Epic Systems Corporation
Epic Hyperspace

RSA Ready Implementation Guide for SecurID

Last Modified: February 9, 2015

Partner Information

Product Information	
Partner Name	Epic Systems Corporation
Web Site	www.epic.com
Product Name	Hyperspace
Version & Platform	2014 on Windows
Product Description	Integrated Electronic Medical Record Software

Solution Summary

Epic Hyperspace can be configured to use RSA SecurID as a login and re-authentication device to allow for two-factor authentication for system access or to verify certain secured actions, such as signing for procedure orders or dispensing medications from the pharmacy.

RSA Authentication Manager supported features	
Hyperspace 2014	
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 Hyperspace 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	C:\ProgramData\Epic\RSA
Node Secret	C:\ProgramData\Epic\RSA
sdstatus.12	C:\ProgramData\Epic\RSA
sdopts.rec	C:\ProgramData\Epic\RSA

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

Stage the environment

The instructions in this section should be applied to the Epic Workstation's host system.

1. Acquire RSA Authentication Agent SDK version 8.1.3.556 (which includes hotfix AAC-705).
2. Extract the Agent SDK and navigate to the following folder:

   `<extracted_folder>\lib\32bit\nt\Release_MT`

3. Copy the **aceclnt.dll** and **sdmsg.dll** into the following location:

   `C:\Program Files (x86)\Epic\v8.1\Shared Files`

   Important: You must use the 32bit versions of these files.

4. Create the following directory and set the permissions such that Epic Hyperspace users have **Full Control** access.

   `C:\ProgramData\Epic\RSA`

5. Download the sdconf.rec configuration file from your RSA Authentication Manager and copy it to the following directory:

   `C:\ProgramData\Epic\RSA`

6. Open the Windows registry editor and change the path in the following registry key:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Epic Systems Corporation\Hyperspace\RSA Integration\ConfigFilePath`

   To:

   `C:\ProgramData\Epic\RSA`

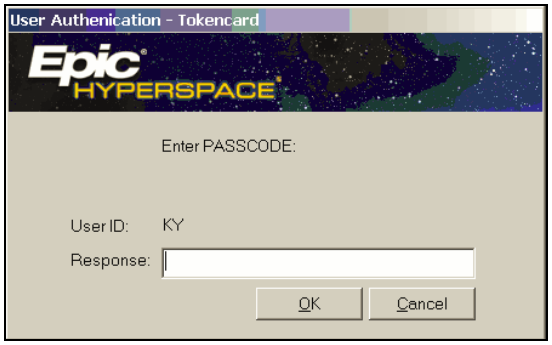
   Note: Create the registry key if it does not already exist. ConfigFilePath should be created as a String Value.

Configure Epic Hyperspace for SecurID Authentication

1. In Epic **System Definitions** (%ZeUSTBL), go to **Security** > **Login Settings** and make sure that the **Login Mode** setting includes the **System Login** option.
2. In **Hyperspace**, go to **Epic** button > **Admin** > **Access Management** > **Authentication Administration**. Select the **default record**, which should appear by default.
3. Configure the **RSA SecurID** (RTM) device for your desired contexts and levels.

RSA SecurID Login Screens

Login screen:



Certification Checklist for RSA Authentication Manager

Date Tested: December 30th, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.1 SP1	Virtual Appliance
RSA Authentication Agent Library	8.1.3.556	Windows Server 2008 R2 x64
Hyperspace	2014	Windows Server 2008 R2 x64

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

PEW/PAR

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

Known Issues

System Generated PINs

System generated PINs longer than 5 characters are trimmed to 5 characters. If the PIN policy is set so that a system generated PIN is longer than 5 characters, the end user will not know the last character(s) of their PIN. The system generated PIN will therefore be unusable. This condition is caused by a bug in the RSA Agent API and will be addressed in an upcoming hotfix.

On Demand Authentication new PIN

After setting a new On Demand PIN, the user should be prompted to enter their On Demand PIN and tokencode. Instead the user will get the error message “Unsuccessful authentication attempt: Next Passcode require”. All subsequent authentications with the new PIN will function as expected.

Appendix

Partner Integration Details	
RSA SecurID API	8.1.3.556 C API (32-bit)
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	Yes

Node Secret:

The node secret file (securid) is located in C:\ProgramData\Epic\RSA. This file is automatically downloaded from the RSA Authentication Manager server during the first authentication.

sdconf.rec:

The sdconf.rec file is located in C:\ProgramData\Epic\RSA.

sdopts.rec:

The sdopts.rec file is located in C:\ProgramData\Epic\RSA. This optional file is used to manually specify IP override and server load balancing.

sdstatus.12:

The sdstatus.12 file is located in C:\ProgramData\Epic\RSA. This file is automatically created and updated during the normal course of SecurID operations.