Openstream Inc.

Cue-me Device Manager

CERTIFIED SECURED BY RSA PARTNER

RSA Adaptive Authentication Implementation Guide

Last Modified: Monday, May 06, 2013

Partner Information

Product Information	
Partner Name	Openstream Inc
Web Site	www.openstream.com
Product Name	Cue-me Device Manager
Version & Platform	2.x, Windows, MAC, Unix and Linux
Product Description	Cue-me Device manager provides the device manager for Cue-me clients along with managing the application access to the users.

Openstream®
Making Communications Smarter

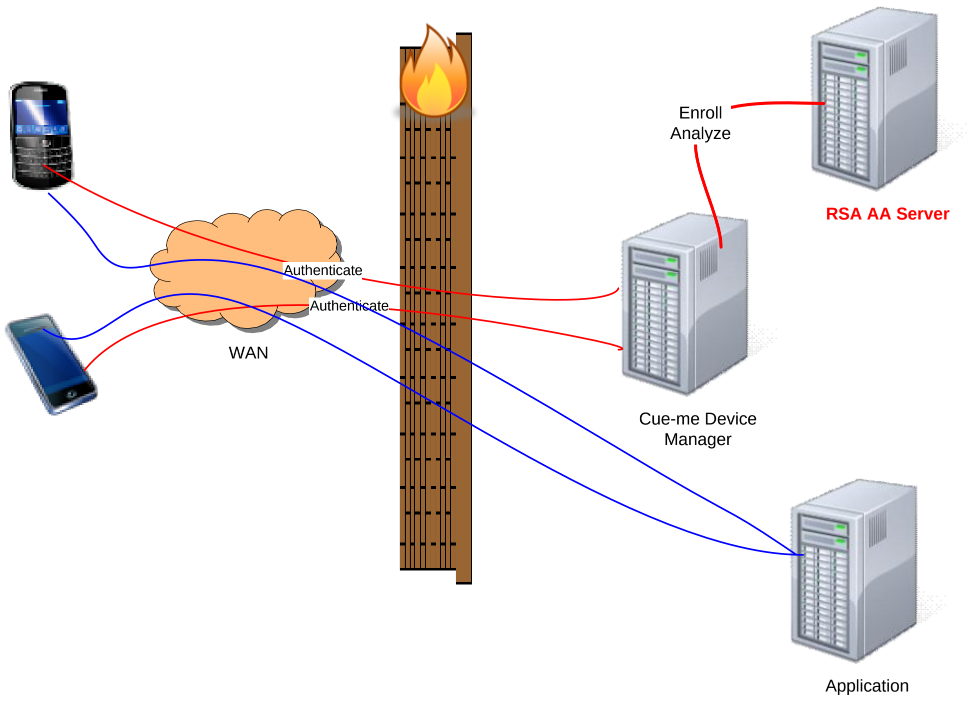
RSA

EMC²

Solution Summary

Cue-me Device Manager provides mobile device management using Cue-me clients. At this time it makes sure the device/user association is proper and makes sure when another user is using the same device proper usage restrictions are enabled based on user credentials. Cue-me DM by integrating into RSA Adaptive Authentication can also evaluate the user risk profile during authentication process. This is required in some financial environments as sensitive information is accessed.

RSA Adapted Authentication supported features	
Cue-me Device Manager 2.1	
RSA Adaptive Authentication Hosted	No
RSA Adaptive Authentication On-Premise	Yes
RSA Adaptive Authentication User Enrollment	Yes
RSA Adaptive Authentication Login Authentication	Yes
RSA Adaptive Authentication Transaction Monitoring	No
RSA Adaptive Authentication Web/Mobile Browser Data Collection	No
RSA Adaptive Authentication Mobile Channel Data Collection	Yes
User Challenge Questions	Yes
Knowledge-based Authentication	No
Site-to-User Authentication	No
Out-of-Band Phone Authentication	No
Out-of-Band Email Authentication	No
Out-of-Band SMS Authentication	No



Partner Product Configuration

Before You Begin

This section provides instructions for configuring Cue-me Device Manager with RSA Adaptive Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of the 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.

Integrating Cue-me Device Manager with RSA Adaptive Authentication

Device Manager supports both RSA AA On Premise 6.0 and RSA AA On Premise 7.0 servers. It can, however, only communicate with one server at a time. Configure the server type and connection settings in the dmserver.properties file on the Device Manager server.

Add the configuration below to enable RSA Adaptive Authentication integration with Cue-me Device Manager:

Configure Cue-me Device Manager with RSA AAOP 6.0

Add the following lines to the dmserver.properties file on your Cue-me Device Manager server:

```
# RSA AA Service Provider
custom.rsa.event.hook=com.openstream.dm.auth.rsa.provider.RSAAuthService6

# RSA AA server URL
rsa.server.url=http://My_AAOP_Hostname/AdaptiveAuthentication/services/Adaptive
Authentication

# RSA AA server caller id
rsa.server.caller.id=My_AAOP_CallerId

# RSA AA server caller password
rsa.server.caller.password=My_AAOP_CallerCredential
```

Configure Cue-me Device Manager with RSA AAOP 7.0

Add the following lines to the dmserver.properties file on your Cue-me Device Manager server:

```
# RSA AA Service Provider
custom.rsa.event.hook=com.openstream.dm.auth.rsa.provider.RSAAuthService

# RSA AA server URL
rsa.server.url=http://My_AAOP_Hostname/AdaptiveAuthentication/services/Adaptive
Authentication

# RSA AA server caller id
rsa.server.caller.id=My_AAOP_CallerId

# RSA AA server caller password
rsa.server.caller.password=My_AAOP_CallerCredential
```

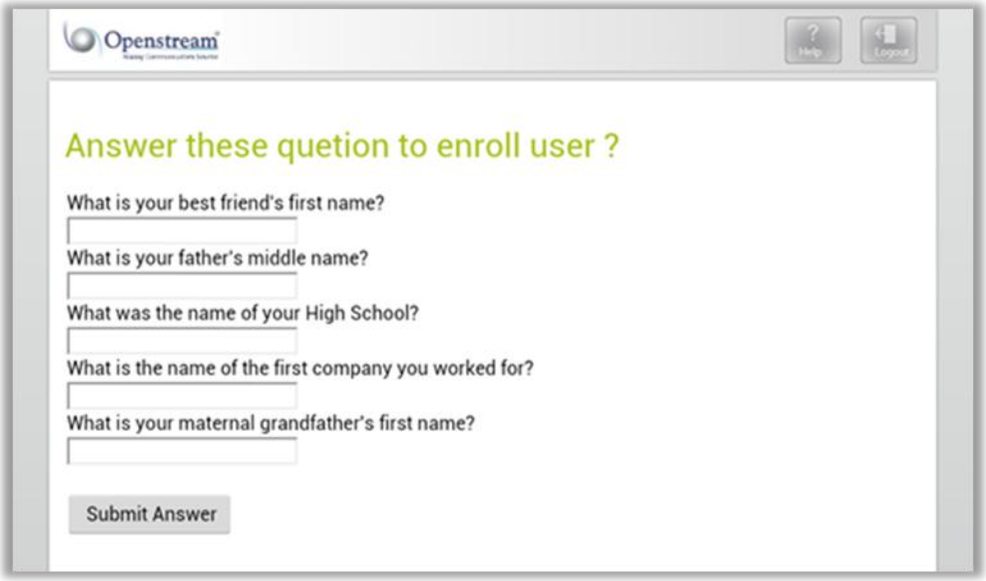
Integrating Cue-me clients with RSA Adaptive Authentication

There is no additional integration work required to enable RSA Adaptive Authentication integration on the Cue-me client. The Cue-me client include the required RSA Adaptive Authentication device collection libraries and integration should be transparent to the users. The UI to be shown can be easily customized to fit the needs of the enterprise.

The Cue-me Device Manager adapts the data retrieved from the mobile SDK for either RSA Adaptive Authentication 6.0 or RSA Adaptive Authentication 7.0 servers. Therefore, clients need not know which servers they are talking to.

Login Screens

User Enrollment Screen:



Answer these quetion to enroll user ?

What is your best friend's first name?

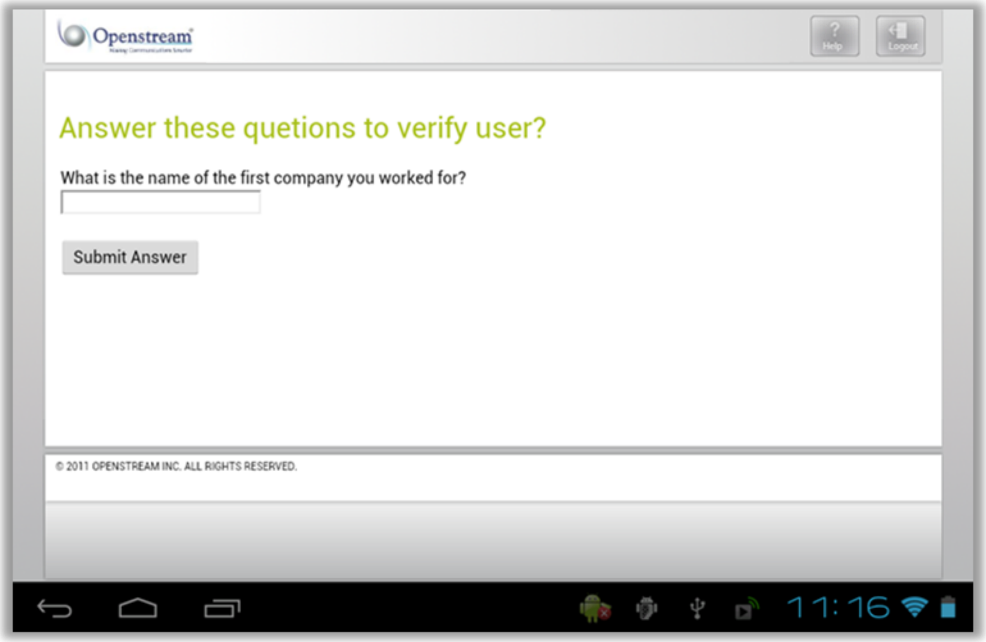
What is your father's middle name?

What was the name of your High School?

What is the name of the first company you worked for?

What is your maternal grandfather's first name?

Challenge Screen:

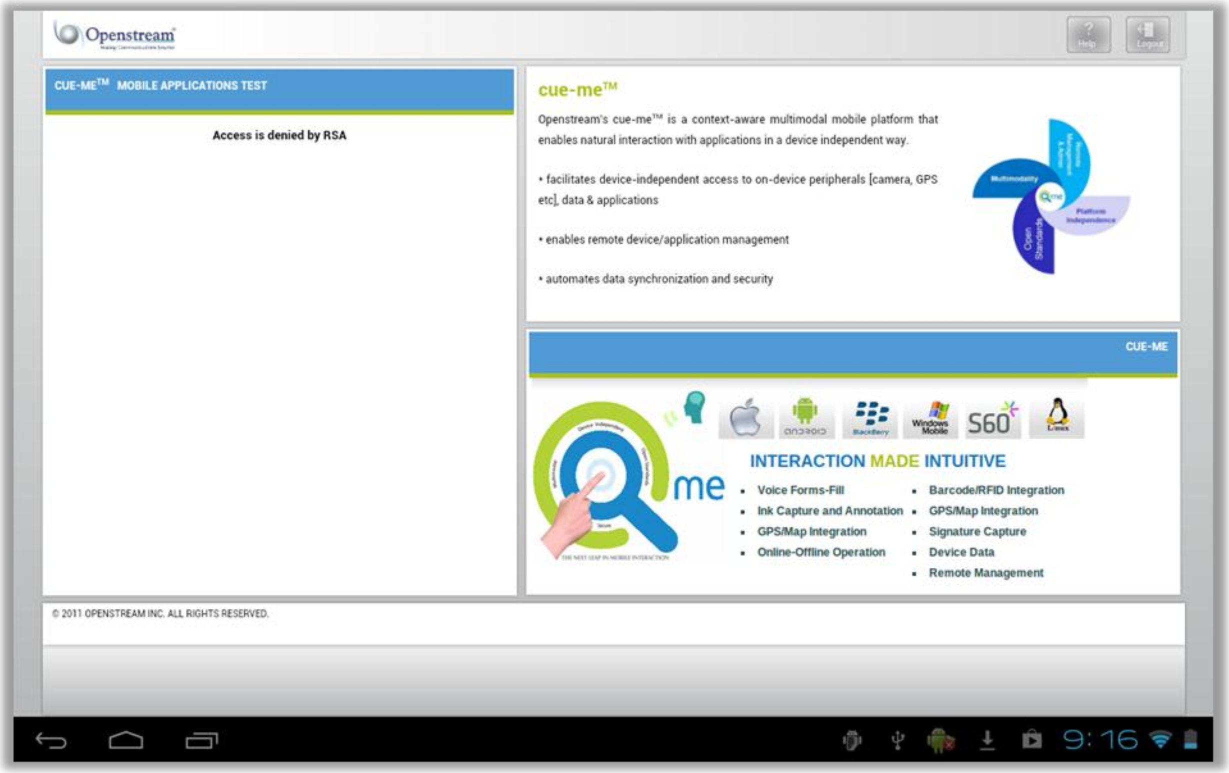


Answer these quetions to verify user?

What is the name of the first company you worked for?

© 2011 OPENSTREAM INC. ALL RIGHTS RESERVED.

Denial Screen:



CUE-ME™ MOBILE APPLICATIONS TEST

Access is denied by RSA

cue-me™

Openstream's cue-me™ is a context-aware multimodal mobile platform that enables natural interaction with applications in a device independent way.

• facilitates device-independent access to on-device peripherals [camera, GPS etc], data & applications

• enables remote device/application management

• automates data synchronization and security

CUE-ME

INTERACTION MADE INTUITIVE

- Voice Forms-Fill
- Ink Capture and Annotation
- GPS/Map Integration
- Online-Offline Operation
- Barcode/RFID Integration
- GPS/Map Integration
- Signature Capture
- Device Data
- Remote Management

© 2011 OPENSTREAM INC. ALL RIGHTS RESERVED.

Certification Checklist for RSA Adaptive Authentication Login

Date Tested: February 26, 2013

Certification Environment		
Product Name	**Version**	**Operating System**
Adaptive Authentication On Premise	7.0	RHEL 5.0
Adaptive Authentication On Premise	6.0.2.1 SP3 P2	RHEL 5.0
Cue-me Device Manager	2.1.0	Linux
Cue-me Client	3.0	Android 4.0

Login Monitoring			
On Premise		**Hosted**	
Analysis			
User Status		**User Status**	
Unknown Bank Users	✓	Unknown Bank Users	N/A
Unenrolled Users	✓	Unenrolled Users	N/A
Unverified Users	✓	Unverified Users	N/A
Deleted Users	✓	Deleted Users	N/A
Locked User Accounts	✓	Locked User Accounts	N/A
Unlocked User Accounts	✓	Unlocked User Accounts	N/A
Verified Users	✓	Verified Users	N/A
Notification		**Notification**	
Updates Server	✓	Updates Server	N/A

Login Authentication			
On Premise		**Hosted**	
Analysis Response Actions		**Analysis Response Actions**	
Allow	✓	Allow	N/A
Review	✓	Review	N/A
Challenge	✓	Challenge	N/A
Deny	✓	Deny	N/A
Challenge Events		**Challenge Events**	
Challenges Unbound Devices	✓	Challenges Unbound Devices	N/A
Challenges High Risk Users	✓	Challenges High Risk Users	N/A

PEW / PAR

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

Checklist for RSA Adaptive Authentication Login (Continued)

Login Authentication (Continued)			
On Premise		**Hosted**	
Authentication Methods		**Authentication Methods**	
User Challenge Questions	✓	User Challenge Questions	N/A
Knowledge-based	N/A	Knowledge-based	N/A
Site-to-User	N/A	Site-to-User	▨
Out of Band Phone	N/A		▨
Out of Band Email	N/A		▨
Out of Band SMS	N/A		▨
External Authentication	N/A		▨
Authentication Policy		**Authentication Policy**	
Locks Account On Failed Attempts	✓	Locks Account On Failed Attempts	N/A
Credential Maintenance		**Credential Maintenance**	
Supports User Credential Maintenance	N/A	Supports User Credential Maintenance	N/A

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

Checklist for RSA Adaptive Authentication Device Data Collection

Mobile Application			
On Premise		Hosted	
Device Data		**Device Data**	
SIM ID	✓	SIM ID	N/A
Hardware ID	✓	Hardware ID	N/A
Other ID	✓	Other ID	N/A
Phone Data		**Phone Data**	
Phone Number	✓	Phone Number	N/A
Country Code	✓	Country Code	N/A
Area Code	✓	Area Code	N/A

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

Checklist for RSA Adaptive Authentication Login Data Collection

Login Monitoring			
On Premise		Hosted	
Failed Login Notification Data		**Failed Login Notification Data**	
User Login ID	✓	User Login ID	N/A
User Type	✓	User Type	N/A

Login Authentication			
On Premise		Hosted	
Enrollment Data		**Enrollment Data**	
Run Risk Action Flag	✓	Run Risk Action Flag	N/A
Device Data	✓	Device Data	N/A
Device Action Type List	✓	Device Action Type List	N/A
Site-to-User Authentication Data		**Site-to-User Authentication Data**	
User Image	N/A	User Image	N/A
User Phrase	N/A	User Phrase	N/A
Notification Data		**Notification Data**	
Auto Create User Flag	N/A	Auto Create User Flag	N/A

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