Apple Computer, Inc.
iOS

RSA SecurID Ready Implementation Guide

Last Modified: March 15, 2012

Partner Information

Product Information	
Partner Name	Apple Computer, Inc.
Web Site	www.apple.com
Product Name	iOS
Version & Platform	5.1
Product Description	iOS is Apple's mobile device operating system, found on their line of iPhone, iPod, and iPad range of devices. The VPN client built in to iOS allows mobile users to securely access email and data on their work networks while on the go.

Solution Summary

Virtual Private Networks (VPNs) are frequently used to allow users to communicate private information securely over a non-private network. For example, a VPN may need to be configured to access company email on an iOS device.

The VPN client built in to Apple iOS devices can be configured to require RSA SecurID two-factor authentication when configured to use the Layer 2 Tunneling Protocol (LT2P) or Point-to-Point Tunneling Protocol (PPTP) with a supported VPN server device.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring iOS 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 iOS components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

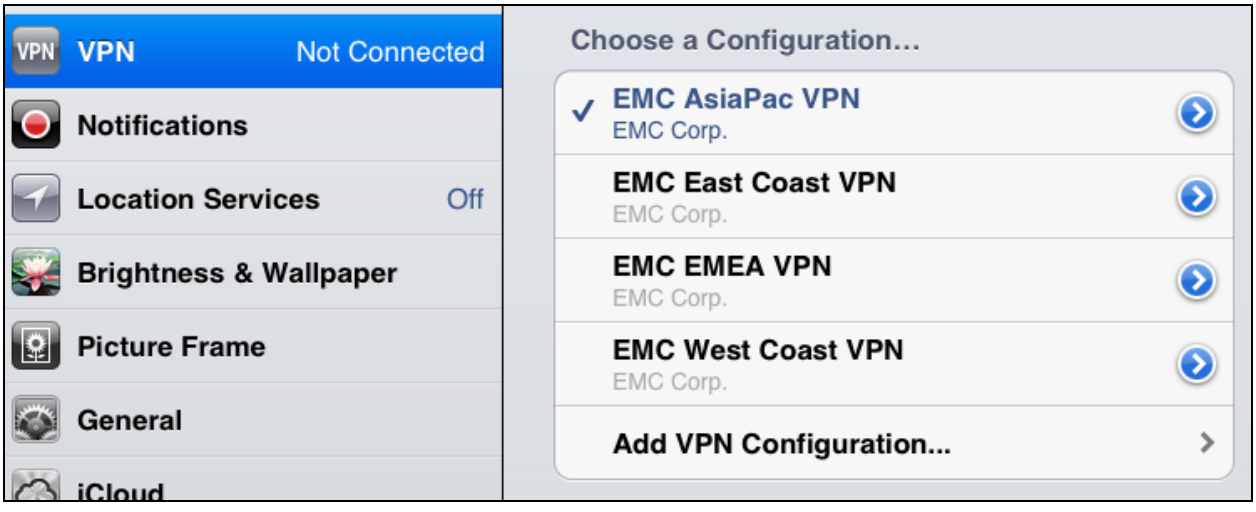
Apple VPN Client Configuration

The iOS VPN client is configured in the **Settings** for the iOS device. Details for configuring the iOS VPN Client can be found in the device's product documentation.

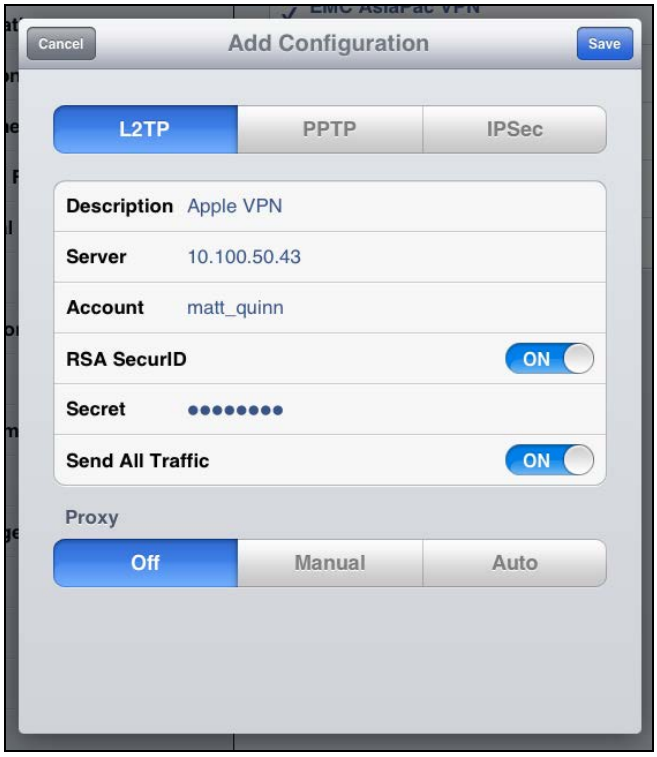
Ask your systems administrator for the necessary information needed to configure the VPN client, such as the VPN server address and connection type. To enable RSA SecurID authentication for the iOS device, follow the instructions below.

> **Note: The screenshots in the following section were taken from an Apple iPad. The screens on a smaller form-factor device will differ, but the configuration steps are essentially the same for both styles of device.**

1. Tap on **Settings** to begin.
2. Tap **VPN** and **Add VPN Configuration…**



3. Enter a description into the **Description** field, the VPN server's hostname or IP address into the **Server** field, and your SecurID username into the **Account** field. Slide the **RSA SecurID** slider to **ON**. If using **L2TP**, enter the shared secret configured on the VPN server into the **Secret** field. Tap **Save** to create the VPN Configuration.



Note: At the time of this writing, only the L2TP and PPTP connection types support RSA SecurID authentication.

iOS's VPN client does not support RSA SecurID authentication using the IPSec connection type. However, if your VPN Server supports authentication using RSA SecurID, it may be possible to configure two-factor authentication using the IPSec connection type. Check with your VPN Server device manufacturer.

4. Tap the newly created VPN Configuration to set it as the active profile, and slide the **VPN** slider to **ON** to connect and authenticate using the profile.

VPN Server Configuration

The iOS VPN Client is capable of passing SecurID credentials to a compatible VPN server. While any L2TP or PPTP-enabled VPN server that supports SecurID authentication may work, RSA has validated the iOS VPN client against the Apple OS X and Microsoft VPN servers. Detailed instructions for configuring each server can be found at their respective product documentation.

Apple VPN Server Configuration

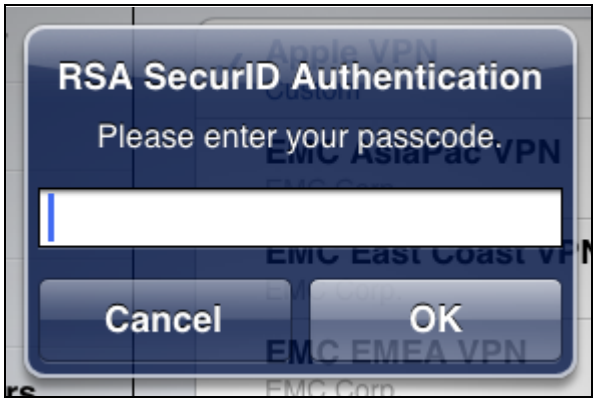
Refer to the RSA Implementation Guide for the **Apple OS X VPN Service** for complete instructions on configuring the service for RSA SecurID authentication.

Microsoft VPN Server Configuration

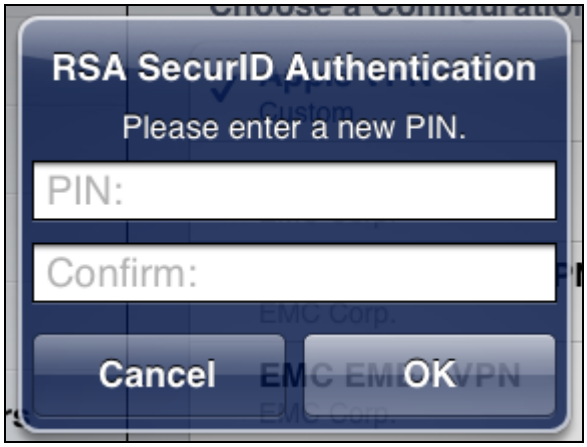
Refer to the RSA Authentication Agent for Windows product documentation. See the section **Deploying Remote Authentication Using EAP with Microsoft IAS RADIUS Server**.

Screens

Login screen:

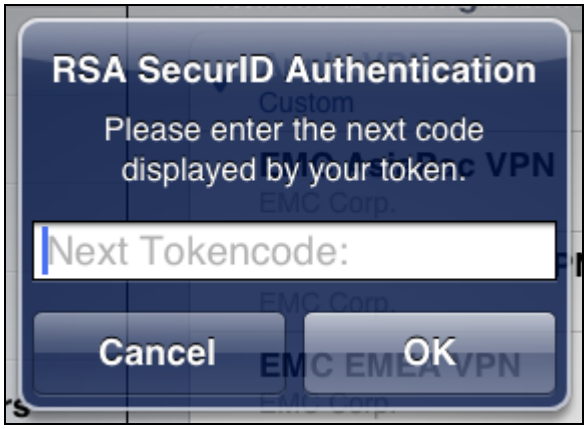


User-defined New PIN:



System-generated New PIN:

Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: March 15, 2012

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1 SP4	Windows Server 2003 SP2
Apple iOS VPN Client		iOS 5.1
Apple Mac OS X VPN Service		Mac OS X Server 10.5.8

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

MRQ

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

Note: For best results, the iOS VPN client must connect to a VPN service that fully supports RSA SecurID authentication and supports L2TP or PPTP connections. Refer to the Secured By RSA Solution Gallery for a list of certified VPN solutions.

This solution was tested using the Apple Mac OS X VPN Service.

Known Issues

If a new PIN is rejected, the VPN client does not notify the user

User-defined PINs are rejected by the RSA Authentication Manager if they do not meet the PIN complexity requirements defined in the user's token policy, or if the user attempts to reuse a previous PIN as defined in their token policy.

When a user-defined PIN is rejected by RSA Authentication Manager, the VPN client does not notify the user in any way as to the failure. Instead, the user is shown a login prompt. This behavior is the same if the user's PIN is accepted. This can lead to confusion if the user supplies an invalid PIN.

New PIN prompts do not display PIN complexity requirements

The New PIN prompts displayed to the user when their SecurID authenticator is in New PIN mode do not display the PIN complexity requirements required by the user's token policy configured on the Authentication Manager Server.

This can lead to confusion when a user unknowingly submits an invalid PIN because the VPN client will not notify them of the failure.