RSA Ready Implementation Guide for

RSA SecurID

Epic Hyperspace 2016

Peter Waranowski, RSA Partner Engineering
Last Modified: September 12th, 2016

RSA READY

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	
Epic Hyperspace 2016	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	Yes
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
RSA SecurID Authentication via IPv6	Yes
On-Demand Authentication via Native SecurID UDP Protocol	Yes
On-Demand Authentication via Native SecurID TCP Protocol	Yes
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No

RSA Authentication Manager Configuration

Agent Host Configuration

To facilitate communication between Epic Hyperspace and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the Epic Hyperspace and contains information about communication and encryption.

RSA Authentication Manager 8.0 introduced a new TCP-based authentication protocol and corresponding agent API. RSA Authentication Manager 8.0 and newer also maintains support for the existing UDP-based authentication protocol and agents. The agent host records for TCP and UDP agents are configured similarly, but there are some important differences.

Include the following information when configuring a UDP-based agent host record.

- Hostname
- IP addresses for network interfaces

> **! Important: The UDP-based authentication agent's hostname must resolve to the IP address specified.**

Include the following information when configuring a TCP-based agent host record.

- RSA agent name (in the hostname field)

> **! Important: The RSA agent name is specified in the rsa_api.properties file.**

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 Epic Hyperspace will occur.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Epic 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 Epic 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

Epic Hyperspace 2016 should be able to integrate using UDP-based SecurID agent (8.1.x) or TCP-based SecurID agent (8.5+), however, certification testing was only performed using agent 8.6. If you wish to integrate using the UDP-based agent, follow the instructions in the RSA Ready SecurID implementation guide for Epic Hyperspace 2014.

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

1. Acquire RSA Authentication Agent SDK version 8.6.
2. Extract the Agent SDK and navigate to the following folder:

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

3. Copy these following files:

   ```
   aceclnt.dll
   aceclnt_tcp.dll
   ccme_asym.dll
   ccme_base.dll
   cryptocme.dll
   cryptocme.sig
   sdmsg.dll
   xeres-c_3_1_vc80.dll
   ```

   into this location:

   ```
   C:\Program Files (x86)\Epic\v8.3\Shared Files
   ```

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

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

   ```
   C:\ProgramData\Epic\RSA
   ```

5. Copy the **rsa_api.properties** file from the <extracted_folder>\samples directory in the SDK to this directory.

   ```
   C:\ProgramData\Epic\RSA
   ```

6. Add the following lines to the **rsa_api.properties** file and save/close it.

```
RSA_AGENT_NAME = <agent_name>
SDCONF_LOC = C:\ProgramData\Epic\RSA\sdconf.rec
RSA_CONFIG_DATA_LOC = C:\ProgramData\Epic\RSA
RSA_BSAFE_LIBRARY_PATH = C:\Program Files (x86)\Epic\v8.3\Shared Files
```

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

```
C:\ProgramData\Epic\RSA
```

8. Open the Windows registry editor and change the path in this 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: September 7th, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.2	Virtual Appliance
RSA Authentication Agent SDK	8.6	Windows Server 2008 R2
Epic Hyperspace	2016	Windows Server 2008 R2

RSA SecurID Authentication

Date Tested: September 7th, 2016

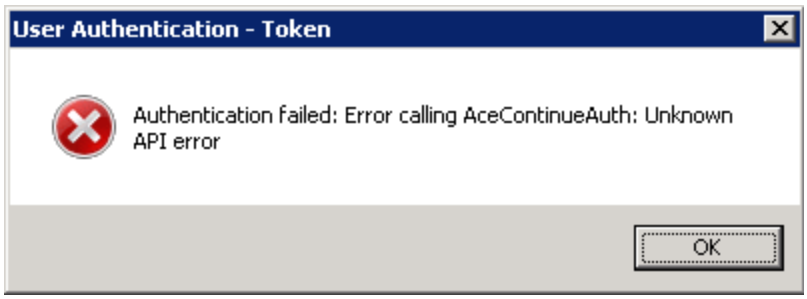
Mandatory Functionality	Native UDP	Native TCP	RADIUS Client
New PIN Mode			
Force Authentication After New PIN	N/A	✓	N/A
System Generated PIN	N/A	✗*	N/A
User Defined (4-8 Alphanumeric)	N/A	✓	N/A
User Defined (5-7 Numeric)	N/A	✓	N/A
Deny 4 and 8 Digit PIN	N/A	✓	N/A
Deny Alphanumeric PIN	N/A	✓	N/A
Deny 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

**See Known Issues section for more information

Known Issues

System Generated PIN w/ TCP-based agent – When integrated with a TCP-based agent, and there is a system-generated PIN policy in place, Hyperspace will throw an error during the new PIN authentication flow.



Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	C:\ProgramData\Epic\RSA\
sdopts.rec	C:\ProgramData\Epic\RSA\
Node secret	C:\ProgramData\Epic\RSA\
sdstatus.12 / jastatus.12	C:\ProgramData\Epic\RSA\
TCP Agent Files	**Location**
rsa_api.properties	C:\ProgramData\Epic\RSA\
sdconf.rec	C:\ProgramData\Epic\RSA\
sdopts.rec	C:\ProgramData\Epic\RSA\
Node secret (optional)	C:\ProgramData\Epic\RSA\

Partner Integration Details

Partner Integration Details	
RSA SecurID UDP API	8.1.3 build 556 (or newer)
RSA SecurID TCP API	8.6
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	All Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	Yes, using agent