Eventide®

NexLog DX
Communications Recording Solutions

Authentication & Active Directory Implementation Guide

Version 2024.1[4306]

P/N: #141341

P/N: #141341 Version 2024.1[4306]

Eventide Communications LLC.
One Alsan Way
Little Ferry, NJ 07643
201-641-1200

www.eventidecommunications.com

Table Of Contents

5. LDAP Authentication

6. Active Directory Authentication

7. Users and Groups

8. NexLog Access Bridge

9. NexLog DX-FIPS ADFS Configuration

A. Troubleshooting

B. AD Powershell Script

This page was intentionally left 99.88% blank.

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:

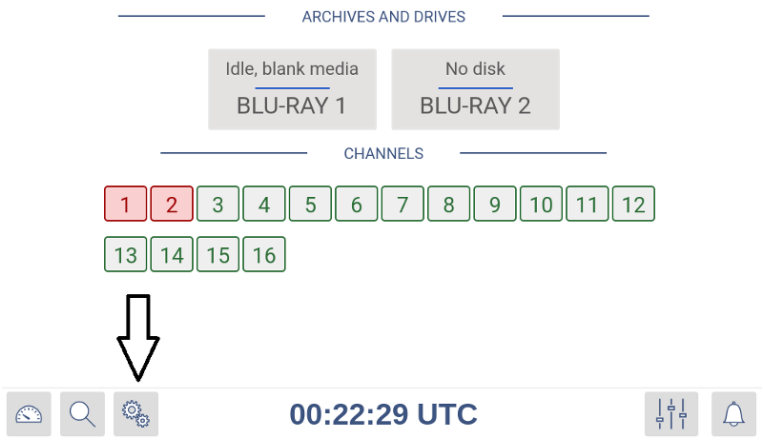


Fig. 1.1 **Front Panel Replay Screen (with arrow pointing to Setup button)**

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

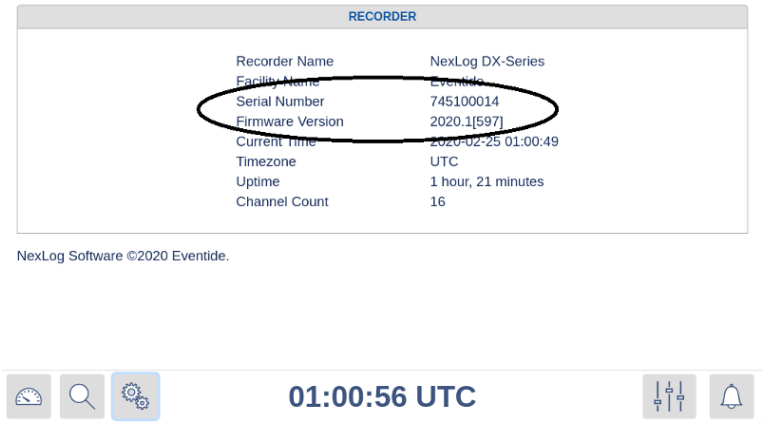


Fig. 1.2 **Front Panel Setup Screen (with serial and software version circled)**

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.

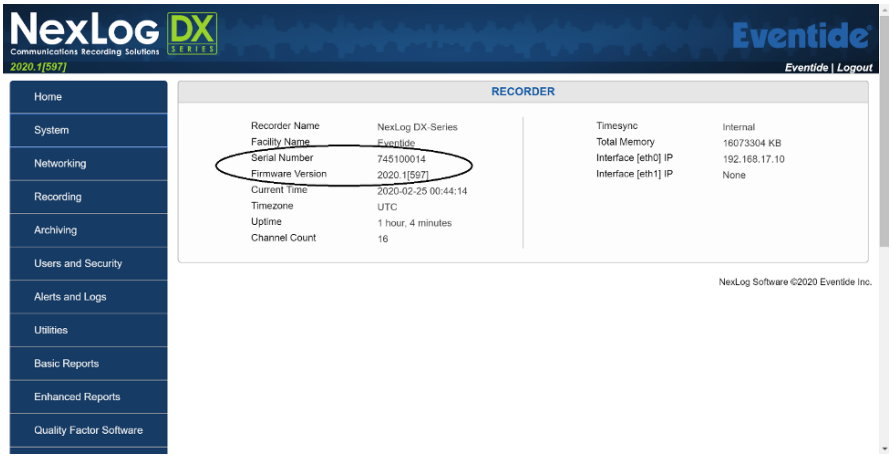


Fig. 1.4 **Configuration Manager Home Screen (with Serial and Firmware circled)**

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

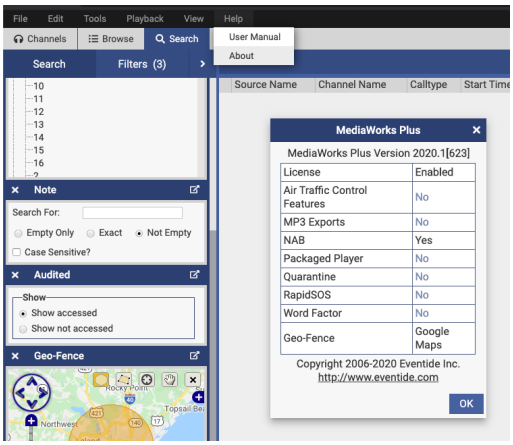


Fig. 1.5 **MediaWorks DX About Pop Up**

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 noteable differences between them.

Table 2.1 **Authentication Mode Comparison**

	Local	SMB	LDAP	Active Directory
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 funtions 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

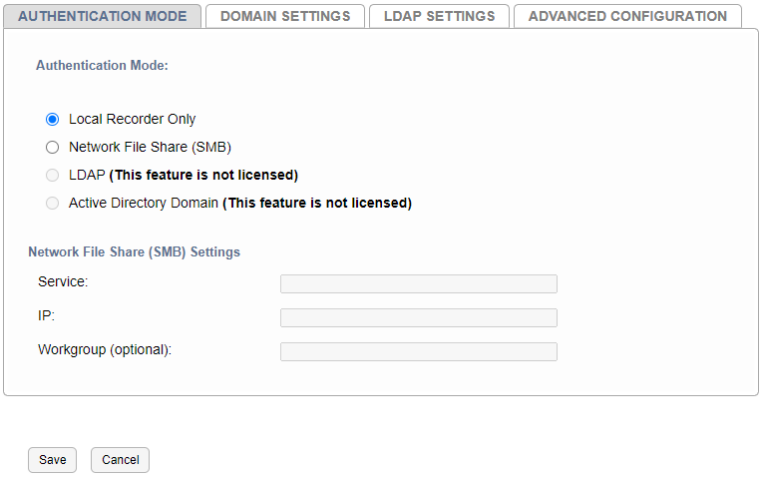


Fig. 2.1 **Authentication Mode Selection - Unlicensed**

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.

This page was intentionally left 99.88% blank.

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.

This page was intentionally left 99.88% blank.

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.

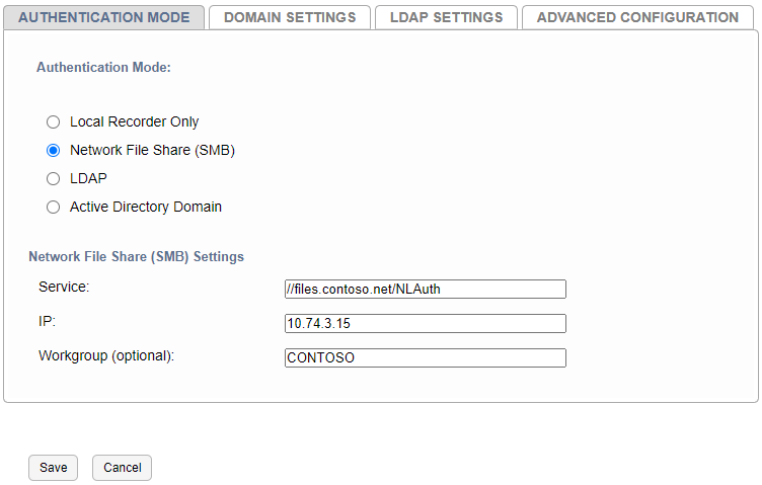


Fig. 4.1 **SMB Authentication Configuration**

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 transmited 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 accidential 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 Dealer for assistance.

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

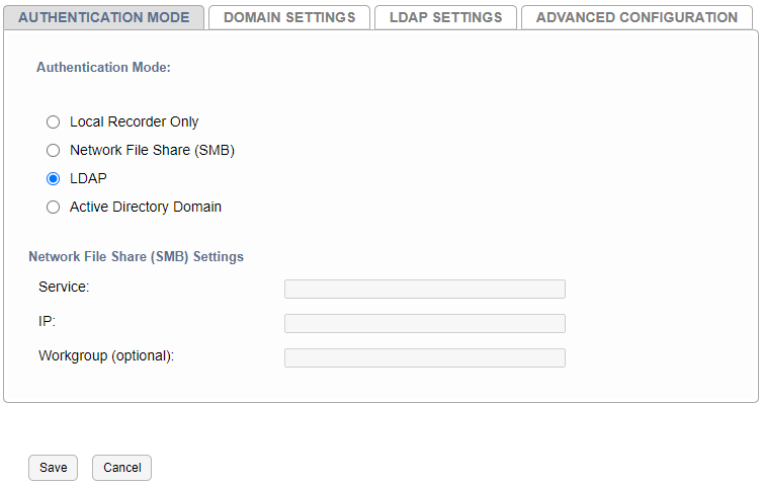


Fig. 5.1 **Authentication Mode - LDAP**

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 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.

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.

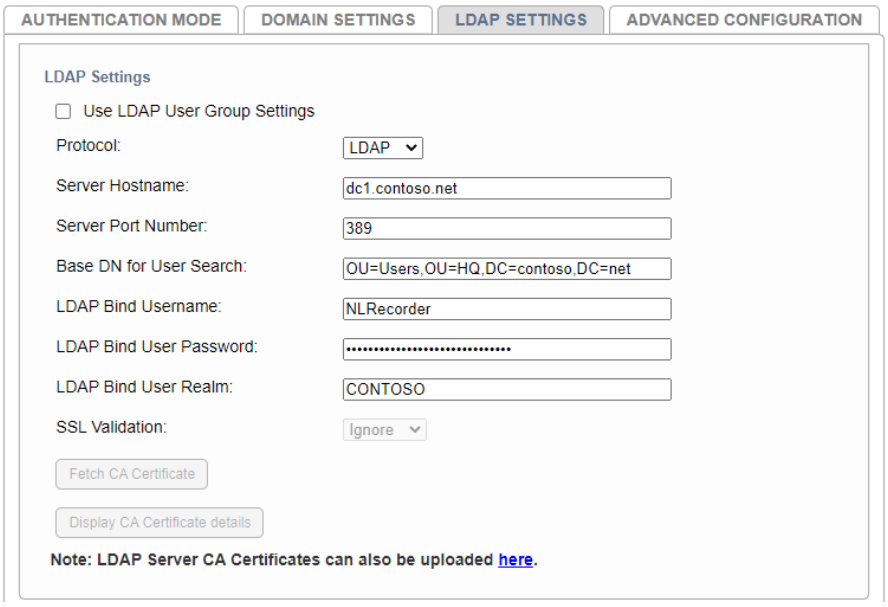


Fig. 5.2 **LDAP Settings Example**

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

Use LDAP User Group Settings

Optional, refer to Section 7.2.1 - 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 intered 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.

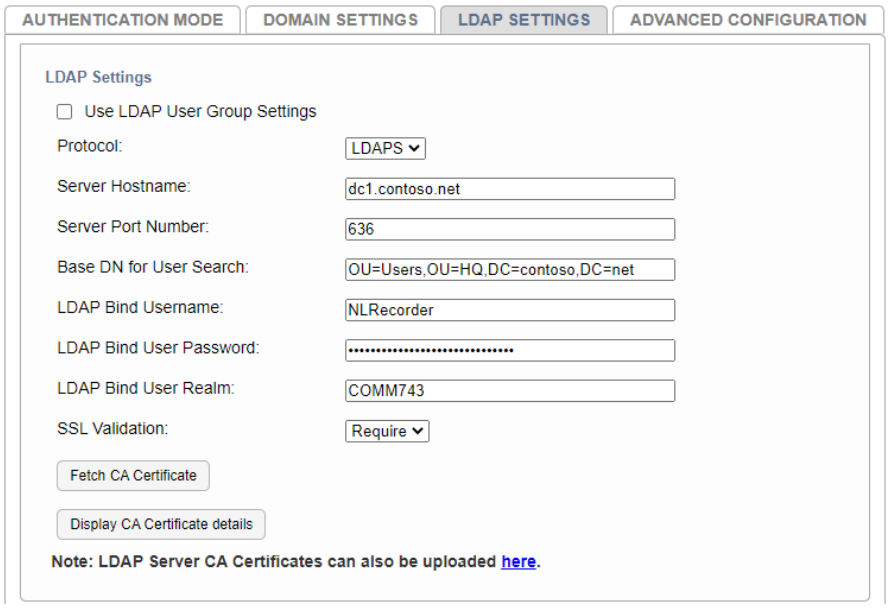


Fig. 5.3 **LDAPS Settings Example**

Use LDAP User Group Settings

Optional, refer to Section 7.2.1 - 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 intered 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.

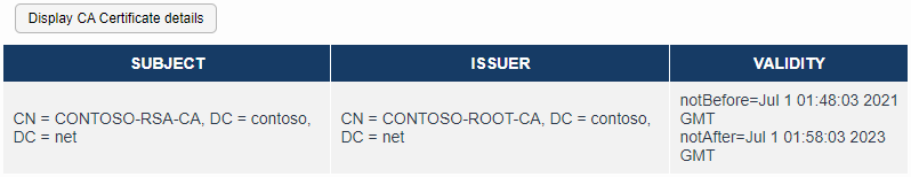


Fig. 5.4 **LDAPS Server CA Certificate Trust**

6. ACTIVE DIRECTORY AUTHENTICATION

License Required

This feature must be licensed to be used. Contact your Eventide 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.

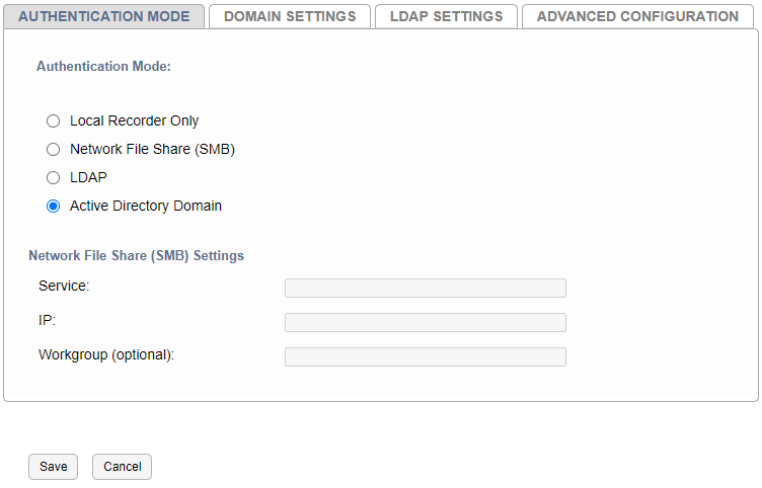


Fig. 6.1 **Authentication Mode - Active Directory**

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.

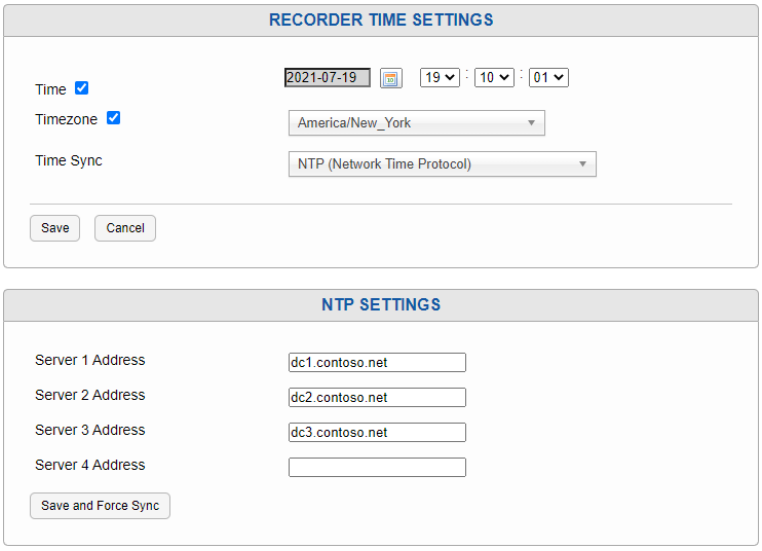


Fig. 6.2 **Date and Time - NTP Settings**

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.

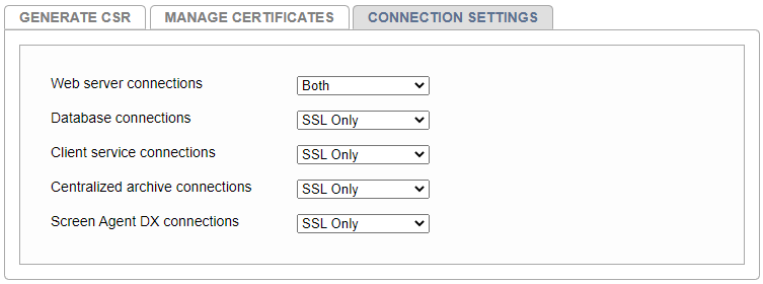


Fig. 6.3 **TLS/SSL Connection Settings**

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).`

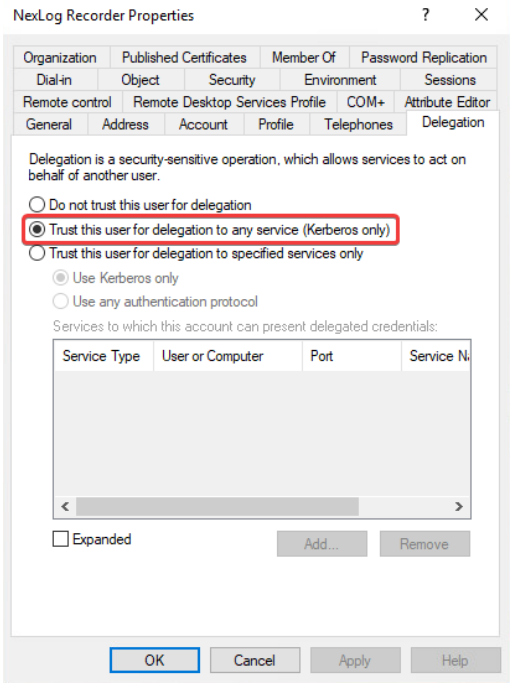


Fig. 6.4 **AD Users and Computer - Delegation**

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.

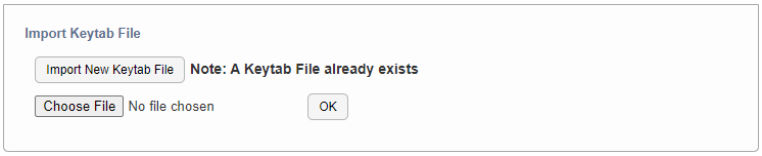


Fig. 6.5 **Domain Settings - Import Keytab File**

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.

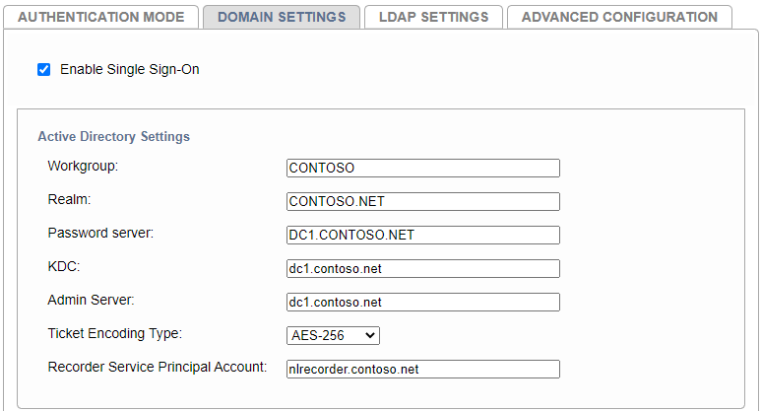


Fig. 6.6 **Domain Settings - Active Directory Settings**

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 kerberose 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 kerberose encrption 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 Plus 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 7: 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.

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.

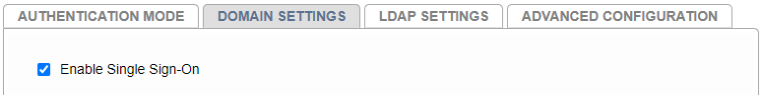


Fig. 6.8 **Domain Settings - Single Sign-On**

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.

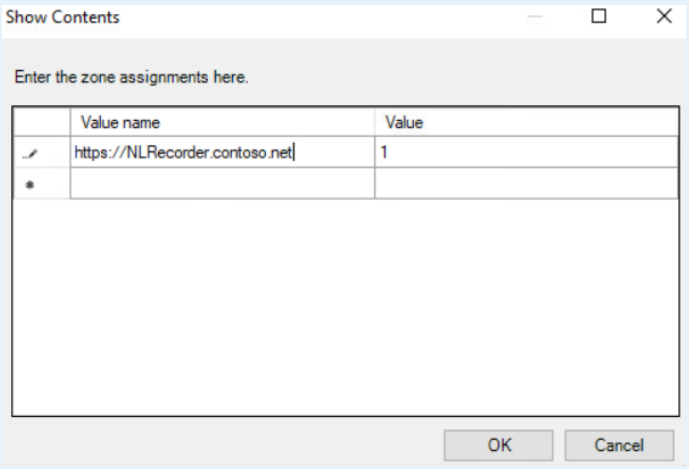


Fig. 6.9 **Site to Zone Assignment List Example**

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 Hive	HKEY_LOCAL_MACHINE or 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	`NLRecorder.contoso.net`

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`

This page was intentionally left 99.88% blank.

7. 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.

7.1. 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.

7.2. 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.

7.2.1. 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 7.1 **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 intered using LDAP syntax.

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

7.2.2. 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 assiegned to certain groups, as a test.

7.3. 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.

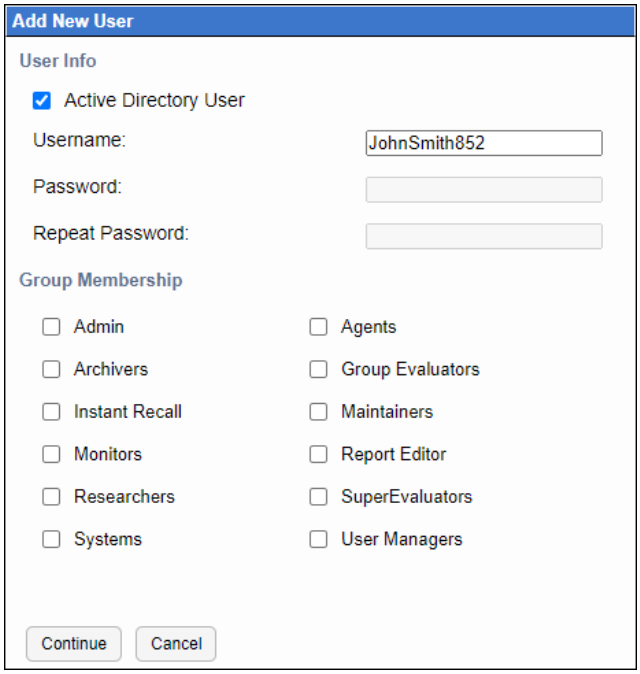


Fig. 7.1 **Add New Active Directory User**

7.4. 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.

8. 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.

8.1. NAB with Active Directory

If the NAB Base and all NAB Sources are configured with Active Directory authenticaton 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.

8.1.1. 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 8.3: NAB Base Database Exemption for how to create the exemption.

8.2. 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 8.3: NAB Base Database Exemption for how to create the exemption.

8.3. 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.

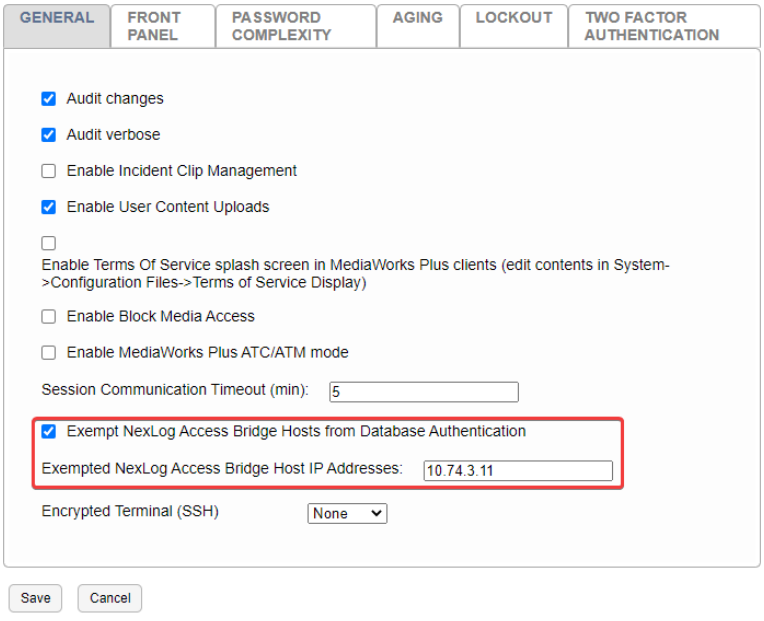


Fig. 8.1 **NAB Base Database Exemption**

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.

This page was intentionally left 99.88% blank.

9. NEXLOG DX-FIPS ADFS CONFIGURATION

New in version 2024.1.

There are two important concepts to understand in configuring SAML with the NexLog 740 DX-Series Recorder. The terms are not specific to NexLog 740 DX-Series Recorder, but are widely known in the SAML paradigm. The two terms are:

Service Provider(SP) - For the purposes of configuration the Service Provider(SP) is the NexLog 740 DX-Series Recorder itself.

Identity Provider(IdP) - The Identity Provider we will configure is a Microsoft ADFS server.

Another important concept to understand is that both the SP, and the IdP, have an entityID. An entityID is nothing more than an identifier. While we programmatically pull the entityID of the IdP from its MetaData file, you will need to provide an entity ID for the SP.

It's important to note that 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.

9.1. ADFS Configuration

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

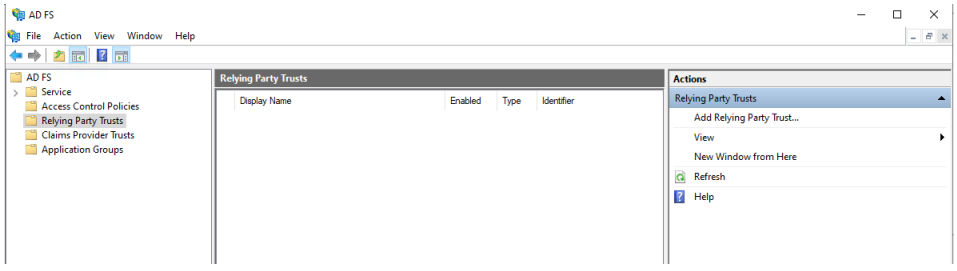


Fig. 9.1 **Relying Party Trusts**

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**

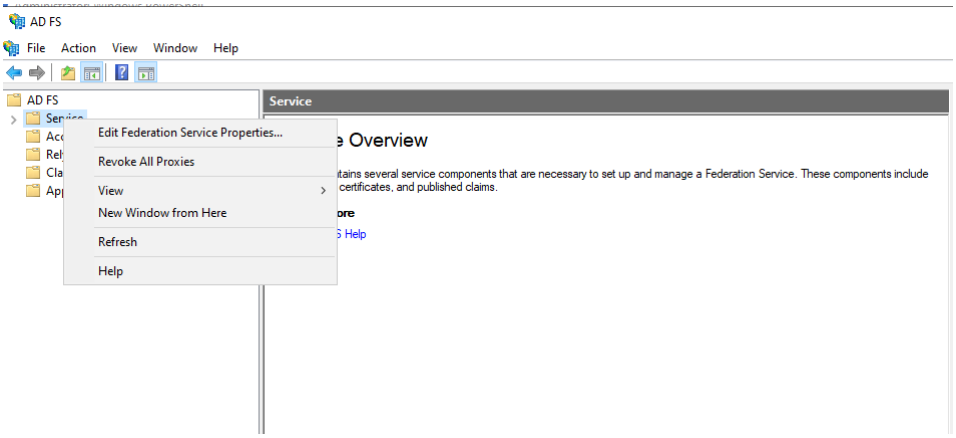


Fig. 9.2 **Edit Federation Service Properties**

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

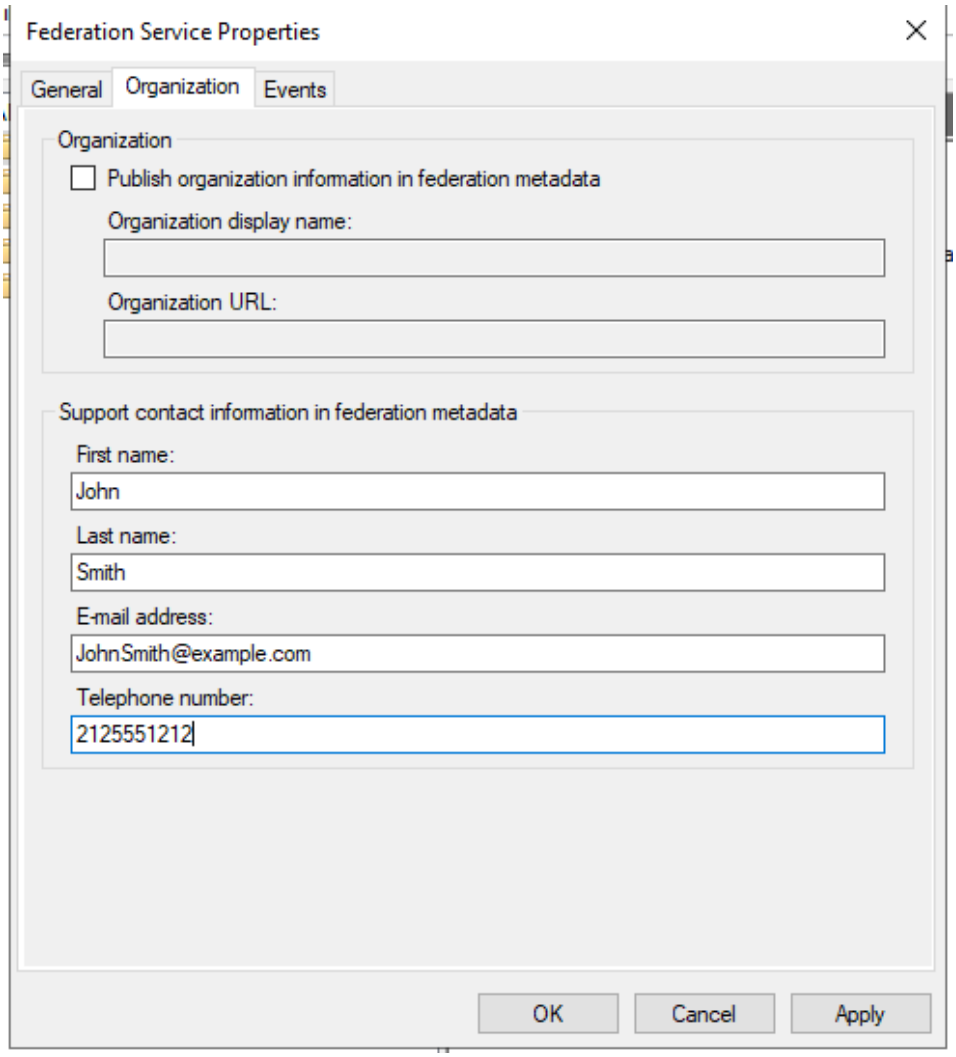


Fig. 9.3 **Organization Tab**

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.**

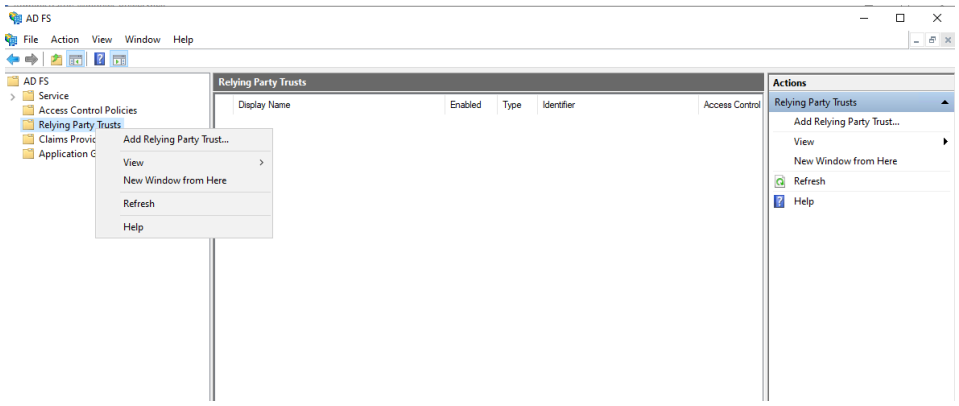


Fig. 9.4 **Add Relying Party Trust**

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

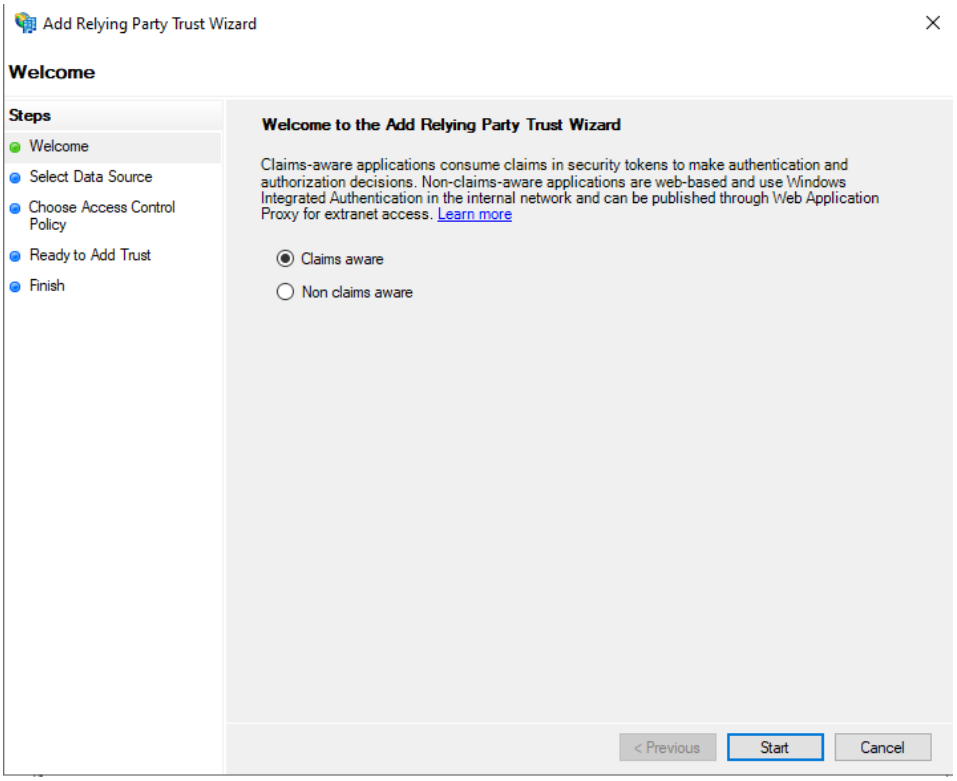


Fig. 9.5 **Add Relying Party Trust Wizard**

Click **Next** to continue.

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

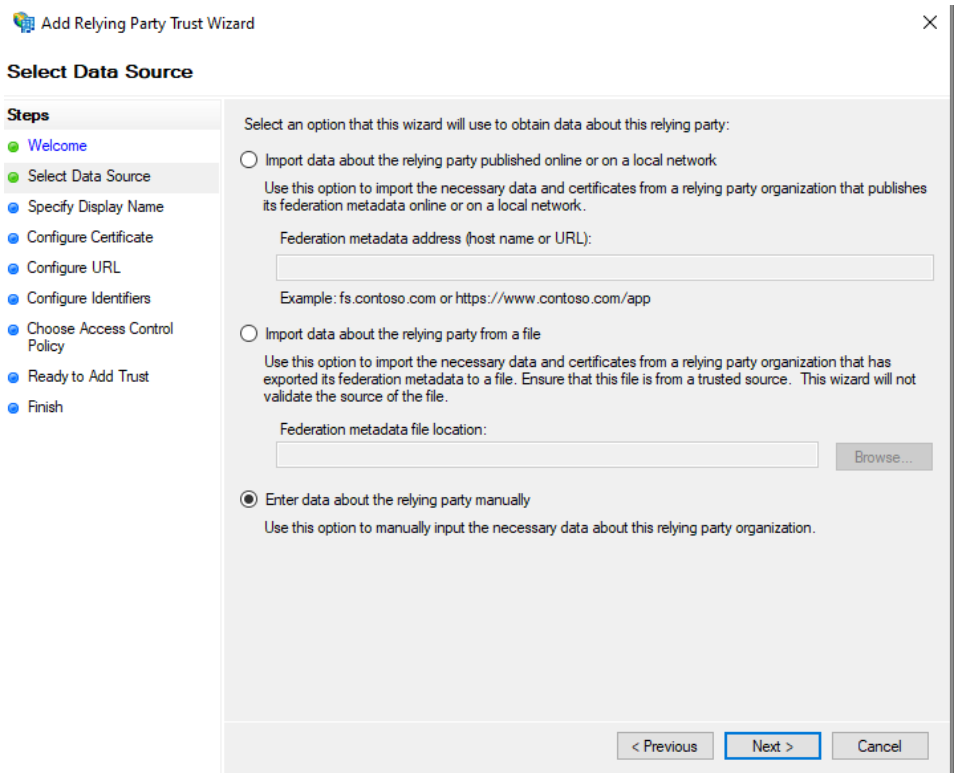


Fig. 9.6 **Enter Data Relying Party Manually**

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.

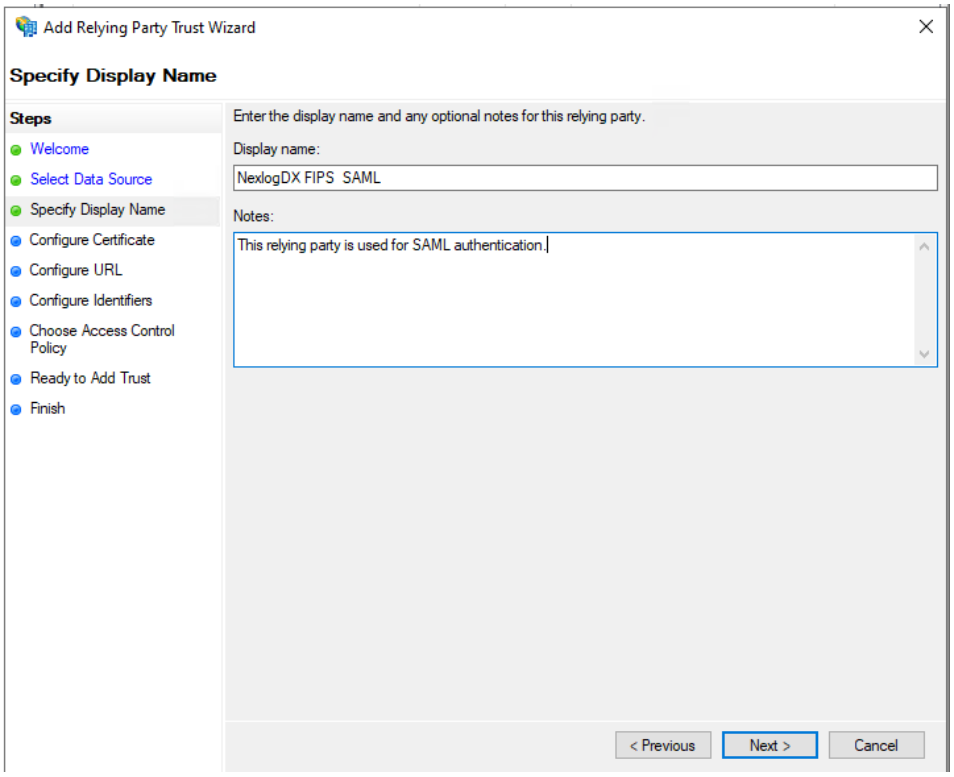


Fig. 9.7 **Give Relying Party Name**

Click **Next** to continue.

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

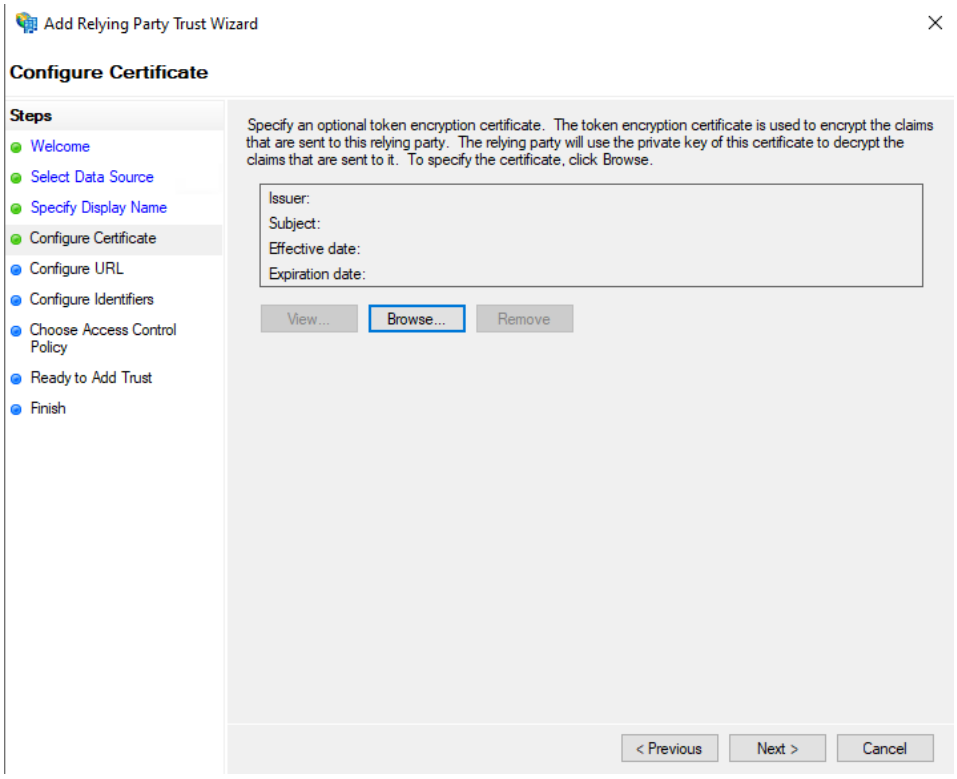
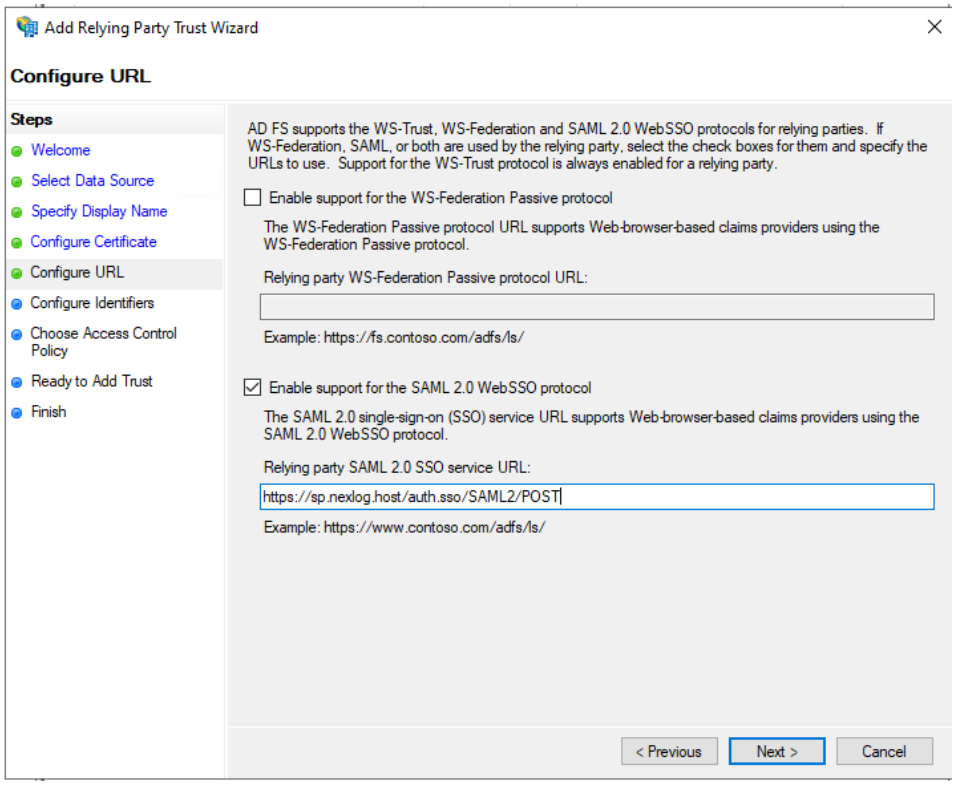


Fig. 9.8 **Configure Certificate**

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.



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.

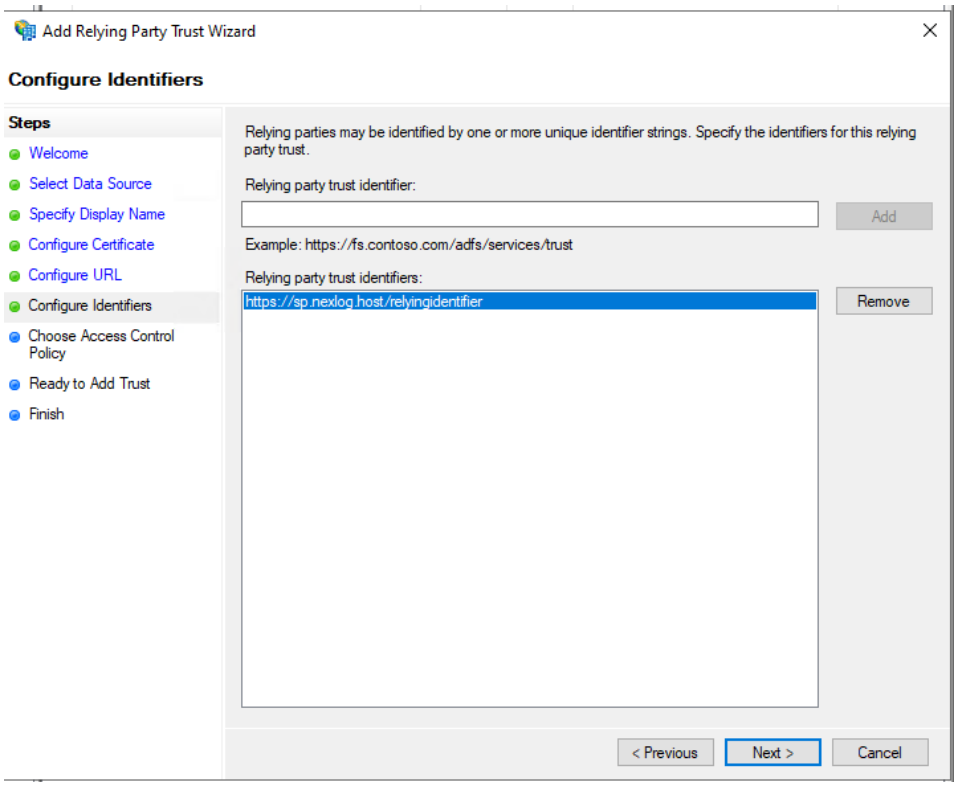


Fig. 9.9 **Configure Identifiers**

Click the **Next** button to continue.

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

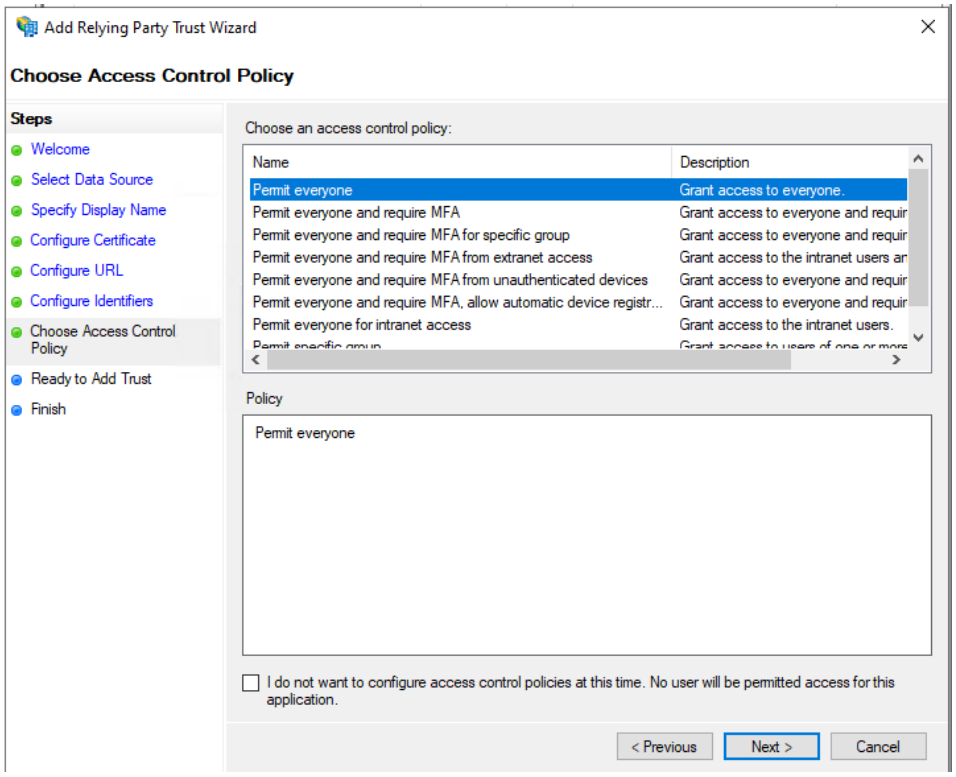


Fig. 9.10 **Choose Access Control Policy**

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

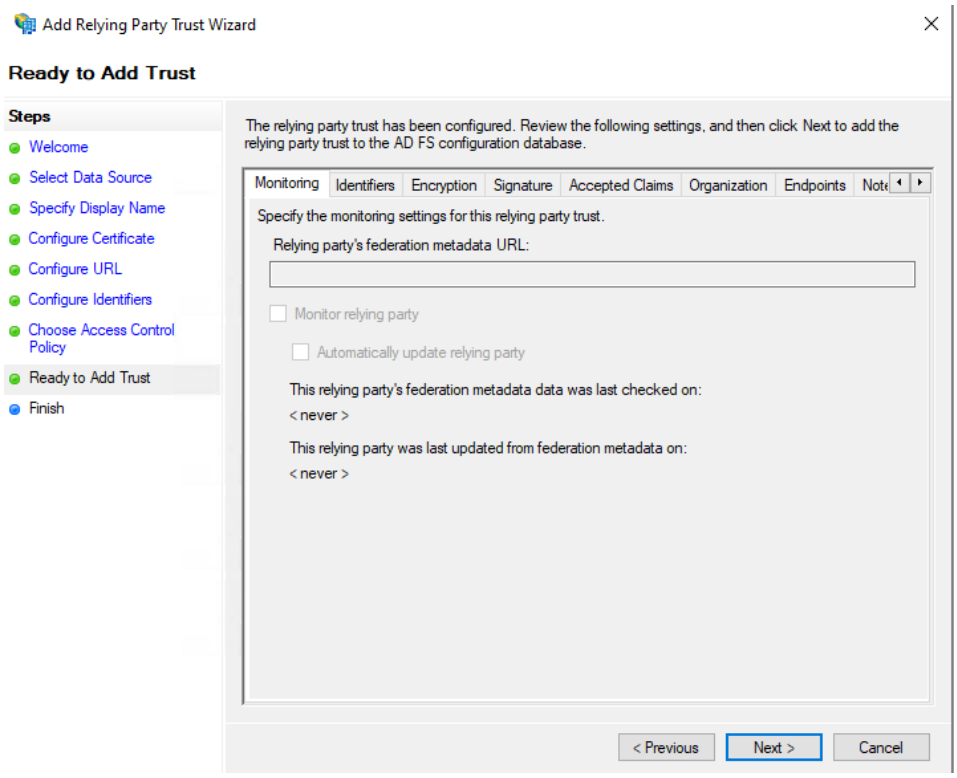


Fig. 9.11 **Ready to Add Trust**

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

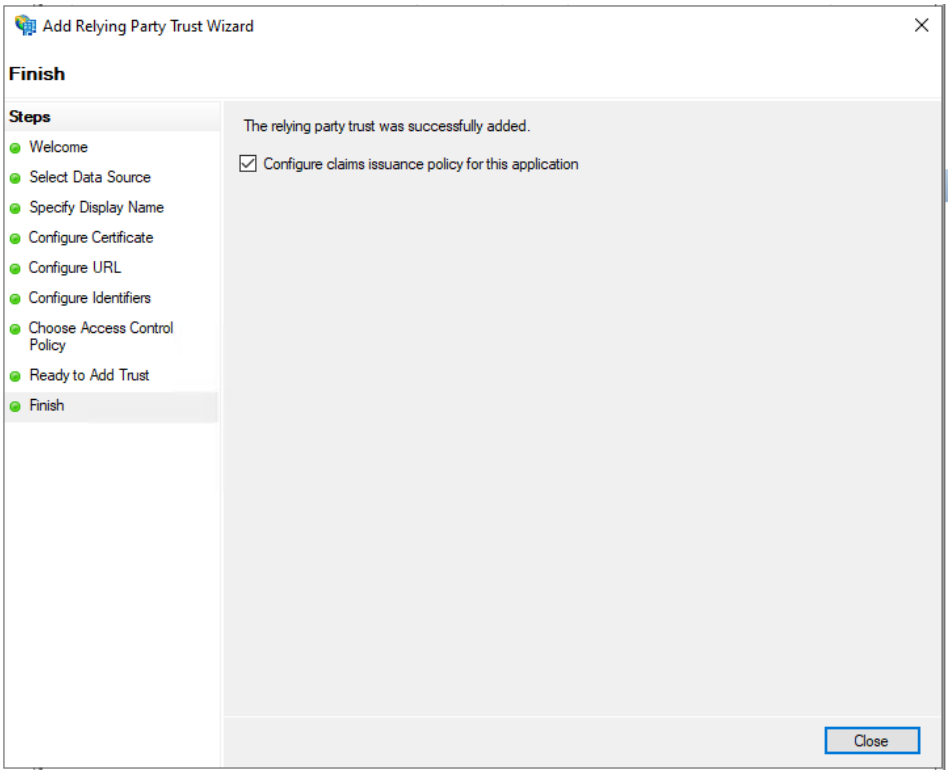


Fig. 9.12 **Finish Configure Claims**

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.

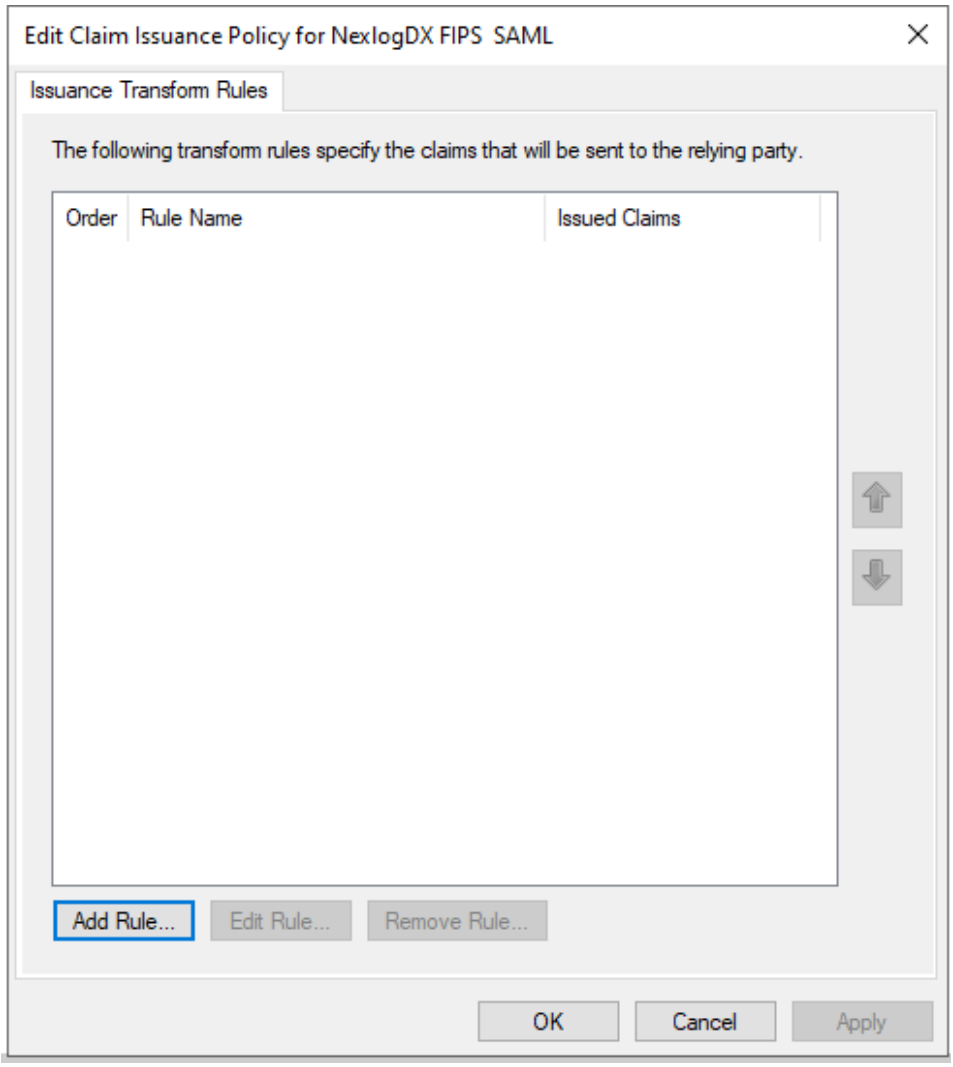


Fig. 9.13 **Edit Claim Issuance Policy**

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

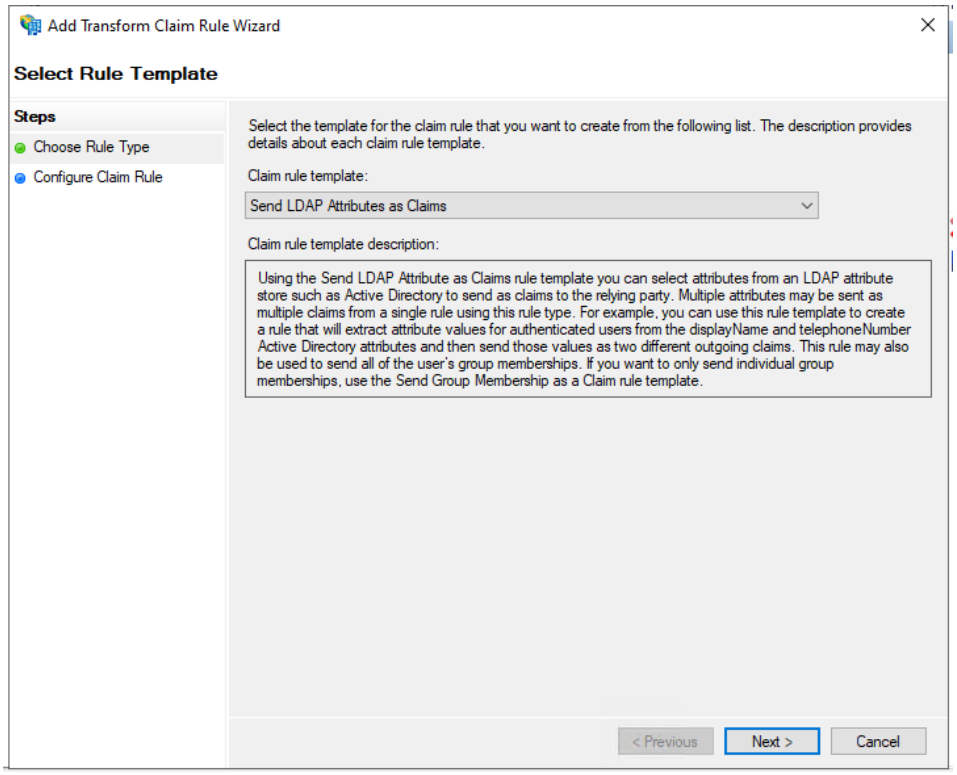


Fig. 9.14 **Add Transform Claim Rule Wizard**

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.

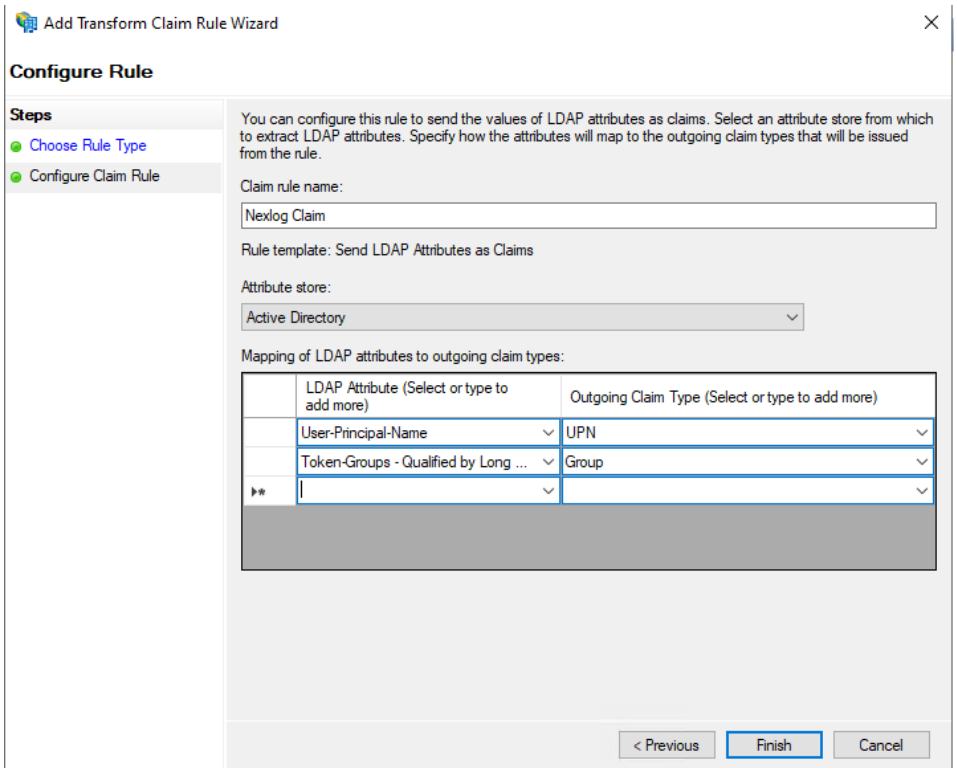


Fig. 9.15 **Configure Claim Rule**

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.

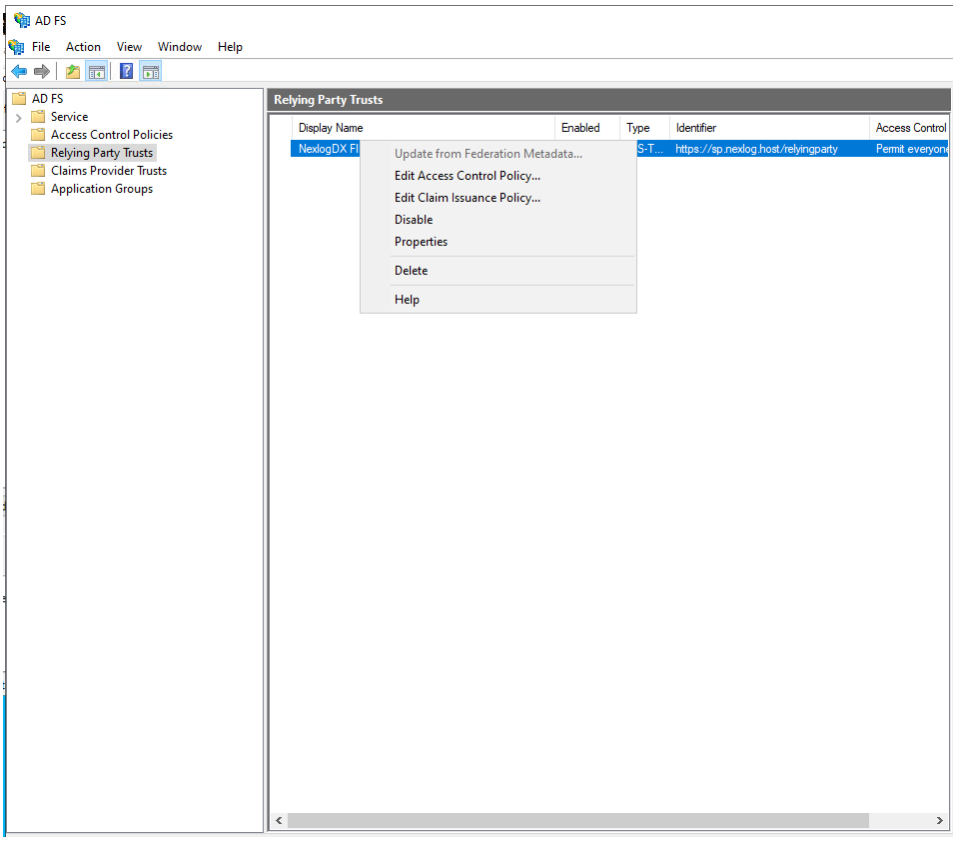


Fig. 9.16 **Relying Party Properties**

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

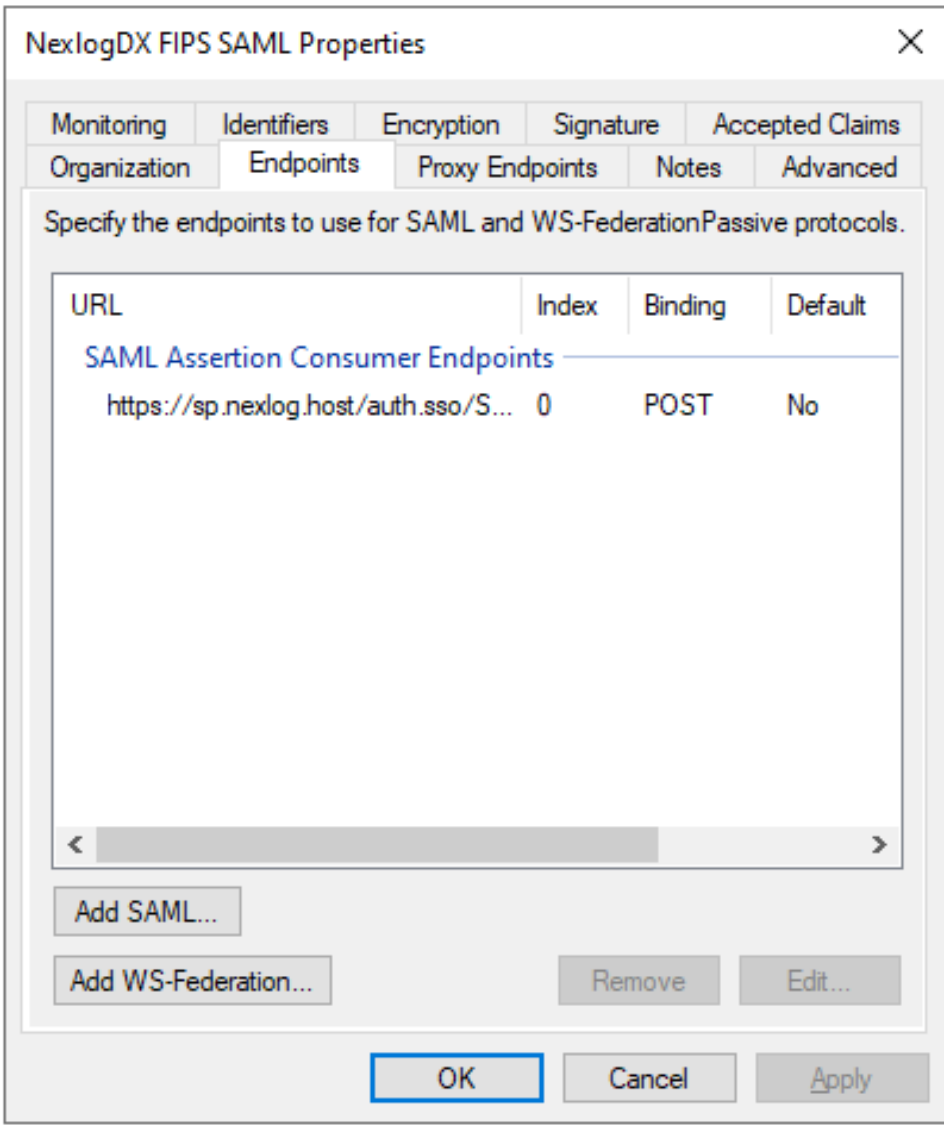


Fig. 9.17 **Endpoints Add SAML**

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.

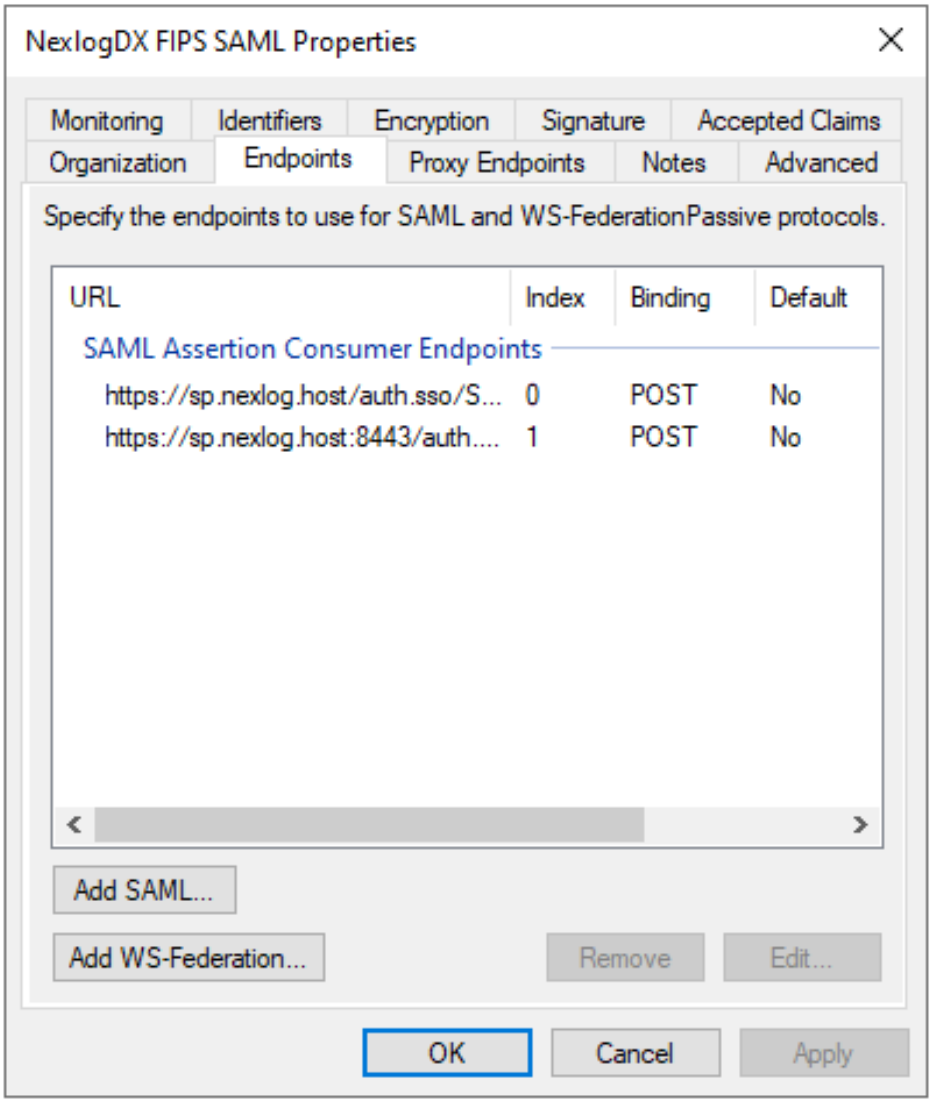


Fig. 9.18 **Add Relying Party Trust 8443**

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

9.2. Recorder SAML Configuration

Once the ADFS server 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

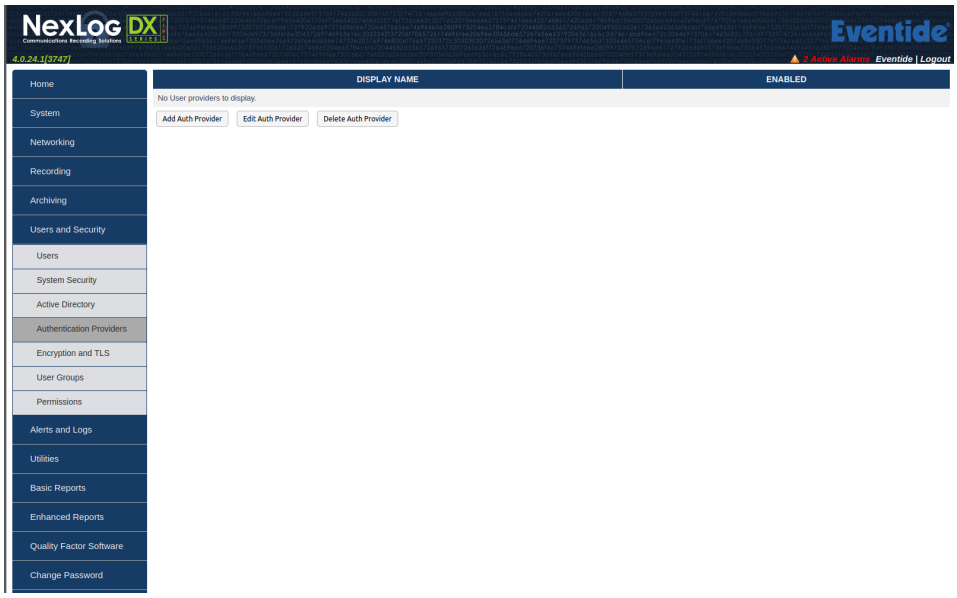


Fig. 9.19 **Auth Providers**

Then click the **Add Auth Provider** button to add ADFS as an Identity Provider.

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.

- **Display Order:** Select a value, this allows you to set the list order of authentication providers configured.
- **Relying Provider Identifier:** Recall from the ADFS configuration, that the service provider is identified by an entityID. This field must match what was configured in ADFS. We'll use the same value outlined in the ADFS configuration document: 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 on the ADFS server.
- **Identity Provider Metadata Configuration**: To populate this box, you first want to download the Metadata file from the ADFS server. ADFS uses a well-known URL to do so. You can point a browser at:
  - https://<FQDN of ADFS Server>/FederationMetadata/2007-06/FederationMetadata.xml

This will trigger a download of the Metadata file, save to your desktop, then click the **Browse** button to choose and upload the file.

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

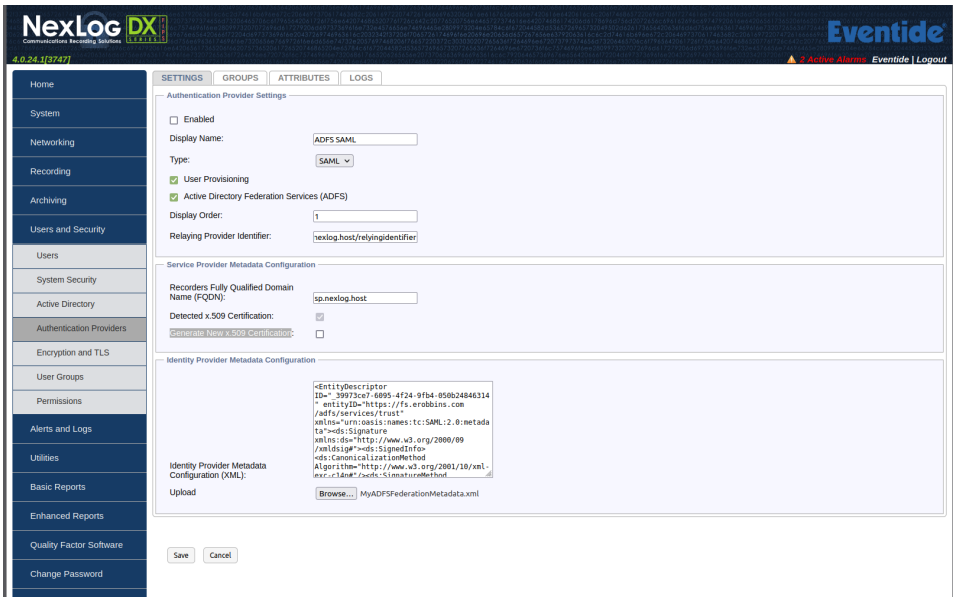


Fig. 9.20 **Auth Provider Setting Full**

9.2.1. SAML Group Mapping

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 Active Directory User Groups

Next, make sure that your Active Directory Users and Computers have user groups configured with the correct permissions, aligning with those defined in the Configuration Manager.

Setting Up Authentication Provider in Configuration Manager

Under ‘Users and Security’, locate the ‘Authentication Providers’ section. Here, you will create a new Authentication Provider. Once created, navigate to the ‘Groups’ page within this section to begin setting up 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 ‘Directory Group Name’ from Active Directory.

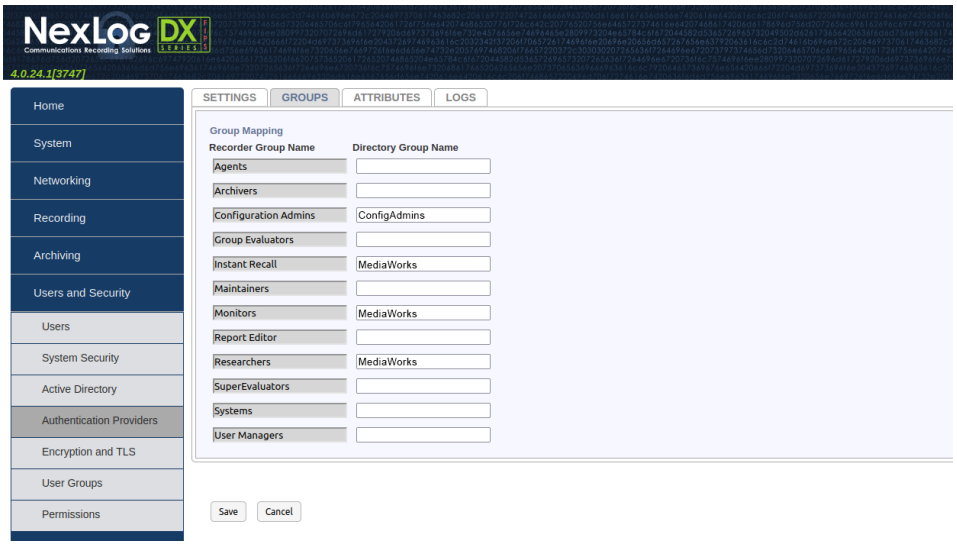


Fig. 9.21 **Groups Mapping**

Accurate Group Name Entry

It's critical to enter the correct Active Directory Group name with exactness. For instance, a group named 'Instant Recall' in the recorder should be mapped to its counterpart in Active Directory, 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.

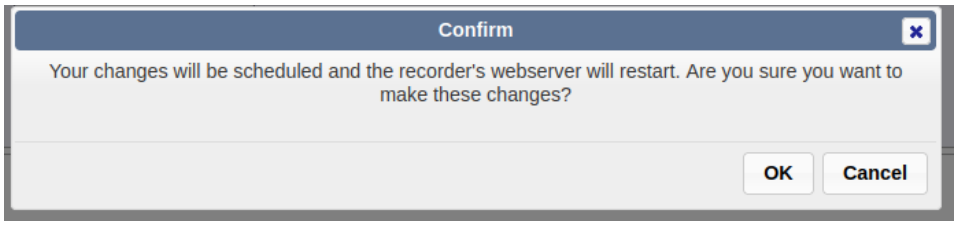


Fig. 9.22 **Webserver Restart**

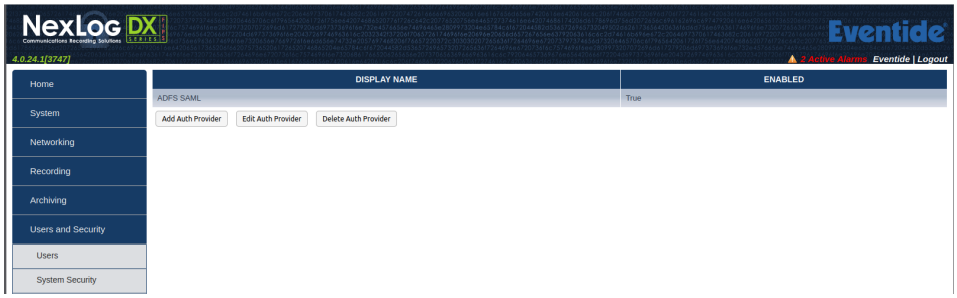


Fig. 9.23 **SAML Complete**

9.3. Verify MediaWorks Replay Configuration

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

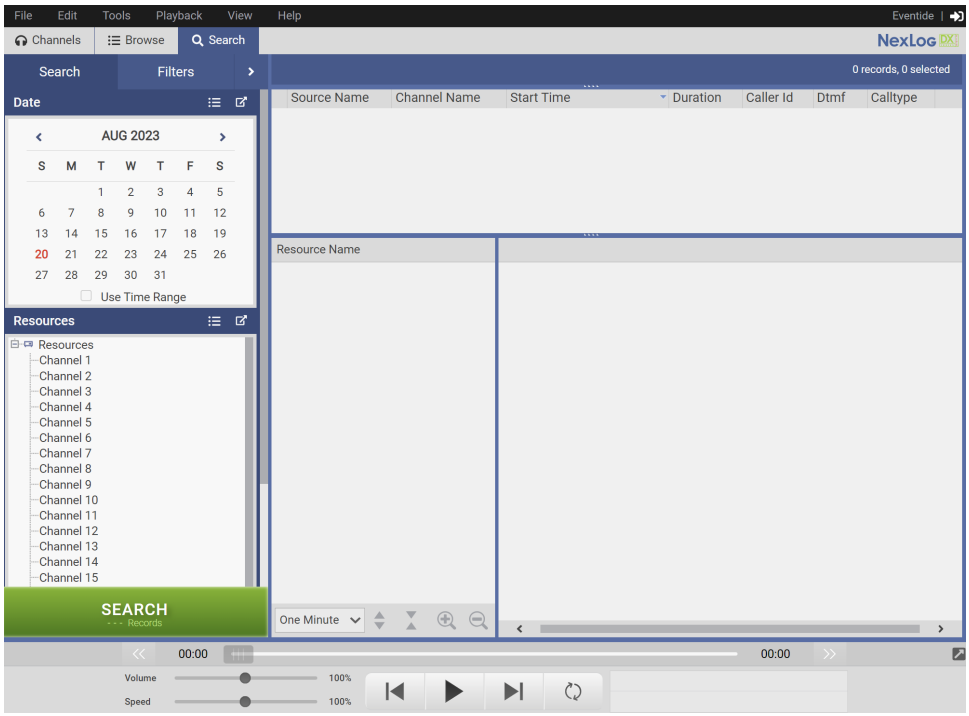


Fig. 9.24 **MediaWorks Login**

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.

This page was intentionally left 99.88% blank.

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
```

This page was intentionally left 99.88% blank.