Forcepoint

Forcepoint CASB

Connecting Office 365 to Forcepoint CASB Using Azure SSO and a Reverse Proxy

Published 2021

Last modified: **28-June-2021**

CONTENTS

Overview of the reverse proxy application for single sign-on

This document provides the setup instructions for configuring single sign-on (SSO) to Microsoft Office 365 with Microsoft Azure Active Directory (AD) as the identity provider. This configuration requires the creation of a reverse proxy application and conditional access policy in Azure AD.

If you use Azure SSO for Office 365, then user activities are not audited in real-time in the Forcepoint CASB proxy when working in reverse proxy mode. To remedy this, Forcepoint recommends configuring a reverse proxy application in Azure AD. Setting up the reverse proxy application allows you to redirect unmanaged endpoints on your network through Forcepoint CASB and block unauthorized access to Office 365 from unmanaged endpoints unless they go through the Forcepoint CASB service.

License requirements

To create the reverse proxy application and conditional access policy, you must have either an **Azure AD Premium P1** license or an **Azure AD Premium P2** license.

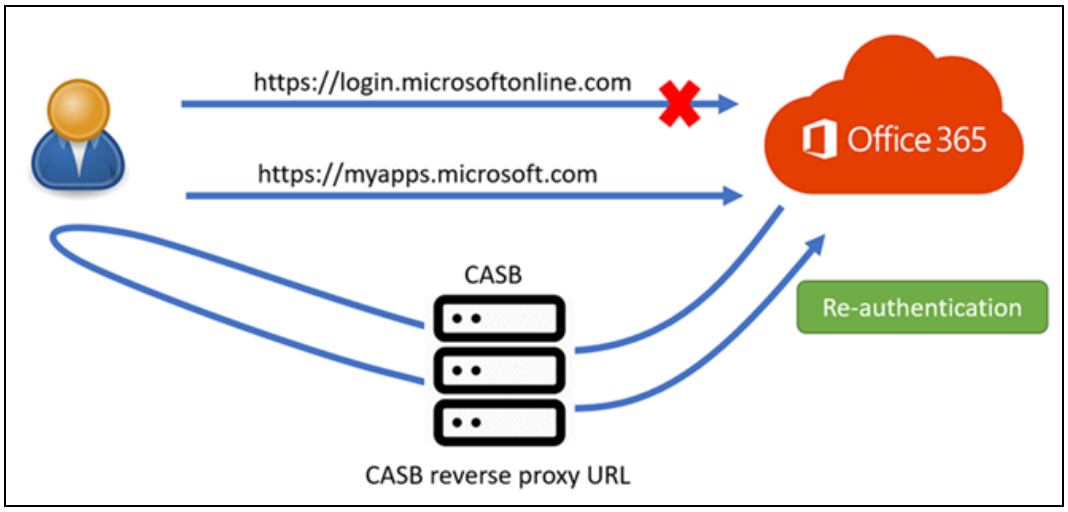
General workflow

To successfully create and configure the reverse proxy application, you must complete the following procedures:

1. **Configure the Forcepoint CASB proxy URL**. Add the proxy URL for Office 365 in Forcepoint CASB. The traffic from unmanaged devices is redirected through this reverse proxy URL. For more information, see "Configuring the reverse proxy URL in Forcepoint CASB" on page 3.
2. **Create the reverse proxy application in Azure**.Create the reverse proxy application in Azure and configure the single sign-on with SAML. For more information, see "Creating the reverse proxy application in Azure" on page 4.
3. **Test the application**. Verify that the traffic is redirected. For more information, see "Test the reverse proxy application" on page 6.
4. **Configure the conditional access policy**. Define the criteria to control which endpoints access your Office 365 services. For more information, see "Configuring the conditional access policy" on page 7.
5. **Validate the conditional access policy**. Verify that the traffic from unmanaged devices cannot access your Office 365 services. For more information, see "Validate the conditional access policy" on page 9.

After the reverse proxy application and conditional access policy are configured and active:

- If a user tries to connect to Microsoft Online (https://login.microsoftonline.com) directly from an unmanaged endpoint, then they will be blocked through the conditional access policy. The policy allows access through the Forcepoint CASB gateways only.
- If a user connects to Microsoft Apps (http://myapps.microsoft.com) and opens the reverse proxy application, then Forcepoint CASB redirects the user to the correct reverse proxy URL. The user can access their applications after they re-authenticate.



Configuring the reverse proxy URL in Forcepoint CASB

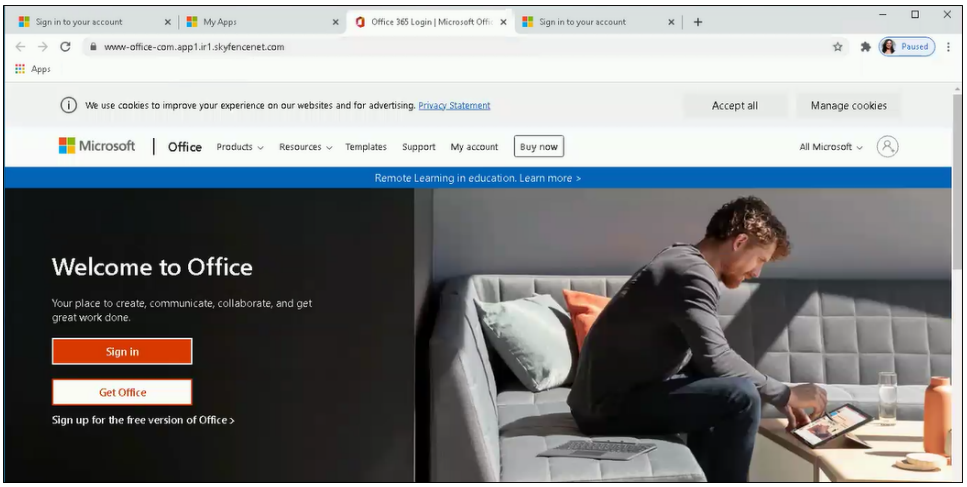
In this section, you will add the proxy URL for Office 365 in Forcepoint CASB. The traffic from unmanaged devices is redirected through this reverse proxy URL.

Before you begin, make sure that you have a Forcepoint CASB administrator account.

Configure the reverse proxy URL

1. In Forcepoint CASB, go to **Settings > Resources > Assets**.
2. Select your Office 365 asset.
3. On the **General Asset Information** page, open the **Access Mapping** section.
4. Click **Add URL Mapping**.
5. Enter the following information:
   - Forcepoint CASB proxy URL: This URL is created by the customer based on their internal environment.
   - Service URL: `login.microsoftonline.com`
6. Click **Save**.

   After you configure this proxy URL, Forcepoint CASB redirects browser requests for **login.microsoftonline.com** to your proxy URL when the user attempts to connect through an unmanaged endpoint.



Creating the reverse proxy application in Azure

In this section, you will create the reverse proxy application in Azure, then test the application to ensure that it works correctly.

Before you begin, make sure that you have:

- Administrator access to the Azure Portal for your organization (Premium P1 or higher license)
- User access to the Office 365 Portal for your organization

Important: The procedures in this section describe the current Azure workflow. Microsoft can change the appearance or workflow of Azure at any time. Forcepoint makes every effort to keep these procedures up-to-date, but they might differ from what is available in Azure. For more information about managing applications in Azure, see the Microsoft Azure documentation.

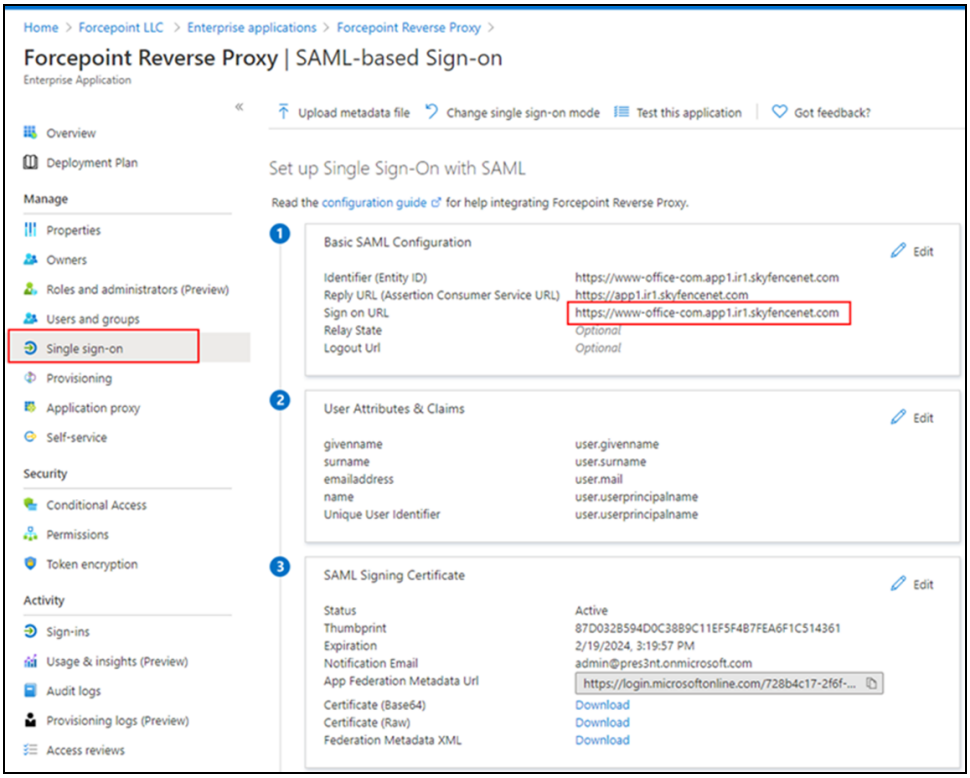
Create the reverse proxy application

1. Sign in to the Azure Portal with an Azure administrator account.
2. Go to **Azure Active Directory > Enterprise Applications**.
3. Click **New Application**.
4. Click **Non-gallery Application**.
5. In the **Add your own application** panel, enter a **Name** for the application, such as **Forcepoint Reverse Proxy**.
6. Click **Add**. Azure opens the application configuration screen. Verify that you are on this page before continuing. The correct page shows your application name in the top left corner.
7. Click **Users and groups**.
8. Click **Add user**.
9. Under **Add Assignment**, click **Users and groups**.
10. Under **Users and groups**, select the users or groups within your Azure Active Directory that need to use the reverse proxy. To search for specific users or groups, type the name or email address into the search box, then select them from the results.

    The users and groups added here will see the Forcepoint Reverse Proxy application in their MyApps list.
11. Click **Select**.
12. Under **Add Assignment**, click **Assign**.
13. On the application's configuration screen, click **Single sign-on** from the left navigation menu.

14. Click **SAML**.
15. On the **Set up Single Sign-On with SAML** page, in the **Basic SAML Configuration** section, click the pencil (edit) icon.
16. Update the following information:
    - **Identifier**: This value uses the reverse proxy URL from Forcepoint CASB and the `https://www-office-com.` prefix.
    - **Reply URL**: This value uses the reverse proxy URL from Forcepoint CASB and the `https://` prefix.
    - **Sign on URL**: This value uses the reverse proxy URL from Forcepoint CASB and the `https://www-office-com.` prefix.

    For example, if the reverse proxy URL in Forcepoint CASB is `app1.ir1.skyfencenet.com`, then you would enter the following information:
    - **Identifier**: `https://www-office-com.app1.ir1.skyfencenet.com`
    - **Reply URL**: `https://app1.ir1.skyfencenet.com`
    - **Sign on URL**: `https://www-office-com.app1.ir1.skyfencenet.com`



17. Click **Save**.

Edit the reverse proxy application

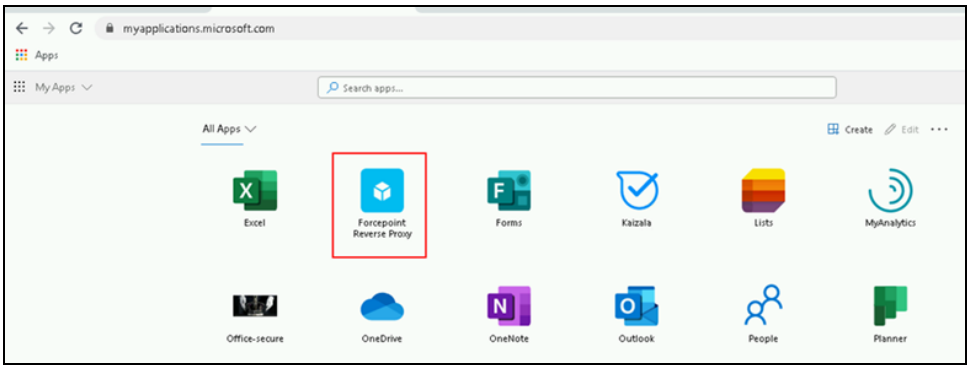
If you need to edit the reverse proxy application after you create it, follow these steps to open the application.

1. Sign in to the Azure Portal with an Azure administrator account.
2. Go to **Azure Active Directory > Enterprise Applications > All applications**.
3. Select your reverse proxy application from the list and edit it as needed.
4. After you complete your edits, click **Save**.

Test the reverse proxy application

After you create the reverse proxy application, it is available for all users added to the application when they sign in. Follow the steps below to make sure that the reverse proxy application works for the configured users.

1. As a user assigned to the reverse proxy application, sign in to http://myapps.microsoft.com.
2. In the Apps list, click the reverse proxy application. In the example above, we created the **Forcepoint Reverse Proxy** application.



3. Re-authenticate the user. After successful re-authentication, Office 365 redirects to the **Sign on URL** configured when you created the application.

Configuring the conditional access policy

In this section, you will define the criteria to control which endpoints access your Office 365 services.

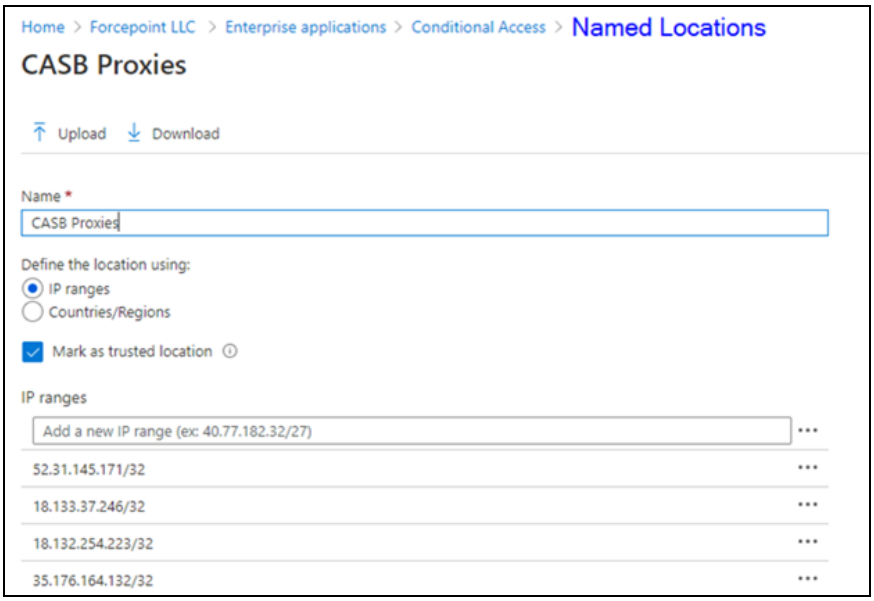
Before you begin, make sure that you have administrator access to the Azure Portal for your organization (Premium P1 or higher license).

Important: The procedures in this section describe the current Azure workflow. Microsoft can change the appearance or workflow of Azure at any time. Forcepoint makes every effort to keep these procedures up-to-date, but they might differ from what is available in Azure. For more information about conditional access policies, see the Microsoft Azure documentation.

Define the locations to exclude from the policy

Before you create the conditional access policy, you need to define the IP ranges that should be excluded from the policy.

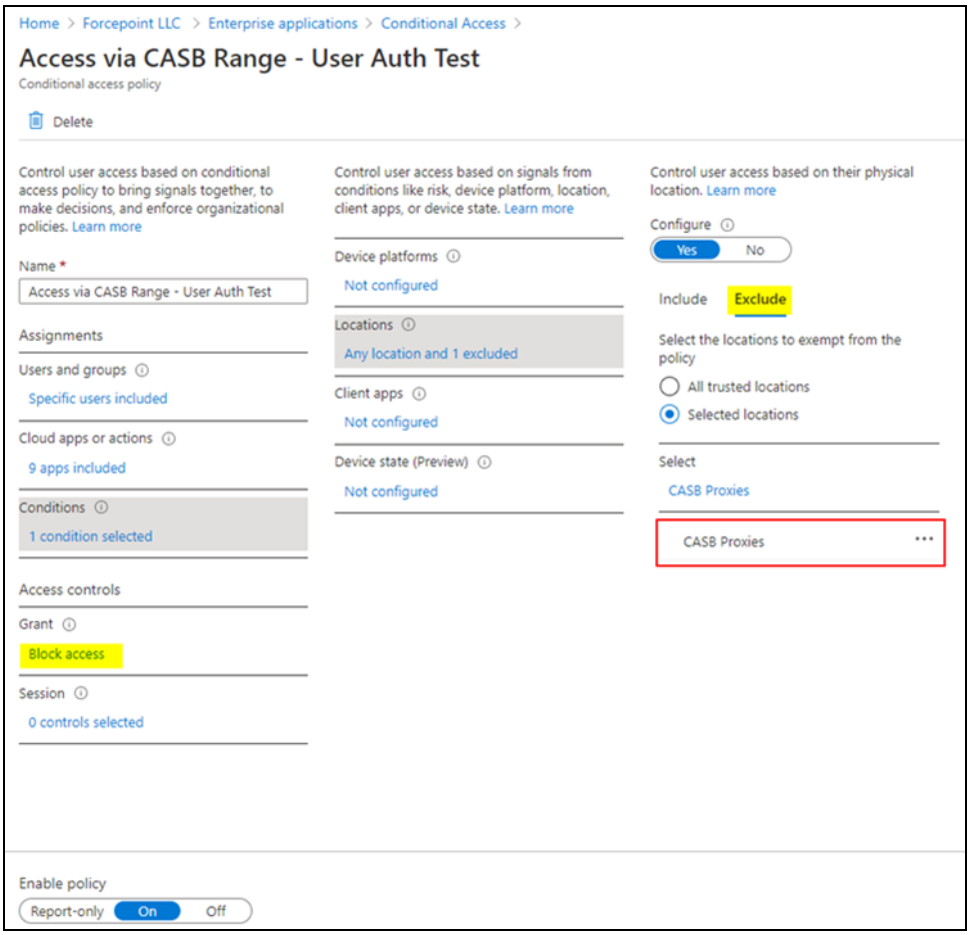
1. Sign in to the Azure Portal with an Azure administrator account.
2. Go to **Azure Active Directory > Security > Conditional Access > Named Locations**.
3. Click **New location**.
4. On the **New** page, enter a **Name** for the location, such as **CASB Proxies**.



5. Under **Define the location using**, select **IP ranges**.
6. Select **Mark as trusted location**.
7. Under **IP ranges**, add the IP address ranges specific to the region for your Forcepoint CASB gateway. For a list of IP address ranges for the gateways, see the **Forcepoint CASB Gateway IP Ranges** article.
8. Click **Save**.

Create the conditional access policy

1. If you are not already in Azure, sign in to the Azure Portal with an Azure administrator account.
2. Go to **Azure Active Directory > Security > Conditional Access**.
3. Click **New policy**.
4. On the **New** page, enter a **Name** for the policy, such as **Access via CASB Range**.
5. Under **Assignments**, select the **Users and groups** to be included in the policy.
6. Under **Assignments**, select the cloud apps to be included in the policy. The Microsoft cloud applications you select here will be blocked from direct access.
    a. Click **Cloud apps or actions**.
    b. Select **Cloud apps**.
    c. Under **Include**, select one of the following options:
        - **All cloud apps** to include all available Microsoft cloud applications in the policy
        - **Select apps** to choose specific Microsoft cloud applications, such as Office 365, Outlook Groups, or Teams.
7. Under **Assignments**, add a condition to exclude the Forcepoint CASB IP ranges:
    a. Click **Conditions**.
    b. Click **Locations**.
    c. Under **Configure**, click **Yes**.
    d. Under **Exclude**, select the condition created above (**CASB Proxies** in this example).



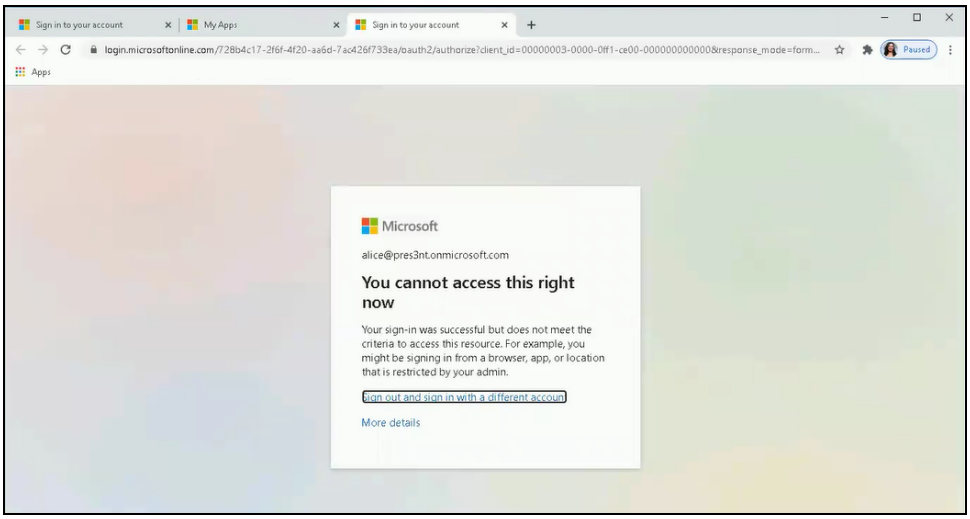
8. Under **Access controls**, click **Grant** and select **Block access**. This will block access to all locations, except for the excluded CASB Proxies locations selected above.
9. Under **Enable policy**, click **On**.
10. Click **Create**.

Validate the conditional access policy

After you create the conditional access policy, validate that unmanaged devices cannot access your Office 365 account.

1. From an unmanaged endpoint, open your browser and go to **https://login.microsoftonline.com**.
2. Authenticate as a user that was added to the conditional access policy.

   If the conditional access policy is configured correctly, then the user sees the following screen (or one similar) and cannot access their Microsoft Apps.



3. To authenticate this user correctly, sign in to **http://myapps.microsoft.com** using the procedure in "Test the reverse proxy application" on page 6.

Managed endpoints can access their Microsoft applications through **https://login.microsoftonline.com**.