



Engage The Power of We™

Avaya idEngines® Ignition® Guest Manager

IT Hands-Free Auditable Guest Access in under 10 seconds

Visitors, customers, business partners, suppliers, temporary workers and a variety of professionals who come into your office to do business now expect you to offer access to your network. However, granting guests access poses security risks. Also, you need to consider the many associated costs, including provisioning, managing and auditing guest accounts.

The Avaya Identity Engines Ignition® Guest Manager allows you to provide more secure network access to your guests — easily and cost-effectively — without taxing IT administrators.

Meeting the challenges of secure guest access

The Ignition® Guest Manager is the leading guest management solution for more secure network access. The solution manages guest and visitor network access across wired and wireless access points, and it enables you to apply granular authorization policies to limit guests' access strictly to permitted network resources.

The solution reduces the demand on IT departments because it's easily administered by front desk personnel or any employee tasked with being a guest "sponsor."

Delegated administration — Guest access is managed using an intuitive, web-based interface that can be easily customized to meet the needs of each organization. An integrated rules engine guarantees user accounts automatically expire at a scheduled time and date.

IT administrators can delegate guest account sponsorship duties to front desk personnel or any other employee. Sponsor accounts are stored on the Avaya Identity Engines Ignition® Server or in an Active Directory or LDAP store while guest accounts are always stored only in the Identity Engines local store.

Delegated administration rules can ensure that each elected sponsor can create guest accounts with only those rights for which the sponsor has authority. New sponsor workflow enables visitors to register themselves using the self-service guest template. A delegated employee receives an e-mail to approve or deny guest.

Improved productivity — A self-provisioning feature offers organizations the ability to have guests provision their own wireless access at a kiosk or online portal. This cost-saving feature allows, for example, conference attendees or school visitors to obtain more secure, authenticated access without requiring the participation of administrative staff. The system can be configured for increased security and audit tracking. The Ignition® Guest Manager can host multiple self-provisioning kiosks simultaneously, each with different privileges, such as access zones and duration. Each can offer different display characteristics and branding.

Stronger security — With SMS integration, organizations can send login credentials to a guest's cell phone. When a visitor registers at a kiosk or online portal, the Ignition® Guest Manager automatically sends a password to the visitor's cell phone or other mobile device. Security is improved because the required credentials are hard to spoof. Only the visitor is privy to the password, and an auditable link between the visitor and the network is created.

Policy enforcement — The Ignition® Guest Manager assigns network access rights and permissions based on a guest's role or relationship to the organization, based on where they are connecting from (conference rooms, labs, lobbies, etc.), and based on how they connect (wireless, wired, VPN). Guests can be provisioned with access to



Identity Engines Guest Manager

More Secure and
Simpler way to
address guest access:

- Provision Guests in under 10 seconds
- Self-Service Kiosk
- Sponsored Guest Access
- Detailed tracking and auditing
- Unified guest access for wired & wireless
- IT hands-free Guest Access
- Delivered as a Virtual Appliance for ESXi
- VMWare vMotion friendly
- Localized for 8 languages
- REST APIs for provisioning of users/devices by 3rd party apps
- Smartphone App for device registration

Avaya Identity Engines Portfolio

The Identity Engines Guest Manager is part of the Avaya Identity Engines portfolio—a comprehensive set of software products designed to interwork and simplify network identity and access management, including Bring Your Own Device (BYOD) and guest access policies. The portfolio includes:

- Ignition® Server
- Ignition® Guest Manager
- Ignition® Access Portal
- Ignition® CASE Wizard
- Ignition® Analytics
- Ignition® AURA® Single Sign On

The Avaya Identity Engines portfolio integrates with any vendor's networking equipment to provide the central policy decisions needed to enforce role-based network access control while supporting federated identity management across all major corporate directories, e.g., Microsoft Active Directory, LDAP, RSA Authentication Server and more.

About Avaya

Avaya is a leading, global provider of customer and team engagement solutions and services available in a variety of flexible on-premise and cloud deployment options. Avaya's fabric-based networking solutions help simplify and accelerate the deployment of business critical applications and services. For more information, please visit www.avaya.com.

particular subnets or VLANs, or you may limit them to outbound web access only. The Ignition® Guest Manager also allows the network administrator to specify precisely which devices a user may use to log in.

Auditing and logging — The Ignition® Guest Manager records a detailed audit trail of network access for each user. It also tracks the actions of the sponsors who create guest accounts to help detect and identify excessive account generation or inappropriately provisioned accounts.

Conclusion

Offering guests access to your network services is essential. Today, the Avaya Identity Engines Ignition® Guest Manager enables organizations to more securely provide network access to guests and visitors without compromising the security of the network. To reduce the burden on IT professionals, the solution can be easily executed by anyone empowered to sponsor network access for guests.

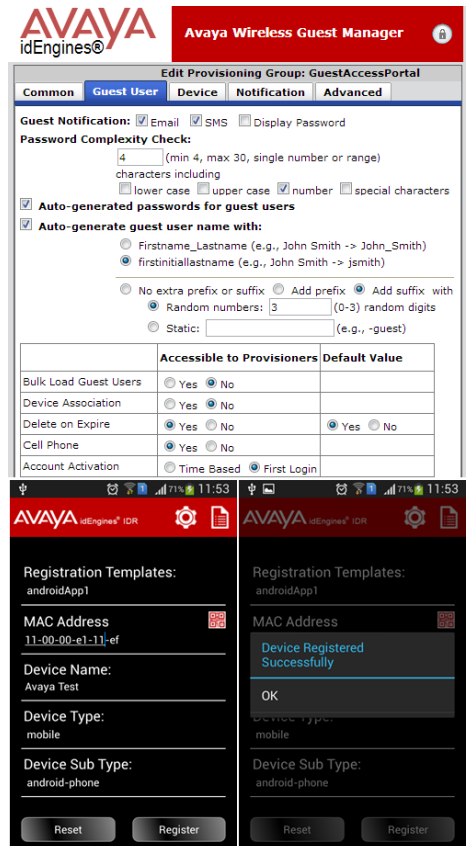


Figure 1: Identity Engines Guest Manager

Key features

- **Fast and Intuitive** — Provision guest accounts in less than 10 seconds.
- **Centralized access control** — Manages guest authentication and access across wired and wireless networks.
- **Delegated provisioning** — Delegated provisioning lets designated greeters create and manage guest user accounts.
- **Self-Service** — Allows guests to provision their own temporary accounts from kiosks or an online portal quickly and easily. Mobile friendly self-service page.
- **Auditing** — Centralized log data enables detailed reporting of guest access.
- **Bulk loading** — Rapidly configures hundreds or thousands of guest accounts from database records.
- **Policy driven** — Network access rights and permissions are assigned based on guest's role in or relationship to the organization, location, time of day, user device and other attributes.
- **SMS integration** — Sends guest login credentials to the user's cell phone, allowing the use of hard-to-spoof guest identifiers.
- **Automatic account termination** — Discontinues guest access rights at a scheduled date and time.
- **Local Database** — Guest Accounts stored in the local store to segregate guest information from enterprise directories.
- **Vendor Agnostic Solution** — Easy to deploy over any vendor's wired or wireless network.
- **Smartphone Application** — For fast and easy device registration.
- **REST APIs** — for programmatic provisioning of Users and Devices by 3rd party applications.

