ALLGEMEINE ERLÄUTERUNGEN

WAS IST MICROSOFT INTUNE?

Microsoft Intune ermöglicht es Organisationen **IT-Infrastrukturen** effektiv zu verwalten und zu sichern.

- **Geräteverwaltung (Mobile Device Management, MDM)**
- **Anwendungsmanagement (Mobile Application Management, MAM)**
- **Sicherheits- und Compliance-Management**
- **Konfigurationsmanagement**

GERÄTEVERWALTUNG (MDM)

Die nachfolgenden Ausführungen beziehen sich auf eine allgemeine Geräteverwaltung. Intunes findet sowohl für dienstliche Laptops, wie auch bei mobilen Smartphones Anwendung.

Registrierung von Geräten:
Unternehmen können Geräte zentral über Intune registrieren und verwalten.

Richtlinienerstellung:
IT-Administratoren können Richtlinien für Sicherheitsanforderungen, wie z. B. Gerätesperren, Passwortkomplexität und Verschlüsselung, erstellen. Spezifische Anmerkungen und Unterscheidungen finden Sie auf Folie 9.

Überwachung und Verwaltung:
Intune überwacht Geräte auf Konformität mit Unternehmensrichtlinien und ermöglicht es Administratoren, Aktionen wie das Sperren oder Zurücksetzen von Geräten aus der Ferne durchzuführen. Spezifische Anmerkungen und Unterscheidungen finden Sie auf Folie 9.

Unterstützung für BYOD (Bring Your Own Device):
Mitarbeiter können ihre eigenen Geräte nutzen, wobei private und geschäftliche Daten getrennt verwaltet werden.

ANWENDUNGSVERWALTUNG (MAM)

Die nachfolgenden Ausführungen beziehen sich auf eine allgemeine Geräteverwaltung. Intunes findet sowohl für dienstliche Laptops, wie auch bei mobilen Smartphones Anwendung.

Verteilung von Anwendungen:
Unternehmen können Anwendungen über das Intune-Portal bereitstellen und verwalten.

Anwendungsschutzrichtlinien:
Schutz von Unternehmensdaten in Anwendungen, wie z. B. durch Verhinderung des Kopierens und Einfügens von Unternehmensdaten in private Anwendungen oder Oberflächen/Betriebssysteme.

Verwaltung auf Anwendungsebene:
Intune schützt Unternehmensdaten auf privaten Geräten (BYOD Szenario), indem es Richtlinien nur auf bestimmte Anwendungen anwendet, nicht auf das gesamte Gerät.

SICHERHEITS- UND COMPLIANCE-MANAGEMENT

Die nachfolgenden Ausführungen beziehen sich auf eine allgemeine Geräteverwaltung. Intunes findet sowohl für dienstliche Laptops, wie auch bei mobilen Smartphones Anwendung.

Sicherheitsrichtlinien:
Administratoren können Sicherheitsrichtlinien festlegen, um den Zugriff auf Unternehmensdaten zu steuern und sicherzustellen, dass nur konforme Geräte auf Unternehmensressourcen zugreifen.

Integration mit Azure Active Directory (AAD):
Ermöglicht bedingten Zugriff basierend auf Geräte- und Benutzerstatus.

Datenschutz:
Intune sorgt dafür, dass Unternehmensdaten geschützt werden, ohne auf persönliche Informationen zuzugreifen.

KONFIGURATIONSMANAGEMENT

Die nachfolgenden Ausführungen beziehen sich auf eine allgemeine Geräteverwaltung. Intunes findet sowohl für dienstliche Laptops, wie auch bei mobilen Smartphones Anwendung.

WLAN- und VPN-Profile:
Automatische Bereitstellung von Netzwerkeinstellungen, damit sich Mitarbeiter sicher und effizient mit den Unternehmensressourcen verbinden können.

E-Mail-Profile:
Intune konfiguriert und schützt E-Mail-Zugänge auf mobilen Geräten und PCs, ohne dass Benutzer manuell etwas einstellen müssen.

ERLÄUTERUNGEN ZU BYOD/COPE*

*BYOD: Bring your own device (Eigenes Gerät)
*COPE: Corporate Owned, Personally Enabled (Gerät gehört dem Bistum und darf gegen Gebühr privat genutzt werden)

SONDERFALL BYOD/COPE

Daten, die Intune auf BYOD-/COPE-Geräten auslesen kann:

- Geräteinformationen (Art des Smartphones, Betriebssystem)
- Anwendungsinformationen (Nutzung von Apps über Intune – Nicht, was generell installiert wurde)
- Sicherheitsrichtlinien und Compliance (generell 6-stelliger PIN statt 4, keine Andorid Version unter Version 12, keine IOS-Version unter Version 12 zur Gewährleistung der Gerätesicherheit)
- Netzwerkverbindungen (Erkennung von betriebsinternen WLAN)

SONDERFALL BYOD/COPE

Daten, die Intune auf BYOD-/COPE-Geräten NICHT auslesen kann:

- Persönliche E-Mails und SMS
- Kontakte, Fotos, Videos und Dateien
- Standortdaten
- App-Nutzung oder -Daten
- Telefonanrufe und sonstige Kurznachrichten (z.B iMessage, WhatsApp)

SONDERFALL BYOD/COPE

Wie schützt Intune persönliche Daten?

- **Getrennte Datenspeicherung:**

Unternehmensdaten werden in verwalteten Anwendungen isoliert, wodurch persönliche Daten unberührt bleiben.

- **Kein Zugriff auf persönliche Anwendungen:**

Intune kann private Apps weder installieren noch deinstallieren oder verwalten. Es verwaltet nur spezifische, vom Unternehmen bereitgestellte Anwendungen.

- **Remote-Löschung:**

Bei Verlust oder Diebstahl eines BYOD-/Cope-Geräts kann Intune nur Unternehmensdaten aus der Ferne löschen, während persönliche Daten wie Fotos oder private Dokumente unberührt bleiben.

FRAGEN

FRAGEN

„Erfolgt eine Gerätesperrung/Zurücksetzung auf Werkzustand nach mehrmaliger falscher Eingabe des PINs?“

BYOD/COPE*: Es gibt keine Zurücksetzung auf Werkzustand des Geräts oder von Daten bei mehrmaliger Falscheingabe des Codes. Lediglich die Auslösung der Abmeldung der Intune-Anwendungen ist möglich.

COBO*: COBO-Geräte werden nach 5-maliger Falscheingabe des Codes auf Werkseinstellung zurückgesetzt. Daten, die nicht in der Cloud oder auf entsprechenden Laufwerken liegen, gehen verloren.

*BYOD: Bring your own device (Eigenes Gerät)
*COPE: Corporate Owned, Personally Enabled (Gerät gehört dem Bistum und darf gegen Gebühr privat genutzt werden)
*COBO: Corporate Owned, Business Only (Gerät gehört dem Bistum und darf nur geschäftlich genutzt werden)

FRAGE

„Können private Daten über Intune tatsächlich technisch nicht ausgelesen werden? Oder ist es so konfiguriert, dass es nicht geht und bei Anpassung der Konfiguration würde es ggf. doch gehen?“

Bei BYOD und COPE wird eine "Containerlösung" genutzt. Arbeitsdaten sind von den privaten Daten strikt getrennt. Das Einsehen von privaten Daten auf den Endgeräten ist **technisch nicht möglich** und könnte nicht konfiguriert werden.

COBO: Auch hier kann nicht auf Daten zugegriffen werden, lediglich wie auch im BYOD/COPE Szenario die Parameter, welche zur Erfüllung der Sicherheit notwendig sind.
Einzige Ausnahme: Da die Anwendungen auf COBO-Geräten restriktiv sind, können alle Apps des Geräts eingesehen werden. Es dürfen nur selektierte Apps aus dem iOS/Android App Store installiert werden.

„Wenn ich in Outlook bspw. Ein Bild hochlade und somit den Zugriff auf meine Bildergalerie freigebe, kann dann immer auf die Bildergalerie zugegriffen werden?“

Der Zugriff muss aktiv vom Inhaber freigegeben werden. Die Freigabe kann verwaltet werden. Die Freigabe ist eine Einbahnstraße. Die IT ist auch dadurch nicht in der Lage die Bildergalerie einzusehen.

Nachfolgend wird die Administrationsansicht eines BYOD-Geräts bebildert.

Marius | Hardware

Search

Overview
Manage
Properties
Monitor
Hardware
Discovered apps
Device compliance
Device configuration
App configuration
Recovery keys
Group membership
Managed Apps
Filter evaluation
Enrollment

System

Name	Marius
Management name	m.endries_IPhone_5/24/2024_9:48 AM
UDID	
Intune Device ID	6414c247-85d0-4a93-b523-26bc82432632
Microsoft Entra Device ID	746adbf9-f3df-4719-8ef1-6aea03f5d281
Serial number	FCJCJ155N70R
Apple Shared iPad	No
Enrollment profile	

Operating system

Operating system	iOS/iPadOS
Operating system version	18.1.1
Operating system language	
Operating system edition	
Security patch level	

Storage

Total storage space	64.00 GB
Free storage space	7.34 GB
Total physical memory	
Resident users	

System enclosure

IMEI	353909108881157
MEID	35390910774916
Manufacturer	Apple
Model	iPhone 11 Pro Max
Product name	iPhone12,5
Processor Architecture	Unknown
Phone number	+*********0164
Battery level	89%

Network details

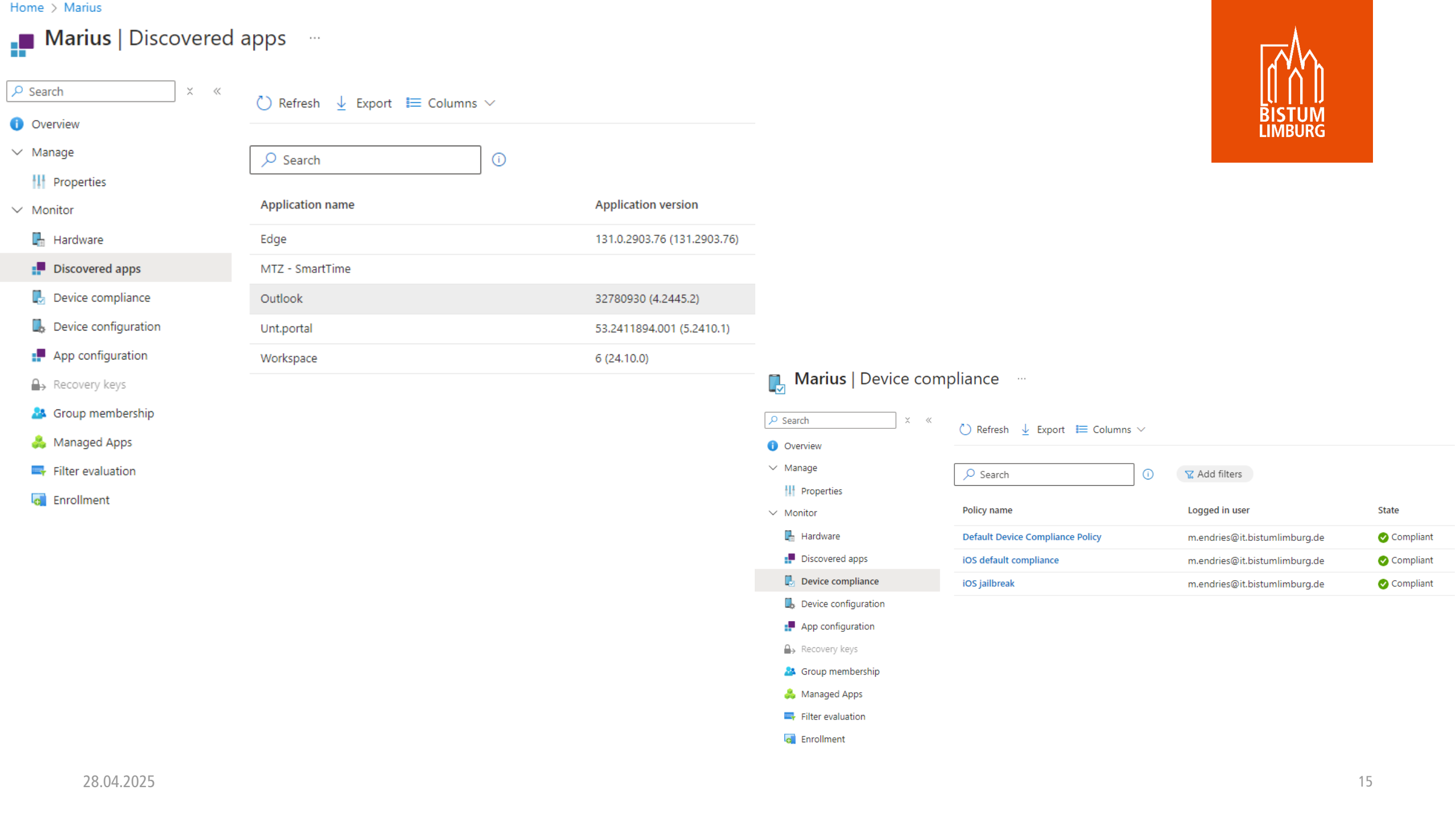
Subscriber carrier	Telekom.de
Cellular technology	None
Wi-Fi MAC	bc09636ac970
Ethernet MAC	
ICCID	8949 0200 0019 6626 9790
EID	89049032005008882600046732635969
Wi-Fi IPv4 address	
Wi-Fi subnet ID	
Wired IPv4 address	

Network service

Enrolled date	24.5.2024, 11:48:05
Last contact	5.12.2024, 14:38:37

Conditional access

Activation lock bypass code	
Microsoft Entra registered	Yes
Compliance	Compliant
EAS activated	Yes
EAS activation ID	T0BQRBH5J56QTBG1SDG8UJSOU0
EAS activation time	24.5.2024, 11:48:54
Supervised	No
Encrypted	Yes
Jailbroken	False


Home > Marius
Marius | Discovered apps
Search
Overview
Manage
Properties
Monitor
Hardware
Discovered apps
Device compliance
Device configuration
App configuration
Recovery keys
Group membership
Managed Apps
Filter evaluation
Enrollment
Refresh
Export
Columns
Search
Application name
Application version
Edge
131.0.2903.76 (131.2903.76)
MTZ - SmartTime
Outlook
32780930 (4.2445.2)
Unt.portal
53.2411894.001 (5.2410.1)
Workspace
6 (24.10.0)
Marius | Device compliance
Search
Overview
Manage
Properties
Monitor
Hardware
Discovered apps
Device compliance
Device configuration
App configuration
Recovery keys
Group membership
Managed Apps
Filter evaluation
Enrollment
Refresh
Export
Columns
Search
Add filters
Policy name
Logged in user
State
Default Device Compliance Policy
m.endries@it.bistumlimburg.de
Compliant
iOS default compliance
m.endries@it.bistumlimburg.de
Compliant
iOS jailbreak
m.endries@it.bistumlimburg.de
Compliant

FRAGE

„Kann ich mich nicht einfach auf einem Privatgerät über die Standard-M365 App mit meinen Daten einloggen?“

Das Anmelden an den Standard M365 Apps ist nur von kompatiblen Geräten gestattet. Dazu zählen:

- Intune registrierte Windows Geräte (Die Intune Registrierung kann nur an Geräten, welche von der IT ausgegeben wurden, erfolgen.)
- Intune registrierte Android/iOS Geräte (Hierzu erhalten User, welche ein Dienstgerät besitzen oder einen BYOD-Antrag gestellt haben Berechtigung.)

Der Zugriff von privaten Endgeräten ist nur via Weboberfläche möglich, ohne die Möglichkeit Daten aus Sharepoint/OneDrive etc. herunterzuladen.

FRAGE

„Können Dateien aus der Intune Umgebung auf mein BYOD-Gerät runtergeladen werden oder Texte rauskopiert und in bspw. WhatsApp eingefügt werden?“

Das Kopieren und Speichern von Textpassagen und/oder Dateien aus der "Intune Umgebung" in die private Umgebung wurde mit einer Richtlinie für alle BYOD-Geräten unterbunden und ist somit nicht möglich.