identity•connect™
device registration

BYOD Management

Identity-Based Personal Device Registration

The explosion of mobile devices, coupled with advances in wireless technologies and readily available cloud-based applications, has driven a fundamental computing shift within large network environments. Today nearly everyone has a smartphone, a laptop computer, and/or tablet in addition to other network-ready devices—which has created the need for IT organizations to implement higher density wireless networks to support the escalating volume of mobile devices.

The number and diversity of devices in any corporation, hospital, college campus, or school district has exploded - easily tripling the number seen just a few years ago. This puts tremendous pressure on IT infrastructure; as devices are added more resources are used, more bandwidth is consumed, more IP addresses are allocated and re-cycled, and more wireless access points are required to handle the increased density. The ability to successfully identify device types, ascertain the identity of the user, and maintain a positive user experience while roaming has also become a formidable challenge. Additionally, organizations are being challenged with the task of correlating device and user identity over time across their networks for regulatory compliance; security forensics purposes; and identity-based web content access and bandwidth management policies.

Identity•Connect™ recognizes when unknown devices attempt access to your wired, wireless, or VPN networks and provides the following essential features and benefits:

- **Agentless Device and Role Profiling** provides visibility into user identities and device types, whether they are a managed (organization-owned) or personally-owned (i.e., BYOD, guest), and when a device is connected to the network
- **Guest User Self-Enrollment** automates the process of provisioning Internet-only network access for guests
- **Device Enrollment** allows end users to self-enroll non-browser devices such as printers, e-readers, or gaming systems by identity
- **Identity Correlation Management** provides real-time **identity-to-device association** and standards-based integration with third-party policy management systems
- Commercially available **replacement for "home-grown" network registration** systems includes hardware/software maintenance
- **Managed Support Services** delivers updates for device type fingerprinting within 48 hours of their official release date

Identity•Connect™ delivers on our promise of a **scalable BYOD solution** with **centralized management**, "**no hands" system updates**, and true **real-time and historical reporting** – providing you with comprehensive visibility and control.

Sessions Tracker™

SessionsTracker™ is a fundamental component of Identity•Connect™ which **tracks and correlates device session information in real-time**. SessionsTracker™ unifies session management of "start", "stop" and "update" data from network sources in a timely and accurate manner. SessionsTracker™ correlates information from network "flow based" technologies like "Netflow" and "sFlow", as well as control protocol services such as RADIUS and DHCP to maintain a "session" for the duration of time

Identity•Connect™ offers the smart choice for device visibility and control for your network!

Get Smarter About….

- **Agentless Device Identification**
- **User Identity**
- **Self-Provisioning Guest Access**
- **Device Enrollment**
- **Real-Time and Historical Reporting**

Impulse.com

a device is active on the network. SessionsTracker™ enables Identity•Connect™ to collect and correlate supplemental data (such as a username or device type) from additional sources.

Real-Time Identity for Devices

Identity•Connect™ delivers the **real-time identity-to-device association** information required to support the networks of today. Identity•Connect™ participates in Single Sign-On (SSO) authentication by processing RADIUS accounting messaging generated by 802.1X-WPA2 Enterprise networks. This identity framework can be extended in our Identity Correlation Manager to publish this information to third party network management devices such as web content filters, bandwidth packet shapers, next generation firewalls and Security Event Information Management (SEIM) devices to enable **identity based policies** within these networking devices.

Guest Management

With Identity•Connect™, users who do not have credentials within an organization may **self-provision accounts via a fully automated process**. Alternatively, access to the Guest Management Portal can be delegated to authorized personnel to manually provision accounts for Guest Users, as needed.

Features	Benefits
Device Type Profiling	Identifies Device Types (PC, MAC, iOS, Android, Windows RT, RIM, Gaming, Media, AppleTV, etc.)
End User Authentication	Prevents unauthorized users from accessing network resources and participates in 802.1X/RADIUS and AD Domain Single Sign-On (SSO)
Device Self-Enrollment	Allows end users to self-enroll non-browser devices by identity
Guest User Self-Provisioning	Automates the guest user self-enrollment process and can restrict endpoint devices to Internet-only access for a period of time
Reporting	Real-Time reporting dashboard, data archiving and historical reporting
Identity Correlation Manager	Provides real-time identity-to-device association and standards-based integration with third-party identity-based policy management systems

Highly Scalable to Go Further

Identity•Connect was built to support large-scale enterprise network environments. Each appliance can manage up to **10,000 concurrent endpoint devices** and can be clustered together to support tens of thousands of users.

24 x 7 x 365 Maintenance and Managed Services

All Impulse Point products include a comprehensive hardware/software maintenance program. This includes **24x7 system monitoring, problem determination and resolution technical support, daily remote backups and overnight hardware replacement, and free software/hardware upgrades .** Impulse Point provides the industry's only continuous system monitoring and update service with standard maintenance. Our technical staff continuously monitors the health of the system and will take proactive corrective action if a problem is detected. This service also includes nightly updates on device profiling, operating systems, and remediation software updates.

Additional Device Management Products Available from Impulse Point

- Safe•Connect™ includes the features and benefits of Identity•Connect™ *plus* real-time security posture and policy assessment, dynamic policy enforcement, and self-guided remediation for Microsoft Windows and MAC OS X devices.
- Xpress•Connect provides automation of 802.1X/WPA2 Enterprise provisioning and on-ramping process for secure wireless networks.

About Impulse Point

Impulse Point delivers the industry's most scalable and easiest to deploy and maintain Bring Your Own Device (BYOD) solutions. Identity•Connect™ and Safe•Connect™ are the solutions of choice for large, diverse environments – such as Education – where the "Consumerization of IT" is driving the need to provide endpoint security policy enforcement for a myriad of personally-owned, non-managed, mobile computing devices. Deployed and supported as a managed service, Safe•Connect's rapid installation, network independence, and track record of reducing help desk calls results in lower total cost of ownership and reduced risk. Customers currently entrust the security of more than three million endpoints to Impulse Point. Visit www.Impulse.com or www.SimplifyBYOD.com

impulse