Desktone, Inc.
Desktone Platform 5.2

RSA SecurID Ready Implementation Guide

Last Modified: December 10, 2012

Partner Information

Product Information	
Partner Name	Desktone, Inc.
Web Site	www.desktone.com
Product Name	Desktone Platform
Version & Platform	5.2
Product Description	By delivering cloud-hosted virtual desktops as a service, Desktone enables companies to rapidly provision desktops to users on any device, anywhere, without the upfront costs and complexity of traditional desktop virtualization.

Solution Summary

Desktone provides enterprises with the option to require Desktone Platform end-users to authenticate with RSA SecurID two-factor authentication. Desktone Platform contains a custom, out-of-the-box RSA Authentication Manager client, allowing you to easily enable RSA SecurID authentication with a few simple configuration procedures. After you complete the integration described in this document, Desktone Platform will prompt end-user for a username and RSA SecurID passcode and pass the credentials to the RSA Authentication Manager Server using RSA authentication API libraries.

RSA SecurID supported features	
Desktone Platform 5.2	
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
On-Demand Authentication via API	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	Yes

Authentication Agent Configuration

Agent Host Records contain information that allows an RSA Authentication Manager server to locate its clients and establish secure communication channels with them. The server's database must contain an Agent Host Record to identify each Desktone Tenant installed in your environment.

The following information is required in order to create an Agent Host record:

- the hostname of each Desktone Tenant in your environment
- IP address for all of the network interfaces on each Desktone Tenant host

Note: Each Desktone Tenant will communicate with RSA Authentication Manager servers using the RSA's API libraries. Ensure that the two applications are visible to one another on your network. In addition, make sure each hostnames resolves to a valid IP address.

You should also set the record's **Agent Type** to *Standard Agent*. RSA Authentication Manager uses this value to determine how it will establish communication with the Desktone Platform.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	You may save the *sdconf.rec* file in any local directory. See the **Desktone Platform Configuration** section for instructions to upload the file to Desktone.
Node Secret	*/var/ace*
sdstatus.12	*/var/ace*
sdopts.rec	Not implemented

Partner Product Configuration

Before You Begin

This section provides configuration instructions to enable RSA SecurID two-factor authentication for the Desktone Platform. This document is not intended to suggest optimum installations or configurations.

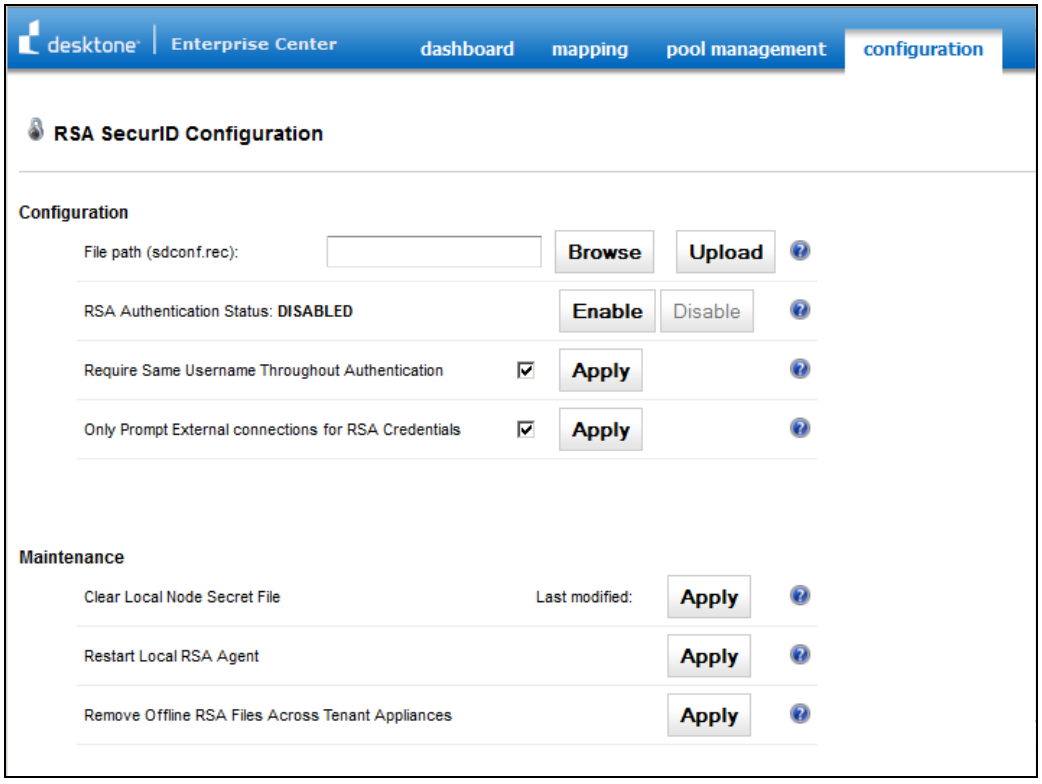
It is assumed that the reader has working knowledge of RSA Authentication Manager and Desktone Platform and access to the appropriate product documentation.

All RSA Authentication Manager and Desktone components must be installed and running before you begin to configure the integration. Perform the necessary tests to confirm that this is true before proceeding.

Desktone Platform Configuration

Follow the steps below to configure Desktop Platform for RSA SecurID authentication:

1. You must use the RSA Authentication Manager Security Console to create a file named *sdconf.rec*. RSA's API uses this file to locate the primary RSA Authentication Manager server. To generate the file, log into the RSA Authentication Manager RSA Security Console, navigate to **Access → Authentication Agents →Generate Configuration Files** and save the file in a local directory.
2. Move the *sdconf.rec* file to a directory on each Tenant host in your environment.
3. Log in to the Desktone Enterprise Center as a Tenant Administrator and select **Configuration → Multi-Factor Authentication**. The RSA SecurID Configuration screen will be displayed:

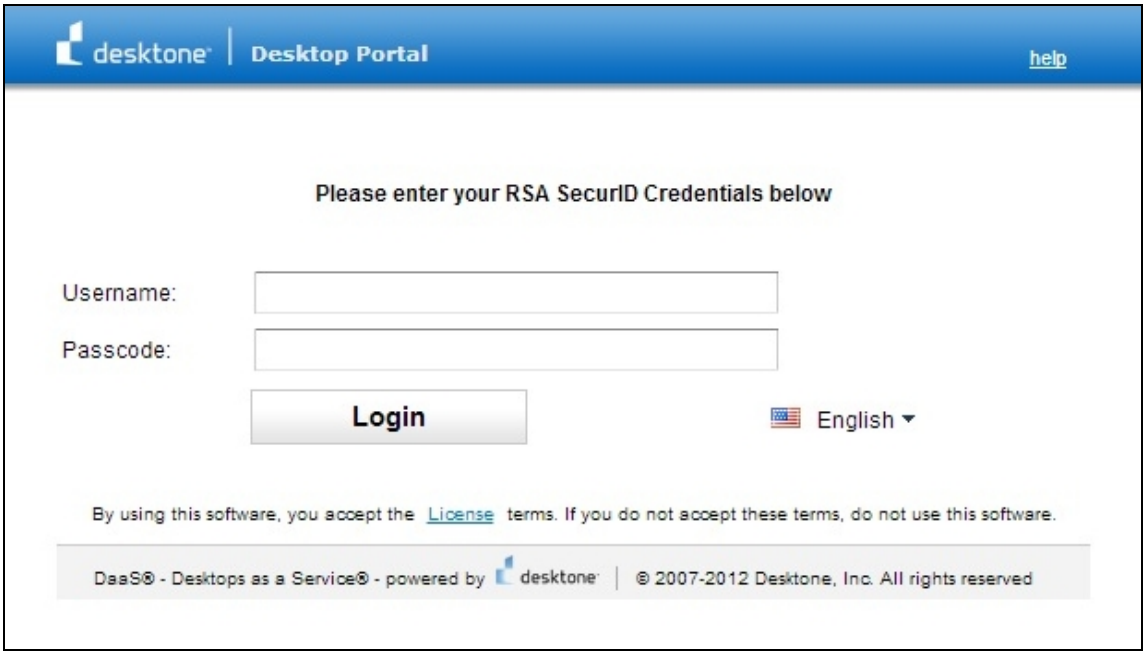


4. Click the *Browse* button, navigate to the directory you chose in step 2 and select the *sdfonf.rec* file. The file's path will appear in the **File path** text field.
5. Click the **Upload** button.
6. RSA SecurID authentication is initially is disabled for Desktone end-users. In order to enable it, you must perform a successful RSA SecurID authentication within the Desktone Enterprise Center. Complete the steps below to do so:
    a. Click **Enable** to display the Test Authentication dialog.
    b. Enter a valid username and the user's RSA SecurID passcode.
    c. Click the **Test** button. If the authentication is successful, the status will change from *DISABLED* to *ENABLED*. Subsequently, all Desktone users will be required to authenticate with RSA SecurID.

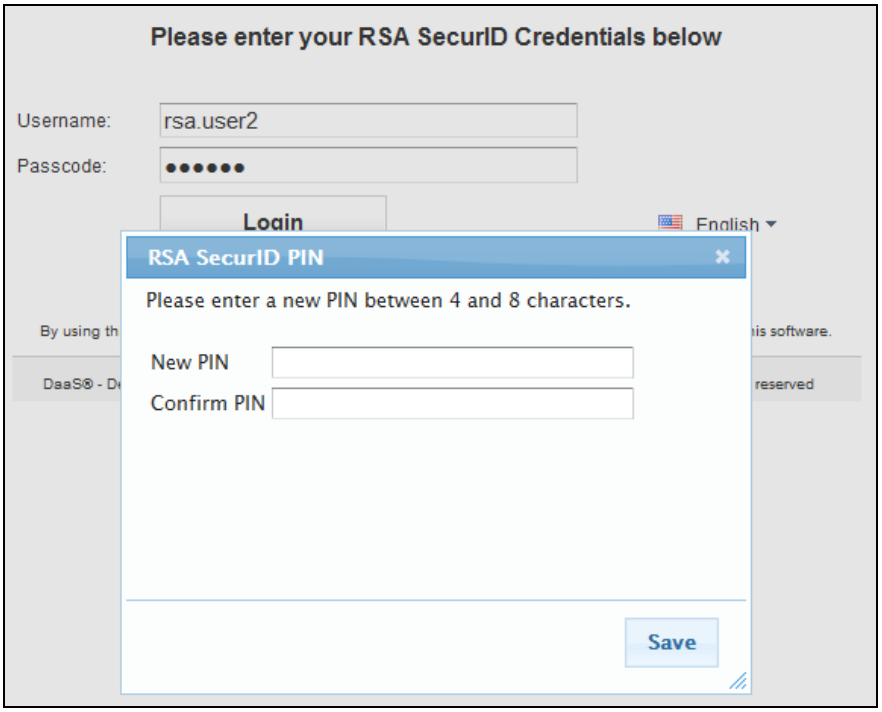
Note: The Service Provider can temporarily override RSA authentication, allowing Enterprise Center Administrators to bypass the RSA authentication step when logging in to the Enterprise Center or the User Portal. If the Tenant Administrator can no longer authenticate on any appliance, he or she should contact the Service Provider to temporarily deactivate RSA Authentication.

7. If you wish to require each end-user to use his/her domain username for RSA SecurID authentication as well, select the **Require Same Username Throughout Authentication** checkbox and click the **Apply** button. Otherwise, the username field will remain unlocked on the Domain Challenge screen and you may assign each user two unique usernames.
8. If you wish to limit RSA SecurID authentication to users who are external to the network, select the **Only Prompt External connections for RSA Credentials** checkbox and click the **Apply** button. Otherwise, all internal and external users will be required to user their RSA credentials.
9. On occasion, you may have to clear the RSA Authentication Manager *Node Secret* on your Tenant host. In order to do so, click the **Apply** button to the right of the **Clear Local Node Secret File** label.

User Login Screens

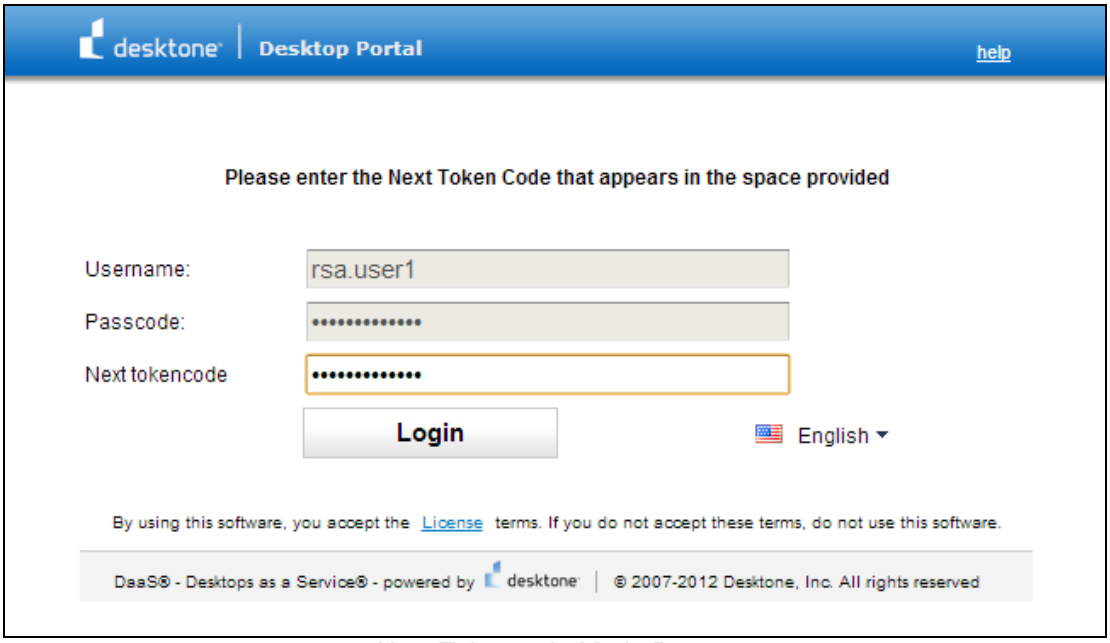


Standard Login Screen



New PIN Mode Prompt

System Generated PIN Prompt



Next Tokencode Mode Prompt

Important: The WYSE P20 Thin Client only allows users to enter 8 characters in the **Next tokencode** field. When prompted for a next tokencode as above, an end-user should omit the RSA SecurID PIN and only enter his/her tokencode.

.

Certification Checklist for RSA Authentication Manager

Date Tested: November 19, 2012

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1 SP4	Windows 2008 Server
RSA Authentication Manager API	8.1.1	LINUX
Desktone Platform	5.2	Ubuntu Linux version 10.04

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			
14 Digit Passcode	✓	14 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

JGS / PAR

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

Known Issues

- If you change RSA Authentication Manager security policies, you must restart the RSA Agent. In order to do so, open the RSA SecurID Configuration screen and click the **Apply** button to the right of the **Restart Local RSA Agent** label.
- If an end-user enters *New PIN Mode* and submits an invalid PIN, the user must close and re-open the login dialog in order to make another attempt. Additionally, Desktone will not inform users if their PIN policy restricts the use alphabetic or numeric characters.