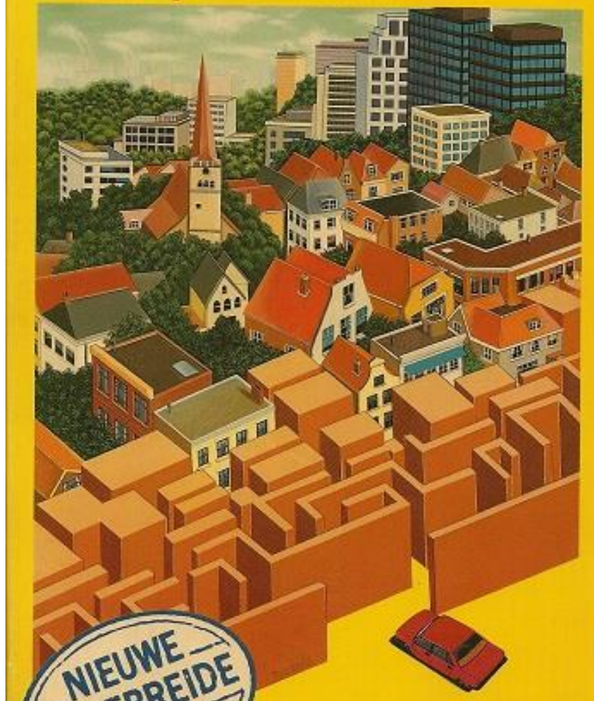
Navigating the landscape of RBAC roles in Microsoft Intune

WORKPLACEDUDES SUMMIT 2024

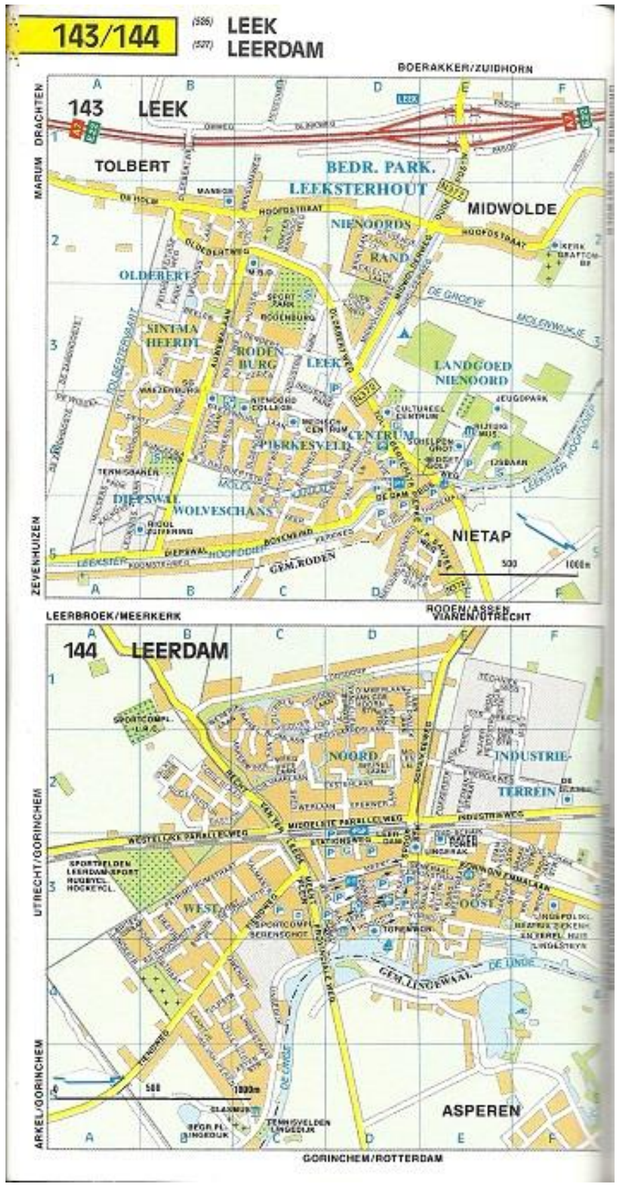
LUDWIG

HET 80.000 STRATENBOEK

Met plattegronden van 122 steden en een register met 80.000 straten.



NIEUWE UITGEBREIDE EDITIE



Who Am I

Ruud Gijsbers Rademakers

Modern Work Technologist & Technical Architect

Working for Avanade since 2018

Working in IT since 1999

avanade

Agenda

Brief introduction to Intune

Different RBAC Roles

How to apply the RBAC Roles

Demo

Questions

Brief introduction to Intune

Microsoft Intune
Self-Service
Remote and hybrid workers
Reporting and data
Intune Suite
Advanced endpoint analytics
Endpoint Privilege Management
Microsoft Tunnel for Mobile Application Management
Remote help
Specialized devices management
Web-based admin center
Apps
Deployment
Updates
Protection
Removal
Identities
Management
Security
Custom roles
Policy assignment
Devices
Compliance
Conditional access
Device configuration
BYOD and org-owned devices
Integration
Configuration Manager
Windows Autopilot
Microsoft Defender for Endpoint
Windows Autopatch
Endpoint Analytics
Microsoft 365
VPN and Microsoft Tunnel
Managed Google Play
Apple tokens
TeamViewer
Mobile threat defense services
Endpoint Security
Zero Trust

Different RBAC Roles

Microsoft Entra roles with Intune access

Global Administrator

Intune Service Administrator

Microsoft Entra roles with Intune access

Global Administrator

Intune Service Administrator

Security Administrator

Security Operator

Security Reader

Global Reader

Helpdesk administrator

Microsoft Entra roles with Intune access

Global Administrator

Intune Service Administrator

Security Administrator

Security Operator

Security Reader

Global Reader

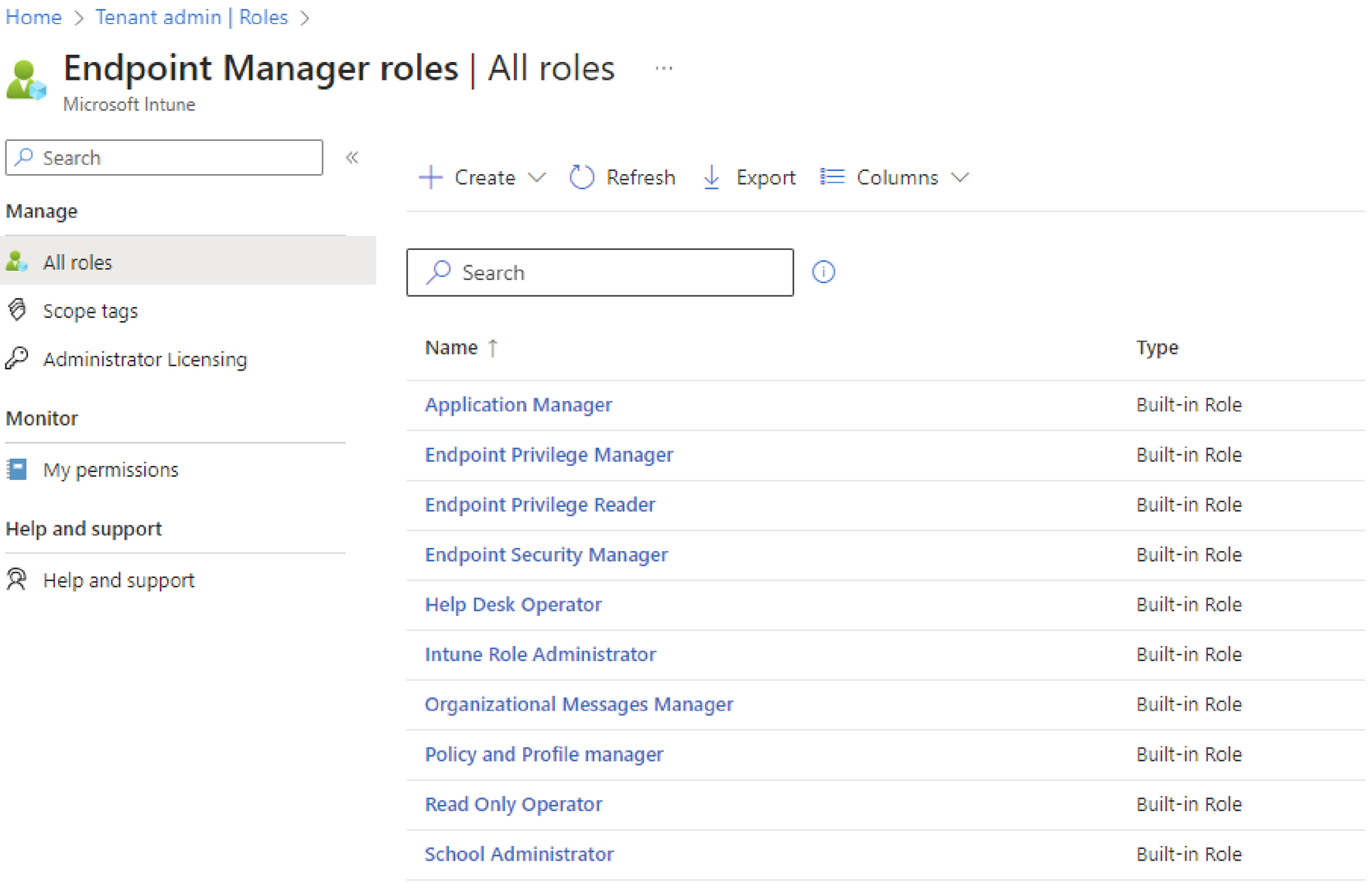
Helpdesk administrator

Compliance Administrator

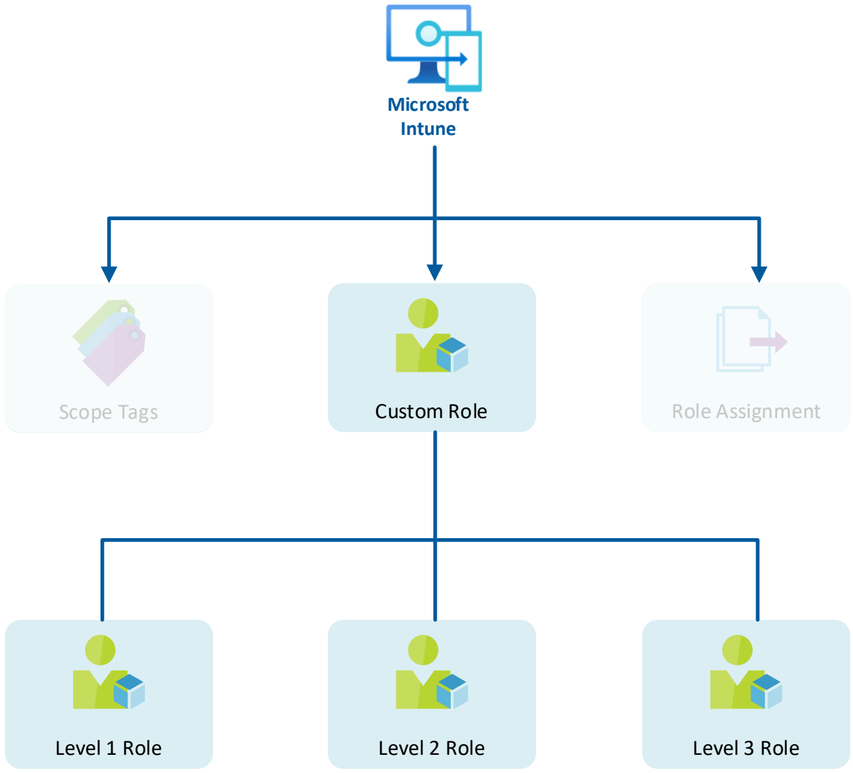
Compliance Data Administrator

Reports Reader

Built-In Roles



Custom Roles

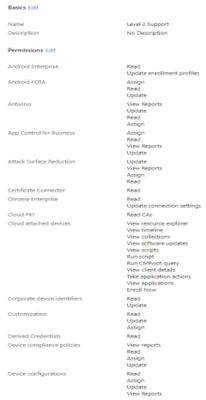


Basics Edit

Name	Level 1 Support
Description	No Description

Permissions Edit

Android Enterprise	Read
Android FOTA	Read
Antivirus	View Reports Read
App Control for Business	Read View Reports
Attack Surface Reduction	View Reports Read
Certificate Connector	Read
Chrome Enterprise	Read
Cloud PKI	Read CAs
Cloud attached devices	View resource explorer View timeline View collections View software updates View scripts View client details View applications
Corporate device identifiers	Read
Customization	Read
Derived Credentials	Read
Device compliance policies	View reports Read
Device configurations	Read View Reports

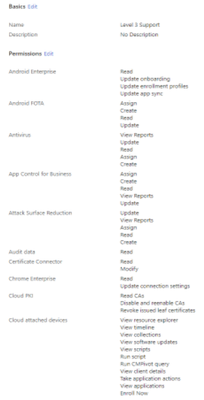


Basics Edit

Name	Level 2 Support
Description	No Description

Permissions Edit

Android Enterprise	Read Update enrollment profiles
Android FOTA	Assign Read Update
Antivirus	View Reports Update Read Assign
App Control for Business	Assign Read View Reports Update
Attack Surface Reduction	Update View Reports Assign Read
Certificate Connector	Read
Chrome Enterprise	Read Update connection settings
Cloud PKI	Read CAs
Cloud attached devices	View resource explorer View timeline View collections View software updates View scripts Run script Run ChxPivot query View client details Take application actions View applications Enroll Now
Corporate device identifiers	Read Update
Customization	Read Update Assign
Derived Credentials	Read
Device compliance policies	View reports Read Assign Update
Device configurations	Read Assign Update View Reports



Basics Edit

Name	Level 3 Support
Description	No Description

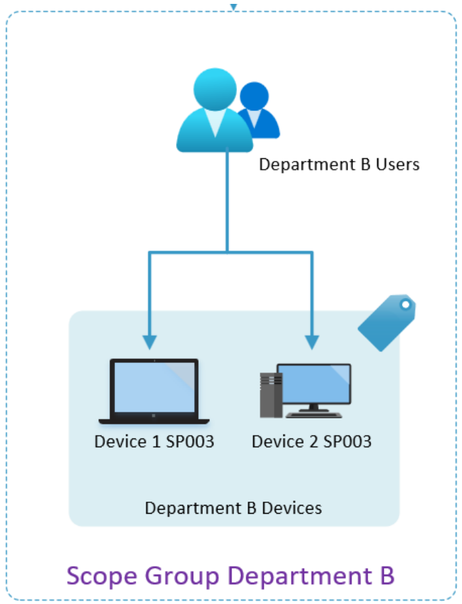
Permissions Edit

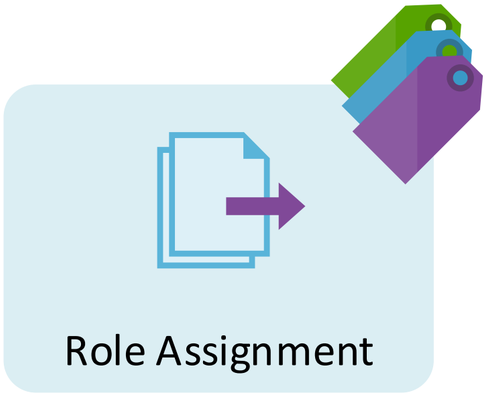
Android Enterprise	Read Update onboarding Update enrollment profiles Update app sync
Android FOTA	Assign Create Read Update
Antivirus	View Reports Update Read Assign Create
App Control for Business	Assign Create Read View Reports
Attack Surface Reduction	Update View Reports Assign Read Create
Audit data	Read
Certificate Connector	Read Modify
Chrome Enterprise	Read Update connection settings
Cloud PKI	Read CAs Disable and reenable CAs Revoke issued leaf certificates
Cloud attached devices	View resource explorer View timeline View collections View software updates View scripts Run script Run ChxPivot query View client details Take application actions View applications Enroll Now

How to apply the RBAC Roles

Intune Scope Groups, Roles and Role Assignments

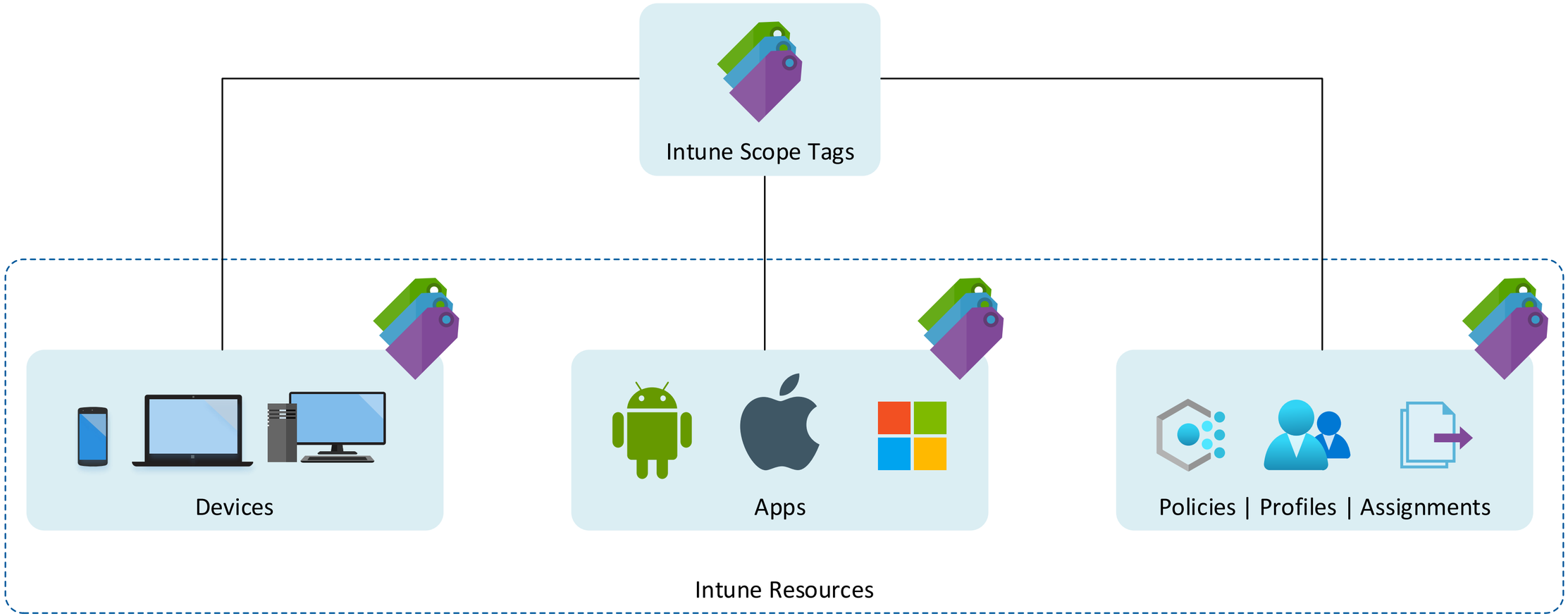
Scope Tags



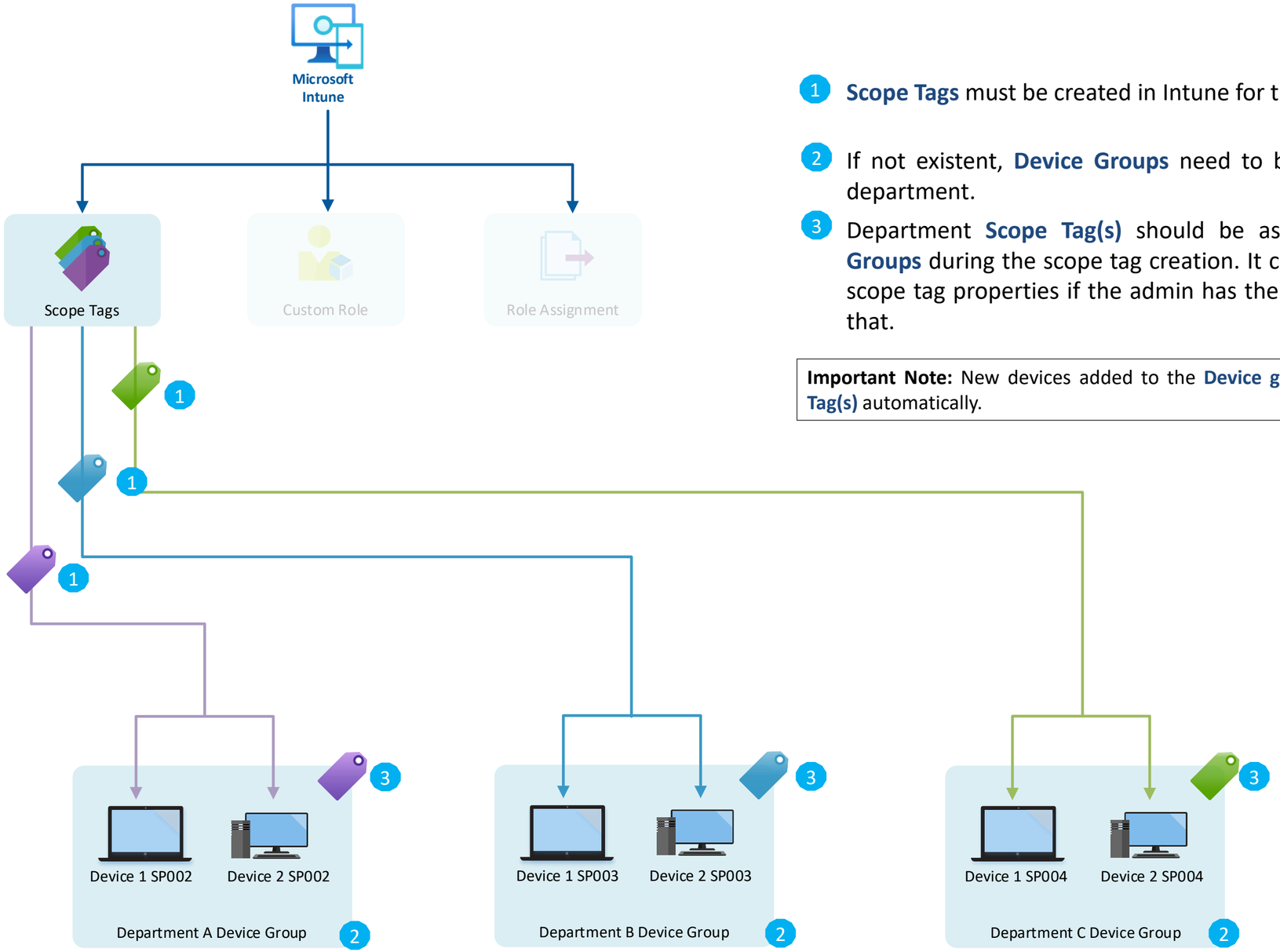


Role Assignment

Intune Tags


Intune Scope Tags
Devices
Apps
Policies | Profiles | Assignments
Intune Resources

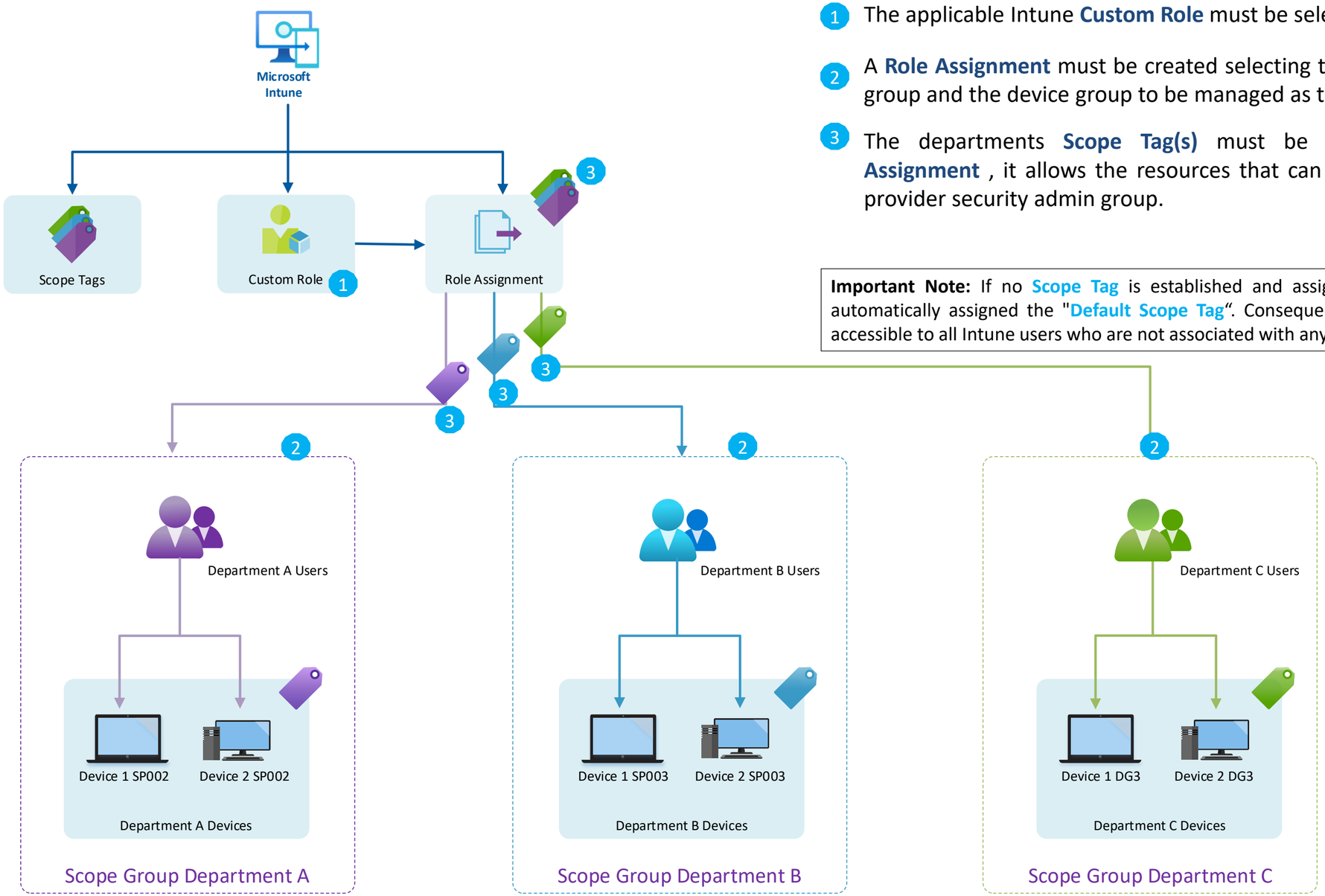
Applying scope tags to Device Groups



1. **Scope Tags** must be created in Intune for the different departments
2. If not existent, **Device Groups** need to be created in AAD for each department.
3. Department **Scope Tag(s)** should be assigned in Intune to **Device Groups** during the scope tag creation. It can also be edited later in the scope tag properties if the admin has the necessary permissions to do that.

Important Note: New devices added to the **Device groups** will get the assigned **Scope Tag(s)** automatically.

Applying scope tags to Scope Groups



1. The applicable Intune **Custom Role** must be selected.
2. A **Role Assignment** must be created selecting the departments admin group and the device group to be managed as the **Scope Group**.
3. The departments **Scope Tag(s)** must be selected to the **Role Assignment** , it allows the resources that can be seen by the service provider security admin group.

Important Note: If no **Scope Tag** is established and assigned to a device, it will be automatically assigned the "**Default Scope Tag**". Consequently, the device will become accessible to all Intune users who are not associated with any specific **Scope Group**.

Demo

DANK AAN ONZE SPONSORS

DANK AAN ONZE SPONSORS

infinity

PATCH MY PC

LIQUIT

Part of RECAST SOFTWARE

venéco

Moving you *forward*

Questions