EVOKO LISO & EVOKO HOME

SECURITY WHITE PAPER

Version v1.0 February 2018

Evoko Liso & Evoko Home Security

Evoko's room booking have been used worldwide since 2010 in many industries where security is of the highest level. This list includes governments, banks and defence contractors. Security is a top priority for Evoko and Evoko Liso / Evoko Home have been specifically developed to be a highly secure, enterprise grade solution, following the best global security practices and guidelines.

As part of our security process, we have also had external experts perform penetration testing on some of the early releases of our software. These tests include a 360-degree assessment of all components included in the solution, and the following steps;

- Attack Surface Mapping
- Embedded Device testing
- Firmware Reverse Engineering and analysis
- Web, Mobile and Cloud endpoints assessment
- Radio communication security assessment

We do not share our PEN-test reports as the testers we use (unlike a hacker) have had access to the actual source code. This is for our internal use only and is considered sensitive and proprietary information that is not shared. We can however share the findings and general comments on the Evoko Liso & Evoko Home:

As an example, during 2017, we identified issues through our regular reviews of our software that were immediately investigated and addressed. With the ever-changing threat landscape, building and maintaining a system with the highest security demands is an ongoing process. New attack vectors and tools are invented by hackers all the time. To ensure the most robust cyber-attack resilience, we have alongside our internal testing processes, engaged an independent company to carry out security reviews on new software releases and to regularly review in-site hardware installations to ensure ongoing compliance with our security requirements. These tests not only simulate real-world installations but, to ensure the highest levels of security, they go even further. With access to all source code, they are able to search for vulnerabilities and variations that wouldn't be available to a regular hacker. Every new software release improves security further, and in the current release (version 1.35) all confirmed security concerns have been addressed.

System architecture and security summary

Definitions

- Evoko Liso: The room manager device mounted outside the meeting rooms
- Evoko Home: The server application used to connect to the booking system and manage the Liso devices
- Booking system: The platform used for booking meetings. Compatible booking systems are Microsoft Office 365, Exchange 2016/2013/2010, IBM/Lotus Domino and Google G Suite.

System overview

The Evoko room booking system consists of Evoko Liso devices that are installed outside the meeting rooms, and the Evoko Home application which connects to the booking system and is used to manage the Liso devices

Evoko Home can be installed as a service in the company network, on-premises or in the cloud, which enables several features like user management, statistics and remote management of the Liso devices (default mode). This is the recommended installation mode and is required to access the systems full functionality.

Optionally, you can manage the Liso devices manually by installing Evoko Home on a desktop where you set up the configuration and transfer it with a USB stick to the devices (limited mode).

Figure 1: System architecture Default mode

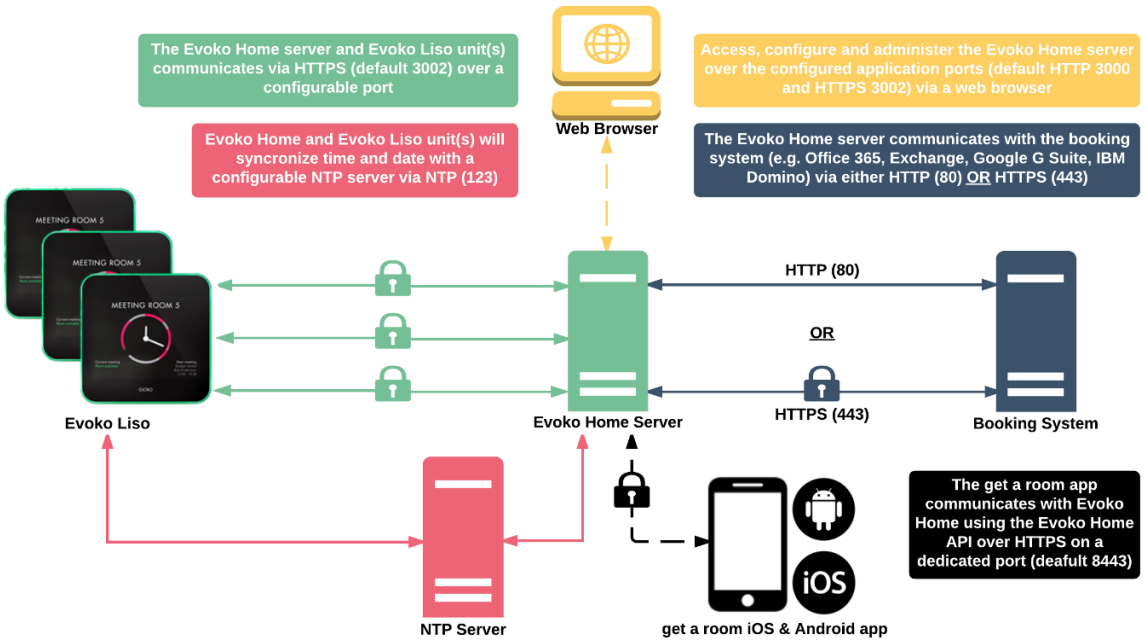
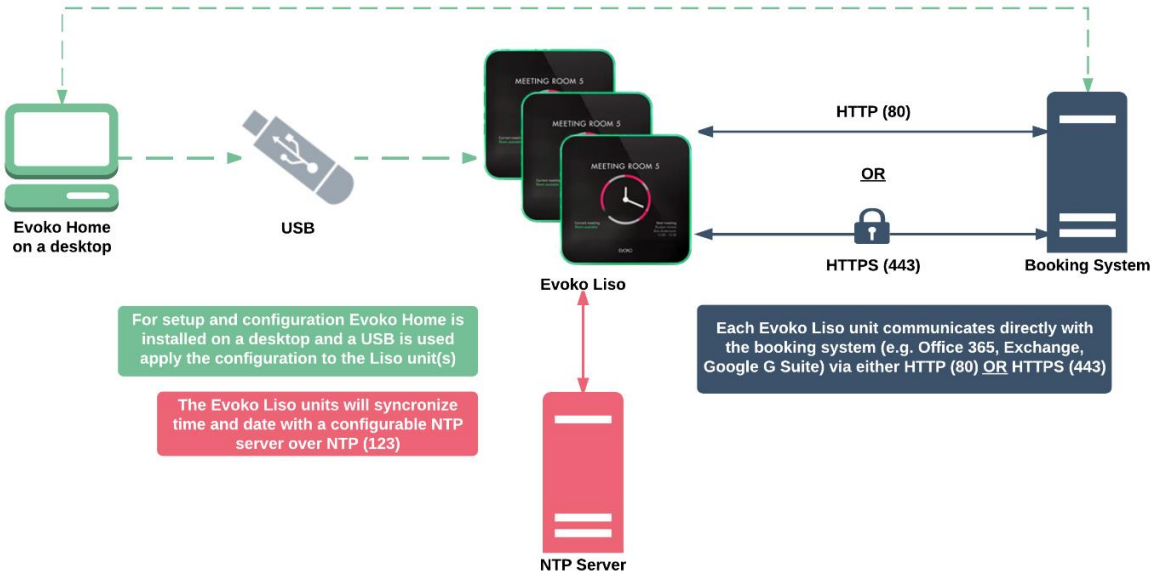


Figure 2: System architecture Limited mode



Security summary

The Evoko Home only uses network and/or Internet to communicate with the native Email Server API (EWS, Google API or other protocol depending on server type). Only secured (https) connections are recommended and since Evoko Home is running on a server the level of encryption and security can be as high as required and updated if these requirements change in the future.

The Evoko Liso devices always boot directly into the application. From within the application, there is no way to leave. As administrator, you are granted limited access to USB, export logs and installing signed firmware images. It is also possible to boot the devices from a special bootable firmware image available. This bootable USB will reset the device and require it to be reconfigured by an administrator before it can connect to Evoko Home again.

For added security, you can set up the Evoko Liso installation as a VLAN (i.e. having the units on a separate network with restricted access).

One of the key architectural benefits with our system is that it plugs into our customers' existing infrastructure. It requires no end user software plug-ins.

Evoko Home securely communicates directly with the **Calendar Service** (Microsoft Exchange 2010 or later, MS Office 365 or Google Apps for Business, IBM Domino etc.) and only accesses information that is needed to display meeting room occupied/available status and meeting details for the meeting rooms. Access to the Calendar Service requires the system to store credentials of a sufficient level to access this information, but these credentials are only stored on the Evoko Home server and not on the actual devices.

The data pushed to the devices is limited to include only the data that is actually going to be displayed on the screen, so the risk of sensitive data being eavesdropped or extracted from the device is effectively removed. The meeting data is stored in the RAM memory of the devices making sure that a stolen unit does not include any retrievable data.

The units plug into the network using Ethernet cables and can be powered using Power over Ethernet (PoE) or by a separate power adapter.

Our three-layer architecture:

- Presentation layer:
    - This is the graphical user interface of our application that shows information and takes input from users.
- Business logic:
    - We process input from the presentation & data layers and update each layer as required.
- Data layer:
    - We have a data layer that resides in Evoko Home outside the actual device. All data is maintained on the Calendar Service. We send requests to read data and to update data. For business-critical data the Calendar System is the "master" which makes the Evoko Home data layer less sensitive. Any data corruption or loss of meeting data would be read back automatically from the Calendar System.

On first installation, the devices need to be pointed towards a configured Evoko Home server and if added security is configured, a customer selected security PIN must also be provided. Not until being authenticated as an Evoko Liso device and with the correct security PIN, will Evoko Home provide the device with a list of rooms so that the installer can associate the device with the correct room.

Any attempt to load malicious firmware on the device will result in loss of connection with Evoko Home. To re-establish it, both server address and security PIN is required or the device will show as "Not Approved" in the device monitoring section.

Evoko Home device manager, is used to assign each device to a resource account in the integrated system and provide the credentials required for the devices to connect to the existing email server. The configuration also includes letting the device know which integrated system it's going to talk to (Exchange, Office 365, Google Apps, IBM Domino), where to access it (server URL) and if http or https should be used.

The Evoko Liso devices then connects to the integrated system based on this information.

Meeting information is pulled from the integrated system and is then displayed on the screen and if a new meeting is booked or an existing meeting is altered on the Evoko Liso device screen this information is sent directly to the integrated system as a request. If that request is approved and a response is given to the Evoko Liso device, it will update accordingly.

The Evoko Liso device always reflects live data on the email server. In summary, in the current release (version 1.35) all confirmed security concerns have been addressed and security will always be a primary concern for us.

Impersonation

Having the Evoko service account granted with Application Impersonation permission is a requirement to successfully integrate Evoko Liso with your Exchange / Office 365 environment.

We use impersonation, instead of delegation, as it has many key advantages, e.g. reducing the number of concurrent connections to the mail server, reducing the load on the network and enabling a more "real time" experience.

Just like with any permissions granted it needs to be configured in a responsible way. Allowing impersonation for all users in the organization ("global impersonation") is not recommended, but for the Evoko Liso to work, impersonation only need to be allowed for the rooms/resources, thereby eliminating the security concerns sometimes associated with impersonation.

Please find more information about impersonation vs. delegation here and impersonation here.

Communication ports

Evoko Home:

- Port 443: Communication with Calendar service: Encryption depends on configuration of calendar system
- Port 3002: Communication with Devices: TLS 1.2
- Port 3000: First time configuration: No encryption, recommended to do as "localhost" on the server Evoko Home gets installed on.

Evoko Liso:

- Port 3002: Communication with Evoko Home: Encryption
- Port 123: Optional NTP time sync: No encryption

Additional security measures/info:

- USB HID block
- Custom soft-keyboard to prevent keyboard escape sequences
- Kiosk mode – not possible to leave application or reach other parts of the system.
- PIN protected admin section (4-9 digits)
- Customer configurable "Secure key" to pair devices with Evoko Home
- RAM based meeting data storage, if removed from the wall all meeting data is lost.
- Signed boot and kernel image.
- Port blocking – all ports not used by the device are closed
- Dynamic SSL certificate generation for customers that don't have custom certificates
- Only high strength Ciphers allowed
- Secured distribution of upgrades and updates
- Basic 802.1X support (beta)