Cisco Systems, Inc.
IOS Router

RSA SecurID Ready Implementation Guide

Last Modified: January 27, 2014

Partner Information

Product Information	
Partner Name	Cisco Systems, Inc.
Web Site	www.cisco.com
Product Name	IOS Router
Version & Platform	15.4
Product Description	Cisco IOS® Software is the world's leading network infrastructure software, delivering a seamless integration of technology innovation, business-critical services, and hardware platform support. Currently operating on millions of active systems, ranging from the small home office router to the core systems of the world's largest service provider networks, Cisco IOS Software is the most widely leveraged network infrastructure software in the world.

Solution Summary

Cisco IOS AAA network security services provide the primary framework to set up access control on a router or access server. Cisco IOS integrates with RSA SecurID via RADIUS AAA server group. This document covers RSA SecurID integration with IPSec VPN and terminal access. SSL VPN gateway has partial support for SecurID.*

* See the Known Issues section of this document for more information.

RSA Authentication Manager supported features	
Cisco IOS Router 15.4	
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 IOS Router will occur.

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

Configure AAA for User Authentication and Group Authorization

Log in to a terminal on the Cisco router and enter the following commands:

```
(config)# aaa new-model
(config)# aaa authentication login userauthen group radius local
(config)# aaa authorization network groupauthor local
```

Create an entry for each of your RSA Authentication Manager servers.

```
(config)# radius server radius-server-name
(config-radius-server)# address ipv4 ip-address auth-port 1645 acct-port 1646
(config-radius-server)# timeout 120
(config-radius-server)# key yourkey
(config-radius-server)# exit
```

Configure Terminal Access for RSA SecurID Authentication

Log in to a terminal on the Cisco router and enter following commands to enable RSA SecurID authentication for terminal access.

> **Note: You must complete the steps in the Configure AAA for user authentication and group authorization.**

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

Configure IPSec VPN with RSA SecurID authentication

Log in to a terminal on the Cisco router and enter following commands to configure a remote access IPSec VPN gateway with RSA SecurID authentication.

> **Note: You must complete the steps in the Configure AAA for user authentication and group authorization.**

1. Create an ISAKMP protocol policy for phase 1 negotiation.

```
(config)# crypto isakmp policy 3
(config-isakmp)# encryption 3des
(config-isakmp)# authentication pre-share
(config-isakmp)# group 2
(config-isakmp)# exit
```

2. Create a group that will be used to specify network information to the client, along with the pre-shared key for authentication.

```
(config)# crypto isakmp client configuration group vpngroup
(config-isakmp-group)# key pre-shared key
(config-isakmp-group)# dns ip-address
(config-isakmp-group)# pool vpnpool
(config-isakmp-group)# exit
```

> **Note:** Settings configured for *vpngroup* and *pre-shared key* should match the group authentication settings configured in the Cisco VPN Client.

3. Create the phase 2 policy for data encryption.

```
(config)# crypto ipsec transform-set myset esp-3des esp-sha-hmac
(cfg-crypto-trans)# exit
```

4. Create a dynamic map and apply the transform set.

```
(config)# crypto dynamic-map dymap 10
(config-crypto-map)# set transform-set myset
(config-crypto-map)# exit
```

5. Create the crypto map and apply the AAA lists created in the previous section.

```
(config)# crypto map clientmap client authentication list userauthen
(config)# crypto map clientmap isakmp authorization list groupauthor
(config)# crypto map clientmap client configuration address respond
(config)# crypto map clientmap 10 ipsec-isakmp dynamic dymap
```

6. Apply your crypto map to the appropriate interface.

```
(config)# interface GigabitEthernet 0/0
(config-if)# crypto map clientmap
(config-if)# exit
```

> **Note: Refer to the RSA SecurID Ready Implementation guide for Cisco VPN client for instructions on configuring the Cisco VPN client for RSA SecurID. RSA Implementation guides can be found at:**
>
> **http://www.securedbyrsa.com**

Certification Checklist for RSA Authentication Manager

Terminal Access

Date Tested: January 27, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Cisco IOS Router	15.4(1)T	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

Certification Checklist for RSA Authentication Manager

Cisco VPN Client

Date Tested: January 27, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Cisco IOS Router	15.4(1)T	IOS
Cisco VPN Client	5.0.07.0440	Windows 7 Enterprise 64bit

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

Known Issues

The SSL VPN gateway component functions properly for single transaction authentications. When the RSA authentication server requires the user to be challenged (for new PIN or next Tokencode), authentication always fails.