



RSA SecurID Ready Implementation Guide

Last Modified: September 30, 2005

Partner Information

Product Information	
Partner Name	Juniper Networks
Web Site	www.juniper.net
Product Name	Juniper Networks NetScreen-5GT Wireless
Version & Platform	5.0.0.R10.p
Product Description	The NetScreen-5GT Wireless brings enterprise level security applications, routing protocols and resiliency features to remote offices, retail outlets or broadband telecommuters that want to deploy 802.11b/g networks in a secure manner. The NetScreen-5GT Wireless offers administrators up to four configurable Wireless Security Zones each with a unique SSID that can be used to provision appropriate levels of security for different types of users. To help ensure wireless security, privacy and interoperability, the NetScreen-5GT Wireless supports a broad set of wireless authentication and privacy mechanisms. The NetScreen-5GT Wireless includes standard Ethernet connectivity with ADSL as a hardware option.
Product Category	Wireless Communications



Solution Summary

The Juniper Networks NetScreen-5GT Wireless has support for a broad set of wireless authentication including RSA SecurID authentication and privacy mechanisms to help ensure wireless security, privacy and interoperability (NetScreen-5GT Wireless appliance only)The Juniper Networks NetScreen 5GT Wireless solution can authenticate using RSA SecurID authentication via RADIUS and PEAP.

Partner Integration Overview	
Authentication Methods Supported	RADIUS
List Library Version Used	N/A
RSA Authentication Manager Name Locking	N/A
RSA Authentication Manager Replica Support	N/A
Secondary RADIUS Server Support	Yes
Location of Node Secret on Agent	'None stored'
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	All Users
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	No
Use of Cached Domain Credentials	No

Product Requirements

Partner Product Requirements: Juniper Networks NetScreen-5GT Wireless	
Firmware Version	5.0.0.R10.p

Additional Software Requirements:	
Application	Additional Patches
Funk Odyssey Client	4.02

Agent Host Configuration

To facilitate communication between the Juniper Networks NetScreen-5GT Wireless and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager local database and RADIUS Server Database. The Agent Host record identifies the Juniper Networks NetScreen-5GT Wireless within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces
- RADIUS Secret

When adding the Agent Host Record, you should configure the Juniper Networks NetScreen-5GT Wireless as Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with the Juniper Networks NetScreen-5GT Wireless will occur.

 **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 Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

Partner Authentication Agent Configuration

Before You Begin

This section provides instructions for integrating the partners' product with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

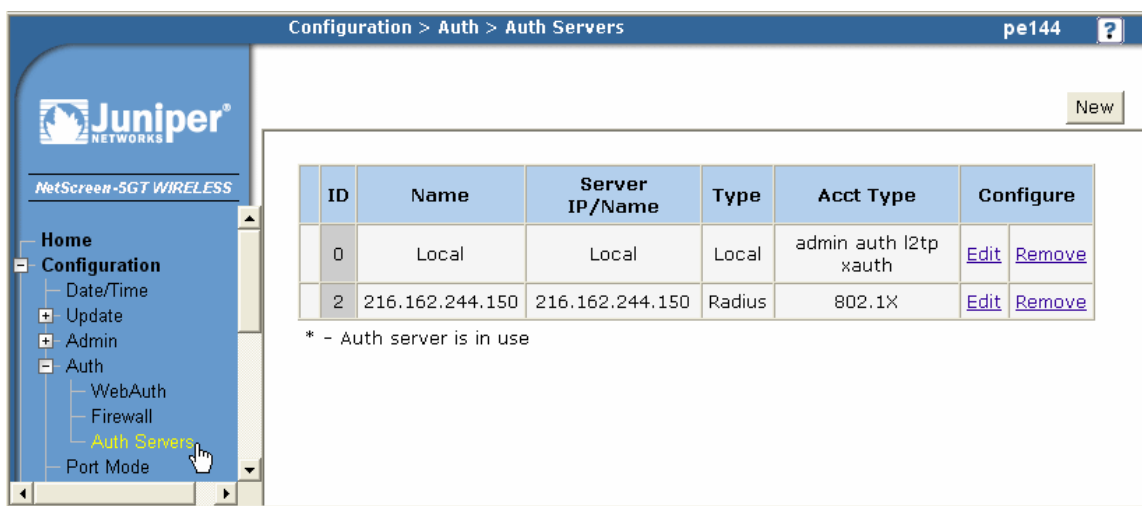
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Documenting the Solution

Juniper Netscreen OS configuration

1. Connect to the Juniper NetScreen wireless device and select Configuration > Auth > Auth Servers.



2. Click **New**.

Name

IP/Domain Name

Backup1

Backup2

Timeout (0 to disable)

Account Type Auth L2TP Admin XAuth 802.1X

RADIUS

Radius port Retry Timeout Sec

Shared Secret

3. Enter the appropriate information for your RADIUS Server.
 - **Name:** Select a descriptive name for the RADIUS server definition.
 - **IP/Domain Name:** IP address or Hostname of the RSA Authentication Manager Radius Server
 - **Account Type :** Select 802.1X
4. Select the RADIUS radio Button
 - **Radius Port:** Type the port number for the RSA Authentication Manager Radius Server. The default is 1812
 - **Shared Secret:** Enter the RADIUS Secret that must match the RADIUS secret entered in the RSA Authentication Manager Radius Server client definition created under the Agent Host Configuration section above in this guide
5. Click **OK**.
6. Select from the side menu Wireless > SSID.

Wireless > SSID Objects (List) pe144 ?

Name	Suppression	Client Isolation	Authentication	Cipher	Interface	Configure
PE	disabled	disabled	WPA	tkip	wireless1	Edit WEP Keys Remove

Note: the wireless configuration changes must be activated to take effect. To activate, press the "Activate Changes" found at the Wireless > Activate Changes section of the webui.

7. Click **New**

8. Fill in the form

- Enter a name for your SSID
- Select the WPA radios button
- Encryption Type: select one of the three options. In this configuration TKIP was used.

SSID

WPA Based Authentication Methods

WPA Pre-shared Key HEX Key (64 hexadecimal)
Confirm Hex Key
 Key by Password (8~63 characters)
Confirm Key by Password
Rekey Interval 30~4294967295, 0: disable
Encryption Type Auto TKIP AES
Rekey Interval 30~4294967295, 0: disable
Encryption Type Auto TKIP AES

WPA

Wireless Interface Binding

Disable SSID Broadcast

SSID Client Isolation

9. Click OK.

10. From the side menu select **Wireless > Activate Changes** and then Click the **Activate Changes** button.

Wireless > Activate Changes pe144

Juniper NETWORKS

NetScreen-5GT WIRELESS

Home

Configuration

Wireless

- General Settings
- MAC Access List
- SSID
- Statistics
- Activate Changes

Network

Screening

Policy

For the wireless configuration, you must save, and then activate the changes before the configuration is updated. Saving changes and reactivating the wireless interfaces, causes a short interruption in the wireless transmission.

Click the **Activate Changes** button to activate the wireless configuration changes.

Certification Checklist

Date Tested: September 9, 2005

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1	Windows 2003
Juniper	5.0.0r10	
Funk Odyssey Client	4.02	Windows XPSP2

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)	✓
User Selectable	N/A	User Selectable	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
PASSCODE			
16 Digit PASSCODE	N/A	16 Digit PASSCODE	✓
4 Digit Password	N/A	4 Digit Password	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
Name Locking Enabled	N/A	Name Locking Enabled	
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓
Additional Functionality			
RSA Software Token API Functionality			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
Domain Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	
Set Domain Credential	N/A	Set Domain Credential	
Retrieve Domain Credential	N/A	Retrieve Domain Credential	

SWA

✓ = Pass ✗ = Fail N/A = Non-Available Function