SmithMicro Software Inc
QuickLink Mobility

RSA SecurID Ready Implementation Guide

Last Modified: May 4, 2011

Partner Information

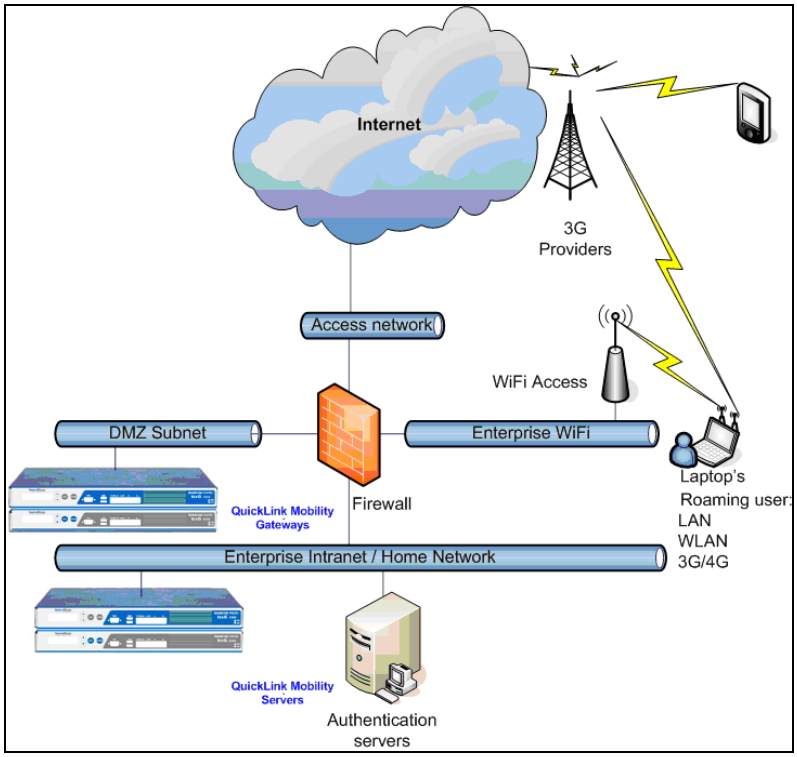
Product Information	
Partner Name	SmithMicro Software Inc
Web Site	www.smithmicro.com
Product Name	QuickLink Mobility (QMBG and QMBS)
Version & Platform	QMBG 7.0.2 (or above) server and QMBS client version 7.0.1 (or above)
Product Description	SmithMicro's QuickLink Mobility is an out-of-the-box, unified client-server solution providing IT departments a carrier and device agnostic solution that unifies the management of mobile workers, mobile devices and mobile expenses. QuickLink Mobility is the first solution to combine enterprise-grade broadband data network connection management features with military-grade security, seamless network roaming and session persistence. This centrally-managed unified mobility solution simplifies the end-user remote access experience while providing a new level of control to enterprise IT organizations.
Product Category	Remote Access

SMITH MICRO SOFTWARE

Solution Summary

RSA SecurID supported features QuickLink Mobility	
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
On-Demand Authentication via API	No
RSA Authentication Manager Replica Support	No
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	Yes

SmithMicro's QuickLink Mobility can be configured to enable RSA SecurID tokens to authenticate users in remote locations.



Authentication Agent Configuration

Agent Host Records contain information that allows an RSA Authentication Manager server to locate its clients and establish secure communication channels with them. The server's database must contain an Agent Host Record to identify each QuickLink Mobility host in a given environment. In order to create this record, the following information is required for each instance of QuickLink Mobility:

- A hostname
- An IP Address for each network interface
- A RADIUS Secret

> **Note: QuickLink Mobility Agent hostnames must resolve to valid IP addresses on the local network.**

When adding the Agent Host Record, the Authentication Agent Type should be set to "Standard Agent". This setting is used by the RSA Authentication Manager server to determine how it will communicate with QuickLink Mobility.

Please refer to the appropriate RSA Security documentation for additional information about creating, modifying and managing Agent Host records.

Before You Begin

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

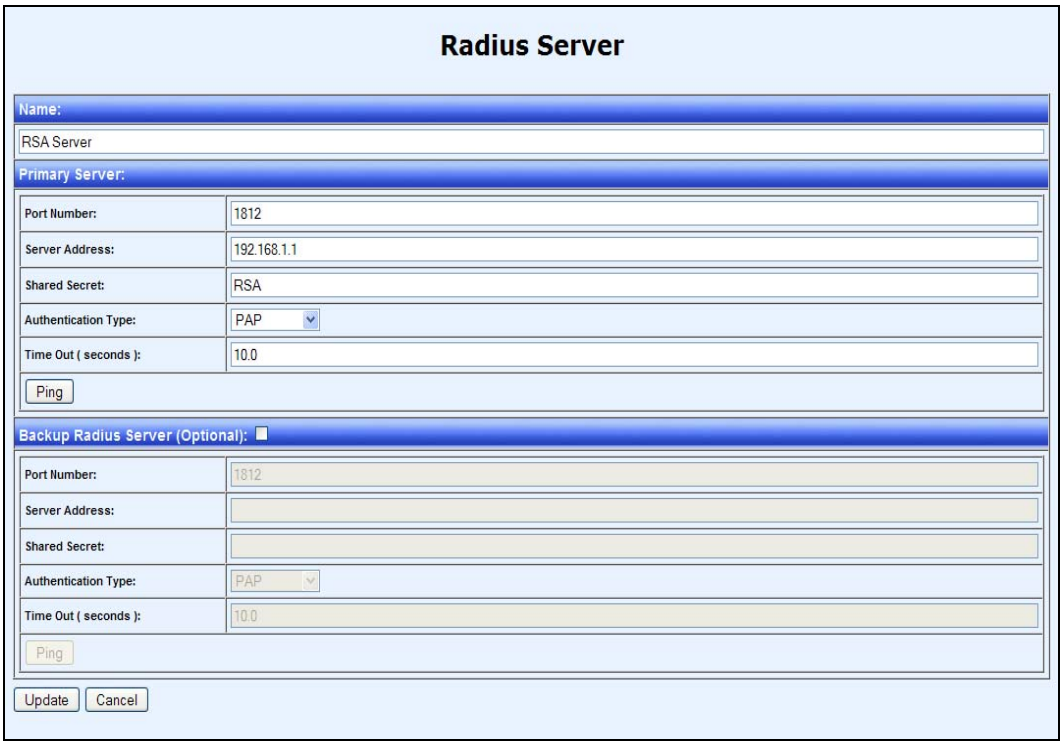
It is assumed that the reader has both working knowledge of the relevant applications, as well as the ability to perform the tasks outlined in this section. Administrators should have access to any documentation required to install and manage the RSA and SmithMicro components.

All products/components should be installed and working prior to implementing the integration detailed below. Perform the necessary tests to confirm that this is true before proceeding.

Configuring QuickLink Mobility Manager

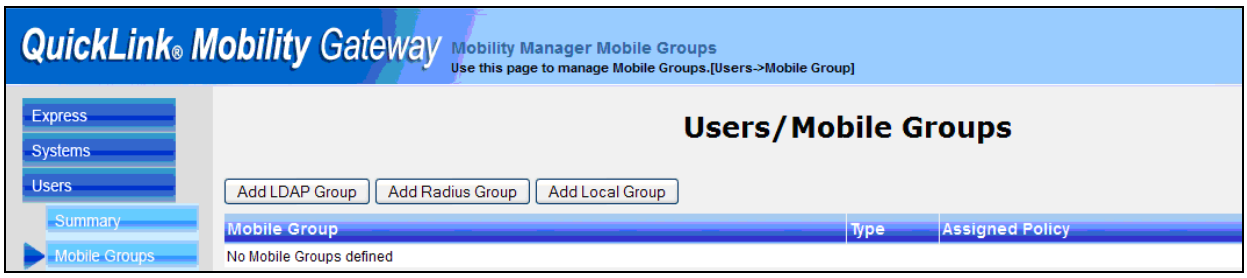
Follow the steps below to create and manage a connection to an RSA RADIUS server:

1. Log in to the QuickLink Mobility Gateway Manager as the *admin* user. (See the QMBG Admin Guide for more information) and navigate to **Users->Radius Servers**.
2. Click the on the **New Radius Server** button to create an RSA server configuration and enter the following information:
   - a logical server name for the RADIUS server in the **Name** field
   - the server's port number in the **Port Number** field
   - the server's IP Address in the **Server Address** field
   - the RADIUS Server shared secret in the **Shared Secret** field
   - an authentication type from the **Authentication Type** dropdown list
3. If you have installed two RADIUS servers, repeat Step 2 once more.



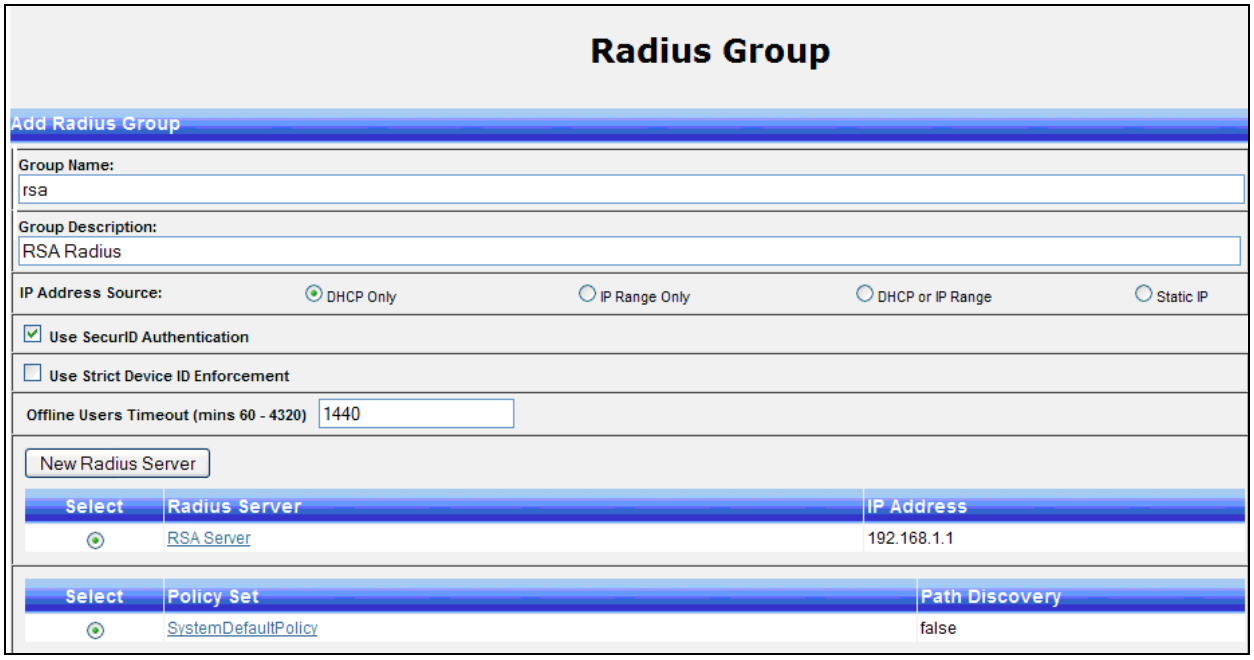
4. Click the **Update** button.

5. Navigate to **Users->Mobile Groups** and click the **Add RADIUS Group** button.



6. Follow the steps below to create a RADIUS group:

- enter a logical name for the RADIUS group in the **Group Name** field
- (optional) enter a description of the group in the **Group Description** field
- check the **Use SecurID Authentication** checkbox
- select the radio button that corresponds to the **RADIUS server you created above**
- select the radio button that corresponds to the security policy you wish to use

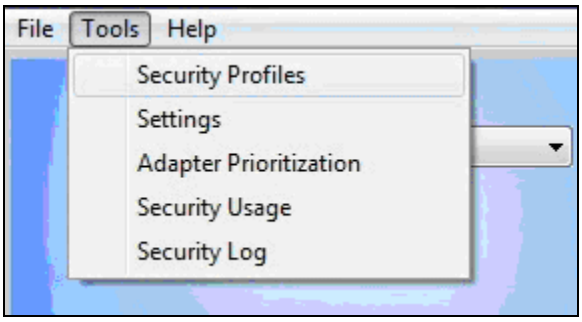


7. Click the **Save** button and the **Apply Config** button to save this configuration.

Configuring QuickLink Client

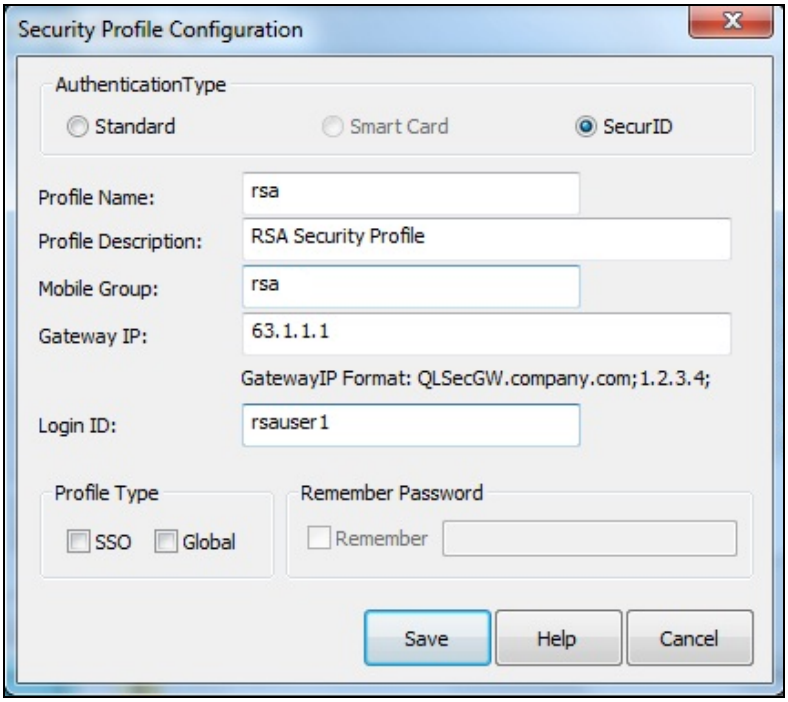
Follow the steps below to configure the QuickLink Client to authenticate against the RSA RADIUS server:

1. Open the QuickLink Client and navigate to **Tools->Security Profiles.**



2. Follow the steps below to complete the integration:

   - click the **SecurID** radio button
   - enter a logical name for the profile in the **Profile Name** field
   - (optional) enter a description of the profile in the **Profile Description** field
   - enter the group name created above in the **Mobile Group** field
   - enter the gateway IP address in the **Gateway IP** field



3. Click the **Save** button.

Certification Checklist for RSA Authentication Manager 7.1

Date Tested: January 28th, 2011

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1 SP2	Microsoft Windows Server 2003
QuickLink Mobility Manager	QMBG 7.0.2	Microsoft Windows Server 2003
QuickLink Mobility Manager	QMBS 7.0.1	Microsoft Windows Server 2003

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	✓
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	N/A
On-Demand New PIN	N/A	On-Demand New PIN	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓

JGS

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