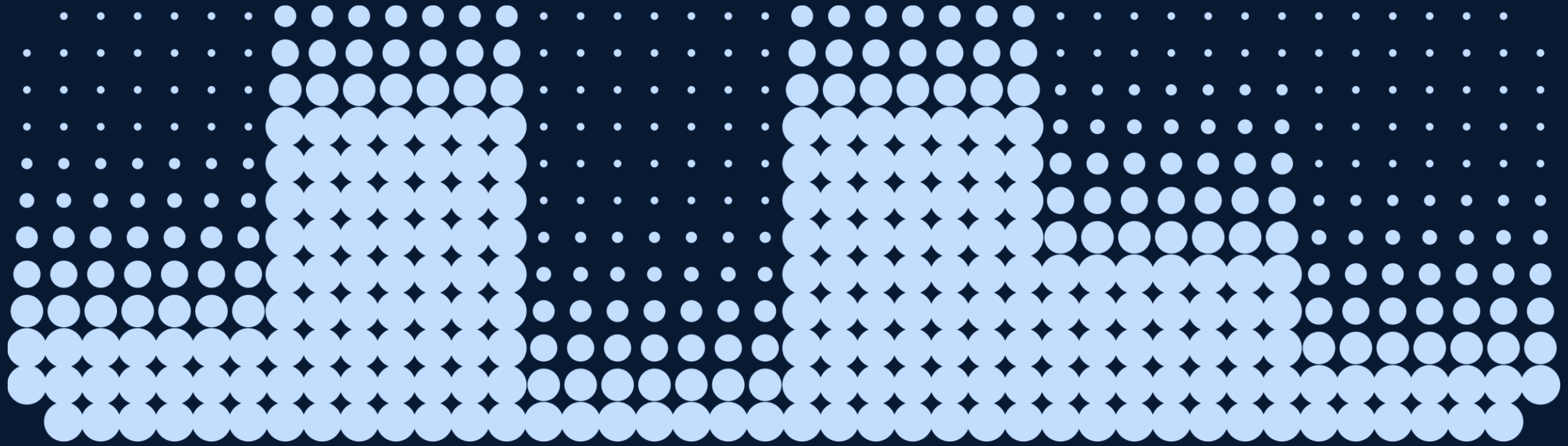


Optimize and Control Entra ID Privileged Roles

Bsure recommended actions

bsure.

5/5-25 Gunnar Weld

5 recommended actions

1. Review and clean-up privileged accounts
2. Remove inactive accounts and free up licenses
3. Protect ALL accounts with MFA, also the inactive ones
4. Review and clean-up overprivileged non-human identities (applications)
5. Activate SSO on all applications that supports it and scope access

What we've learned:

Lack of visibility leads to:

Overprivileged access
Security risks
Compliance challenges

Bsure recommendations

Create a strategy on how you provide roles to your co-admins

- Recommendations:
  - Use dedicated personal cloud-only user accounts for administrative purposes.
  - Enforce phishing resistant MFA on all administrative user accounts
  - Use privileged identity management (PIM)
  - Configure approval for highly privileged roles
  - Configure User risk and Sign-in risk policies using Conditional Access
  - Create a privileged access workstation

  - Review role assignments frequently

These recommendations requires Entra ID P2 licenses

Best practice

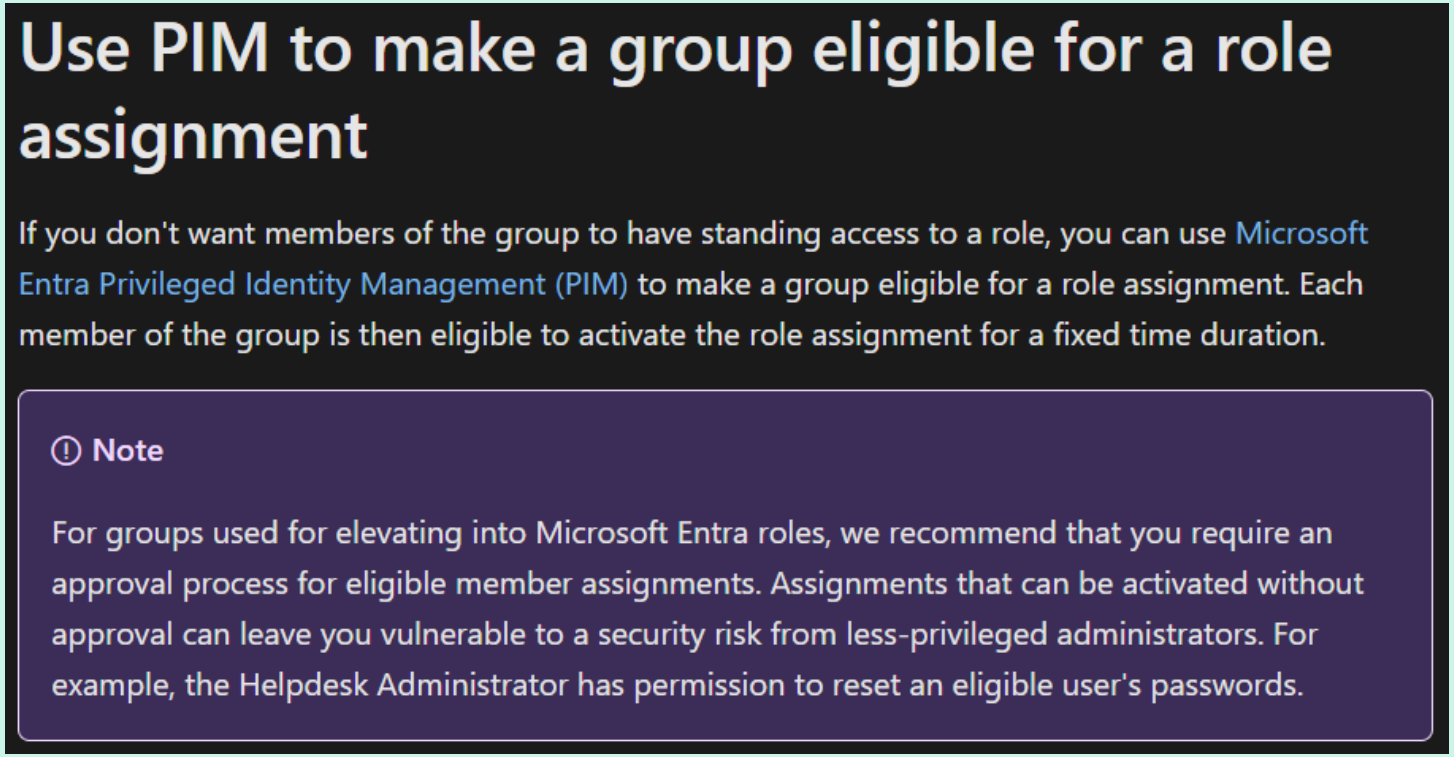
Avoid assigning Entra ID roles to on-premises synchronized users

Best practice

Avoid assigning Entra ID roles to normal user accounts using Teams and Outlook

Bsure recommendations

If You decide to distribute Entra ID roles using Groups



Some limitations in:

- Exchange admin center*
- Azure Information Protection Portal (the classic portal)*
- Access review of Microsoft Entra roles in PIM**

* https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-concept#known-issues

** https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-create-roles-and-resource-roles-review

Bsure recommendations

How to Begin?

- Evaluate existing role assignments – demo
- Eliminate unnecessary role assignments
- Ensure only dedicated cloud-only user accounts holds privileged roles
- Enforce phishing-resistant MFA for these user accounts
- Use Privileged Identity Management and assign privileged roles as eligible
  - Configure approval step on the most critical roles
- Establish User risk and Sign-in risk policies using Conditional Access
- Configure Access Reviews for Entra ID Roles and review frequently
- Create and enforce usage of privileged access workstation

Bsure tip:

MICROSOFT ENTRA BLOG 4 MIN READ

Microsoft Entra ID Governance licensing clarifications

kamurphy MICROSOFT

Jun 19, 2024

One person, one license

Note that this philosophy includes administrative accounts. In some organizations, administrators use standard user accounts for day to day tasks, and separate administrator accounts for privileged access. A person with a standard user account and an administrator account only needs one Entra ID Governance license for both identities to be governed. Of course, they could also leverage Entra ID Governance's Privileged Identity Management (PIM) to temporarily elevate the access rights of a single account, instead of maintaining two accounts.