CORTADO
MOBILE SOLUTIONS

iOS Business Container

Implementation of Apple's Business Features in the Enterprise

White Paper

Contents

Outline

Situation. **The post-PC era: Is corporate data no longer secure?**
Companies throughout the world are becoming more mobile. The subject of data security in corporate environments, and security gaps associated with it, are a major issue for CIOs and CEOs.

Problem. **Mobile complexity and specific security gaps.**
Mobile device operating systems seem slow to meet the security requirements of companies. Enterprise mobility still faces skepticism. In order to combat this, complicated solutions are brought into the market, and this ultimately results in employees bypassing the provided systems and requirements, causing significant security gaps.

Solution. **How to build a secure business container with iOS.**
After the release of iOS 8 in 2014, important steps have been taken towards making enterprise mobility more secure. Achieving a high level of security is simply a question of using the Apple products practically. Choose apps for your employees, add extra business apps and select the appropriate VPN provider for “per app VPN”. The Mobile Device Management of choice should not only be compatible with iOS, but should also map its range of functions as broadly as possible. These steps will result in secure corporate data when using iOS.

Result. **Trust in iOS is good, but an adequate MDM is indispensable.**
iOS is of no significant benefit if there is no adequate Mobile Device Management in place. Many companies still shy away from this and create their own workarounds, or they use MDM systems that have only a very limited compatibility with iOS. With Cortado MDM – the MDM/MAM solution from Cortado – you are guaranteed effective and comprehensive use of iOS functions.

1. The Post-PC Era: Is Corporate Data No Longer Secure?

Millions of people worldwide use smartphones for business purposes. As a result, data security is an important part of enterprise mobility.

Mobility is increasingly becoming an integral part of daily work processes. Employees use smartphones and tablets for information management, sending and receiving work-related e-mails, visiting social media sites for work purposes, writing notes, taking part in web conferences and using software from office packages. At the same time, the challenges in connection with protecting corporate data on mobile devices are becoming greater and more urgent.

The continual refinement of mobile technology and the wide-ranging ways in which devices are used is indeed a double-edged sword for companies. On the one hand, increasingly sophisticated technology improves employee productivity and flexibility, increases the competitive advantage and possibly even company profits, as well as reduces operational costs. On the other hand, the threat of attacks to a company's data security and the consequences of such attacks are multiplied significantly. According to the Data Breach Report by the Identity Theft Resource Center (ITRC), there were 932 data breaches in 2018 in the US alone[1], and on average it takes 191 days for a company to realize that there has been a data breach at all.[2]

A company must balance guaranteeing its own security interests while also increasing employee productivity. But the variety of devices and system environments makes it more difficult to define security guidelines. If complexity is ignored, then strictly confidential data can be released to the outside world unimpeded. The IT department no longer has control over corporate data. The financial impact due to the loss of sensitive data, which follows on from the loss of competitive advantages, legal violations and erosion of shareholder values, for example, cannot be underestimated. The average cost for each lost data record, for example, was $141 in 2017.[3]

1 Identity Theft Resource Center (ITRC)
https://www.wombatsecurity.com/blog/2018-us-data-breach-statistics-plenty-of-ghosts-in-the-graveyard (October 2018)
2 Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN& (June 2017)
3 Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN& (June 2017)

2. Mobile Complexity and Specific Security Gaps

Mobile technologies are developing and improving rapidly, but at the same time they are becoming increasingly complex. Across all the different versions of the platforms, there are many specific weak points that appear on a regular basis[4] which can be exploited by malware and hacker attacks. According to an American study, a laptop is lost or stolen every 53 seconds.[5] For the individual user this is an inconvenience, but for the corporate world it opens up the possibility for serious compromises of data. The level of severity depends on which sensitive data the respective employee has saved on his device and how easy it is to access it. For example, if the data on the device is not encrypted, then important corporate information is not secure. Likewise, apps can cause significant damage on unmanaged devices and unsecure operating systems.

Without special rules and a Mobile Device Management solution, corporate data is exposed to significant security risks. 77% of employees say their organization did not make them aware of security risks with BYOD[6] This is partly due to the fact that in many cases there are not any guidelines in the first place, or there may be formal requirements in place that are not being enforced. This is added to the fact that generally security risks remain unknown on both sides.

4 Lintell, Andrew: "Complexity is the enemy of security" **https://www.computing.co.uk/ctg/opinion/3026461/complexity-is-the-enemy-of-security**. (February 2018)

5 Olenski, Steven: Is The Data On Your Business' Digital Devices Safe? **https://www.forbes.com/sites/steveolenski/2017/12/08/is-the-data-on-your-business-digital-devices-safe/#391dc1224c6a** (December 2017)

6 Franklin, Roger, E.: 5 Legal Issues Your Company's BYOD Policy Must Address **https://toughnickel.com/business/5-Legal-Issues-Your-Companys-BYOD-Policy-Must-Address** (June 2018)

2.1 Mobile security risks at a glance

The following table describes the most important mobile security risks:

Risk	Description
Downloads from unknown sources/ Public app stores	On Android and Windows devices, you can easily download applications from unknown sources, such as the Internet or from SD cards. Public app stores have a reputation for hosting fraudulent or severely flawed applications. This is presumably due to the very relaxed rules according to which applications are checked and accepted. These apps may be harmful and could copy, transmit or modify important corporate data.
Jailbreaking	Many users hack their device to install applications that are not accepted by the original operating system. This makes it much more likely that harmful applications could be installed.
Unencrypted communication	If a corporate application communicates with backend systems without mutual authentication and encryption of the communication channel encryption, data can be intercepted easily during the transmission and misused.
Lost/Stolen devices	If an employee loses his device with important corporate data, or if it is stolen, it is not difficult to retrieve unencrypted data. This is simple if a basic password – or none at all – has been assigned to data.
Personal mobile devices	Personal devices can be a risk to the security of corporate data if they are not managed and therefore do not follow the same security guidelines as corporately owned devices.
Mobile tethering	Mobile tethering is a useful productivity tool. That being said, if tethering is carried out via an unsecure WLAN with a weak WEP encryption, then it is not difficult for someone in close proximity to intercept the entire communication.
P2P/Adhoc sharing	Many attacks caused by harmful applications are committed via P2P channels such as Bluetooth. The malware can intercept sensitive data and can impair the user's productivity due to reduced device performance. Due to the undesired use of message and service functions, this can also result in a financial loss.

Cumbersome and unrounded mobility management solutions or guidelines often result in employees seeking their own risky workarounds. This does not have to be the case if iOS business features are used correctly.

3. How to Build a Secure iOS Business Container

With iOS, Apple provides the tools required to build a native container and significantly increase mobile data security in the company. First, a Mobile Device Management solution is necessary to manage the applications with the corresponding iOS business features. The minimum requirements of the new APIs, which enable the functionality of the new business features, such as “per app VPN”, are specified by Apple. Application developers must add these to the app source code, thereby standardizing the interface. The functions are only called up by the app, the operating system does the rest and sends the required information back to the app.

In five simple steps, it is possible to create a secure container based on the iOS operating system. These steps are explained in detail below.

3.1 Five steps to a secure, native container

Step 1 **Choose applications for your employees**

Begin by considering which applications should be used in your company and for your employees’ mobile work. The end users should be involved in this step. Also take into account any feedback from employees regarding the applications specified by the company. It is worth setting up a site on the intranet or the company’s social network. Employees can then make suggestions for relevant apps suitable for corporate use. These can be evaluated by the IT department and tested based on the defined security criteria. Finally, the apps that have been given the green light can be pushed to the devices via the MDM system.

Step 2 **Add further necessary apps**

In your company, you probably use a range of intranet applications, such as time management systems, address management, accounting systems for travel expenses, documentation systems, project or schedule planning systems as well as social media platforms. From time to time, these are used to process sensitive data. This is reason enough to offer a secure browser for protected access. Safari can be considered a secure browser when used with Apple's "managed domains" feature. A corresponding enterprise mobility solution that fully supports this feature will be needed. With this feature domains to certain intranet sites can be specified. If a document is downloaded via these sites, it can now only be opened with the managed apps. This makes the Safari browser part of the native container. Domains can also be specified for the native e-mail client, meaning if you receive an e-mail from a listed domain, the attachments can only be opened in the managed apps.

It is important that you use an efficient, secure file sharing solution. In some companies, file sharing is discouraged and in other cases no mobile file sharing is offered at all. As a result cloud storage solutions only intended for private use may end up being used in enterprises. To avoid this, efficient file sharing app should be offered, which increases productivity and flexibility rather than restricting it, while at the same time guaranteeing data security. An on-premise file sharing system is especially recommended. This is advantageous, as the company's own, existing network, already protected by a secure internal firewall, is accessed. The implementation of a new system can therefore be avoided.

Step 3 **Select the right solution for "per app VPN"**

With the "per app VPN" function, all managed apps are routed through the VPN tunnel. Private and unmanaged apps, such as YouTube, Skype or Spotify are excluded. The data traffic is limited to business applications. This draws a clear line between private and business data. The burden due to increased data traffic is also eliminated. The per app VPN should be configured by the IT department. Per app VPN is also relevant in the area of managed domains, as any domains that have been specified for the Safari browser will now use the VPN tunnel.

Step 4 **Can your MDM handle iOS?**

To put it bluntly, without Mobile Device Management to cover all iOS features, all other considerations regarding iOS are meaningless. MDM is the prerequisite for using iOS business features. With viable MDM it is possible to create the business container – the virtual space where all apps and business e-mail accounts are pushed to, and through which all devices can be regulated with per app VPN, app extensions or managed open in. App extensions, for example, offer users a more elegant form of interaction between various apps and enable the direct opening of files in other apps.

Step 5 **Increase data protection**

Here a short clarification to previously mentioned function "managed open in": with managed open in, your administrator can prevent business documents from being opened in unsecure or unmanaged apps. If "managed domains" are not initially used, or the MDM provider has not included e-mail in this feature, then the native Apple e-mail app can be set up as a managed app. Then attachments can only be opened by apps from within the secure business container.

All managed apps with the features "managed open in", "managed domains" and "per app VPN" thus create a native and secure container on the device. At the same time, in iOS, all files are encrypted regardless of whether they contain core data from iOS or from third party applications. All apps are automatically encrypted by default.[7]

In five steps, you now have a secure, native container. There is therefore no need for container solutions from third party providers and complex app-wrapping projects. Bring Your Own Device or Corporate Owned Personally Enabled projects using iOS can actually be implemented securely.

In the next chapter, we take a look at the Enterprise Mobility solution called Cortado MDM. Right from the start, the concept was based on using the natural resources of mobile operating systems to avoid sources of error and ineffective processes.

7 **https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf** (November 2018)

4. Trust in iOS is Good, an Adequate MDM is Indispensable

With Cortado MDM, you have a service at your disposal that can quickly and easily manage your smartphones and tablets centrally.

4.1 Cortado MDM functions in connection with iOS

Now let’s take a look at how the Cortado MDM uses iOS business functions.

Mail account push

In the Cortado MDM management console, you create a profile in which the necessary parameters, such as domain, e-mail address of the user, etc. are entered for the Exchange server (Fig. 1). To add a new new user, simply add the name of the staff member and the user’s company email address. The user then appears on the dashboard, ready to be assigned, under “Assign User”.

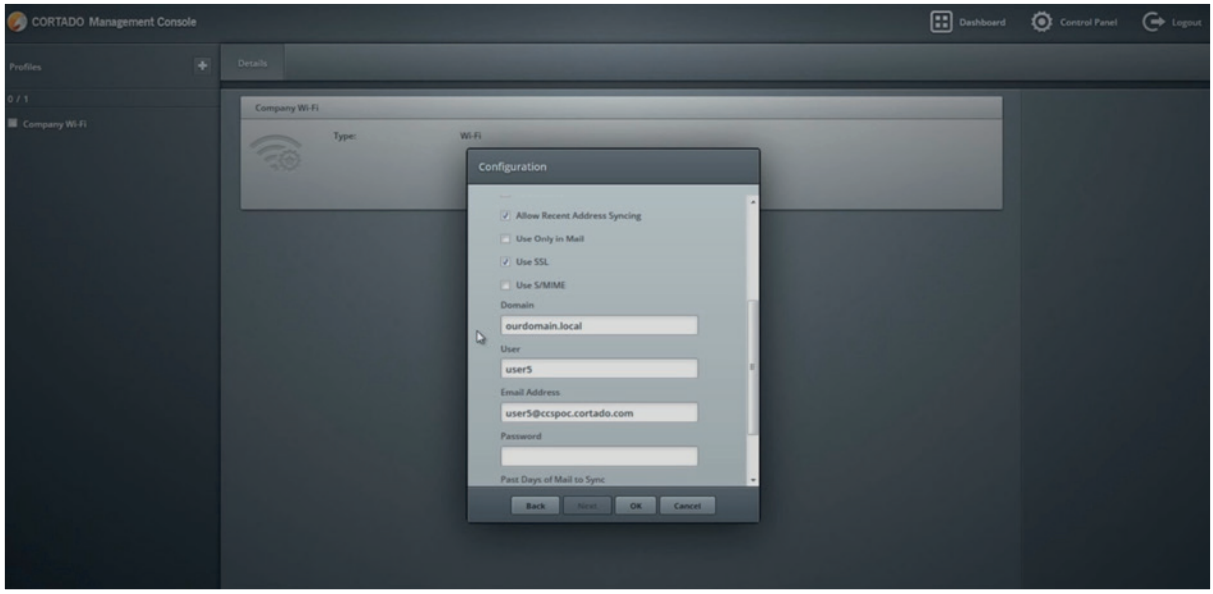

Fig. 1

The profile is then assigned to the user on the respective device. If the employee then logs in with his or her iPhone or iPad, then a single input of their password for the business e-mail account must be given (Fig. 2). After refreshing the mailbox, the account is ready in “Mail”.

Fig. 2

Application push

In the management console, under the “Apps” setting (Fig. 3) the IT administrator can find all business apps. He can assign the corresponding apps to users and user groups. If the employee logs in on his iPad or iPhone, he must simply confirm the installation (Fig. 4) and the application will be available.

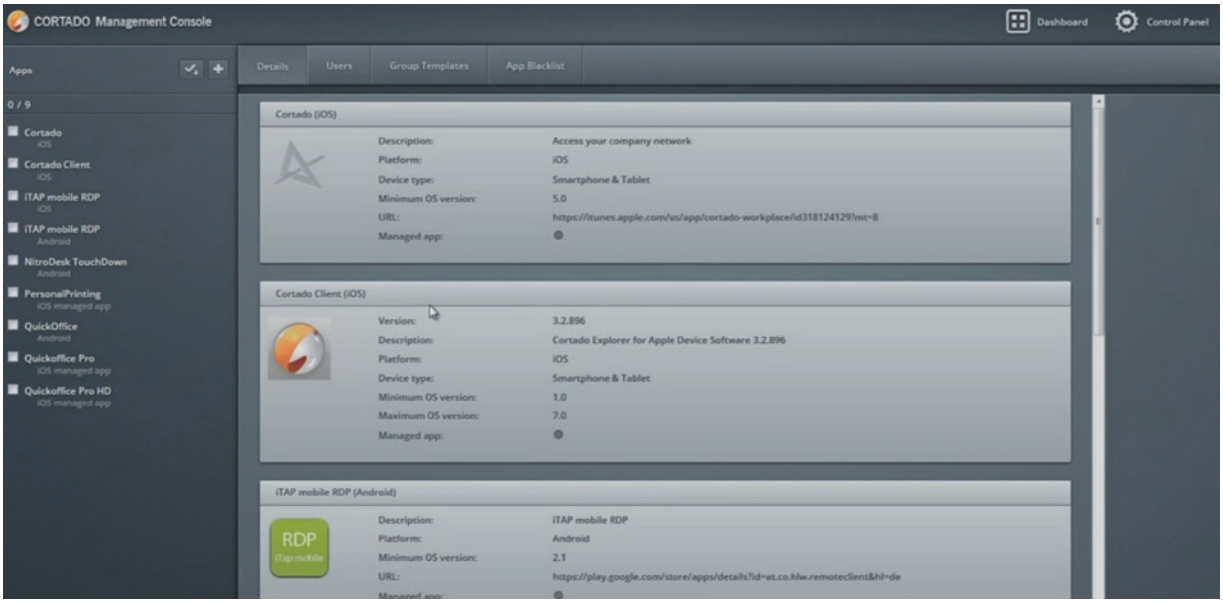

Fig. 3

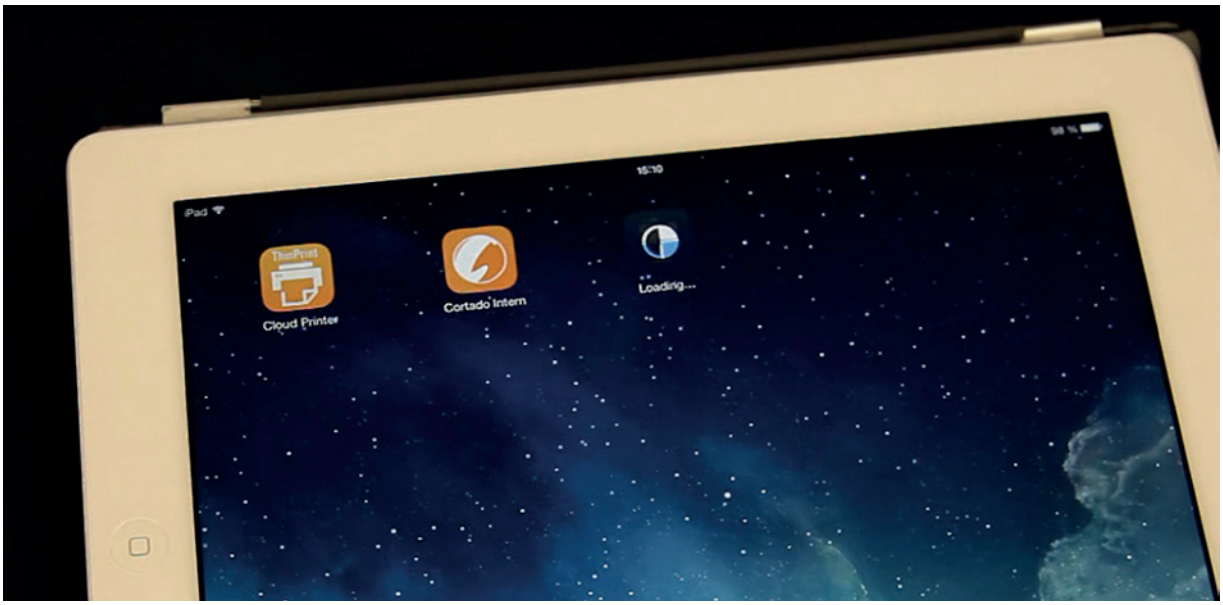

Fig. 4

Managed open in

This is where the policies for app use are defined in the management console. By selecting only “Allow open from managed” as an option, the possibilty to “Allow open from unmanaged” is deactivated (Fig. 5). This means documents can only be opened with the apps that have previously been determined by the IT department.

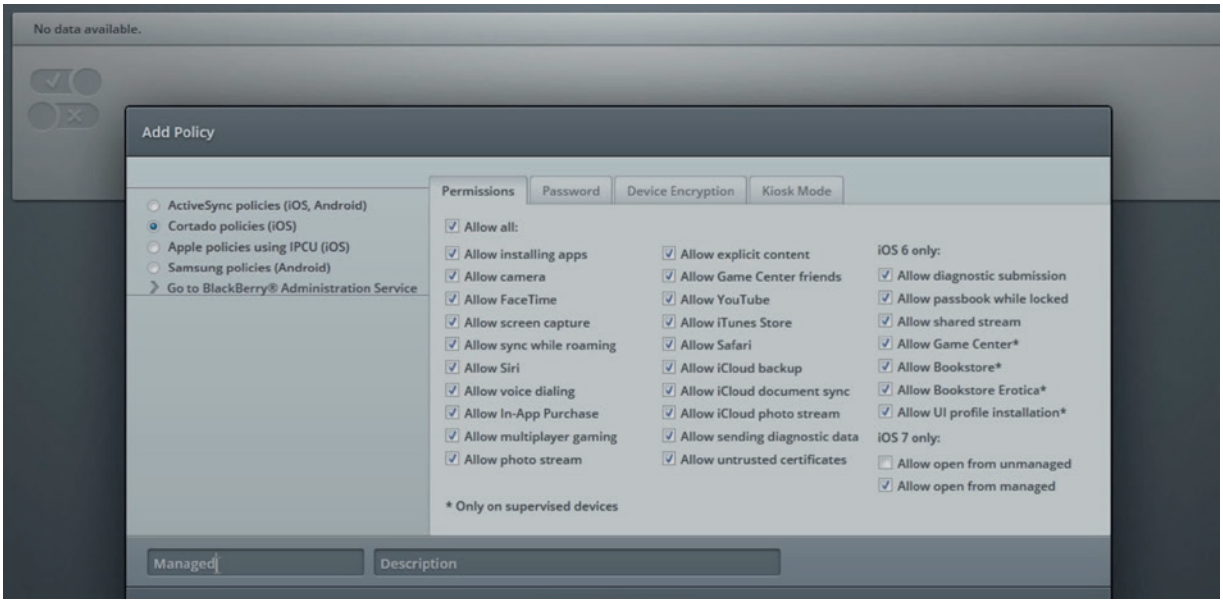

Fig. 5

For example, you can classify a particular productivity application suite as a secure application, and only allow all Microsoft Office documents to be viewed and processed via this app.

App extensions make it possible to add features from other apps within an app, for example editing photos, widgets for the message center, sharing and new keyboards. Previously the function “open in” had to be used to transfer documents within various apps. Documents were then always saved in the storage of the app used, resulting in duplicate files and complex searching for the correct version of files. This is no longer necessary with the help of iOS and Cortado Server. Documents are opened via Cortado Server with their desired app. Changes are then saved back to the corporate server or to the original location.

Managed domains

As previously mentioned Apples native browser Safari is available to use as a secure browser since the release of iOS 8. With “managed domains”, the native e-mail app as well as Safari can be included in the secure container. With the browser, downloaded documents remain in the container and can only be used with MDM controlled managed apps. Via “per app VPN” it is ensured that the traffic of these managed domains only runs through the secure VPN.

Per App VPN

Only managed apps in the native container use the company’s VPN connection, as defined as a policy in the management console. Data is only exchanged via this secure interface. For apps like YouTube, Skype or Spotify, a VPN connection can be deliberately dispensed with. The result is a lower VPN load as well as effective VPN access for the user.

Wi-Fi profile push

In the Cortado Management Console, different Wi-Fi profiles are initially created (Fig. 6).

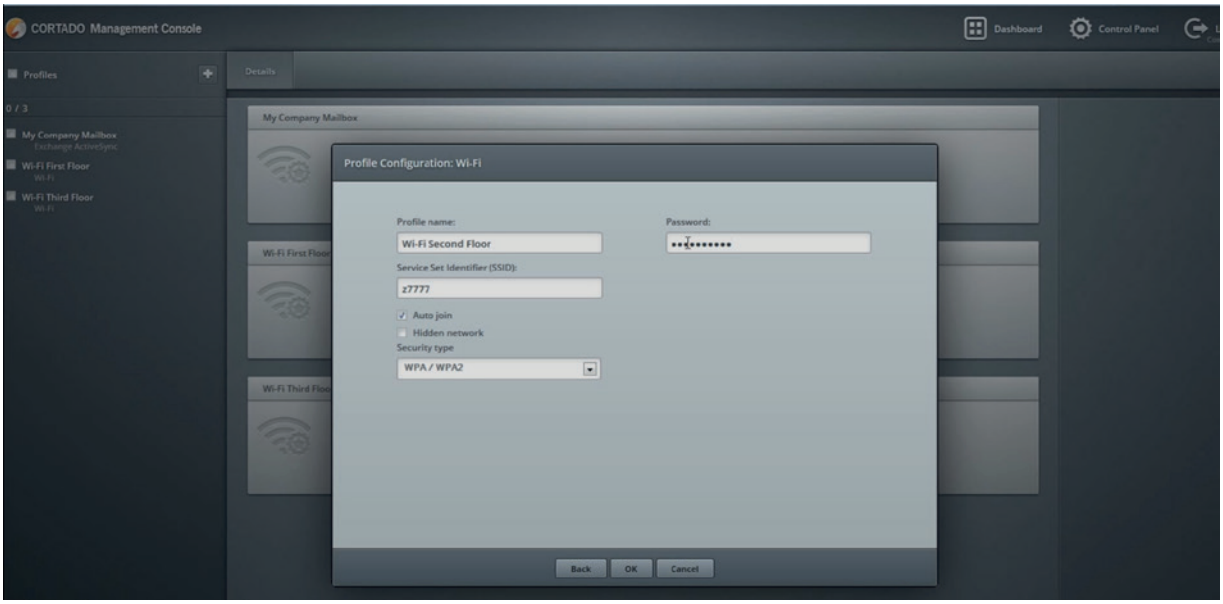

Fig. 6

The respective Wi-Fi profile is then assigned in the user profile in combination with the device used and is then available on the device (Fig. 7, Fig. 8). It is not sufficient to know only the WPA password, but rather the user with the associated iPad or iPhone is also required for verification.

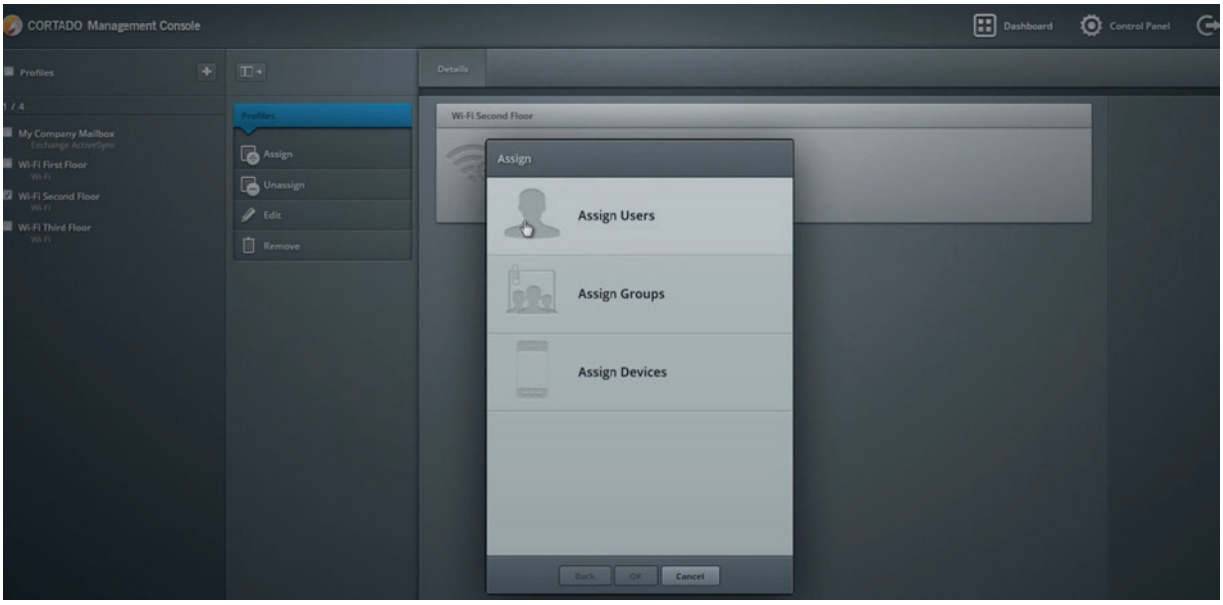

Fig. 7

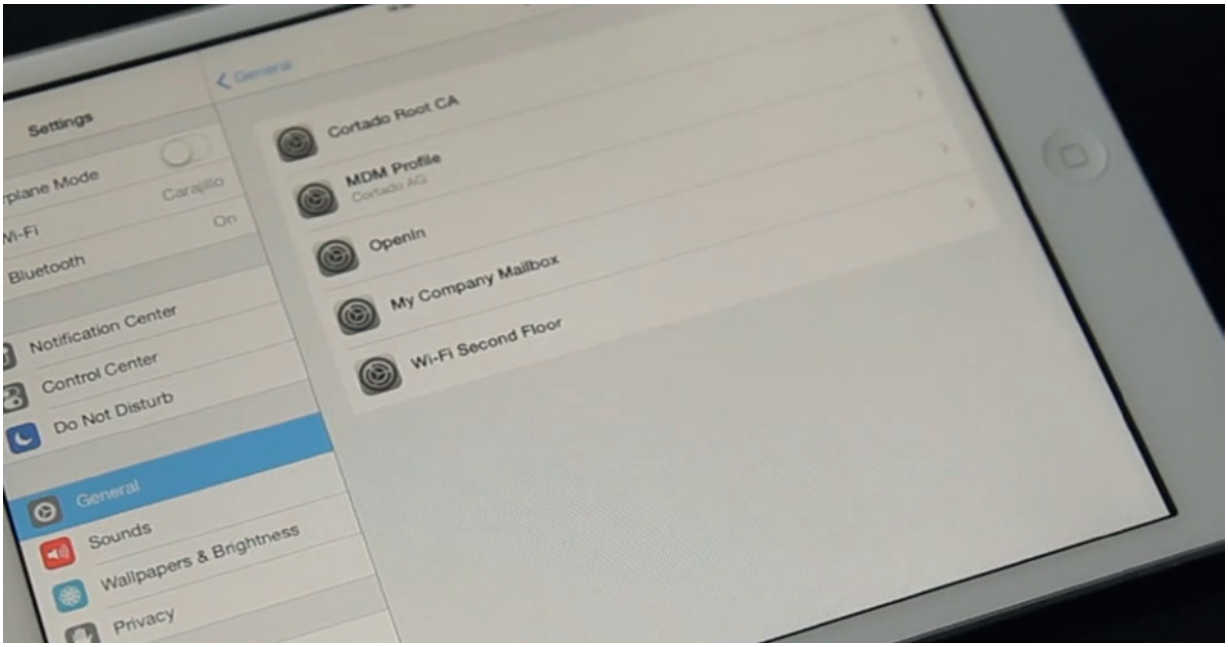

Fig. 8

If, for example, an employee wanted to log on using an unregistered device with the Wi-Fi password, access would be refused. The same applies to unknown Wi-Fi hotspots. These have not been created as profiles for the user and are thus not accepted for use of Cortado MDM.

Secure & native container

Since all the above-mentioned features are set up via the Management Console, a secure and native container is created. All iOS devices and the business applications found on them are managed by Cortado MDM. The user barely notices that there is a distinction between business and private use on his iPhone or iPad.

Summary

While mobile data security is at times a secondary consideration for private mobility users, businesses have completely different considerations to take into account. Unfortunately, many companies are willing to accept the existence of security gaps instead of utlizing existing mobile management solutions. Without the company-wide management or even excessive regulatory constraints on mobile devices, these security gaps will only become greater. In the meantime, there are sufficient offers on the market to meet the need for secure data traffic from a corporate perspective and to ensure smooth, effective mobile work from the employee's perspective. With iOS, Apple offers business features that enable a secure, native container on mobile devices:

- **Quick and efficient setup:** With mail account push and application push, corporate mail accounts and apps are automatically pushed to employees' devices via for example Cortado MDM Console with just a few clicks. Employees no longer have to worry about setting up corporate mail and essential apps on their devices.

- **More security, less workarounds:** By enabling "managed open in", "per app VPN", "Wi-Fi push", "managed domains" and "app extensions" in the Cortado's MDM, a native, secure container is created on employee iPads and iPhones. This includes the native mail app, the native Apple browser and all other managed iOS and Cortado apps used for effective network access and file sharing. This ensures a complete and secure business area or business container with native apps on iOS devices.

- **Increased acceptance of BYOD:** Employees feel more secure and protected when using BYOD. The acceptance of a BYOD program is also increasing, as personal and business data on the iPhone and iPad are separated. IT administration only has access to the data in the native business container.

Additional white papers or questions:
You can download this and many other white papers on relevant IT subjects here:
www.cortado.com/whitepapers.

Any questions?
The Cortado team will be happy to help. We can be contacted at the following telephone number: **+49 (0)30 408 198 500** or send an e-mail to **info@cortado.com**.

Headquarters

Cortado Mobile Solutions GmbH
Alt-Moabit 91a/b
10559 Berlin, Germany
Tel.: +49 (0)30 408 198 500
Fax: +49 (0)30 408 198 501
E-Mail: info@cortado.de
www.cortado.de

Australia

Cortado Pty Ltd.
Level 12, Plaza Building,
Australia Square, 95 Pitt Street
NSW 2000 Sydney, Australia
Tel.: +61-(0)2-8079 2989

USA (Colorado)

Cortado, Inc.
3858 Walnut Street, Suite 130
Denver, CO 80205, USA
Tel.: +1-303-487-1302
E-mail: info@cortado.com
www.cortado.com

Japan

Cortado Japan
5F Yaesu Dori Building,
3-4-15 Nihonbashi,
Chuo-ku Tokyo
Tokyo 103-0027
Tel.: +81-(0)3-6870 3467

CORTADO
MOBILE SOLUTIONS

Follow Cortado at: facebook twitter youtube linkedin