baramundi

White Paper

Fast and Secure Using Automation

One Management Software For All End Devices

Empower your IT

CONTENTS

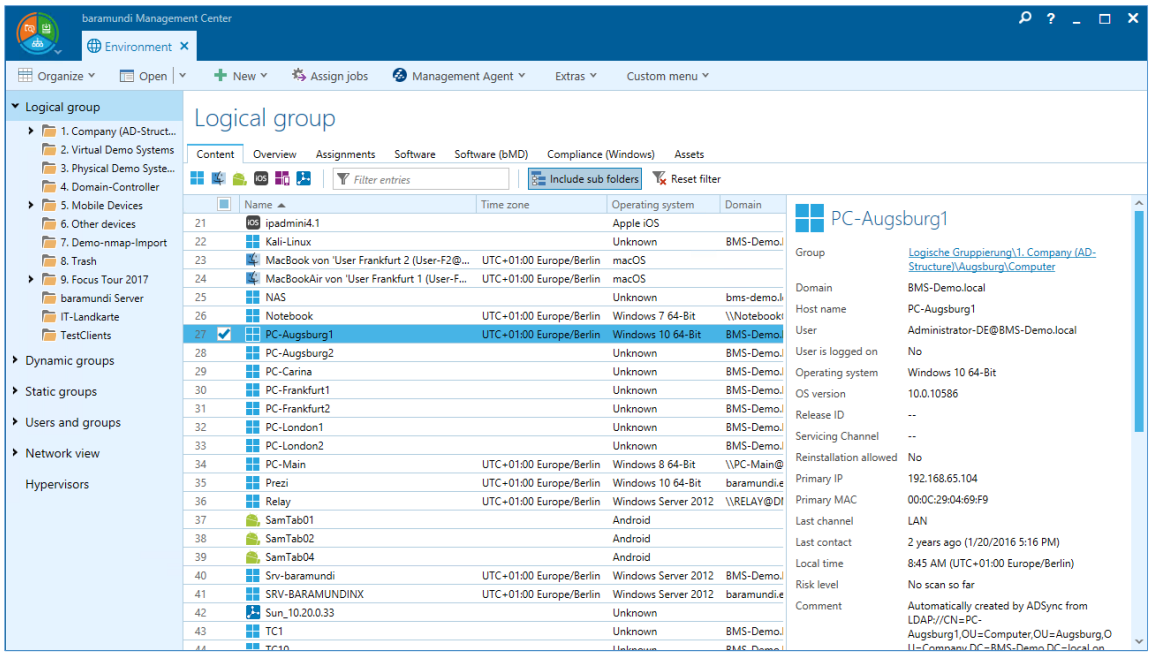
Board: Graduate Engineer (FH) Uwe Beikirch | Dr. Lars Lippert
Chairman of supervisory board: Dr. Dirk Haft
Registered office and register court: Augsburg, HRB No. 2064 | VAT ID No. DE 210294111

1 IT departments face ever more demanding requirements

IT development is soaring at an ever-growing pace. While decades have elapsed between Zuses Z1 and the first PCs, the industry is now evolving – almost on a monthly basis. But as the performance and variety of devices increases, so do the administrative requirements.

For example, many users no longer work solely on PCs and notebooks and also use smartphones and tablets in parallel or sequentially. E-mails are answered while on the move, searches may be started on the desktop and continued via smartphone and presentations are controlled via tablet. While mobile devices use operating systems and applications that differ from traditional endpoints, they also require access to company data and e-mails and must therefore be secured just as reliably.

At the same time, the boundaries between mobile devices and the PC world are also becoming increasingly blurred: For example, spawning tablets with PC operating systems, or mobile apps running on Windows endpoints. This is why it makes sense to bundle the administration of all end devices with which users work in-house, into a single solution. This paves the way to enforce uniform standards and gain a comprehensive overview of the network status and all end devices. It also represents a holistic solution, which can easily accommodate future new devices emerging.



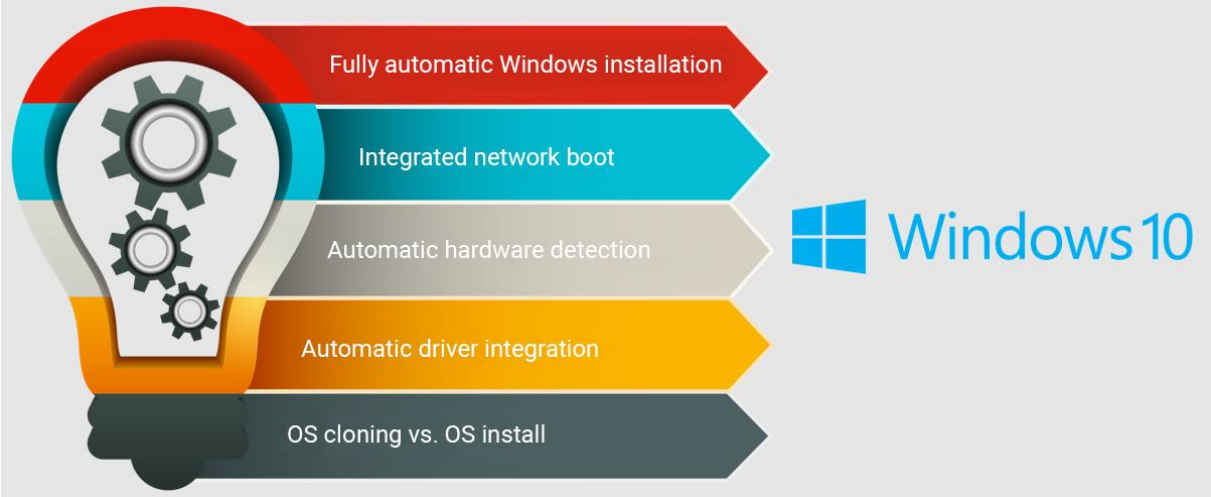
Uniform overview of all device types/platforms

A unified endpoint management solution also automates routine tasks, streamlining and accelerating them and making them easier to perform. As well as providing the necessary overview, this also boosts the security of the company network. This document provides an overview of administration tasks that should be automated regardless of circumstances.

2 How to automate routine tasks

2.1 Distributing operating systems and applications

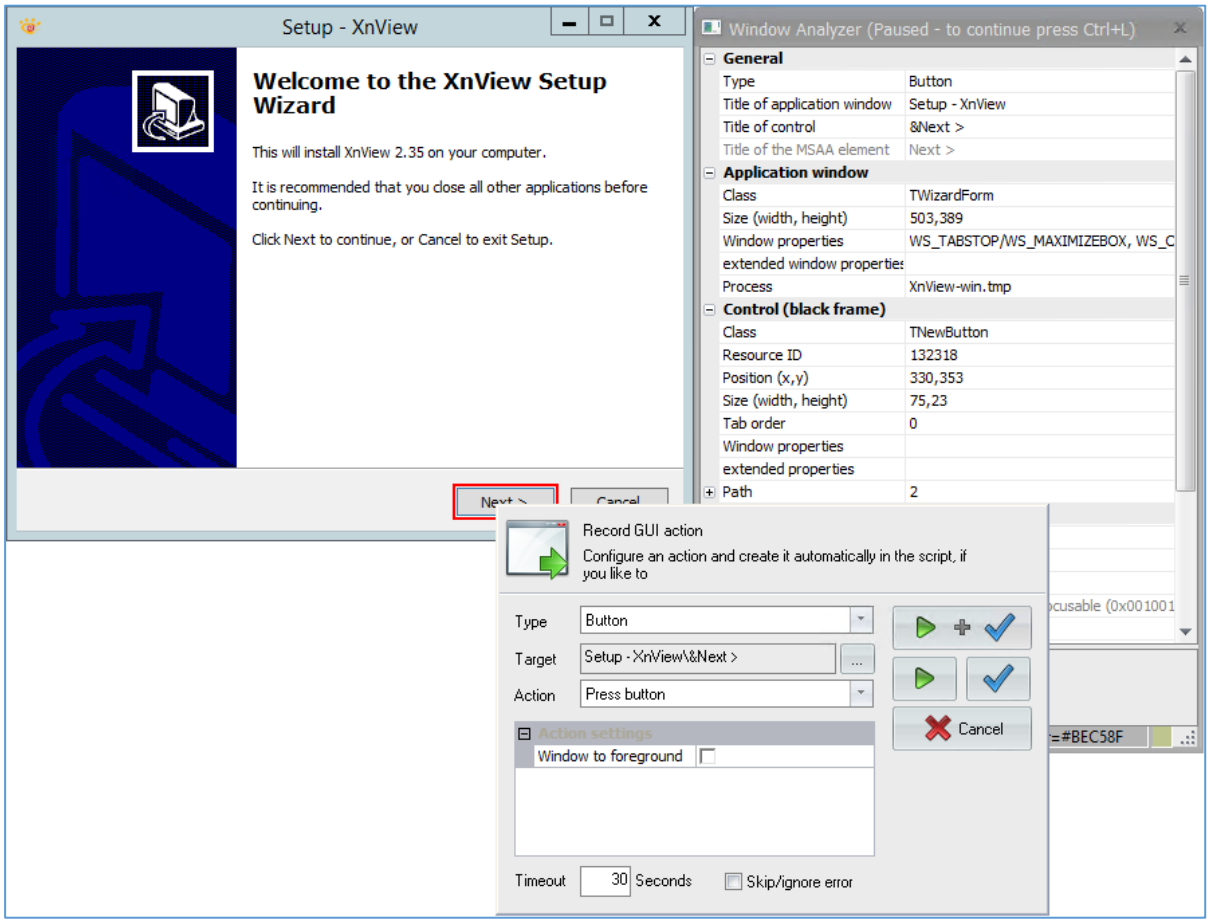
A new employee is appointed. This means the IT department is tasked with the following: A PC workstation or possibly a laptop must be provided. Reinstalling a computer with an operating system and all required applications – including all necessary restarts, selecting the appropriate drivers, etc. – can take several hours. A management solution, on the other hand, reduces the effort involved to a mere series of mouse clicks.



Instead of running a setup manually or by script, the new device is automatically detected in the network. At a single swoop, the hard disk is readied and the required drivers assigned. Since intelligent solutions use the native installation method from the OS manufacturer, they also benefit from the full warranty. Computers can even be re-installed overnight via the Wake-on-LAN service.

Software can also be distributed automatically. This usually involves defining a standard configuration for a usage profile. As required, the IT administrator can roll out this software package onto the target system by clicking a mouse – even on multiple devices in parallel, including the necessary restarts and ensuring optimal installation quality using original setup methods. The automation solution also delivers feedback on the installation status and any errors that may have occurred at any time. Once defined, tasks can be reused at any time if a new colleague comes on board a few months later or a device has to be replaced. At the same time, automating the installation helps ensure standardized computer configurations and minimize the number of errors.

There is often a need to install software without any standardized manufacturer installation packages. Here, tools integrated in common management software can be harnessed to create the necessary scripts for surface automation easily and intuitively. Even problematic setups can be installed centrally and automatically using the setup procedure provided by the software manufacturer, leaving the manufacturer's warranty intact.



Wizard-based surface automation with the baramundi Automation Studio

Management software not only distributes applications, but can also remove them from the endpoint. When selecting a solution, it is best to also ensure programs not installed using the management software also remain usable. Accordingly, for example, applications that users have installed on their computer without authorization can be efficiently removed.

Installing applications and operating systems in this centralized and automated manner can also benefit IT administrators and end users: If performance problems or stubborn errors strike, re-installing the workstation overnight is a breeze – instead of having to isolate the cause. This also means a fully functional device is made available to the administrator as quickly as possible with minimal downtime. Such automation can also be applied when

migrating numerous workstations, for example to a new operating system such as Windows 10 or a new Office version.

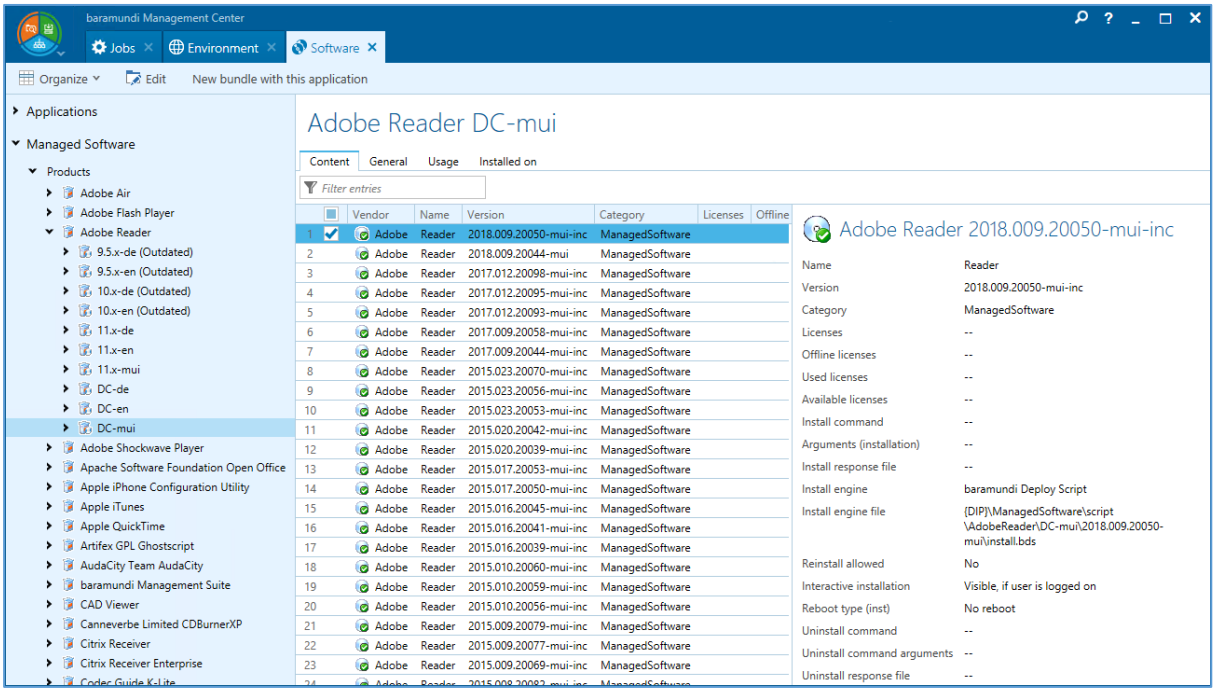
2.2 Detecting vulnerabilities and automating updates

After installing and completing, is that it? Unfortunately not. Updates for applications and operating systems emerge on an ongoing basis and have to be installed on all relevant machines as soon as possible. This is not only a question of new features but about security above all: New versions and patches safeguard against security gaps that could potentially infiltrate the corporate network and cause major damage. The consequences range from image impairment and the disclosure of internal company information to legal consequences following any theft of customer data and breach of data protection laws.

While firewalls and virus scanners are key components of an effective security concept, they are largely ineffective against attacks if vulnerabilities have not been patched. If an employee's computer is forced to establish a connection with the attacker's control server by exploiting a vulnerability in a so-called reverse connection attack, the firewall usually fails to step in, because the contact is established in encrypted form on standard channels from within the company. This makes it all the more important to monitor the vulnerabilities of each individual end device and close them off as quickly as possible, depending on the degree of susceptibility.

However, about 100 new vulnerabilities are identified and documented each week, as statistics from the National Vulnerability Database of US-CERT show. Here, the management software can support IT administrators by conducting automated and regular scans of all endpoints and servers. Following this, the administrator receives clear lists of the most dangerous security gaps within the corporate network or the most vulnerable endpoints. Any loopholes can then be prioritized and rectified.

If the solution includes a patch management system alongside the vulnerability scanner, any gaps detected can also be closed off centrally and automatically. As well as Microsoft patches, the management solution should, as a minimum, also distribute updates for frequently used applications such as Adobe Reader, Java or Firefox centrally and automatically, given their widespread distribution and corresponding popularity among attackers. Current software packages for numerous applications are also available as Managed Software from the UEM manufacturer. In line with in-house guidelines, these can also be released for productive use or testing.

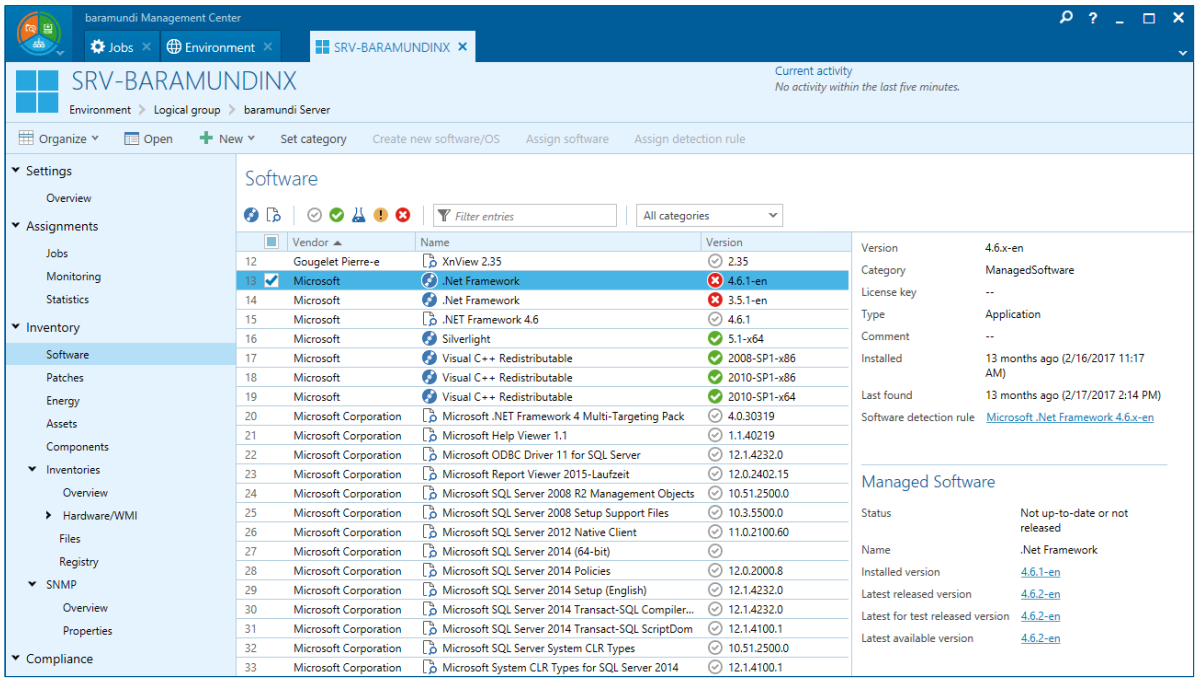


Ready-to-distribute software packages at a range of release levels

Effective vulnerability management, however, requires more than just knowing gaps and initiating the installation of a patch. Also crucial is knowing whether the update needed to ensure security has actually arrived on all endpoints. Installations may fail or be blocked by users themselves, or a laptop in the field might be unavailable. Accordingly, any solution used must include feedback on the installation status and any errors that may have occurred to ensure all gaps really can be closed.

2.3 Inventorying hardware and software, managing licenses

A comprehensive overview is not only important to identify vulnerabilities and guarantee security. IT managers must also be able to report on the use of hardware and software or, in the event of a license audit by a software manufacturer, be able to prove the correct licensing. From a cost perspective, it is also important to detect unused software that ‘slumbers’ on endpoints and ties up expensive licenses.



Listing of installed software

Management software can be used to generate an automated inventory to clarify quickly and clearly which hardware and software is being used in the company network. This means that an up-to-date database is always available for assessment by management. With volume and upgrading of licenses in mind, monitoring it all is a real challenge. In response, a license management solution, which can be connected to the management solution via an interface, provides a clear overview and compliance.

There is also scope to record the actual use of a program to eliminate any needless costs. The start of an application on individual devices is logged for this purpose. This shows the computers on which a program remains unused within a given period of time – and which licenses can be saved as a result. Important: The solution used must comply with European data protection regulations and must not allow monitoring of individual employee behavior.

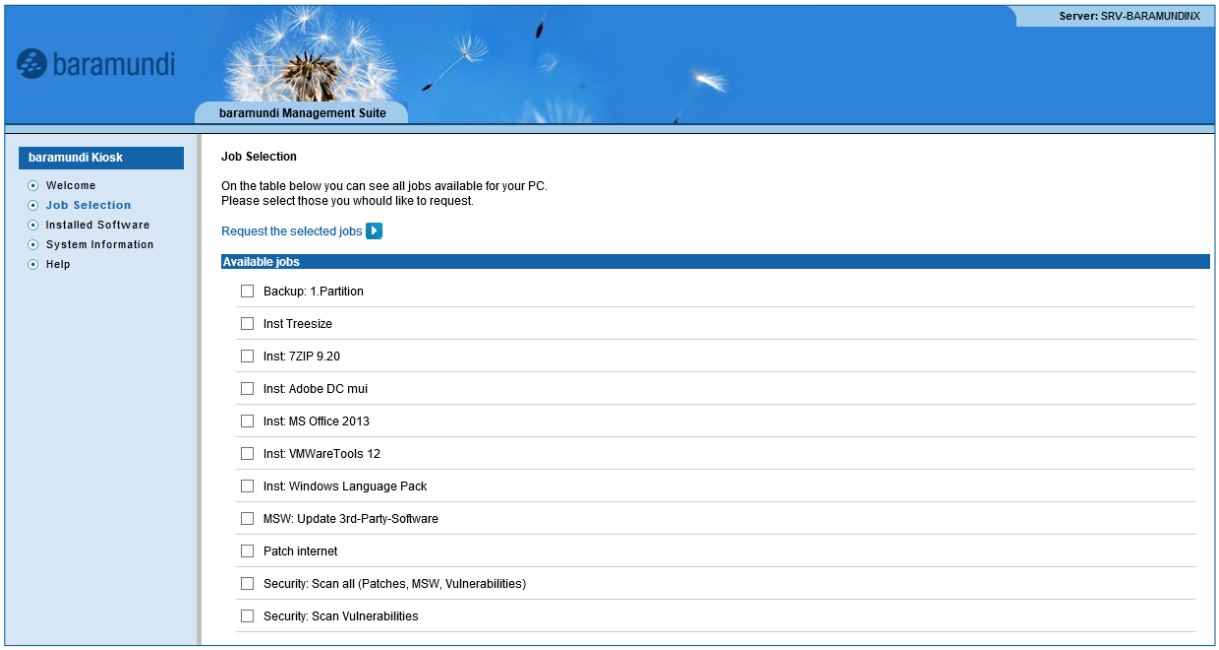
IT support also benefits from the automated inventory: Helpdesk solutions can be connected to the management software via interfaces. Accordingly, support staff can quickly record the hardware and software equipment of the workstation in question for queries. Having the right data from the relevant terminal device is crucial to process users' requests swiftly and competently.

2.4 Automating intelligently: Timing control and self-service

Many companies have maintenance windows which specify that administrative tasks on certain computers can only be performed at specified times. Therefore, efficient management software paves the way for time-controlled tasks. It also makes it possible, for example, to run a patch installation on a particular device within a certain period.

In contrast, event-driven tasks relieve the burden on the IT administrator of responding to events. For example: If the XY game is discovered on an endpoint during inventory, it should be removed automatically. Instead of having to intervene each time the game is found, the administrator only receives a report about an executed uninstall.

IT administrators and users, however, will welcome the convenience of providing installation procedures prepared beforehand in a self-service kiosk. This enables faster and simpler handling of standard queries, such as Firefox installation – right when the user wants it and needs it to work smoothly. The support scope is also reduced at the same time, since this task runs fully automatically and on demand. The administrator should also be able to monitor such self-service installations on an ongoing basis.



Self-service kiosk for users

High-performance management software means scope to include users in installation processes without having to surrender control to administrators. For example, the user may be given the right to move a patch installation requiring a reboot within a given time window. This helps avoid disrupting the workflow of colleagues and means, for example, the installation

can be scheduled for a coffee break. It also serves to ensure the distribution of a critical patch cannot be excessively postponed.

2.5 Integration into existing infrastructure

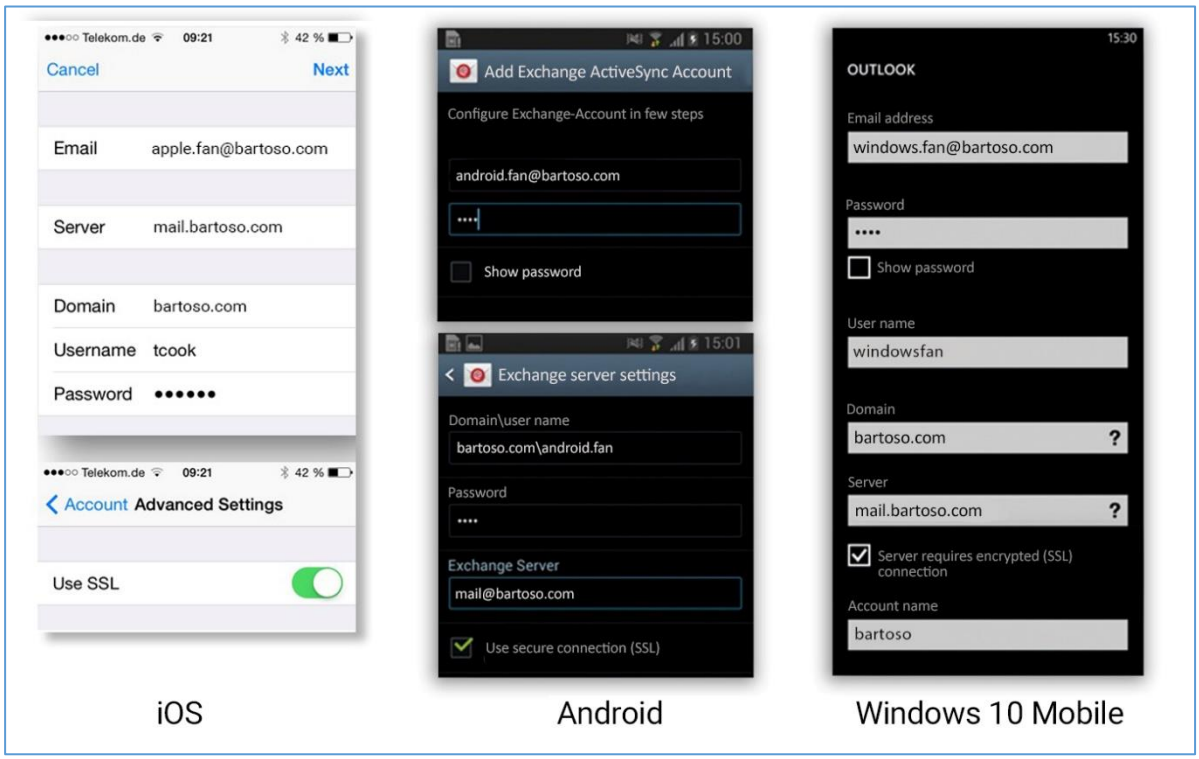
It is also best to avoid seeing the management software as a new island within the existing infrastructure. Seamless integration is contingent on the management software, including modern interfaces. This is the only way that further organizational processes can also be automated. For example, after the new PC has been registered in the ERP system, an endpoint including all key data – such as inventory number and cost center, etc. – can be automatically created in the management solution and immediately supplied with software and configurations.

Integrating into the existing ticket system is just as easy. This all means that support staff receive the latest information on the software and hardware used at the endpoint at all times and new installations can be initiated as required.

3 Manage mobile devices

The use of mobile devices has become standard in many companies, and many employees want to access enterprise data from their own mobile devices. This can bring some benefits for companies, but IT Managers should also be aware of the risks. Effective protection and keeping an inventory are basic requirements to safely integrate laptops, tablets, and smartphones into the professional world. Ideally, mobile device management will be integrated into the UEM solution, as many such tasks can also be automated.

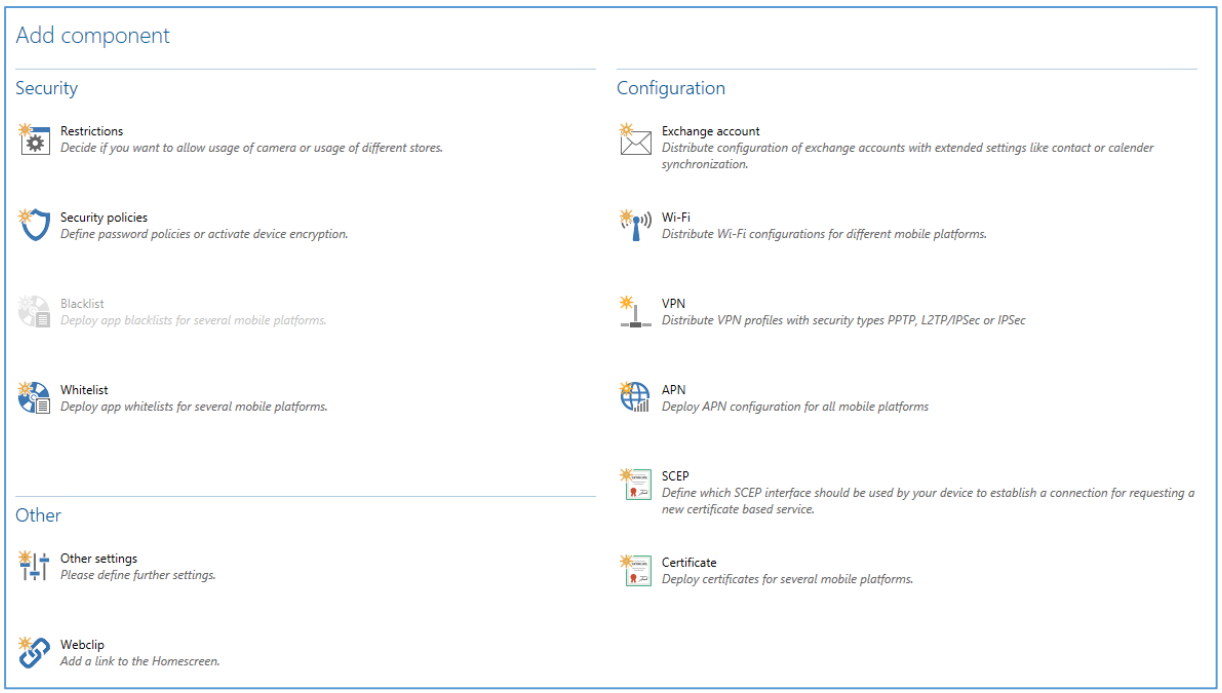
Compare the three most common mobile platforms – iOS, Android, and Windows 10 Mobile – and you soon see that the same parameters – name, e-mail address, server, domain, and encryption for setting up exchange accounts – have to be entered in different places. In practical terms, this entails enormous effort and needs the administrator to know all the input masks. This workflow can be simplified considerably by using cross-platform profile modules and centralized device management.



Exchange configuration on different mobile platforms

One-time inclusion of the smartphone or tablet in the management solution is required ('enrollment'), for example by using the Apple Device Enrollment Program (DEP) or scanning a QR code. The next step sees scope to implement management tasks – the example given

shows the exchange configuration – centrally via the solution. First, the appropriate settings are configured on a uniform, cross-platform interface and then transferred to the managed devices.



Cross-platform profile modules for configuring mobile devices

The advantages are clear: The administrator no longer needs to know where and on which mobile device each setting is made, since the familiar interface of their central management console is always the starting point. This simplifies, accelerates and further improves the accuracy of the process. Bottom line: This also makes everything safer.

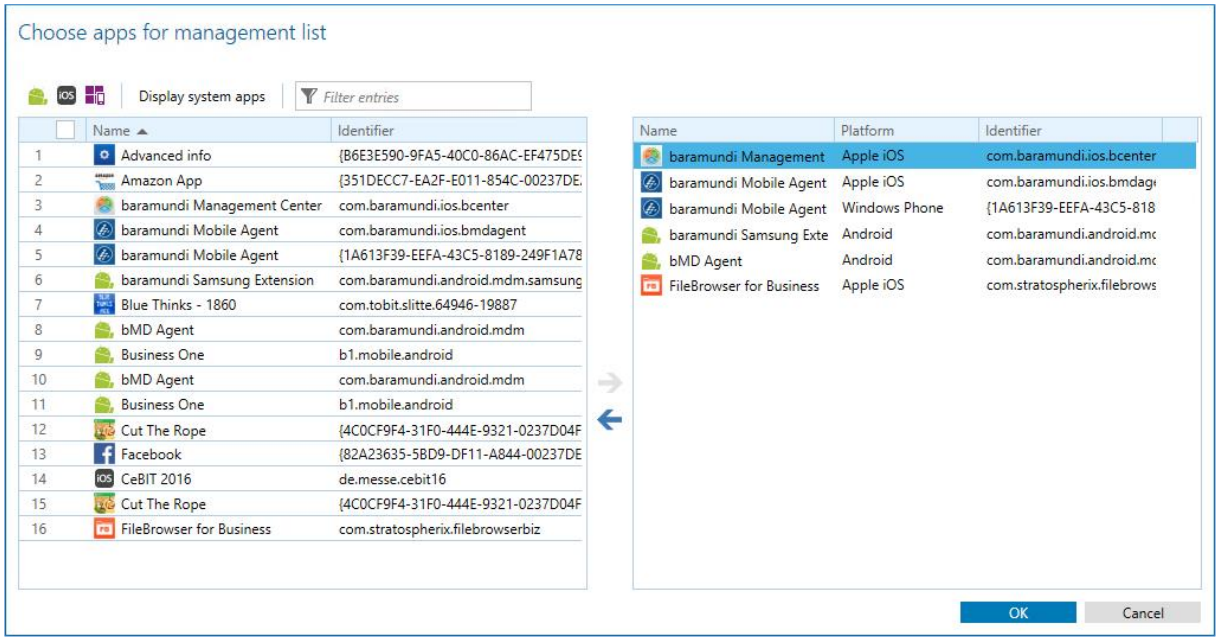
One more plus: Tasks can also be performed “over-the-air” via management software, eliminating the need for an administrator to take control of the device. For example, if a user puts a new iOS device into operation at a remote location, it is automatically registered in the management system via Apple DEP. The administrator then has scope to set up the further configuration. The processes and tasks used can also be prepared and reused time and time again – even for a larger number of devices simultaneously.

Mobile devices are also more likely to go missing than a PC, hence the need for sufficient precautions. Possible options include automatic locking when the screen is switched off, scope to delete the assigned profile remotely and, last but not least, assigning strong passwords.

There is also a need to ensure the administrator retains an overview of the devices at all times and can monitor any instance of a user compromising the operating system. With this in mind, any management solution should include the ability to define compliance rules, which are then checked automatically and on an ongoing basis. If any violations occur, the administrator is informed and has the possibility to take countermeasures, such as emailing the user until the device is deleted remotely. Just as important as preventing any tampering with the firmware is updating the firmware promptly as soon as the manufacturer brings out a new version. As a rule, this not only allows new functions to be rolled out, but also helps eliminate vulnerabilities. Such upgrades can already be remotely controlled on modern platforms.

To prevent dangerous apps from running or to provide a selection of apps that are trusted by the company, the solution should support blacklisting or whitelisting. The administrator can then prevent unwanted apps from being installed or executed on compatible mobile devices. Conversely, a whitelisting approach allows explicitly permissible apps to be defined, and by definition prevents all unlisted apps from being installed or executed.

The administrator has the option of adopting a whitelisting or blacklisting approach for each separate end device. After deciding on the list type, the corresponding apps are added to the list and then transferred to the mobile device as a profile.



App selection for black- and whitelisting

As an active member of the AppConfig Community, an initiative of leading EMM manufacturers, baramundi is committed to simplifying the distribution and configuration of apps using native resources from operating system manufacturers. The suite offers wide-ranging functionalities for Mobile Device Management (MDM) and Mobile Application

Management (MAM) and is supplemented by suitable third-party apps from document management systems (DMS)/Personal Information Management (PIM) environment with Mobile Content Management (MCM) functionalities. These areas are connected via configuration standards at the iOS and AppConfig level, meaning the management solution also provides for the comfortable distribution and configuration of the MCM functions, with content functions such as data synchronization and data processing reserved for third-party apps.

Integrating Enterprise Mobility Management into a software suite for endpoint management not only saves time and effort during the setup, maintenance and operation. It also makes it possible to manage mobile devices and PCs in shared groups and organizational units and enforce uniform standards. This is arguably also a more forward-looking approach, since new device classes can be integrated more easily into a uniform solution.

4 Data security and data protection

IT administration also means responsibility for data protection and data security, for which an automated backup is crucial. This means data and user settings can be easily restored when an incident occurs – including Word Dictionary and desktop icons. These processes can also be reliably automated using management software.

Compliance with applicable data protection legislation is just as important. Since individual user behavior could be inferred from the high volume of user data potentially captured by a management system, compliance with such data must be ensured, for example via differentiated rights management or a summarized representation and storage of data. So it is important for the manufacturer of the management solution to have already taken the applicable data protection requirements into consideration when designing the solution and having implemented them accordingly.

About baramundi software AG

baramundi software AG opens the way for companies and organizations to manage workstation environments efficiently, securely and independently of platforms. More than 2,500 customers – covering all scales and industries – benefit worldwide from the many years of experience and the outstanding products of the German manufacturer. These come together in the baramundi management suite as part of a holistic, forward-looking and unified endpoint management approach: Endpoint Management, Enterprise Mobility Management, and Endpoint Security are all implemented via a common interface – within a single database and in line with uniform standards.

The baramundi Management Suite optimizes IT management processes by automating routine work and providing a comprehensive overview of the status of network and endpoints. It relieves the burden on IT administrators and ensures users have the rights and applications they need at all times and wherever they are – on all platforms and form factors: on PCs, notebooks, mobile devices or in virtual environments.

baramundi software AG is headquartered in Augsburg. All products and services of the company, which was founded in 2000, are proudly Made in Germany. baramundi cooperates successfully with partner companies worldwide to facilitate sales, consulting and user support.

Read various user reports from baramundi customers here. For further information, please see our website www.baramundi.com.

baramundi

We are looking forward to meeting you!

Get in touch!

baramundi software AG
Beim Glaspalast 1
86153 Augsburg, Germany

+49 (821) 5 67 08 - 380
request@baramundi.de
www.baramundi.de

+49 (821) 5 67 08 - 390
request@baramundi.com
www.baramundi.com

+44 (2071) 93 28 77
request@baramundi.co.uk
www.baramundi.co.uk

+48 (735) 91 44 54
request@baramundi.pl
www.baramundi.pl

baramundi software Austria GmbH
Landstraßer Hauptstraße 71/2
1030 Wien, Austria

+43 (1) 7 17 28 - 545
request@baramundi.at
www.baramundi.at

baramundi software USA, Inc.
550 Cochituate Road, Suite 25
Framingham, MA 01701, USA

+1 (508) 861 75 61
requestUSA@baramundi.com
www.baramundi.com

Empower your IT