safe•connect

Three Editions—Same Proven Technology

SafeConnect NAC's traditional best of breed NAC offering has been successfully meeting a wide array of network access control needs for over 15 years. However, as Impulse expanded to new vertical market spaces, it became clear that there are organizations whose needs are a subset of the overall capabilities of SafeConnect. If your organization does not need the breadth of our Enterprise solution, Impulse now offers an Essentials and Standard Edition in addition to our existing Enterprise offering.

Essentials is oriented toward customers in verticals like banking and finance that are heavily compliance driven, who have clear security needs, or for smaller organizations that, perhaps, cannot afford to invest as much in Network Access Control. Essentials is designed to be customer-deployable with minimal assistance from Impulse's Support team.

Essentials Edition Summary

- RADIUS
- Visibility
- 802.1X Authentication
- Port Level Control

Standard includes all of the Essentials capabilities and goes further to include the most commonly requested capabilities across verticals, such as, device posture assessment, a guest portal, and Contextual Intelligence Publishing to share the valuable information NAC collects with other components of your security ecosystem.

Standard Edition Summary

- *Essentials +*
- End User & Guest Portals
- Posture Assessment
- Reporting
- Contextual Intelligence Publishing
- Optional HA

Enterprise includes all that Standard includes, plus the full complement of SafeConnect NAC's traditional enterprise-level offering—including powerful capabilities such as Threat Enforcement and clustering capability to scale to hundreds of thousands of concurrent devices. Moreover, for a limited time, Enterprise includes Impulse's SafeConnect SDP offering to provide a more secure alternative to a traditional VPN.

As your needs grow, stepping up from Essentials to Standard, or Standard to Enterprise is as easy as getting a new license key from Impulse's Sales team.

Enterprise Edition Summary

- *Standard +*
- 30K devices per appliance
- Threat Enforcement
- SAML Authentication
- Optional Secure BYOD Onboarding

Technology Shared by all Editions

SafeConnect NAC is delivered as a virtual appliance and can be hosted on either VMware ESX or Microsoft's Hyper-V. It sits out-of-line on your network, utilizing the standard network integration capabilities of your infrastructure (such as DHCP Syslog, IP Helper, and RADIUS accounting) to get the inputs it needs. Meanwhile, it uses standards such as RADIUS or 802.1X to control access to the network. SafeConnect NAC's network integration approach is infrastructure neutral and proven across a long list of vendors.

SafeConnect NAC's device discovery and profiling leverages fingerprints for DHCP requests, User Agent Strings, and other techniques that are automatically pulled down from Impulse's centralized cloud service; thereby ensuring customer's appliances have the latest fingerprints for the ever-growing number of IoT and other device types.

When SafeConnect NAC does discover a device on the network, it correlates device attributes, user, location, authentication, and compliance information to inform the policy to be applied and the action to take to ensure the device and user get only the intended level of access.

Appliance settings and policy configuration backups are backed up automatically to Impulse's cloud service or an FTP end point provided by the customer.

When new versions of SafeConnect NAC are available, or maintenance updates are required, Impulse will proactively notify your organization and will perform the update, for the term of your subscription.

SafeConnect NAC's licensing permits customers to spike over the licensed concurrent device count for short periods—the total usage is based on looking at the 95th percentile of concurrent device usage.

SafeConnect NAC has proven scalability, the Enterprise edition can scale up to hundreds of thousands of devices, but all Editions share the underlying architecture to easily scale to the licensed concurrent device level.

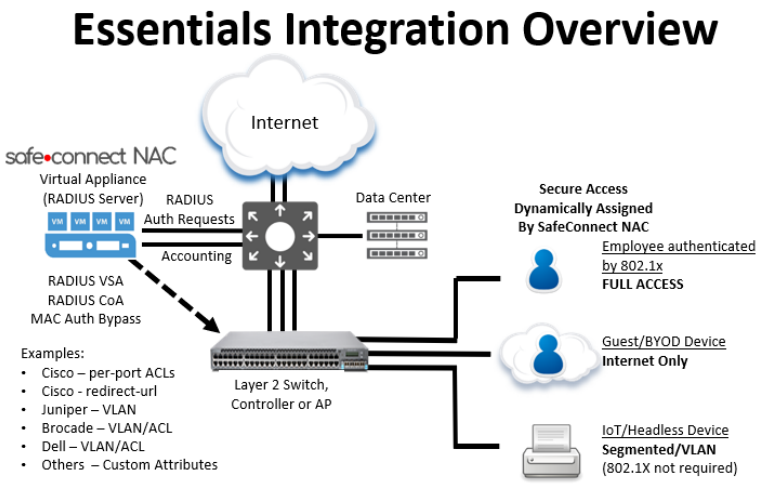
SafeConnect NAC has a modern user interface, designed for ease of use for all types of users, help desk, security staff, network engineers, and end users.

Essentials: Visibility, Control, and Compliance

For organizations that may not require all the capabilities of the SafeConnect NAC solution, Essentials is more than enough to ensure only authorized devices are allowed secure, compliant access.

SafeConnect Essentials provides port-level control and 802.1X control for wired and wireless devices. The devices that are permitted on can be automatically assigned to a segment (VLAN, etc.) to isolate IOT devices from sensitive portions of your network.

SafeConnect Essentials Device Authorization feature automatically segments your network by leveraging a MAC address whitelist, which can be bulk uploaded, to ensure only specifically authorized devices are permitted access. This is especially useful for IoT and headless devices that do not support 802.1X. Meanwhile on managed networks, the included RADIUS server can provide 802.1X/WPA2E to authenticate and ensure the connection is secure. SafeConnect NAC is pre-Configured for major vendors such as: Dell, Juniper, Cisco, and Brocade—just select the vendor from a dropdown. For vendors not supported out of the box, there is support for 3rd Party Custom Vendor/Attributes to control access.



Secure your Organization with the Standard

For organizations that need more than the essential level of access control, the Standard Edition provides the features small and medium-sized organizations need, this includes, a captive portal to ensure identity is collected for guest or BYOD users, real-time posture assessment to ensure Windows and macOS devices are complying with your organizations security policies, Contextual Intelligence Publishing, which shares the valuable context about devices, users, and identity to your SIEM, NGFW, or other security appliances.

SafeConnect NAC Standard leverages its built-in policy engine fed by the context correlation engine and optionally the Impulse end-point agent, the SafeConnect Policy Key, to control devices as they connect and then continues to reevaluate policy while connected. SafeConnect can then respond by auditing, warning, blocking, quarantining, or permitting access as your policies dictate.

Also, users and device can be authenticated in a variety of ways to fit your needs. Users on managed devices can be automatically signed-on through Active Directory (AD) Single-Sign-On (SSO). BYOD users and devices can also leverage AD or LDAP for authentication and authorization, while guests can make user of SafeConnect NAC's integrated guest portal.

For ease of on-boarding guests, a Guest Portal is included. Guest profiles can be configured to control if approval is required and the level of access a guest will be granted, including the duration of access. Support for SMS delivery of a one-click link for guests users tap for authentication

from a mobile device and support for emailing connection details is also included.

SafeConnect NAC Standard processes all the network inputs and presents help desk, network engineers, and security staff with visibility into the real-time posture assessment of all wired and wireless devices and users accessing SafeConnect secured networks. While SafeConnect' s automation reduces help desk incidents, when they do occur, help desk staff can easily view the state of users and devices and efficiently help end-users.

Standard also includes a full reporting module for further visibility into current and historical data. Reports can be customized and scheduled for email distribution. The per-device history can also be replicated to an external relational database for access by your organizations reporting tool or for integration purposes.

Deployment assistance is included in the Standard Edition, an Impulse Engineer will work remotely with your organization through our 5-step implementation process. This includes integrating with your network infrastructure, establishing communications with your directory services with self- service scripts and guides, and any other security integrations for Contextual Intelligence like a SIEM or NGFW.

Trusted and Proven for Enterprises

SafeConnect Enterprise, the edition Impulse has traditionally provided, scales up to hundreds-of-thousands of devices by clustering multiple appliances. Beyond that, it also provides network security orchestration by way of SafeConnect's Threat Enforcement capabilities.

Enterprise customers can optionally purchase Secure BYOD Onboarding, which offers a web-based, self-service solution that automates the configuration of user devices to ensure they connect securely with fewer hassles.

Identify. Secure. Orchestrate.

SafeConnect is an essential network security solution for protecting your critical data and intellectual property, combining the real-time visibility, security and orchestration required to address regulatory compliance and security policy automation. SafeConnect is delivered as a Cloud- Managed Service that relieves the organization of costly technical support related to on-going proactive monitoring, maintenance, and upgrades.

SafeConnect automates your security policies – from assessing compliance with security policies to determining if a specific application is running on a device while it is on the network. Other features include the following:

- Real-time agentless device identification of endpoints and user authentication prevents unauthorized devices and users from accessing critical network resources
- Dynamic identity-based network and application access assignment based on the role a user plays at your organization
- Guest self-enrollment and automated verification, including multiple guest access profile options and approval policies
- Self-guided remediation allows users to conform to security policies without help desk support

SafeConnect Solution Offerings

Identify and Authenticate. SafeConnect automatically recognizes when devices attempt access to wired, wireless, or VPN networks and provides agentless device profiling, user authentication, browserless Internet of Things (IoT) device enrollment, self-provisioning guest access management and real-time contextual intelligence reporting. This is an ideal solution to enable context-aware device visibility (identity/role, device type profiling, location, IP/MAC Address, and ownership/liability). Network access policies can be assigned by role, for example, enabling different privileges for employees, guests or vendors.

Posture Assessment. SafeConnect enhances the security posture of your network by providing real-time policy assessment, enforcement, and self-remediation for Windows & MAC OS X devices. Every user's system is checked prior to granting network access to ensure that the device adheres to your acceptable use policies (anti-virus, operating patches, personal firewalls, peer-to-peer software, etc.) as well as on a continuous basis after access is granted. Web-based, self-remediation orchestration enables users to conform to security policies without help desk involvement.

Secure BYOD On-Boarding. Welcome every new user with a captive web portal that authenticates the end user, configures the device's embedded 802.1X supplicant, and automatically transfers the device to a designated secure SSID network segment. By eliminating manual configuration, the solution delivers a more secure solution with a reduction in help desk calls and dramatically accelerates user adoption of WPA Enterprise or certificate-based secure wireless. Users are automatically associated with their secure

wireless network on subsequent network connections without the need for repeated logins

Network Security Orchestration. SafeConnect's Network Security Orchestration capabilities offer context-aware device visibility, security compliance, access control, and reporting through a single-pane-of-glass that provides enhanced cyber security defenses. With this approach, the focus is on blocking unauthorized devices.

- Automate policy enforcement based upon the risk levels reported by threat detection systems such as intrusion detection system (IDS) and Advanced Threat Protection (ATP)
- Publish real-time Contextual Intelligence information to next-generation firewalls, web content & bandwidth managers to enable much more granular policies
- Integrate with SIEM providers which enables much more detailed reporting for enhanced security assessment decisions in a timely manner.

Managed Support Services. 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 from excess time, risk and negative experiences to all facets of the organization.

In addition to its simplified architecture and enhanced user experience design, a key benefit is how the SafeConnect solution is delivered and supported. SafeConnect solutions are premise-based and come with a service that keeps the system updated regarding the latest devices, operating systems, and AV packages. In a world where users change and update their devices on a frequent basis, it is imperative that a security solution keeps ahead of these changes. SafeConnect's Remote- Managed Support Service includes the following:

- Remote installation, training and deployment assistance
- 24x7 proactive system monitoring
- Problem determination and resolution ownership
- Daily device type, security updates and policy configuration data remote backups
- Installation of all maintenance updates and application version upgrades

impulse

Impulse | A SafeConnect Network is a Secure Network Impulse is the leading provider of Secure Access for traditional networks as well as remote and cloud access. Impulse securely and efficiently automates this access for organizations of all sizes and needs by combining our simplified access control architecture, remote managed support services, and customer-centric business philosophy to enable customer and IT security freedom. Our customers know this as the Impulse Experience. Visit www.impulse.com

Specifications

for the latest and more complete specifications, readers should visit "SafeConnect Technical Requirements."

Appliances

Virtual Appliance

Standalone Appliance

Standalone Appliance Large Footprint

Appliance Specifications	SafeConnect VMWare Enforcer
VMWare Version	ESXi 5.1 or newer
Virtual Hardware Version	Minimum version 8
CPU	2 Quad Core CPUs (2-3Ghz)
Memory	16 GB Minimum
Hard Drive Storage	300 GB Minimum
Appliance Scalability	Up to 25,000 Devices
Network Interface	Gigabit NIC

Standalone Appliance Small Footprint

Appliance Specifications	SafeConnect VMWare Enforcer
VMWare Version	ESXi 5.1 or newer
Virtual Hardware Version	Minimum version 8
CPU	2 CPU Cores (2-3Ghz)
Memory	4 GB Minimum
Hard Drive Storage	300 GB Minimum
Appliance Scalability	Up to 1,000 Devices
Network Interface	Gigabit NIC

Microsoft Hyper-V

Standalone Appliance

Appliance Specifications	SafeConnect Hyper-V Enforcer
Server	Microsoft Server 2012 R2
Hyper-V Version	Hypervisor Generation
CPU	2 Quad Core CPUs (2-3Ghz)
Memory	18 GB Minimum
Hard Drive Storage	350 GB Minimum
Appliance Scalability	Up to 20,000 Devices
Network Interface	Gigabit NIC

Directory Server

Requirements	Additional Information
LDAP	LDAP compliant directory server
Microsoft AD	Windows Server 2012 or higher
MySQL	v4.2 or higher
Secure LDAP	• Public CA • Self-Signed Certificate • Copy of organizations Trusted Root Cert in PEM or Base64 format • Copies of other server certificates may also be needed

Layer 2 Wired Integration Switch Support

Function/Feature	Switch Requirement
802.1X Authentication (supplicant)	802.1X

MAC Authentication (no supplicant)	802.1X, MAB
MAC Authentication (no supplicant) with Identity	802.1X, MAB, COA, Redirect-URL or VLAN Assignment plus upstream Layer3 Redirect/PBR (for Enterprise)
Layer2 Network Access Assignment	802.1X, MAB, COA, Filter/VSA or VLAN Assignment
Layer2 Network Access Quarantine	802.1X, MAB, COA, Redirect-URL or VLAN Assignment plus upstream Layer3 Redirect/PBR (for Enterprise)

DHCP Service

Requirements		**Additional Information**
Aruba	Wireless Controllers	
Cisco	Cisco, CiscoCatalyst, ASA	
Windows	Server 2003 or higher	Windows Server 2003 or newer Requires installation of SafeConnect DHCP Syslog Relay service Minimum 700 MB disk space
Other	Bluecat, Infoblox, Lucent, SonicWALL	

SAML Single Sign On (SSO)

Requirements	
Google	Google Apps for Business/Education
Azure AD	Azure AD Premium
Duo Two-Factor	Duo Access Gateway
Okta	
OneLogin	
Dell One Identity Cloud Access Manager	
Gluu	
Other	