

[Home](#) > [Public Applications](#) > [Entra ID](#) >

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

Steps

Step 1: Register a Service Tunnel for Public Domains

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

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

Expected Behaviour

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](#)).

PUBLIC DOMAINS

What domains should be routed through this tunnel?

login.microsoftonline.com	-
login.live.com	-
ex. www.public-domain.com	+

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.

New location (IP ranges) ×

[↑](#) Upload [↓](#) Download

Configure named location IPv4 and IPv6 ranges. [Learn more](#)

Name *

✓

Mark as trusted location

[+](#)

Enter a new IPv4 or IPv6 range

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).

[Home](#) > [Conditional Access | Policies](#) >

Banyan Service Tunnel Requirement

Conditional Access policy

 Delete  View policy information (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Banyan Service Tunnel Requirement

Assignments

Users ⓘ

0 users and groups selected

Cloud apps or actions ⓘ

1 app included

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

Block access

Session ⓘ

0 controls selected

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps

Include Exclude

None

All cloud apps

Select apps

Edit filter (Preview)

None

Select

Office 365



Office 365 ⓘ



- **Conditions:**

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

Banyan Service Tunnel Requirement

Conditional Access policy

Delete View policy information (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *
Banyan Service Tunnel Requirement

Assignments

Users
0 users and groups selected

Cloud apps or actions
1 app included

Conditions
1 condition selected

Access controls

Grant
Block access

Session
0 controls selected

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

Device platforms
Not configured

Locations
Any location and 1 excluded

Client apps
Not configured

Filter for devices
Not configured

Control user access based on their physical location. [Learn more](#)

Configure
Yes No

Include Exclude

Select the locations to exempt from the policy

All trusted locations
Selected locations

Select

Banyan Service Tunnel

Banyan Service Tunnel ...

- **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).



carlos@banyansecurity.io

You cannot access this right now

Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.

[Sign out and sign in with a different account](#)

[More details](#)



© 2026. All rights reserved.

Site generated at YYYYMMDD

Links

[Concepts](#)

[Components](#)

[Release Notes](#)

Guides

[Quick Start Guides](#)

[Solutions](#)

[Feature Guides](#)

[API Guide](#)