Radia Client Automation Enterprise

For the Windows®, Android, and iOS operating systems

Software Version: 9.00

Mobile Device Management User Guide

Document Release Date: April 2013

Software Release Date: June 2013

Legal Notices

Warranty

The only warranties for products and services are set forth in the express license or service agreements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Persistent Systems shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Persistent Systems or its licensors required for possession, use or copying. No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Persistent Systems.

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Android™ is a trademark of Google Inc.

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

Intel® is a trademark of Intel Corporation in the U.S. and other countries.

IOS is a registered trademark of Cisco in the U.S. and other countries and is used under license by Apple.

Microsoft®, Windows®, Windows® XP, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.

Acknowledgements

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software written by Daniel Stenberg (daniel@haxx.se).

This product includes OVAL language maintained by The MITRE Corporation (oval@mitre.org).

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://support.persistentsys.com/

This site requires that you register for a Persistent Passport and sign in. Register online at the above address.

For more details, contact your Persistent sales representative.

Support

Persistent Software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by being able to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Submit enhancement requests online
- Download software patches
- Look up Persistent support contacts
- Enter into discussions with other software customers
- Research and register for software training

To access the Self-solve knowledge base, visit the Persistent Support home page.

Note: Most of the support areas require that you register as a Persistent Support user and sign in. Many also require an active support contract. More information about support access levels can be found on the Persistent Support site.

To register for a Persistent Support ID, go to: Persistent Support Registration.

Disclaimer for PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

Note: Some topics do not convert properly to PDF, causing format problems. Some elements of online help are completely removed from the PDF version. Those problem topics can be successfully printed from within the online help.

Contents

Chapter 1

Managing Mobile Devices

Radia Client Automation (RCA) is a real-time, policy-based, desired state management client management solution that automates the administrative tasks for the physical and virtual clients devices in highly complex and ever changing environments. The client devices can be a desktop, laptop, virtual device, or a mobile device. A mobile device can either be a smartphone or a tablet. RCA supports only Android and iOS operating system-based devices. For more information on the supported operating system, see the Radia Client Automation Support Matrix available at: http://support.persistentsys.com/. For more details, contact your Persistent Support representative.

Using RCA, you can perform various Mobile Device Management (MDM) tasks, such as software management, inventory management, and security management. This chapter provides information on how you can set up RCA servers for MDM, notify end-user for the agent application download, and publish and deploy mobile applications. This chapter also describes the steps to create mobile device security profiles, such that you can protect mobile devices in your environment from unauthorized access.

Abbreviations and Variables

Abbreviations Used in this Guide

Abbreviation	Definition
APNS	Apple Push Notification service
Core and Satellite	RCA Enterprise environment consisting of one Core server and one or more Satellite servers.
CSDB	Configuration Server Database
GCM	Google Cloud Messaging
RCA	Radia Client Automation
MDM	Mobile Device Management

Variables Used in this Guide

Variable	Description	Default Values
InstallDir	Location where the RCA server is installed	For a 32-bit operating system: `C:\Program Files\Hewlett-Packard\HPCA` For a 64-bit operating system: `C:\Program Files(x86)\Hewlett-Packard\HPCA`
SystemDrive	Drive label for the drive where the RCA server is installed	C:

Configuring RCA Servers for MDM

Complete the pre-configuration, configuration, and post-configuration tasks listed in this section to set up MDM capabilities on RCA Core and Satellite servers.

Pre Configuration Tasks

Before configuring RCA servers for MDM, you must complete the following tasks, based on the type of devices you plan to manage using RCA:

Managing Android devices

- Open the required ports on the RCA Core and Satellite servers. For more information on the ports that you must enable, see the *Radia Client Automation Enterprise Installation and Upgrade Guide*.
- You must have a valid Google account. This must be an active account and Google services, such as email or chat must have been used at least once using this account on the device.
- You must have a valid Google project number and API key. To obtain these credentials, follow the steps listed on the Google website at http://developer.android.com/guide/google/gcm/gs.html. These details are required to use the Google Push Notification services to send notification requests to the mobile device.
- You must enable the Google Cloud Messaging (GCM) for Android service. To enable this service, follow the steps listed on the Google website at http://developer.android.com/guide/google/gcm/gs.html#gcm-service.

Managing iOS devices

- Open the required ports on the RCA Core and Satellite servers. For more information on the ports that you must enable, see the *Radia Client Automation Enterprise Installation and Upgrade Guide*.
- You must have one or more full-service Satellite servers in your RCA infrastructure that are accessible from the Internet.
- You must have a SCEP server configured in your environment for a single challenge password, that does not expire. This password is required by RCA servers to authenticate the mobile devices that connect to the Apple servers.
  To implement SCEP on a Microsoft Windows 2008 server, see the Microsoft website at http://www.microsoft.com/en-us/download/details.aspx?id=1607.
- You must have OpenSSL version 0.9.8r or above installed in your environment.
- You must obtain an APNS certificate, also known as MDM certificate. RCA uses the APNS certificate to communicate with the iOS devices. Complete the following steps to generate the APNS certificate:
  a. Create a CSR using OpenSSL. Open command prompt and run the following command:
  `openssl req -new -newkey rsa:2048 -out cert.csr -config "path_openssl.cfg"`
  In this instance, *path_openssl.cfg* is the path for the OpenSSL configuration file `openssl.cfg`, which is available at the location where you installed OpenSSL.
  When you run this command, OpenSSL prompts you to provide values for a few fields, such

as Country Name, Locality Name, and Organization Name. Make sure that these fields are not left blank and you provide values that are specific to your organization. The above command generates a CSR `cert.csr` and a private key `privateKey.pem`.

b. Email this CSR to Persistent at rcamobility@persistent.co.in. Persistent then provides you with a base-64 encoded file that contains the property list.

c. Log on to the Apple Push Certificates Portal at https://identity.apple.com/pushcert using your Apple ID. It is recommended that you log on to this web page using the Safari web browser.

d. Click **Create a Certificate**.

e. Click **Choose File** and browse to the property list file that you received from Persistent, and then click **Upload**. After you successfully upload the file, Apple generates the APNS certificate that you can view under Certificates for Third-Party Servers.

f. Click **Download** to download the signed MDM certificate. The certificate is in the `.pem` format. You must convert this certificate to the `.p12` format. To convert the certificate in `.pem` format to a certificate in `.p12` format, open the command prompt and run the following command:
`openssl pkcs12 -export -out <cert.p12> -inkey <privateKey.pem> -in <cert.pem>`
In this instance,
   - *cert.p12* is the certificate file in `.p12` format that OpenSSL generates. You must provide the complete path where this file must be stored.
   - *privateKey.pem* is the key that you obtained while generating the CSR. You must provide the complete path where this key is stored.
   - *cert.pem* is the certificate you downloaded from the Apple website. You must provide the complete path where this file is stored.When you run this command, OpenSSL prompts you for a password. Make sure that you do not provide a blank password. This password is required when you set up Satellite servers for MDM.

   Save a copy of this certificate on each Satellite server that you want to use for MDM.

Configuring RCA Servers for Android Devices

RCA uses the Google Cloud Messaging (GCM) service to send connection requests from the RCA servers to the Android-based mobile devices. The requests are first sent to the Google servers, and then the Google servers forward these messages to the mobile devices. For more information on GCM, see the Google web site at http://developer.android.com/guide/google/gcm/index.html.

Complete the following steps to configure the RCA servers to use the Google servers for sending notifications to the Android device users:

1. Log on to the RCA Core Console and click **Configuration** tab.
2. Expand Mobile Management, click **Vendor Configuration**, and then click **Android**. The

Notification Settings view opens in the details pane.

3. Enter the details for the following fields and click **Save**:

Field	Description
GCM API Key	The API key provides RCA servers authorized access to Google services. Enter the API key for server apps that you received when you configured API access on the Google APIs Console page at https://code.google.com/apis/console. A sample GCM API Key appears as follows: Key for server apps (with IP locking) API key: AIzaSyAS0yrMCGrgdzjbsdc8ZwVnFTyzV6_EB7Q
GCM Project ID	The Project Number is required to validate that the RCA Android application is registered to send messages to the mobile device. Enter the project number that you received as a part of URL when you created your Google API project. For example: 4915162343 in the `https://code.google.com/apis/console/#project:4915162343` URL.

Configuring RCA Servers for iOS Devices

To manage iOS devices, you must complete the following tasks:

1. **"Task 1: Enable SSL" below**
2. **"Task 2: Add MDM Server" below**
3. **"Task 3: Set up MDM Server Properties" on next page**

Note: This document explains the certificate-related procedures—Certificate Signing Request (CSR) generation, certificate conversion, and Apple Push Notification service (APNS) UID creation using OpenSSL on Windows platform.

Task 1: Enable SSL

You must enable SSL on the RCA Satellite server that you will be setting up for MDM. For more information on how to enable SSL on the RCA Satellite server, see the *Radia Client Automation Enterprise SSL Implementation Guide*.

Task 2: Add MDM Server

Full-service Satellite servers are required to manage the iOS mobile devices. Complete the following steps to add an existing full-service Satellite server as an MDM server:

1. Log on to the RCA Core Console and click **Configuration** tab.
2. Expand **Mobile Management** in the left-navigation pane and then click **Vendor Configuration**>**iOS**. The iOS settings page opens.
3. Click **MDM Configuration** tab.

4. Click **Add New MDM Server** icon. The MDM Server Creation Wizard opens.
5. Enter the details for the following fields and click **Save**:

Field	Description
Name	Name of the Satellite server. The Satellite server is referenced using this name on the MDM Configuration page.
Description	Description of the Satellite server.
Full-Satellite Server URL	Select the Satellite server that you want to set up for MDM.

Task 3: Set up MDM Server Properties

After you identify and add the Satellite server that provides the MDM functionality, you must configure the Satellite server properties, such that these servers can process the jobs that an administrator creates for mobile devices.

MDM Satellite Server Settings for APNS

You must configure the APNS settings on each Satellite server set up as MDM server.

Complete the following steps:

1. Open command prompt and run the following command:
   `openssl exe x509 -in <cert.pem> -text`
   In this instance,
   cert.pem is the certificate you downloaded from the Apple website during APNS generation process.
   This command provides a UID that you must add in each MDM Satellite server properties file.
2. Modify the `mdm.properties` file for each Satellite server that you have set up for MDM:
   a. Navigate to the directory `<InstallDir>\tomcat\webapps\mdm\WEB-INF\classes`.
   b. Open the file `mdm.properties` in a text-editor.
   c. Provide the UID that you generated in step 2 of this procedure as the value for the `mdm.Topic` property. For example, if the following output is displayed when you run the command in step 2: `Subject: UID=com.apple.mgmt.External.b66302d9-7fb2-44e7-8a23-6d7b6e9b0b6e, CN=APSP:b66302d9-7fb2-44e7-8a23-6d7b6e9b0b6e, C=IN`, the UID value is `com.apple.mgmt.External.b66302d9-7fb2-44e7-8a23-6d7b6e9b0b6e`. Set the value for the property as `mdm.Topic=com.apple.mgmt.External.b66302d9-7fb2-44e7-8a23-6d7b6e9b0b6e`.
   d. Restart the `HPCA Tomcat Server` service.

MDM Satellite Server Common Properties

Complete the following steps to configure the common properties that are shared across all MDM Satellite servers:

1. Log on to the RCA Core Console and click **Configuration** tab.
2. Expand **Mobile Management** in the left-navigation pane and then click **Vendor Configuration>iOS**. The iOS settings page opens.
3. Enter the details for the following fields and click **Save**:

Field	Description
SCEP Name	The name of the certificate authority that SCEP server uses to issue certificates.
SCEP URL	The URL of the SCEP server. If you have implement SCEP server on Microsoft Windows, enter the URL in the following format: http://*SCEP_hostname*/certsrv/mscep/mscep.dll, where *SCEP_hostname* is the hostname of the SCEP server.
Single Challenge Password	The enrollment challenge password that you obtain from the SCEP server administrator. To obtain password on a SCEP server implemented on Microsoft Windows Server 2008, open the URL http://*SCEP_hostname*/CertSrv/mscep_admin/ in a web browser, where *SCEP_hostname* is the hostname of the SCEP server.
MDM Configuration Profile Name	The name of the profile that a mobile device user views during the device enrollment process. This profile contains details of the SCEP server certificate and the APNS certificate.
Security Configuration Payload Display Name	The name of the security profile. This profile contains details on the security policies that an administrator has applied on the device. Note that end-users cannot remove a security profile that you have entitled to the device.
Security Configuration Payload Description	The description of the security profile.

MDM Satellite Server-Specific Properties

Complete the following steps to configure Satellite-server specific properties:

Note: You can also modify these properties by logging on to the RCA Satellite Console of the Satellite server that you have identified as an MDM server. Click **Configuration** tab, and then click **iOS MDM Settings** in the left-navigation pane.

General Settings

1. Log on to the RCA Core Console and click **Configuration** tab.
2. Expand **Mobile Management** in the left-navigation pane and then click **Vendor Configuration>iOS**. The iOS settings page opens.
3. Click **MDM Configuration** tab.
4. Click the URL for the full-service Satellite server. The Configuration tab view opens.
5. Click **iOS MDM Settings** and then click **General Settings**.
6. Enter the details for the following fields and click **Save**:

Field	Description
Socks Proxy: These settings are required only if your enterprise has blocked the ports required to connect to APNS. You can then route the access to APNS using a SOCKS proxy.	
Socks Proxy Enable	Select if the Satellite server connects to the APNS through a SOCKS proxy server. To send notification messages to mobile devices, Satellite servers require access to the APNS.
Socks Proxy Host	Enter the hostname of the SOCKS proxy server.
Socks Proxy Port	Enter the port number of the SOCKS proxy server.
Key Store: These settings are required to modify the certificate settings that are required to connect the iOS operating system-based devices with APNS.	
Certificate File Path	Specify the path for the root certificate of the certification authority that you used to enable SSL on the Satellite server. Make sure that the certificate is not a self-signed certificate. For example, specify the path in the following format: `C://Certificates//certificate.crt` You must store the certificate locally on the Satellite server.
MDM Certificate Path	Specify the path to the APNS certificate. Make sure that you provide the certificate in `.p12` format. For example, specify the path in the following format: `C://Certificates//certificate.p12` For more information on how to convert a certificate in `.pem` format to `.p12` format, see "Pre Configuration Tasks" on page 10. You must store the certificate locally on the Satellite server.

Field	Description
MDM Certificate Password	Specify the password that you provided while converting the certificate in `.pem` certificate to a certificate in `.p12` format.

Advanced Settings

The MDM server component on the full-service Satellite server manages the iOS mobile devices. This component includes the following sub-modules that aid in managing and processing the jobs for a mobile device:

- Staging Manager: This module processes all commands required to run an agent connect job.
- Persistent Store: A persistent data store that stores the push notification jobs created by an administrator, the timer-based jobs, and jobs created when an end-user manually connects to the RCA servers. The jobs exceeding the existing job processing limit of the Staging Manager are added in this data store. The jobs are processed using the First In, First Out principle, with the priority-set jobs processed first as an exception. A priority is set for a job in the following scenarios:
  - The device sends a notification to the Staging Manager to run a connect.
  - The job was not completed because of one of the following reasons, and added to the Persistent Store for a retry:
    - The device is switched off.
    - The Apple gateway is too busy to process the request.
    - The device is not on a corporate network.
    - The port on the device is not enabled for accepting the incoming messages from APNS.
    - The device is password protected and is currently in locked mode. A few connects, for example security connect do not run if the device is in locked mode. The device sends a "NotNow" message when a notification request is sent.

    If a job is not successful at the first instance, it is added to the processing queue for another try, before it is permanently removed from the job queue. A status flag is used to track if the job is added for a retry.

    If the device receives a delayed notification, after the job has already been moved out of the Staging Manager, it sends a message to the Staging Manager requesting the tasks to be performed. The Staging Manager searches for the job in the current processing queue, and then in the Persistent Store. If the Staging Manager is not processing maximum number of permissible requests, it adds the job in the current processing queue and sends a notification to the Notifier module to connect to the APNS. If the Staging Manager is processing maximum number of permissible requests, the job is added in the Persistent Store with a high priority.
- Job Processor: This module polls the Persistent Store and sends the jobs to the Staging Manager.
- Notifier: This module sends requests to the APNS, to be sent to the iOS mobile devices.

- Command Processor: This module performs all the post-processing of the tasks that are run by the Staging Manager. For example, after you run an audit connect job, this module sends the data received from the device to the Reporting server database.

You can modify the properties for each sub-module by configuring the Advanced Settings of the MDM server.

To modify the Advanced Settings, complete the following steps:

1. Log on to the RCA Core Console and click **Configuration** tab.
2. Expand **Mobile Management** in the left-navigation pane and then click **Vendor Configuration**>**iOS**. The iOS settings page opens.
3. Click **MDM Configuration** tab.
4. Click the URL for the full-service Satellite MDM server. The Configuration tab view opens.
5. Click **iOS MDM Settings** and then click **Advanced Settings**.
6. Enter the details for the following fields and click **Save**:

Field	Description
Server FQDN	The fully qualified domain name (FQDN) of the Satellite server.
Server Port	The port that the Satellite server uses for communications. If you select HTTPS in the Server Method list, you must specify the SSL port that you use for HTTPS communications. The default SSL port is 443.
Server Method	Select the HTTP/HTTPS protocol for Satellite server communications. If you enable HTTPS, the communication between Satellite Server and the built-in iOS MDM agent on the device is SSL-based. The communications between the Satellite server and the RCA agent are HTTP even if you select the HTTPS method. The communications between the Satellite server and APNS are always SSL-based.
Number of Maximum Concurrent Connections	Specify the maximum number of device connections that the Staging Manager processes at any instance.
Notifier Interval in Minutes	Specify the time (in minutes) that Notifier module must wait before sending requests to the APNS. The Notifier waits only if it is processing maximum number of permissible requests.
Number of Notifier Workers	Specify the number of workers that can send notification request to the APNS. The workers share load based on the current number of device connections.
Number of Command Processor Workers	Specify the number of workers for performing post-processing tasks.
Staging Manager Sleep	Specify the time (in minutes) Staging Manager must sleep before

Field	Description
Period in Minutes	polling the Persistent Store.
Staging Maximum Inactivity Time	Specify the maximum time (in minutes) a job can stay in the Staging Manager without any response from the device. After the maximum inactivity time lapses, the job is moved out of the Staging Manager and added to the Persistent Store, with a status flag set to true.
Persistent Store Polling Interval in Minutes	Specify the time (in minutes) after which the Staging Manager polls the Persistent Store for jobs.
Maximum Number of Concurrent Jobs to be run	Specify the number of parallel threads that can add jobs to the Staging Manager.
Maximum Number of Record to be Processed from the Persistent Store per Polling	Specify the maximum number of jobs that the Staging Manager must select for processing from the Persistent Store per poll.

Post Configuration Tasks

After you have configured the RCA servers, you must run a synchronization between the Core and Satellite servers in your environment. You must synchronize the Satellite servers with the Core server after you modify any configurations.

You might receive the following error message during Satellite synchronization:

```
Synchronization Failed
```

To resolve this problem, see the workaround mentioned for the problem "Core and Satellite: Satellite synchronization fails from SSL enabled Core" in the Known Problems section of the *Radia Client Automation Enterprise Release Notes*.

Modifying RCA Satellite Server Configuration File

You can optionally modify the Mobile server configuration file in a full-service Satellite server. The values in this configuration file are set by default. If you want to modify these parameters, edit the `ConfigServerAdapter.cfg` file.

1. Using a text-editor, open the file `ConfigServerAdapter.cfg` available at the location `<InstallDir>\MobileServer\etc`.
2. Modify the following parameters and save this file:

Parameter	Description
`http-port`	The HTTP port that Satellite server uses for communications with RCA Core server and RCA agents.

Parameter	Description
`max-threads`	Maximum number of threads that must run on a Satellite server to process the mobile device jobs.
`ds-refreshtime`	Directory service refresh time in seconds.

Enabling Administrators to Notify End-users for Agent Installation

To manage a mobile device, an agent is installed on the device that connects to the RCA servers to perform policy resolution and maintain the desired state. Based on the device platform, mobile users can download the agent application from Google Play or App Store.

The RCA agent for mobile devices is a light-weight application that enables RCA servers to communicate with the mobile device. Using the Email Notification settings, you can send an email to the mobile device user to download the mobile agent. The following sections list the prerequisites and the steps to configure email notification settings.

Prerequisites

The following prerequisites must be met before you configure RCA to send an email notification to the end-user:

- The directory service, in which the mobile device user is listed, must be configured for use with RCA. To make sure that the directory service is configured for use with RCA, perform the following steps on RCA Console.
  a. Click the **Configuration** tab.
  b. Expand **Infrastructure Management** and then click **Directory Services**.
  c. Select the Directory Service that the mobile device user is a part of to open the **Directory Service Properties** window.
  d. Click the **Properties** tab in the **Directory Service Properties** window.
  e. Click **UI Settings**.
  f. Select the **Used for Authentication** check box.
- The directory service user must have a valid email ID.

Configuring Email Notification Settings

Note that RCA currently supports only SMTP-based mail servers for sending email notifications.

1. Log on to the RCA Core Console and click **Configuration** tab.
2. Expand Mobile Management in the left-navigation pane and click **Email Notification Settings**. The Notification Settings view opens in the details pane.

3. Enable the Socks Proxy settings only if your enterprise is configured to use SOCKS proxy. Enter the details for the following fields:

Field	Description
Proxy Enable	Select this check box if your enterprise is configured to use a SOCKS proxy.
Proxy Host	Enter the IP address or fully qualified domain name (FQDN) of the SOCKS proxy server.
Proxy Port	Enter the port number of the SOCKS proxy server.
User Name	Enter the user name that the RCA servers use to authenticate to the SOCKS proxy server. The entries in this field are required only if the proxy server requires a username and password.
Password	Enter the password for the user name you provided to authenticate RCA servers to the SOCKS proxy server.
Confirm Password	Re-enter the password.

4. Enter the details for the following fields under Email Server Details. These settings are required to configure access to the mail server used in your environment.

Field	Description
SMTP Host	Enter the IP address or fully qualified domain name (FQDN) of the SMTP mail server.
SMTP Port	Enter the SMTP port number.
Basic Authentication	Select this check box if the mail server requires authentication.
User Name	Enter the user name RCA servers will use to authenticate to the mail server. This field is available only if you select the Basic Authentication check box.
Password	Enter the password for the user name you provided to authenticate the RCA servers to the mail server. This field is available only if you select the Basic Authentication check box.
Confirm Password	Re-enter the password. This field is available only if you select the Basic Authentication check box.
Enable SSL	Select if the mail server is configured to use the SSL protocol for SMTP connections.
Enable TLS	Select if the mail server is configured to use the Transport Layer Security (TLS) protocol for SMTP connections.

5. Enter the details for the following fields under Mail Details, and then click **Save**. These settings enable you to configure how the agent installation email appears to the mobile device user.

Field	Description
Sender Name	Enter the name that should appear in “From” field when the user receives an email.
Sender EmailID	Enter the email ID that is used to send emails to the user or user groups.
Subject	Enter the subject for the installation mail that is sent to the user. For example, you can set this value as RCA Mobile Agent Installer.
Body	Enter the email body text. Provide the following details in the email text: ▪ Agent download URL: The Google Play URL from where the mobile device user can download the Android or iOS agent. ▪ RCA sever IP or hostname: The IP address or hostname of the full-service Satellite server to which the RCA agent will connect to fetch the entitlement policies. ▪ Port: The port number through which the mobile device connects to the RCA server IP address you provided. ▪ Install instructions: Instructions on how to install the RCA mobile agent. For more information on how to install the agent application on a mobile device, see: ○ For Android operating system-based devices: "Installing the RCA Agent on Android Devices" on page 33 ○ For iOS operating system-based devices: "Installing RCA Agent on iOS Devices" on page 34 ▪ Registration instructions: Instructions on how to register the mobile device to the RCA servers.

Creating Mobile Connect Job

After you have configured the Email Notification settings, create a job for the user or group of users to whom you want to send the email notification.

To create a job, complete the following steps:

1. Log on to the Core Console, click **Management** tab, and then click the directory service that you have added to RCA.
2. Navigate to the user for which you want to create a job.
3. Select the user and click **Launch HPCA Job Creation Wizard** to open the HPCA Job Creation Wizard.
4. From the Job Type list select **Notify**.
5. Enter a Name and Description of the job.

6. From the Job Action Template list, select **Mobile Email Connect**, and then click **Next**.
7. Review the information on the Job Confirmation Summary page and click **Submit**.

Provisioning Mobile Applications

Using RCA you can publish mobile applications and entitle these applications to user or user groups. You can also upgrade or uninstall an application installed on a mobile device.

Publishing Mobile Applications

Use the RCA Administrator tools to publish packages for the Android and iOS platform.

Note: For iOS operating system based devices, RCA supports software management of in-house applications only. You must enroll for iOS Developer Enterprise Program to create in-house applications. For more information on how to obtain the membership, see the Apple website at http://developer.apple.com/programs/ios/enterprise.

Complete the following steps to publish mobile applications to the CSDB:

1. Open the Radia Client Automation Administrator Publisher.
   a. From the computer where you have Administrator Tools installed, click **Start**>**All Programs**>**Radia Client Automation Administrator**>**Radia Client Automation Administrator Publisher**.
   b. Enter the user ID and password, and click **OK**. The default user ID is `admin`. The default password is `secret`. The Radia Client Automation Admin Publisher window opens.
2. Select **Mobile Application** from the Publishing Options drop-down list, and click **OK**. The Edit page opens.
3. Under Select Mobile application to publish, select the folder that contains the application file that you want to publish:
   - For Android devices, select `.apk` file to create the package.
   - For iOS devices, select `.ipa` file to create the package.
4. Click **Next**. The Configure page opens.
5. Under the Package Information area, enter the following details:

Field	Description
Name	The name of the package. An instance with the value you provide in this field is created in the PACKAGE class of the MOBILE domain. This is a mandatory field.
Display Name	The friendly name of the package. This is a mandatory field.
Domain	The domain in which this instance is stored. The MOBILE domain is selected by default for mobile applications. It is recommended that you do not change the value for this field.

Field	Description
Description	Description of the package.
Release	The version number of the application that you are packaging. This value is pre-populated from the application manifest file; you must not modify this value. For Android only: An application can be upgraded only if a new version number is available for the application.
Class	The class for which this package instance is created.

6. Under the Limit package to systems with area, select the operating system for the device on which you want to deploy the application. Note that if you do not select any operating system, the application can be distributed to all devices with supported operating system. The Hardware settings are not applicable for mobile applications.
7. Click **Next**. The Service Information window opens. You can create a new service or use an existing service to deploy the package. Select **Use existing** if you want to publish update for an existing application. Select **No service** if you do not want to associate this package with a service.
8. Click **Create new** and enter the values for the Name, Display Name, Web URL, and Author field. The Name and Display Name fields are mandatory fields.
9. Click **Next**. The Publish window opens.
10. Review the Summary section to verify the service information you provided in the previous steps. When you are finished, click **Publish**.
11. Click **Finish** when the publishing process is completed to exit the Publisher.
12. Click **Yes** to confirm that you want to close the Publisher window.
13. The mobile application is published as a service in the CSDB. You can then entitle this service using Policy Management Wizard to a user or a user group.

For more information on publishing applications, see the *Radia Client Automation Enterprise Administrator User Guide*.

Updating an Application

You can provide update for an application that is already published in the CSDB. Follow these instructions based on the application for which you are providing an update:

- Updating applications for Android devices: Republish the application to the CSDB if a new version of the application is available. The application version is stored in the application manifest file. You must link this new package with the existing service that was used to deploy the package.
- Updating applications for iOS devices: You can provide update for an application in the following scenarios:
  - New version of the application is available: Republish the application to the CSDB if there is a change in the application version. You must link this new package with the existing service that was used to deploy the package.

- Provisioning Profile has expired: Each iOS package (`.ipa` file) contains an application and a provisioning profile. This provisioning profile expires every 12 months. If the provisioning profile expires, the end-user will not be able to access the application. In such scenarios, an administrator must rebuild the application with the renewed provisioning profile, and publish it to the CSDB. You must link this new package with the existing service that was used to deploy the package.

Deploying Mobile Applications

Complete the following steps to entitle a mobile application to a mobile user or a user group:

1. Log on to the RCA Core Console.
2. Click **Management**, and then click the directory service that you have added to RCA.
3. Navigate to the user or user group for which you want to create the policy.
4. Select the user or a user group, and click **Launch Policy Management Wizard (Policy)** to open the Policy Management Wizard.
5. In the Service Selection page, select **Mobile domain** from the Service Domain list.
6. Select the service that you want to entitle to this user or user group and click **Add to Selection**.
7. Click **Next**. The Policy Configuration page opens.
8. Click **Next**. The Confirmation Summary page opens.
9. Click **Commit** to assign this policy to the selected users or group.

Managing Mobile Device Security

To manage security on a mobile device, you can create and deploy security profiles that enable securing the data on a mobile device if the device is lost or stolen. These profiles can also prevent unauthorized access to the device.

By default, RCA provides a pre-configured Wipe security profile that you can use to remotely wipe the device data. Note that you can apply the Wipe security profile only if RCA can contact the device. You cannot modify or delete this profile.

Caution: If you entitle Wipe security profile to a device, all device data is lost and the device is reset to factory settings.

You can also create new profiles that enable you to set the password settings or send commands to lock the device. The Security profile is published as a service in the CSDB. You can then entitle this service using Policy Management Wizard to a user or user group.

After you entitle the security profile, the device receives the new entitlements only when the next automatic timer is triggered on the mobile device.

A notification appears on the mobile device only if user intervention is required. For example, if the security profile is configured to set the user password, an RCA security connect notification

appears in the notifications panel on the mobile device indicating the changes that are pending from the user.

Note: If you entitle more than one security profile to a user, the profile that imposes maximum security will be enforced on the device. For example, if you entitle following profiles to a user:

- At user level: Simple password value=true; Alphanumeric Password Value=true; Minimum Password Length=7
- At group level: Simple password value=false; Alphanumeric Password Value=true; Minimum Password Length=5; Number of complex characters in a password: 2

The resulting security profile that is enforced on the user is:

Simple password value=false; Alphanumeric Password Value=true; Minimum Password Length=7; Number of complex characters in a password: 2

Creating Android Security Profile

Complete the following steps to create a security profile for Android device:

1. Log on to the RCA Core Console and click **Operations** tab.
2. Expand **Mobile Management** in the left-navigation pane and click **Security**. The Security view opens in the details pane.
3. Click **Create a New Profile**, and then click **Android**. The Profile Creation Wizard opens.
4. In the Define Profile page, enter the details for the following fields, and click **Next**:

Field	Description
Display Name	The display name for the profile. The service will be referenced in the CSDB Editor using this name.
Description	The description of the profile.

5. In the Configure Profile Parameters page, enter the following details, and click **Submit**:

Field	Description
Password Settings: These settings are available only when you select the Password Required check box.	
Password Required	Select this check box if the managed mobile device user must have a password set for the mobile device.
Minimum Password Length	Enter a value for the minimum length of the password.
Password Strength	Select the type of characters the user must use when creating the password. The password quality and the password length determine the total password complexity.
Maximum Failed Password Attempts	Enter a value that defines the maximum number of times a user can enter a wrong password, after which the device is

Field	Description
	reset to factory settings.
Screen Settings: This setting determines the time a device can remain in idle state.	
Maximum Inactivity Time Lock	Enter the time (in minutes) the device can remain in idle state, after which the device is locked automatically. The maximum inactivity time set on the device overrides the Maximum Inactivity Time Lock value that you set in the profile, if the inactivity time already set on the device is greater than this value. An end-user might not be able to view the Maximum Inactivity Time Lock value that you set in the profile on the device because of device limitations.
Operational Settings: These setting can be applied only if RCA can contact the device. At any instance, you can apply only one of the operational settings. All other settings on this page are disabled.	
Reset Password	Select this check box to reset the password for the device.
Lock Now	Select this check box to lock the device.

Creating iOS Security Profile

Complete the following steps to create a security profile for iOS device:

1. Log on to the RCA Core Console and click **Operations** tab.
2. Expand Mobile Management in left-navigation pane and click **Security**. The Security view opens in the details pane.
3. Click **Create a New Profile**, and then click **iOS**. The Profile Creation Wizard opens.
4. In the Define Profile page, enter the details for the following fields, and click **Next**:

Field	Description
Name	The display name for the profile. The service will be referenced in the CSDB Editor using this name.
Description	The description of the profile.

5. In the Configure Profile Parameters page, enter the following details, and click **Submit**:

Field	Description
Password Settings: These settings are available only when you select the Password Required check box.	
Password Required	Select this check box if the managed mobile device user must have a password set for the mobile device.

Field	Description
Allow Simple Password Value	Select if the password must not contain any special character.
Alphanumeric Password value	Select if the password must contain alphanumeric characters.
Minimum Password Length	Enter a value for the minimum length of the password.
Number of Complex Characters in Password	Enter the number of non-alphanumeric characters that the password must contain.
Maximum Password Age	Enter the time (in days) after which the user must change the password.
Time Before Auto-lock	Enter the time (in minutes) the device can remain in idle state, after which the device is locked automatically.
Password History	Enter the number of passwords that the device remembers. A user cannot set a new password that matches the passwords available in the history list.
Grace Period for Device Lock	Enter the time (in minutes) for which the user is not required to enter the password again, if the user unlocks the device within the time you specify.
Maximum Failed Password Attempts	Enter a value that defines the maximum number of times a user can enter a wrong password, after which the device is wiped.
Restriction Settings: These settings are available only when you select the Restriction Settings Required check box.	
Restriction Settings Required	Select if you want to restrict the features a user can access on a device.
Allow Installing Apps	Select to allow the user to install applications on the device. By default, this setting is enabled.
Allow use of iTunes Store	Select to allow the user to use the iTunes store on the device.By default, this setting is enabled.
Allow Backup	Select to allow the user to create a backup on an iCloud account. By default, this setting is enabled.
Allow Document Sync	Select to allow the user to sync documents with an iCloud account. By default, this setting is enabled.
Allow Photo Stream	Select to allow the user to use the Photo Stream functionality. By default, this setting is enabled.
Operational Settings: These setting can be applied only if RCA can contact the device. At	

Field	Description
any instance, you can apply only one of the operational settings. All other settings on this page are disabled.	
Clear Password	Select this check box to reset the password for the device.
Lock Now	Select this check box to lock the device.

Modifying Security Profiles

You can modify an existing security profile. You must re-deploy the profile such that the changes are implemented in the device.

Complete the following steps to modify a security profile:

1. Log on to the RCA Core Console and click **Operations** tab.
2. Expand Mobile Management in left-navigation pane and click **Security**. The Security view opens in the details pane.
3. Click the name of the profile you want to modify. The profile window opens. Modify the settings in the Properties tab and then click **Save**.

Connecting RCA Servers to RCA Agents

The RCA agent on a mobile device must connect to the RCA servers, such that the desired state is always maintained for the mobile user. You can schedule a timed event when the mobile device connects to the RCA servers, or send a notify message to the mobile device to connect to the RCA servers. The connection can also be initiated manually from the mobile device, where the mobile device user triggers a software connect, audit connect, or a security connect.

Scheduling Timed Events

The RCA agent timers are run immediately after the agent install is complete. Note that all connects for software management, inventory management, and security management are run at this instance.

If the agent identifies that the mandatory applications defined in your entitlements are not installed on the mobile device, the message `RCA Software Connect->Installations are pending` appears in the Notifications Panel. You can then install the required applications.

By default, the agent timer runs once every day.

To modify the timer schedule, complete the following steps:

1. Log on to the RCA Core Console and click **Configuration** tab.
2. Expand Mobile Management in the left-navigation pane and click **Timer Settings**. The Timer Settings view is displayed in the details pane.
3. Specify the number of hours or days after which the timer should run, and then click **Save**.

To avoid simultaneous agent connections to the RCA servers, the hour-based timer is not run exactly after the number of hours you specify; instead a random number is added to the time you enter:

- If you specify the frequency between 0-6 hours, a random number between 0-3 hours is added to the actual time.
- If you specify the frequency between 6-12 hours, a random number between 0-6 hours is added to the actual time.
- If you specify the frequency between 12-24 hours, a random number between 0-12 hours is added to the actual time.

For example, if you set the timer to be run every 5 hours, a random number 2 is added. As a result, the timer is run after 7 hours for that device.

The new timer settings are applied only when the next timer-based connect starts. The timer-settings are not provided to the mobile agent as part of the user-initiated or push notifications.

Note that the when you schedule a timer-based event, all agent connects, Software connect, Audit connect, and Security connect are initiated at that instance.

Sending Notification from the Server

You can create a Notify job for a user or group of users to send a notification message to connect to the RCA server.

The following procedure shows how you can schedule a Mobile Audit Connect notify job:

1. Log on to the Core Console, click **Management** tab, and then click the directory service that you have added to RCA.
2. Navigate to the user or user group for which you want to create the job.
3. Select the user and click **Launch HPCA Job Creation Wizard** to open the RCA Job Creation Wizard.
4. From the Job Type list select **Notify**.
5. Enter a Name and Description for the job.
6. From the Job Action Template list, select the predefined mobile template. For example, select **Mobile Audit Connect** to schedule an Audit connect.
7. Select the platform from the OS Type list under Action Parameters.
8. Select the type of device from the Device Type list under Action Parameters, and then click **Next**.
9. Set the job schedule details and click **Next**.
10. Review the information on the Job Confirmation Summary page and click **Submit**.

For more information on how to schedule a job, see the chapter *Managing the Enterprise* in *Radia Client Automation Enterprise User Guide*.

Mobile Device Management Reports

The Mobile Management reports provide hardware and software related information for mobile devices managed using RCA. The reports include information on the device platform, applications downloaded and installed on the device, and the type of devices that are managed (smartphones or tablets) using RCA.

Note: For mobile devices, the columns in the inventory reports and the reports accessible from the Dashboard tab are populated based on the mobile device capability. For example, the RCA Agent Version, IP Address, and MAC Address columns are shown blank for any mobile device in the **Reporting**>**Inventory Information**>**View Managed Services** report.

The Mobile Management reports include the following reporting options:

- Executive Summaries: The Hardware Summary report provides details on the managed mobile devices by platform and by vendor. These reports can be viewed in bar graph view or a detailed view.
- Operational Reports: These reports provide details on the number of mobile device connections and service events sent by the mobile device to the RCA server. The Managed Devices report provides the number of devices that have connected in the last 24 hours, 30 days, and 12 months. The Managed Services report provides the number of service events that are sent in the last 24 hours, 30 days, and 12 months.
- Hardware Reports: These reports provide hardware specific information for the mobile devices in your RCA environment. This section includes the following reports:
  - Hardware Summary: Displays details for the managed mobile devices that are filtered based on the platform, platform version, vendor, and device model.
  - Managed Devices: Displays details for the mobile devices that are managed using RCA. The details include last connect time, device ID, operator name, and platform details.
  - Devices by Platform: Displays details for the managed mobile devices that are filtered based on the platform.
  - Devices by Vendor: Displays details for the managed mobile devices that are filtered based on the vendor.
  - Devices by Device Type: Displays details for the managed mobile devices that are filtered based on the device type, such as tablet or a smartphone.
- Software Reports: These reports provide information related to the services that you have entitled to the mobile devices in your environment. This section includes the following reports:
  - Managed Service Reports: This section includes the following reports:
    - Service Summary: Provides the summary of the services that have been entitled to the mobile devices. This report shows the number of users for each service, and whether the service has been downloaded or installed on the mobile device. The Download column is updated when a subscriber downloads a service, but does not install that service. Whenever a service is installed, the value in the Download column is decreased, and the value in the Install column is updated.

  - Managed Services: Displays details for services entitled to the mobile devices, such as number of users, number of downloads, and number of uninstall attempts.
  - Pending Services by Device: Displays the details of the service entitled to the mobile user that has been downloaded on the mobile device, but has not been installed.
- Managed Software Reports: The Manage Software by Product report in this section contains the details for the devices where each software application is installed.

- Security Reports: The Security Details Reports contains details on current security settings on the device. The security profile on a mobile device can be enabled only when the device administrator is activated on the mobile device. To verify the devices that have not activated the device administrator, check the Enabled column. A true value indicates that the device administrator (security administration) is activated. A false value indicates that the device administrator has not been activated on the mobile device. The other columns in this report, such as Minimum Password Length and Maximum Screen Lock Time provide the current security settings on the device even if the device administrator is disabled. This report also provides the number of remote wipe commands that have been attempted on a device.
- Registration Reports: The PUSH Registration Detail Reports provides the current registration status for a device. For iOS devices, the reports are populated only if the registration is successful, after all the profiles have been installed. For Android devices, this report contains details related to the push notification mechanism between the RCA servers, Google servers, and the mobile device. The GCM process does not guarantee a 100% data delivery to the mobile device. To verify if the mobile device is receiving messages from the Google servers, check the PUSH Registration Status column in this report. A true value indicates that the messages are delivered to the mobile device. A false value indicates that the message delivery has failed. The error message for the message delivery failure is listed in the Registration Error column. The following table lists the possible error messages and cause if the push notification fails for a mobile device:

Error	Cause
SERVICE_NOT_AVAILABLE	This error can occur if one of the following conditions are true: ▪ Auto-sync is not enabled on the mobile device. ▪ Mobile device does not have Internet access.
ACCOUNT_MISSING	The Google account ID is not configured on the mobile device.

Limitations

This section provides the list of known limitations in RCA for MDM:

- *For iOS only*: You can publish and manage in-house mobile applications only. You cannot publish and distribute the applications that you download from App Store.
- *For Android only*: You can publish and manage free and in-house mobile applications. To distribute the paid applications available on Google Play, you must have an appropriate license agreement with the application vendor.

- For a single user, RCA cannot manage multiple types of devices on the same platform; you can manage only a single phone and a single tablet for that user. For example, you cannot manage two iPhone devices or two iPad devices for the same user.
- After a device has registered successfully with RCA servers, you cannot change the directory service for the user. The end-user must reinstall the agent and then register again with the new directory service.
- The RCA agent works in the following screen layouts:
  - For Android devices, the RCA agent works in portrait mode for phones, and in landscape mode for tablets.
  - For iOS devices, the RCA agent works in portrait mode for iPhone and iPad.

  Screen auto-rotation is not supported in the current release.
- On Android phones with small display screen size, the text in the Notification Panel appears truncated when opened from an application that supports portrait mode. To view the complete text, open Notification Panel from an application that supports landscape mode.

Chapter 2

Using the RCA Agent on Mobile Devices

This chapter lists the prerequisites and tasks that a mobile device user must perform to install the Radia Client Automation (RCA) agent. The chapter also lists the steps to manually connect to the RCA servers.

Note: As an administrator, you can provide this help on you company's intranet, such that the mobile device users can access this help.

This chapter uses touch-based mobile devices as an example in all client-side procedures. The steps may vary if the RCA mobile agent is installed on a keypad-based device.

Installing the RCA Agent on Android Devices

You must install the RCA agent application when you receive an email from your enterprise administrator. The application runs primarily in the background and becomes active only when communication between the device and RCA server is initiated, to manage the device as per your enterprise policies set by the administrator. The RCA agent connects automatically to an RCA server to receive the latest entitlements.

Agent Prerequisites

The mobile device must meet the following prerequisites before installing the RCA mobile agent:

- If the device is accessing RCA servers from a corporate Wi-Fi, open the port 5228 (outbound) on the RCA agents to allow communication with the Google Cloud Messaging service.
- The device must have access to the Internet.
- The following requirements are specific to Android devices:
  - The mobile device must have a Secure Digital (SD) card.
  - A Google account must be configured and accessed at least once on the Android device. For example, xx@gmail.com.

Installing the Agent

Complete the following steps to install the agent:

1. Download the agent installer from Google Play on your device. The email that you received from your administrator contains the URL from where you can download the RCA mobile agent installer. After the download is complete, the file download details appear in the Notifications Panel.

2. Navigate to the file `RCAMobileAgent.apk` and click this file to start the installation. The RCAMobileAgent confirmation prompt appears that confirms the device features that this application accesses.
3. Tap **Install** to continue with the installation.
4. Tap **Done** to close the confirmation prompt. RCA Agent is listed on the Applications screen.

Registering the Mobile Device

To register the mobile device with the RCA servers, complete the following steps:

1. Tap **RCA Agent** listed on the Applications screen. The RCA Agent License screen appears.
2. Tap **I Agree** to continue with the installation. The RCA Server Details screen appears.
3. Enter the RCA server name or IP address in the Server field. You can obtain this value from the agent installation email that you received from your administrator.
4. Enter the port number in the Port field. You can obtain this value from the agent installation email that you received from your administrator.
5. Tap **Next**. The Authentication screen appears.
6. Enter your directory service logon name in the User Name field. This logon name is the name using which you log on to your corporate network. For example, if you log on to your corporate network as `Americas\ssimpson`, `ssimpson` is the directory service log on name.
7. Enter the password for the directory service logon name in the Password field.
8. Tap the down arrow for the Directory Source drop-down list, and then tap the domain name to which your logon name is associated with. For example, if you log on to your corporate network as `Americas\ssimpson`, `Americas` is your domain name.

   Note: If your administrator has provided a different display name when configuring this directory service with RCA, the domain name you use may not appear. Contact your administrator to identify your directory source.

9. Tap **Register** to start the registration process. The registration process can take a few minutes to complete.

After the registration process is successful, the Activate Device Administrator screen appears. Tap **Activate** to allow the RCA agent to collect the information listed on this screen.

Installing RCA Agent on iOS Devices

You are expected to install the Radia Client Automation (RCA) agent application when you receive an email from your enterprise administrator. The application runs when communication between the device and RCA server is initiated, to manage the device as per your enterprise policies set by the administrator. The RCA agent connects to the RCA server when you accept the application alerts in the Notification Center to receive the latest entitlements.

Agent Prerequisites

The mobile device must meet the following prerequisites before installing the RCA mobile agent:

- The device must be activated, and must have access to the Internet.
- If the device is accessing RCA servers from a corporate Wi-Fi, open the port 5223 (outbound) on the RCA agents to allow communication with the Apple Push Notification service (APNS).

Downloading the Agent

You can download the agent installer from the App Store. The email that you received from your administrator contains the URL from where you can download the RCA mobile agent installer.

Registering the Mobile Device

To register the mobile device with the RCA servers, complete the following steps:

1. Start the agent application installation:
   a. Tap the **Radia Client Automation Agent** icon on the Home screen to start the installation. The Radia Client Automation End User License Agreement screen appears.
   b. Tap **Accept** to continue with the installation.
2. Enter the RCA server name (or IP address) and port number in the Server and Port fields. Your administrator will provide this information to you before you can register.
3. Tap **Next**. The RCA Registration screen appears.
4. Enter your enterprise directory service logon name in the User field. This logon name is the name you use to log on to your corporate network.
5. Enter the password for the directory service logon name in the Password field.
6. Tap the domain name to which your logon name is associated with, from the Directory Services view. For example, if you log on to your corporate network as `Americas\ssimpson`, `Americas` is your domain name.

   Note: If your administrator has provided a different display name when configuring this directory service with RCA, the domain name you use may not appear. Contact your administrator to identify your directory source.

7. Tap **Enroll** to start the enrollment process. The Install Profile screen appears. During enrollment, the RCA agent installs RCA profile that contains certificates to authenticate your device connection with RCA and Apple servers. Tap **More Details** to view the certificates, RCA server details that your device connects to, and the administrative rights that an administrator has on your device.
8. Tap **Install** to start the profile installation process. A warning screen appears that provides you the information on what changes are made during the agent installation.
9. Tap **Install** to continue the installation process. After the registration process is successful, the Profile Installed screen appears.
10. Tap **Done** to complete the registration process.

On the Home screen, tap the **Radia Client Automation Agent** icon. A message box appears confirming the device connection to the RCA server. Tap **OK** to initiate this connection. If your

administrator has set up device management policies, you will receive the required software applications and security settings entitled to your device.

At regular intervals, set by your administrator, RCA agent requests connection to RCA servers to obtain the latest entitlements. To access RCA servers, RCA agent issues notifications that you can view in the Notifications Center on your device. You must accept these notifications, such that the RCA agent can successfully connect to the RCA servers. Make sure that the RCA agent application is enabled for notifications. You can view the notification settings for your device using **Settings**>**Notifications**. Additionally, based on the alert style that you have set for the notifications, the RCA agent notifications appear in the Notification Center, or as a pop-up message.

If the device is locked when the notification is issued, the notification appears on the locked screen. After unlocking the device, you can view the notification in the Notifications Center on your device.

Manually Connecting to the RCA Server

Note: RCA agent connects to RCA server automatically on a regular basis to receive the latest entitlements. You will normally not run this agent manually, but only at the direction of your RCA administrator.

To connect manually to the RCA servers, complete the following steps:

1. Search for the RCA Agent application:
   a. Android devices: Open **Applications** screen, tap **RCA Agent** icon.
   b. iOS devices: On the Home screen, tap **Radia Client Automation Agent** icon.

   The RCA Agent screen opens with the options to initiate one of the agent connects.
2. Tap one of the available icons, under Applications, Device Info, or Security Profiles to initiate the connection with the RCA servers.
   - Software Management: Tap **Applications** icon to retrieve the latest software entitlements from the RCA servers. A notification message appears if there is a new application, an update to an existing application, or if the application must be deleted.
   - Inventory Management: Tap **Device Info** icon to send the latest inventory details about your device to the RCA servers, such as software and hardware details.
   - Security Management: Tap **Security Profiles** icon to retrieve the latest security profile settings, if entitled to your device. You cannot delete any security profile that is entitled to your device.

Uninstalling the RCA Agent

Complete the following steps to uninstall the RCA agent:

Android Device

1. On the home screen, tap **Settings**>**Security**>**Device administrators**.
2. Tap **Radia Client Automation** to disable it.

3. On the home screen, tap **Applications** >**Downloaded**.
4. Tap **RCA Agent**. The App info screen opens with the Uninstall option.
5. Tap **Uninstall**.

iOS Device

Note: When you uninstall the RCA agent and the Radia Client Automation configuration profile, all the applications that are managed using RCA are uninstalled from your device.

1. On the home screen, tap **Settings**>**General**.
2. Tap **Profiles**. The Profiles screen appears that lists all the Configuration and Provisioning Profiles installed on your device.
3. Under Configuration Profiles, tap the **Radia Client Automation** configuration profile, and then tap **Remove**.
4. On the Home screen, tap and hold the **Radia Client Automation Agent** icon. The delete symbol icon appears on left-top corner of the icon.
5. Tap the delete symbol to remove the agent.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click here.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to radiadocfeedback@persistent.co.in.

Product name and version: Radia Client Automation Enterprise, 9.00

Document title: Mobile Device Management User Guide

Feedback: