# Columbitech
## Columbitech Mobile VPN

# RSA SecurID Ready Implementation Guide

Last Modified: May 22, 2013

## Partner Information

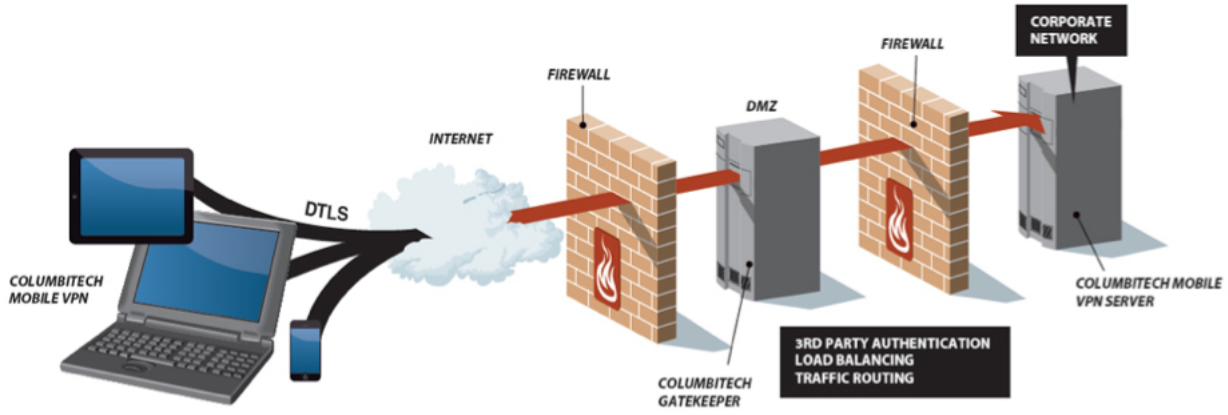
| Product Information | |
|---|---|
| **Partner Name** | Columbitech |
| **Web Site** | www.columbitech.com |
| **Product Name** | Columbitech Mobile VPN |
| **Version & Platform** | Version 6.5.0 for Windows |
| **Product Description** | Columbitech Mobile VPN is a software-based mobile virtual private network and provide mobile worker secure and reliable wireless access to mission-critical data and applications. It establishes an authenticated, encrypted tunnel, which enables mobile users to access network resources securely from any wireless network. |

# Solution Summary

Columbitech Mobile VPN is a software-based mobile virtual private network and provides mobile workers secure and reliable wireless access to mission-critical data and applications.

Columbitech uses a strong security framework specially designed and optimized for communication in a wireless environment. The solution is completely software-based and allows you to extend your existing communication infrastructure rather than replace it. To re-enforce the security of the Columbitech Environment, RSA SecurID two-factor authentication has been integrated into the Columbitech products.

| RSA Authentication Manager supported features<br>Columbitech Mobile VPN version 6.5.0 | |
|---|---|
| **RSA SecurID Authentication via Native RSA SecurID Protocol** | Yes |
| **RSA SecurID Authentication via RADIUS Protocol** | No |
| **On-Demand Authentication via Native SecurID Protocol** | Yes |
| **On-Demand Authentication via RADIUS Protocol** | No |
| **Risk-Based Authentication** | No |
| **Risk-Based Authentication with Single Sign-On** | No |
| **RSA Authentication Manager Replica Support** | Yes |
| **Secondary RADIUS Server Support** | No |
| **RSA SecurID Software Token Automation** | No |
| **RSA SecurID SD800 Token Automation** | No |
| **RSA SecurID Protection of Administrative Interface** | No |



# Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

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 Columbitech Mobile VPN will occur.

**Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.**

To install the RSA Authentication Agent, follow the instructions provided in the **RSA Authentication Agent 7.1 for Microsoft Windows Installation and Administration Guide**.

# RSA SecurID files

| RSA SecurID Authentication Files | |
|---|---|
| **Files** | **Location** |
| sdconf.rec | %SystemRoot%\SysWOW64 |
| Node Secret | %SystemRoot%\SysWOW64 |
| sdstatus.12 | %SystemRoot%\SysWOW64 |
| sdopts.rec | %SystemRoot%\SysWOW64 |
| | |

**Note: The appendix of this document contains more detailed information regarding these files.**

# Partner Product Configuration

## *Before You Begin*

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

## *Authenticating users with RSA SecurID*

Both Columbitech Mobile VPN™ Server and Columbitech Gatekeeper can be configured to require users to authenticate using RSA SecurID one-time password tokens You must add the RSA Authentication Agent to one or both of these servers, depending on your original network architecture and the specific implementation of your Columbitech Mobile VPN™ environment.

## *Server Configuration*

In order to protect your Columbitech Mobile VPN™ environment with RSA SecurID authentication, enable RSA SecurID authentication on either your Columbitech Gatekeeper or Columbitech Mobile VPN™ Server as follows:

- Install the RSA Authentication Agent on the Columbitech server you have selected. If you have e.g. multiple Columbitech Mobile VPN™ Servers you will have to install the RSA Authentication Agent on all Columbitech Mobile VPN™ Servers.
- Using the Columbitech server configuration, select the **Security** tab and ensure the **SecurID authentication** checkbox is checked.

RSA and Columbitech recommend RSA Authentication Agent version 7.1.

1. Download the RSA Authentication Agent API and Copy the 32-bit versions of *aceclnt.dll* and *sdmsg.dll* to the *%SystemRoot%\SysWOW64* folder on the Columbitech server. You can download the API from the Columbitech support site **http://support.columbitech.com/support/download/RSAAuthentication Agent32bitDLLs.zip** or from RSA's SecurCare Online website.

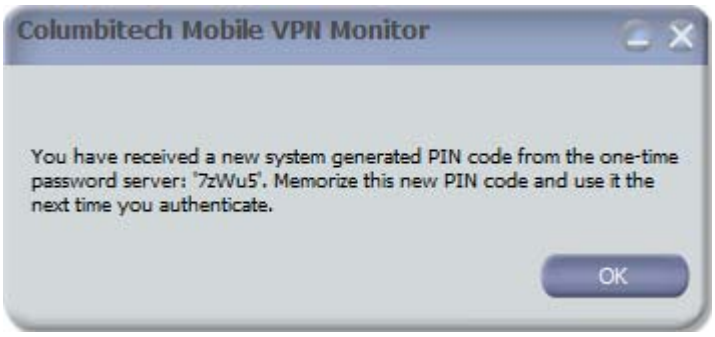
Verify the RSA Authentication Agent installation with a test logon Use the RSA Authentication Agent's Control Center to run a test authentication. Once you have successfully authenticated, copy the node secret file, *securid*, from the *C:\Program Files\Common Files\RSA Shared\Auth Data* folder to the *%SystemRoot%\SysWOW64* folder.

# RSA SecurID Login Screens

Login screen:


User-defined New PIN:

System-generated New PIN:




Next Tokencode:

# Certification Checklist for RSA Authentication Manager

Date Tested: May 22, 2013

| Certification Environment | | |
|---|---|---|
| **Product Name** | **Version Information** | **Operating System** |
| **RSA Authentication Manager** | 8.0 | Virtual Appliance |
| **RSA Authentication Agent** | 7.1.2 | Windows Server 2008 R2 |
| **Columbitech Mobile VPN Server** | 6.5.0.239 | Windows Server 2008 R2 |
| **Columbitech Mobile VPN Client** | 6.5.0.232 | Windows 7 x64 |

| 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 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 |

DRP / PAR

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

# Appendix

| Partner Integration Details | |
|---|---|
| **RSA SecurID API** | Version 8.1.2 |
| **RSA Authentication Agent Type** | Standard Agent |
| **RSA SecurID User Specification** | All Users |
| **Display RSA Server Info** | No |
| **Perform Test Authentication** | No |
| **Agent Tracing** | Yes |
| | |

## *API Details:*

## *SecurID:*

To clear the node secret on the agent host delete securid. You must also clear the node secret on the AM to insure proper registration of the Agent Host.

## *sdconf.rec:*

To register the host with a new RSA Authentication Manager delete the sdconf.rec file located in %SystemRoot%\SysWOW64.

## *sdopts.rec:*

The sdopts.rec file can be created and modified to address issues with multi-homed systems. The sdopts.rec file is located in %SystemRoot%\SysWOW64.

## *sdstatus.12:*

The sdstatus.12 file provides the agent host with status information about the AM hosts and is located in %SystemRoot%\SysWOW64.

## *Agent Tracing:*

The Columbitech Mobile VPN diagnostic log file, C:\DebugLog.txt, will include trace information from the RSA SecurID Agent.