SafeConnect™

Network Access Management

Visibility, Security and Control for BYOD

The explosion of mobile devices, coupled with advances in wireless technologies and readily available cloud-based applications, has driven the adoption of Bring Your Own Device (BYOD). Today, nearly everyone owns a smart-phone, laptop, or tablet—which has created the need for security policies to support the escalating volume and diversity of personally-owned computing devices accessing business-critical network resources.

An everyday challenge for IT managers is enforcing security compliance policies while maintaining a positive user experience and reducing help desk calls in support of BYOD and guest users. Organizations are also faced with the daunting task of correlating mobile device information and user identity (over time and across network segments) for regulatory compliance; security forensics; and enabling identity-based firewall, web content, SIEM, and bandwidth management policies.

SafeConnect automates device security compliance and network access assignment policies (based on identity/role, device type, location, and ownership); and gathers a wealth of real-time and historical context-aware device information that allows for more timely and informed security decisions.

The Dell-Aerohive-Impulse Advantage

In combination with Dell and Aerohive Networks, Impulse's SafeConnect solution offers a highly-simplified and scalable approach to providing a secure networking environment while delivering a superior user experience for managed, BYOD, and guest devices.

The certified integration of Dell Networking Layer 2 and Layer 3 wired switches, Aerohive controller-less wireless access points, and Impulse's SafeConnect Network Access Management Service Offering represents a unique industry value proposition that addresses the cost, resource burden, and business risk associated with deploying and supporting an enterprise-wide secure network.

Key features

Identity Access Control

- Integrated RADIUS Server
- User Authentication Portal
- Agentless Device Profiling
- Guest User Self-Enrollment
- Network Device Self-Registration
- Role-Based Access Control
- Contextual Intelligence Publishing
- Real-Time and Historical Reporting

Secure BYOD On-Boarding

- 802.1X-WPA2 Enterprise Automated Self-Provisioning

Device Security

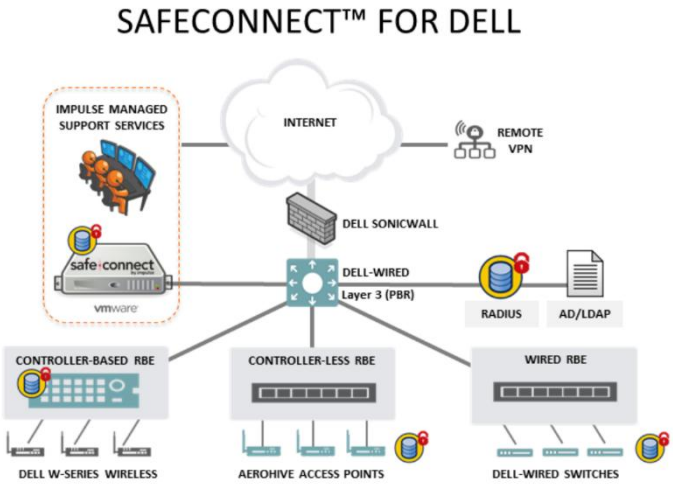
- Acceptable Use Policy Enforcement
- Real-Time Security Posture Assessment and Remediation
- Application Usage Policies
- MDM Network Enforcement

Managed Support Services

- Remote Installation and Deployment Assistance
- 24x7 Proactive Monitoring
- Problem Determination and Resolution Ownership
- Daily System Updates and Backup
- Overnight Hardware Replacement
- Installation of All Software Maintenance and Version Upgrades
- Free Hardware Upgrades

Leveraging Dell Networking Technology

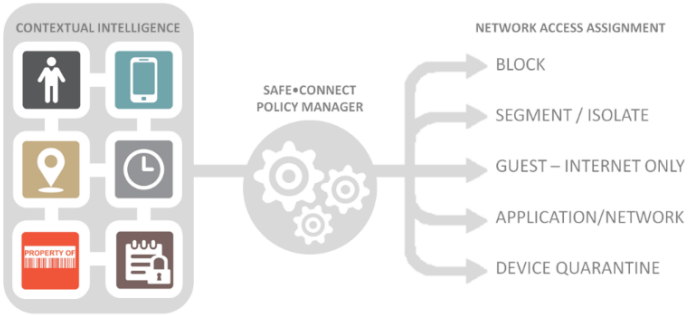
SafeConnect integrates with Dell Networking technology to deliver the industry's most scalable and easiest-to-deploy network access management offering. Dell Networking N-Series, S-Series, and C-Series wired switches provide a range of performance solutions from 1G to 40G and fixed- or chassis-based form factors.



SafeConnect's Network Access Control (NAC) architecture utilizes Layer 3 Policy Based Routing (PBR) and Layer 2 RADIUS-Based Enforcement (RBE) technology to offer the industry's broadest range of device enforcement options.

SafeConnect's Layer 3 (PBR) access control approach offers the simplest device enforcement alternative based on its Layer 2 independent design and can be rapidly deployed.

RBE delivers dramatic scalability and granular network access control for 802.1X-WPA2 Enterprise and Open wireless networks, and Layer 2 wired network switches based on contextual intelligence-driven policies.



A key benefit of RBE is its non-reliance on VLAN Steering. RBE assigns network access privileges to a specific device versus moving a device to a shared VLAN. SafeConnect's RBE offers the following benefits:

- Easier to design, deploy, and support – Fewer technical resources required
- Real-time post-admission security posture assessment and enforcement – No need to remove or re-authenticate a device to conduct a security posture check
- Better user experience – No IP address/VLAN changes
- Higher level of device quarantine/segmentation – Devices are restricted/isolated individually, not placed into a shared/common/dirty VLAN

SafeConnect also delivers consistent identity and device type awareness, and security posture assessment, enforcement, remediation for remote VPN devices. Due to SafeConnect's Layer 2 independent architecture, VPN networks are viewed as another VLAN or IP address range segment. Therefore, SafeConnect supports any VPN gateway provider.

Multi-Vendor Networking Support

A key benefit of SafeConnect is its network vendor independence. SafeConnect can be integrated with any combination of Layer 3 and/or Layer 2 wired network switch technology in addition to Controller-based and Controller-less wireless network devices. SafeConnect integrates directly with most network vendors and can support any Layer 2 (wired, wireless or VPN) vendor network architecture using its Layer 3 device enforcement approach.

SafeConnect for Dell Product Overview

SafeConnect delivers a range of capabilities that provides a comprehensive enterprise-wide network access management solution to address the flexibility and security needed to support today's wired, wireless, and VPN network environments.

Identity Access Control SafeConnect recognizes when devices attempt access to wired, wireless, or VPN networks and provides agentless device type profiling, user authentication, network "non-browser" device registration, guest access self-enrollment management, and real-time or historical contextual intelligence-based reporting. This is an ideal solution for customers that desire context-aware network access assignment and visibility for computing devices based on identity/role, device type, location, IP-MAC Address, and ownership (company managed or BYOD).

RADIUS Server SafeConnect includes a standards-based RADIUS Server that integrates with an organization's AD-LDAP directory services infrastructure to deliver 802.1X authentication services that enable both secure WPA2 Enterprise wireless networks, as well as 802.1X-based wired and VPN environments. SafeConnect can

also leverage and support an organization's existing standards-based RADIUS server platform as required.

Secure BYOD On-Boarding SafeConnect solves a complicated problem for end users by automating the process required to provision devices onto secure 802.1X-WPA2 Enterprise wired and wireless networks. By eliminating end user manual configuration, the solution delivers dramatic reductions in help desk support calls and accelerates user adoption of secure wireless. When combined with Identity Access Control this feature enables an organization to welcome every new user with a captive web portal that authenticates the user, configures the device's embedded 802.1X supplicant, ensures that RADIUS server certificate validation has been configured properly, and automatically assigns (moves) the device to a designated secure SSID network segment. Users are automatically associated with their secure wireless network on subsequent network connections without the need for repeated logins.

Device Security SafeConnect enhances the security posture of your network by providing real-time policy assessment, enforcement, and self-remediation for Windows and MAC OS X devices. SafeConnect's Policy Key (agent) provides in-depth compliance assessment prior to granting network access to ensure that the device adheres to the organization's acceptable use policies (anti-virus, operating patches, personal firewalls, P2P, etc.) as well as on a continuous basis after access is granted. Web-based self-remediation guidance enables users to conform to security policies without end user help desk support involvement. The SafeConnect Policy Key can be pre-deployed to managed devices using standard AD Domain Group Policies or via the organization's chosen software distribution product. BYOD users will be prompted to install the SafeConnect Policy Key (if required) prior to accessing the network.

SafeConnect also integrates with premise- or cloud-based Mobile Device Management (MDM) offerings to provide comprehensive network-based policy enforcement for mobile devices that delivers the following benefits:

- Automate MDM provisioning by detecting, blocking, and redirecting all unknown mobile devices to the MDM registration portal to ensure compliance
- Apply network-level quarantine to all mobile devices that are either not registered or are non-compliant with MDM policies and provide web-based self-remediation user guidance
- Assign application and network access privileges based on identity/role (i.e., employee, faculty, staff, guest, vendor, etc.), device type, location, ownership and policy status

Cloud-Managed Support Services

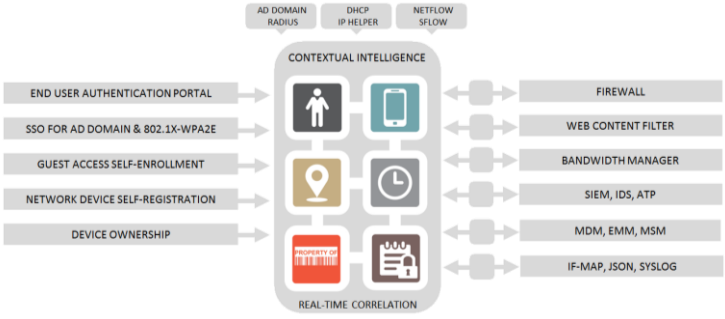
All SafeConnect products come with an industry exclusive and comprehensive hardware and software maintenance program and includes the following:

- Remote installation, deployment, support, training
- 24x7 proactive system monitoring
- Problem determination and resolution support
- Daily device type profiling, operating systems, and remediation anti-virus security software updates
- Nightly policy configuration remote backups
- Overnight hardware replacement and restoration
- Installation of all application version upgrades and software maintenance updates

Contextual Intelligence

Impulse's Contextual Intelligence™ technology delivers real-time device information that correlates identity/role, device type, location, ownership, and security compliance status over time to power SafeConnect.

Better visibility of information gleaned "in context" regarding devices on the network allows IT managers to make better decisions on network capacity, risk mitigation, and forensic analysis required for addressing regulatory compliance.



Contextual Intelligence Publishing provides real-time contextual intelligence to other network management and security systems (i.e., next-gen firewalls, web content filters, SIEMs, IDS/APT, and bandwidth management providers) that enable granular identity-based policy assignment, single sign-on, one-time user authentication, and enhanced analytics to provide more informed and timely security decisions.

The ability to leverage real-time contextual data for authentication persistence also reduces the number and length of help desk calls by improving the end user experience (no multiple log-in prompts).

SafeConnect Network Access Management	
Identity Access Control	
RADIUS Authentication Server	Provides RADIUS to AD/LDAP Authentication Services in support of Open and Secure 802.1X-WPA2 Enterprise wireless networks, as well as 802.1X based wired and VPN environments.
User Identity Authentication	Prevents unauthorized users from accessing network resources and supports 802.1X-RADIUS and AD Domain Single Sign-On (SSO).
Agentless Device Profiling	Provides visibility into device types and ownership (whether a device is company-owned and liable or personally-owned - i.e. BYOD).
Guest User Self-Enrollment	Automates the process of provisioning Internet-only network access for guests without help desk involvement.
Network Device Registration	Allows end users to self-enroll non-browser devices such as printers, e-readers, media, or gaming systems using their user identity credentials.
Real-Time & Historical Context-Aware Reporting	Provides real-time reporting views and historical policy event data that depict authentication, compliance, and remediation status.
Contextual Intelligence Publishing (CIP)	Delivers real-time correlated user identity/role, device type, ownership, and compliance information to third-party firewalls, web content filters, SIEMs, and bandwidth managers that allows for more granular identity-based policies for BYOD mobile devices and enhances the user experience via authentication persistence.
Secure BYOD On-Boarding	
WPA2 Enterprise / Auto-Provisioning	Automates the user experience of “on-boarding” devices onto WPA2 Enterprise - 802.1X secure wireless and wired networks.
Device Security	
Acceptable Use Policy Enforcement	Flexible real-time AUP enforcement for devices including audit-only, periodic grace-period, warnings and immediate network quarantine.
Real-Time Security Compliance	Manages compliance with Anti-Virus, Anti-Malware, OS Patch and Personal Firewall policies for Windows and MAC OS X devices.
Application Usage Policies	Prohibits the use of peer-to-peer (P2P) file sharing for DMCA compliance and other non-approved applications.
Custom Policy Builder	Enables customers to easily build policies based on the existence or non-existence of file types, services, processes, or registry settings.
MDM On-Boarding and Network Enforcement	Ensures that end users install and retain the organization’s preferred MDM solution on their mobile devices and adhere to policy.
Cloud-Managed Support Services	
24x7 Proactive Monitoring and Technical Support	Includes 24x7 system monitoring; problem determination and resolution technical support; daily remote backups, device type profiling, operating systems, and remediation anti-virus security software updates; overnight hardware replacement; and no-charge software version and hardware upgrades.

Learn more at Dell.com/Networking