



Einfache und sichere Konfiguration von Smartphones & PDA



Der Einsatz mobiler Geräte ist kein Selbstzweck. Sinnvoll eingesetzt, können Geschäftsprozesse beschleunigt, Abläufe optimiert und die Informationsversorgung verbessert werden. Einen echten Gewinn für Unternehmen stellen mobile Geräte aber erst dar, wenn die Benutzung gleichsam sicher und einfach für den Endbenutzer realisiert wird. Die Herausforderungen mobiler Geräte sind bekannt und erfordern neue Lösungsansätze, damit Handy's, Smart Phones und Pocket PCs ähnlich einfach in Unternehmen eingebunden werden können, wie Desktop PCs und Notebooks.

Eine der wichtigsten Aufgaben ist dabei, die Administration und Konfiguration der mobilen Geräte, mit dem Ziel, die Funktionsfähigkeit einfach zu gewährleisten. Dies bedeutet bspw. risikoreiche Schnittstellen wie WLAN, Bluetooth und Kameras abzuschalten oder spezielle Anwendungen zu ermöglichen, sowie Netzwerkkonfiguration, Internetzugang oder VPN Einstellungen zentral zu konfigurieren und gegen Manipulation zu schützen.

Benötigt werden Sicherheit, Konfiguration und Administration aller im Unternehmen eingesetzten Geräte. Dabei werden Unternehmen mit zentralen Fragestellungen konfrontiert.

- **Roll-Out:** Wie konfigurieren Sie effizient eine Vielzahl mobiler Geräte?
- **Helpdesk:** Wie minimieren Sie die Fehlbedienungen der Geräte?
- **Usability:** Wie vereinfachen Sie die Bedienung für die Benutzer?
- **Security:** Wie verhindern Sie die unerwünschte und risikoreiche Nutzung von WLAN, Bluetooth und IrDa?
- **Governance:** Wie verhindern Sie den Einsatz eingebauter Digitalkameras auf dem Firmengelände?

WIE KONFIGURIEREN SIE EFFIZIENT EINE VIELZAHL MOBILER GERÄTE?

Eine Herausforderung der effizienten Administration und Konfiguration von mobilen Geräten liegt in den Verbindungseinstellungen. Viele Unternehmen nutzen eigene Access Points für den Internetzugang, spezifische Konfigurationen für das Unternehmensnetzwerk und E-Mail, sowie Lösungen wie VPN für einen sicheren Zugang. Eine typische Grundinstallation eines mobilen Geräts verändert daher nicht selten über 30 Parameter in unterschiedlichen Dialogen. Zudem erfordert die korrekte Konfiguration spezielle Kenntnisse, so dass in den meisten Fällen eine End-Benutzer-Konfiguration aufgrund der hohen Fehlerquote nicht praktikabel ist. Die Usability herkömmlicher Geräte ist nur bedingt für die Mehrzahl der Mitarbeiter ausreichend. Im Normalfall bedeutet dies, der Administrator muss jedes Gerät vor der Auslieferung konfigurieren. Daher führt der Administrator oftmals ein und dieselbe Netzwerkkonfiguration auf einer Vielzahl von Geräten durch, um bspw. allen Mitarbeitern des Außendienstes mobilen Zugriff auf das Netzwerk via VPN zu geben. Eine zeit- und kostenintensive Routineaufgabe, die wertvolle Ressourcen blockiert aber durch die Möglichkeit, vorkonfigurierte Profile zu erstellen, leicht zu vermeiden ist. An dieser Stelle setzt die CORISECIO – Mobile Suite an.

CORISECIO – Device Control erlaubt das Set-Up mobiler Geräte über vorkonfigurierte Profile und die Usability wird für alle Endbenutzer optimal eingestellt! Über eine zentrale Oberfläche konfiguriert der Administrator entsprechende Verbindungen, Einstellungen und Sicherheitsfunktionalität und erstellt im Ergebnis ein Konfigurationsprofil.



Dieses wird einfach auf die mobilen Geräte aufgespielt. Mit wenigen Maus-klicks können auf diese Weise hunderte mobiler Geräte konfiguriert werden. Der Roll-Out erfolgt vollständig automatisiert. Die Enterprise Erweiterung ermöglicht eine OTA-Verteilung mit automatischen Workflows. Der Benutzer packt das neue Gerät aus und authentisiert sich am Web Portal – das Gerät wird vollständig installiert und konfiguriert. Zudem unterstützt CORISECIO auch vorhandene Lösungen zur Softwareverteilung, wie ActiveSync, Afaia, OneBridge, etc. sowie die (semi-) automatische Verteilung über via E-Mail oder FTP- Filetransfer.

CHALLENGES

- Effiziente Administration mobiler Benutzer
- Automatischen (OTA-) Roll-Out
- Vorkonfigurierte Geräte
- Durchsetzung der Security Policy
- Einfache „Ein-Hand“- Bedienung
- Geräte-Login, S/Mime E-Mail, VPN, etc.
- Hardresetfähigkeit

WIE MINIMIEREN SIE DIE FEHLBEDIENUNGEN DER GERÄTE?

Eine weitere Herausforderung besteht im Schutz vorkonfigurierter Einstellungen. Im Gegensatz zu Desktop Betriebssystemen bietet Windows Mobile keine Benutzerrechtestruktur. Dies bedeutet, jeder hat Zugriff auf alle Einstellungen, Funktionen und Applikationen. Die Folge sind erhöhte Supportkosten durch die (un)wissentliche Veränderung durch den Benutzer in der Konfiguration der Geräte.

CORISECIO – Mobile Firewall erlaubt dem Administrator die getätigte Konfiguration wirkungsvoll zu schützen, indem definierte Masken und Funktionen gesperrt werden! CORISECIO realisiert damit die Umsetzung eines Rechtekonzepts auf der mobilen Plattform. Der Administrator definiert entsprechende Sperren und legt damit bspw. fest, ob VPN-Einstellungen ganz ausgeblendet oder schreibgeschützt sein sollen. Auch die Nutzung sicherer Verbindungen kann durch diese Technik einfach vorgeschrieben werden. Mobile Firewall unterstützt dabei auch proprietäre Software und Eigenentwicklungen durch einen generischen Ansatz. Ohne Softwareänderungen oder Programmieraufwand kann nahezu jede Windows Mobile Software vor Manipulation und Zugriff geschützt werden. Dem Benutzer werden lediglich definierte manuelle Änderungen erlaubt und Supportanfragen dadurch nachhaltig minimiert.

WIE VEREINFACHEN SIE DIE BEDIENUNG FÜR DIE BENUTZER?

Benutzer sind von der Komplexität moderner Geräte oftmals überfordert. Überladene Menüs für Einstellungen und Programme verhindern oftmals den effizienten Einsatz. Zudem ist die Konfiguration der Geräte, insbesondere der Internetzugang sowie Einstellungen für geschützte Netzwerkverbindungen nicht trivial. Anstatt das neue Gerät direkt nutzen zu können, bedeutet dies zusätzlichen Zeitaufwand bei Einrichtung der Geräte - für Nutzer sowie Helpdesk-Mitarbeiter.

Mit der CORISECIO – Mobile Suite erhalten Endanwender ein benutzbares, vorkonfiguriertes Gerät, das ihnen den sofortigen Einsatz im Unternehmen ermöglicht! Durch die Verwendung von vorkonfigurierten und geschützten Profilen wird der Benutzer erst gar nicht mit der Konfiguration konfrontiert - das mobile Gerät ist sofort einsatzbereit. Aufwendige Einstellungen für den mobilen Zugang zum Firmennetz sind verlässlich geschützt und jederzeit funktionsfähig. Versehentliche Fehlkonfigurationen können wirkungsvoll ausgeschlossen werden.

CORISECIO – Easy Phone erhöht die Usability für den Endanwender durch einfache Oberflächen und große Symbole. Nicht benötigte Menüs, Verknüpfungen und Applikationen werden einfach ausgeblendet. Mit der zentralen Definition von Hintergrundbildern und Menüfarben lässt sich die Corporate Identity auch





auf Smartphones und PDA's umsetzen. Die Bedienung wird nachhaltig vereinfacht und Helpdesk-Kosten gesenkt.

WIE VERHINDERN SIE DIE UNERWÜNSCHTE UND RISIKOREICHE NUTZUNG VON WLAN, BLUETOOTH UND IRDA?

Nahezu alle mobilen Geräte folgen einem Always-On Konzept. Dies betrifft nicht nur den schnellen Zugriff auf Informationen und Funktionalitäten, sondern auch viele Schnittstellen. Funk- und Drahtlostechnologie bergen zahlreiche Sicherheitsrisiken und bieten Raum für potentielle Angriffsszenarien. Moderne mobile Geräte sind mit WLAN, Bluetooth und IrDA ausgestattet, deren unkontrollierte Nutzung Risiken wie Datenspionage, Manipulation oder Viren- und Malwareprobleme birgt.

CORISECIO – Mobile Firewall sperrt WLAN, Bluetooth und IrDA oder erlaubt nur die gezielte Nutzung der Schnittstellen! Mit der CORISECIO Technologie können potentielle Sicherheitsrisiken durch WLAN, Infrarot oder Bluetooth gemäß unternehmensweiter Security Policy einfach ausgeschlossen werden. Die Mobile Firewall ist in der Lage, die Verwendung zu unterbinden, indem diese Features bis auf Treiberebene gesperrt werden. Auch können Administratoren über vorkonfigurierte Profile die gezielte Nutzung erlauben, indem bspw. nur definierte WLAN Hotspots erlaubt werden oder eine Bluetooth Verbindung nur zu bestimmten Geräten, wie Headsets, möglich ist.

WIE VERHINDERN SIE DEN EINSATZ EINGEBAUTER DIGITALKAMERAS AUF DEM FIRMENGELÄNDE?

Kritisch beurteilen viele Unternehmen auch die Verwendung von Kamerafunktionen. So sind Kameras auf oft dem Firmengelände z.B. in der Automobilindustrie, verboten. Um dies umzusetzen wurden bisher Kameras auf den Handys irreversibel unbrauchbar gemacht.

Die CORISECIO – Mobile Firewall sperrt zuverlässig eingebaute Digitalkameras! Die Mobile Firewall bietet die Möglichkeit, unerwünschte Funktionalität einfach zu sperren und Unternehmen können somit alle gängigen Gerätetypen einzusetzen - ohne gültige Sicherheitsregelungen zu umgehen.

CORISECIO bietet Ihrem Unternehmen einen effizienten, einfachen und schnellen Weg unternehmensweit mobilen Geräten einzusetzen. Durch die Möglichkeit, vorkonfigurierte Einstellungen und unerwünschte Funktionen zu sperren wird die Sicherheit deutlich erhöht und Kosten für Administration und Support nachhaltig gesenkt.

SOLUTION

- Remote-Konfiguration mobiler Geräte über Profile
- Benutzerrechte & Schnittstellen- und Synchronisationskontrolle
- OTA - Roll-Out bspw. via Unternehmensportal
- Durchsetzung von Synchronisationsrechten
- Benutzerfreundlichkeit
- Company-eigenen Look & Feel.
- Erstellung, Verteilung und Nutzung von Zertifikaten
- Single-Sign On, Dateiverschlüsselung
- E-Mail Verschlüsselung & VPN-Verbindungen.

LEARN MORE

- CORISECIO – Mobile Suite
- CORISECIO – Mobile PKI

