Cisco Systems, Inc.
Catalyst Switches

RSA SecurID Ready Implementation Guide

Last Modified: November 11, 2013

Partner Information

Product Information	
Partner Name	Cisco Systems, Inc.
Web Site	www.cisco.com
Product Name	Catalyst Switches
Version & Platform	IOS 15.0
Product Description	Cisco access switches create new user experiences and support network and application requirements. They help you scale your infrastructure for growing business needs, increase network intelligence with visibility and control, simplify operations, and improve security for users and applications.

Solution Summary

Cisco Catalyst switches integrate with RSA SecurID using RADIUS to protect console access.

RSA Authentication Manager supported features	Cisco Catalyst switch
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 Catalyst switches will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for the Cisco Catalyst switch 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 Catalyst switch 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 Catalyst switch components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configure Console Access for RSA SecurID Authentication

1. Enable AAA.

```
Switch(config)#aaa new-model
```

2. Specify the RADIUS server settings.

```
Switch(config)#radius server servername
Switch(config-radius-server)#address ipv4 radius_server_ip auth-port 1812
Switch(config-radius-server)#key radius_server_key
Switch(config-radius-server)#exit
```

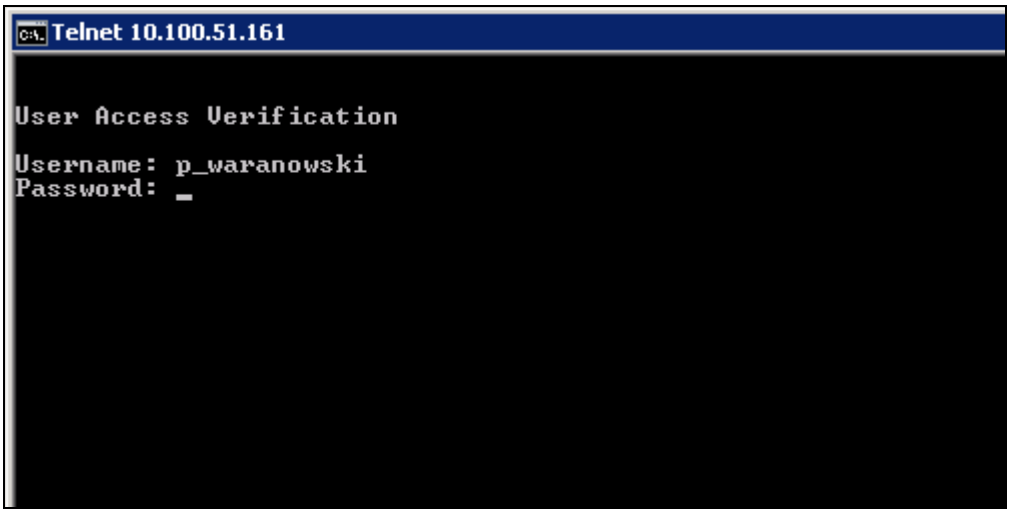
> **Note: Repeat these steps using different servernames for any replica servers in your deployment.**

3. Configure authentication.

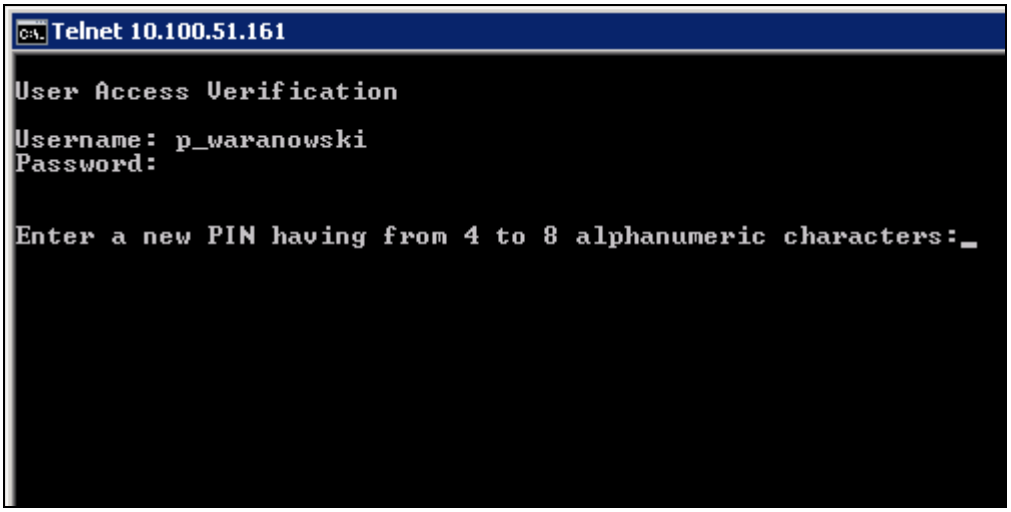
```
Switch(config)#authentication login default group radius
```

RSA SecurID Login Screens

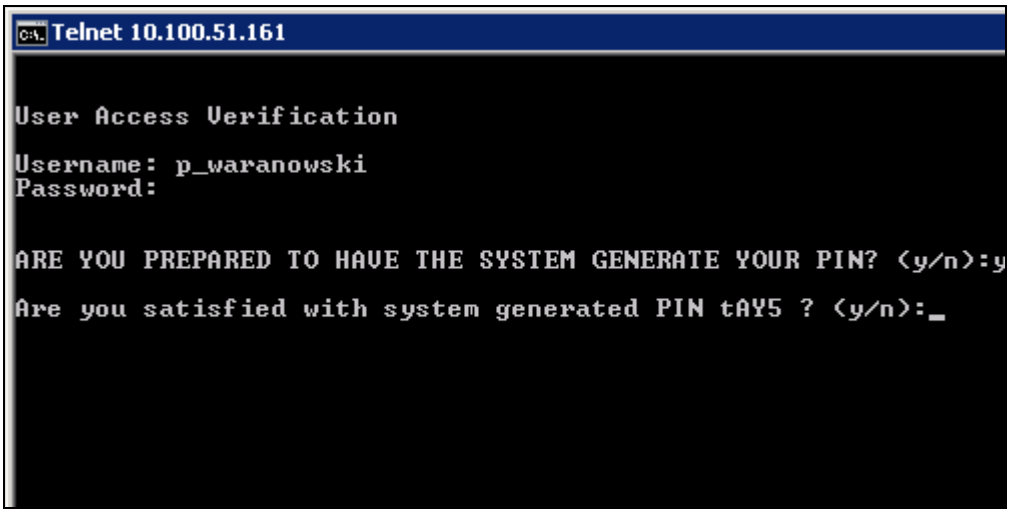
Login screen:



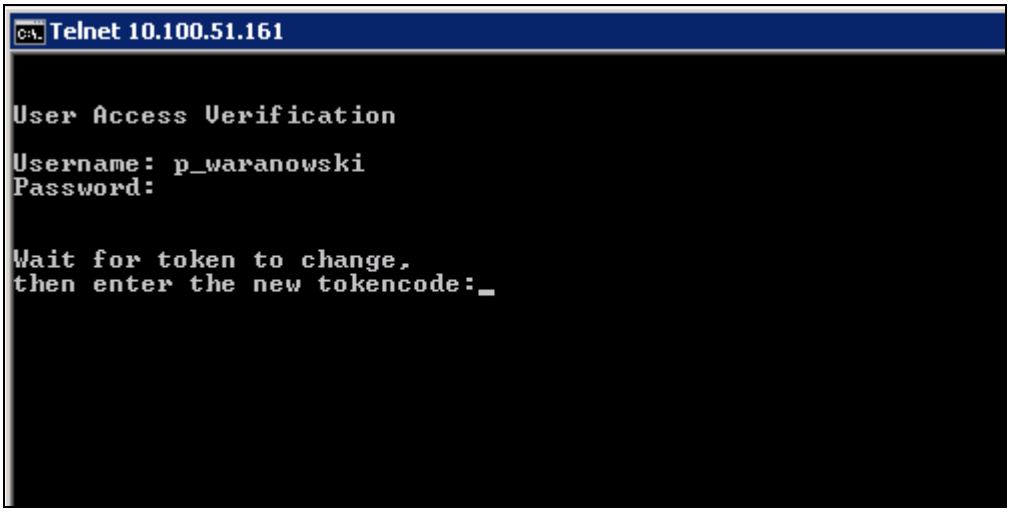
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: November 11, 2013

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Cisco Catalyst 2960	5.0(2)SE5	IOS

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