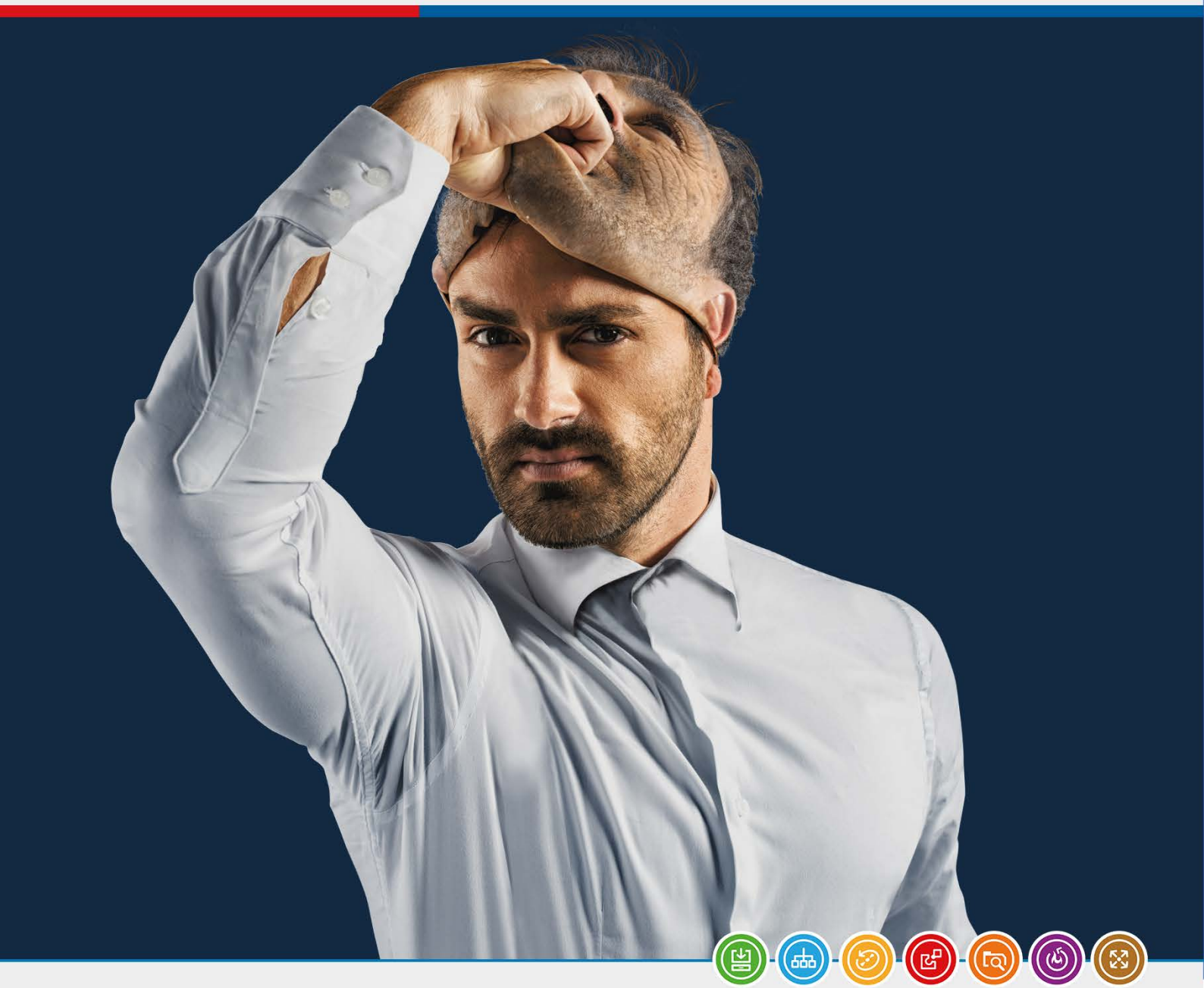
baramundi

Fast and Secure Using Automation

One Management Software For All End Devices



IT management - simply clever

CONTENTS

Management Board: Uwe Beikirch, Dipl.-Ing. (FH) | Dr. Lars Lippert
Chairman of the Supervisory Board: Dr. Dirk Haft
Registered office and court: Augsburg, Commercial Register (HRB) no. 2064 | Tax ID number DE 210294111

1 Increasing Demands on IT Departments

Developments in IT are advancing with ever-greater speed. Where decades passed between Zuse's Z1 and the first PCs, now the industry is seeing evolutions practically every month. As the performance and variety of devices grows, so do the demands involved in managing them.

Many users nowadays work not just on PCs and notebooks, but use smartphones and tablets alongside or in addition to them. Emails are answered on the move, searches are launched on a PC and continued on a smartphone, and presentations are controlled from a tablet. Mobile devices use different operating systems and applications to conventional clients, but they similarly require access to company data and emails and so they need to be secured with similar reliability.

At the same time, the boundaries between mobile devices and the PC world are becoming blurred: for example, nowadays tablets are available with PC operating systems, while mobile apps also run on Windows clients. It therefore makes sense to bundle management of all end devices that users work with in a company into a single solution. That way, administrators can implement consistent standards and obtain a comprehensive overview of the status of the network and all clients. At the same time, future new device types can be integrated easily into a comprehensive solution of this kind.

Routine tasks can be automated using an endpoint management solution, and completed more efficiently, more rapidly, and more easily as a result. This provides the necessary overview, whilst simultaneously improving the security of the company network. This document gives an overview of management tasks that should definitely be automated.

2 Automating Routine Tasks

2.1 Deploying operating systems and applications

A new employee is hired. For the IT department, this means a PC workstation and possibly a notebook computer must be provided. Reinstalling a computer with an operating system and all the applications required – including all the necessary reboots, selecting the right drivers, etc. – can easily take several hours. Using an endpoint management solution, this effort is reduced to just a few clicks of the mouse:

Instead of running an installation manually or using a script, the new device is automatically recognized on the network. The hard drive is formated and partitioned automatically, and the necessary drivers are selected in a single operation. Intelligent solutions use the OS manufacturer's native installation method, thus preserving the full warranty. Computers can even be reinstalled overnight, using wake-on-LAN.

Software can also be deployed automatically. In most cases, standard equipment is defined for a user profile. When needed, the IT administrator then rolls out this software package onto the target system with a click of the mouse – and even onto several devices in parallel, including the necessary reboots and to the highest installation quality, using OEM set-up methods. During setup, the automated solution offers feedback on the installation status at all times and, if applicable, on any errors that have occurred. Once a task has been defined, it can be reused at any time, for example if another new colleague starts a few months later or a device needs to be replaced. At the same time, automated installation guarantees standardized computer configurations and the lowest possible number of errors.

Software frequently needs to be installed for which the manufacturer has not made standardized installation packages available. The scripts that are then needed to automate the interfaces can be created easily and intuitively, using tools that are integrated into current endpoint management software. Even tricky set-ups can be installed centrally and automatically using the set-up procedures provided by the software manufacturer, and the manufacturer warranty remains intact.

But endpoint management software is not only able to deploy applications – it can also uninstall them from the client device. When choosing a solution, care needs to be taken to ensure that this is also possible for programs that were not installed using the management software. In this way, it is possible – for instance – to efficiently remove applications that users have installed on their computers without permission.

Central, automated installation of applications and operating systems also has a positive side-effect for IT administrators and end users: in the event of performance problems and stubborn errors, the workstation can simply be reinstalled overnight, instead of laboriously searching for the cause of the problem. This means that a fully-functioning device is again available as quickly as possible, with minimum time expended by the administrator. It is also possible to handle migration of a large number of workstations, for instance to a new operating system such as Windows 10 or a new version of Office, via an automated operation.

Video OS Installation with baramundi

2.2 Identifying vulnerabilities and automating updates

Installed once and job done? Unfortunately not. Updates for applications and operating systems are constantly being brought out. These need to be uploaded as quickly as possible onto all your computers. This is not just about new features – above all it is about security: New versions and patches close security gaps which cybercriminals can use to penetrate the company network and cause major damage. The consequences range from damage to the corporate image, through disclosure of internal company materials, to legal consequences if customer data is stolen and there are breaches of data protection laws.

A firewall and virus scanner are certainly vital components of an effective security concept, but they are largely ineffective against attacks via unpatched vulnerabilities. If an employee's computer can be induced to connect to the attacker's server under what is known as a reverse engineering attack exploiting a vulnerability, then the firewall does not intervene, because the contact has been initiated from within the company. It is therefore vital to maintain an overview of vulnerabilities on every single client, and to close the gap as quickly as possible, depending on the threat level involved.

However, around 100 new vulnerabilities are identified and documented every week, as is evidenced by statistics from the US-CERT National Vulnerability Database. Here, the endpoint management software can support the IT administrator by carrying out an automated, regular scan of all clients and servers. This results in the administrator receiving comprehensible lists, for example of the most dangerous vulnerabilities in the company network, or of the clients with the most security gaps. This allows the administrator to prioritize and to close the gaps in a targeted manner.

If the solution also offers patch management alongside the vulnerabilities scanner, then any gaps identified can also be closed centrally and automatically straight away. In addition to Microsoft patches, the endpoint management solution should as a minimum also deploy

updates for frequently-used applications such as Adobe Reader, Java, or Firefox centrally and automatically, as the widespread use of these programs makes them particularly popular with attackers. Current software packages for numerous applications are also available from the endpoint management manufacturer as managed software.

However, effective vulnerability management calls for more than simply knowing about gaps and triggering a patch installation. It is also vital to know whether the security-relevant update has actually been received on all client computers. Installations can fail or be blocked by the user, or it may prove impossible to establish contact with a notebook being used in the field. The solution used therefore needs to provide feedback on installation status and on any errors that may have arisen, to ensure that all gaps really have been closed.

Video Patch Management with baramundi

2.3 Taking an inventory of hardware and software, managing licenses

A comprehensive overview is not only important in identifying vulnerabilities and guaranteeing security. For instance, IT managers need to be able to report on hardware and software deployment or, in the event of a license audit by a software manufacturer, demonstrate correct licensing. From the cost viewpoint, it is important to identify unused software that is idling on clients and taking up expensive licenses. Moreover, in the event of support inquiries it is vital to have current and correct data about the hardware and software equipment on the client in question, in order to be able to address the user's concerns quickly and competently.

An automated inventory with endpoint management software explains precisely and rapidly which hardware and software is actually in use anywhere in the company network. This means that a current data base for management-appropriate evaluation is available at all times. Particularly when it comes to volume and upgrade licenses, maintaining an overview is not easy. This is where a license management solution capable of being connected to endpoint management via an interface can supply both an overview and licensing compliance.

In addition, the actual use of a program can be recorded, to avoid unnecessary costs. To that end, each time an application is launched it is logged on the individual client. This shows on which computers a program is never used over a specified period – and which licenses can therefore be saved. It is important to remember that the solution used must comply with the European data protection requirements and must not allow any monitoring of individual employee behavior.

IT support also benefits from the automated inventory: help desk solutions can be connected to the endpoint management software via interfaces. This means that support employees can quickly record the hardware and software equipment on the workstation in question in the event of inquiries.

2.4 Timing control and self service

In many companies, there are maintenance windows which specify that administration tasks may only be carried out on particular computers at designated times. High-performance endpoint management software therefore makes time-controlled tasks available. This enables a patch installation to be deliberately run on a client within a particular time window, for example.

By contrast, event-controlled tasks relieve the IT administrator from responding to events. As an example: If Game XY is discovered on a client when taking inventory, the aim is that this can be removed automatically. Instead of needing to intervene itself every time the game is detected, admin now simply receives a report on the completed uninstallation.

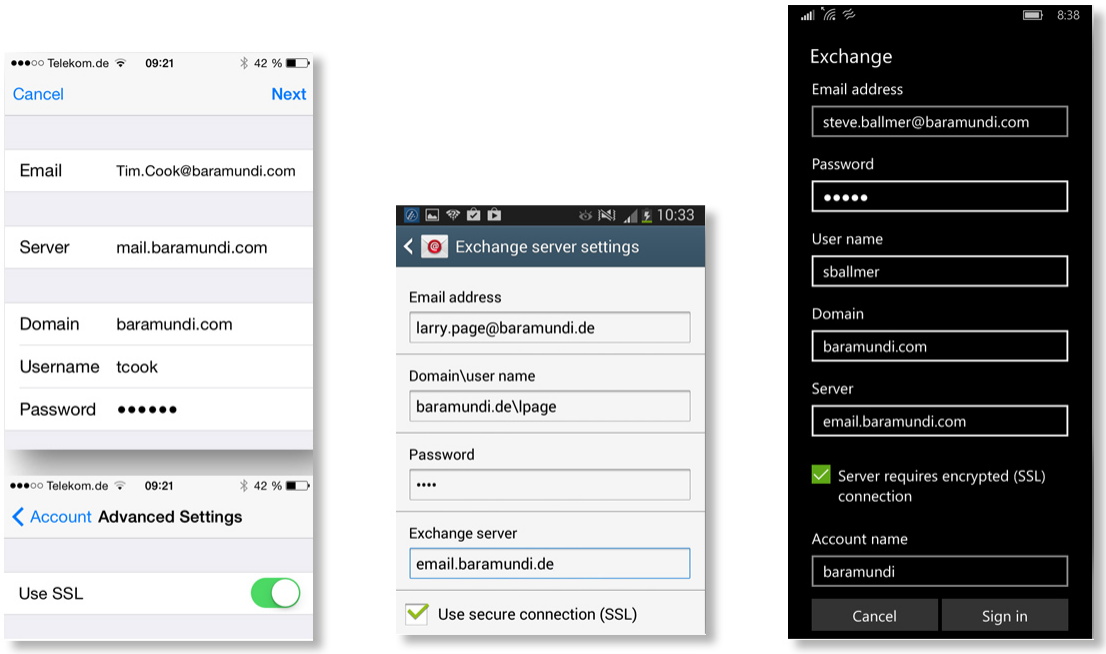
The option of making prepared installation runs available in a self-service kiosk makes things easier for the IT administrator and for users. It allows for rapid, straightforward processing of standard inquiries, for instance a request to install Firefox - and it can be done at precisely the time the user wishes it and needs it to enable them to continue working undisturbed. At the same time, the expenditure on support is reduced, since this task runs fully automatically when it is requested. The administrator should also be notified about these self-service installations, so that they retain the overview of the status of their client computers at all times.

High-performance endpoint management software also offers the option of involving users in installation processes without the administrator having to surrender control. For example, the user can be given the right to postpone a patch installation requiring a reboot within a specified time window. This means that colleagues are not disturbed during their workflow, and the installation can run during a coffee break. At the same time, it ensures that deployment of a critical patch cannot be put off for too long.

3 Managing Mobile Devices

While servers and PCs are automatically subject to IT monitoring and are firmly integrated, different dangers and challenges need to be considered when managing mobile devices. Most of today's popular smartphones and tablets were originally developed for private users. As a consequence, the management options for mobile operating systems are often still significantly more restricted than for PCs. On top of this, administrators need to support several mobile platforms as a rule, setting up the devices and configuring them securely. That is a complex and time-consuming process.

If you compare the three most current mobile platforms, for instance (iOS, Android, and Windows Phone), it rapidly becomes apparent that the same parameters – such as name, email address, server, domain, and encryption for setting up exchange accounts – need to be entered at different points in each case. In practice, this means a huge expense and it also assumes that the administrator is familiar with all the input masks. This workflow can be significantly simplified by using cross-platform profile elements and by managing devices centrally.



Picture: Exchange configuration on different mobile platforms

For this, the smartphone or tablet must first be included in the management solution ("Enrollment"), for example by scanning a barcode which is provided. After that, management tasks – in this example, the exchange configuration – can be carried out centrally via the solution. The relevant settings are set on a standard, cross-platform interface and can then be transferred onto the managed device.

The advantages are self-evident: The administrator no longer needs to know where which setting is made on which mobile device – they always use the familiar interface of their central management console. This reduces the complexity, saves time, and lowers the possibility of errors in the process. The bottom line is that this also results in greater security.

Another advantage is that management tasks can also be carried out "remotely" via management software, without an administrator needing to get their hands on the actual device. For example, if a user in a field location starts to use a new mobile phone, they simply scan the barcode which the administrator has sent them from the central office via email, and then the administrator can handle the rest of the configuration. The processes and tasks used for this can be prepared in advance and used repeatedly – including for a larger number of devices simultaneously or using time control.

It is also the case that mobile devices can go astray more easily than a PC. Corresponding precautions need to be taken to guard against this. The options to consider include automatic blocking when the screen is switched off, the option of deleting the assigned profile, including remotely, and not least the issuing of strong passwords.

In addition, it must be ensured that the administrator has an overview of the devices at all times and is notified if a user compromises the operating system, for example.
For that reason, an MDM solution should offer the option of defining compliance rules which are then checked automatically and regularly. In the event of violations, the administrator is informed and then has the opportunity to adopt counter-measures, ranging from an email alert to the user through to full remote deletion.

In the ideal scenario, mobile device management is integrated into one endpoint management software suite. Not only does that save on expense over set-up, maintenance, and operation; it also enables mobile devices and PCs to be managed in joint groups and organizational entities, and consistent standards to be implemented. This approach is also more future-proof, since new device classes can be more easily integrated into a standardized solution.

4 Data Protection and Data Security

IT administration also means being responsible for data backup and data security. Automated backup is therefore vital. In the event of a crash, it means that data and user settings can be restored easily and straightforwardly – right through to the Word dictionary and desktop icons. These processes too can be reliably automated using endpoint management software.

Equally important is ensuring compliance with the applicable legal regulations on data protection. Since it is possible to identify individual user behavior from the wealth of user data that an endpoint management system potentially records, compliance with the data protection regulations must be guaranteed – for example, through differentiated rights management or summarized display and storage of data. It is therefore important that the endpoint management manufacturer has already taken the data protection specifications applicable in this country (Germany) into account when designing the solution and has implemented suitable solutions.

About baramundi software AG

baramundi software AG provides companies and organizations with efficient, secure, and cross-platform management of workstation environments. Around the world, over 2000 customers of all sizes and from every sector benefit from the independent German manufacturer's many years of experience and outstanding products. These are compiled into an integrated, future-orientated unified endpoint management approach in baramundi Management Suite: endpoint management, mobile device management, and endpoint security are provided via a common interface, in a single database, and according to uniform standards.

baramundi Management Suite optimizes IT management processes by automating routine tasks and providing an extensive overview of the status of all endpoints. It relieves the pressure on IT administrators and ensures that wherever users are located, they always have the necessary rights and applications on all platforms and form factors, whether on PCs, notebooks, mobile devices, or in virtual environments.

baramundi software AG is headquartered in Augsburg. The products and services of the company, which was founded in 2000, are fully Made in Germany. baramundi successfully works with partner companies around the world in sales, consultancy, and user support.

You can read various user reports by baramundi customers here. For more information, please visit our website www.baramundi.com.

You want to learn more about the baramundi Management Suite? Register for the live webinar!

Discover cross-platform management for PCs, servers, mobile devices, Macs, and virtual environments by using the baramundi Management Suite in a free webinar.

www.baramundi.com/webinar

baramundi

baramundi software AG
Beim Glaspalast 1
86153 Augsburg
Germany

Tel: +44 (20) 71 93 28 77
Fax: +49 (821) 5 67 08 - 19
Email: request@baramundi.com
www.baramundi.com

IT management - simply clever