



The Power of We™



Guest Access

Avaya-on-Avaya Delivering secure guest access instantly

The scenario sounds familiar, and has been repeated hundreds of times. It is frustrating. It is inhibiting, and, in the age of great consumer cloud experiences, it seems unbelievable.

The Scenario

Imagine you are a visitor at a client or vendor's location. You boot up the laptop, open your application, and then remember that you need a file that was just sent by a colleague. Your heart sinks knowing that you need wi-fi access to retrieve the email. You ask your host the dreaded question. She replies with a sigh and says, "Well, you need to go talk to Robert - he has the latest password to the wi-fi network." Dragging your feet you make your way to Robert's cube...

Robert's view

Robert has his own dilemma to deal with. He has been bound by his IT management to be a sentinel against rogue users on the Wi-Fi network. He guards the network with sword in hand. He routinely gets complaints from employees and guests alike. He chooses to err on the side of security and sacrifice ease of user access.

Avaya felt the pain

Avaya found itself in a similar situation when visitors to their Executive Briefing Centers had difficulty connecting to the Avaya network. For a company that sells productivity solutions, the situation had to change.

It starts with identity

Avaya had merged with a company that had a product called, Identity Engines. As the IT staff started to understand the capabilities of Identity Engines, it became clear that this product was not just for wireless access, but was really a solution for universal network access.

The solution starts at the point of network access and ends when the user is connected to the portion of the network that the IT policies deem appropriate for them. It enables unlimited policy creation, is corporate database friendly, and is easy to configure.

How it was done

Using the Identity Engines interface, the IT staff did the following to get the solution going:

- Created a new profile called, "Guest" and assigned access policies against the profile. The profile included internet access only for a period of eight hours.
- There were two options to consider: Visitor Self-service access and Visitor Sponsored access.
- With Visitor Self-service access, the IT staff set up a simple web page that would pop up when a user connects to the corporate Guest@Avaya SSID. The

Now, instead of chasing a person down to get network access, the guest can do it themselves in less than 10 seconds.

visitor then creates an account by completing a short form with his or her email address or cellphone number. The access credentials are immediately sent to the visitor's smartphone either via email or SMS over the cellular network.

- The visitor then logs in with the credentials and gains access to the Internet.
- In parallel, Identity Engines automatically creates a record with the visitor's information and device fingerprint that may be needed for any future audit. The whole cycle is completed less than 10 seconds, and is IT hands-free with full audit logging for compliance.
- With Sponsored Visitor access, either an Avaya employee or front desk personnel creates a guest account for the visitor for those cases where visitors from other countries may not have SMS roaming plans.

From “how it goes” to “how it went”

Instead of what happened in the opening scenario, now when customers and guests visit the Avaya Santa Clara, Basking Ridge, Westminster, New York and Boston facilities this is their experience:

1. Upon clicking on the corporate SSID, the guest requests access by providing their name and mobile number (or email address).
2. The guest receives a password immediately via text (or email).
3. The guest enters the password and gains access to the internet.

This process has now been repeated thousands of times. With this experience in hand, Avaya has measured the time from access request to network access. The results are a great improvement. Now, instead of chasing a person down to get network access, the guest can do it themselves in less than 10 seconds.

The solution

The Avaya Identity Engines portfolio provides a complete integrated solution for managing network guest user access. This guest management solution consists of the following integrated components:

- The Identity Engines Ignition Server — a centralized network access control solution
- The Identity Engines Ignition Guest Manager — an administrative application for guest user management
- The Identity Engines Ignition Compliance Portal — Web authentication, fingerprinting and compliance portal for handling non-802.1X clients

Conclusion

Guest access to network services has become an essential part of today's business environment. User experience with cloud-based networks has set the bar for ease of use. The Avaya Identity Engines portfolio provides fast network access to guests and visitors without compromising the overall security of the enterprise network.

About Avaya

Avaya is a global provider of business collaboration and communications solutions, providing unified communications, contact centers, networking and related services to companies of all sizes around the world. For more information please visit www.avaya.com.

