Conditional Access Templates: Simplify Security - Microsoft Entra ID

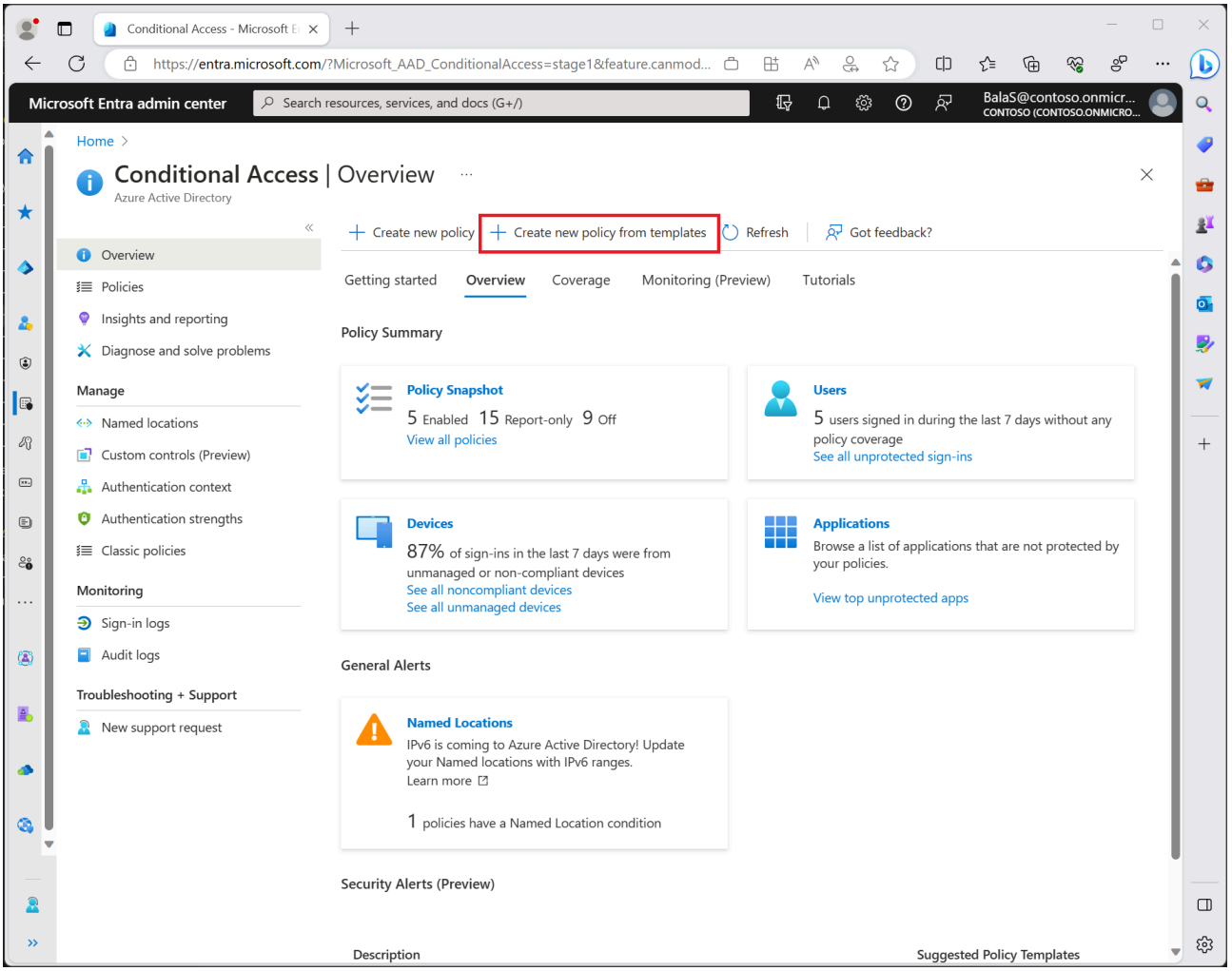
By kenwith

Archived: 2026-04-05 15:04:59 UTC

In this article

Overview

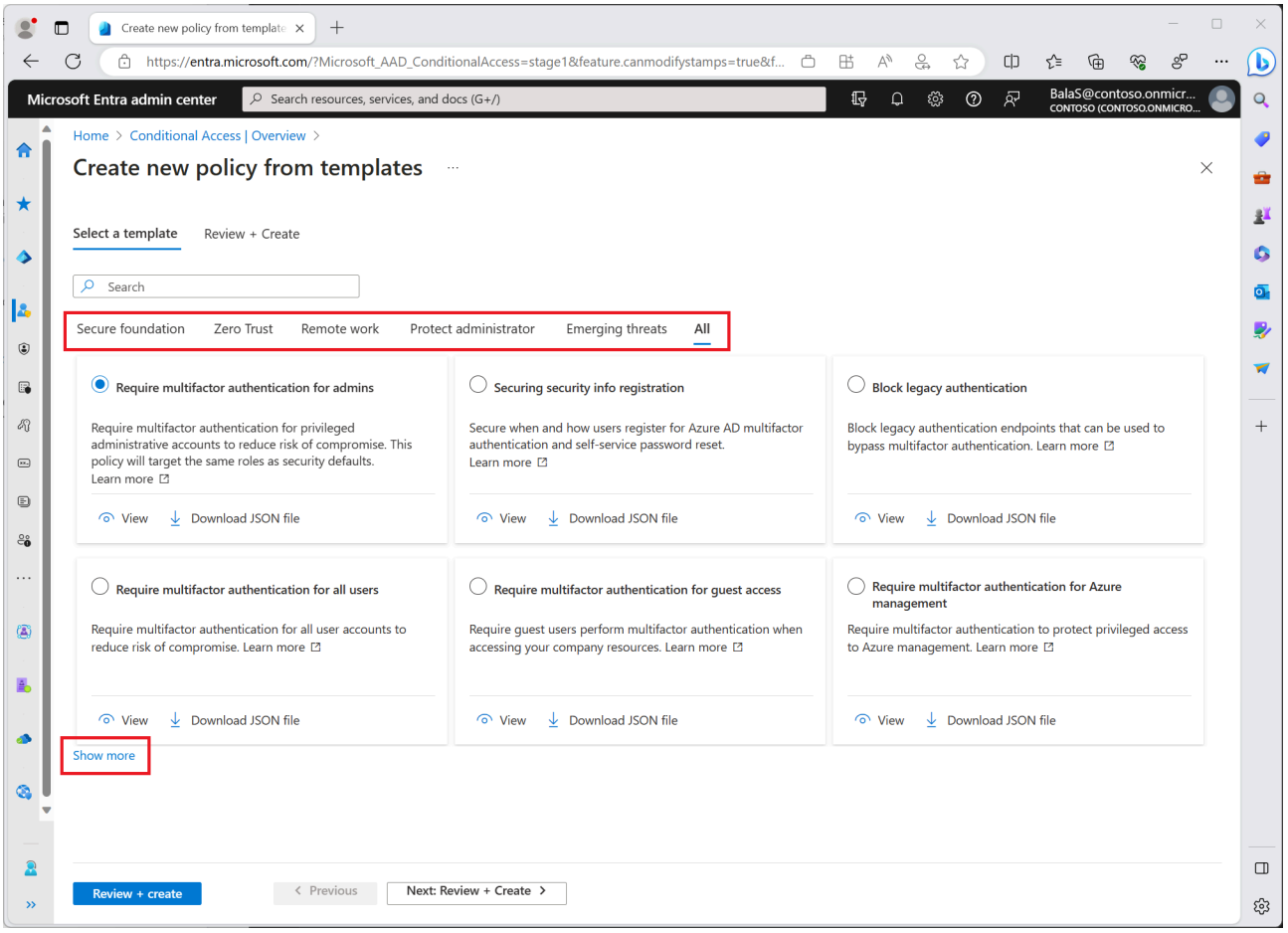
Conditional Access templates provide a convenient method to deploy new policies aligned with Microsoft recommendations. These templates are designed to provide maximum protection aligned with commonly used policies across various customer types and locations.



Template categories

Conditional Access policy templates are organized into the following categories:

Find these templates in the Microsoft Entra admin center > **Entra ID** > **Conditional Access** > **Create new policy from templates**. Select **Show more** to view all policy templates in each category.



Important

Conditional Access template policies targeting users exclude only the user creating the policy from the template. If your organization needs to exclude other accounts, modify the policy after it's created. You can find these policies in the Microsoft Entra admin center > **Entra ID** > **Conditional Access** > **Policies**. Select a policy to open the editor and modify the excluded users and groups to select accounts you want to exclude.

By default, each policy is created in report-only mode. Test and monitor usage to ensure the intended result before turning on each policy.

Organizations can select individual policy templates and:

- View a summary of the policy settings.
- Edit, to customize based on organizational needs.
- Export the JSON definition for use in programmatic workflows.
    - These JSON definitions can be edited and then imported on the main Conditional Access policies page using the **Upload policy file** option.

Other common policies

- Require multifactor authentication for device registration
- Block access by location

- Block access except specific apps

User exclusions

Conditional Access policies are powerful tools. We recommend excluding the following accounts from your policies:

- **Emergency access** or **break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario where all administrators are locked out, your emergency access administrative account can be used to sign in and recover access.
    - More information can be found in the article, Manage emergency access accounts in Microsoft Entra ID.
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are noninteractive accounts that aren't tied to any specific user. They're typically used by backend services to allow programmatic access to applications, but they're also used to sign in to systems for administrative purposes. Calls made by service principals aren't blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies that target service principals.
    - If your organization uses these accounts in scripts or code, replace them with managed identities.

Next steps

- Simulate sign in behavior using the Conditional Access What If tool.
- Use report-only mode for Conditional Access to determine the results of new policy decisions.

Additional resources

Training

- Last updated on 03/24/2026
