RSA Ready Implementation Guide for

RSA SecurID

ManageEngine ADSelfService Plus 5.3

RSA Partner Engineering
Last Modified: October 26th, 2016

RSA READY

Solution Summary

ManageEngine[1] ADSelfService Plus (ADSSP) is a secure, web-based self-service password management solution. The product allows end users to reset their Microsoft Windows Active Directory (AD) domain passwords, unlock their accounts and update their personal information without any help desk intervention.

ADSelfService Plus supports Active Directory and LDAP password authentication out-of-the-box. Its integration with RSA Authentication Manager introduces an extra level of security by enabling RSA SecurID two-factor authentication.

ADSSP communicates with RSA Authentication Manager using the RSA Authentication Agent API. During the authentication process, ADSSP prompts the user for a username and an Active Directory or LDAP domain password. After validating the user's password, ADSSP prompts the user for an RSA SecurID passcode and submits it to RSA Authentication Manager for validation.

Important: Each ADSelfService Plus user's Active Directory/LDAP domain username must match his or her RSA Authentication Manager username.

Supported Features	
ManageEngine ADSelfService Plus 5.3	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	Yes
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No
RSA SecurID Authentication via RADIUS Protocol	No
RSA SecurID Authentication via IPv6	No
On-Demand Authentication via Native SecurID UDP Protocol	Yes
Risk-Based Authentication	No
RSA Authentication Manager Replica Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	Yes

[1] ManageEngine is a division of Zoho Corp.

RSA Authentication Manager Configuration

Authentication Agent Configuration

RSA Authentication Agents are custom or ready-made software applications that securely pass user authentication requests to and from RSA Authentication Manager. RSA provides the RSA Authentication Agent API for building custom agents, as well as a variety of out-of-the-box agents for protecting access to various operating systems and web resources.

All agents must be registered with RSA Authentication Manager in order for the server to locate them and establish secure communication channels with them. Use the RSA Security Console to register an agent for you ADSSP server.

You need the following information to register the agent:

- the ADSSP server's hostname
- IP addresses for all of the ADSSP server's network interfaces

When you register the authentication agent, set its agent type to *Standard Agent*.

> **Note:** The ADSSP server's hostnames must resolve to a valid IP address on your local network.

Consult the *RSA Authentication Manager Administrator Guide* for more information about configuring authentication agents.

Partner Product Configuration

Before You Begin

This section provides instructions for enabling RSA SecurID two-factor authentication for ManageEngine ADSelfService Plus users. You should have working knowledge of ADSSP and RSA Authentication Manager, as well as access to the appropriate end-user and administrative documentation. Ensure that that both products are running properly prior to configuring the integration, and that each user's Active Directory/LDAP domain username matches match his/her RSA Authentication Manager username.

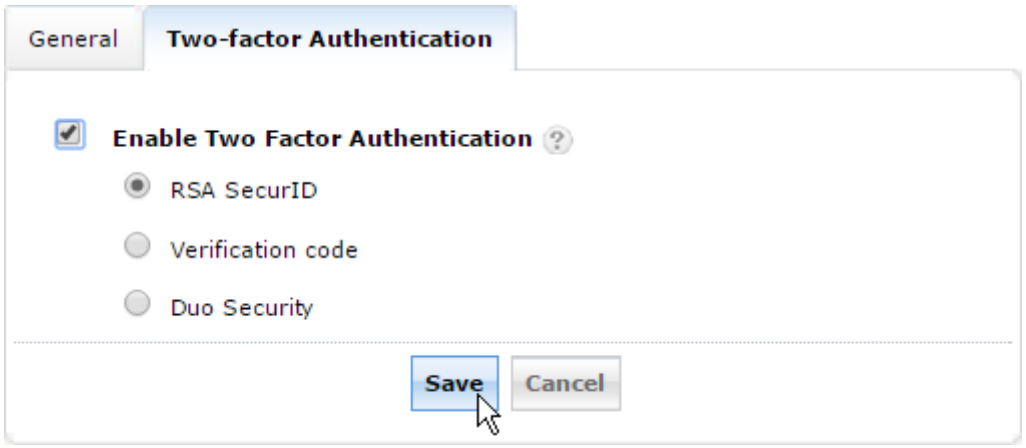
> **Important**: Each ADSelfService Plus user's Active Directory/LDAP domain username must match his or her RSA Authentication Manager username.

This document is not intended to suggest optimal installations or configurations.

Configure ADSelfService Plus for RSA SecurID Authentication

1. Download a copy of your RSA Authentication Manager server's *sdconf.rec* file and copy it to your ADSelfService Plus installation folder's *bin* directory. This directory is *C:\ManageEngine\ADSelfService Plus\bin* by default.
2. Log in to ADSSP as administrator and click the **Admin** tab.
3. Expand the **Customize** dropdown menu on the left side of the page and select *Logon Settings*.

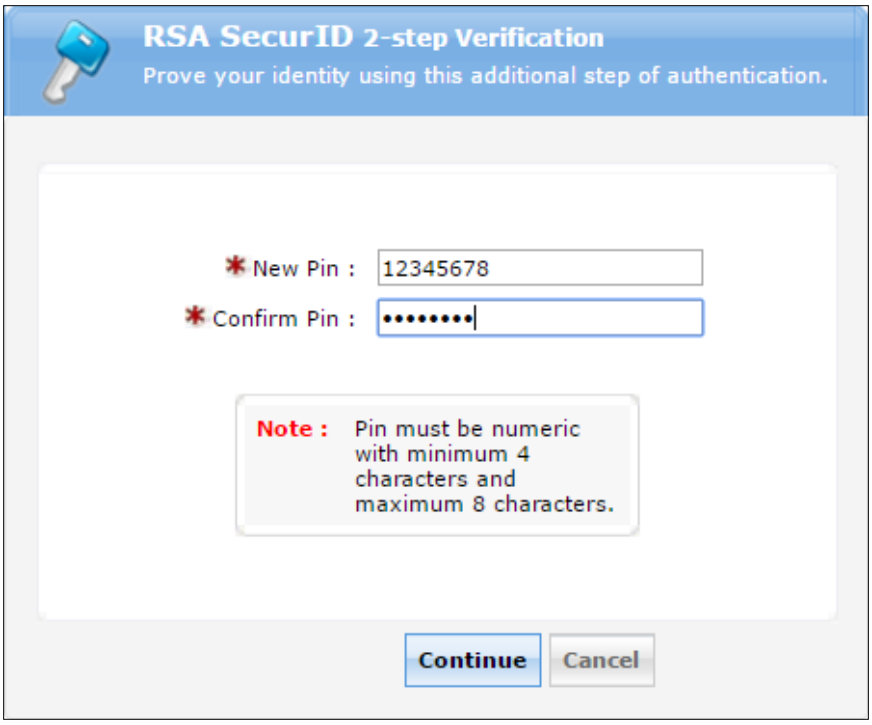
4. Click the **Two Factor Authentication** tab.
5. Check the **Enable Two Factor Authentication** checkbox.
6. Select the **RSA SecurID** radio button and click the **Save** button.



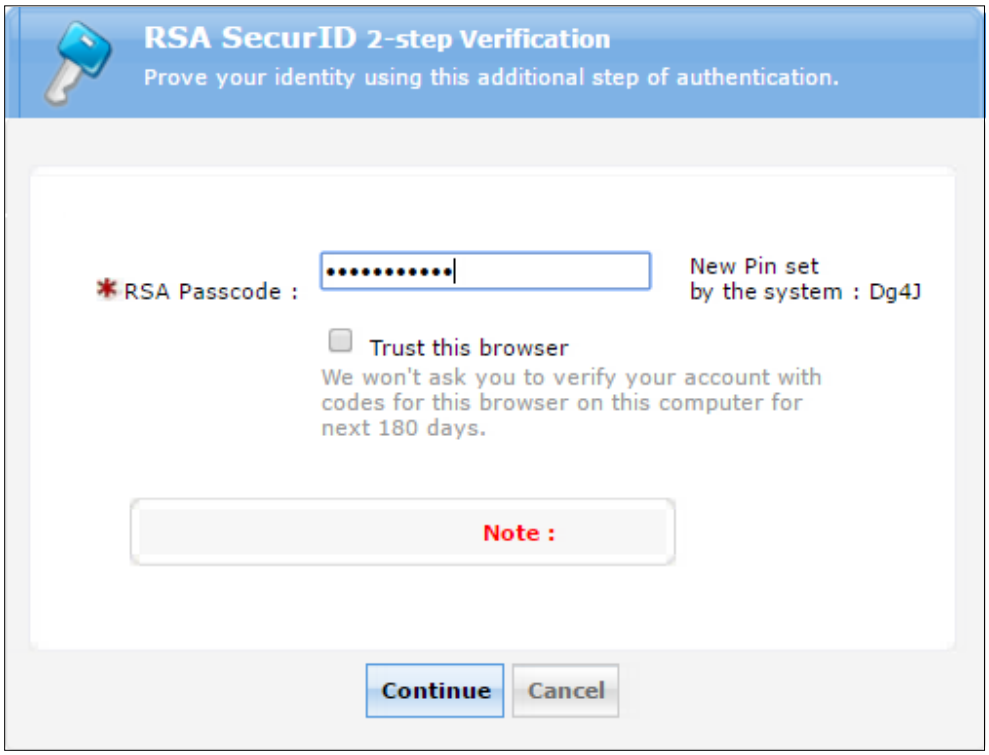
RSA SecurID Login Screens

Domain User Password Login Prompt

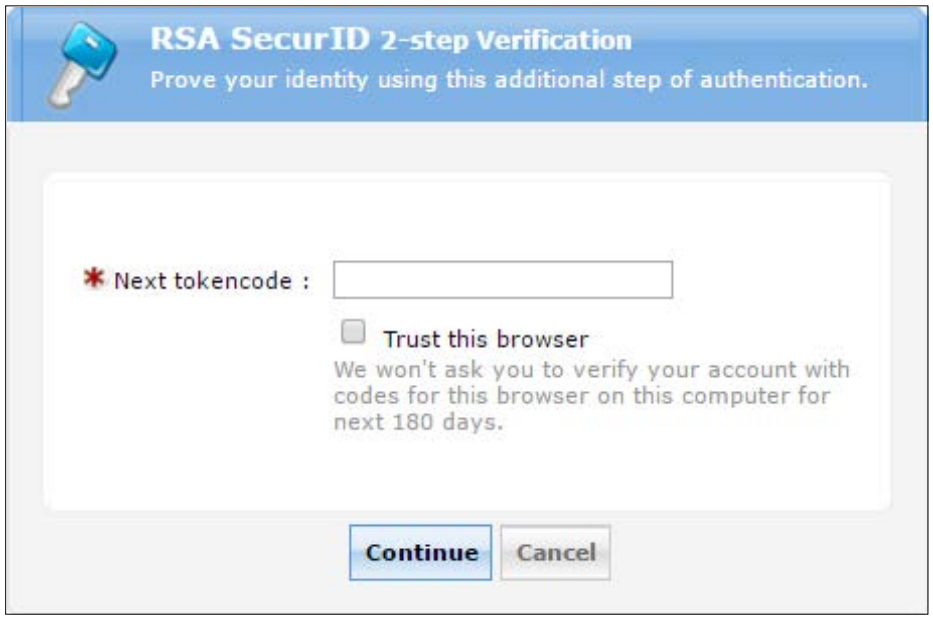
Standard SecurID Login Prompt



New PIN Mode Prompt



System-Generated PIN Prompt



Next Tokencode Prompt

Certification Checklist for RSA Authentication Manager

Date Tested: October 20th, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.2	Virtual Appliance
ManageEngine ADSelfService Plus	5.3 (build 5319)	Windows 7

RSA SecurID Authentication

Date Tested: October 20th, 2016

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

✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	*<ADSSP_ROOT>/bin*[2], where *<ADSSP_ROOT>* is the ManageEngine ADSelfService Plus installation folder.
sdopts.rec	*<ADSSP_ROOT>/bin*
Node secret	*<ADSSP_ROOT>/bin*
sdstatus.12 / jastatus.12	*<ADSSP_ROOT>/bin*

Partner Integration Details

Partner Integration Details	
RSA SecurID UDP API	8.1.3
RSA SecurID TCP API	N/A
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	No

RSA Configuration Files

Node Secret:

To clear the node secret on the ADSelfService Plus server, navigate to the *<ADSSP_ROOT>/bin* directory and delete the *securid* file.

sdconf.rec:

To update *sdconf.rec* on the ADSelfService Plus server, navigate to the *<ADSSP_ROOT>/bin* directory and replace the old *sdconf.rec* file with the new copy.

[2] This directory is *C:\ManageEngine\ADSelfService Plus\bin* by default.