CAPABILITIES:
- Wireless & Wired Networks
- Extends WPA2 to All Users
- Flexible BYOD & Guest Policies
- Next Generation Guest Access
- Differentiates BYOD vs IT Assets
- Integrates with the Enterprise:
  Microsoft Active Directory®
  Microsoft® Certificate Authority
- Extends Beyond the Enterprise:
  LinkedIn®, Facebook®, Google™
- Automated Configuration Includes:
  Windows® XP & Greater
  Mac® OS X 10.5 & Greater
  Ubuntu® 9.04 & Greater
  iOS (iPhone®, iPad®, iPod Touch®) 2.0 & Greater
  Android™ 2.1 & Greater

SECURE ACCESS ENROLLMENT SERVER

SECURE ACCESS FOR ALL

The Secure Access Enrollment Server provides a simple approach that unlocks the power of Wi-Fi Protected Access 2 Enterprise (WPA2-Enterprise) Security by offering a single point-of-entry to the enterprise network for all non-domain devices. Its highly flexible workflow engine gives network administrators control by blending the best of traditional policies, like Active Directory® and Microsoft® CA integration, with powerful new policy capabilities, including integration with external sources like LinkedIn®, Facebook®, and Google™. Built upon Extensible Authentication Protocol Transport Layer Security (EAP-TLS), the Secure Access Enrollment Server extends standards-based wireless security to personal devices in an automated, self-service manner without the need for IT assistance.

EMPLOYEES WITH PERSONAL DEVICES (BYOD)

Employees walking into the enterprise with personal devices has garnered considerable attention. The challenges involved in BYOD include security, usability, and differentiation of personal devices from corporate-issued devices.

The Secure Access Enrollment Server provides automated, self-service access to the WPA2-Enterprise wireless network for employees authorized to use BYOD devices. Authorization may come from a variety of sources, including authentication via Microsoft Active Directory and acceptance of a use policy.

Once authorized, the device may be given access indefinitely or for a period of time along with additional policy options based on WPA2-Enterprise, including dynamic VLAN, ACL, and/or bandwidth assignment.

With support for a wide array of device types and operating systems, the Secure Access Enrollment Server enables employees to utilize their favorite devices without IT involvement. The user also benefits from the elimination of annoying web logins.

The network administrator benefits from knowing that all wireless users are secure and that personal devices have been segregated from IT-owned assets. The network administrator also gains visibility and control on a device-by-device basis.

A NEW SPIN ON GUEST ACCESS

Providing guest access is desirable; provisioning guest accounts is annoying. The Secure Access Enrollment Server negates traditional guest servers by automatically moving guests to encrypted WPA2-Enterprise wireless networks without the need to provision an account and generate yet another set of credentials.

The Secure Access Enrollment Server eliminates the need to provision guest accounts by introducing an integration of WPA2-Enterprise with external identity services, such as Facebook, LinkedIn, and Google. Based upon your customized policy, the user simply authenticates via an external source and is granted the appropriate level of network access.

With a customizable workflow, this all happens very intuitively for users. They login via an authentication source for which they are accustomed and which the network administrator permits. The Secure Access Enrollment Server automates the movement to the secure wireless network. With support for a wide array of device types and operating systems, your guests are assured self-service access to the WPA2-Enterprise wireless network.

The Secure Access Enrollment Server provides the network administrator visibility and control over who is granted network access. With flexible policy options and control over the length of time guests are permitted access, the Secure Access Enrollment Server provides "set-it-and-forget-it" simplicity that eliminate the maintenance headaches of traditional guest servers.

IT-OWNED NON-WINDOWS ASSETS

Today, the need to provision thousands of IT-owned mobile devices is a consistent challenge. IT-based provisioning scales poorly when dealing with large numbers of devices or geographically dispersed populations.

Early approaches to the BYOD problem focused on device fingerprinting to categorize devices based on type. In this way, the proposition was that "all Windows devices are IT assets" and "all iPads are personal devices (BYOD)".

In reality, IT-owned, non-Windows Domain devices are proliferating in networks. It started slowly with Mac OS X laptops and has exploded with IT-issued phones and tablets. The use cases for these new devices range from IT-Owned/Single-User uses to IT-Owned/Multi-User uses to kiosk-style uses.

The Secure Access Enrollment Server provides the ability to transform the provisioning process and provide a user-driven, self-service provisioning process. Based on your policies, these IT assets may be given the appropriate network access without IT ever touching them.

SPECIFICATIONS

Deployment Options:
- Cloud Hosted
- VMWare® Virtual Appliance (ESXi)

Supported Identity Stores:
- Microsoft Active Directory®
- Facebook®
- LinkedIn®
- Google™ Play

Automated Operating Systems:
- Windows® XP SP2 & Greater
- Mac® OS X 10.5 & Greater
- Ubuntu® 9.04 & Greater
- Android™ 2.1 & Greater
- iOS (iPhone®, iPad®, iPod Touch®) 2.0 & Greater

Contact your sales representative regarding additional operating system support.

For more information on the Secure Access Enrollment Server, please visit us on the web at:
www.motorolasolutions/enrollmentserver

MOTOROLA