Radio IP
Radio IP MTG

RSA SecurID Ready Implementation Guide

Last modified: May, 17, 2010

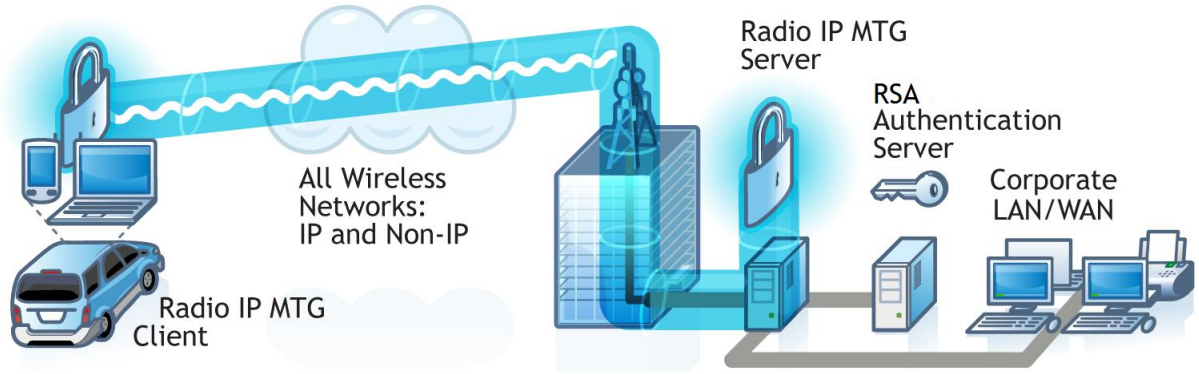
Partner Information

Product Information	
Partner Name	Radio IP
Web Site	www.radio-ip.com
Product Name	Radio IP MTG
Version & Platform	2.5 SP3
Product Description	Radio IP MTG™ is a software solution that extends a corporate LAN to a wireless network on most private or public systems. Radio IP MTG uses virtual network interface cards which link mobile applications to LAN servers. In effect, Radio IP MTG is a router or gateway that does not hook directly to your corporate LAN. Instead, it creates a separate virtual network segment in your IP address range for use by Radio IP MTG Server and mobiles running Radio IP MTG Client.
Product Category	VPNs IPsec

Solution Summary

Radio IP MTG™ possesses an extensive toolkit designed to enforce secure wireless mobile access to corporate LANs. To meet the challenge raised by corporations committed to the highest levels of confidentiality, Radio IP has integrated RSA SecurID authentication on its MTG mobile VPN solution based on a server/client platform.

Partner Integration Overview	
Authentication Methods Supported	RADIUS
RSA SecurID API Version	N/A
RSA Authentication Manager Replica Support	N/A
Secondary RADIUS Server Support	Yes (unlimited through Local Radius Proxy)
RSA Authentication Agent Host Type for 7.1	Standard Agent
RSA SecurID User Specification	All Users
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	No



The above drawing illustrates the end-to-end secure data tunnel using Radio IP MTG. The RSA Authentication Manager server uses the Radius protocol to authenticate user and token information received from the MTG Server. In turn, MTG Server interacts with a fleet of mobile clients running MTG Client which boast built-in security measures designed to ensure registration persistence from one work session to the next (in the form one-time certificate exchange and so on). RSA's two-factor authentication intervenes whenever MTG Client first connects or whenever the MTG session needs to be re-synchronized pursuant to such events as prolonged out-of-coverage conditions or user-triggered connection reset.

Product Requirements

Radio IP MTG Server Requirements:

Partner Product Requirements: Radio IP MTG Server	
Version	2.5 SP3
CPU	1.9 GHz
Memory	512 MB RAM
Hard Disk Space	200 MB free disk space

Operating System	
Platform	**Required Patches**
Windows 2003 Server	SP2
Windows 2008 Server R2	

Radio IP MTG Client Requirements – Windows Client:

Partner Product Requirements: Radio IP MTG Client	
Version	2.5 SP3
CPU	1.7 GHz
Memory	512 MB RAM
Hard Disk Space	50 MB free disk space

Operating System	
Platform	**Required Patches**
Windows XP	SP2 or later
Windows Vista	SP1 or later
Windows 7	

Radio IP MTG Client Requirements – Windows Mobile Client:

Partner Product Requirements: Radio IP MTG Client	
Version	2.5 SP3
CPU	624 MHz
Memory	64 MB RAM
Hard Disk Space	12 MB free disk space

Operating System	
Platform	**Required Patches**
Windows 5.X	
Windows 6.X	

Additional Software Requirements:

Additional Software Requirements	
Platform	**Additional Patches**
Windows 5.X	.Net Framework update

Authentication Agent Configuration

> **Important: All "Authentication Agent" types for 7.1 should be set to "Standard Agent".**

To facilitate communication between the Radio IP MTG and the RSA Authentication Manager / RSA SecurID Appliance, an Authentication Agent record must be added to the RSA Authentication Manager database. The Authentication Agent record identifies the Radio IP MTG within the RSA Authentication Manager database and contains information about communication and encryption. You will also need to configure a RADIUS client.

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

- Hostname
- IP Addresses for all network interfaces

When adding the Agent Host Record, you should configure the Radio IP MTG as a Standard Agent. This setting is used by the RSA Authentication Manager to determine how communication with the Radio IP MTG will occur.

To create the RADIUS client record, you will need the following information.

- Hostname
- IP Addresses for all 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 Security documentation for additional information about Creating, Modifying and Managing Agent Host, and RADIUS client records.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	'None stored'
Node Secret	'None stored'
sdstatus.12	'None stored'
sdopts.rec	"Not implemented'

Partner Product 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.

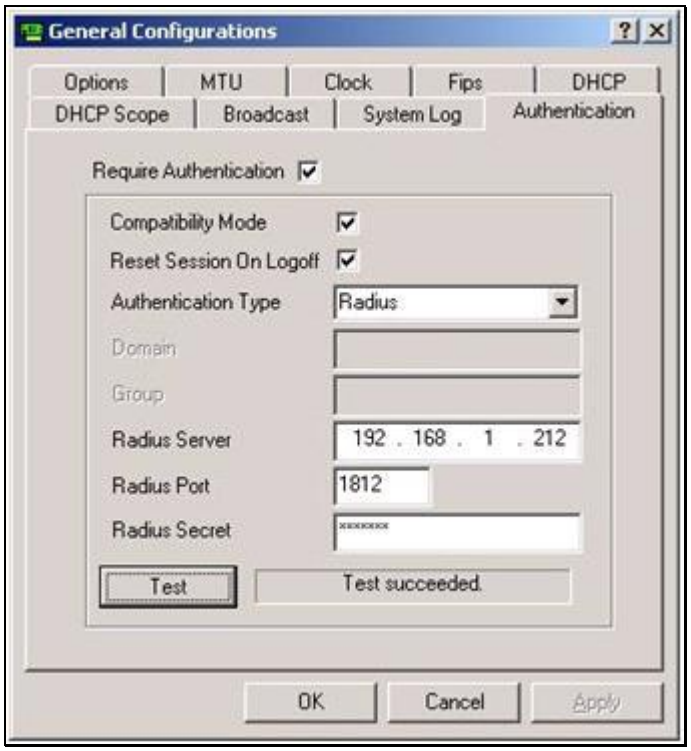
Enable RSA SecurID Authentication in Radio IP MTG Server

Complete the following steps to enable RSA SecurID Authentication in Radio IP MTG Server.

> **Note: Support of the Radius authentication protocol is optional to Radio IP MTG. This component is subject to license extension.**

1. Click the MTG Server system tray icon in advanced mode, and select **General Configuration**.

2. Open the **Authentication** tab in the General Configuration window. Check **Require Authentication** option. Select **Radius** from the **Authentication Type** drop-down menu. Enter the IP address, authentication port and secret for the RADIUS client and click **OK**.



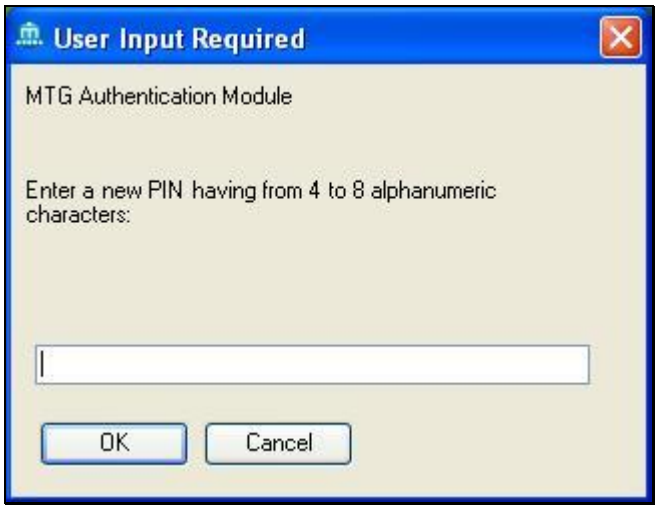
Radio IP MTG Server is now configured for RSA SecurID authentication. All subsequent Radio IP Client authentications will be performed by RSA Authentication Manager.

Note: Radio IP MTG clients with existing registrations in Radio IP MTG Server must Reset Connection to authenticate using updated authentication configuration.

Logon Screenshots

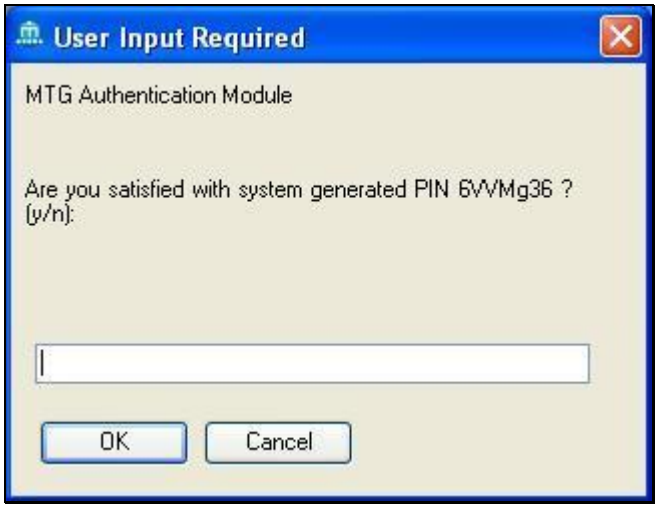
Logon:

User-defined New PIN:



Next Tokencode mode:

System generated PIN:



Certification Checklist for RSA Authentication Manager

Date Tested: 04/21/2010

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1 sp2	Windows Server 2003
Radio IP MTG Server	2.5 sp3 (Rel. 2060)	Windows Server 2003
Radio IP MTG Client	2.5 sp3 (Rel. 2060)	Windows XP SP3

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 Numeric PIN	N/A	Deny Numeric PIN	✓
PIN Reuse	N/A	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	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓

Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

PEW/PAR

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