



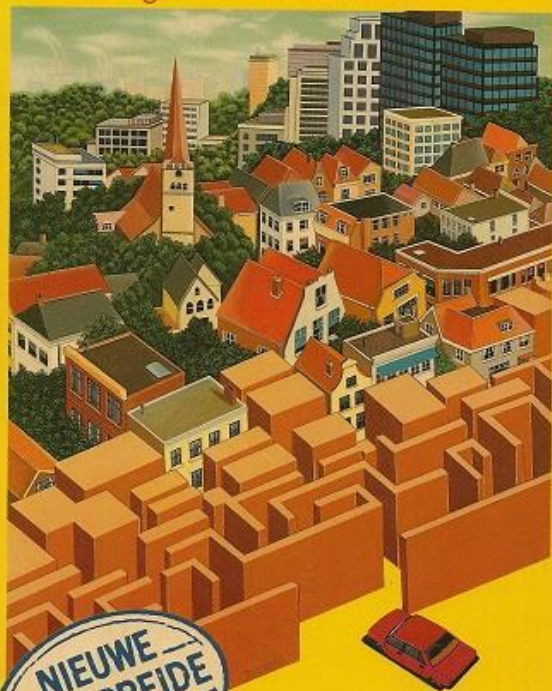
Navigating the landscape of RBAC
roles in Microsoft Intune

Ruud Gijsbers Rademakers

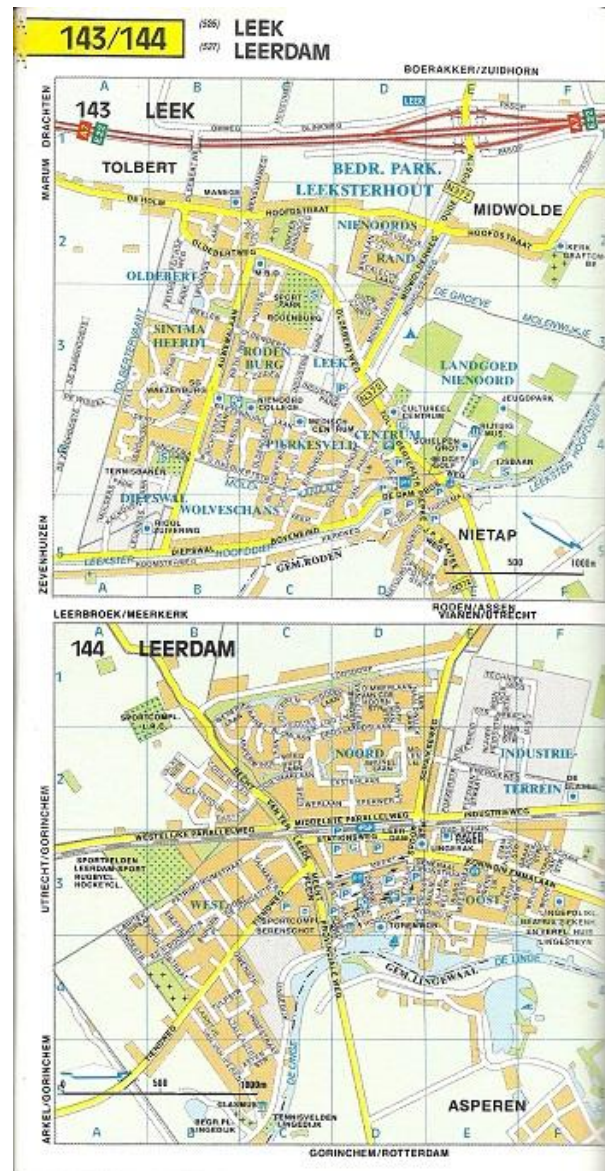


HET 80.000 STRATENBOEK

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





Agenda

What is Intune

Different RBAC Roles

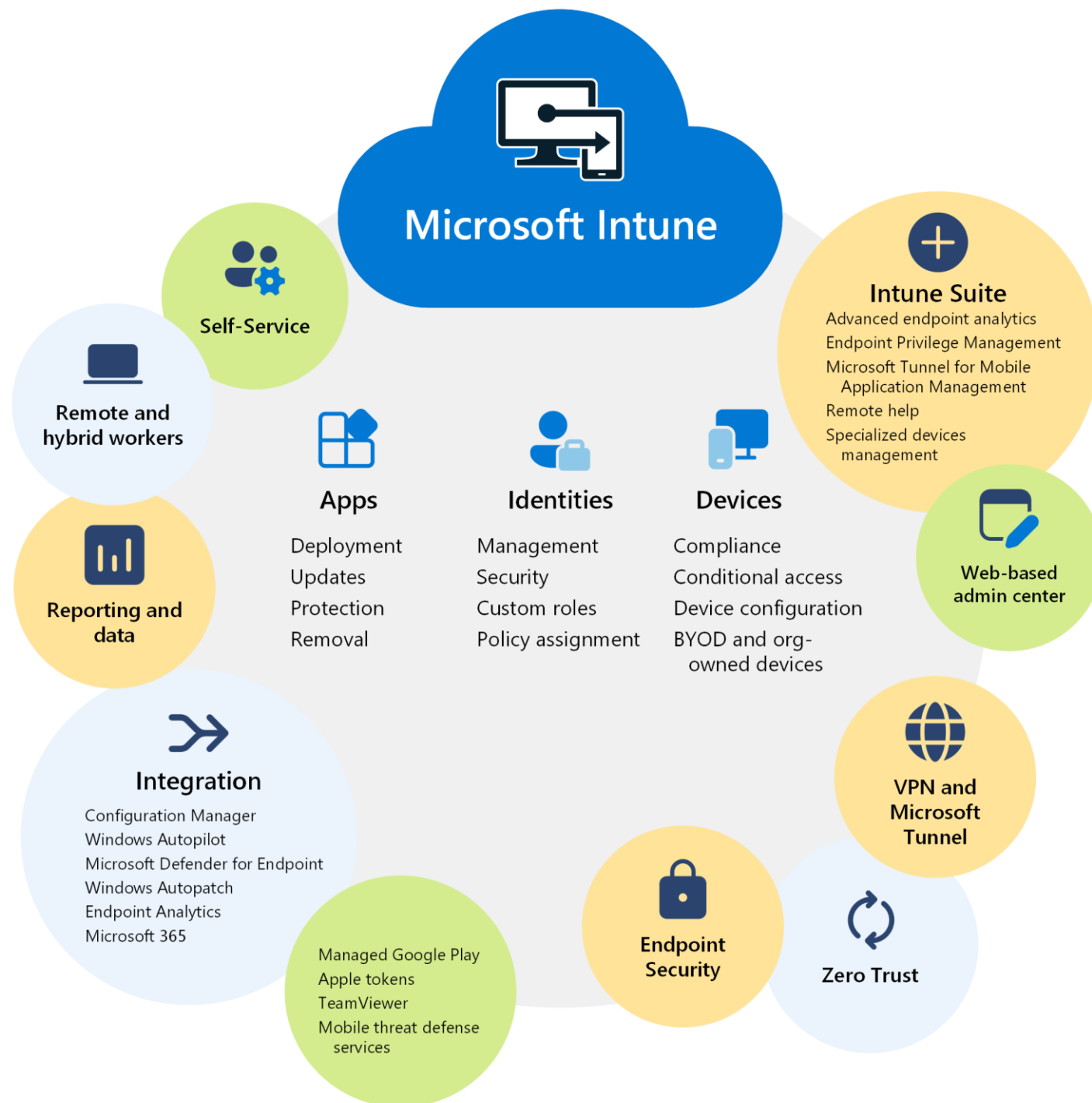
How to apply the RBAC Roles

Demo

Questions

The background features two large, decorative, curved lines. One line, in shades of blue and green, curves from the top right towards the center. Another line, in shades of green and blue, curves from the bottom left towards the center. The text is centered between these two curves.

What is Intune



The background features two large, decorative, curved lines. One line, in shades of blue and green, curves from the top right towards the center. Another line, in shades of green and blue, curves from the bottom left towards the center. The text is centered between these two curves.

Different RBAC Roles

Microsoft Entra roles with Intune access

Global Administrator

Intune Service Administrator

Microsoft Entra roles with Intune access

Global Administrator

Global Reader

Intune Service Administrator

Helpdesk administrator

Security Administrator

Security Operator

Security Reader

Microsoft Entra roles with Intune access

Global Administrator

Global Reader

Intune Service Administrator

Helpdesk administrator

Security Administrator

Compliance Administrator

Security Operator

Compliance Data Administrator

Security Reader

Reports Reader

Built-In Roles

[Home](#) > [Tenant admin](#) | [Roles](#) >



Endpoint Manager roles | All roles ...

Microsoft Intune

«

Manage

All roles

Scope tags

Administrator Licensing

Monitor

My permissions

Help and support

Help and support

Create Refresh Export Columns

ⓘ

Name ↑

Type

Application Manager

Built-in Role

Endpoint Privilege Manager

Built-in Role

Endpoint Privilege Reader

Built-in Role

Endpoint Security Manager

Built-in Role

Help Desk Operator

Built-in Role

Intune Role Administrator

Built-in Role

Organizational Messages Manager

Built-in Role

Policy and Profile manager

Built-in Role

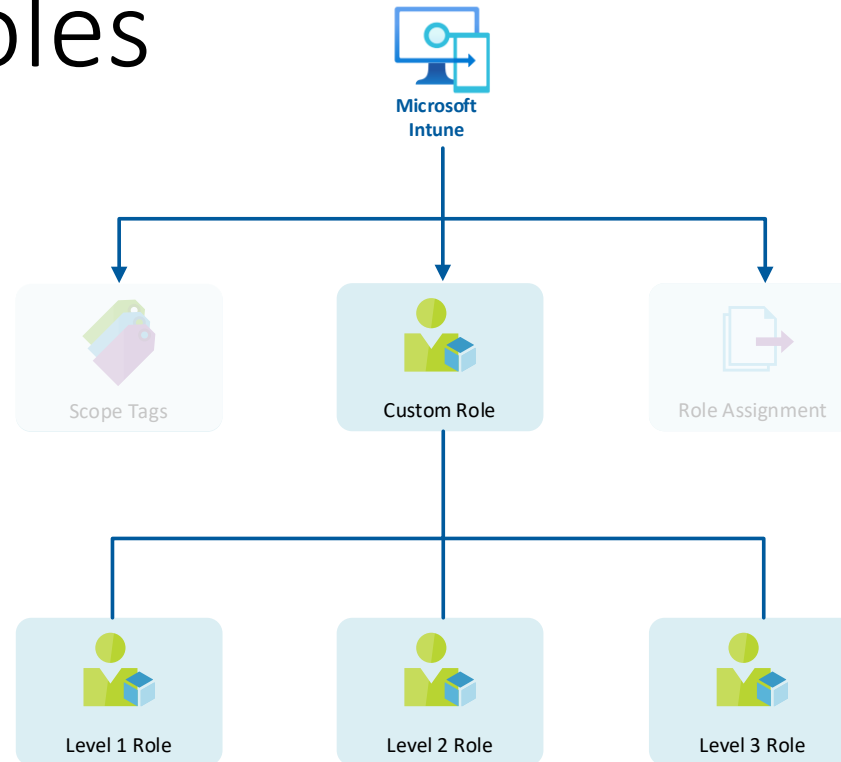
Read Only Operator

Built-in Role

School Administrator

Built-in Role

Custom Roles



Basic edit

Name
Description

Level 1 Support
No Description

Permissions edit

Android Enterprise	Read
Android FOTA	Read
Antivirus	View Reports
App Control for Business	Read
Attack Surface Reduction	View Reports
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
Device Credentials	Read
Device compliance policies	View reports
Device configurations	Read
	View Reports

Basic edit

Name
Description

Level 2 Support
No Description

Permissions edit

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

Basic edit

Name
Description

Level 3 Support
No Description

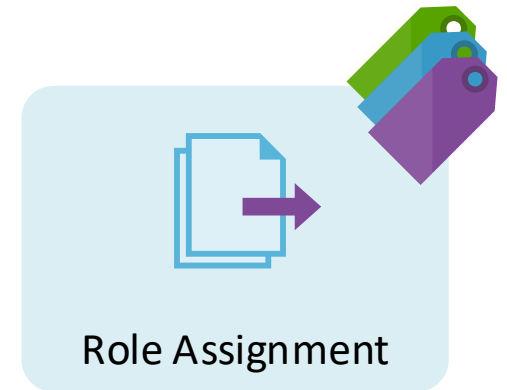
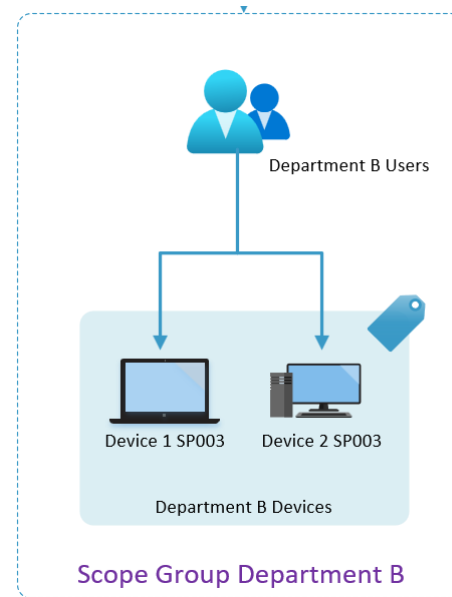
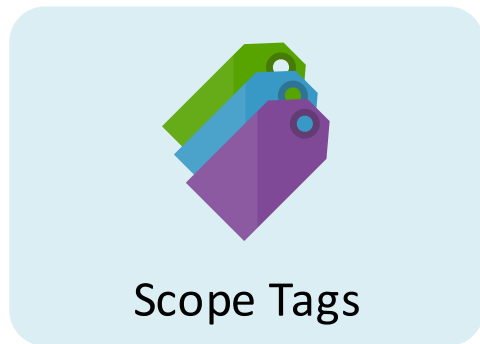
Permissions edit

Android Enterprise	Read Update enrollment Update enrollment profiles Update app sync
Android FOTA	Assign Create Read Update
Antivirus	Assign Read Update View Reports
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 self certificates
Cloud attached devices	View resource explorer View timeline View collections View software updates View scripts Run scripts Run client query View client details View application actions View applications Install/Uninstall

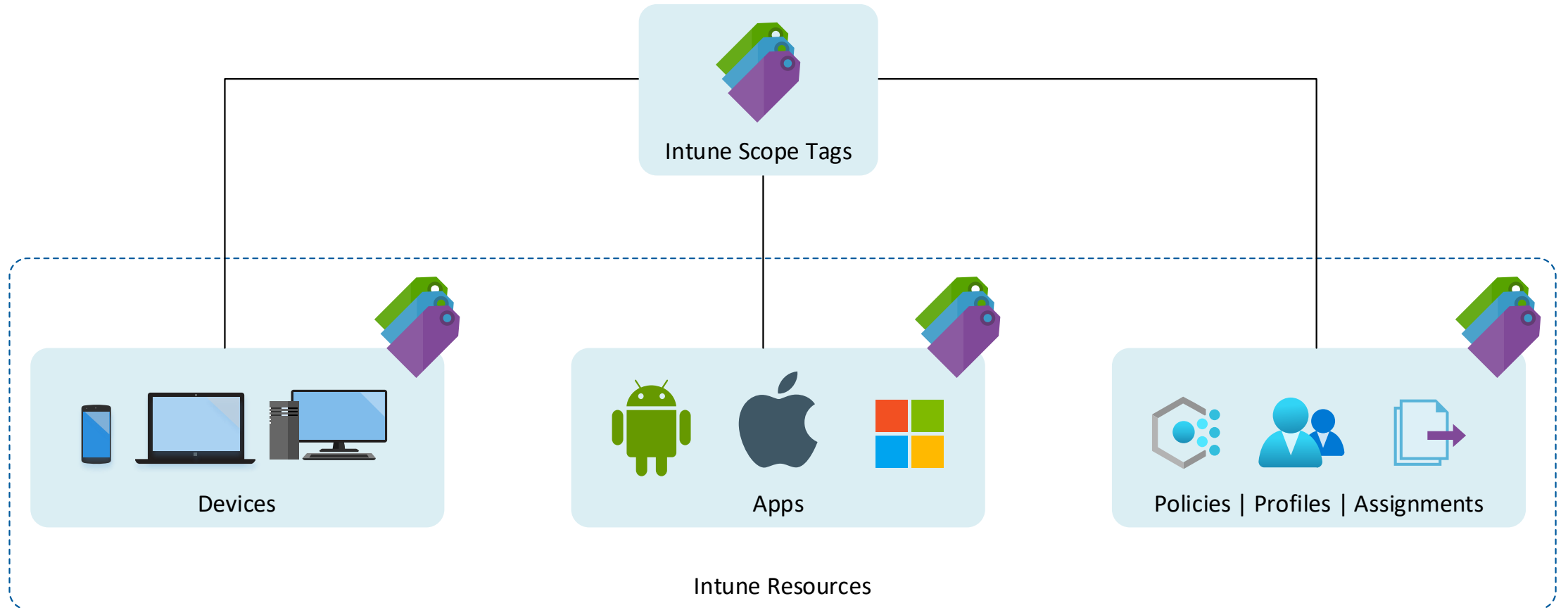
The background features decorative curved lines in the corners. In the top-right corner, there is a thick, multi-layered arc transitioning from light blue to light green. In the bottom-left corner, there is a similar thick, multi-layered arc transitioning from light green to light blue.

How to apply the RBAC Roles

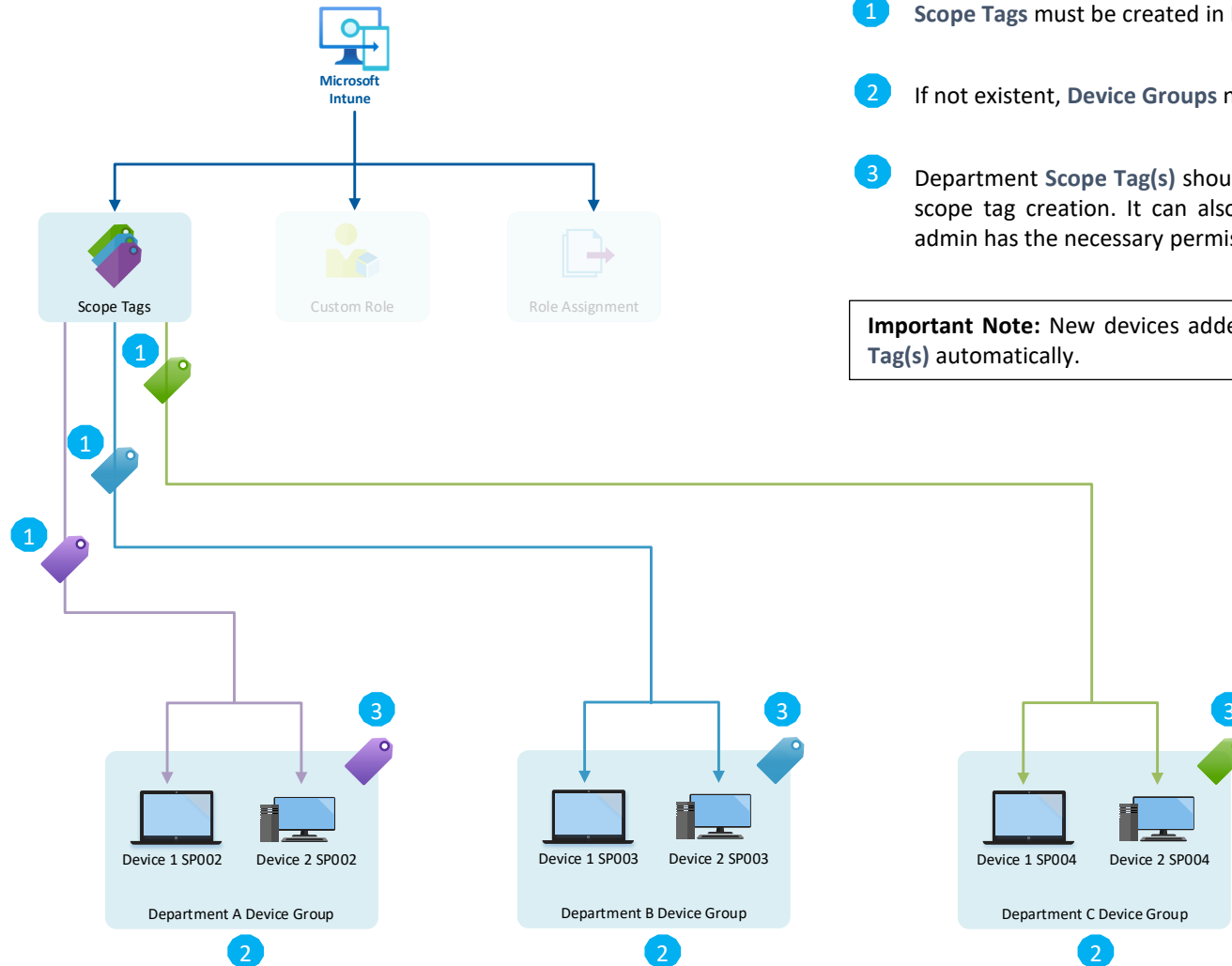
Intune Scope Groups, Roles and Role Assignments



Intune Scope Tags



Applying scope tags to Device Groups



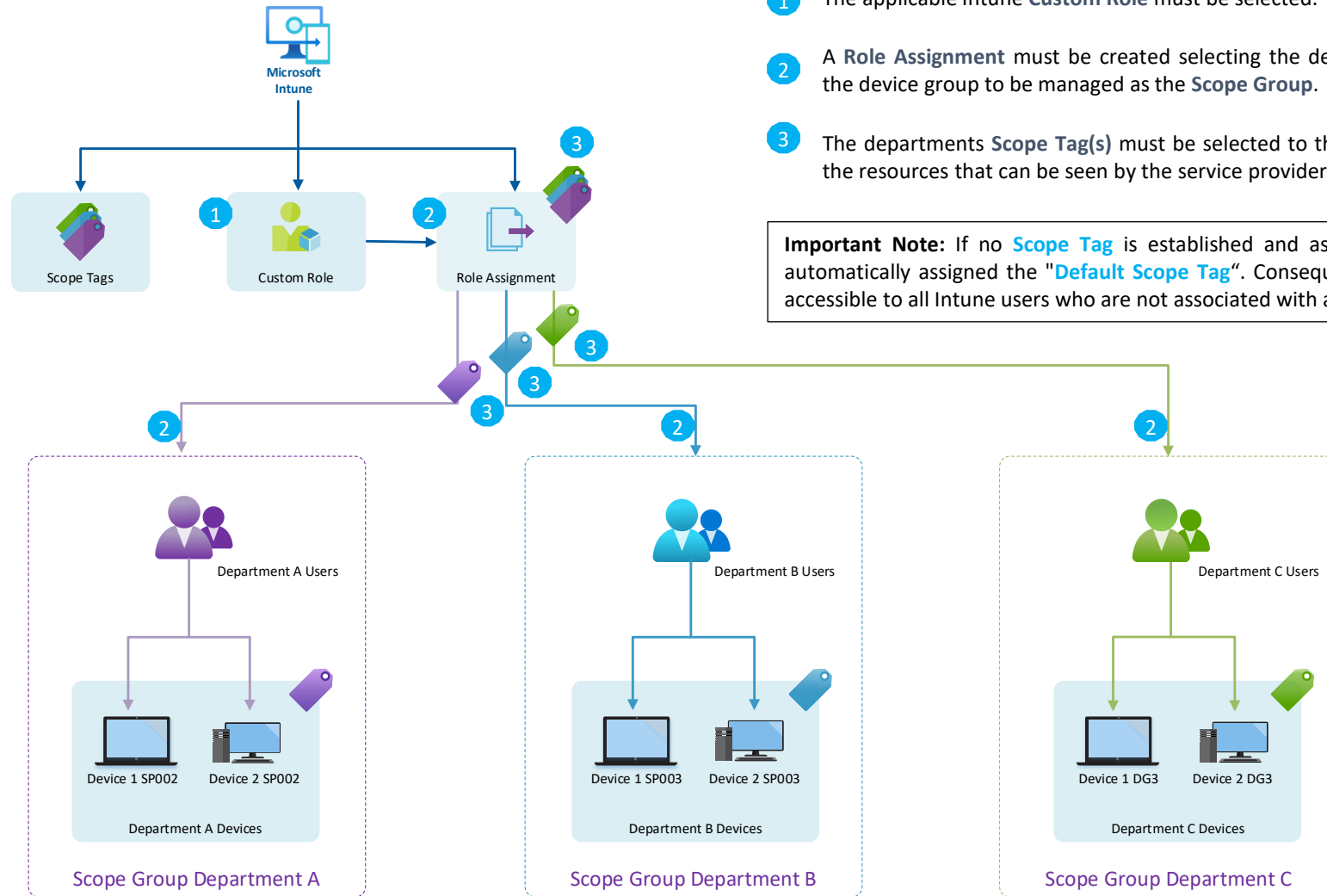
1 Scope Tags must be created in Intune for the different departments

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**.

The image features a white background with decorative curved lines in the corners. In the top-left and bottom-left corners, there are light green and blue curved lines. In the top-right corner, there are blue and green curved lines. The word "Demo" is centered in the middle of the image.

Demo



Questions?