



Technology Solution Guide

Deploying Impulse Point's SafeConnect Network Access Control (NAC) with Aruba Networks' Secure Mobility Solution

S/W Version : SafeConnect V5.2 - 2011

This document describes the best practices for configuring the Impulse Point Safe Connect network access control with Aruba's secure mobility infrastructure.

WARRANTY DISCLAIMER

THE FOLLOWING DOCUMENT, AND THE INFORMATION CONTAINED HEREIN IS PROVIDED ON AN "AS IS" BASIS. ARUBA MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR GUARANTEES AS TO THE USEFULNESS, QUALITY, SUITABILITY, TRUTH, ACCURACY OR COMPLETENESS OF THIS DOCUMENT AND THE INFORMATION CONTAINED IN THIS DOCUMENT.

DISCLAIMER OF LIABILITY

Aruba Networks, Inc. disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the certification program or the acts or omissions of any company or technology that has been certified by Aruba Networks.

Certification does not mean that the company is a subcontractor or under the technical control or direction of Aruba Networks. In conducting the certification program Aruba Networks is not undertaking to render professional or other services for or on behalf of any person or entity.

Table of Contents

Table of Contents	2
Introduction	3
Solution Components	3
Aruba Campus WLAN Solution	3
Impulse Point and Aruba Solution	4
ArubaEdge Solution Qualification	5
Qualification Objective	5
Network Topology	5
SafeConnect and Aruba Controller Integration Overview	5
Aruba Networks Controller Configuration Guide	6
SafeConnect Configuration Guide	10
Summary of Test Results	11
Product Support Information.....	11
Conclusion.....	12
Appendix 1	13
Sample Deployment Overview	13
Dynamic Role Assignment on a Single Open SSID	13
Dynamic Role Assignment and On-Ramping with an Open and Secure SSID	15

Introduction

This document describes the steps and guidelines necessary to configure Aruba's wireless LAN infrastructure to work interoperably with Impulse Point's SafeConnect's Network Access Control (NAC) Solution. The guide is intended to be used in conjunction with Aruba and Impulse Point configuration guides. Please contact the respective company's sales engineering or support groups should additional information be required.

Solution Verified:	Impulse Point
Aruba Product:	Aruba Campus WLAN Solution OS version 6.0.1.x and 6.1.2.2
Partner Solution Tested:	SafeConnect v5.2

Solution Components

Aruba Campus WLAN Solution

Secure and reliable mobility is the responsibility of the enterprise network, which must support a wide range of converged clients over wireless, wired, and remote access networks. Laptops and smartphones are capable of simultaneously running voice, data, and now video applications, an operating model that breaks traditional dedicated VLAN and SSID architectures. Delivering the quality of service (QoS), bandwidth, and management tools necessary to accommodate these devices on a grand scale – within a campus environment, to users on the road, and in branch offices – requires a specially tailored system design.

Aruba's unique application and device fingerprinting enable the system to detect the types of traffic flows, and the devices from which they originate. The network can then be dynamically conditioned to deliver QoS - on an application-by-application, device-by-device basis - as needed to ensure highly reliable application delivery. Aruba's integrated policy enforcement firewall isolates applications from one another to essentially create multiple dedicated virtual networks, and then allocates the necessary bandwidth for each user and application.

To ensure reliable application delivery in changing RF environments, Aruba's Adaptive Radio Management (ARM) technology forces client devices to shift away from the noisy 2.4GHz band to the quieter 5GHz band, adjusts radio power levels to blanket coverage areas, load balance by shifting clients between access points, and even allocates airtime based on the capabilities of each client device. The result is a superb user experience without any user involvement.

These services are complemented by security systems that ensure the integrity of the network. Rogue detection, wireless intrusion and prevention, access control, remote site VPN, content security scanning, end-to-end data encryption, and other services protect the network and users at all times.

Aruba's extensive portfolio of campus, branch/teleworker, and mobile solutions simplify operations and secure access to unified communications applications and services - regardless of the user's device, location, or network. This dramatically improves productivity, lowering capital and operational costs while providing a superior uninterrupted user experience.

SafeConnect NAC Solution

Impulse Point was originally founded to address the unique endpoint policy management requirements of higher education and the need to provide a flexible policy management framework to support personally-owned computing devices within highly mobile, transient, and diverse network environments. SafeConnect is an enterprise-wide NAC solution that operates across wired, wireless, and VPN in a consistent fashion.

Impulse Point and Aruba Solution

The SafeConnect Policy Enforcer Appliance is installed out-of-line on the organization's premises and is connected to an aggregation point. NAC posture policies and enforcement rules are configured using the SafeConnect Policy Management Console by network segment or directory services group.

Policy enforcement firewall (PEF) policies on the Aruba controller are then configured to manage the client's network access based on its NAC posture. When the client connects to the network, its NAC posture is reported back to the SafeConnect policy enforcer, which returns the NAC posture / role information to the Aruba controller to grant network access to the client based on the posture assessment. The Aruba session aware firewall then enforces the network access.

Endpoint devices connecting to the network will be intercepted, authenticated, presented with the organization's acceptable use policies, and issued a SafeConnect Policy Key. The key certifies that the endpoint device adheres to endpoint security policies on a continuous/real-time basis, and reports non-compliance to the SafeConnect Policy Enforcer for individualized remediation guidance. The endpoint device remains completely isolated using I-LAN quarantine technology until the policy breach is resolved.

Aruba Networks Wireless Integration

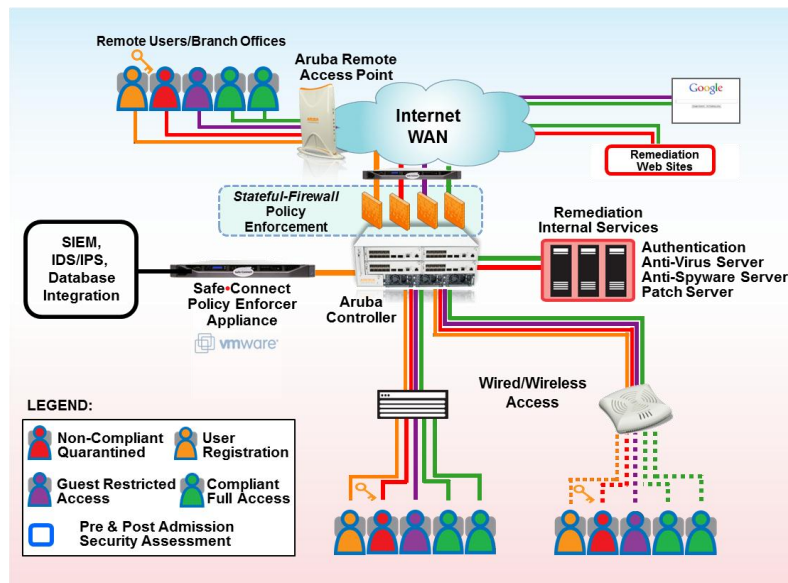


Figure 1. Aruba Impulse Pint Integration Topology

ArubaEdge Solution Qualification

Qualification Objective

Validate the interoperability of Impulse Point's SafeConnect with the Aruba's wireless LAN infrastructure

Network Topology

SafeConnect leverages Aruba's PEF technology to assign per-user restricted-access quarantine roles in real-time, pre- and post-network admission, for devices that are not compliant with security requirements. SafeConnect also participates in Single Sign-On (SSO) using Aruba's Native Portal or 802.1x-WPA2 Enterprise authentication as a standard option.

SafeConnect and Aruba Controller Integration Overview

SafeConnect's continuous posture assessment capability leverages Aruba's PEF technology to assign per-user quarantine roles for clients in real time who are not compliant with security requirements. Within the Aruba network, each user is assigned a role on the network. These roles are groupings of Access Control Lists (ACLs) that are used to grant or revoke network privileges.

The integration process involves defining the required roles and the corresponding ACLs on the Aruba controller, identifying SafeConnect as an XML API server, establishing a GRE tunnel between the controller and the SafeConnect enforcer, and configuring the Aruba PEF to properly mirror traffic. Additionally, for end-to-end policy enforcement, the initial role for an SSID under policy should be

configured as SC_Detection. This document outlines the necessary configuration. For the purpose of this document four roles were created on the Aruba controller: SC_Compliant, SC_Quarantine, SC_Guest, and SC_Detection (default role).

Aruba Networks Controller Configuration Guide

Impulse Point provides a complete script for use with the Aruba controller(s) and this document is intended for explanatory and not configuration purposes. Step 1 describes the information needed by Impulse Point to generate the configuration script.

Step 1. Pre-setup information gathering

The following information is required to set-up the Aruba WLAN and SafeConnect Enforcer.

The IP of the SafeConnect Enforcer:	_____
The IP of the Aruba Controller:	_____
The IP of the Aruba Controller side of the Tunnel:	_____
The IP of the Tunnel Source:	(the IP of the Aruba controller)
The IP of the Tunnel Destination:	(IP of the SafeConnect Enforcer)
The SSIDs to apply policy to:	_____
The XML API Key:	_____
The SNMP Community String:	_____

Note: When the deployment has multiple Aruba WLAN controllers, the SafeConnect Enforcer entry needs to be made for every controller. The following values will be used for illustrative purposes only:

The IP of the SafeConnect Enforcer	10.100.5.43
The IP of the Aruba Controller	172.16.193.195
The IP of the Aruba Controller side of the Tunnel	192.168.10.202 255.255.255.0
The IP of the Tunnel Source	172.16.193.195
The IP of the Tunnel Destination	10.100.5.43
SSIDs to which policies are applied	Customer_Open and Customer_Secure
XML API Key	supersecret
SNMP Community String	impulse

Step 2. Setup GRE Tunnel

A GRE Tunnel must be established between each Aruba controller and the SafeConnect Enforcer. The Tunnel ID should be the same across the controllers, and the “tunnel source” should be the primary IP Address of the Aruba controller. The “tunnel destination” should be the IP address of the SafeConnect Enforcer.

```

conf t
  interface tunnel 58008
    description "SafeConnect Interface"
    ip address 192.168.10.202 255.255.255.0
    tunnel source 172.16.193.195
    tunnel destination 10.100.5.43
    trusted
  !
end

```

Step 3. Create XML API Server Object

An XML API server object must be created and attached to each of the Aruba SSIDs for which SafeConnect is providing Dynamic Role Assignment. The key (password) must be shared with Impulse Point at the point of configuration. The example below creates an XML-API pointing to the SafeConnect Enforcer at 10.100.5.43 with a key of “supersecret”.

```

conf t
  aaa xml-api server "10.100.5.43"
    key supersecret
  !
end

```

Step 4. Define and Create ACLs

The following ACLs will be created on the Aruba controllers.

- **sc_compliant** - contains any restrictions required for compliant users. Normally there are no restrictions in this group and all traffic flows freely.
- **sc_guest** - contains any restrictions for guest users. Normally, guest users are restricted to internet access only and restrictions are added that deny all traffic routing internally. The “any network 10.100.0.0 255.255.0.0 any deny” entry is a placeholder and should be modified to meet specific guest restriction needs.
- **sc_quarantine** - contains the restrictions for non-compliant users. Web traffic is forwarded to the SafeConnect appliance to properly display remediation warnings, and all other traffic is typically dropped. Any exceptions to this are handled in the intranet ACL.
- **sc_intranet** - contains any exemptions for non-compliant users. Typical exemptions may include helpdesk Web sites, student portals and ERP Software. The “any host 10.0.0.100 any permit” entry is a placeholder and should be modified to meet specific restriction needs.
- **sc_redirect** - provides SafeConnect functionality and ensures Policy Key communication and proper client detection.

Step 5. Create and Define Roles

The following default roles and their respective ACLs will be created on the Aruba controller. These are the *minimum* roles required for SafeConnect to function. Additional roles may be created if required. (i.e., Faculty/Staff/Student roles)

- **SC_Compliant** – this role is used for normal operations, and is where users who are compliant with all policies are placed. This role contains the following ACLs:
 - **sc_redirect**
 - **sc_compliant**
- **SC_Guest** – this role is used for guest accounts. This role contains the following ACLs:
 - **sc_redirect**
 - **sc_guest**
- **SC_Quarantine** – this role is where non-compliant endpoints are placed for redirection to the appliance. This role contains the following ACLs:
 - **sc_redirect**
 - **sc_intranet**
 - **sc_quarantine**
- **SC_Detection** - this role is the default role for the SSIDs whose endpoints are under policy management, and enables the SafeConnect appliance to detect new endpoints. This role contains the following ACLs:
 - **sc_redirect**
 - **sc_compliant**

```
conf t
user-role SC_Compliant_Role
  session-acl sc_redirect
  session-acl sc_compliant
!
user-role SC_Guest_Role
  session-acl sc_redirect
  session-acl sc_guest
!
user-role SC_Quarantine_Role
  session-acl sc_redirect
  session-acl sc_intranet
  session-acl sc_quarantine
!
user-role SC_Detection_Role
  session-acl sc_redirect
  session-acl sc_compliant
!
end
```

Step 6. Set Up Session Mirror Destination

The SafeConnect appliance must be configured as a “Session Mirror Destination” for the Aruba PEF.

```
conf t
  firewall session-mirror-destination ip-address 10.100.5.43
  !
end
```

Step 7. Set Up SNMP

SNMP information must be configured to send trap information from the Aruba controller to the SafeConnect Enforcer. The IP used here is the IP of the SafeConnect Enforcer. The community string can be any secure passphrase, though Impulse Point recommends against using the same password for the XML API server. The community string (password) must be shared with Impulse Point at the time of configuration.

```
conf t
  snmp-server host 10.100.5.43 version 1 impulse udp-port 162
  !
end
```

Step 8. Apply Roles and XML API Server to SSID

The default role for the aaa-profile should be changed to the SC_Detection_Role, and the XML API server should be associated with the appropriate SSIDs.

```
conf t
aaa profile "Customer_Open-aaa_prof"
  initial-role "SC_Detection_Role"
  dot1x-default-role "SC_Detection_Role"
  xml-api-server "10.100.5.43"
  !
end

conf t
aaa profile "Customer_Secure-aaa_prof"
  initial-role "SC_Detection_Role"
  dot1x-default-role "SC_Detection_Role"
  xml-api-server "10.100.5.43"
  !
end
```

Step 9. Save your changes

```
conf t
 write memory
 !
end
```

SafeConnect Configuration Guide

The following configuration was tested in Aruba's solutions lab. Two SafeConnect Policy Groups consisting of (1) Guests and (2) Faculty, Staff, and Students. Each of these groups was assigned a compliant and a non-compliant role, meaning that users in a particular group who are compliant with policy were given a one role, and users who were non-compliant with policy were given different a role.

The Guests Policy Group contained the following devices and criteria:

- Devices
 - All devices
- Qualifiers
 - All Authentication roles used within the Guest Database
- Policies
 - Any desired policies
- Role Assignment
 - Compliant
 - SC_Guest
 - Non-Compliant
 - SC_Quarantine

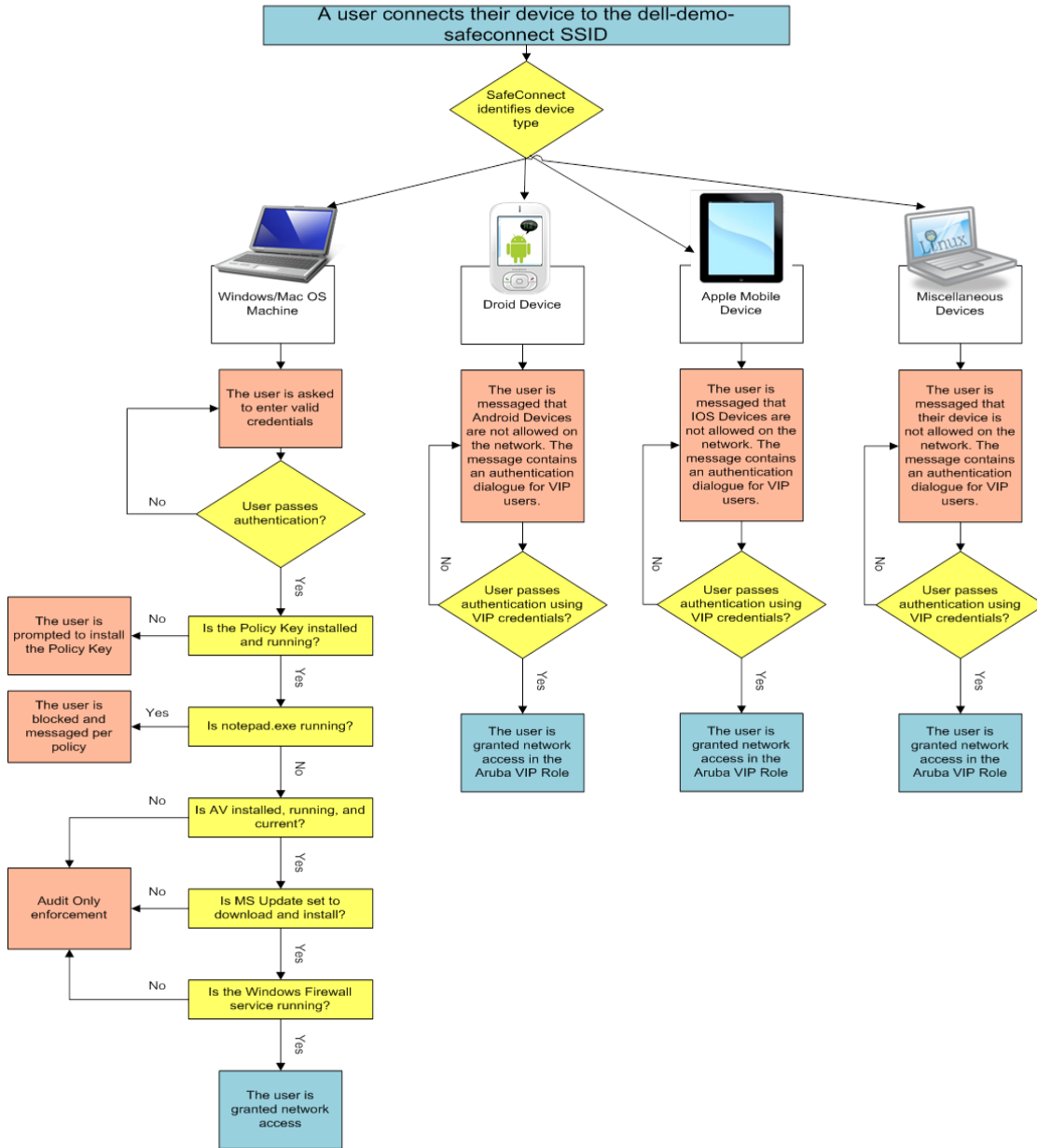
The Faculty, Staff and Students Policy Group had the following criteria:

- Devices
 - All devices*
- Qualifiers
 - All IP addresses associated with the Customer_Open SSID
- Policies
 - Authentication
 - Any desired policies
- Role Assignment
 - Compliant
 - SC_Compliant
 - Non-Compliant
 - SC_Quarantine

*Depending on the desired Endpoint Policy assessment, additional groups may be needed for Non-Policy Key devices, and Policy Key enabled Devices.

Summary of Test Results

The following set of mobile device policies were successfully demonstrated using an Aruba controller platform and access points:



Product Support Information

Aruba Support: www.arubanetworks.com/support.php

Impulse Point Support: Support@Impulse.com

Conclusion

The interoperability tests were successfully concluded, validating the interoperability of SafeConnect with Aruba's controller.

© 2011 Aruba Networks, Inc. Aruba Networks' trademarks include ®, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, and Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

Specifications are subject to change without notice.

Appendix 1

Sample Deployment Overview

The following conditions must be in force for the sample deployment:

- A GRE Tunnel must be established between each Aruba controller and the SafeConnect Enforcer.
- An XML API server must be created and attached to each of the Aruba SSIDs to which SafeConnect is providing Dynamic Role Assignment.
- The Key (password) must be shared with Impulse Point at the point of configuration.
- The SafeConnect appliance must be configured as a “Session Mirror Destination” for the Aruba PEF.
- SNMP information must be sent from the Aruba controller to the SafeConnect Enforcer.
- The initial role of the SSIDs under policy must be changed to SC_Detection.

SafeConnect Configuration Overview

SafeConnect Enforcers integrate with Aruba controller(s) as follows:

- The combination of mirrored traffic in the ACLs and SNMP information is used by the SafeConnect Appliance to detect active clients on the network and to direct XML API commands to the appropriate Aruba controller in clustered environments.
- The XML API is used by the SafeConnect Appliance to move users between the different roles mentioned in this configuration document.
- The GRE tunnel is configured in such a way that the SafeConnect Appliance will respond to all HTTP and HTTPS requests made by end users. This facilitates SafeConnect's system for authenticating, messaging and remediation of policy issues.

Dynamic Role Assignment on a Single Open SSID

Customer_Open is an open network serving as the primary wireless network. SafeConnect leverages the Aruba PEF to provide access control over users connecting to the Customer_Open SSID. To facilitate integration, several roles are created within the Aruba controllers, and based on a user's status on the network, roles are assigned dynamically. The following are example roles and their potential uses for users associated to the Customer_Open SSID:

- **SC_Quarantine**
 - A Faculty, Staff or Student device that is non-compliant with a (non-warning) configured SafeConnect Policy will be quarantined and given appropriate remediation instructions.
- **SC_Guest**
 - Guests with limited bandwidth and port access.
- **SC_Compliant**
 - A Faculty, Staff or Student device that is fully compliant with all configured SafeConnect policies will be granted unrestricted network access.

Required Aruba Configuration

In addition to the general configuration provided for at the beginning of this document, this deployment scenario requires that the default role be changed and the XML API server be associated with the Customer_Open SSID.

```
conf t
aaa profile "Customer_Open-aaa_prof"
    initial-role "SC_Detection_Role"
    xml-api-server "10.100.5.43"
!
end
```

Required SafeConnect Configuration

Two SafeConnectPolicy Groups will need to be created to support this scenario:

- Guests
- Faculty, Staff, and Students

Each group will be assigned a Compliant and a Non-Compliant role, meaning that users who are in a particular group and are compliant with policy will be given a particular role, and users who are non-compliant with policy can be given different roles. The default roles are used, however, custom roles can be used wherever desired.

The Guests Policy Group should contain the following devices and criteria:

- Devices
 - All devices
- Qualifiers
 - All Authentication roles used within the Guest Database
- Policies
 - Any desired policies
- Role Assignment
 - Compliant
 - SC_Guest
 - Non-Compliant
 - SC_Quarantine

The Faculty, Staff and Students Policy Group should have the following criteria:

- Devices
 - All devices*
- Qualifiers
 - All IP addresses associated with the Customer_Open SSID
- Policies
 - Authentication

-
- Any desired policies
 - Role Assignment
 - Compliant
 - SC_Compliant
 - Non-Compliant
 - SC_Quarantine

*Depending on the desired Endpoint Policy assessment, additional groups may be needed for Non-Policy Key devices, and Policy Key enabled Devices.

Dynamic Role Assignment and On-Ramping with an Open and Secure SSID

The goal of this deployment is to provide a multi-purpose open network as well as a secure network. This provides an easy to use method for on-ramping end users onto a secure wireless network, without the difficulty of configuring supplicants. SafeConnect will control two wireless networks, Customer_Open and Customer_Secure. Customer_Open is an open network serving as the on ramping SSID as well as the Guest Access SSID. Customer_Secure is a WPA2 Enterprise encrypted SSID, serving as the production SSID for Faculty, Staff and Students.

The Customer_Open SSID will be used for both Guest Access and to provide Faculty, Staff and Students an easy way to access the XpressConnect utility for the purposes of on ramping to the Customer_Secure SSID. When a machine connects to the Customer_Open Wireless and attempts to open a web page, SafeConnect will present them a Web page with two options:

- **Option 1:** (WPA2 Enterprise Enablement) Users will be greeted with the XpressConnect utility and follow the appropriate instructions to migrate to the Customer_Secure secure SSID.
- **Option 2:** (Guest Authentication System) Users who cannot connect to the secure network (due to device limitations) or who do not have appropriate credentials can log in as guests provided they have credentials in the SafeConnect guest authentication database.

SafeConnect leverages the Aruba PEF to provide Access Controls to users connecting to the networks. To facilitate the integration, several roles are created within the Aruba controllers, and based on a user's status on the network, roles are dynamically assigned. To improve the end user experience while on-ramping, SafeConnect will be configured to provide redirection and delivery of the XpressConnect utility. The following are example roles and their uses for users associated to the Customer_Open SSID:

- **SC_Quarantine**
 - Faculty, Staff or Students who have not completed the XpressConnect on-ramping process.
- **SC_Guest**
 - Guests with limited bandwidth and port access.
- **SC_Compliant**
 - Guests, Faculty, Staff or Students devices which cannot join secure SSID (for any reason) but that need unrestricted wireless network access.

The Customer_Secure SSID will be protected via WPA2 Enterprise encryption (configured separately within the Aruba infrastructure). SafeConnect will be configured to process single sign-on requests from the WPA2 enterprise handshakes that occur between the client's supplicant and the Aruba controllers. Users will not be prompted for authentication via a captive portal. The following are example roles and their uses for users associated to the Customer_Secure SSID:

- **SC_Compliant**
 - A Faculty, Staff or Student that is fully compliant with all configured SafeConnect policies will be granted unrestricted network access.
- **SC_Quarantine**
 - A Faculty, Staff or Student that is non-compliant with a (non-warning) configured SafeConnect Policy will be quarantined and given appropriate remediation instructions.

Required Aruba Configuration

To provide for this deployment scenario, the default roles will need to be changed, the XML API server will need to be added to the Customer_Open and Customer_Secure SSIDs.

```
conf t
aaa profile "Customer_Open-aaa_prof"
    initial-role "SC_Detection_Role"
    xml-api-server "10.100.5.43"
!
end

conf t
aaa profile "Customer_Secure-aaa_prof"
    initial-role "SC_Detection_Role"
    dot1x-default-role "SC_Detection_Role"
    xml-api-server "10.100.5.43"
!
end
```

Required SafeConnect Configuration

Four SafeConnect Policy Groups will need to be created to support this scenario:

- XpressConnect On-Ramping
- Guests
- Non-WPA2 Devices
- Faculty, Staff, and Students

Each of these groups will be assigned a compliant and a non-compliant role, meaning that users who are in a particular group, and are compliant with policy will be given a particular role. Users who are non-compliant with policy can be given a different role. The default roles are used, however, custom roles can be used wherever desired.

The XpressConnect On-Ramping Policy Group should contain the following devices and criteria:

-
- Devices
 - All devices
 - Qualifiers
 - All IP addresses associated with the Customer_Open SSID
 - Policies
 - An Authentication Policy that allows Guest Users to authenticate via the SafeConnect internal guest database. The Web message associated with this authentication policy should have a link to the XpressConnect utility (either hosted on the SafeConnect appliance or externally).
 - Role Assignment
 - Compliant
 - SC_Quarantine
 - Non-Compliant
 - SC_Quarantine

The Guests Policy Group should contain the following devices and criteria:

- Devices
 - All devices
- Qualifiers
 - All Authentication roles used within the guest database
- Policies
 - Any desired policies
- Role Assignment
 - Compliant
 - SC_Guest
 - Non-Compliant
 - SC_Quarantine

The Non-WPA2 Devices Policy Group should contain the following devices and criteria:

- Devices
 - All Non-WPA2 devices (Media/Gaming Consoles)
- Qualifiers
 - All IP addresses associated with the Customer_Open SSID
- Policies
 - Any desired policies
- Role Assignment
 - Compliant
 - SC_Compliant
 - Non-Compliant
 - SC_Quarantine

Lastly, the Faculty, Staff and Students Policy Group should have the following criteria:

- Devices
 - All devices*
- Qualifiers
 - All IP addresses associated with the Customer_Secure SSID
- Policies
 - Authentication

-
- For Single Sign On to function properly, the same authentication servers used by WPA2 Enterprise must be configured and used within SafeConnect
 - Any desired policies
 - Role Assignment
 - Compliant
 - SC_Compliant
 - Non-Compliant
 - SC_Quarantine

**Depending on the desired endpoint policy assessment, additional groups may be needed for non-policy key devices, and policy key-enabled devices.*

About Aruba

Aruba is a global leader in distributed enterprise networks. Its award-winning portfolio of campus, branch/teleworker, and mobile solutions simplify operations and secure access to all corporate applications and services – regardless of the user’s device, location, or network. This dramatically improves productivity and lowers capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook.

About Impulse Point

Impulse Point offers Network Access Control (NAC) solutions including the SafeConnect managed service. To learn more, visit Impulse Point at www.impulse.com.

© 2011 Aruba Networks, Inc. Aruba Networks’ trademarks include ®, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, and Green Island®. All rights reserved. All other trademarks are the property of their respective owners. Specifications are subject to change without notice.

