Aruba Networks
Mobility Controllers and Access Points

RSA SecurID Ready Implementation Guide

Last Modified: December 10, 2014

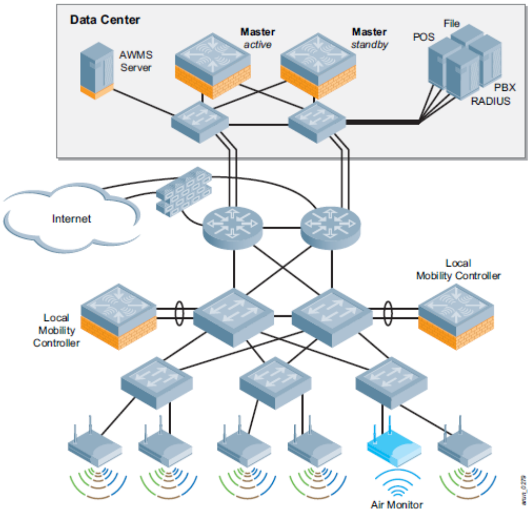
Partner Information

Product Information	
Partner Name	Aruba Networks, Inc.
Web Site	www.arubanetworks.com
Product Name	Mobility Controllers and Access Points
Version & Platform	ArubaOS 6.4.2.1
Product Description	Aruba Mobility Controllers create a single, unified network that manages wired and wireless access across indoor, outdoor and remote locations. Aware of all network devices, users, applications and locations, Mobility Controllers also maintain configurations and automate software updates for other Aruba Mobility Controllers, Mobility Access Switches and access points (APs). Running the ArubaOS operating system, Mobility Controllers support integrated capabilities, including the stateful Policy Enforcement Firewall™ (PEF™), RFProtect™ spectrum analyzer and wireless intrusion protection, the Virtual Intranet Access™ (VIA™) agent for secure remote connectivity, advanced cryptography, and Adaptive Radio Management™ (ARM™) to optimize Wi-Fi client behavior.

Solution Summary

The Aruba Mobility controller takes the guesswork out of provisioning a wireless infrastructure, allowing an administrator to painlessly provision and configure all of the Aruba wireless access points on their network. The Mobility Controller also provides comprehensive logging and monitoring of the wireless network and provides many other useful services. When integrated with RSA SecurID over the RADIUS protocol, administrators can add two-factor authentication to their wireless networks by configuring Authentication Manager as the AAA server for wired and wireless 802.1x authentication. When configured this way, users accessing the network with a compatible network supplicant must provide their SecurID PIN and tokencode to successfully join the network.

RSA Authentication Manager supported features	
Mobility Controllers and Access Points 6.4.2.1	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	No
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
RSA SecurID Authentication via IPv6	No
On-Demand Authentication via Native SecurID UDP Protocol	No
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	No
RSA Authentication Manager Replica Support	No
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No



Agent Host Configuration

Aruba Mobility Controllers will be communicating with RSA Authentication Manager via RADIUS. A RADIUS client that corresponds to the agent host record must be created in the RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

Note: The RADIUS client's hostname must resolve to the IP address specified.

Please refer to the appropriate RSA documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Aruba Mobility Controller with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Aruba Mobility Controller components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

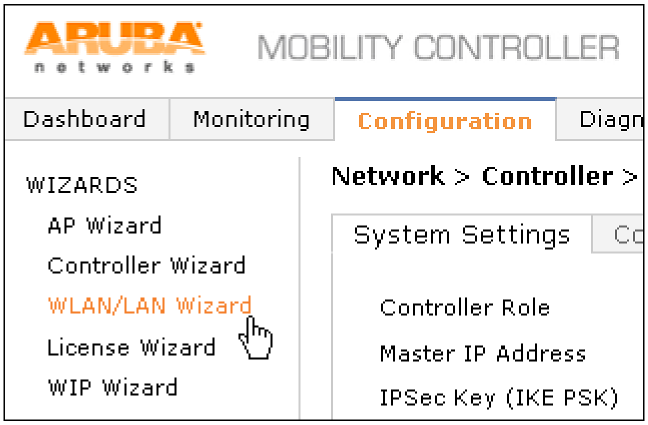
Configuring the Aruba Mobility Controller

Once you have completed the initial setup of the Mobility controller and connected the controller and access points to your network, you must configure a Wireless LAN (WLAN) that takes advantage of RSA SecurID to provide two-factor authentication.

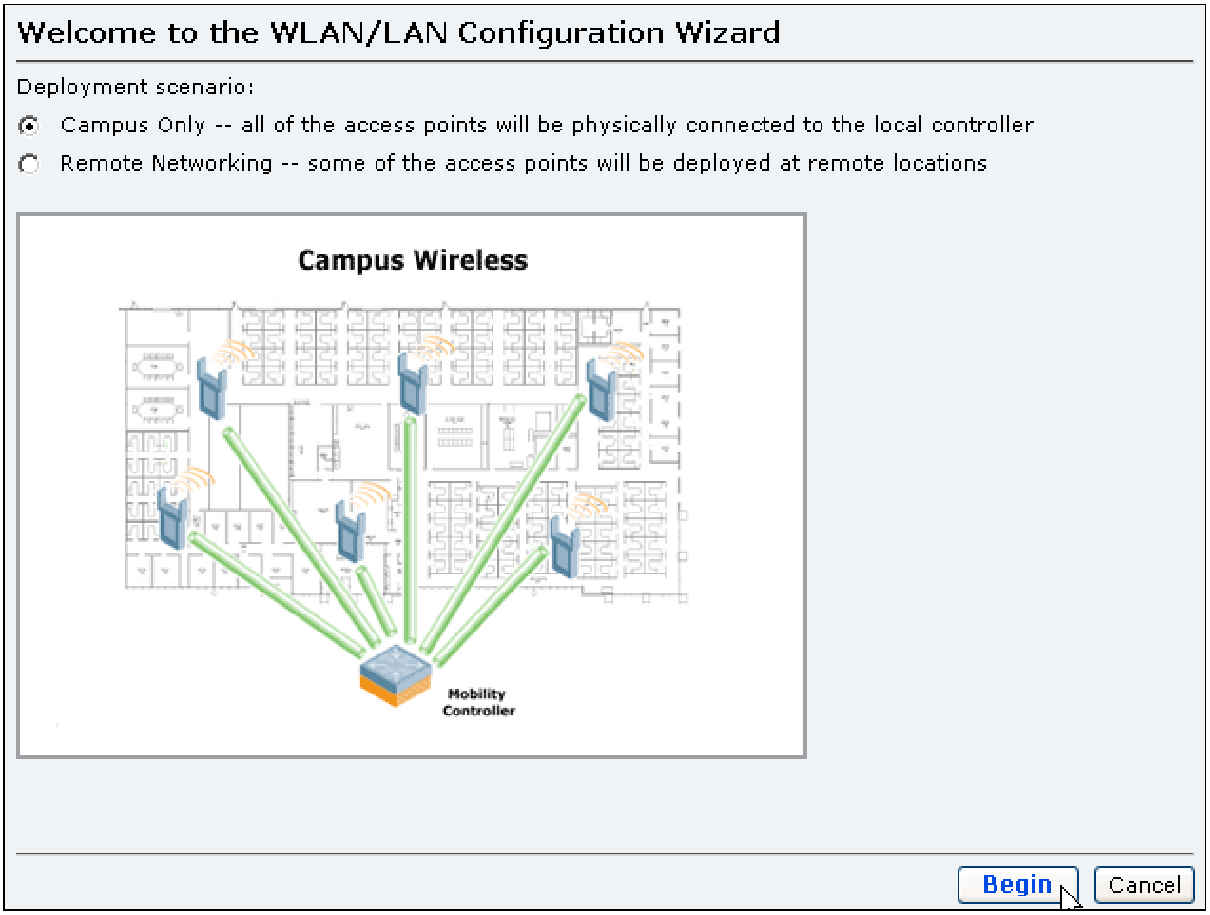
Note: This guide assumes you have correctly configured your Mobility controller and your access points are able to communicate with the controller and receive configuration data from it. Please ensure this is true before proceeding.

For a complete reference on creating an Aruba user-centric network, refer to the ArubaOS 6.x User Guide

1. To configure a wireless LAN (WLAN) to a group of access points, log into the controller by browsing to **https://controller-dns-name-or-ip-address**
2. Click the **Configuration Tab**. In the left panel, locate the **WIZARDS** section and click the link for the **WLAN/LAN Wizard**.



3. Select the deployment scenario that fits your requirements and click the **Begin** button to begin the wizard.



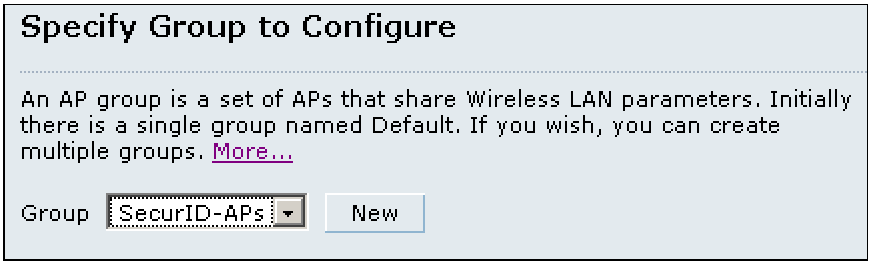
Welcome to the WLAN/LAN Configuration Wizard

Deployment scenario:

● Campus Only -- all of the access points will be physically connected to the local controller

○ Remote Networking -- some of the access points will be deployed at remote locations

4. Select the AP Group that you wish to configure. You may also choose to create a new AP Group for which to configure the WLAN. Click **Next** to continue.

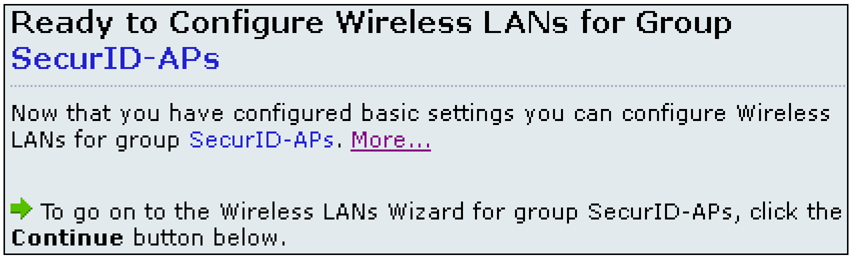


Specify Group to Configure

An AP group is a set of APs that share Wireless LAN parameters. Initially there is a single group named Default. If you wish, you can create multiple groups. More...

Group: SecurID-APs

5. Once you have chosen an AP Group to configure, click the **Continue** button to start the WLAN configuration wizard.

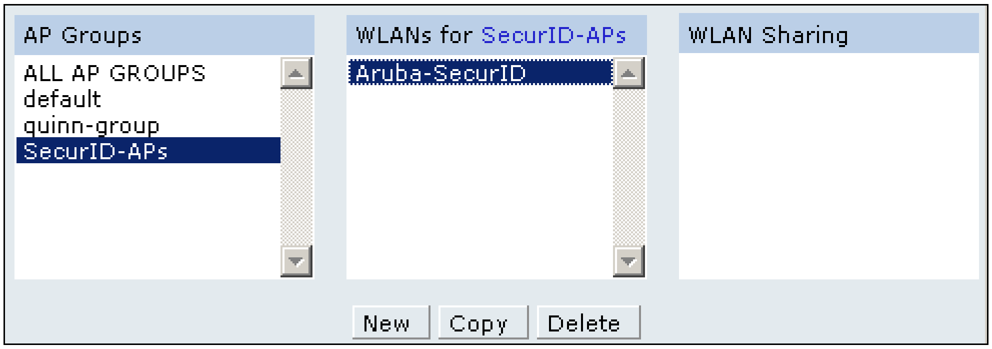


Ready to Configure Wireless LANs for Group SecurID-APs

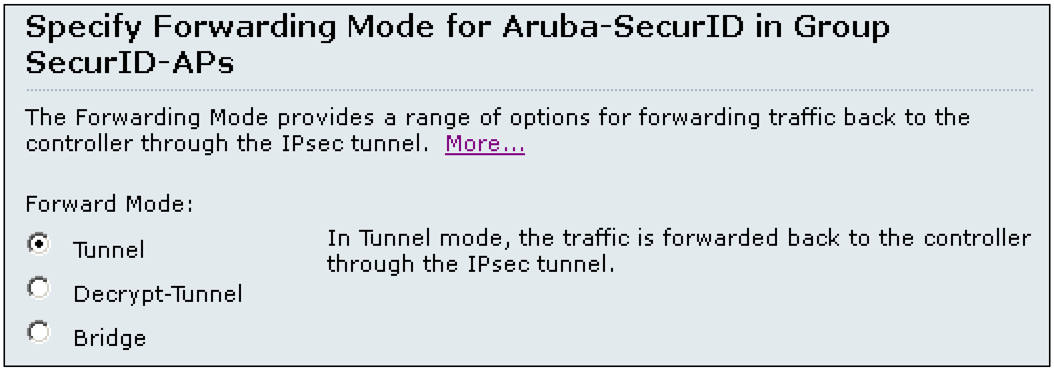
Now that you have configured basic settings you can configure Wireless LANs for group SecurID-APs. More...

To go on to the Wireless LANs Wizard for group SecurID-APs, click the **Continue** button below.

6. If you are editing an existing WLAN, select the appropriate group and WLAN to edit. If you wish to create a new WLAN, select the appropriate group and click the **New** button. Once you have chosen the WLAN to configure, click the **Next** button.



7. Choose the forwarding mode for the WLAN that meets your requirements. Click **Next** to continue.



Specify Forwarding Mode for Aruba-SecurID in Group SecurID-APs

The Forwarding Mode provides a range of options for forwarding traffic back to the controller through the IPsec tunnel. More...

Forward Mode:

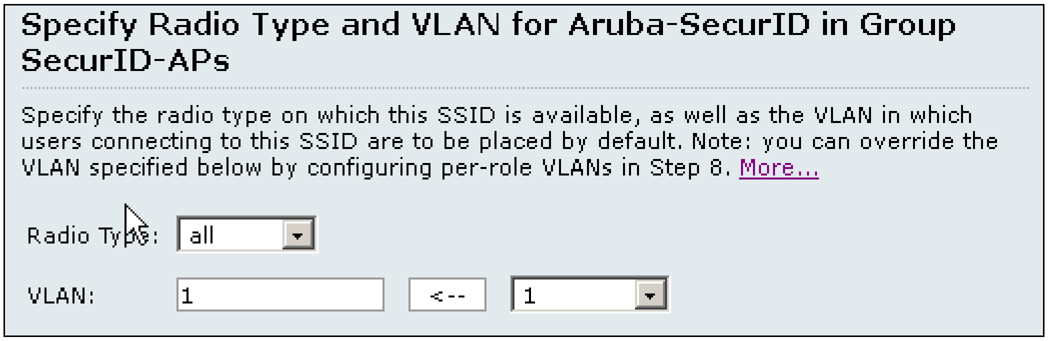
● Tunnel

○ Decrypt-Tunnel

○ Bridge

In Tunnel mode, the traffic is forwarded back to the controller through the IPsec tunnel.

8. Choose the radio type that the APs should use to serve the WLAN. Specify the VLAN that members of this WLAN will join. Click **Next** to continue.



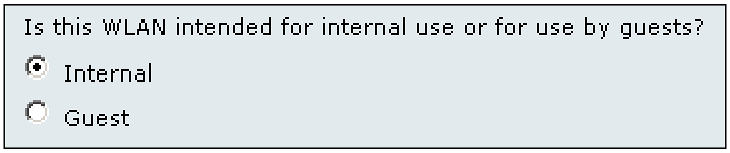
Specify Radio Type and VLAN for Aruba-SecurID in Group SecurID-APs

Specify the radio type on which this SSID is available, as well as the VLAN in which users connecting to this SSID are to be placed by default. Note: you can override the VLAN specified below by configuring per-role VLANs in Step 8. More...

Radio Type: all

VLAN: 1 <-- 1

9. Specify whether the WLAN is intended for internal use or guests. Click **Next** to continue.

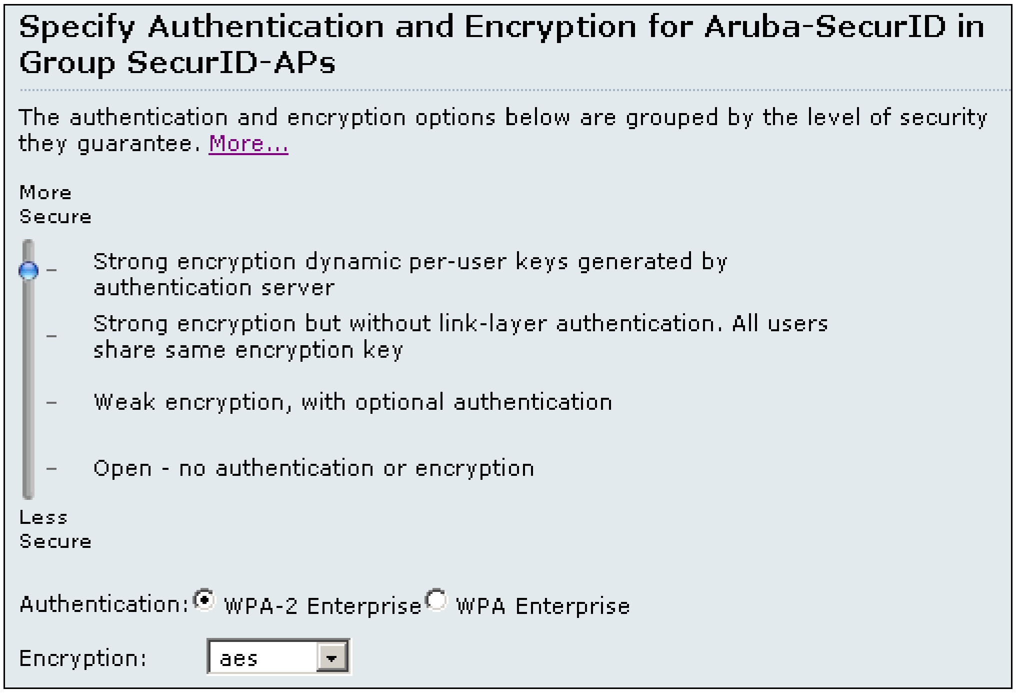


Is this WLAN intended for internal use or for use by guests?

● Internal

○ Guest

10. Specify the authentication and encryption scheme that the WLAN will require. RSA SecurID authentication can be used to secure any 802.1x-compatible authentication scheme. Click **Next** to continue.



Specify Authentication and Encryption for Aruba-SecurID in Group SecurID-APs

The authentication and encryption options below are grouped by the level of security they guarantee. More...

More Secure

- Strong encryption dynamic per-user keys generated by authentication server
- Strong encryption but without link-layer authentication. All users share same encryption key
- Weak encryption, with optional authentication
- Open - no authentication or encryption

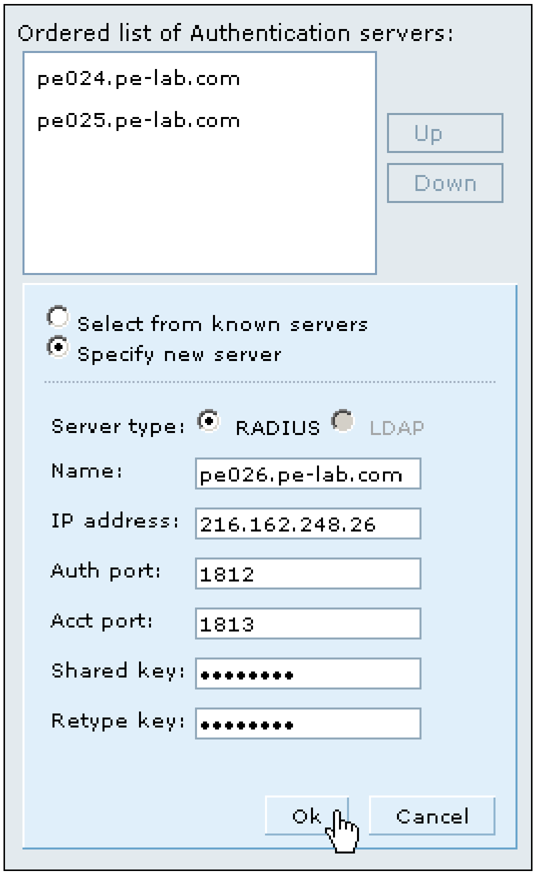
Less Secure

Authentication: ● WPA-2 Enterprise ○ WPA Enterprise

Encryption: aes

11. Enter the information corresponding to your Authentication Manager Servers. If you have already configured these servers as AAA Servers in the Mobility controller's configuration, you can select them from the list of **known servers**. Otherwise, add them now. For each Authentication Manager server you wish to authenticate WLAN clients, specify the following information. Click **Next** when finished.

    - **Name:** a descriptive name.
    - **IP address:** the IP address of the Authentication Manager Server.
    - **Auth port:** the RADIUS authentication port of the Authentication Manager's RADIUS server.
    - **Acct port:** the RADIUS accounting port of the Authentication Manager's RADIUS server.
    - **Shared key:** the RADIUS shared secret that was specified when configuring the RADIUS Client that corresponds to the Mobility controller.



Ordered list of Authentication servers:

pe024.pe-lab.com
pe025.pe-lab.com

○ Select from known servers
● Specify new server

Server type: ● RADIUS ○ LDAP

Name: pe026.pe-lab.com

IP address: 216.162.248.26

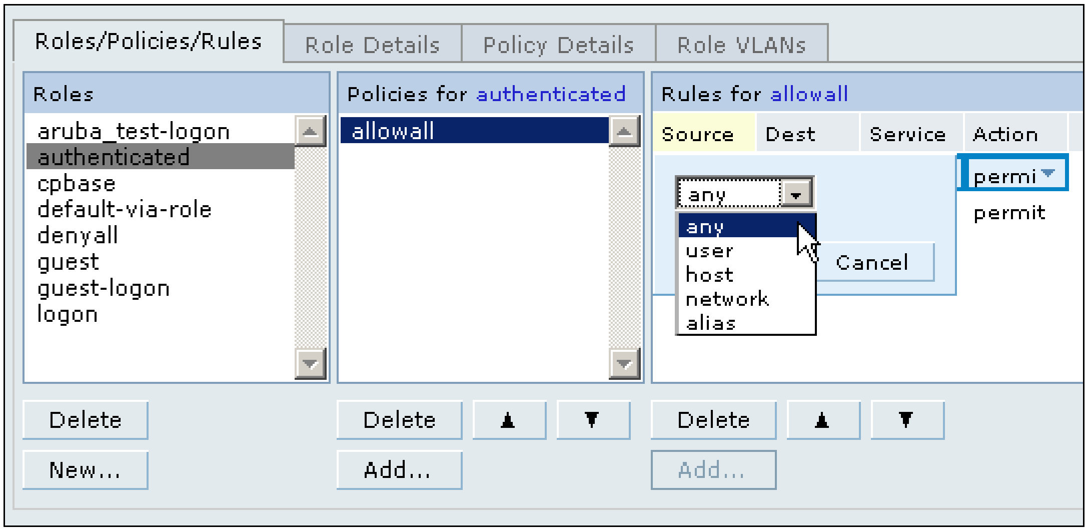
Auth port: 1812

Acct port: 1813

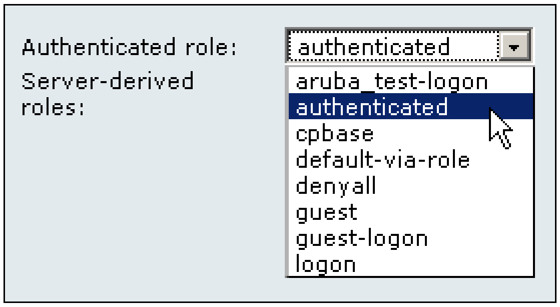
Shared key: ••••••••

Retype key: ••••••••

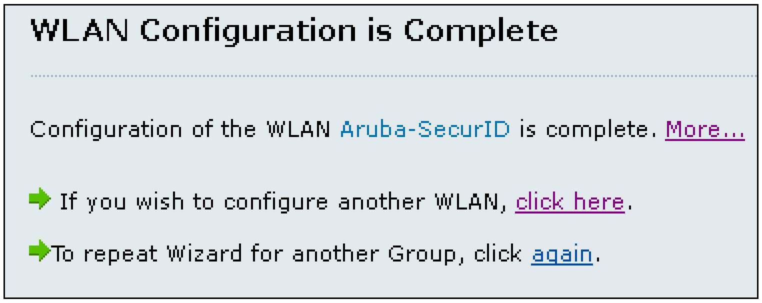
12. The Aruba controller provides robust role, policy, and rule definitions that allow you to govern client behavior during different stages of connection to the WLAN which are outside the scope of this guide. This screen allows you to configure these settings according to your needs. Refer to the ArubaOS User Guide for complete information. Click **Next** when finished.



13. Choose the role that will be assigned to authenticated clients. Click **Next** to continue.



14. Click **Finish** to complete the WLAN configuration wizard. A summary of the configuration settings will be displayed. Click **Finish** once more to push the configuration to the Mobility controller. The new WLAN will become active for all access points that are in the AP Group(s) that have this WLAN configured.



WLAN Configuration is Complete

Configuration of the WLAN Aruba-SecurID is complete. More...

➡ If you wish to configure another WLAN, click here.

➡To repeat Wizard for another Group, click again.

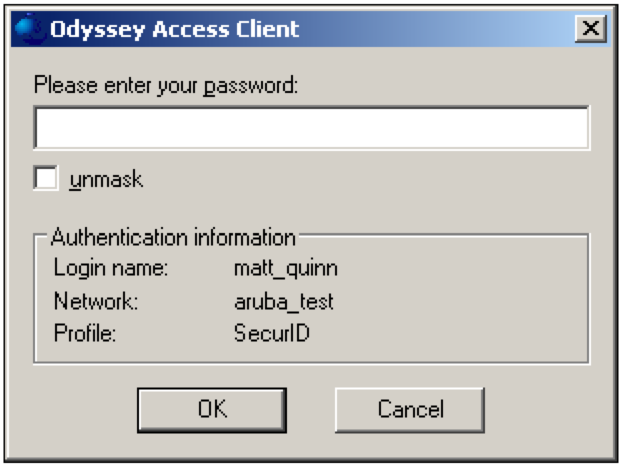
Configuring the Network Supplicant

After you have configured the Mobility controller to use RSA SecurID authentication, a compatible 802.1X supplicant will prompt the end user for their two-factor credentials before the end point is allowed to communicate on the wireless LAN. The supplicant may require additional configuration. While any 802.1X-compatible supplicant should work, please refer to the Secured By RSA solutions gallery (**http://www.rsasecured.com**) for more information on certified wireless supplicants.

Note: For the purposes of this test, Juniper's Odyssey Access Client was used.

RSA SecurID Login Screens

Login screen:



Odyssey Access Client

Please enter your password:

□ unmask

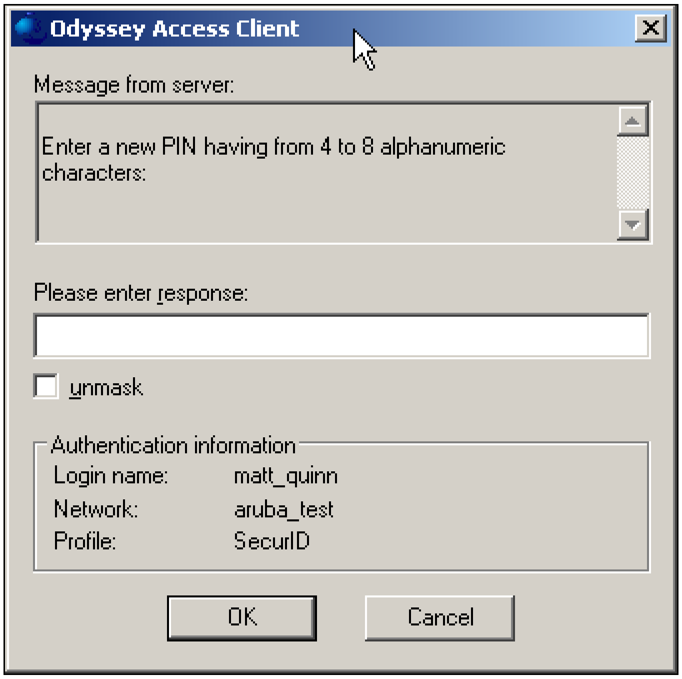
Authentication information

Login name: matt_quinn

Network: aruba_test

Profile: SecurID

User-defined New PIN:



Odyssey Access Client

Message from server:

Enter a new PIN having from 4 to 8 alphanumeric characters:

Please enter response:

□ unmask

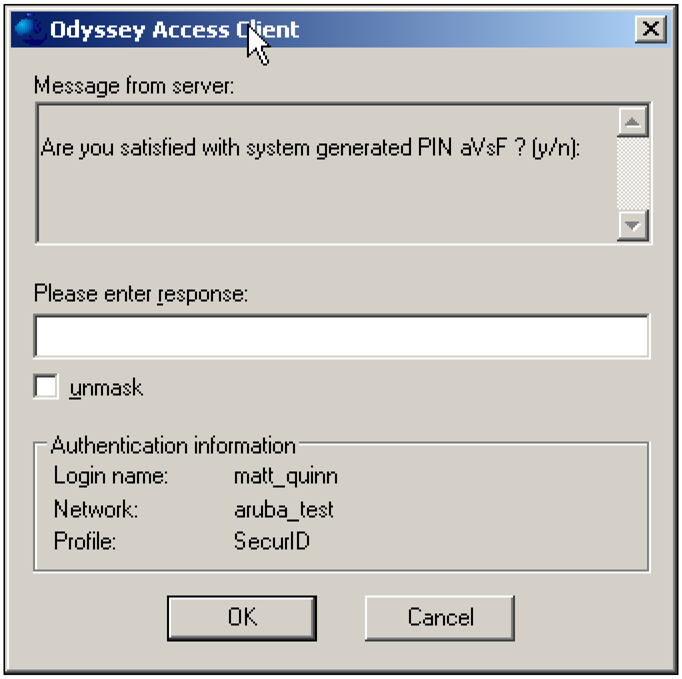
Authentication information

Login name: matt_quinn

Network: aruba_test

Profile: SecurID

System-generated New PIN:



Odyssey Access Client

Message from server:

Are you satisfied with system generated PIN aVsF ? (y/n):

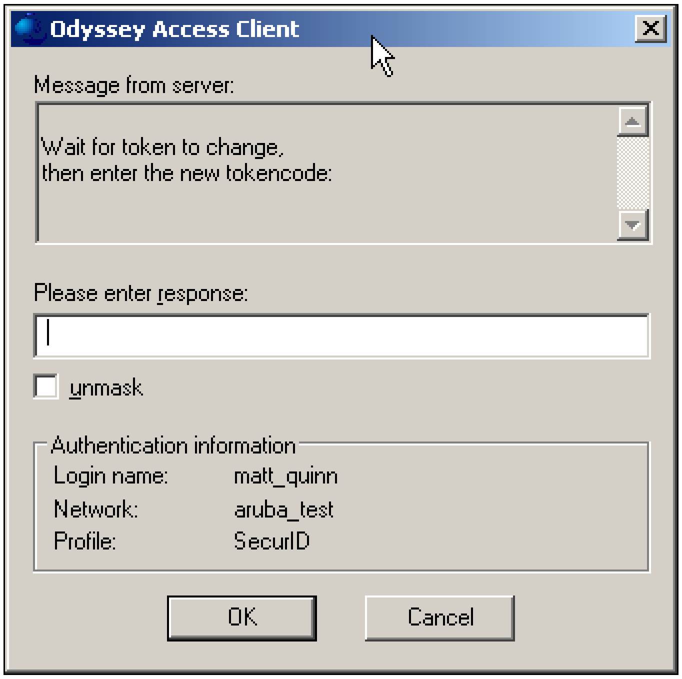
Please enter response:

□ unmask

Authentication information

Login name:	matt_quinn
Network:	aruba_test
Profile:	SecurID

Next Tokencode:



Odyssey Access Client

Message from server:

Wait for token to change,
then enter the new tokencode:

Please enter response:

□ unmask

Authentication information

Login name:	matt_quinn
Network:	aruba_test
Profile:	SecurID

Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1	Virtual Appliance
Aruba 3600 Mobility Controller	6.4.2.1	ArubaOS
Juniper Odyssey Access Client	5.2 R3	Windows 7

RSA SecurID Authentication

Date Tested: December 10, 2014

Mandatory Functionality	RSA Native UDP Agent	RSA Native TCP Agent	RADIUS Client
New PIN Mode			
Force Authentication After New PIN	N/A	N/A	✓
System Generated PIN	N/A	N/A	✓
User Defined (4-8 Alphanumeric)	N/A	N/A	✓
User Defined (5-7 Numeric)	N/A	N/A	✓
Deny 4 and 8 Digit PIN	N/A	N/A	✓
Deny Alphanumeric PIN	N/A	N/A	✓
Deny PIN Reuse	N/A	N/A	✓
Passcode			
16 Digit Passcode	N/A	N/A	✓
4 Digit Fixed Passcode	N/A	N/A	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	N/A	✓
On-Demand Authentication			
On-Demand Authentication	N/A	N/A	✓
On-Demand New PIN	N/A	N/A	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	N/A	✓
No RSA Authentication Manager	N/A	N/A	✓

GLS / PAR

✓= Pass ✗ = Fail N/A = Not Applicable to Integration