

NexLog
Advanced Recording Solutions



NexLog DX MS Teams Recording
Implementation Guide
Version 2025.1[6258]

Copyright 2025 Eventide Communications LLC

P/N: #142441 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

2. Prerequisites

2.1. Networking	8
-----------------	---

3. Creating and Assigning Your Compliance Policy

3.1. Create the Application Instance	9
3.2. Create a Compliance Policy	10
3.3. Assign the Compliance Policy	11
3.4. Configure and Sync the Recording Application	12

4. Grant Permission to Record to the NexLog Teams Recording Service

4.1. Giving NexLog Teams Recording Service Permission to Query Phone Numbers	16
--	----

5. Connecting your Recorder to the NexLog Teams Recording Service

5.1. Create the Teams Recording Interface on your NexLog DX Recorder	19
5.2. Configuring the Teams Recording Interface	20
5.3. Verify that the recorder is communicating with the NexLog Teams Recording Service	21

6. Redundant MS Teams Call Recording

6.1. Creating and Pairing Compliant Recording Applications	23
6.2. Configuring Both Nexlog DX	24

7. Troubleshooting and Alerts

7.1. Failed to connect to NexLog Teams Recording Service (24)	25
7.2. Failed to detect any heartbeats from NexLog Teams Recording Service (74)	25
7.3. Failed to record teams call <ms teams call id/callguid(tbd)> properly (74)	25

A. Required Permissions

A.1. API Permissions	27
A.2. Role Permissions	27

1. INTRODUCTION

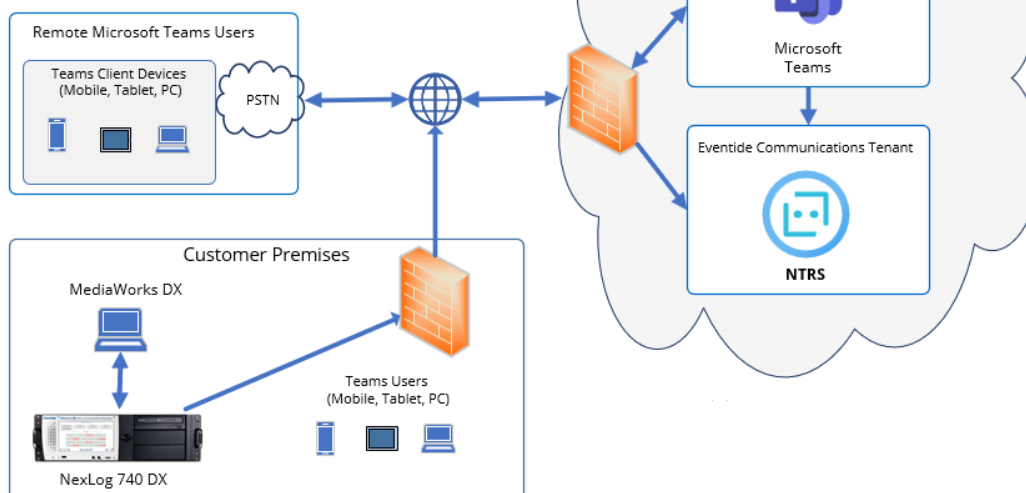
This guide will assist you in configuring both your Microsoft Teams application and a NexLog DX recorder to selectively transfer and record MS Teams call audio in the NexLog DX system for future search, playback, and compliance analysis from the MediaWorks DX user interface. The NexLog DX recorder can be either an appliance or virtualized model that you host or Eventide Communications™ SaaS cloud computing option.

NexLog DX MS Teams Recording Solution

Network Requirements:

The NexLog DX-Series recorder periodically opens HTTPS/443 connections to the Eventide Communications SaaS Azure tenant for the following NTRS component endpoints:

- <https://<Eventide Proxy ID>.blob.core.windows.net/recordings>
- <https://<Eventide Proxy ID>.blob.core.windows.net/logs>
- <https://<Eventide Proxy ID>.blob.core.windows.net/heartbeats>



© 2024 Eventide Communications LLC.

Fig. 1.1 Microsoft Teams Diagram

In either case, sending the recordings to a NexLog DX is simply a matter of configuring the Teams compliance policy to record selected groups or users and the Eventide Communications recorder to ingest the selected Teams recordings.

This document will describe the configuration.

This includes:

1. Creating and applying Teams compliance policies.
2. Configuring your Microsoft tenant to securely allow authentication from the Eventide Communications NexLog DX recorder.
3. Configuring your NexLog DX recorder to record the Microsoft Teams recordings.

2. PREREQUISITES

These will be the prerequisites you will need to follow the guide

The following information is provided by Eventide Communications in order to complete installation. Please contact Eventide Communications Support to get the information.

Application ID

Used to point your MS Teams system to the NexLog Teams Recording Service.

Application Name

The name of the NexLog Teams Recording Service

Eventide Proxy Id

Used on the recorder to identify the NexLog Teams Recording Service.

Eventide Proxy Key

Used on the recorder to securely authenticate to the NexLog Teams Recording Service.

This information is provided via a secure one time download link. This link should be secured and destroyed after configuration.

If Eventide Communications is hosting the recorder, then the Proxy credentials are not needed.

Before being able to configure Microsoft Teams, you will have to import the Microsoft Teams cmdlet

To install the MicrosoftTeams cmdlet on powershell, please run the below commands:

```
Install-Module -Name PowerShellGet  
Install-Module -Name MicrosoftTeams
```

If you already have the MicrosoftTeams cmdlet, please make sure that you are running the latest version. If not, update to the latest:

`Get-Module MicrosoftTeams`

If these commands are not running, please check your execution policy on powershell.

In order to configure your Eventide Communications NexLog DX recorder, you will need a recorder user with admin privileges.

2.1. Networking

The recorder will need to connect to three endpoints using HTTPS 443. In the event your firewall is very secure, please open up these endpoints.

- <https://<Eventide Proxy ID>.blob.core.windows.net/recordings>
- <https://<Eventide Proxy ID>.blob.core.windows.net/logs>
- <https://<Eventide Proxy ID>.blob.core.windows.net/heartbeats>

3. CREATING AND ASSIGNING YOUR COMPLIANCE POLICY

The first section of this document will guide you through configuring your MS Teams environment to send recordings to the NexLog Teams Recording Service. The MS Teams administrator will use the PowerShell program built into any Windows computer to execute commands to tell your Teams environment to record. The commands will require specific information for your recording service to be entered. It is suggested that the commands with your specific information be constructed in a text file before being copy/pasted into PowerShell. If you are unsure about the commands to run, then please provide a text file with your commands to Eventide Communications Support.

3.1. Create the Application Instance

The NexLog Teams Recording Service requires the creation of an Application Instance in order for it to join and record calls.

The following information is variable to your deployment and is either provided by Eventide Communications or decided by your organization:

User Principal Name

A new service account that is used to identify the compliance policy. It will be formatted like `example_name@contoso.com`.

Example: `eventide_teams_recording_service@contoso.com`

Display Name

The displayed name for the Application Instance. We recommend “NexLog Teams Recording Service”.

Application ID

Eventide Communications will provide the Application ID of the NexLog Teams Recording Service

Open PowerShell as Administrator on any Windows computer connected to the internet, and run the following commands. When prompted for authentication, login with your Microsoft Domain admin credentials.

```
Import-Module MicrosoftTeams  
Connect-MicrosoftTeams
```

```
New-CsOnlineApplicationInstance -UserPrincipalName <User Principal Name> -  
DisplayName '<Display Name>' -ApplicationId <Application ID>
```

The command will display an output with the Application Instance. Take note of the ApplicationId and the ObjectId. If the command failed, please stop, and take action to correct the error. Contact Eventide Communications Support for more details.

3.2. Create a Compliance Policy

Compliance policies allow the NexLog Teams Recording Service to automatically join and record Teams calls with users that have the compliance policy.

The following information will be required to create the Compliance Policy:

Policy Description

User-readable description of the recording policy. This could be something like, “Record security phone lines”.

Policy Identity

The visible name of the policy being created. This name should not contain spaces. (Example, ‘recording-security-phones’)

Object Id

This is the Object Id returned in the previous step, where the Application Instance was created.

Continue your PowerShell session and run the following commands:

```
New-CsTeamsComplianceRecordingPolicy -Enabled $true -Description "<Policy  
Description>" <Policy Identity>  
Set-CsTeamsComplianceRecordingPolicy -Identity <Policy Identity> -  
ComplianceRecordingApplications `@(New-  
CsTeamsComplianceRecordingApplication -Parent <Policy Identity> -Id <Object  
Id>)  
Set-CsTeamsComplianceRecordingPolicy -Identity <Policy Identity> -  
DisableComplianceRecordingAudioNotificationForCalls $true
```

After 30-60 seconds, the policy should show up.

To verify your policy was created correctly:

```
Get-CsTeamsComplianceRecordingPolicy <Policy Identity>
```

For additional configuration, please visit the Microsoft Documentation on Set-CsTeamsComplianceRecordingPolicy.

[Set-CsTeamsComplianceRecordingPolicy Documentation](#)

3.3. Assign the Compliance Policy

In this step, users and/or groups will be added to the policy created above.

You should identify the users and groups required for recording under the Microsoft 365 Admin center → Users → Active Users page.

Here you can also create a user group to be recorded and then assign the group to the policy.

See [Microsoft's knowledgebase](#) for more information about creating policies in Azure for users and groups.

The following information will be required to assign the Compliance Policy

Policy Identity

The name of the policy as defined in the previous step.

User to be recorded

A user to be recorded.

Group to be recorded

A group to be recorded.

Run the following command in PowerShell for each user you wish to record:

```
Grant-CsTeamsComplianceRecordingPolicy -Identity <User to be recorded> -  
PolicyName <Policy Identity>
```

Run the following command in PowerShell for each group you wish to record:

```
Grant-CsTeamsComplianceRecordingPolicy -Group <Group to be recorded> -  
PolicyName <Policy Identity>
```

To verify your policy was assigned correctly:

```
Get-CsOnlineUser <user or group under policy> | ft sipaddress, tenantid,  
TeamsComplianceRecordingPolicy
```

3.4. Configure and Sync the Recording Application

To configure the recording application, we need to gather variable information by running a command.

In PowerShell, please run:

```
Get-CsTeamsComplianceRecordingApplication
```

Take note of Identity as it is needed in the next command.

Identity

Taken from the result of the previous command.

The format will be: `Tag:recording_policy_name/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx`

In PowerShell, please run:

```
Set-CsTeamsComplianceRecordingApplication -RequiredBeforeMeetingJoin $false  
-RequiredDuringMeeting $false -RequiredBeforeCallEstablishment $false -  
RequiredDuringCall $false -Identity <Identity>
```

To verify the above command, please run:

```
Get-CsTeamsComplianceRecordingApplication
```

Note

Please note that the parameters in the previous command are now false.

Now that the recording application is configured, we can sync the application registration from the Eventide Tenant to the created Application Instance

```
Sync-CsOnlineApplicationInstance -ObjectId <Object Id> -ApplicationId  
<Application Id>
```


4. GRANT PERMISSION TO RECORD TO THE NEXLOG TEAMS RECORDING SERVICE

The NexLog Teams Recording Service requires permission from your tenant in order to record and join calls.

The following information is required for the next step:

Tenant ID

Your organization's Microsoft Tenant ID.

Application ID

Application ID provided by Eventide Communications to identify your organization.

Replace the variable information in the link below with your information and paste it into a web browser:

https://login.microsoftonline.com/<Tenant ID>/adminconsent?client_id=<Application ID>

Sign in with an administrator account and select Accept to add NexLog Teams Recording Service to your tenant.

It is expected for the webpage to display a warning that you cannot sign up. This is not an issue.

In order to authenticate and give consent to the NexLog Teams Recording Service, sign into the Microsoft Entra Admin Center (<https://entra.microsoft.com/>) and follow these steps:

1. Browse to Identity > Applications > Enterprise applications > All applications
2. Select the NexLog Teams Recording Service. The name of the service will be provided. Note that in the example image "Contoso" is used for the granting of permission.
3. Select Permissions under Security. Note that the application name will be what you provided above.

4. The application permissions will automatically be set to the required permissions for recording. Select “Grant admin consent”.

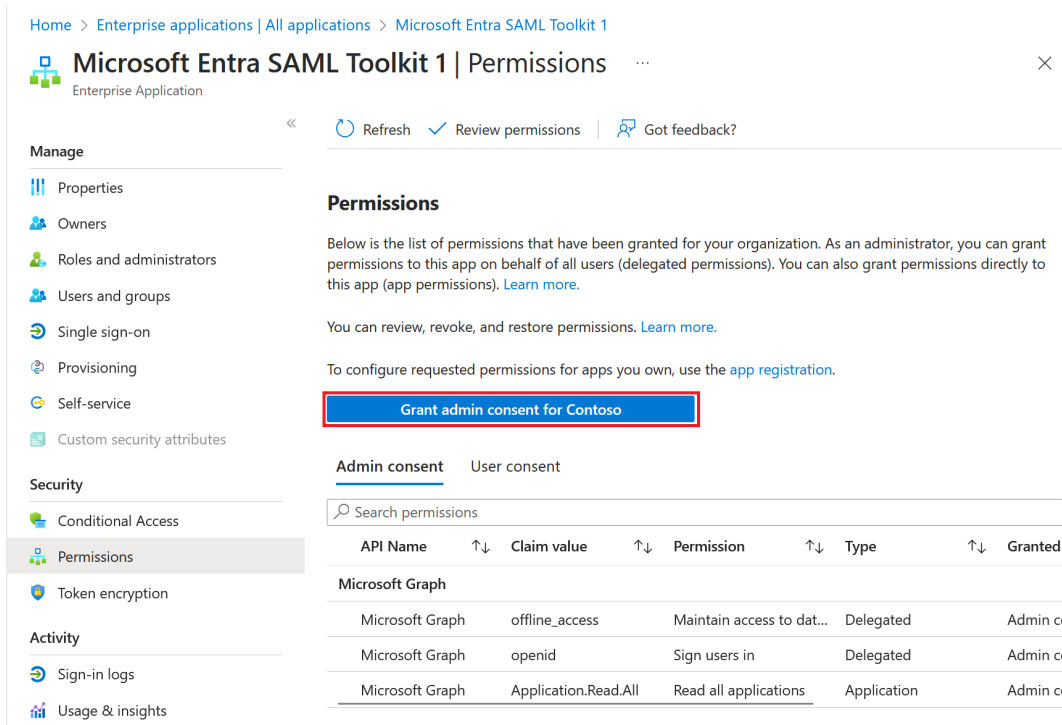


Fig. 4.1 Grant Admin Consent

4.1. Giving NexLog Teams Recording Service Permission to Query Phone Numbers

Please have you Microsoft administrator sign into <https://entra.microsoft.com/> and follow these steps:

1. Browse to Identity > Applications > Enterprise applications > All applications
2. Select the NexLog Teams Recording Service
3. Select **Roles and Administrators** under **Manage**
4. Click on the “here” in the Administrative roles description

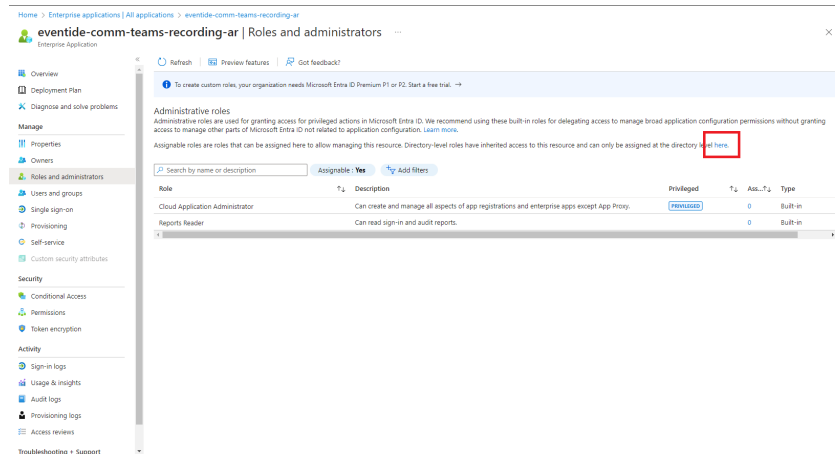


Fig. 4.2 Accessing Directory Level Roles

5. Type in "Teams" in the search bar
6. Right-click on "Global Reader" and select "Description"
7. Click on "Add assignment"
8. Type in the Application ID, that Eventide Communications provides, into the search bar of the new window
9. Select the NexLog Teams Recording Service Enterprise Application and click "Add"

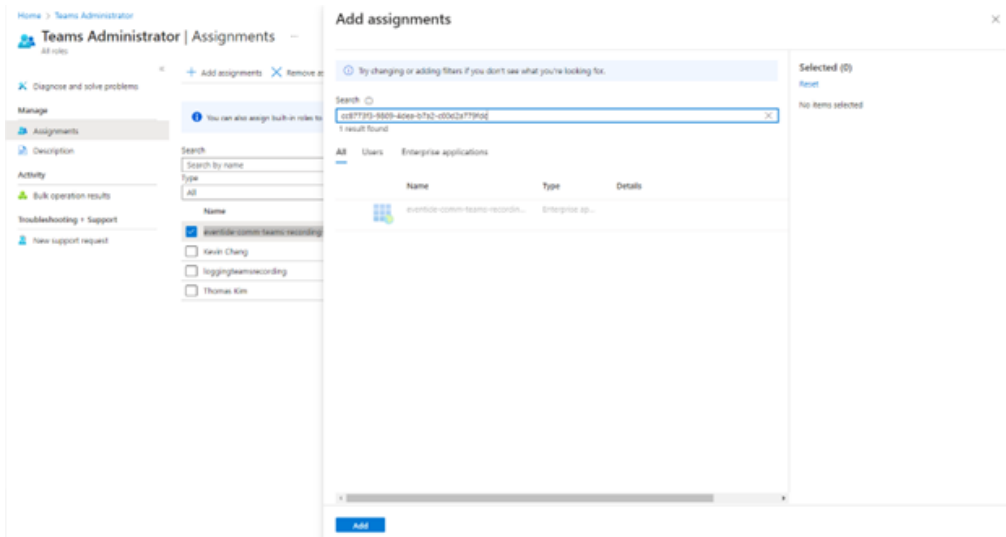


Fig. 4.3 Assigning the Application a Role

The NexLog Teams Recording Service will now be able to query for Teams phone numbers.

Note

Please reference Appendix A for a full list of required permissions for the NTRS

5. CONNECTING YOUR RECORDER TO THE NEXLOG TEAMS RECORDING SERVICE

In this section, we will cover how the recorder receives the calls from the MS Teams application. The recorder will securely communicate through the internet over port 443 to stream the encrypted calls back to the recorder in real time.

If your recorder is being hosted by Eventide Communications, then this section will be done for you.

5.1. Create the Teams Recording Interface on your NexLog DX Recorder

Log into your recorder's configuration interface by navigating to the <recorder's address>/admin.

Go to your recorder's Configuration page and access the Recording Interfaces page. Then click "Add Virtual Recording Interface".

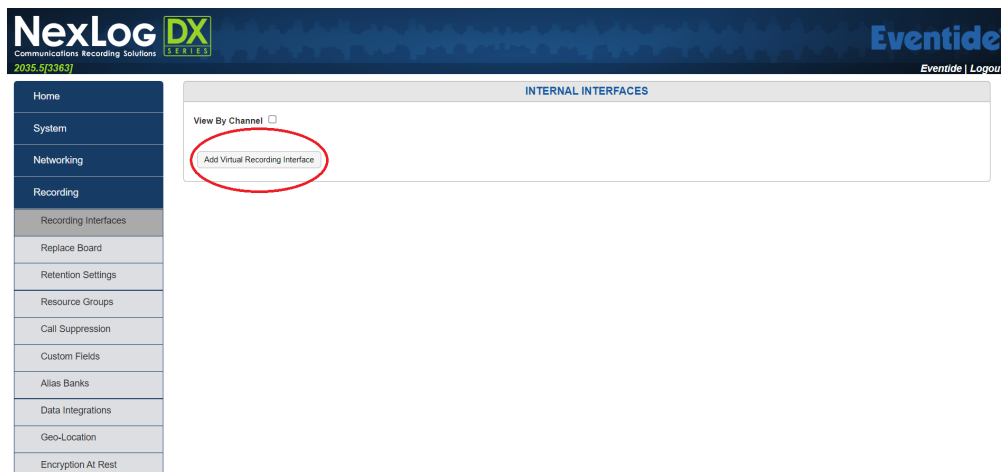
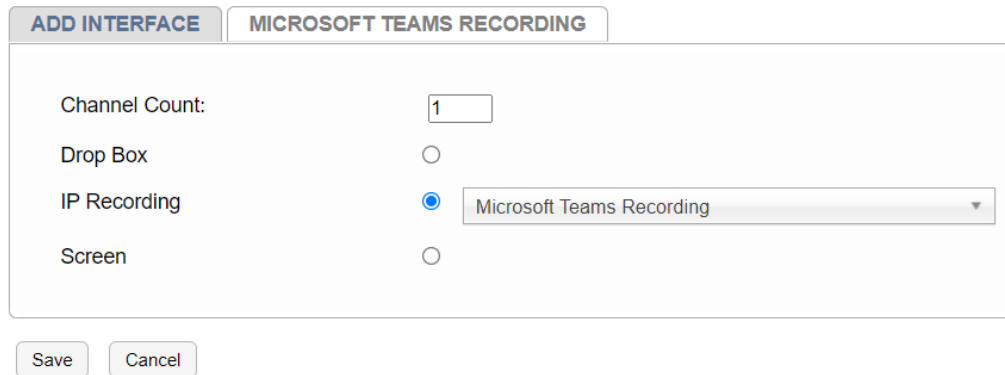


Fig. 5.1 Add Virtual Recording

A page to configure the new virtual recording interface will be displayed.

5.2. Configuring the Teams Recording Interface

- Change the Channel Count to the number of licensed users.
- Select “IP Recording”
- Select “Microsoft Teams Recording” from the dropdown menu.



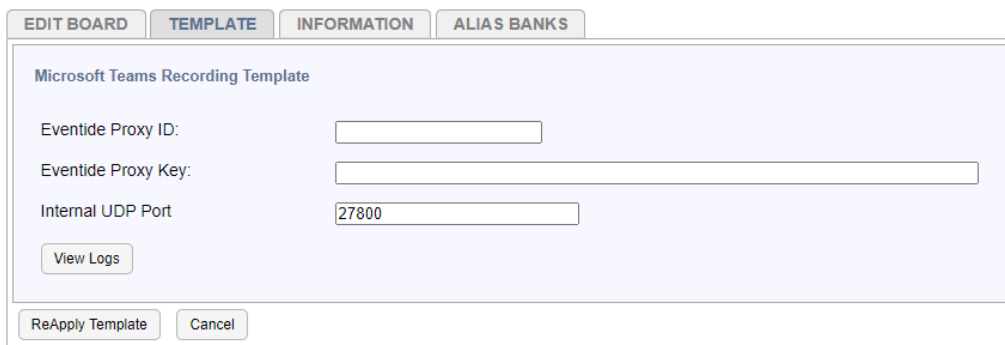
The screenshot shows a configuration window titled "MICROSOFT TEAMS RECORDING". It has two tabs: "ADD INTERFACE" and "MICROSOFT TEAMS RECORDING". The "MICROSOFT TEAMS RECORDING" tab is active. Inside the tab, there are four rows of configuration options:

- Channel Count: A text input field containing the number "1".
- Drop Box: A radio button that is not selected.
- IP Recording: A radio button that is selected, followed by a dropdown menu showing "Microsoft Teams Recording".
- Screen: A radio button that is not selected.

At the bottom of the window, there are two buttons: "Save" and "Cancel".

Fig. 5.2 Microsoft Teams Recording Template

You will automatically be navigated to enter the required information to communicate with the NexLog Teams Recording Service. Please fill out “Eventide Proxy ID” and “Eventide Proxy Key” with the information provided by Eventide Communications.



The screenshot shows a configuration window titled "Microsoft Teams Configuration". It has four tabs: "EDIT BOARD", "TEMPLATE", "INFORMATION", and "ALIAS BANKS". The "TEMPLATE" tab is active. Inside the tab, there are three rows of configuration options:

- Eventide Proxy ID: A text input field.
- Eventide Proxy Key: A text input field.
- Internal UDP Port: A text input field containing the value "27800".

Below the input fields, there is a button labeled "View Logs". At the bottom of the window, there are two buttons: "ReApply Template" and "Cancel".

Fig. 5.3 Microsoft Teams Configuration

5.3. Verify that the recorder is communicating with the NexLog Teams Recording Service

You will now be recording MS Teams calls. Make a call that involves a user with the required compliance policy. Navigate to MediaWorks and search for the call.

It should look similar to this:

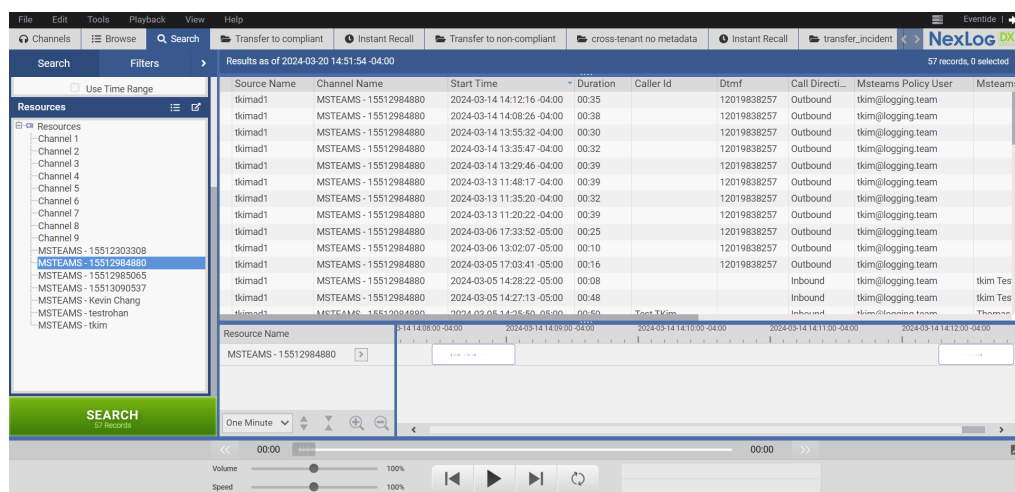


Fig. 5.4 MediaWorks DX Example

Congratulations! You should now be recording Microsoft Teams call audio.

Please contact your Eventide Communications reseller or Eventide Communications Support if you have any questions.

6. REDUNDANT MS TEAMS CALL RECORDING

Eventide Communications also provides a redundant solution for NexLog DX Ms Teams Recording. To ensure calls are always recorded even if a recorder were to become unavailable for any reason, it is recommended that a second recorder be installed in a separate location and configured to simultaneously record MS Teams calls. This primary and secondary solution implementation approach ensures access to recorded calls even if one of two recorders suffers a failure or if there is a network issue that prevents access to a single recorder. This approach also provides redundancy for the SaaS NTRS, which is a fundamental component of the NexLog DX MS Teams Recording solution.

On a rudimentary level, redundant MS Teams Call Recording requires having two NexLog DX and two NTRS. Compliant Recording Applications (the NTRS in this case) have the ability to be paired with another, enabling them to be under the same compliance policy.

Since multiple compliance policies cannot be put into effect at the same time, we achieve redundancy by pairing two NTRS. When assigning the paired NTRS to a compliance policy, the compliance policy will know to have both NTRS record the call.

Each NTRS will also store the recordings separately in addition to sending it to different NexLog DX, thereby creating true redundancy.

6.1. Creating and Pairing Compliant Recording Applications

In order to pair Compliance Recording Applications to each other, we must first have both Compliance Recording Applications created.

Once that is done please run the following command:

```
Get-CsTeamsComplianceRecordingApplication
```

Please take note of both the Identity and Object ID values of both applications. These will be needed for the next command.

Identity

Full identity of the application. This includes the `Tag:policy_name`. Format: `Tag:policy_name/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`

Object Id

Strictly the unique identifier of the application. Format: `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`

Please determine which compliance policy you would like to assign to your user. Whichever application that compliance policy is tied to will go into the Identity parameter.

The secondary application will be inserted into the Id parameter.

```
Set-CsTeamsComplianceRecordingApplication -Identity <Identity> -
ComplianceRecordingPairedApplications @(New-
CsTeamsComplianceRecordingPairedApplication -Id <Object Id>)
```

Example:

```
Set-CsTeamsComplianceRecordingApplication -Identity 'Tag:my-recording-app/
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx' -ComplianceRecordingPairedApplications
@(New-CsTeamsComplianceRecordingPairedApplication -Id 'xxxxxxxx-xxxx-xxxx-
xxxx-xxxxxxxxxxxx')
```

6.2. Configuring Both Nexlog DX

Now that both NTRS are recording, each recorder will need to connect to each NTRS' storage.

Eventide Communications will provide the credentials for both NTRS that you will input into each NexLog DX MS Teams Recording Template.

7. TROUBLESHOOTING AND ALERTS

- When running the powershell commands, please get rid of any line breaks. PowerShell will interpret the line breaks as separate commands.
- When running the powershell commands, if a command is not recognized, please update your PowerShell modules.
- During your Compliance Policy setup, please double check that the Application ID is correct.
- When you are running the Set-CsTeamsComplianceRecordingPolicy, please make sure that you are inputting the Object ID from the previous command. Not the Application ID.
- If you cannot find the NexLog Teams Recording Service in the Microsoft Entra Admin Center, please double check the link you are creating.

7.1. Failed to connect to NexLog Teams Recording Service (24)

Please verify that credentials were entered correctly, or if there is a firewall issue preventing HTTP/HTTPS requests over port 80/443.

7.2. Failed to detect any heartbeats from NexLog Teams Recording Service (74)

Please contact Eventide Communications Support for more assistance.

7.3. Failed to record teams call <ms teams call id/callguid(tbd)> properly (74)

Please contact Eventide Communications Support for more assistance.

service@eventidecommunications.com

A. REQUIRED PERMISSIONS

The required permissions for the NTRS can be split into two parts. API permissions and role permissions.

Below are the required API permissions and role permissions.

A.1. API Permissions

The API permissions are used by the NTRS in order to join the call of the compliance policy holder.

- Calls.AccessMedia.All
- Calls.JoinGroupCall.All

See [Microsoft's Documentation on API permissions here](#) for more information.

A.2. Role Permissions

The role permission is used by the NTRS in order to query user information of the users in the call. This includes phone number, address, etc.

- microsoft.directory/externalUserProfiles/standard/read

See [Microsoft's Documentation on role permissions here](#) for more information.

