Idea Device Technologies
Epsilon

RSA SecurID Ready Implementation Guide

Last Modified: August 16th, 2013

Partner Information

Product Information	
Partner Name	Idea Device Technologies Pvt. Limited
Web Site	www.ideadevice.com
Product Name	Epsilon
Version & Platform	v2.3, Linux
Product Description	Epsilon is a suite of IT Process Automation products aimed at automating L1 IT activities in an organization. Epsilon eliminates manual errors, guarantees process compliance, eliminates password sharing & scales the abilities of your existing IT team. Large banks, exchanges & MNCs use Epsilon to automate all Unix, Windows, Network, Database, Application & Password-Reset activities. Customers have improved IT reliability & IT-operational maturity without scaling up IT teams linearly. Epsilon's agentless automation technology is non-disruptive and zero-risk allowing incremental automation by existing administrators.

Solution Summary

Epsilon is a flexible Secure Run Book Workflow Automation product to address the security, workflow & process needs of SME & Enterprise IT/OPS departments.

Epsilon has a built in authentication mechanism to provide secure access to the product. Alternatively, Epsilon can be configured to authenticate with RSA SecurID authentication, using the Native RSA SecurID protocol. When configured to authenticate with RSA SecurID, access to Epsilon is secured by RSA Authentication Manager. Epsilon will present a screen to accept user name and password (passcode). Based on the response from the Authentication Manager, Epsilon will either prompt for changing the PIN on the token or may prompt for Next Tokencode mode for token synchronization.

RSA Authentication Manager supported features	
Epsilon v2.3	
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 Epsilon 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.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	/var/lib/<tomcat>**
Node Secret	/var/lib/<tomcat>**
JAstatus.1	/var/lib/<tomcat>**
sdopts.rec	/var/lib/<tomcat>**
**<tomcat> refers to the default tomcat installation directory (e.g: */var/lib/tomcat6)*	

> **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 Idea Device Technologies Epsilon 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 Idea Device components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring Epsilon for Native SecurID Authentication

To enable RSA Native SecurID authentication in Epsilon, perform the following actions:

1. Login to the Epsilon server console.

2. Open the Epsilon configuration file (***epsilon.ini***) with a text editor. This file resides in ***<epsilon root>/conf/*** directory***.*** Add the following section to the end of the file:

```
[rsa]
enabled = True
```

Note: *<epsilon root>* is the base installation directory for Epsilon.

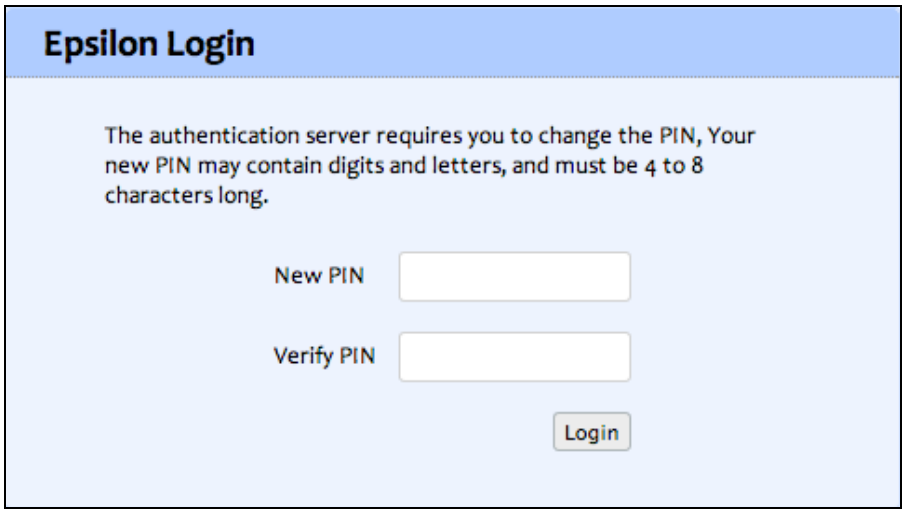
3. Copy the RSA **sdconf.rec** file to the /var/lib/<tomcat> directory on the Epsilon server. The **sdconf.rec** is downloaded from the Authentication Manager server and contains configuration information that controls the behavior of the RSA Authentication API. Set file owner and group permission to ***tomcat***.

4. Restart the Epsilon server. All users now will be authenticated using RSA SecurID except the Administrator account.

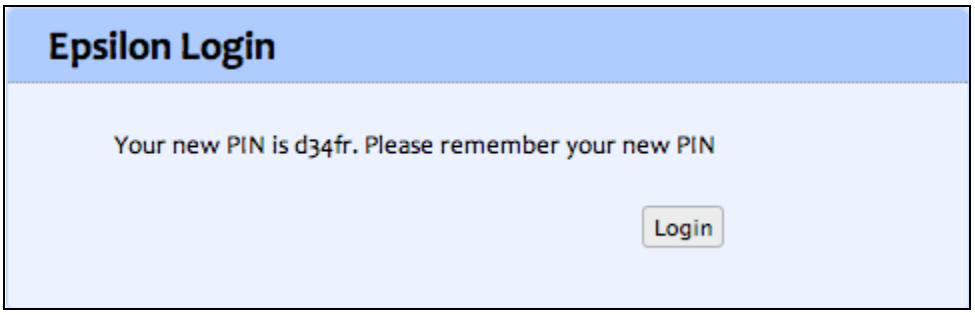
RSA SecurID Login Screens

Login screen:

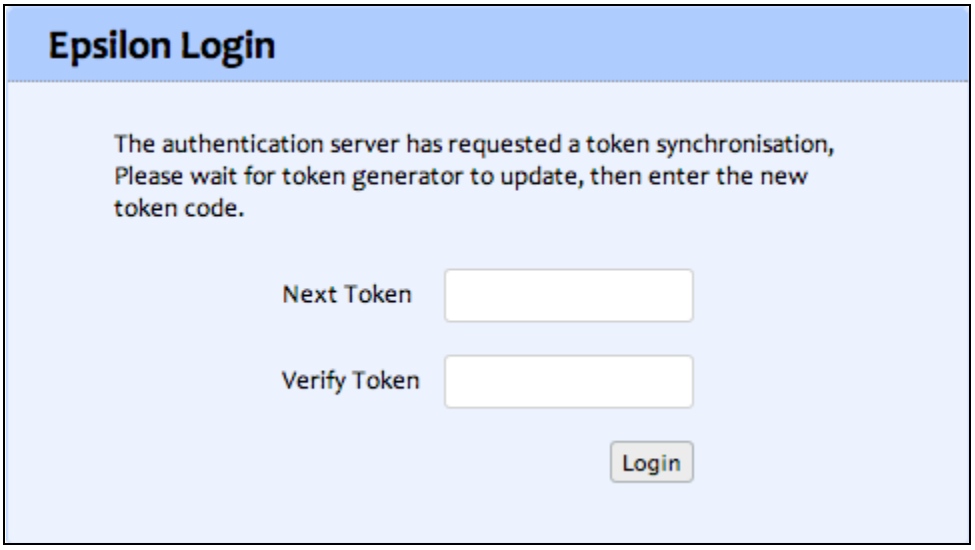
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: August 16th, 2013

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Idea Device Epsilon	2.3	Linux Debian 6

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

JJO / PAR

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

Appendix

Partner Integration Details	
RSA SecurID API	RSA Authentication Agent API 8.1 SP2 for Java
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	All Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	Yes

Node Secret:

The file resides in the */var/lib/<tomcat>* directory. This file should be owned by user tomcat. To clear the node secret from the Epsilon server, delete the securid file.

sdconf.rec:

The file resides in the */var/lib/<tomcat>* directory. This file is generated by RSA Authentication Server. This file should be owned by user tomcat.

sdopts.rec:

The sdopts.rec file resides in the */var/lib/<tomcat>* directory. This file should be owned by user tomcat.

JAstatus.1:

The JAStatus.1 file resides in the */var/lib/<tomcat>* directory. This file should be owned by user tomcat.