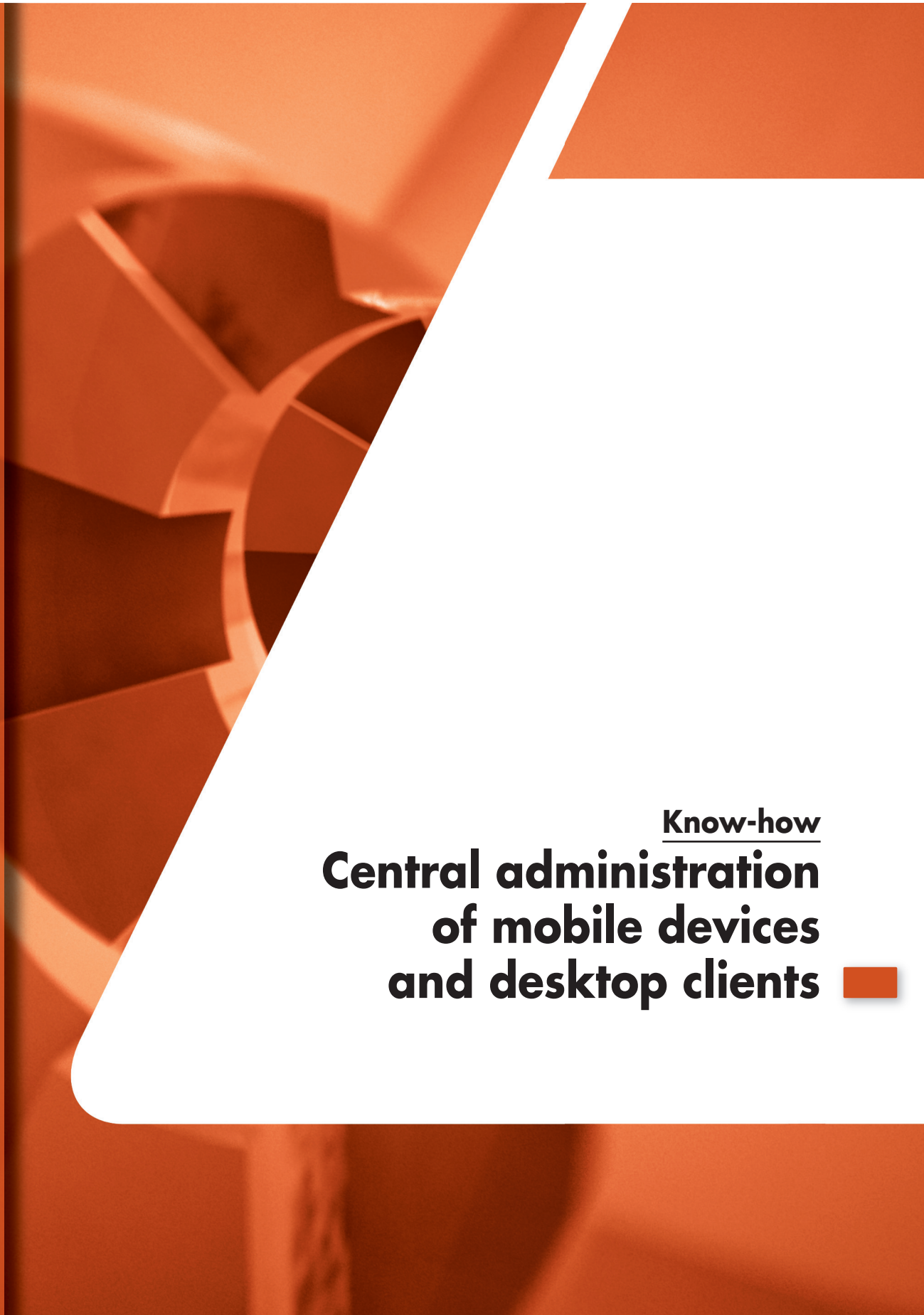
IT-ADMINISTRATOR.COM

08/2013

iadministrator

The magazine for professional system and network administration

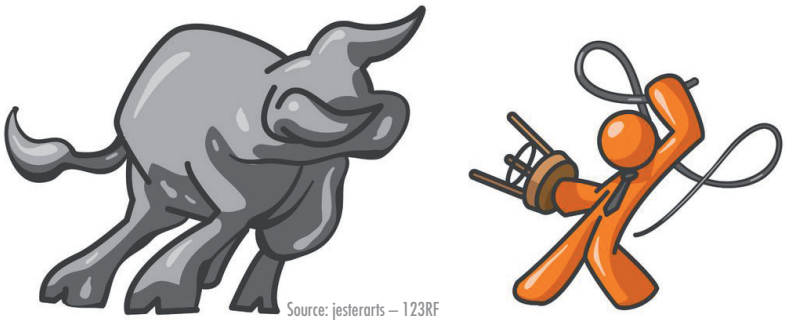
Special Edition for baramundi software AG



Know-how

Central administration of mobile devices and desktop clients

Central administration of mobile devices and desktop clients



Source: jesterarts – 123RF

Directing the Device Circus

by Armin Leinfelder

Administrators face numerous hurdles when it comes to administering mobile terminal devices as securely and reliably as PCs or laptops. For one thing, the number of device types and operating system versions is large. And the risk that one of these small devices is lost or stolen – complete with the user's confidential data – is significantly higher than for laptop computers. This article illustrates how combined client lifecycle and mobile device management suites can help administrators keep their overview of all devices, big and small.

In classic client management, the administrator is the absolute ruler over all the terminal devices. By setting sound IT policies and especially by keeping administrative rights out of the hands of end users, administrators can easily prevent more substantial intervention, such as the installation of unauthorized software. But smart phones and tablet computers are different, because the owners of these devices are generally also their administrators, and decide themselves which apps to install or deinstall. Thus, companies can set policies at the organizational level on what their employees can and can't install, but preventive measures at the technical level are only possible in specific constellations.

Given trends such as Bring Your Own Device (BYOD), in which employees use their private devices for work purposes, managing mobile devices is and will continue to be different than management of the company's own Windows client: BYOD users who have been their own administrators generally don't want to give up that privilege, even when they use their private devices for work. Yet even in companies without BYOD provisions, there are good reasons for allowing users to have administrative rights. For example, consumer devices that run on iOS or Android often have only one user, who is also the device's administrator. And sales employees in the field often need more rights than personnel who work in an office and can reach an administrator during regular office hours.

Client and mobile device management

IT departments that have traditionally spent their time managing Windows clients and servers now also need to manage mobile devices and their platforms – iOS, Android or Windows Phone 8, for example. And it isn't just the new platforms that mean changes for IT administrators. Even established desktop systems such as Windows are developing in the direction of mobility, a trend currently visible in the modern Windows 8 UI apps. So it's no surprise that according to market studies, mobile device management is currently one of the hottest IT topics.

That being the case, IT administrators naturally want to know which tools are best for dealing with mobile devices. Most administrators use classic client lifecycle management (CLM) systems to manage computers. From this starting point, we can differentiate between three classes of mobile device management (MDM) tools: dedicated MDM products, combined CLM-MDM tools and integrated CLM-MDM solutions.

Dedicated MDM products are relatively new solutions that focus exclusively on the management of mobile devices and offer no options for desktop operating systems. These tools generally offer a variety of features and can be used with all the popular mobile platforms. Their functional scope is oriented to the options that platform manufacturers provide for managing their devices. Yet their exclusive focus on mobile devices means that administrators need a separate solution for managing classic clients. In other words, they need to maintain and use two tools to cover all the employees' devices. There are certainly tools for each arena that are easy to use and, individually, offer optimal results, but the constant need to switch between them nonetheless increases complexity: different user concepts and interfaces and redundant data on the same employees in both systems mean more work for IT staff, and offer no global overview. Maintaining relationships with several software suppliers also increases the workload.

Two worlds grow together

Combined CLM-MDM products offer a first approach to solving this problem. In these products, a classic CLM supplier ensures MDM functionality by adding MDM components from independent manufacturers and creating a new package. However, the customer should pay close attention to the depth of the integration: is it merely commercial – i.e. is the CLM provider simply selling the MDM components alongside its own –

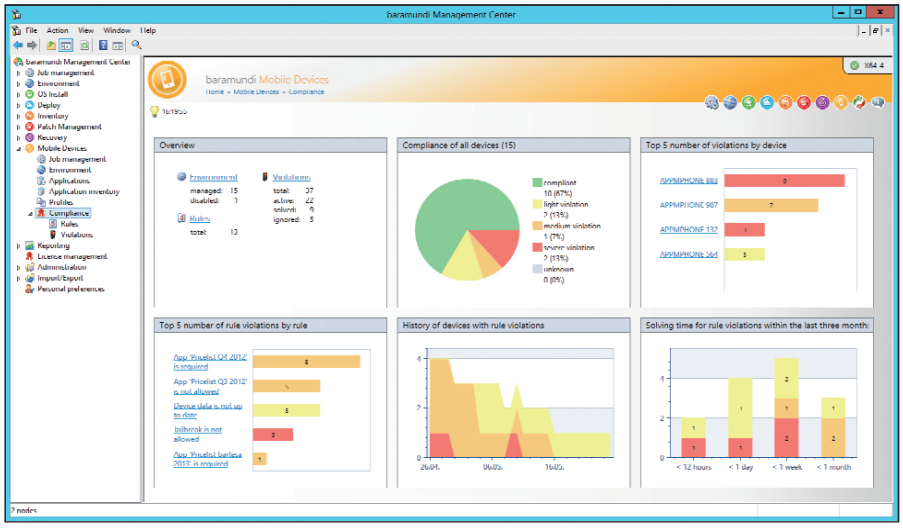


Illustration 1: Combined management suites like those from baramundi offer administrators a sound overview

or has the manufacturer invested in technical integration? If the latter (which is definitely the more attractive solution for users), the homogeneity of the combination in actual use should be evaluated: Is there a common UI or are there still two? Is the operating concept homogeneous or are there differences? Is the master data shared or does certain data have to be compiled twice?

Integrated CLM-MDM products offer a more elegant option for the joint management of classic clients and mobile devices. "Integrated" here refers to all those solutions in which a – generally more experienced – CLM manufacturer has expanded the functional scope of its product from classic clients and servers to mobile devices. The advantages of such a suite are clear: both parts of the product are from just one manufacturer, and administration is possible using just one product. Operating concepts and UIs can be provided in a significantly more homogeneous fashion, there is no need to maintain a second solution, and uniform security standards are easier to uphold in one holistic system. Furthermore, trends can be considered from the vantage point of both desktop and mobile platforms, enabling coherent and consistent administration in the future, too.

Working across platforms

Users tend to work in parallel or sequentially when they are using multiple devices. For example, a user may begin to research a topic or draft an e-mail message on a mobile device while on the road, and then continue the task on a desktop PC at home or after arriving at the office. When different devices are used in this way for one and the same task, then all of them should ideally have the same programs, files and rights. Security guidelines for this process also need to be considered holistically. For IT managers, this is likely to mean performing the same administrative duties for all the platforms involved, and ensuring consistency.

What are the typical administrative tasks and functions that can be currently automated with an MDM product? Large platforms such as iOS, Android and Windows Phone offer a variety of options at the detail level. When introducing an MDM solution, these options should be carefully scrutinized using the solution's feature matrix. Moreover, some device manufacturers – one example is Samsung, with its SAFE and KNOX solutions – are extending the possibilities of Android through additional functionalities and APIs that are accessible to MDM tools. I will therefore present only the most common functions.

Requirements of management suites

Before a management suite can be used to manage a mobile device, the device itself must be integrated in the company's network. That is, the device must be connected to the system – a process called enrollment. On the server side, a reference to the mobile device is created and the device is introduced to its management server. This may require an agent app on the device. Alternatively, the mobile platform's on-board facilities can be used. The necessary files can be exchanged in a variety of ways – via e-mail to smart phone users or by scanning a QR code with the mobile device's camera.

Following enrollment, functions are available for inventorying, configuring settings, distributing apps or even deleting files remotely from a lost device – a function known as remote wipe. Key functions are:

- Locking and unlocking
- Complete deletion of devices and memory cards
- Activation of device encryption
- Identification of firmware manipulation (jailbreaks, rooting)
- Compliance dashboards, rules and automated responses
- Hardware information
- Installed apps, profiles and certificates
- SIM card information
- Roaming status
- Security settings
- Software distribution and configuration
- Installation and deinstallation of apps
- Configuration of WLAN and VPN
- Setup of Exchange accounts
- Camera deactivation

Suitable solutions enable values to be parameterized so that the settings listed above can be applied simultaneously to multiple end terminals. Using e-mail configuration as an example, this means that the server name is the same for all users, but the e-mail address is entered individually for each single person. At the time of definition, the administrator parameterizes the value using a corresponding variable in the management system.

Self-service is another trend that an MDM solution can support: administrators can provide skilled users with self-service options for certain functions. This could be, for example, a selection of apps offered to end users via a kiosk app. In contrast to the enormous range of apps in app stores, the company can suggest useful apps or even restrict users to installing only the apps available from the kiosk. Other fea-

tures, such as compliance checks, can also be made available to end users via app. Both these approaches offer users quick solutions and relieve administrators of the time and work of providing routine information and support.

Don't forget data protection and compliance

Users should pay particularly close attention to data protection, because not all the solutions on the market meet German and European guidelines. For example, can the administrator monitor the user's movements via geolocation without additional safeguards? Is there a difference made between private (BYOD) and company devices when deleting data and software? Does application usage tracking allow conclusions to be drawn about the way employees work? These and other questions must be clarified at the organizational level and the results must be codified in the form of company agreements or IT guidelines. In the process, the company's data protection officer, works council and, if necessary, its legal advisors should be consulted in addition to its IT experts. Once the data protection rules have been set down, the management solutions under consideration should be evaluated as to how well they follow those rules and can ensure that others comply with them.

Tools with appropriate overviews offer an advantage in continuously ensuring the compliance – that is, adherence to company IT guidelines – of end terminals. The idea behind this is that the administrator determines the technical rules in line with the company's guidelines and continually monitors compliance with them. In the event of violations, the administrator can then respond in a targeted fashion or even set up automatic functions to ensure that a preconfigured activity is carried out immediately when a compliance violation is detected. This type of compliance monitoring uses basic functionalities of the MDM solution and offers dashboards for visualization purposes as well as configurable rules.

Illustration 2: During enrollment, mobile devices are connected to the management suite, which then monitors them

Aggregated diagrams offer the IT administrator a rapid overview of all devices and make it possible to drill down to the affected device. The administrator can then approach the affected employee and, for example, ask him or her to deinstall unauthorized apps, or, if necessary, directly withdraw profiles that permit access to the company network. It is even possible to completely delete a device via remote wipe, although intervention this drastic is usually restricted to events such as the loss or theft of a device.

Summary

The use of mobile devices makes employees' lives easier and more efficient. Over the next few years, their platforms will continue to develop at an astonishing speed, placing new demands on management tools. That means that the lives of IT administrators in the "device circus" will initially become more difficult as they try to "tame" all the devices employees want to use. The need for mobile device management solutions is thus clear, and fortunately the market already offers a broad array of solution approaches.

If we consider the different types of device together rather than in isolation, it seems only logical to search for administrative solutions that enable the management of both client and mobile devices. Mobile devices will not replace traditional platforms completely in work settings any time soon, but this means that businesses need solutions that can combine both worlds. *(dr)*

Armin Leinfelder is a product manager for baramundi software AG.