Identity Engines Access Portal

Simplifying how employees and guests authenticate and connect to the network:

- Supports network access for BYOD devices while keeping you in control
- Unifies access for both wired and wireless networks
- No special client-side software needed
- Enables non 802.1x device access to the network in a controlled fashion
- Device fingerprinting
- Manages access for employees, business partners and guests
- A solution for BYOD on-boarding
- CASE Wizard hosting

AVAYA

The Power of We™

Avaya idEngines® Ignition® Access Portal

Visibility and control over BYOD (Bring Your Own Device) Access

The spread of mobile devices across the enterprise is challenging IT departments to achieve higher levels of visibility and control over network access, without limiting the flexibility and value these devices deliver for anytime, anywhere productivity and collaboration.

The Avaya Identity Engines Ignition® Access Portal meets this challenge—it establishes a portal that intercepts traffic from employees and guests, simplifying how devices authenticate and connect to the network while providing new tools to monitor, manage and control the level of access that is provided, including detailed visibility into the profiles of individual devices.

Instead of imposing arbitrary restrictions on mobile solutions, the Ignition® Access Portal enables employees to safely connect a wide range of smartphones and tablets. It's an ideal solution for on-boarding and enterprise-wide management of Bring Your Own Device (BYOD) policies.

With the Access Portal, IT can now easily capture information on a wide range of devices—personal or enterprise-issued—and use the Identity Engines Ignition® Server to make policy decisions and enforce appropriate access levels.

Ignition® Access Portal in Action

- User opens browser and enters corporate or guest account credentials
- User authentication takes place against the Identity Engines Ignition® Server leveraging the Identity Routing capabilities across federated directories
- Upon successful authentication, access is granted
- User device is "fingerprinted" and recorded

Avaya Identity Engines Portfolio

The Identity Engines Ignition® Server 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® Posture
- 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 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**.

The Avaya Access Portal solution requires no special client software. It works across any vendor's wireless or wired network, delivering a unified solution that effectively meets the needs of both users and IT for a simple, centralized approach to managing and controlling network access. A single license allows deployment of multiple Ignition® Access Portals for a range of network access situations.

802.1x Enablement

The Avaya Identity Engines Ignition® Access Portal can authenticate and provide access to:

- User devices that do not have the 802.1x capability
- User devices in which the 802.1x is there, but not configured

In addition to unifying wireless and wired device access, the Ignition® Access Portal manages access for employees with either corporate-issued or personal devices, as well as guest devices.

No Client-side Software Needed

The Ignition® Access Portal establishes a 'captive portal' page. When a user seeks access to the network, the Access Portal intercepts the user traffic until the proper authentication and authorization is met.

On the portal page (which enterprises can customize, for example, with company branding), users can be asked to enter login credentials, agree to terms of service, etc. Taking advantage of the user's browser to prompt for and collect credentials eliminates the need for client side software. User authentication takes place against the Identity Engines Ignition® Server leveraging its identity routing capabilities across federated directories.

Creating Device Fingerprints

The Identity Engines Ignition® Access Portal analyzes user traffic and captures device-specific attributes that make it possible for enterprises to set up comprehensive policies and enforce them using the Identity Engines Ignition® Server. For example, employees may be granted full network access when connecting via a corporate-issued PC, but only restricted network access if they connect via a personal Apple iPad device.

A single license allows deployment of multiple Ignition® Access Portals for different use cases, all against one Ignition® Server instance (or HA-pair).

Learn More

To learn more about the Avaya Ignition® Access Portal and the entire Avaya Identity Engines Portfolio, contact your Avaya Account Manager, Avaya Authorized Partner, or visit us at **www.avaya.com**.

Provide FEEDBACK for this document

10/13 • DN7082-02