Configuration Note

Firewall Rules for AudioCodes Devices

IP PHONES & MEETING ROOM DEVICES

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: July-30-2026

Security Vulnerabilities

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

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

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 here.

Stay in the Loop with AudioCodes

Abbreviations and Conventions

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

Related Documentation

Document Name
C430HD IP Phone for Microsoft Teams User's and Administrator's Manual
C435HD IP Phone for Microsoft Teams User's and Administrator's Manual
C436HD IP Phone for Microsoft Teams User's and Administrator's Manual
C455HD IP Phone for Microsoft Teams User's and Administrator's Manual
C456HD IP Phone for Microsoft Teams User's and Administrator's Manual
C470HD IP Phone for Microsoft Teams User's and Administrator's Manual
RX-PAD Room Controller User's and Administrator's Manual
RXV81 MTRA User's and Administrator's Manual
RXV81 BYOD MTRA User's and Administrator's Manual

Document Revision Record

LTRT	Description
11312	Initial document release

1 Cloud Endpoints, Ports, Protocols – Overview

This document describes:

- Which public Internet services an AudioCodes phone or meeting room device communicates with.
- Which outbound connections must be permitted by the enterprise firewall to allow the device to provision successfully, remain managed, obtain certificates, and support AI meeting summaries.

Rules of Thumb

- **Allowlist by FQDN, not IP Address.** AudioCodes services are hosted in Azure. Because the underlying IP addresses can change without notice, firewall policies should be based on fully qualified domain names (FQDNs) rather than IP addresses. Any IP addresses referenced in this document are provided for illustration only and must not be used as permanent firewall rules.
- **TLS interception prevents device provisioning.** AudioCodes devices authenticate to both the Redirect Server and Device Manager using a factory-installed client certificate and mutual TLS.

  TLS/SSL inspection or interception of these connections can prevent successful authentication and provisioning. Ensure that the relevant AudioCodes service FQDNs are excluded from SSL/TLS inspection.
- **Microsoft Teams Devices Require Additional Microsoft Endpoints.** For AudioCodes Teams-native phones and meeting-room devices, the endpoints specified in this document cover AudioCodes services only.

  The Microsoft Teams application running on the device also requires access to Microsoft-managed network endpoints for services such as:

  - User sign-in and authentication
  - Teams signaling
  - Real-time media traffic
  - Application and firmware updates

  Ensure that the Microsoft 365 and Teams endpoints documented by Microsoft are also permitted:
  learn.microsoft.com/microsoft-365/enterprise/urls-and-ip-address-ranges

2 Zero Touch Provisioning (Redirect Server)

A factory-default device that does not receive DHCP Option 160 or DHCP Options 66/67 automatically contacts the AudioCodes Redirect Server. The device authenticates using its factory-installed client certificate, and the Redirect Server responds with an HTTP 302 redirect to the provisioning URL associated with the device's MAC address.

The provisioning URL returned by the Redirect Server is not necessarily an AudioCodes service. Customers can register their own provisioning services against device MAC addresses. As a result, the firewall destinations that must be permitted depend on who manages the device:

- **Devices Managed by AudioCodes Live Platform**

  For devices managed by AudioCodes Live Platform, the Redirect Server returns the tenant's Service Device URL. The device then connects to the corresponding Live Platform Device Manager service for provisioning and lifecycle management.

  See Live Platform Device Manager for the required endpoints and firewall rules.

- **Devices Managed by Customer Provisioning Services**

  When a customer or partner operates its own provisioning service, the Redirect Server returns the URL of that service. In this scenario, the enterprise firewall must allow access to the endpoints published by the provisioning service provider.

  Other than access to the AudioCodes Redirect Server itself, the AudioCodes-specific firewall requirements described in this document do not apply.

- **AudioCodes Zoom Devices**

  For AudioCodes Zoom devices, follow Zoom's firewall guidance:

  Zoom network firewall or proxy server settings

The Zero Touch Provisioning chain is as follows:

DHCP option 160 → DHCP option 66/67 → redirect.audiocodes.com → 302 → Provisioning Service URL

The following table describes the redirect endpoints:

Endpoint	Port	Protocol	Direction	Purpose
redirect.audiocodes.com	443	HTTPS / TLS	Outbound *device → cloud*	ZTP discovery: ■ Device sends `GET /<MAC>` with mutual TLS. ■ Server returns an HTTP 302 redirect with the provisioning URL. Firmware default: `provisioning/redirect_server_url= https://redirect.audiocodes.com`

Endpoint	Port	Protocol	Direction	Purpose
Customer / partner provisioning URL	443	HTTPS	Outbound *device → provisioning service*	If the MAC is registered to a non-AudioCodes provisioning service, the Redirect Server returns an HTTP 302 redirect to that service instead of to an AudioCodes Service Device URL. In this scenario, the destination FQDN is defined by the provisioning service provider, not by AudioCodes. The enterprise firewall must therefore allow access to the endpoints published by that service. The only AudioCodes-specific requirement is access to the Redirect Server itself; additional AudioCodes provisioning endpoints do not apply. **AudioCodes Zoom devices:** Follow Zoom's published network and firewall requirements, as referenced above.
redirectapp.audiocodes.com	443	HTTPS	Outbound *admin browser*	Redirect Service management portal, used to register MAC addresses to a tenant. Needed by administrators, not by devices.

2.1 Prerequisites for Zero Touch Provisioning

Service	Port	Protocol	Direction	Purpose
Public DNS resolver	53	UDP / DNS	Outbound	The device must be able to resolve public names.
NTP time source	123	UDP / NTP	Outbound	Clock sync. A wrong clock fails certificate validity checks and fails the TLS handshake.
Time Zone Database (tz / zoneinfo)	443	HTTPS	Outbound	Time zone data refresh on Android-based devices.

3 Live Platform Device Manager

> **This section applies only to devices managed by AudioCodes Live Platform Device Manager.**
>
> The requirements in this section apply exclusively to devices managed by AudioCodes Live Platform Device Manager. Devices redirected to a customer or partner provisioning service follow that service's network and firewall requirements instead.

The connection path of a device to the Live Platform Device Manager is as follows:

Device — keep-alive 443 → Imperva Cloud WAF → Azure Aggregator → Device Manager

The device accesses Azure storage to retrieve firmware and configuration files:

Device — 443 → Azure Blob Storage (firmware + configuration files)

3.1 Device Traffic Required from the Device VLAN

Endpoint	Port	Protocol	Direction	Purpose
Service Device URL *Tenant-specific URL returned by the Redirect Server*	443	HTTPS / TLS	Outbound	Maintains device connectivity, keep-alive messages, and status reporting to AudioCodes Live Platform Device Manager through the Web Application Firewall (WAF). The URL is in the following format: `https://<live-platform-host>/ltcfordevice/c/<ServiceID>/` Where: ■ `<live-platform-host>` is the tenant's regional Live Platform host. The regional FQDNs are listed below. ■ Device Manager is hosted on Live Platform and is reached through the same regional host used for administrative access.
Imperva Cloud WAF *IP ranges only required for IP-based firewall rules*	443	HTTPS	Outbound *terminates at WAF*	The Imperva Cloud WAF is not a separate destination. The WAF fronts all Live Platform web and REST interfaces, including Device Manager. Allowlisting the FQDNs above is therefore sufficient for environments that support FQDN-based firewall rules. Only firewalls that filter traffic by destination IP address rather than FQDN require Imperva's published IP ranges to be maintained. Because these ranges may change, they should be retrieved periodically from Imperva's published documentation. For details see Allowlisting Imperva IP addresses and Setting IP restriction rules [c85245b7]

Endpoint	Port	Protocol	Direction	Purpose
*.blob.core.windows.net	443	HTTPS	Outbound	Firmware, software, and configuration file downloads from Azure Storage. AudioCodes does not rely on a single Azure Storage account, so firewall policies should allow access to the required Azure Storage endpoints in accordance with Microsoft's Azure Storage networking guidance.

3.2 Administrator Access to the Live Platform Portal

Administrator access is regional, allowing only the region from which the tenant is served from.

Region	Portal FQDN	Port	Protocol
EMEA	emea-ltc.audiocodesaas.com	443	HTTPS
Americas	americas-ltc.audiocodesaas.com	443	HTTPS
Canada	canada-lp.audiocodesaas.com	443	HTTPS
APAC	apac-ltc.audiocodesaas.com	443	HTTPS
India	india-lc.audiocodesaas.com	443	HTTPS
Japan	japan-lp.audiocodesaas.com	443	HTTPS
China	china-lc.audiocodes.zzxt.com	443	HTTPS

3.3 Administrator Access to the IAM (Browser Only)

The following table lists the IAM access endpoints for administrators:

Endpoint	Port	Protocol	Purpose
iam.audiocodesaas.com	443	HTTPS	AudioCodes identity service
acservicesiam.b2clogin.com	443	HTTPS	Azure AD B2C sign-in. Path: **/tfp/acservicesiam.onmicrosoft.com**
acservicesiamfiles.blob.core.windows.net	443	HTTPS	Sign-in page assets
services.audiocodes.com	443	HTTPS	Services portal landing

Sign-in uses pop-up windows. A browser or proxy that blocks pop-ups for these hosts will stall the login silently.

4 Cloud NDES Certificate Enrollment

Devices use the AudioCodes cloud-hosted Network Device Enrollment Service (NDES) to obtain and maintain their operational device certificates. Certificate enrollment, renewal, and rollover are performed using the Simple Certificate Enrollment Protocol (SCEP).

4.1 SCEP Enrollment — Cloud NDES

The following endpoint must be accessible from the device VLAN:

Endpoint	Port	Protocol	Direction	Purpose
ndes.audiocodesaas.com */certsrv/mscep/mscep.dll/pkiclient.exe*	443	HTTPS / SCEP	Outbound	Certificate signing request, issuance, renewal and rollover over SCEP against Microsoft Network Device Enrollment Service.

5 AI Summary

On RXV meeting-room devices, the AI Summary feature triggers a cloud-based bot that joins the Teams meeting and produces the meeting summary.

The device only initiates the request. The transcription and summarization happen entirely in the AudioCodes cloud service.

Endpoint	Port	Protocol	Direction	Purpose
https://aisummary-emea.meetinginsights.com/	443	HTTPS	Outbound	Triggers the AI Summary service from the device. The device sends a request to initiate summary generation for the meeting. All subsequent transcription and summarization processing occurs in the AudioCodes cloud.

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-11312