IBM Cognos Mobile

- Author once, consume on the desktop, iOS and Android native apps
- Secure access to you Cognos BI content
- Connected or disconnect

What is IBM Cognos Mobile?

IBM Cognos Mobile is a Business Intelligence solution for executives and mobile workers who require wireless access to important information. IBM Cognos Mobile extends the full value of Cognos 10 Business Intelligence to mobile workers requiring timely, personalized and secure information beyond their traditional office. Users can access and interact with reports and dashboards on their mobile device while they are offline or online. It supports standard reports, Active Reports as well as Cognos Workspace content.

Deployment options for IBM Cognos Mobile

- Native Apps: iOS and Android tablets and phones
- Web App: iOS and Android phones and tablets
- See the Supported Environment page for details: http://www-01.ibm.com/support/docview.wss?uid=swg27037784

What are the prerequisite for using IBM Cognos Mobile?

- For IBM Cognos BI v10.1.1 to 10.2.1, the equivalent Cognos Mobile installkit needs to be added. See the Mobile Installation and Administration Guide for complete instructions
- For IBM Cognos BI v10.2.2 and up, the Cognos Mobile service comes pre-installed with BI.
- The web app is also available in the 10.1.0.0 version but needs an iFix to scale to larger screens
- While the iOS and Android apps are free downloads from the Apple App Store/Google Play, the user requires a proper license to connect to a BI Mobile server or to consume authored Active Reports.
- The iOS and Android native apps are backwards compatible all the way back to the Mobile server version 10.1.1.0. Meaning that users can freely upgrade their iOS and Android apps without needing to upgrade their Cognos BI servers.

How to install IBM Cognos Mobile client on your device?

- From your mobile device, go to:
  - iOS: https://itunes.apple.com/app/ibm-cognos-mobile/id455326089?mt=8
  - Android: https://play.google.com/store/apps/details?id=com.ibm.cogmob.artoo&hl=en
- From the app, create a connection to your BI server using your Gateway URL. For example: http://myserver/ibmcognos
- To use the IBM Cognos Mobile WebApp on the other supported devices, open a web browser to the following URL: *http://servername/ibmcognos/m* or *http://servername/ibmcognos/m/isapi*

What authentication mechanisms does IBM Cognos Mobile support

- IBM Cognos Mobile leverages and relies on the same authentication mechanism that exists in the IBM Cognos BI environment. Users enter the same credentials for IBM Cognos Mobile as they do in the IBM Cognos BI environment.
- If your authentication server uses an HTML page, CJAP or Siteminder, you may need to enable Pass-through Authentication via the apps' settings.
- Starting in the 10.2 release, users need to be granted the Mobile capability to be able to connect to the Mobile server

What security mechanisms does IBM Cognos Mobile support?

Customers typically have 3 major concerns when it comes to mobile app security: security for data at rest on the device, data in motion between the device and the server and the ability to remove data from the device should it be stolen or lost. Here are the security mechanisms that come with IBM Cognos Mobile. Also, please refer to the IBM Cognos Mobile Security White Paper: http://public.dhe.ibm.com/common/ssi/ecm/en/ytw03199caen/YTW03199CAEN.PDF

Data at Rest:

- The IBM Cognos Mobile iPad and Android native apps use the AES encryption algorithm to encrypt cached server based content on the device. The Cognos Administrator can choose between three levels: NONE, 128, and 256 bit encryption. (Default is 128bit)
- IBM Cognos Mobile uses a Lease Key mechanism to govern access to the stored content on the device. The reports that are cached on the device are only accessible for the duration of the Lease Key. As soon as it expires, the reports are no longer accessible. The user must re-authenticate with the BI server to renew the Lease Key to regain access to the stored reports. The IBM Cognos Administrator can set the length of time in hours for the duration of the Lease Key.
- The action of Logging Off has the effect to invalidate the Lease Key and prevents all local content to be viewed until the user re-authenticates with the BI Server
- The IBM Cognos Mobile iOS and Android native apps can enforce a user to enter an application specific security code (or PIN). If the user fails to enter the correct security code, the application will delete all the local cached Cognos content from the device.

Data in Motion:

- The IBM Cognos Mobile iOS and Android apps use HTTP to communicate with the BI Server. The apps can therefore work within a secure network using SSL, VPN, or reverse proxy.
- The mobile administrator can enforce SSL Pinning to restrict the app to only connect specific servers with a known certificate.
- The admin can import a client-side certificate onto the device to allow the app to communicate to the web server.

Removing Data from the Device:

- The IBM Cognos Mobile iOS and Android native apps can be managed by a third party Mobile Device Management (MDM) solution. If it is required, the MDM tool can remote wipe the entire content of the device.

Tips & Best Practices

Getting set up:
Establishing a connection between the device and the server. Secure networks, firewalls and other network policies can make it tricky to make contact between the IBM Cognos Mobile app and your server the first time you try it out. If you run into difficulties, first try to connect to Cognos Connections on the BI server from the mobile browser on your device. You can then work through any issues with your network security team by focusing on this simple test.

Satisfying user needs:
Mobile apps for business use are new and evolving. Often, executives and others will simply demand their existing reports and dashboards on mobile. Going down this path without first evaluating the real requirements of the users can lead to a mis-match between expectations and results. Taking the time to think it through from requirements gathering to implementation, a great mobile app has the power to transform your business and make you more competitive. Make sure you start with a requirements gathering exercise to find out what kinds of information and metrics your users need from their mobile devices. What decisions will they be making? How do they work with a mobile device? Are there different types of users with different needs?

Using Active Reports on the IBM Cognos iOS and Android native apps:
All the Active Reports that can be consumed in standard web browsers can also be accessed on your iOS and Android devices. You can run Active Reports from the BI server or import them manually into the App as MHT files. The Active Report file size grows as the volume of data and number of charts increases. It is recommended to follow the authoring techniques highlighted in the Active Report Proven Practices guide:
http://www.ibm.com/developerworks/data/library/cognos/reporting/active_report/page593.html

How-To-Videos
Refer to educational How-To-Videos to understand the key features that IBM Cognos Mobile app supports:
https://www.youtube.com/user/IbmBaEducation/videos?query=mobile

Performance Tuning Guide
As of the 10.2.1 release, the BI server handles the rendering of the Cognos content for mobile devices. Meaning that the Mobile service acts only as a conduit between the device and the BI Server without requiring any special hardware requirements.
More details of how to configure your environment for Mobile can be found in our Mobile Performance Tuning Guide.
http://www-01.ibm.com/support/docview.wss?uid=swg27042134

Deployment Guide
This guide outlines all the capabilities and mechanisms to consider when you are ready to deploy Cognos Mobile to either a small group of individuals or your entire enterprise.
http://www-01.ibm.com/support/docview.wss?uid=swg27045211