Solution Brief

Data security in a mobile world

Highlights

As the global workforce becomes increasingly mobile, organizations are turning to handheld wireless devices to provide personnel with the information they need to make informed decisions any time, anywhere.

But with the advantages of mobile information delivery come legitimate concerns about security. Small and highly portable mobile devices are easily misplaced or lost. Many feature removable memory sources. And those with their own IP addresses can be vulnerable to the same types of attack as any computer.

In short, wireless devices face all the vulnerabilities of traditional wired networks, plus a few that are unique to the wireless world. Before deploying mobile wireless technology, organizations need to be confident that those threats have been effectively addressed, and that their valuable corporate data is secure.

Making security priority one with IBM Cognos 8 Go! Mobile

IBM Cognos® 8 Go! Mobile significantly raises the value of handheld mobile devices by enabling organizations to use them to deliver accurate, complete, mission-critical IBM Cognos 8 Business Intelligence (BI) to personnel in the format they need, where and when they need it. This generates better decision making, competitive advantage, and higher productivity. And it enables organizations to leverage their existing investment in IBM Cognos 8 BI for a lower total cost of ownership and a higher return on their investment.

But as IBM Cognos 8 Go! Mobile increases the value of the information you can receive, send, and store on mobile devices, the need to ensure the security of information on those devices also increases. That's why, when developing IBM Cognos 8 Go! Mobile, security was the number one priority, addressing the challenge with a comprehensive system of security that includes

- IBM Cognos 8 BI security
- Manufacturer-based security
- IBM Cognos lease key security

Information Management

Cognos. software

IBM Cognos 8 BI security

IBM Cognos 8 Go! Mobile leverages all of the security already in place for other components of the IBM Cognos 8 BI solution. This includes security through authentication, authorization, and encryption.

Authentication

Authentication ensures that only users with valid passwords, IDs, and related identifiers can access a system.

IBM Cognos 8 BI is security-agnostic. It works with your existing security model to define and maintain identifiers that include user, group, and role names, IDs, passwords, regional settings, and personal preferences.

IBM Cognos 8 BI security also provides support for multiple user communities, including the ability to assign appropriate permission rights for users and groups to ensure that only those with the proper permission can access specific folders, sub-folders, reports, analyses, metrics, scorecards, dashboards, events and alerts, shared group-based portal pages, data connections, and IBM Cognos 8 BI capabilities such as authoring.

With IBM Cognos 8 BI, you leverage your existing organizational security to secure all BI content, including content used on mobile devices with IBM Cognos 8 Go! Mobile.

Authorization

Authorization ensures that only certain users, groups, and roles can access specific data or information – such as a data source, report, or folder – and can perform only certain actions on that data or information.

IBM Cognos 8 BI security includes the ability to assign access and activity permissions to selected users, groups, and roles. This ensures that only authorized personnel can view, change, and perform a variety of other activities with IBM Cognos 8 Business Intelligence.

When setting access permissions for IBM Cognos 8 BI, you can leverage users and groups defined within your existing authentication providers. As with authentication, the authorization security measures that you establish apply to all of your IBM Cognos BI, including BI used by IBM Cognos 8 Go! Mobile.

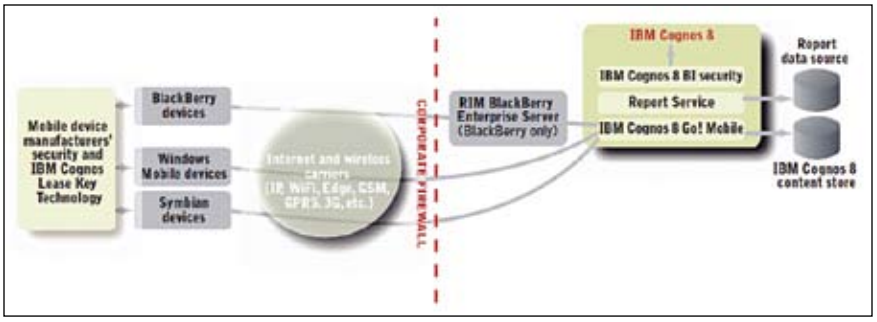
Encryption and decryption

Encryption is a standard security measure that IBM Cognos 8 BI uses to ensure that data cannot be read by unauthorized sources or people. Only authenticated and authorized sources and users can decrypt the data, converting it back into a meaningful form that can be accessed and used.

IBM Cognos 8 BI comes with a 56-bit encryption mechanism for encrypting all IBM Cognos 8 BI data and communications. Enhanced security encryption modules are available for configuring IBM Cognos 8 BI with a data encryption key size up to 168-bit.

As with authentication and authorization, IBM Cognos 8 BI encryption security applies to all data communicated between and used on mobile devices with IBM Cognos 8 Go! Mobile.

Security from mobile device manufacturers The manufacturers of mobile devices and their security partners are acutely aware of the security issues that face users of their devices, and of the need to address those issues with security geared specifically to their products.



The IBM Cognos partnership with the manufacturers of devices on which IBM Cognos 8 Go! Mobile operates, and with their partners, ensures that corporate, device-based, and IBM Cognos security are compatible and integrated.

Security for mobile devices is typically very strong, because it must meet stringent standards to be approved for use by NATO and governments. Security typically includes

- Standard secure data transmission and encryption specific to the mobile device or mobile operating system
- Password protection, so that only an authenticated user can use a device
- Remote shut down and wiping capabilities to protect data on a device that is lost or stolen

Secure data transmission

The system architecture for mobile devices includes a firewall-protected server that stores security and other information about each user.

An administrator configures rules and encryption key information for users, and information is encrypted and decrypted by the server and on the user's handheld device. The server knows when it is talking to the right device, and the device knows when it is talking to the right server. This minimizes the chance of transmissions being intercepted, and it ensures that, even if a transmission is intercepted, the data is unintelligible.

Password protection

Just as passwords are used to protect IBM Cognos 8 BI data, they are used to control who can use a mobile handheld device. To maximize password protection, it is highly recommended to have a strong password that aligns with password policies for the enterprise.

After a device is dormant for a period of time, it locks. A password is needed to use the device again. Entering an incorrect password, even as few as ten times, typically results in the device being wiped of all data. Once wiped, the user must present the device to an administrator in person in order to gain access.

Remote shut down and wiping

If a device is reported lost or stolen, an administrator can prevent data stored on the device from being accessed. The administrator sends a remote "kill" command to the device, erasing all of the data on the device – including data in memory – and disabling it from further use. The action can be verified with a logging message to the administrator.

IBM Cognos lease key technology

For the remote "kill" command to work on a device, the device must be turned on and connected to the network. If connections are disabled on a lost or stolen device, there is no ability to remotely wipe the data. To address this, IBM Cognos 8 Go! Mobile uses "lease key" technology.

The IBM Cognos 8 BI data stored on a mobile device is encrypted. During normal functioning of IBM Cognos 8 Go! Mobile, the user can view and interact with the locally stored reports. If the device does not connect to the network for an extended period of time (a feature that is configured by

Security when devices are lost or stolen

There is no doubt that mobile devices are more prone to being lost or stolen than traditional technologies. The following combination of security measures ensures that data remains secure:

- All IBM Cognos BI data stored locally is encrypted.
- Device passwords block unauthorized access to data on the device.
- All data is erased after multiple failed attempts at device passwords.
- Access to IBM Cognos 8 BI from the device requires IBM Cognos credentials.
- Administrators can remotely wipe all data on a device when it is connected.
- All IBM Cognos BI data is completely locked down if the device's lease key expires without being connected.

the IBM Cognos Administrator), the locally stored data is locked and made inaccessible until the user reconnects to the IBM Cognos environment and is re-authenticated.

A good analogy of the lease key functionality is the concept of a hotel key. The key is enabled for the duration, or lease, of your stay. When you check out – when the lease has expired – your key is disabled, and you are unable to access the room. The room is still there, but you can't gain access until you make appropriate arrangements – or, in the case of IBM Cognos 8 Go! Mobile, until you connect, re-authenticate, and are granted a new lease key.

IBM Cognos lease key technology ensures that, even if a device is offline and cannot be contacted by an administrator, the data stored on it is safe. As a result, IBM Cognos BI data is even more secure on mobile devices than e-mail.

Summary

Ensuring mobile security in your organization

The security provided by IBM for IBM Cognos 8 Go! Mobile, and by the manufacturers of the devices on which IBM Cognos 8 Go! Mobile is used, effectively addresses the security challenges of a wireless world.

By combining the security technology that is provided with sound, well-documented, well-enforced policies for mobile information use, and with security-related education for mobile device users, you can be confident that the IBM Cognos BI used by your mobile workers is well protected.

About IBM Cognos BI and Performance Management:

IBM Cognos business intelligence (BI) and performance management solutions deliver world-leading enterprise planning, consolidation and BI software, support and services to help companies plan, understand and manage financial and operational performance. IBM Cognos solutions bring together technology, analytical applications, best practices, and a broad network of partners to give customers an open, adaptive and complete performance solution. Over 23,000 customers in more than 135 countries around the world choose IBM Cognos solutions.

For further information or to reach a representative: www.ibm.com/cognos

Request a call

To request a call or to ask a question, go to www.ibm.com/cognos/contactus. An IBM Cognos representative will respond to your enquiry within two business days.

IBM Canada
3755 Riverside Drive
Ottawa, ON, Canada K1G 4K9

Produced in Canada
March 2009

IMS14091CAEN