Citrix Systems, Inc.
GoToMyPC Corporate

RSA SecurID Ready Implementation Guide

Last Modified: March 19th, 2015

Partner Information

Product Information	
Partner Name	Citrix Systems, Inc.
Web Site	www.gotomypc.com
Product Name	GoToMyPC Corporate Edition
Version & Platform	8.3
Product Description	GoToMyPC is for individuals needing remote desktop access to 1-20 computers. It's an easy and secure remote-access solution that enables you to conveniently access email, files, programs and network resources from home or the road. Get unlimited access to your computers from any Web browser anywhere.

GoToMyPC

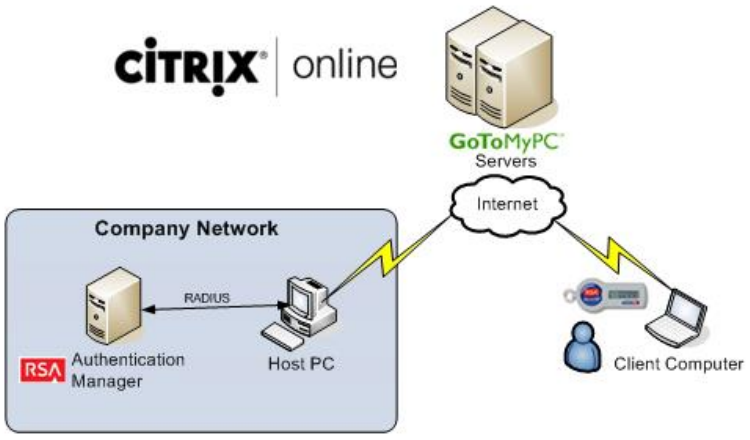
Solution Summary

If you are a GoToMyPC Corporate user, your administrator may configure your GoToMyPC Corporate account to integrate with RSA SecurID via RADIUS.

RSA SecurID is a two-factor authentication method based on something you know (a password or PIN) and something you have (an authenticator), providing a more robust level of user authentication.

Use of RSA SecurID will prompt you to enter your credentials (PIN and tokencode) after your access code each time you access the host PC.

RSA Authentication Manager supported features	
Citrix GoToMyPC Corporate	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	No
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
RSA SecurID Authentication via IPv6	No
On-Demand Authentication via Native SecurID UDP Protocol	No
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	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



Agent Host Configuration

To facilitate communication between GoToMyPC and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies GoToMyPC and contains information about communication and encryption.

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 <Partner Product> will occur.

Since the GoToMyPC will be communicating with RSA Authentication Manager via RADIUS, then a RADIUS client that corresponds to the agent host record must be created in the 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: The RADIUS client's hostname must resolve to the IP address specified.**

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

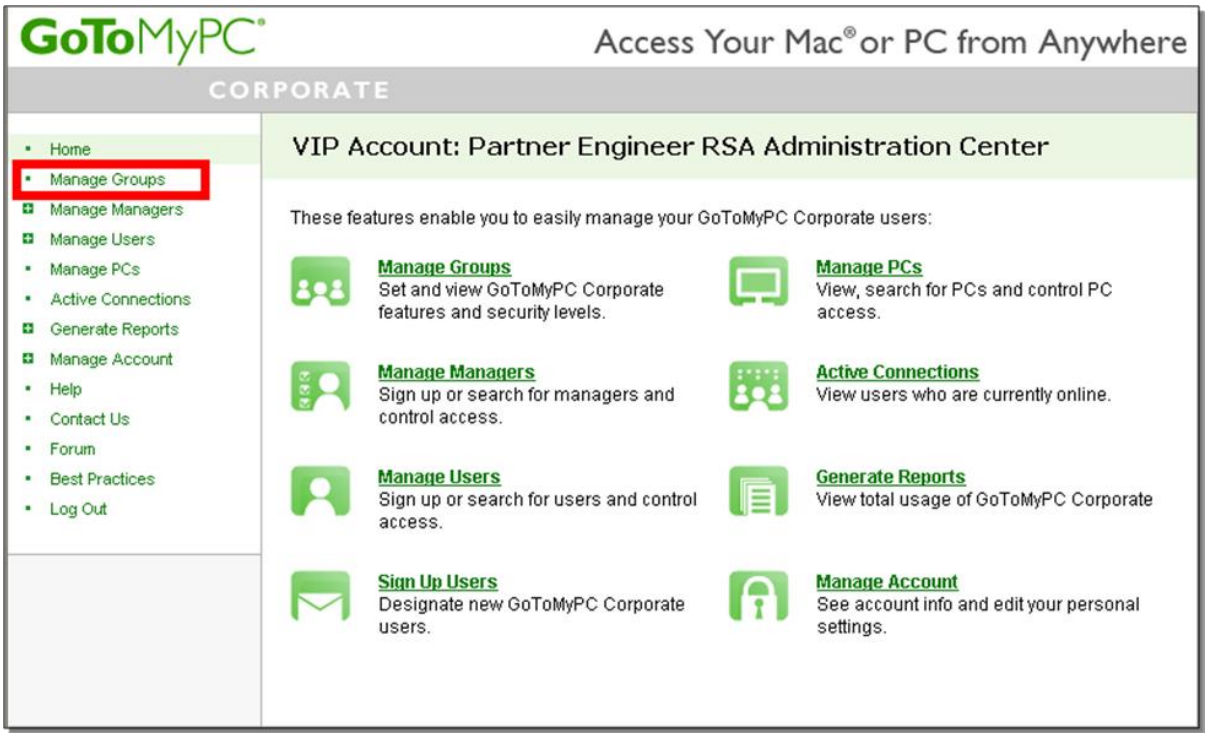
Configure GoToMyPC Corporate for RSA SecurID Authentication

RSA SecurID Authentication can be enabled in GoToMyPC Corporate completely from the GoToMyPC administration website or by enabling RADIUS on the administration website and configuring RADIUS at the host computer. This guide will focus on the latter scenario.

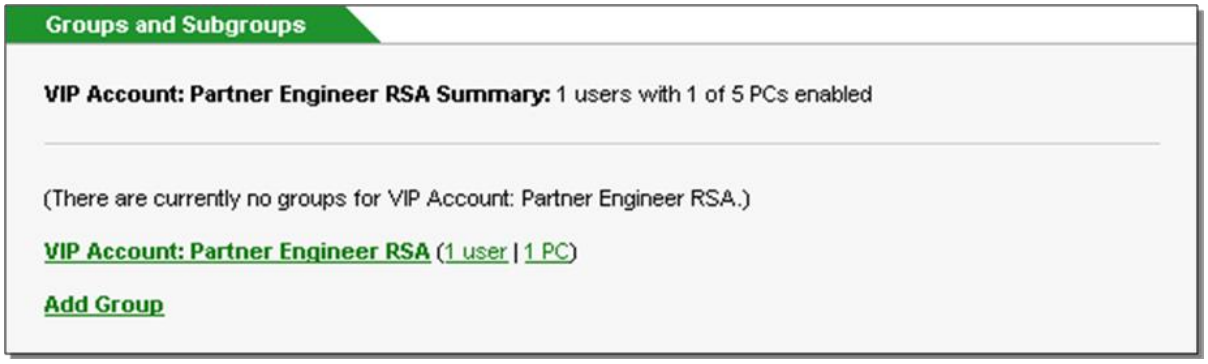
Enable RADIUS within the Administration Center

Log into your VIP Account: Administration Center by opening the URL: https://www.gotomypc.com in your web browser, and enter your Company Manager Account credentials.

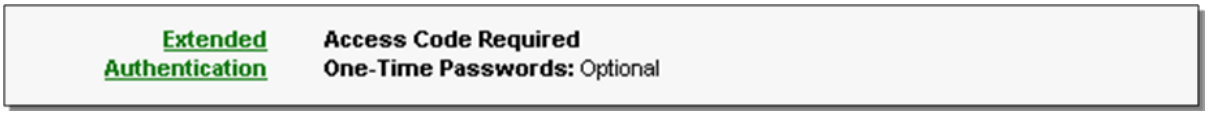
1. Click **Manage Groups** from the left side navigation menu.



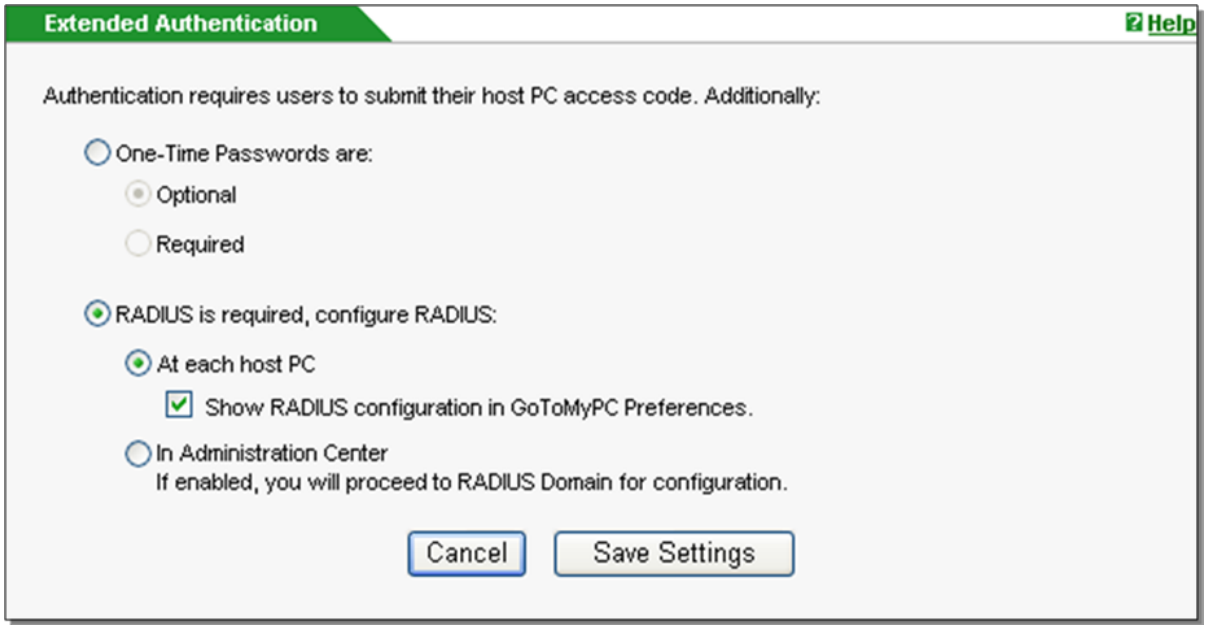
2. Select the group for which you are enabling SecurID Authentication.



3. Click **Extended Authentication** from the **Group Settings** menu.



4. Set the radio button to **RADIUS is required, configure RADIUS,** mark the **Show RADIUS configuration in GoToMyPC Preferences** checkbox and click **Save Settings**.

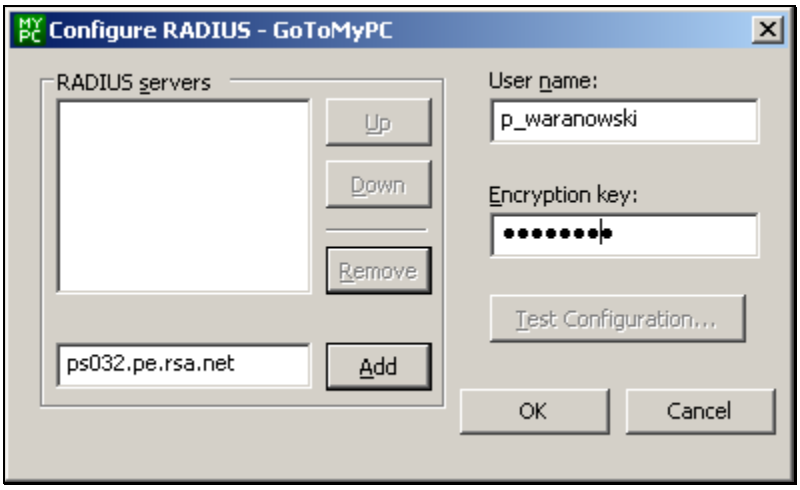


Configure RADIUS on GoToMyPC host system

5. Right click on the GoToMyPC icon in the system tray of the host system, and click **Preferences**.

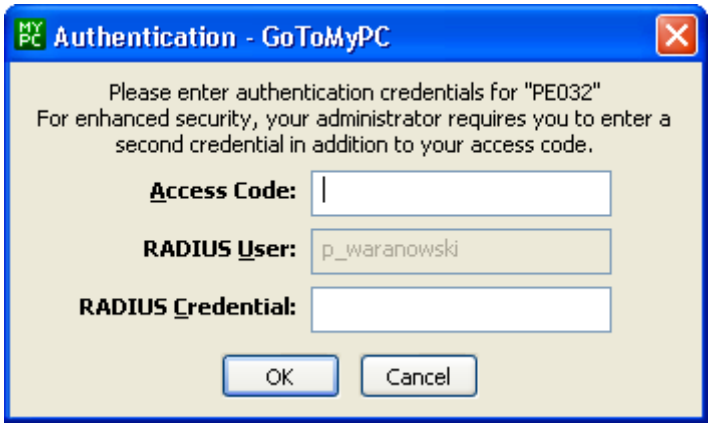
6. Open the **Authentication** tab and click **Configure RADIUS…**

7. Enter the RADIUS username into **User_name** and shared secret into **Encryption key**. Enter the hostname/IP address, and click **Add** for each RADIUS server. Click **OK** when finished.



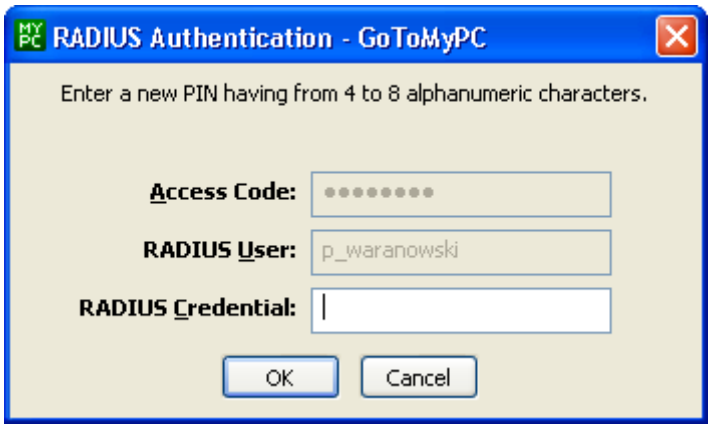
RSA SecurID Login Screens

Login screen:

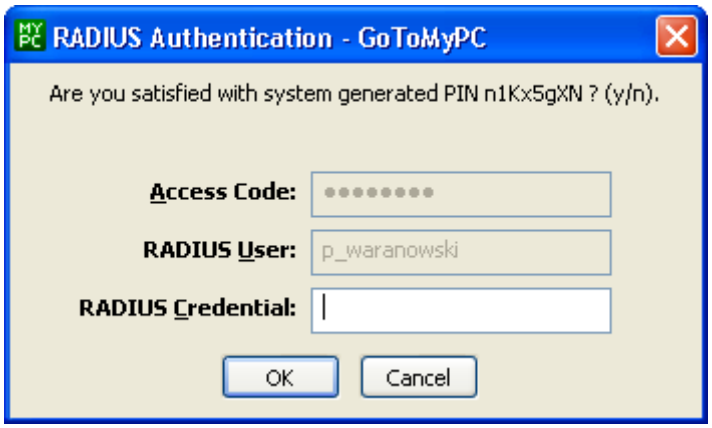


Note: Enter your RSA SecurID passcode into the RADIUS Credential field.

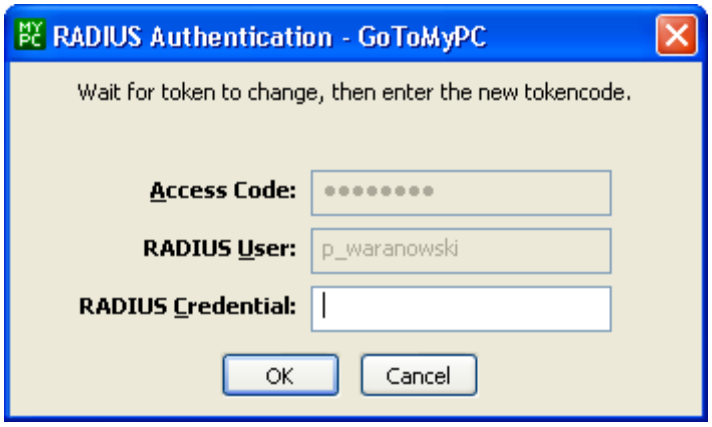
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1 SP1 P1	Virtual Appliance
GoToMyPC Corporate	8.3 (1606)	Windows Server 2012 R2

RSA SecurID Authentication

Date Tested: March 19th, 2015

Mandatory Functionality	RSA Native UDP Agent	RSA Native TCP Agent	RADIUS Client
New PIN Mode			
Force Authentication After New PIN	N/A	N/A	✓
System Generated PIN	N/A	N/A	✓
User Defined (4-8 Alphanumeric)	N/A	N/A	✓
User Defined (5-7 Numeric)	N/A	N/A	✓
Deny 4 and 8 Digit PIN	N/A	N/A	✓
Deny Alphanumeric PIN	N/A	N/A	✓
Deny PIN Reuse	N/A	N/A	✓
Passcode			
16 Digit Passcode	N/A	N/A	✓
4 Digit Fixed Passcode	N/A	N/A	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	N/A	✓
On-Demand Authentication			
On-Demand Authentication	N/A	N/A	✓
On-Demand New PIN	N/A	N/A	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	N/A	✓
No RSA Authentication Manager	N/A	N/A	✓

PEW

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