Mobile Connect Powered by Tango Networks for Microsoft Teams

For End-Customer IT Admins

Version 1.0

audiocodes

Table of Contents

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: January-30-2025

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Stay in the Loop with AudioCodes

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Related Documentation

Document Name

Document Revision Record

LTRT	Description
31205	Initial document release.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

1 Introduction

This document is intended for the Microsoft Teams IT administrator of the subscribers belonging to the end-customer.

2 Microsoft Teams Administrator

This section describes the procedures that the Microsoft Teams administrator needs to perform. These procedures are done in the Teams Admin Center.

The Teams Admin must make sure that the following are fulfilled prior to end user onboarding of the Mobile Connect service:

- Verify user access to Microsoft SIP Gateway. The Calling Policy assigned to users must have **SIP devices can be used for calls** enabled.
- Verify users have Teams calling plan and DID.
- Configure access to the Tango Extend Provisioning app in Teams:
  - Ensure that the Extend app is set to **Allowed**.
  - Review app permissions and provide consent.
  - Define Permissions policies to control access to the Extend app.
  - (Optional) Setup policy to control installed and pinned apps.
- Verify that the end-user has a compatible mobile device that is carrier unlocked:

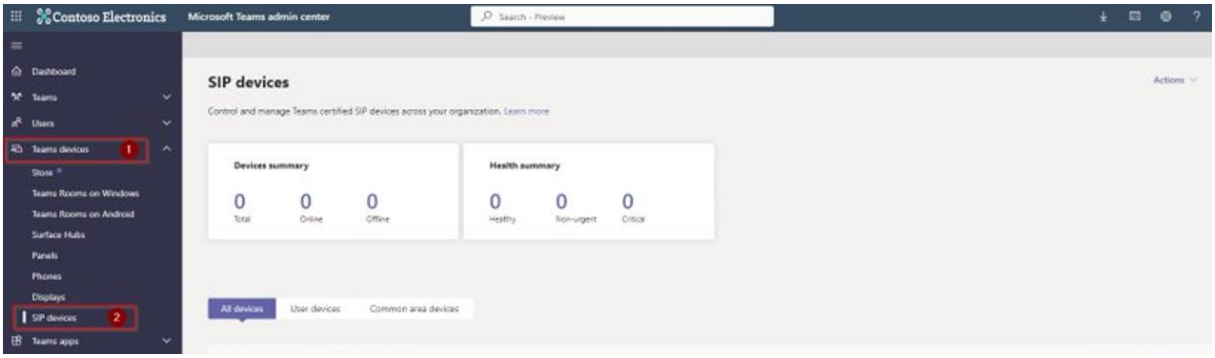
  See Supported Phones - Tango Networks for supported devices.

2.1 Verifying User Access to Microsoft SIP Gateway

The following procedure describes how to verify that Microsoft SIP Gateway is available for your organization.

To verify user access to Microsoft SIP Gateway:

1. Sign into the Teams admin center.
2. In the navigation pane, expand **Teams devices** and check if the **SIP devices** item is listed under it. If yes, the SIP Gateway service is enabled for your organization. If no, continue to Step 3 to enable SIP Gateway for Teams users.

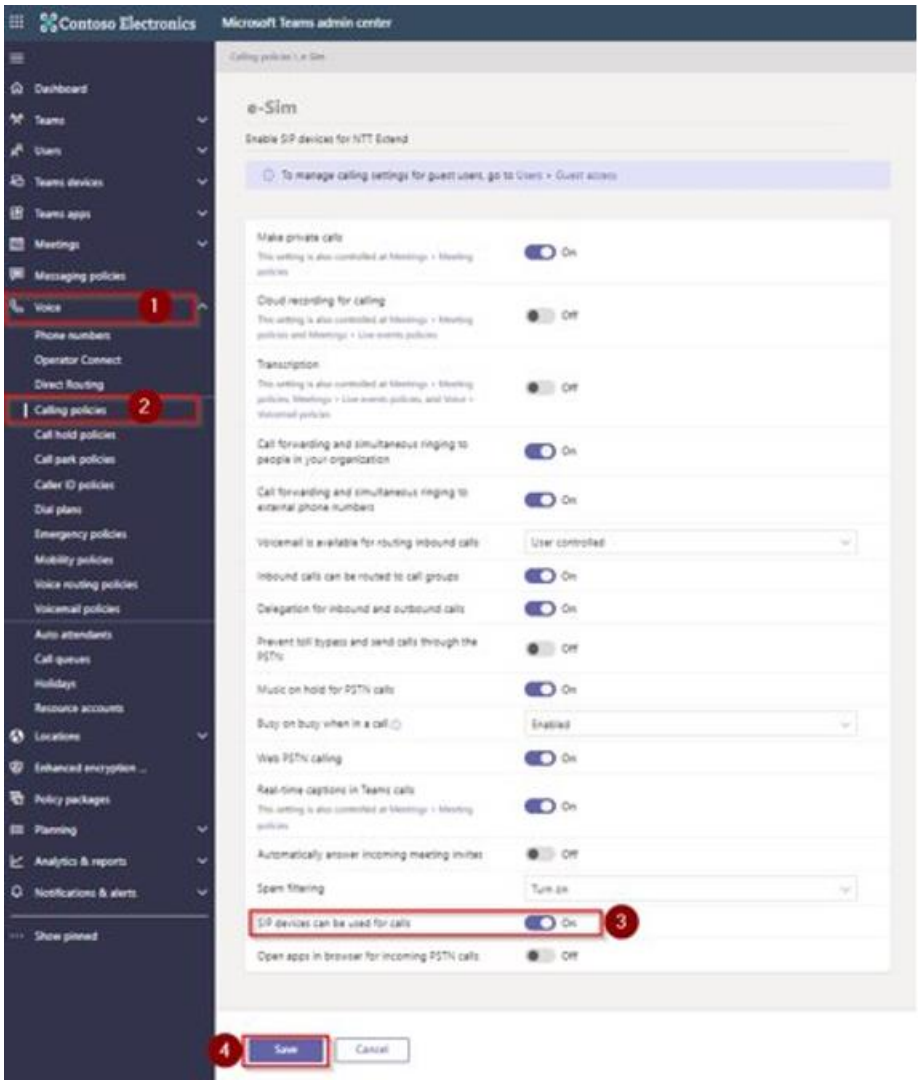


2.1.1 Enabling SIP Gateway for Teams Users

The following procedure describes how to enable SIP Gateway for your Teams users.

To enable SIP Gateway for Teams users:

1. In the navigation pane of Teams admin center, expand **Voice**, and then click **Calling policies**.
2. Select **Manage policies**, and then select the appropriate calling policy assigned to users or, if necessary, create a new calling policy and assign it to the required users.
3. Click the toggle button to turn on the SIP devices that can be used for calls.
4. Click **Save**.

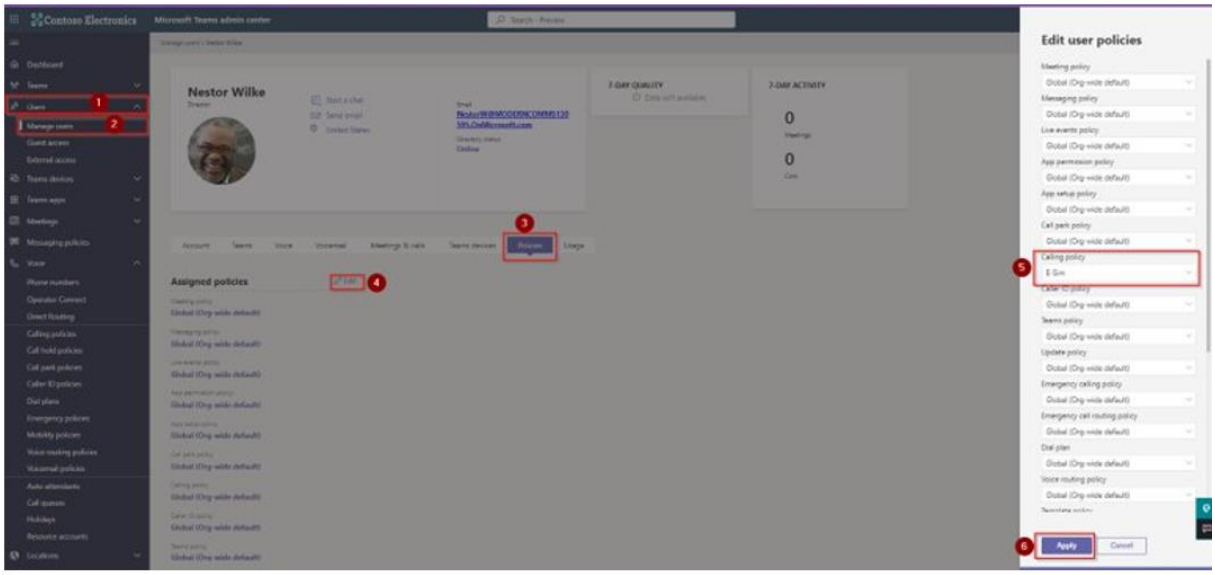


2.1.2 Assigning a Specific Teams Calling Policy to Users

The following procedure describes how to assign a specific Teams Calling Policy to a user.

To assign Calling Policy to Teams users:

1. In the navigation pane of Teams admin center, expand **Users**, and then click **Manage users**.
2. On the page, select the user to update.
3. Select the **Policies** tab, and then click **Edit**.
4. Select the appropriate Calling Policy, and then click **Apply**.

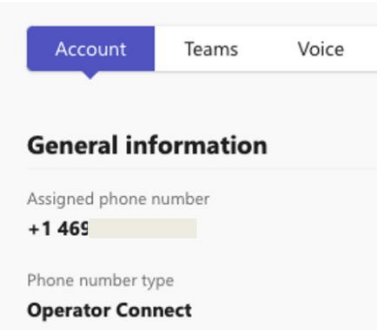


2.2 Verifying Users have Teams Calling Plan and DID

Verify that users have an Operator Connect or Direct Routing number type and DID.

To verify users have Calling Plan and DID:

1. In the navigation pane of Teams admin center, expand **Users**, and then click **Manage users**.
2. On the page, select the user to update.
3. Select the **Account** tab, and then verify that there is an assigned phone number and that the phone number type is one of the following:
   - **Operator Connect**
   - **Direct Routing**

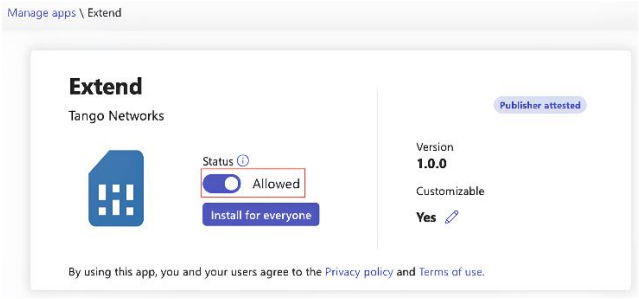


2.3 Configuring Access to Tango Extend Provisioning App

2.3.1 Ensuring Extend App is "Allowed"

To ensure Extend app is "Allowed":

1. In the navigation pane of Teams admin center, expand **Teams apps**, and then click **Manage apps**.
2. In the 'Search by name' box on the right side of the page, type "Extend".
3. From the resultant search list, click the **Extend** app.
4. Verify that the 'Status' field is switched to **Allowed**.



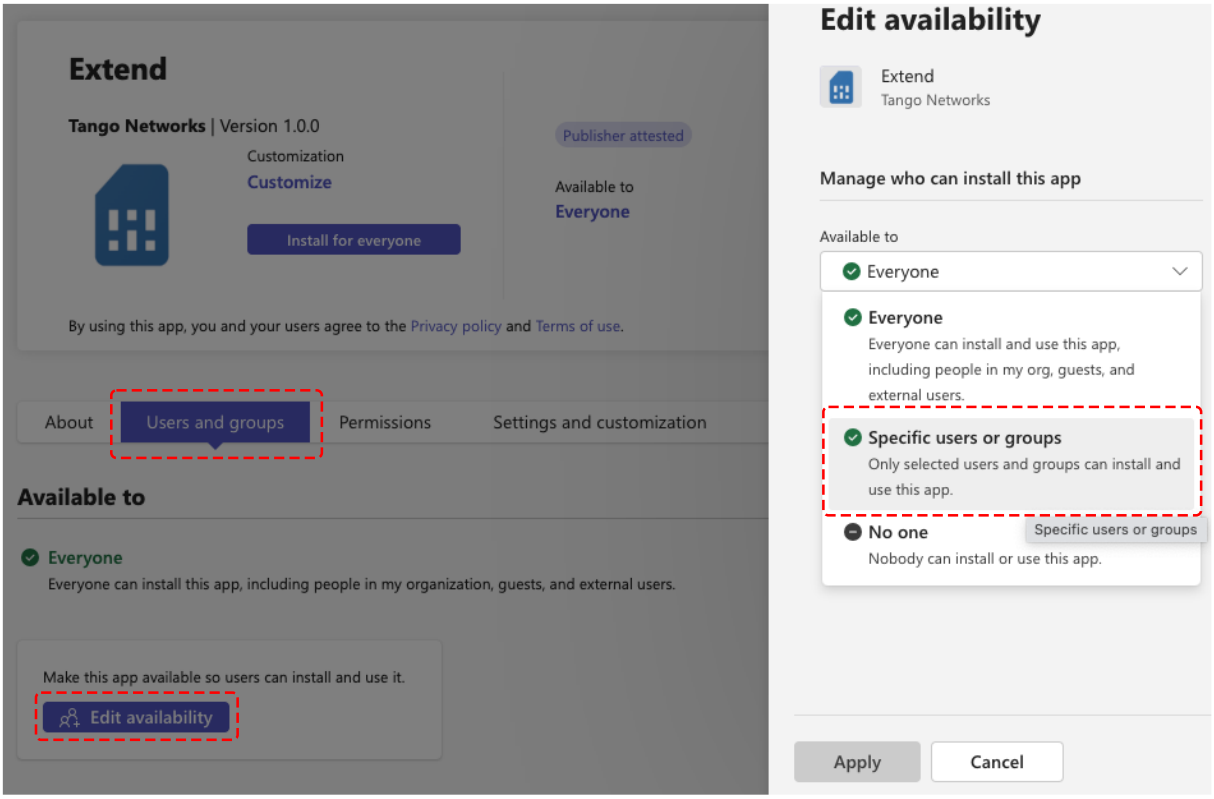
Do **NOT** install the Extend app for everyone, unless the entire organization will be using the service and there are enough resources (eSIMs) available. Instead, follow the instructions in the next section to control which users are entitled to the Extend service

2.3.2 Control Entitlement to Extend for Teams Service

You can control which users can access the Extend app, as described in the following procedure.

To control access to Extend:

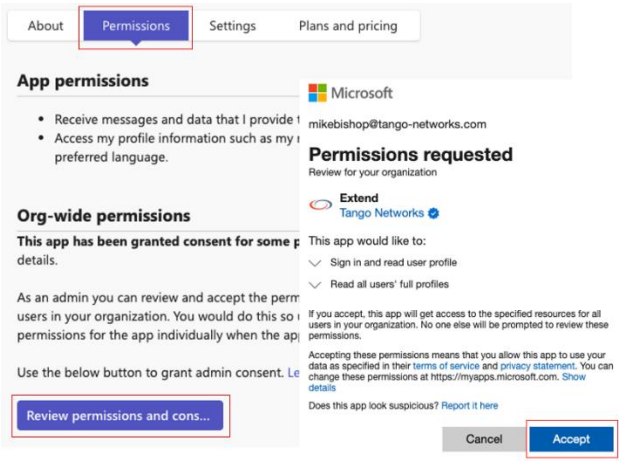
1. In the navigation pane of Teams admin center, expand **Teams apps**, and then click **Manage apps**.
2. Select the **Users and groups** tab.
3. Under the Available To group, click the **Edit availability** button; a dialog box appears on the right pane.
4. From the 'Available to' drop-down list, select **Specific users and groups** to control entitlement to the Extend for Teams service.
5. Select the users and/or groups, and then click **Apply**.



2.3.3 Consenting to Extend App Permissions

To consent to app permissions:

1. In the navigation pane of Teams admin center, expand **Teams apps**, and then click **Manage apps**.
2. In the 'Search by name' box on the right side of the page, type "Extend".
3. From the resultant search list, click the Extend app.
4. Select the **Permissions** tab.
5. Click the **Review permissions and consent** button.
6. Provide or select your Teams admin user credentials; a pop-up dialog box appears.
7. Review the required permissions and then click the **Accept** button.



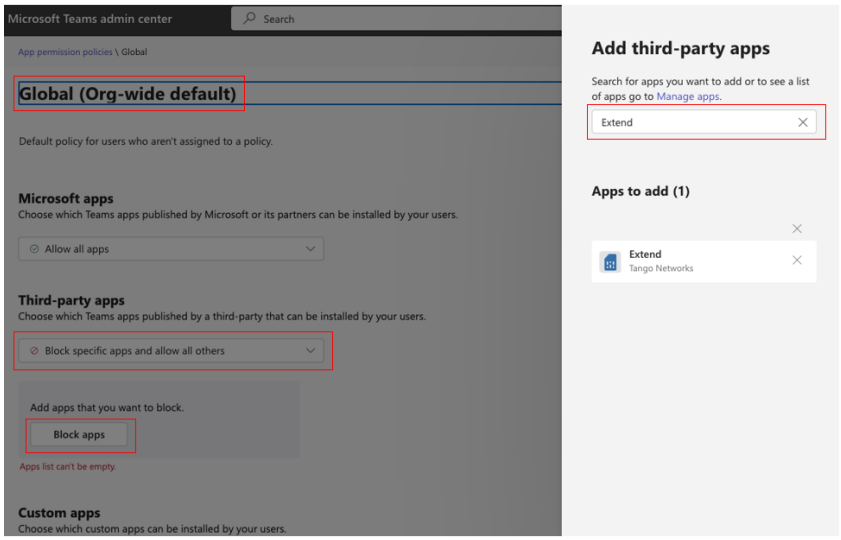
2.3.4 Defining Permissions Policies for Access to Extend App

To control user access to the Extend service, it is required that access to the Extend app be limited to only those users requiring the service. Therefore, use Permission policies to control access to the Extend app.

The following procedure uses an example that restricts access using the "Global (Org-wide default)" policy.

To define access permissions to Extend app:

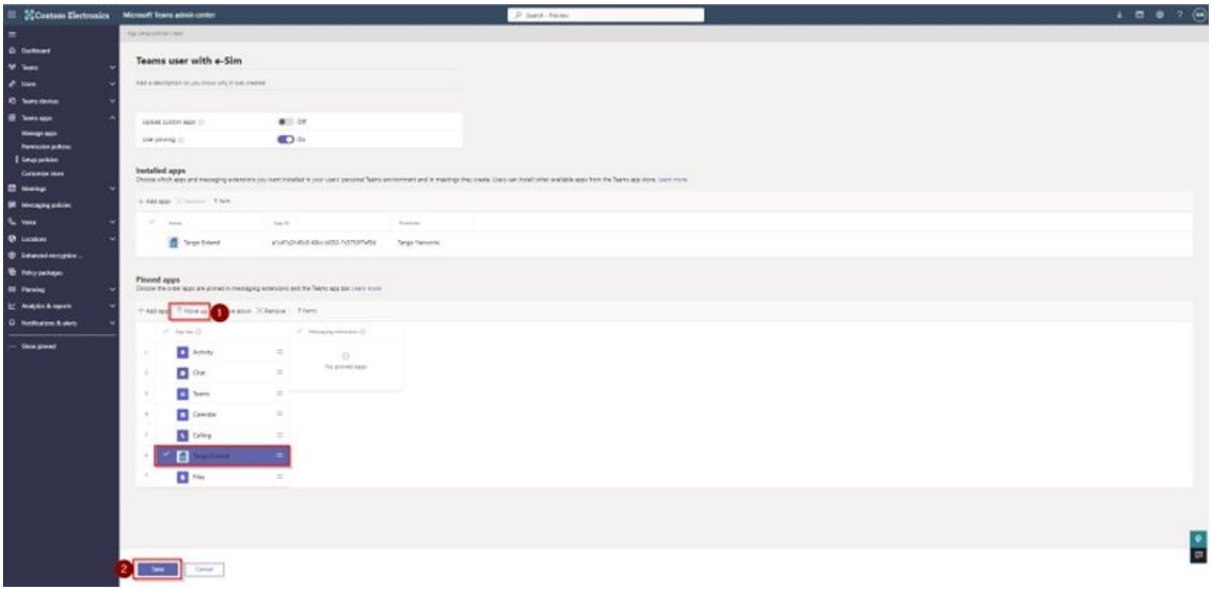
1. In the navigation pane of Teams admin center, expand **Teams apps**, and then click **Permission policies**.
2. Select **Global (Org-wide default)**.
3. From the 'Third-party apps' drop-down list, select **Block specific apps and allow all others**.
4. Click the **Block apps** button.
5. In the 'Search by name' field, type "Extend", and then click **Add**.
6. Click the **Block** button to confirm the app(s) to block.
7. Click the **Save** button.



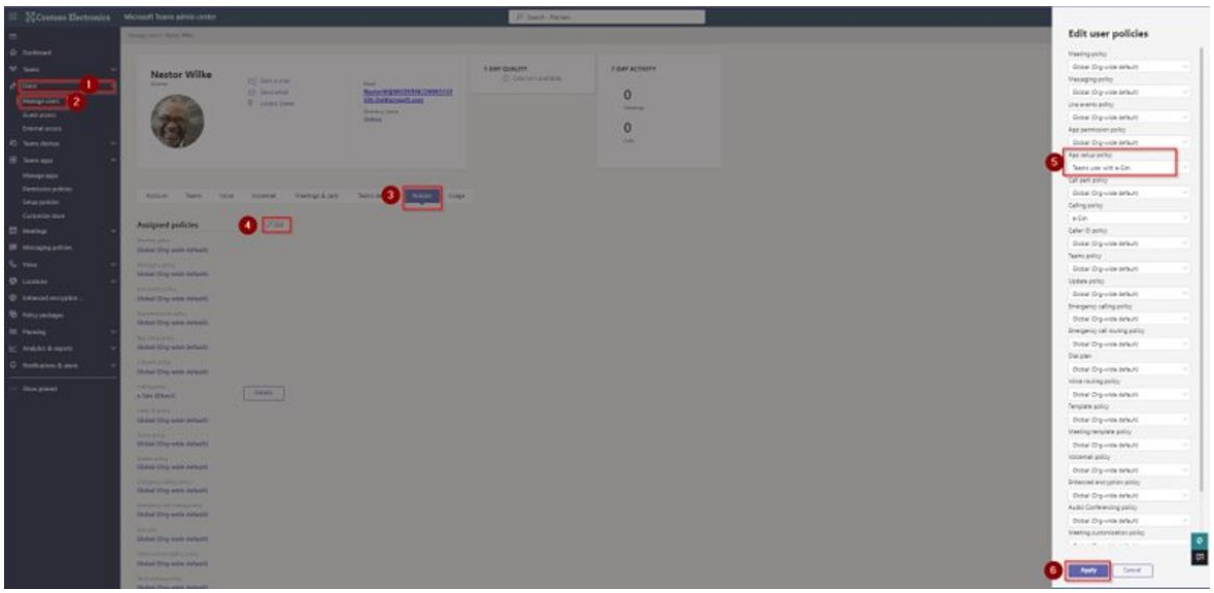
2.3.5 Creating and Assign App Setup Policies

To create app setup policies:

1. Move up.
2. Click the **Save** button.



3. In the navigation pane of Teams admin center, expand **Users**, and then click **Manage users**.
4. Select the user whose policies you need to update.
5. Select the **Policies** tab, and then click the **Edit** button.
6. Select the Teams user with e-Sim.
7. Click the **Apply** button.



International Headquarters
Naimi Park
6 Ofra Haza Street
Or Yehuda, 6032303, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com

Document #: **LTRT-31205**