# Moka5, Inc.
## Moka5 Suite

# RSA SecurID Ready Implementation Guide

Last Modified: October 3rd, 2013

## Partner Information

| Product Information | |
|---|---|
| **Partner Name** | Moka5, Inc. |
| **Web Site** | www.moka5.com |
| **Product Name** | Moka5 Suite |
| **Version & Platform** | 3.16 |
| **Product Description** | Moka5 is a next-generation solution harnessing the power of virtualization to transform how desktops are delivered, managed and secured. Moka5 provides IT organizations a virtual desktop solution that blends enterprise security and policy control with end user flexibility and ease-of-use. It provides an extensive set of features that supports both Windows and Macintosh computers. |

## Solution Summary

Moka5 Suite allows you to deploy secure, encrypted virtual desktops that run locally on desktops or laptops. A Moka5 administrator can create a single golden image and deploy it to thousands of Mac, Windows, or bare metal endpoints. The Moka5 Management Server is used to centrally manage images and enforce policies. Moka5 Player is the client component that authenticates an end user before granting access to the virtual desktop, also known as a LivePC.

Moka5 Suite integrates with RSA SecurID to provide two-factor authentication for the Moka5 Player. Moka5 administrators can now provide a greater level of security when accessing network resources through the Moka5 Suite software.

| RSA SecurID supported features | |
|---|---|
| **Moka5 Suite 3.16** | |
| **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 |
| **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 Moka5 Suite will occur.

> **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 documentation for additional information about creating, modifying and managing Authentication Agents and clients.

# RSA SecurID files

| RSA SecurID Authentication Files | |
|---|---|
| **Files** | **Location** |
| sdconf.rec | C:\Program Files (x86)\MokaFive\conf |
| Node Secret | C:\Program Files (x86)\MokaFive\conf |
| JAStatus.1 | C:\Program Files (x86)\MokaFive\conf |
| sdopts.rec | C:\Program Files (x86)\MokaFive\conf |
| | |

> **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 the Moka5 Suite 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 Moka5 Suite components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

## *Prerequisites*

- Fully configured Moka5 Suite 3.16 environment:
    - Moka5 Management Server (integrated with Active Directory configured)
    - Moka5 Desktop Application Gateway Server
    - LivePC image deployed to an endpoint (Mac, Windows, or BareMetal)
- RSA Authentication Manager Server
- Cisco VPN 5.0.x (integrated with RSA SecurID)

## *Configure the Moka5 Desktop Application Gateway Server for SecurID*

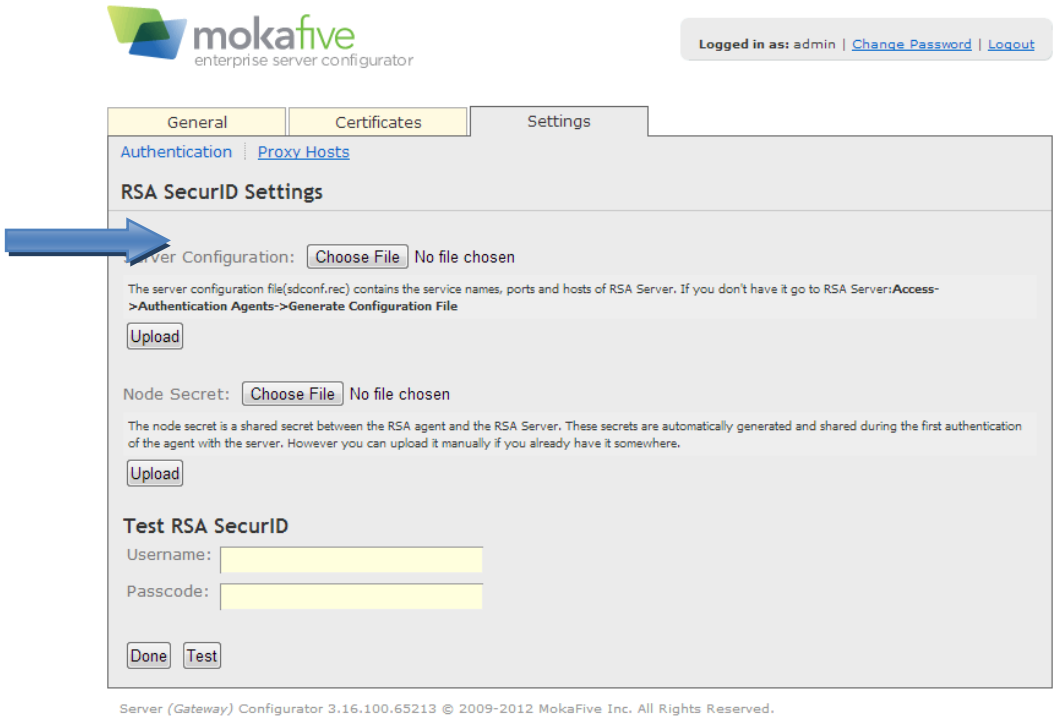
The Moka5 Desktop Application Gateway server may be configured to use SecurID authentication. Follow the steps below to setup SecurID authentication.

1. Open a web browser and enter the URL for the Moka5 Desktop App Gateway's iconfig page. The default administration page is **https://<Moka5_Desktop_Gateway>/iconfig** where **<Moka5_Desktop_Gateway>** is:
    - **FQDN hostname** of the Moka5 server.
    - - OR - **IP address** of the Moka5 server.
    - - OR - **localhost**, if you are connected to the server using remote desktop.

2. Login to iconfig with the bootstrap administrator account. This is the local account you created when you first installed the Moka5 Desktop Application Gateway Server.


**3.** Go to **Settings** tab > **Authentication** panel > click **Edit Settings**

4. Click **Choose File** to upload the *sdconf.rec* configuration file. This file is obtained from the RSA Authentication Manager server.




5. Click the **Upload** button.

Next, test the connection to the RSA Authentication Manager server.

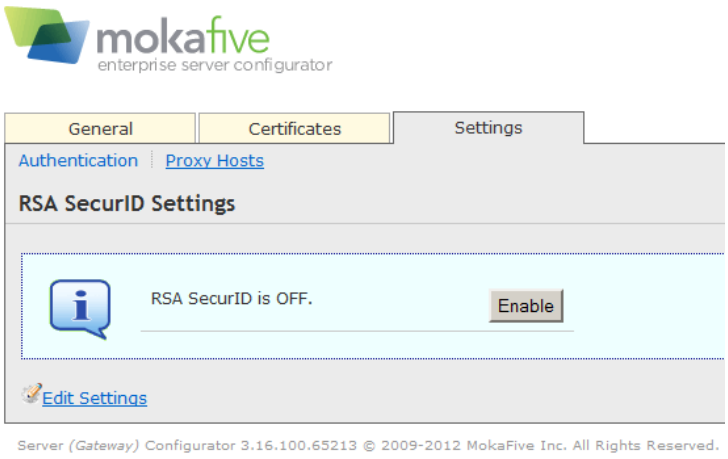
6. Input a valid **Username** and **Passcode** and click **Test**.

> **Note: The Moka5 server needs to be configured as an Authentication Agent within the RSA Authentication Manager server.**

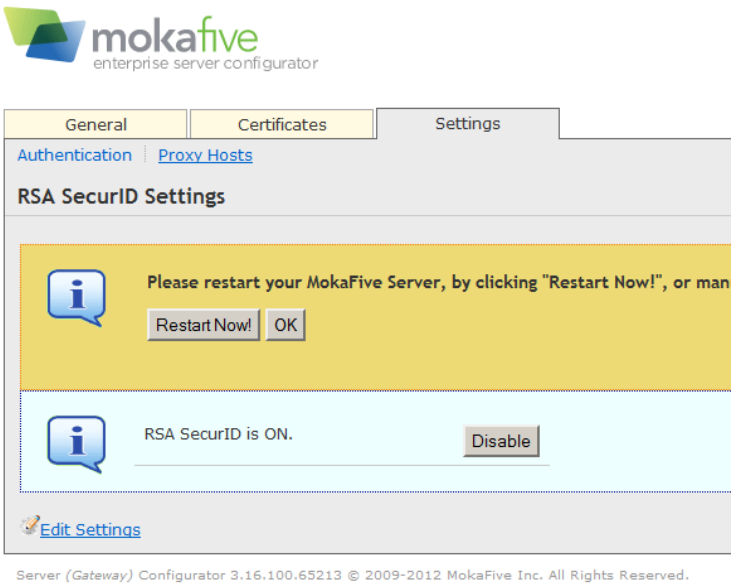
The Moka5 server should respond with ***Successfully authenticated to RSA Server*** as shown below. Do not continue until you have successfully authenticated.


7. Click **Done** to return to the previous page.

8. Click the **Enable** button. From this point forward, all Moka5 authentication requests that come to the Desktop Application Gateway Server will be prompted for RSA SecurID authentication.



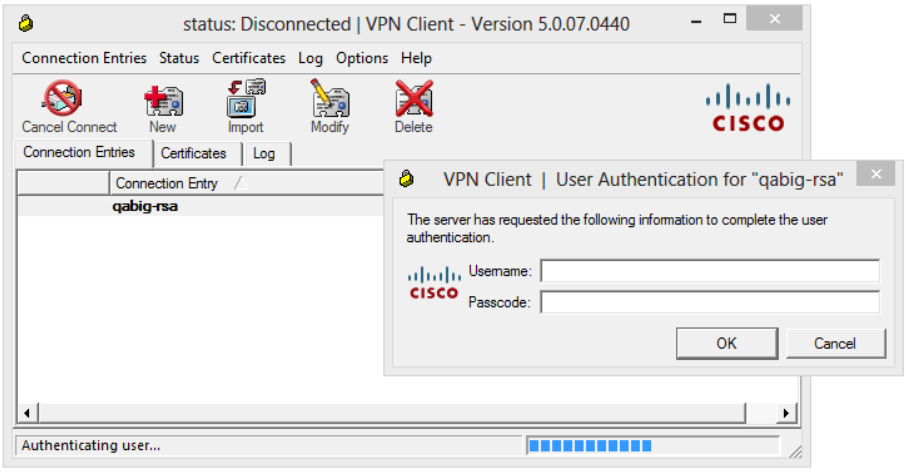

9. Click the **Restart Now** button to complete the setup process. The Moka5 server is now configured for RSA SecurID authentication.



## *How to change your RSA PIN*

When a user's token requires a PIN change, the user must use the Cisco VPN client. The Moka5 player does not support New PIN mode. This section describes the procedure for changing the PIN.

1. Launch the Cisco VPN client.
2. Connect using the VPN profile that is integrated with RSA.




3. You will be prompted to enter:
    - Username
    - Passcode
4. The VPN client will prompt you to change your **PIN**.
5. Enter the new **PIN**, confirm the **PIN**, then click **Done**.

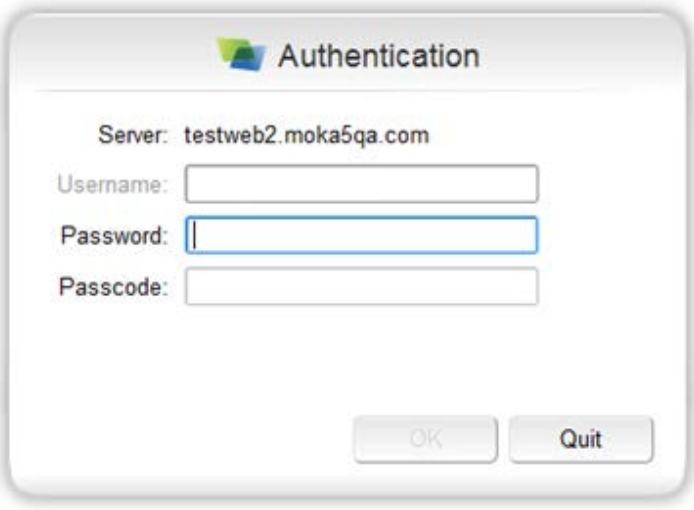
**Note: Next Tokencode Mode does not require the use of the Cisco VPN Client.**

## *Log in to Moka5 Player with RSA SecurID Authentication*

Use the following steps to log in to Moka5 Player with RSA SecurID authentication configured.

1. Launch the Moka5 Player.


2. Enter your Active Directory **username**.
3. Enter your Active Directory **password**.
4. Enter your RSA **passcode**.

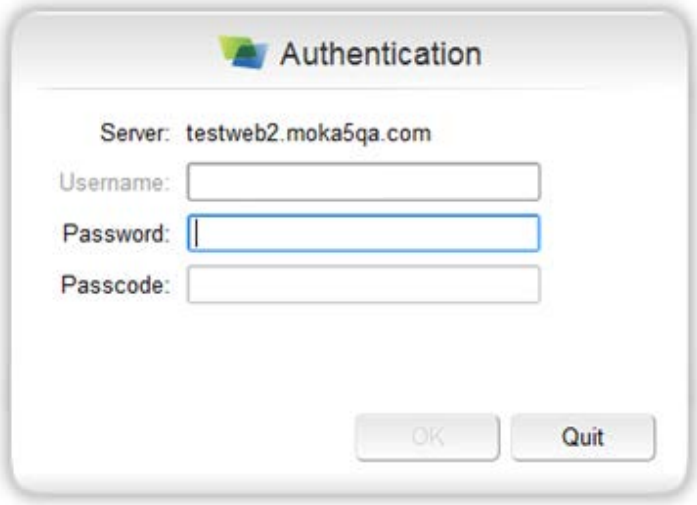



5. Once successfully authenticated, the Moka5 Player will open and you can start your LivePC.

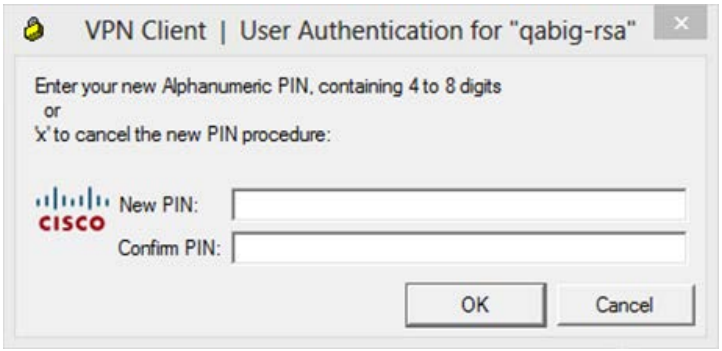
**Note: If the RSA token is in New PIN mode, you must use the Cisco VPN client to change the PIN prior to launching the Moka5 Player or the authentication will fail.**

## RSA SecurID Login Screens

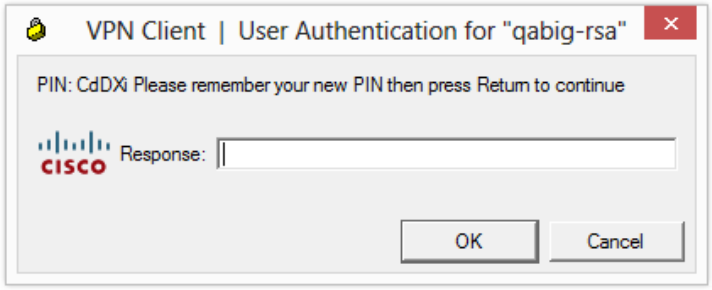
Login screen:



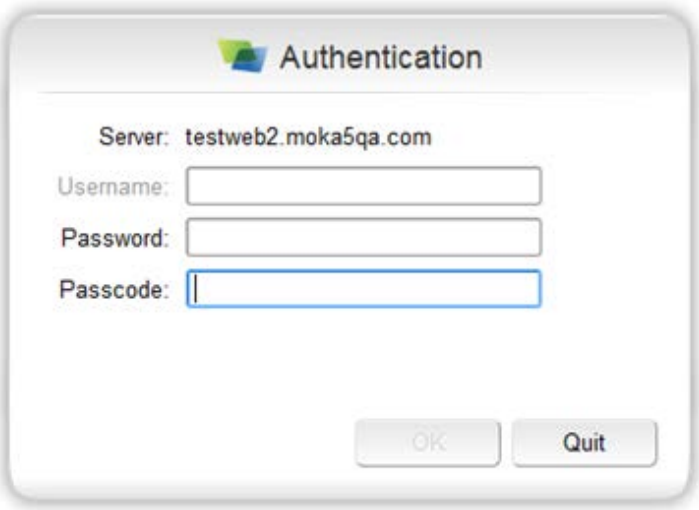

User-defined New PIN:



System-defined New PIN:




Next Tokencode:



# Certification Checklist for RSA Authentication Manager

Date Tested: October 3rd, 2013

| Certification Environment | | |
|---|---|---|
| **Product Name** | **Version Information** | **Operating System** |
| **RSA Authentication Manager** | 8.0 | Virtual Appliance |
| **Cisco VPN Client** | 5.0 | Microsoft Windows 7 |
| **Moka5 Suite** | 3.16 | Microsoft Windows 7 |

| 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 |

JJO / PAR

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

# Appendix

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

## *API Details:*

The Moka5 Suite uses the RSA SecurID Authentication SDK 5.0.3.2 for Java.

## *Node Secret:*

The node secret (securid) is created after a successful authentication. The file resides in the **C:\Program Files (x86)\MokaFive\conf** directory. To clear the node secret from the Moka5 server, delete the securid file.

## *sdconf.rec:*

The sdconf.rec file is copied to the **C:\Program Files (x86)\MokaFive\conf** directory after configuring SecurID authentication through the Moka5 administration interface.

## *sdopts.rec:*

The sdopts.rec file resides in the **C:\Program Files (x86)\MokaFive\conf** directory.

## *JAStatus.1:*

The sdstatus.12 file is created in the **C:\Program Files (x86)\MokaFive\conf** directory after a successfully authentication.