Release Notes – SafeConnect Version 6.4

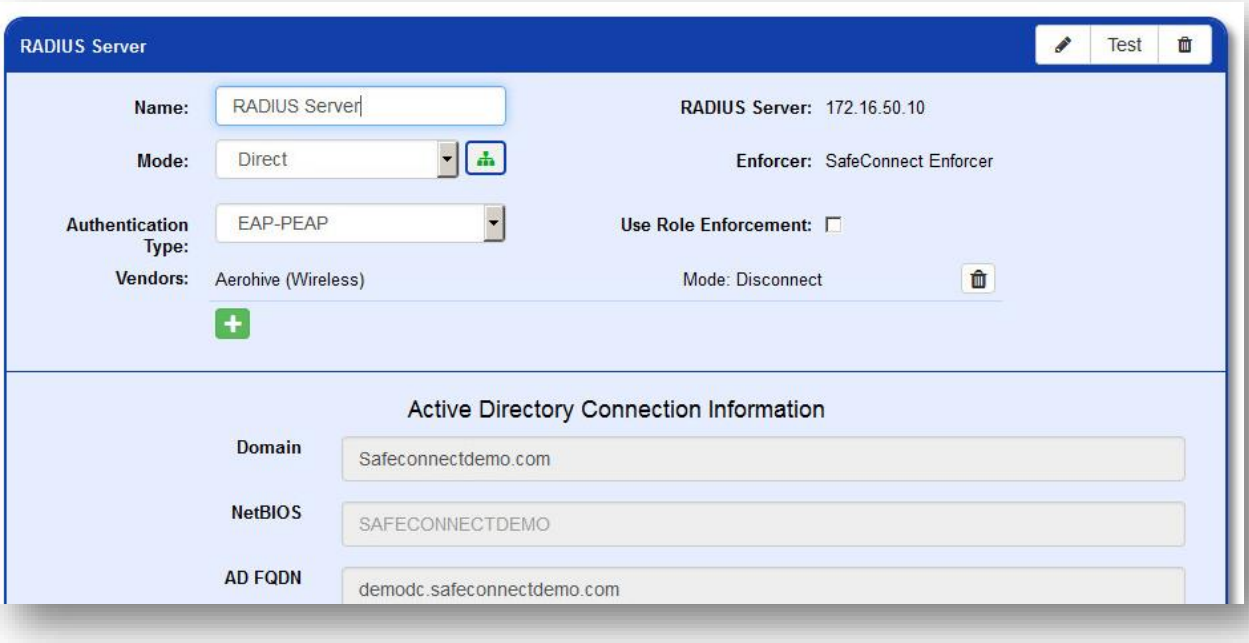
This document contains the latest release notes for the SafeConnect Product. All significant changes to the product in Version 6.4 are listed here.

Contents

RADIUS Enhancements

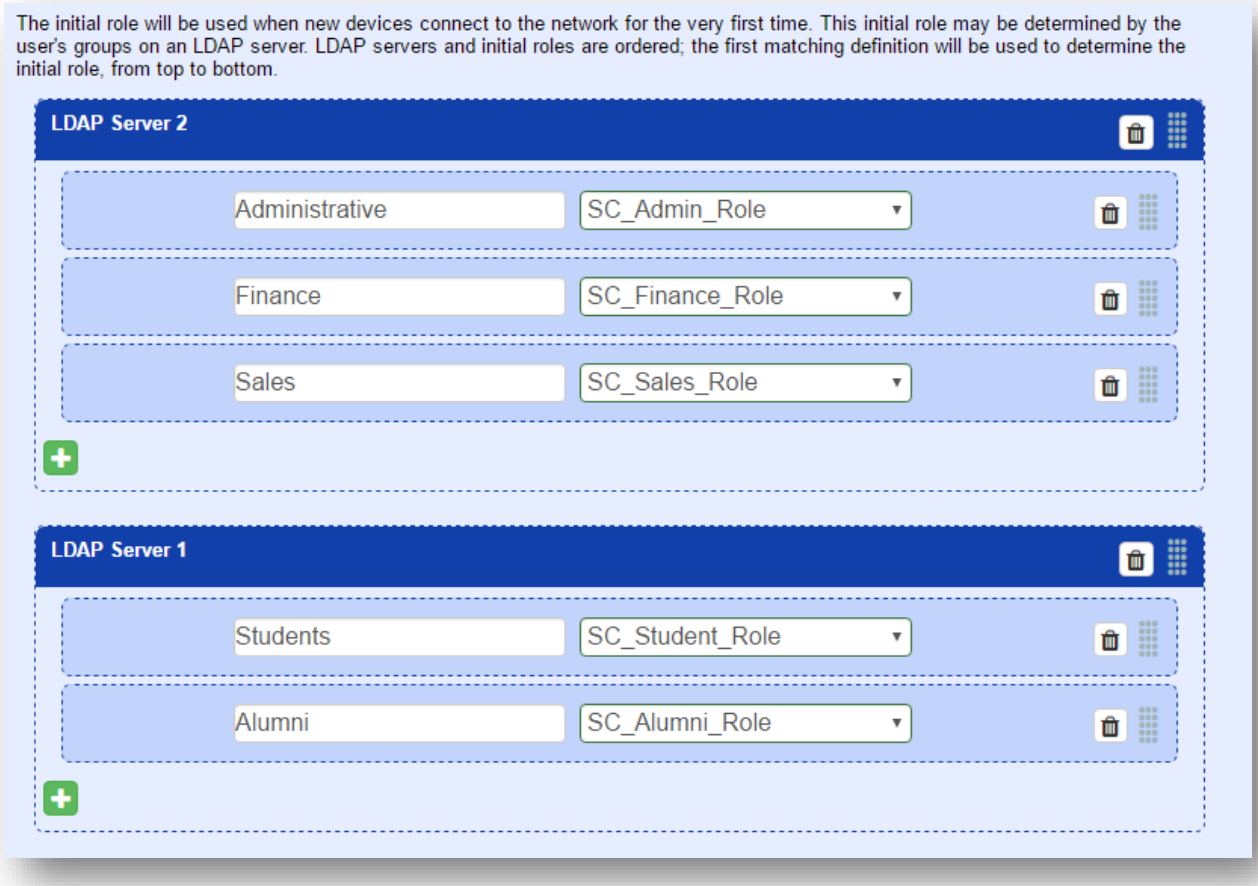
Authentication Only RADIUS Server

Configuration of SafeConnect as a standalone RADIUS authentication server has been streamlined for quicker, more intuitive configuration.



Initial Role Assignment Based on LDAP Group Membership

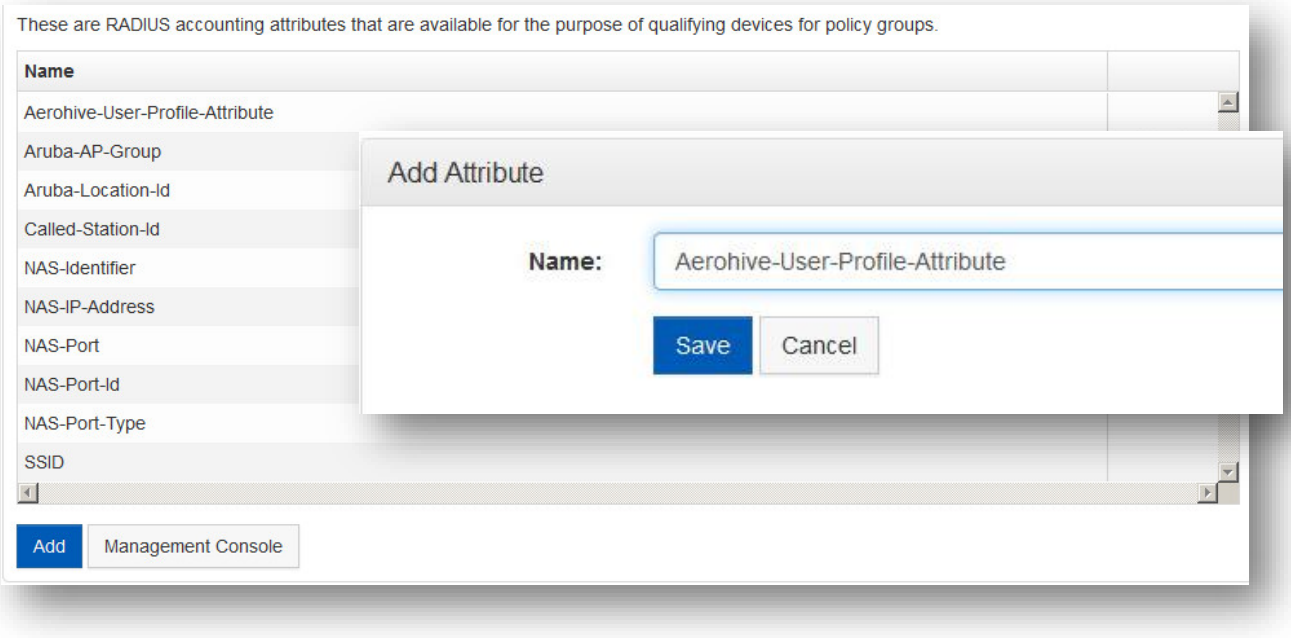
SafeConnect RADIUS now can assign a default role based on a user's LDAP group membership. This feature is available to devices using EAP-PEAP or EAP-TTLS authentication methods with an Active Directory or LDAP backend. Once configured, SafeConnect will assign the role to a device at the point a device associates with a RADIUS network. This feature is available in both RADIUS standalone and RADIUS-Based Enforcement (RBE) implementations.



Accounting Attributes as Qualifiers

SafeConnect can now use any attribute value that is present in RADIUS accounting as a qualifier for a policy group. This feature includes the ability to apply regex filters on the values for more advanced processing of values. Using this feature, Policy Groups can be created based on virtually any criteria desired, such as AP Group, REALM, Location ID, or any other attributes.

While there are many potential use cases, one example is assigning users to a different policy based on the Wireless Access Point to which they are connected, such as a common area (like a cafeteria) or an outside location. In this case, the AP Group could be used to qualify devices to an appropriate policy.



Out-of-Line RADIUS Enforcement for Aruba Wireless

SafeConnect now can optionally perform enforcement in Aruba Wireless environments without being present in the RADIUS authentication chain. With this feature, integrating SafeConnect into an existing Aruba Open or WPA2 wireless environment can now be deployed in an "out-of-line" fashion. The resulting implementation option means that SafeConnect can "fail-open" for Aruba Wireless deployments, and reduces a touchpoint in the RADIUS authentication process.

RADIUS-Based Enforcement Integrations

Juniper Layer 2 Wired Support

SafeConnect RADIUS-Based Enforcement (RBE) now supports Dynamic VLAN assignment and Layer2 port level control (including device security enforcement) for Juniper Network wired switches. Please contact Impulse Support to verify switch OS support and compatibility.

Meraki Wireless Support

SafeConnect RADIUS-Based Enforcement (RBE) now supports Meraki Wireless Access Point environments (including device security enforcement) for Open and Secure SSIDs. PSK SSIDs are currently not supported. Please contact Impulse Support to verify access point OS support and compatibility.

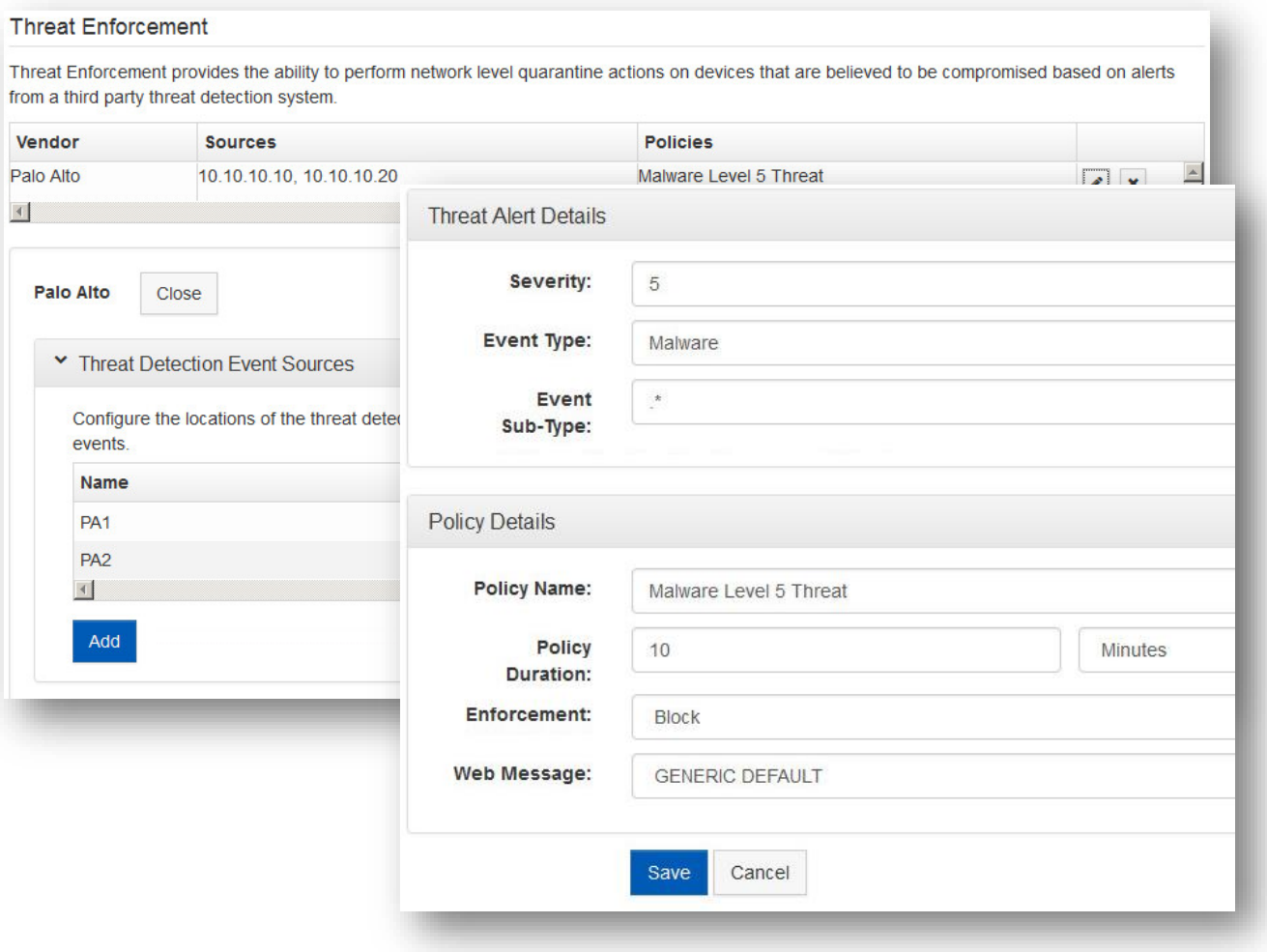
Policy Enhancements

Network Security Orchestration - Threat Enforcement Automation

SafeConnect can now define enforcement policies for threats detected by third-party systems such as intrusion detection system (IDS), next generation firewall (NGFW), advanced threat detection (ATD), mobile device management (MDM) or security information and event management (SIEM) providers. Using a threat enforcement policy, it is now possible to quarantine a device from the network based on security events that are received outside of SafeConnect. Included in this feature is the ability to display a customized web message to end users outlining the reason for the enforcement action and self-remediation guidance like other standard SafeConnect policies.

SafeConnect's Network Security Orchestration (NSO) also offers real-time context aware intelligence for device visibility, security compliance, access control, and reporting through a single-pane-of-glass for enhanced cyber security defenses.

Support for Palo Alto, SonicWALL and Juniper SRX Firewalls is included in this feature. Support for additional vendors will be added based on customer requests.



Managed Policies for Java, Adobe, and Acrobat

Java, Adobe Flash, and Adobe Acrobat are three significant sources of security vulnerabilities. As such, many organizations using SafeConnect have existing policies requiring devices to have the latest versions of these software technologies. SafeConnect Version 6.4 now includes automated updates for these policies; that is, as new versions of Java, Flash, and Acrobat are released, Impulse is providing these updates as part of our ongoing managed service maintenance (on a quarterly basis and for all major updates). Organizations no longer need to update these policies to the newest version, the SafeConnect will automatically receive the latest updates.

Management Interface Enhancements

Integrated Management Interface

Announced as a Version 6.3 pre-release, the SafeConnect Integrated Management Interface is now officially available. This is a significant redesign of the management interfaces using the latest user interface (UI) technology and techniques. Impulse continues to evolve the integration with the inclusion of Guest and User management in Version 6.4.

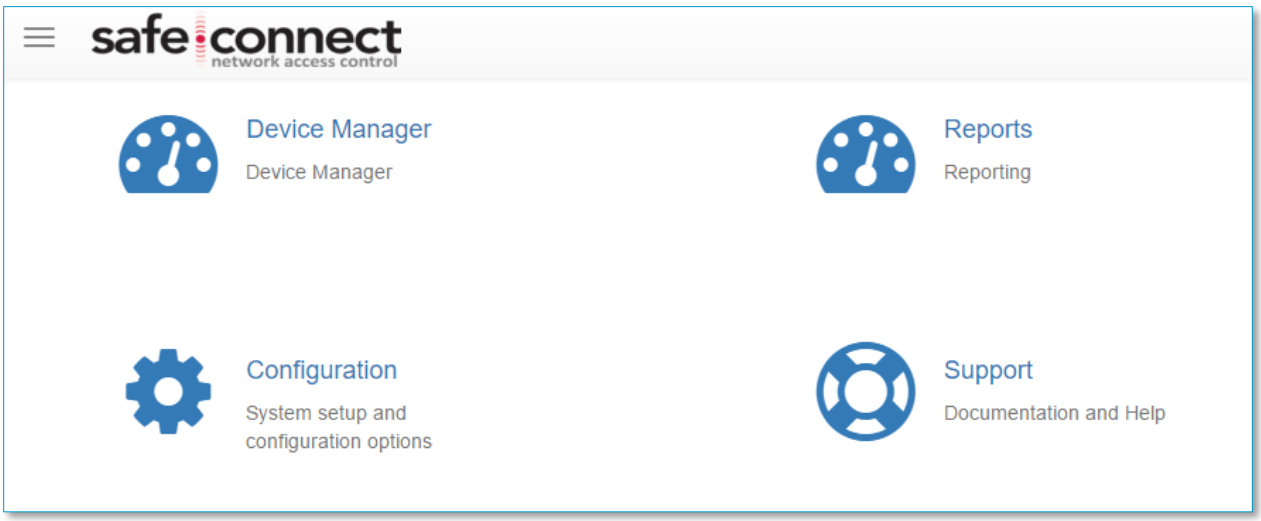
In addition to integrating the separate portions of the interface under one UI framework, portions of the UI were significantly improved, not just stylistically, but also in terms of the user experience and the functionality provided. Prime examples of going beyond the prior UI are the new Configuration Manager, Device Manager, and Report Manager.

Impulse will continue to flow through the rest of the UI over the next few releases, adapting all of it into this framework (e.g., the Policy Manager). While the new UI is evolving, the existing UI you currently use will remain in place.

Note: This new UI is not enabled by default, but is available to experience at your request. To gain access to the new UI, please send a request to support@impulse.com.

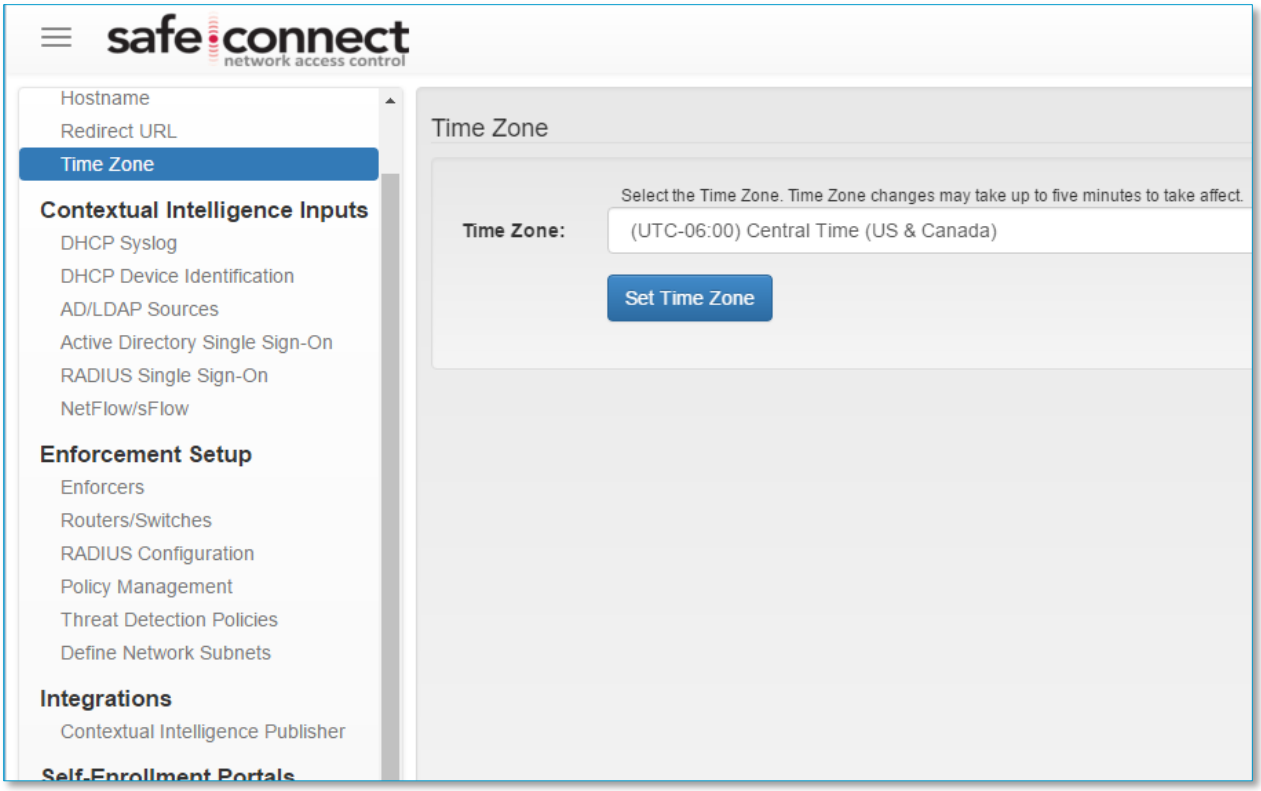
SafeConnect Integrated Start Page

The newly designed unified start page, shown immediately below, highlights the integration of the new UI. All aspects of the SafeConnect UI are available under a single login, from a central menu. Note that the menu in the upper-left of each manager also permits easy navigation between the different managers.



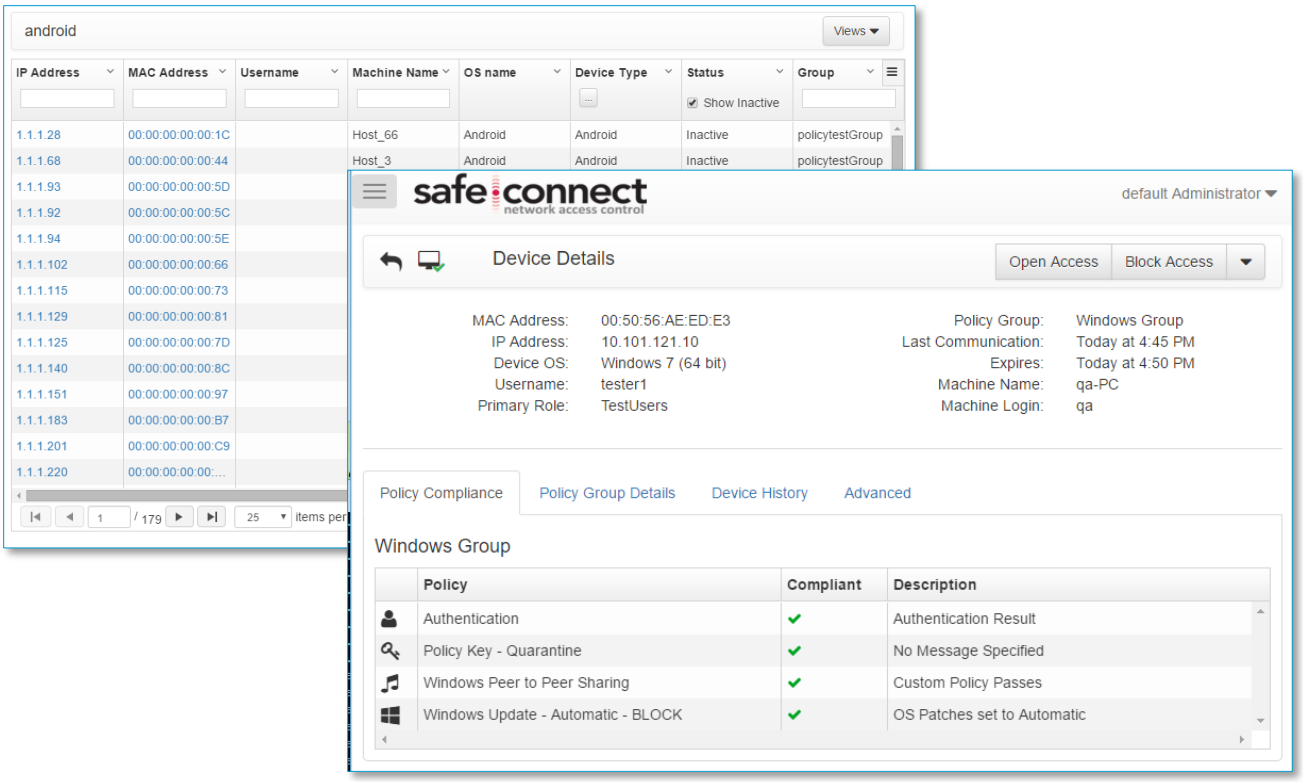
Configuration Manager

SafeConnect's new Configuration Module provides a centralized location for all configuration. Not only is the style updated, but new functionality has been added to enable customers to view and control more of the configuration, and perhaps most significantly, this new UI permits validation for all data input streams such as DHCP, NetFlow, etc. This validation provides needed visibility to customers to the various flows of information into SafeConnect from their network.



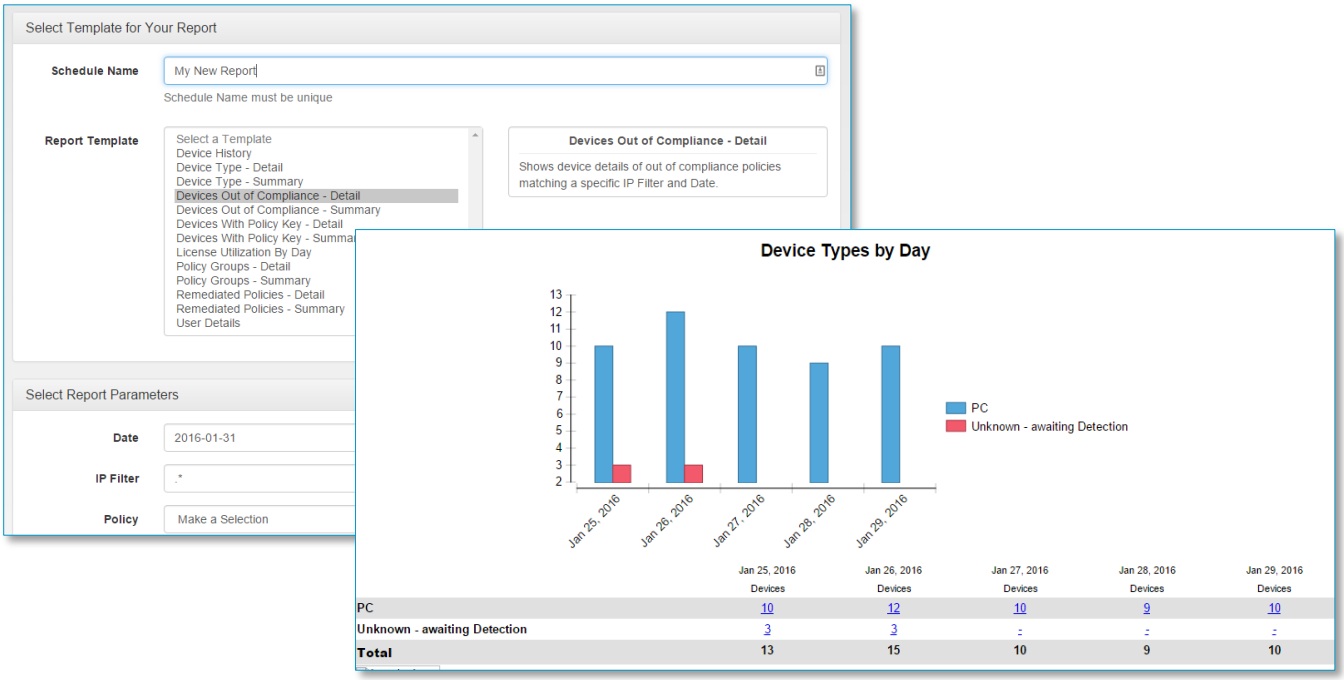
Device Manager

SafeConnect's new Device Manager interface offers a more intuitive and flexible user experience than the existing SafeConnect Dashboard, and provides enhanced functionality, such as the ability to create customs views. The Device Manager will ultimately include all the existing functionality of the existing SafeConnect Dashboard, but as of this release, aspects such as the charts are not yet included.



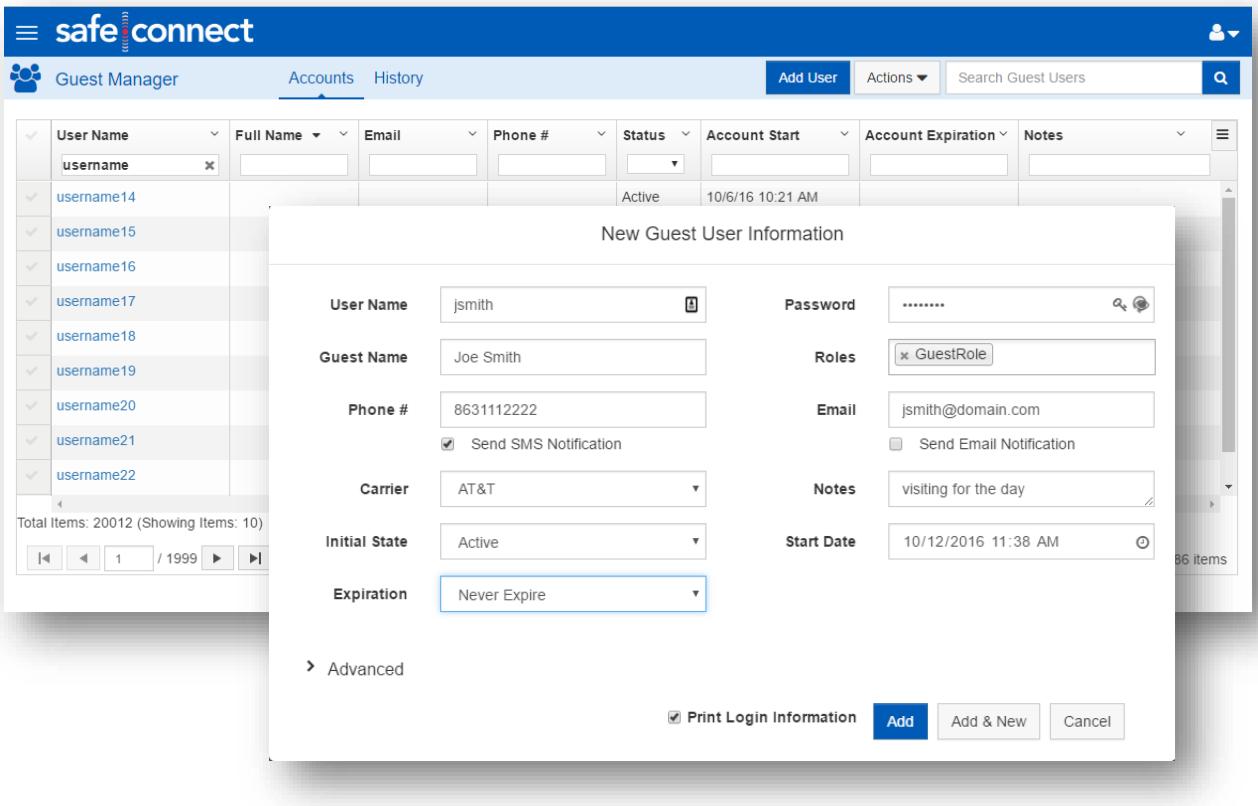
Report Manager

SafeConnect's new Report management module allows for enhanced reporting capabilities and the ability for customers to tailor and schedule pre-defined historical reports that can be emailed to the desired individuals on a periodic basis.



Guest Manager

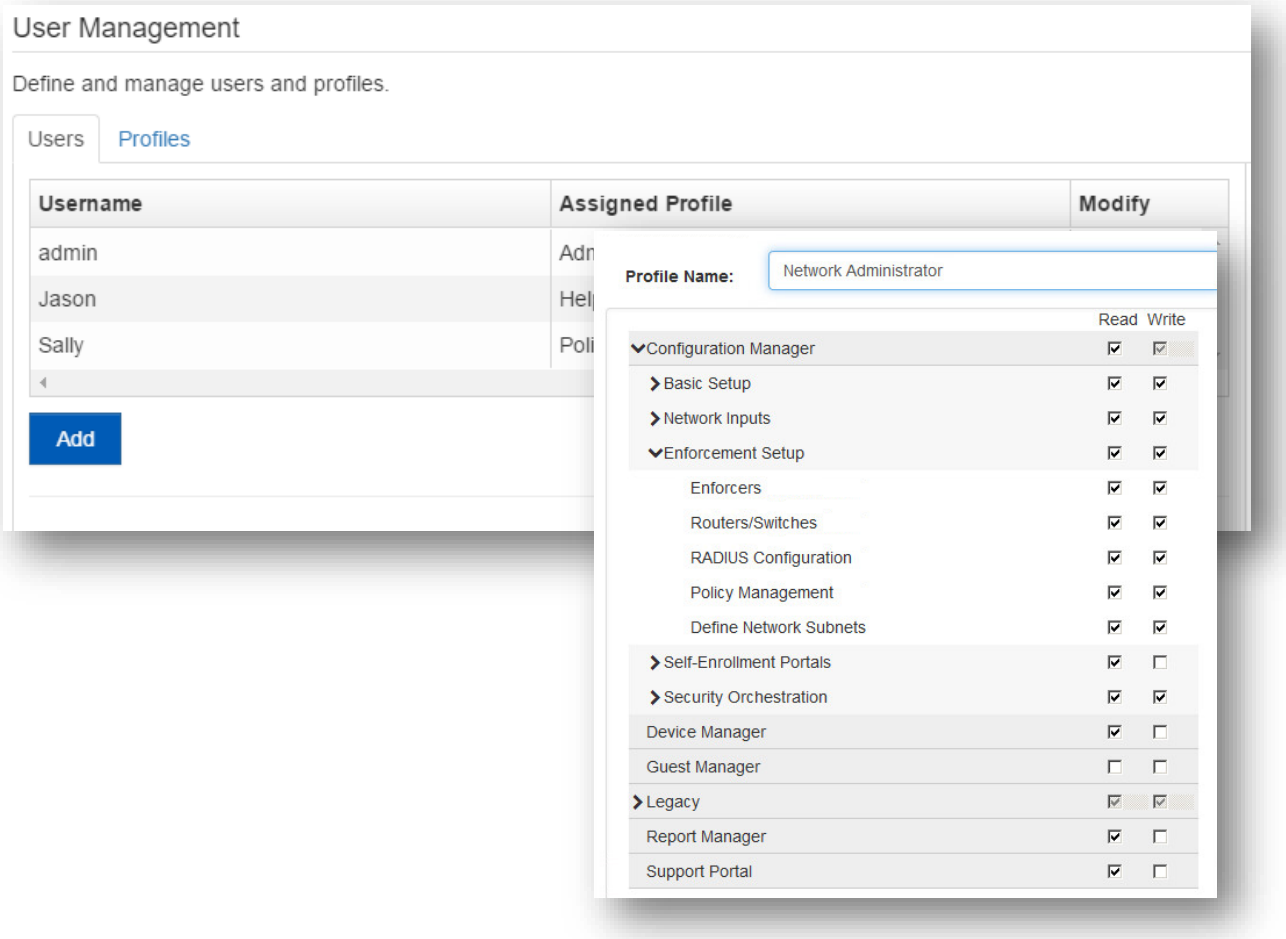
The SafeConnect Guest Manager has been updated for the new Management User Interface. All features from the legacy Guest Management Interface have been moved over and streamlined to better match the updated look and feel.



User Manager

The enhanced User Manager interface provides more fine-grained control over what aspects of the user interface help desk and administrative users can interact with. With the new enhancements, profiles are created with different permissions and then assigned to users. This gives the flexibility of creating profiles ahead of time and then granting access to the system by associating a user with a profile, which negates the need to add specific permissions for each user that is created.

A default set of profiles is included with the update as well as the ability to create customized profiles.



Transitioning to a Virtual Appliance

Due to the advantages of server virtualization (e.g., energy savings, improved availability, reduced rack space, and scalability at a lower cost), a growing number of SafeConnect customers are deploying SafeConnect as a virtual appliance. Given this rapidly increasing trend, over the next 18 months it is Impulse's intention to transition to a distribution model standardized around a virtualized deployment. If you are currently running on a hardware platform today, and are ready to make the transition, our Support Team will work with you to schedule this migration.

Note that SafeConnect's preferred virtualization platform is VMWare. SafeConnect does support the free version of VMWare ESXi, and this is how many of our customers have SafeConnect deployed today.