Cisco Systems, Inc.
Nexus 7000 Series Switches

RSA SecurID Ready Implementation Guide

Last Modified: September 4, 2013

Partner Information

Product Information	
Partner Name	Cisco Systems, Inc.
Web Site	www.cisco.com
Product Name	Nexus 7000 series switches
Version & Platform	NX-OS 6.2
Product Description	Cisco Nexus 7000 Series Switches create the network foundation for your next-generation Unified Fabric data center. Modular Cisco Nexus 7000 Series Switches, including the Cisco Nexus 7000 and Cisco Nexus 7700 switches, deliver a comprehensive Cisco NX-OS feature set. They offer high-density 10, 40, and 100 Gigabit Ethernet with application-awareness and comprehensive performance analytics for the data center.

Solution Summary

Cisco Nexus switches integrate with RSA Authentication Manager via RADIUS AAA server group. Once configured, the RSA SecurID RADIUS AAA server group can be applied to many services provided by the Nexus switch, including console access, Telnet, SSH, 802.1x and more.

RSA Authentication Manager supported features	
Cisco Nexus 7000 Series Switches	
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 the Cisco Nexus 7000 Series Switch will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for the Cisco Nexus 7000 Series 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 Nexus 7000 Series 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 Nexus 7000 Series Switch components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring the Cisco Nexus Switch for RSA SecurID Authentication

RADIUS Server Configuration Process

Follow these steps to configure RADIUS servers:

Step 1 Establish the RADIUS server connections to the Cisco NX-OS device (see the “Configuring RADIUS Server Hosts” section).

Step 2 Configure the RADIUS secret keys for the RADIUS servers (see the “Configuring a Key for a Specific RADIUS Server”).

Step 3 (If needed) Configure RADIUS server groups with subsets of the RADIUS servers for AAA authentication methods (see the “Configuring RADIUS Server Groups” and the “Configuring AAA” section).

Step 4 Configure Remote AAA Services (see the “Configuring Remote AAA Services”).

Configuring RADIUS Server Hosts

To access a remote RADIUS server, configure the IP address or hostname of a RADIUS server. A maximum of 64 RADIUS servers is supported.

> **Note: By default, the RADIUS server is added to the default RADIUS server group. For information about creating RADIUS server groups, see the ("Configuring RADIUS Server Groups").**

BEFORE YOU BEGIN

- Ensure that you are in the correct VDC (or use the **switchto vdc** command).
- Ensure that the server is already configured as a member of the server group.
- Ensure that the server is configured to authenticate RADIUS traffic.
- Ensure that the Cisco NX-OS device is configured as a RADIUS client of the AAA servers.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*}
3. **show radius-server**
4. **show radius {pending | pending-diff}**
5. **radius commit**
6. **exit**
7. **copy running-config startup-config**

DETAILED STEPS

Command	Purpose
Step 1 configure terminal **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2 switch(config)# **radius distribute** **Example:** switch(config)# radius distribute	Enable RADIUS configuration distribution. The default is disabled.
Step 3 exit **Example:** switch(config)# exit switch#	Exits configuration mode.
Step 4 show radius status **Example:** switch(config)# show radius status	(Optional) Displays the RADIUS CFS distribution configuration.
Step 5 copy running-config startup-config **Example:** switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring a Key for a Specific RADIUS Server

You can configure a key on the Cisco NX-OS device for a specific RADIUS server. A RADIUS key is a secret text string shared between the Cisco NX-OS device and a specific RADIUS server.

BEFORE YOU BEGIN

- Ensure that you are in the correct VDC (or use the **switchto vdc** command).
- Configure one or more RADIUS server hosts (see the "Configuring RADIUS Server Hosts").
- Obtain the key value for the remote RADIUS server.
- Configure the key on the RADIUS server.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} key [0 | 7] *key-value*
3. **exit**
4. **show radius-server**
5. **copy running-config startup-config**

DETAILED STEPS

Command	Purpose
Step 1 configure terminal **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2 radius-server host {ipv4-address | ipv6-address | host-name} **key** [**0** | **7**] key-value **Example:** switch(config)# radius-server host 10.10.1.1 key 0 PlljUhYg	Specifies a RADIUS key for a specific RADIUS server. You can specify that the *key-value* is in clear text (**0**) format or is encrypted (**7**). The Cisco NX-OS software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters. This RADIUS key is used instead of the global RADIUS key.
Step 3 exit **Example:** switch(config)# exit switch#	Exits configuration mode.
Step 4 show radius-server **Example:** switch# show radius-server	(Optional) Displays the RADIUS server configuration. **Note** The RADIUS keys are saved in encrypted form in the running configuration. Use the **show running-config** command to display the encrypted RADIUS keys.
Step 5 copy running-config startup-config **Example:** switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring RADIUS Server Groups

You can specify one or more remote AAA servers for authentication using server groups. All members of a group must belong to the RADIUS protocol. The servers are tried in the same order in which they are configured A maximum of 100 server groups per VDC is supported..

Note: CFS does not distribute RADIUS server group configurations.

BEFORE YOU BEGIN

- Ensure that you are in the correct VDC (or use the **switchto vdc** command).
- Ensure that all servers in the group are RADIUS servers.

SUMMARY STEPS

1. **configure terminal**
2. **aaa group server radius** *group-name*
3. **server** {*ipv4-address* | *ipv6-address* | *host-name*}
4. **deadtime** *minutes*
5. **source-interface** *interface*
6. **use**-vrf *vrf-name*
7. **exit**
8. **show radius-server groups** [*group-name*]
9. **copy running-config startup-config**

DETAILED STEPS

Command	Purpose
Step 1 configure terminal **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2 aaa group server radius group-name	Creates a RADIUS server group and enters the RADIUS server group configuration sub mode for that group. The *group-name* argument is a case-sensitive alphanumeric string with a maximum length of 127 characters.
Step 3 server {ipv4-address | ipv6-address | host-name} **Example:** switch(config-radius)# server 10.10.1.1	Configures the RADIUS server as a member of the RADIUS server group. **Tip** If the specified RADIUS server is not found, configure it using the **radius-server host** command and retry this command.

Step 4 deadtime minutes **Example:** switch(config-radius)# deadtime 30	(Optional) Configures the monitoring dead time. The default is 0 minutes. The range is from 1 through 1440. **Note** If the dead-time interval for a RADIUS server group is greater than zero (0), that value takes precedence over the global dead-time value
Step 5 source-interface interface **Example:** switch(config-radius)# source-interface mgmt 0	(Optional) Configures a source interface to access the RADIUS servers in the server group. You can use Ethernet interfaces, loopback interfaces, or the management interface (mgmt 0). The default is the global source interface.
Step 6 use-vrf vrf-name **Example:** switch(config-radius)# use-vrf vrf1	(Optional) Specifies the VRF to use to contact the servers in the server group.
Step 7 exit **Example:** switch(config-radius)# exit switch(config)#	Exits configuration mode.
Step 8 show radius-server groups [group-name] **Example:** switch(config)# show radius-server group	(Optional) Displays the RADIUS server group configuration.

Remote AAA Services

Remote AAA services provided through RADIUS and TACACS+ protocols have the following advantages over local AAA services:

- It is easier to manage user password lists for each Cisco NX-OS device in the fabric.
- AAA servers are already deployed widely across enterprises and can be easily used for AAA services.
- You can centrally manage the accounting log for all Cisco NX-OS devices in the fabric.
- It is easier to manage user attributes for each Cisco NX-OS device in the fabric than using the local databases on the Cisco NX-OS devices.

AAA Server Groups

You can specify remote AAA servers for authentication, authorization, and accounting using server groups.

A server group is a set of remote AAA servers that implement the same AAA protocol. The purpose of a server group is to provide for fail-over servers in case a remote AAA server fails to respond. If the first remote server in the group fails to respond, the next remote server in the group is tried until one of the servers sends a response. If all the AAA servers in the server group fail to respond, then that server group option is considered a failure. If required, you can specify multiple server groups. If the Cisco NX-OS device encounters errors from the servers in the first group, it tries the servers in the next server group.

AAA Service Configuration Options

AAA configuration in Cisco NX-OS devices is service based, which means that you can have separate AAA configurations for the following services:

- User Telnet or Secure Shell (SSH) login authentication
- Console login authentication
- Cisco TrustSec authentication
- 802.1X authentication
- Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP)
- Authentication for Network Admission Control (NAC)
- User management session accounting
- 802.1X accounting

You can specify the following authentication methods for the AAA services:

- RADIUS server groups—Uses the global pool of RADIUS servers for authentication.
- Specified server groups—Uses specified RADIUS or TACACS+ server groups for authentication.
- Local — Uses the local username or password database for authentication.
- None — Uses only the username

Configuring Console Login Authentication Methods

This section describes how to configure the authentication methods for the console login. The authentication methods include the following:

- Global pool of RADIUS servers
- Named subset of RADIUS or TACACS+ servers
- Local database on the Cisco NX-OS device
- Username only (**none**)
- The default method is local.

> **Note: The configuration and operation of the AAA for the console login apply only to the default VDC**

BEFORE YOU BEGIN

- Ensure that you are in the default VDC.
- Configure RADIUS or TACACS+ server groups as needed.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication login console** {group *group-list* [none] | local | none}
3. **exit**
4. **show aaa authentication**
5. **copy running-config start-config**

DETAILED STEPS

Command	Purpose
Step 1 configure terminal **Example:** switch# configure terminal switch(config)#	Enters configuration mode.
Step 2 aaa authentication login console {**group** group-list [**none**]| **local**	**none**} **Example:** switch(config)# aaa authentication login console group radius	Configures login authentication methods for the console. The *group-list* argument consists of a space-delimited list of group names. The group names are the following: • **radius**—Uses the global pool of RADIUS servers for authentication. • *named-group*—Uses a named subset of TACACS+ or RADIUS servers for authentication. The **local** method uses the local database for authentication. The **none** method uses the username only. The default console login method is **local**, which is used when no methods are configured or when all the configured methods fail to respond.
Step 3 exit **Example:** switch(config)# exit switch#	Exits configuration mode.

Configuring Default Login Authentication Methods

The authentication methods include the following:

- Global pool of RADIUS servers
- Named subset of RADIUS or TACACS+ servers
- Local database on the Cisco NX-OS device (Default)
- Username only

BEFORE YOU BEGIN

- Ensure that you are in the correct VDC (or use the **switchto vdc** command).
- Configure RADIUS or TACACS+ server groups, as needed.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication login default** {group *group-list* [none] | local | none}
3. **exit**
4. **show aaa authentication**
5. **copy running-config start-config**

Command	Purpose
configure terminal **Example:** switch# configure terminal switch(config)#	Enters configuration mode.
Step 2 aaa authentication login default {**group** group-list [**none**]| **local** | **none**} **Example:** switch(config)# aaa authentication login default group radius	Configures the default authentication methods. The *group-list* argument consists of a space-delimited list of group names. The group names are the following: • **radius**—Uses the global pool of RADIUS servers for authentication. • *named-group*—Uses a named subset of TACACS+ or RADIUS servers for authentication. The **local** method uses the local database for authentication. The **none** method uses the username only. The default login method is **local**, which is used when no methods are configured or when all the configured methods fail to respond.
Step 3 exit **Example:** switch(config)# exit switch#	Exits configuration mode
Step 4 show aaa authentication **Example:** switch# show aaa authentication	(Optional) Displays the configuration of the console login authentication methods.
Step 5 copy running-config startup-config **Example:** switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Certification Checklist for RSA Authentication Manager

Date Tested: August 31, 2013

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Cisco ACS	5.4	Virtual Appliance
Cisco Nexus 7000 Series Switches	6.2.2.S42	NX-OS

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 / PAR

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