Ensuring the security of your mobile business intelligence
Ensuring the security of your mobile business intelligence

Executive summary
The number of mobile devices has now surpassed personal computers in sales. Many are used for business. Therefore, users expect to access all the applications they need to do their jobs, including business intelligence (BI), on these devices. Because BI can be sensitive and confidential, they also want to be sure it is protected from unauthorized users such as hackers and that it can't be accessed if the device is lost or stolen.

IBM® Cognos® Mobile software enables users to interact with trusted BI content on their Apple iPad and iPhone and on their Android tablets and smartphones. Making Cognos Business Intelligence available to more mobile device users invariably raises questions about the security of the BI they view and work with.

IBM is aware of these concerns and has gone to significant lengths to ensure the security of Cognos Mobile on smartphones and tablets. Cognos Mobile security is derived from a combination of sources. From IBM, you get the same security-rich features provided to all IBM Cognos Business Intelligence by the Cognos platform, along with other security features specific to Cognos Mobile. Other features are provided from device vendors or your IT department. This paper describes how Cognos Mobile is secured on Apple and Android tablets and smartphones, with additional information about the Cognos Mobile web application.

Securing BI on mobile devices
One of the biggest concerns that organizations have when it comes to adopting mobile BI is security. This is hardly surprising, given that the term “mobile” conjures up an image of important data being transmitted over unsecured networks, increasing fears of unauthorized access to or loss of sensitive corporate data.

Mobile security can be broken down into several areas:

- **Data access.** Providing users with only the data they are authorized to see
- **Data transmission.** Securing communication channels
- **Data storage.** Protecting data stored on a device
- **Device security.** Protecting the device from unauthorized usage
- **Deployment security.** Configuring, provisioning, implementing or monitoring the mobile solution safely

For Cognos Mobile, IBM has addressed these areas as they relate to the ways that users access BI on their devices:

- Apple iPads and iPhones
- Android tablets and smart phones
- Optimized web applications for Apple iPad and iPhone, Android tablets and smart phones, and Microsoft Surface tablets
In addition, no matter how you access Cognos Mobile—from a native application or the web—your underlying security base will be the Cognos platform. The Cognos platform provides integration with enterprise authentication and a central place to control access and authorization for all Cognos Business Intelligence objects, capabilities and data. This integration makes single sign-on for authentication possible, thereby simplifying the login process and restricting access to data according to business requirements.

In addition, the Cognos platform supports LDAP, NTLM, Microsoft Active Directory, Netegrity and SAP Business Information Warehouse, among others. In essence, it makes the most of your existing enterprise security deployments and includes the ability to link to one or more security systems simultaneously as you require.

**Native application and device security**

The Cognos Mobile native application uses a combination of Cognos platform, IT and device enabled security (Figure 1).

**Securing data access**

For security-rich data access, Cognos Mobile uses Cognos platform authentication and role-based security.

A device lease key prevents access to disconnected Cognos content when a time out period elapses. A good analogy of the lease key functionality is the concept of a hotel key. The key is enabled for the duration (lease) of your stay. Then, at the checkout time on the last day of your stay, your key is disabled (your lease has expired) and you are unable to access the room. The room is still there, but you will not be able to gain access until you make appropriate arrangements.
In the case of IBM Cognos Mobile, upon expiration of the lease key, content is not accessible until the user authenticates and a new key is granted. Therefore, disconnected content is inaccessible without wiping the entire device.

**Securing data transmission**

Cognos Mobile takes advantage of standard VPN protocols or an SSL connection to ensure a secure communication channel. Support for your enterprise network WiFi enables secure access to your corporate network when you are on the premises.

This secure access can be enabled with the VPN client that is part of your device operating system or third-party applications from Juniper, Cisco and F5 networks. Apple iPad comes with support for Cisco IPSec, Layer 2 Tunneling Protocol (L2TP) over IPSec and Point-to-Point Tunneling Protocol (PPTP). If your company supports one of these protocols, you do not have to make any additional configurations to connect your iPad to your VPN. Applications from Juniper and Cisco are also available for enabling SSL VPN. For the iPad and iPhone, you can configure these connections manually.

Your device also supports IPv6, proxy servers, split tunneling and other industry standards to ensure you have a rich VPN experience when connecting to your network. Cognos Mobile also works with a number of authentication methods, such as passwords, two-factor tokens and digital certificates. VPN On Demand, which initiates a VPN session dynamically when connecting to specific domains, is also available to streamline environments that use digital certificates.

**Securing data storage**

For the iPad and iPhone, Cognos Mobile fully supports the Apple hardware encryption that secures any data you store on the device.

Apple Sandbox prevents other applications from accessing Cognos Business Intelligence data on the device. Apple Sandbox protects your system by limiting application operations, such as opening documents or accessing the network. Sandboxing makes it more difficult for a security threat to take advantage of an issue in a specific application that can affect the greater system. The Apple Sandbox system consists of:

- A set of user space library functions for initializing and configuring the sandbox for each process
- A Mach server for handling logging from the kernel
- A kernel extension using the TrustedBSD API for enforcing individual policies
- A kernel support extension that provides regular expression matching for policy enforcement

If a device that is storing Cognos Business Intelligence data is lost or stolen, it’s important to deactivate and erase the device. In the case of the Apple iPad application, the Cognos Business Intelligence content stored on the device is protected by an Apple feature called remote wipe. With this feature, your administrator or device owner can issue a command that removes all data and deactivates the device.

For your Android devices, the Android platform takes advantage of Linux user-based protection as a means of identifying and isolating application resources. The Android system assigns a unique user ID (UID) to the Cognos Mobile application and runs the application as that user in a separate process. This approach is different from other operating systems, where multiple applications run with the same user permissions.
The UID sets up a kernel-level application sandbox. The kernel enforces security between the Cognos Mobile application, other applications and the system at the process level. Standard Linux facilities, such as user and group IDs that are assigned to applications, are used for this enforcement. The BI data downloaded by Cognos Mobile is protected with appropriate user privileges. Therefore, it is inaccessible to other applications that are on the device. The sandbox is simple, auditable and based on decades-old UNIX-style user separation of processes and file permissions.

Cognos Mobile supports the use of Android full file system encryption, so user data can be encrypted in the kernel. The encryption key is protected by AES128 with a key derived from the user device password, which prevents unauthorized access to stored data. To resist systematic password guessing attacks (such as “rainbow tables” or brute force), the password is combined with a random salt. It is hashed repeatedly with SHA1 by means of the standard PBKDF2 algorithm before it can decrypt the file system key. To resist dictionary password guessing attacks, Android provides password complexity rules that can be set by the device administrator and enforced by the operating system. File system encryption requires the use of a user device password; it is not possible to use pattern-based screen lock. The password protects the entire Android device, and the Cognos Mobile application PIN protects BI server content.

A local wipe feature is also part of your Apple iPad device security. By default, iPad automatically wipes the device after 10 failed passcode attempts. However, you can configure your iPad to wipe the device after a different maximum number of failed attempts with a configuration profile.

For your Android devices, the Android operating system can be configured to verify a user-supplied password before providing access to a device. In addition to preventing unauthorized use of the device, this password protects the cryptographic key for full file system encryption. A device administrator can require the use of a password, password complexity rules or both.

**Secure deployment**
The Apple iPad Configuration Utility manages the configuration of the iPad so an administrator can set up the corporate resources that the mobile users can use. This utility provides a centralized configuration of settings, such as WiFi network connectivity, LDAP authentication information and secure VPN access. It can also load provisioning profiles onto a device. Such centralized administration can ensure that devices are configured correctly and according to security standards set by your organization. In addition, an iPhone Configuration Utility can install configuration profiles on devices when connected by USB.

The configuration profile is an XML file that is distributed to users and loaded on the mobile device, and this file is protected by a password that is only known to the administrator. After the profile has been loaded on the iPad, the settings cannot be changed from that profile unless someone uses the profile password. The profile can also be locked to the device and cannot be removed without completely erasing all of the device contents.
Configuration profiles can be both signed and encrypted. Signing a configuration profile ensures that the settings being enforced cannot be altered in any way. Encrypting a configuration profile protects the contents of that profile and ensures installation only on the devices for which it was created. Configuration profiles are encrypted with CMS (Cryptographic Message Syntax, RFC 3852), supporting 3DES and AES128.

A configuration profile can be loaded on to the device several ways:

- The device can be connected directly to the computer or server where the Apple Configuration Utility is installed.
- A link can be provided on a web page that will load the profile onto the device after it is accessed from a web browser on the device.
- An email message can provide a link that will load the configuration profile.

In addition, Apple over-the-air enrollment and configuration provide an automated way to configure devices securely. This process provides IT with assurance that only trusted users are accessing corporate services and that their devices are properly configured to comply with established policies. Because configuration profiles can be both encrypted and locked, the settings cannot be removed, altered or shared with others.

For Android devices, the Android Device Administration API provides device administration features at the system level. Administrators can also remotely wipe (that is, restore factory defaults on) lost or stolen devices. These APIs are available to third-party providers of Device Management solutions.

Cognos Mobile includes the ability to protect the lease key used to encrypt local data with an application PIN. A Cognos Mobile Server administrator can use an advanced setting in Cognos Mobile Administration to enforce the use of application PIN for all Cognos Mobile clients.

**Secure mobile device management**

With mobile device management capabilities provided by Apple and Android, IT can easily scale the application deployment for your entire organization. These management capabilities serve as a central point for managing all mobile devices. Administrators can take advantage of configuration profiles, over the air enrollment and push notifications to enroll, configure, update settings, monitor compliance and remote wipe or lock devices. Updates can be automatically installed on devices without any user intervention. In addition, monitoring capabilities can query devices for information related to compliance.

**Web application security**

The Cognos Mobile web application uses a combination of Cognos platform and web application enabled security (Figure 2). Because the web application does not store anything on your mobile device, unauthorized access to BI content if your device is lost or stolen is not possible. In addition, use of the HTTPS protocol prevents caching on your device’s web browser. Device security is also not as critical because there is no stored BI data that could be exploited.
For secure data access, Cognos Mobile uses Cognos platform and role-based security. In addition, Cognos Business Intelligence server authentication is required every time a user accesses the application.

For secure data transmission, Standard VPN protocols or an SSL connection ensure a secure communication channel. Support for your enterprise network WiFi enables secure access to your corporate network when you are on site.

When you install the Cognos Mobile service, the mobile web application is automatically configured to “/m” on the end of your gateway URL. IT can provide the link and you can create a bookmark on the devices for easy access to the application. Upgrades of the application occur on the server side without affecting those who are using it on their devices.

**Conclusion**

Cognos Mobile is designed for users who need to view, analyze and share Cognos Business Intelligence content wherever they are. Whether you are on the road or at the office, you get the same great insight. With this mobile capability, however, comes the inevitable question: Is my BI secure? The answer is yes. Cognos Mobile relies on a combination of security-rich features provided by the Cognos platform, lease key technology, the device and operating system developers and IT security measures. These measures help protect your BI content so it is kept safe from hackers and device loss or theft.
About Business Analytics

IBM Business Analytics software delivers data-driven insights that help organizations work smarter and outperform their peers. This comprehensive portfolio includes solutions for business intelligence, predictive analytics and decision management, performance management and risk management.

Business Analytics solutions enable companies to identify and visualize trends and patterns in such areas as customer analytics that can have a profound effect on business performance. They can compare scenarios; anticipate potential threats and opportunities; better plan, budget and forecast resources; balance risks against expected returns and work to meet regulatory requirements. By making analytics widely available, organizations can align tactical and strategic decision making to achieve business goals. For more information, see ibm.com/business-analytics.

Request a call

To request a call or to ask a question, go to ibm.com/business-analytics/contactus. An IBM representative will respond to your inquiry within two business days.