

February 6th-7th

NIE
20/20 VISION

Oslo Spektrum



**Role-based access control (RBAC)
and more**

@mirkocolemberg





About me...



- **Mirko Colemberg**
Workplace Sommelier baseVISION
- Windows Insider MVP / Endpoint Manager MVP
- MVM FY20 Q2 (Most Valuable Mentor)
- **Contact Me**

Twitter: <https://twitter.com/mirkocolemberg>

Blog: <http://blog.colemberg.ch>

Mail: mirko.colemberg@basevision.ch



New Tenant

- What to do first?
- What's next
- What's about rights management?

Enterprise applications

[Manage how end users launch and view their applications](#)

App registrations

Users can register applications ⓘ

☒ Yes ☐ No

Administration portal

Restrict access to Azure AD administration portal ⓘ

☐ Yes ☒ No

LinkedIn account connections

Allow users to connect their work or school account with LinkedIn.

Data sharing between Microsoft and LinkedIn is not enabled until users consent to connect their Microsoft work or school account with their LinkedIn account.

[Learn more about LinkedIn account connections](#) ⓘ

☒ Yes ☐ Selected group ☐ No

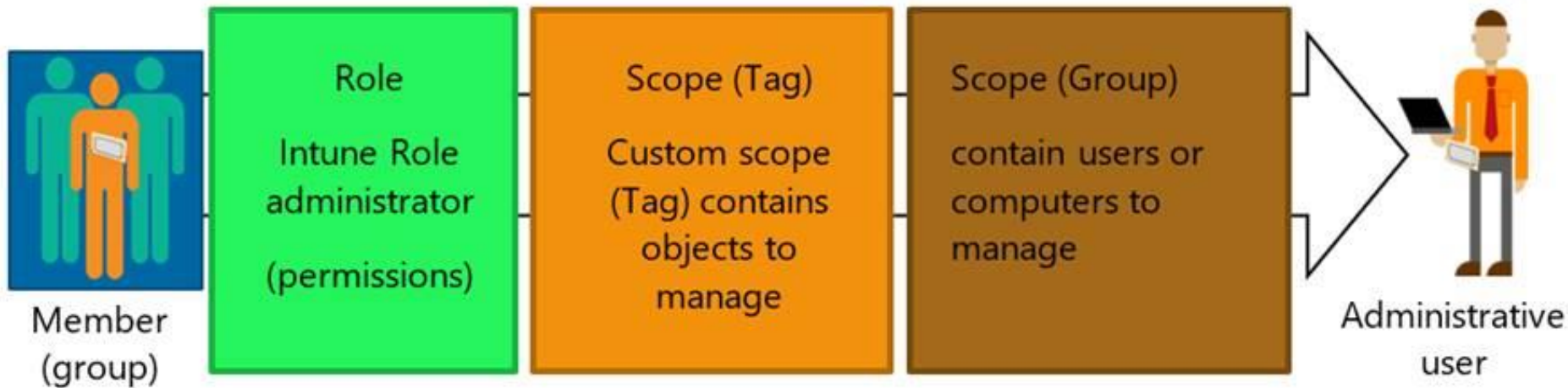
External users

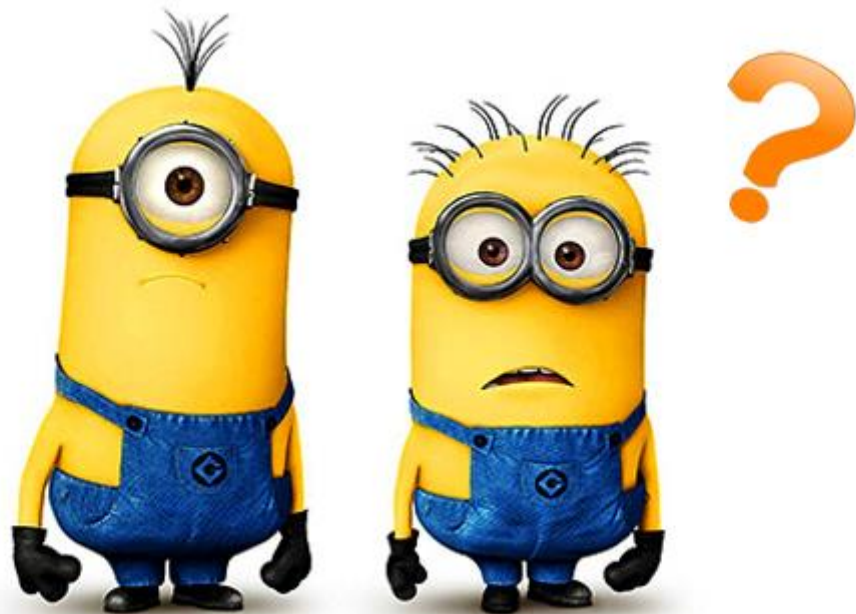
[Manage external collaboration settings](#)

User feature previews

[Manage user feature preview settings](#)

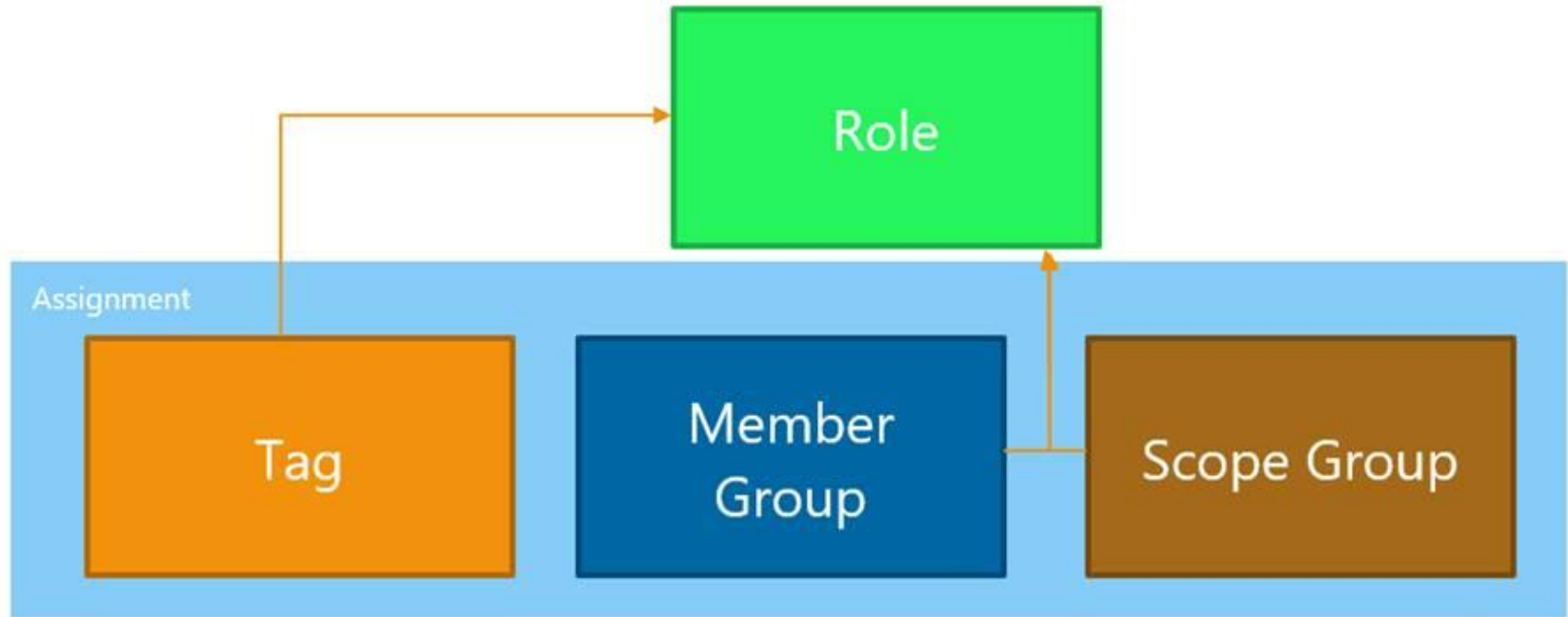
RBAC in Azure/Intune





NIC

Overview RBAC



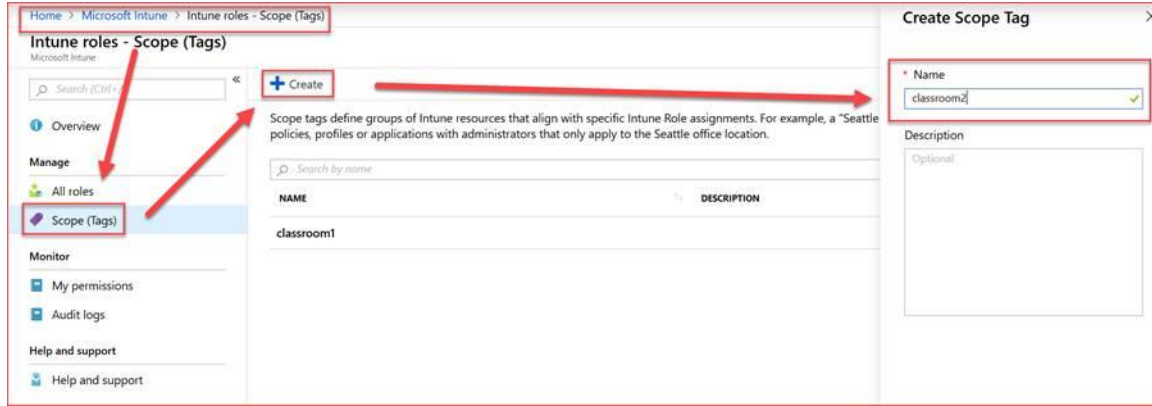


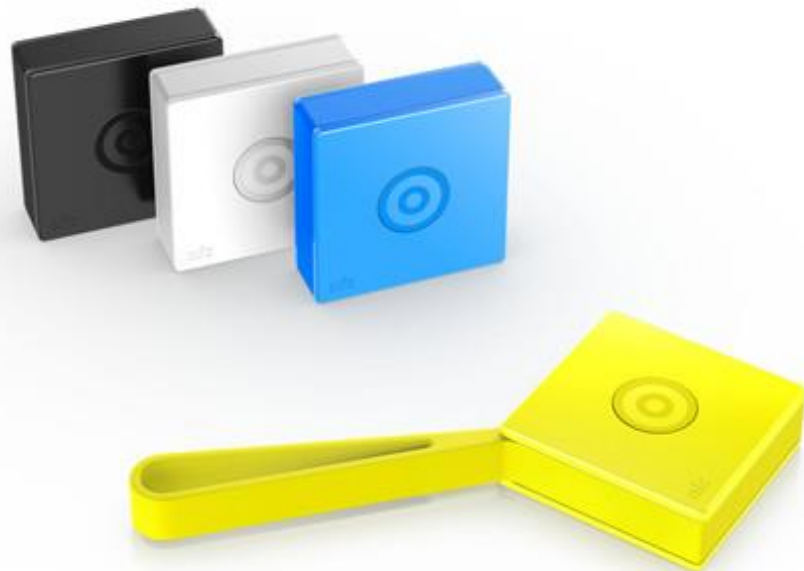
NIC

Scope Tags

Tags are used to tag for example objects in Intune. These objects can be devices, policies, profiles and so on. If you have a group of device objects, you can Tag a security Group.

If you like to tag every Device it self, it is easier to use a script and do it with Graph API: https://github.com/microsoftgraph/powershell-intune-samples/tree/master/RBAC#12-rbac_scopetags_deviceunassignps1





NIC

Scope tag on a Device

Home > Microsoft Intune > Devices - All devices > [Device Name] - Properties

DESKTOP-J2AN30M Properties

Search (Ctrl+J)

Save Discard

Device name [Redacted] [Rename](#)

Management name

Device category: Unassigned

Device ownership: Corporate

Scope (Tags)
1 scope tag(s) selected

Notes

Left Sidebar:

- Overview
- Manage
 - Properties**
- Monitor
 - Hardware
 - Discovered apps
 - Device compliance
 - Device configuration
 - App configuration
 - Security baselines
 - Managed Apps
 - Recovery keys - Preview

Scope Group

Scope Group means that there are some users or devices to manage such as a limited group of objects like devices (iOS, Android or Windows) or only part of them such as all iOS from Marketing, etc.



NIC

Member Group

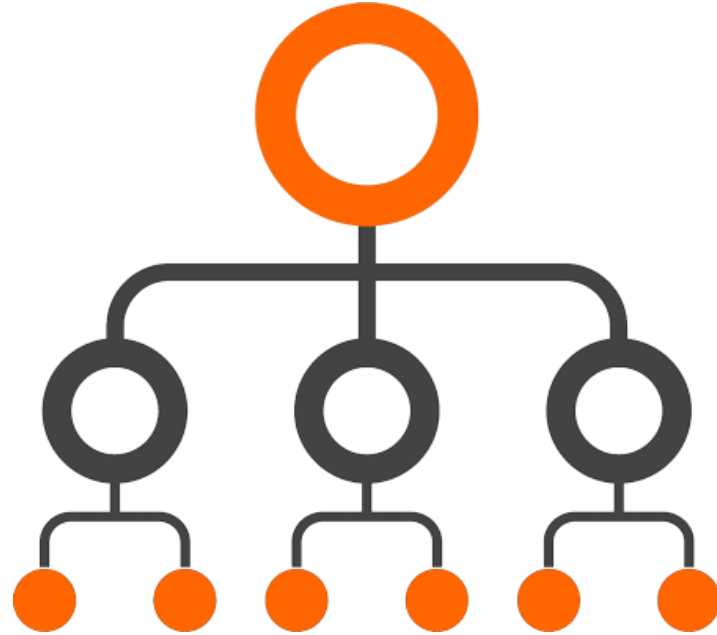
Member are one persona or a group of people who have to manage the objects in the Scope Group.



NIC

Role

Roles have different kinds of permissions. A role can have only “Read” rights on specific objects or “Write” or “Create” rights. We can for example grant access to create a new configuration profile or only change a Config profile with reading and writing access. A role can be used multiple times.



NIC

Role

Home > Microsoft Intune > Intune roles - All roles > Add Custom Role > Permissions > Remote tasks

Add Custom Role

Name
Intune for Classroom 2 ✓

Description
Enter a description...

Permissions
Configure

Scope (Tags)
0 scope(s) selected

Create

Permissions

0 / 1 permissions enabled

Managed apps 0 / 6 permissions enabled

Managed devices 0 / 3 permissions enabled

Mobile apps 0 / 5 permissions enabled

Organization 0 / 4 permissions enabled

Remote assistance 0 / 2 permissions enabled

Remote tasks 0 / 23 permissions enabled

Roles 0 / 5 permissions enabled

Security baselines 0 / 5 permissions enabled

Telecom expenses 0 / 2 permissions enabled

Terms and conditions 0 / 5 permissions enabled

OK

Remote tasks

Get filevault key.

Locate device

Manage shared device users

Play lost mode sound

Reboot now

Remote lock

Request remote assistance

Reset passcode

Retire

Revoke App Licenses

Manage encryption keys (preview)

Rotate filevault key.

Set device name

Shut down

Sync devices.

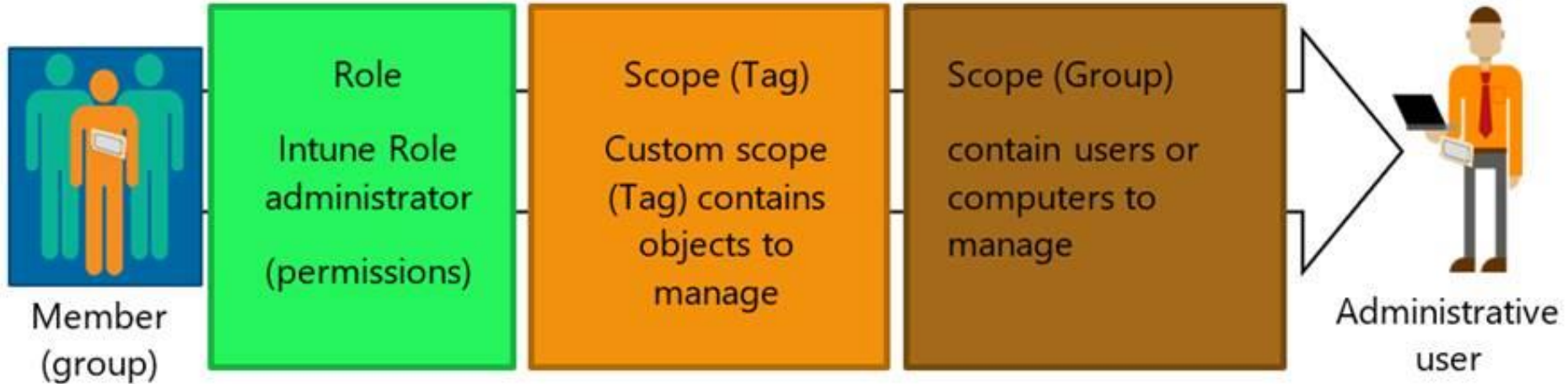
Update device account

Windows defender

Wipe

OK

RBAC in Azure/Intune



Assignment

The Assignment contains Tags, Groups and Group Members. They are assigned to a role, which is able to only one or even multiple assignments.

The screenshot displays the Microsoft Intune console interface for configuring an assignment. The breadcrumb navigation at the top reads: Home > Microsoft Intune > Intune roles - All roles > Intune roles - Assignments > Intune for Classroom 1 > Members. The main window is titled "Intune for Classroom 1" and contains several sections:

- Assignment name:** "Classroom2 Teachers" (highlighted with a red box and arrow).
- Assignment description:** "Enter a description..." (highlighted with a red box and arrow).
- Members (Groups):** "0 member(s) selected" (highlighted with a red box and arrow).
- Scope (Groups):** "0 scope(s) selected" (highlighted with a red box and arrow).
- Scope (Tags):** "0 scope(s) selected" (highlighted with a red box and arrow).

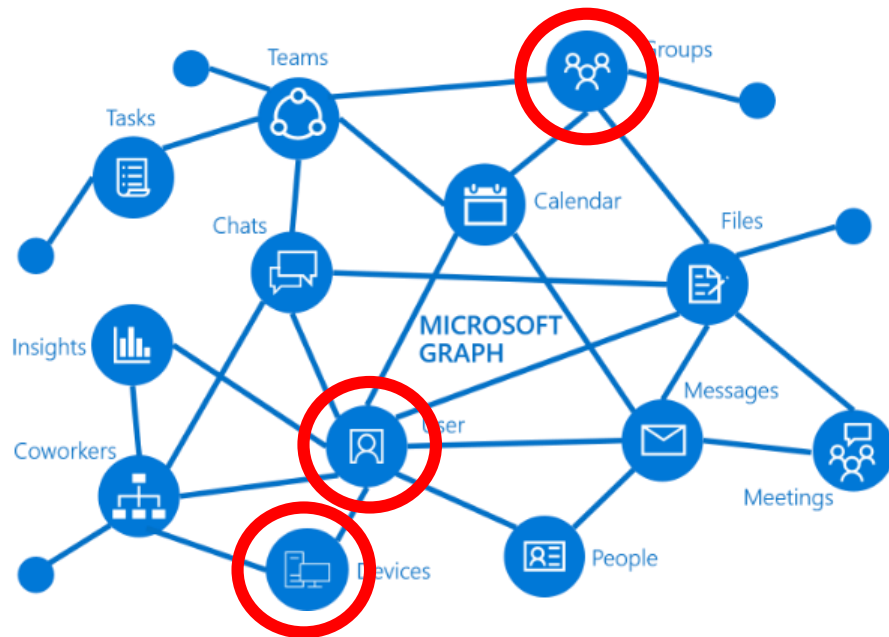
On the right side, there are two panels:

- Members:** A panel titled "Members" with a "+ Add" button (highlighted with a red box and arrow) and a "Member Group assigned to" dropdown.
- Scopes:** A panel titled "Scopes" with a "Set scope (groups) to:" dropdown (highlighted with a red box and arrow) and a "Select groups to include" button (highlighted with a red box and arrow).

Below the main window, there are two smaller panels:

- Tags:** A panel titled "Tags" with a "+ Add" button (highlighted with a red box and arrow) and a "SCOPE TAG" dropdown.
- Select tags:** A panel titled "Select tags" with a "Select" dropdown and a list of tags: "classroom1" and "classroom2" (highlighted with a red box and arrow).

GRAPH



Intune – Powershell SAMPLES GITHUB

The screenshot shows the GitHub repository page for 'microsoftgraph / powershell-intune-samples'. The repository has 25 stars and 9 forks. The description states: 'This repository of PowerShell sample scripts show how to access Intune service resources. They demonstrate this by making HTTPS RESTful API requests to the Microsoft Graph API from PowerShell.' The repository has 30 commits, 1 branch, 0 releases, and 3 contributors. The latest commit is 98dc4ed, 3 days ago. The repository is licensed under MIT. The file list shows folders for AppProtectionPolicy, AppleEnrollment, Applications, Authentication, and CheckStatus, all with v2.0 updates 8 days ago.

Repository: [microsoftgraph / powershell-intune-samples](#)

Unwatch 25 Star 20 Fork 9

Code Issues 1 Pull requests 1 Projects 0 Wiki Settings Insights

This repository of PowerShell sample scripts show how to access Intune service resources. They demonstrate this by making HTTPS RESTful API requests to the Microsoft Graph API from PowerShell. [Edit](#)

[Add topics](#)

30 commits 1 branch 0 releases 3 contributors MIT

Branch: master New pull request Create new file Upload files Find file Clone or download

Latest commit 98dc4ed 3 days ago

AppProtectionPolicy	v2.0 Update	8 days ago
AppleEnrollment	Added Readme.md	2 months ago
Applications	v2.0 Update	8 days ago
Authentication	v2.0 Update	8 days ago
CheckStatus	v2.0 Update	8 days ago

<https://github.com/microsoftgraph/powershell-intune-samples>

NIC

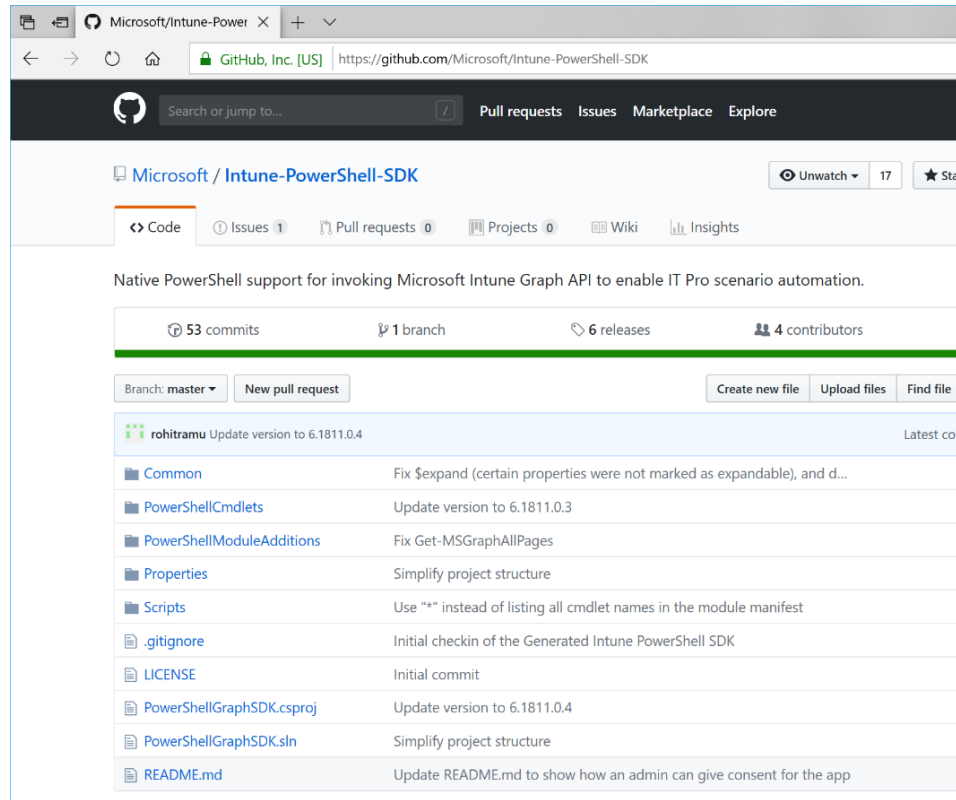
Intune – PowerShell Module

Available on GitHub today and in PowerShell Gallery:

- <https://aka.ms/intunepowershell>
- <https://www.powershellgallery.com/packages/Microsoft.Graph.Intune>

Supports

- v1.0 Graph Endpoints
- Parameter sets for properties
- PowerShell credentials for Authentication
- PowerShell Pipeline



Slides and demos from the conference will be available at

<https://github.com/nordicinfrastructureconference/2020>

