Release Notes – SafeConnect Version 6.2

Multi-NIC Awareness for Policy Key Devices . . . . . Page 2
- End User Experience . . . . . Page 2
- Reporting . . . . . Page 2

RADIUS Server Enhancements . . . . . Page 3

Simplified RBE Network Configuration . . . . . Page 3

Operating System and Security Updates . . . . . Page 4

- **Windows 10 Support . . . . . Page 5**
- **Security Updates . . . . . Page 5**
- **Anti-Virus Updates . . . . . Page 5**

Other SafeConnect Enhancements . . . . . Page 5
- Policy Key Optionally Triggers Re-Authentication . . . . Page 6
- Improved Xbox One Detection . . . . . Page 7
- Enhanced Visibility In to Enforcement Stages . . . . Page 7
- “Always Pass” Authentication Policy . . . . . Page 8
- User Count by Group Includes “Not Under Policy” View . . . Page 9
- Simplified Navigation to Guest and Device Enrollment . . . Page 9

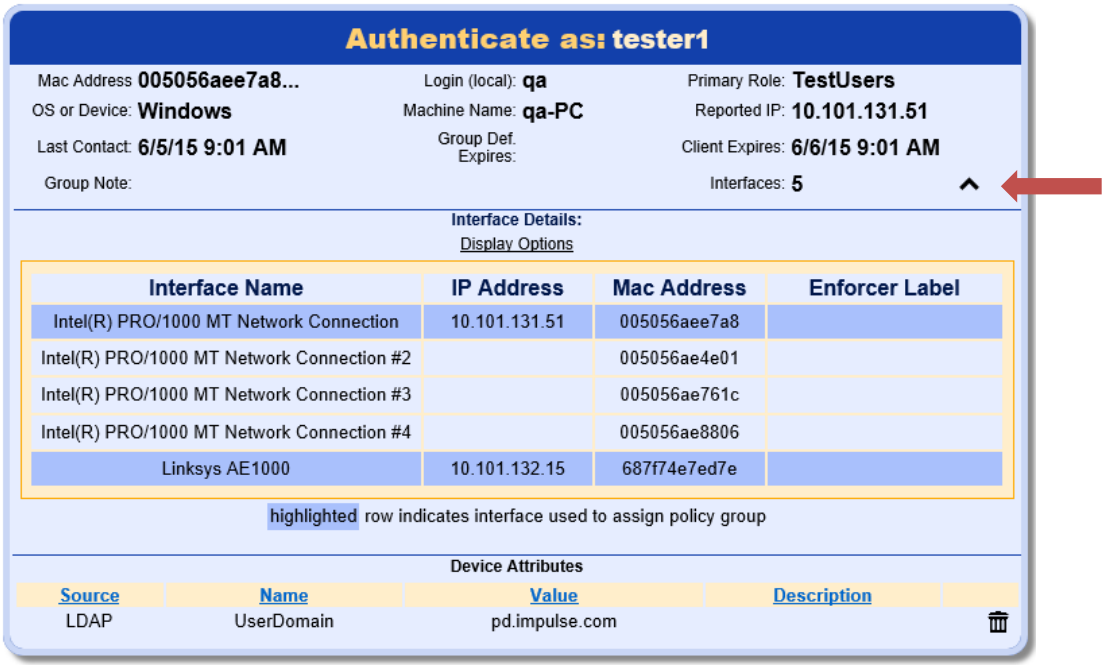
Multi-NIC Awareness for Policy Key Devices

End User Experience

The Policy Key now simultaneously discovers all Network Interfaces (NICs) associated with a device. As a result, SafeConnect consistently views each NIC of a given device as belonging to the same device, enabling SafeConnect to prompt the user to re-authenticate or reinstall the Policy Key only when necessary.

Reporting

The Dashboard Client Details now shows every NIC on an endpoint. Additionally, it highlights the NIC(s) used to assign the Policy Group (see below). In the event that the device could qualify for multiple Policy Groups on different NICs, the group with the highest precedence is applied. To view the list of interfaces, as shown below, click the "^"next to the Interfaces field.

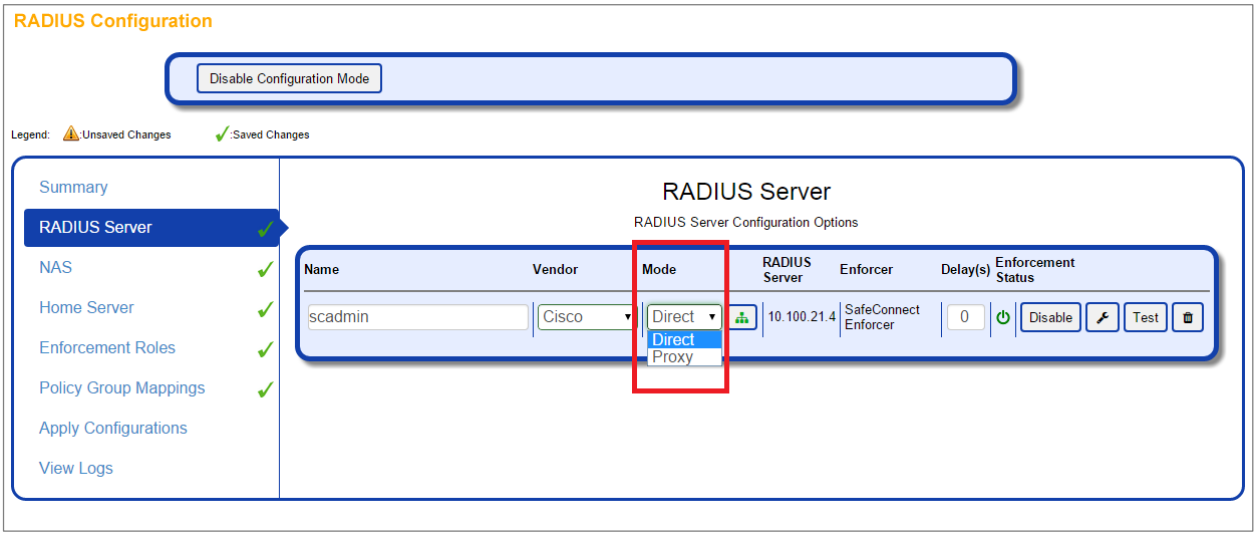


RADIUS Server Enhancements

SafeConnect already leveraged its embedded RADIUS server to handle various aspects of authentication, authorization, and accounting (AAA). Now, in Version 6.2, it supports an additional authentication use case. SafeConnect can now be configured to act as the RADIUS server. This greatly simplifies support for secure wireless where 802.1X and WPA2 Enterprise are being utilized to authenticate against an Active Directory domain. In such a case, there is no need to configure and maintain an external RADIUS server.

As a result, SafeConnect customers migrating their wireless network to use 802.1X and WPA2 Enterprise will not only gain the inherent security benefits but now also benefit from Impulse managing the RADIUS server as part of SafeConnect functionality.

To enable this, the configuration UI has been extended to permit SafeConnect to be configured in "Direct Mode" (see below). In "Direct Mode" SafeConnect acts as the RADIUS server. Note that the user interface (UI) also supports specification of the Active Directory server against which access requests are to be authenticated.



Simplified RADIUS-Based Enforcement (RBE) Network Configuration

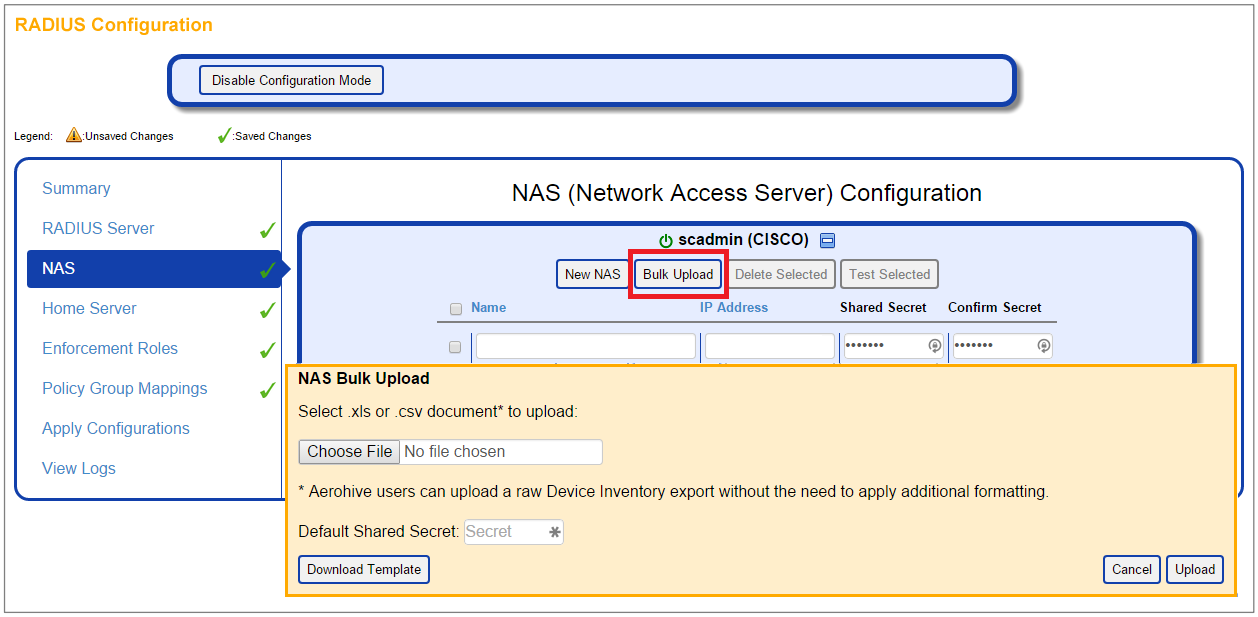
Configuring and maintaining SafeConnect's RADIUSB-ased Enforcement is now much simpler, especially for environments where there are many controllers or access points.
In keeping with industry terminology, SafeConnect's UI generically refers to configured RADIUS clients, such as controllers and access points, as Network Access Servers (NAS).

SafeConnect Version 6.2 greatly simplifies NAS device configuration in the following ways:

1) Subnet Range: SafeConnect NAS configuration now accepts a subnet range in CIDR notation. Previously, the specific address of each NAS was required, but now a range (along with a common shared secret) can be provided; greatly reducing the amount of initial data input and also making it easy to change a common shared secret.

2) Automated Aerohive AP detection: In keeping with Aerohive's Zero-Touch Provisioning approach, as APs are added to the network or happen to acquire a new IP address, SafeConnect will automatically detect this change. To make use of this feature, the AP must be connected within a subnet range utilizing the feature mentioned in #1, above.

3) Bulk Upload: NAS devices and their shared secret can now be imported using the new Bulk Upload feature. The import supports either the Aerohive native export format or, alternatively, using a template format downloadable within SafeConnect (as a CSV or XLS file).



Operating System and Security Updates

As part of Impulse's ongoing commitment to delivering updates of new endpoint operating systems, security software anti-virus applications, and addressing potential security vulnerabilities, the following improvements have been made:

- **Windows 10 Support**

  SafeConnect Version 6.2 has been updated to support the Windows 10 preview release.

  The Policy Key is being updated so that prior versions of SafeConnect will also be compatible with Windows 10. As such, customers on prior versions of SafeConnect will not need to upgrade immediately when Windows 10 is released. One caveat is that Version 6.2 is required to create new custom policies for Windows 10.

  The official Windows 10 release is expected from Microsoft on July 29, 2015. Impulse will re-certify support against the official release build and provide any necessary enhancements within 48 hours of Microsoft's release.

- **Security Updates**

  As part of Impulse's ongoing analysis of security vulnerabilities, this update addresses industry reported vulnerabilities with infrastructure libraries like gLibc, JDK, and MySQL by automatically updating to use the most recent versions.

- **Anti-Virus Updates**

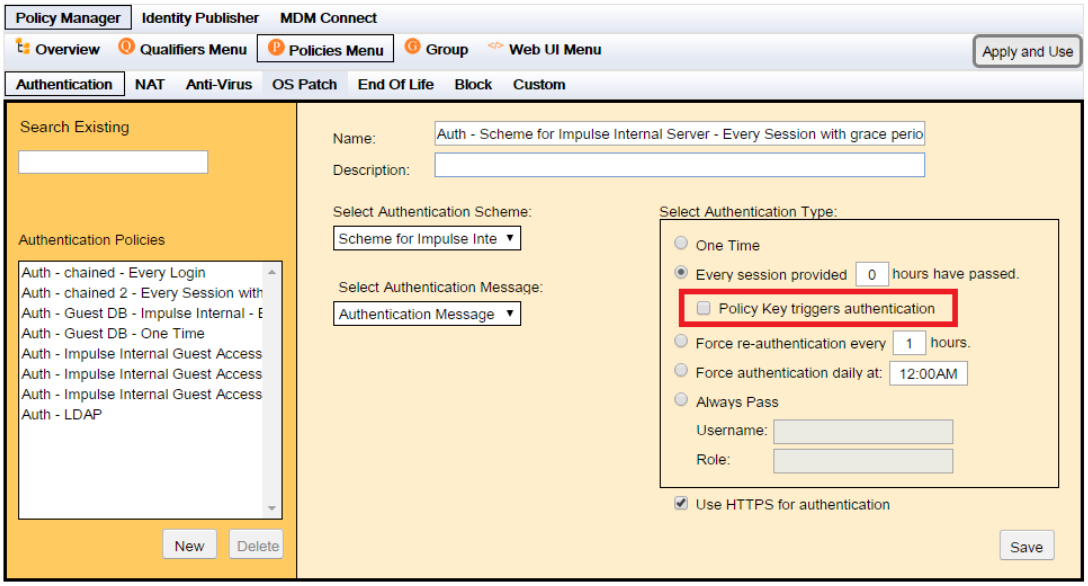
  - Signatures detection updated for Version 15.0.2.361 of Kaspersky Anti-Virus
  - Signature detection updated for ESET Trial for Mac OS X
  - Installation and signature detection updated for 2015 AVGuard/Avira for Microsoft Windows

Other SafeConnect Enhancements

Policy Key Optionally Triggers Re-Authentication

In Version 5 and earlier, SafeConnect could be configured so that users would be prompted to re-authenticate whenever logging-in to a Policy Key endpoint. This allowed for easy validation of each user in a lab environment, for example.

This ability was not part of the initial Version 6.0 release, but has been re-added in response to customer feedback. The screenshot below shows how to configure it in the Management Console.



Improved Xbox One Detection

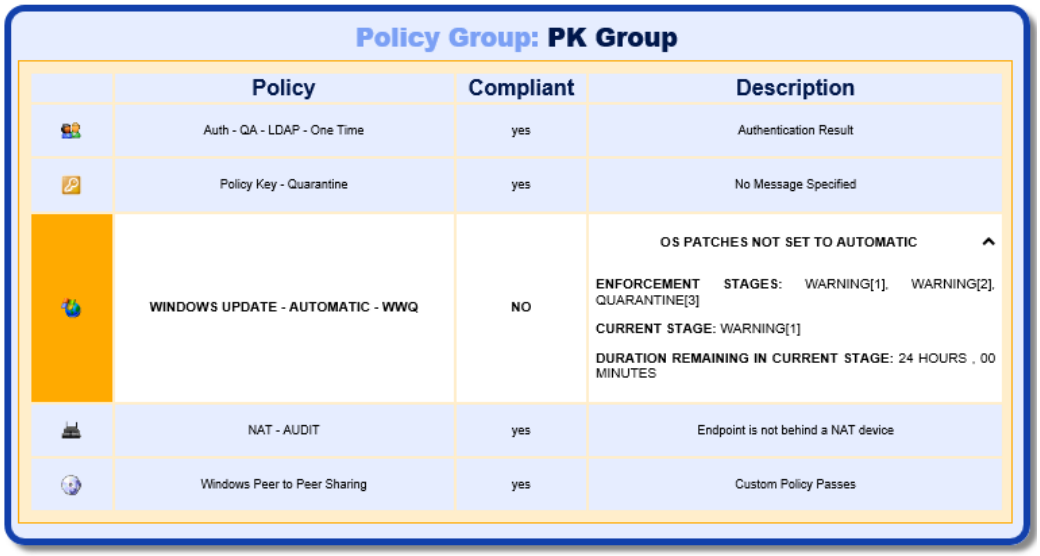
There were some known issues with identifying the Xbox One gaming system in previous versions leading to an inconsistent end user experience and potential confusion in the reporting. SafeConnect Version 6.2 introduces a new method of device identification that provides a much more streamlined and convenient end user experience and more consistent reporting.

Note: this currently only applies to environments utilizing Policy Based Routing (PBR) and Aruba Wireless (RBE).

Enhanced Visibility In to Enforcement Stages

As depicted below, when a device fails a policy, the Dashboard details shows the stages the device will go through for enforcement, the current stage, and the length of time before it moves to the next stage.

This same information is now included in the exported Client History data. This feature was developed in cooperation with customers to automate a proactive response to policy failures. For example, a 3rd party application can now use this exported data to drive Help Desk tickets, so that staffers can assist managed users in remediating outstanding issues before a quarantine enforcement occurs.



Policy Group: PK Group

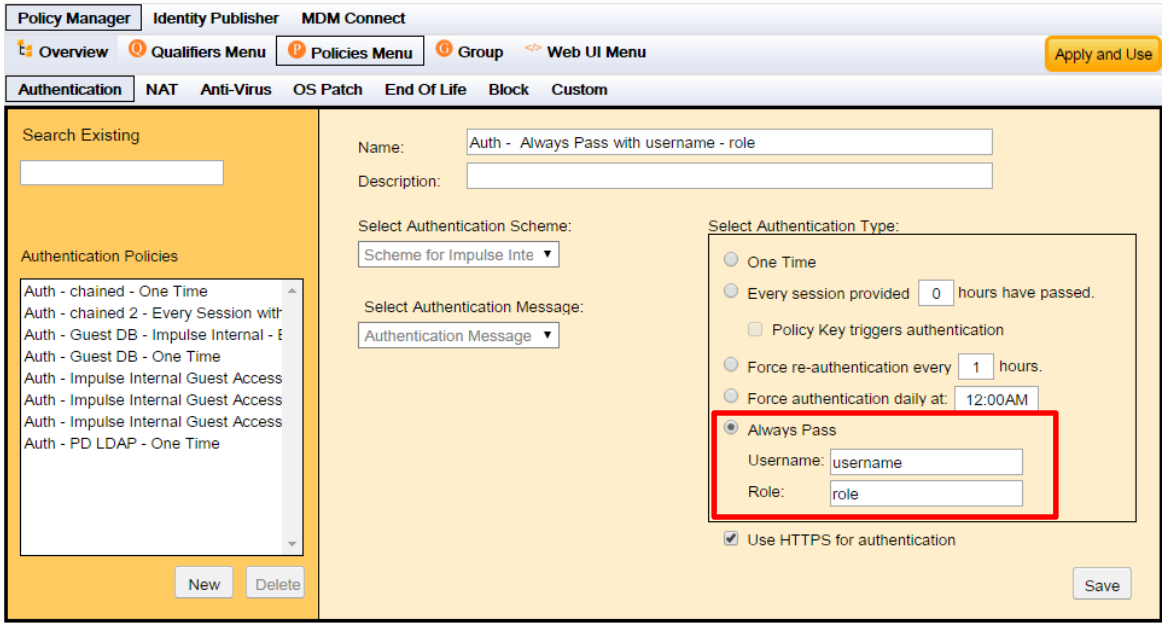
	Policy	Compliant	Description
	Auth - QA - LDAP - One Time	yes	Authentication Result
	Policy Key - Quarantine	yes	No Message Specified
	WINDOWS UPDATE - AUTOMATIC - WWQ	NO	OS PATCHES NOT SET TO AUTOMATIC ENFORCEMENT STAGES: WARNING[1], WARNING[2], QUARANTINE[3] CURRENT STAGE: WARNING[1] DURATION REMAINING IN CURRENT STAGE: 24 HOURS , 00 MINUTES
	NAT - AUDIT	yes	Endpoint is not behind a NAT device
	Windows Peer to Peer Sharing	yes	Custom Policy Passes

“Always Pass” Authentication Policy

SafeConnect Version 6.2 includes a new option for authentication to allow devices in a specific policy group to automatically pass authentication with a predefined Username and Role. When this policy is in place, no authentication schemes are used and the Username and Role specified in the UI (see below) will be automatically associated with all devices in the Policy Group.

While there are likely a number of potential applications, this feature is primarily helpful for environments leveraging SafeConnect’s Contextual Intelligence Publisher (CIP) that require browser-less devices to be intelligently managed. Browser-less devices often do not require authentication, as a result, without this feature, there would be no Username or Role for SafeConnect to publish.

As an example, consider a firewall consuming the intelligence collected and published by SafeConnect. When a browser-less media device connects to the network and SafeConnect notifies the firewall, the firewall will require a Username or Role to determine which firewall policy to apply. Without this feature there would be no Username or Role to publish to the firewall because the user is not prompted to enter the information. With this feature, the Username and Role are taken from the Always Pass Authentication Type settings (see below).



User Count by Group Includes "Not Under Policy" View

This new view can be used to ensure all devices and networks are being correctly subjected to enforcement. If you see devices in this view that are expected to be under enforcement, it suggests configuration issues, such as a network being included in a policy group for Windows/OSX devices but not being included in a mobile device policy group. If you find devices in this view that you expect to be under enforcement and cannot understand why they are in this view, please contact Impulse Support.

More technically, the "Not Under Policy" view identifies devices that have an IP address that SafeConnect is configured to manage but the host type of the device is not defined in a Policy Group.

Simplified Navigation to Guest and Device Enrollment

Previously, the URLs used for registering as a guest or for enrolling a device required a port number to be specified, this is no longer the case. Requiring the port made it difficult to navigate back to the respective page when entering the URL from memory.

Now http://my.domain.edu/enroll can be used in place of https://my.domain.edu:9443/enroll . And http://my.domain.edu/guest can be used in place of https://my.domain.edu:9443/guest.