Recast

Configure Layered Access with Two Contexts

Last Modified on 2026-11-05

You can target a specific group of users, then further narrow access to a network location, by combining two contexts. The first context identifies members of the security group. The second context filters by membership in the first context and an IP-address condition. Then you apply an access policy based on both the security-group membership and the approved IP address or range.

Prerequisites

- Administrative permissions to create and modify contexts and assign access policies.
- A Microsoft Entra security group available through your Application Workspace identity integration.
- An approved IP address or range in a format supported by the IP-address filter.
- An access policy for the required resources and access permissions, or permissions to create one.

NOTE: The steps below use **'Users — Entra Security Group'** and **'Access — Group and Approved IP'** as example context names. We suggest that you use names that fit in your environment.

Create a Context for the Security Group

To create a context based on Microsoft Entra security-group membership:

1. In Application Workspace, navigate to **Manage** > **Identities** > **Contexts** and click **Create**.
   - On the **Type** tab, choose **Filter.**
   - On the **Overview** tab, name your context (for example, **'Users — Entra Security Group'**) and add a description.
   - On the **Summary** tab, click **Finish**.

2. Open your new context and select the **Filters** tab.

3. Click **Create filter** and add the Microsoft Entra security group. Click **Confirm**.

Create a Context for the Group and IP Address

To require membership in the first context and an approved IP address:

1. On the **Contexts** page, click **Create**.
   - On the **Type** tab, choose **Filter.**
   - On the **Overview** tab, name your context (for example, **'Access — Group and Approved IP'**) and add a description explaining that it combines the approved network scope with membership in the first context.
   - On the **Summary** tab, click **Finish**.

2. Open your second context and select the **Filters** tab.

3. Click **Create filter** and add an IP-address filter and with the approved address or range.

4. Add another filter that requires membership in another context and select **Users — Entra Security Group'**.

   NOTE: This filter is a reference to the first context, not a second independent Entra-group filter.

5. Select **AND** as the **Operator** so that both conditions are required.

6. Click **Save filters** on the toolbar.

Assign an Access Policy to the Combined Context

Recast

To assign an access policy to the context that requires both conditions:

1. Create or select the policy for the intended resources and access.

2. Associate the access policy with the '**Access — Group and Approved IP**' context.