kCura Corporation
Relativity

RSA SecurID Ready Implementation Guide

Last Modified: December 3rd, 2015

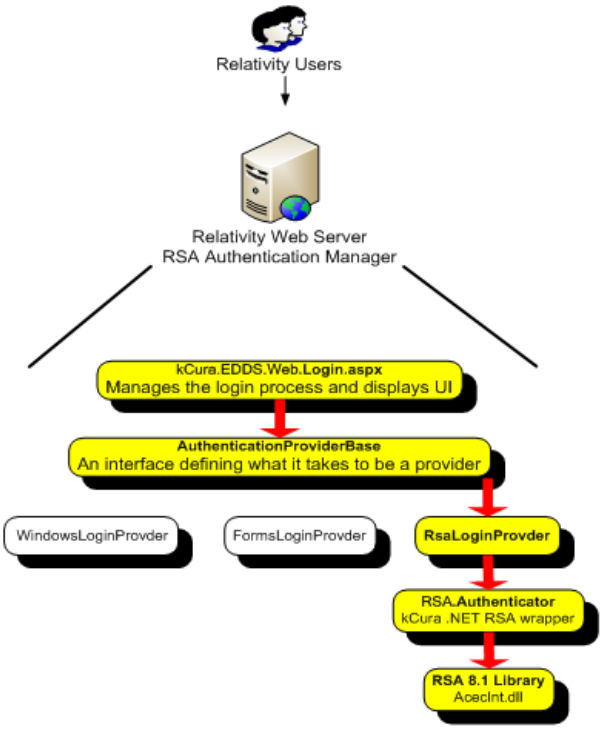
Partner Information

Product Information	
Partner Name	kCura Corporation
Web Site	www.kcura.com
Product Name	Relativity
Version & Platform	9.3 for Windows
Product Description	kCura's Relativity is a document review solution designed for simple and complex litigation. A feature-rich, online review application, Relativity provides you with image and native file review, powerful searching, diverse coding options, strong work-flow management tools, flexible security options, and full-production capabilities, all in a highly scalable solution.

Solution Summary

kCura Relativity utilizes RSA SecurID as one of its authentication methods to allow secure access to the system. Relativity interacts with the RSA Authentication Agent installed on the same web server as Relativity to communicate with the RSA Authentication Manager during the authentication process if the user is set to authenticate with RSA. This setting is made on a per-user basis in Relativity and details are included in this document.

RSA Authentication Manager supported features	
kCura Relativity 9.3	
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
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	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



Agent Host Configuration

To facilitate communication between kCura Relativity 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 kCura Relativity and contains information about communication and encryption.

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

- Hostname
- IP addresses for network interfaces

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

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 kCura Relativity will occur.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring kCura Relativity 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 kCura Relativity components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring Relativity for SecurID Authentication

In order to enable SecurID authentication for kCura Relativity users, the following steps must be completed:

- Copy RSA Authentication Manager Configuration Files to Relativity Server
- Associate kCura users with RSA users

Copy RSA Authentication Manager Configuration Files to Relativity Server

1. Download the **sdconf.rec** configuration file from the RSA Authentication Manager Security Console.
2. Copy the **sdconf.rec** and optional sdopts.rec file(s) to the RSAConfigFilePath directory. The default location is below:

```
%SYSTEMDRIVE%\Program Files\kCura Corporation\Relativity\EDDS\RSA
```

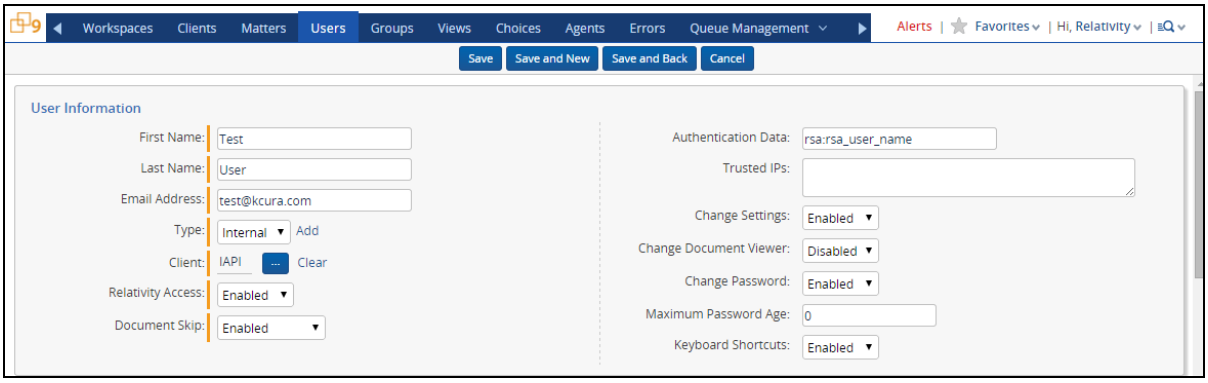
> **Note: This location can be changed by setting the RSAConfigFilePath configuration value in the EDDS database.**

3. Verify that the user **DOMAIN\EDDSServiceAccount** (the account that the Relativity application pool runs as) has **WRITE** permission to the RSAConfigFilePath directory.

> **Important: Make sure the above considerations are made before proceeding with configuration of the kCura Relativity software.**

Associate kCura Users with RSA Users

1. Log in to Relativity as an Administrator, click the **Admin link** to the upper right, and then click the **Users** tab.
2. Click the **New User** button to create a user or click the **Edit** link associated with a user to edit an existing user.
3. In the User view, set the **Authentication Data** field to the value "**RSA:**" followed by the appropriate RSA user's Default Login field.

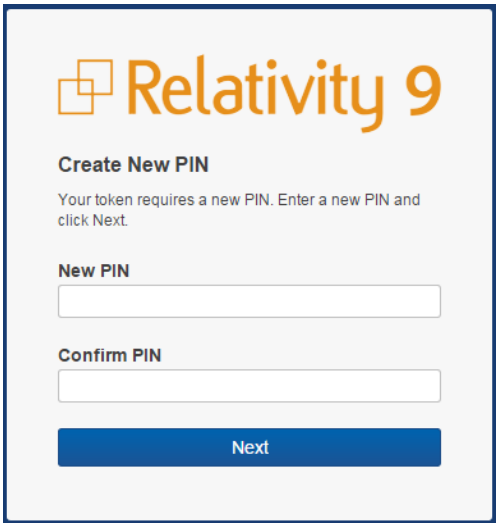


For example, the screenshot above illustrates a user with an email address of test@kcura.com (which is used to log in to Relativity) and the user's Authentication Data field set to the value "RSA:rsa_user_name." This indicates that this user should be authenticated with RSA SecurID using the RSA user with a Default Login value of "rsa_user_name" and any tokens associated with that user. This user would then authenticate to Relativity with a username of test@kcura.com and the appropriate passcode for the RSA user with Default Login rsa_user_name.

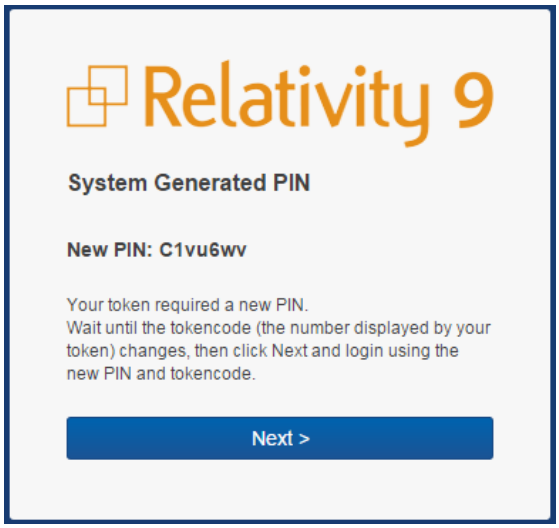
RSA SecurID Login Screens

Login screen:

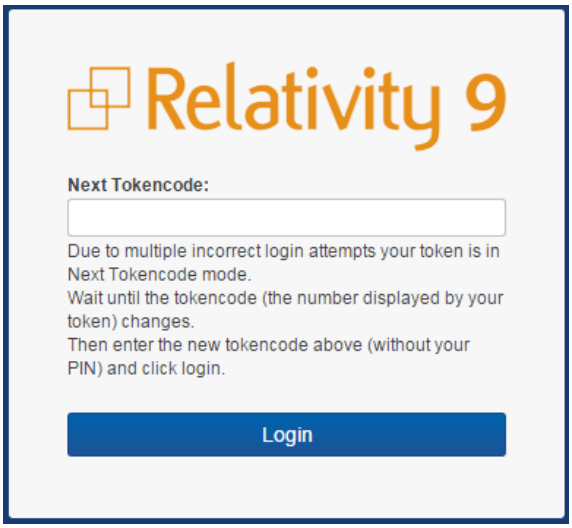
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1 SP1	Virtual Appliance
kCura Relativity	9.3	Windows Server 2008 R2

RSA SecurID Authentication

Date Tested: December 3rd, 2015

Mandatory Functionality	RSA Native UDP Agent	RSA Native TCP Agent	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

PEW / PAR

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

Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	%SYSTEMDRIVE%\Program Files\kCura Corporation\Relativity\EDDS\RSA
sdopts.rec	%SYSTEMDRIVE%\Program Files\kCura Corporation\Relativity\EDDS\RSA
Node secret	%SYSTEMDRIVE%\Program Files\kCura Corporation\Relativity\EDDS\RSA
sdstatus.12 / jastatus.12	%SYSTEMDRIVE%\Program Files\kCura Corporation\Relativity\EDDS\RSA
TCP Agent Files	**Location**
rsa_api.properties	N/A
sdconf.rec	N/A
sdopts.rec	N/A
Node secret	N/A

Partner Integration Details

Partner Integration Details	
RSA SecurID UDP API	8.1
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	Yes
Agent Tracing	Yes

Node Secret:

To remove the Node Secret, delete the securid file from the file system and restart the kCura software.

sdconf.rec:

To install the sdconf.rec file, copy the sdconf.rec file to the file system and start the kCura software.

sdopts.rec:

To install the sdconf.rec file, copy the sdconf.rec file to the file system and start the kCura software.

sdstatus.12:

The sdstatus.12 file will be created upon first successful authentication in the same directory as the node secret, sdconf.rec and optionally the sdopts.rec files.

Agent Tracing:

Agent tracing may be enabled either through System Environment Variables or the Windows Registry. Consult RSA Agent and/or SDK documentation for more information on agent tracing.