

baramundi & Intune Co-Management

Die Lösung für hybrides Endpoint Management

Inhalt

Was ist Co-Management?	03
Vorteile von Co-Management	03
Stärken der einzelnen Lösungen	04
Stärken von Intune	04
Stärken der baramundi Management Suite	05
Praktische Umsetzung von Co-Management	07
Microsoft Intune Connector in baramundi	08
baramundi Management im existierenden Intune Umfeld	09
Integration und Datensynchronisierung zwischen baramundi und Intune	10
Neue Endgeräte ausliefern	11
Stärken nutzen – Zeit und Aufwand sparen	12

© 2026 baramundi software GmbH | Aussagen über Ausstattung und technische Funktionalitäten sind unverbindlich und dienen nur der Information. Änderungen vorbehalten.



Was ist Co-Management?

Als Co-Management bezeichnet man in der IT die parallele Verwaltung von Endgeräten durch mehrere Management-Systeme – typischerweise durch die Kombination etablierter On-Premises-Verwaltung mit cloudbasierten Management-Ansätzen. Ziel ist es, die jeweiligen Stärken der Systeme gezielt zu nutzen, ohne bestehende Prozesse, Automatisierungen und Investitionen vollständig aufzugeben.

Dieses Whitepaper betrachtet die Kombination aus klassischem Unified Endpoint Management von baramundi und dem Modern-Management-Ansatz von Microsoft Intune. Sie verbindet die Tiefe und Prozessreife etablierter Endgeräteverwaltung mit der Flexibilität cloudbasierter Funktionen – und bildet damit einen praxisnahen Ansatz für Unternehmen, die ihre Endgeräteverwaltung modernisieren, aber kontrolliert weiterentwickeln möchten.

Vorteile von Co-Management:

Der parallele bzw. hybride Betrieb von On-Premises- und Cloud-Systemen ermöglicht die Nutzung der Stärken beider Ansätze nach dem Best-of-Breed-Prinzip. Voraussetzung dafür ist, dass beide Systeme sauber integriert, klar abgegrenzt und passend zum jeweiligen Einsatzszenario konfiguriert sind. Daraus ergeben sich mehrere Vorteile:

- ✓ **Flexibilität**
Unternehmen können neue Cloud-Dienste und -Funktionen evaluieren und produktiv nutzen, ohne bestehende IT-Infrastruktur und bewährte Prozesse vollständig aufzugeben.
- ✓ **Betriebliche Kontinuität**
Bestehende Verwaltungsprozesse können weiter genutzt werden, während neue cloudbasierte Funktionen schrittweise eingeführt werden. Dadurch lassen sich Migrationen kontrollierter planen und operative Risiken reduzieren.
- ✓ **Heterogene Umgebungen**
Der hybride Betrieb deckt eine größere Bandbreite an Endgeräten und Betriebssystemen ab – von klassisch verwalteten Windows-Clients bis hin zu mobilen und externen Geräten.
- ✓ **Kontrollierte Daten- & Prozesshoheit**
Unternehmen können gezielt steuern, welche Verwaltungsaufgaben lokal, cloudbasiert oder kombiniert umgesetzt werden. Das unterstützt eine differenzierte Umsetzung interner Sicherheits-, Betriebs- und Compliance-Vorgaben.
- ✓ **Erhöhte Sicherheit**
Die Kombination aus lokaler Kontrolle und cloudbasierten Sicherheitsfunktionen unterstützt ein mehrschichtiges Schutzkonzept.

Auch Microsoft beschreibt Co-Management als Ansatz, Windows-Geräte gleichzeitig mit einer bestehenden Management-Lösung und Microsoft Intune zu verwalten. Der Gedanke dahinter: Bestehende Investitionen und bewährte Prozesse bleiben nutzbar, während zusätzliche cloudbasierte Funktionen ergänzt werden.

Stärken der einzelnen Lösungen

Intune und baramundi ergänzen sich in vielen Bereichen mit ihren unterschiedlichen Stärken. Dabei ziehen IT-Verantwortliche den größten Nutzen aus dem Hybridbetrieb, wenn sie folgende Aspekte im Hinterkopf behalten:



Stärken von Intune

Detaillierte Konfiguration per Richtlinie

Intune ermöglicht die zentrale Konfiguration von Endgeräten über Gerätekonfigurationsrichtlinien, den Settings Catalog und Administrative Templates. Dadurch lassen sich viele Windows-, macOS-, iOS-/iPadOS- und Android-Einstellungen cloudbasiert steuern, ohne auf individuelle Skripte oder lokale Tools angewiesen zu sein. Neue und aktualisierte Einstellungen werden kontinuierlich ergänzt.

Zugriffssteuerung mit Conditional Access

In Kombination mit Microsoft Entra ID und Compliance-Richtlinien unterstützt Intune granulare Zugriffsentscheidungen für Unternehmensressourcen. So kann beispielsweise gesteuert werden, dass nur verwaltete und konforme Geräte auf geschützte Cloud-Ressourcen zugreifen dürfen. Conditional Access bleibt damit ein zentraler Baustein für Zero-Trust-Szenarien.

Dieses Zusammenspiel kann durch baramundi ergänzt werden: Die baramundi Management Suite übermittelt den Compliance-Status verwalteter iOS- und Android-Endpunkte in Co-Management-Szenarien an Intune, von wo dieser an Entra ID weitergeleitet und in die dortigen Conditional-Access-Richtlinien eingebunden werden kann. Die Entscheidung über den Zugriff verbleibt dabei vollständig bei Intune bzw. Microsoft Entra ID. Wichtig ist eine saubere Abgrenzung: baramundi liefert einen zusätzlichen Compliance-Datenpunkt, ersetzt aber nicht die Conditional-Access-Logik von Microsoft. Die zugrunde liegenden Compliance-Richtlinien werden weiterhin in Microsoft Intune definiert und verwaltet. baramundi ergänzt diese Szenarien durch die Bereitstellung und Verarbeitung von Compliance-Informationen, die in Co-Management-Umgebungen für Transparenz und operative Prozesse genutzt werden können.

Umfangreiches Defender Management

Als Teil des Microsoft-Ökosystems lässt sich Microsoft Defender for Endpoint über Intune zentral konfigurieren und mit Sicherheitsrichtlinien verknüpfen. Dadurch können Unternehmen Schutzvorgaben konsistent ausrollen, Compliance-Anforderungen durchsetzen und Sicherheitszustände besser überwachen.

Moderne App-Verwaltung

Intune unterstützt Unternehmen bei der zentralen Bereitstellung, Aktualisierung und Verwaltung von Anwendungen auf Windows-, macOS-, iOS-/iPadOS- und Android-Geräten. Anwendungen können gezielt Benutzern oder Geräten zugewiesen und automatisiert bereitgestellt werden. Dadurch lassen sich neue Geräte schneller produktiv einsetzen, Softwarestände standardisieren und der administrative Aufwand reduzieren. Gleichzeitig ermöglicht die cloudbasierte Bereitstellung eine flexible Versorgung von Endgeräten unabhängig vom Standort der Benutzer.



Betriebssystem-Installation

Mit der baramundi Management Suite lassen sich Windows-Geräte automatisiert installieren, konfigurieren und bereitstellen. Betriebssysteme, Treiber, Anwendungen und Einstellungen können zentral verwaltet und entsprechend den Unternehmensrichtlinien ausgerollt werden. Dadurch werden die Einrichtung neuer Geräte sowie die Neuinstallation bestehender Systeme standardisiert und vereinfacht.

Umfangreiche Inventarisierung von Hard- und Software

Die baramundi Management Suite bietet eine detaillierte Inventarisierung von Hardware, Software und Konfigurationsdaten. Die erfassten Informationen bilden die Grundlage für Transparenz, Compliance-Prüfungen, Automatisierung und Reporting. Dynamische Gruppen sowie individuell anpassbare Inventurdaten ermöglichen die Abbildung komplexer IT-Landschaften und erleichtern die Verwaltung großer Endpunktbestände. Besonders in heterogenen Umgebungen unterstützt die Inventarisierung dabei, den Überblick über eingesetzte Systeme und Anwendungen zu behalten.

Softwarebereitstellung und Patch-Management

Mit der baramundi Management Suite können Anwendungen zentral installiert, aktualisiert und entfernt werden. Auch komplexe Softwarepakete lassen sich automatisiert verteilen und verwalten. Ergänzend stellt baramundi mit Managed Software für zahlreiche Drittanbieter-Anwendungen getestete und verteilfertige Pakete bereit. Das integrierte Update Management unterstützt Unternehmen dabei, Windows- und Anwendungsupdates kontrolliert bereitzustellen, Sicherheitslücken zeitnah zu schließen und Softwarestände konsistent zu halten. Durch zentrale Steuerung, Automatisierung und transparente Statusrückmeldungen lassen sich Verwaltungsaufwände reduzieren und Update-Prozesse effizienter gestalten.

Ausführung von Administrationsaufgaben nahezu in Echtzeit

Administrationsaufgaben können zentral geplant und ausgeführt werden. Durch die direkte Kommunikation mit verwalteten Endpunkten erhalten Administratoren zeitnah Rückmeldungen über den Ausführungsstatus von Jobs. Dies vereinfacht die Steuerung von Änderungen, unterstützt eine schnelle Fehleranalyse und reduziert den manuellen Aufwand im täglichen Betrieb. Wartungsfenster und gezielte Jobsteuerung ermöglichen eine kontrollierte Ausführung auch in sensiblen Umgebungen.

Verwaltung heterogener Umgebungen

Die baramundi Management Suite unterstützt die zentrale Verwaltung unterschiedlicher Gerätetypen, Betriebssysteme und Konfigurationen. Neben Windows können – abhängig vom jeweiligen Funktionsumfang – auch macOS-, Linux-, Android- und iOS-Geräte sowie Netzwerkgeräte in einer gemeinsamen Management-Plattform abgebildet werden. Gerade in heterogenen Umgebungen hilft das, unterschiedliche Endgeräte zentral zu verwalten und Verwaltungsaufgaben effizienter zu organisieren. Die funktionale Tiefe unterscheidet sich je nach Plattform, wodurch die jeweiligen Besonderheiten der Betriebssysteme berücksichtigt werden können.





Linux-Management

baramundi unterstützt zahlreiche Linux-Distributionen und bietet Funktionen für Inventarisierung, Software-Paketmanagement und Skriptausführung. Individuell anpassbare Inventur-Templates ermöglichen die Erfassung zusätzlicher Informationen entsprechend den Anforderungen der jeweiligen Umgebung.

Darüber hinaus können Linux-Systeme zentral bereitgestellt, verwaltet und in bestehende Management-Prozesse integriert werden. Neben der Verwaltung installierter Systeme unterstützt baramundi auch die Installation und Bereitstellung neuer Linux-Geräte. So lassen sich Linux-Umgebungen effizient betreiben, standardisieren und in zentrale Verwaltungs- und Automatisierungsprozesse einbinden.

Automatisierung und Compliance

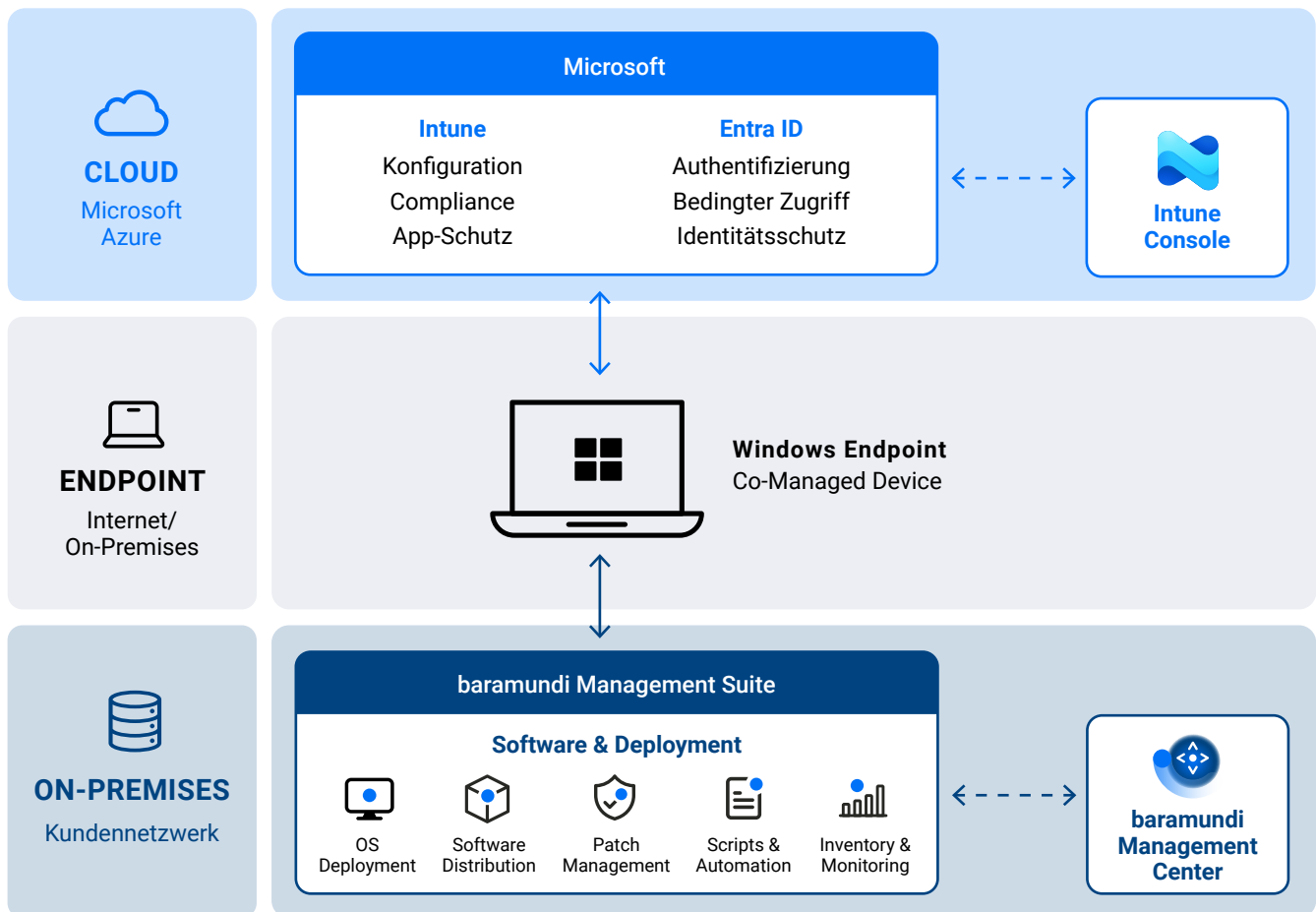
IT-Prozesse lassen sich mit der baramundi Management Suite automatisieren und standardisieren. Wiederkehrende Aufgaben wie Softwareverteilung, Patch-Management oder Konfigurationsanpassungen werden zentral gesteuert und regelbasiert ausgeführt. Integrierte Compliance-Funktionen überwachen kontinuierlich den Zustand von Endgeräten und machen Abweichungen von Unternehmensvorgaben transparent. So unterstützt die Lösung einen effizienten IT-Betrieb sowie die Einhaltung interner Sicherheits- und Compliance-Anforderungen.

Zentrale Verwaltung mehrerer Microsoft-Tenants

Die baramundi Management Suite unterstützt Co-Management-Szenarien mit mehreren Microsoft-Tenants. Intune- bzw. Entra-ID-bezogene Informationen können über die Tenant-Synchronisierung in der baramundi Management Suite verfügbar gemacht werden. Das hilft insbesondere Managed Service Providern und größeren Organisationen, co-verwaltete Endpunkte tenantübergreifend transparenter abzubilden und operative Prozesse zu vereinheitlichen.

Praktische Umsetzung von Co-Management

In der Praxis werden Windows-Clients über Microsoft Intune verwaltet, um beispielsweise Richtlinien bereitzustellen, Sicherheitsfunktionen zu nutzen oder cloudbasierte Zugriffskonzepte umzusetzen. Ergänzend übernimmt die baramundi Management Suite Aufgaben wie Betriebssystembereitstellung, Inventarisierung, Softwareverteilung, Update Management, Schwachstellenmanagement für Windows-Endpunkte sowie die Automatisierung von Verwaltungsprozessen. Auch Windows-Server können über baramundi verwaltet werden. So nutzen Unternehmen die jeweiligen Stärken beider Lösungen, ohne sich vollständig auf eine einzelne Management-Plattform festlegen zu müssen. Für heterogene Umgebungen bringt baramundi zusätzlich Funktionen für Linux-, macOS-, Android- und iOS-Endpunkte mit – jeweils abhängig vom verfügbaren Funktionsumfang der Plattform. Dadurch lassen sich unterschiedliche Endgerätetypen in eine gemeinsame Verwaltungsstrategie einbinden.



Grafische Darstellung der beiden Welten: Oben die Cloud mit Microsoft Entra ID und Intune, unten die On-Premises-Welt mit der baramundi Management Suite. Dazwischen steht ein moderner Windows-Client, der als Co-Managed Device über beide verwaltet wird.

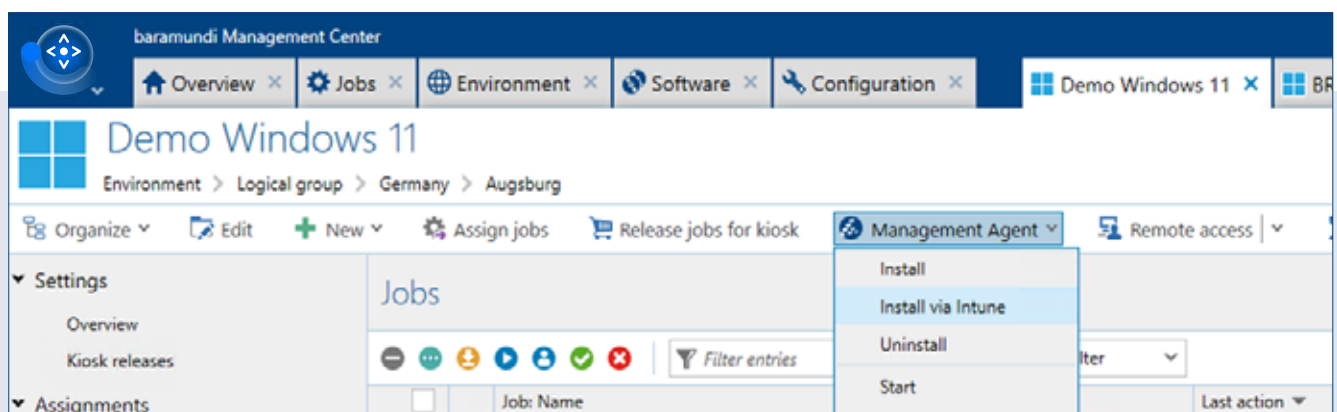
Unterschiedliche Endpoint Typen, welche durch die baramundi Management Suite verwaltet werden:

- Heterogene IT-Umgebungen mit Windows-, Linux- und macOS-Systemen sowie mobilen Endgeräten können in einer gemeinsamen Management-Plattform abgebildet werden.
- Die Verwaltung erfolgt abhängig vom jeweiligen Betriebssystem und dem verfügbaren Funktionsumfang.
- Inventarisierung, Softwareverteilung, Update Management, Skriptausführung, Compliance-Informationen und weitere Verwaltungsaufgaben lassen sich zentral steuern – je nach Plattform mit unterschiedlicher funktionaler Tiefe.
- Für Linux stehen unter anderem Inventarisierung, Software-Paketmanagement, Skriptausführung und ein einfaches OS-Deployment-Szenario zur Verfügung.

Microsoft Intune Connector in baramundi

Die Einrichtung des Co-Managements über den baramundi Microsoft Intune Connector erfolgt in mehreren Schritten: Zunächst werden die Geräte in die Intune-Verwaltung aufgenommen. Anschließend wird in der baramundi Management Suite die Synchronisierung von Microsoft Intune- bzw. Entra-ID-verwalteten Windows-Geräten eingerichtet.

Über die Aktion „Management Agent“ > „Installieren über Intune“ kann der baramundi Management Agent auf Intune-verwalteten Windows-Geräten verteilt werden. Dabei ist wichtig: Der Intune-/Entra-ID-Sync selbst ist nicht mit der Gateway-Anforderung für die spätere baramundi-Kommunikation gleichzusetzen. Für die Kommunikation des baramundi Management Agent außerhalb des Unternehmensnetzwerks kann – je nach Szenario – weiterhin eine passende Internet-/Gateway-Konfiguration erforderlich sein.



Nach erfolgreicher Installation des baramundi Management Agent können beide Systeme ihre jeweiligen Aufgaben im Co-Management-Szenario übernehmen: Intune für cloudbasierte Richtlinien, Compliance, Conditional Access und Modern-Management-Funktionen; baramundi für klassische UEM-Aufgaben wie Inventarisierung, Softwareverteilung, Update Management, Automatisierung und Betriebssysteminstallation.

baramundi Management im existierenden Intune Umfeld

IT-Abteilungen, die bisher Microsoft Entra ID und Intune im Einsatz haben, können bei neu hinzukommenden Windows-Geräten Co-Management mit baramundi aktivieren.

- ✓ Der Benutzer meldet sich in Windows an.
- ✓ Das Endgerät wird in Microsoft Entra ID aufgenommen.
- ✓ Das Endgerät wird durch Intune verwaltet.
- ✓ Die baramundi Management Suite synchronisiert die relevanten Geräteinformationen aus Intune bzw. Entra ID.
- ✓ Der baramundi Management Agent wird über Intune installiert.
- ✓ Das Endgerät kann anschließend in einem Co-Management-Szenario durch beide Lösungen genutzt werden.

Diese Vorgehensweise stellt sicher, dass Intune weiterhin für Modern-Management-Szenarien genutzt werden kann, während baramundi zusätzliche klassische UEM-Funktionen bereitstellt.

Job Name	Ergebnis	Letzte Aktion	Zustandsmeldung
1 SSA: Update-IntuneDeviceId-ellen-AutoPilotRegistration	OK	Vor 16 Minuten	Successfully finished at 19.02.2025 14:35:47
2 RUN: AutoPilotOOBE with BMA	OK	Vor 35 Minuten	Successfully finished at 19.02.2025 14:16:24
3 RUN: WindowsAutoPilotRegistration	OK	Vor 82 Minuten	Successfully finished at 19.02.2025 13:29:51
4 SSA: Set BMA dynamic mode	OK	Vor 2 Stunden	Successfully finished at 19.02.2025 13:02:27
5 RMUAI: Scan Online	OK	Vor 2 Stunden	Successfully finished at 19.02.2025 13:02:17
6 SET: Energy Full Power	OK	Vor 2 Stunden	Successfully finished at 19.02.2025 13:00:47
7 RMUAI: Scan & Update Online	OK	Vor 4 Stunden	Successfully finished at 19.02.2025 11:21:10
8 RUN: Microsoft Telemetry	OK	Vor 20 Tagen	Successfully finished at 30.01.2025 13:33:48
9 SSA: Intune scan last action result	OK	Vor 20 Tagen	Successfully finished at 30.01.2025 13:33:36
10 ✓ SSA: Intune Restart	OK	Vor 20 Tagen	Successfully finished at 30.01.2025 12:30:52
11 SSA: Intune Inventory	OK	Vor 20 Tagen	Successfully finished at 30.01.2025 12:28:58
12 RWI: Hard- & Software	OK	Vor 26 Tagen	Successfully finished at 24.01.2025 14:14:55
13 INST: Chrmid4 (MSW)	OK	Vor 3 Monaten	Successfully finished at 07.11.2024 11:35:50
14 INST: Shadid (MSW)	OK	Vor 3 Monaten	Successfully finished at 07.11.2024 11:34:52
15 INST: Adapic Reader (MSW)	OK	Vor 3 Monaten	Successfully finished at 07.11.2024 11:34:32
16 INST: Puffy id4 (MSW)	OK	Vor 3 Monaten	Successfully finished at 07.11.2024 11:32:42
17 INST: Notebook++ (MSW)	OK	Vor 3 Monaten	Successfully finished at 07.11.2024 11:32:39
18 RUN: Install-Certificates 1.0	OK	Vor 3 Monaten	Successfully finished at 07.11.2024 11:31:57
19 INST: Install (MSW)	OK	Vor 3 Monaten	Successfully finished at 07.11.2024 11:31:43
20 OS: Win11 24H2 PRO DE	OK	Vor 3 Monaten	Successfully finished at 07.11.2024 11:27:09

SSA: Intune Restart

Gerät: 0000-0011-14

Job: SSA: Intune Restart

Zustandsmeldung: Successfully finished at 30.01.2025 12:30:52

Initiator: Trier-Admin@baramundi.local

Startzeit: Vor 20 Tagen (30.01.2025 12:28)

Letzte Aktion: Vor 20 Tagen (30.01.2025 12:30)

Nextster Start: --

Priorität: 500

Voraussetzung ist erfüllt: Ja

Erfolgreiche Ausführungen: 1

Fehlgeschlagene Ausführungen: 0

Wiederholungen nach Fehler: 0

Abweichungen durch Benutzer: 0

Schritte

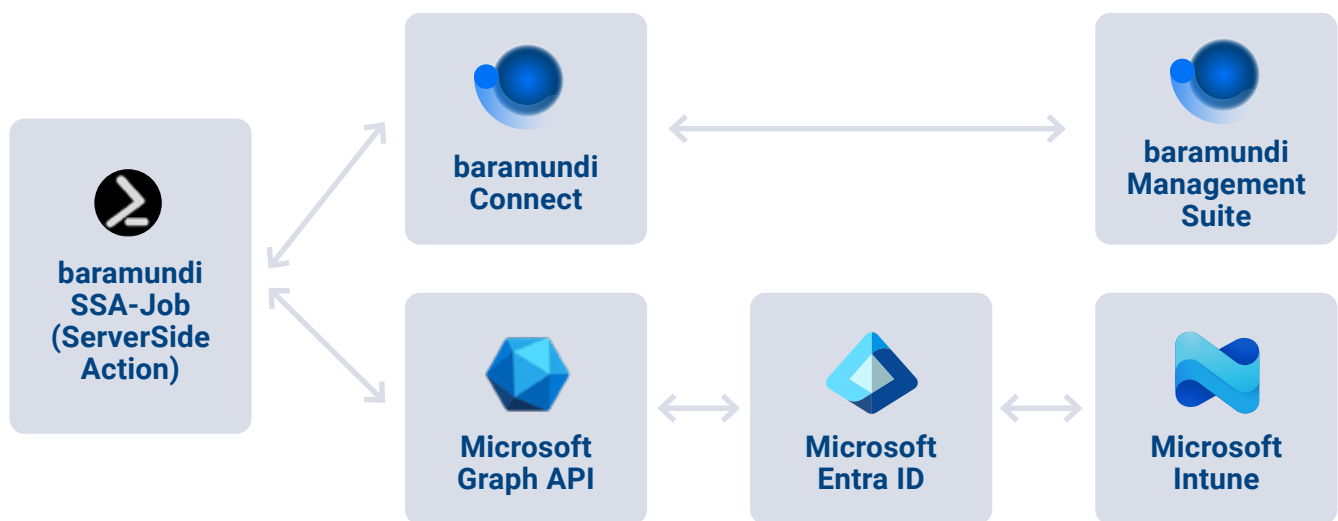
Beachten Sie: Nicht jeder Bereitstellungs- oder Registrierungsweg ist automatisch für Co-Management mit Intune geeignet. Wird ein Gerät über einen baramundi-spezifischen Bereitstellungsprozess vorbereitet, muss geprüft werden, ob die MDM-Verwaltung durch Intune weiterhin möglich bleibt. Für Co-Management-Szenarien sollte deshalb ein Bereitstellungsweg gewählt werden, bei dem Intune den Zugriff auf die Modern-Management-Funktionen behält.

Integration und Datensynchronisierung zwischen baramundi und Intune

Über Microsoft Graph und die baramundi-Schnittstellen können ausgewählte Intune- und Entra-ID-Informationen in der baramundi Management Suite verfügbar gemacht werden. Dazu zählen insbesondere synchronisierte Endgeräte sowie verfügbare Geräteattribute, die in baramundi weiterverwendet werden können. baramundi unterstützt außerdem Co-Management-Szenarien mit mehreren Microsoft-Tenants und Entra-ID-Gruppen. Damit lassen sich tenantübergreifende Umgebungen, etwa bei Managed Service Providern oder größeren Organisationen, transparenter abbilden.

Damit entsteht keine vollständige gegenseitige Steuerung beider Managementsysteme, sondern eine gezielte Integration für klar definierte Co-Management-Szenarien. Intune bleibt die Instanz für cloudbasierte Richtlinien, Conditional Access und Microsoft-spezifische Remote-Aktionen; baramundi ergänzt diese Szenarien durch Inventarisierung, Softwareverteilung, Update Management, Automatisierung, OS-Installation und die zentrale operative Sicht auf co-verwaltete Endpunkte.

Co-Management



Damit sind Daten aus Intune jetzt auch in der baramundi Management Suite abrufbar

Durch die Synchronisierung können ausgewählte Informationen aus Microsoft Intune und Microsoft Entra ID in der baramundi Management Suite sichtbar gemacht und für operative Prozesse genutzt werden. Dazu gehören – abhängig von Konfiguration und Release-Stand – synchronisierte Geräte, verfügbare Geräteattribute sowie Informationen aus angebotenen Tenants und Entra-ID-Gruppen.

Wichtig ist die technische Abgrenzung: Die Synchronisierung macht relevante Daten in baramundi verfügbar, ersetzt aber nicht die Verwaltungslogik von Intune und bedeutet keine vollständige bidirektionale Steuerung beider Systeme. Sie bildet vielmehr die Grundlage, um co-verwaltete Endpunkte in der baramundi Management Suite transparenter darzustellen und ausgewählte Prozesse besser zu unterstützen.

Co-Management Use Case: Remote-Aktion für ein verlorenes Windows-Gerät

Ein Co-Management-Szenario kann IT-Teams dabei unterstützen, zeitkritische Aufgaben schneller einzuordnen und auszuführen. Ein Beispiel ist der Umgang mit einem verlorenen Windows-Gerät: Intune stellt hierfür Remote-Aktionen wie Wipe, Retire oder weitere gerätebezogene Aktionen bereit. In einem integrierten Szenario können solche Aktionen organisatorisch mit den Informationen und Prozessen aus der baramundi Management Suite zusammengedacht werden.

Welche Intune-Aktionen direkt aus der baramundi Management Suite heraus verfügbar sind, hängt vom eingesetzten Release, der Konfiguration und der Freigabe der jeweiligen Funktion ab. Destruktive Aktionen wie Wipe, Retire, Fresh Start oder Autopilot Reset sollten immer eine explizite Bestätigung erfordern und abhängig vom Join-Status, Gerätekontext und internen Sicherheitsprozess bewertet werden. So bleibt Intune die ausführende Instanz für Microsoft-spezifische Remote-Aktionen, während baramundi zusätzliche Transparenz und operative Einordnung liefern kann.



Neue Endgeräte ausliefern

Entra ID/Intune Only – Intune|baramundi Enrollment ohne lokales Active Directory

Unternehmen, die neue Windows-Geräte ohne lokales Active Directory bereitstellen möchten, können Co-Management mit Intune und baramundi nutzen, um moderne Cloud-Registrierung mit klassischen UEM-Prozessen zu verbinden. Ziel ist es, Geräte kontrolliert vorzubereiten, mit Software und Konfigurationen auszustatten und anschließend für die Nutzung über Entra ID und Intune bereitzustellen.

Ein möglicher Bereitstellungsansatz sieht vor, dass Windows-Geräte zunächst über baramundi OS Deployment aufgesetzt werden. Anwendungen, Konfigurationen und Updates können anschließend über die baramundi Management Suite verteilt werden. Für Autopilot- bzw. OOBESzenarien kann die Registrierung in Microsoft Entra ID und Intune in den Bereitstellungsprozess eingebunden werden. So lassen sich etablierte UEM-Prozesse mit modernen Cloud-Management-Szenarien kombinieren und neue Endgeräte effizient für den produktiven Einsatz vorbereiten.

Stärken nutzen – Zeit und Aufwand sparen

Das stärkste Argument für Co-Management von baramundi und Intune: IT-Teams können bestehende Prozesse weiter nutzen und gleichzeitig moderne Cloud-Funktionen gezielt ergänzen.

- ✓ Sie behalten co-verwaltete Endpunkte zentral im Blick,
- ✓ automatisieren wiederkehrende Aufgaben,
- ✓ nutzen je nach Szenario die passende Stärke von baramundi oder Intune,
- ✓ steuern Aufgaben rollenbasiert und mit möglichst wenigen notwendigen Rechten,
- ✓ reduzieren Konsolenwechsel dort, wo Informationen und ausgewählte Aktionen in der baramundi Management Suite zusammengeführt werden,
- ✓ schaffen eine Brücke zwischen klassischer Endgeräteverwaltung und modernen Cloud- sowie Conditional-Access-Szenarien.

Viele Unternehmen arbeiten heute mit hybriden On-Premises- und Cloud-Infrastrukturen, um mobile, externe und klassische Arbeitsumgebungen sicher und effizient zu unterstützen. Dafür benötigen IT-Administratoren flexible Werkzeuge, mit denen sie Endgeräte kontrolliert verwalten, absichern und aktuell halten können.

Die Kombination aus baramundi Management Suite und Microsoft Intune bietet dafür einen praxisnahen Ansatz: Intune ergänzt moderne Cloud-, Richtlinien- und Zugriffssteuerungsfunktionen, während baramundi bewährte UEM-Funktionen wie Inventarisierung, Softwareverteilung, Update Management, Automatisierung und OS-Installation bereitstellt. Co-Management schafft damit mehr Flexibilität in der Endgeräteverwaltung – ohne bewährte Prozesse vorschnell aufzugeben.

Unternehmen, die ihre Endgeräteverwaltung modernisieren möchten, können Co-Management nutzen, um bestehende baramundi-Prozesse gezielt mit cloudbasierten Intune-Funktionen zu kombinieren. So entsteht ein flexibler Verwaltungsansatz, der klassische IT-Betriebsmodelle und moderne Cloud-Szenarien pragmatisch verbindet.

Über die baramundi software GmbH

Die baramundi software GmbH sorgt als Spezialist für Unified Endpoint Management (baramundi Management Suite) und Proactive Endpoint Operations (baramundi Proactive Hub) dafür, dass Unternehmen und Organisationen effizient, sicher und plattformübergreifend Arbeitsumgebungen und digitale Arbeitsplätze managen – On-Prem und in der Cloud. Der Hauptsitz der baramundi software GmbH befindet sich in Augsburg. Die Produkte und Services des im Jahr 2000 gegründeten Unternehmens sind komplett Made in EU. Beim Vertrieb, der Beratung und Betreuung von Kunden arbeitet baramundi weltweit erfolgreich mit Partnerunternehmen zusammen.

www.baramundi.com



Sie möchten mehr über die baramundi Management Suite erfahren?

Melden Sie sich zum Live-Webinar an! Erleben Sie im kostenfreien Webinar, wie Sie die baramundi Management Suite Ihre Endpoints, Server und Mobilgeräte automatisiert verwaltet und absichert.

<https://www.baramundi.com/de-de/it-training/webinare/>

Kontaktieren Sie uns.

Wir freuen uns auf Sie!



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



+43 1 928 0136 0010
request@baramundi.com



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



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



+49 821 56708-390
request@baramundi.com



Making IT Admins Smile