Cisco Systems, Inc.
NAC Appliance (Clean Access)

RSA SecurID Ready Implementation Guide

Last Modified: December 3, 2013

Partner Information

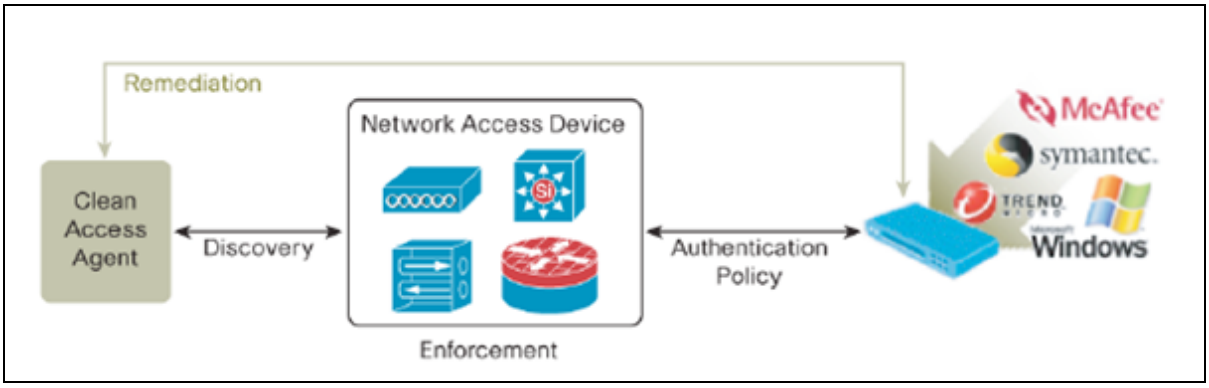
Product Information	
Partner Name	Cisco Systems, Inc.
Web Site	www.cisco.com
Product Name	NAC Appliance (Clean Access)
Version & Platform	4.9
Product Description	The Cisco Network Admission Control (NAC) Appliance (formerly known as Cisco Clean Access) is a powerful, easy-to-use admission control and compliance enforcement solution. With comprehensive security features, In-Band or Out-of-Band deployment options, user authentication tools, and bandwidth and traffic filtering controls, Cisco NAC Appliance is a complete solution for controlling and securing networks. As the central access management point for your network, Cisco NAC Appliance lets you implement security, access, and compliance policies in one place instead of having to propagate the policies throughout the network on many devices.

Solution Summary

Cisco NAC Appliance integrates with RSA SecurID by configuring the RSA authentication server(s) as an external authentication provider via RADIUS protocol. The authentication provider is applied to a user login role which determines which users are challenged for SecurID authentication based on a number of configurable criteria.

Users can be challenged using RSA SecurID authentication at both the Cisco Clean Access Authentication web page and the Cisco NAC Agent.

RSA Authentication Manager supported features Cisco NAC Appliance 4.9	
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
Risk-Based Authentication	No
Risk-Based Authentication with Single Sign-On	No
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 NAC Appliance will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for Cisco NAC Appliance 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

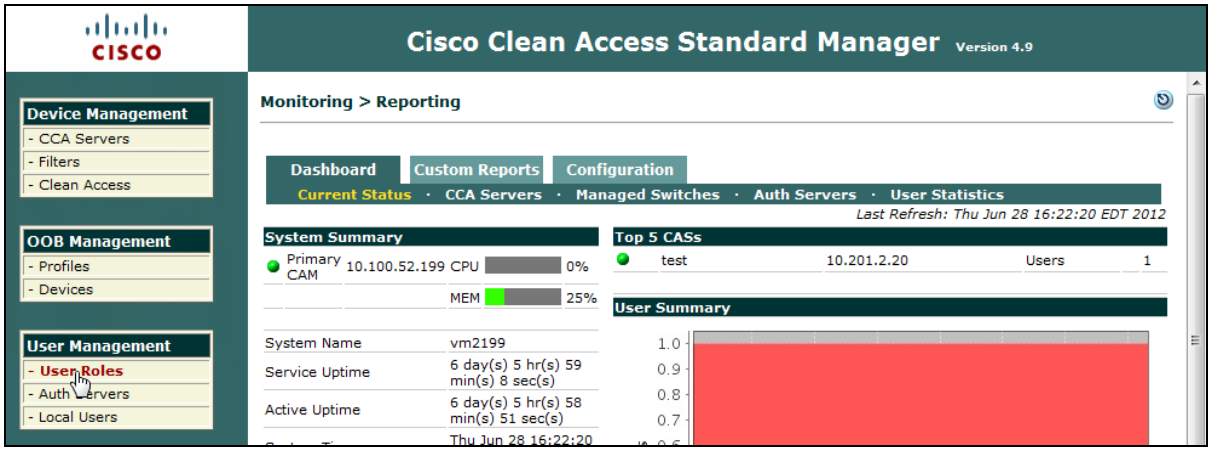
This section provides instructions for configuring the Cisco NAC Appliance with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

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 NAC Appliance components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

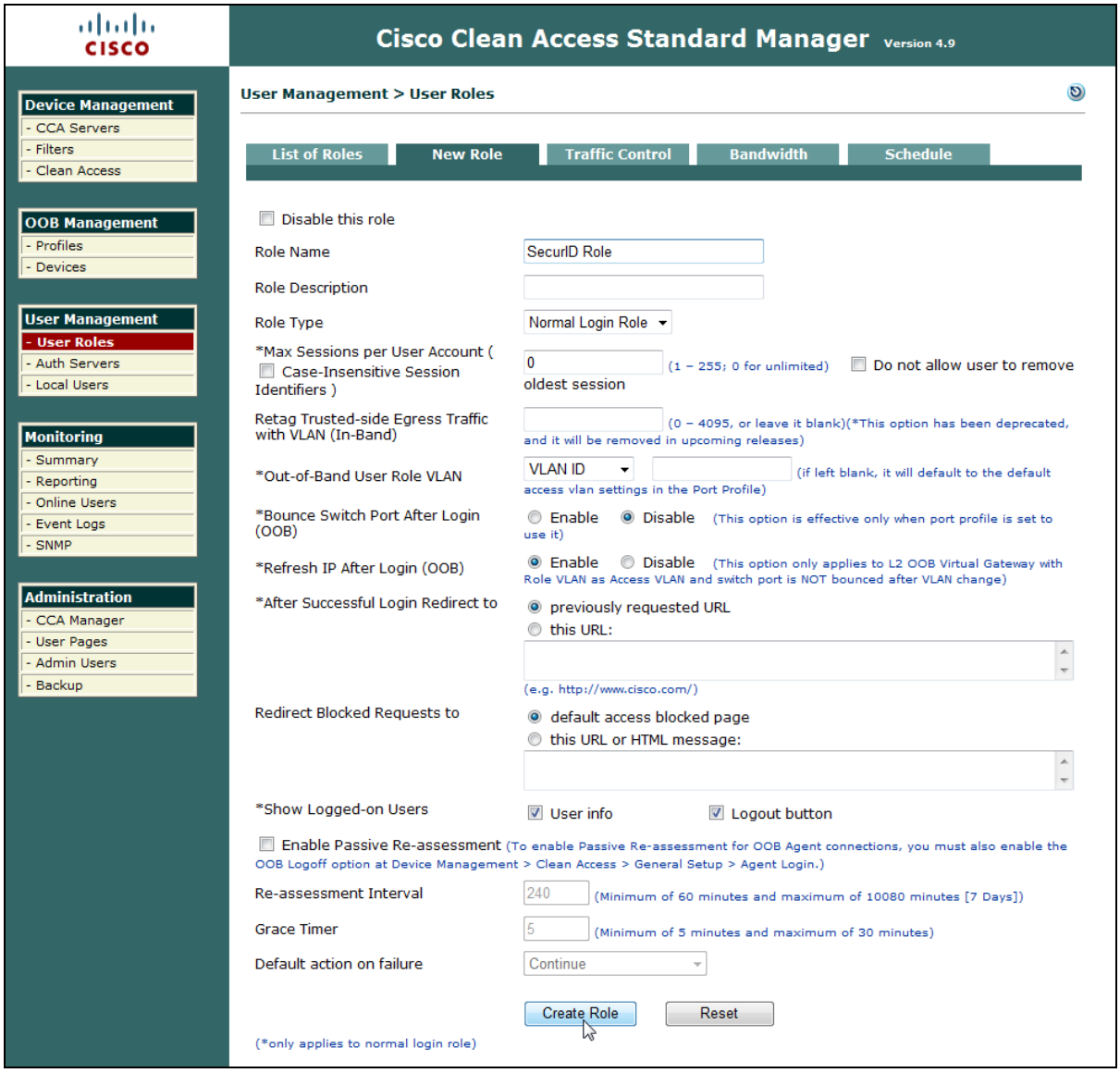
Configure a User Role

1. Login to the Cisco Clean Access Standard Manager.
2. Select **User Roles** from the **User Management** menu.



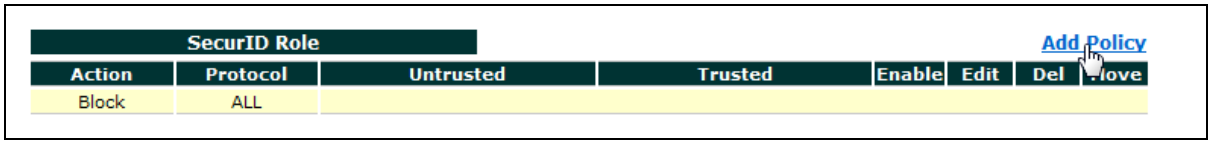
3. Click the **New Role** tab.

4. Enter a **Role Name**, select **Normal Login Role** from the **Role Type** drop-down menu and click **Create Role**.

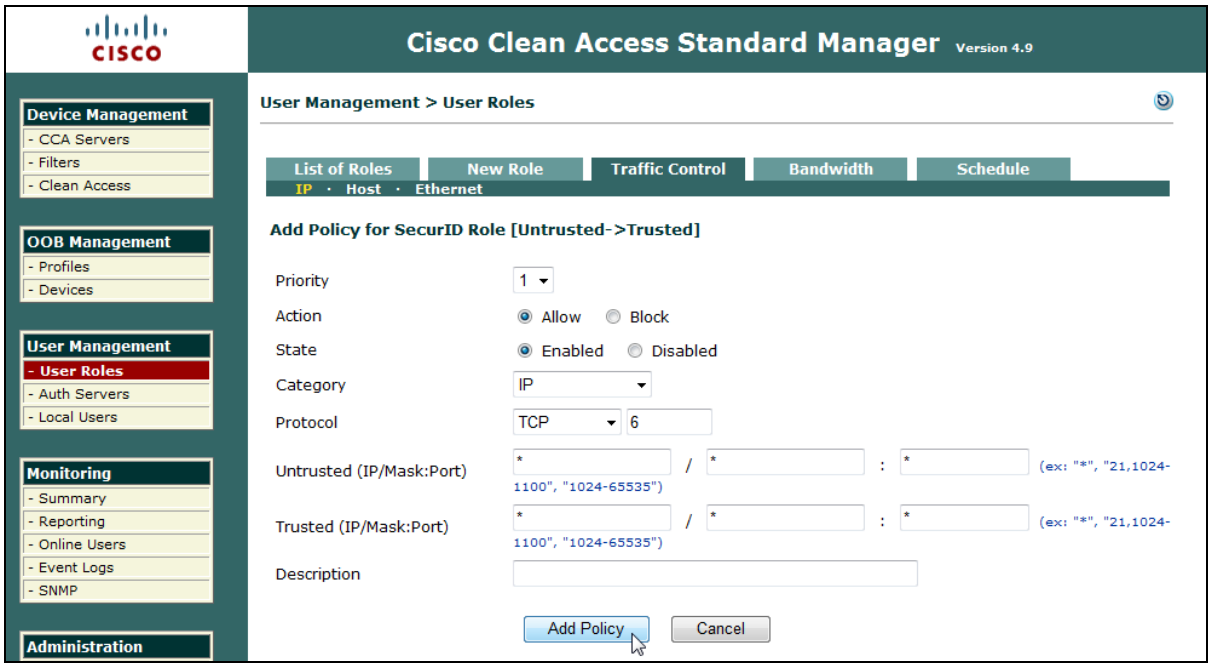


5. Click the **Traffic Control** tab.

6. Click **Add Policy** next to the role you just created.

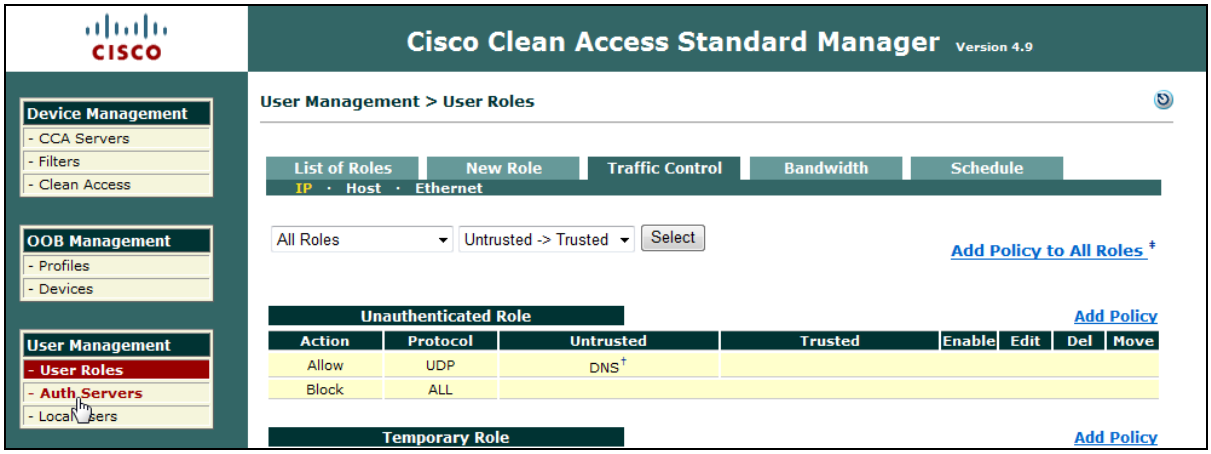


7. Click **Add Policy**.

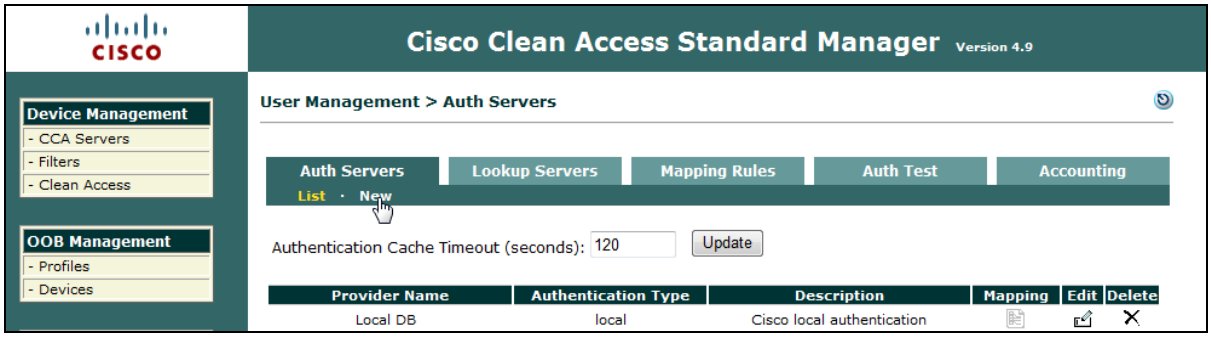


Configure an Authentication Provider

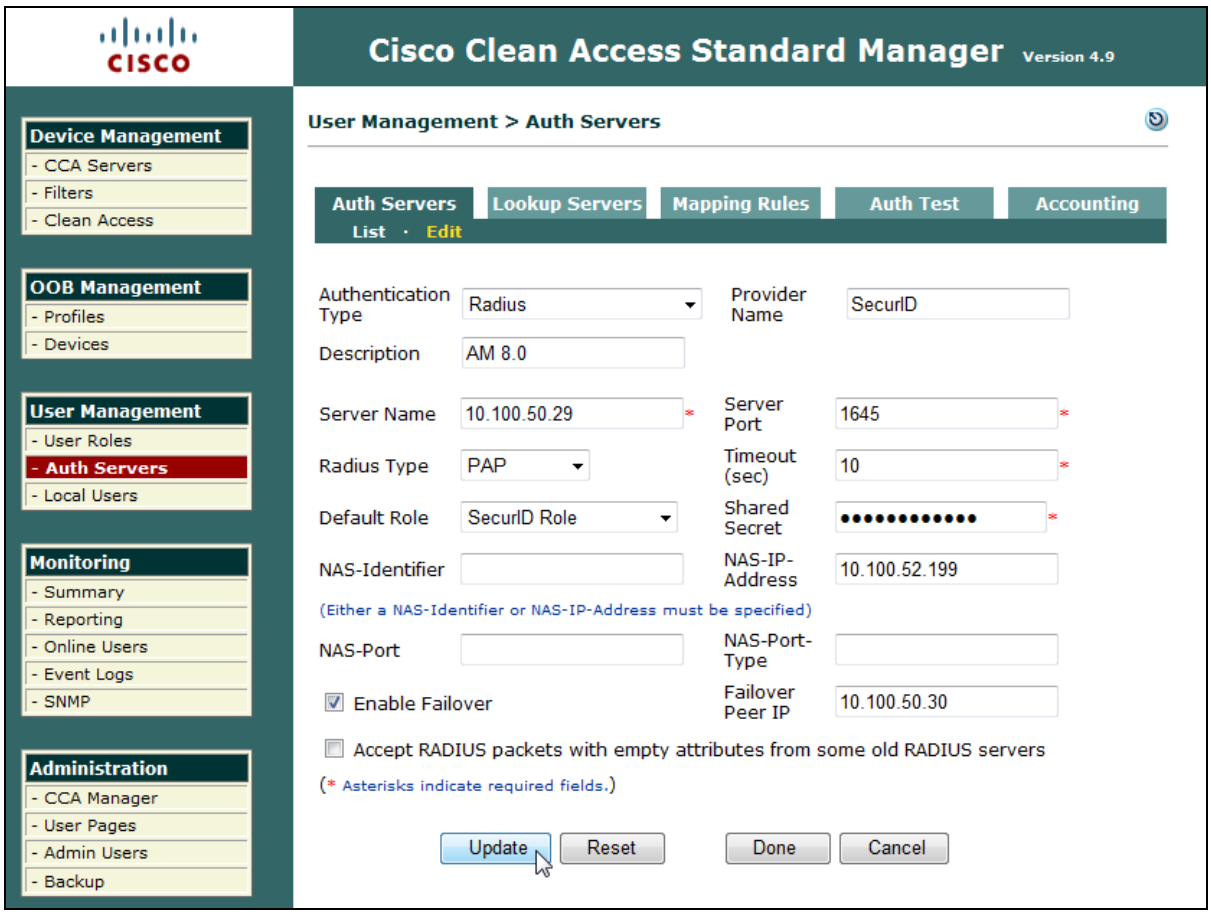
8. Click **Auth Servers** from the **User Management** menu.



9. Click **New**.



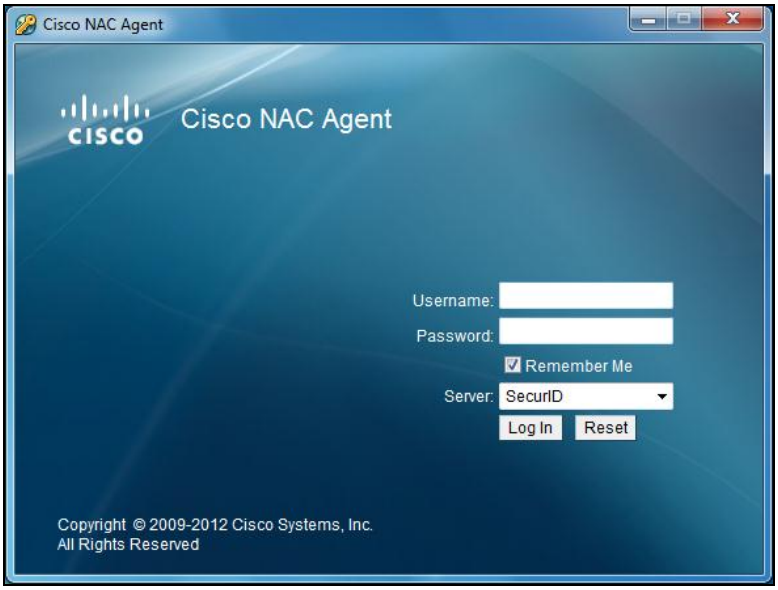
10. Configure the Auth Server and click **Add**.



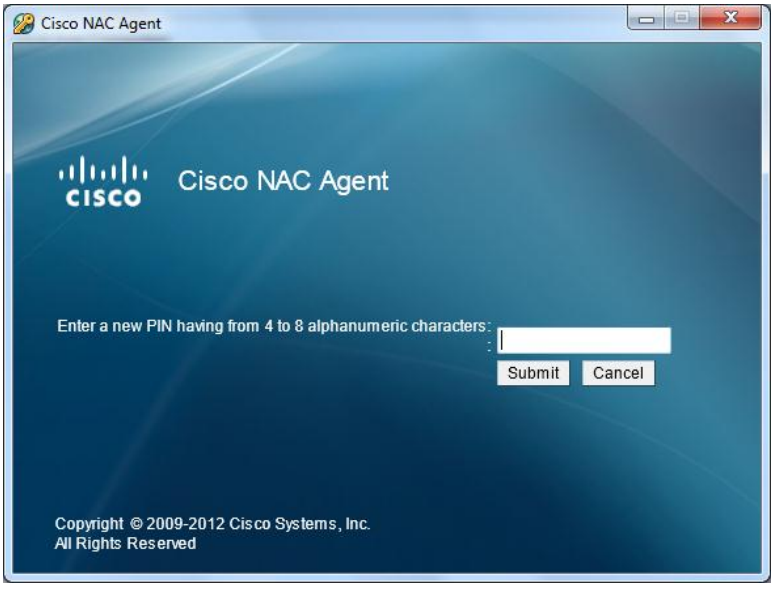
- **Authentication Type**: Select Radius from the drop-down menu.
- **Description**: Enter a description to identify the RSA Authentication Manager server(s).
- **Server Name**: Enter the hostname or IP address of the primary RSA Authentication Manager server.
- **Server Port**: Enter the port on which RADIUS will communicate. RSA defaults are both 1645 and 1812.
- **NAS-Identifier** or **NAS-IP-Address**: Configure either or both. RSA does not require this information.
- **Enable Failover (optional):** Mark the checkbox to enable failover.
- **Failover Peer IP (optional):** Enter the hostname or IP address of the RSA Authentication Manager replica.

RSA SecurID Login Screens

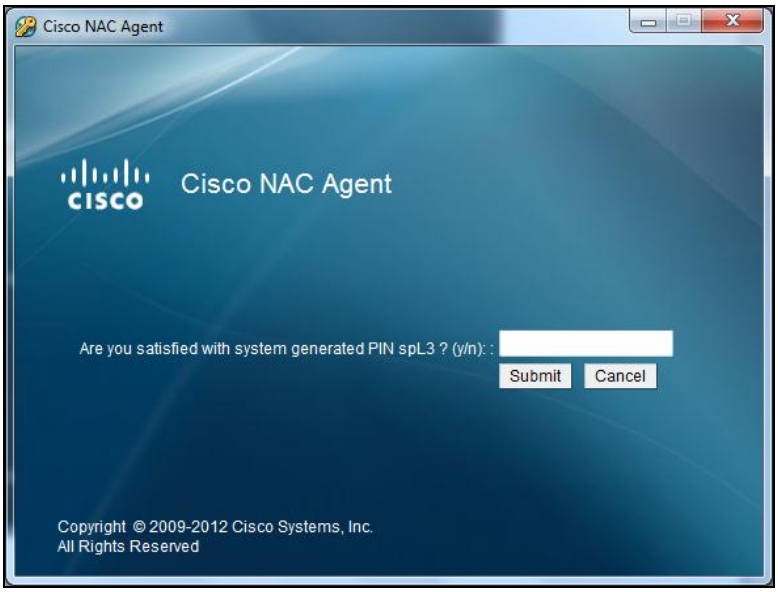
Login screen:



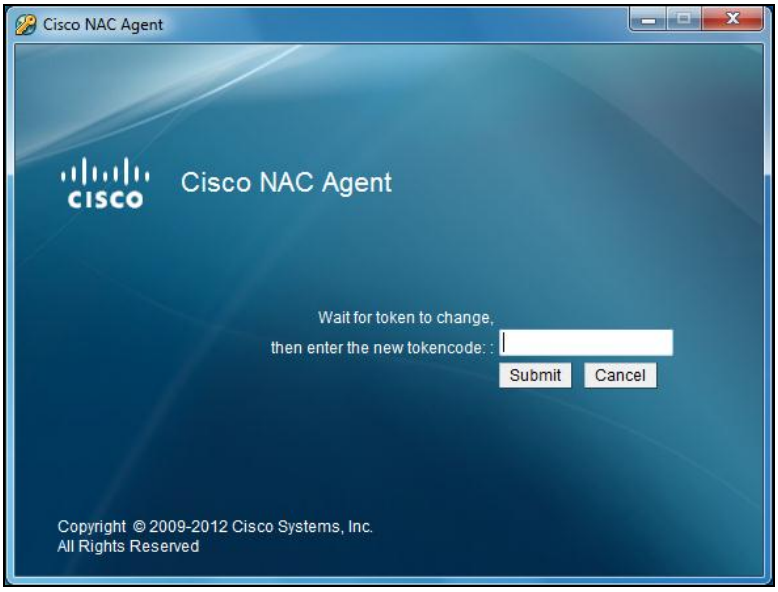
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: December 3, 2013

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Cisco Clean Access Manager	4.9.3	Virtual Appliance
Cisco Clean Access Server	4.9.3	NME Module
Cisco NAC Agent	4.9.3.5	Windows 7 Enterprise 64 bit

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 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