Use IP Allowlisting to enforce zero trust policies for specific SaaS Applications integrated with Entra ID

Use Named Locations and Conditional Access policies in Azure AD to ensure use of a Service Tunnel when authenticating to a SaaS Application like O365

Updated on 5 minutes to read Contributors 

ON THIS PAGE:

Overview

This guide explains how to use Named Locations and Conditional Access policies in Entra ID to require that end users have Service Tunnel for authenticating to specific SaaS application(s). In the steps below, we use Office 365 as the example application.

Steps

Step 1: Register a Service Tunnel for Public Domains

1.1 Register a Service Tunnel for Public Domains.

1.2 Configure the Service Tunnel to include the **Azure portal domains used for authentication**:

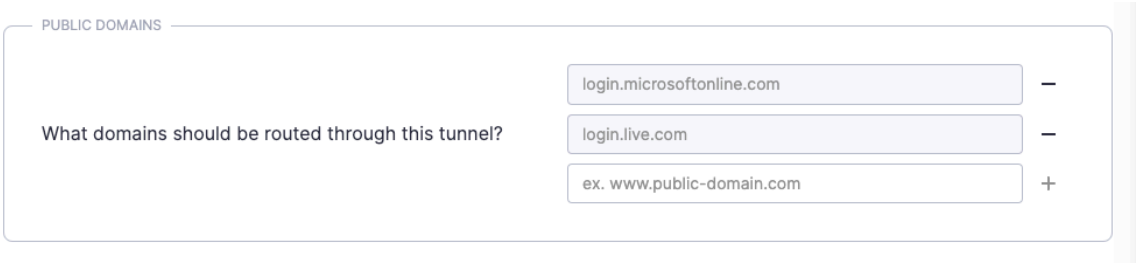
```
login.microsoftonline.com aadcdn.msftauth.net aadcdn.msftauthimages.net
aadcdn.msauthimages.net logincdn.msftauth.net login.live.com msauth.net
aadcdn.microsoftonline-p.com microsoftonline-p.com
```

AND/OR

The public IPv4 ranges listed in ID 56 for Microsoft 365 Common and Office Online:

`20.20.32.0/19`, `20.190.128.0/18`, `20.231.128.0/19`, `40.126.0.0/18`

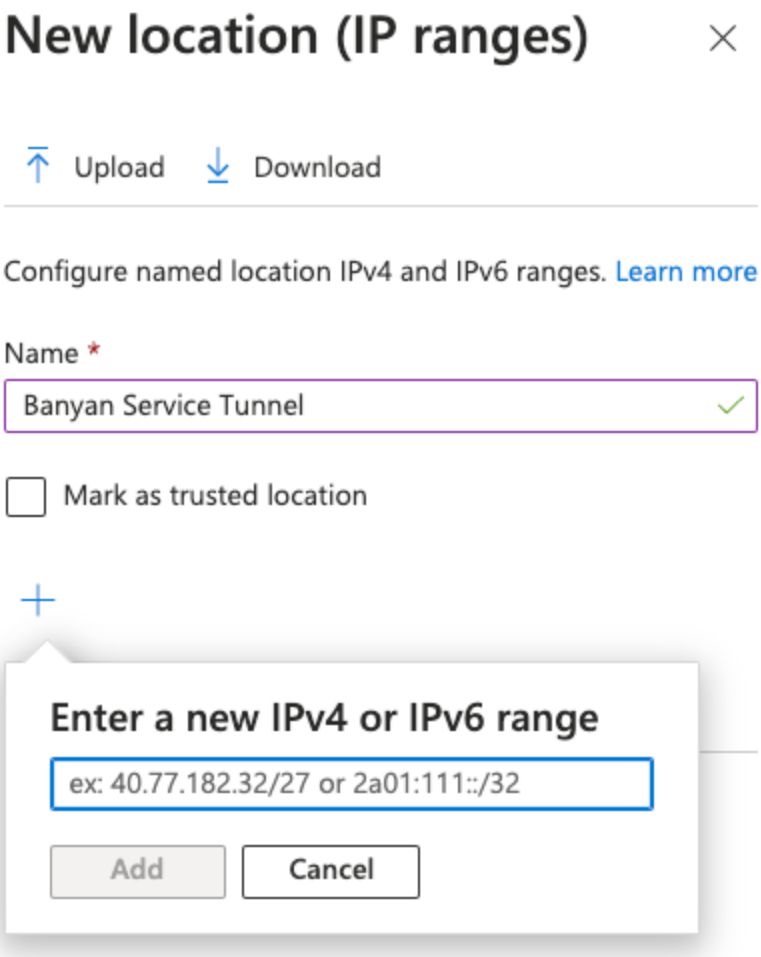
Note: The above portal domains and public IPv4 addresses are subject to change; for the latest, always consult the latest list in Microsoft 365 Common and Office Online documentation).



Step 2: Create a named location to use in a Conditional Access policy

2.1 In the Microsoft Entra admin center, navigate from **Protection** > **Conditional Access** > **Named locations**, and select **+ IP ranges location**.

2.2 Enter a name (e.g., *Service Tunnel*) and the IP address(es) of the relevant Access Tiers.

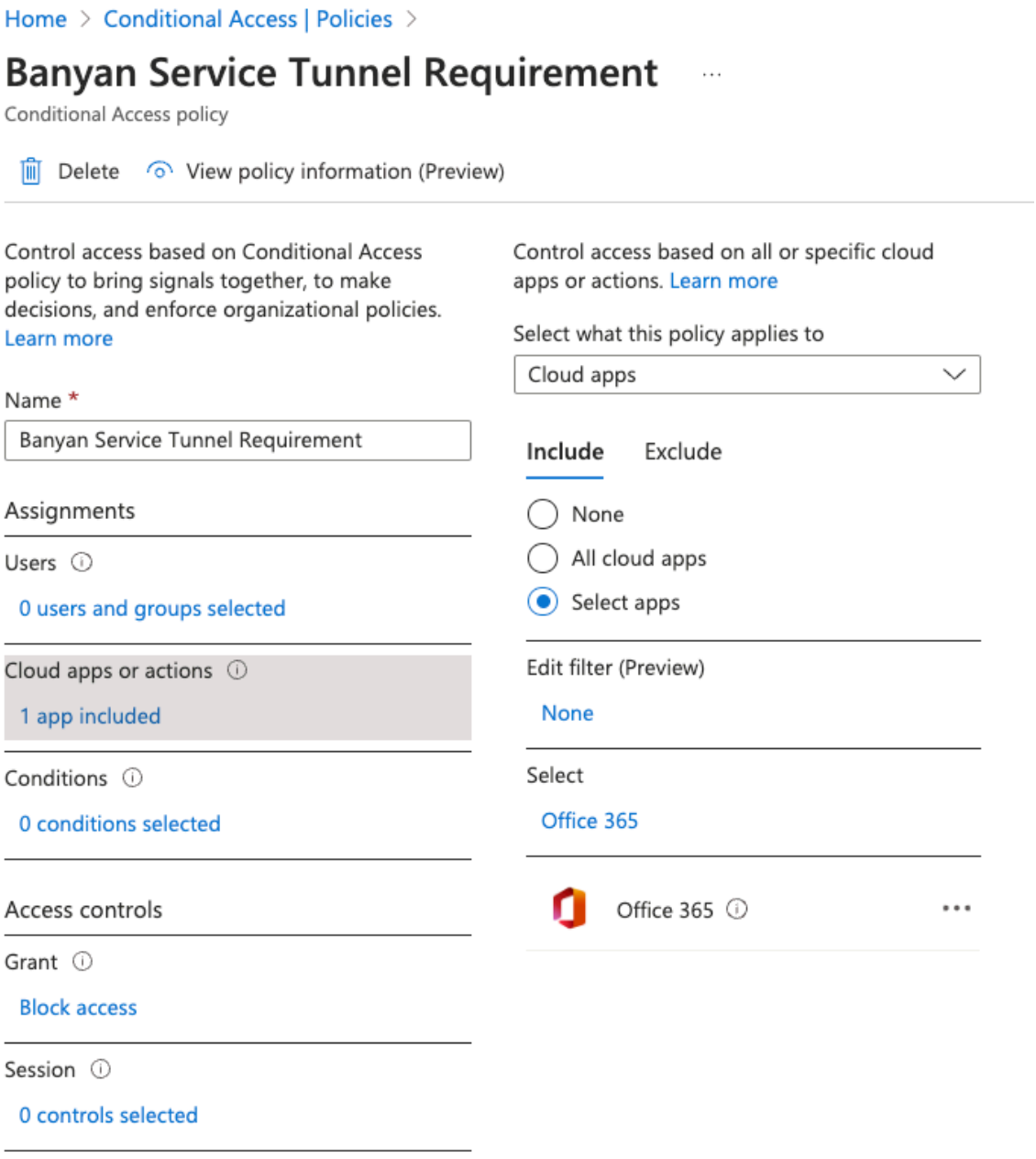


Step 3: Create a Conditional Access policy and assign the location condition

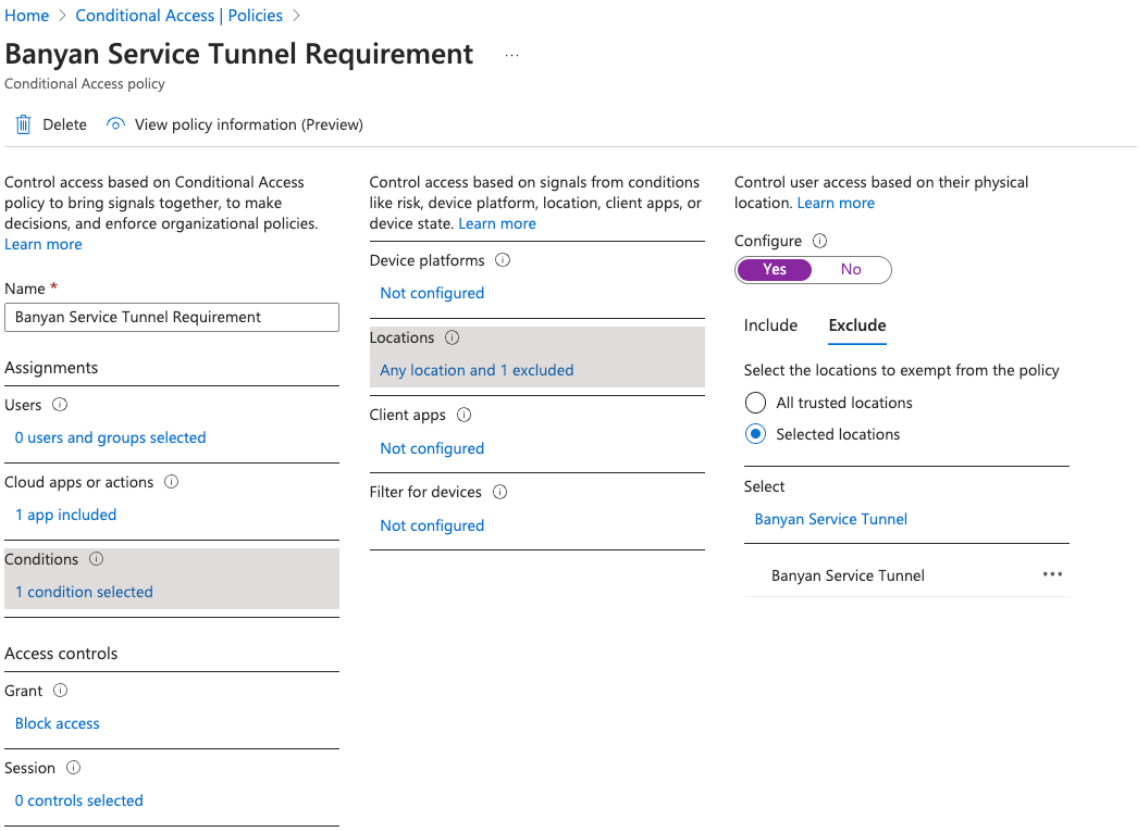
3.1 Navigate from **Entra admin center** > **Protection** > **Conditional Access** > **Policies**, and select **Create new policy**.

3.2 Enter a name for the policy and include the following configurations:

- **Assignments:**
  - Cloud apps or actions - Select the relevant application(s) that you want to require a Service Tunnel to be registered for before authenticating to specific SaaS application(s) (e.g., Office 365).



- **Conditions:**
  - Locations - Set **Configure** to **Yes**, and **Exclude the location(s)** defined in **Step 2**.

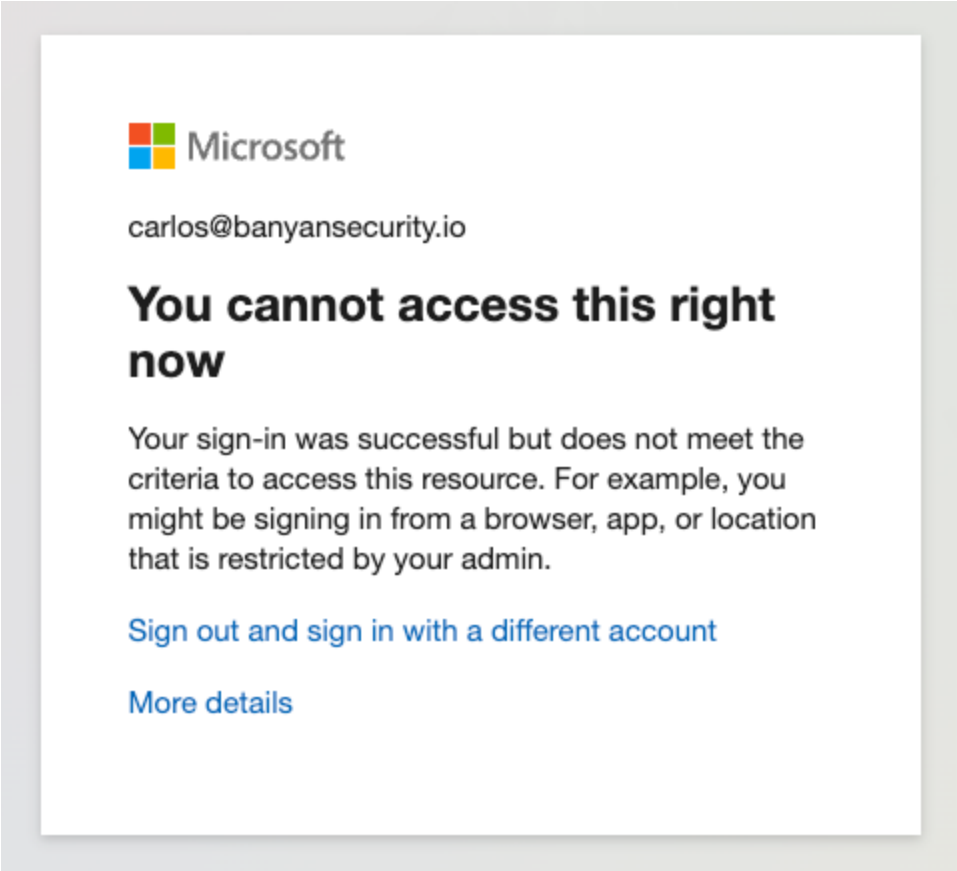


- **Access Controls:**
  - Grant - Set to **Block access**.

3.3 Enable the policy, and **Save**.

Expected Behaviour

If the user DOES NOT have the Service Tunnel connection established, the user will receive an error message indicating that they cannot access the resource (see below). The user(s) must have the relevant Service Tunnel connection established in order to access the resource (e.g., Office 365).



SONICWALL
CLOUD SECURE EDGE

Site generated at YYYYMMDD

Links

- Concepts
- Components
- Release Notes

Guides

- Quick Start Guides
- Solutions
- Feature Guides
- API Guide