Cisco Systems, Inc.
Aironet Access Point

RSA SecurID Ready Implementation Guide

Last Modified: November 18, 2013

Partner Information

Product Information	
Partner Name	Cisco Systems, Inc.
Web Site	www.cisco.com
Product Name	Aironet Access Point
Version & Platform	12.4 IOS
Product Description	Wireless LANs enable users to establish and maintain a wireless network connection throughout or between buildings, without the limitations of wires or cables. Cisco provides a family of wireless LAN products that combine the mobility and flexibility users want from a wireless LAN product with the throughput and security they demand from a business LAN.

Solution Summary

This integration enables end users to authenticate using RSA SecurID to gain access to a Cisco Aironet WLAN via Cisco ACS.

The end user connects to the Aironet Access Point using a supported WLAN connection utility (i.e. Cisco AnyConnect). The Aironet Access Point uses RADIUS to communicate with Cisco ACS for authentication. Cisco ACS uses RSA SecurID or RADIUS authentication protocol to communicate with RSA Authentication Manager.

RSA SecurID supported features	
Cisco Aironet Access Point via Cisco ACS	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	Yes
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 ACS will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for Cisco ACS 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	In Memory
Node Secret	In Memory
sdstatus.12	In Memory
sdopts.rec	In Memory

Note: Refer to the RSA SecurID Ready Implementation Guide for Cisco ACS for more detailed information regarding these files.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Aironet Access Point 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 Aironet Access Point components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

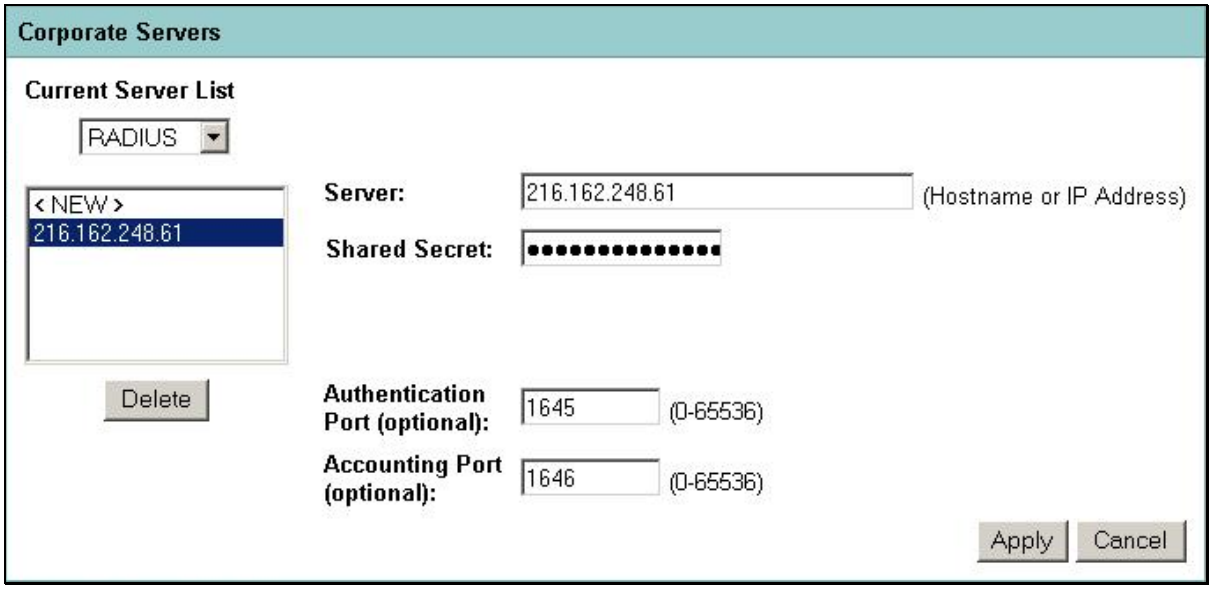
Configure Cisco Aironet AP WLAN clients for SecurID Authentication

There are 3 components that need to be configured in order to enable SecurID authentication to Cisco Aironet WLAN clients:

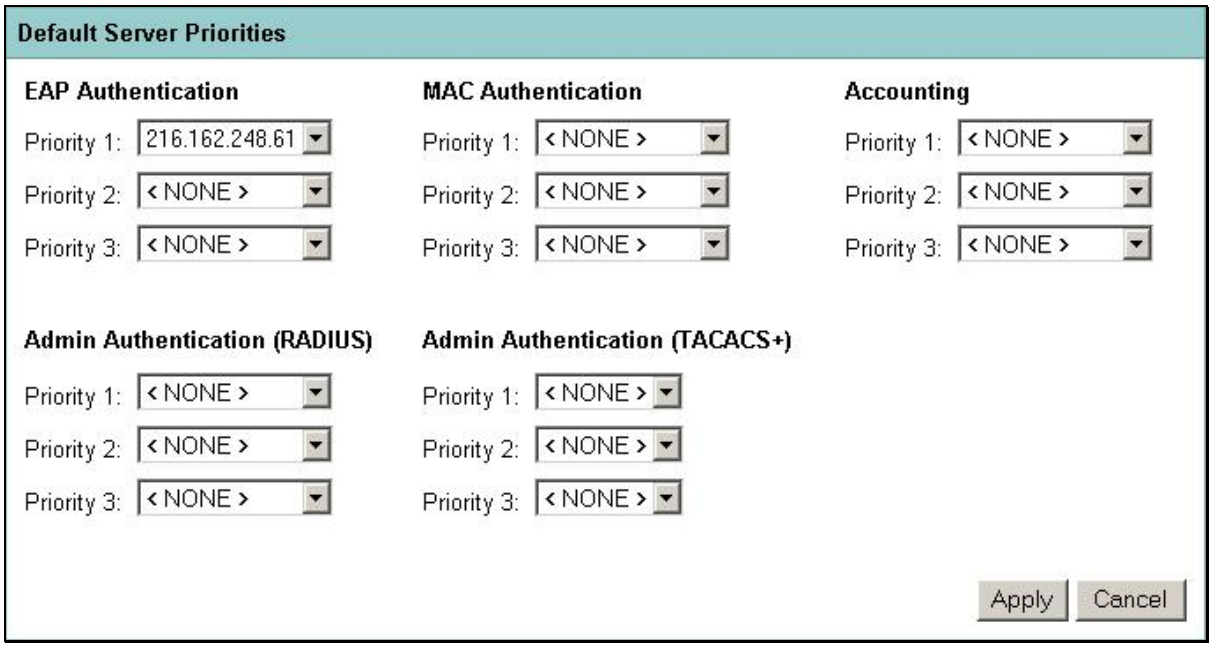
1. Configure Cisco Aironet AP for authentication with Cisco ACS
2. Configure Cisco ACS for authentication with RSA Authentication Manager
3. Configure Cisco AnyConnect

Configure Cisco Aironet Access Point

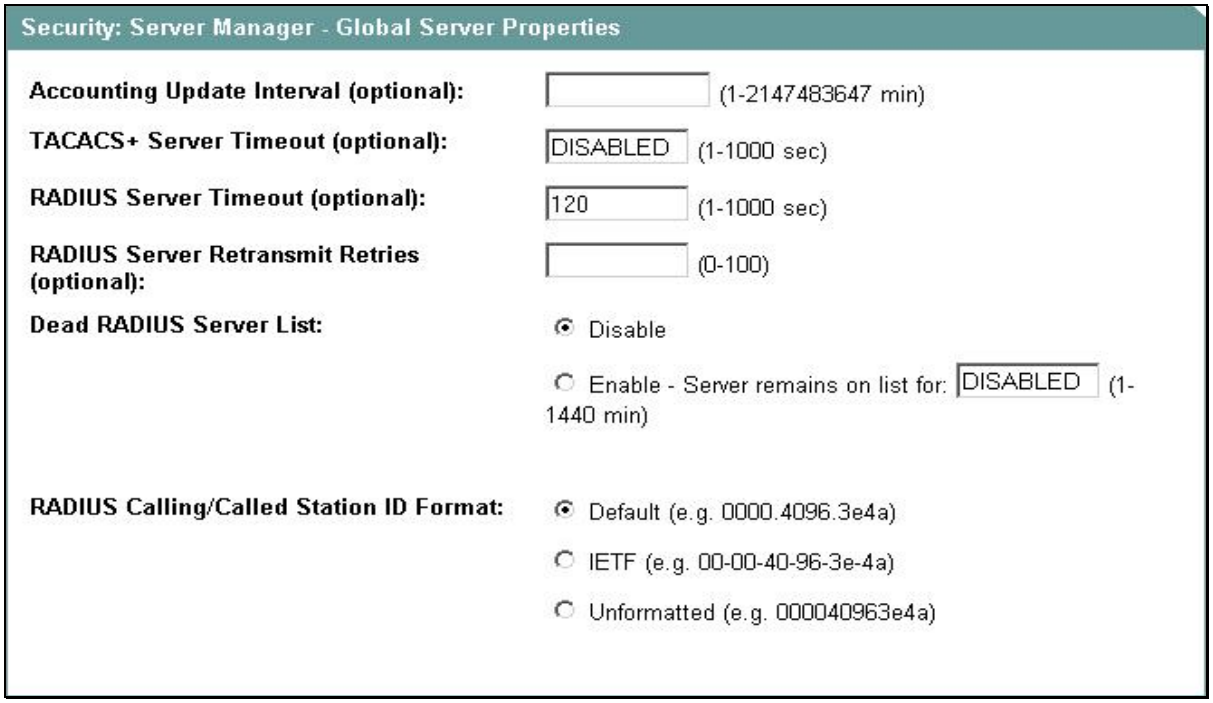
1. Browse to **SECURITY** > **Server Manager** > **Corporate Servers**. Enter the ACS server's **IP address**, **Shared Secret** (created in Step 2) and select **RADIUS** from the drop down menu and click **Apply**.



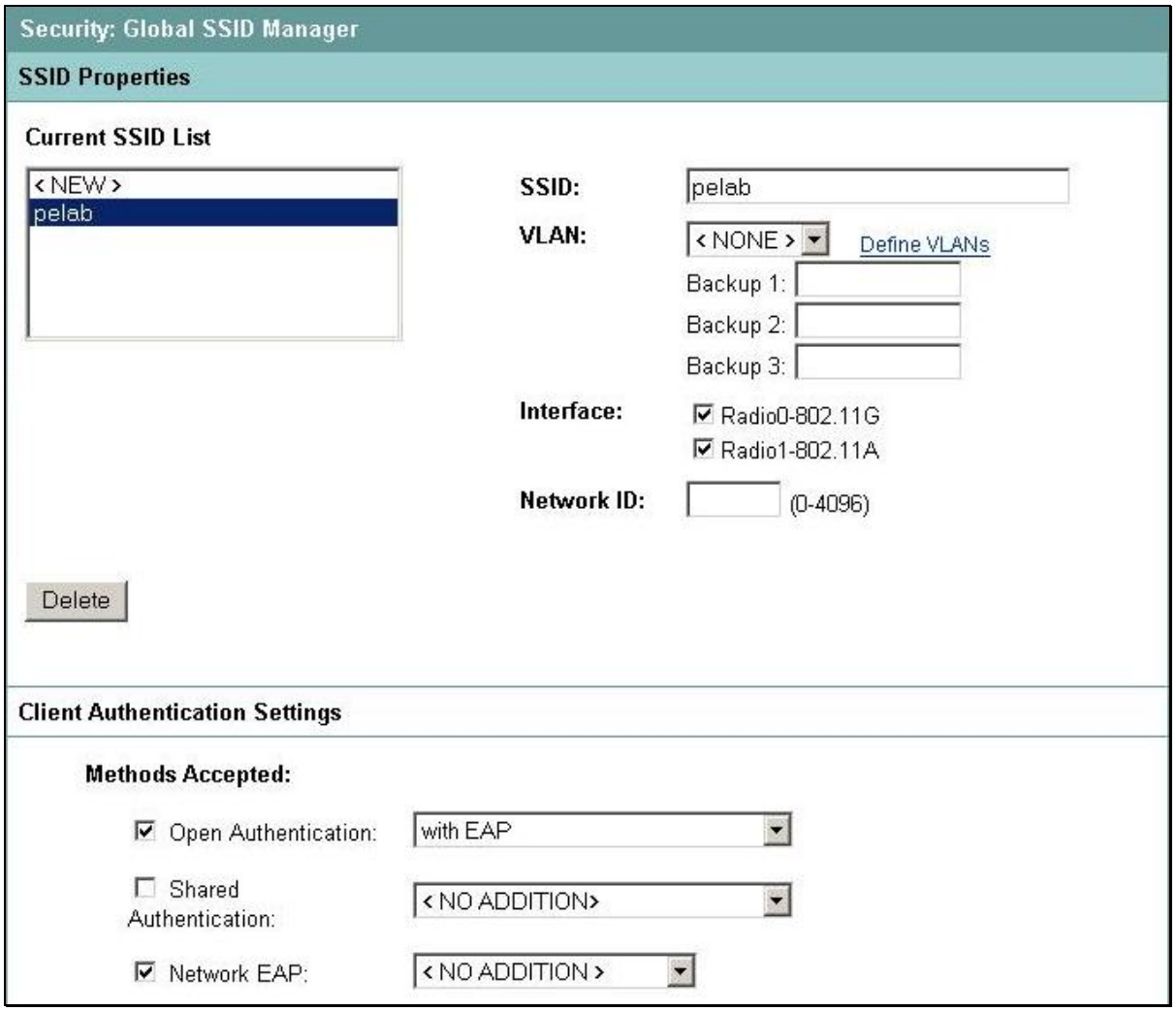
2. Browse to **SECURITY** > **Server Manager** > **Default Server Properties**. Select the server created in the previous step from the **Priority 1** drop down menu in the **EAP Authentication** section and click **Apply**.



3. Browse to **SECURITY** > **Server Manager** > **GLOBAL PROPERTIES**. Set the **RADIUS Server Timeout** to **120** seconds, and click **Apply**.



4. Browse to **SECURITY** > **SSID Manager**. Enable **Open Authentication**, select **with EAP** from the drop down menu and click **Apply**.



Configure Cisco ACS

1. Enable the PEAP-GTC authentication protocol for the network service you are implementing SecurID authentication.
2. Configure an AAA client for the Cisco Aironet Access Point.
3. Configure an Authentication Manager External Identity source (using either native agent or RADIUS) and apply it to the Network Access Policy.

Note: Refer to the Cisco ACS Configuration Guide for more information on configuring Cisco ACS. Refer to the RSA SecurID Ready Implementation Guide for Cisco ACS for more information on configuring Cisco Secure ACS for SecurID authentication.

Configure Cisco AnyConnect

1. Open the AnyConnect Network Access Manager.
2. Set the 802.1x configuration settings to PEAP – token in the WLAN connection profile.

Note: Refer to the Cisco AnyConnect Configuration Guide for more information on configuring Cisco AnyConnect.

Certification Checklist for RSA Authentication Manager

Date Tested: November 18, 2013

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Cisco Secure ACS	5.4.0.46	Proprietary
Cisco Aironet Access Point	12.4(25d)	IOS
Cisco AnyConnect (NAM)	3.0.2052	Windows 7 Enterprise

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

PEW

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