April 24, 2019

COLLABORATION APPLICATION PROXIMITY BASED GUEST WIRELESS ACCESS PROVISIONING

Adam Schaeffer

Jason Beltrame

Christopher Bogdon

COLLABORATION APPLICATION PROXIMITY BASED GUEST WIRELESS ACCESS PROVISIONING

AUTHORS:
Adam Schaeffer
Jason Beltrame
Christopher Bogdon

ABSTRACT

Techniques are described herein to consolidate existing technologies to allow end and guest users to rapidly self-provision wireless network access via a collaboration application. The users may obtain their own guest wireless credentials before starting to work. The process automatically learns a valid email address for the user through the collaboration application and a wireless connection. The users selects a "provision" option (e.g., button) on a video endpoint, which pushes identity information to the collaboration application to ultimately configure the user. The user obtains the credential details in the collaboration application only seconds later. Through backend configuration, content and network limits are in place based on the domain or user.

DETAILED DESCRIPTION

Provisioning accounts for guest wireless access is typically a manual and time-consuming process. Because of this, self-provisioning processes that are handled by the user can be very cumbersome. More often than not, generic accounts are created and shared rather than per-user accounts, which leads to a user experience that is not user friendly or consistent. In addition, a person, such as a lobby ambassador or a receptionist, is sometimes hired to create guest wireless accounts. Some customers choose to use Open wireless as a solution, but this method is insecure and there is no record of accountability.

Advances in identity solutions and wireless networks have simplified the process of onboarding guests onto a network. However, customers still experience pain points when adding users. For example, creating the guest account requires manual intervention, e.g., from a lobby ambassador or guest sponsor. Some customers are unable to open a captive portal due to customer restrictions, which makes it impossible to log onto the network. Moreover, once a user has been successfully onboarded, the host company has

little visibility of what the user has been doing. User frustration can lead to use of hotspots or cell phones for accessing networks.

These are just some of the problems that are associated with onboarding guest users. Contractor access is even more problematic. Contractors are on-site so infrequently that Information Technology (IT) departments often have to re-enable contractor credentials at each visit. Even worse, IT departments attempt to avoid this by giving the contractor an account with credentials permanently enabled (e.g., no password 60- or 90-day age restrictions). These problems are further exacerbated when the number of guest users increase (e.g., at a customer trade show with thousands of guest or contractor users).

As described herein, the increase of technological features enables an improved solution to provide better provisioning as well as increase the control and accountability system-wide. One example is based upon wireless connection and collaboration application features. This solution allows endpoints to dynamically detect devices and users that are in range. The wireless connection feature may serve as the backbone of this onboarding solution. The solution may automatically detect guest or contractor users and, based on their identity information, begin to onboard the user onto the network. An identity service, which is a powerful policy platform with an open Application Programming Interface (API) may also be used. The identity service may have platform exchange capabilities that enable control and policy in many different environments. To provide visibility, a secure Internet gateway may be leveraged to monitor and track user activity. With these features, customers may enjoy a more streamlined workflow to bring on new users.

This solution may be deployed in many different use cases, such as conference rooms, kiosks, and registration areas. For example, when guest users enter a conference room, they may be automatically onboarded as users on the network. Similarly, users can walk up to kiosks and automatically be onboarded onto the network. In one example, the kiosk may initially identify the user if the user has a smart phone that contains the user identity. Also, instead of registering for services by entering identification information (e.g., social security numbers) this onboarding feature may be used to quickly register these users with the capabilities built into their mobile devices. For example, the solution simplifies

the process of passing information back and forth between a user and the company representative when the user attempts to register with guest Wi-Fi®.

Figure 1 below illustrates the overall architecture of the solution.

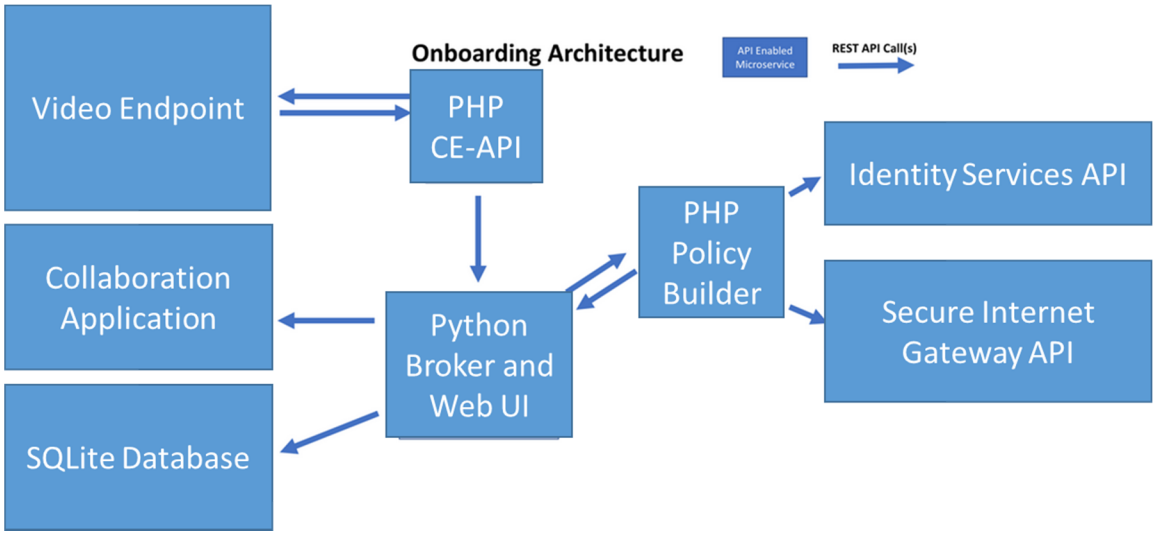

Figure 1

The architecture is built around a microservices framework to demonstrate how multiple solutions can work together provided there is a well-defined API. There are three main modules in the solution: Customer Edge API (CE-API), broker, and guest-update.

The CE-API module listens for provisioning requests from video endpoints. When the "Network Registration" option is selected, the endpoint sends a HyperText Transfer Protocol (HTTP) feedback request to the CE-API module. This service then requests the broker to provision the account. The CE-API module may perform the following functions. First, the CE-API module listens for HTTP feedback requests. Second, the CE-API module validates and receives requests. Third, the CE-API module sends a pop-up confirmation back to the video endpoint. Fourth, when the user confirms he/she would like an account provisioned, the CE-API module makes a call to the broker to have the request processed. Fifth, a confirmation message is sent to the video endpoint so the user knows the process is underway.

The broker is responsible for receiving requests from the CE-API module to provision guest users. It uses a database to whitelist both video endpoints and email domains to provide a very simple security mechanism. The broker may perform the following functions. First, the broker waits for requests from the CE-API module to

provision a user. Second, the broker validates any received requests against the security whitelist database. Third, the broker stores the requests in an internal database for later tracking. Fourth, the broker leverages the Representational State Transfer (REST) API to initiate the actual provisioning process with the guest-update module. Fifth, the broker waits for a response from the guest-update module for a Wi-Fi password. Sixth, the broker provides status updates to the end user in a room of the collaboration application.

The guest-update module is responsible for receiving user requests from the broker to provision guest users within the identity service. It uses various identity service APIs to validate and create users. The guest-update module may perform the following functions. First, the guest-update module waits for requests from the broker to provision a user within the identity services guest database. Second, the guest-update module checks whether the user is already there. If not, the guest-update module provisions the new user. If the user already exists, the guest-update module re-activates the account and reset the password. In either case, third, the guest-update module sends an update back to the broker with a status of "complete" as well as the current password. Fourth, the infrastructure itself (identity services, Wireless Local Area Network (LAN) Controller (WLC), and secure Internet gateway) are set up and integrated with APIs to allow for dynamic policies based on the company associated with the user.

An overall example process is described as follows. First, a guest users opens the collaboration application on his/her mobile device in the presence of a video endpoint configured as a self-registration kiosk. A wireless connection relationship is established between the user mobile device and the video endpoint. This relationship enables the kiosk to determine the identity of the user as well as the user email address. This information is presented on the kiosk, and the guest user selects the "self-provision" option. The guest user receives an option to confirm the request, and at the time the user selects the confirmation option, a request is sent to the provisioning application.

The provisioning application may collect a collaboration application identifier from a collaboration service cloud API. The results include an email address for the user account. The email address may serve as the user name. If the user is not authorized for guest access based upon the whitelist database, a message will be sent back to deny the registration. If the user is authorized, a random password is generated by the application, and the username,

password, and details for connecting are sent to the user through the collaboration application which is encrypted in transit and at rest. The user may then retain this information for the length of the visit to the network. At the end of the lifetime of the account, the system may de-provision the user and potentially generate a report of his/her usage should the administrator desire.

Figure 2 below illustrates an example flowchart.

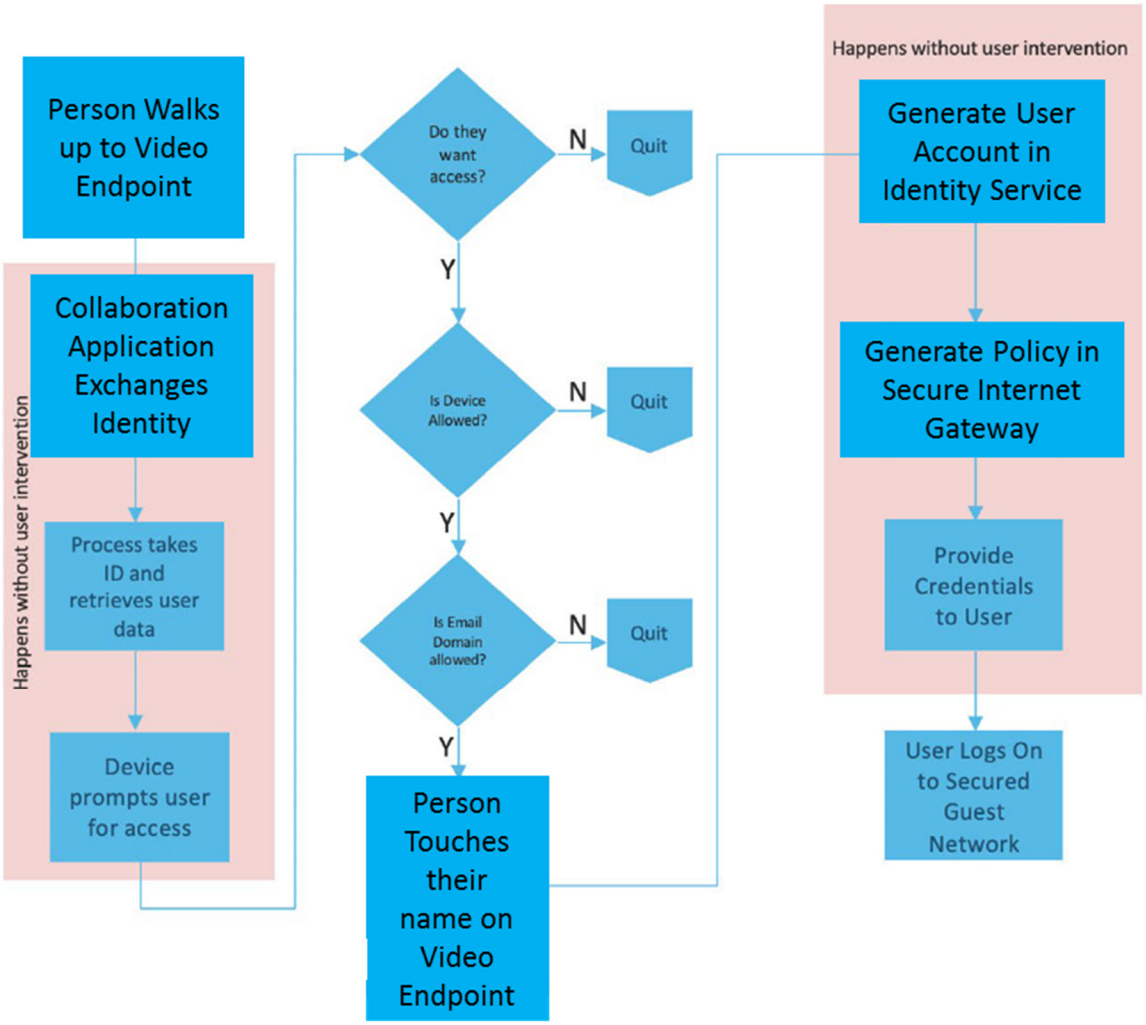

Figure 2

The techniques described herein improve the process of joining wireless networks by leveraging options for user identification other than, for example, the last name and room number of the user. For example, the collaboration application may be installed on a smart phone and communicate wirelessly to share the identity of the user. The solution is also generic enough to leverage other mechanisms for identification such as Bluetooth®,

Radio-Frequency Identification (RFID), Near-Field Communication (NFC), Bluetooth Low Energy (BLE), Intelligent Proximity™, etc. The solution reduces the steps necessary for identification and allows the network to automatically determine user identity.

Also, provisioning operations may be performed in examples other than guest Wi-Fi. For example, the solution may be extended to automatically check in to flights from an airport kiosk without entering flight number or credit card information. Instead, the device (e.g., phone) may provide user information when in presence of the kiosk. Once the user's identity is determined, the kiosk may automatically look up information based on that identity and proceed with next steps. In this example, the wireless connection capability may be built into the airline application, which is residing on the smart phone. Therefore, the kiosk may obtain the user identity when in close proximity to the kiosk.

Described herein is a self-service provisioning process that greatly reduces time and key strokes required to join a network. The self-provisioning process results provides the administrator with a higher level of confidence and visibility into which users have joined the network. Because the user is already authenticated to the collaboration application via his/her email address, the user's claim to that identity may be more trusted, thereby improving monitoring and compliance enforcement. Furthermore, this requires no printed or written name tags with guest credentials thereon. This is both environmentally-friendly and more secure.

In summary, techniques are described herein to consolidate existing technologies to allow end and guest users to rapidly self-provision via a collaboration application. The users may obtain their own guest wireless credentials before starting to work. The process obtains a valid email address for the user through the collaboration application and a wireless connection. The users selects a "provision" option (e.g., button) on a lobby video endpoint, which pushes information to the collaboration application to ultimately configure the user. The user obtains the credential details in the collaboration application only seconds later. Through backend configuration, content and network limits are in place based on the domain or user.