Simplifying Security Provisioning for Mobile Devices

AutoConnect™ is the Smart Choice for 802.1X-WPA2 Enterprise On-Boarding

AutoConnect™ offers a web-based approach to automating the end user process of configuring a device for secure wireless access. AutoConnect's MultiOS technology simplifies WPA2 Enterprise wireless deployments for end users while enabling unparalleled visibility with both device and real-time connection reporting. Your secure wireless network adoption is increased due to the superior user experience.

Improved End User Experience. AutoConnect simplifies 802.1X and WPA2-Enterprise wireless deployments, creating a simple and straightforward experience by significantly reducing the number of configuration steps—from 15 to only five! User frustration, and understanding the complex settings required to keep both user and network secure, can be mishandled, compromising security. Enterprise IT departments looking to standardize wireless provisioning now have a way to extend a helping hand without burdening the helpdesk. A configuration assistant guides the user through the initial onboarding process until the device is successfully joined to the secure network. Any subsequent visits are automatically connected to the secure network.

Error Handling and Reporting. AutoConnect also provides unique and powerful error handling and reporting capabilities. When a user attempts to connect to the Secure WLAN but encounters an error, the AutoConnect MultiOS connection assistant software conducts multiple checks to resolve the issue. The software confirms all the correct processes are running and subsequently makes necessary adjustments to ensure reliable connections. The status of the device is reported throughout the process and viewable within the management portal.

AutoConnect reports not only device identity but user identity as well, an incredibly powerful tool for both the support and network administration staff. Users are often unable to provide knowledgeable information about their device to the support desk, and often struggle to provide identifying data such as MAC address or device/ model data. The ability to search and view the connectivity behavior based on user identity provides IT departments with the opportunity to utilize better tools to service the customer.

Automatically configure devices for secure 802.1X/WPA2E wireless access to benefit both end users and your helpdesk.

- Reduce number of steps (15 to 5)
- Increase speed to access
- Increase secure wireless adoption
- Ensure configuration accuracy
- Reduce helpdesk calls
- Increase customer satisfaction with better user experience
- Enhance reporting capabilities
- No Java required

Secure Deployment Options. AutoConnect offers a variety of deployment options and customers may host their software locally on a web server or multiple web servers in case of distributed environments. Cloud-based hosting is also available to all customers. AutoConnect integrates seamlessly with SafeConnect's captive portal technology, and can automatically install the SafeConnect Policy Key (NAC Agent) as part of the onboarding process to further streamline your deployment. Finally, AutoConnect can be deployed on physical media such as CDs and distributed to users utilizing traditional desktop or laptop platforms.

Unparalleled Troubleshooting. A defining feature of AutoConnect is its troubleshooting capabilities. Most configuration utilities simply push a package to the device and think the job is done. AutoConnect performs a host of tests in the background, follows up on the connection, and ensures the user is properly configured and connected to the network. If an error is detected, AutoConnect steps in to determine and assist with fixing the connectivity issue. Furthermore, helpdesk desk staff can login to the management portal, view the associated error and assist remotely.

Helpdesk and Administrative Accounts. Different users require different levels of access. AutoConnect allows access for multiple levels of users and permissions, including read-only helpdesk accounts. Helpdesk accounts receive access to device and error logs for troubleshooting purposes. Other settings are kept safe and out of reach, accessible by administrative users who are deploying the AutoConnect technology.

Enterprise Backend Connectivity (No Java Required). AutoConnect offers server side connectivity technology to enable the use of unique credentials (certificates) for WLAN authentication. Traditionally, certificates have been a challenge to deploy. AutoConnect makes this simple and straight forward by utilizing the industry standard SCEP protocol. AutoConnect customers with Microsoft Active Directory and Certificate Services environments will benefit from lightweight CA connectors that tightly integrate AutoConnect configuration assistants to the identity environment. AutoConnect configuration assistants prompt the end user for their Active Directory or LDAP credentials and subsequently help generate and utilize that certificate for wireless access. Certificate templates and enrollment policies help determine who can and cannot receive access, giving network administrators maximum flexibility in their access policies.

Any Device, Any Security Type. AutoConnect is one of the most diverse and compatible deployment technologies on the market. Customers have the flexibility of using identity-based authentication (PEAP/MSCHAPv2 or EAP-TTLS/PAP), token-based authentication (PEAP/GTC) or certificate-based authentication (EAP-TLS) for their authentication needs. AutoConnect is vendor-agnostic, and supports major operating systems and devices including Windows, Windows RT, Mac OS X, Apple iOS, Android, Linux and Kindle/E-Readers. Beyond major EAP and Encryption type support, AutoConnect provides all the server integration components to connect to major commercial and open source Certificate Authorities (CAs) via the SCEP enrollment protocol. Specifically for Microsoft Certificate Services customers, AutoConnect provides sophisticated Microsoft CA connectors for significant functionality and enrollment flexibility beyond Microsoft's built-in NDES solution.

impulse

Experience the Freedom

The Impulse Experience is the result of our real-time contextual intelligence, simplified access control architecture, remote managed support services, and customer-centric business philosophy that delivers freedom to all facets of the organization. It's not one thing, it's everything. Visit impulse.com