avaya.com

Avaya Identity Engines Portfolio

Avaya Identity Engines Portfolio solutions enable businesses to control who accesses a network, when, where, and how the network is accessed, and which devices will be allowed on the network.

IT departments today are faced with a growing challenge: to maintain network security while facilitating access via wired, wireless and VPN networks for employees, contractors, guests and others who may be on or off premise. They're being asked to provide only as much access as each user requires, to ensure that user devices are healthy and in compliance with the chosen security policy, and to provide that access in real time. Managing these demands is a critical element of your success.

An analogy to the use of network access control (NAC) is your experience at an airport. Prior to boarding, you must show your ID to prove that you are indeed who you say you are. Next, you must walk through a metal detector to ensure that you're not bringing anything harmful onto the plane. And finally, based on the ticket you purchased, you'll be allowed access to a particular area of the aircraft.

In much the same way, NAC manages access to the network. It checks your identity against an identity store (Microsoft Active Directory, for example), performs a device health check to make sure your PC doesn't have any viruses or worms, and then, based on your predetermined role, gives you access to only a certain portion of the network.

Avaya introduced this process with its first generation of NAC, and is leveraging advances in technology to deliver enhanced options. The Identity Engines portfolio is Avaya's second generation of NAC, a standards-based solution that will integrate with your existing network infrastructure to provide the central policy decision needed to enforce role-based access.

This portfolio combines the best elements of a next-generation RADIUS/AAA server, the deep directory integration found in application identity offerings with one of the industry's most advanced policy engines to create a NAC solution that provides unprecedented access flexibility without compromising network security.

The Avaya Identity Engines portfolio is standards-based, vendor-agnostic, scalable, easy to use and cost effective. It integrates into your current infrastructure — no need to upgrade, no matter your vendor — supporting heterogeneous networks and delivering investment protection.

The portfolio consists of five products:

- **Identity Engines Ignition Server:** The main component of the portfolio, providing a centralized policy-decision point across all access methods while also supporting multiple directory stores
- **Identity Engines Ignition Compliance Portal:** Clientless health and compliance checking via a captive portal for unmanaged devices to ensure that endpoints comply with the chosen security policy
- **Identity Engines Ignition Posture:** Endpoint health checking for employee/managed devices that is flexible and integrated with the Identity Engines Ignition Server
- **Identity Engines Ignition Guest Manager:** A quick, safe and easy way to let front-desk staff create guest user accounts for access to specific resources for a designated time period
- **Identity Engines Ignition Analytics:** A powerful reporting application with over 25 preconfigured audit, compliance and usage reports

KEY BENEFITS

- **Improved security and granular control:** Secured wireless and guest access, role-based access control and compartmentalization of the network to segment and protect data
- **Reduced costs:** Supports current network infrastructures and identity stores and offers investment protection via a standards-based solution and a VMware virtual appliance
- **Simplicity:** A centralized policy decision (breaking down silos), policy expression in plain language (not tied to technology) and simplified policy creation through virtual groups
- **Regulatory compliance:** Full network visibility and comprehensive reporting and analytics

Avaya Identity Engines portfolio products are robust and easy to use. There's no need to write different policies for each directory; user groups can be taken from multiple active directories and combined to create virtual groups — the tools are provided to make top-notch NAC a breeze.

But what makes the Avaya Identity Engines solution outstanding is its ability to express policies in plain language.

Table 1 shows that if a user is in the "Employee" user group and connects over wireless or wired, the policy engine can identify it — thus providing more flexibility — and the device's posture will be checked. If the device is compliant, the user is granted employee access; if it's non-compliant or if posture information isn't available, the user receives quarantined access.

Similar policies can easily be written for remote employees and guests and can include additional attributes like time of day or day of week.

In addition to its powerful security benefits, the Identity Engines portfolio can improve operational effectiveness by eliminating the need to pre-assign each switch port to specific VLANs, filters, etc., and then, when devices move, manually re-configuring these ports. Because the Identity Engines Ignition Server knows the identity of users and the types of devices attempting to connect to the network, VLANs are dynamically assigned at the time of access. No IT resources are needed to move a device from port to port or VLAN to VLAN. Process simplification like this can significantly reduce operational costs.

Think of the new Avaya Identity Engines portfolio as NAC 2.0 — a more secure, robust, and simpler approach to network access and policy creation, enabling identity information previously gathered to be leveraged. This can reduce costs and protect your investment.

AVAYA IDENTITY ENGINES AUTHENTICATED NETWORK ARCHITECTURE BENEFITS

The Avaya Identity Engines portfolio enables enterprises to:

- Comply with regulatory requirements
- Control who enters the network
- Deliver differentiated access based on user roles
- Provide data privacy and restricted access to applications
- Provide true network protection, preventing data loss and the spread of viruses and worms

Rule name	Rule summary
Employee_local	IF (User.group-member exactly matches [Employees] **AND** (Authenticator. Authenticator Type = Wireless **OR** Authenticator.Authenticator Type = Wired)). THEN **Check Posture Profile** employee_posture_policy. If Compliant Send Outbound Values employee_access If Non-Compliant Remediate Using quarantine_access If Posture Not Available Send Outbound Values quarantine_access
Employee_remote	IF (User.group-member exactly matches [Employees] **AND** Authenticator. Authenticator Type = VPN) THEN **Check Posture Profile** employee_ posture_policy. If Compliant Send Outbound Values employee_access If Non-Compliant Remediate Using restricted_access If Posture Not Available Send Outbound Values restricted_access
Guests	IF (User.group-member does not match [Employees] **AND** System.Time between 8:00 AM and 5:00 PM **AND** Week day is between Monday and Friday) THEN **Check Posture Profile** guest_posture_policy If Compliant Send Outbound Values guest_access If Non-Compliant — Deny If Posture Not Available — Deny **No_VPN** IF (User.group-member does not match [Employees] **AND** Authenticator.Authenticator Type = VPN) THEN Deny

Table 1. Rules

Centralized security

Easy to deploy, the portfolio's policy engine, called the Identity Engines Ignition Server, resides in the data center, providing centralized authentication and authorization for wired, wireless and VPN network devices. It delivers centralized integrated security services for Avaya and third-party Ethernet switching, WLAN and VPN products.

The Ignition Server assigns network access rights and permissions based on a user's role or relationship to the organization, where they connect from (conference rooms, labs, lobbies, etc.), and how they connect (wireless, wired, VPN).

For example, an IT director may apply more rigorous posture checking to users who act

as system administrators, granting those users access to critical network assets, while applying less rigorous checking to other users and granting them access only to the standard corporate network.

Guests, on the other hand, can be provisioned with access to particular subnets or VLANS or limited to outbound web access only, depending on their roles and needs.

The Identity Engines Ignition Guest Manager enables a network administrator to specify which device types are granted access. Identity Engines Ignition Analytics delivers extensive automated reporting enabling IT professionals to be more effective in carrying out compliance, planning and security mandates.

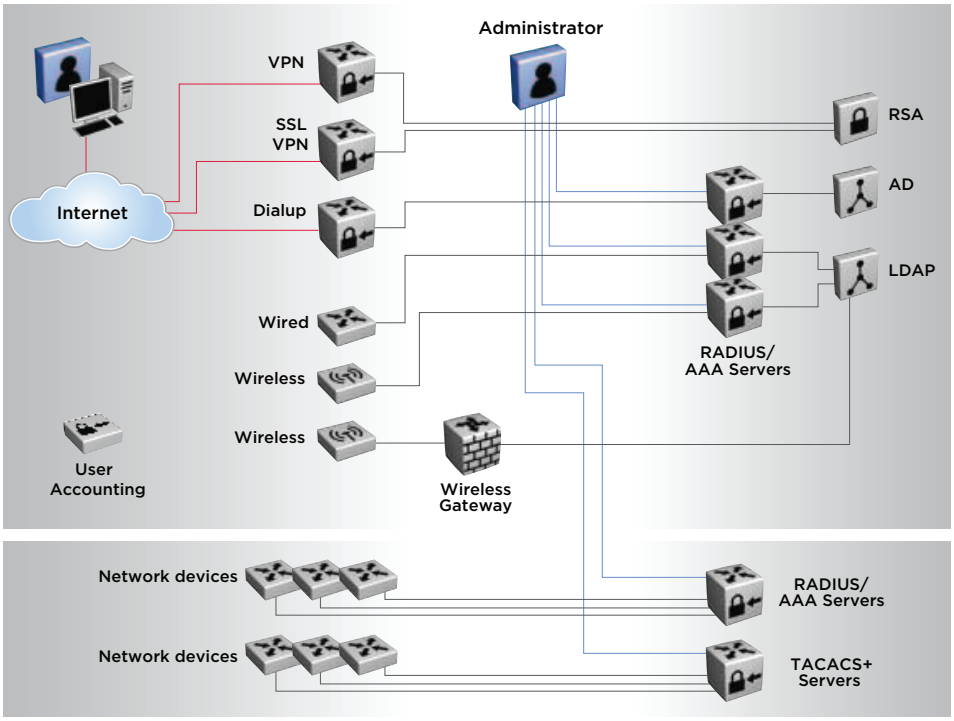

Figure 1. Complex architecture with multiple AAA servers and network overlays

The products

Identity Engines Ignition Server

The Identity Engines Ignition Server is the centerpiece of the Identity Engines portfolio. It is a virtualized standard; no new hardware is required. As most organizations have already invested in VMware environments, the Ignition Server leverages existing investment, saves costs and provides additional deployment flexibility.

The Ignition Server breaks down silos. It simplifies network identity management across the enterprise, enables consistent, centralized access policy, and reduces the potential for administrative error. By putting user information and policy in a single location, policies can be created on a full network-wide basis, supporting LAN, WLAN and VPN consistently.

Offering a new level of accuracy with identity and policy based control, the Ignition Server enables policies to determine who accesses the network, where, when, how and with what type of device. User identity, device identity, and health of device can be assessed and policies can be created based on a multitude of variables including user-group membership (such as student, teacher,

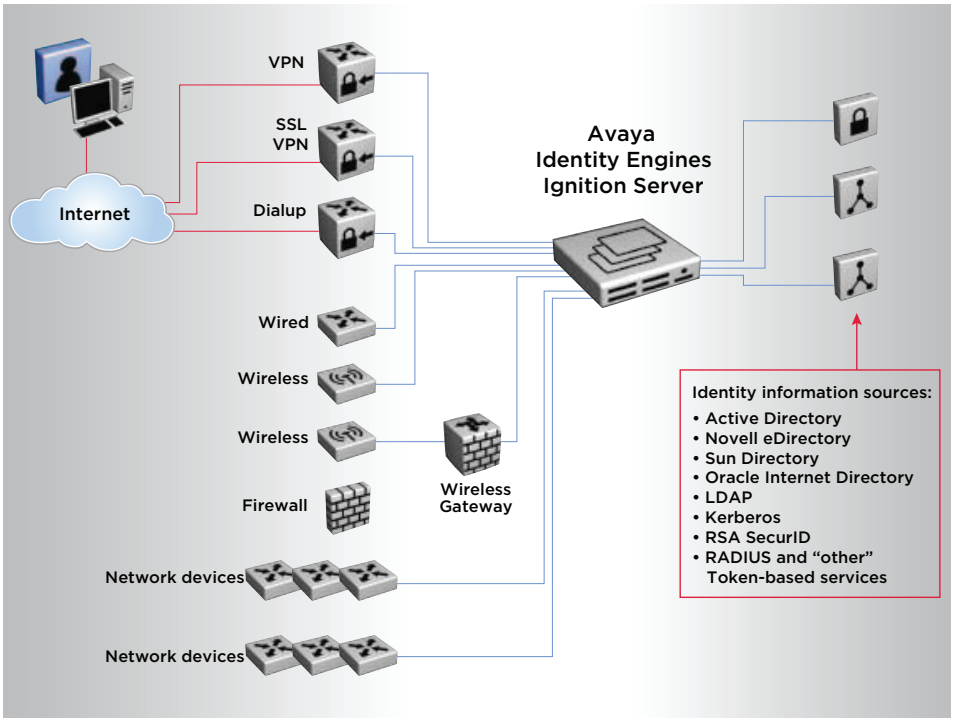

Figure 2. Simplified authenticated network architecture with centralized policy decision provided by the Identity Engines Ignition Server

staff, guest), access method (such as, wireless vs. LAN), health of device, time of day, day of the week, and more.

The Ignition Server is easy to deploy, connecting with your existing identity system and switching infrastructure. It provides a central policy decision point that streamlines access management, improves security and satisfies reporting requirements. It connects to complex store environments and offers centralized editing of network access policies. With the Ignition Server, access policies can evaluate user data, equipment data and the context of the access request. It handles multiple EAP types and supports network hardware from all major vendors.

Identity Engines Ignition Compliance Portal

Posture and health checking add a third layer to access policies. The two traditional layers, authentication and authorization, evaluate the user, with the authentication policy specifying how the user must prove identity and the authorization policy specifying which network the user can connect to. Health checking policy enables inspection of the user's device itself.

The Avaya Identity Engines Ignition Compliance Portal offers advanced posture and health checking capabilities through a clientless captive portal. Since no client installation is required, it seamlessly addresses the needs of guest users and unmanaged devices.

Ignition Compliance Portal enables verification of the health of a device. It checks antivirus and other security software before allowing connection, and can even specify a particular vendor and version required. It can check for specific files and registry entries and can prevent the use of specific applications such as instant messaging applications, P2P, hacker tools, etc. Depending on your enterprise's risk comfort level, policies can be as general or as specific as necessary, customized to meet your needs. The Ignition Compliance Portal presents a range of options when a client fails a health check. The administrator can choose to grant limited access on a remediation network, allow Internet-only access or deny access altogether.

WHY NOT PLAIN OLD NAC/RADIUS?

First-generation NAC doesn't include multiple directory information in its access decision — such as a member of a specific active directory group. It can't enumerate effective policy when multiple conditions are met, such as allowing a member of a specific group to access remotely during a quiet period and then otherwise restrict access.

Identity Engines Ignition Posture

The Ignition Posture is a practical, cost-effective solution, offering an easy-to-deploy, standards-based client supporting all major desktop operating systems, as well as policy options targeted at employee and other managed devices. Like the Ignition Compliance Portal, it interrogates endpoints for security and compliance and, based on health check outcomes, grants appropriate levels of network access to enhance network integrity.

Identity Engines Ignition Guest Manager

The Ignition Guest Manager oversees guest and visitor network access across wired and wireless access points. Accounts can quickly and easily be set up and administered by front-desk personnel or any employee tasked with being a guest "sponsor," thereby freeing up valuable IT resources.

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

For large events or conferences, the Ignition Guest Manager's bulk-loading capability can configure hundreds or thousands of guest accounts. In addition, it can host multiple self-provisioning kiosks simultaneously, each with different privileges, such as access zones and duration. As a result, guests can create their accounts themselves. Each can have different display characteristics and branding.

Identity Engines Ignition Analytics

Ignition Analytics is a powerful reporting application that enables in-depth analysis of network activity including ingress and usage. Report data comes from the Avaya Identity Engines Ignition Server. Ignition Analytics adds reporting to the Ignition Server by enabling automated data retrieval and report generation. An extensive feature set, which is easily customized to comply with policies and requirements, provides precise data that can be delivered automatically to anyone requiring it. Over 25 preconfigured audit, compliance and usage reports are available and custom reports can be easily generated. Sample reports include:

- Top five users with most usage
- RADIUS authentication attempts top 20 clients
- RADIUS authentication attempts failed by authenticators
- Authentications by user provisioning and date
- Usage summary
- Failed authentications by authenticator
- Authentication by client

Use case scenarios: Real-world examples

Guest access

Guest access was once an all-or-nothing proposition: you either locked down your network, preventing guests from entering, or left it wide open, allowing any wireless user to tap in and consume your resources.

Now, with an Avaya Identity Engines solution, you can control who enters, where in the network a user is allowed to go and for how long.

And, all that's required to accomplish this is filling in a template. No technical expertise and/or resources are required, *and* it can be done in real time.

Guests receive a user ID on the spot and a password is sent to their mobile phone or BlackBerry.

Conference room access

Once guests are inside the building, you can write a policy that says how much access they are given. You may want to give employees unrestricted network access within a conference room and grant restricted access to guests in the same room. You can do this even if they're using the same means of access. Identity-based policies remove the need to manage ports as "open" or "restricted." It doesn't matter what you're plugged into; all that matters is who you are and what you need.

Validated remote access

The Identity Engines portfolio enables you to perform posture assessments on remote devices to ensure they're equipped with valid antivirus software, updates, a personal firewall, etc. To protect sensitive information you might stipulate that employees cannot access everything in an office.

You might also set a different policy if an employee is at home as opposed to an airport kiosk, and for different times of day.

Bottom line, what matters is who, where, when, how and type of device. With an Identity Engines solution, you have control.

Authorized fixed assets

An Identity Engines solution enables you to define authorized fixed assets or non-interactive devices such as IP phones, printers and fax machines. You can conduct MAC-level authentication to help ensure that only authorized devices connect to the network and connect only where they're expected to connect. This prevents intruders from unplugging a printer and accessing the network and prevents employees from bringing in their own wireless access points and sharing network services, compromising network security.

The payoff

The Avaya Identity Engines portfolio delivers a wide range of role-based access options without compromising network security. It's a standards-based solution that integrates with your existing network infrastructure, leveraging your investment. It centralized and simplifies policy decision-making throughout your network, expressing policies in simple language thus removing technology from the equation.

Learn More

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

About Avaya

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

AVAYA

The Power of We™

06/11 • DN5115-01

avaya.com