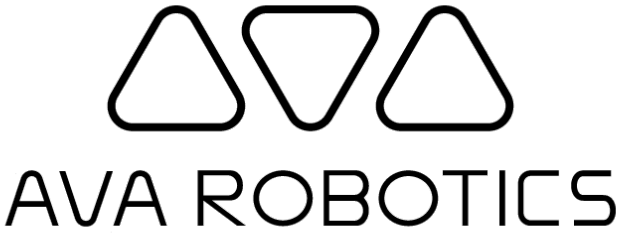


Ava Security and Privacy

v5.1.2

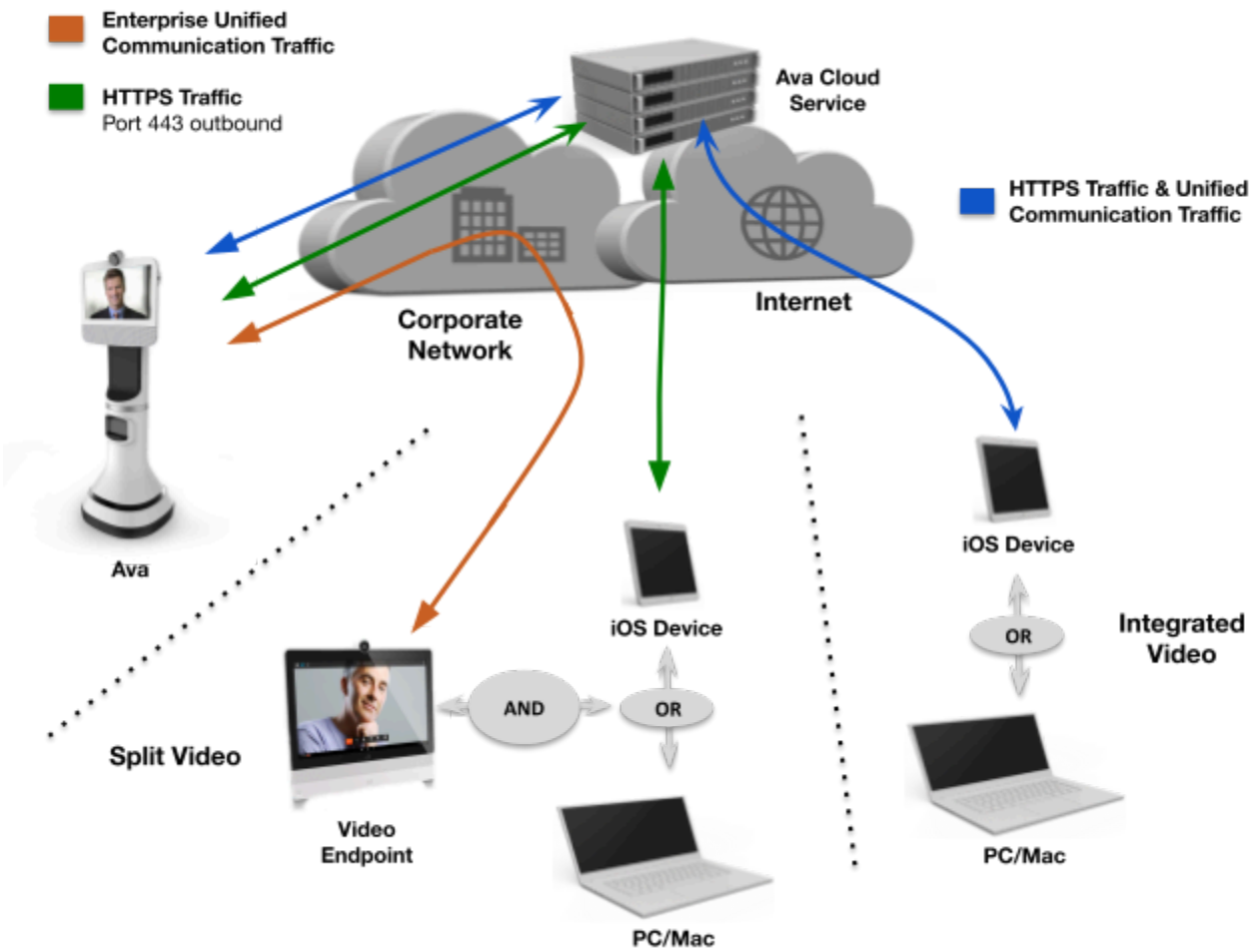
Table of Contents

Ava Overview

Ava Communications

Ava Robotics is committed to ensuring data security and protecting the privacy of your information. The Ava solution is built with industry-standard security practices and employs strict policies to protect your data.

At the highest level, Ava Communications consists of robot operational communications (outbound https) and video communications (SIP calls and associated control traffic). The following topology diagram provides a high-level view of the flow of robot operational and video communications for customer managed registration utilizing split video (green and orange flow) and Ava managed registration utilizing integrated video (blue flow). Hybrid versions of these two options also can be employed.



Robot Operational Communications: The Ava Control Application (Ava App) transmits operational commands from the remote user to the Ava Cloud Service, which in turn communicates with the Ava robot.

All communications between the Ava App and the Ava Cloud Service, and between the Ava Cloud Service and the Ava, are sent over a secure WebSocket connection through port 443, using a Transport Layer Security (TLS) protocol for encryption and authentication. The Ava Cloud Service is the termination point for all Ava App and robot communications. No information or data passes directly between the Ava App and the Ava.

Video Communications: The Ava solution is designed to integrate easily into your existing video infrastructure environment. The video codec that is part of the Ava Robot is completely configurable through its own user interface to match your specific environmental requirements for video call control and media.

There are two options for video communication deployment:

- Option 1: Customer-managed video infrastructure – In this deployment mode, all video communications between the Ava robot and the remote users are managed by the infrastructure policies you have in place. No video call control or media traffic is routed through the Ava Cloud Service.
- Option 2: Video infrastructure managed by Ava Robotics. In this deployment mode, the video codec is registered to a cloud video infrastructure, managed under the umbrella of the Ava Cloud Service.

When using customer managed video registration, there are multiple options such as a video infrastructure on premise, on a dedicated cloud, or to Cisco Webex public cloud.

For a remote user with a video endpoint, the Ava solution offers two options: integrated video into the Ava apps, or split video (video call to an external endpoint/software or to a video conferencing service such as Webex Meetings). The following should be noted regarding remote user video:

- Integrated video to the Ava apps uses Cisco Webex Video SDKs, and calls are routed from the apps to the Cisco cloud, then to the Ava robot (whether on customer-managed or Ava-managed video infrastructure)
- In split video, the call is routed from the Ava robot to the SIP URI of the device or conferencing service being used.

In addition to what is covered above, administrative access to the Ava Cloud Service is through the IT Administrator Console web application using HTTPS over port 443.

Firewall Ports and Domains for the Ava Telepresence Robot

Operational Communications

For successful deployment of the Ava Telepresence Robot onto your network, the following destinations need to be reachable by the Ava robot for the purposes of management, user control of the robot in session.

Purpose	Source IP	Protocol	Destination	Dest. Ports
Management and control	Robot's IP address	TLS/TCP	**.ava8.net (1)*	443
Software upgrades	Robot's IP address	TLS/TCP	robotsw.ava8.net	443
NTP service (optional) (2)	Robot's IP address	UDP	us.pool.ntp.org	123
Autoframe feature (optional)	Robot's IP address	TLS/TCP	*.amazonaws.com (1)	443

Notes:

(1) Your Ava representative can provide the exact subdomain(s) if needed
(2) This can be configured to any NTP server if there are site specific requirements

Firewall Ports for Ava Video Calls

Ava carries within itself a video conferencing "codec" which enables its video conferencing capability. This allows for a variety of high quality video experiences, whether inside of Ava's app, or conferencing services such as Webex, Zoom and others.

The video conferencing traffic from Ava will originate and terminate with the codec inside of Ava. The Ava's wireless IP address (obtained from the site's wireless network via DHCP) is the address on which the codec will appear on the network.

The codec needs to be registered to an infrastructure that supports video communication, firewall traversal, etc. This infrastructure needs to be compatible with the codec used.

The information provided in the remainder of this document applies if the infrastructure for video calling is being provided by Ava Robotics. If the video calling infrastructure is provided by your IT team, please consult with them for equivalent information. Ava Robotics uses the Cisco Webex public cloud for video calling. The following Cisco Webex technical note details network requirements for "Webex Room Devices":
https://collaborationhelp.cisco.com/article/en-us/WBX000028782.

The two most relevant sections in the above note are:

- Webex Services – Port Numbers and Protocols: look at rows for "All" and "Webex Room Devices"
- Domains and URLs that need to be accessed for Webex Services: specifically the services Software Upgrade, Registration Service, and Device Onboarding

Ava Security Policies

Ava Wireless Encryption and Authentication

Ava supports a wide variety of encryption and authentication methods for accessing your WiFi network - from open access to WPA2-Enterprise with 802.1X authentication. A complete listing of wireless network encryption and authentication methods supported by Ava follows.

The Ava Installation and Configuration Guide provides instructions on how to enroll Ava to a wireless network.

Open Network

This mode allows an Ava robot to connect to the wireless network without encryption or authentication.It is the least secure connection to the wireless network.

MAC-Based Authentication

Handled from the customer's infrastructure, MAC-Based Authentication is based on a factory-assigned, "burned-in" address given to every Ethernet device in existence. Because MAC addresses can be easily cloned by malicious attackers, MAC-based authentication is not considered a secure way to protect a network.

Pre-Shared Key Encryption (WPA/WPA2)

A pre-shared key (PSK) allows anyone who has the key to use the wireless network. Wired Equivalent Privacy (WEP) is the original 802.11 pre-shared key; however, it is not supported because it is vulnerable to being hacked.

WPA and WPA2 (WiFi Protected Access) use stronger encryption than WEP. (WPA uses TKIP with RC4 encryption, while WPA2 uses AES encryption.)

WPA/WPA2-Enterprise with 802.1X Authentication

802.1X is an IEEE standard framework for authenticating a user who is trying to associate to a wired or wireless network. 802.1X uses the Extensible Authentication Protocol (EAP) to establish a secure tunnel between participants involved in an authentication exchange. The Ava robot supports multiple EAP types, as detailed below:

- **EAP-PEAP (Often referred to as MS-PEAP or PEAPv0)** – PEAP provides a method to connect to a wireless network using a username/password. As part of the standard, before a client will give its username/password to an infrastructure, the client inspects

a certificate from a RADIUS server in order to confirm it is who it claims to be. This prevents a client or device from being tricked into sending a username and password to a malicious attacker, since the attacker will not be able to provide a trusted certificate.

	Because the password must be configured onto Ava and cannot be changed easily, the password should be set not to expire. While some clients can be configured to “always accept” the server certificate, Ava must have the proper certificate installed in order to authenticate. It will not blindly accept the certificate presented to it.

- **EAP-TLS** – The TLS method of EAP requires the use of a client certificate. In EAP-TLS, two certificates are in play: one is from the server confirming it can be trusted to receive credentials, and the other is from the client acting as its credentials. In order for this EAP type to be successful, the client must trust the certificate from the RADIUS server, and the RADIUS server must trust the certificate provided by the client. Therefore, two certificates must be installed on the Ava: the client certificate and the certificate of the CA (certificate authority) that generated the certificate being given to the client by the RADIUS server.

	Client certificates are generated by the customer’s IT department and installed on the Ava as part of the configuration process.

- **EAP-FAST** – EAP-FAST does not require a certificate, only a username and password. EAP-FAST establishes a shared secret between the client and the authentication server referred to as the Protected Access Credential Key (PAC-Key). The PAC consists of the PAC-Key and PAC info (metadata about the PAC). The PAC is used to establish a secure tunnel that is then used to perform authentication.

	For Ava, the PAC is distributed using automatic provisioning.

Protecting Data in Transit

As described in *Ava Communications Overview*, all communications between the Ava App and the Ava Cloud Service, and between the Ava Cloud Service and the Ava robot, are sent over a secure WebSocket connection using port 443, using a TLS protocol for encryption and authentication. All TLS communications are v1.2 only.

Similarly, Administrator Console access to the Ava Cloud Service is over a secure HTTPS

connection, also over port 443.

Authentication is one-way between the Ava Cloud Service and either the Ava App or the Ava Cloud Service Administrator Console, and mutual between the Ava Cloud Service and the Ava robot.

One-Way Authentication

In one-way authentication, the Ava Cloud Service presents its certificate to the Ava iOS App, Ava Web App or the Administrator Console. When remote users access the Ava Cloud Service through these interfaces, they authenticate over TLS using their unique username and password combination. Because the Ava Cloud solution presents a trusted TLS certificate, users can be assured that they are authenticated to a legitimate Ava Cloud Service instance. DigiCert is the Certificate Authority (CA) for the authentication used in the Ava Cloud solution.

Mutual Authentication

In mutual authentication, the Ava Cloud Service and the Ava robot exchange certificate information. Mutual Authentication is a widely implemented defense for Man-In-The-Middle (MITM) attacks against IT infrastructure components, and is inherently more secure than one-way authentication.

At a high level, the process of authenticating using certificate-based mutual authentication involves the following steps:

- A client (Ava robot) requests access to a protected resource (Ava Cloud Service).
- The server (Ava Cloud Service) presents its certificate to the client.
- The client sends its client certificate to the server.
- The server verifies the client's certificate.
- If successful, the server grants access to the protected resource requested by the client.

The Ava solution implements Mutual Authentication between the Ava Cloud Service and Ava robot by installing a client certificate, generated with a private key, and a CA certificate the Ava robot before it leaves the factory. The Ava solution provides its own root CA and client certificates for Mutual Authentication purposes.

By using TLS for all Ava communication, and by using client certificates for robot authentication, the Ava solution prevents an attacker from obtaining or intercepting any Ava robot traffic unless the attacker also has a client certificate and private key of each robot the attacker wants to intercept. This is true even if that attacker has received, stolen, or cracked a server certificate for the Ava Cloud Service.

Protecting Data at Rest

All Ava Cloud Services are hosted on Amazon Web Services (AWS). AWS is a well-respected cloud service provider employing security management best practices.

Upon request, a customer can be assigned a private cloud instance in the Ava Cloud Service. Ava Robotics personnel and assigned customer administrators have access to a private cloud instance. Only Ava Robotics personnel have admin access to a shared cloud instance.

Our security policies around protecting the Ava Cloud Service make it unlikely that your data would be compromised. That said, for even further security, the Ava Cloud Service encrypts user account credentials using a Salted Hash. The intention behind a Salted Hash is to protect against “Dictionary Attacks” of the account credentials by attaching a random value - the “salt” - to each password and only then computing and storing the resulting hash over both the password and the salt.

In addition, backups of the Ava Cloud Service are performed monthly. If preferred that backups are not taken, Ava Robotics will comply upon request. See the Privacy Policy section for details about the type of data that is stored in the Ava Cloud Service.

Single Sign-On (SSO)

The Ava Cloud Service supports SSO for the Ava Web Teleport App and for the Administrator Console using your company credentials. Ava uses OpenID Connect (OIDC) for SSO.

When SSO is enabled, password management and standards, and access are controlled by the Identity Provider. User login via a password managed by the Ava Cloud Service itself is disabled.

More information about Ava's implementation of Single Sign-On can be found in the Ava Administrator's Guide.

Account Password Complexity Policy

If SSO is not enabled, then management of user credentials is performed by the Ava applications. Upon creation of an account by an Ava Administrator, users receive an account with an initial password that should be reset by the end user when they first login to the Ava App.

At this time, the Ava Cloud Service does not enforce a mandatory password change upon initial login nor does it enforce password expiration after a certain duration.

The Ava Cloud Service recommends password complexity according to the following

requirements when user accounts are created.

- Passwords must be at least 8 characters long and contain at least 1 digit
- Passwords may not contain the user's username
- Passwords may not contain the user's first or last name

Password fields in the Ava Cloud Service and Ava Applications are obscured so that password entry is not viewable by non authorized persons.

Ava Robot Access on Local WiFi & via Ethernet Port

Administrative Interfaces to Robot

The robot's admin functions encompass 4 interfaces that can be accessed via local WiFi and via robot's local Ethernet service port:

- Ava Configuration Interface: The Ava Configuration Interface (ACI) is a web interface which provides direct access to Ava's configuration parameters and provides feedback on Ava's current status. It can be accessed via WiFi by pointing a web browser to the WLAN IP address of the robot at port 82, and via ethernet to the internal IP address of the Ava CPU (172.18.0.1) on port 82. These are HTTP only, they do not support HTTPS.
- Ava Web Drive: Web Drive is a web interface which provides access for trained engineers to create and manage "robot maps". It can be accessed via WiFi by pointing a web browser to the WLAN IP address of the robot at port 8800, and via ethernet to the internal IP address of the Ava CPU (172.18.0.1) on port 8800. These are HTTP only, they do not support HTTPS.
- Cisco Codec Admin Web UI: The Cisco codec offers a Web-based admin interface which is standard to the product. It can be accessed via WiFi by pointing a web browser to the WLAN IP address of the robot on port 80 or 443, and via ethernet to the internal IP address of 172.18.0.50 on port 80 or 443.
- SSH: SSH available via WiFi on port 2222 and ethernet on port 22, though its use is not meant for IT administrators. Use is expected only by Ava development and support engineers.

Securing Local Interfaces

Via local WiFi, access to the administrative interfaces is controlled by a software switch called "Install Mode" available on the Ava Configuration Interface. When "Install Mode" is set to Off, the ports necessary for access are turned off. Note however, that Install Mode does not affect

the Ethernet service port.

Access to the administrative interfaces is protected as follows:

- ACI: visible only to users reaching to port 82, with access via a hardcoded username and password (which is publicly documented in the Ava Installation and Configuration Guide, and frequently shared with customers via email and messaging)
- Web Drive: visible only to users reaching to port 8800, and access is not challenged
- Cisco Codec Admin Web UI: username and password, which are controlled by the administrator responsible for managing the Cisco Codec. When Ava Robotics is the administrator, the username and password are managed by the support team and not publicly documented.
- SSH: a hardcoded username and password (which is not publicly documented, but has been shared widely)

SSH access is disabled via WiFi when install mode is set to off in the Ava Configuration Interface. SSH access is always possible when connected to an Ava Robot via ethernet.

With few exceptions, all incoming port traffic is routed to the video codec and is subject to its security configuration.

Customer Policies and Site Physical Security

Equally important to securing Ava robot access are customer policies:

- Strong WiFi authentication policies prevent unauthorized network access.
- Physical plant security policies prevent unauthorized physical access to the robot.
- Ava Robotics recommends a strong passwords on any passwords managed by customers

Ava Robotics security policies, together with strong customer policies for physical plant security and WiFi Authentication, provide a robust security implementation.

Privacy Policy

This section informs you of our policies regarding the collection, use and disclosure of information we receive from users of the Ava solution.

We use your information only for providing and improving the Ava solution. By using the Ava solution, you agree to the collection and use of information in accordance with this policy.

Data Collection

We collect the following information:

- Account information: your name, username and password for login, email address, video endpoint addresses, and robot session preferences
- Facility information: information about your building layout, including office names and map images
- Robot information: name, overall health information, battery levels, software and firmware revisions
- Session information: frequency and length of sessions, usernames, facility locations, and robot driving commands used

Data Removal

When you discontinue service on a private instance, your Ava Cloud Service is deleted. This administrative process removes all data stored on the instance. Once completed, the private Ava Cloud Service is no longer operational.

When you discontinue service on a shared instance, an Ava Administrator removes all customer data stored on the instance. Once the process is completed, the existing Ava Cloud Service instance will be operational without any customer data.

Backups of data taken while the Ava Cloud Service was in operation can be deleted upon request.

Use and Disclosure of Information

We use the information we collect to provide services as part of the Ava solution. We may share it as discussed under *Tracking Technologies*, but we never sell it to advertisers or other third parties.

We may also use the information for internal purposes such as auditing, data analysis, and

research to improve the Ava solution.

Administrative and remote user software may display information like your name, username and facility information to other users.

Tracking Technologies

We use authentication cookies for the Ava Cloud Service Administrator Console and Web App. This allows us to keep you logged in as you navigate between various pages.

Like many service operators, we may collect log data that your browser or app sends whenever you connect with the Ava Cloud Service. This log data may include information such as your computer's Internet Protocol (IP) address, browser type, browser version, the pages of our site that you visit, the time and date of your visit, the time spent on those pages, and other statistics.

The Ava Cloud Service also logs all of its operational commands and stores that information for a two-week period. This data is used should debugging a problem become necessary.

In order to improve the performance of the Ava iOS App, crash logs are transmitted to Apple if the user has selected to share crash logs with developers. The logging information that is transmitted to Apple may contain such things as:

- Ava App version
- Session start time
- Ava App errors and warnings
- Ava App actions and breadcrumbs
- Ava Robot pose and movement commands
- Facility location information