

Avaya Identity Engines Portfolio

Avaya introduces a second-generation network access control solution, with standards-based support that allows you to not only control who uses your network, but where, when, how and with what type of device, and to do it without compromising security.

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, from on premises, home or on the road. 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. Such is the nature of network access control in today's enterprise environment. How you manage it can be 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 now is leveraging advances in technology to provide you with still more options, more simply. 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.

The Avaya Identity Engines portfolio brings the best elements of a next-generation RADIUS/AAA server, the deep directory integration found in application-identity offerings and 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 of products 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 is made up of four 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 Posture:** Endpoint health checking 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



The Avaya Identity Engines portfolio products are robust, but are also 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 truly separates the Avaya Identity Engines solution 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 will be granted employee access; if it's non-compliant or if posture information isn't available, the user will receive 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 the week. Think of the new Avaya Identity Engine portfolio as NAC 2.0, an evolution of NAC 1.0, a more secure and robust, but simpler, approach to network access and policy creation — one that allows you to leverage the identity information you've already gathered and protect your investment.

Centralized security

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

For employees, contractors, customers and guests, the Ignition Server assigns network access rights and permissions based on a user's role or relationship to the organization, based on where they are

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

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

connecting from (conference rooms, labs, lobbies, etc.), and based on 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.

Or: Guests can be provisioned with access to particular subnets or VLANS or you may limit them to outbound web access only, depending on their roles and needs.

The Identity Engines Ignition Guest Manager allows the network administrator to specify precisely with which devices a user may log in. And the Identity Engines Ignition Analytics delivers extensive automated reporting functionality that allows IT professionals to be more effective in carrying out their mandates or compliance, planning and security.

The products

Identity Engines Ignition Server

The Identity Engines Ignition Server is the centerpiece of the Identity Engines portfolio. It's a virtualized standard; no new hardware is required. As most organizations have already invested in VMware environments, the Ignition Server allows you to leverage your existing investment, saving costs and allowing for additional deployment flexibility.

The Ignition Server breaks down the silos. Not only does it simplify network identity management across your enterprise, it allows you to provide consistent, centralized access policy while eliminating the potential for administrative errors. 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.

It offers a new level of accuracy, with identity- and policy-based control that allows you to write policies for who accesses the network, where, when, how and with what type of device. It allows you to assess the user's identity, the device's identity and the health of that device. It can then create policies based on a multitude of variables, including user-group membership (for example, student, teacher, staff, guest), access method (for example, wireless vs. LAN), the health of the 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

WHY THE AVAYA IDENTITY ENGINES AUTHENTICATED NETWORK ARCHITECTURE?

The Avaya Identity Engines portfolio allows 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

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 Posture

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 his or her identity and the authorization policy specifying what network the user can connect to. Posture checking policy adds the ability to inspect the user's device itself.

The Avaya Identity Engines 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 to handle all types of users.

Ignition Posture allows you to verify the health of a device by checking antivirus and other security software before allowing connection, and can even specify a particular vendor and

version required. Depending on your enterprise's risk comfort level, this policy can be as general or as specific as necessary, customized to meet your needs. It 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.

Identity Engines Ignition Guest Manager

The Ignition Guest Manager oversees guest and visitor network access across wired and wireless access points. It's a simple process. 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 allows you to perform 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 allowing you to set up automated data retrieval and report generation. An extensive feature set, which is easily customized to comply with your policies and requirements, helps equip you with precise data that can be delivered automatically to anyone you choose. Creating reports is easy. You select from over 25 preconfigured audit, compliance and usage reports. In addition, you can easily produce a custom report to fulfill your specific reporting requirements. Example 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 used to be an all-or-nothing proposition: your options were to lock down your network, preventing guests from entering, or leave it wide open, allowing any wireless user in the vicinity to tap in, consuming your resources.

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 — and 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 but then otherwise restrict access.

But that's no longer the case. With a Avaya Identity Engines solution, you can control who enters, where in the network you'll allow them to go and for what period of time.

And it's easy to do, requiring only that a quick template be filled out — 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 cell phone or BlackBerry. They're then authorized to enter.

Conference room access

Once guests are inside the building, you can write a policy that says how much access they'll be provided. 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; it matters who you are and what you need.

Validated remote access

The Identity Engines portfolio allows you to perform posture assessments on remote devices to ensure they're equipped with valid antivirus software, updates, a personal firewall, etc. You might stipulate that employees not have access to everything they can access while in the office — too much potential for sensitive materials to be compromised.

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

Again: it's all about who, where, when, how and with what type of device. With an Identity Engines solution, it's all in your control.

Authorized fixed assets

An Identity Engines solution allows 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 ensure that only authorized devices can connect to the network and connect where they're expected to connect. This prevents intruders from simply unplugging a printer and accessing the network and prevents employees from bringing in their own wireless access points and sharing network services, thereby compromising network security.

The payoff

Bottom line, the Avaya Identity Engines portfolio is about providing a wide range of role-based access options without compromising the security of your network. It's a standards-based solution that integrates with your existing network infrastructure, leveraging your investment; and it centralizes, and thus simplifies, policy decision-making throughout your network, then expresses policies in simple language, removing technology from the equation.

To learn more about the Avaya Identity Engines portfolio, visit www.avaya.com.

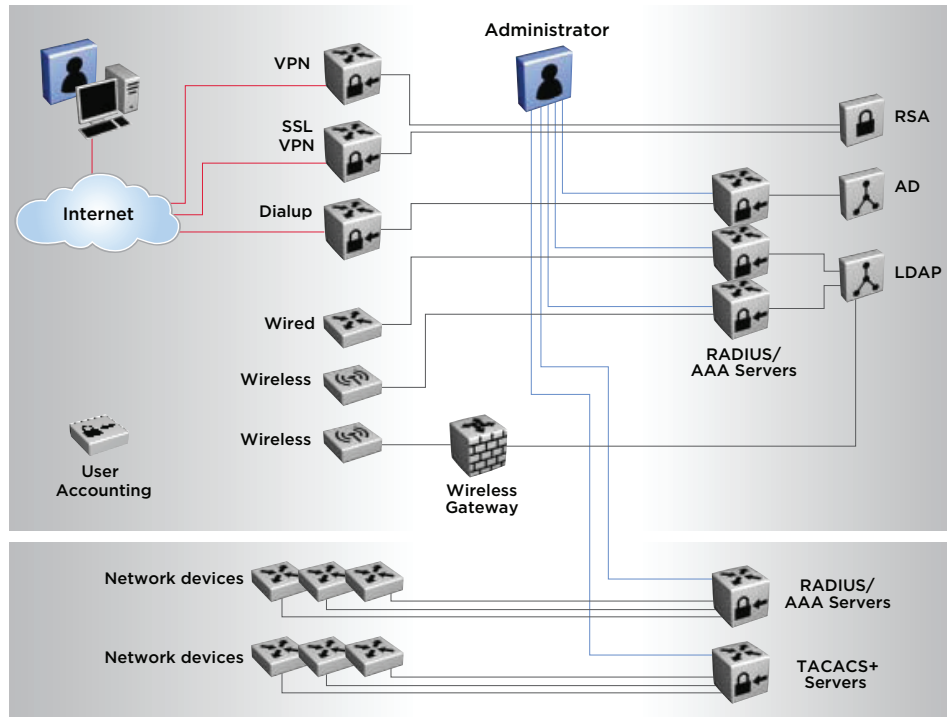


Figure 1. Complex architecture with multiple AAA servers and network overlays

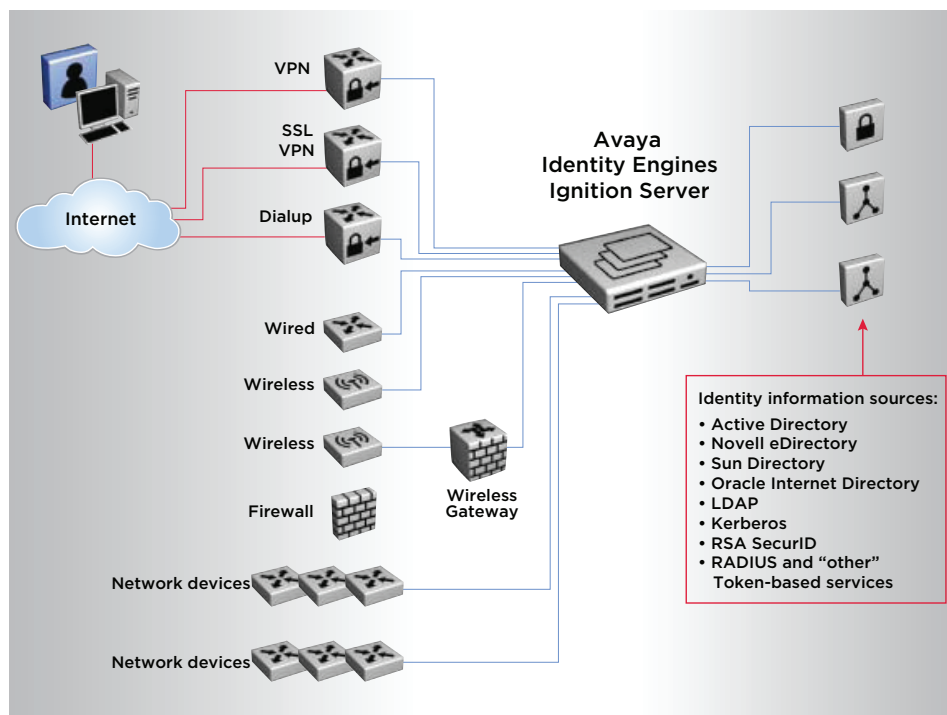


Figure 2. Simplified authenticated network architecture with centralized policy decision provided by the Identity Engines Ignition Server

About Avaya

Avaya is a global leader in enterprise communications systems. The company provides unified communications, contact centers, and related services directly and through its channel partners to leading businesses and organizations around the world. Enterprises of all sizes depend on Avaya for state-of-the-art communications that improve efficiency, collaboration, customer service and competitiveness. For more information please visit www.avaya.com.

The Avaya logo consists of the word "AVAYA" in a bold, red, sans-serif font. The letters are closely spaced, and the 'A's and 'Y' have a distinctive shape.

INTELLIGENT COMMUNICATIONS

© 2009-2010 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. and are registered in the United States and other countries.

All trademarks identified by ®, TM or SM are registered marks, trademarks, and service marks, respectively, of Avaya Inc.

All other trademarks are the property of their respective owners. Avaya may also have trademark rights in other terms used herein.

12/09 • DN5020

The Avaya.com logo is a red rectangular button with the text "avaya.com" in white, lowercase, sans-serif font.