

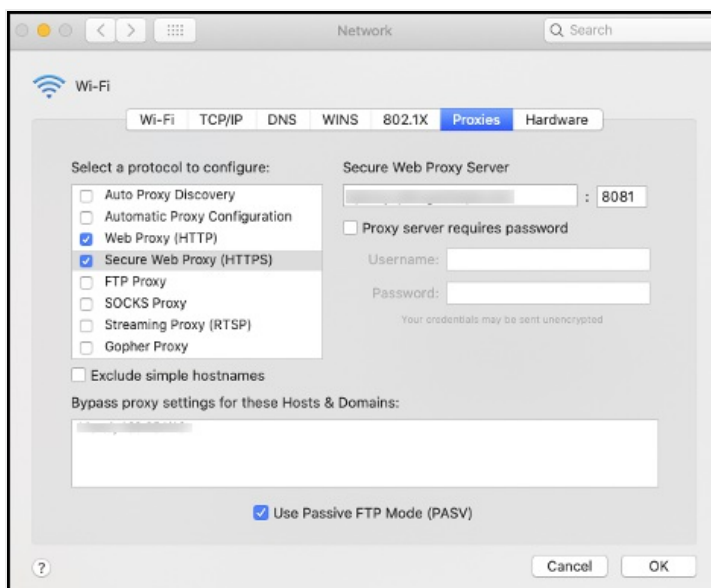
Explicit Proxy

Explicit Proxy provides a new method for steering traffic from any device to the Netskope Cloud using a Proxy Auto Configuration (PAC) file. A PAC file tells a browser to forward traffic to a proxy server instead of the destination server. When a user opens a browser, the browser sends a request for the default PAC file, and then uses the instructions to forward traffic to the Netskope URL in the PAC file.

A PAC file template can be downloaded from the Netskope UI for you to create your own custom PAC file. Your modified PAC file can be hosted on-premises so that devices can retrieve it automatically. User identity can be retrieved with the help of an IdP that uses SAML 2.0, and this can be configured in the Netskope UI under **Settings > Security Cloud Platform > Forward Proxy > SAML**.

Explicit Proxy can be used these ways:

- Modify the [PAC file template](#) (or modify an existing PAC file), and then distribute your PAC file. Click **Download Sample PAC File** on the Explicit Proxy page to get a PAC file template you can modify.
- Configure SAML 2.0 authentication using [SAML Forward Proxy](#). The user's browser must be set up to use port . Authentication is used to get the identity of the user, which can be applied in Policies, for example. To enable authentication after configuring the forward proxy, refer to [Forward Proxy Authentication](#).
- Endpoints can be configured to use the proxy directly. For example:



- HTTP and HTTPS traffic (typically on ports 80, and 443, but Netskope also supports custom ports) for the Explicit Proxy. Do not send any other traffic through these ports.
- Consider these factors for Box endpoints when using explicit proxy:
 - Policies that are user specific for access to specific apps, instances, or SSL decryption, etc., will not be enforced.
 - Events (Application/Page) will not show user information, but will show the IP address of the user.

If the Netskope root CA has not been previously installed on the endpoint, download it from the Netskope UI at **Settings > Security Cloud Platform > Manage > Certificates > Signing CA** and install it on your endpoints (for macOS: install it in Certificates from the Keychain Access tool). There is a separate certificate available for remote users.

When finished with the above preparations, go to **Settings > Security Cloud Platform > Traffic Steering > Explicit Proxy**.

Explicit Proxy [DOWNLOAD SAMPLE PAC FILE](#)

Cloud Explicit Proxy helps you steer traffic directly from endpoints to the Netskope Cloud. This can be done using Proxy Auto-Configuration (PAC) files or by modifying the endpoints' or applications' Proxy configuration settings. A PAC file template can be downloaded from the Netskope admin console, and modified to suit your deployment.

In order to build policies that leverage user identity, authentication using an Identity Provider (IdP) is required and can be configured in the Netskope admin console. This steering method supports traffic originating from known locations (offices or branches) or unknown locations (home offices). [View the help documentation](#) for configuring different scenarios.

Note: Explicit Proxy over a GRE or IPsec is a different steering method. [Learn more](#) about it in the help documentation.

Explicit Proxy Destination

Use this proxy endpoint and certificates for your devices. You can also find the certificates on the [Certificates](#) page.

Explicit Proxy Destination: eproxy-easyskope.stg.local:8081

[DOWNLOAD ROOT CERTIFICATE \(REMOTE USERS\)](#)

Tenant Lookup Service

Tenant Lookup Service is used when users are coming in from unknown locations, such as remote users. Netskope will prompt the end user to enter the tenant (organization) name.

Tenant Name: easyskope

[PREVIEW](#)

IP Address Allowlist & User Identity

Unauthenticated Traffic: ● Allow [EDIT](#)

Netskope will allow unauthenticated traffic originating from the IP addresses listed below. Authentication is required for users from unknown locations.

[ADD IP ADDRESS](#)

There are three sections on this page:

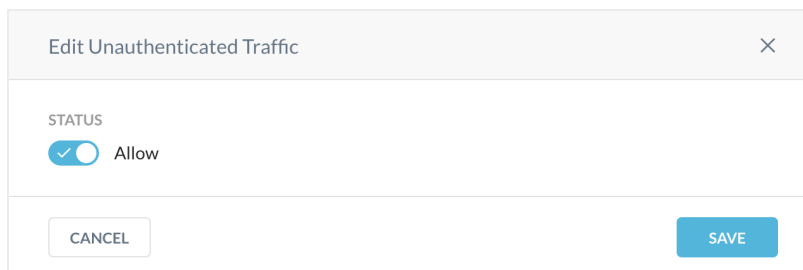
- **Explicit Proxy Destination:** Provides the explicit proxy destination and a link to download the Netskope Certificate for remote users (also available on the Certificates CA Signing .
- **Tenant Lookup Service:** Prompts remote users to enter the Tenant Name shown here. Once configured, users will be prompted for an organization (tenant) name that is provided to them by their administrators. Once validated, users will be redirected to

authenticate with their IdP before being able to access the web. Authentication is mandatory for remote users.

To view an example of the notification users see, click **Preview**.

- **IP Address Allowlist & User Identity:** Enables you to allow unauthenticated traffic.

To use this feature, click **Edit** and enable the **Allow** toggle.




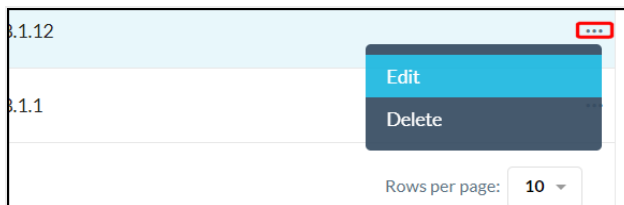
This section also allows you to specify source egress IP addresses for your on-premises users.


To allowlist your on-premises source egress IP address(es) in the Netskope UI:

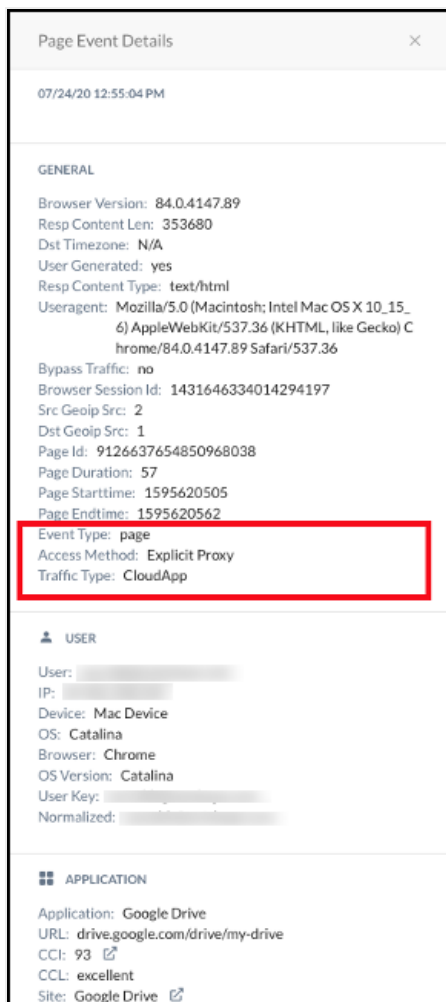
1. Go to the IP Address Allowlist & User Identity section, click **Add IP Address**.
2. Enter a name and the source egress IP address for your office location to allowlist so that Netskope will accept the traffic from devices behind the IP address or CIDR. Multiple IP addresses need to be separated by a comma, or you can add them separately using the **Add Another** button. When finished, click **Add**.



To edit or delete an IP address or range, click the  icon. Only one IP address or CIDR can be edited at a time.



Now your web traffic will be sent to the Netskope Cloud and users will be asked to authenticate to the IdP once they attempt to navigate to any website. To see events in SkopeIT, go to **SkopeIT > Page Events** and click the  icon to view page event details. Explicit proxy will be shown as the access method.



PAC File Template

Modify this PAC file template for Explicit Proxy. Enter the domains not to proxy, the substrings (HTTP/HTTPS) to proxy, and your tenant name.

```
function FindProxyForURL(url, host) {
    /* Normalize the URL for pattern matching */
    url = url.toLowerCase();
    host = host.toLowerCase();
    /* Don't proxy local hostnames */
    if (isPlainHostName(host)) {
        return 'DIRECT';
    }
    /* Don't proxy IDP servers. */
    /*
    if ((dnsDomainIs(host, '.okta.com'))
    {
        return 'DIRECT'
    }
    */
    /* Don't proxy for domains. */
    /*
    if ((dnsDomainIs(host, '.domain-example1.com')) ||
        (dnsDomainIs(host, '.domain-example2.com')))
    {
        return 'DIRECT'
    }
    */
    if (url.substring(0, 5) === 'http:' || url.substring(0, 6) ===
    'https:') {
        return 'PROXY eproxy-<tenant-name>.goskope.com:8081';
    }
    return 'DIRECT';
}
```