Cisco Systems, Inc.
Wireless LAN Controller

RSA SecurID Ready Implementation Guide

Last Modified: November 19, 2013

Partner Information

Product Information	
Partner Name	Cisco Systems, Inc.
Web Site	www.cisco.com
Product Name	Wireless LAN Controller
Version & Platform	7.0
Product Description	Cisco Wireless Controllers help reduce overall operational expenses by simplifying network deployment, operations, and management. These controllers extend the same policy and security from the wired network core to the wireless edge. They deliver visibility, scalability, centralized management, and reliability for building highly secure, enterprise-scale wireless networks for branch offices, small enterprises, main campuses, and more. Centralized management is supported by all Cisco Wireless Controllers.

Solution Summary

Cisco Wireless LAN Controllers (WLC) integrates with RSA Authentication Manager via RADIUS protocol to provide RSA SecurID authentication to users accessing wireless networks.

RSA SecurID supported features	
Cisco Wireless LAN Controller 7.0	
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
RSA Authentication Manager Replica Support	Yes
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 Cisco Wireless LAN Controller will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for the Cisco Wireless LAN Controller 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.

Partner Product Configuration

Before You Begin

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

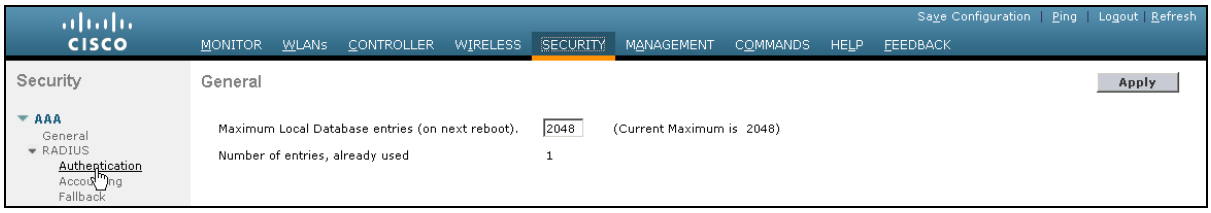
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

Configure RSA Authentication Manager Server(s)

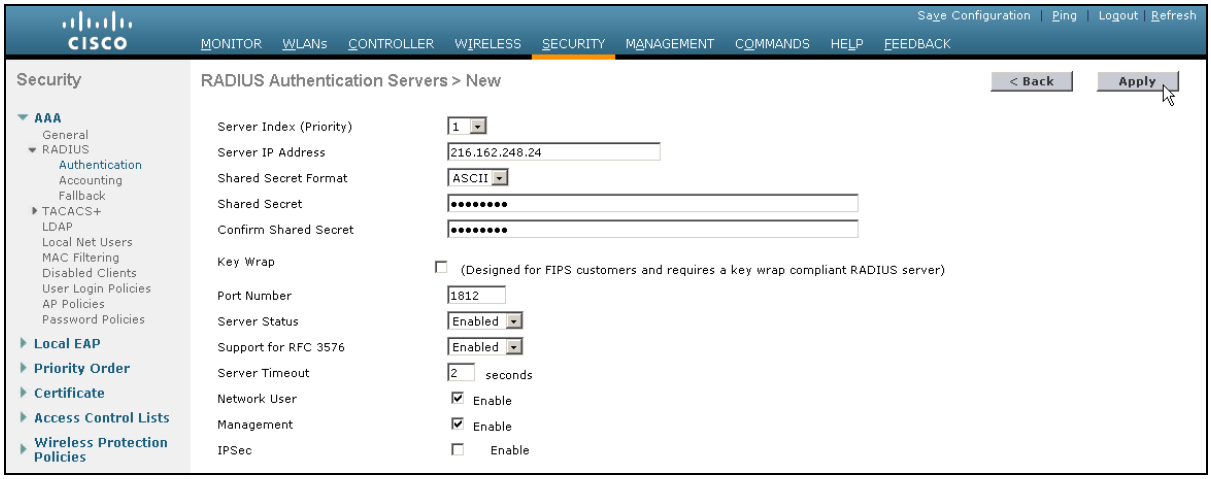
1. Log on to the Cisco Wireless LAN Controller web management console.
2. Open the **SECURITY** tab.

3. Browse to **Security** > **AAA** > **RADIUS** and click **Authentication**.



4. Click **New**.

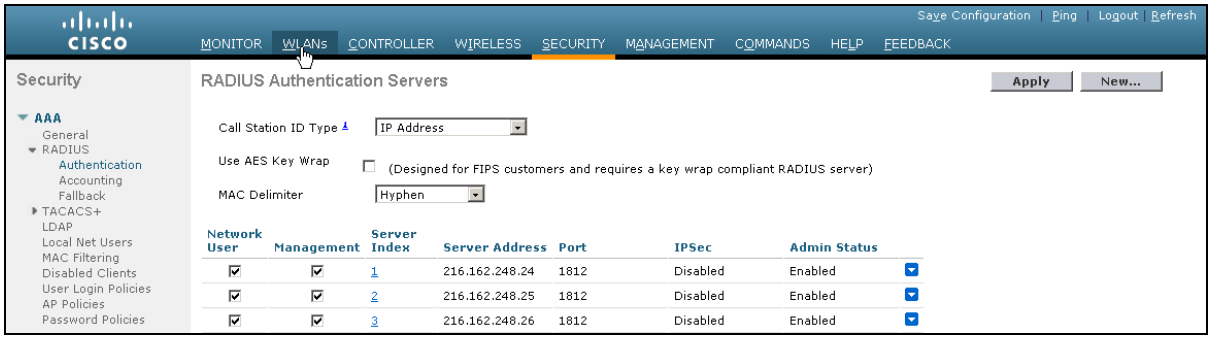
5. Enter the **Server IP Address**, **Shared Secret** for your Authentication Manager server and click **Apply**.



Note: Repeat steps 4 and 5 for Authentication Manager replica servers.

Configure WLAN for SecurID Authentication

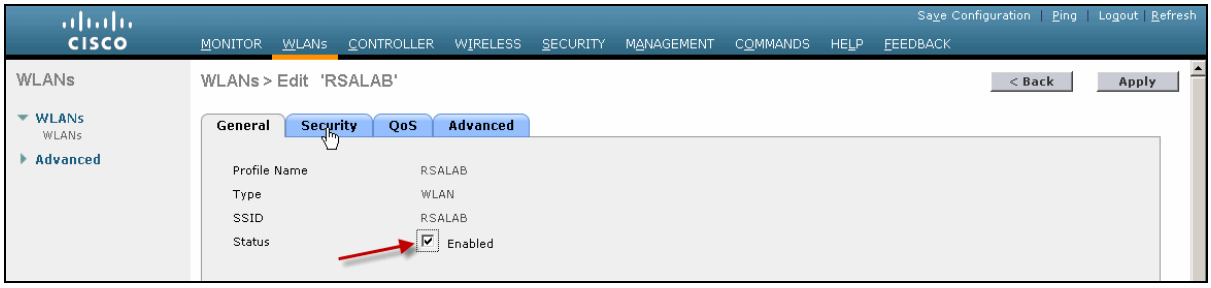
1. Click the **WLANs** tab.



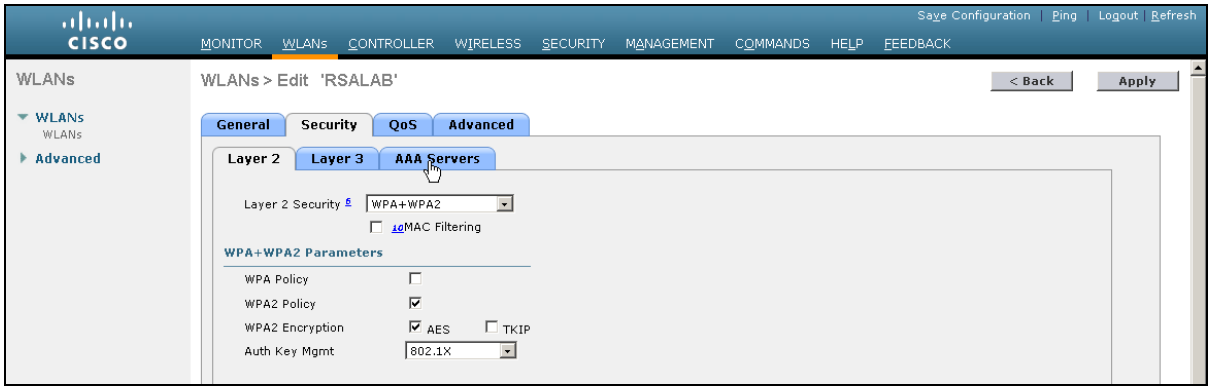
2. Select **Create New** from the drop-down menu and click **Go**.

3. Enter a **Profile Name** and **SSID** for your WLAN and click **Apply**.

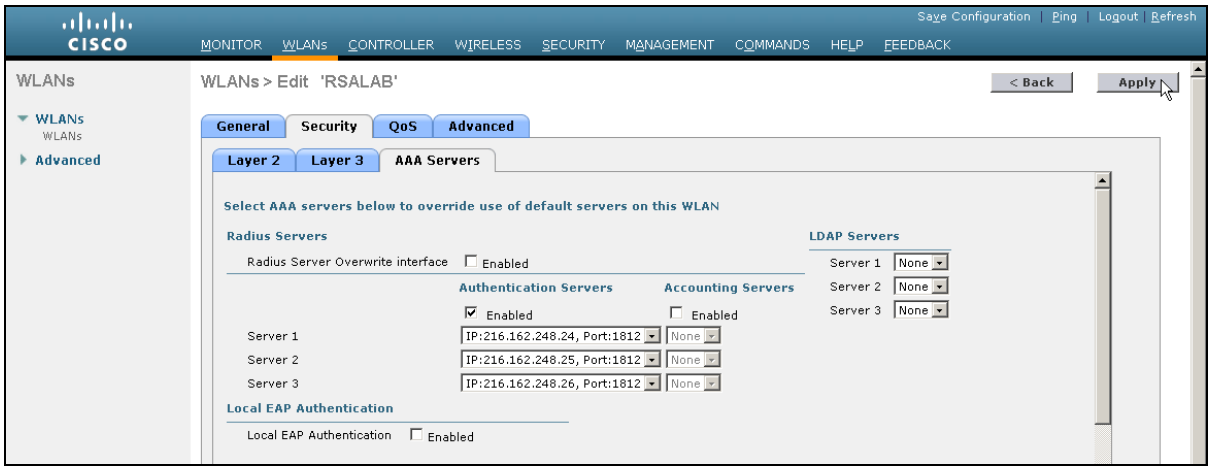
4. Mark the **Enabled** checkbox and open the **Security** tab.



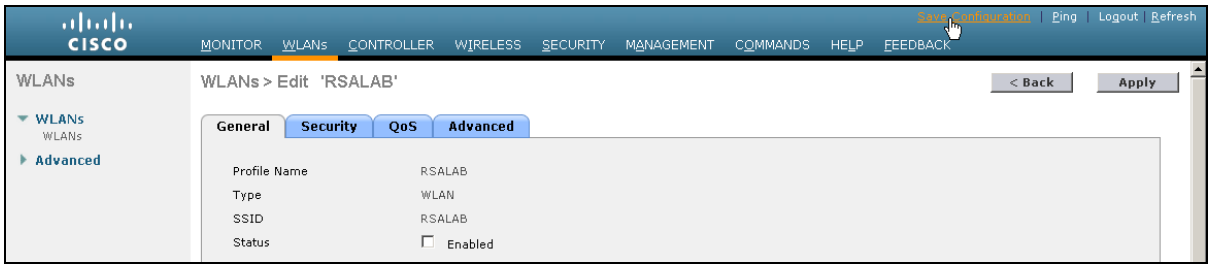
5. Open the **AAA Servers** tab.



6. Select the RSA Authentication Manager server(s) created in the previous section from the **Server 1** (and optionally **Server 2** and **Server 3**) drop-down menus and click **Apply**.



7. (Optional) Click **Save Configuration** to save changes to the startup configuration.



Certification Checklist for RSA Authentication Manager

Date Tested: November 19, 2013

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Cisco Wireless LAN Controller	7.0.116.0	Proprietary
Cisco Lightweight Access Point	7.0.116.0	Proprietary
Cisco AnyConnect Secure Mobility Client (NAM 802.1x supplicant)	3.0.2052	Windows 7 Enterprise

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
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	✓
Passcode			
16-Digit Passcode	N/A	16-Digit Passcode	✓
4-Digit Fixed Passcode	N/A	4-Digit Fixed Passcode	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
On-Demand Authentication			
On-Demand Authentication	N/A	On-Demand Authentication	✓
On-Demand New PIN	N/A	On-Demand New PIN	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓

PEW

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