SOPHIA

Network Security

Sophia: An Online Application Paired with a Highly Secure Network

Being an online application, the Sophia platform is a website that does not require any local installation on our client's computer, therefore guaranteing more privacy and efficiency.

On top of that, we have made sure that both available brewer connection methods avoid public internet and, therefore, cannot compromise our clients' server nor data.

Cellular Connection

- The **SIM card** inside the brewer's modem* connects to the closest available cellular tower's **APN** through our private connection. Our cellular network does not go over the public internet, therefore offering more reliability, faster speed, lower latencies and higher security than typical internet connections.
- It is impossible to reach the coffee machine or customer's private data using an external network.
- This solution enables the cloud to appear as another endpoint on Evoca North America's **MPLS VPN** network, making the cloud accessible to any coffee machine and avoiding the need to send data over the public internet.
- Advantages of this approach include:
    - Superior network performance, with as much as 50 % lower latency.
    - Up to 3x greater availability.
    - Enterprise grade security, avoids routing traffic over the public internet.
    - Data from the coffee machine are **encrypted** each time new data is transferred to the server.
    - User information is **encrypted** into the database (**one-way hash**).

Wi-Fi Connection

- Coffee machines using a Wi-Fi connection will connect the same way as a portable computer or a mobile phone.
- The coffee machine uses a **TCP/IP** protocol to connect to the router. To obtain an IP address, the **DHCP** of the machine is set to **Dynamic allocation**. For security purposes, it is impossible to set this parameter other than **Dynamic**.
- Once the internet connection is established, the machine sends a signal to Evoca North America's server to indicate that it is now online. Evoca North America's server then sends an acknowledgement to the coffee machine to confirm that the link between them is established. Every 5 minutes, an acknowledgement is sent to validate the connection.
- When a user makes a request from Sophia via the online application, the server asks the coffee machine to provide him the data of the requested file (e.g.: recipe).
- The coffee machine then converts the file into a string and sends it to the server.
- The Sophia online application finally re-converts this string to viewable data.

Whether your brewer is connected to the cellular or Wi-Fi network, these security features guarantee Evoca North America will not be able to access your server or your data.

**Cellular modem is optional on some models.*

A Short Glossary of Terminology

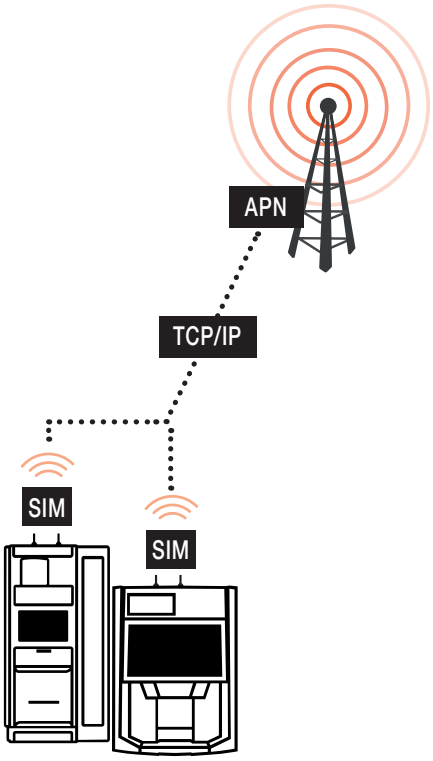
Network Communications

APN - Access Point Network

Imagine that each cellular tower has 2 doors. 1 door is used to go on public internet, the other one opens to a private tunnel (VPN).

Evoca North America have its own Access Point/door.

Each coffee machine has the key to pass through the Evoca North America door, but this door only.



DHCP - Dynamic Host Configuration Protocol

It's a network management protocol that automatically set configuration parameters. Basically, it makes it possible for the brewers to connect to the cellular network by assigning them temporary IP addresses.

Dynamic Allocation

This DHCP allocation method assigns a temporary IP address. When your brewer needs to connect to the network, it gets assigned an IP address for a limited period of time to ensure the privacy of the data.

SIM Card - Subscriber Identification Module

A SIM card is used by the modem to get the authorization to connect to a cellular tower. It needs to be activated in order to transmit data over a network.

TCP/IP - Transmission Control Protocol / Internet Protocol

Communication protocol used by the coffee machine to transfer data with the server.

Security

Encryption

Process of encoding a message or information in such a way that only authorized parties can access it, and those who are not authorized cannot. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.

One-Way Hash

Encryption cryptographic function which is practically unfeasible to invert.

MPLS VPN - Multiprotocol Label Switching

Virtual Private Network

Private tunnel between 2 points, creating a private network.

In our case, we have a VPN tunnel between the cellular network providers and the Evoca North America server.

On our network, every machine has a VPN path leading to our server. The brewer runs a small software opening the tunnel, all communications going exclusively through it.