



## CORISECIO - Mobile Firewall

*Mobile Suite - more than just Device Management*

The Mobile Firewall provides functions for the protection of the device configuration as well as for blocking and monitoring of risky interfaces. User rights for modification of settings, rules for use of Bluetooth- and WLAN-adapters, IrDa- interfaces and digital cameras may be realized to driver level. Protected settings for internet connections, Access Points, VPN-Tunnel and Proxy Server protect the infrastructure as well as the mobile devices and business critical data.

### USER RIGHTS

The absence of user rights on Windows Mobile based platforms turns every user into an administrator. Consequences are unwanted configuration modifications and thereby increasing helpdesk activities as well as problems and risks caused by use of unwanted applications. The Mobile Firewall provides the possibility to grant access rights for settings modification. There by network management, internet and corporate networks are supported. Rights for installing, editing and manipulating for modems, Proxy Server, VPN-connections, email accounts etc. have to be explicitly granted by the administrator.

### SECURE CONNECTIONS

The implemented rights concept may used for the enforcement of secured connections as well. By using the remote configuration e.g. the use of in-house Proxy Servers and Internet Access Points may be enforced. Frequent use cases like an obligatory VPN for all IP-connections are easily to be realized.

### CONNECTIVITY

CORISECIO avoids the risk of the Always-On radio technologies with firewall functionality for wireless interfaces. Use of WLAN-, Bluetooth- and Infrared-Adapters need explicit authorization from the firewall settings. If it's not allowed these interfaces are blocked reliably. Additionally with this technology dedicated rules for use may be established. Rights for specified use of defined (in-house) Access Points may be generated as well as restrictions for Bluetooth use on certain device types (e. g. headsets) .

### USB ACTIVE SYNC

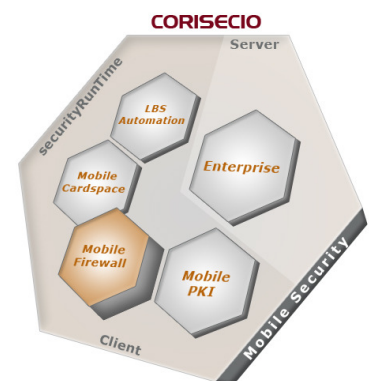
Besides the wireless interfaces CORISECIO also controls the local Active Sync connection to Desktop PC and Notebooks. IT-administrators specify, which mobile devices are authorized to exchange, update or copy data (e.g. e-mails, contacts) with which Desktop PCs. The assignment of ac-

### FACTS

- Implementation of Security Policy
- Closing security holes
- Control of applications
- Control of features, interfaces & synchronization
- Reduction of maloperation
- Safe use of Over-the-Air technology

### BENEFITS

- Increased security
- Efficient use of PDA
- Considerably decreased Helpdesk costs
- Increased availability
- Improved usability
- Platform independence



cess rights is flexible, so that even in-house rights can be assigned on corporate, department or employee level.

In conjunction with the optionally Desktop component in-house PC, Notebooks and Netbooks will be protected against unwanted synchronization. Only the data exchange between company devices can be allowed. During the initiation process of an ActiveSync connection, Sync Control verifies the authorization and only builds up a data connection in case of success. Unwanted connections like, the unauthorized use of private Pocket PCs with company-owned notebooks or the synchronization of company Smartphones with home Desktop PCs are reliably disabled.

### MOBILE APPLICATIONS AND FEATURES

Mobile devices are equipped with a multitude of applications and features. As not every application is wanted for company use, the Mobile Firewall prevents use of unwanted applications. Via positive- or negative lists administrators define which programs will be executed and which features are allowed to use. Thus program requests, network accesses as well as the use of built-in digital cameras or SD cards may easily be regulated. Besides standard applications CORISECIO also supports proprietary- and 3rd Party software. The graphic Window-Scanner provides administrators with a simple generic tool for definition of firewall rules for mobile applications. To enhance usability unused and blocked program- and settings can be removed easily.

### DEVICE CONTROL CONFIGURES – MOBILE FIREWALL PROTECTS

Mobile Firewall is a powerful extension of the securityRunTime. Combined, the devices may be completely preconfigured and the settings may be effectively protected against modifications. IT officers so receive a powerful solution, which increases security, decreases costs and significantly enhances stability, user comfort and productivity.

## KEY FEATURES

- Protected network settings
- Protected email accounts
- Protected Exchange configuration
- Control of WLAN interface
  - *Disabling of WLAN Adapters*
  - *Defined Access Points (SSID-positive list)*
  - *Defined authentication/encryption*
- Control of Bluetooth interface
  - *Disabling of Bluetooth Adapter*
  - *Disabling of Scan Option*
  - *Only defined profiles (e. g. Headset)*
  - *Only defined devices (optional)*
- Control of IrDA interface
  - *Blocking of incoming connections*
- Application lock
  - *Windows Mobile Standard applications*
  - *Any applications*
- Configuration of programs and settings
  - *Black & White Lists*
  - *TOP Programs*
- Feature lock
  - *Disabling of digital camera*
  - *Disabling SD card access*
- Control of USB Synchronization
- Registry monitoring
- Backup Enforcement

