Ava Security and Privacy

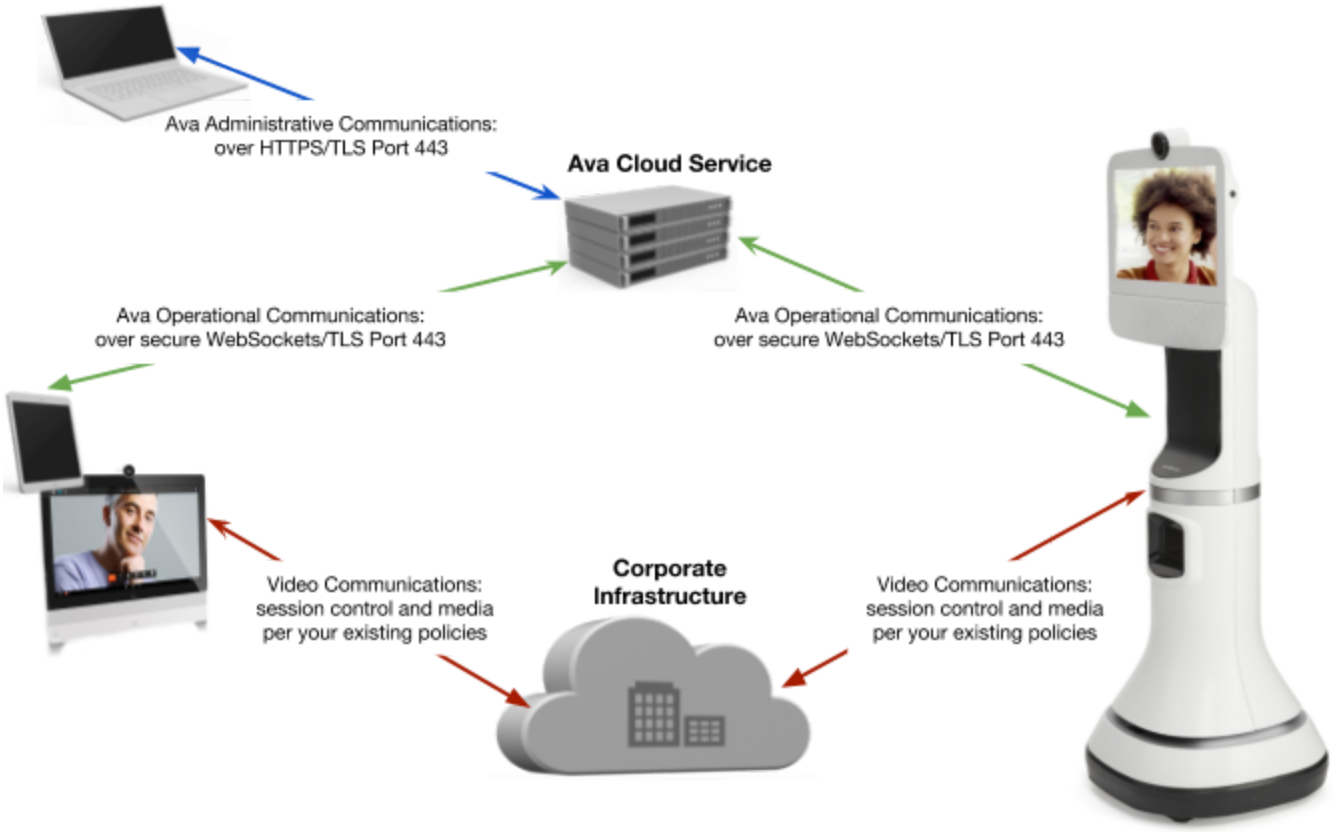
v3.0b

Table of Contents

Ava Communications Overview

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 can be divided into three major categories: robot operational communications, video communications, and administrative communications.



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 Cisco 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 – the video communication experience is provided in a dedicated video endpoint or video communications software. In this deployment mode, all video communications between the Ava robot and the endpoints that you supply for your 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 – the video communications are integrated into the Ava app. In this deployment mode, the Cisco Codec is registered to a CUCM in the cloud, managed under the umbrella of the Ava Cloud Service.

Administrative Communications: Administrative access to the Ava Cloud Service is through the IT Administrator Console web application using HTTPS over port 443.

Ava Security Policies

Ava Wireless Encryption and Authentication

Ava supports a wide variety of encryption and authentication methods for accessing your Wi-Fi 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.

Open

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 (Wi-Fi 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** – This EAP method was designed by Cisco and is used by a number of enterprises. 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.

Web Proxy Configuration

If a web proxy server is part of the customer security configuration, the Ava robot and the Ava App can be configured as proxy clients using the following methods:

Ava Robot

Manual, including the ability to specify hosts for which a direct connection should be used.
Automatic, by specifying a URL to the proxy configuration file.

For additional security, the Ava robot can be configured to authenticate to the web proxy server with a username and password.

Ava App

The Ava app uses the proxy functionality inherent in the iOS. Proxy settings are configured as part of the Wi-Fi settings in the iOS device, and can be:

- Manual
- Automatic, by specifying a URL to the proxy configuration file

For additional security, the iOS device can be configured to authenticate to the web proxy server with a username and password using Negotiate/NTLM, Digest, or Basic Authentication. Because iOS does not pass authentication information to the Ava App, if iOS proxy authentication is enabled then proxy fields are added to the Ava App login page.

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 employ a 2048-bit key cipher.

Similarly, Administrator Console access to the Ava Cloud Service is over a secure HTTPS connection, also over port 443.

All fixes for the Heartbleed and Poodle exploits have been incorporated into the Ava solution. Ava Robotics continually monitors and applies critical security fixes as needed.

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 App or the Administrator Console. When remote users access the Ava Cloud Service through the Ava App or the Administrator Console, 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. RapidSSL 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 verifies the server's certificate against its CA certificate.
- If successful, 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

See the Privacy Policy section for details about the type of data that is stored in the Ava Cloud Service.

The Ava Cloud Service is 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. Only Ava Robotics personnel have access to your 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.

Account Password Complexity Policy

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

Securing Ava Robot Access

As part of our ongoing development and testing efforts, Ava Robotics performs regular security scans of the Ava, and takes remedial action to address detected vulnerabilities. SSH access to the robot is disabled by default.

With few exceptions, all incoming port traffic is routed to the Cisco Codec and is subject to its security configuration. Ava Robotics recommends a strong password security policy on the administrative interface to the Cisco Codec.

Equally important to securing Ava robot access are customer policies. Strong Wi-Fi authentication policies prevent unauthorized network access. Plant security policies prevent unauthorized physical access to the robot. Ava Robotics security policies, together with strong customer policies for physical plant security and Wi-Fi 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 reset. The reset, run through an automated administrative process, 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.

The logs from these transactions can be provided on request, to confirm data removal.

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 IT Administrator Console and Web App. This allows us to keep you logged in as you navigate between various pages. Your session times out after a period of inactivity, which forces you to log in again.

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 App, it communicates with the Crashlytics crash reporting service. Crash logs and other information are transmitted to Crashlytics upon an iOS Ava App crash. A crash log is transmitted to Apple as well. The logging information that is transmitted to Crashlytics 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