

RSA Archer eGRC Platform 1.2.0

January 2013

RSA Archer Business Continuity Management Mobile App Overview

The RSA® Archer™ Business Continuity Management (BCM) mobile app provides authorized users on-the-go access to Business Continuity or IT Disaster Recovery (BC/DR) plans. The mobile app establishes a one-way communication to each synchronized mobile digital device, which means data is only downloaded from the BCM solution to the mobile app. For more information, see [Synchronizing the Mobile App](#).

The mobile app allows users to do the following:

- Browse and search BC/DR plans.
- Drill down into recovery strategies, recovery tasks, plan requirements, call trees, and contacts for each plan.
- Connect the mobile app to the RSA® Archer™ Business Continuity Management solution for the most recent updates.

This guide provides administrators and users with the following information about the mobile app:

- **Deploying the Mobile App.** Provides administrators with the requirements for deploying and connecting to the mobile app.
- **Maintaining Security.** Provides administrators with information about how the mobile app keeps data secure
- **Recommendations.** Provides administrators with recommendations for providing full functionality to mobile app users.
- **Using Common Mobile App Functions.** Provides mobile app users with instructions for using the main features available in the mobile app, including synchronizing the mobile app.
- **Receiving and Making Calls.** Provides mobile app users with instructions for receiving and making calls while using the mobile app.

Deploying the Mobile App

The mobile app requires proper connection information that identifies the RSA® Archer™ eGRC Platform as its resource. The mobile app must be installed on a compatible mobile digital device, and have access to the Platform and the correct connection information. For more information, see the following topics:

- [Supported Mobile Digital Devices](#)
- [Supported Platform Version](#)
- [Supplying the Mobile App Resource to Mobile Digital Devices](#)

Supported Mobile Digital Devices

The mobile app runs on mobile digital devices with Apple iOS versions 5.1.1 and later, including:

- iPhone 4 through iPhone 5
- iPod 3rd generation through iPod 5th generation
- iPad 1st generation through iPad 3rd generation

Supported Platform Version

The mobile app is only compatible with the Platform version 5.3 or later.

Supplying the Mobile App Resource to Mobile Digital Devices

The uniform resource identifier (URI) scheme provides an easy, convenient way for Platform administrators to download resource information from the Platform instance to mobile digital devices. The connection is made through a URI scheme that only the mobile app recognizes. When a user taps the link to the URI scheme on the mobile digital device, the mobile app launches and automatically populates the configuration settings specified for the Platform instance through the query part of the URI scheme.

The query part is optional and contains a sequence of <key>=<value> pairs separated by an ampersand. The following example describes the syntax in the query part of a URI scheme. In this example url={Archer URL}, domain={Archer Domain}, and company={Company} are <key>=<value> pairs:

```
ar cher - bcm / / ?ur l={ Ar cher URL} &domai n={ Ar cher Domai n} &company={ Company}
```

The following <key>=<value> pairs are optional:

- **url.** The URL to the Platform instance, for example https://myserver.com/Archer
- **domain.** The authentication domain of the user, if required
- **company.** The Platform instance to authenticate against, for example, 50000

To create the query part of a URL scheme, insert the appropriate information where the placeholders appear in the preceding example. Provide a link to the URI scheme in an email or on a web page.

Maintaining Security

The mobile app ensures that data is protected while residing on mobile digital devices.

- All data is encrypted using a unique key that is different for every mobile app user.
- After three failed logon attempts, the mobile app locks the user out for 10 minutes. Additional failed attempts follow the same process.
- If a user updates the Platform instance configuration settings in the mobile app after completing the initial setup, the mobile app validates any changes to the user credentials. If a user changes any credentials other than password, all existing BCM solution data in the mobile app is permanently erased.
- If a user forgets the password in the mobile app, the user cannot access the mobile app. The user must uninstall the mobile app and repeat the setup process.

- If the user password is changed in the Platform, the password is not changed in the mobile app until the user synchronizes the mobile app. For more information, [Synchronize the Mobile App](#).
- RSA Archer recommends that a Mobile Device Management (MDM) software solution is used to ensure the highest degree of security and sensitivity for the content displayed in the mobile app.

Recommendations

This section includes recommendations for ensuring certain conditions are avoided in the mobile app.

Do Not Remove Tracking ID Fields

If any Tracking ID-type fields are removed from the solutions or applications in the Platform or users do not have permission to see any of the following applications, the mobile app will not function properly:

- BC/DR Plans
- Recovery Strategies
- Recovery Tasks
- Emergency Notifications
- Requirements
- Contacts

Do Not Remove Other Important Fields

If any of these fields are removed from the solutions or applications in the Platform or users do not have permissions to the fields, the text “[empty]” is displayed in the mobile app:

- BC/DR Plans: Plan Name
- Recovery Strategies: Strategy Name
- Recovery Tasks: Task ID, Recovery Task Overview, and Task Order Number
- Emergency Notifications: Notification Title
- Requirements: Requirement Type and Name
- Contacts: First Name and Last Name

Do Not Remove Access to Required Applications

If users do not have access to the following applications, that application is not available in the mobile app.

- BC/DR Plans
- Recovery Strategies
- Recovery Tasks
- Emergency Notifications
- Requirements
- Contacts

Note: If a user does not have access to the Business Continuity Management solution, the solution is not available in the mobile app and the BC/DR plan records will not exist on the mobile digital device for that user.

Do Not Forget RSA Archer Web API Access Rights

If users do not have the read-only access rights to Web Services API, the mobile app does not function. The mobile app uses the Web Services API to communicate with the RSA Archer Web application.

Using Common Mobile App Functions

The mobile app contains multiple functions designed to help track data and contacts. For more information, see the following topics:

- [Synchronize the Mobile App](#)
- [Expand or Collapse Truncated Fields](#)
- [Adjust Font Size](#)
- [Search Plans](#)

Synchronizing the Mobile App

Before working with the mobile app the first time, you must synchronize the mobile app to the BCM solution.

After the initial synchronization, you must synchronize each time there is a change to the user profile (other than password) and when a plan changes in the BCM solution.

The synchronization process automatically updates all plans and related data. If connection cannot be established, the mobile app automatically retries to connect. Data is only downloaded from the BCM solution to the mobile app. Data is never uploaded from the mobile app to the BCM solution.

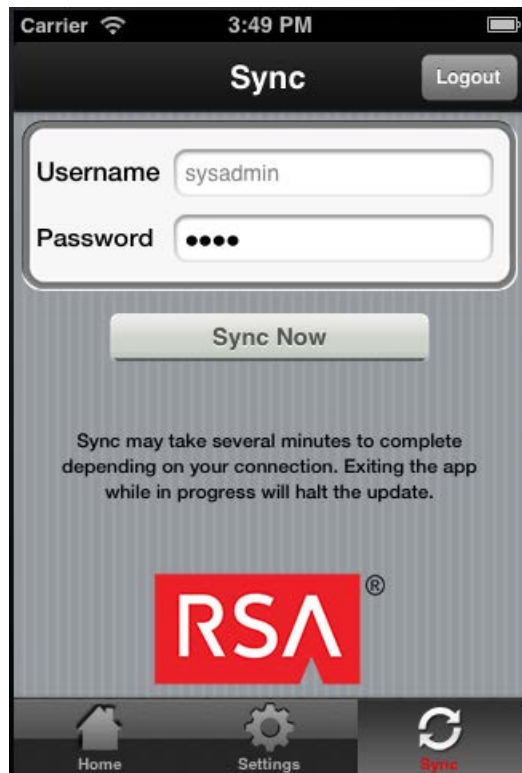
You must provide your current user name and password from your Platform user profile. Your password and user name is not changed in the mobile app until the mobile app is synchronized. If you changed your password on the Platform, you must log on to the mobile app using your old password until you synchronize. After synchronization, use the current user name and password.

Synchronize the Mobile App

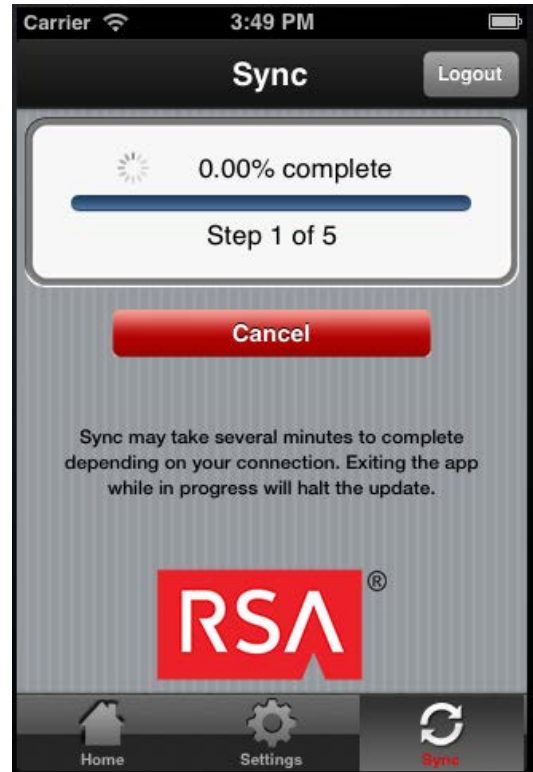
You must synchronize the mobile app to update data stored on the mobile digital device.

1. Tap the **Sync** icon.
2. In **Username**, enter your current **user name**.
3. In **Password**, enter your current **password**.
4. Press **Sync Now** to begin the synchronization.

You are presented with a series of prompts. Answer each prompt according to your current situation. For example, if you are synchronizing through a cell network, you are prompted to confirm that current data rates will apply.



A progress bar is displayed throughout the synchronization process. You may cancel this process at any time. If you cancel, all newly downloaded data is removed, leaving all data previously downloaded intact.



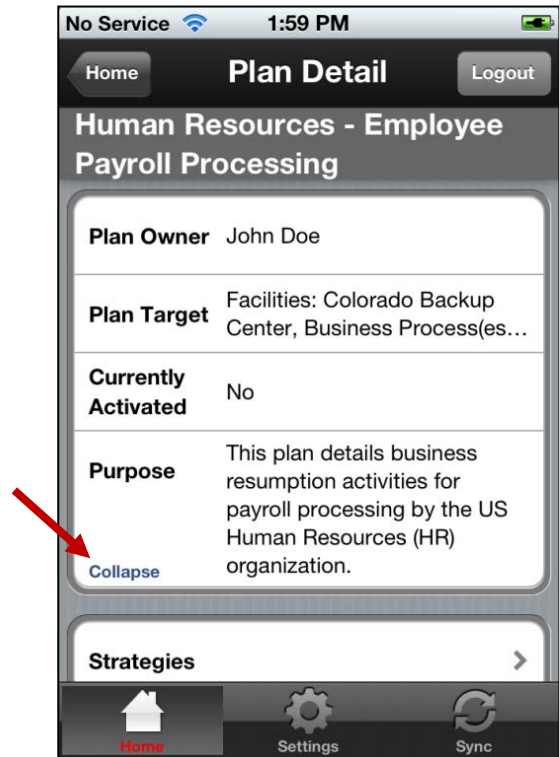
Expand or Collapse Truncated Fields

To give you a better view of all data at a glance, the tables in the mobile app truncate the field data. If information is truncated, an ellipsis (...) is displayed.

- To expand truncated data, tap the field that is truncated for at least one second. Do not scroll while tapping.
- To collapse expanded data, tap **Collapse** or tap the expanded field for one second. Do not scroll while tapping.



This example shows the result of expanding truncated information in the Purpose field.

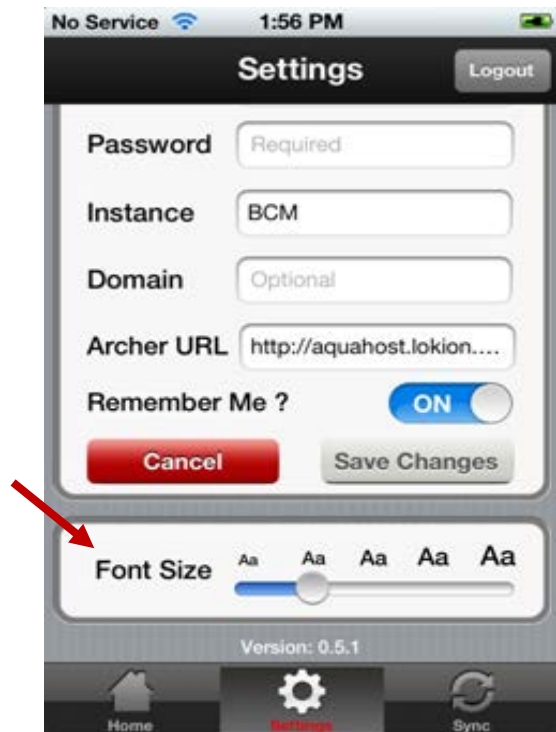


Adjust Font Size

You can adjust the font size for most screens in the mobile app. Five font sizes are available. When you select a new font size, the change is applied immediately to the home screen and all screens for plan details, strategies, tasks, requirements, call trees, and contacts.

Procedure

1. Tap the **Settings** icon.
2. Move the font slider to the appropriate font size.



Search Plans

The list of plans on the home page enables you to search all plans by Plan Name, Plan ID, Currently Activated, Business Owner, Plan Target, or Purpose.

To search for a plan, enter text in the search field and tap the magnifying glass icon.

Receiving and Making Calls

This functionality is only available on mobile digital devices that support phone calls. If this functionality is not supported, the “Not Supported” error alert is displayed when you tap the phone icon. This section includes the following:

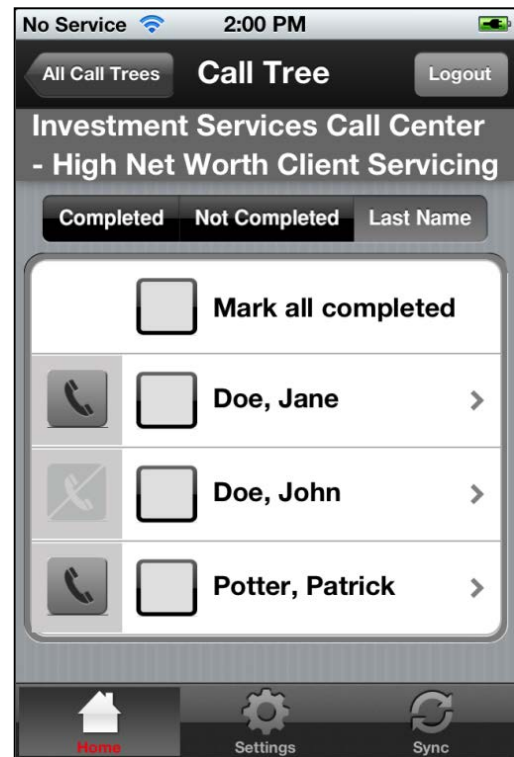
- [Tap to Call](#)
- [Resume after an Interruption or Session Timeout](#)

Tap to Call

You can call any contact in a call tree directly from the mobile app. When you finish the call, you are returned to the screen that you last visited in the mobile app.

To make a call, tap the phone icon on the Call Tree or Call Tree Detail screen.

- If the contact has only one phone number, the mobile app calls that number immediately when you tap the phone icon.
- If the contact has more than one phone number, the mobile app prompts you to choose a number before calling.
- If the contact does not have a phone number listed in the mobile app, the phone icon is disabled.
- After a call is placed, you can mark the check box next to the contact name as completed, indicating the contact was called. This information is for informational purposes only and is not uploaded to the BCM solution.



Resume after an Interruption or Session Timeout

If the mobile app is inactive (idle) for 15 minutes or longer after the initial authentication, you must log on again. This precaution prevents unwanted access to your mobile app.

You can receive calls or notifications while working in the mobile app. In most cases, after an interruption and before the session times out, you are returned to the last screen in the mobile app that you were viewing before the interruption.

Support and Service

Customer Support Information	www.emc.com/support/rsa/index.htm
Customer Support E-mail	archersupport@rsa.com
RSA Archer Community	https://community.emc.com/community/connect/grc_ecosystem/rsa_archer
RSA Archer Exchange	https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange
RSA Solution Gallery	https://gallery.emc.com/community/marketplace/

The Community enables collaboration among eGRC clients, partners, and product experts. Members actively share ideas, vote for product enhancements, and discuss trends that help guide RSA Archer product roadmap.

The Exchange is an online marketplace dedicated to supporting eGRC initiatives. The Exchange brings together on-demand applications along with service, content, and integration providers to fuel the success of RSA Archer clients.

The RSA Solution Gallery provides information about third-party hardware and software products that have been certified to work with RSA products. The gallery includes Secured by RSA Implementation Guides with step-by-step instructions and other information about interoperation of RSA products with these third-party products.

Copyright © 2013 EMC Corporation. All Rights Reserved. Published in the USA.

Trademarks

RSA, the RSA Logo, RSA Archer, and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

iPad and iPhone are trademarks of Apple Inc., registered in the U.S. and other countries.