1

Thank you Sponsors

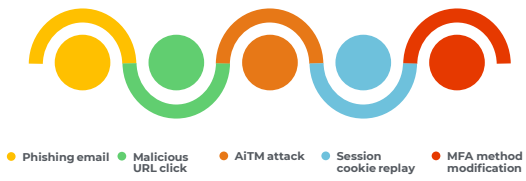
liquidware
2Pint
Gold
PINK
RECAST SOFTWARE
Silver
PATCH MY PC
Technical Partners
CONSULTEQ
PROXSYS
Daalmans consulting
Secure At Work

2

3

4

Adversary in The Middle (AiTM)



Detecting and mitigating a multi-stage AiTM phishing and BEC campaign | Microsoft Security Blog

5

6

About Nicklas Ahlberg

Focus
Endpoint Management and Windows

From
Sweden

My Blog
https://rockenroll.tech

Certifications
Dual MVP (Intune and Windows)
MCT

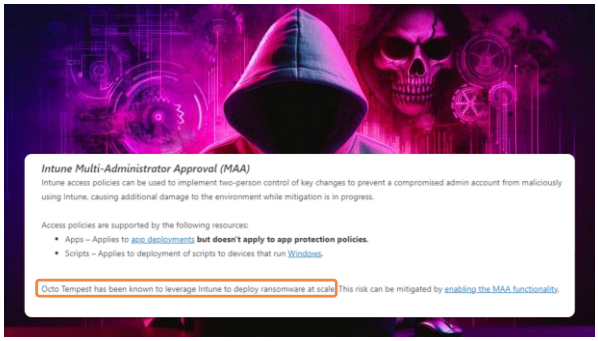
Hobbies
BBQ and #membeer
Football coach

Contact
Twitter, Bluesky, LinkedIn
AND HERE TODAY, DON'T BE SHY!

7

Octo Tempest: Hybrid identity compromise recovery - Microsoft Community Hub

8



Intune Multi-Administrator Approval (MAA)

Intune access policies can be used to implement two-person control of key changes to prevent a compromised admin account from maliciously using Intune, causing additional damage to the environment while mitigation is in progress.

Access policies are supported by the following resources:

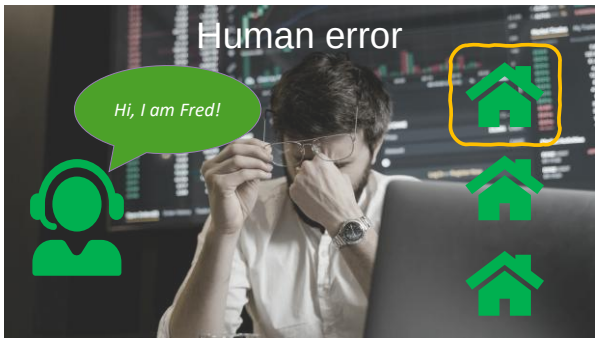
- Apps – Applies to app deployments **but doesn't apply to app protection policies.**
- Scripts – Applies to deployment of scripts to devices that run Windows.

Octo Tempest has been known to leverage Intune to deploy ransomware at scale. This risk can be mitigated by enabling the MAA functionality.

9

The modern threat actor be like...

10



11

12

13

14

Your typical IT-admin be like...

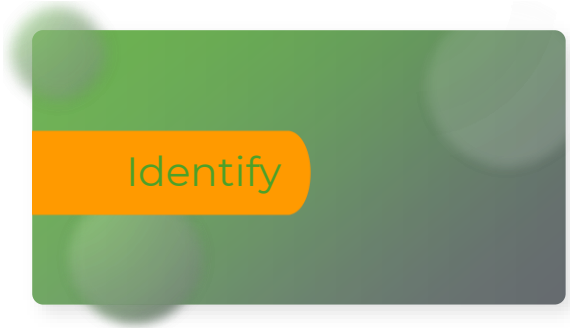
15

16

WHY: Notes from the field

- 💵 Security is top of mind after an attack.
- 🔐 MFA is no longer enough (number matching doesn't mitigate AiTM).
- 🕯️ Crucial to monitor MFA registrations.
- 🔒 FIDO2 security keys can easily be fully adopted and used by administrators.
- 👑 Global, Intune, Applications, Security and Groups admin role is handed out too easily.
- 🎯 Scoped permissions have become a frequent ask by customers and the community.
- 👍 Suppliers are getting better at asking for least privileges.

17



18

Common questions

- Specific Windows 365 administrators?
- Specific site administrators?
- Different support levels (first, second, third-line)?
- How will objects be tagged?
- Privileged Access Workstation (PAW)?

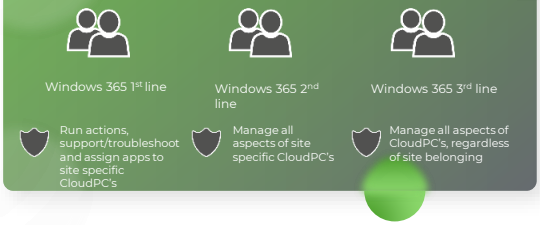
19

Example: What

- Site specific first line W365 administrators
  - Paris
  - Amsterdam
- Custom roles:
  - Entra ID
  - Windows 365
  - Intune
- Conditional Access
  - Phishing resistant MFA
  - Compliant device
- Access packages to request and review privileges

20

Personas



21

Personas

22

Our goal (success criterias)

-Limit the impact after an admin account has been **breached**

-Limit the impact of human errors

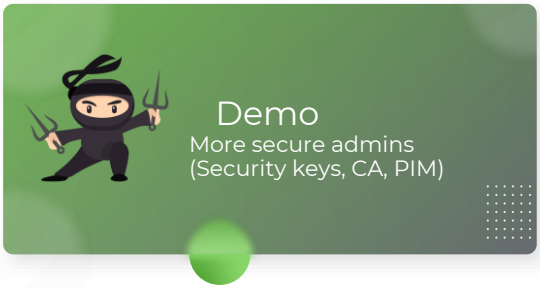
-Require more secure admin **authentication**, Mitigate **AiTM**

-Make it **easy** and **secure** to manage and receive extended privileges if needed

23

Configuration

24



25

Intune vs Windows 365 Entra roles

Intune administrator
- Privileged role
- Includes full W365 privileges

Windows 365 administrator
- Full W365 privileges

Intune administrator: Use only when absolutely needed

26

Role-Based Access Control (RBAC)

Intune v2406 gave us granular endpoint security permissions
- Endpoint detection and response
- App control for business
- Attack surface reduction (ASR)

Granular RBAC permissions for endpoint security workloads - Microsoft Community Hub

27

Scope tags:
What we are allowed to see
EX: Users, groups, policies, devices

Roles:
What we are allowed do with what we can see
EX: Initiate sync or read the Bitlocker key

28

Windows 365: scope tags **(preview)**

The following bulk actions don't honor scope tags when called directly from the **Graph API**:

- Restore
- Reprovision
- Place Cloud PC under review
- Remove Cloud PC under review
- Share Cloud PC restore point to storage
- Create Cloud PC manual restore point

29

Scope tags: Good to know

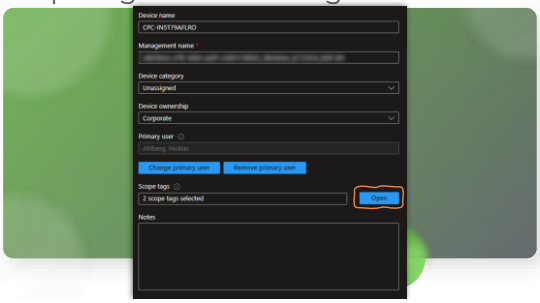
Determine what admins can **see** in the admin portals

Default tag is automatically added to all **untagged** objects

Automatic tag assignments will **overwrite** manually assigned tags

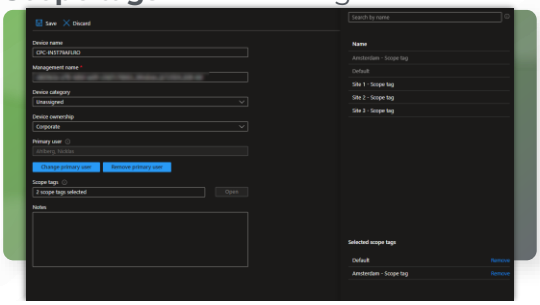
30

Scope tags: manual assignment



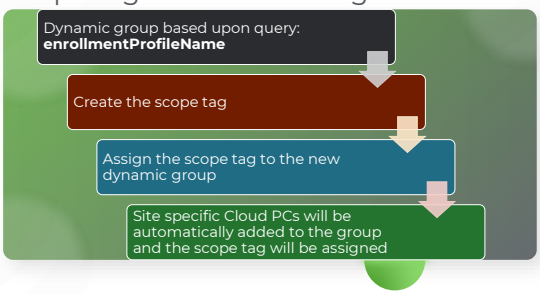
31

Scope tags: manual assignment

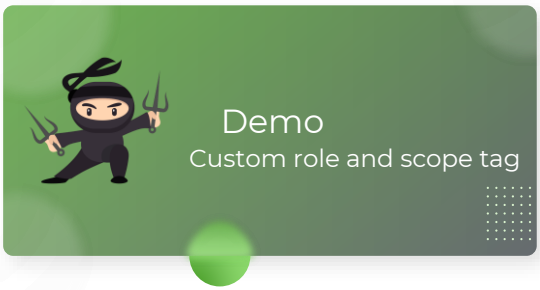


32

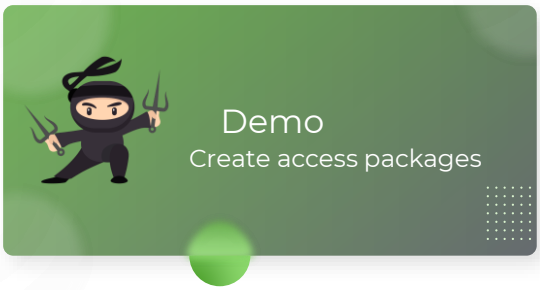
Scope tag: automatic assignment



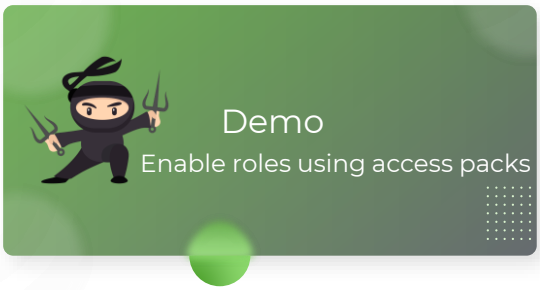
33



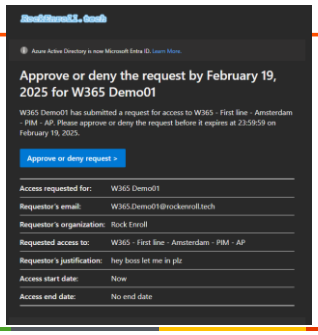
34



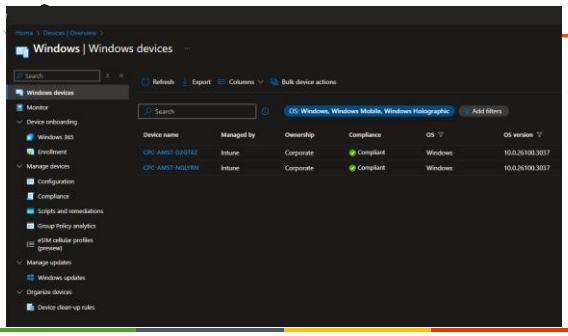
35



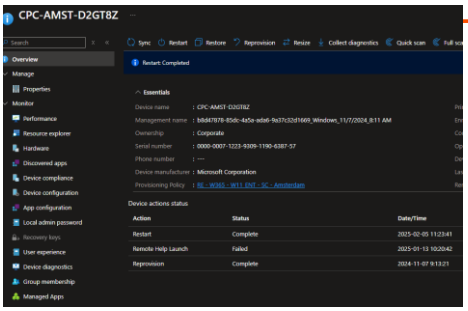
36



37



38



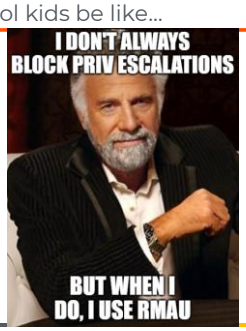
39

Administrative units: Requirements

- Divide users/devices/groups into administrative units to add site specific permissions
- Microsoft Entra ID P1/P2 for assigned admins
- Microsoft Entra ID free for members
- Default scope: tenant-level
- We don't want group admins to add themselves to our groups…
- **[PREVIEW]** Restricted management admin units will protect against privilege escalations

40

The cool kids be like…



41

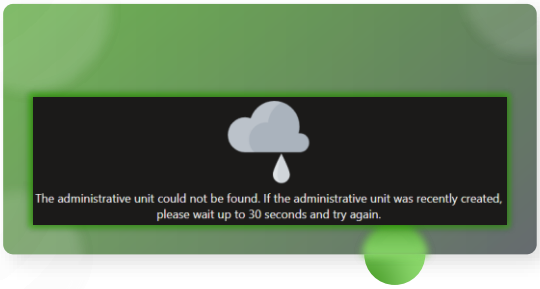
💡 Administrative units: graph

https://graph.microsoft.com/beta/administrativeUnits

```
{
    "displayName": "W365 - Paris CloudPCs - RMAU",
    "description": "This administrative unit contains Paris cloudPCs
and is mainly used for WLAPS",
    "isMemberManagementRestricted": true
}
```

The administrative unit could not be found. If the administrative unit was recently created, please wait up to 30 seconds and try again.

42



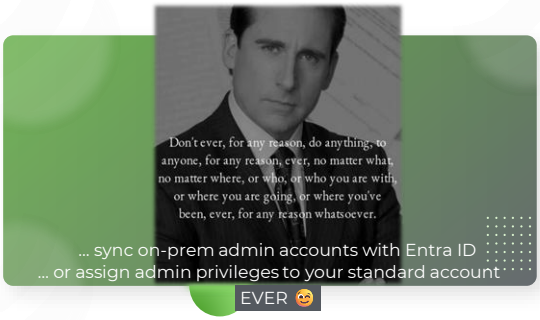
43

44

⭐Important practices

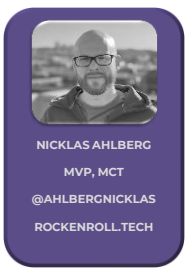
- Use security keys, begin with administrators
- Do not sync on-prem admin accounts to Entra ID
- Always use separate admin accounts

45



46

47



Thank You

48