Resco Mobile CRM Security

Having your CRM data in a mobile app can be a scary thing. After all, how sure can you be your data is safe? Pretty sure actually. Thanks to security offerings of Resco Mobile CRM.

Supported mobile platforms:
 iPhone/iPad Android ⊞ Windows

resco.net
technology on the move

Resco Mobile CRM Airtight Security

Companies have a strong need to secure their data, especially when they're used outside of their premises, let's say in a mobile app. We go above and beyond to ensure your information is safe & secure. Here's how:

Server-side precautions

TThere's one common misconception amongst the majority of customers seeking a mobile solution. And that is: "We need to expose our server to the Internet, which is very dangerous."
You don't, in fact, have to expose your server to the Internet. Nor is it that risky if you did.

? How can the mobile app connect to Microsoft Dynamics CRM?

When connecting to Microsoft Dynamics CRM, the minimal requirement for synchronizing the app with the server is the Dynamics CRM Web Services and the authentication services availability.

You can opt for IFD with Claim-Based Authentication or, in case when the Dynamics CRM server and the Active Directory Federation Services cannot be exposed to the Internet, you can use VPN or Direct Access connection.

Note: The default configuration of Microsoft Dynamics CRM with Active Directory authentication uses HTTP protocol. It is highly insecure to expose the server to the Internet in this configuration. We strongly recommend using either VPN or Direct Access, or changing the configuration to use HTTPS to secure the data exchange between the mobile CRM client and the Dynamics CRM server.

Dynamics CRM Online server is already accessible to users via a secure HTTPS protocol, which works also for accessing the data from Resco Mobile CRM.

? How is the data transfer secured?

The CRM data is transferred directly from the server to the application via standard Dynamics CRM Web Services provided by Microsoft. Companies can choose to use:

- VPN or Direct Access connections in case IFD is not desirable
- HTTPS instead of HTTP protocol
- SSL to secure the data transfer

? How does the mobile app connect to Resco's CRM server?

Every Resco Mobile CRM license now also enables access to Resco's own CRM server. To synchronize the app with a cloud-based instance of this server, availability of Resco Web Services is required.

The cloud-based Resco CRM server configuration always uses HTTPS protocol to enable the communication between the server and the app.

? How is the data transfer secured?

The data is transferred directly from the server to the mobile application via standard Web Services provided by Resco. HTTPS is always used as a default communication protocol and secured by the TLS 1.2, TLS.1.1 and TLS 1.0 certificates.

If deploying an on premise instance of Resco's CRM server, companies can also use VPN and Direct Access connection to secure the data transfer.

Out-of-the-box security

No middleware

Resco Mobile CRM does not use any middleware server or component, which means that no data is stored (or cached) anywhere except for the client's local storage. This increases the safety as there's no data stored in a 3rd party solution, which it could leak from.

Password protection

The main security token for the application is the user password. This is the password used for authentication with the Dynamics CRM server.

The application can be configured to either:

- Store the password in the device's secured storage
- Require the user to enter the password each time the application is launched or resumed
- Require the user to enter the password after X minutes of inactivity (this time period is specified by you, e.g. every 30 minutes)

Data Encryption

The locally stored database on the device (used for offline capability and faster performance of the app) is encrypted by default. The data encryption is based on an application key. The application key is randomly generated when the database is created and protected by the user password. The key is stored in an encrypted form in device's file system and decrypted when needed.

There are 2 data stores: the database and the blob store (attachments). For encrypting the SQLite database, the application key is passed to the SQLite database driver. The driver uses the application key and IV to encrypt/decrypt individual database pages using AES128 in CFB mode. Each page (1024 bytes) is encrypted separately. The IV is the page header (contains variable/unpredictable data). Each file in the blob store (attachment store) contains a header with random IV (16 bytes) and encrypted data. The blob data is encrypted with AES256 in CBC mode using the application key, file header IV. PKCS7 is used for data alignment.

And this it is only the tip of the iceberg. There's more!

Going to the next level

You can apply advanced security measures and restrictions, set rules and user rights, select which data can be downloaded to the application or even wipe-out the data from the application if the device gets lost or stolen. And you can do it all remotely, fortified with push technology.

It does not matter anymore what mobile platform your employees use, you can take control of all your mobile device's security through one simple management console.

1. Online only entities

Some CRM entities can be configured to be accessible 'online only', in which case they are not stored in the local database of the client.

2. Device management

You can index all your mobile devices in one structured list. This view shows you the details on each device: its model, ID, running OS, currently installed version of Mobile CRM app and date of the last synchronization. If you want to make sure employees use only devices approved by you, you can automatically block all new devices. If you do that, users will not be able to connect to the server via a phone or tablet that has not yet been enabled.

3. Resco license validation

The Resco Mobile CRM client access license is validated online by Resco Licensing Service available at https://iservices.resco.net. Resco uses only a minimum set of data (CRM Organization ID and CRM User unique ID), which allows validating the license for a particular Dynamics CRM user. If case the access to the Resco Licensing Service can't be granted, Resco licenses can be stored directly on the Dynamics CRM organization.

4. License assignment

The professional licenses you purchase from Resco can be automatically distributed to users, who log into the server via the app (comes in handy if you've got a couple of hundred mobile users) or they can be distributed only by an admin via the tool we provide.

5. Push actions

System admins can also remotely lock the application or wipe out data from it. This can be done manually (when needed) or automatically in case the app has not been connected to the server for a longer time (time frame specified by admin), or if the user exceeded specified number of incorrect password entries (again decided by the admin). Business hour option allows user to work with the app only during defined working hours.

6. Mobile Device Management tools

There are a plenty of great mobile device management tools on the market that you can use to protect a tablet/phone (in case you want to also secure other applications your employees use). Resco Mobile CRM currently supports Symantec, MobileIron and AirWatch.

See? Resco Mobile CRM is the safest choice out there.

- Save ways for connecting to the server
- No middleware that stores the data
- User password protection
- Encrypted local database
- Password validation option
- Online-only access to chosen entities
- Custom security policies
- Remote lock of the application
- Remote data wipe out
- Mobile Device Management tools support

Get in touch!

www.resco.net
mobilecrm@resco.net

North America: +1 (617) 336-7238
Rest of the World: +421 2 209 02 019

Follow us: @RescoMobileCRM YouTube @RescoDevelopers LinkedIn linkedin.com/company/resco-net