2017

Resco Mobile CRM Security

Out-of-the-box Security

Contents

1. Overview

1.1. Resco Cloud

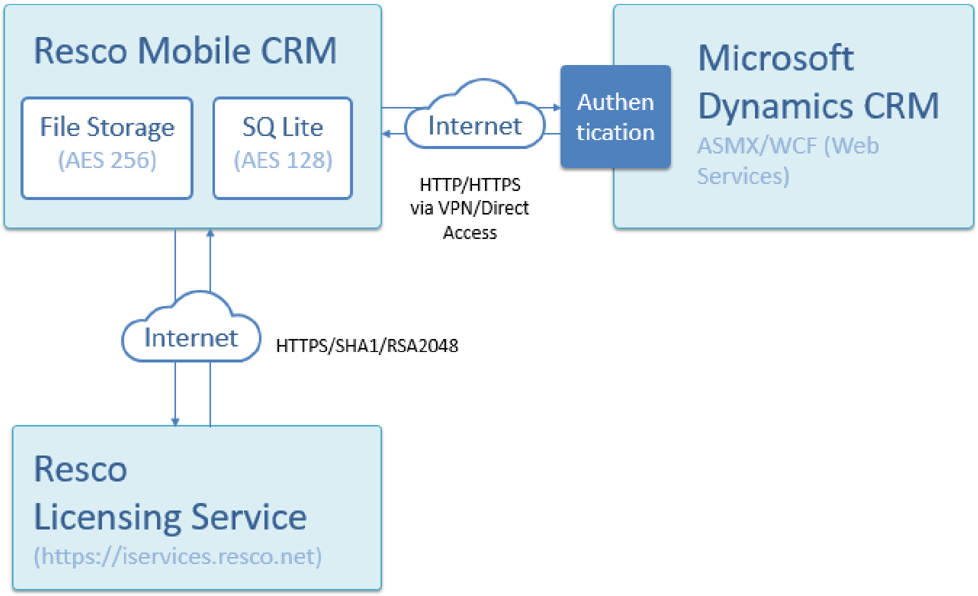
The Resco Mobile application (client) communicates directly with the Resco Cloud server (public or private).

To synchronize the Resco Mobile CRM application with Resco Cloud, only the connectivity to the standard Resco Web Services is required. All the communication between the app and Resco Cloud uses a standard Web Services via HTTPS protocol secured by the **TLS 1.2 and TLS.1.1** certificates.

If deploying an **on premise instance of Resco's CRM server**, customers can also take advantage of **VPN** and **Direct Access Connection** for additional security of the data transfer.

1.2. Microsoft Dynamics CRM and Dynamics365 synchronization

The Resco Mobile application (client) communicates directly with the Dynamics CRM server.



When synchronizing the Resco Mobile app with Microsoft Dynamics CRM, the communication uses standard Dynamic CRM Web Services provided by Microsoft. There is no middleware or transient data storage. The CRM data is not stored (or cached) anywhere except for the local storage on the client. The local storage (SQL database and files) contains only the configured subset of the

CRM data. Selected CRM data (entities) can be configured to be "online only", in which case it is not stored on the client at all.

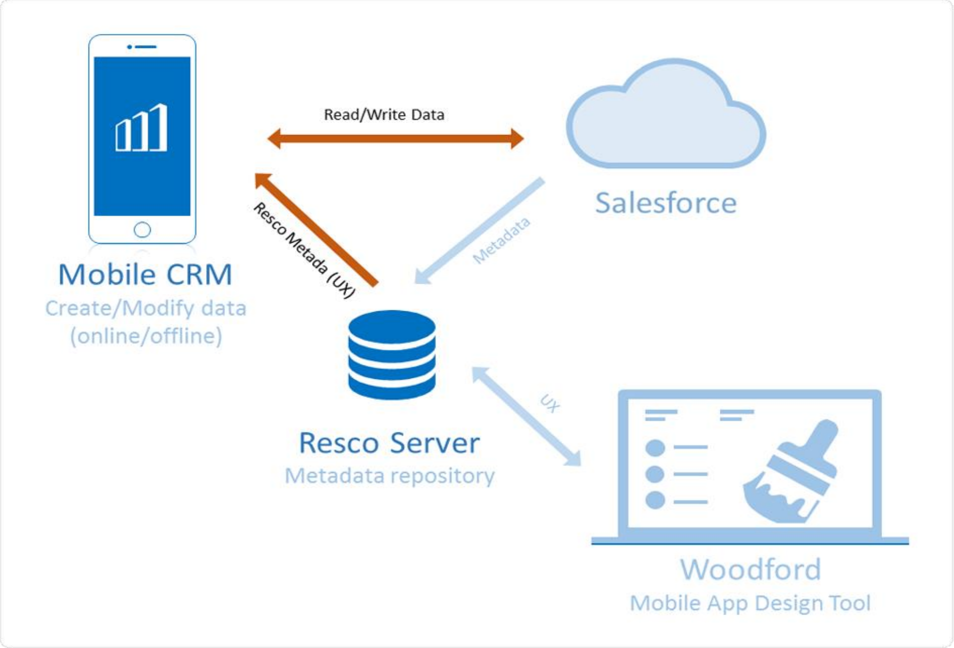
For Mobile CRM Client Access License validation, the system uses only a minimal dataset needed for validation of the license for the particular Dynamics CRM users. Section 4 provides more details about the data sent to the Resco Licensing Service.

For overall architecture security there are 3 important parts described in the following sections:

- Mobile client security
- Dynamics CRM/Communication security
- Data provided for the license validation

1.3. Salesforce synchronization

When connected to Salesforce, the Resco Mobile app communicates with **Resco Cloud** to download metadata (object schema, mobile customizations) and with **Salesforce's** SOAP and REST APIs to manipulate the business data (objects and fields).



To download metadata from Resco Cloud, connectivity to standard Resco Web Services is required. All the communication between the app and Resco Cloud uses standard Web Services via HTTPS protocol secured by the TLS 1.2 and TLS.1.1 certificates.

Data synchronization with Salesforce, the target organization, must support access to its data via standard Salesforce API.

2. Resco Mobile CRM Client

The local storage encryption is enabled by default and cannot be disabled by the user. The administrator can use the Woodford tool to disable the encryption, but this is not recommended.

2.1. User Password

The main security token for the application is the application password. The application uses this password to encrypt the application database as described later in more detail.

In case of legacy authentication methods which require the app to submit the user's password to server (standard user, external user), the server password is used as an application password for user's convenience. With the OAuth2 authentication, the user must provide a dedicated application password. Regarding password storage, the app can be configured to either:

- Require the user to enter the password each time the application is launched (or resumed from background), or
- Store the password in the device secure storage so that the user does not need to type it in repeatedly.

Explanation:

The device's PIN protects the secure storage so that it cannot be decrypted until the device is unlocked. The device secure storage implementation is platform specific. [1]

The device's PIN prevents access to the device. Most platforms allow for the PIN to be disabled, in which case the application should not rely on storing the password in the device secure storage.

2.2. Data Encryption Details

Data encryption is based on an application key. The application key is randomly generated and protected by the user password. The key is used to encrypt all local CRM data. The details of this procedure are explained below.

[1] iOS secure storage (keychain) security http://sit.sit.fraunhofer.de/studies/en/sc-iphone-passwords.pdf

The application generates the random application key when it creates its local database. Afterwards, it is stored in an encrypted form on the device file system and the application decrypts it when needed. The application key AES256 is used together with the user password (PBKDF2), a random IV and salt for encryption/decryption.

The following explains how the application key is used to secure application data. Remember, there are two 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.

3. Back-end solution

Regardless of the target backend system, it is of utmost importance to ensure there is a reliable and secure network connection between mobile devices and the backend servers, the servers are kept up-to-date with the latest security updates and configured to reject all unauthorized requests.

3.1 Resco Cloud

Servers in Resco Cloud are by default configured to be accessible via internet by the Resco Mobile solution and no special configuration is necessary. Resco Cloud makes use of HTTPS protocol for all communication. When deployed as a Private Cloud solution it is important for the company infrastructure to make sure the servers are accessible from mobile devices.

3.2. Microsoft Dynamics CRM / Dynamics365

The minimal requirement for the synchronization with the Dynamics CRM server is the Dynamics CRM web services and the authentication services availability. In case of the Internet Facing configuration, the Active Directory Federation Services (ADFS) must be accessible, too.

In cases where the Dynamics CRM server and the Active Directory Federation Services are not exposed to the Internet, use VPN or Direct Access connection.

Note: The default configuration of 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.

3.3. Salesforce

In addition to the HTTPS network connection to Salesforce cloud, the Resco Mobile solution requires the target Salesforce organization to have API Access enabled. It is also crucial that Resco Cloud utilized for storing customizations and metadata (https://connect.rescocrm.com) is accessible from the mobile device.

4. Resco Licensing Service

The Resco Mobile CRM Client Access License is validated online by Resco Licensing Service (https://iservices.resco.net).

For this purpose, the mobile application sends the server organization specific information, such as server organization ID and user unique ID, to Resco Licensing Service. This information is also stored in the encrypted local database just as all the other data.

A typical request looks like

```
<MobileClient>
	<Version>6.1.0.0</Version>
	<Edition>Resco</Edition>
	<DeviceId>45d780e4f18354949676f743b0h11633951652bc</DeviceId>
	<DeviceInfo>iPad 2 Wi-Fi only (iPad2,1) iPhone OS 6.0</DeviceInfo>
	<OrganizationId>4F767AFF-B33F-437C-A7CB-00249948C82B</OrganizationId>
	<OrganizationUrl>https://testcrm.resco.net</OrganizationUrl>
	<OrganizationName>testcrm</OrganizationName>
	<UserId>661BAC34-1128-40B1-9653-00B9F54158CD</UserId>
</MobileClient>
```

For deployment scenarios where the Resco Licensing Service is not reachable from client devices, an offline license can be stored in the CRM organization. Still the OrganizationId, OrganiationUrl and UserId must be supplied for an offline license to be issued.

Enterprise Security

As important as it is to get the data about your customers, is to keep them secure once you have them. Especially on a mobile device. With Resco Enterprise Security pack, you don't need to worry anymore. Now you are able to apply enterprise 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. 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 rules through one simple mobile device management (MDM) console.

Mobile Device Management tools

1. Index

   You can index all your mobile devices in one structured list. This feature will give you a quick access to all the necessary information about all the mobile devices used to access CRM data in your company.

2. Groups.

   Divide the mobile devices into groups and apply different security rules. You can create unlimited number of groups and assign them various security policies. The group can consist of many devices or contain just a single device. It is up to you and your needs.

3. Model, OS and ID.

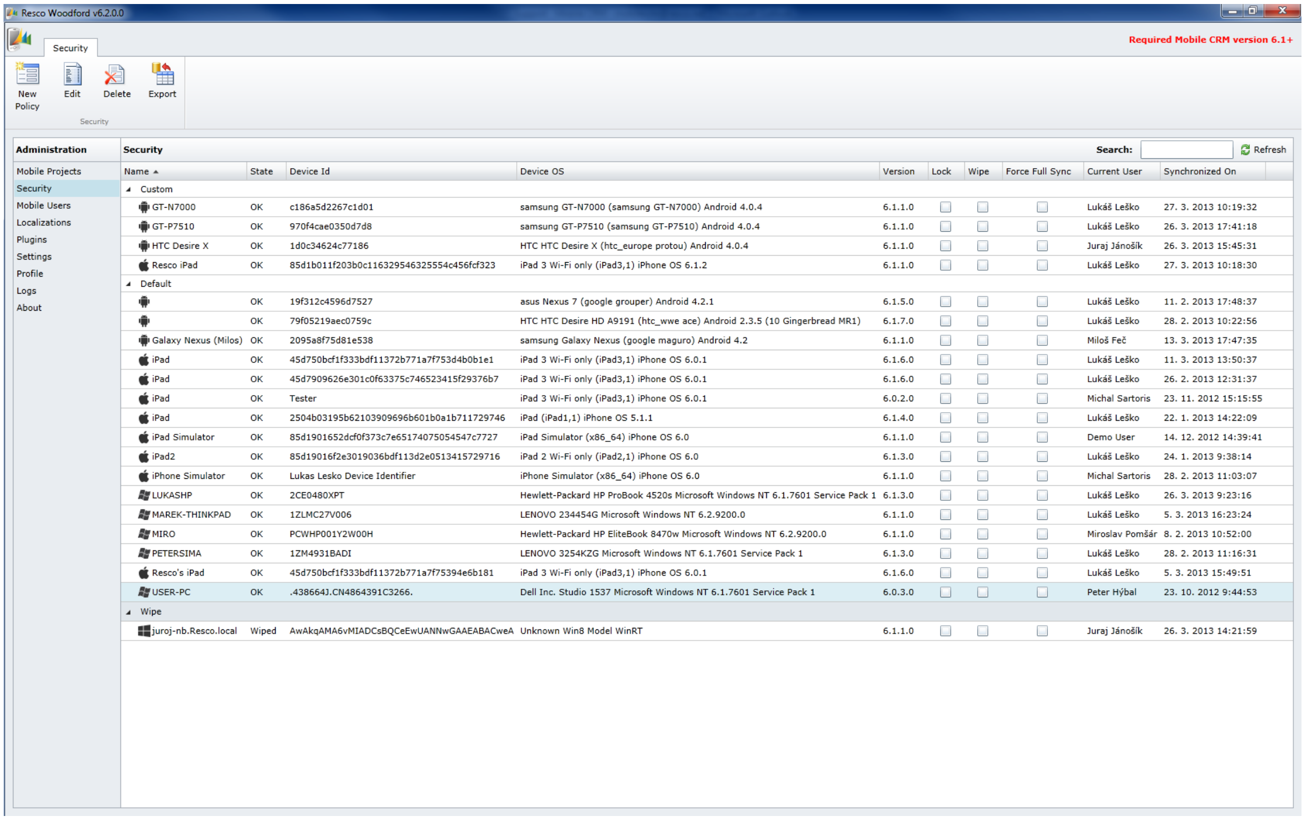
   View details about a mobile device like the model, running OS, and device ID.

4. App version and user.

   Woodford allows you to also see the currently installed version of the MobileCRM app and user of the mobile device. This is helpful to keep your staff updated. You can just view which version of the app is your mobile user currently using and force the update.

5. Synchronization log.

   See when your employees lastly synchronized the app. Keep track of the synchronizations and if it is necessary, force the synchronization remotely.



Name	State	Device Id	Device OS	Version	Lock	Wipe	Force Full Sync	Current User	Synchronized On
Custom									
GT-N7000	OK	c186a5d2267c1d01	samsung GT-N7000 (samsung GT-N7000) Android 4.0.4	6.1.1.0	□	□	□	Lukáš Leško	27. 3. 2013 10:19:32
GT-P7510	OK	970f4cae0350d7d8	samsung GT-P7510 (samsung GT-P7510) Android 4.0.4	6.1.1.0	□	□	□	Lukáš Leško	26. 3. 2013 17:41:18
HTC Desire X	OK	1d0c34624c77186	HTC HTC Desire X (htc_europe protou) Android 4.0.4	6.1.1.0	□	□	□	Juraj Jánošík	26. 3. 2013 15:45:31
Resco iPad	OK	85d1b011f203b0c116329546325554c456fcf323	iPad 3 Wi-Fi only (iPad3,1) iPhone OS 6.1.2	6.1.1.0	□	□	□	Lukáš Leško	27. 3. 2013 10:18:30
Default									
	OK	19f312c4596d7527	asus Nexus 7 (google grouper) Android 4.2.1	6.1.5.0	□	□	□	Lukáš Leško	11. 2. 2013 17:48:37
	OK	79f05219aec0759c	HTC HTC Desire HD A9191 (htc_wwe ace) Android 2.3.5 (10 Gingerbread MR1)	6.1.7.0	□	□	□	Lukáš Leško	28. 2. 2013 10:22:56
Galaxy Nexus (Milos)	OK	2095a8f75d81e538	samsung Galaxy Nexus (google maguro) Android 4.2	6.1.1.0	□	□	□	Miloš Feč	13. 3. 2013 17:47:35
iPad	OK	45d750bcf1f333bdf11372b771a7f753d4b0b1e1	iPad 3 Wi-Fi only (iPad3,1) iPhone OS 6.0.1	6.1.6.0	□	□	□	Lukáš Leško	11. 3. 2013 13:50:37
iPad	OK	45d7909626e301c0f63375c746523415f29376b7	iPad 3 Wi-Fi only (iPad3,1) iPhone OS 6.0.1	6.1.6.0	□	□	□	Lukáš Leško	26. 2. 2013 12:31:37
iPad	OK	Tester	iPad 3 Wi-Fi only (iPad3,1) iPhone OS 6.0.1	6.0.2.0	□	□	□	Michal Sartoris	23. 11. 2012 15:15:55
iPad	OK	2504b03195b62103909696b601b0a1b711729746	iPad (iPad1,1) iPhone OS 5.1.1	6.1.4.0	□	□	□	Lukáš Leško	22. 1. 2013 14:22:09
iPad Simulator	OK	85d1901652dcf0f373c7e65174075054547c7727	iPad Simulator (x86_64) iPhone OS 6.0	6.1.1.0	□	□	□	Demo User	14. 12. 2012 14:39:41
iPad2	OK	85d19016f2e3019036bdf113d2e0513415729716	iPad 2 Wi-Fi only (iPad2,1) iPhone OS 6.0	6.1.3.0	□	□	□	Lukáš Leško	24. 1. 2013 9:38:14
iPhone Simulator	OK	Lukas Lesko Device Identifier	iPhone Simulator (x86_64) iPhone OS 6.0	6.1.1.0	□	□	□	Michal Sartoris	28. 2. 2013 11:03:07
LUKASHP	OK	2CE0480XPT	Hewlett-Packard HP ProBook 4520s Microsoft Windows NT 6.1.7601 Service Pack 1	6.1.3.0	□	□	□	Lukáš Leško	26. 3. 2013 9:23:16
MAREK-THINKPAD	OK	1ZLMC27V006	LENOVO 234454G Microsoft Windows NT 6.2.9200.0	6.1.1.0	□	□	□	Lukáš Leško	5. 3. 2013 16:23:24
MIRO	OK	PCWHP001Y2W00H	Hewlett-Packard HP EliteBook 8470w Microsoft Windows NT 6.2.9200.0	6.1.1.0	□	□	□	Miroslav Pomšár	8. 2. 2013 10:52:00
PETERSIMA	OK	1ZM4931BADI	LENOVO 3254KZG Microsoft Windows NT 6.1.7601 Service Pack 1	6.1.3.0	□	□	□	Lukáš Leško	28. 2. 2013 11:16:31
Resco's iPad	OK	45d750bcf1f333bdf11372b771a7f75394e6b181	iPad 3 Wi-Fi only (iPad3,1) iPhone OS 6.0.1	6.1.6.0	□	□	□	Lukáš Leško	5. 3. 2013 15:49:51
USER-PC	OK	.438664J.CN4864391C3266.	Dell Inc. Studio 1537 Microsoft Windows NT 6.1.7601 Service Pack 1	6.0.3.0	□	□	□	Peter Hýbal	23. 10. 2012 9:44:53
Wipe									
juroj-nb.Resco.local	Wiped	AwAkqAMA6vMIADCsBQCeEwUANNwGAAEABACweA	Unknown Win8 Model WinRT	6.1.1.0	□	□	□	Juraj Jánošík	26. 3. 2013 14:21:59

Picture 1: Resco's MDM tool

MAM tools—push actions (Mobile Application Management tools):

1. Lock

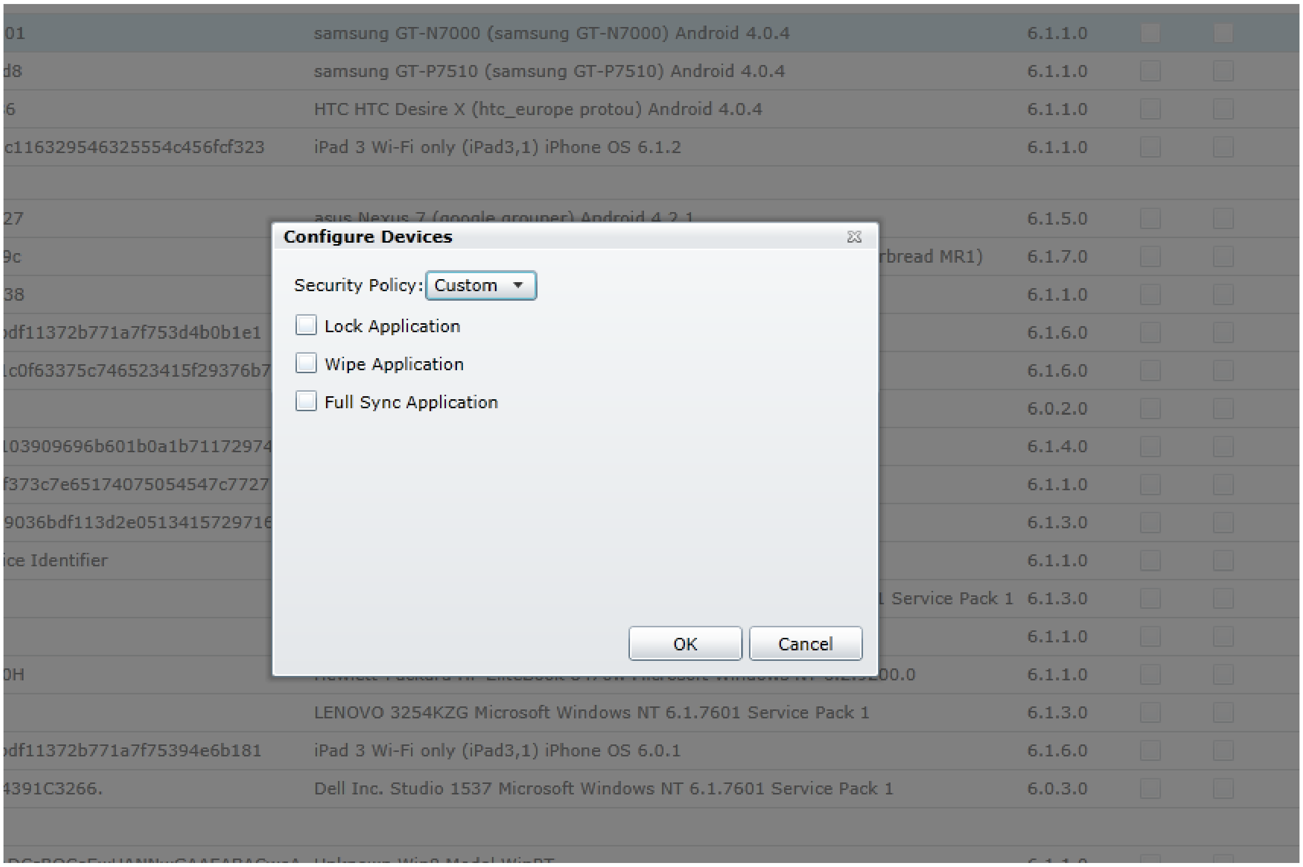
If a device is stolen or there are concerns about the security of offline data, the administrator is able to lock the application remotely on a single device, or a whole group of devices, in just one click and block the user from opening the application.

2. Wipe out

In the worst-case scenario you can completely wipe out the data from the application. All is done remotely just by one click and regardless the synchronization. This means that you delete the data remotely from the mobile device and nobody will be longer available to see them.

3. Force full sync

By just one click, you can force the application to perform a full synchronization of the data during the next synchronization of the app.



01	samsung GT-N7000 (samsung GT-N7000) Android 4.0.4	6.1.1.0	□	□
d8	samsung GT-P7510 (samsung GT-P7510) Android 4.0.4	6.1.1.0	□	□
6	HTC HTC Desire X (htc_europe protou) Android 4.0.4	6.1.1.0	□	□
c116329546325554c456fcf323	iPad 3 Wi-Fi only (iPad3,1) iPhone OS 6.1.2	6.1.1.0	□	□
27	asus Nexus 7 (google grouper) Android 4.2.1	6.1.5.0	□	□
9c	rbread MR1)	6.1.7.0	□	□
38		6.1.1.0	□	□
bdf11372b771a7f753d4b0b1e1		6.1.6.0	□	□
1c0f63375c746523415f29376b7		6.1.6.0	□	□
		6.0.2.0	□	□
103909696b601b0a1b71172974		6.1.4.0	□	□
f373c7e65174075054547c7727		6.1.1.0	□	□
9036bdf113d2e0513415729716		6.1.3.0	□	□
ice Identifier		6.1.1.0	□	□
	l Service Pack 1	6.1.3.0	□	□
		6.1.1.0	□	□
0H	00.0	6.1.1.0	□	□
	LENOVO 3254KZG Microsoft Windows NT 6.1.7601 Service Pack 1	6.1.3.0	□	□
bdf11372b771a7f75394e6b181	iPad 3 Wi-Fi only (iPad3,1) iPhone OS 6.0.1	6.1.6.0	□	□
4391C3266.	Dell Inc. Studio 1537 Microsoft Windows NT 6.1.7601 Service Pack 1	6.0.3.0	□	□

Configure Devices

Security Policy: Custom

□ Lock Application

□ Wipe Application

□ Full Sync Application

Picture 2: Resco's MAM tool

Mobile Application Management tools

1. Session Timeout:

   By enabling this option, you set the rule that the application locks automatically after X minutes of inactivity. After the lock, login is required to resume work with the application. Assuming that the device is lost, with this feature enabled there is very little possibility left for the unauthorized person to access the data using the mobile application.

2. AppLock:

   In a case of need you can remotely locks the application. The user will not be able to work with the application until the access is enabled again by the admin.

3. AppWipe:

   Wipe out the data from the application remotely.

4. Check security policy on login

   If there is a policy set for the user or for the group of users, the application will verify it directly before the login. This makes sure the security policies apply on every launch of the application.

5. Force server connection:

   The mobile device must connect to the server every (x) hours otherwise the login is refused. This way you can force the mobile users to use application and synchronize offline date on regular basis.

6. Force wipe:

   If the app does not connect to the server in (x) hours, all the local data will be wiped out. You can set the interval you consider most fitting to your data security policy. This means that even if the device is left somewhere unattended, the unauthorized user will not be able to access the data after a configured period because it will be already gone. Simple, smart & safe.

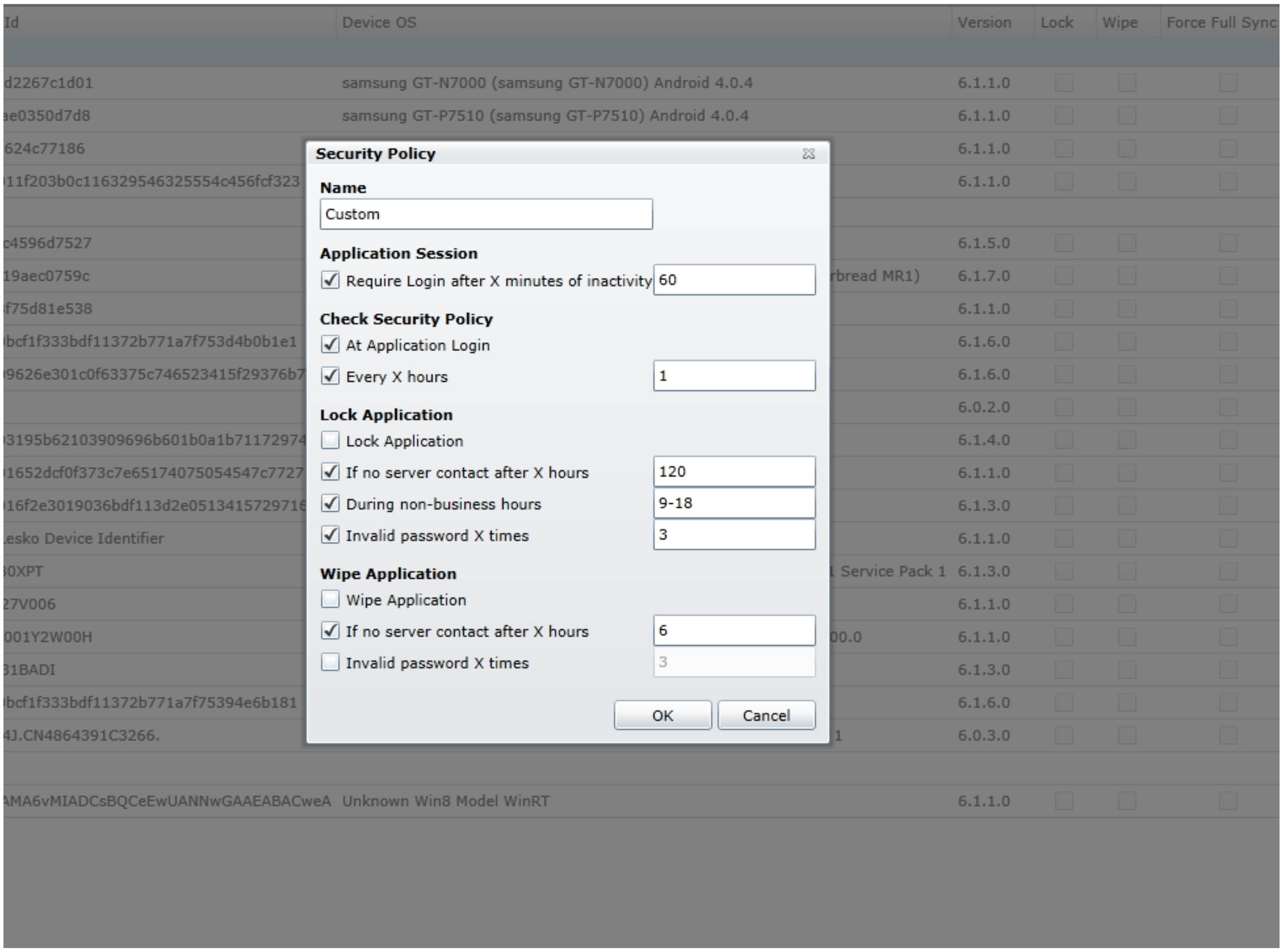
7. Business hours

   You can allow users to access the application only within the configured business hours. For example, if you set the working hours to be 10am-5pm the user will not be able to work with the application at any other time, prior or after these hours. You can set this rule for one user or for a group of users, and you can do it all remotely, even without notifying the users.

8. Password validation

   Locks the app or wipes out the data after a number of incorrect password entry attempts. This is a great feature to prevent dictionary based or brute force attacks. If somebody will try to login to your mobile CRM application and you have this option enabled, they will lock the application directly after the configured number of incorrect logins.

All the Enterprise Security features can be combined to create an ideal security policy to keep your data safe from misusage.



Id	Device OS	Version	Lock	Wipe	Force Full Sync
d2267c1d01	samsung GT-N7000 (samsung GT-N7000) Android 4.0.4	6.1.1.0	☐	☐	☐
ae0350d7d8	samsung GT-P7510 (samsung GT-P7510) Android 4.0.4	6.1.1.0	☐	☐	☐
624c77186		6.1.1.0	☐	☐	☐
11f203b0c116329546325554c456fcf323		6.1.1.0	☐	☐	☐
c4596d7527		6.1.5.0	☐	☐	☐
19aec0759c	rbread MR1)	6.1.7.0	☐	☐	☐
f75d81e538		6.1.1.0	☐	☐	☐
bcf1f333bdf11372b771a7f753d4b0b1e1		6.1.6.0	☐	☐	☐
9626e301c0f63375c746523415f29376b7		6.1.6.0	☐	☐	☐
		6.0.2.0	☐	☐	☐
3195b62103909696b601b0a1b71172974		6.1.4.0	☐	☐	☐
1652dcf0f373c7e65174075054547c7727		6.1.1.0	☐	☐	☐
16f2e3019036bdf113d2e0513415729716		6.1.3.0	☐	☐	☐
esko Device Identifier		6.1.1.0	☐	☐	☐
0XPT	Service Pack 1	6.1.3.0	☐	☐	☐
27V006		6.1.1.0	☐	☐	☐
001Y2W00H	00.0	6.1.1.0	☐	☐	☐
31BADI		6.1.3.0	☐	☐	☐
bcf1f333bdf11372b771a7f75394e6b181		6.1.6.0	☐	☐	☐
4J.CN4864391C3266.	1	6.0.3.0	☐	☐	☐
AMA6vMIADCsBQCeEwUANNwGAAEABACweA	Unknown Win8 Model WinRT	6.1.1.0	☐	☐	☐

Security Policy

Name

Custom

Application Session

☑ Require Login after X minutes of inactivity: 60

Check Security Policy

☑ At Application Login

☑ Every X hours: 1

Lock Application

☐ Lock Application

☑ If no server contact after X hours: 120

☑ During non-business hours: 9-18

☑ Invalid password X times: 3

Wipe Application

☐ Wipe Application

☑ If no server contact after X hours: 6

☐ Invalid password X times: 3

Picture 3: Resco's MSM tool

Remote Application Management tools

To simplify the initial user access to the Resco app, use push applications via Remote Device Management. Follow the below mentioned parameters in your MDM to have control over your enterprise mobility.

Note: that this is the Apple-defined protocol, therefore, it applies only to iOS users for all MDM providers. Since iOS version 9.3, the mobile application supports MDM key-value pair provisioning on iOS devices.

You are able to specify the following parameters in your MDM:

UserMode	(0:Standard, 1:External, 2: Anonymous, 3:CurrentWinUser, 4: OAuth2)
OrganizationUrl	
UserName	
Password	
Domain	
HomeRealm	
ADFSUsername	
SavePassword	(true/false)

ExchangeUrl	
ExchangeEmail	
ExchangeUserName	
ExchangePassword	

SharePointServerType	(0: SameAsCrm, 1: AD, 2: Online, 3: ADFS)
SharePointUserName	
SharePointPassword	

Once the above configuration is specified, the application skips the initial tutorial and shows the synchronization window (with the above values pre-filled) on the first run.