



Automation in Endpoint Management

*Optimize routine tasks –
from OS deployment to security compliance*

Contents

1	Increased IT Complexity, Higher IT Workloads	03
2	Automate Routine Tasks	04
2.1	Distribute operating systems and applications automatically	04
2.2	Identify vulnerabilities and automate updates	06
2.3	Inventory hardware and software, manage licenses	07
2.4	Intelligent automation: maintenance windows and self-service	09
2.5	Integration into the existing infrastructure	10
3	Interfaces and Co-Management	11
4	Managing Mobile Devices	12
5	Data Security and Data Protection	15

© 2026 baramundi software GmbH | Statements regarding equipment and technical functionalities are non-binding and for informational purposes only. Subject to change without notice.

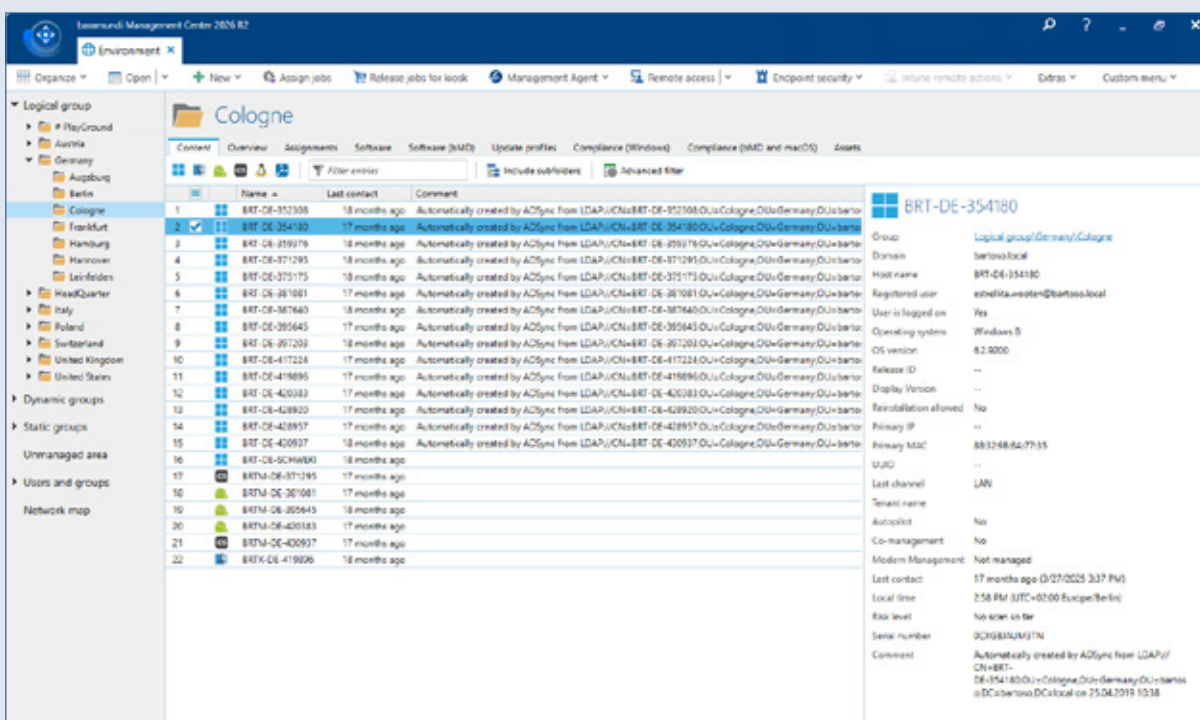


1 Increased IT Complexity, Higher IT Workloads

The proliferation of device types, operating systems, remote work models, and security mandates has transformed endpoint management from a background function into a critical factor in business success. Manual IT processes don't scale, lead to tool sprawl, add complexity, and increase the risk of errors, downtime, and compliance exposures. Centralized, policy-based unified endpoint management (UEM) using a configurable mix of tools integrated into a single solution with a consistent administrator interface is required to give IT teams operational control. It simplifies and streamlines management tasks for diverse devices, provides a framework for enforcing security standards, and ensures real-time visibility into every device on the network.

Automation provides multiple benefits

A UEM system delivers its greatest value when you combine those IT management tools with automation. Routine tasks that once consumed hours of manual effort — OS installations, software and patch deployment, inventory updates — can run unattended at scale across all devices or in highly targeted endpoint groups. The result is increased IT efficiency, consistently higher-quality outcomes, and a more reliable, secure environment. To help IT teams prioritize which tasks to automate, this whitepaper outlines the areas that deliver the highest returns.



Comprehensive visibility for all device types and platforms

2 Automate Routine Tasks

Automated OS and software distribution, patch management, inventory, self-service, and API integrations are the operational core of endpoint security. This chapter covers the tasks that should be automated first and why.

2.1 Distribute operating systems and applications automatically

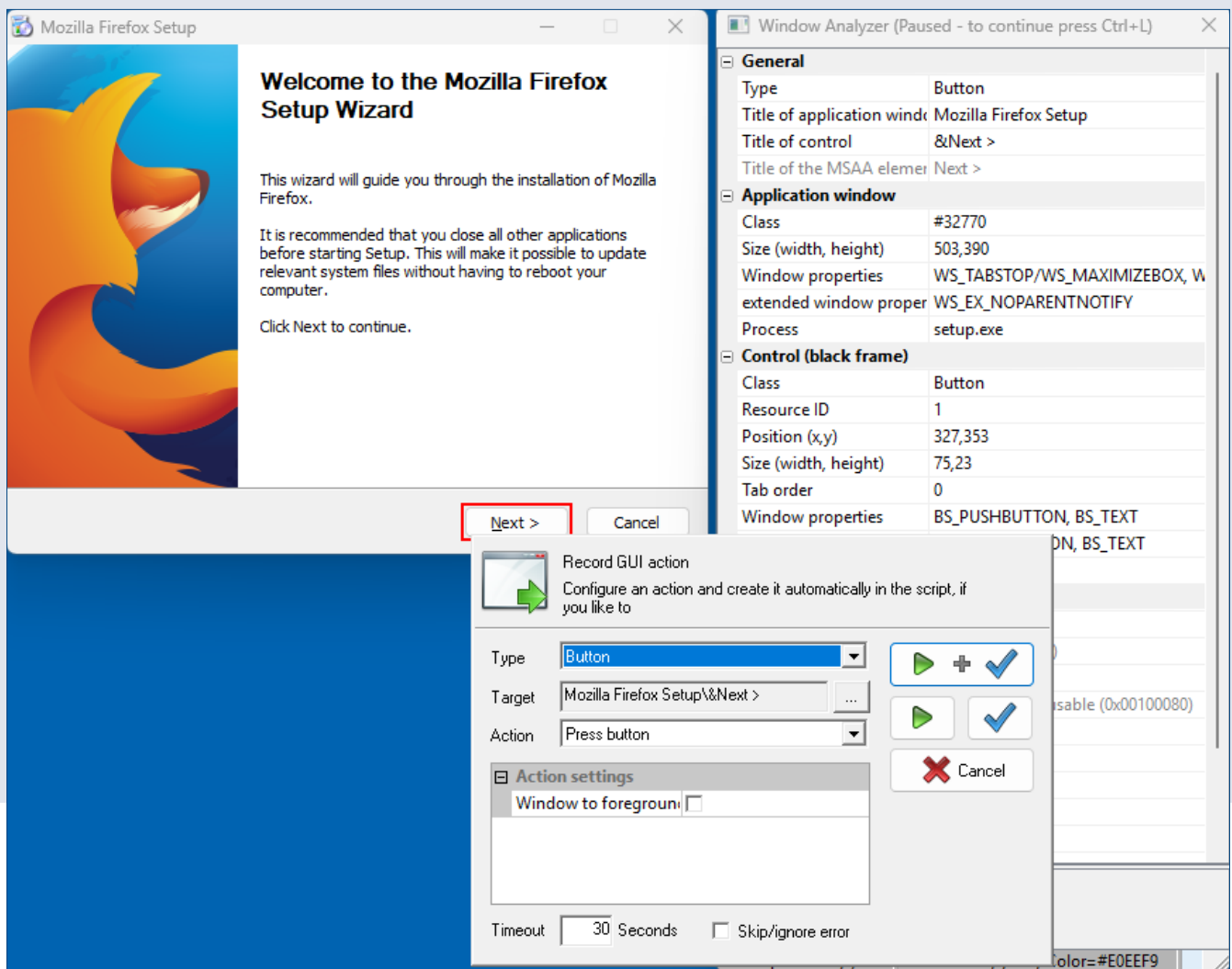
Provisioning a new endpoint typically involves OS configuration and installation, driver selection, multiple restarts, and application deployment—a repetitive process that can take hours of IT staff time per device. With a modern UEM solution, provisioning becomes an automated, predefined, and precisely controlled workflow rather than a series of manual tasks. The new device is detected on the network, drivers are prepared, drivers are assigned, and the OS and approved applications are installed automatically. This includes Windows Autopilot and co-management integration with Microsoft Intune for hybrid environments.

The benefits of standardized configurations

Automated software distribution reduces repetitive IT workloads and creates standardized endpoint environments. A defined configuration is stored for each application and can be rolled out to individual or multiple devices simultaneously, including restarts, real-time status feedback, and error logging. Automations can be stored and reused as needed to ensure consistent installations, minimize manual effort, and eliminate errors.

Automating installation of non-standard software

Automation also works for software without standardized installation packages. Modern UEM systems enable IT teams to create installation scripts by drag-and-drop selection of required steps and responses to dialog options. Even complicated setups can be automated and installed from a centralized admin interface using the manufacturer's setup procedure to maintain warranty coverage. Automation also applies to uninstalling outdated or unused applications to free up licenses and to remove unauthorized shadow IT apps.



Using the baramundi Automate wizard to create a standardized installation script

The centralized, automated installation of applications and operating systems also enables IT administrators to quickly reinstall an application in response to a support ticket reporting a performance or stability issue. Even the migration of multiple PCs to a new version of an OS or Microsoft Office can be automated, including synchronization with Microsoft Intune.

2.2 Identify vulnerabilities and automate updates

Patching is not optional. Updates for operating systems and applications must be deployed to all endpoints as quickly as possible, not just to access new features, but to close vulnerabilities. The consequences of delayed patching range from data breaches and operational disruption to legal and regulatory exposure under laws such as HIPAA, PCI DSS, CCPA, NIS2, and other applicable statutes.

Unpatched vulnerabilities are a primary attack vector

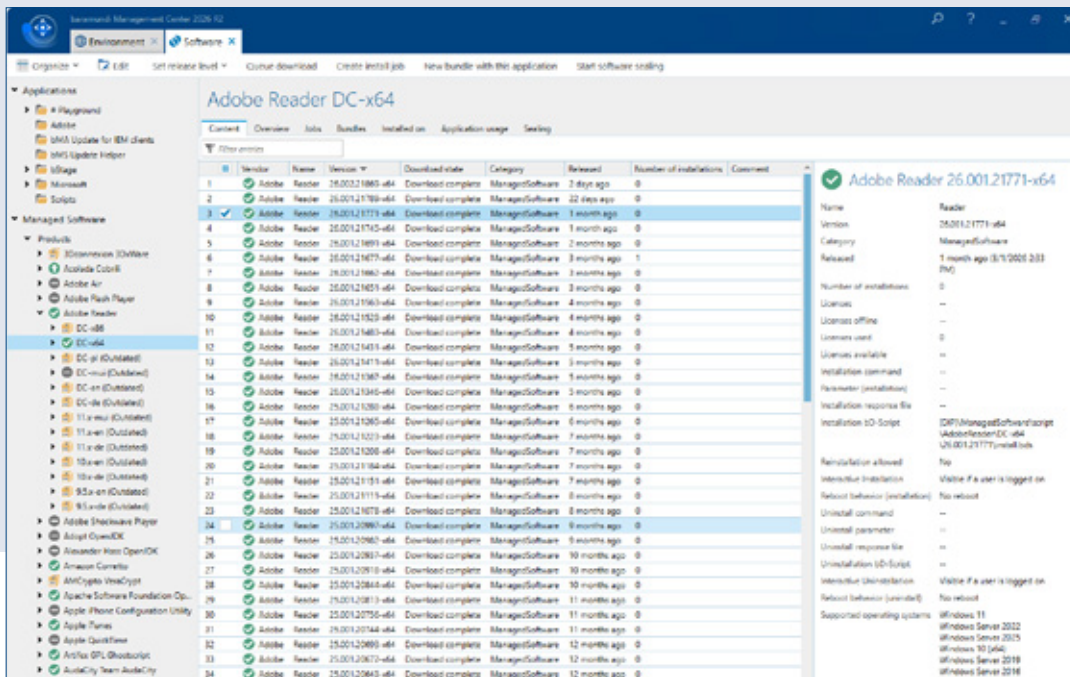
Firewalls and antivirus software are essential components of an effective security strategy, but they are largely ineffective against attacks exploiting unpatched vulnerabilities. In a so-called reverse shell attack, an employee's computer is compromised to establish an encrypted connection to the attacker's control server. The firewall usually does not intervene because the connection uses standard channels. This makes it essential to monitor vulnerabilities on every endpoint and to close them as quickly as possible, based on the level of risk.

NIST's National Vulnerability Database (NVD) published 48,185 CVEs in 2025, with roughly 130 new vulnerabilities disclosed each day. More than 40% were classified as High or Critical severity. No manual patch program can keep pace with that volume. Compounding the challenge, NIST acknowledged in 2026 that it can no longer enrich all NVD entries and will prioritize only a subset. Accordingly, raw CVE counts increasingly understate overall risk. Effective vulnerability management now requires automated scanning that uses multiple sources: NIST NVD for breadth, CISA's Known Exploited Vulnerabilities (KEV) catalog for exploitation priority, and vendor advisories for product-specific risk.

Vulnerability scanning in modern UEM solutions aggregates and prioritizes information from these sources, giving IT teams a continuously updated view of which endpoints have the most exposure and which remediations to prioritize first.

Vulnerability scanning and update management

Comprehensive UEM solutions also provide automated patch management for third-party applications. Patches and updates for commonly used applications such as Adobe Reader, Chrome, or Firefox are delivered as packages that can be configured and deployed to affected endpoints.



Ready-to-distribute software packages with different approval levels

However, effective vulnerability management requires more than just knowing about a vulnerability and distributing a security patch. IT admins must also confirm that the update has been successfully installed on all affected devices. Installations can fail or be blocked by the user, or a device may be offline. The patch management solution must promptly report the installation status and any errors encountered on each device to ensure that all gaps are closed.

2.3 Inventory hardware and software, manage licenses

A comprehensive, up-to-date IT asset inventory is important for identifying vulnerabilities and compliance gaps. Detailed inventories also enable IT managers to report the status and utilization of hardware and software, to repurpose or remove unused software to manage licensing costs, and to document license compliance in the event of an audit by a software manufacturer.

Compliance through automation

It is easy to lose track of IT assets, especially as the number and types of devices, along with the volume of licenses and upgrades, increase. UEM solutions that automatically update IT inventories in real time can quickly show the configurations of all installed hardware and software in granular detail, down to versions, builds, firmware, drivers, and more. This ensures that IT teams always have complete, up-to-date data for operational, budgeting, and maintenance decisions. Integrated license management provides added clarity and simplifies compliance management and reporting.

Application usage data also informs licensing decisions. By tracking application launches on each endpoint, IT teams can identify infrequently used software and reclaim those licenses to reduce SaaS and volume licensing costs. Usage tracking must comply with applicable US and EU privacy laws and must not monitor individual user behavior.

The screenshot displays the Baramundi Management Center 2024 R2 interface. The top navigation bar shows the environment 'BRT-DE-860672' and the current activity status. The left sidebar contains a tree view with categories like Settings, Assignments, Inventory, and Compliance. The main area is titled 'Software' and displays a table of installed software. The table has columns for Name, Vendor, Version, Last found, Category, and License key. The right sidebar shows a detailed view of the selected .Net Framework software, including its version, category, license key, and installation details.

Name	Vendor	Version	Last found	Category	License key
.Net Framework	Microsoft	3.5.1-en	17 months ago	ManagedSoftware	
.Net Framework	Microsoft	4.7.2-en	17 months ago	ManagedSoftware	
Chrome	Google	51.0.2704.136-x64	17 months ago	ManagedSoftware	
Firefox	Mozilla	10.0.2-de	17 months ago	ManagedSoftware	
iTunes	Apple	12.9.4.102-x64	17 months ago	ManagedSoftware	
Java JRE	Oracle	6.30-x64	17 months ago	ManagedSoftware	
Baramundi Management Suite	Baramundi	baseDIP	17 months ago	ManagedSoftware	
Notepad++	Notepad++ Team	5.9.5-x64-de	17 months ago	ManagedSoftware	
SumatraPDF	Krzysztof Kowalik	1.8	17 months ago	ManagedSoftware	
Thunderbird	Mozilla	45.2.0-de	17 months ago	ManagedSoftware	
Updates	Windows	Root Certificates november2011	17 months ago	ManagedSoftware	
Visual C++ Redistributable	Microsoft	2010-SP1-x64	17 months ago	ManagedSoftware	
Visual C++ Redistributable	Microsoft	2010-SP1-x86	17 months ago	ManagedSoftware	
VLC	Videolan	2.2.4-x64	17 months ago	ManagedSoftware	

.Net Framework

Vendor: Microsoft
Version: 4.7.2-en
Category: ManagedSoftware
License key: --
Type: Application
Comment: --
Installed: 7 years ago (4/9/2019 4:00 PM)
Last found: 17 months ago (4/1/2021 4:37 PM)
Software detection rule: --

Managed Software

Status: Up-to-date
Name: .Net Framework
Installed version: 4.7.2-en
Latest version released: 4.7.2-en
Latest version released for testing: 4.7.2-en
Latest version available: 4.7.2-en

List of installed software

Advantages for IT support

IT support teams also benefit from automated inventory updates. Integrated helpdesk solutions allow support staff to quickly view a user's hardware and software configuration when responding to a support request, enabling faster, more accurate issue resolution.

2.4 Intelligent automation: maintenance windows and self-service

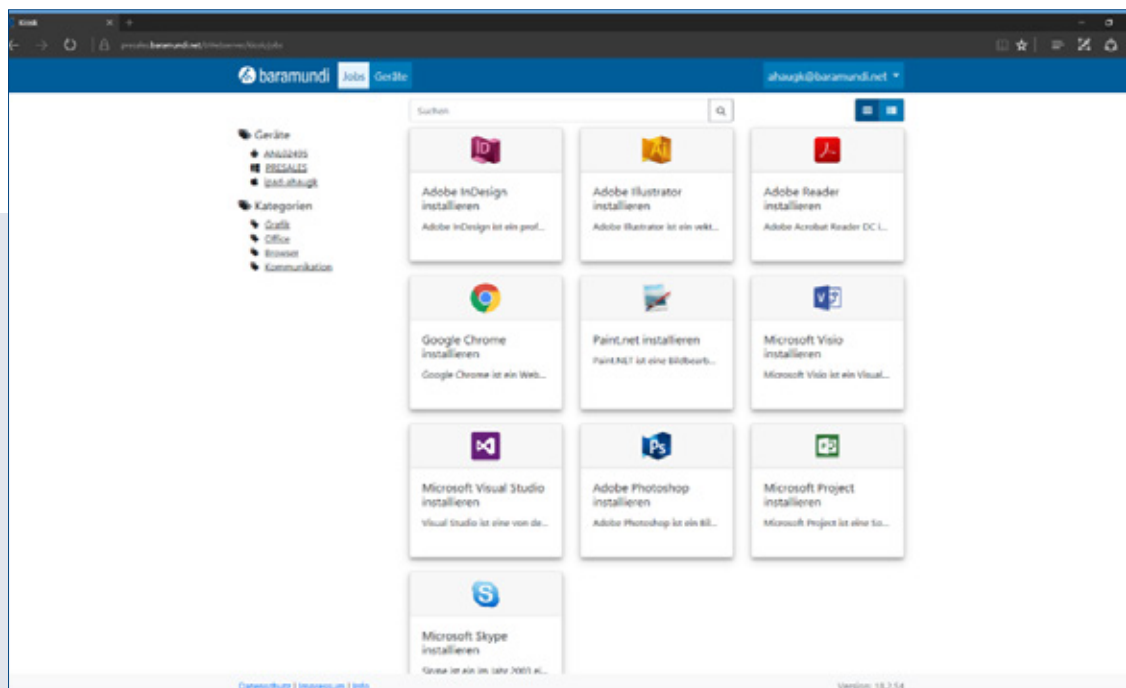
Many IT teams define maintenance windows to perform tasks on specific end devices. Modern UEM solutions provide a high degree of control for setting or adjusting maintenance windows and accommodating user preferences. This allows OS updates, patch installations, and other tasks to be performed at times that eliminate or minimize disruptions to users and business operations.

Event-driven automation

Event-driven automation reduces the need for IT administrators to respond to unplanned circumstances that require manual intervention. For example, if unauthorized software is detected on an endpoint during an inventory update, the management solution can automatically uninstall it, update the inventory, and report the action and outcome to the IT team.

User self-service

Self-service software kiosks or company app stores provide convenience for IT administrators and users alike. IT administrators can provide pre-configured installation packages that users can access quickly and easily to install commonly used apps and tools. Automated self-service options reduce the volume of support requests, enable admins to track installations via dashboards and reports, and automatically update IT inventories.



Self-service kiosk for users

Modern UEM platforms also provide users with a measure of control over patch and update installations while maintaining security and IT oversight. For example, users can postpone a patch installation that requires a restart to a time that doesn't interrupt their workflows, such as during a planned break or after hours. IT teams can set a time limit for any postponement to ensure that the distribution of a critical patch is completed in a timely manner.

2.5 Integration into the existing infrastructure

UEM solutions should integrate seamlessly with existing IT management systems to support consistent workflows and maximize ROI. Modern APIs provide two-way connectivity between the endpoint management solution and ITSM, ERP, and other systems. For example, after a new IT device is entered in the ERP system, it can be automatically enrolled in the management solution, with details such as inventory number, acquisition date, cost center, and other data. The management system can then automatically provision the device with the appropriate software, configurations, and policies.

ITSM integration extends these capabilities to help desk staff, who receive real-time hardware and software data for any endpoint directly within their ticketing workflow. They can use the data to trigger installations or configuration changes and update device details in inventory, reducing resolution time.

3 Interfaces and Co-Management

Open interfaces, co-management, and DEX integration turn endpoint management into a connected enterprise capability. Those features reduce manual handoffs, improve asset data quality, and proactively resolve device and user experience issues.

Comprehensive UEM solutions rely on standardized, open APIs such as REST with JSON/XML support, as well as PowerShell and CLI tools, to exchange data between systems. Inventory, device status, vulnerability information, compliance details, and other data flow bidirectionally between the management solution and a variety of ITSM, IT asset management, network monitoring, remote access, and security operations systems. This eliminates manual data entry and enriches system records with device details. APIs also enable automated, consistent, and more accurate workflows across operational areas.

Co-management for hybrid environments

Co-management enables a consistent management approach across hybrid work environments by connecting on-premises UEM solutions with cloud management systems such as Microsoft Intune. Endpoint data is synchronized at regular intervals to provide a stable, scalable database for orchestrating automated OS deployments, patch distributions, and configuration changes. New devices are enrolled in both systems in parallel, while device data, such as licenses or inventory numbers, remains consistent. This reduces administrative overhead and eliminates duplicate work.

DEX integration for proactive IT management

Digital Employee Experience (DEX) solutions supplement UEM and ITSM systems by collecting real-time user experience data, such as boot times, app crashes, battery life, and network latency. Analyzing endpoint data enables early detection and proactive resolution of issues, even before a support ticket is created. These proactive workflows reduce ticket volumes and improve employee satisfaction.

Seamless automation across systems

Many multi-step workflows can be automated by exchanging data across multiple IT management systems. For example:

- ERP systems can automatically synchronize device inventory, cost center, and other data with UEM and ITSM systems.
- Vulnerability scanning results from the UEM system can trigger automated remediation processes in the ITSM system.
- IT teams can use DEX analyses of common endpoint problems to create automated fixes for use by help desk staff.

In addition to co-management capabilities with Microsoft Intune, the baramundi Management Suite provides extensive options for cross-system synchronization and automation through bConnect, a powerful REST API for bidirectional integrations.

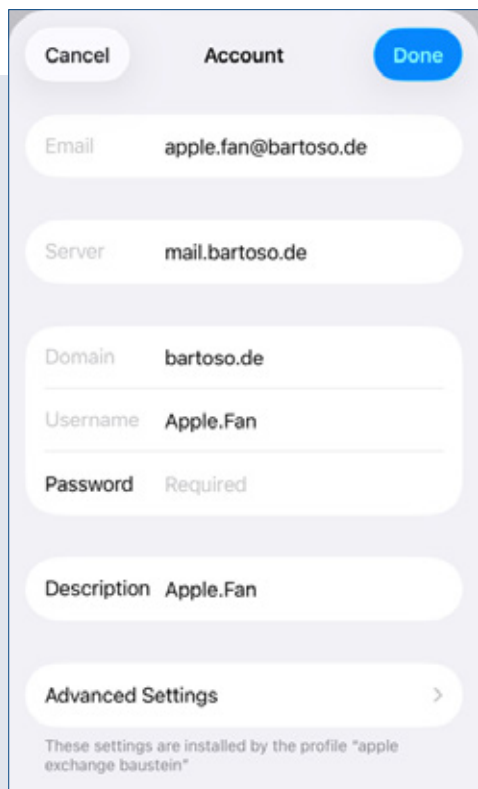
4 Managing Mobile Devices

BYOD is now standard across most organizations, yet unmanaged personal devices remain a significant attack surface. This chapter explains how modern UEM delivers consistent policy enforcement, app management, and security controls across iOS, Android, and PCs without compromising employee privacy.

Bring Your Own Device (BYOD) is the norm across most US and EU organizations. Employees access corporate data and applications on personal laptops, tablets, and smartphones, and IT must manage the security implications without direct control over the hardware. Unmanaged personal devices are a significant attack surface, and organizations subject to NIS2, SOC 2, HIPAA, or the FTC Safeguards Rule cannot afford gaps in endpoint visibility. A UEM solution that enforces security policies on personal devices – without requiring full corporate MDM enrollment or exposing personal data – helps balance workforce flexibility with security obligations.

Comprehensive management of all device types

UEM solutions must be capable of consistently managing all device types, from iOS, iPadOS, and Android devices to Windows, macOS, and Linux desktops and laptops. Without uniform management processes, IT staff training becomes fragmented, work quality becomes inconsistent, and tool sprawl increases. For example, a system that requires different inputs to configure Exchange settings (name, email, server, encryption) on iOS and Android devices is more prone to error and re-work. However, modern UEM systems enable automated deployment of cross-platform profiles for every device type.

A screenshot of an iOS 'Account' settings screen. At the top, there are three buttons: 'Cancel', 'Account', and 'Done'. Below these are several input fields: 'Email' with the value 'apple.fan@bartoso.de', 'Server' with 'mail.bartoso.de', 'Domain' with 'bartoso.de', 'Username' with 'Apple.Fan', and 'Password' with 'Required'. Below these is a 'Description' field with 'Apple.Fan'. At the bottom, there is an 'Advanced Settings' section with a right-pointing arrow. A small note at the very bottom states: 'These settings are installed by the profile "apple exchange baustein"'.

Cancel Account Done

Email apple.fan@bartoso.de

Server mail.bartoso.de

Domain bartoso.de

Username Apple.Fan

Password Required

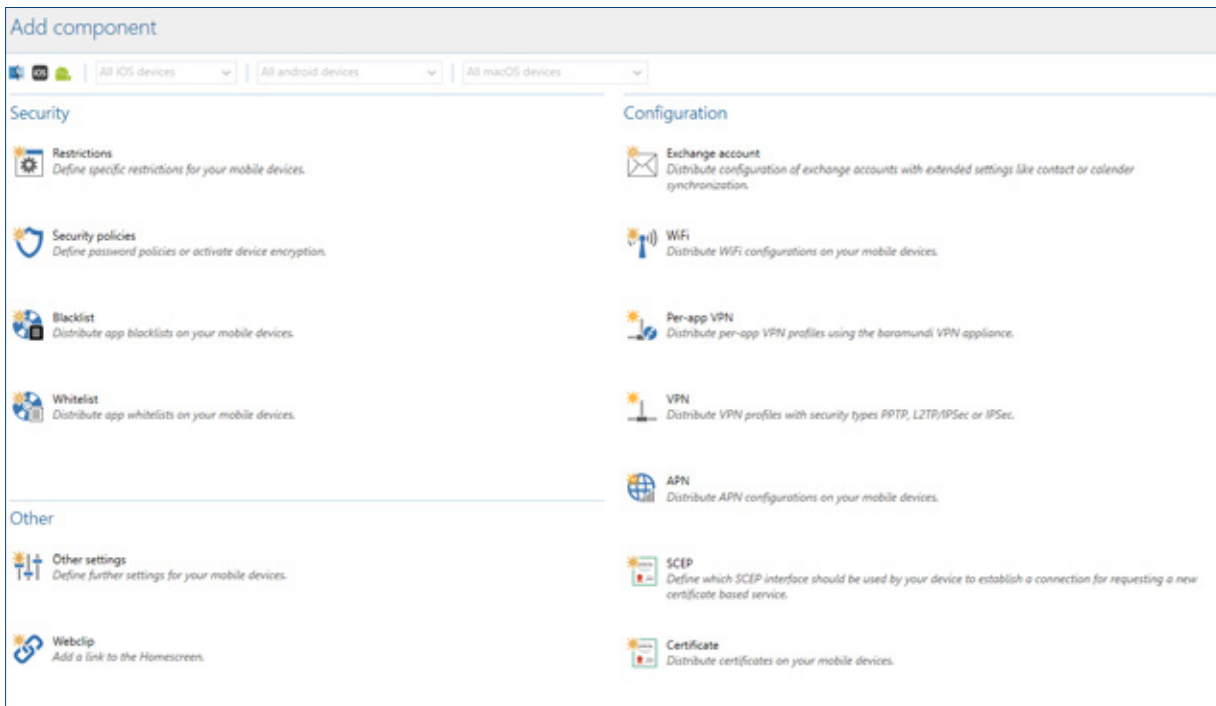
Description Apple.Fan

Advanced Settings >

These settings are installed by the profile "apple exchange baustein"

Exchange configuration on different mobile platforms

Today, automated enrollment of mobile devices in IT management is quick and easy via Apple Automated Device Enrollment (ADE) or a QR code. After enrollment, IT teams can deploy profiles for email setup, security policies and other functions from a central, uniform, cross-platform interface.



Cross-platform profile modules for configuring mobile devices

Automated policy enforcement across platforms

The key advantage is simple, error-free management without manual intervention. Workflows can be prepared, automated, and applied to both iOS and Android devices, saving time and ensuring security. Mobile devices are lost or improperly modified more often than traditional PCs, making automated security measures, including secure passwords, automatic locking, remote deletion, and continuous monitoring, even more important.

Modern management solutions automatically check device compliance, detect jailbreaks or violations, and initiate remediation, remote locking, or deletion if necessary. Automated firmware updates also close security gaps in a timely manner.

Co-management features tightly integrated with Microsoft environments enhance protection. For example, the baramundi Management Suite reports the compliance status of managed iOS, Android, and Mac endpoints to Intune, which forwards it to Entra ID and integrates it into Conditional Access policies. Non-compliant devices are automatically denied access without manual intervention.

The risk-based approach enhances control over access to Microsoft 365 and other Microsoft-protected applications, enabling companies to improve security with their existing management tools and processes. Automated synchronization between baramundi and Intune creates a consistent security workflow: baramundi handles device management, while Intune and Entra ID secure access to sensitive data. This gives IT administrators a unified view of compliance, access, and device status across their existing infrastructure.

Control over apps

Current UEM solutions support software block and allow lists to control which apps can be installed on managed devices. This prevents unauthorized installations while allowing approved apps to be downloaded and installed, often as pre-configured packages available from a company's self-service kiosk.

As an active member of the AppConfig community, baramundi uses established standards and native platform functions to automate the distribution, configuration, and security of mobile applications. The baramundi Management Suite integrates mobile device, application, and content management (MDM, MAM, MCM) into a single platform. This enables IT administrators to efficiently manage, enforce policies, and automatically roll out security updates to PCs and mobile devices through a single interface. This integrated approach reduces administrative overhead, closes security gaps more quickly, and ensures that companies can seamlessly integrate future device types into endpoint management workflows.

5 Data Security and Data Protection

UEM solutions should be included in compliance practices because they handle sensitive data and have broad system access. This chapter covers UEM backup, access controls, privacy requirements, and security-by-design principles.

Automated backups in UEM

Comprehensive UEM solutions support automated backups with regular integrity checks, redundancy, and recovery features required for business continuity. Management practices should include regular backups of critical systems, drives and databases with secure off-site storage, to ensure rapid recovery and restoration of operations in the event of a cyberattack, natural disaster, or other emergencies.

Data protection and compliance

Risk analysis, incident management, encryption during storage and transmission, and multi-factor authentication are essential IT management practices worldwide and required in the EU under NIS2 and GDPR. UEM solutions can collect user data, so differentiated rights management (IAM, access restrictions), pseudonymization, and aggregated storage are required to prevent profiling.

UEM vendors must also apply security-by-design principles not only as required by law but also as best practices in software development. This includes embedding privacy and security in the design and operation of a UEM solution's policy enforcement, patch management, and asset inventory functions, and implementing supply chain security measures for distributing and installing updates and upgrades.

baramundi UEM advantages for NIS2 compliance in the EU

For companies in the EU, the baramundi Management Suite standardizes endpoint security across all device types, including mobile devices and operational technology (OT) systems such as industrial process controllers used in manufacturing. It supports vulnerability scanning, automated resets after cyberattacks, and audit reporting, helping companies ensure business continuity and NIS2 compliance.

About baramundi software GmbH

baramundi software's Unified Endpoint Management (baramundi Management Suite) and Proactive Endpoint Operations (baramundi Proactive Hub) solutions enable organizations to manage IT environments and digital workplaces efficiently, securely, and across platforms – on-premises and in the cloud. baramundi software GmbH is headquartered in Augsburg, Germany. Founded in 2000, the company develops its products and services in the EU and supports them through offices in the U.S., Italy, and Poland. baramundi also collaborates with sales, consulting, and customer support partners worldwide.

More information about baramundi: www.baramundi.com



Register for our live webinar to learn more about the baramundi Management Suite!

Discover how the baramundi Management Suite automatically manages and secures your endpoints, servers, and mobile devices, then try it free for 30 days in your own network.

<https://www.baramundi.com/en-us/events-trainings/webinars/>

Get in Touch.

We are looking forward to meeting you!



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany
+49 821 56708-380
request@baramundi.com



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



+43 1 928 0136 0010
request@baramundi.com



baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA
+1 508 861 7561
requestUSA@baramundi.com



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+49 821 56708-390
request@baramundi.com

