



Mira Connect Network Considerations

Introduction

The Mira Connect and Mira Connect 10 products are cloud-configured network-attached room controllers for audio-visual equipment using wired or wireless network interfaces to access equipment on a host IT network. Mira Connect products control audio visual equipment on the local network using telnet, SSH, or HTTPS depending on how the underlying equipment can be controlled.

Mira Portal is a multi-tenant cloud-based provisioning server and management portal for configuring and managing Mira Connect systems. Mira Portal has strict permission rules that determine access to Mira Connect’s configuration and status information.

Audience

This document applies to IT professionals who manage corporate networks and AV integration partners who need to install and provision Mira Connect products within a corporate network environment.

Mira Connect Network Interfaces

Mira Connect products have two network interfaces - a wired and a wireless interface - and only one network interface can be used at a time with the wired interface taking precedence over the wireless interface.

Wireless Network Security modes supported are Open (no security), WPA, and WPA2 Personal. If the wireless interface is used, it must have access to the AV LAN to control the equipment as shown in Figure 2.

When Mira Connect’s Wireless Network interface is used, a PoE connection that provides power is required periodically to re-charge Mira Connect’s battery. Mira Connect 10 does not include a battery and requires an external power supply for applications where there is no PoE network connection. See the [Mira Connect 10](#) Technical Specifications for more information.

Mira Connect Network Port Usage

Mira Connect products use the network ports shown in the following table as it communicates with Mira Portal and with the local equipment that it controls.

Table 1. Mira Connect Network Port Usage

Connection Initiation	Port	Network	Protocol	Outbound Data	Inbound Data	Configurable Port Number
Outbound	443	WAN	HTTP over TLSv1.2	Status information to Mira Portal	Configuration download, remote control commands, firmware updates	No
Outbound	Various	AV LAN	Dependent on controlled equipment	Control of AV equipment at ports specific to the controlled equipment	Status messages from controlled equipment at ports specific to the equipment	Dependent on the controlled equipment

During initial provisioning and operation, Mira Connect initiates an encrypted outbound secure socket over port 443 to Mira Portal (<https://mira.aveosystems.com>). **Mira Connect Me** touchless AV control feature requires that users’ devices can access <https://miraconnect.me>.

For Mira Connect to download a Visual Theme background image, logo, and channel favorite icons requires access to: <http://firebasestorage.googleapis.com/>.

WAN Bandwidth requirements are very low and are on the order of kilobytes / hour for status information once the unit has been provisioned and visual theme images downloaded.

Capabilities supported regardless of WAN connectivity once Mira Connect has been provisioned include controlling equipment on the local AV LAN. Regardless of WAN connectivity, Mira Connect operates as a control system for users in the room.

Capabilities that require WAN connectivity include:

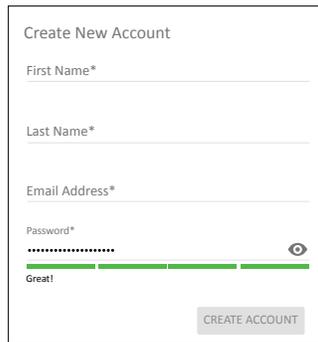
- Re-provisioning Mira Connect with equipment changes and management changes including Visual Theme updates (background and logo images, and custom colors)
- Remote Control of the Mira Connect by an authorized user via Mira Portal
- Updating Mira Portal dashboard with equipment status and recent events including recent calls
- Mira Portal text messaging with updates on equipment online/offline status
- Office 365 Calendar integration to access meeting invitations for the specified service user account
- Mira Connect firmware updates

Mira Connect Operating System

Mira Connect products run the Android operating system version 6.0.1 or newer.

Mira Portal Access

Mira Portal access requires a Mira Portal account. The Mira Portal password must contain at least 6 characters. Users are provided a password strength indicator when creating a new account as shown in Figure 1.



The screenshot shows a 'Create New Account' form with the following fields: 'First Name*', 'Last Name*', 'Email Address*', and 'Password*'. The password field is filled with dots and has a green progress bar below it, indicating a 'Great!' password strength. An eye icon is visible to the right of the password field. A 'CREATE ACCOUNT' button is located at the bottom right of the form.

Figure 1. Creating a new Mira Portal account provides a visual indicator of the password security.

Permissions to access a particular organization, site, or room information are assigned within Mira Portal by the organization's administrator. Administrator permissions for a specific organization or site can create and assign other permissions on the customer's organization, site, and room settings as well as create new sites within that organization and new rooms within sites. By default, the Mira Portal user who creates the organization has administrative permissions on that organization. See the [Mira Connect Administrator's Guide](#) for additional information on user permissions and a description of the *Technical*, *Help Desk*, and *Reporting* permissions.

Mira Connect Network Interface Considerations

For proper operation, Mira Connect products require:

- A DHCP server that provides an IP address to the Mira Connect product. The DHCP server will also provide the gateway IP address for Mira Connect to connect to Mira Portal. The DHCP server can be part of the AV LAN or part of the Corporate LAN.
- Mira Connect's network connection must have access to the network of the local equipment to be controlled -

ideally Mira Connect and the local equipment are on the same subnet.

- A PoE network connection (PoE Plus may be used, but is not required) to use the Mira Connect wired network connection or to charge the battery in certain Mira Connect products. If a PoE network interface is not available, a 48V PoE injector must be used. An external power supply can be used for the [Mira Connect 10](#).

Typical Network Configuration

Mira Connect is typically connected to the local AV network as shown in Figure 2. In this example, the AV LAN is used to create network connections to the equipment to be controlled. A DHCP server provides a dynamic IP Address for Mira Connect. At least during initial provisioning, the WAN port of the DHCP server/router needs to be connected to either a corporate network, or temporarily shared network with access to Mira Portal.

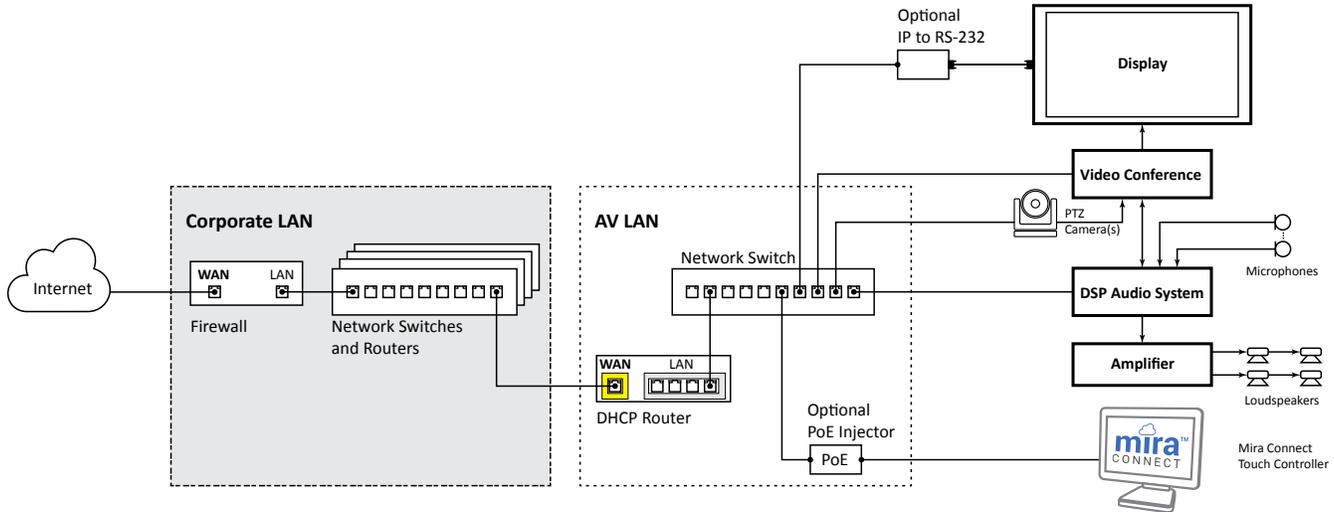


Figure 2. Typical Mira Connect network connections. A DHCP server is required either on the corporate LAN or AV LAN for Mira Connect products.

An alternative to connecting to the corporate LAN is to temporarily share WAN from a local computer as shown in Figure 3. A laptop can be used to share its wireless Ethernet interface to its wired interface. This way a mobile device hotspot can be used to provide WAN access through the PC to the AV LAN. For more information, see our Sharing Networks application note:

https://Aveosystems.com/wp-content/uploads/product_pdfs/SharingNetworks_AppNote.pdf

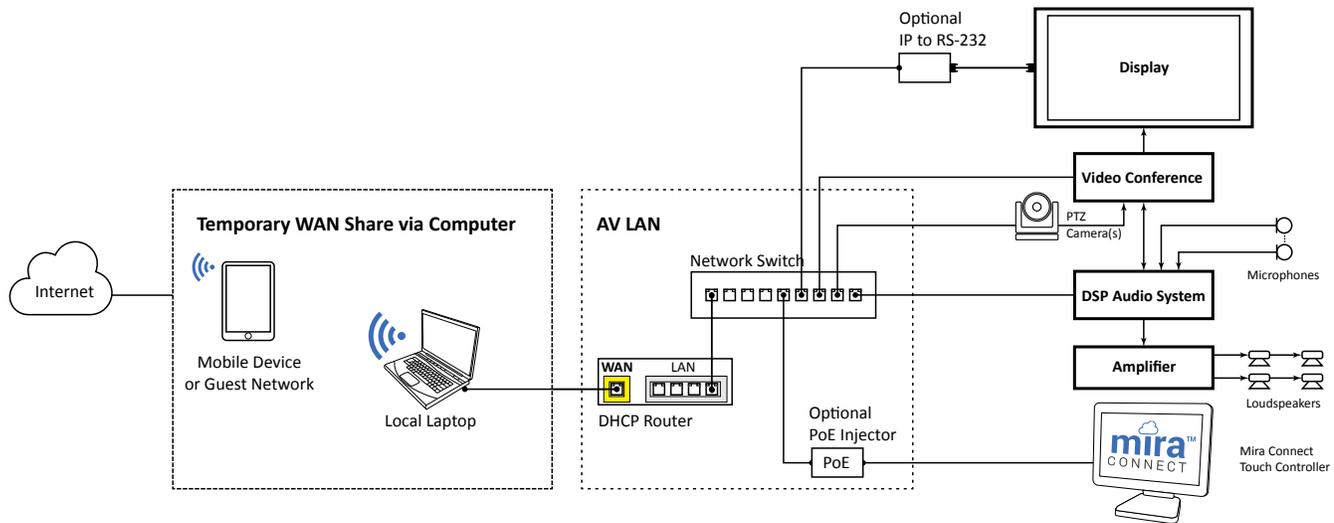


Figure 3. Temporary WAN share for access to Mira Portal during set up.

For more information please contact our Sales Department at sales@aveosystems.com.

About Aveo Systems

Aveo Systems is a leading provider of intuitive and easy-to-use solutions for audio, video, and collaboration, improving how systems are used and managed by customers world-wide.

Specifications subject to change without notice. Aveo Systems and the Aveo logo are registered trademarks. All other trademarks are the property of their respective owners.



DS-11024-001
Version 20230619