

# Security Considerations for Formotus<sup>™</sup> Mobile Solutions

---

*A Formotus White Paper*

## Contents

The challenge of mobile security .....	2
Overview: How the Formotus Solution Works.....	2
Securing Data on Devices .....	4
Windows Mobile Perimeter Security .....	4
Formotus Data Protection.....	4
Securing Data in Transit .....	6
Securing Data on Servers .....	6
Four Lines of Defense.....	7
Conclusion.....	11
Disclaimer .....	12

## **The challenge of mobile security**

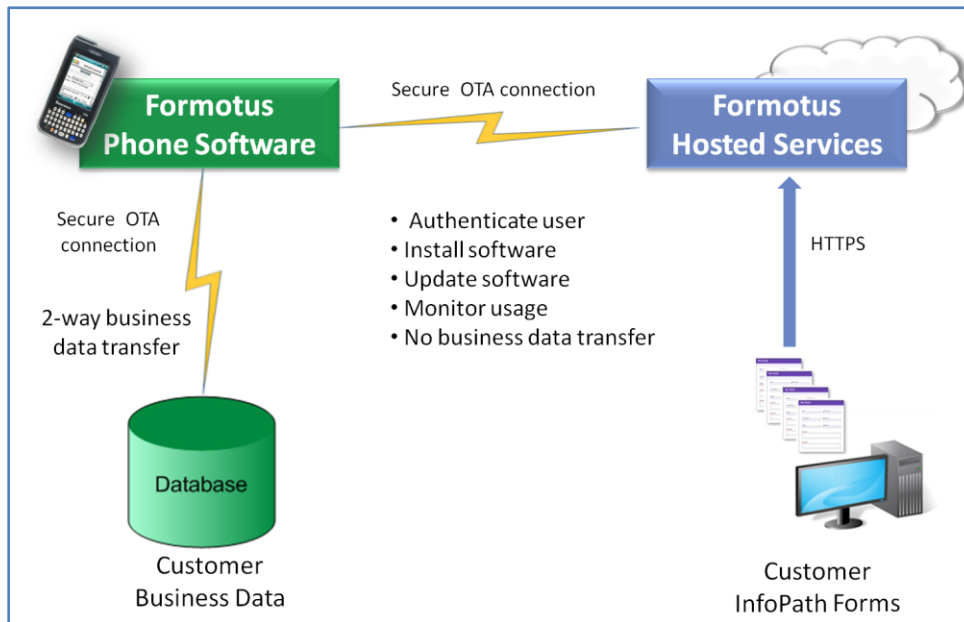
Mobile phones are increasingly capable of performing as the primary device for mobile information workers, and this puts companies in a bind. On one hand, mobile phones offer unprecedented convenience and the promise of higher productivity at lower costs. On the other hand, IT departments are wary of trusting sensitive company information and network access to devices that can be so easily lost or stolen. Formotus understands these security concerns, and has designed the Formotus solution with data security in mind.

This paper addresses the issue of mobile security for companies using Formotus Software + Services to connect a workforce carrying Windows phones to their own backend data systems.

## **Overview: How the Formotus Solution Works**

The Formotus solution uses hosted services to deploy mobile phone software over-the-air. Customers sign in to their Management Console on the Formotus site to deploy applications to their mobile users. The client software on the phone connects to the Management Console on the Web for authentication and to receive notification of new or updated applications. The phone client pulls and installs the deployed applications, which connect directly to the customer's backend business data.

One key feature of this architecture from a security viewpoint is that the customer business data is never transmitted to or stored on any Formotus-controlled server. As the diagram below illustrates, the software on the mobile device exchanges customer business data only with the customer's own designated data servers. The interaction between the mobile device and the Formotus servers is limited to authenticating the user, and provisioning the device with Formotus mobile software, and monitoring the use of that software.



**Figure 1: Formotus hosts software services, not customer business data**

The other architectural feature that is important to understand is the degree to which the customer is in control of all the workflow processes. By logging in as an organization administrator on the Formotus Management Console, the customer controls which InfoPath forms are uploaded and converted to Windows Mobile applications and which mobile users have access to each form.

The manner in which the mobile user is able to interact with company business data is determined by the design of the InfoPath form, which is also entirely under customer control. InfoPath forms can be designed, for example, to extract data from the server onto the mobile device, which involves a greater level of data risk than a form that simply submits field data to the server. Customers can design their forms in accordance with their own security policies.

Finally, notice that the credentials used by the device to exchange company data with the customer's server is entirely separate from the credentials used to authenticate the user on the Formotus service. Since the user must be authenticated on both servers, Formotus authentication merely adds an additional layer of security to whatever level of credentials the customer's own security policies require.

With this general understanding of the Formotus solution architecture, let's turn now to the more specific topics of securing data on devices, in transit, and on servers.

---

## Securing Data on Devices

The greatest concern of many IT departments around mobile deployments is the security of data that resides on a device in the event the device is lost or stolen. Windows Mobile provides features to enhance perimeter security around the whole device, and the Formotus solution is designed both to protect and to minimize the amount of company data on the device at any given time.

### Windows Mobile Perimeter Security

The most important step customers can take to secure their devices is to utilize power-on passwords to lock the devices. Windows Mobile devices support power-on authentication and hashed password storage. Windows Mobile 6 offers enhanced device locks to help protect passwords and PINs.

Companies desiring even stronger perimeter security have additional options. They can develop custom power-on password applications for their devices. They can also explore the advanced server features, such as remote device wiping, available in the Microsoft System Center Mobile Device Manager solution.

### Formotus Data Protection

Formotus applications use strong Windows Mobile encryption to protect any customer business data stored on the device. Windows Mobile encryption algorithm implementations are certified as compliant with the US Federal Information Processing Standard (FIPS), and Windows Mobile 6 uses the Enhanced Advanced Encryption Standard (AES).

Before installing the Formotus mobile software, each user must authenticate online by supplying an automatically generated password that is sent to the user's registered email address. No one else knows the user's password. If necessary, a new password may be generated from the Web, and it will be sent to the email address the organization administrator entered when adding the mobile user to the account.

The user must periodically re-authenticate online with the Formotus service. By default the device saves the user's password on the device, but for enhanced security it is possible to disable the saved password feature by unmarking the Saved Password checkbox on the device.

Formotus mobile software is also designed to minimize the amount of company data being carried on the device at any given time, thereby minimizing risks.

When the user completes a form and submits it, the form is by default sent immediately to the customer's backend data system. This removes the submitted data from the device immediately, thereby minimizing amount of business data residing on the device at any given time.

It is possible to disable this auto-send feature for situations where the customer prefers the ability to work offline intentionally.



Figure 2: Periodic online authentication required

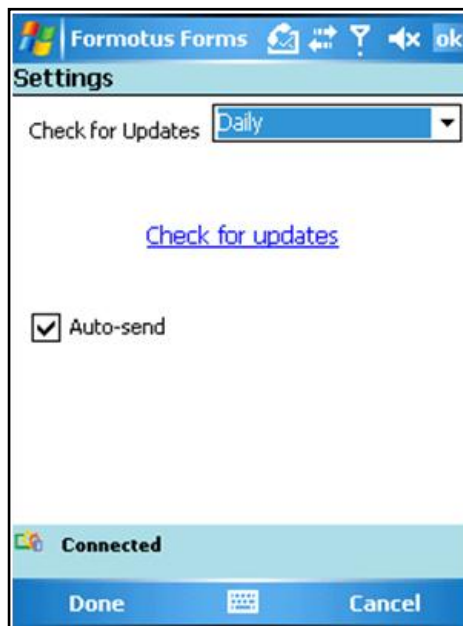


Figure 3: Submitted data sends immediately by default, and is no longer on the device

---

Forms that have been started but not yet submitted are saved as drafts on the device. Unsubmitted drafts may contain sensitive business data, so companies with very high security requirements may need to address this issue with their mobile users.

One other scenario needs to be addressed. Formotus forms can be designed in such a way that they either open an existing form or retrieve data from a backend system such as SharePoint. In this case a device might contain company information beyond only that which has been entered by the mobile user of the device. Customers should consider this possibility when designing their forms and business processes, and avoid enabling mobile devices to access server data that is deemed too sensitive to reside on a mobile device.

## **Securing Data in Transit**

Formotus is not in the business of hosting data services. Customer business data travels directly from the mobile device to the customer's destination, whether that is an in-house server or a hosted service. Formotus servers never make contact with customer business data, only with the mobile software and form templates.

Formotus makes use of the strong encryption and authentication features in Windows Mobile to secure the transfer of data between the device and the customer's server. The customer can make the device-to-network connection as secure as desired. Windows Mobile supports network level encryption for VPN, HTTPS and WPA. Formotus mobile software handles sensitive company data entirely within the security controls the company has implemented.

If the customer builds a Formotus application that submits mobile data to a SharePoint site, for example, it is the SharePoint server that defines the credentials requirements and Windows Mobile that secures the connection with the SharePoint server. Formotus software merely sends the data across the secure connection created between Windows Mobile and SharePoint.

## **Securing Data on Servers**

Customers are responsible for securing their own business data on servers of their choice. Formotus is responsible for securely storing the InfoPath forms that

customers upload to the Formotus service, along the Windows Mobile installation (.cab) files that are created from those forms. Customer forms are protected behind state-of-the-art firewall technology and security monitoring. Proactive security testing is used to simulate attacks, and thorough backup protocols guarantee the persistence of customer forms.

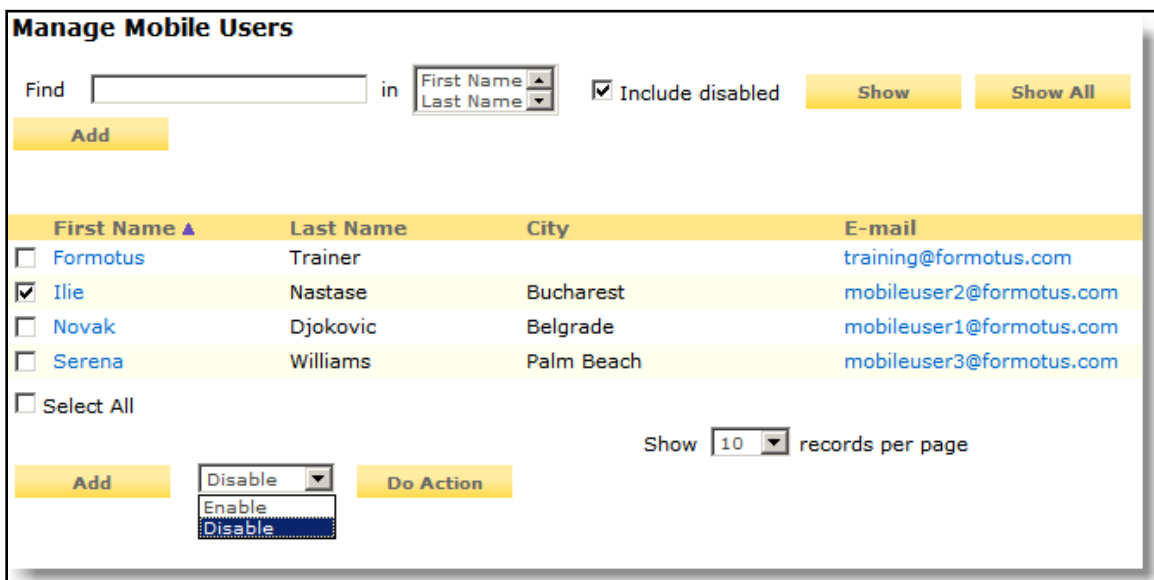
## Four Lines of Defense

The single greatest security concern of companies considering mobile solutions is this: *What is the risk that a mobile device in the wrong hands could compromise sensitive data on the customer server?*

The Formotus solution offers four lines of defense against this risk.

**1. Perimeter security.** We've already discussed how power-on passwords and Formotus authentication can prevent unauthorized access. Let's assume though that this perimeter has failed, and someone has gained access to the Formotus software on the device. Even if the Formotus login credentials have been saved, the device will not be able to exchange business data with the customer's server unless the person holding the device knows server credentials.

**2. Remote Disabling.** As soon as a device is discovered lost or stolen, the customer can immediately disable the Formotus software on the device from the Management Console.



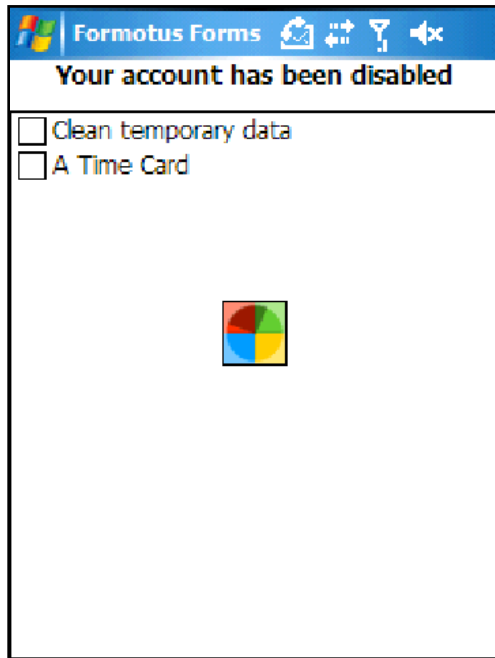
The screenshot shows the 'Manage Mobile Users' interface. At the top, there is a search bar with a 'Find' label and a dropdown menu for 'First Name' and 'Last Name'. To the right of the search bar is a checkbox labeled 'Include disabled' which is checked. Below the search bar are two yellow buttons: 'Add' and 'Show All'. Below these is a table with the following columns: 'First Name', 'Last Name', 'City', and 'E-mail'. The table contains four rows of user data:

First Name	Last Name	City	E-mail
<input type="checkbox"/> Formotus	Trainer		training@formotus.com
<input checked="" type="checkbox"/> Ilie	Nastase	Bucharest	mobileuser2@formotus.com
<input type="checkbox"/> Novak	Djokovic	Belgrade	mobileuser1@formotus.com
<input type="checkbox"/> Serena	Williams	Palm Beach	mobileuser3@formotus.com

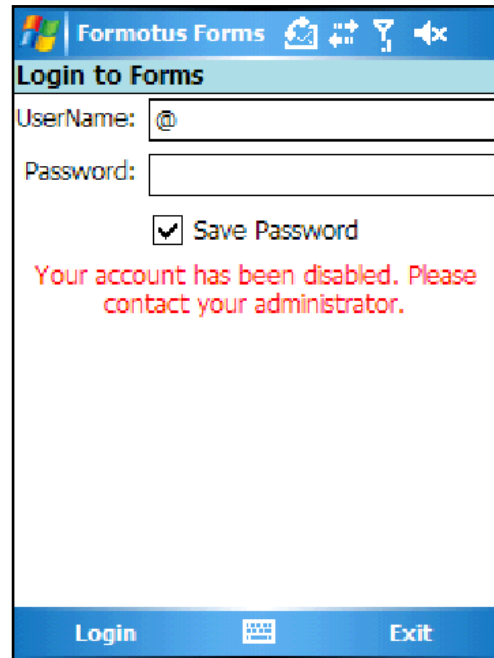
Below the table is a 'Select All' checkbox. To the right of the table is a 'Show' dropdown menu set to '10' records per page. At the bottom left is an 'Add' button. In the center is a dropdown menu with 'Disable' selected, and a 'Do Action' button. Below the dropdown menu, the options 'Enable' and 'Disable' are visible.

Figure 5: Customer can disable a mobile user remotely

Disabling the mobile user of the device not only prevents logging in to the Formotus software, it also removes all the installed customer forms and any business data that may be saved as drafts or unsent outbox items.



**Figure 6: Formotus software removes customer data when a user account is disabled**



**Figure 7: Disabled user accounts cannot launch Formotus software on the device**

But next let's imagine a worst case scenario in which the company is not even aware the device has gone missing. What is the risk and how is it mitigated?

**3. Risk Mitigation.** Remember that Formotus forms cannot access any server data at all unless the customer has intentionally designed a form with that capability. But even forms that do access server data do not give a malicious user wide ranging access to backend data stores. A browser-based or custom coded data application might give a user access to extensive data on the server, but a Formotus form can only access the specific data that the form was designed to acquire.

For example, a form might be designed to reach out to the server and pull a list of customers with addresses for a salesperson to visit. If that salesperson's mobile device were to fall into the wrong hands, there is no way the Formotus software could access anything else from the customer database except the names and

addresses of that particular salesperson's customers. By contrast, a browser-based or custom coded solution might let the salesperson peruse all the data in the customer database, which would be far more harmful in the wrong hands.

**4. Breach Recovery.** Finally, let's consider the situation when a device was missing for a period of time before its software was disabled. The customer in this case needs to determine whether and how the Formotus software on the missing device was used by an unknown person. Every user interaction with the Formotus server is logged and time-stamped, so there will be an audit record of any usage of the Formotus applications that took place during the time the device was out of the customer's control. The user activity reports in the Formotus Web console may help the customer determine the extent of the breach and whether any business data has been compromised.

**Mobile Usage Report**

From:  To:  Select:

13 of 35 100% pforms Find | Next Excel Export

Mobile User	Device Name	Application	Action	Action Date
pforms@formotus.com	Touch_Diamond	Client-PacificID-InventorySheet	Installed	12/3/2008 6:27:54 PM
pforms@formotus.com	Touch_Diamond	Client-MaxHealthcareServ-Pediatric	Installed	12/3/2008 6:27:54 PM
pforms@formotus.com	Touch_Diamond	Client-MaxHealthcareServ-Pediatric	Submit Success	12/3/2008 6:27:54 PM
pforms@formotus.com	Touch_Diamond	Client-Levis-Levis1	Installed	12/3/2008 4:55:26 PM
pforms@formotus.com	Touch_Diamond	SPInstance-Demo-HealthOfficerChecklist	Installed	12/1/2008 8:01:02 PM
pforms@formotus.com	Touch_Diamond	SPInstance-Demo-HealthOfficerChecklist	Submit Success	12/1/2008 8:01:02 PM
pforms@formotus.com	Pocket_PC	SingTel Container Tracking	Submit Success	11/25/2008 12:04:44 AM
pforms@formotus.com	Pocket_PC	Client-LifeTouch-WorkOrderH0e	Submit Success	11/25/2008 12:04:44 AM
pforms@formotus.com	Pocket_PC	SPInstance-Demo-HealthQuestionnaire	Installed	11/25/2008 12:04:44 AM
pforms@formotus.com	Pocket_PC	SPInstance-Demo-HealthQuestionnaire	Submit Success	11/25/2008 12:04:44 AM
pforms@formotus.com	Pocket_PC	SingTel Container Tracking	Installed	11/25/2008 12:04:44 AM
pforms@formotus.com	Pocket_PC	SingTel Container Tracking	Used	11/25/2008 12:04:44 AM
pforms@formotus.com	Pocket_PC	Client-Levis-Levis1	Used	11/25/2008 12:04:44 AM

**Figure 8: Customer can track every time the mobile software was used**

This reporting capability is also beneficial for companies with regulatory compliance requirements. The ability to audit all user interactions with company data can help meet the requirements of regulations such as HIPAA or Sarbanes Oxley. By generating and reviewing Formotus reports regularly, you can supplement your existing audit controls with extra information such as:

- 
- A record of how many and exactly which devices have applications installed that can access your data at any given time.
  - A time stamped log of every attempt by every user to access your data with any Formotus application, and whether the attempt succeeded or failed.

You can use this reporting capability to continuously monitor and control your mobile devices' interactions with protected information, and to create an audit trail demonstrating you have done so.

---

## Conclusion

No data is ever 100 percent secure, and the use of mobile devices to handle company data is inherently riskier than using fixed computers on secure premises. The Formotus solution, however, is carefully designed with layers of protection around customer data along every step of the customer's business processes.

Customer business data is never transferred to Formotus servers, only application usage information. Customer business data is transferred using a secure direct connection between Windows Mobile and the customer's data server, using whatever level of security the customer chooses to implement. Formotus provides an added layer of security by requiring hashed-password authentication even to run the application on the mobile device.

The greatest mobile security concern most companies have is the impact of a lost or stolen device. The Formotus solution provides multiple layers of protection for that situation:

- ✓ Perimeter security requiring up to three different user passwords to access company data: Windows Mobile power-on password, Formotus software login credentials, and the customer's own database access credentials.
- ✓ Remote disabling of the Formotus software in the event a device is lost or stolen, causing the deletion of business data, the removal of business forms, and inability to log in to the mobile client software.
- ✓ Risk mitigation for on-device data including strong Windows Mobile encryption, minimization of the amount and duration of business data stored on the device, and an application architecture strictly limits access to server data from the device. Customers with heightened security concerns can easily design forms that do not access any sensitive server data at all.
- ✓ Breach mitigation through server reports that log every use of the Formotus mobile software, including failed and successful attempts to interact with company business data.

The Formotus Software + Services solution is secure by design and secure by default. Companies with less sensitive data may choose not to use some of the security features available by default, while companies handling more sensitive information can design and use their solutions in such a way as to implement even higher levels of protection.

---

## Disclaimer

The general guidance provided in this document is intended to help improve awareness of HIPAA security principles and how they relate to Formotus technology. It is not legal advice. For specific questions about HIPAA security and privacy requirements as they relate to your organization, you should contact an attorney with expertise in these matters.

The information contained in this document represents the current view of Formotus, Inc., on the issues discussed as of the date of publication. Because Formotus must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Formotus, and Formotus cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is not legal advice and is for informational purposes only. FORMOTUS MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Complying with all applicable copyright laws is the responsibility of the user.

© 2008 Formotus, Inc. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.