Note
Before using this information and the product it supports, read the information in "Notices" on page 79.

Product Information
This document applies to IBM Cognos Business Intelligence Version 10.2.1.4 and may also apply to subsequent releases.

Licensed Materials - Property of IBM
© Copyright IBM Corporation 2007, 2014.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
# Contents

**Introduction** ........................................ vii

**Chapter 1. What's new** ................................ 1

New features in version 10.2.1.4 ........................................ 1
- Report annotations in the Cognos Mobile Android app ........................................ 1
- Cognos Mobile iOS app optimized for iOS7 ........................................ 1
- Report URL in the email to enhance collaboration ........................................ 1
- Hiding the application toolbar ........................................ 2
- Screen obfuscation in the Cognos Mobile iOS app ........................................ 2
- Maintaining application state ........................................ 2
- Support for SSL and TLS certificate pinning ........................................ 2
- Mobile theme for the Cognos Mobile Android app ........................................ 2

New features in version 10.2.1.2 ........................................ 2
- Restricted access to Cognos Mobile administration ........................................ 2
- Cognos Mobile administration console ........................................ 3
- Mobile theme for iOS applications ........................................ 3
- Local encryption of manually imported active reports on iOS devices ........................................ 3
- Support for Good Dynamics (Good Technology) ........................................ 3
- Cognos Mobile iPad application in portrait mode ........................................ 4
- Cognos workspaces on iOS and Android devices ........................................ 4
- Drill-through enhancements for active reports ........................................ 4
- Access to active reports saved outputs ........................................ 4
- Active reports in the Cognos Mobile web application ........................................ 4
- Thumbnails in the Cognos Mobile web application ........................................ 5
- Bookmarks in HTML saved report outputs on iOS and Android devices ........................................ 5

New features in version 10.2.1 ........................................ 5
- User interface enhancements ........................................ 5
- Faster mobile reports ........................................ 5
- High-fidelity reports ........................................ 5
- Zooming on active reports ........................................ 6
- Touch-friendly HTML5 prompts ........................................ 6
- Audit logging ........................................ 6

New features in version 10.2.0.2 ........................................ 6
- Remote configuration of the Mobile iPad application ........................................ 6

New features in version 10.2.0 ........................................ 6
- Restricted access to Cognos Mobile ........................................ 6
- Apple push notifications ........................................ 6
- Burst reports on Cognos Mobile ........................................ 7
- Support for new languages ........................................ 7

Deprecated features in version 10.2.0 ........................................ 7
- Cognos Mobile native client for BlackBerry on sustaining support ........................................ 7

Removed features in version 10.2.0 ........................................ 7
- End of support for Symbian and Windows Mobile native clients ........................................ 7

New features in version 10.1.1.3 ........................................ 7
- Local security codes and timeouts (iPad native app) ........................................ 7
- Limit on security code tries (iPad native app) ........................................ 8
- Support for new languages ........................................ 8
- Simplified authentication (iPad native app) ........................................ 8

Changed features in version 10.1.1.3 ........................................ 9
- Support for inline prompts in reports viewed on mobile devices ........................................ 9

New features in version 10.1.1.1 ........................................ 9
- Support for active reports in email (iPad) ........................................ 9
- Support for inline prompts ........................................ 9

New features in version 10.1.1 ........................................ 9
- Native support for the iPad tablet computer ........................................ 9

© Copyright IBM Corp. 2007, 2014
Introduction

This document is intended for use with IBM® Cognos® Mobile.

Cognos Business Intelligence is a web product with integrated reporting, analysis, scorecarding, and event management features. IBM Cognos Mobile extends the functionality of your existing Cognos BI installation so that users can view and interact with IBM Cognos BI content on their tablet computers or smartphone devices.

Audience

To use this document, you should be familiar with

• The existing IBM Cognos BI environment, including the location of distributed components
• IBM Cognos BI reports
• One or more tablet computers or smartphone devices
• Windows or UNIX operating system administration, or both

Accessibility features

Cognos Mobile does not currently support accessibility features that help users with a physical disability, such as restricted mobility or limited vision, to use this product.

IBM Cognos HTML documentation has accessibility features. PDF documents are supplemental and, as such, include no added accessibility features.

Finding information

To find product documentation on the web, including all translated documentation, access IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter).

Forward-looking statements

This documentation describes the current functionality of the product. References to items that are not currently available may be included. No implication of any future availability should be inferred. Any such references are not a commitment, promise, or legal obligation to deliver any material, code, or functionality. The development, release, and timing of features or functionality remain at the sole discretion of IBM.

Samples disclaimer

The Sample Outdoors Company, Great Outdoors Company, GO Sales, any variation of the Sample Outdoors or Great Outdoors names, and Planning Sample depict fictitious business operations with sample data used to develop sample applications for IBM and IBM customers. These fictitious records include sample data for sales transactions, product distribution, finance, and human resources. Any resemblance to actual names, addresses, contact numbers, or transaction values is coincidental. Other sample files may contain fictional data manually or
Chapter 1. What's new

This information will help you plan your upgrade, application deployment strategies, and training requirements for users.

For information about upgrading IBM Cognos Business Intelligence, see the *IBM Cognos Business Intelligence Installation and Configuration Guide* for your product.

For information about new features in IBM Cognos Business Intelligence, see the *IBM Cognos Business Intelligence New Features Guide*.

To find product documentation on the web, including all translated documentation, access [IBM Knowledge Center](http://www.ibm.com/support/knowledgecenter).

To review an up-to-date list of environments supported by IBM Cognos products, including information on operating systems, patches, browsers, web servers, directory servers, database servers, and application servers, go to the [Supported Software Environments](http://www.ibm.com/support/docview.wss?uid=swg27037784) website.

### New features in version 10.2.1.4

The following topics describe the new features in 10.2.1.4 version of IBM Cognos Mobile.

**Report annotations in the Cognos Mobile Android app**

The report annotations (comments) feature that was added for the IBM Cognos Mobile iOS app in a previous release is now supported for the IBM Cognos Mobile Android app as well.

You can use this feature to collaborate with your coworkers by adding annotations to reports and emailing screen captures of the annotated reports.

**Cognos Mobile iOS app optimized for iOS7**

The IBM Cognos Mobile iOS app was redesigned to adopt the iOS7 look and feel.

Some of the changes include a more intuitive report selection mechanism and consistent user interface for deleting connections on the start-up screen and deleting reports.

**Report URL in the email to enhance collaboration**

When users choose to send reports with annotations (comments) by email, the IBM Cognos Mobile applications automatically include the report URL in the body of the email. The recipients can tap on the URL to open the report.

This functionality is available for regular reports, active reports, workspaces, and saved report outputs.
Hiding the application toolbar

IBM Cognos Viewer can now hide the toolbar on the mobile device screen when a report is larger than the device viewing area.

This functionality, which is available for the IBM Cognos Mobile app on Android and on iPhone, is especially useful in the landscape mode because users can see more of the report canvas.

Screen obfuscation in the Cognos Mobile iOS app

The screen in the IBM Cognos Mobile iOS app changes to the Cognos Mobile logo when the app is in the background.

This feature protects sensitive data when the app is not in the foreground.

Maintaining application state

Users can specify a setting that forces the IBM Cognos Mobile application to reopen to the location where the application was closed.

For more information, see "Pre-configuring the Cognos Mobile native apps for users" on page 51.

Support for SSL and TLS certificate pinning

Administrators can protect IBM Cognos Mobile Android and iOS apps from man-in-the-middle attacks by restricting the apps to connect only to those IBM Cognos BI servers that use trusted certificates.

For more information, see "Pre-configuring the Cognos Mobile native apps for users" on page 51.

Mobile theme for the Cognos Mobile Android app

The Cognos Mobile theme that was introduced for the Cognos Mobile iOS app in the previous release is now supported for the Android app as well. The theme is applied automatically for the users who can access it.

For more information, see "Configuring a Mobile theme" on page 49.

New features in version 10.2.1.2

The following topics describe the new features in 10.2.1.2 version of IBM Cognos Mobile.

Restricted access to Cognos Mobile administration

You can now restrict access to the administration interface for IBM Cognos Mobile using the Mobile Administration secured feature.

**Mobile Administration** is one of the secured features of the **Administration** secured function. Only users who are granted access to this secured feature can access the **Mobile** tab in IBM Cognos Administration. A new role named **Mobile Administrators** was added to the predefined roles in the Cognos namespace in IBM Cognos Administration to help with setting up access permissions for the **Mobile Administration** secured feature.

For more information, see "Cognos Mobile capabilities" on page 42.
Cognos Mobile administration console
This release of IBM Cognos Mobile introduces a new administration interface to manage the Mobile configuration settings.

Administrators can manage all instances of the IBM Cognos Mobile service from the Mobile tab, Server Configuration page in IBM Cognos Administration. The values are automatically applied to all Mobile services.

For more information, see "Configuring Cognos Mobile services" on page 53.

Mobile theme for iOS applications
Cognos Mobile administrators can customize the appearance of the welcome page in Cognos Mobile iOS applications for specific user groups and roles by applying a custom theme. The theme is applied automatically for the users who can access it.

This feature allows companies to change the appearance of their applications to properly represent the company.

For more information, see "Configuring a Mobile theme" on page 49.

Local encryption of manually imported active reports on iOS devices
If a device PIN is configured on an iOS device, the IBM Cognos Mobile application encrypts the manually imported Cognos BI reports that are stored on the device.

This feature applies to active reports that are manually imported through email, iTunes, or a file server. The Cognos BI server-based content continues to be encrypted through our existing mechanism.

For more information, see "Password protection" on page 42 or "Report data security on mobile devices" on page 44.

Support for Good Dynamics (Good Technology)
The IBM Cognos Mobile for Good Technology application on iOS is integrated with Good Dynamics to leverage its security and networking infrastructure.

Using the IBM Cognos Mobile for Good Technology, users can:
• Authenticate to IBM Cognos Business Intelligence (BI) server using the Good Technology network operation centers (NOCs).
• Browse the Cognos BI directories.
• Consume Cognos BI content that includes regular reports, active reports, and Cognos Workspace workspaces.
• Synchronize the inbox.
• Delete the mobile application data (administrators only).

With the IBM Cognos Mobile for Good Technology application, users can consume only the content that is securely delivered using the Good Technology servers. The following capabilities are disabled in this application:
• Manual import of Cognos active reports through email or iTunes.
• Access to the Cognos Mobile samples.
• Apple Push Notification mechanism.
For more information about Good Dynamics, see the Good Technology documentation.

**Cognos Mobile iPad application in portrait mode**

On iPad, in addition to the landscape mode, the Cognos Mobile application can also be viewed in the portrait mode.

Reports that are authored to stretch to fit the size of the screen automatically adjust to the new width. For reports that are authored with a fixed size, the application does its best to scale the report to fit the new width. In this case, users are presented with a zoomed-out view of the report. They can then use the pinch gesture to zoom into the desired portion of the report.

**Cognos workspaces on iOS and Android devices**

You can view and interact with the IBM Cognos Workspace workspaces on iOS and Android devices.

Cognos Workspace interactive workspaces provide insight into the Cognos Business Intelligence (BI) content and facilitate informed decision making. The workspace interface is optimized for touch, which allows users to quickly and easily interact with the workspace using only a finger. Users can use filters, drills, and sorting; view comments, move between tabs, and much more. All features and capabilities are focused on the user experience rather than authoring.

Workspaces are available only when the device is connected to the server.

**Drill-through enhancements for active reports**

Cognos Mobile users can now drill through from active reports to reports that use OLAP or DMR data sources, or to reports that use different packages. Drill-through actions to and from an active report saved output are also supported.

**Access to active reports saved outputs**

Users of the iOS and Android applications can access the latest saved output version of an active report through the saved output list.

Users can browse for and download the latest version of the saved report output. They can open and view the saved output, and drill through from and to the saved output.

**Active reports in the Cognos Mobile web application**

Active reports can now be accessed through the Cognos Mobile web application on all supported platforms.

With this application, users can access all types of active reports, including reports with and without prompts, and reports that use OLAP and relational data sources. Users can interact with the content using the zoom, tap, and swipe gestures.

Drill-through functionality in this application works as in client applications: a report runs in the web application and is cached in the Mobile inbox to be retrieved when the same drill action is repeated. Users can drill through from active reports to regular reports, from active reports to active reports, and from active reports to reports with unanswered prompts.
**Thumbnails in the Cognos Mobile web application**

For reports that are present in the mobile inbox, thumbnails are generated in the Cognos Mobile web application.

The thumbnails allow users to quickly see the report content and high-level structure before opening the report. Users can open the report by tapping on the thumbnail.

Thumbnails must be enabled for the Cognos Mobile service. For more information, see “Cognos Mobile service configuration settings” on page 54.

**Bookmarks in HTML saved report outputs on iOS and Android devices**

Cognos Mobile users can use bookmarks that are defined in Cognos BI interactive reports and saved HTML report outputs.

The bookmark behavior on a mobile device is the same as in a web browser.

---

**New features in version 10.2.1**

The following topics describe the new features in 10.2.1 version of IBM Cognos Mobile.

**User interface enhancements**

With the new IBM Cognos Mobile interface, you can navigate BI content in a more visual way. In addition to other features, you can sort your local content and pause and restart report downloads.

**Faster mobile reports**

Multi-page reports that are manually executed are retrieved and presented one page at a time, rather than all at once.

This reduces peak server loads and also enables IBM Cognos Mobile users to open and interact with large reports quickly, without waiting for the entire report to download. Users can swipe the screen or tap a button to retrieve the remaining pages in the report, up to the maximum number of pages, as defined by the mobile administrator.

The behavior of scheduled reports remains unchanged.

**High-fidelity reports**

IBM Cognos Mobile has enhanced its support for HTML reports on mobile devices.

The enhancements include:

- Rendering of additional fonts
- Page layout
- Prompt controls
- Drill-through actions
- Saved html output
The capabilities for IBM Cognos Workspace on mobile devices and the drill-through actions between active reports and regular reports remain unchanged from the previous release.

### Zooming on active reports
When viewing 10.2.1 versions of active reports on Apple iOS devices, users can zoom in and out using the standard pinch gesture.

### Touch-friendly HTML5 prompts
The date, time, and multi-select prompt controls have been enhanced with HTML5 controls and are now more touch-friendly on mobile devices.

### Audit logging
Administrators can now audit the mobile users data. Examples of actions recorded in audit logs include user logon and logoff times, expired user sessions, scheduled report delivery, saved output, and so on.

For more information, see “Enabling Cognos BI logging for Mobile server” on page 62.

---

**New features in version 10.2.0.2**

The following topics describe the new features in 10.2.0.2 version of IBM Cognos Mobile.

### Remote configuration of the Mobile iPad application
Administrators can pre-configure the IBM Cognos Mobile iPad application to streamline the setup for users and control how the application works.

For more information, see “Pre-configuring the Cognos Mobile native apps for users” on page 51.

---

**New features in version 10.2.0**

The following topics describe new features in 10.2.0 version of IBM Cognos Mobile.

### Restricted access to Cognos Mobile
You can now restrict access to IBM Cognos Mobile using the Mobile secured function.

Only users who are granted access to this secured function can access the IBM Cognos content through IBM Cognos Mobile. A new role named Mobile Users was added to the predefined roles in the Cognos namespace in IBM Cognos Administration to help with setting up access permissions for the Mobile secured function.

For more information, see “Cognos Mobile capabilities” on page 42.

### Apple push notifications
You can now use Apple push notifications to notify the users of the IBM Cognos Mobile native iPad application about the availability of new IBM Cognos BI reports.
The supported notifications include badges and text alerts. Sounds are not supported.

For more information, see "Configuration of Apple push notifications for the iPad native application" on page 35.

**Burst reports on Cognos Mobile**

Reports can now be distributed to IBM Cognos Mobile users by bursting.

Users receive burst reports in the language specified in their preferences in IBM Cognos Connection. If the report is not burst in the language specified by the user's preference in Cognos Connection, the user receives the report in the server default language.

Users can also receive multiple versions of burst reports, with the burst key appended to the report name. For example, a sales manager who is responsible for multiple regions receives the burst report for each region.

For more information about burst reports, see the *IBM Cognos Report Studio User Guide* and the *IBM Cognos Business Intelligence Administration and Security Guide*.

**Support for new languages**

IBM Cognos Mobile now supports Thai.

---

**Deprecated features in version 10.2.0**

The following topics describe the deprecated features in 10.2.0 version of IBM Cognos Mobile.

**Cognos Mobile native client for BlackBerry on sustaining support**

Starting with this version, no new features will be added for IBM Cognos Mobile native client on BlackBerry. However, any critical issues will be addressed.

**Removed features in version 10.2.0**

The following topics describe removed features in 10.2.0 version of IBM Cognos Mobile.

**End of support for Symbian and Windows Mobile native clients**

IBM Cognos Mobile native client applications are no longer supported on Nokia Symbian and Microsoft Windows Mobile operating systems.

---

**New features in version 10.1.1.3**

Listed below are features that were new in version 10.1.1.3.

**Local security codes and timeouts (iPad native app)**

Cognos Mobile now offers an advanced setting so that you can control local security codes and timeouts.
You can require an iPad user to enter a security code to access the Cognos Mobile application and the amount of time that the Cognos Mobile application can remain inactive before the user must reenter the code to use the application.

**Tip:** Starting with IBM Cognos Mobile version 10.2.1.2, the advanced setting `SecurityCode.SessionTimeoutSeconds` was replaced by the **Security code session timeout** configuration setting.

For more information, see "Apple iPad application security" on page 43.

**Limit on security code tries (iPad native app)**

Cognos Mobile now offers an advanced setting so that you can limit the number of times that an iPad user can try to log on to the Cognos Mobile iPad app.

You can specify the number of times that an iPad user can try to enter a valid security code.

**Tip:** Starting with IBM Cognos Mobile version 10.2.1.2, the advanced setting `SecurityCode.MaxLoginAttempts` was replaced by the **Maximum number of attempts to enter a security code when accessing an iPad app** configuration setting.

For more information, see "Apple iPad application security“ on page 43.

**Support for new languages**

IBM Cognos Mobile now supports several new languages.

The following languages are now supported on the iPad native app:

- Czech
- Danish
- Dutch
- Finnish
- Hungarian
- Norwegian
- Polish
- Romanian
- Russian
- Swedish
- Turkish

The following languages are now supported on the Mobile server:

- Chinese - Traditional
- Korean

**Simplified authentication (iPad native app)**

IBM Cognos Mobile now offers simplified authentication on the iPad.

Previously, the iPad logon window looked like the IBM Cognos Connection logon page. The simplified authentication includes:

- A revised logon window.
- A single password that the user cannot change.
• The ability for the user to log on to one namespace only.
• Support for credential caching.
• The ability for the user to toggle between the new logon window and the previous one using an iPad setting called **Pass-through Authentication**. The user would typically use this feature after encountering unusual behavior and being told by the administrator to use the previous logon window.

### Changed features in version 10.1.1.3

Listed below are features that were changed in version 10.1.1.3.

**Support for inline prompts in reports viewed on mobile devices**

IBM Cognos Mobile now supports several inline prompt types. Previously, all inline prompts in reports viewed on a mobile device appeared in a prompt page.

The prompt types that Cognos Mobile supports as inline prompts are:

- Text Box
- Value
- Date
- Time
- Date and Time
- Interval

For more information, see the **IBM Cognos Report Studio User Guide**.

### New features in version 10.1.1.1

Listed below are features that were new in version 10.1.1.1.

**Support for active reports in email (iPad)**

IBM Cognos Mobile now supports importing active reports from email.

**Support for inline prompts**

IBM Cognos Mobile now supports inline prompts through the Apple iPad native application and the web application of IBM Cognos Mobile.

The following text box and value prompts are available:

- Single-select
- Multi-select
- Single range
- Multi-range
- Cascading

### New features in version 10.1.1

Listed below are new features since the last release.

**Native support for the iPad tablet computer**

IBM Cognos Mobile now supports the iPad tablet computer.
iPad users can download a native application of IBM Cognos Mobile from the Apple App Store or use a web-based version.

iPad users can access the same business intelligence content and IBM Cognos Mobile features that were available on other mobile devices in previous releases.

**Web Support for the iPad, Android, and BlackBerry PlayBook Tablet Computers**

As of the IBM Cognos Mobile 10.1.0 FP1 release, IBM Cognos Mobile supports Web versions of the iPad, Android, and BlackBerry PlayBook tablet computers.

Using a Web browser, users of these tablet computers can access the same business intelligence content and IBM Cognos Mobile features that were available on other mobile devices in previous releases.

Users can search and browse for reports and create a list of favorites.

**Support for active reports**

IBM Cognos Mobile now supports active reports on the Apple iPad with the native application of IBM Cognos Mobile installed.

Report authors can now use IBM Cognos Report Studio to create active reports. IBM Cognos Active Report is a report output type that provides a highly interactive and easy-to-use managed report. Active reports are built for business users, allowing them to explore their data and derive additional insight. Active reports make business intelligence easier for the casual user. Report authors build reports targeted at their users' needs, keeping the user experience simple and engaging. Active reports can be consumed by users who are offline, making them an ideal solution for remote users such as the sales force.

**New features in version 10.1.0**

Listed below are features that were new in version 10.1.0.

**Support for iPhone devices**

IBM Cognos Mobile now supports Apple iPhone devices.

Users can use the look and feel of the web-based iPhone to access the same business intelligence content and IBM Cognos Mobile features that have been available on other devices in previous releases. In addition, users can create a list of favorites and select one workspace or report to automatically display on the Welcome screen whenever they start IBM Cognos Mobile.

**Support for workspaces**

Along with reports and analyses, users can now have Cognos Business Insight workspaces delivered to their devices.

**Drill up and drill down**

Cognos Mobile now offers drill up and drill down capabilities. These capabilities allow users to gain additional insight into the information they are consuming.
Users can see which fields within the Business Intelligence content on their devices they can drill up or drill down on. After drilling up or drilling down on one or more of those fields, they can return to the original report where they began the drilling process.

**Mobile sample reports**
In this release, Cognos Business Intelligence provides sample reports that are optimized for mobile devices.

The sample reports illustrate product features and technical and business best practices. Users can also use them for experimenting with and sharing report design techniques and for troubleshooting.

The Mobile sample reports are included with the Cognos BI samples. For information about installing and setting up the Cognos BI samples, including the Mobile samples, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

---

**Changed features in version 10.1.0**
Listed below are features that were changed in version 10.1.0.

**Enhanced user interface for BlackBerry devices**
Cognos Mobile uses an enhanced user interface for all Research in Motion BlackBerry editions. This enhanced user interface is easier to navigate and provides the user with an improved experience.

**Improved prompting**
Cognos Mobile offers improved prompting in the web application for the Apple iPhone.

Now, prompting can include the surrounding text and formatting that desktop users see. Users are able to run prompted reports intuitively using prompting mechanisms that suit the mobile device.

**Improved navigation and performance**
The latest version of Cognos Mobile offers easier navigation and enhanced performance, particularly with large tables.

---

**Removed features in version 10.1.0**
Listed below are features that were removed for version 10.1.0.

**Research in Motion BlackBerry version 4.1 is no longer supported**
IBM Cognos Mobile no longer supports the Research in Motion BlackBerry version 4.1 mobile device.
Chapter 2. Cognos Mobile

IBM Cognos Mobile extends IBM Cognos Business Intelligence and performance management to mobile devices.

With its rich client, Cognos Mobile enables users to view on their devices Cognos BI reports, workspaces, and analyses produced by tools such as Report Studio, Query Studio, Analysis Studio, and Cognos Workspace. Cognos Mobile delivers timely, informative, and interactive information to support mobile users in their decision-making processes, regardless of where the users are located.

Cognos Mobile processes each Cognos BI report that it receives and renders it in a mobile-friendly version.

Cognos Mobile uses the Cognos BI prompts functionality and scheduling mechanisms to deliver customized reports in a timely fashion.

For more information about prompts, see the IBM Cognos Report Studio User Guide.

For more information about schedules, see the IBM Cognos Business Intelligence Administration and Security Guide.

Cognos Mobile uses Cognos BI security, implements additional security measures specific to a mobile application, leverages various vendor-specific security architectures, and takes advantage of device-based and server-based security measures.

Many of the device-specific management servers and administration tools used by Cognos Mobile offer the ability to remotely remove content from a device or to disable the device completely. So, for example, if a device is lost or stolen, the Cognos BI administrator can use this functionality to protect sensitive content on the device. Or, a Cognos BI administrator could set an expiry date for a report after which the report becomes inaccessible until the user re-authenticates.

For more information about Cognos BI security, see the IBM Cognos Business Intelligence Administration and Security Guide. For more information about device management and security, see the documentation for the device.

Cognos Mobile also supports requests between the mobile device and the server environment for the following product functions:

- Search
- Browse
- Run

You must install and run the same version of Cognos Mobile and Cognos BI server.

Cognos Mobile components

To implement IBM Cognos Mobile, you add components to the application tier and the gateway where IBM Cognos Business Intelligence is installed.
Cognos Mobile includes Cognos Mobile service and Cognos Mobile rich client. On BlackBerry devices, Cognos Mobile also interacts with BlackBerry Enterprise Server and the BlackBerry MDS Connection Service component.

The following diagram shows how the components interact within the Cognos BI environment. The mobile devices connect to the content store through the internet and wireless carriers, a firewall, BES, and the Cognos Mobile service.

Before you install the Cognos Mobile components, you should understand the architecture of your existing Cognos BI environment. For more information, see the IBM Cognos Business Intelligence Architecture and Deployment Guide.

### Cognos Mobile service

The IBM Cognos Mobile service manages the activities related to the IBM Cognos Mobile client.

The service handles the following operations:

- Transforms Cognos Business Intelligence reports and analyses for mobile consumption.
- Compresses Cognos BI report and analysis content for fast distribution over-the-air to the mobile devices and access from those devices.
- Pushes report and analysis content to the mobile devices.
- Facilitates incoming and outgoing report-related and analysis-related requests between the mobile device and the environment to search, browse, or run reports.
- Synchronizes the mobile content store on the server with the mobile database on the mobile device.
- Translates Cognos BI Simple Object Access Protocol (SOAP) messages into wireless-friendly messages.
Communicates with the mobile device.

IBM Cognos Mobile rich client

The mobile device contains the IBM Cognos Mobile rich client and the compressed and encrypted mobile content store. These components provide the functionality that the mobile device user needs to work with IBM Cognos Business Intelligence reports, dashboards, and analyses.

The BlackBerry Enterprise Server

BlackBerry Enterprise Server manages security, devices, content, and data flow between BlackBerry devices and resources that are internal to an organization.

BlackBerry Enterprise Server is installed and maintained by your organization. The Cognos BI administrator must work with the BlackBerry administrator to validate required settings and configuration options to support IBM Cognos Mobile functionality.

BlackBerry MDS Connection Service

BlackBerry MDS Connection Service is a component of BlackBerry MDS Services.

BlackBerry Enterprise Server provides BlackBerry MDS Services support to enable secure connections behind the corporate firewall. Through the existing secure connection, BlackBerry devices and BlackBerry applications can communicate easily with resources throughout the corporate infrastructure.

BlackBerry MDS Connection Service allows BlackBerry device users to communicate with the Cognos BI server. BlackBerry MDS Connection Service must be enabled for Cognos Mobile to function correctly.

Cognos BI uses the BlackBerry MDS Connection Service to install the Cognos Mobile rich client remotely, either by pushing the installation to the BlackBerry device or by providing an over-the-air installation for the user.

Cognos BI also uses the BlackBerry MDS Connection Service to deliver reports, dashboards, and analyses to BlackBerry devices. To enable Cognos BI to deliver reports, dashboards, and analyses, you must provide the location of BlackBerry MDS Connection Service and its web listen port number during configuration.

For more information about BlackBerry Enterprise Server and BlackBerry MDS Connection Service, see the BlackBerry Enterprise Server documentation.
Chapter 3. Cognos Mobile installation and configuration

You must plan in advance how to install and configure IBM Cognos Mobile to provide the best integration with the existing IBM Cognos Business Intelligence environment. The options that you choose depend on your reporting requirements, resources, and preferences.

When installing Cognos Mobile, use the following guidelines:

- Install the IBM Cognos Mobile application tier component in the same location where Cognos Business Intelligence is installed. In a distributed installation, the Cognos Mobile application tier components must be installed on the systems that will run the IBM Cognos Mobile service.
- Install the gateway and Cognos Mobile client components on your gateway systems. The gateway and Cognos Mobile client components include the sample Cognos Mobile over-the-air installation pages and the Cognos Mobile client components.
- For BlackBerry devices, the user must install the Cognos Mobile rich client components on the mobile device or push it over-the-air to Cognos Mobile users.
- For the iPad that supports the Cognos Mobile native application, users download the application from the Apple App Store.
- For the iPad (web version), Android, BlackBerry PlayBook, and iPhone, users must configure Cognos Mobile using a web application that they access using a URL.

For more information, see the IBM Cognos Business Intelligence Architecture and Deployment Guide.

Cognos Mobile service installation and configuration

To install the IBM Cognos Mobile service, use the installation wizard to select the components and the installation location.

You must install the Cognos Mobile service on a system where a dispatcher is installed.

Before installing Cognos Mobile service, you must decide how to provide the best integration with the existing Cognos BI environment. The installation options that you choose depend on your reporting requirements, resources, and preferences. For more information, see the IBM Cognos Business Intelligence Architecture and Deployment Guide.

Ensure that the following conditions are met:

- IBM Cognos BI is installed and working, and both Cognos Mobile and Cognos BI server have the same version.
- If your installation uses BlackBerry devices, BlackBerry Enterprise Server with the BlackBerry MDS Connection Service is enabled on the server. This service allows BlackBerry device users to browse the web.

Tip: If users can currently browse the web, this service is already enabled.
For each BlackBerry operating system version, Cognos Mobile is packaged with cognos_mobile-for-whitelist.alx files that can be used to configure the BlackBerry Enterprise Server whitelist feature.

For more information about BlackBerry Enterprise Server and BlackBerry MDS Connection Service, see the BlackBerry Enterprise Server documentation.

To install and configure the Cognos Mobile service in your existing Cognos BI environment, perform the following procedure.

**Procedure**
1. Review and select a distribution option.
2. If you are using a BlackBerry device, configure IBM Cognos Mobile to communicate with the BlackBerry MDS Connection Service on the BlackBerry Enterprise Server.
3. Test the server installation and configuration.
4. Install the Cognos Mobile client components and test the installation.

**Distribution options for Cognos Mobile**
IBM Cognos Mobile is an integrated component of the IBM Cognos Business Intelligence architecture. You can install all IBM Cognos Mobile components on one computer, or distribute them across a network.

Cognos Mobile consists of the following components:
- Application tier components
- A gateway
- The Cognos Mobile client

If you are installing Cognos Mobile on one computer, you must install all those components where Cognos BI is installed.

If Cognos BI is installed on different computers, you must install the components in the following way:
- The Cognos Mobile application tier components with the Cognos BI application tier components
- The Cognos Mobile gateway and client with the Cognos BI gateway

All required components are installed and enabled by default.

**Cognos Mobile components installed on one computer**
You can install and configure IBM Cognos Mobile on a single computer.

The following diagram shows an example where all server components are installed on one computer.
Cognos Mobile components installed on separate computers

You distribute IBM Cognos Mobile components using the same installation and configuration method that you use to distribute IBM Cognos BI components.

Run the installation on each computer and then complete the configuration by specifying the location of distributed IBM Cognos BI components.

In a distributed installation, you install the Cognos Mobile application tier components on the systems where you want to run the Cognos Mobile service. You must install the Cognos Mobile gateway component on your gateway systems. These components include the sample mobile over-the-air installation pages and the Mobile client component themselves.

All instances of the IBM Cognos Mobile service must be able to access the database where the IBM Cognos Mobile tables are stored. If an IBM Cognos BI server instance is not configured with the database details for the IBM Cognos content store, or if you want IBM Cognos Mobile to use a database instance other than the IBM Cognos content store, use IBM Cognos Configuration to add a database.

The following diagram shows a scenario where the Cognos Mobile gateway is installed on one computer and the application tier components are installed on a different computer.

Figure 2. Cognos Mobile server components installed on one computer
The following diagram shows a scenario where the gateway components are installed on one computer, and the application tier components are installed on three computers. This installation is suitable for a medium to large environment.
Installing and configuring Cognos Mobile

Download the IBM Cognos Mobile package, and then use the installation wizard to install the IBM Cognos Mobile components on your computer.

Before installing the IBM Cognos Mobile components, ensure that IBM Cognos Business Intelligence is installed and working. Both IBM Cognos Mobile and IBM Cognos BI server must be at the same version.
To ensure IBM Cognos Mobile works properly, apply all required operating system patches and use only the versions of third-party software that are supported for an IBM Cognos product.

To review an up-to-date list of environments supported by IBM Cognos products, including information about operating systems, patches, browsers, web servers, directory servers, database servers, and application servers, visit the Supported Software Environments site (http://www.ibm.com/support/docview.wss?uid=swg27037784).

**Procedure**

1. If you are installing to a directory that contains other IBM Cognos BI components, stop the IBM Cognos BI service.
2. Go to the location where you downloaded IBM Cognos Mobile and choose the setup program for your operating system:
   - On Microsoft Windows, in the operating system directory, double-click the issetup.exe file.
   - On UNIX or Linux operating systems, in the directory that is appropriate for your operating system, if you use XWindows, type ./issetup.
   If you do not use XWindows, run an unattended installation. For more information, see the IBM Cognos Business Intelligence Installation and Configuration Guide.

   **Important:** When you use the issetup command with XWindows, Japanese characters in messages and log files may be corrupted. When installing in Japanese on UNIX or Linux, first set environment variables LANG=C and LC_ALL=C (where C is the language code, for example ja_JP.PCK on Solaris), and then start the installation wizard.
3. Select the language to use for the installation.
4. Follow the directions in the installation wizard.
   You are installing application tier components, the gateway, and the Cognos Mobile client components. The application tier components are used by the IBM Cognos Mobile service. The gateway and Mobile client components are used for an over-the-air installation or a connected installation.
   Next, you must configure IBM Cognos Mobile.
5. In the Finish page of the installation wizard, click Start IBM Cognos Configuration.

   **Tip:** You can also start IBM Cognos Configuration later, from the Start menu > Programs > IBM Cognos 10 > IBM Cognos Configuration.
6. To enable the IBM Cognos Mobile service, in the Explorer window, under Environment, IBM Cognos services, set Mobile service enabled to True.
7. To enable the BlackBerry push feature, set the BlackBerry MDS Connection Service host names and port numbers as follows:
   a. Obtain the host names and port numbers from your BlackBerry administrator.
   b. In the Explorer window, click Environment.
   c. In the Properties window, under Mobile BlackBerry Settings, for the MDS host names and port numbers property, click in the Value column and then click the edit icon.
   d. In the Value - MDS host names and port numbers dialog box, click Add
   e. Type a value, using the format host_name_of_Blackberry_Server:port
The port used for the push feature is usually port 8080 of the Blackberry Enterprise Server.

Test the URL in a browser first. The result displays a status page. For distributed installations, specify multiple servers.

f. Repeat steps d and e until you enter all values, and then click OK. For more information, see “BlackBerry MDS Connection Service” on page 27.

8. If Cognos BI Content Manager and Cognos Mobile application tier components are not installed in the same location, you must configure a Cognos Mobile database.
   a. In the Explorer window, under Data Access, click Mobile.
   b. From the Edit menu, click New resource > Database.
   c. In the Name field, type the name for your database.
   d. In the Type field, click the database type that you want.
   e. Click OK.
   f. In the Database - Resource Properties window, type the Database name and other details for the database that you chose.

9. From the File menu, click Save.

10. From the Actions menu, click Start or Restart.
    The Cognos Mobile tables are automatically created after the Mobile service starts for the first time. Unless you specified a different Cognos Mobile database, the tables are created in the BI content store database and use the same credentials as the BI content store.
    If the Cognos Mobile application tier components are installed in a different location than Cognos Content Manager and if the Mobile tables are not created upon startup, ensure that the Cognos Mobile database is configured.
    If the tables were not created, perhaps because the IBM Cognos BI security credentials do not allow it, you can create them manually. The creation scripts are available in the c10_location/configuration/schemas/mobile directory.

**Setting up the database client**

The IBM Cognos Mobile service must access the content store database directly rather than through the Content Manager. Therefore, the service must have access to the same Java Database Connectivity (JDBC) drivers that are installed with IBM Cognos Business Intelligence.

The service has direct access to the JDBC drivers installed with Cognos BI if Cognos Mobile uses the same Content Manager as Cognos BI, or if it uses a Microsoft SQL Server database or a Derby database. However, if IBM Cognos Mobile does not use the IBM Cognos BI Content Manager or if it uses a DB2® database or Oracle database, you need to set up the database client software to allow direct access to the content store database.

For information about setting up database connectivity for the content store database, see the IBM Cognos Business Intelligence Installation and Configuration Guide.

If you want to use a database other than the Content Manager database that IBM Cognos BI is configured to use, you must define the other database using IBM Cognos Configuration. Ensure that you use one of the supported database servers to create the database. For more information about creating a content store, see the IBM Cognos Business Intelligence Installation and Configuration Guide.
Setting up the database client on Oracle

If you use Oracle as the database server for the content store, you must set up the Java™ Database Connectivity (JDBC) driver.

Procedure

1. On the computer where the Oracle client is installed, go to the ORACLE_HOME/jdbc/lib directory.
2. Copy the .jar file for your version of Oracle to the c10_location/webapps/p2pd/WEB-INF/lib on computers where IBM Cognos Mobile is installed as follows:
   - For Oracle 10g, copy the ojdbc14.jar file.
   - For Oracle 11g, copy the ojdbc5.jar file.

   These files include the driver required by the content store.

Setting up the database client on DB2

If you use DB2, you must set up the database client software and the Java Database Connectivity (JDBC) 2.0 driver. You must do this on every computer where Content Manager is installed after installing and before configuring IBM Cognos BI.

Procedure

1. Install the DB2 client software on the appropriate computers.
2. If the content store is on a different computer from IBM Cognos Mobile, do the following:
   a. Configure a database alias to the content store by running the DB2 Client Configuration Assistant.
      - On UNIX or Linux operating systems, use the DB2 command line interface.
   b. When you configure the IBM Cognos Mobile computers, ensure that they are all configured to use the same content store.
3. On Microsoft Windows operating systems, stop the DB2 services and the HTML Search Server.
4. On UNIX, ensure that the 32-bit DB2 libraries are in the library search path, which is usually the $DB2DIR/1ib directory or the $DB2DIR/1ib32 directory.
5. Copy the universal driver file, db2jcc.jar, from the DB2_installation/sql1ib/java directory to the c10_location/webapps/p2pd/WEB-INF/lib directory.
   If you are connecting to DB2 on z/OS®, use the driver version from Linux, UNIX, or Windows version 9.1 fix pack 5 or version 9.5 fix pack 2.
   To check the driver version, run the following command:
   ```java -cp path\db2jcc.jar com.ibm.db2.jcc.DB2Jjcc -version```
6. Copy one of the following license files from the DB2_installation/sql1ib/java directory to the c10_location/webapps/p2pd/WEB-INF/lib directory:
   - for DB2 on Linux, UNIX, or Windows, db2jcc_license_cu.jar
   - for DB2 on z/OS, db2jcc_license_cisuz.jar
7. On Windows, restart the DB2 services and the HTML Search Server.
8. On UNIX, if you are using type 2 JDBC connectivity, ensure that the 32-bit DB2 libraries are in the library search path, which is usually the $DB2DIR/1ib directory or the $DB2DIR/1ib32 directory.
9. Repeat the steps on the other IBM Cognos BI computers where the software must be installed.
Results

You can tune the database to take advantage of DB2 features. For more information, see the IBM Cognos Business Intelligence Architecture and Deployment Guide.

DB2 on z/OS as a Mobile database

You can use DB2 on z/OS as your mobile database.

Connection settings to DB2 on z/OS are similar to those for DB2 on Linux, UNIX, and Microsoft Windows operating systems. However, additional advanced settings must be configured.

A database administrator must run scripts to create a set of tablespaces required for the mobile database. The scripts must be modified to replace the placeholder parameters with ones that are appropriate for your environment.

Suggested settings for creating a DB2 Mobile database on z/OS

The database you create for the mobile database must contain the specified configuration settings.

To ensure a successful installation, use the following guidelines when creating the Cognos Mobile database.

- Create a database instance, storage group, and a user account for the Cognos Mobile store.
  A user must have permissions to create and delete tables in the database. IBM Cognos Business Intelligence uses the credentials of the user account to communicate with the database server.
- Ensure you reserve a buffer pool with a page size of 32 KB, and a second one with a page size of 4 KB, for the database instance.
- Administrators must run a script to create tablespaces to hold Large Objects and other data for the Cognos Mobile database to use the tablespaces.
- Database administrator must back up the IBM Cognos BI databases regularly because they contain IBM Cognos data. To ensure the security and integrity of the databases, protect them from unauthorized or inappropriate access.

Creating tablespaces for the Cognos Mobile database on DB2 for z/OS

A database administrator must run scripts to create a set of tablespaces required for the mobile database. The scripts must be modified to replace the placeholder parameters with ones that are appropriate for your environment.

Ensure that you use the naming conventions for DB2 on z/OS. For example, all names of parameters must start with a letter and the length must not exceed eight characters.

For more information, see the IBM DB2 documentation.

Procedure

1. Connect to the database as a user that has privileges to create and drop tablespaces and to allow execution of SQL statements.
2. Go to the directory that contains the scripts:
   c10_location/configuration/schemas/mobile/db2zOS.
3. Open the `tablespace_db2zOS.sql` script file.

4. Add a connection statement to the beginning of the script.
   For example,
   ```
   connect to databasename/
   ```

5. Use the following information to help you replace the generic parameters with ones appropriate for your environment.
   - **COGMOBDB**
     Specifies the name of the mobile database.
   - **DB0AUSR**
     Specifies the name of the storage group.
   - **BP32K**
     Specifies the name of the buffer pool.

6. Save and run the script `tablespace_db2zOS.sql`.
   For example,
   ```
   db2 -td/ -vf tablespace_db2zOS.sql
   ```

7. Open the `rightsGrant_db2zOS.sql` script file and replace the **COGMOBDB** and **MOBUSR** placeholder parameters with the required database name and user name respectively.

8. Add a connection statement to the beginning of the script.
   For example,
   ```
   connect to databasename/
   ```

9. Save and run the script `rightsGrant_db2zOS.sql`.
   For example,
   ```
   db2 -td/ -vf rightsGrant_db2zOS.sql
   ```

10. Open the `initialize-schema-version-table.sql` script file, replace the `COGMOBDB` placeholder parameter with the required database name, and save the script.

11. Open the `upgrade-lock-object-init.sql` script file, replace the `COGMOBDB`, `DB0AUSR`, and `BP32K` placeholder parameters with the required database, storage group, and buffer pool names, and save the script.

12. Open the remaining script files starting with `upgrade`, and replace the `COGMOBDB` and `DB0AUSR` placeholder parameters with the required database name and storage group name respectively.

13. Save the scripts, but do not run them manually.
   The scripts will run automatically when the Mobile Service is started.

### Results

The Cognos Mobile database is created. You can now specify the Cognos Mobile database in IBM Cognos Configuration.

For more information about IBM Cognos Configuration, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

### Redeploy IBM Cognos BI to the application server

If IBM Cognos Business Intelligence is running on an application server other than Tomcat, then after installing and configuring IBM Cognos Mobile, you must regenerate the EAR or WAR files and redeploy them to the application server.
Testing the installation and configuration

You can test your configuration settings before you start the IBM Cognos Mobile service.

Procedure

1. From the Start menu, click Programs, IBM Cognos BI, IBM Cognos Configuration.
2. In the Explorer window, click Environment.
3. Click IBM Cognos BI service.

   In the Properties window, if you see Mobile service enabled displayed and set to True, your installation is working.

Results

You can now install and configure IBM Cognos Mobile Client Components.

BlackBerry MDS Connection Service

Before BlackBerry devices can communicate with the IBM Cognos Mobile service, the BlackBerry MDS Connection Service component of BlackBerry MDS Services must be enabled.

If NTLM is used, HTTP authentication support must also be enabled. This instructs the BlackBerry Enterprise Server to help the BlackBerry mobile devices navigate the security exchange needed by Microsoft Internet Information Services (IIS).

Additionally, Cognos Mobile can use the BlackBerry MDS Connection Service capabilities to push reports to BlackBerry device users and to synchronize the reports. The push notifications that allow the IBM Cognos server to notify a BlackBerry device that new content is available for it on the server, are very small messages that do not impact the server in any significant way. The IBM Cognos administrator must work with the BlackBerry administrator to ensure that this functionality is configured correctly.

If you have multiple BlackBerry MDS Connection Service servers and you have users across these servers who need to connect to the same IBM Cognos Business Intelligence server, you must designate one of the servers as the primary Connection Service push server. Then, you must set IBM Cognos Mobile to use that server, which will in turn pass connection requests to the appropriate Connection Service server.

You can have multiple primary servers. For example, if your organization has a Sales department and a Finance department, each with multiple BlackBerry Enterprise Servers, you would designate one server in each department as the primary server.

After the BlackBerry MDS Connection Service is enabled, BlackBerry device users can browse the web using the BlackBerry browser on their devices. Browsing increases the load on the BlackBerry Enterprise Server. If this is a concern, it is possible to configure the BES to restrict MDS-CS data services to only the IBM
Cognos Mobile application. An alternative would be to have a firewall on the BES server to allow access only to the IBM Cognos Mobile server.

IBM Cognos Mobile uses data in the same way that the browser on the BlackBerry does. Push notifications are very small messages that don't impact the server in a significant way.

For information about enabling Connection Service and primary push servers, see the BlackBerry Enterprise Server documentation.

---

**Methods of installing and configuring IBM Cognos Mobile client components**

After you install and configure IBM Cognos Mobile server components, with the exception of the iPad, Android, BlackBerry PlayBook, and iPhone, you must install the IBM Cognos Mobile client components on each mobile device that must access IBM Cognos Business Intelligence reports or analyses.

With the iPad (native version), users download IBM Cognos Mobile from the Apple App Store.

With the iPad (web version), Android, BlackBerry PlayBook, and iPhone, you do not install the client components. Instead, you configure IBM Cognos Mobile using a web application that you access using a URL.

IBM Cognos Mobile client components can be installed in one of the following ways:

- Using a push deployment
  For BlackBerry installations, the BlackBerry administrator can use the BlackBerry Handheld Configuration tool and then push the configured software over-the-air to users.
- Installing from the device
  Users of BlackBerry devices can download the client from the web.
- Using a desktop deployment.
- Installing from the device
  Users of BlackBerry devices can download the client from the web.
- Using a desktop deployment.

With the web application, the IBM Cognos Mobile client components are not installed on the tablet or device. Instead, users configure and run IBM Cognos Mobile using a web application which they access using one of the following URLs.

- For the default IBM Cognos BI location, type http://servername/ibmcognos
- and, when prompted, select the Mobile portal or the desktop portal
- For the CGI gateway, type http://servername/ibmcognos/m
- For an ISAPI gateway, type http://servername/ibmcognos/m/isapi

**Tip:** After opening the web application in the browser, add this page to your home screen.

For BlackBerry device installations, BlackBerry Enterprise Server must have the BlackBerry MDS Connection Service component enabled for each BlackBerry account that needs access to IBM Cognos Mobile. For more information, see the BlackBerry Enterprise Server documentation.
Installing IBM Cognos Mobile client using the BlackBerry handheld configuration tool

An IBM Cognos Mobile installation includes all the files needed for a BlackBerry administrator to package and push the rich client to mobile device users.

This is done by copying the rich client files to a shared location. Using a tool available with the BlackBerry Enterprise Server, BlackBerry administrators package the application that will be pushed to the mobile device users.

Typically, the BlackBerry administrator pushes the IBM Cognos Mobile client components to the BlackBerry device users. The BlackBerry administrator should perform this type of installation during off-peak hours.

The user is not involved but may notice some background activity and server communication during the installation. For most first time installations or upgrades, no reboot is needed. If a reboot is needed, the BlackBerry device prompts the user before it reboots the device.

Procedure

1. Use the BlackBerry Handheld Configuration tool to generate a software configuration that specifies the base operating system software for a BlackBerry device, and includes the IBM Cognos Mobile client application.
   
   For more information, see the BlackBerry Enterprise Server documentation.

2. Push the configuration to the BlackBerry device users.

Install and configure IBM Cognos Mobile client so that users can install from the web

You can configure IBM Cognos Mobile so that users can install the client over-the-air from their mobile devices. This type of installation is useful for remote users who must upgrade their installation without intervention by the device administrator.

The IBM Cognos Mobile rich client program files are located in the c10_location\webcontent\mobile directory.

For mobile device browsers to recognize the file extensions that are used to install mobile applications over-the-air, you must also register additional files or MIME types with your web server. You must register MIME types for the BlackBerry devices.

You must register the following MIME types on your web server:

<table>
<thead>
<tr>
<th>File extension</th>
<th>MIME type</th>
</tr>
</thead>
<tbody>
<tr>
<td>.cod</td>
<td>application/vnd.rim.cod</td>
</tr>
<tr>
<td>.jad</td>
<td>text/vnd.sun.j2me.app-descriptor</td>
</tr>
</tbody>
</table>

Only the steps for IIS web server versions 5.x and 6.0 are included here. If you are creating MIME types for a different web server, see the documentation for that web server.
Before you begin

Before installing IBM Cognos Mobile client on the mobile device, ensure that the user has access to the web browser application on the device and that the browser can access the IBM Cognos BI server through its regular webpage address, c10_location.

Procedure

1. From the Windows Control Panel, click Administrative Tools, Internet Information Services.
2. Right-click the IBM Cognos BI web site, and click Properties.
3. On the HTTP Headers tab
   • for IIS 5.x, click File Types
   • for IIS 6.0, click MIME Types
4. Click New Type.
5. For a BlackBerry installation, do the following:
   • In the Associated extension box, type .cod.
   • In the Context type (MIME) box, type application/vnd.rim.cod.
   • Click OK.
   • Click New Type.
6. For a BlackBerry do the following:
   • In the Associated extension box, type .jad
   • In the Context type (MIME) box, type text/vnd.sun.j2me.app-descriptor
   • Click OK.
7. Click OK.
8. Stop and restart your IIS service. From the Windows Control Panel, click Administrative Tools, Services. Click World Wide Web Publishing to stop the service and click it again to start the service.

Results

After you install the IBM Cognos Mobile server components and configure your web server as needed to support an over-the-air installation by users, mobile device users can install the IBM Cognos Mobile client.

The default URL for the web installation is http://c10_location/mobile/index.html

Installing IBM Cognos Mobile client components using a desktop deployment

Device users can install IBM Cognos Mobile and manage synchronization settings for their devices using a desktop deployment.

BlackBerry devices

For a desktop deployment using a BlackBerry device, users can use the BlackBerry Desktop Manager.

The files are located in the c10_location\webcontent\mobile\rim_desktop directory.
For information about installing client components using a desktop deployment, see the BlackBerry Desktop Application Loader documentation.

Performance maintenance

This section includes topics about estimating and maintaining the performance of your IBM Cognos Mobile environment.

Estimate the bandwidth required by IBM Cognos Mobile

IBM Cognos Mobile sends compressed versions of reports from the server to the mobile device. The size of a compressed report might range from 2 KB for a single-page report that contains text and a crosstab, up to possibly 500 KB for a 10-page report that contains multiple detailed charts on every page.

Each version of a report is sent only once. It is then stored in a cache on the mobile device. A mobile user can then view the report any number of times on the device without consuming any additional bandwidth.

Other operations, such as browsing the content store and answering prompts, also consume bandwidth. The bandwidth consumed is proportional to that used by a desktop browser performing the same action, but smaller because extraneous formatting information would not be exchanged.

IBM Cognos Mobile engages in intelligent polling to detect changes on the server. In an idle state, each mobile device sends a small data message to the server every 24 hours. (Note that this value is configurable). If there is heavy usage, where a mobile device user runs many reports throughout the day and schedules many reports for delivery to the mobile device, the device automatically checks in with the server more frequently.

To estimate bandwidth costs, an administrator can use the following formula as a guide:

\[(\text{number of users}) \times (\text{average size of a report}) \times (\text{number of adhoc reports run each day per user} + \text{number of scheduled reports sent to each user per day}).\]

BlackBerry offers a tool called the Performance Engineering Resource Kit (PERK). You could use this tool to benchmark IBM Cognos Mobile’s resource usage given the specific usage patterns in your environment. For more information, see the BlackBerry documentation.

Estimate the required number of servers

The load generated by one user using IBM Cognos Mobile on a given server (dispatcher) is roughly equal to the load generated by that same user using the IBM Cognos desktop products.

Specifically, if you compare the resources it takes for a desktop user to browse some folders, run a report, answer some prompts, and view the resulting report, and the resources it takes for a mobile user to do the same thing, the resources consumed are approximately the same.

So, to estimate the number of servers needed for your mobile users, you can use the same formula that you use to estimate the number of servers needed for your desktop users.
Estimating the size of a report

You can use typical reports to determine the size of the content that is transferred over the wireless carrier’s network to the mobile device.

Procedure

1. Remove all reports from the mobile device.
2. Run the report that you want to know the size of.
3. On your desktop browser, type the following request: http://servername/alias/cgi-bin/cognos.cgi/mobileService?mob_op=about
4. If you have security enabled, log on.
   Ensure that you log on as the same user that ran the report on the mobile device.
   A small XML document appears. Within the document there is a section that looks like the following example showing the number 28. The actual number you see depends on your report:
   <s2><inbox>28</inbox></s2>

   Tip: Because you have only one report, only one number should appear. If you see multiple numbers separated by colons, this means that you did not delete all reports. You must delete all reports and repeat steps 1 to 3.
5. Type the following request, replacing the number 28 with the number that you obtained in step 4: http://servername/alias/cgi-bin/cognos.cgi/mobileService?mob_op=downloadDB&mob_ir=28
   The response to this request is the actual report contents.
6. Save this response as a file, and record its size.
   This file is what is transferred over the network.
7. Repeat these steps for a number of typical reports to get an idea of the amount of data that your mobile users use.

Background synchronization

With a default installation of the IBM Cognos Mobile service, users can run and view all supported reports. With background synchronization, which uses the BlackBerry push feature, you can automatically push reports to a device as they become available.

To support background synchronization, the BlackBerry MDS host names and port numbers must be configured, as described in “Installing and configuring Cognos Mobile” on page 21.

After configuration, background synchronization is always available on the server for BlackBerry.

Clients automatically use background synchronization by default.

Uninstall IBM Cognos Mobile

To uninstall IBM Cognos Mobile, uninstall the components from the server and the rich client from the device.
All mobile device administration programs, such as BlackBerry Enterprise Server, provide a process for uninstalling client software over the air. For more information, see the documentation for the device.

**Uninstall from the server**

IBM Cognos Mobile components on the server are removed when you uninstall IBM Cognos Business Intelligence. You can uninstall IBM Cognos Mobile server components all at once if they are all installed on one computer, or individually for a distributed installation. For instructions, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

**Location-aware reports**

A location-aware report filters report data based on the user’s current location as determined by the mobile device’s Global Positioning System (GPS) coordinates.

For example, a vice president of sales who travels frequently to visit his or her regional sales managers could use location-aware reports to see information about the region he or she is currently visiting.

Location-aware reporting is available only on GPS-enabled BlackBerry devices.

The Mobile administrator must set up location-aware parameters so that report authors can create location-aware reports in Report Studio. These reports must contain at least one prompt that asks for location information. Location information can be determined by either GPS coordinates or defined regions, such as states, provinces, cities, or voter regions. The administrator defines the parameter names for the prompts, and the report author must know the parameter names when adding the location prompts to reports.

**Setting up location-aware parameters for prompts**

Before specifying the location-aware prompts, consider whether the prompts will use parameters based on coordinates or defined regions.

If your data does not have associated latitude and longitude information for each data point, use geographic regions. For example, sales data can be associated with a city or sales territory. However, if your data is geo-encoded, that is, the data has associated latitude and longitude coordinates that can pinpoint a precise location, use these coordinates to specify the location-specific information for users.

Location aware reports that use prompts based on pre-defined regions, such as states, provinces, cities, or voter regions, can also use prompts based on GPS coordinates. Prompts based on GPS coordinates can also use prompts based on predefined regions.

Differentiate the parameter names used in location-aware reports from the parameter names used in other reports. Choosing a generic name, such as city, will extend the search to every prompt named city in any report.

**Defining report prompts based on region**

Location-aware reports can use prompts based on pre-defined regions, such as states, provinces, cities, or voter regions.
Procedure

1. Create a text file where you will define the regions to be used in the reports. Define one region per line using the following format:

   11.1111;-22.2222;Region1

   where 11.1111 is the latitude at the center of Region1, and -22.2222 is the longitude at the center of Region1. For example, 40.7499;-73.9980;Manhattan.

   You can format the entries differently from the example. The entries are parsed based on the regular expression that you define in step 4.

2. Save the text file in the c10_location/configuration/mobile/ directory.

3. In an XML editor, open the file location.xml from the c10_location/configuration/mobile directory.

   Note that all entries in this file are case-sensitive.

4. Edit the regular expression in the regex element to match the format that is used in the text file that you created in step 1. In the following example, the regular expression, ^(.*);(.*);(.*);$ includes three capture-group elements that match the three items separated by semi-colons:

   <location>
   <file active="true" filename="regions.data">
   <regex latitude="1" longitude="2">
   ^(.*);(.*);(.*);$ <capture-group index="3" name="CityCenter"/>
   </regex>
   </file>
   </location>

   If you are using more than one location-aware prompt in a report, you can accommodate the prompts by inserting additional file elements.

5. Edit the latitude and longitude attributes to identify the capture-group elements within the regular expression that contain the latitude and longitude data.

   In the example, the first capture group is latitude, so the latitude attribute is 1.

6. Within the regex element, add capture-group elements to indicate which capture-group elements correspond to the parameter fields in the location-aware report.

   In the example, the third capture-group in the expression identifies the parameter value for "CityCenter" as Manhattan.

7. Save your changes.

Defining report prompts based on GPS coordinates

Location aware reports can use prompts based on GPS coordinates.

Procedure

1. In an XML editor, open the location.xml file from the c10_location/configuration/mobile directory.

   Note that all entries in this file are case-sensitive.

2. Add the following sample code into the file.

   ```xml
   <location version="1.0" encoding="UTF-8">
   <location>
   <projection active="true">
   <proj4>
   +init=epsg:2263+x_0+984252
   </proj4>
   <columns x="x_coord" y="y_coord"/>
   </projection>
   </location>
   ```
3. In the columns element, enter the parameters that were created in the location-aware report. Use the x_coord attribute to specify the latitude and the y_coord attribute to specify the longitude.

   When the user runs a report in IBM Cognos Mobile, the GPS coordinates are retrieved from the device.
   
   Note that the GPS information is returned to the server as raw latitude and longitude data. This data may need to be converted to match the geo-encoding used by your existing enterprise data. The server handles the conversion automatically using a mathematical algorithm based on the PROJ.4 specification.

4. Enter the PROJ.4 description of your coordinate system into the location.xml file. In the example, the description "+init=epsg:2263 +x_0=984252" is used.

5. Save your changes.

Results

When the user runs a report in IBM Cognos Mobile, the GPS coordinates are retrieved from the device. In the text file that defines the regions for the report, the entry that most closely matches the user's location populates the parameters values.

---

Using the buildSettings tool to configure a BlackBerry client (Microsoft Windows only)

The buildSettings tool generates a deployment package that embeds a specified IBM Cognos Business Intelligence server URL so that the BlackBerry users do not need to enter the URL.

The tool pre-configures the list of available server URLs in the IBM Cognos Mobile client. The client configurations are created and stored in the c10_location/configuration/mobile directory. You can have a maximum of four server URLs.

To configure the BlackBerry clients, the rapc.exe BlackBerry compiler is required. The compiler runs only on the Windows operating system. To use the rapc.exe BlackBerry compiler, a JDK must be installed.

Procedure

1. Back up any existing build settings before continuing.

2. Run the buildSettings tool from the command line using the following syntax:
   
   `buildSettings "url1" ["url2" "url3" "url4"]`
   
   Here is an example of a command:
   
   `buildSettings "http://server1/c10/cgi-bin/cognos.cgi"
   "http://server2/c10/cgi-bin/cognos.cgi"`


4. Modify the index.html file before users can install the client application.

---

Configuration of Apple push notifications for the iPad native application

Apple push notifications notify the iPad native application users about the availability of new IBM Cognos BI reports.
To send push notifications, the Cognos Mobile server requires an SSL certificate from Apple. The SSL certificate is included with each released version of IBM Cognos Mobile, and it is valid for 12 months from the date when it was issued by Apple. The administrator must monitor the certificate expiry date and update the certificate before it expires. Otherwise, the users stop receiving push notifications. For more information, see “Managing the SSL certificate for Apple push notifications.”

The following TCP ports are used for communication between the Cognos Mobile server, the Apple iPad device, and the Apple Push Notification Service (APNS):

- Port 2195 is used by Cognos Mobile server to send notifications to APNS.
- Port 2196 is used by Cognos Mobile server to reach the APNS feedback service.
- Port 5223 is used by the iPad device connecting to APNS using Wi-Fi.

Keep these ports open in the internet connection firewall.

### Managing the SSL certificate for Apple push notifications

The administrator monitors the log files and emails for messages about the approaching certificate expiry date, and updates the certificate when needed.

#### About this task

The SSL certificate for Apple push notifications is valid for 12 months from the date when it was issued by Apple. Fourteen days before the certificate expiry date, the Cognos Mobile server starts logging warnings in the `c10_location\logs\mob.log` file about the approaching certificate expiry date. To ensure that the warnings about the certificate expiry date are logged, server logging must be set to the Warn level at minimum. When the logging level is set to Error, the certificate expiry messages are not logged.

In addition to the log file warnings, the Cognos Mobile server can also be configured to send emails to administrators about the approaching certificate expiry date.

The text of the warning in the log file or in the email body, in English only, specifies the certificate expiry date and the URL of the IBM Support website (http://www.ibm.com/support/) where the latest IBM Cognos Mobile fix pack with updated Apple SSL certificate is available.

#### Procedure

1. Ensure that the following configuration settings are specified in IBM Cognos Administration. These settings are used to configure the Cognos Mobile server to send email messages to administrators about the certificate expiry date.
   - Notification email for Apple push notifications
   - Frequency check for Apple push notification certificate expiry date
   - Expiry threshold for Apple push notifications
   For more information, see “Enabling Apple push notifications” on page 37.

2. Monitor the log messages and emails for information about the certificate expiry date.

3. To update the certificate, go to the IBM Support website (http://www.ibm.com/support/), and download the latest Cognos Mobile fix pack that includes a valid certificate for Apple push notifications.

4. Install the new certificate on all affected servers.
Enabling Apple push notifications

The administrator must configure the Mobile service settings that are associated with Apple push notifications before users are able to receive push notifications.

About this task

The first time that a push-enabled application registers for push notifications, the users receive an alert asking them if they want to receive notifications. After responding to this alert, the users do not see the alert again unless their device is restored or the application was uninstalled for at least a day.

Procedure

1. In IBM Cognos Administration, click the Mobile tab.
2. Click Server Configuration.
3. Specify the following Notification settings:

   Support for Apple push notifications
   Enables Apple push notifications for the iPad native application, and specifies the wording of the message that is displayed to iPad users. The values are:
   - None - Apple push notifications are disabled and messages are not sent from the server to the Apple Push Notification Service.
   - Name - Apple push notifications are enabled. The messages sent from the server to the Apple Push Notification Service include the report name.
   - Generic - Apple push notifications are enabled. The messages sent from the server to the Apple Push Notification Service do not include the report name. Instead, a generic message is displayed.
   Default: Name

   Notification email for Apple push notifications
   Specifies the email address or addresses of administrators that are notified about the Apple push notifications certificate expiry date. The value for this setting is an email address in the following format: admin@domain.com. Multiple email addresses must be separated with a semicolon (;). For example, admin1@domain.com;admin2@domain.com

   Expiry threshold for Apple push notifications
   Specifies the number of days before the Apple push notifications certificate expiry date when the administrators start receiving emails about the approaching expiry date.
   Value: 1 to 365
   Default: 14

   Feedback interval for Apple push notifications
   Specifies the time interval, in hours, for the Cognos Mobile server to check the Apple push notifications feedback service for failed notifications. The feedback service maintains a list of devices for which there were repeated, failed attempts to deliver notifications. The Cognos Mobile server will stop sending notifications to the devices that it obtained from the feedback service.
   Values: 1 to 720
   Default: 24
Frequency check for Apple push notification certificate expiry date
Specifies, in hours, the frequency with which the Cognos Mobile service checks for the Apple push notifications certificate expiry date. The first check is done when the Cognos Mobile service is started.

Value: 1 to 8760
Default: 24

4. Click the Apply mobile configuration button.
5. Specify the Database.DeviceExpiryIntervalDays advanced setting for the Mobile service. For more information, see Appendix A, “Specifying Cognos Mobile advanced settings,” on page 69.

Push notifications on the user's iPad device
A text alert notifies the iPad user when a new report is available and the application icon is updated with the number of new reports. The user can open the application from the notification.

The IBM Cognos Mobile native iPad application can receive push notifications from multiple Cognos BI servers. If users no longer want notifications to be displayed, they must turn off notification settings for the application in iOS settings.

Cognos Mobile fix packs
If a fix pack is available when you are installing or upgrading IBM Cognos Mobile, you must install it after you install the IBM Cognos Business Intelligence components.

For more information, see the IBM Cognos Business Intelligence Installation and Configuration Guide.

If a fix pack becomes available after you have deployed Cognos Mobile, you must stop the service, install the fix pack in the same location as the Cognos BI components, and then start the service.

Fix packs are available for download from the IBM Support website (http://www.ibm.com/support/).

Important: Fix packs are not standalone installations. You must install them on computers that have IBM Cognos BI server components installed. Install the fix pack or packs that are appropriate for IBM Cognos Mobile. To check your version, open the component list file at c10_location\cmplst.txt and check the line that starts with CBBISRVR_version=.

Installing fix packs on Microsoft Windows
Use the following steps to install a fix pack.

Before you begin
1. If IBM Cognos Mobile is running, open IBM Cognos Configuration and stop the IBM Cognos Mobile service.
2. Create a backup of the content store database.
3. Back up any customized files from the current installation.
4. Download the appropriate compressed tar file.
Procedure

1. Change to the directory where you downloaded the fix pack.
2. Using your file compress and decompress utility, decompress the .tar.gz file. If you are using WinZip, choose Use folder names.
3. If you want to see the version of a component before you install it, unpack the tar file to disk, or read the table of contents of the tar file.
4. Go to the location where you downloaded and extracted the fix pack files.
5. In the download location, go to the win32 directory and double-click the issetup.exe file.
6. Follow the directions in the installation wizard, installing in the same location as your existing IBM Cognos components.
   The issetup program prompts you to allow the fix pack to create a backup copy in the installation folder before copying new files.
7. To return your deployed IBM Cognos Mobile product to service, open IBM Cognos Configuration, save the configuration, and then start the IBM Cognos Mobile service.
8. If you have a distributed environment, repeat these steps for all remaining IBM Cognos servers.
9. If you are running IBM Cognos Mobile on an application server other than the default, Tomcat, redeploy IBM Cognos Mobile to the application server.
   For instructions, see the IBM Cognos Business Intelligence Installation and Configuration Guide.

Installing fix packs on UNIX or Linux

Use the following steps to install a fix pack.

Before you begin

1. If IBM Cognos Mobile is running, open IBM Cognos Configuration and stop the IBM Cognos Mobile service.
2. Create a backup of the content store database.
3. Back up any customized files from the current installation.
4. Download the appropriate compressed tar file.

Procedure

1. Copy the fix pack to the appropriate operating system.
2. Change to the directory where you have downloaded the fix pack installation image.
3. Enter the following command: gunzip <filename>.tar.gz | tar xvf –
4. If you want to see the version of a component before you install it, unpack the tar file to disk, or read the table of contents of the tar file.
5. Go to the location where you downloaded and extracted the fix pack files.
6. To start the installation wizard, type
   ./issetup
   If you do not use X Window System, run an unattended installation. For more information, see the IBM Cognos Business Intelligence Installation and Configuration Guide.
7. Follow the directions in the installation wizard to install to the same location as your existing IBM Cognos components.
The issetup program prompts you to allow the fix pack to create a backup copy in the installation folder before copying new files.

8. To return a deployed IBM Cognos product to service, open IBM Cognos Configuration, save the configuration, and then start the IBM Cognos service.

9. If you have a distributed environment, repeat these steps for all remaining IBM Cognos servers.

10. If you are running the IBM Cognos product on an application server other than the default, Tomcat, redeploy the IBM Cognos product to the application server. For instructions, see the IBM Cognos Business Intelligence Installation and Configuration Guide.
Chapter 4. Security

IBM Cognos Mobile combines the security measures of IBM Cognos Business Intelligence with the extra measures needed for mobile devices.

The security measures offer protection against loss and theft and against unauthorized access to the wireless network. The security applies whether the device is used in connected or disconnected mode.

The Cognos Mobile solution includes the following security measures that are implemented in the IBM Cognos and device-specific environments:

- Standard IBM Cognos data encryption
- Standard IBM Cognos authentication, including support for custom IBM Cognos authentication providers
- Lease key technology
- Device user authentication policies
- Device-based mobile encrypted database
- Standard device-specific secure data transmission and encryption
- Device-based password protection
- Remote device wiping

For information about Cognos BI security, see the IBM Cognos Business Intelligence Administration and Security Guide. For information about device security, see the documentation for that device.

Cognos Mobile supports web servers that are configured to use basic authentication. BlackBerry devices support Integrated Microsoft Windows authentication (NTLM) and Microsoft Active Directory.

Cognos Mobile supports single signon security configurations. However, typically, mobile device users are not preauthenticated to the security domain in the same way that desktop users are. Therefore, mobile device users usually have to provide their single signon credentials the first time they access the Cognos BI server.

**Important:** The IBM Cognos Mobile iPad application also supports single signon security configurations. Users can enable single signon from their iPad **Settings** by turning on the **Pass-through authentication** setting for the IBM Cognos application. When this setting is enabled, the iPad users are prompted for signon credentials the first time they access the Cognos BI server.

Optionally, logon credentials can be cached on the mobile device so that the user must log on only once to access both the device and Cognos Mobile. Cognos Mobile offers encrypted database technology as the content store on the device. Access to local device storage is controlled by a centrally-granted lease key that must be renewed periodically. You can configure the length of the lease, so that if the device is lost or stolen, the data will be inaccessible.

You can have different levels of security, depending on the needs of your organization. In addition to storing logon credentials on the device, you can allow anonymous logon or rely on the network security features of the mobile device.
For a higher level of security, you can use Cognos security for all communication or use lease key technology to control access to data.

## Cognos Mobile capabilities

The IBM Cognos Mobile capabilities in IBM Cognos Administration are used to restrict access to IBM Cognos Mobile for users and administrators.

**Tip:** The IBM Cognos Business Intelligence capabilities are also referred to as secured functions and features.

The Cognos Mobile capabilities include:

- **Mobile**
  This secured function is used to restrict access to Cognos Mobile for users. Only users, groups, or roles that have execute permissions for this secured function can log on to Cognos Mobile. When users who do not have the required permissions try to log on, they see an error message asking them to contact a Cognos BI administrator.

- **Mobile Administration**
  This secured feature of the Administration secured function is used to restrict access to the administration pages on the Mobile tab in Cognos Administration. Only users, groups, or roles that have execute permissions for this secured feature can access this tab to perform administration tasks, such as Mobile service configuration, for Cognos Mobile.

To simplify the process of setting access permissions for the Mobile and Mobile Administration capabilities, you can use the predefined roles Mobile Users and Mobile Administrators that exist in the Cognos namespace in Cognos Administration. The Mobile Users role contains permissions that are needed for access to Cognos Mobile for regular users. The Mobile Administrators role contains permissions that are needed for access to Cognos Mobile administrative functions on the Mobile tab in Cognos Administration. You can add users, groups, or roles from your organization’s directory to these roles and include these roles in your Cognos BI security policies. You can also ignore these roles, or delete them, and create your own security groups or roles to use for setting access permissions to Cognos Mobile.

Setting access permissions for the Mobile and Mobile Administration capabilities is one of the initial tasks that an administrator must perform when configuring Cognos Mobile. For more information, see the section about secured functions and features, and the section about initial security in the *IBM Cognos Business Intelligence Administration and Security Guide*.

## Password protection

Typically, organizations want to have password protection on mobile devices.

After a specified period of inactivity, users are prompted to reenter their device password and there may be a limit on the number of times they can try to enter a password. For example, by default, a BlackBerry user can try up to 10 times to enter the correct password. After that, the mobile device is reset, removing all data from the device. The user must reregister the device with the BlackBerry Enterprise Server. The data will then be restored to the device.
You can store IBM Cognos credentials for users on their mobile devices so that they need to enter their credentials only the first time they access Cognos Mobile. After that, they are still asked for their credentials each time they log on, but Cognos Mobile automatically enters their passwords for them. Only when the time limit is reached on the stored credentials do users need to reenter their credentials.

If a device PIN is configured on an iOS device, the IBM Cognos Mobile application encrypts the manually imported Cognos active reports that are stored on the device. This feature applies to active reports that are manually imported through email, iTunes, or a file server.

For information about how to enable or set password policies for a mobile device, see the documentation for the device.

### HTML and HTTP support during logon

The IBM Cognos Mobile product used on mobile devices is a native application, as opposed to a web application. It does not use a web browser, and does not use HTML to display reports on mobile devices.

However, IBM Cognos Mobile does use HTTP to communicate with the IBM Cognos BI server, and so it must interoperate with any web-based security mechanisms that govern access to the Cognos BI server.

To allow users to authenticate and to navigate through these security mechanisms, IBM Cognos Mobile shows basic HTML form elements and allows the user to perform the actions associated with them.

The following table shows the HTTP and HTML functions that are supported by IBM Cognos Mobile.

**Table 2. HTTP and HTML functions supported by Cognos Mobile**

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Redirects</td>
<td>Supports HTTP 301 Moved Permanently and HTTP 302 Moved Temporarily. It will follow both relative and absolute URLs given in the Location header.</td>
</tr>
<tr>
<td>HTML Redirects</td>
<td>Supports the HTML equivalent of an HTTP redirect, for example <code>&lt;meta http-equiv=&quot;Refresh&quot; content=&quot;3;URL=http://...&quot;&gt;</code>.</td>
</tr>
<tr>
<td>HTTP Authentication</td>
<td>Supports HTTP 401 Unauthorized both with the basic scheme and with NTLM. NTLM is predominantly a Microsoft authentication scheme, known also as Windows Integrated Authentication. Support for NTLM is present on BlackBerry devices if the HTTP Authentication Assistance setting is enabled on the BES.</td>
</tr>
<tr>
<td>HTML Forms</td>
<td>Shows the text of an HTML page (including text with anchor tags), buttons, and the input field types text, password, and hidden. It also shows the select input type, which is used to show a list of items that you can choose from, such as a list of security namespaces.</td>
</tr>
</tbody>
</table>

### Apple iPad application security

A security code can be used to restrict access to the IBM Cognos Mobile app for iPad users.
The Cognos administrator can specify that an iPad user must enter a security code to access the IBM Cognos Mobile app, and the amount of time that the Mobile app can remain inactive before the user must reenter the code to use the app. This functionality is controlled by the **Security code session timeout** configuration setting.

If the value of this setting indicates that the user needs a security code, this value also represents the number of seconds that the Mobile app can remain inactive before the user is prompted to reenter the security code to access the Mobile app.

In addition to this setting, there is also a default timeout value that is included with the Mobile iPad app. The value that you specify for the server setting overrides the default value in the app.

The users can turn off the server setting on the iPad, but they cannot change its value. If the setting is off, but the server setting requires the user to use a security code, the next time the user tries to run the app, he or she needs to re-authenticate with the server and is prompted to create a security code. Without this code, the users cannot see any local content.

The Cognos administrator can also set a limit on the number of failed attempts to enter the security code when logging on to the Mobile iPad app. This is controlled by the **Maximum number of attempts to enter a security code when accessing an iPad app** configuration setting. If the user exceeds the maximum number of attempts, all Cognos content on their iPad is destroyed. If the user needs a PIN to access the server, the number of retries specified by the server overrides the retry value on the iPad.

For more information, see the security settings in "Cognos Mobile service configuration settings" on page 54.

---

**Report data security on mobile devices**

All compiled and compressed versions of IBM Cognos BI reports are encrypted and stored locally in the mobile encrypted database of the mobile device. These reports can be read or otherwise interpreted only by the IBM Cognos Mobile client application.

You can use lease key technology to set an expiry time for report data that is stored on the mobile device. After the expiry time, the report data cannot be accessed on the device until the device can reestablish communications with the server, and the user is able to re-authenticate with the server.

If a device PIN is configured on an iOS device, the IBM Cognos Mobile application encrypts the manually imported Cognos active reports that are stored on the device. This feature applies to active reports that are manually imported through email, iTunes, or a file server.

---

**Erasing content from a device**

You may need to erase all content from a mobile device.

This may be necessary if a device is lost or stolen or an employee changes roles or leaves the company. Device passwords and lease key technology ensure that content is available only to authorized users.
For all devices, security and management is handled by third-party mobile device management solutions. For example, BlackBerry devices are managed through the BlackBerry Enterprise Server console.

If the mobile device is not connected to the BI server for a predetermined period of time, based on the hours specified in the Maximum number of hours to access Mobile local data stored on a device configuration setting, IBM Cognos data becomes inaccessible from the device. For more information about configuration settings, see “Cognos Mobile service configuration settings” on page 54.

### Setting a lease key

IBM Cognos Mobile uses the concept of a lease to govern access to data stored on mobile devices.

Data is leased from the server for a length of time controlled by the IBM Cognos administrator through the server setting named Maximum number of hours to access Mobile local data stored on a device. This setting specifies the maximum amount of time that a user can access data on a mobile device that is not in contact with the server. For example, the device is offline or out of wireless range. If the device is unable to renew its lease within the specified period of time, the data on the device becomes inaccessible.

**Procedure**

1. From a desktop browser, log on to IBM Cognos Connection with administrator privileges.
2. Click Launch > IBM Cognos Administration, and click the Mobile tab.
3. Click the Server Configuration page.
4. For the Maximum number of hours to access Mobile local data stored on a device, specify the required value in hours. Valid settings are 0 to 8760. The default is 36 hours. The value of 0 disables the lease key mechanism.
5. Click the Apply mobile configuration button.

### Setting user authentication policies for a mobile device

IBM Cognos Mobile device user authentication policies define whether IBM Cognos Business Intelligence authentication credentials are cached on the mobile device and how often users must reenter these credentials. Users must enter their credentials at least once.

All IBM Cognos BI timeouts apply to the mobile device user. The device user authentication policies are on top of timeouts associated with IBM Cognos BI.

There are one or two timeouts that affect the duration of a user session, depending on the device. The first is the CAM (IBM Cognos security control mechanism) passport setting in IBM Cognos BI, which applies to all devices. The second is the BlackBerry MDS HTTP authentication cache, which applies only to BlackBerry devices and is used for any HTTP authentication, including Microsoft Windows Integrated Authentication (NTLM).

If your IBM Cognos BI logons are based on NTLM, you can cache this information on your BlackBerry MDS Services server and prevent the logon window from
appearing for the duration of this cache timeout. You can enable the BlackBerry MDS Services HTTP authentication cache time limit, or increase it on the BlackBerry Enterprise Server.

When the passport setting limit expires, or in the case of BlackBerry devices, when the lower of the two time limits is reached, the user session ends. However, if the device authorization time limit exceeds the timeout that ended the session, the device authorization time limit remains in effect after the user session ends. Only when the device authentication time limit is reached do users need to reenter their credentials.

To simplify the authentication process for the user, the IBM Cognos administrator can allow credentials to be cached on the mobile device. Use the following steps to do that:

**Procedure**

1. From a desktop browser, log on to IBM Cognos Connection with administrator privileges.
2. Click **Launch > IBM Cognos Administration**, and click the **Mobile** tab.
3. Click the **Server Configuration** page.
4. For **Maximum number of hours to store cached credentials**, type a value in hours.
   Valid settings are 0 to 8760. The default is 0. The default value of 0 means that you do not want to store credentials on a device.

**Setting the timeout for the CAM passport setting**

You can set the CAM timeout on the computer where IBM Cognos Content Manager is installed.

**Procedure**

1. Open **IBM Cognos Configuration** on the computer where IBM Cognos Content Manager is installed.
2. In the **Explorer** window, click **Explorer > Authentication**.
3. In the **Properties** window, for **Inactivity timeout in seconds**, type the value that you want.
   For more information about IBM Cognos Configuration, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.

**Setting the timeout for the NTLM-based BlackBerry MDS HTTP authentication cache**

If your IBM Cognos Business Intelligence logons are based on NTLM, you can cache this information on your BlackBerry MDS Services server and prevent the logon window from appearing for the duration of this cache timeout.

On the BlackBerry Enterprise Server, you can enable the BlackBerry MDS HTTP authentication cache time limit, or increase it.

**Procedure**

1. In the BlackBerry MDS Services Connection Service properties window, on the BlackBerry administration page, click the **HTTP** tab.
2. Click the **Allow the Mobile Data Service to support HTTP Authentication** check box.
3. For **HTTP Authentication timeout (milliseconds)**, enter a value.
   The higher the value, the less often users will need to log on.
Chapter 5. Cognos Mobile administration

After IBM Cognos Mobile is installed and configured, you can perform the administration tasks to manage the delivery of IBM Cognos content to mobile devices. You can also customize the Cognos Mobile user interface by applying different themes for different users.

The Mobile tab in IBM Cognos Administration provides centralized administration capabilities for IBM Cognos Mobile. To access this tab, the administrator must have the required access permissions for the Mobile Administration capability. Mobile Administrators, one of the predefined roles in the Cognos namespace, can be used to specify access permissions for this capability. For more information, see “Cognos Mobile capabilities” on page 42.

Cognos Mobile uses the same set of users as IBM Cognos Business Intelligence (BI). For information about administering IBM Cognos BI, see the IBM Cognos Business Intelligence Administration and Security Guide. For information about IBM Cognos Connection, see the IBM Cognos Connection User Guide.

Configuring a Mobile theme

The Mobile theme defines the appearance of the IBM Cognos Mobile application welcome page. By default, the client applications use the default theme that is built into the product. You can create your own Mobile theme to customize the appearance of the application and configure the theme to make it available to the user groups and roles that you choose. At any time, administrators can revert to the default theme.

About this task

The configuration tasks include enabling support for Mobile themes; adding, editing, or deleting the themes; and defining which groups and roles can use the themes.

The same user can belong to different groups and roles and can, therefore, have access to different themes. To ensure that proper themes are applied for the users, the administrators must carefully consider which groups and roles they can choose when configuring the theme.

The Cognos Mobile default theme is defined in the defaultTheme.zip template that is installed with the product. Administrators can use this template as a starting point when creating a custom theme. Other than that, this template is not required for the product to function properly. For more information, see “Creating a custom Mobile theme” on page 50.

Procedure

1. From a desktop browser, log on to IBM Cognos Connection with mobile administrator privileges.
2. Go to IBM Cognos Administration, and click the Mobile tab.
3. Complete the following steps to ensure that theme support is enabled for the Mobile service:
   a. Click Server Configuration.
b. In the **Policy** group of settings, locate the **Mobile theme support** setting and ensure that the value of **themesOn** is specified for this setting.

c. Click the **Apply mobile configuration** button to save the configuration.

4. Open the **Mobile Theme Configuration** page.

5. To add a new theme, click the **New Theme** icon.

6. In the **Mobile Theme Configuration** page, complete the following steps:
   a. In the **Specify a name for the theme** box, type the theme name. You can specify any name that is meaningful for your environment.
   b. In the **Specify a theme file to upload** box, browse for a zip file that contains the theme resources.
   c. In the **Specify a group or role** box, click the **Choose Group** button and choose the groups or roles that need to use the theme. You can choose groups and roles from the Cognos namespace or from other active namespaces.
   d. Click **OK** when all parameters are properly specified.

   The theme name appears in the **Mobile Theme Configuration** page.

7. If you want to edit the theme, click its **Set properties** icon in the **Actions** column. You can edit any of the theme parameters.

8. If you want to delete the theme, select its check box and click the **Delete** icon in the toolbar.

   To revert to the Cognos Mobile default theme, delete the theme that is currently configured. The users who were using this theme automatically return to using the default theme when they connect to the Cognos BI server the next time.

9. Using an iOS device, connect to server for which the theme was configured to test if your changes were properly applied.

**Results**

The users can continue using the application while the theme resources are downloaded to their devices. The theme is applied when the users connect to the Cognos BI server the next time or refresh their application.

When a user wants to connect to multiple servers that might have different themes configured, the theme that is applied for the user is the theme that is configured for the server to which the client successfully connected first. Connecting to other servers does not change the user's theme even if the servers use different themes. To change the theme to the one that is configured for a different server, remove the connection to the server with the current theme. Then, the user can connect to the server that uses the required theme.

**Creating a custom Mobile theme**

You can create a custom Mobile theme to replace the default theme that is supplied with IBM Cognos Mobile.

**Before you begin**

Plan the design of your custom theme and prepare the required resources, such as image files.
About this task

When Cognos Mobile is installed, the installation directory `c10_location/templates/mobile` contains the `defaultTheme.zip` file. This is the default theme template. You can use this template as a starting point when creating your own custom theme.

The `defaultTheme.zip` file contains different directories and files. The `main_panel/index.html` file is the only file that is required for your custom theme. In this file you define all resources, such as images, that you want to use in your custom theme, and modify the color scheme and font styles.

The `nls` directory in the default theme template contains a directory structure for language-specific themes. You can emulate this structure or implement your own mechanism for creating language-specific themes.

You can use the following procedure as a guidance when creating a custom mobile theme based on the default theme.

Procedure

1. Go to the `c10_location/templates/mobile` directory, make a copy of the `defaultTheme.zip` file, and save it under a different name.
2. Extract the files from the `.zip` file that you created in the previous step.
3. Edit the `main_panel/index.html` file as required. This file must contain references to all resources that are included with the theme.
4. Compress all of your theme resources in one `.zip` file. At minimum, the `.zip` file must contain the modified `main_panel/index.html` file.
5. Save your theme `.zip` file to a directory of your choice.

Now, you can configure IBM Cognos Mobile to use the custom theme. For more information, see "Configuring a Mobile theme" on page 49.

Pre-configuring the Cognos Mobile native apps for users

Configure the IBM Cognos Mobile application to streamline the setup for users and control how the application works on iOS and Android devices.

About this task

You can encode and generate configuration settings in a URL to distribute to Cognos Mobile application users in an email message, a chat, or by other methods. With this URL, the users can automatically configure the application on their mobile devices.

The Cognos server URL is included in the configuration so that users do not need to type the URL on their mobile devices when configuring the application.

As an additional security measure, a password can also be included in the configuration. The mobile configuration password provides a tamper-evident seal to ensure integrity of the configuration URL and confirms that the source of the URL is valid. The configuration URL and password should never be transmitted together using the same medium, such as email or chat, at the same time. Users need to enter this password only once when they open the configuration URL.
Procedure

1. From a desktop browser, log on to IBM Cognos Connection with administrator privileges.
2. Go to IBM Cognos Administration, and click the Mobile tab.
3. Click Remote Configuration.
4. For IBM Cognos Server URL, type your IBM Cognos BI server URL, such as http://cognos_bi_server/ibmcognos.
5. Enable or disable the following settings:
   
   **Pass-Through Authentication**
   Enable this setting so that users can navigate to the Cognos BI server through the different intervening web pages that are displayed to them.
   By default, IBM Cognos Mobile requires direct connectivity with the IBM Cognos BI server. If direct connectivity is not possible because of intervening security products or third-party portals, this setting must be enabled. The intervening products could include CA SiteMinder, Tivoli® Access Manager, Microsoft ISA Server, or landing pages in public WiFi networks.
   
   **Automatic Downloads**
   Enable this setting for the Cognos Mobile apps to automatically download new report outputs from the user's inbox and from reports pushed to the user. This setting should be enabled, unless bandwidth is a concern.
   
   **Display Sample Server**
   Enable this setting for the Cognos Mobile apps to access the Cognos Mobile sample server. The sample server contains sample IBM Cognos reports that illustrate the capabilities of IBM Cognos software. The sample reports are optimized for use on mobile devices.
   
   **Maintain Application State**
   Enable this setting so that the application can restore its latest content space after the application is restarted. For example, if the application is closed while viewing a report in the content space "My Reports", the application reopens the content space "My Reports" after a restart. If this setting is disabled, the application displays the main panel after a restart.
   Default: Off
6. Optional: Select the Mobile Configuration Password check box and type a password of your choice. The password can contain a maximum of 20 alphanumeric characters, and cannot contain spaces.
   If you decide to specify this password, ensure that you provide it to the users separately from the configuration URL.
7. Optional: Select the SSL/TLS Certificate Pinning check box and paste the SHA-1 fingerprint of the SSL or TLS certificate that secures the entry point to your Cognos BI server. An example of the Cognos BI server entry point is a web server, a proxy server, or a load balancer.
   Enable this setting to ensure that the client communicates only with the servers that are configured with the X.509v3 certificate and that have the same SHA-1 fingerprint.
The value for this setting is a sequence of 40 hexadecimal characters (a-f and 0-9) without any punctuation marks. Remove the punctuation marks from the value before pasting it in this field. You can specify multiple SHA-1 fingerprint values separating them with a colon (:).

**Tip:** In Firefox, you can obtain the SHA-1 fingerprint by clicking on the padlock icon in the browser URL bar and then clicking More Information > View Certificate.

8. Click **Generate Mobile Configuration Code**. A base64-encoded URL is generated that includes the specified configuration settings.

The following is an example of the generated URL:

cmug://aHR0cDovL3ZvdHRtb2IxL2NzcDI-dmVyc2lvb3QwLjAmcGFzcz1vZmYmYXV0b 2R3bj1vZmYmZGlzNHh4MyswMj0xMDIyMjUwTmV0b3ItYmVyc2lvbj0xLjAmcGFzcz1vZmYmYXV0b

9. Copy the configuration URL and provide it to the Cognos Mobile application users by email, chat, or by other methods.

Ensure that the following conditions are met when copying and transmitting the URL:

- All characters in the URL, including underscores (_), are selected when copying the URL.
- The application that you use to transmit the configuration URL maintains the case of the URL. The URL is case-sensitive.

**Results**

When users tap on the configuration URL from the administrator, the Cognos Mobile application is opened on their iOS or Android device. The users must confirm if they want to proceed with automatic configuration. If the mobile configuration password was specified in step 5, the users must enter the password when prompted. The application is then configured with the settings specified in the URL.

If the users enter an incorrect password or tap on the **Cancel** button, the application opens without applying any configuration settings.

**Tip:** Some email applications deliver the configuration URL to users as plain text. In this situation, the users can copy and paste the URL into the browser and open it from there.

---

**Configuring Cognos Mobile services**

You can globally configure all instances of the IBM Cognos Mobile service.

**About this task**

Applying the Mobile configuration settings globally ensures that all instances of the Mobile service are synchronized, which helps to avoid errors.

**Important:** The settings cannot be customized for different tenants in a multitenant environment.

**Procedure**

1. From a desktop browser, log on to IBM Cognos Connection with mobile administrator privileges.
2. Go to IBM Cognos Administration, and click the **Mobile** tab.
3. Click the **Server Configuration** page.
4. Locate the setting that you want to configure and specify its value as required.
   - **You can configure multiple settings. For a list of settings, see “Cognos Mobile service configuration settings.”**
5. Click the **Apply mobile configuration** button.

**Cognos Mobile service configuration settings**

These settings are used to administer the delivery of IBM Cognos Business Intelligence content to mobile applications.

Some configuration advanced settings can also be configured for the Cognos Mobile service. For more information, see “Cognos Mobile advanced settings” on page 69.

**Policy settings**

These settings define how to deliver Cognos BI content to mobile applications.

**Maximum number of pages to store for each report**

Pages over the specified limit are automatically discarded from the device.

Default: 5

**Tip:** If your Cognos Mobile environment includes only iPad native clients, set up the default to 50 pages. Otherwise, use the suggested default of 5.

**Maximum number of days to store a report**

Specifies the maximum time, in days, that a report is stored in the database. Reports that exceed this limit are automatically removed from the device.

Value: 1 to 999

Default: 30

**Maximum number of hours between runs of the source and target reports**

Specifies, in hours, the maximum amount of time allowed between the runs of the source and target reports when using the application drill-through feature with active reports in the iOS native app. When the difference between the two runs exceeds this amount, the application drill-through target is not used.

The default value of 1 means that as long as the target report was run within 1 hour after the source report was run, the target report can be opened successfully.

The value of 0 disables the application drill-through functionality. When running the source report after the target report using this value, the target report does not open and an error message is displayed. The error message states that the target report does not exist and needs to be run first.

This setting is not applicable for the Android native app.

**Permission to email report screen captures**

Allows or disallows the users of iOS and Android apps to email screen captures of the reports that they are viewing.

Value: True or False
Default: True

**Generate report thumbnails only for the first page**
This is a legacy setting that is currently not used in the product.

**Mobile root folder**
Specifies the name of the root folder that Cognos Mobile users must start from when browsing or searching content from a mobile device.

Default: blank

The value for this setting must be the Content Manager search path in the following format: `/content/package[@name='<root_folder_name>']`.

If the setting is blank, Cognos Mobile uses the root content folder or the root folder that is specified in the portal `system.xml` file stored in the `c10_location/templates/ps` directory. If you add a root folder, use the syntax of the consumer-root setting in the `system.xml` file.

**Tip:** You can find the search path in IBM Cognos Connection. For the package or folder that you want to use as the Cognos Mobile root folder, click the **Set properties** icon. Then, click **View the search path, ID and URL**.

**Maximum packet size for reports sent from Cognos Mobile server to a BlackBerry device**
Specifies in KB the maximum packet size for reports that are sent from the Cognos Mobile server to a mobile device.

Value: 0 to 1000000000

Default: 128000

The packet size must be equal to or less than the corresponding maximum packet size setting on the BlackBerry Enterprise Server. A value of 0 means that there is no size restriction.

**Mobile web application thumbnails**
Specifies if thumbnails are generated for the IBM Cognos Mobile web application.

Values: **thumbsOn** and **thumbsOff**

Default: **thumbsOn**

**Mobile theme support**
Specifies if custom mobile themes are supported for the IBM Cognos Mobile web application.

Values: **themeOn** and **themeOff**

Default: **themeOff**

**Maximum number of hours to access Mobile local data stored on a device**
Specifies the maximum number of hours when users of mobile devices can access the Cognos Mobile local data stored on a device.

Value: 0 to 8760

Default: 36

The value of 0 disables the lease key mechanism.

**Maximum number of hours to store cached credentials**
If you do not want to store credentials on a device, type 0. To store credentials on a device, type any value that is greater than the current
timeout setting for IBM Cognos Business Intelligence. As long as users are logged on, they will have access to their cached credentials.

Value: 0 to 8760
Default: 0

**Maximum number of hours that the client can remain out of date with scheduled reports**

This setting applies to the cases where an administrator schedules reports for a user on the server and the user does not otherwise communicate with the server before the time expires, for example, to retrieve other reports or to browse the IBM Cognos Business Intelligence portal. In the majority of cases, such as when reports originate from existing schedules or from user-initiated actions, this setting will not be a factor because, typically, the device lags behind the server by only seconds.

Value: 0 to 999
Default: 24

The value of 0 pushes reports to be downloaded on devices immediately.

**Security settings**

These settings are used to secure the Cognos Mobile application.

**Local storage encryption level for IBM Cognos Mobile applications**

Specifies the method by which data that is stored on iOS or Android devices is encrypted.

Values: NONE, AES128, AES256
Default: AES128

BlackBerry device storage is also encrypted, but you cannot configure it.

**Tip:** The web application does not store data locally and is not affected by this setting.

**Security code session timeout**

Specifies the need for a security code when accessing the Mobile iPad application and the maximum number of seconds that the application can remain inactive. The security code cannot contain consecutive or repeated numbers.

Value: 1 to 8760
Default: -1

A value of -1 means that no security code is needed. A value of 0 means that the iPad user must create a security code and enter it every time to access the app.

A value greater than 0 indicates that the iPad user must create a security code and can leave the app inactive for the number of seconds specified in the setting before needing to reenter the code to use the app. For example, if the value is set to 60, the user must enter a security code and can leave the Mobile app inactive for 60 seconds.

**Maximum number of attempts to enter a security code when accessing an iPad app**

Specifies the maximum number of times that users can try to enter their security code when accessing the Mobile iPad application.
Notification settings

These settings are used to configure Apple push notifications.

Notification email for Apple push notifications

Specifies the email address or addresses of administrators that are notified about the Apple push notifications certificate expiry date.

The value for this setting is an email address in the following format: admin@domain.com. Multiple email addresses must be separated with a semicolon (;). For example, admin1@domain.com;admin2@domain.com

Support for Apple push notifications

Enables Apple push notifications for the iPad native application, and specifies the wording of the message that is displayed to iPad users. The values are:

- None - Apple push notifications are disabled and messages are not sent from the server to the Apple Push Notification Service.
- Name - Apple push notifications are enabled. The messages sent from the server to the Apple Push Notification Service include the report name.
- Generic - Apple push notifications are enabled. The messages sent from the server to the Apple Push Notification Service do not include the report name. Instead, a generic message is displayed.

Default: Name

Frequency check for Apple push notification certificate expiry date

Specifies, in hours, the frequency with which the Cognos Mobile service checks for the Apple push notifications certificate expiry date. The first check is done when the Cognos Mobile service is started.

Value: 1 to 8760

Default: 24

Feedback interval for Apple push notifications

Specifies the time interval, in hours, for the Cognos Mobile server to check the Apple push notifications feedback service for failed notifications. The feedback service maintains a list of devices for which there were repeated, failed attempts to deliver notifications. The Cognos Mobile server will stop sending notifications to the devices that it obtained from the feedback service.

Values: 1 to 720

Default: 24

Expiry threshold for Apple push notifications

Specifies the number of days before the Apple push notifications certificate expiry date when the administrators start receiving emails about the approaching expiry date.

Value: 1 to 365

Default: 14
Location Intelligence settings

These settings are used by the BlackBerry clients. For more information, contact IBM Support (http://www.ibm.com/support/entry/portal).
Chapter 6. Report management on a mobile device

IBM Cognos Mobile users can run IBM Cognos Business Intelligence reports on their mobile devices.

Users access a report in the following ways:
- Browse and navigate to a report and then run it.
- Search for a report, choose one from the list of search results, and then run that report.

Reports can also be delivered in other ways:
- You can schedule reports to be delivered to users at specified intervals on their devices.
- You can send users bursted reports.
- You can run a number of different reports as a job and send them to the users' devices.
- Defined events can trigger a report to run and then be delivered to the users' devices.

If your organization provides reports based on current location, users can turn on the GPS capability on their phones and have these customized reports delivered to their devices.

Users can delete reports from their devices. If they do this, they delete only the copy on the device, not the actual report.

Accessing the server

Users can use the standard IBM Cognos URL that desktop users use to access the server.

Users using the IBM Cognos URL, http://servername/alias see a page describing a set of options based on their device type.

BlackBerry users can go to the desktop web portal, or to the native client installation page.

iPhone or Android users can go to the desktop web portal, or to the mobile-optimized portal.

Users can use the URL http://servername/alias/m to go directly to the mobile-optimized web portal, but it is best to use the standard IBM Cognos URL.

Running reports based on location

Your organization may have location aware reports that are customized according to the geographical locations of the users. The contents of these reports are determined automatically by the device, without any user input.
After IBM Cognos Mobile is installed on a device, users can select one of the following preferences to control how the device handles reports that have location prompts:

- **Always**
  When users run a location aware report, location prompts are completed automatically using the GPS data on the device.

- **Ask**
  When users run a location aware report, they are prompted about whether they want to complete the location prompt using the GPS data.

- **Never**
  When users run a location aware report, they are prompted to complete the location information manually. They are not prompted to use the GPS data.

For this feature to work, the GPS must be enabled on the device. Users should refer to the documentation for the device to find out how to enable the GPS.

### Cognos Mobile shortcuts on a mobile device

While you are working with IBM Cognos Mobile on your device, you can use a number of shortcuts for navigation and to perform other actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
<td>1</td>
</tr>
<tr>
<td>End</td>
<td>9</td>
</tr>
<tr>
<td>Up</td>
<td>2</td>
</tr>
<tr>
<td>Down</td>
<td>8</td>
</tr>
<tr>
<td>Left</td>
<td>4</td>
</tr>
<tr>
<td>Right</td>
<td>6</td>
</tr>
<tr>
<td>Enter</td>
<td>Open</td>
</tr>
<tr>
<td>Zoom In</td>
<td>Q</td>
</tr>
<tr>
<td>Zoom Out</td>
<td>A</td>
</tr>
<tr>
<td>Zoom</td>
<td>Z</td>
</tr>
<tr>
<td>Page</td>
<td>P</td>
</tr>
<tr>
<td>Mark Cell</td>
<td>5</td>
</tr>
</tbody>
</table>
Chapter 7. Cognos Mobile logging capabilities

Logging for IBM Cognos Mobile is provided by the product own logging capabilities and by logging capabilities in IBM Cognos Business Intelligence.

Both logging methods produce log files that are used to monitor activities and troubleshoot problems. These files are located in the `c10_location/logs` directory. The configuration files located in the `c10_location/configuration` directory, with the application tier components, are used to modify the Cognos Mobile logging capabilities.

Both logging methods can coexist at the same time. For example, the default Mobile logging mechanism can be used to track the Mobile service activity and the Cognos BI logging mechanism can be used to enable debug tracing. Audit logging is available only through the Cognos BI logging capabilities.

Events associated with starting and stopping the Cognos Mobile service are logged in the Cognos BI `c10_location/logs/cogserver.log` file.

In addition to the Cognos Mobile and Cognos BI logging capabilities, you can use the iOS and Android diagnostic capabilities to log events associated with the Cognos Mobile native apps.

Cognos Mobile logging

IBM Cognos Mobile records activities related to service startup, configuration setup, and running reports in the `mob.log` file in the `c10_location/logs` directory. This is the default type of logging in Cognos Mobile.

The logging information that appears in the `mob.log` file is determined by the `c10_location/configuration/mob.log4j.xml` file.

When using the default `mob.log4j.xml` file, an administrator can monitor the Mobile service for events such as database schema upgrades, Mobile service configuration settings and advanced settings changes, and warnings and errors. However, the default `mob.log4j.xml` file does not include the `Debug` logging level. If you need this level of logging in your `mob.log` file, you must enable debugging. For more information, see “Increasing default Cognos Mobile logging capabilities to debug levels” on page 62.

The following table specifies the logging levels in the `mob.log` file, from the highest to the lowest level:

<table>
<thead>
<tr>
<th>Logging level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug</td>
<td>Provides debugging information. This level is typically used for debugging specific problems. This level is not available by default and must be enabled. For more information, see “Increasing default Cognos Mobile logging capabilities to debug levels” on page 62.</td>
</tr>
<tr>
<td>Info</td>
<td>Provides information about IBM Cognos Mobile.</td>
</tr>
</tbody>
</table>
Table 4. Logging levels in mob.log (continued)

<table>
<thead>
<tr>
<th>Logging level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warn</td>
<td>Indicates a suspicious occurrence that might warrant further investigation.</td>
</tr>
<tr>
<td>Error</td>
<td>Indicates a serious error condition that requires intervention.</td>
</tr>
</tbody>
</table>

The level of logging that the user chooses includes all the levels below it. For example, if the user chooses Info, then warning and error messages are also written to the log file.

**Increasing default Cognos Mobile logging capabilities to debug levels**

You can enable the Debug logging level for the mob.log file.

**About this task**

The default mob.log4j.xml file does not include the Debug level logging. To enable debugging, use the c10_location/configuration/mob.log4j.xml.DEBUG.sample file.

**Procedure**

1. Stop the Mobile service in IBM Cognos Configuration.
2. In the c10_location/configuration directory, complete the following changes:
   a. Rename mob.log4j.xml to mob.log4j.xml.original.
   b. Rename mob.log4j.xml.DEBUG.sample to mob.log4j.xml.
3. Start the Mobile service.

**Results**

Full debug logging is now enabled for IBM Cognos Mobile.

**Enabling Cognos BI logging for Mobile server**

IBM Cognos Mobile records activities and debugging information as well as information about user and report activity.

**About this task**

The type of information that is logged in the Cognos Mobile log files is determined by the logging level defined in the ipfclientconfig.xml file in the c10_location/configuration directory. The same directory contains the ipfMOBclientconfig.xml.sample file. To enable logging, you only need to rename ipfMOBclientconfig.xml.sample to ipfclientconfig.xml.

The following logging levels can be defined for Cognos Mobile:

Table 5. Cognos Mobile logging levels

<table>
<thead>
<tr>
<th>Logging level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug</td>
<td>Provides debugging information. This logging level is typically used for debugging specific problems.</td>
</tr>
<tr>
<td>Info</td>
<td>Provides information about IBM Cognos services.</td>
</tr>
</tbody>
</table>
Table 5. Cognos Mobile logging levels (continued)

<table>
<thead>
<tr>
<th>Logging level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warn</td>
<td>Indicates a suspicious occurrence that might warrant further investigation.</td>
</tr>
<tr>
<td>Error</td>
<td>Indicates a serious error condition that requires intervention.</td>
</tr>
</tbody>
</table>

The level of logging that the user chooses includes all the levels below it. For example, if the user chooses Info, then warning and error messages are also written to the log file.

You can also enable logging in IBM Cognos Administration. For more information, see “Setting up audit logging in IBM Cognos Administration.”

**Procedure**

1. Stop the Mobile service in IBM Cognos Configuration.
2. In the `c10_location/configuration` directory, rename `ipfMOBclientconfig.xml.sample` to `ipfclientconfig.xml`.
3. Open the `ipfclientconfig.xml` file, specify the logging levels that you want, and save the file.
4. Start the IBM Cognos service.

**Results**

Depending on the logging levels specified in the `ipfclientconfig.xml` file, the following log files are generated in the `c10_location/logs` directory.

- `ipf-MOB_xxxx.log`
  
  This file records Cognos Mobile audit event information. If a logging database is defined in IBM Cognos Configuration under Environment, Logging, the audit events are also logged in this database. This type of logging is enabled by default in the `ipfMOBclientconfig.xml.sample` file.
  
  For information about setting up a logging database, see the IBM Cognos Business Intelligence Installation and Configuration Guide.

- `ipfMOBtrace_xxxx.log`
  
  This file records Cognos Mobile trace and debug log data. The type of data captured in this file is the same as the data in the `mob.log` file. However, this file can be configured to a different logging level to record more or less information. This type of logging is enabled by default in the `ipfMOBclientconfig.xml.sample` file.

- `ipfMOBperf_xxxx.log`
  
  This file records Cognos Mobile performance data. This type of logging is disabled by default in the `ipfMOBclientconfig.xml.sample` file.

**Setting up audit logging in IBM Cognos Administration**

Use audit logs to view information about IBM Cognos Mobile user and report activity.

**About this task**

Examples of actions recorded in audit logs include user logon and logoff times, expired user sessions, scheduled report delivery, saved output, and so on.
You can also enable audit logging in the `c10_location/configuration/ipfclientconfig.xml` file. For more information, see “Enabling Cognos BI logging for Mobile server” on page 62.

For more information about audit reporting, see the IBM Cognos Business Intelligence Administration and Security Guide. This document also contains information about the sample Cognos Mobile audit reports.

**Procedure**

1. Open Cognos Administration.
2. On the Configuration tab, click Dispatchers and Services.
3. Click the dispatcher name.
4. In the list of the dispatcher services, find the MobileService, and in the Actions column, click its Set properties icon.
5. Click the Settings tab, and under Category, choose Logging.
6. For Audit logging level for mobile service, select any value except for Minimal.
   
   The following logging levels can be specified to enable audit logging: Basic, Request, Trace, and Full. The Minimal logging level disables audit logging.
7. Click OK.
8. To apply the value, stop and restart the IBM Cognos service.

**User diagnostics**

Users can turn logging on and off in their native iOS and Android apps and choose the level of logging detail that is captured.

The following list shows the supported levels of logging, from the highest to the lowest level:

- Network
- Debug
- Info
- Warning
- Error

The level of logging that the user chooses includes all the levels below it. For example, if the user chooses Info, then Warning and Error messages are also written to the log file.

The maximum size of a logged message is 2 KB. If a message exceeds this size, it is truncated.

**iOS applications**

When logging is turned on, a directory named SupportArtifacts is created in the application documents directory. A file named mobile_ios.log is created in the SupportArtifacts directory. All logged events are written to this file.

The maximum size of an active log file is 1 MB. When this size is reached, the active log file contents are moved to a file named mobile_ios.log.old. If a mobile_ios.log.old file exists, it is removed first. A new mobile_ios.log file is created and becomes the active log file.
When logging is disabled, the directory and all its contents are removed from the application documents directory.

**Android applications**

When logging is turned on, a directory named `SupportArtifacts` is created in the `/Android/data/com.ibm.cogmob.artoo/files` directory. A file named `cogmob.log` is created in the `SupportArtifacts` directory. All logged events are written to this file.

The maximum size of an active log file is 1 MB. When this size is reached, the active log file contents are moved to a file named `cogmob.log.old`. If the `cogmob.log.old` file already exists, it is removed first. A new `cogmob.log` file is created and becomes the active log file.

When logging is disabled, the directory and all its contents are removed from the application documents directory.
Chapter 8. Cognos Mobile samples

The IBM Cognos Business Intelligence server installation includes a set of sample active reports for the iPad and a set of sample static reports optimized for mobile devices.

The iPad and static sample reports illustrate product features and technical and business best practices. Users can use them for experimenting with and sharing report design techniques and for troubleshooting.

iPad users can try out the interactive functionality of active reports. These reports let users compare different areas of their business to determine trends, for example, over time, by region, by departments or in combination, or compare business methods and statistics.

The iPad sample active reports include:

- Employee Recruitment
  This active report compares the effectiveness of various employee recruitment methods for each department and country or region. It shows the organization names, positions filled, planned positions, and a bulleted chart of positions filled versus planned positions.

- Customer Satisfaction
  This active report compares the number of returns by customers by order method and region. The report provides additional information about the order method with the highest number of returns. It also shows customer survey results for different regions.

- Inventory turnover report
  This active report shows information about the regional product inventory turnover, based on two years of comparative data. The report provides key inventory metrics that a company might use to manage its inventory. You can drill down on each product category to view the detailed inventory information and the number of failed orders related to the inventory.

- Financial report
  This active report shows current performance and changes in the financial position of an enterprise. This type of information is useful to all users who are involved in making business decisions. However, the Finance department is most likely to benefit from this information when implementing the checks and controls in the system to comply with legal, tax, and accounting regulations and requirements, and when providing advice about future directions, performance, and opportunities for the business.

Cognos Mobile sample active reports demonstrate the following product features:

- Interactive behavior between controls.
- Access to Details on Demand by leveraging drill-down functionality.
- Conditional palette and drill-down to details from a chart.
- Specific design for iPad gestures, such as swiping and scrolling.
- Particular user interface design, such as cover page and color palette.
- Different type of active report items, such as Deck, Tab Control, Chart, Buttons, Drop-down list, Iterator and Slider.
The static sample reports let users try the following features:

- Drilling through from one IBM Cognos Mobile report to another.
- Using tree prompts to filter reports.
- Viewing different report types, such as charts, crosstab, and list reports.
- Using calculated values and showing the results as a percentage.

The Mobile sample static reports include:

- Running Total For Promotion
  This report shows planned revenue by percentage for each product line. The report uses charts, crosstab reports, and list reports.

- Sales Revenue Expectation
  This report shows the goal for the percentage change in sales revenue for retailers. It uses a calculated value for forecasted revenue.

- Tree Prompt Retailers Set
  This report shows the revenue for a set of retailers. The report is a drill-through target for the Sales Revenue Expectation report.

For more information about the IBM Cognos BI samples, including how to set up and install the Mobile samples, see the *IBM Cognos Business Intelligence Installation and Configuration Guide*.
Appendix A. Specifying Cognos Mobile advanced settings

You can configure IBM Cognos Mobile advanced settings globally for all services, for a specific dispatcher, or for a specific Mobile service.

When the settings are configured globally, the values that you specify are acquired by all instances of the Mobile service. You can override the global values by specifying custom values at the dispatcher or Mobile service level.

If the configuration entry contains child entries with settings that override the global settings, the custom settings on the child entries can be reset to use the default values. To reset the value of any setting to its default, delete the setting.

Procedure
1. Log on to IBM Cognos Connection, and click Launch > IBM Cognos Administration.
2. On the Configuration tab, click Dispatchers and Services and complete one of the following actions:
   - To configure advanced settings globally, in the toolbar on the Configuration page, click the Set properties – Configuration icon, and proceed to step 3.
   - To configure advanced settings for a specific dispatcher, find the dispatcher, and in the Actions column, click its Set properties icon. Then, proceed to step 3.
   - To configure advanced settings for a specific Mobile service, click the dispatcher that includes this service. In the list of dispatcher services, find MobileService. In the Actions column, click the Set properties icon associated with the service, and proceed to step 3.
3. Click the Settings tab.
4. For Advanced settings, click Edit.
   - If the parameter is not listed, type its name. For a list of advanced settings that you can configure for Cognos Mobile, see "Cognos Mobile advanced settings."
5. Specify the appropriate value for the setting and click OK.

Note: To delete an advanced setting, select its check box, and click Delete.

Cognos Mobile advanced settings

You can use some of the advanced settings to manage various functions related to IBM Cognos Mobile.

Advanced settings are a property of the configuration object. The settings might not appear in the list of settings for a new installation, but if you add them, the Mobile service retains and uses them, even if you upgrade your installation.
The following advanced settings can be configured for IBM Cognos Mobile:

**Database.MaxConnectionPoolSize**
Specifies the maximum number of connections that are allowed for the Cognos Mobile service to communicate with the content store database. You can change connection pool settings to increase performance.

Value: 1 to 999
Default: 5

**Database.DeviceExpiryIntervalDays**
Specifies the time interval, in days, after which the client iPad devices that are not connected to the Cognos Mobile server are marked as inactive. The devices no longer receive push notifications, and any existing device data might no longer be usable.

Value: 1 to 365
Default: 45

**ThreadPool.MaxSize**
Specifies the maximum size of the thread pool on the server that is used to manage IBM Cognos Mobile operations.

Value: 1 to 999
Default: 20

For information about defining the advanced settings, see Appendix A, “Specifying Cognos Mobile advanced settings,” on page 69.

**Important:** Do not change or remove the advanced setting `_internal`. 
Appendix B. Troubleshooting IBM Cognos Mobile

This section describes some common problems you might encounter while using IBM Cognos Mobile. Problems might occur on the server or on the client.

For troubleshooting problems related to IBM Cognos Business Intelligence, see the IBM Cognos Business Intelligence Troubleshooting Guide.

IBM Cognos Mobile server problems

You may encounter server problems while working with IBM Cognos Mobile.

Charts and images not appearing

Charts and other images do not appear in reports on a mobile device if IBM Cognos Business Intelligence and IBM Cognos Mobile have been installed on a UNIX operating system that does not have X server software installed.

To resolve this problem, configure IBM Cognos BI to run with X server software.

Procedure

1. Find the bootstrap_*.xml file located in the `c10_location\bin` directory or in the `c10_location\bin64` directory.
   The exact `bootstrap_*.xml` filename depends on the version of UNIX that you are using.
2. Add the line `<param>-Djava.awt.headless=true</param>` to the following startup parameter in the `bootstrap_*.xml` file:
   `<process name="catalina">
     <start>
       <spawn sync="1" wait_time="5">
         <path>${java_home}/bin/java</path>
         <param>-d64</param>
         <param>-Djava.awt.headless=true</param>
         <param condName="${ip_protocol}" condValue="IPv6">-Djava.net.preferIPv6Addresses=true</param>
         <param>-Xmx${dispatcherMaxMemory}m</param>
         <param>-XX:MaxNewSize=${dispatcherMaxMemoryBy2}m</param>
       </spawn>
     </start>
   </process>`
3. Save the modified file, and then restart the IBM Cognos BI server from the IBM Cognos Configuration tool.
   For more information, see the IBM Cognos Business Intelligence Installation and Configuration Guide.

List prompt items consisting of only a single space are not supported

While running a report, a user chooses an item from a list prompt that consists of only a single space and the report generates an error and fails to run.

To resolve this problem, either do not include single space items in list prompts or, if you do include the single space then ensure that the user does not select it when running the report.
IBM Cognos Mobile service configuration settings are reset to the defaults after upgrading

The IBM Cognos Mobile configuration settings and advanced settings may be reset to their defaults after IBM Cognos Business Intelligence is upgraded.

To resolve this problem, reapply the settings.

MOB-SVR-1164 (HTTP error 413 (Too large)) the server was not configured correctly

The BlackBerry Enterprise Server MDS Connection Service stops transferring data to the mobile device. This happens only in BlackBerry version 4.2, 4.3, and 4.5 when reports are sent in packet sizes that are larger than the packet sizes that are acceptable to the BlackBerry Enterprise Server.

To resolve this problem, ensure that the packet size in the Maximum packet size for reports sent from Cognos Mobile server to a BlackBerry device on the IBM Cognos Mobile server is equal to or less than the Connection Service packet size on the BlackBerry Enterprise Server. For more information about configuration settings, see "Cognos Mobile service configuration settings" on page 54.

Advanced HTML functionality is not supported

Some advanced HTML functionality, such as Javascript and HTML tables, cannot be viewed in IBM Cognos Mobile.

To obtain table functionality, you can use IBM Cognos Report Studio to create a table.

java.lang.NoClassDefFoundError

This error can occur while a report is running on a UNIX operating system if the server is running in headless mode.

To resolve this problem, in the c10_location/bin directory, in the IBM Cognos Business Intelligence startup.sh file, add the following parameter:

JAVA_OPTS=-Djava.awt.headless=true

java.lang.InternalError: Can't connect to X11 Windows server using ':0.0' as the value of the DISPLAY variable

The server cannot run a report because the DISPLAY environment variable was not set or was set incorrectly.

To render a report to a .png file, IBM Cognos Mobile invokes graphics routines. As part of this process, IBM Cognos Mobile must also invoke the Java Abstract Windows Toolkit (AWT) libraries. This error occurs when the DISPLAY environment variable was not set or was set incorrectly and IBM Cognos Mobile cannot find the AWT libraries.

To resolve this problem, ensure that the DISPLAY environment variable is set to X11.

IBM Cognos Mobile service starts but then stops

IBM Cognos Mobile service fails during system startup. This means that the service has encountered a fatal error, such as being unable to create database tables.
Check the logs for additional information, take the appropriate action to correct the problem, and restart the service.

**Cognos Mobile database tables are not created**

After IBM Cognos Mobile was installed, the scripts to create the MOB_* tables were not run.

Under normal circumstances, the Cognos Mobile tables are created automatically after the Mobile service starts for the first time.

This problem might occur when Cognos Mobile application tier components and Cognos BI Content Manager are installed in different locations, and the Cognos Mobile database is not configured properly.

Ensure that the Cognos Mobile database is configured as documented in “Installing and configuring Cognos Mobile” on page 21.

**Changing default gateway redirects if you are not using the CGI gateway**

If you are not using the CGI gateway with IBM Cognos BI, you can modify the default gateway web pages to ensure that any automatic web page redirects that are used in IBM Cognos Mobile access the correct gateway. You can change the default web pages if you are using either the ISAPI or Apache module gateway as your default gateway.

**Important:** If you intend to use the CGI gateway as well, for example, as an alternative to the ISAPI gateway, modifying the default web page forces any automatic redirects to use the gateway that you identify in the default web page.

**Procedure**

1. Go to the `c10_location\webcontent` directory where the IBM Cognos BI gateway components are installed.
2. Open the `default.htm` or `index.html` page in a text editor, depending on which is the default document for your web server.
3. Locate the following line:
   ```javascript
   window.setTimeout("window.location.replace('cgi-bin/cognos.cgi?b_action=xts.run&m=portal/main.xts&startwel=yes')",5);
   ```
4. Edit the `cognos.cgi` value to redirect to the appropriate gateway.
   - If you are using ISAPI, change `cognos.cgi` to `cognosisapi.dll`. If you are using the Apache modules, change `cognos.cgi` to the `apache_module` value that has been defined.
   - For example, if you are using ISAPI as your default gateway, the line should be:
     ```javascript
     window.setTimeout("window.location.replace('cgi-bin/cognosisapi.dll?b_action=xts.run&m=portal/main.xts&startwel=yes')",5);
     ```
5. Save and close the file.

**IBM Cognos Mobile service client problems**

Users might encounter problems when working with IBM Cognos Mobile on their mobile devices.
Images do not appear on mobile devices

Report images do not appear on the mobile devices. This happens when users use their own SSL certificates, which are not trusted by the Java virtual machine (JVM).

To resolve this problem, users need to use the Oracle Sun keytool utility to import their SSL certificate into their JVM. For more information, see the Sun software documentation.

IBM Cognos Mobile does not filter downstream prompts for cascading prompts using reprompt

Users do not see the expected results in reports that have been set up with cascading prompts that require reprompting, that is where the user must click Reprompt in Cognos Viewer.

IBM Cognos Mobile does not apply the filters correctly downstream for the cascading prompts.

To resolve this problem, change the report's prompt options to Auto-Submit. With this option, IBM Cognos Business Intelligence will apply the filters to the downstream prompts as expected.

IBM Cognos Mobile client should not be installed over a previous client (BlackBerry devices only)

The IBM Cognos Mobile icon does not appear on the mobile device, so you cannot launch the application.

This may happen when the IBM Cognos Mobile client is installed on top of an older version of the client application.

To resolve this problem, delete the old client application from the BlackBerry device before installing a new version of the client application.

Repeater tables render incorrectly

A report that includes a repeater table that is within a block or table element does not render correctly on a mobile device.

To resolve this problem, rewrite the report so that repeater tables are not within blocks or table elements.

IBM Cognos Mobile does not support multi-select range prompts for BlackBerry 4.2, 4.3, and 4.5

Multi-select range prompts, which allow users to select more than one range of values, (for example, both January 1-15 and June 1-15 for a multi-select range date prompt) do not behave correctly in reports on mobile devices.

Users will experience one of the following situations, depending on whether the prompt is mandatory or optional:

• For a mandatory prompt, the user sees an error on the prompt page when trying to run the report and the report does not run.
• For an optional prompt, the user sees a warning on the prompt summary page when trying to run the report and cannot enter values in that prompt. However, the report will run using other prompt values, if there are any.
Calendar prompts show only the Gregorian calendar
When a report with a non-Gregorian calendar date prompt is displayed in IBM Cognos Mobile, the prompt appears in the Gregorian calendar format. The report runs after the user enters values in the prompt, but the results may be empty or inaccurate.

Two To fields appear on the email form (BlackBerry 4.2 and 4.3 only)
Two To fields appear on the email form that users use to email an IBM Cognos Mobile report. One of the To fields can be edited. Users can complete this field, ignore the other To field, and email the report.

To resolve this problem, users must upgrade to a BlackBerry version 4.5 or 4.6 device.

IBM Cognos Mobile fails to connect to the database
IBM Cognos Mobile accesses Microsoft SQL Server through the Java Database Connectivity (JDBC) driver, which uses a TCP socket to connect to the database.

If Microsoft SQL Server is not configured to allow TCP connections, then IBM Cognos Mobile will not connect to the database and will report errors in the logs.

To resolve this problem, enable TCP connectivity in Microsoft SQL Server.

Long text messages may be truncated
Long text messages may appear truncated on some parts of the device user interface for some languages.

For example, the user may observe that report long names and some translated text messages are truncated.

907 invalid cod error message (BlackBerry 4.2, 4.3, 4.5 only)
This error can occur while the user is installing the client application on BlackBerry device that runs out of space and stops the installation.

To resolve this problem, the user should increase the available space on the device by deleting applications or emails, clear the browser cache, and restart the download.

BlackBerry browser does not pick up configuration changes during over the air installations (BlackBerry 4.2, 4.3, 4.5)
The first time a BlackBerry user uses the link http://server/cognos10/mobile/index.html to install IBM Cognos Mobile client over the air, the BlackBerry browser caches the content by default.

Because it does not clear the cache automatically, subsequent attempts to install the product by using this link may not include the file or server configuration changes.

From the BlackBerry browser, the user must clear the cache and then click the link again.
User cannot log on from the mobile device

A user cannot log on to the server from the mobile device.

For a BlackBerry device, the user must check device connectivity to ensure that Connection Service is enabled for the device and for the user's BlackBerry account and that the connection to the IBM Cognos Business Intelligence server is valid.

**Procedure**

1. Run the device browser program.
2. Use the browser to open the main web page of your IBM Cognos BI server, for example, http://myserver/ibmcognos
   - Note that you may need to enter the full URL to the IBM Cognos BI gateway.
   - On the Options page of the mobile device, ensure that the server URL shows the correct, fully-qualified path to the IBM Cognos BI gateway, for example, http://server/cognos10/cgi-bin/cognos.cgi or http://server:5999/c10/cgi-bin/cognosisapi.dll.
   - If necessary, navigate to the IBM Cognos BI installation in a browser and copy the full path from the browser's address field.

**Results**

If the main web page does not appear, it might be because the user has a connectivity issue that the mobile device administrator needs to resolve.

No reports available when logged on from the Cognos Mobile client

The user is logged on to IBM Cognos Mobile, but cannot access any reports.

Reports need to be run before they appear in the mobile device inbox.

**Procedure**

1. On the mobile device, click **Browse**.
2. Click a report.
3. Click **Run Report**.
   - The report runs on the server.
4. Click **Refresh inbox** to refresh the inbox.
   - The report appears in the list.

Some Mobile users do not receive burst reports

All IBM Cognos Mobile users specified as recipients of a burst report should receive the report on their mobile devices as scheduled. If some users do not receive the report, the report might not be properly scheduled.

In IBM Cognos Connection, click the schedule icon for the report and ensure that the following check boxes are selected:

- **Burst the report** under **Bursting**.
- **Send the report to mobile recipients** under **Delivery**.
  - Do not select recipients for this option because burst reports are delivered to users defined in the burst specification. Any recipients selected here are ignored.

Next time when the report is run, all Mobile users should receive it.
Only those reports for which the report author defined burst options can be distributed by bursting. For more information about burst reports, see the IBM Cognos Report Studio User Guide and the IBM Cognos Business Intelligence Administration and Security Guide.
Notices

This information was developed for products and services offered worldwide.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service. This document may describe products, services, or features that are not included in the Program or license entitlement that you have purchased.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Software Group
Attention: Licensing
3755 Riverside Dr.
Ottawa, ON
K1V 1B7
Canada

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Depending upon the configurations deployed, this Software Offering may use session and persistent cookies that collect each user's:

- name
- user name
- password
for purposes of

- session management
- authentication
- enhanced user usability
- single sign-on configuration
- usage tracking or functional purposes other than session management, authentication, enhanced user usability and single sign-on configuration

These cookies cannot be disabled.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.


### Trademarks

IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

The following terms are trademarks or registered trademarks of other companies:

- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Index

Numerics
907 invalid cod 75

A
accessing the server 59
administration user interface 49
advanced settings
  Cognos Mobile service 69
  Mobile service 69
resetting while upgrading IBM Cognos BI 72
Android devices
  configuring for users 51
Android diagnostics
cogmob.log 64
Apple push notifications 7
SSL certificate 36
application server
  redeploying IBM Cognos BI 27
architecture 14
authentication policies 46
automatic synchronization 32

B
background synchronization 32
bandwidth
  estimating 31
BlackBerry
  location aware reports 60
  MDS HTTP authentication 46
BlackBerry devices
  icon does not appear 74
BlackBerry Enterprise Server 15
  configuring BlackBerry MDS Connection Service 27
BlackBerry MDS
  configuring Connection Service 27
BlackBerry MDS Connection Service
  configuring 27
BlackBerry MDS Services
  enabling Connection Service 27
burst reports
  Cognos Mobile 7, 76

calendar prompts
  incorrect results 75
CAM
  passport settings 46
  setting a timeout 46
capabilities
  Mobile 42
  Mobile Administration 2, 42
cascading prompts
  problems with filters 74
charts on UNIX 71
client (continued)
  installation methods 28
  installing from the web 30
  installing using a desktop deployment 30
  installing using the BlackBerry Handheld Configuration tool 29
  troubleshooting installations 75
cognob.log 64
Cognos Mobile
  enhanced user interface 5
  faster reports 5
  high-fidelity reports 5
Cognos Mobile components 14
Cognos mobile service
  global configuration 53
Cognos Mobile service
  advanced settings 69
components
  configuring 17
  distributing 18
  installing 17
  server 14
configuration
  server testing 27
configuring
  BlackBerry MDS Connection Service 27
  client from the web 30
  Cognos Mobile native apps 51
  components 17
  JDBC drivers 24
  MIME types 30
  Mobile iPad application 6
Connection Service
  configuring BlackBerry MDS 27
content store
  JDBC drivers 24
  setting up database clients 24

data
  erasing from devices 45
data transferring
  stops 72
database
  client fails to connect 75
  DB2 on z/OS 25
  tables not created 73
database client
  setting up 24
DB2
  creating a mobile database on z/OS 25
  JDBC drivers 24
  on z/OS as database 25
desktop deployment
  installing mobile clients 30
devices
  unable to install 75
  unable to log on 76
distributed installations
  options 18
downloading
  reports automatically 32
drilling
  in Cognos Mobile reports 5

E
  encryption
    local content 3
environments
    supported 22
erasing
  device data 45

F
  features 13
    features deprecated in version 10.2.0 7
    Blackberry native client 7
features removed in version 10.2.0 7
  Symbian operating system 7
  Windows Mobile operating system 7
filtering cascading prompts 74
fix pack
  installing 38

G
  gateway
    changing default redirects 73
groups
    assigning mobile theme 49

H
  HTML
    advanced functionality 72
HTTP authentication 46

I
  IBM Cognos BI
    resetting mobile settings while upgrading 72
icon does not appear on BlackBerry devices 74
images
  do not appear on UNIX 71
    not appearing 74
installation
  troubleshooting over the air 75
installing
  client from the web 30
  client using a desktop deployment 30
  client using the BlackBerry Handheld Configuration tool 29
components 17
  configuring MIME types 30
distributing components 18
fix pack 38
  from the device 75
methods for the client 28
  mobile clients 28
  mobile server 22
  options 18
installing (continued)
  server components 18
  testing servers 27
iOS devices
  configuring for users 51
iOS diagnostics
  mobile_ios.log 64
iPad
  languages supported 8

J
  java.lang.InternalError 72
  java.lang.NoClassDefFoundError 72
JDBC drivers
  configuring 24
  DB2 24
  Oracle databases 24

L
  languages
    support 7, 8
lease key 45
lease key technology 44
list prompts
  single spaces not supported 71
location aware reports 60
location-aware reports
  setting up 33
logging
  Cognos BI logging for Cognos Mobile 62
  methods 61
  mob.log file 61
logon
  from devices 76

M
  MDS 15
MIME types
  configuring 30
  mob.log file 61
    adding debug level 62
Mobile administration 49
Mobile Administration 2
Mobile Administration capability 42
Mobile Administrators role 42, 49
Mobile capability 42
mobile clients
  installing 28
Mobile Data Service 15
mobile devices
  inline prompts 9
Mobile samples 67
Mobile secured function 6
mobile server
  installing 22
Mobile service
  advanced settings 69
mobile settings
  resetting while upgrading IBM Cognos BI 72
mobile theme
  configuring 49
  deleting 49
  editing 49
mobile theme (continued)
  enabling 49
Mobile Users role 42
mobile_ios.log 64
multi-select
  range prompts unsupported 74

N
names
  truncating 75
new features in version 10.2.0 6
  Apple push notifications 7
  burst reports 7
  Mobile secured function 6
new features in version 10.2.0.2 6
  pre-configuring Mobile iPad application 6
new features in version 10.2.1 5
new features in version 10.2.1.2 2
new features in version 10.2.1.4 1

O
Oracle
  JDBC drivers 24

P
password protection 43
performance
  estimating bandwidth 31
  estimating servers 31
  maintaining 31
problems,
  See troubleshooting
prompts 59
  Cognos Mobile reports 5
  incorrect calendar results 75
  inline 9
  problems with filters 74
  single spaces not supported in lists 71
  unsupported multi-select range 74
  push notifications 36
    Apple 36

R
redeploying
  IBM Cognos BI to the application server 27
rendering
  repeater tables 74
repeater tables
  rendering incorrectly 74
report data security 44
reports
  data transferring stops 72
  downloading automatically 32
  estimating sizes 32
  iPhone
    location aware reports 60
    location aware 60
  not visible from devices 76
  running from a desktop computer 59
  running from a device 59
rich client 15

roles
  assigning mobile theme 49
  Mobile Administrators 42
  Mobile Users 42

S
samples
  Mobile 67
scheduling 59
secured functions and features
  Cognos Mobile 42
security 41
  authentication policies 46
  CAM passport settings 46
  iPad native app 44
  lease key 45
  lease key technology 44
  MDS HTTP authentication 46
  password protection 43
  report data 44
  setting the CAM timeout 46
server
  accessing 59
  languages supported 7, 8
  mobile installations 22
  server components 14
    installation process 18
  server configuration
    testing 27
  server configuration settings 54
  server installations
    testing 27
  server problems 71
  servers
    estimating numbers 31
    setting up location-aware reports 33
    settings
      resetting while upgrading IBM Cognos BI 72
  shortcuts 60
    starting
      Cognos BI service 27
supported environments 22
system requirements 18
system startup
  service fails 73

T
tables
  not visible 72
tables in content store 22
tablespaces
  creating for the DB2 mobile database on z/OS 25
testing
  server configurations 27
  server installations 27
text
  truncating 75
themes
  extra 75
  creating 50
timeouts
  setting for CAM 46
to field
  extra 75
troubleshooting 71
troubleshooting (continued)
  client 74
  data transferring stops 72
  database tables not created 73
  logging into devices 76
  over the air installation 75
  server 71
  system startup 73
  users are not receiving burst reports 76
truncating
  names 75
  text 75

U
uninstalling
  components 33

UNIX
  charts and images do not appear 71
  users
    accessing the server 59

Z
z/OS
  creating a DB2 mobile database 25
  creating table spaces for the DB2 mobile database 25
  zooming
    on iOS devices 6