



## RSA SecurID Ready Implementation Guide

Last Modified: August 25, 2011

### Partner Information

---

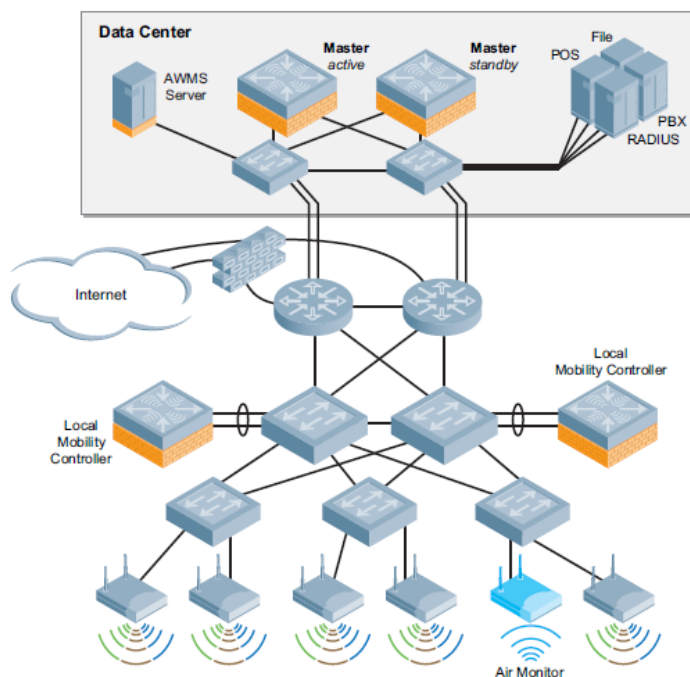
Product Information	
Partner Name	Aruba Networks
Web Site	<a href="http://www.arubanetworks.com">www.arubanetworks.com</a>
Product Name	Mobility Controllers and Access Points
Version & Platform	ArubaOS 6.1.2.2
Product Description	<p>Aruba Mobility Controllers create a single, unified network that manages 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).</p> <p>Running the ArubaOS operating system, Mobility Controllers support integrated capabilities, including the stateful ICSA-certified 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.</p>



## 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 SecurID supported features	
Aruba Mobility Controller—ArubaOS 6.1.2.2	
RSA SecurID Authentication via Native RSA SecurID Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
On-Demand Authentication via API	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



## Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

Set the Agent Type to “Standard Agent” when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with the Mobility controller will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for <Partner Product> to communicate with 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: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.**

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

## RSA SecurID files

RSA SecurID Authentication Files	
Files	Location
sdconf.rec	N/A
Node Secret	N/A
sdstatus.12	N/A
sdopts.rec	N/A

 **Note: The appendix of this document contains more detailed information regarding these files.**

## Partner Product Configuration

### Before You Begin


This section provides instructions for configuring the 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 Mobility 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.

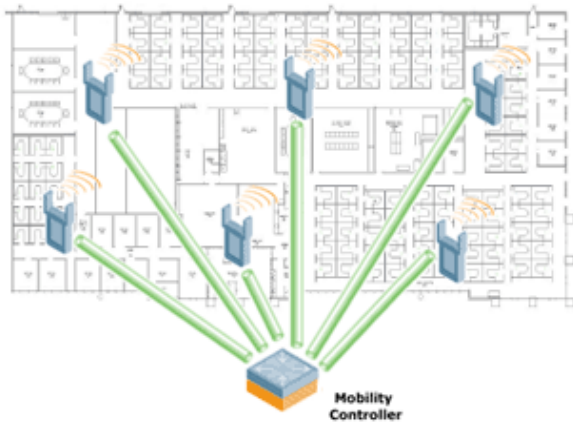
### Welcome to the WLAN/LAN Configuration Wizard

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

#### Campus Wireless



The diagram illustrates a 'Campus Wireless' deployment. It shows a floor plan of a building with several access points (APs) distributed throughout. All APs are connected via green lines to a central 'Mobility Controller' located at the bottom center of the diagram. The APs are represented by blue icons with orange signal waves emanating from them.

**Begin** **Cancel**

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 New

- 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.

- 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.

AP Groups	WLANs for SecurID-APs	WLAN Sharing
ALL AP GROUPS default quinn-group SecurID-APs	Aruba-SecurID	

New Copy Delete

- 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:

VLAN:  <--

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:

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.

The screenshot shows a configuration window titled "Ordered list of Authentication servers:". At the top, there is a list box containing two entries: "pe024.pe-lab.com" and "pe025.pe-lab.com". To the right of this list are "Up" and "Down" buttons. Below the list box, there are two radio buttons: "Select from known servers" (which is unselected) and "Specify new server" (which is selected). Under the "Specify new server" section, there are several input fields: "Server type" with radio buttons for "RADIUS" (selected) and "LDAP"; "Name" with the text "pe026.pe-lab.com"; "IP address" with the text "216.162.248.26"; "Auth port" with the text "1812"; "Acct port" with the text "1813"; "Shared key" with a masked field of seven dots; and "Retype key" with another masked field of seven dots. At the bottom right of the dialog are "Ok" and "Cancel" buttons, with a mouse cursor clicking on the "Ok" button.



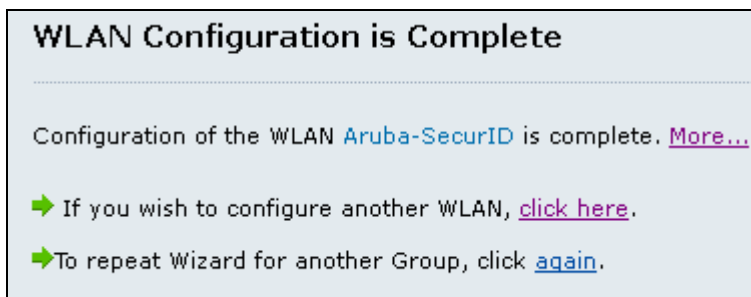
12. The Aruba controller provides robust role, policy, and rule definitions that allow you to govern client behavior during different stages of connection to the WLAN which are outside the scope of this guide. This screen allows you to configure these settings according to your needs. Refer to the ArubaOS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

The screenshot shows the 'Roles/Policies/Rules' configuration page. It has four tabs: 'Roles', 'Role Details', 'Policy Details', and 'Role VLANs'. The 'Roles' tab is active, showing a list of roles: 'aruba\_test-logon', 'authenticated', 'cpbase', 'default-via-role', 'denyall', 'guest', 'guest-logon', and 'logon'. The 'authenticated' role is selected. Below the list are 'Delete' and 'New...' buttons. The 'Policy Details' tab is also visible, showing 'Policies for authenticated' with a list containing 'allowall'. Below this are 'Delete' and 'Add...' buttons. The 'Role VLANs' tab is also visible, showing 'Rules for allowall' with a table. The table has columns: 'Source', 'Dest', 'Service', and 'Action'. The 'Source' column has a dropdown menu open with options: 'any', 'any', 'user', 'host', 'network', and 'alias'. The 'Action' column has a dropdown menu open with options: 'permi' and 'permit'. Below the table are 'Delete', 'Add...', and navigation arrows.

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

The screenshot shows a dialog box for selecting an authenticated role. It has a label 'Authenticated role:' and a dropdown menu. The dropdown menu is open, showing a list of roles: 'aruba\_test-logon', 'authenticated', 'cpbase', 'default-via-role', 'denyall', 'guest', 'guest-logon', and 'logon'. The 'authenticated' role is selected. Below the dropdown menu is a label 'Server-derived roles:'.

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.



### ***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.

---

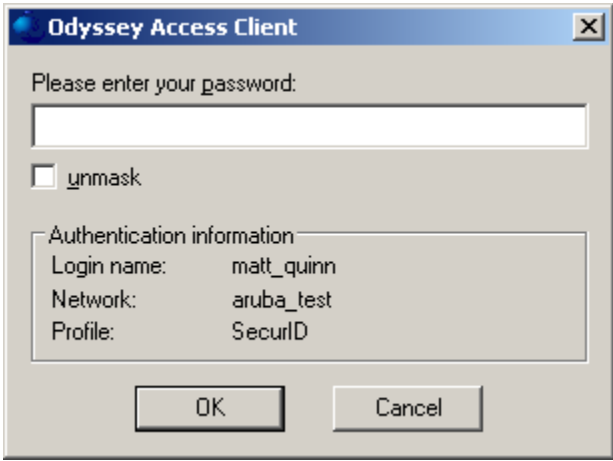
 **Note:** For the purposes of this test, Juniper's Odyssey Access Client was used.

---

## Screens

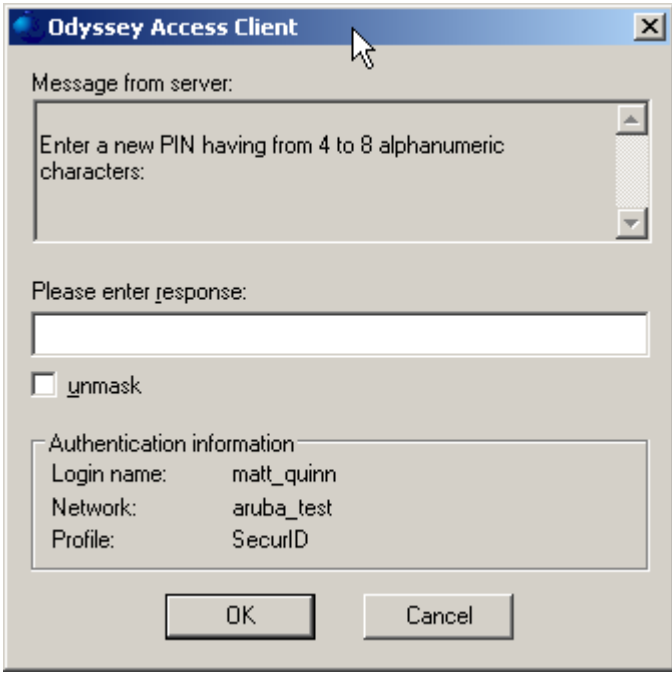
---

Login screen:



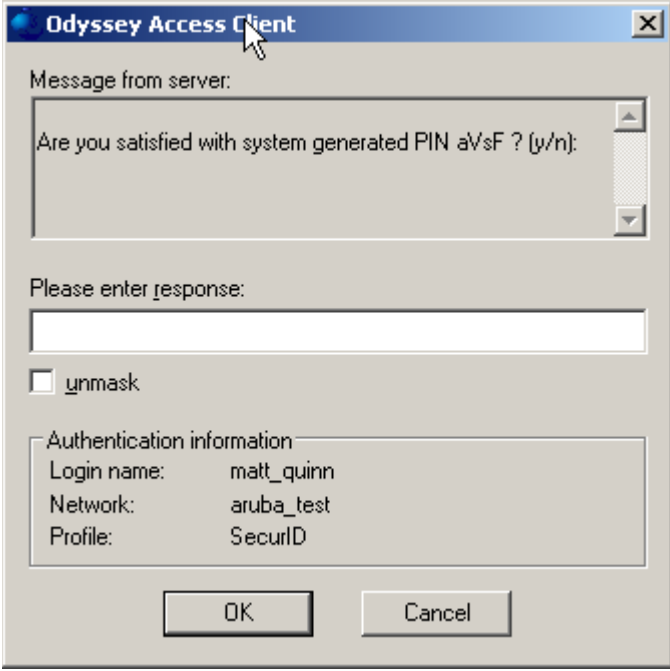
The login screen is a window titled "Odyssey Access Client". It contains a text box for a password with the label "Please enter your password:". Below the text box is an unchecked checkbox labeled "unmask". A section titled "Authentication information" contains three labels and values: "Login name: matt\_quinn", "Network: aruba\_test", and "Profile: SecurlD". At the bottom are "OK" and "Cancel" buttons.

User-generated New PIN:



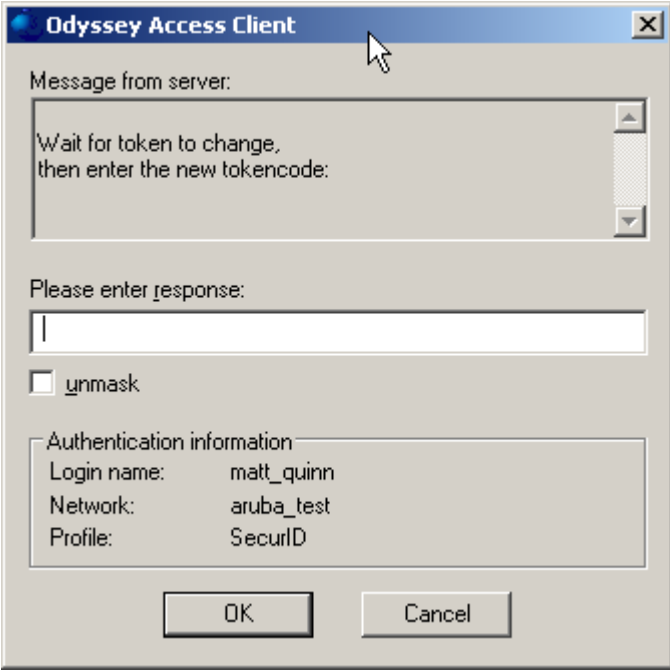
The "New PIN" screen is a window titled "Odyssey Access Client". It features a message box with the text "Message from server:" and "Enter a new PIN having from 4 to 8 alphanumeric characters:". Below this is a text box for the response with the label "Please enter response:". An unchecked checkbox labeled "unmask" is positioned below the text box. The "Authentication information" section at the bottom shows "Login name: matt\_quinn", "Network: aruba\_test", and "Profile: SecurlD". "OK" and "Cancel" buttons are at the bottom.

System-generated New PIN:



The image shows a Windows-style dialog box titled "Odyssey Access Client". It contains a "Message from server:" section with a text area displaying "Are you satisfied with system generated PIN aVsF ? (y/n):". Below this is a "Please enter response:" text input field. A checkbox labeled "unmask" is present. At the bottom, there is an "Authentication information" section showing "Login name: matt\_quinn", "Network: aruba\_test", and "Profile: SecurlD". "OK" and "Cancel" buttons are at the bottom right.

Next Tokencode:



The image shows a similar "Odyssey Access Client" dialog box. The "Message from server:" section displays "Wait for token to change, then enter the new tokencode:". The "Please enter response:" text input field is empty. The "unmask" checkbox and "Authentication information" section (Login name: matt\_quinn, Network: aruba\_test, Profile: SecurlD) are identical to the previous screen. "OK" and "Cancel" buttons are at the bottom right.

## Certification Checklist for RSA Authentication Manager

Date Tested: August 25, 2011

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1 SP4	Windows Server 2003 SP2
Aruba Mobility Controller 3600	6.1.2.2	ArubaOS
Juniper Odyssey Access Client	5.2 R3	Windows XP Professional SP3

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
<b>New PIN Mode</b>			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	✓
System Generated PIN	N/A	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	N/A	User Defined (5-7 Numeric)	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
Deny Numeric PIN	N/A	Deny Numeric PIN	✓
Deny PIN Reuse	N/A	Deny PIN Reuse	✓
<b>Passcode</b>			
14 Digit Passcode	N/A	14 Digit Passcode	✓
4 Digit Fixed Passcode	N/A	4 Digit Fixed Passcode	✓
<b>Next Tokencode Mode</b>			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
<b>On-Demand Authentication</b>			
On-Demand Authentication	N/A	On-Demand Authentication	✓
On-Demand New PIN	N/A	On-Demand New PIN	✓
<b>Load Balancing / Reliability Testing</b>			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓

MRQ

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