HOB
Cyber Security

HOBLink Mobile and HOBCOM Universal Server

Secure Access to Enterprise Resources with Mobile Devices

Overview

Current studies show that ever more employees want to access enterprise data and applications via their mobile devices. Many IT managers, however, see in this trend a great security risk for their companies, as mobile devices often are not properly secured and in many cases are not integrated into the enterprise-internal security plan. The danger exists, that highly sensitive corporate data could get lost or end up in the wrong hands, or that the user unwittingly allows malware to infiltrate the company network.

HOB has recognized this security risk and has developed a solution for mobile devices that enables secure remote access to centrally stored enterprise data: HOBLink Mobile. HOBLink Mobile also provides for optimal bandwidth utilization and reduction of the time needed to make a connection.

The special advantage of HOBLink Mobile is that the user is provided with secure access to his e-mail, contacts, calendar and notes without saving any of the data on the mobile device. Should the mobile device fall into the wrong hands or malfunction, there will be no sensitive data on it to be compromised.
The user can continue to work with a replacement device, as all data are stored completely and securely on the company server.

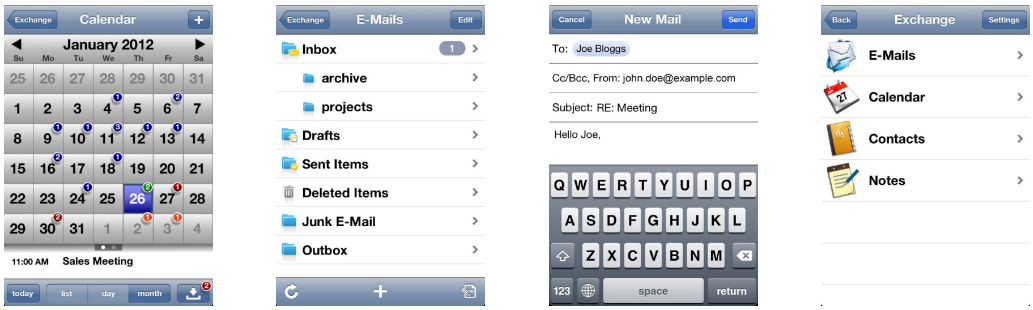
The central component of this solution is the HOBCOM Universal Server (HCU). This is installed in the corporate DMZ or LAN. The HOBLink Mobile Client is used to access the HCU Server from the mobile device. Inside the LAN, the HOBCOM Universal Server communicates with a Microsoft Exchange Server, from which it receives the requested data. The information is then sent to the

Advantages at a Glance

- Data security even in the event of loss, theft or manipulation of the mobile device
- No data loss due to disruption of the WLAN / mobile network
- Secure access to data centrally stored in the enterprise
- Optimal bandwidth utilization and reduction of time needed to make a connection
- Central user administration
- Low memory requirements
- VPN connection not necessary
- Ideal solution for “Bring Your Own Device”

HOBLink Mobile Client. Hereby, it is important to note that only the data that is immediately required for the display is sent to the mobile device. Only as long as the application is active is this data loaded into the main memory. When the application is terminated, none of this data remains on the device. Hereby, the encryption of all communications is ensured.

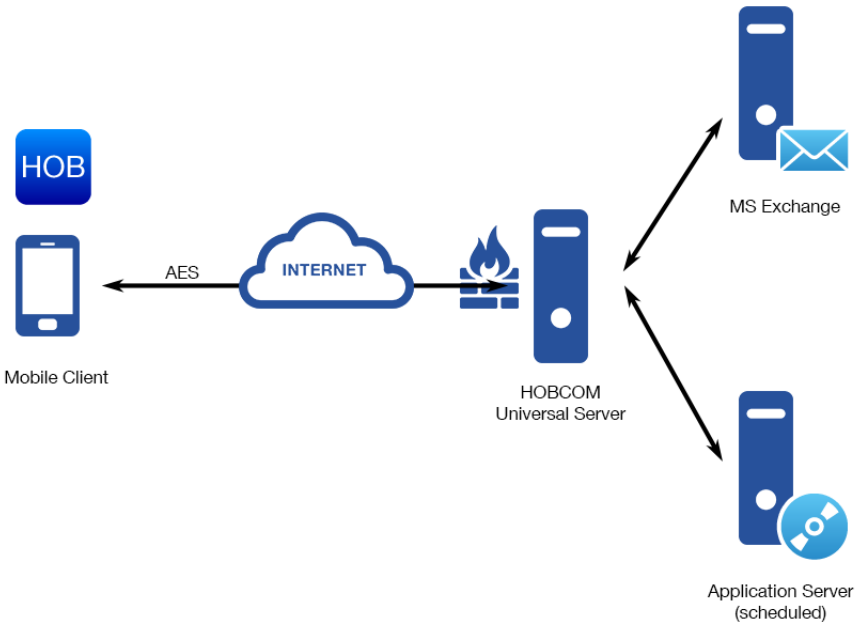
HOBLink Mobile thus allows secure access to centrally stored enterprise data without saving them locally to the mobile device. This enables the secure and best possible deployment of mobile devices – at any time and from anywhere in the world.



Secure Communication with HOBLink Mobile

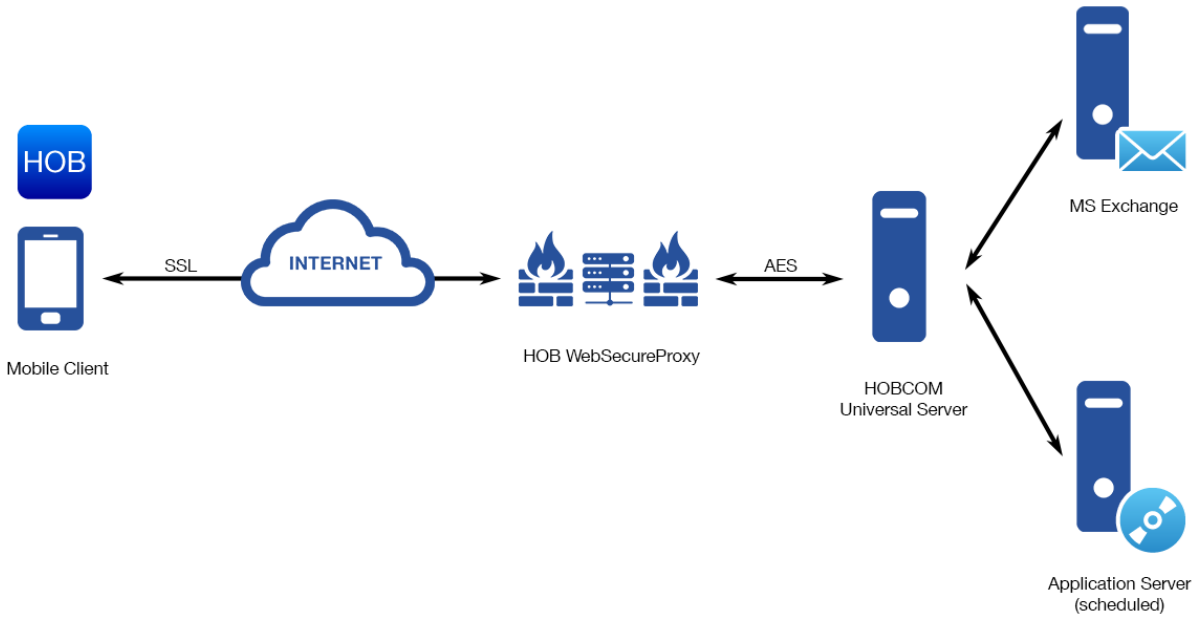
HOBLink Mobile offers you two possible methods for secure communications with the HCU Server: Either direct communication or communication over HOB RD VPN's HOB WebSecureProxy.

1. Direct Communication between the HOBLink Mobile Client and the HCU Server



The connection between the HOBLink Mobile Client and the HCU Server is always encrypted with AES (128bit). For communications between the HOBLink Mobile Client and the HCU Server, an HCU protocol developed by HOB is used.

2. Communication between the HOBLink Mobile Client and the HCU Server over HOB RD VPN‘s HOB WebSecureProxy:



The connection between the HOBLink Mobile Client and the HCU Server is always encrypted with AES (128bit). For communications between the HOBLink Mobile Client and the HCU Server, an HCU protocol developed by HOB is used.

Authentication

Even more security is provided by the various authentication methods which are available to HOBLink Mobile. Authentication for a direct connection to the HCU Server is carried out via a username and password combination. When communicating with the HOB WebSecureProxy, additional authentication methods, such as Radius, certificates or One-Time Password Tokens are available. To display the data, a connection to the HCU Server with previous authentication is always required.

Data Security in the Event the Mobile Device is Lost

If the mobile device is lost, the user must immediately inform the responsible administrator, who can then block the user’s account on the HCU Server right away. Furthermore, HOB recommends to activate code locking on the mobile device. It must be emphasized that the data cannot be read by any third-party, as they are stored centrally and not at all on the mobile device.

Reconnecting a Disconnected Session

If the mobile device‘s connection is interrupted, the disconnected session can be restored. When a connection is broken or the mobile device switched off, the reconnect function can be used to restore the last context. This avoids annoying re-logins and the accompanying delays.

Access with Self-Developed Java Programs

If you would like to access other data, there is the possibility to write your own Java programs and make them available to your users. This is enabled by the Byte-Code Interpreter Interface (BCI Interface), a Java Virtual Machine developed by HOB. The BCI Interface provides a Java environment and serves as a “Sandbox” for user programs. Hereby, the server’s integrity is protected.

HOBLink Mobile Functions

In conjunction with the HOBCOM Universal Server, HOBLink Mobile supports complete e-mail access. Additionally, the following functions are also available:

E-Mail:

- Personal e-mail signature
- Move, write and delete e-mails
- Respond and forward
- Create new folders
- Display attachments
- Search function

Calendar:

- Calendar views: List, Today, Day and Month
- Create and receive invitations
- Create and edit appointments

Contacts:

- Display of personal contacts
- Create, edit, or delete contacts
- Search contacts in the company directory (Active Directory)
- Customization of the sort function

Notes:

- Create notes
- Edit, delete notes
- Send notes via e-mail

Highlights

- Secure access to confidential and centrally stored enterprise data
- Data are not saved to the mobile device
- Data security in the event of theft, loss or manipulation of the mobile device
- Avoidance of data loss through flaws in the WiFi / mobile network
- Central user management
- Low connectivity costs via compressed data volume
- Functions even over very slow connections, e.g., GPRS
- Easy integration into an existing Exchange environment

System Requirements

For HCU Server

- Windows Platform: Windows Server 2008, Windows Server 2008 R2, Windows Server 12, Windows Server 2012 R2

Minimum Hardware Requirements:

- CPU: at least 1GHz, recommended, 2GHz
- RAM: Depends on the number of users
  who simultaneously communicate with, or are logged onto, the server:
  - » 1 user: at least 1MB main memory, recommended, 2MB
  - » For small installations up to 100 users - at least 512MB
  - » Network card: at least one must be available, recommended, 100MBit/s
  - » HDD: 500MB hard-disk storage
  - » Microsoft Visual c++ 2010 SP1 Redistributable Package (x86)

HOBLink Mobile Client

- iPhone, iPod touch, iPad: min. iOS 5.1.1
- Mobile devices with Android: min. Version 4.0.3

MS Exchange Server

- From version 2007 SP1 up - Exchange Web Services (EWS) must be activated

Authentification

- LDAP directory - Microsoft Active Directory Domain Services