



## RSA SecurID Ready Implementation Guide

Last Modified: April 8, 2014

### Partner Information

---

| Product Information |   |
|---------------------|---|
| Partner Name        | Citrix Systems, Inc.  |
| Web Site            | <a href="http://www.cisco.com">www.cisco.com</a>  |
| Product Name        | XenApp  |
| Version & Platform  | 7.5   |
| Product Description | Citrix XenApp is an on-demand application delivery solution that enables any Windows® application to be virtualized, centralized, and managed in the datacenter and instantly delivered as a service to users anywhere on any device. In use by over 100 million users worldwide, XenApp delivers on the promise of proven application compatibility. |



## Solution Summary

---

XenApp Server provides local, remote, and mobile users access to enterprise applications over a variety of transports. Companies who make enterprise data available with XenApp server must ensure that all users who access that content be positively identified. Using strong two-factor authentication, RSA Authentication Manager can be configured to create secure end-to-end transactions between XenApp servers and clients.

| <b>RSA Authentication Manager supported features</b>              |     |
|---|-----|
| <b>Citrix XenApp 7.5</b>  |     |
| <b>RSA SecurID Authentication via Native RSA SecurID Protocol</b> | Yes |
| <b>RSA SecurID Authentication via RADIUS Protocol</b>             | No  |
| <b>On-Demand Authentication via Native SecurID Protocol</b>       | Yes |
| <b>On-Demand Authentication via RADIUS Protocol</b>               | No  |
| <b>Risk-Based Authentication</b>                                  | No  |
| <b>Risk-Based Authentication with Single Sign-On</b>              | No  |
| <b>RSA Authentication Manager Replica Support</b>                 | Yes |
| <b>Secondary RADIUS Server Support</b>                            | No  |
| <b>RSA SecurID Software Token Automation</b>                      | No  |
| <b>RSA SecurID SD800 Token Automation</b>                         | No  |
| <b>RSA SecurID Protection of Administrative Interface</b>         | 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 Citrix XenApp 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 RADIUS clients.

## RSA SecurID files

---

| RSA SecurID Authentication Files |                                |
|----------------------------------|--------------------------------|
| Files                            | Location                       |
| sdconf.rec                       | Dependent on RSA Agent Version |
| Node Secret                      | Dependent on RSA Agent Version |
| sdstatus.12                      | Dependent on RSA Agent Version |
| sdopts.rec                       | Dependent on RSA Agent Version |

---

 **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 Citrix XenApp with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

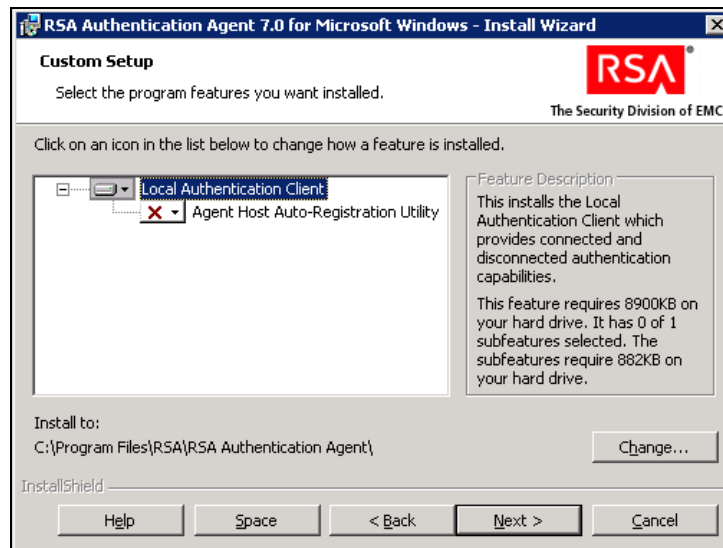
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

### RSA SecurID Agent Configuration

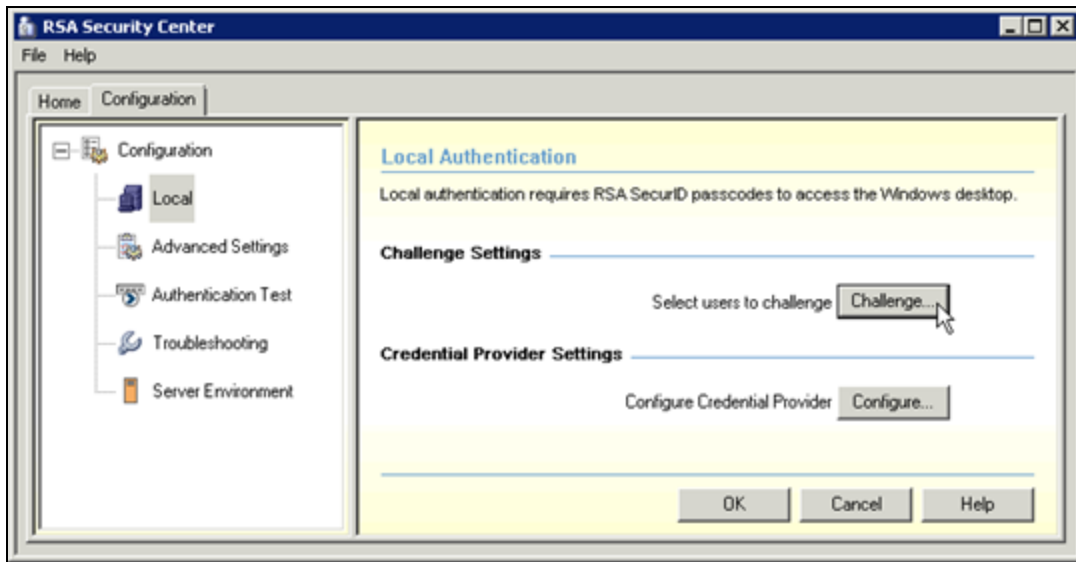
1. To begin, install the RSA Authentication Agent for Windows on the Citrix XenApp server. During the installation, select a custom installation and make sure that only the **Local Authentication Client (LAC)** component is checked.

 **Note:** Refer to RSA documentation to determine which RSA Authentication Agent is appropriate for your version of Windows.

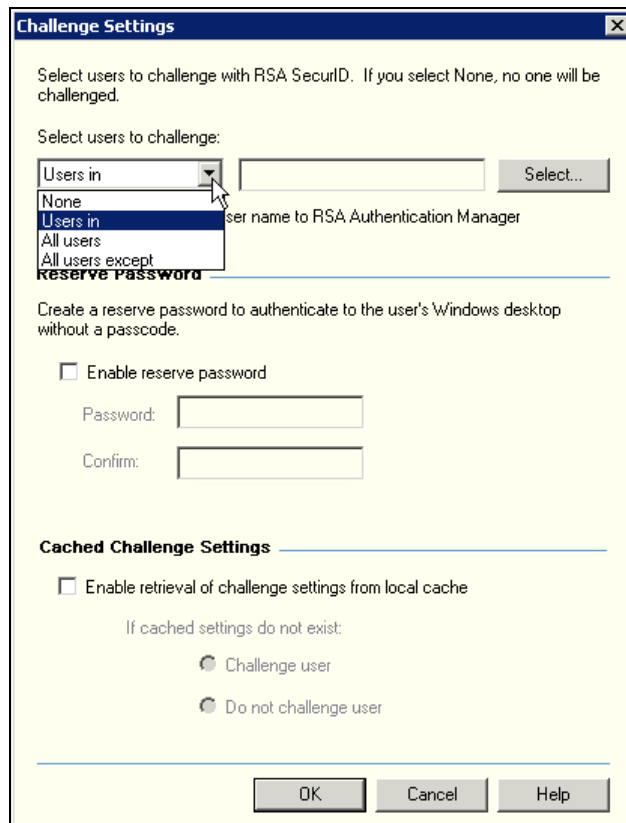


2. Enter the location of the sdconf.rec file from your primary RSA Authentication Manager server and accept the rest of the installer defaults. Reboot the system to complete the installation.

3. After the system reboots, launch the RSA Security Center from the Start Menu or Control Panel and open the **Configuration** tab.
4. Click **Local** from the left navigation window and click **Challenge** from the **Challenge Settings** section.



5. Make your selection from **Select users to challenge** drop down menu and click **OK**.



## Citrix Client Configuration

No additional configuration is required on the Citrix client machine. Once an application has been published from the RSA SecurID-protected XenApp Server, clients can access it from their lists of published applications. Users who launch one of these published applications are challenged for RSA SecurID authentication prior to gaining access.

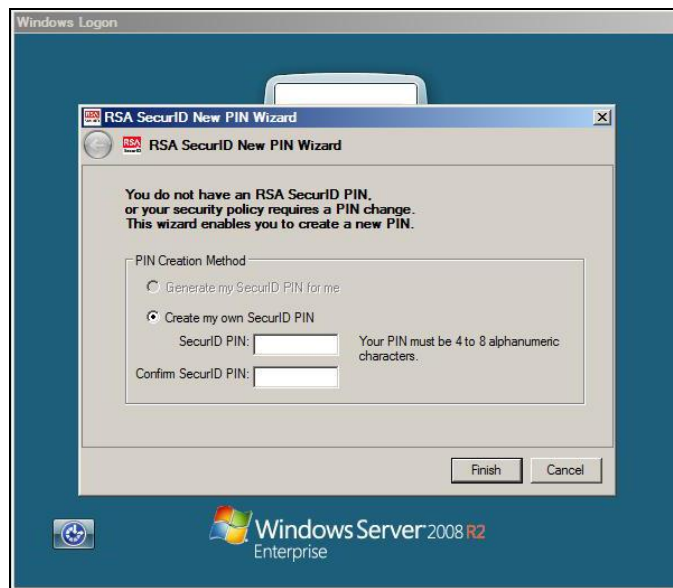
## Screens

---

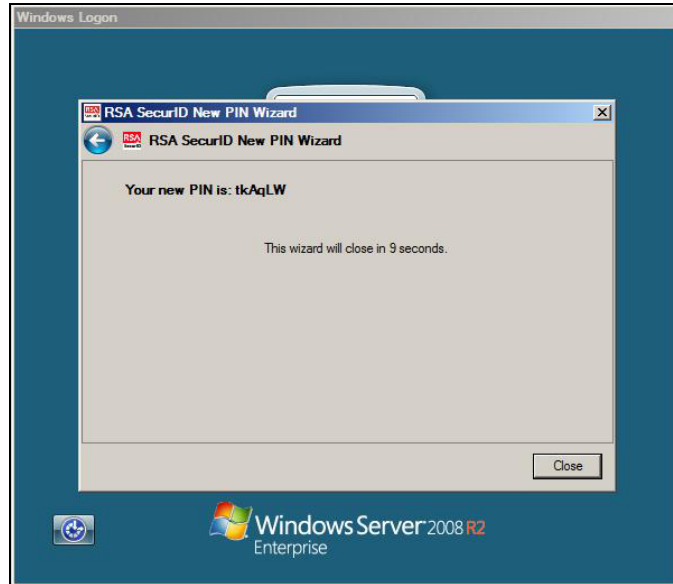
Login screen:



User-defined New PIN:



System-generated New PIN:



Next Tokencode:





## Certification Checklist for RSA Authentication Manager

Date Tested: April 8, 2014

| Certification Environment  |                     |                        |
|----------------------------|---------------------|------------------------|
| Product Name               | Version Information | Operating System       |
| RSA Authentication Manager | 8.1                 | Virtual Appliance      |
| RSA Authentication Agent   | 7.2                 | Windows Server 2008 R2 |
| Citrix XenApp              | 7.5                 | Windows Server 2008 R2 |
| Citrix Receiver            | 4.1.0.56461         | Windows Server 2008 R2 |

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

PEW

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

## Known Issues

---

### **Citrix client 'hangs' when Windows Password Integration is disabled.**

This issue applies if you are using the RSA Authentication Agent 7.0 and have disabled Windows Password Integration with RSA Authentication Manager's Offline Authentication Policy. Under these conditions, after each time a user sets a new SecurID PIN, the LoginUI.exe process will grow to ~600MB and then restart. As the process grows, the Citrix client will be unresponsive. Once the process restarts, the user will be able to log in as usual.

## Appendix

---

| Partner Integration Details    |   |
|--------------------------------|---|
| RSA SecurID API                | Dependent on RSA Authentication Agent version |
| RSA Authentication Agent Type  | Standard Agent                                |
| RSA SecurID User Specification | Designated Users                              |
| Display RSA Server Info        | Yes; via RSA Security Center                  |
| Perform Test Authentication    | Yes; via RSA Security Center                  |
| Agent Tracing                  | Yes; via RSA Security Center                  |
|                                |   |

### ***Node Secret:***

Refer to documentation for the version of RSA Authentication Agent for information regarding Node Secret.

### ***sdconf.rec:***

Refer to documentation for the version of RSA Authentication Agent for information regarding sdconf.rec configuration file.

### ***sdopts.rec:***

Refer to documentation for the version of RSA Authentication Agent for information regarding sdopts.rec configuration file.

### ***sdstatus.12:***

Refer to documentation for the version of RSA Authentication Agent for information regarding sdstatus.12 configuration file.

### ***Agent Tracing:***

Refer to documentation for the version of RSA Authentication Agent for information regarding Agent Tracing.