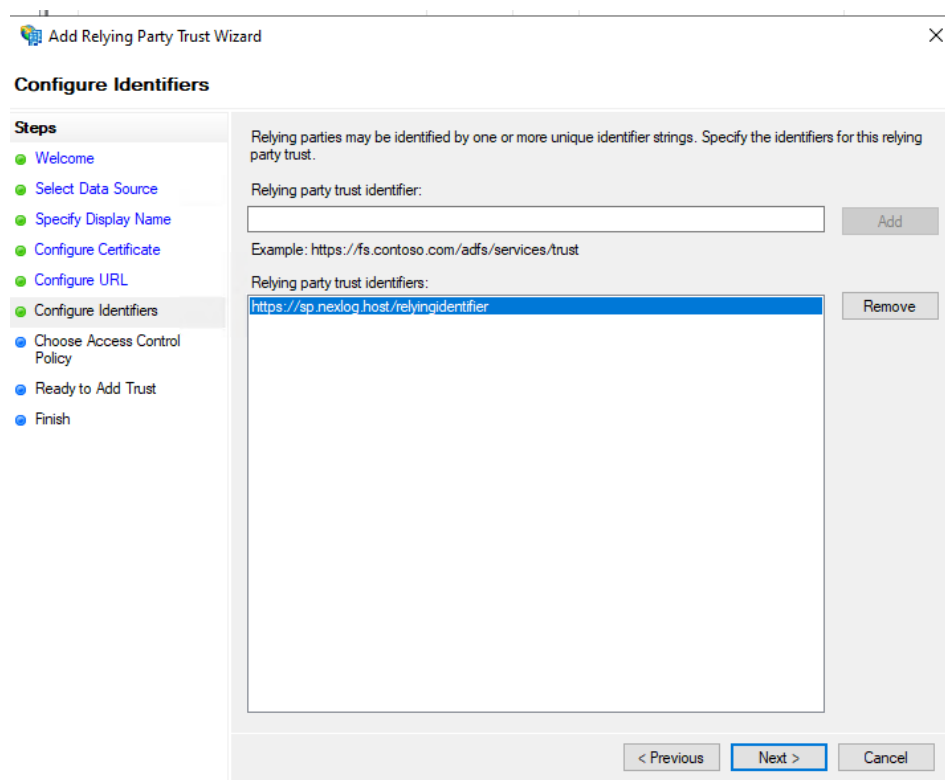


Fig. 7.9 Configure Identifiers

Click the **Next** button to continue.

On the **Choose Access Control Policy** page, highlight the **Permit everyone** entry, then click **Next**.

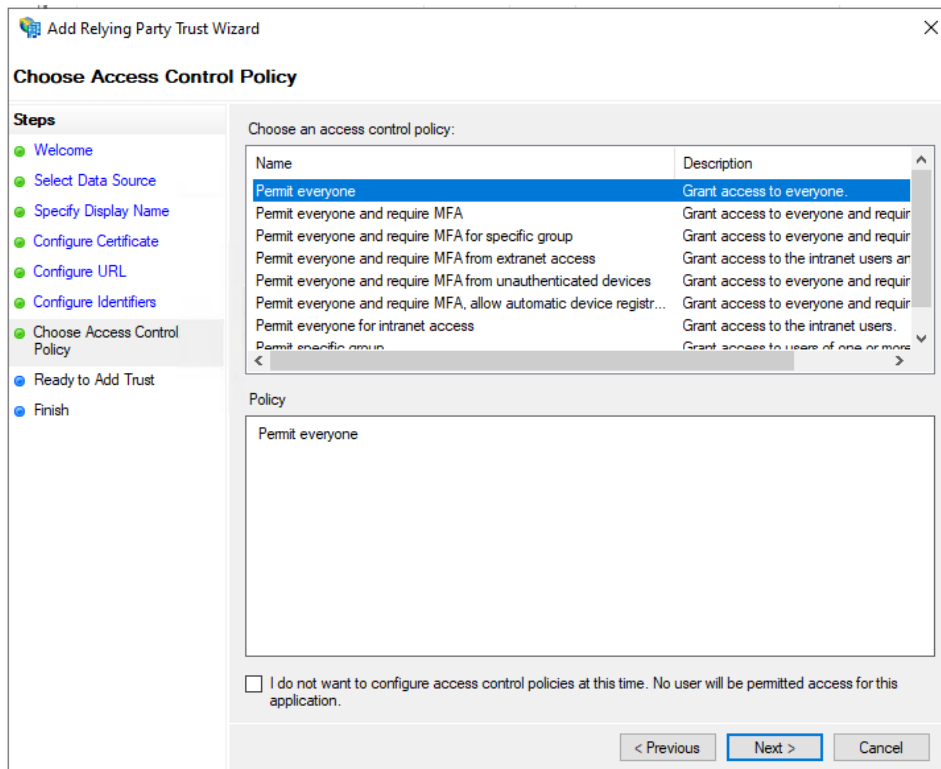


Fig. 7.10 Choose Access Control Policy

On the **Ready to Add Trust** page, click **Next** to continue to the last page in the dialog.

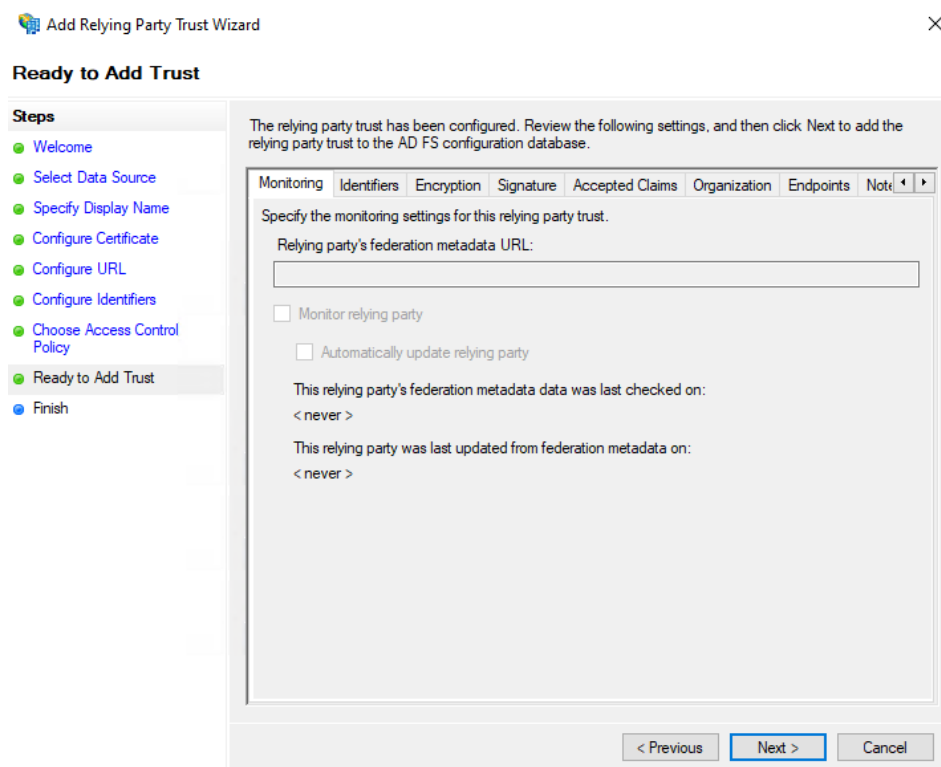


Fig. 7.11 Ready to Add Trust

Finally, on the **Finish** page, leave the **Configure claims issuance policy for this application** checkbox checked, and click **Close**.

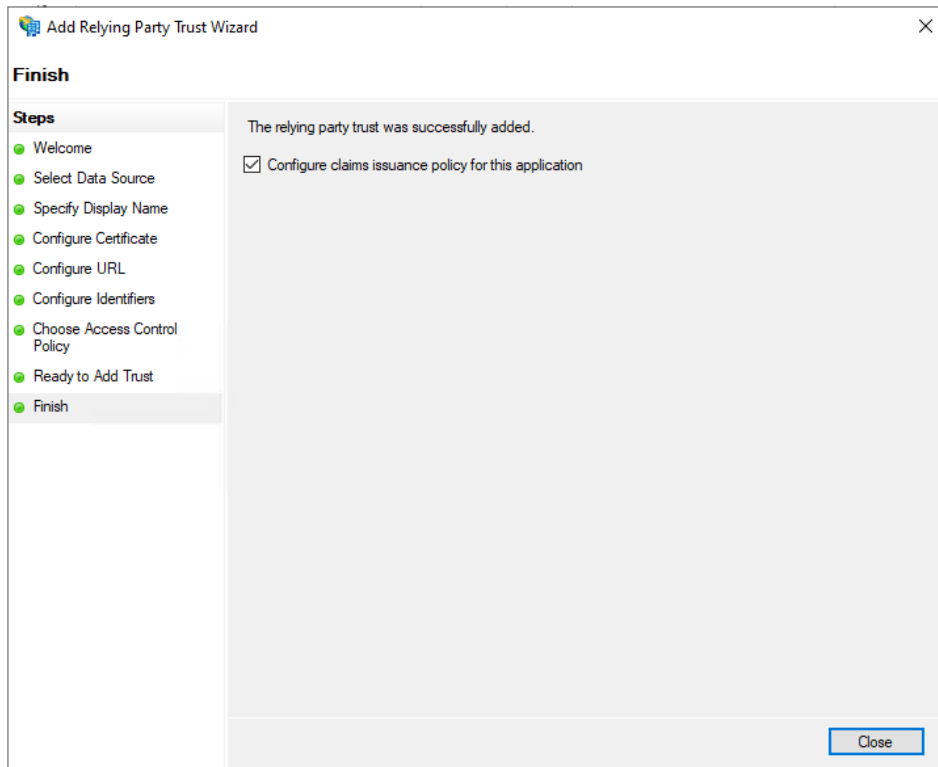


Fig. 7.12 Finish Configure Claims

When you click the **Close** button, a new dialog will appear that will allow you to edit the claims for the newly configured relying party.

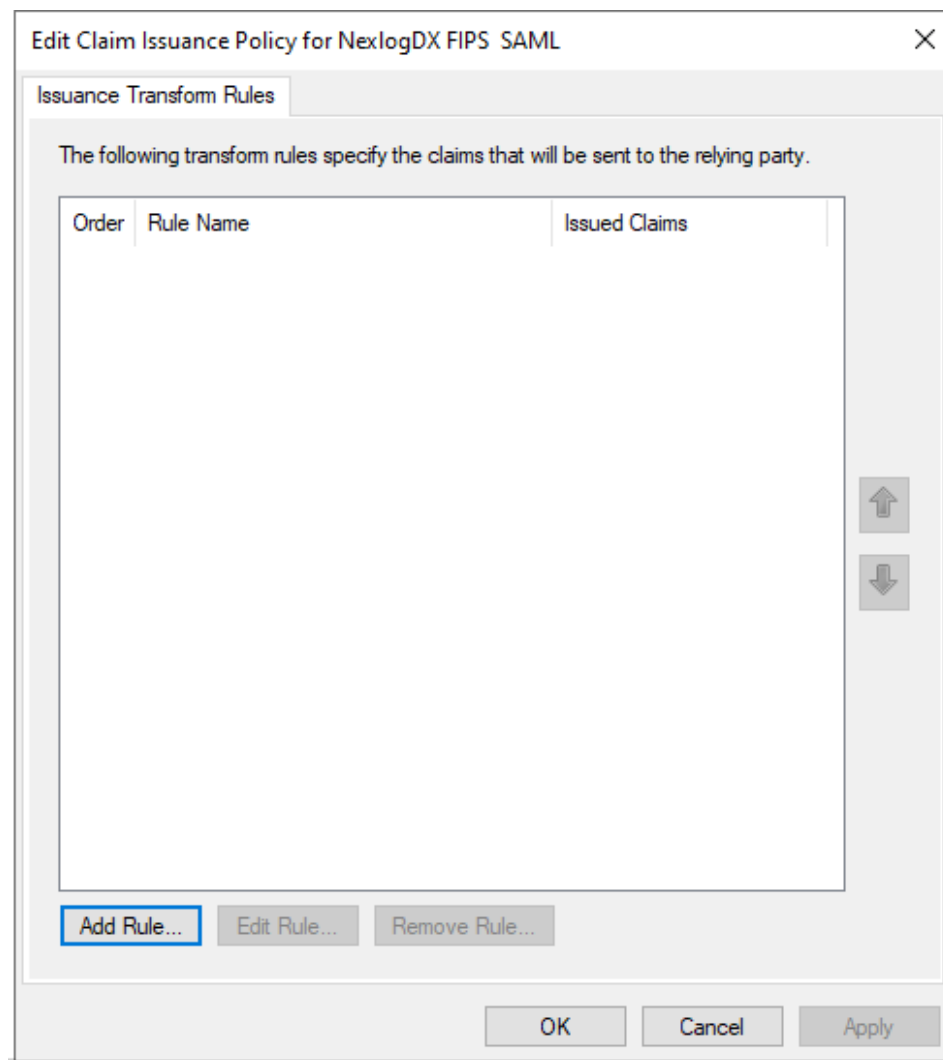


Fig. 7.13 Edit Claim Issuance Policy

Click the **Add rule** button to add a claims rule. There are several that will need to be added.

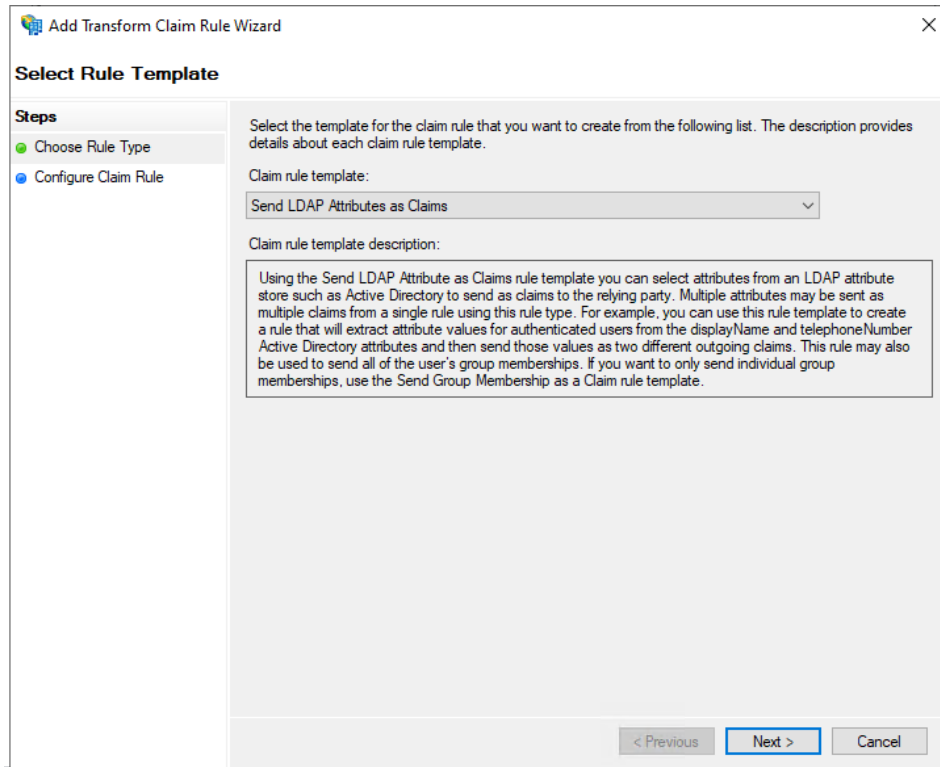


Fig. 7.14 Add Transform Claim Rule Wizard

Click **Next** to continue.

The first claim will add is a UPN claim. You can provide any name you wish, for the purpose of this document the name **NexLog Claim** will be used.

Under **Attribute store**, select the **Active Directory** entry.

Under the left side drop down, choose the **User-Principal-Name** option, and on the right side drop down, select the **UPN** option.

In the next row, on the left side, choose the **Token-Groups - Qualified by Long Domain Name**, and on the right, choose the **Group** option.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
Nexlog Claim

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	User-Principal-Name	UPN
	Token-Groups - Qualified by Long ...	Group
▶*		

< Previous Finish Cancel

Fig. 7.15 Configure Claim Rule

Click **Finish**, **Apply**, then **Ok** to finish the process and dismiss the dialogs.

We need to add one more URLs to the configuration, and since ADFS doesn't support adding two via the wizard, we need to edit the properties of the newly configured relying party.

Right click on the relying party that was just created and choose the **Properties** option.

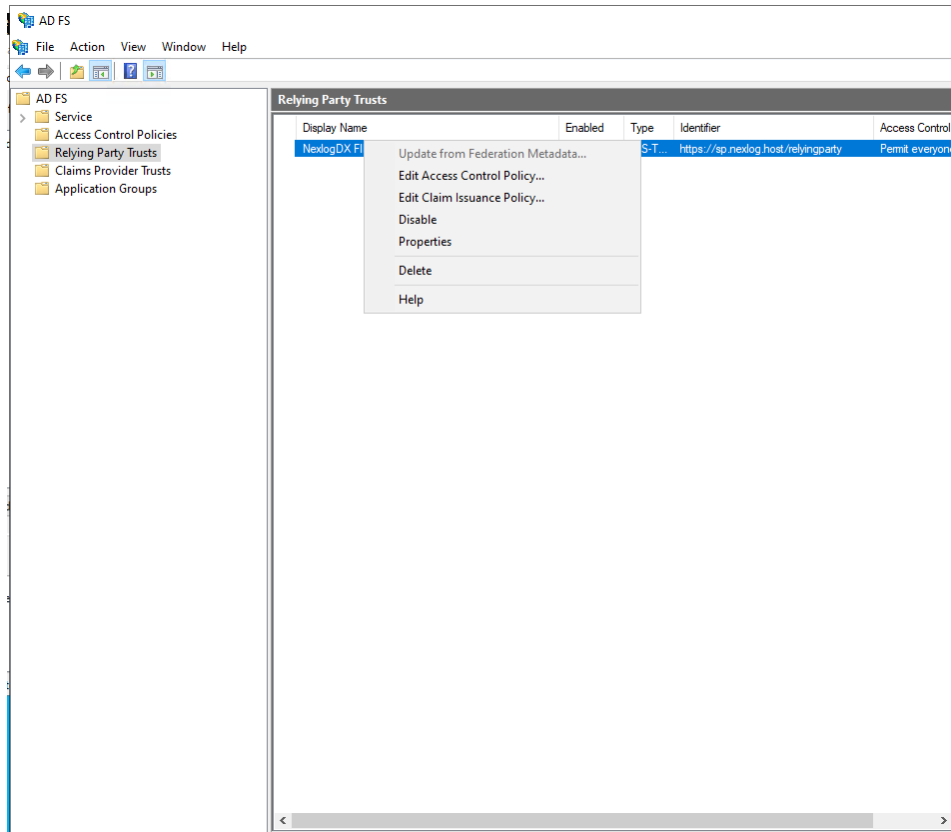


Fig. 7.16 Relying Party Properties

In the properties dialog, choose the **Endpoints** tab, then click on the **Add SAML** button.

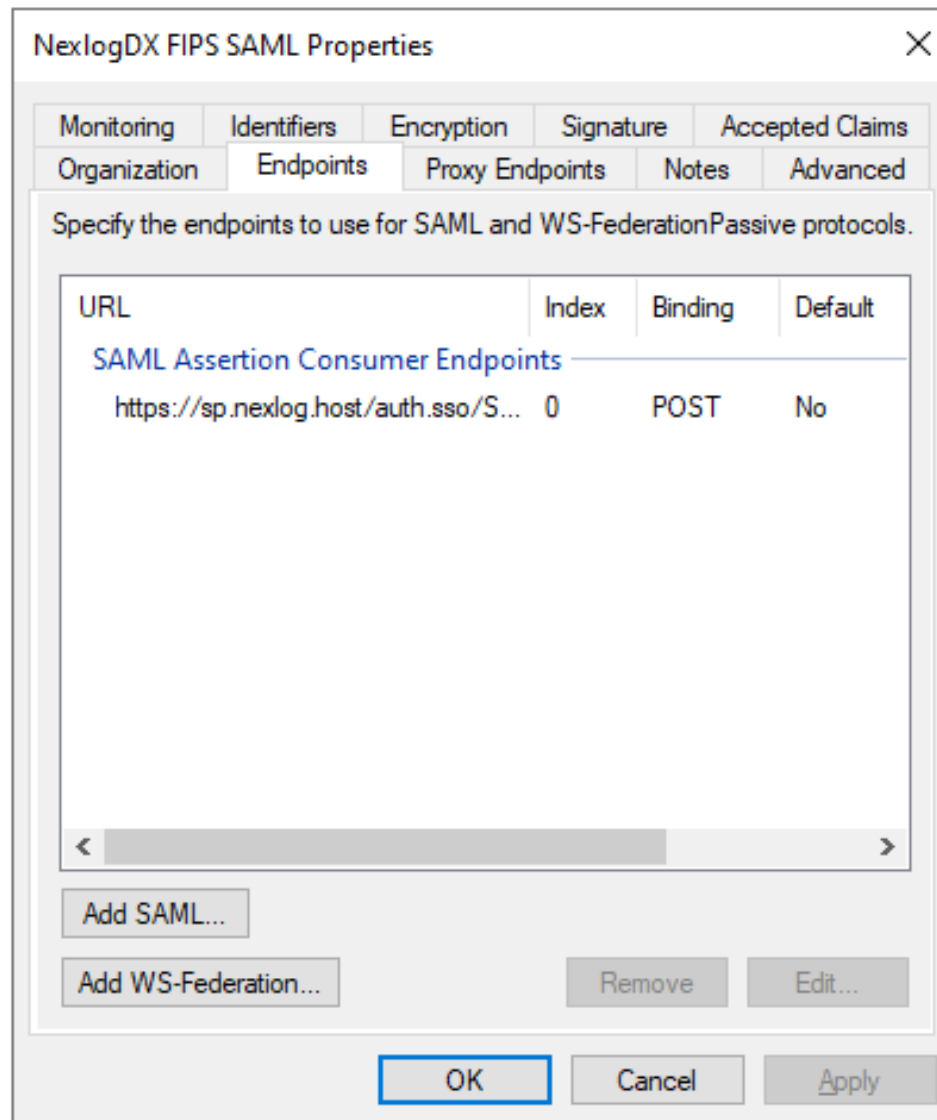


Fig. 7.17 Endpoints Add SAML

On the **Add an Endpoint** dialog. Choose the **POST** binding.

Increase the **Index** value by 1.

Enter the shown URL in the **Trusted URL** text box replacing **sp.nexlog.host** with your FQDN.

This is the same URL that was in step one of the **Add Relying Party Trust Wizard**, with the addition of port 8443.

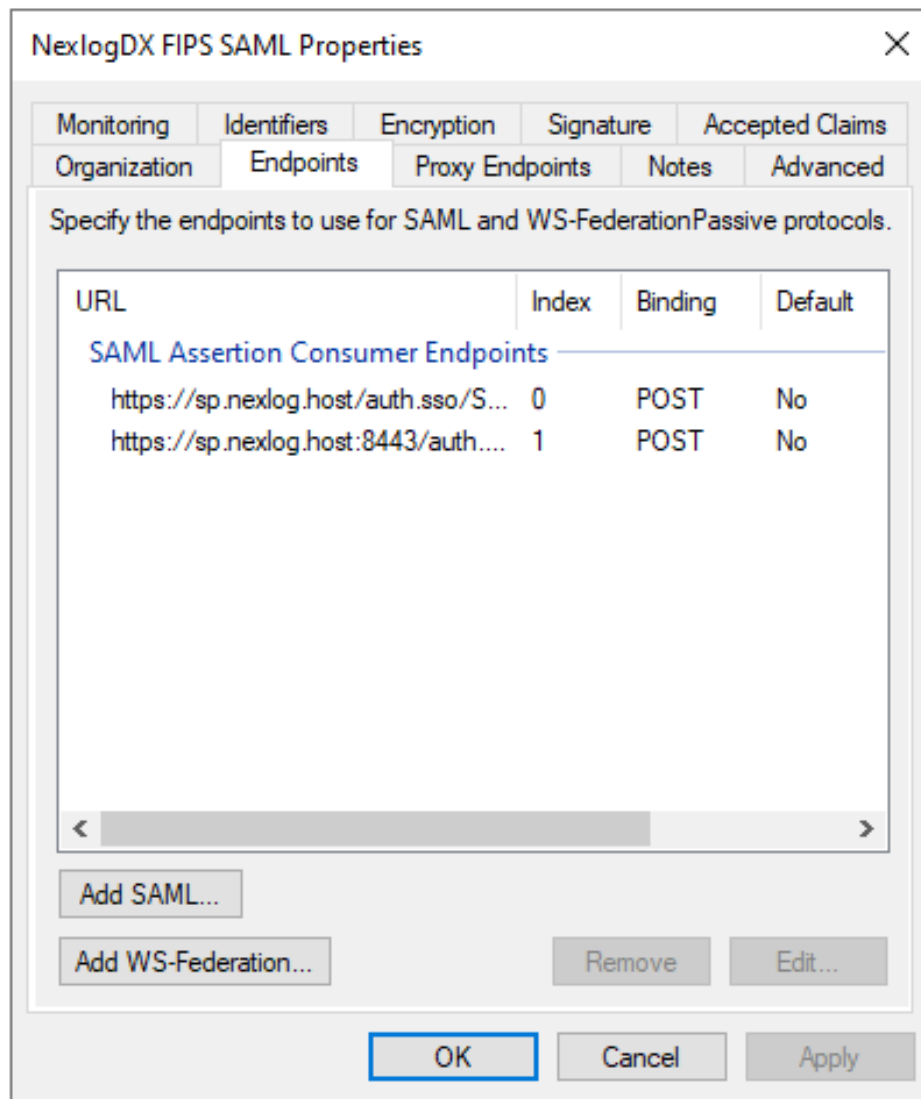


Fig. 7.18 Add Relying Party Trust 8443

Click **Apply**, then **OK** to finish the configuration.

This completes the Microsoft ADFS side of the configuration and you can now move on to Recorder SAML Configuration.

7.3.2. Duo Configuration

7.3.2.1. Prerequisites

Duo SSO authentication source configuration

This guide assumes the your SSO authentication source has already been configured.

Duo Permissions

You will need the appropriate Duo permissions to create the application and groups for mapping recorder permissions.

TLS Certificate

A valid TLS certificate must be installed and enabled on the recorder.

Entity ID

The entity ID is a unique identifier for the service provider (SP) and the identity provider (IdP). The entity ID for the SP must be provided, and the entity ID for the IdP is programmatically pulled from its metadata file.

Metadata File

The metadata file is an XML document that contains information about the IdP. It includes the IdP's entity ID, public key, and other relevant information. The metadata file is used to configure the SP to trust the IdP. This can be obtained from Duo when configuring the application.

User Groups

User groups must be correctly set up on the recorder and Duo. The groups in the recorder must align with those in Duo to ensure proper group mapping for SAML authentication. Ensure groups in Duo have been created and users assigned.

Configuration Manager

Access to Configuration Manager is required to configure the SAML authentication provider on the recorder. The Configuration Manager login icon will not be available in the lower righthand corner when accessing Configuration Manager. You will need to log in by going to **<host>/admin**.

MediaWorks Replay

After successfully configuring Duo, log in to MediaWorks by navigating to the recorder and logging in.

7.3.2.1.1. Configuration Steps

From Duo's admin console, select Applications → Protect an Application:

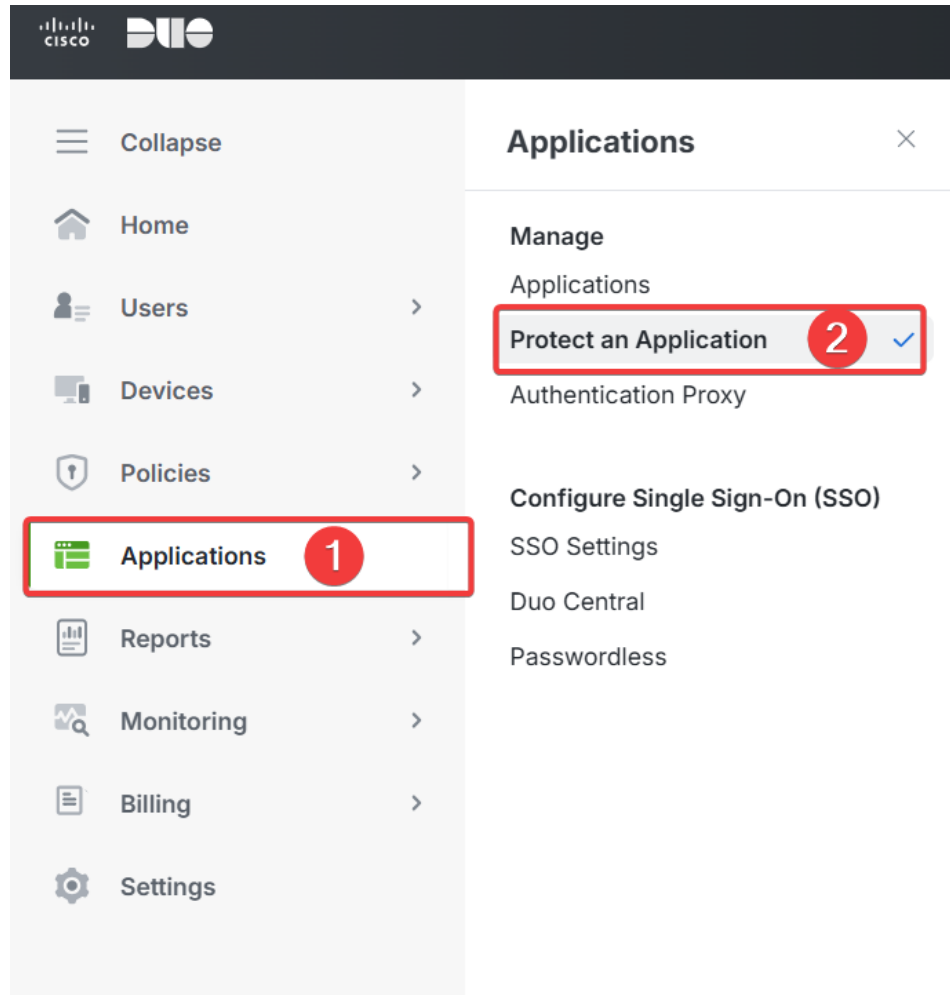


Fig. 7.19 Select “Protect an Application”

In the search bar type `Generic SAML` and select Configure for the application named `Generic SAML Service Provider`:

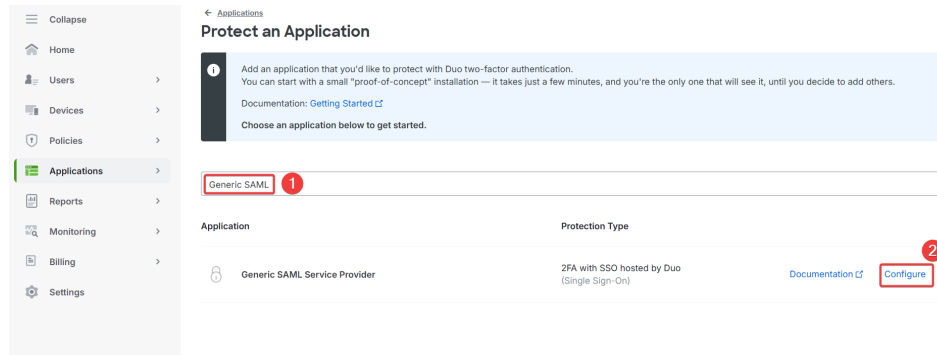


Fig. 7.20 Add a SAML application

On the next page, click Download XML for the **SAML Metadata** option. This will be used when configuring the recorder for SAML.

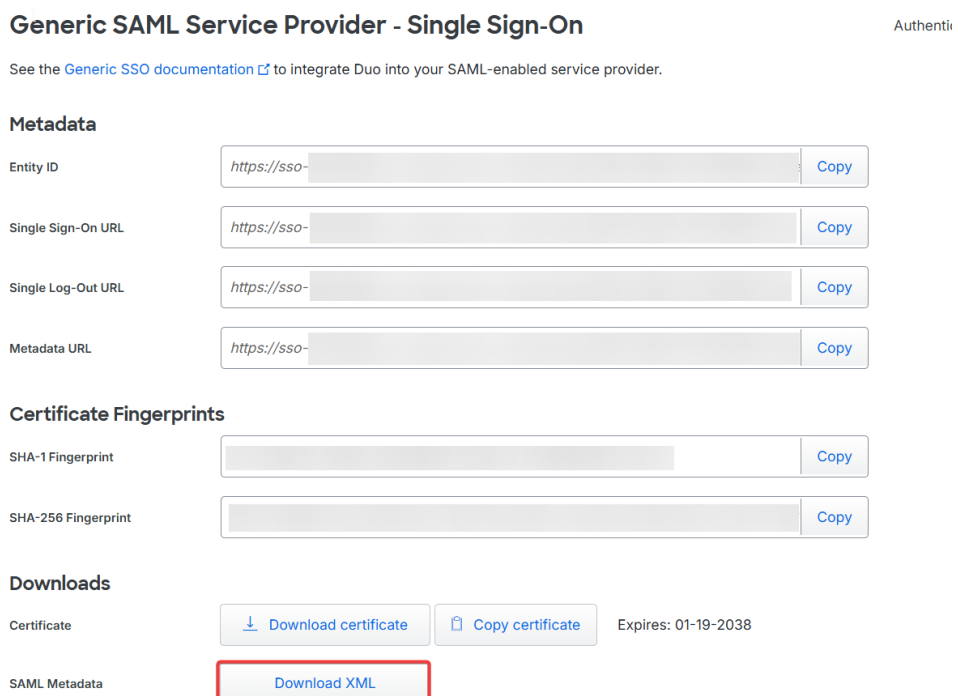


Fig. 7.21 Download Duo metadata

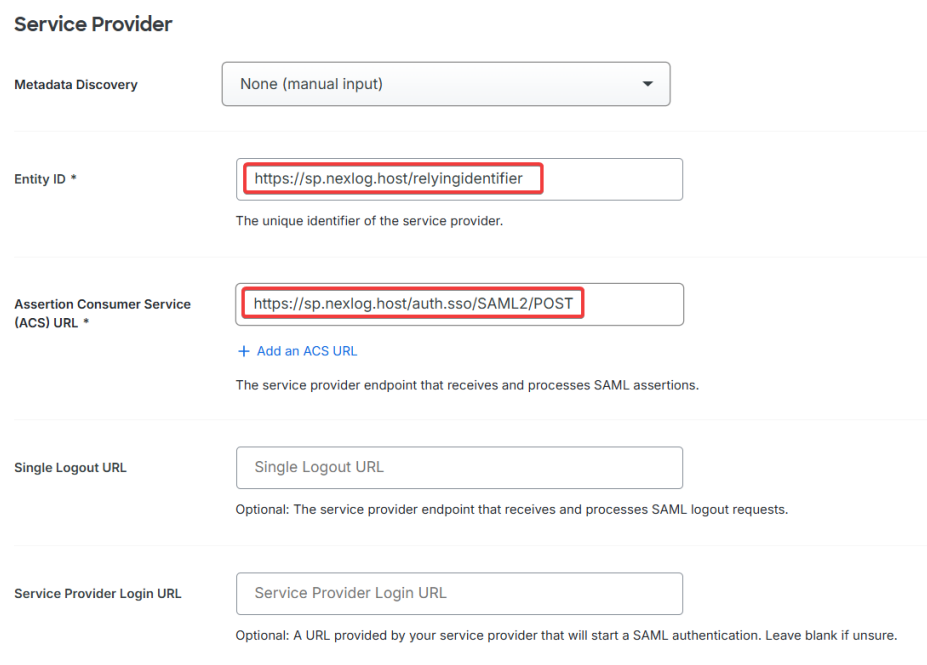
In the **Service Provider** section, enter the required values as shown in the below screenshot.

Entity ID - This can be any value as long as it is unique within your Duo tenant. Standard practice is to make this a URL, though the URL does not have to point to anything, nor does it need to resolve. It's simply used as a unique identifier. For this document, we will use the value,

`https://sp.nexlog.host/relyingidentifier` . Make note of this value, as it will be used later to configure the recorder side of SAML.

Assertion Consumer Service (ACS) URL - This will be `https://<RECORDER_FQDN>/auth.sso/SAML2/POST` - in the case of this example `https://sp.nexlog.host/auth.sso/SAML2/POST` .

If you elected to limit config access to port 8443 (On the recorder Users and Security → Encryption and TLS → Connection Settings), you can add an additional ACS URL by clicking Add an ACS URL. This will be the same value as above but specifying port `8443` (e.g. `https://sp.nexlog.host:8443/auth.sso/SAML2/POST`).



The screenshot shows the 'Service Provider' configuration page in Duo. It contains several input fields and a dropdown menu. The 'Metadata Discovery' dropdown is set to 'None (manual input)'. The 'Entity ID *' field contains the URL 'https://sp.nexlog.host/relyingidentifier'. The 'Assertion Consumer Service (ACS) URL *' field contains 'https://sp.nexlog.host/auth.sso/SAML2/POST'. Below this field is a link '+ Add an ACS URL'. The 'Single Logout URL' field contains 'Single Logout URL'. The 'Service Provider Login URL' field contains 'Service Provider Login URL'. Each field has a descriptive text below it.

Service Provider	
Metadata Discovery	None (manual input)
Entity ID *	<code>https://sp.nexlog.host/relyingidentifier</code> The unique identifier of the service provider.
Assertion Consumer Service (ACS) URL *	<code>https://sp.nexlog.host/auth.sso/SAML2/POST</code> + Add an ACS URL The service provider endpoint that receives and processes SAML assertions.
Single Logout URL	Single Logout URL Optional: The service provider endpoint that receives and processes SAML logout requests.
Service Provider Login URL	Service Provider Login URL Optional: A URL provided by your service provider that will start a SAML authentication. Leave blank if unsure.

Fig. 7.22 Duo SP settings

Leave the defaults and scroll down until you reach the **Map attributes** section. Configure the attributes as shown below and creating the mapping of Duo groups (required prerequisite) to recorder permissions:

Map attributes

IdP Attribute	SAML Response Attribute
<Email Address>	Email
<First Name>	FirstName
<Last Name>	LastName

Map the values of an IdP attribute to another attribute name to be included in the SAML response (e.g. Username to User.Username). Enter an IdP attribute chooses the NameID attribute based on the IdP. Create custom bridge attributes or select from the preconfigured options: <Email Address>, <Username>. Consult your service provider for more information on their attribute names.

Create attributes

Name	Value

Specify attributes with hard-coded values to optionally send in the SAML response (e.g. accountNumber with value of 48152547). Consult your service

Role attributes

Map Duo groups to different roles in this service provider. A Duo group can be mapped to multiple roles and each role can have m

[Learn more about Duo groups.](#)

Attribute name

groups

The name of the attribute which will carry the mapped roles.

Service Provider's Role	Duo groups
Monitors	x NLTest_Monitors (1 user)
Researchers	x NLTest_Researchers (1 user)

Fig. 7.23 Duo attributes and groups

The default SAML attribute mapping used by recorders utilize **UPN** for the username, stripping everything after the @ symbol. Since we are using email in the above configuration, adding groups and additional attributes as well, the attribute mapping will need to be updated by logging into Configuration Manager, navigating to System → Configuration Files → SAML attribute map and clicking View / Edit at the bottom of the page.

Below is a mapping that could be used with this example configuration:

```
<Attribute name="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress" id="remote_user"/>
<Attribute name="groups" nameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" id="attr_group"/>
<Attribute name="FirstName" nameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" id="attr_firstname"/>
<Attribute name="LastName" nameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" id="attr_lastname"/>
<Attribute name="Email" nameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" id="attr_email"/>
```

Scroll down until you reach **Name** and **Permitted Groups**. Give the application an appropriate name. You can also restrict users who can authenticate via groups. If you didn't configure this, users could try

to log in and their account would be created but login would fail since they wouldn't be assigned any permissions:

Name **Nexlog DX SAML**
Duo Push users will see this when approving transactions.

Self-service portal ☐ Let users remove devices, add new devices, and reactivate Duo Mobile
See [Self-Service Portal documentation](#).
To allow Duo to notify users about self-service portal activity, select [Settings > Notifications](#)

Username normalization Username normalization for Single-Sign On applications is controlled by the e
Controls if a username should be altered before trying to match them with a Duo user accc

Voice greeting **Welcome to Duo.**
Specify the message read to users who use phone callback, followed by authentication ins

Notes
For internal use. Maximum 512 characters.

Administrative unit Assign administrative unit

Optional

Permitted groups ☒ Only allow authentication from users in certain groups
x NLTest_Monitors (1 user)
x NLTest_Researchers (1 user)
When unchecked, all users can authenticate to this application.

Fig. 7.24 Duo applicaiton name and group restriction

Click Save.

This completes the Duo side of the configuration and you can now move on to Recorder SAML Configuration.

7.3.3. Entra ID Configuration

7.3.3.1. Prerequisites

Microsoft Entra ID Permissions

You will need the appropriate Microsoft Entra ID permissions to create the enterprise application and groups for mapping recorder permissions.

TLS Certificate

A valid TLS certificate must be installed and enabled on the recorder.

Entity ID

The entity ID is a unique identifier for the service provider (SP) and the identity provider (IdP). The entity ID for the SP must be provided, and the entity ID for the IdP is programmatically pulled from its metadata file.

Metadata File

The metadata file is an XML document that contains information about the IdP. It includes the IdP's entity ID, public key, and other relevant information. The metadata file is used to configure the SP to trust the IdP. This can be obtained from Microsoft Entra ID after configuring the enterprise application.

User Groups

User groups must be correctly set up on the recorder and Microsoft Entra ID. The groups in the recorder must align with those in Microsoft Entra ID to ensure proper group mapping for SAML authentication. Ensure groups in Microsoft Entra ID have been created and users assigned

Configuration Manager

Access to Configuration Manager is required to configure the SAML authentication provider on the recorder. The Configuration Manager login icon will not be available in the lower righthand corner when accessing Configuration Manager. You will need to log in by going to **<host>/admin**.

MediaWorks Replay

After successfully configuring Microsoft Entra ID, log in to MediaWorks by navigating to the recorder and logging in.

7.3.3.1.1. Configuration Steps

Within Microsoft Entra ID navigate to Enterprise Applications and select New Application:

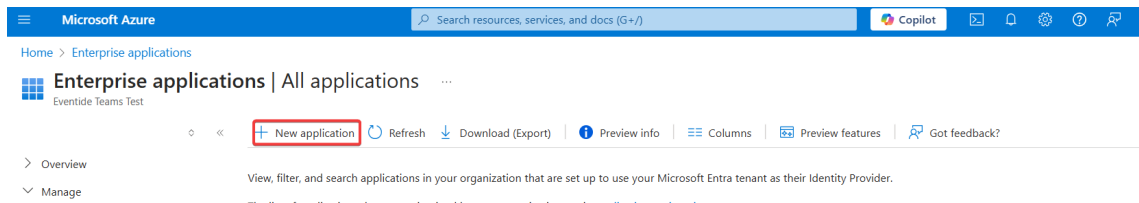


Fig. 7.25 **Add Enterprise Application**

On the next page, select the option at the top titled Create your own application, enter a name and click Create:

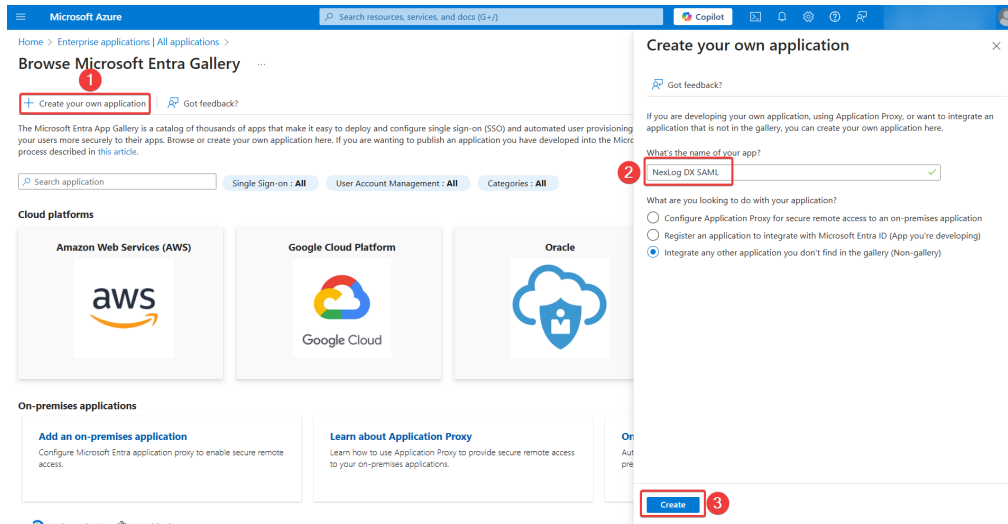


Fig. 7.26 Create your own application

Once on the Overview page for the new application, click Manage → Single sign-on and then select SAML:

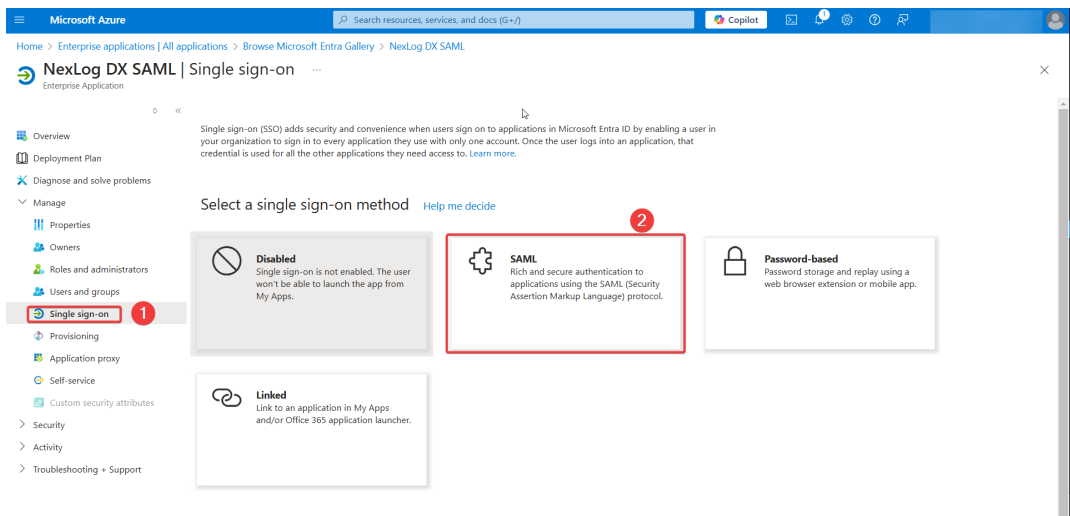


Fig. 7.27 Enable SAML

Next select the Edit button in box 1 (**Basic SAML Configuration**), enter the required values and click Save.

Identifier (Entity ID) - This can be any value as long as it is unique within your Entra ID tenant. Standard practice is to make this a URL, though the URL does not have to point to anything, nor does it need to

resolve. It's simply used as a unique identifier. For this document, we will use the value, `https://sp.nexlog.host/relyingidentifier`. Make note of this value, as it will be used later to configure the recorder side of SAML.

Reply URL (Assertion Consumer Service URL (ACS)) - This will be

`https://<RECORDER_FQDN>/auth.sso/SAML2/POST` – in the case of this example

`https://sp.nexlog.host/auth.sso/SAML2/POST`.

If you elected to limit config access to port 8443 (On the recorder Users and Security → Encryption and TLS → Connection Settings), you can add an additional ACS URL. This will be the same value as the ACS value above but specifying port `8443` (e.g.

`https://sp.nexlog.host:8443/auth.sso/SAML2/POST`).

Basic SAML Configuration

Save
 Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
<code>https://sp.nexlog.host/relyingidentifier</code>	☒ ⓘ

[Add identifier](#)

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
<code>https://sp.nexlog.host/auth.sso/SAML2/POST</code>		☒ ⓘ
<code>https://sp.nexlog.host:8443/auth.sso/SAML2/POST</code> Optional	☒	☐ ⓘ

[Add reply URL](#)

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

ⓘ

Relay State (Optional) ⓘ

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a

Fig. 7.28 Configure SAML

The default SAML attribute mapping used by recorders utilize **UPN** for the username, stripping everything after the @ symbol. If you plan to add no other claims, you can edit the **SAML Attribute Mapping** on the recorder by logging into Configuration Manager, navigating to System → Configuration Files → SAML attribute map and clicking View / Edit at the bottom of the page. You should then adjust the **remote_user** mapping like shown below:

```
<Attribute name="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress" id="remote_user"/>
```

Hint

The above mapping can also be used for the **attr_email** mapping if you chose to configure it on the recorder

Example UPN Claim Creation

Alternatively, you could add the default UPN claim or use any other claim you'd like but the SAML attribute mapping on the recorder would need to be updated to reflect this. Below is an example of creating the UPN claim.

Back on the **SAML-based Sign-on configuration** page select edit for box 2 (**Attributes & Claims**). On this page, select **Add new claim**.

Home > NexLog DX SAML | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims ...

[+ Add new claim](#) [+ Add a group claim](#) [Columns](#) [Got feedback?](#)

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...] ***

Additional claims

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

▼ Advanced settings

Fig. 7.29 Add a new claim

Configure the claim as shown below and click **Save**.

Home > Enterprise applications | All applications > NexLog DX SAML | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >

Manage claim ...

[Save](#) [Discard changes](#) [Got feedback?](#)

Name * 1 ✓

Namespace 2 ✓

▼ Choose name format

Source * ☒ Attribute ☐ Transformation ☐ Directory schema extension

Source attribute * 3 ✓

▼ Claim conditions

▼ Advanced SAML claims options

Fig. 7.30 Configure new claim

Next, we will need to create a group claim so the groups the user belongs to are part of the assertion and can be used with the group to permission mapping on the recorder.

Back on the **Attributes & Claims** page, select **Add a group claim** and configure as shown below. If you have a Microsoft Entra ID tenant that is synchronized with on-premise you may want to choose a different option than shown such as **sAMAccountName**. It is also possible to leave the default of **Group ID** although the group mapping configuration on the recorder would be less clear than using names.

Home > Enterprise applications | All applications > NextLog DX SAML | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	SAML	user.userprincipalname [...]

Advanced settings

Group Claims

Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

☐ None
☐ All groups
☐ Security groups
☐ Directory roles
☒ Groups assigned to the application

Source attribute *

Cloud-only group display names

☐ Emit group name for cloud-only groups

Advanced options

Save

Fig. 7.31 Add a group claim

You will also need to edit the SAML attribute map (System → Configuration Files → SAML attribute map) for the group claim using the example below:

```
<Attribute name="http://schemas.microsoft.com/ws/2008/06/identity/claims/groups" id="attr_group"/>
```

The last thing you will want from the SAML configuration page is to download the **Federation Metadata XML**, this is in box 3 (**SAML Certificates**):

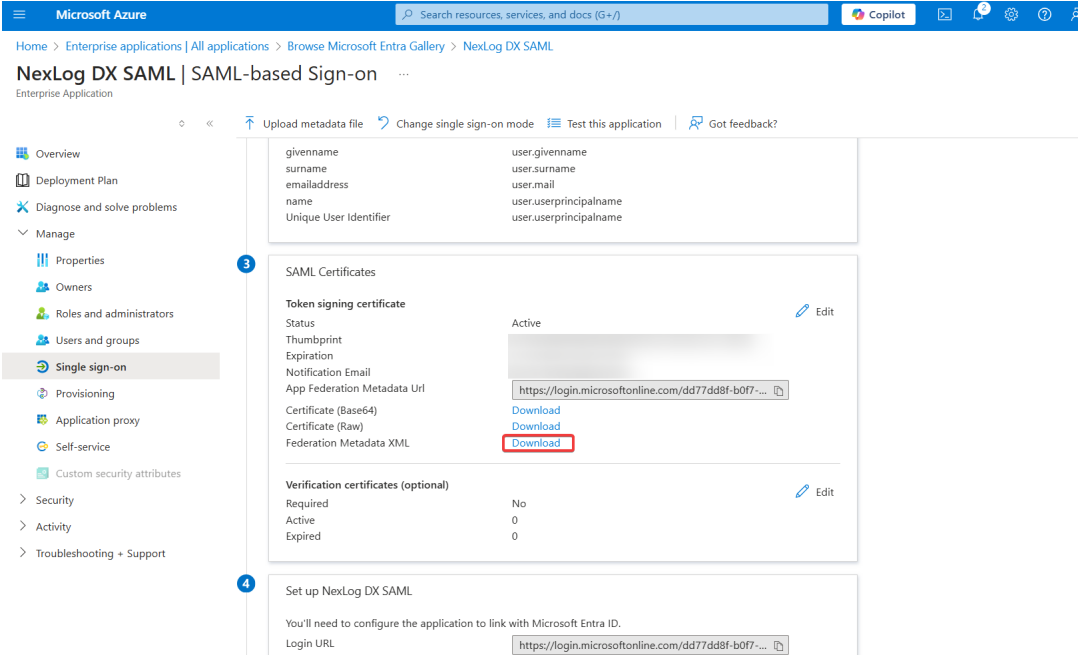


Fig. 7.32 Download metadata from Entra ID

If you do not have groups created, you should now create groups that can be mapped to one or more permissions on the recorder. These groups should then be added to the enterprise application.

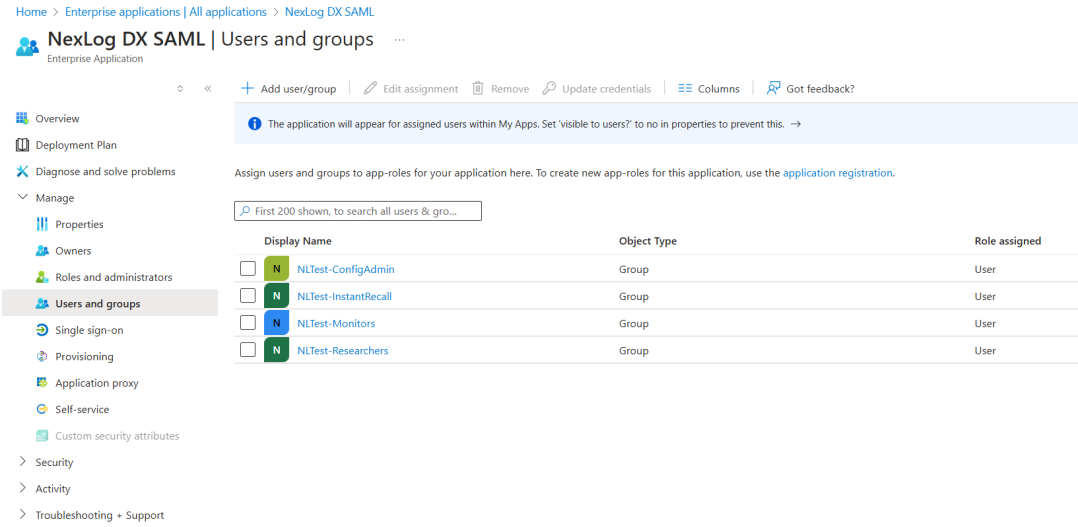


Fig. 7.33 Example group configuration

This completes the Microsoft Entra ID side of the configuration and you can now move on to Recorder SAML Configuration.

7.3.4. Okta Configuration

7.3.4.1. Prerequisites

Okta Permissions

You will need the appropriate Okta permissions to create the application and groups for mapping recorder permissions.

TLS Certificate

A valid TLS certificate must be installed and enabled on the recorder.

Entity ID

The entity ID is a unique identifier for the service provider (SP) and the identity provider (IdP). The entity ID for the SP must be provided, and the entity ID for the IdP is programmatically pulled from its metadata file.

Metadata File

The metadata file is an XML document that contains information about the IdP. It includes the IdP's entity ID, public key, and other relevant information. The metadata file is used to configure the SP to trust the IdP. This can be obtained from Okta after configuring the application.

User Groups

User groups must be correctly set up on the recorder and Okta. The groups in the recorder must align with those in Okta to ensure proper group mapping for SAML authentication. Ensure groups in Okta have been created and users assigned.

Configuration Manager

Access to Configuration Manager is required to configure the SAML authentication provider on the recorder. The Configuration Manager login icon will not be available in the lower righthand corner when accessing Configuration Manager. You will need to log in by going to **<host>/admin**.

MediaWorks Replay

After successfully configuring Okta, log in to MediaWorks by navigating to the recorder and logging in.

7.3.4.1.1. Configuration Steps

In the Okta admin console, navigate to Applications → Applications and select Create App Integration:

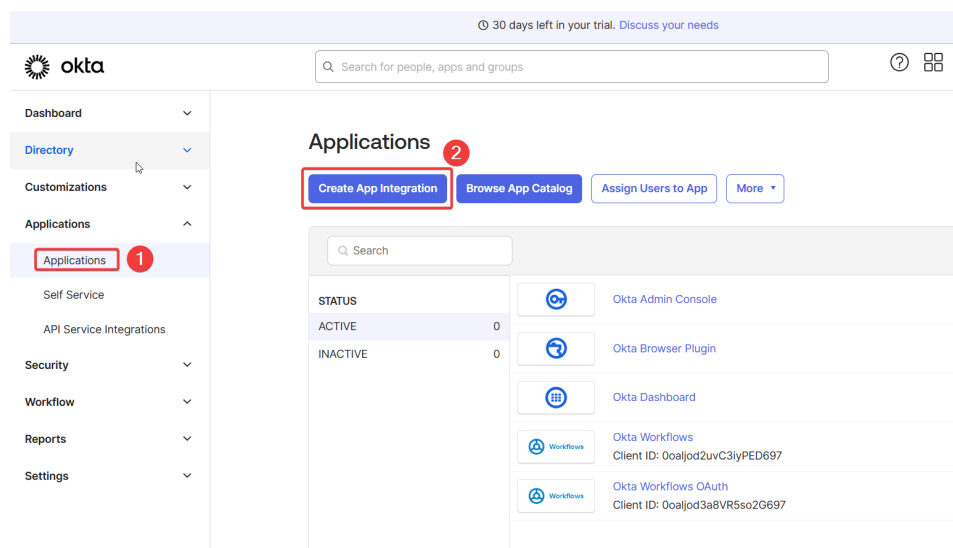


Fig. 7.34 Create app integration

Select **SAML 2.0** for the sign-in method and click Next:

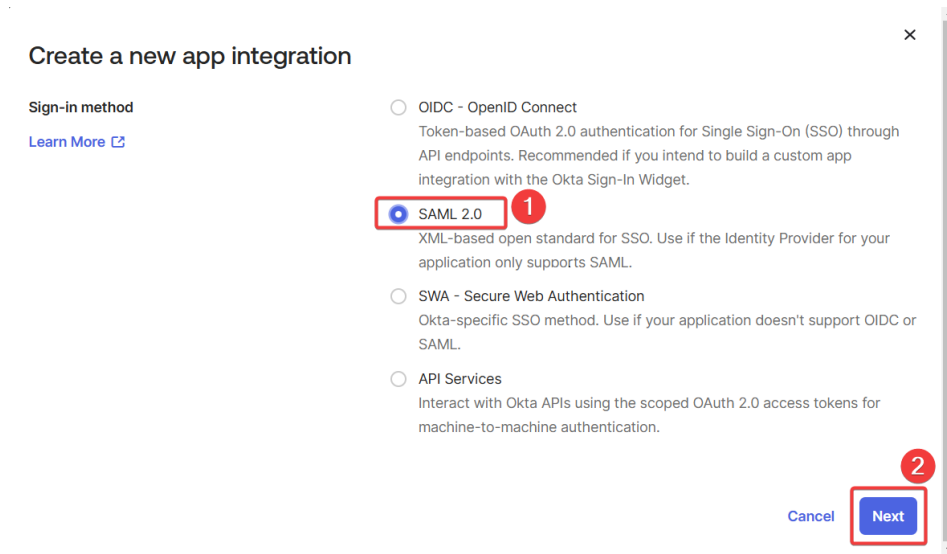


Fig. 7.35 Select SAML 2.0 as sign-in method

Enter a name on the **General Settings** page and click Next:

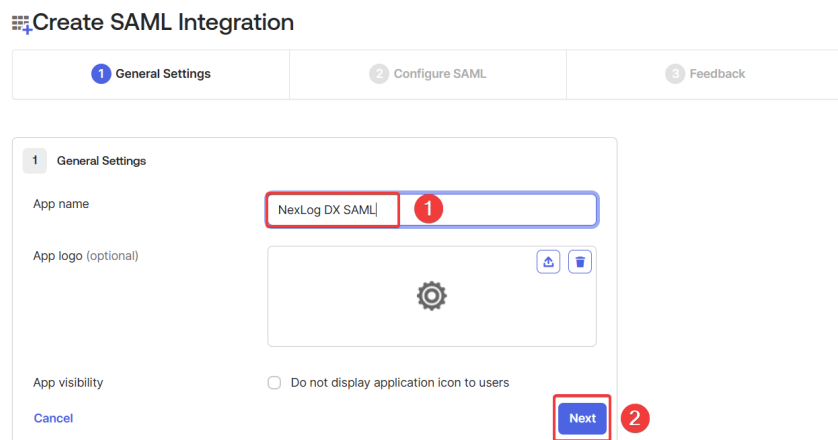


Fig. 7.36 SAML General Settings

On the **Configure SAML** page, enter the required values as shown in the below screenshot.

Single sign-on URL (Assertion Consumer Service URL (ACS)) - This will be `https://<RECORDER_FQDN>/auth.sso/SAML2/POST` – in the case of this example `https://sp.nexlog.host/auth.sso/SAML2/POST`.

Audience URI (SP Entity ID) - This can be any value as long as it is unique within your Okta tenant. Standard practice is to make this a URL, though the URL does not have to point to anything, nor does it need to resolve. It's simply used as a unique identifier. For this document, we will use the value, `https://sp.nexlog.host/relyingidentifier`. Make note of this value, as it will be used later to configure the recorder side of SAML.

1 General Settings 2 Configure SAML 3 Feedback

A SAML Settings

General

Single sign-on URL `https://sp.nexlog.host/auth.sso/SAML2/POST` 1
☒ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) `https://sp.nexlog.host/relyingidentifier` 2

Default RelayState
If no value is set, a blank RelayState is sent

Name ID format EmailAddress 3

Application username Email 4

Update application username on Create and update

[Show Advanced Settings](#)

What does this form do?
This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?
The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Fig. 7.37 SAML Settings

If you elected to limit config access to port 8443 (On the recorder Users and Security → Encryption and TLS → Connection Settings), you can add an additional ACS URL expanding Show Advanced Settings and clicking Add Another under **Other Requestable SSO URL**. This will be the same value as the **Single sign-on URL (Assertion Consumer Service URL (ACS))** above but specifying port `8443` (e.g. `https://sp.nexlog.host:8443/auth.sso/SAML2/POST`).

[Hide Advanced Settings](#)

Response ?	Signed						
Assertion Signature ?	Signed						
Signature Algorithm ?	RSA-SHA256						
Digest Algorithm ?	SHA256						
Assertion Encryption ?	Unencrypted						
Signature Certificate ?	Browse files...						
Enable Single Logout ?	☐ Allow application to initiate Single Logout						
Signed Requests ?	☐ Validate SAML requests with signature certificates. SAML request payload will be validated. SSO URLs will be read dynamically from the request. Read more						
Other Requestable SSO URLs	<table><thead><tr><th>URL</th><th>Index</th></tr></thead><tbody><tr><td> https://sp.nexlog.host:8443/auth.s </td><td> ×</td></tr><tr><td colspan="2">+ Add Another</td></tr></tbody></table>	URL	Index	https://sp.nexlog.host:8443/auth.s	×	+ Add Another	
URL	Index						
https://sp.nexlog.host:8443/auth.s	×						
+ Add Another							

Fig. 7.38 Optional Additional ACS for config access on port 8443

Scroll down to the **Attribute Statements (optional)** section. If you'd like to map attributes such as name, you can add them as shown below:

Attribute Statements (optional) [LEARN MORE](#)

Name	Name format (optional)	Value
FirstName	Basic	user.firstName
LastName	Basic	user.lastName
Email	Basic	user.email

[Add Another](#)

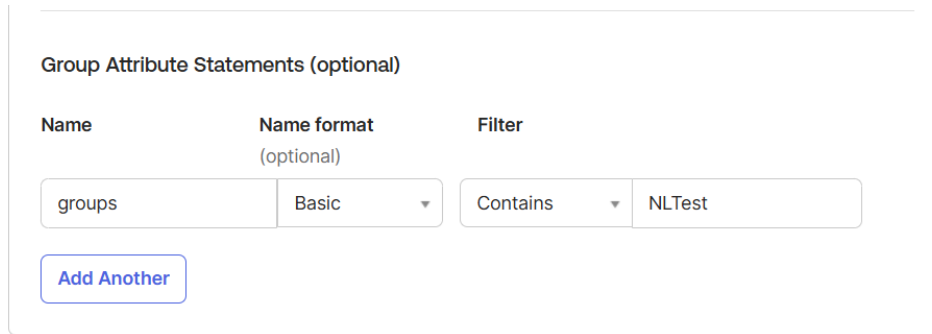
Fig. 7.39 Additional attributes

The default SAML attribute mapping used by recorders utilize **UPN** for the username, stripping everything after the @ symbol. Since we are using email in the above configuration, adding groups and additional attributes as well, the attribute mapping will need to be updated by logging into Configuration Manager, navigating to System → Configuration Files → SAML attribute map and clicking View / Edit at the bottom of the page.

Below is a mapping that could be used with this example configuration:

```
<Attribute name="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress" id="remote_user"/>
<Attribute name="FirstName" nameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" id="attr_firstname"/>
<Attribute name="LastName" nameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" id="attr_lastname"/>
<Attribute name="Email" nameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" id="attr_email"/>
```

Scroll down to **Group Attribute Statements (optional)** and configure as shown below, replacing the filter with the prefix of the groups you created within Okta:



Name	Name format (optional)	Filter
groups	Basic	Contains NLTest

[Add Another](#)

Fig. 7.40 SAML Group Settings

In order for the groups to be mapped correctly, you will need to update the SAML attribute map for this as well using the below example:

```
<Attribute name="groups" nameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" id="attr_group"/>
```

Click Next at the bottom of the **Configure SAML** page and then Finish on the **Feedback** page.

Navigate back to Applications → Applications and select your new application. On the **Sign On** tab, scroll down and copy the Metadata URL. You will use this when completing the recorder side of the configuration.

The screenshot shows the 'Sign On' tab in the Okta admin console. Under 'Settings', the 'Sign on methods' section is active. It explains that the sign-on method determines how a user signs into and manages their credentials for an application. Below this, the 'SAML 2.0' method is selected. In the 'Metadata details' section, the 'Metadata URL' is shown as 'https://[redacted]/saml/metadata'. A 'Copy' button is highlighted with a red box.

Fig. 7.41 Download Metadata

This completes the Okta side of the configuration and you can now move on to Recorder SAML Configuration.

7.4. Configuring the recorder

7.4.1. Recorder SAML Configuration

7.4.1.1. Before You Begin

SAML Attribute Mapping

The default claim used for username is different depending on the IdP. To confirm the mapping matches your setup, the SAML attribute map can be viewed/edited on the recorder by navigating to System → Configuration Files → SAML attribute map and clicking **View / Edit** at the bottom of the page.

You should also confirm mappings for other values such as name and email are correct.

Verify User Groups in Configuration Manager

Begin by ensuring that your recorder has User Groups correctly set up. Log in to Configuration Manager and go to 'Users and Security', and select the 'User Groups' page. Here, you will find different groups with varying access levels. Some groups may have access only to the MWP (Media Workflow Platform), others solely to Configuration Manager, and some may have access to both.

Configure IdP User Groups

Next, make sure that your IdP has groups configured appropriately, aligning with those defined in the Configuration Manager. Refer to our IdP specific implementation guides for additional details.

7.4.1.2. Adding an Authentication Provider

Once the SAML IdP is configured, we can turn our attention to configuring SAML on the recorder itself.

Note

When accessing Configuration Manager, the login icon will not be available in the lower righthand corner. You'll need to login by going to **<host>/admin**.

Once logged in as an administrator, you can select:

Users and Security → Authentication Providers

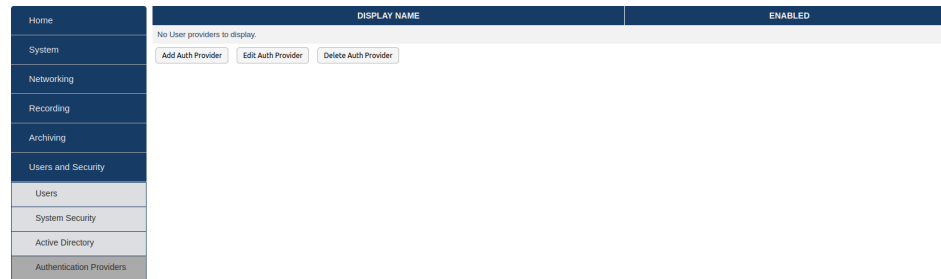


Fig. 7.42 Auth Providers

Then click the **Add Auth Provider** button to add details about your IdP.

You will not be able to click on the **Enabled** button until certain fields are filled in. We'll start from top to bottom.

- **Type:** Will default to SAML, but if it isn't, click the Type drop down and choose SAML
- **Display Name:** This can be any value and is simply a name to give to the configuration, for example "DISA".
- **User Provisioning:** Click this checkbox.
- **Active Directory Federation Services (ADFS):** Click the checkbox if you followed the ADFS Configuration guide.
- **Display Order:** Select a value, this allows you to set the list order of authentication providers configured.
- **Relying Provider Identifier:** Recall from your IdP configuration, that the service provider is identified by an entityID. This field must match what was configured in your IdP. We'll use the same value outlined in all of our example configurations: <https://sp.nexlog.host/relyingidentifier>
- **Recorders Fully Qualified Domain Name (FQDN):** This is the FQDN configured on the recorder and matching the TLS certificate installed on the recorder.
- **Generate New x.509 Certification:** You can leave this unchecked, however checking the box will trigger new certificates to be generated. The certificates are used in the SAML process itself. If you are editing a previously configured authentication provider, generating new certificates may require you to delete the old signing and encryption certificates for your IdP.
- **Identity Provider Metadata Configuration:** To populate this box, use the file downloaded during the IdP configuration steps.

Click on the **Enabled** button on the top of the page.

Fig. 7.43 Auth Provider Setting Full

7.4.1.3. SAML Group Mapping

Mapping Recorder Groups to Directory Groups

On the 'Groups' page, you will see a list of 'Recorder Group Name' entries. These are the User Groups previously identified on the 'User Groups' page. Your task here is to map each 'Recorder Group Name' to the corresponding group configured in your IdP.

Fig. 7.44 Groups Mapping

Accurate Group Name Entry

It's critical to enter the correct group name from your IdP with exactness. For instance, a group named 'Instant Recall' in the recorder should be mapped to its counterpart in your IdP, like 'ADJJM123-NLInstant Recall'. Pay attention to punctuation and spaces in the names.

Finalizing the Process

This mapping ensures that when a SAML AD user is created and made a member of a group like 'ADJJM123-NLInstant Recall', the system correctly identifies the mapping. This allows the user to log in to the MWP with the appropriate 'Instant Recall' permissions.

Important

If the mapping is incorrect, the user may be authenticated but will not gain access to MWP functionalities.

Click the **Save** button, then **OK** to acknowledge the webserver restart. You will then be returned to the Authentication Providers list, where you will see your newly configured provider.

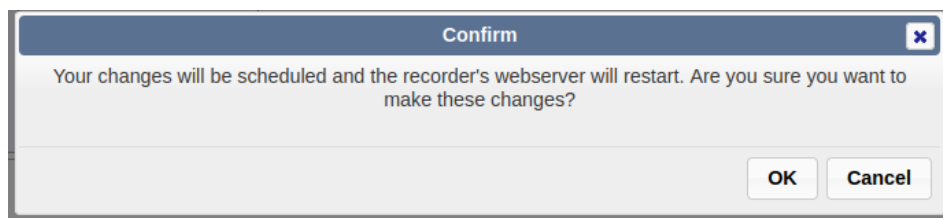


Fig. 7.45 Webserver Restart

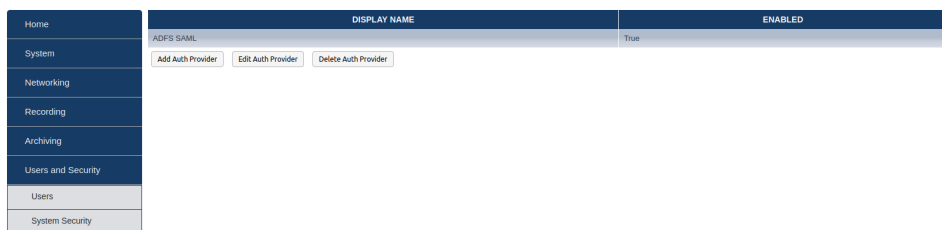


Fig. 7.46 SAML Complete

7.4.1.4. Verify MediaWorks Replay Configuration

After successfully configuring your authentication provider, log in to MediaWorks by navigating to the recorder and logging in using the **Login with <Authentication Provider Name>** option.

If there are any issues, you can still log in using the **Use Local Login** option.

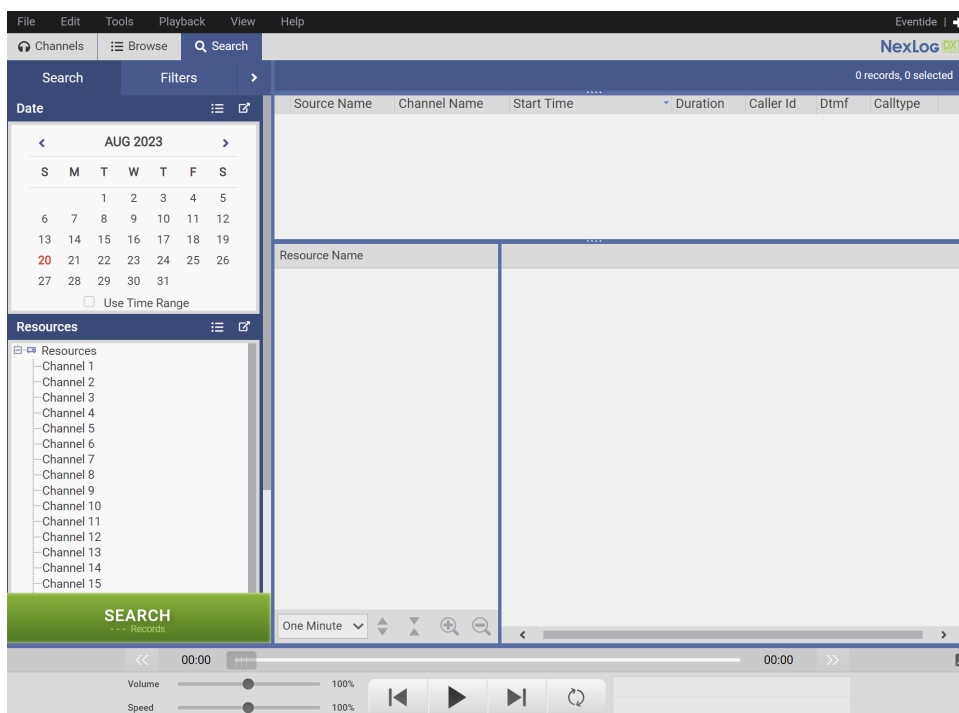


Fig. 7.47 MediaWorks Login

8. USERS AND GROUPS

When using directory service authentication, user group memberships can be managed locally or via the directory service.

One of the primary values of using LDAP or Active Directory authentication is a streamlined user creation and permission management workflow. Users already exist in groups on the domain, and by telling the recorder what those groups (or new groups added specifically for recorder permissions) mean, you can manage users more easily than before.

8.1. Local Users with LDAP

Users that only exist on the recorder remain the same as always. Users can be created and administrated entirely on the recorder as on any system without an Active Directory integration.

Note

In the case that user names on the domain overlap with existing users on the recorder, the recorder user's permissions take precedence over the domain user.

8.2. Domain Users with LDAP Group Mapping

With LDAP Group Mapping, users are automatically created on the recorder at first log in, with the user group membership and channel permissions based on the LDAP Group Mapping. So, with the default mapping, if there is a user `LBertucci` on the domain who is an `NLResearcher`, when they log in for the first time they will be added as a `Researcher` on the recorder, and get the resource groups that the Researcher group has access to.

With LDAP Group Mapping on, you cannot edit user group membership of LDAP users on the recorder. You can however edit their resource groups for resource permissions and you can grant additional recorder level permissions individually. Resources granted by user groups are just defaults, as explained in the NexLog DX-Series system user manual, so you can change them as you wish after a user has been created.

8.2.1. Enable LDAP Group Mapping

LDAP Group Mapping can be configured in the web configuration manager at Users and Security → Active Directory → LDAP Settings.

Enable the Use LDAP User Group Settings checkbox.

In the LDAP Group Mapping section, enter the LDAP Group Name, from the directory service, that corresponds with the local recorder group name.

Table 8.1 **Default LDAP Group Mapping**

Recorder Group	LDAP Group
Admin	NLAdmin
Agents	NLAgents
Archivers	NLArchivers
Group Evaluators	NLGroupEvaluators
Instant Recall	NLInstantRecall
Maintainers	NLMaintainers
Monitors	NLMonitors
Report Editor	NLReportEditor
Researchers	NLResearchers
SuperEvaluators	NLSuperEvaluators
Systems	NLSystems
User Managers	NLUserManagers

LDAP Groups Base DN

This field should contain the root path containing all mapped groups. It should be entered using LDAP syntax.

Example: `OU=Groups,OU=HQ,DC=contoso,DC=net`

8.2.2. Export Recorder Groups to LDAP

This is an optional step, but a useful one. This allows you to import the permission groups the NexLog recorder is looking for to assign permissions to domain users at log in. If you have multiple NexLog recorders in your domain and they share the same group associations, then this procedure only needs to be run once.

This will save implementation time by not having to create each LDAP group one at a time. This should be completed after the LDAP or Active Directory settings are fully configured and saved, including LDAP Groups Base DN.

Navigate to Users and Security → Active Directory → LDAP Settings.

Export Eventide LDAP Security Group Schema

Click this button to generate a `groups.ldif` file which should be downloaded and verified for correctness.

For Microsoft Windows Active Directory, load `groups.ldif` onto a domain controller, then open an elevated shell. The program **ldifde** should already be installed on the server. Run the following command to import the schema:

```
ldifde.exe -i -f groups.ldif
```

Running **ldifde.exe -?** will bring up a help menu with further options.

Once that is done, verify the groups were added to the Active Directory. Users can now be assigned to certain groups, as a test.

8.3. Domain Users without LDAP Group Mapping

Without LDAP Group Mapping, you have to add each domain user individually, but then you can manage their group memberships at the recorder side as you would any other recorder user. This may be a better fit depending on how the recorder is being administered.

To add a domain user, enable the Active Directory User checkbox at creation time; this will disable the password fields because passwords are managed on the directory service only.

Add New User

User Info

☒ Active Directory User

Username:

Password:

Repeat Password:

Group Membership

☐ Admin	☐ Agents
☐ Archivers	☐ Group Evaluators
☐ Instant Recall	☐ Maintainers
☐ Monitors	☐ Report Editor
☐ Researchers	☐ SuperEvaluators
☐ Systems	☐ User Managers

Fig. 8.1 Add New Active Directory User

8.4. Passwords

In all cases, passwords for domain users are managed via the directory service. You cannot change passwords via the NexLog DX-Series recorder and if a user account is marked “Must Change Password at Next Login”, the user cannot log in to MediaWorks DX nor the web configuration manager until the password has been changed in the directory service.

9. NEXLOG ACCESS BRIDGE

NexLog Access Bridge (NAB) is a feature that allows a user to access media from multiple recorders (NAB Source), using a single recorder (NAB Base).

For NexLog Access Bridge to work smoothly, the Base and Source recorders should all be configured with the same Authentication Mode.

9.1. NAB with Active Directory

If the NAB Base and all NAB Sources are configured with Active Directory authentication in the same domain, login attempts will work smoothly. Each recorder included in the NAB network should be joined to the domain using a unique hostname and service account.

When creating the service accounts, be sure to enable delegation as shown in Figure 6.4 of Section 6.6.2: Set Service Principals.

If the NAB Base is joined to the domain, but the NAB Source is not, it will prompt for a login and you can enter the appropriate credentials to log into that recorder.

9.1.1. NAB with Single Sign-On

If Single Sign-On is enabled on a NAB Base, then ideally, all of the recorders involved in the NexLog Access Bridge network should be configured to use SSO as part of the same domain. That way, the login experience will be smooth.

If the NAB Base is configured for Single Sign-On, and the NAB Sources are not, then any SSO log in will fail back to the standard log in prompt when connecting to those sources.

The more complicated situation is the reverse. If the NAB Base is not configured for Single Sign-On, but a NAB Source is, then the NAB Source will require specific configuration to allow the connection to happen.

This might happen in a situation where your NAB Sources are all on one network and domain, but the NAB Base is remote or on a different domain.

In this case, an administrative user on the NAB Sources must create an exemption for the NAB Base to connect to its database.

See Section 9.3: NAB Base Database Exemption for how to create the exemption.

9.2. NAB with SMB

If the NAB Base is configured for SMB Authentication, each NAB Source it is connected to should also be configured for SMB authentication.

If the NAB Source is unable to be configured for SMB authentication, you must create an exemption for the NAB Base.

See Section 9.3: NAB Base Database Exemption for how to create the exemption.

9.3. NAB Base Database Exemption

When a NAB Source is unable to be configured for SMB, LDAP, or AD authentication due to network topology or configuration, a database exemption may be required.

The user must still have an account on the NAB Sources.

The screenshot shows a configuration window with several tabs: GENERAL, FRONT PANEL, PASSWORD COMPLEXITY, AGING, LOCKOUT, and TWO FACTOR AUTHENTICATION. The GENERAL tab is selected. Inside the GENERAL tab, there are several checkboxes:
- ☒ Audit changes
- ☒ Audit verbose
- ☐ Enable Incident Clip Management
- ☒ Enable User Content Uploads
- ☐ Enable Terms Of Service splash screen in MediaWorks Plus clients (edit contents in System->Configuration Files->Terms of Service Display)
- ☐ Enable Block Media Access
- ☐ Enable MediaWorks Plus ATC/ATM mode
Below these is a text field for "Session Communication Timeout (min):" with the value "5".
A red rectangle highlights the following section:
- ☒ Exempt NexLog Access Bridge Hosts from Database Authentication
- Below this, a text field "Exempted NexLog Access Bridge Host IP Addresses:" contains the value "10.74.3.11".
At the bottom of the GENERAL tab is a dropdown menu for "Encrypted Terminal (SSH)" set to "None".
At the very bottom of the window are "Save" and "Cancel" buttons.

Fig. 9.1 NAB Base Database Exemption

To create an exemption, login to the web configuration manager on each **NAB Source** and navigate to Users and Security → System Security.

Enable the checkbox for Exempt NexLog Access Bridge Hosts from Database Authentication.

In the field provided, enter the IP address of the NAB Base users will log in from. If the NAB network has a redundant Base, enter the IP address for each Base separated by a comma (,).

Save your changes and reboot the NAB Source.

A. TROUBLESHOOTING

Active Directory is complex and some of the error messages you can encounter while configuring the system are esoteric and could be caused by a variety of misconfigurations. This section will help point you in the correct direction when encountering errors.

The following are potential errors that may occur during user account authentication due to misconfiguration in the recorder Active Directory settings or Active Directory Domain Server. Each error message has typical issues and solutions listed, in addition to an optional explanation. The issues listed are not comprehensive, but are commonly encountered due to configuration errors.

Key Table entry not found

Explanation

An entry is not found in the keytab file that was imported to the recorder or there is a configuration error.

Common Causes

- The encryption type configuration on the recorder Active Directory page doesn't match the encryption type of the keytab.
- The recorder's service principal name in the keytab file doesn't match what is configured in the recorder Active Directory page

Solutions

- The encryption type configuration on the recorder Active Directory page should be changed to match that of the keytab file or vice versa.
- The correct recorder's service principal name should be configured on the recorder Active Directory page and the keytab file.

Kerberos Error

Explanation

Incorrect Kerberos configuration on the recorder Active Directory page.

Common Causes

- The Realm is incorrect.
- The KDC is incorrect.
- The encoding type is incorrect.
- The Recorder Service Principal is incorrect.
- Invalid keytab file is uploaded.
- The recorder may not be synced to the same time source as the domain.

Solutions

- The settings on the recorder Active Directory page should be correctly entered.
- The time sync configuration on the recorder should be checked to see if the recorder and domain agree on the time.

Credential Delegation Configuration Error

Explanation

The host recorder is unable to authenticate the user to the source recorder.

Common Causes

- The host recorder account on the Active Directory Domain does not have the “Trust this user for delegation to any service (Kerberos only)” option selected.
- The Browser is not set up for credential delegation on the user's PC.

Solutions

- Make sure the “Trust this user for delegation to any service (Kerberos only)” option is selected under the “Delegation” tab in the recorder's user account properties section on the Active Directory Domain.

- Make sure the browser (Chrome or Firefox) is set up for credential delegation. Refer to Section 6.6.6: Single Sign-On for instructions.

Unsupported encryption type is configured on the recorder

Explanation

The Active Directory Domain does not recognize the encryption type configured on the recorder.

Common Causes

- The recorder is configured for AES encryption when the Domain Server is not compatible with AES.

Solutions

- Make sure the encryption type in the recorder Active Directory page matches that of the keytab file.

Invalid Kerberos realm is configured on the recorder

Common Causes

- The realm information is configured incorrectly in the recorder Active Directory page.

Solutions

- Make sure the realm (on the recorder Active Directory page) matches that of the Domain Controller. For example, if the fully qualified domain name is example.eventide.local, the realm is typically EVENTIDE.LOCAL

The connection to the LDAP server timed out

Common Causes

- The recorder lost connection to the LDAP server due to a timeout.

Solutions

- Ensure that the recorder can reach the LDAP server.

The recorder's LDAP configuration might be incorrect

Explanation

The LDAP settings on the recorder Active Directory page may be incorrect.

Common Causes

- The port number or host name of the LDAP server may be incorrectly configured.

Solutions

- Make sure the LDAP settings on the recorder Active Directory page are correctly configured.

The recorder keytab file might not be valid

Common Causes

- The keytab file on the recorder might be out of date. That is, a new keytab was generated on the Domain Controller for the recorder account but not yet imported into the recorder.

Solutions

- Make sure the keytab file on the recorder is the most recent version, by importing it in the recorder Active Directory page. The recorder will then need to be rebooted.

The LDAP Server cannot be reached

Common Causes

- The LDAP Server might be down or the recorder cannot connect to it.

Solutions

- Make sure the LDAP Server is running and can be reached by the recorder

The recorder's password has expired in the Active Directory database

Common Causes

- The password for the recorder user account on the Domain has expired.

Solutions

- The recorder user account password on the Domain needs to be reset. If it is set to a new password, the keytab file will need to be regenerated and imported to the recorder. The recorder will then need to be restarted. It is advised to set the recorder user account password to not expire.

The recorder account has expired in the Active Directory Database

Common Causes

- The recorder's user account has expired in the Active Directory Database.

Solutions

- The recorder's user account on the Domain needs to be re-enabled.

Time skew between the recorder and the domain

Common Causes

- The time between the Active Directory Domain Controller and the recorder is not synchronized.

Solutions

- Configure the same NTP time source in the recorder's NTP page as the Active Directory Domain Controller.

The recorder's key table entry doesn't match the Active Directory database

Common Causes

- The realm configured may be incorrect.
- The keys in the recorder keytab file may not match those in the Active Directory Database for the recorder service principal.
- There may be a DNS problem.

Solutions

- Make sure the realm is correctly configured in the Active Directory page.
- Make sure the keys in the recorder keytab file match those in the Active Directory Database for the recorder service principal. The keytab file may need to be regenerated and re-imported.
- Make sure there are no DNS issues preventing the Domain Controller from correctly identifying the recorder and vice versa

The recorder domain account has incorrect credentials

Common Causes

- The recorder's keytab might be out of date.

Solutions

- Import the most recent keytab file in the recorder Active Directory page. The recorder will then need to be rebooted.

The recorder account was not found in the domain

Common Causes

- The account for the recorder's service principal name doesn't exist in Active Directory or is incorrect in Active Directory.

Solutions

- Make sure the recorder's user account still exists (and valid) in the Active Directory.

SSO login attempts return Authentication Failure

Common Causes

- The recorder's AD service account `sAMAccountName` does not match the hostname or FQDN that the user is attempting to log in from.

Solutions

- Check the recorder's service account Active Directory and verify that the `sAMAccountName` is the same as the hostname used to access the recorder. If `NLRecorder.contoso.net` is the URL used to access the recorder, `NLRecorder` **MUST** be the recorder service account's username.

SSO login results in Windows Authentication prompt

Common Causes

- The password for the recorder's service account was updated (even if to the same value) or a new keytab file was generated but not uploaded to the recorder (we recommend setting the password for the service account to not expire)
- The registry key values for the browser are not set appropriately
- The recorder's FQDN was not added to your group policy's Trusted Site list

Solutions

- Create and upload a new keytab file to the recorder then reboot
- See Single Sign-On for configuring registry settings for popular browsers
- Add the recorder's FQDN to your group policy's Trusted Sites list (see Single Sign-On)

B. AD POWERSHELL SCRIPT

Below is a complete powershell script that can be used for the creation of a new Active Directory service account, Service Principal Names, and a keytab.

Only the variables at the top of the script should be changed. You can save this file with a `.ps1` extension and run it with powershell.exe.

PowerShell

```
# Replace these variables
$recorderUser = "NLRecorder"
$recorderPassword = "1qazXSW2!@"
$recorderGivenName = "Eventide"
$recorderSurname = "NexLogDX"
$recorderOU = "CN=Users,DC=contoso,DC=net"
$fullDomain = "contoso.net"
$outputLocation = "C:\${recorderUser}\"

##### DO NOT EDIT BELOW THIS LINE #####

# DO NOT edit these variables
$recorderFQDN = "${recorderUser.ToLower()}.${fullDomain.ToLower()}"
$kerberosRealm = "${fullDomain.ToUpper()}"

# Create AD User
New-ADUser -Name "${recorderGivenName} ${recorderSurname}" `
    -GivenName "${recorderGivenName}" `
    -Surname "${recorderSurname}" `
    -SamAccountName "${recorderUser}" `
    -UserPrincipalName "${recorderUser}@${fullDomain}" `
    -Path "${recorderOU}" `
    -Enabled $true `
    -KerberosEncryptionType "AES256-SHA1" `
    -TrustedForDelegation $true `
    -ChangePasswordAtLogon $false `
    -PasswordNeverExpires $true `
    -AccountPassword (ConvertTo-SecureString -String
```

```
$recorderPassword -AsPlainText -Force) `
    -PassThru

# Create Service Principal Names (SPN)
Set-ADUser -Identity $recorderUser -PassThru -ServicePrincipalNames
@{Add=`
    "HTTP/$recorderFQDN@$kerberosRealm",
    "POSTGRES/$recorderFQDN@$kerberosRealm"} `
    -TrustedForDelegation $true

# Check if the output directory exists, if not, create it
if (-not (Test-Path -Path $outputLocation)) {
    New-Item -ItemType Directory -Path $outputLocation
}

# Creates the initial keytab for the HTTP SPN
Ktpass -out "${outputLocation}\NexLog_initial.keytab" `
    -princ "HTTP/$recorderFQDN@$kerberosRealm" `
    -mapUser "${fullDomain.Split(".",2)[0]}\$recorderUser" `
    -mapOp set `
    -pass $recorderPassword `
    -crypto AES256-SHA1 `
    -pType KRB5_NT_PRINCIPAL

# Adds the POSTGRES SPN to the HTTP keytab
Ktpass -in "${outputLocation}\NexLog_initial.keytab" `
    -out "${outputLocation}\NexLog_final.keytab" `
    -princ "POSTGRES/$recorderFQDN@$kerberosRealm" `
    -mapUser "${fullDomain.Split(".",2)[0]}\$recorderUser" `
    -mapOp add `
    -setUpn `
    -setPass `
    -pass $recorderPassword `
    -crypto AES256-SHA1 `
    -pType KRB5_NT_PRINCIPAL
```