Release Notes - Version 6.01

Management Portal Enhancements . . . . . Page 2
- New Policy Manager . . . . . Page 2
- Group Structure . . . . . Page 2
- Bulk Import . . . . . Page 6
- Role Management . . . . . Page 7

Device Life Cycle Enhancements . . . . . Page 7
- SessionsTracker™ . . . . . Page 7
- Performance Improvements . . . . . Page 7

Identity Publisher . . . . . Page 7
Universal Device Attribute Qualifier . . . . . Page 8
MDM•Connect™ . . . . . Page 9
AD•Connector . . . . . Page 10
RADIUS-Based Enforcement (RBE) . . . . . Page 11
Enhanced Clustering . . . . . Page 12
Auto•Connect™ . . . . . Page 13
Impulse Point Licensing . . . . . Page 14
Other Feature Updates . . . . . Page 14
- Safe•Connect Policy Key . . . . . Page 14
- Broadcast Messaging . . . . . Page 14
- Historical Trending . . . . . Page 14
- Device Enrollment . . . . . Page 15
- NetFlow 9 Support . . . . . Page 15
- Guest Users Provisioning . . . . . Page 15
- Client History . . . . . Page 15
- NAT Behavior . . . . . Page 15
- High Availability . . . . . Page 16

Management Portal Enhancements

Impulse Point has introduced an integrated Web-based Management Portal as seen in Figure 1, below. Customers can control all policy management aspects of the Safe•Connect™ and Identity•Connect™ systems from a single Web-based portal interface. Components of the Management Console include the Policy Manager, Reporting Dashboard, and System Configuration, as well as Identity Publisher and MDM•Connect™ integration modules.

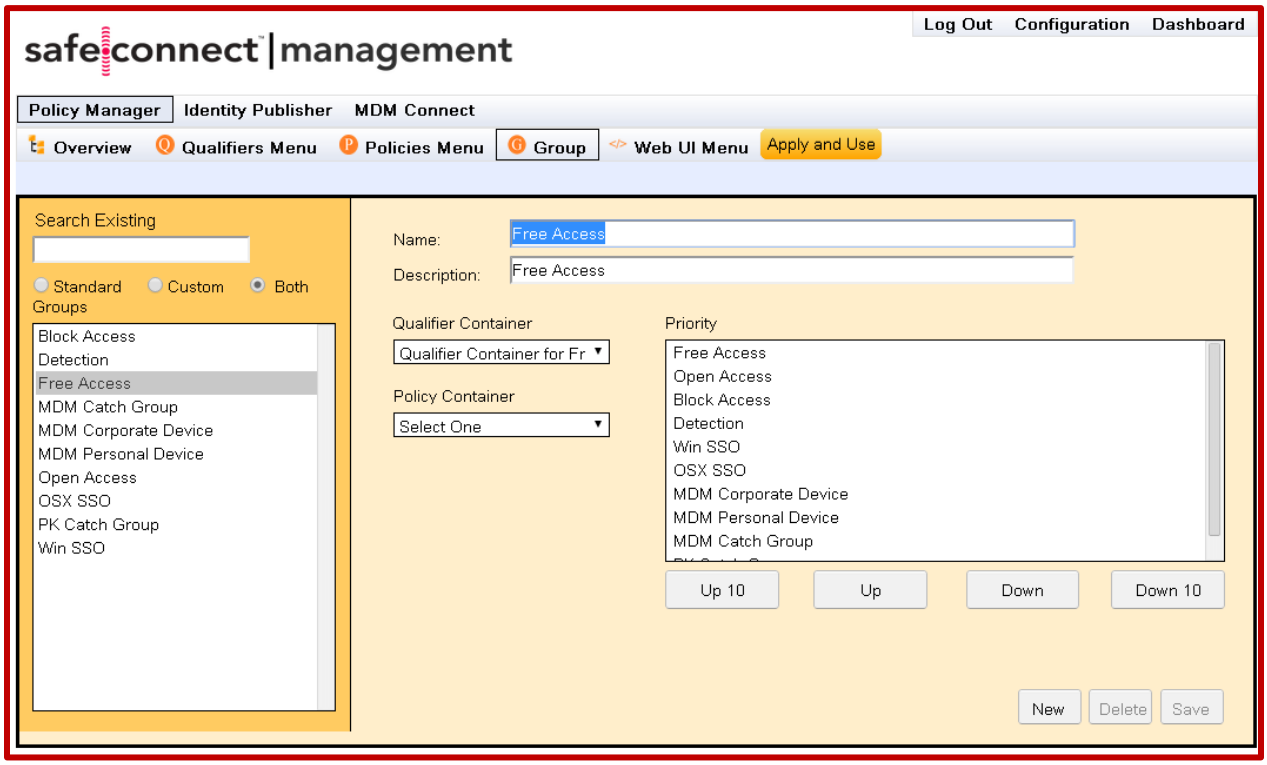

Figure 1. Policy Manager Group Screen (new Web-based interface)

New Policy Manager

The Policy Manager has been architecturally redesigned to present a browser-independent, common look and feel. This browser independence frees the Policy Manager from specific platforms or operating systems thus removing the need for software upgrading when enhancements are made. The Policy Manager can be accessed from any workstation or laptop using the policy administrator's browser of choice.

The Policy Manager integrates all functions of policy management for both Safe•Connect™ and Identity•Connect™ with a modular approach to configuring Policies and Groups by defining reusable "templates" and "components" such as Qualifiers, Qualifier Sets, Policies and

Containers that make system-wide changes simple, efficient, and resistant to human error. The new architecture supports tens-of-thousands of Qualifiers and Policy components (for example, IP address, MAC address, subnets, etc.) with intuitive operations like *move, update* and *bulk load.*

The redesigned Policy Manager also removes the requirement of "downloading and uploading" policies in a single session as well as eliminating the problem of simultaneous changes by multiple administrators. Policy Administrators can now create, delete, or edit policies over multiple sessions until they are ready to "*apply and use"* the new policy(s) in production.

Based on customer feedback, Impulse has greatly simplified the interface for editing Web messages in Safe•Connect by removing features that overlapped with more full-featured Web editors. The new interface now provides the ability to easily download the pages for offline revision in your editor of choice. Once local edits are complete, simply upload and preview them via the new interface before pushing them to production. The screenshot below (Figure 2) illustrates the Policy Manager's new, easy to use "Web Messages" interface, including the "*Search Existing*" tool which accelerates the task of locating and changing web messages and other components or policies.

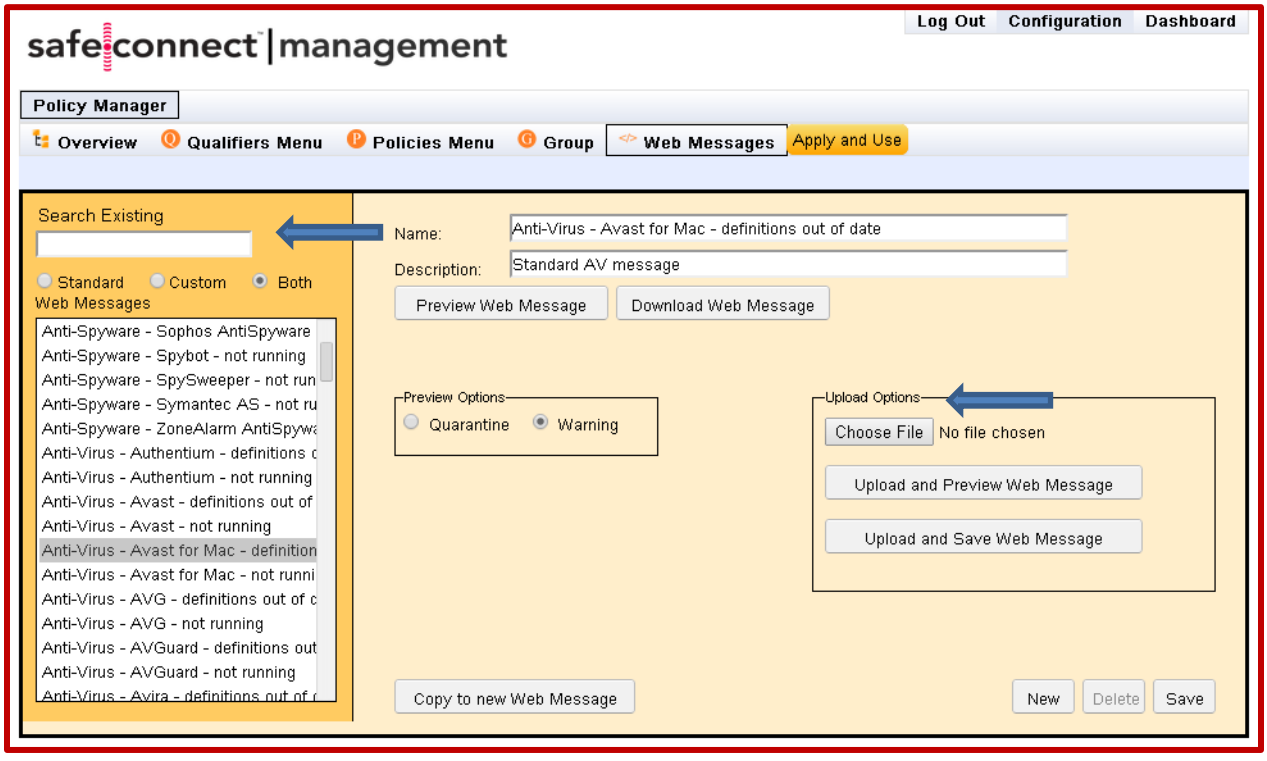

Figure 2. The Web Message Upload Options and Existing Message Search Tool in the Policy Manager

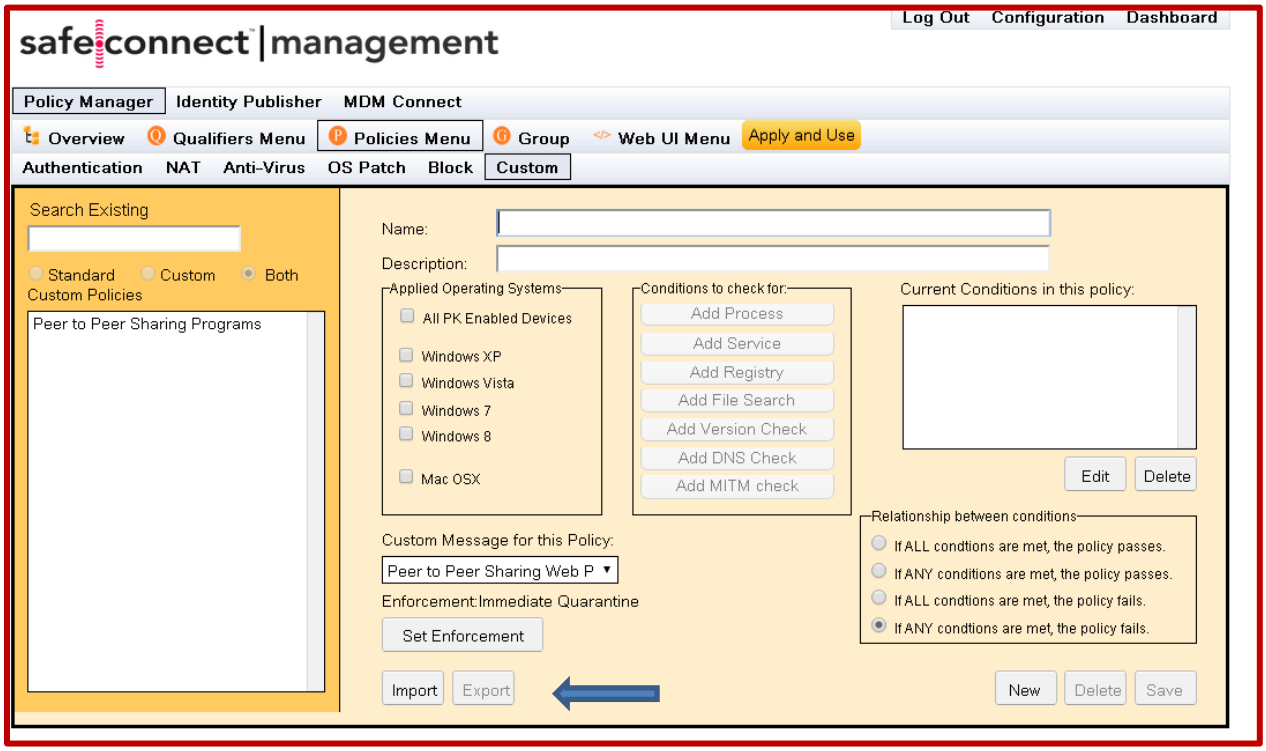

Figure 3. The Import and Export Tools in the Policy Manager

Policy Enforcement options have been streamlined based on customer feedback and best practices. Customers can now choose from a number of preselected enforcement options including Audit, Warning, and Quarantine Enforcement actions. In addition, policy administrators now have the ability to "import" and "export" custom policies in XML format within the Policy Manager as seen above in Figure 3.

Group Structure

Version 6.01 of Safe•Connect™ and Identity•Connect™ provide a new, highly flexible group structure which takes advantage of newly introduced reusable components such as Qualifiers, Qualifier Sets, Policies and Containers. When placing clients in Policy Groups, the Policy Manager now validates that a client matches each Qualifier Set in the Container. The new group structure also allows administrators to create groups using "AND" conditions that support policies based on multiple attributes such as Identity and Network Locations (i.e., students in the dorms, vs. students in classrooms).

The diagram below depicts the new qualifier and policy configuration flow approach:

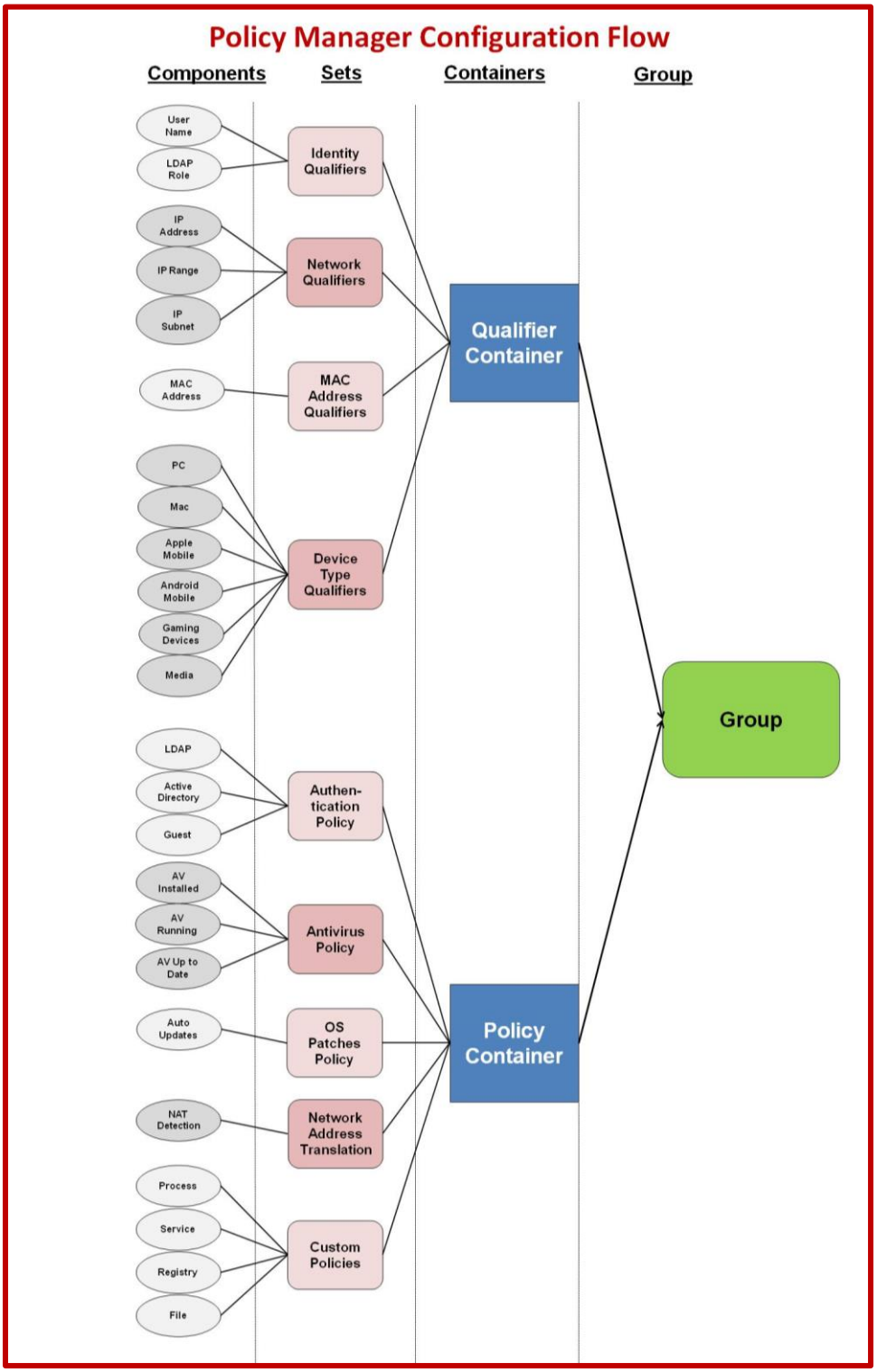

Diagram 1. Qualifier and Policy Container Organization and Flow in the Policy Manager

Qualifier Container organization and configuration flow is depicted in Diagram 1, above. As the diagram indicates, Qualifier Containers can contain one or more Qualifier Sets. Additionally, each Qualifier Set can contain one or more Qualifiers.

Policy Containers can contain one or more Policies. Additionally, Policies can contain one or more Policy Components. A Group is the assignment of a Qualifier Container and a Policy Container.

Bulk Import

When creating new Groups, customers can now leverage the new Bulk Import feature. A template is provided that streamlines the creation of Qualifer Sets. Customers can bulk load any type of Qualifier (IP address, IP range, Subnet, MAC address, etc). When uploading from the template, qualifiers are automatically added into a Qualifier Set and ready for use.

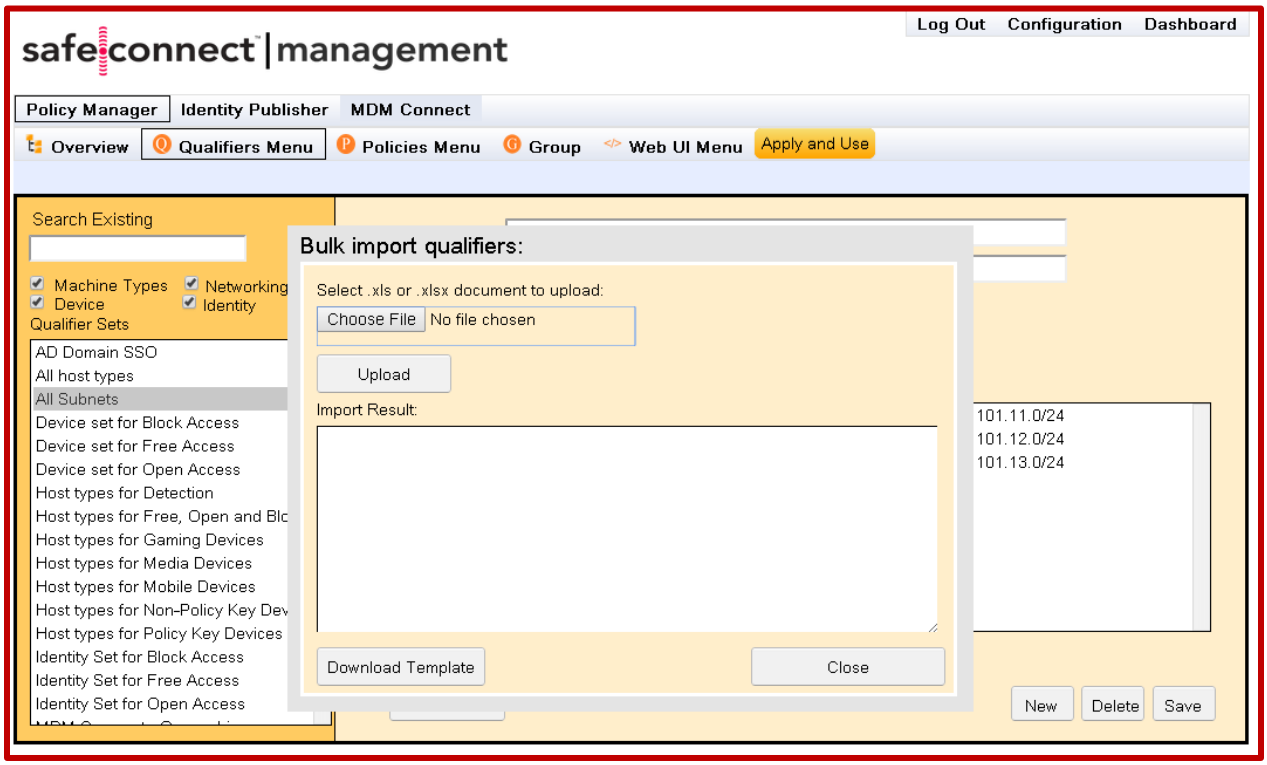

Figure 4. Bulk Import

Role Management

Enforcement Role Management has also been updated in support of RADIUS-Based Enforcement (RBE), as described later in this document on page 11. Customers can now create new enforcement roles and control which Vendor Specific Attributes (VSAs) are attached to these roles. Enforcement roles can be assigned globally, or per policy group.

Policy groups can have different enforcement roles for compliant devices and non-compliant devices. Version 6.01 introduces support for Cisco and Aruba VSAs. Additional vendor VSAs will be added based on customer demand.

Device Life Cycle Enhancements

SessionsTracker™ (Impulse Point's identity-to-device session correlation engine) was originally introduced in Safe•Connect™ Version 5.5 as a standalone component. Beginning with Version 6.01, SessionsTracker™ is now an embedded and distributed component of every instance of Impulse Point's product architecture. This allows for increased correlation of information from network technologies like RADIUS, DHCP, and Netflow/sFlow to formulate real-time "session information" for specific devices and users in a highly scalable manner. All aspects of client lifecycle behavior are now configurable. For example, customers can now match specified DHCP lease times to each corresponding network segment where Impulse Point is deployed to enhance the granularity of client lifecycle information.

Performance Improvements – Life-cycle management has been improved by centralizing the management and coordination of all network observation services. These improvements, coupled with numerous Version 6.01 enhancements in packet processing, queuing and multi-threading have demonstrated upwards of quadruple the performance previously seen in earlier versions of SessionsTracker™ and Impulse Point products. As a result, Version 6.01 is able to process, in real time, the required Netflow, DHCP, and RADIUS data to accurately track the dynamic nature of today's networks.

Identity Publisher

Version 6.01 introduces real-time identity publishing which allows direct integration with third-party management systems that require real-time access to identity-to-device information in support of identity-based policy management.

Identity Publisher is compliant with the Trusted Network Computing Group's IFMAP 2.0 Standard, enabling the publishing of all relevant metadata to an IFMAP Server. In addition to IFMAP, Impulse Point also provides direct integration identity publishing support for iBoss (web

content filtering), Procera Networks (bandwidth management), and Palo Alto Networks (application-aware firewall) platforms as well as the Native JSON Interface format. Additional third-party solutions will be added based on customer demand. Please contact Impulse Point Customer Support for additional information.

Universal Device Attribute Qualifier

Safe•Connect Version 6.01 introduces the new Universal Device Attribute Qualifier which enables policy group creation for Identity•Connect and Safe•Connect based on additional device attributes. Customers can use this new qualifier to place users in policy groups based on a number of criteria, such as domain membership and device ownership. Impulse also has extended the functionality of Policy Keys to now store the domain membership of an endpoint as a device attribute. Additionally the AD•Connector and MDM•Connect™ (described below) also support the capture and storing of device attribute information.

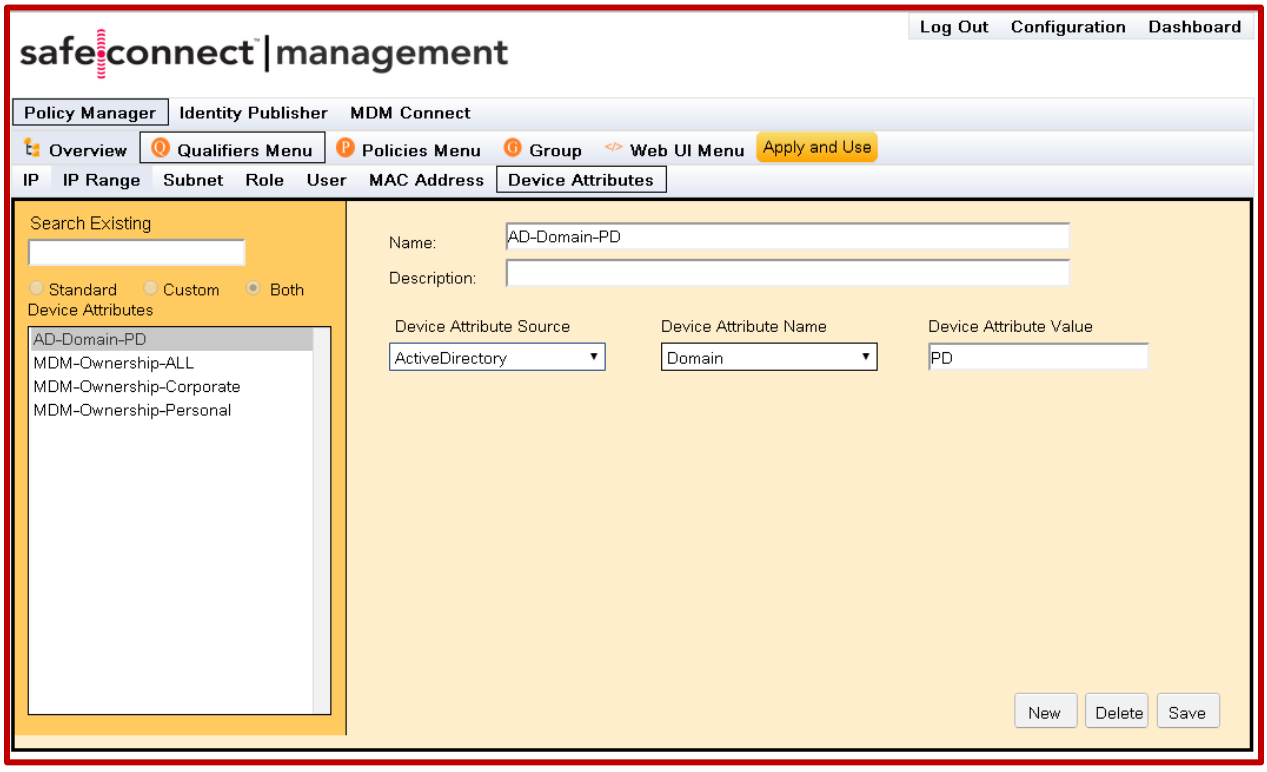

Figure 5. Device Attributes in the Policy Manager

MDM•Connect™

Continuing with Impulse Point's endpoint security policy management heritage, Version 6.01 now directly integrates with industry leading Mobile Device Management (MDM) providers. Impulse Point's MDM•Connect™ integrates with premise or cloud-based MDM solutions like AirWatch and Tangoe to provide a comprehensive policy management framework to address mobile computing devices. MDM•Connect™ was designed with an open standards-based approach to enable a universal and consistent method of quickly integrating new MDM•Connect™ partners.

MDM•Connect™ can be configured to query a customer's MDM solution on-demand, at predefined time intervals, or accept event-driven information published by MDM providers. Safe•Connect™ and Identity•Connect™ leverage this information in real-time to deliver the following incremental benefits:

- Provides certified integration with industry-leading MDM providers
- Allows customer flexibility to choose which MDM solution is best for their business, industry, and user environment
- Automates MDM provisioning/onboarding user experience by detecting, blocking (at a network level – not dependent on active sync email enforcement), and redirecting all unknown mobile devices to the MDM Registration Portal to ensure MDM compliance
- Provides the ability to apply network-level quarantine to all mobile devices that are not registered or are non-compliant with MDM policies as well as provide Web-based self-remediation guidance
- Assigns application and network resource access privileges to mobile devices based on MDM role assignment (i.e., company-owned, BYOD personally-owned, device type, policy status, location and identity/role (faculty, staff, guest, vendor, etc.))

MDM•Connect™ enables the enforcement of the following pre-defined MDM policies:

- Policy Information
    - Registration Status
        - Has the mobile device completed MDM server registration?
    - Compliance Status
        - Does the device comply with MDM configuration and security policies (a roll-up of multiple MDM-configured policy settings)?
    - Passcode Lock
        - Does the mobile device have a password enabled?
    - Disk Encryption

        - Does the mobile device have encryption enabled for local storage?
    - Compromised OS
        - Has the mobile device been “jail-broken” or “rooted”?

The Impulse Point reporting dashboard also benefits from the addition of MDM•Connect™. The following real-time and historical reporting information will be published in the dashboard.

- Device Reporting Information
    - IMEI (International Mobile Station Equipment Identity)
    - Manufacturer
    - Model
    - OS Version
    - Phone Number
    - Serial Number

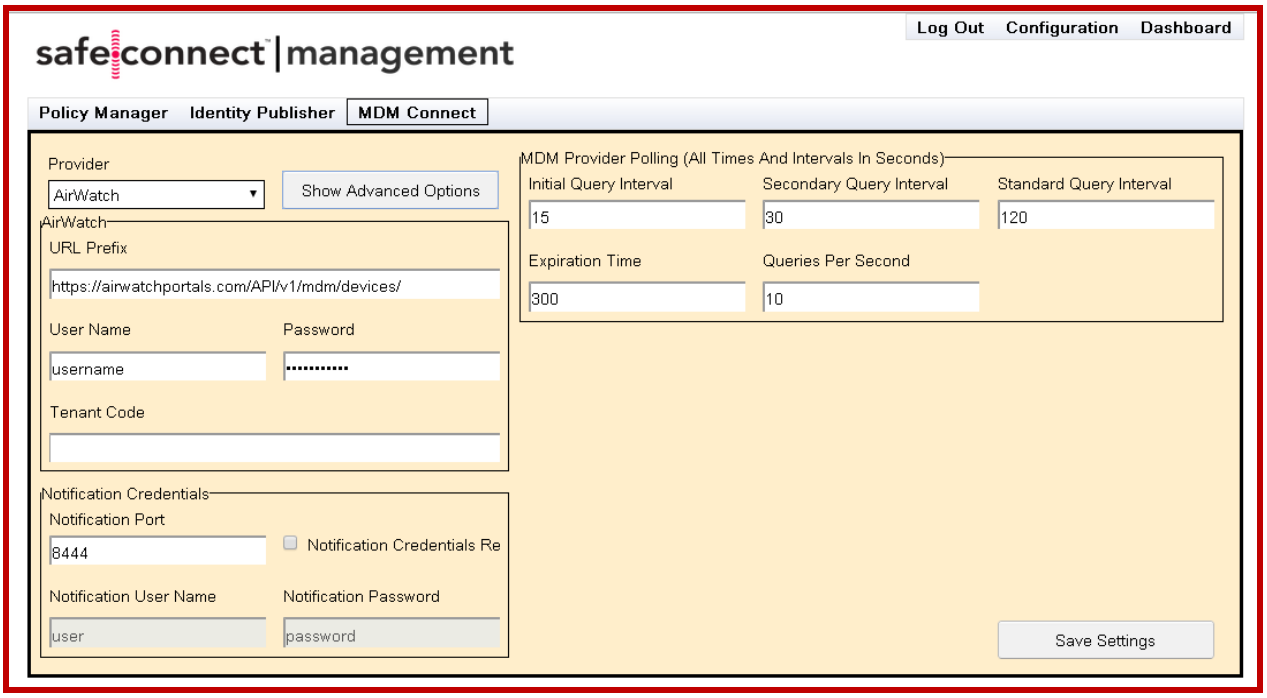

Figure 6. MDM•Connect in the Policy Manager

AD•Connector

Also new in Version 6.01 is the Impulse Point AD•Connector which allows for the centralized collection of Active Directory user sign-on events from one or more Active Directory servers (supports Windows Server 2003, Windows Server 2008, and Server 2012). The sign-on events will be relayed from the active directory servers to the Policy Manager for single sign-on (SSO)

purposes as well as associating the domain membership device attribute for assigning policies to managed (i.e., company-owned) Windows or Apple OS X devices. This allows the above functionally to be delivered without the need for a Safe•Connect Policy Key.

RADIUS-Based Enforcement (RBE)

In addition to Impulse Point's existing Layer3 Policy Based Routing (PBR) network enforcement, Version 6.01 introduces a new device enforcement option; RADIUS-Based Enforcement (RBE) which delivers dramatic scalability enhancements, and more granular network and application access role assignments for 802.1X/WPA2 Enterprise and Open wireless network environments.

As mobile devices exponentially increase network density, a more flexible, scalable and dynamic mechanism is needed to manage device enforcement. Recognizing this, Impulse Point has announced RBE to support the massive increase of mobile devices on the network. Capitalizing on existing customer investments in wireless technologies, RBE utilizes network-based communication standards to manage user/device role and access control.

Impulse Point's RBE module includes a RADIUS proxy server that (in conjunction with a customer's existing RADIUS authentication environment) leverages the "Vendor Specific Attributes" (VSAs) of wireless network controller platforms to control network access privileges. Unlike other industry approaches, RBE does not require customers to change/abandon their existing investment in RADIUS infrastructure. Customers are free to choose which RADIUS "authentication" platform is best for their organization and RBE handles the device's RADIUS "authorization" access on the network.

It is important to note that the customer's RADIUS infrastructure continues to provide primary authentication services. For example: If a customer's RADIUS environment is configured appropriately, Impulse Point's RBE will fail-open whereby the wireless network will revert to its original state of RADIUS authentication-only.

Another key benefit of Impulse Point's RBE is its non-reliance on VLAN Steering. Within a wireless network environment, VLAN manipulation is a resource burden to design, deploy, and support; in addition to contributing to a poor end user experience every time a device is forced to change VLANs. Impulse Point's RBE utilizes "*Dynamic*ACL" technology to assign network access privileges to a specific device versus moving a device to a common VLAN. RBE's non-VLAN approach for wireless networks offers the following benefits over other vendor alternatives:

- Easier to design, deploy, and support – Fewer technical resources required

- Real-time post-admission network access assignment – No need to remove or re-authenticate a device to change network access status
- A better end user experience – No IP address/VLAN changes
- Higher level of device quarantine/segmentation – Devices are restricted/isolated directly, not placed into a shared/quarantine VLAN

An example of an RBE device access transaction is detailed below that fully supports both Secure 802.1X/WPA2 Enterprise and Non-encrypted Open SSID wireless network environments.

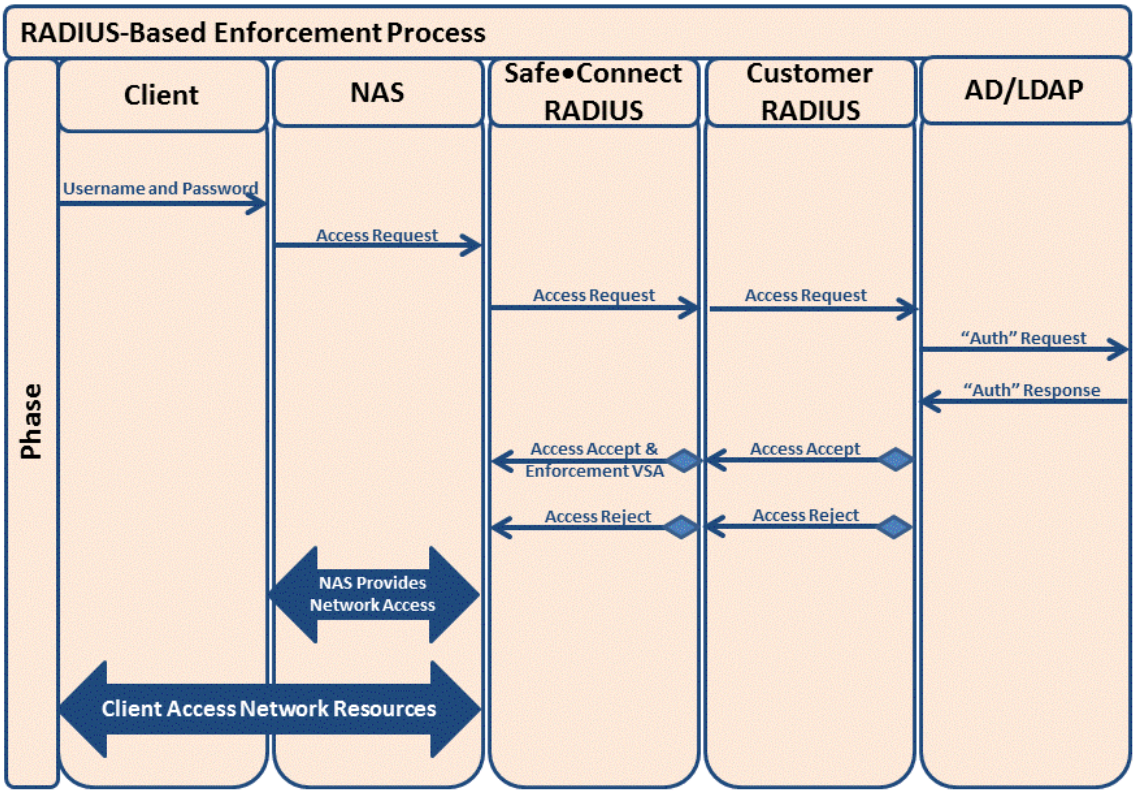

Figure 7. Sample Impulse Point RBE Transaction

Enhanced Clustering

Version 6.01 of Impulse Point products has increased the density and capacity of clustered configurations to support 300,000 devices in a single installation. Additionally, customers can now see the list of Policy Enforcer appliances and control which Enforcers manage which enforcement devices. Subnets are now mapped directly to enforcement devices, allowing customers to control how networks are managed, and by which enforcement device.

Auto•Connect™

Auto•Connect™ is a new optional product that automates the process of on-ramping devices onto secure 802.1X-WPA2 Enterprise wired and wireless network environments.

Auto•Connect™ provides an easy to deploy and manage solution that addresses the challenges of an end user manually configuring their device to access a secure 802.1X-WPA2 Enterprise wired or wireless network.

In conjunction with Safe•Connect™ or Identity•Connect™, Auto•Connect™ enables a customer to welcome every new user with a captive Web portal that authenticates the end user, configures the device's embedded 802.1X supplicant to support the organization's secure network, and automatically assigns (or moves) the device to a designated secure network segment where it will immediately associate in single-sign-on fashion on subsequent network connections.

Impulse Point Licensing

The following are definitions relating to Impulse Point Licensing:

Device - A device is defined as any network addressable system associated with a "Qualified Network" managed by Safe•Connect™ or Identity•Connect™.

Concurrent Device Count - The concurrent device count is determined by the highest number of concurrent devices that Impulse Point is managing over a 30 minute period per day.

License Determination - Impulse Point employs a 95th percentile concurrent device utilization method to determine license tier. Impulse Point records the top concurrent device count on a daily basis and uses this information to determine licensing over the previous year. This 95th percentile approach removes a customer's extreme device count peaks from the license calculations.

Bursting Allowance - The Impulse Point system is designed to allow customers to "burst" above their concurrent device count license tier without restriction. This means the system will continue normal operations if the concurrent device count exceeds the license tier level. This method will not require the purchase of additional licenses as long as the 95th percentile concurrent device count remains within the current license tier level.

Other Feature Updates

Safe•Connect™ Policy Key

- The Safe•Connect Policy Key included in Version 6.01 fully supports Windows 8 and OS X 10.9 Mavericks.
- The Policy Key policy (which enforces the installation of a Policy Key) can now be configured as a Warning or Audit Enforcement action in addition to a Quarantine Enforcement action. Administrators can choose which option works best for their deployment. If an end user installs the Safe•Connect Policy Key, administrators can observe and enforce the policy compliance status of an end point in the Safe•Connect Dashboard.

Safe•Connect™ Broadcast Messaging

- Based on customer utilization, the Broadcast Messaging functionality is no longer required due to the prevalence of multi-modal emergency alerting mechanisms and has been removed from Safe•Connect.

Historical Trending

- The Safe•Connect dashboard now provides graphical trending charts that allow customers to see statistics over time. Customers can view historical trends that show:
    - Device Types, Groups, Access Roles, Policy Compliance, and License Count

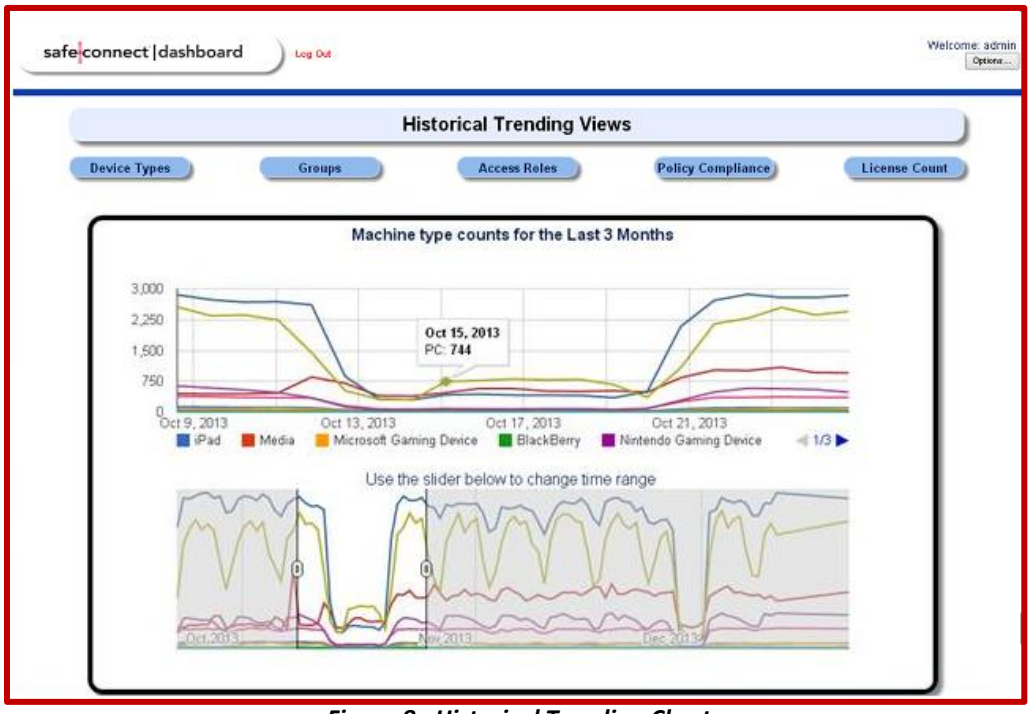

Figure 8. Historical Trending Charts

Device Enrollment

- User names contained in device enrollment are now used for single-sign-on purposes. When an enrolled device enters the network, the username will automatically be submitted for authentication.

NetFlow 9 Support

- Impulse Point products now support NetFlow v9 as well as v5.

Guest User Provisioning

- Guest users now have the option to select from additional SMS providers when creating their guest accounts.

Client History

- The following client history events have been updated
    - **Startup PK**
        - Indicates a Policy Key Startup at the beginning of a session.
    - **Scan PK**
        - Indicates the Policy Key has updated the Policy Results for a client.
    - **Start SES**
        - A new Network Session has started.
    - **Stop SES**
        - An existing Network Session has stopped.
    - **Expire Col SES**
        - Network data has caused a collision between two sessions resulting in the expiration of the existing session.
    - **Expire Col SC**
        - Safe•Connect™ (Policy Key) data has caused a collision between two sessions resulting in the expiration of the existing session.
    - **Expire Dash**
        - The SessionsTracker client was expired via the Dashboard.
    - **Expire Timeout**
        - The SessionsTracker client went a prolonged period without a heartbeat, and expired.

NAT Behavior

- Version 6.01 has standardized behavior around personal wireless routers and virtualization software performing Network Address Translation (NAT). Impulse Point considers it a ***best practice*** to block/quarantine devices performing NAT.

- In all situations, the first device behind the NAT device will be elected as the controlling device and all other devices will inherit the policy and enforcement status of this new controlling device—regardless of whether the device is Policy Key-enabled or not. During a transition, a new controlling device will be selected which may potentially result in a disruption of service for other clients behind the NAT'd Device.

High Availability

An automated High-Availability (HA) option is now available for a stand-alone appliance or a Policy Manager within a cluster. An individual Policy Enforcer failure will not cause a system-wide outage and will fail-open.

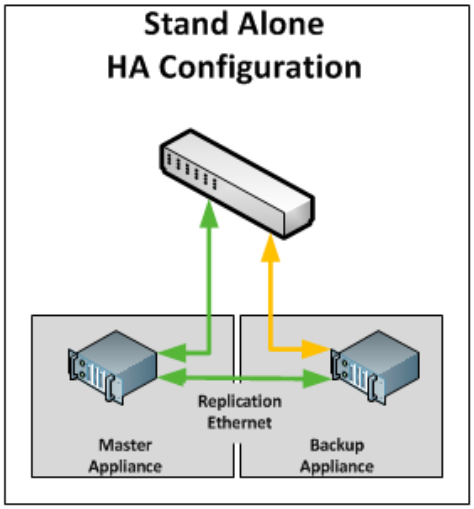

Diagram 2. Stand Alone Manager Enforcer Configuration

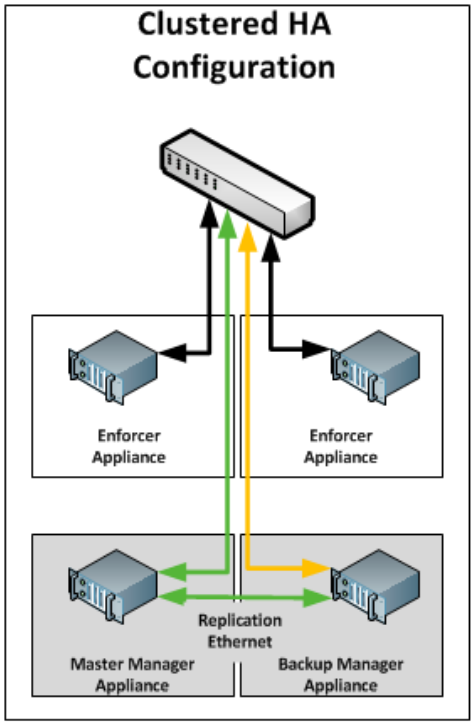

Diagram 3. Cluster Configuration