Anforderungen Axing Authentification Server
Requirements Axing authentification server

AXING AG
Gewerbehaus Moskau
8262 Ramsen
Switzerland

Beschreibung | Description

Dieses Dokument beschreibt die Anforderungen und den Aufbau eines „Axing Authentification Servers". Mithilfe dieser Anwendung werden mobile Geräte der Gäste mit dem Chromecast Gerät der Einrichtung vernetzt. Auf dem Middleware Server läuft eine „Authentification Server Applikation" die auf alle WLAN-Access-Points (APs) in dem Projekt verweisen muss. Dazu müssen die APs das IEEE 802.1X Authentifizierungsverfahren unterstützen.

Im gesamten Projekt muss ein WLAN mit dem IEEE 802.1X Standard ausgerollt werden. Zusätzlich benötigt jeder Google Chromecast **ein verstecktes, virtuelles WLAN** in einem **eigenen VLAN** (dies ist nötig, da der Google Chromecast kein IEEE 802.1X unterstützt). So kann ein AP, der 8 WLANs verarbeiten kann, wie folgt konfiguriert werden:

- Gäste WLAN (IEEE 802.1X VLAN 1)
- Raum 101 (verstecktes WLAN verbunden mit dem Chromecast im Zimmer und auf VLAN 101)
- Raum 102 (verstecktes WLAN verbunden mit dem Chromecast im Zimmer und auf VLAN 102)
- Raum 103 (verstecktes WLAN verbunden mit dem Chromecast im Zimmer und auf VLAN 103)
- Raum 104 (verstecktes WLAN verbunden mit dem Chromecast im Zimmer und auf VLAN 104)
- Raum 105 (verstecktes WLAN verbunden mit dem Chromecast im Zimmer und auf VLAN 105)
- Raum 106 (verstecktes WLAN verbunden mit dem Chromecast im Zimmer und auf VLAN 106)
- Raum 107 (verstecktes WLAN verbunden mit dem Chromecast im Zimmer und auf VLAN 107)

Durch den IEEE 802.1X Standard, ist es uns möglich, dynamisch dem Kunden ein VLAN und ein intern generiertes Passwort zuzuweisen. Dies macht die Middleware automatisch, wenn ein Gast eincheckt. Checkt der Kunde aus, wird das WLAN-Passwort geändert, sodass wenn der Kunde in ein paar Tagen wieder im Hotel ist, sich nicht mehr automatisch mit dem WLAN verbindet, sondern den neu generierten QR-Code scannen muss, um sich erneut zu verbinden.

This document describes the requirements and structure of an Axing authentification server. With the help of this application, mobile devices of the guests are linked with the Chromecast device of the facility. The middleware server runs a "authentification server application" which must refer to all WiFi access points (APs) in the project. The APs must support the IEEE 802.1X authentication procedure.

In the entire project, WiFi must be rolled out with the IEEE 802.1X standard. In addition, each Google Chromecast requires a hidden, virtual WiFi in its own VLAN (this is necessary because the Chromecast does not support IEEE 802.1X). An access point of the 8 WiFi can be configured as follows:

- • Guest WiFi (IEEE 802.1X VLAN 1)
- • Room 101 (hidden WiFi connected to the Chromecast in the room and on VLAN 101)
- • Room 102 (hidden WiFi connected to the Chromecast in the room and on VLAN 102)
- • Room 103 (hidden WiFi connected to the Chromecast in the room and on VLAN 103)
- • Room 104 (hidden WiFi connected to the Chromecast in the room and on VLAN 104)
- • Room 105 (hidden WiFi connected to the Chromecast in the room and on VLAN 105)
- • Room 106 (hidden WiFi connected to the Chromecast in the room and on VLAN 106)
- • Room 107 (hidden WiFi connected to the Chromecast in the room and on VLAN 107)

The IEEE 802.1X standard allows us to dynamically assign a VLAN and an internally generated password to the customer. This makes the middleware automatic when a guest checks in. If the customer checks out, the Wi-Fi password is changed so that when the customer is back in the hotel in a few days, he no longer automatically connects to the Wi-Fi, but has to scan the newly generated QR code in order to reconnect.

Anforderungen Axing Authentification Server
Requirements Axing authentification server

AXING AG
Gewerbehaus Moskau
8262 Ramsen
Switzerland

Anwendungsseitige Funktion | Application side function

Der Anwender wählt im Frontend der Middleware einfach die Chromecast Funktion aus. Dort sieht er ein Fenster mit kurzer Anleitung und einen QR-Code, der das Passwort darstellt. Wenn er diesen scannt, wird er mit dem Netzwerk verbunden. Nach Bestätigung über den „OK"-Button auf der Fernbedienung wird zum Chromecast weitergeleitet.

The user simply selects the Chromecast function in the Frontend of the middleware. There he sees a window with short instructions and a QR code that represents the password. When it scans this, it is connected to the network. After confirming via the OK" button on the remote control is forwarded to the Chromecast.