



# Deliver Conditional Access for ChromeOS in Azure Active Directory Guide

April 2023

## Contents

<b>Introduction</b>	<b>3</b>
<b>Azure Conditional Access for ChromeOS - Microsoft Defender for Cloud Apps</b>	<b>4</b>
Requirements	4
Configuration	4
Overview	4
Certificate Enrollment	5
SSO	5
Conditional Access	5
Defender for Cloud Apps	8
<b>Azure Conditional Access for ChromeOS - Netskope</b>	<b>13</b>
Requirements	13
Configuration	13
Google SSO with Azure	13
Netskope SSO with Azure	15
Configure Chrome traffic steering	19
Conditional Access	21
<b>Verified Access for ChromeOS via SAML SSO - Netskope</b>	<b>26</b>
Requirements	26
Configuration	26
Google Cloud Verified Access API	26
Netskope SAML Reverse Proxy	30
3P SAML IdP for Netskope (Azure AD in this example)	33
Chrome Device policy	36
Google SAML SSO with Netskope	37



## Introduction

As an Azure AD customer, you probably use Conditional Access. By following this guide, you can learn how to deliver Conditional Access for ChromeOS in Azure AD environments using various integrations<sup>1</sup>.

For more details on Conditional Access, see [What is Conditional Access?](#)

---

<sup>1</sup> While ChromeOS is not a directly Microsoft-supported device platform for Azure AD Conditional Access, this guide shows how you can still implement this functionality in your environment.

## Azure Conditional Access for ChromeOS - Microsoft Defender for Cloud Apps

A solution that enables ChromeOS integration, authorized by device certificate, with Azure Conditional Access through [Microsoft Defender for Cloud Apps](#).

### Requirements

1. Managed ChromeOS devices
2. ChromeOS device certificates deployed via SCEP
3. Azure AD as source of identity, federated into google
4. MDCA

### Configuration

#### Overview

This solution is intended to allow administrators to restrict access in the following two scenarios:

1. Only allow authorized enterprise users logged in to enterprise-managed ChromeOS devices to access Microsoft Azure applications, such as Office365.
2. Prevent enterprise users from logging in to unmanaged ChromeOS devices.

This solution utilized Azure Active Directory [Conditional Access](#). AADCA makes policy decisions based on signals. Signals describe the user, device, application and so on.

User authentication is outside the scope of this document, but we assume that authorized enterprise users are able to authenticate against Azure AD using one or more factors.

Azure AD Applications include Microsoft provided ones, such as Office365, and custom applications, such as the Enterprise Application used to provide SAML SSO for the Google tenant.

The device signal that can be used for ChromeOS devices is a valid device certificate, verified via MDCA. For other device types, such as Windows, Microsoft Intune agent can provide device signals to be used in AADCA policy decisions.

For the first scenario, an AADCA policy with conditions of authorized user and valid

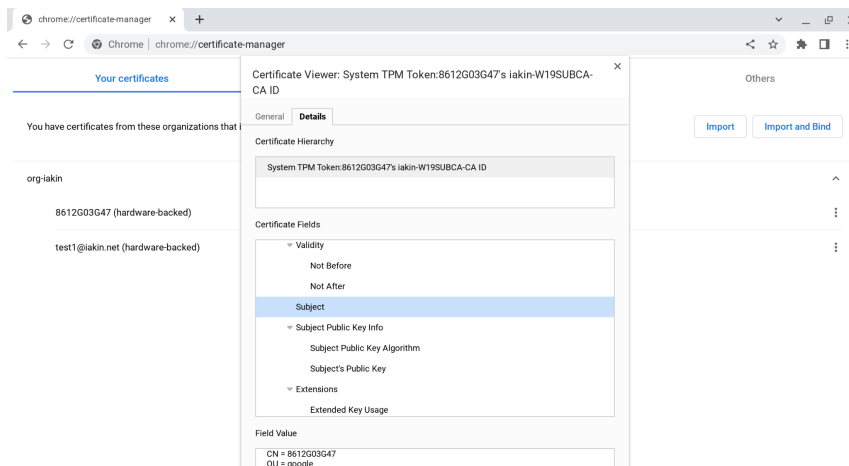
device certificate can be used, with the relevant applications selected, such as Office365.

For the second scenario, the same user and certificate conditions apply, with the Enterprise Application used for Google SAML SSO selected.

**Note that with the policy applied to the Google SSO app, any user subject to Azure SSO can only sign in to any Google services from a managed device with a valid certificate.**

## Certificate Enrollment

1. Configure ChromeOS devices to receive a **device** certificate using [this guide](#) or another mechanism.  
The Root and signing CA certificates from the CA above will need to be added to MDCA.
2. Verify that a ChromeOS device belonging to the relevant tenant and organizational unit is successfully obtaining a certificate via `chrome://certificate-manager`.

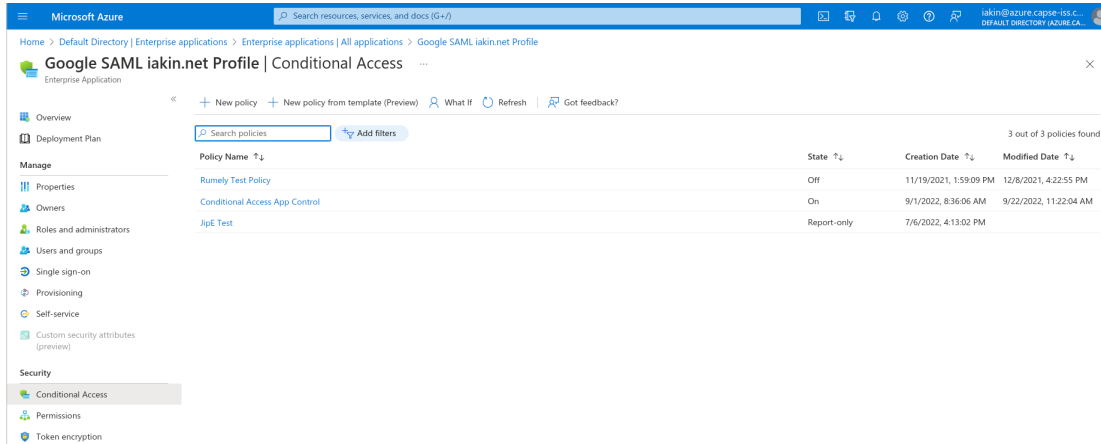


## SSO

1. Configure SSO and user provisioning between Azure and the Google tenant [per documentation](#).
2. Verify that a user can log in to a ChromeOS device with Azure AD credentials.

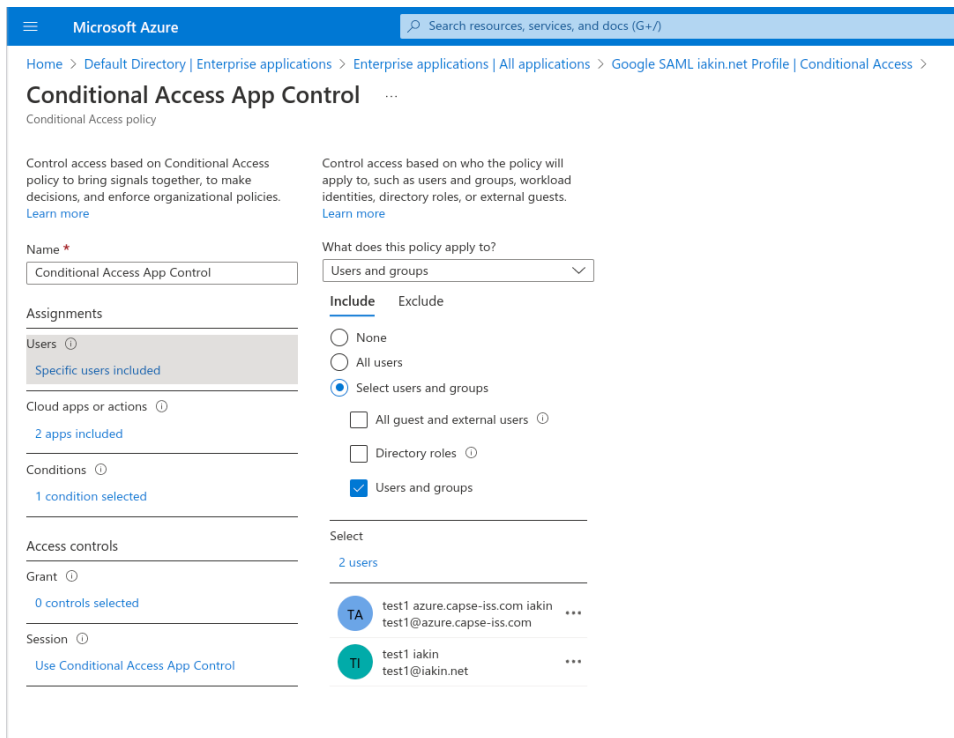
## Conditional Access

1. In Azure Enterprise Application with SAML SSO for the Google tenant, click on [Conditional Access](#).
  - a. Create a new policy.



Policy Name	State	Creation Date	Modified Date
Rumely Test Policy	Off	11/19/2021, 1:59:09 PM	12/8/2021, 4:22:55 PM
Conditional Access App Control	On	9/1/2022, 8:36:06 AM	9/22/2022, 11:22:04 AM
IpE Test	Report-only	7/6/2022, 4:13:02 PM	

b. Specify the users to whom the policy will apply.



**Conditional Access App Control**

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

Name \*  
Conditional Access App Control

What does this policy apply to?  
Users and groups

**Include** Exclude

None  
 All users  
 Select users and groups

All guest and external users  
 Directory roles  
 Users and groups

**Assignments**

Users  
Specific users included

Cloud apps or actions  
2 apps included

Conditions  
1 condition selected

Access controls

Grant  
0 controls selected

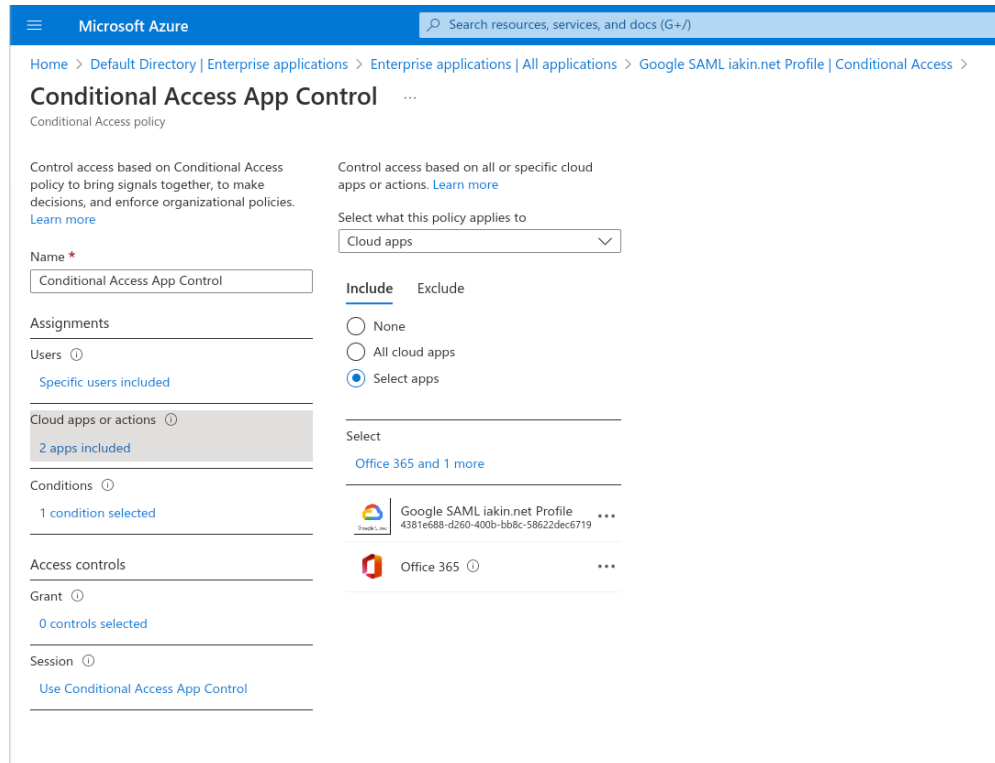
Session  
Use Conditional Access App Control

Select  
2 users

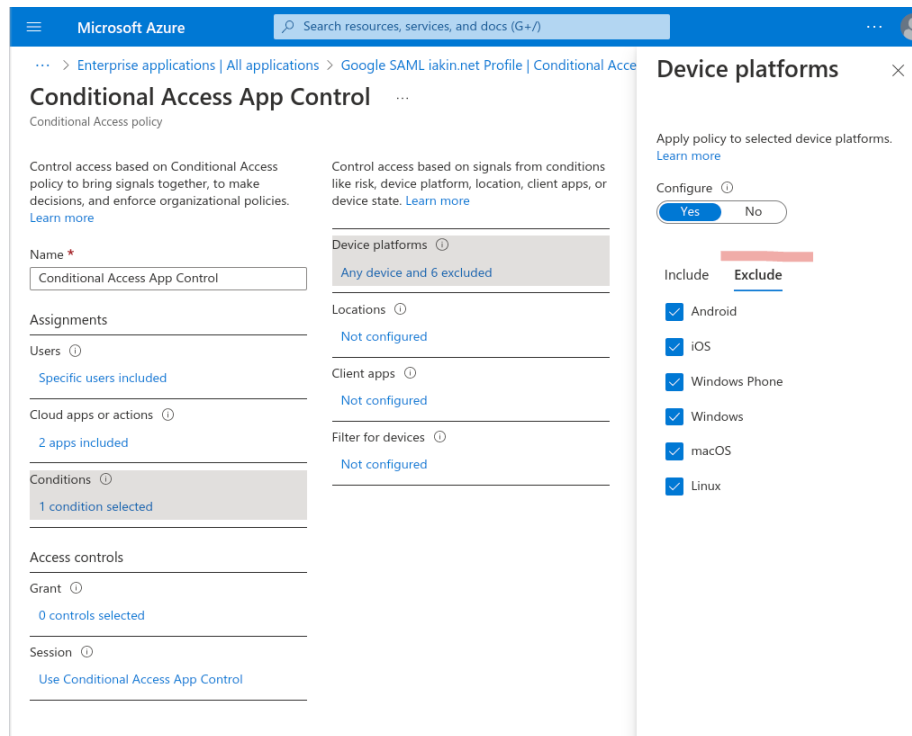
- TA test1.azure.capse-iss.com iakin  
test1@azure.capse-iss.com
- TI test1 iakin  
test1@iakin.net

c. Select the appropriate Cloud apps.

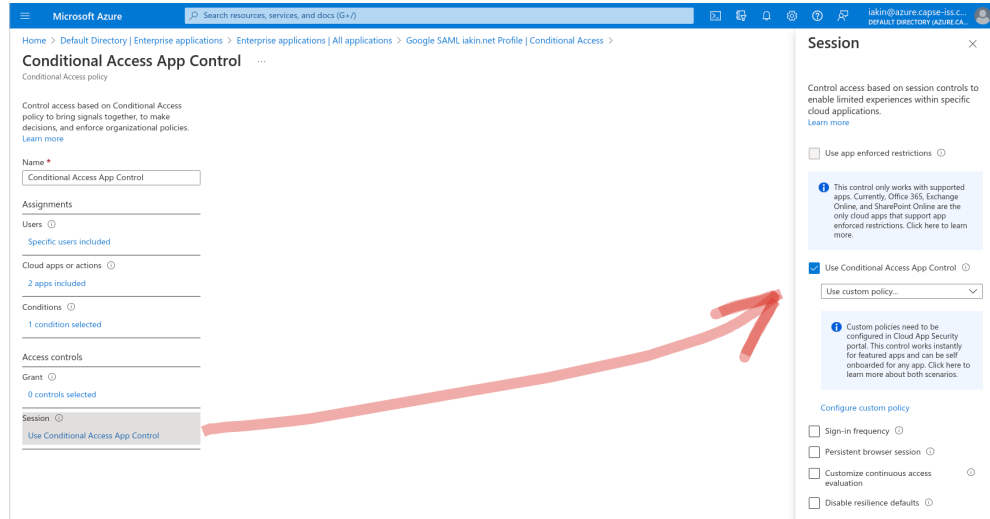
- i. To implement BYOD control, select the Enterprise App for Google SAML SSO, as the policy will apply to any login attempts from the Google tenant via Azure SSO.
- ii. To implement app control in session, select the relevant apps such as Office365.



- d. Exclude all Intune-managed devices since they can be accommodated by other Conditional Access policies.

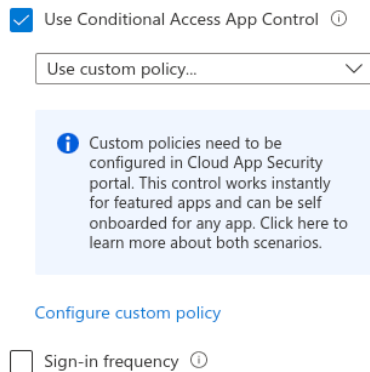


- e. Under Session, check Use Conditional Access App Control to [enable redirection to Defender](#).

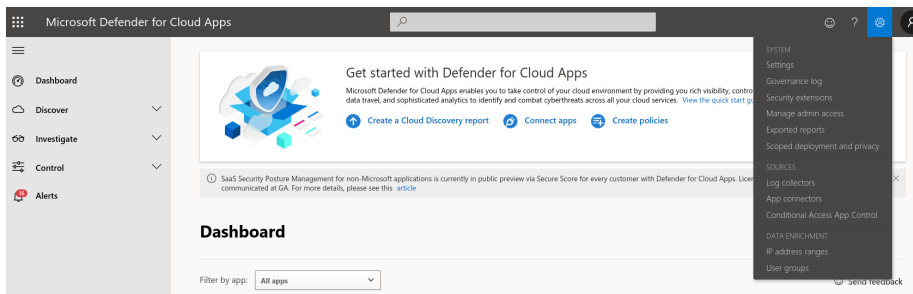


## Defender for Cloud Apps

1. In the Azure Conditional Access policy Session screen, click on Configure custom policy. This opens [Defender for Cloud Apps](#).

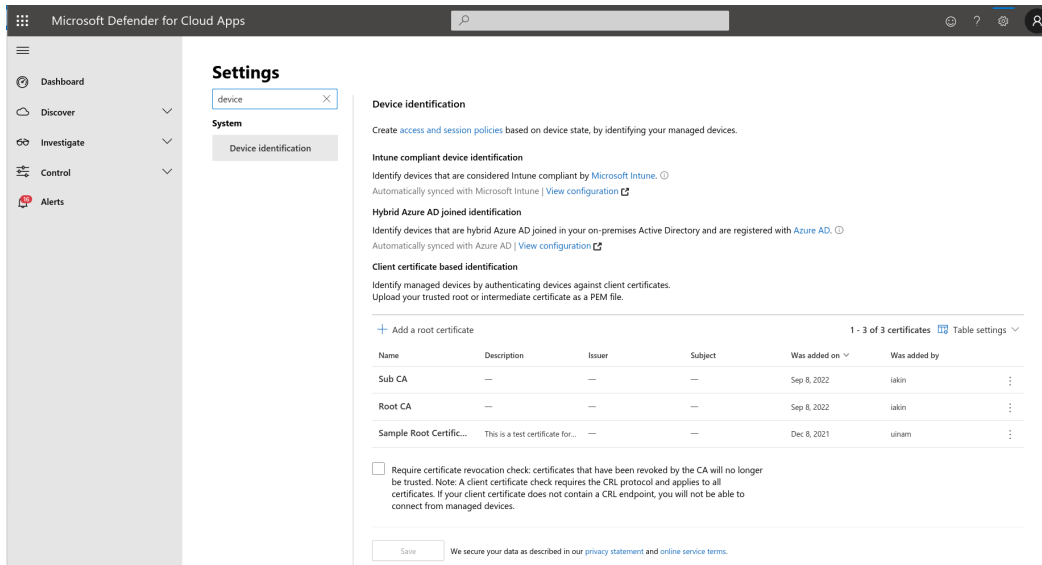


2. Import issuing CA certificate chain
  - a. Open the Settings menu via the gear icon, then choose Settings under System.

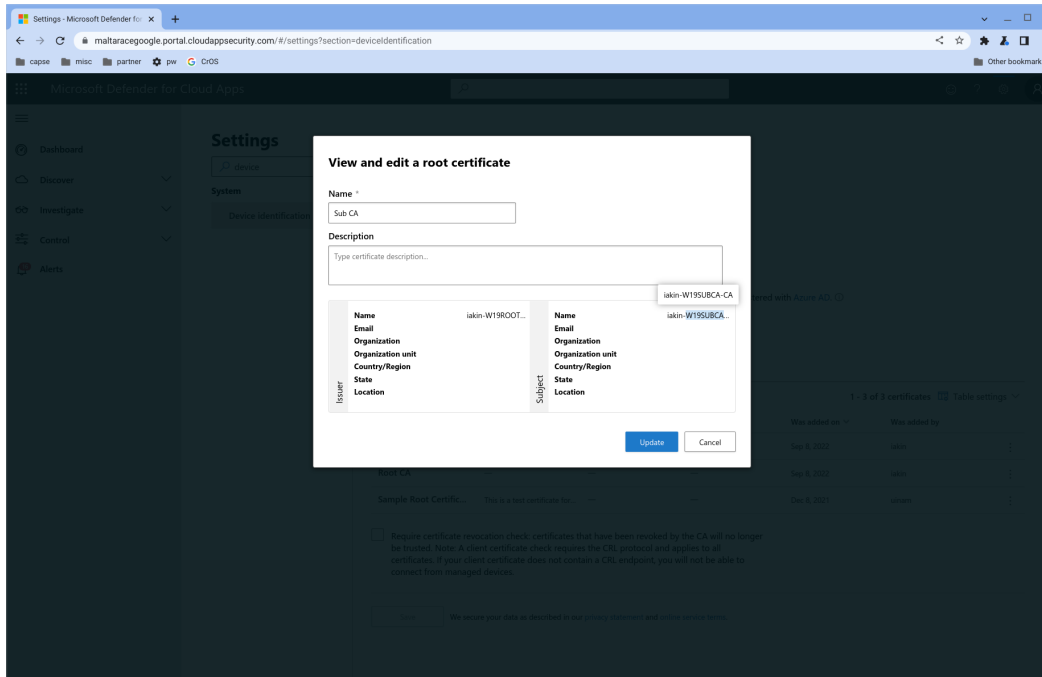


3. Type 'device' in the search box under Settings and click on Device Identification.

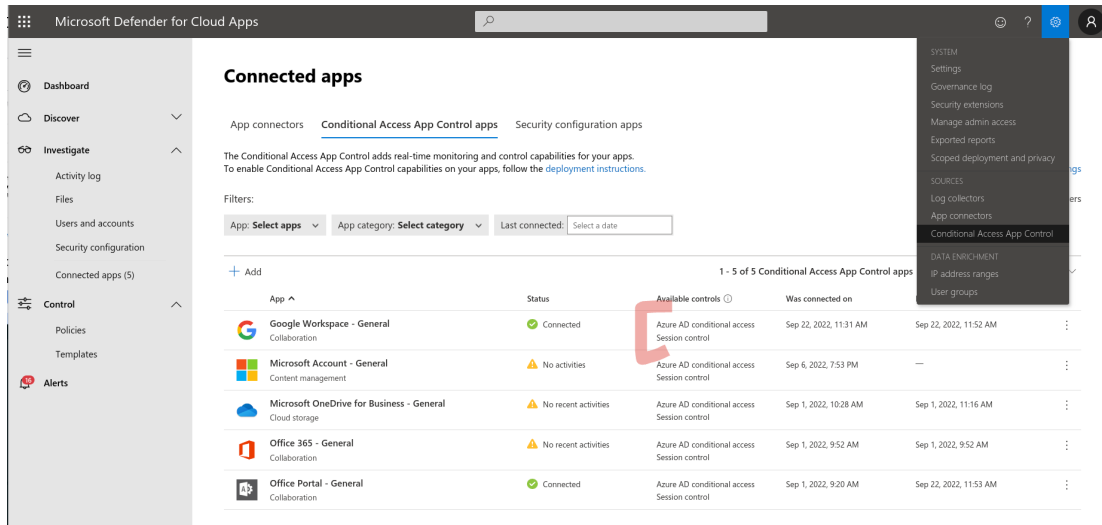




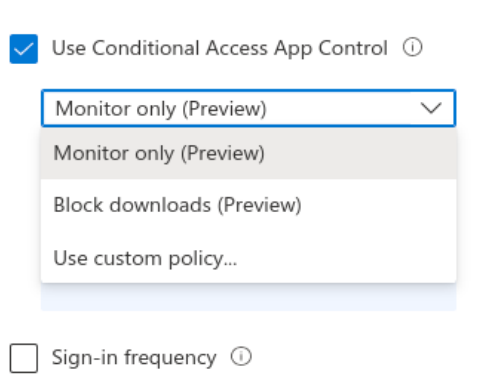
- a. In this screen, import the certificate chain for the CA issuing the ChromeOS device certificates. This is the same certificate chain [imported](#) into Google Admin console during SCEP configuration.



4. [Configure Connected Apps](#)
  - a. Under the Settings gear menu, select Conditional Access App Control.

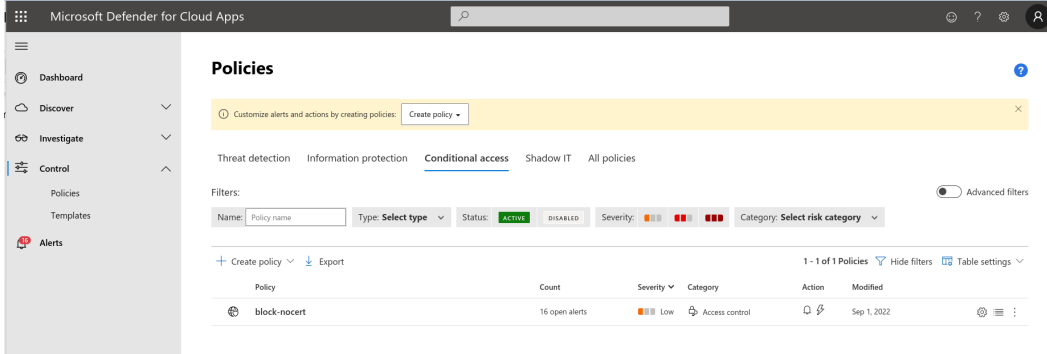


- b. Follow Microsoft Guidance from the above linked document:
- i. *“After you've created the policy, sign in to each app configured in that policy. Make sure you sign in using a user configured in the policy. Defender for Cloud Apps will sync your policy details to its servers for each new app you sign in to. This may take up to one minute. The preceding instructions helped you create a built-in Defender for Cloud Apps policy for catalog apps directly in Azure AD. In this step, verify that the access and session controls are configured for these apps.”*
- c. Ensure that all required apps have Azure AD conditional access and Session control configured. If not, click the three dots to the right of the app, select Edit App and enable Session control. Note that the list of apps here is dynamically populated as users access the apps. In order to populate the list, it is possible to set the [policy in Conditional Access](#) to Monitor Only.

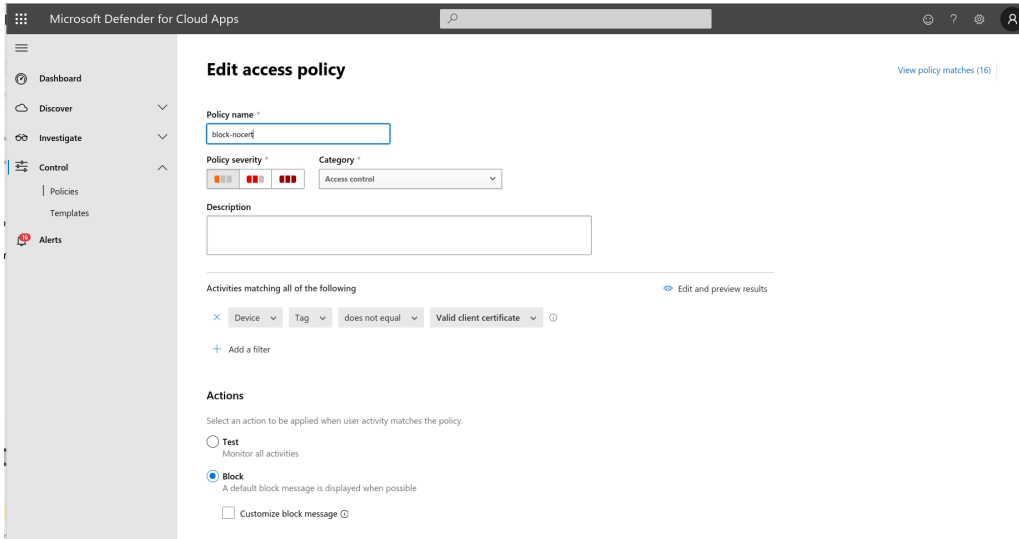


5. In Defender, navigate to [Control->Policies->Conditional Access](#).

6. Create a policy to require a valid device certificate.
  - a. Device Tag
  - b. Not Equals
  - c. Valid client certificate
7. Action Block.



The screenshot shows the 'Policies' page in Microsoft Defender for Cloud Apps. The left sidebar contains navigation options: Dashboard, Discover, Investigate, Control, Policies, Templates, and Alerts. The main content area is titled 'Policies' and includes a 'Create policy' button. Below this, there are tabs for 'Threat detection', 'Information protection', 'Conditional access', 'Shadow IT', and 'All policies'. The 'Conditional access' tab is selected. A 'Filters' section allows filtering by Name, Type (Set to 'Select type'), Status (Set to 'ACTIVE'), Severity (Set to 'Low'), and Category (Set to 'Select risk category'). A table below shows one policy: 'block-nocerf' with 16 open alerts, Low severity, and Access control category. The table has columns for Policy, Count, Severity, Category, Action, and Modified.



The screenshot shows the 'Edit access policy' page in Microsoft Defender for Cloud Apps. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Edit access policy' and includes a 'View policy matches (16)' link. The 'Policy name' field contains 'block-nocerf'. The 'Policy severity' is set to 'Low' and the 'Category' is 'Access control'. There is a 'Description' text area. Below this, the 'Activities matching all of the following' section shows a filter: 'Device Tag does not equal Valid client certificate'. There is an 'Add a filter' button. The 'Actions' section has two options: 'Test' (Monitor all activities) and 'Block' (A default block message is displayed when possible). The 'Block' option is selected. There is also a 'Customize block message' checkbox.

## Azure Conditional Access for ChromeOS - Netskope

Provide Azure Conditional Access for ChromeOS authorized by egress IP address with [Netskope](#).

### Requirements

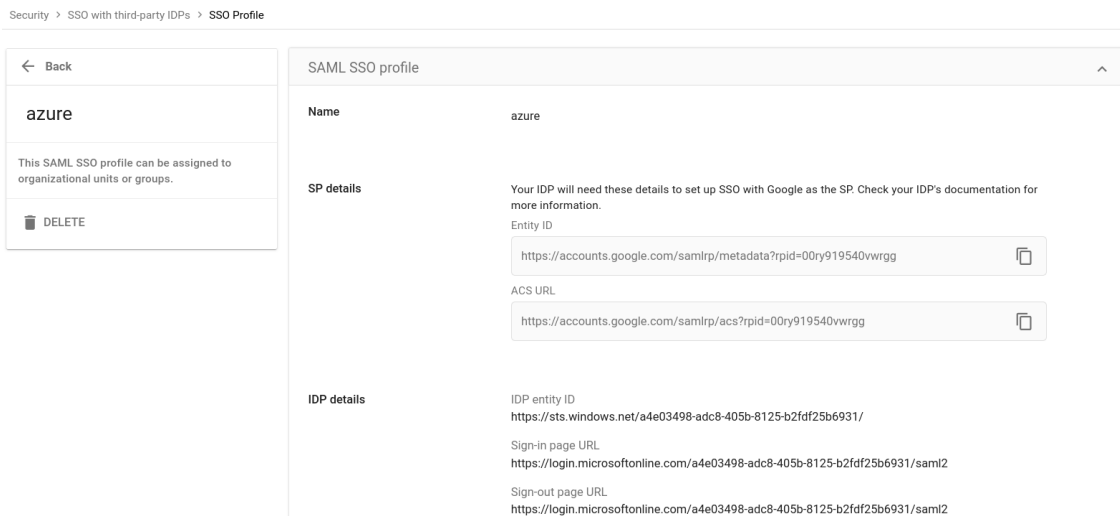
1. Google Chrome Enterprise or Education managed ChromeOS or Flex devices.
2. Netskope Cloud Security Platform tenant.
3. Azure AD tenant.
4. Google tenant [configured](#) for SSO with SAML to Azure AD.
  - a. In majority of deployments, Azure users will be auto provisioned to Google using [Google Cloud/G Suite Connector by Microsoft](#).
  - b. While strictly speaking users can authenticate separately to ChromeOS, Azure and/or Netskope, and Conditional Access via egress IP address would still work, this is an unlikely deployment scenario.
5. Netskope tenant configured for SSO with SAML to Azure AD.
6. ChromeOS devices configured to steer traffic to Netskope.
  - a. Netskope [Chrome Extension installed and configured](#) via Chrome Admin Policy.
  - b. OR Netskope explicit proxy settings [configured](#) via Chrome Admin Policy.

### Configuration

#### Google SSO with Azure

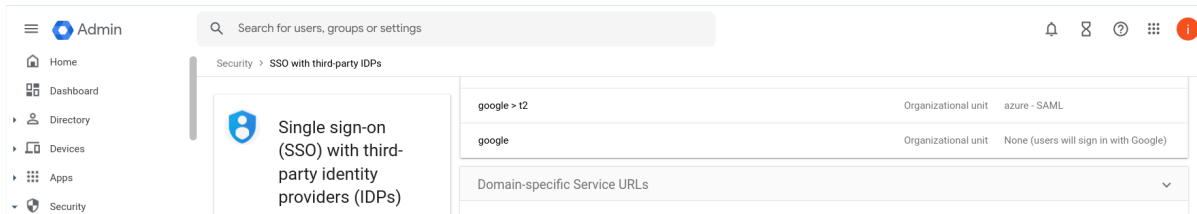
1. In Google Admin, [configure](#) Security-> Authentication -> SSO with Third Party IDP -> SSO Profile for the Azure tenant.

Security > SSO with third-party IDPs > SSO Profile

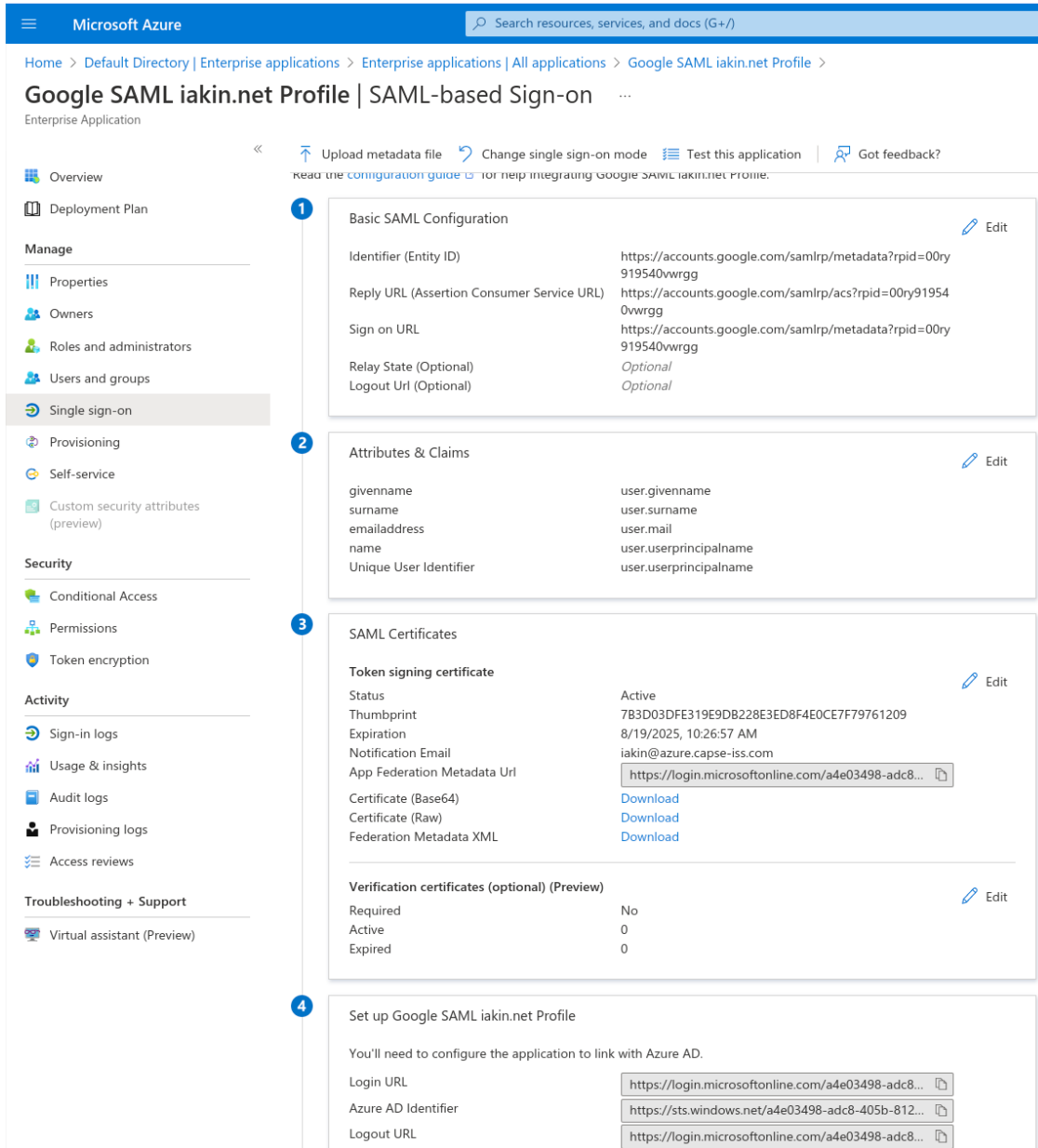


SAML SSO profile	
Name	azure
SP details	Your IDP will need these details to set up SSO with Google as the SP. Check your IDP's documentation for more information. Entity ID <input type="text" value="https://accounts.google.com/samlrp/metadata?rpId=00ry919540vrrgg"/> ACS URL <input type="text" value="https://accounts.google.com/samlrp/acs?rpId=00ry919540vrrgg"/>
IDP details	IDP entity ID <input data-bbox="797 1682 1146 1703" type="text" value="https://sts.windows.net/a4e03498-adc8-405b-8125-b2fdf25b6931/"/> Sign-in page URL <input data-bbox="797 1730 1230 1751" type="text" value="https://login.microsoftonline.com/a4e03498-adc8-405b-8125-b2fdf25b6931/saml2"/> Sign-out page URL <input data-bbox="797 1778 1230 1799" type="text" value="https://login.microsoftonline.com/a4e03498-adc8-405b-8125-b2fdf25b6931/saml2"/>

2. Make sure it is assigned to an organizational unit or group under Manage SSO profile assignments.



3. In [Azure](#), [configure](#) Enterprise Application with SAML SSO for the Google tenant.



4. For Azure users to be able to log in via SAML SSO from Chrome, be sure to assign these users and/or groups to the Enterprise Application.

Home > Default Directory | Enterprise applications > Enterprise applications | All applications > Google SAML iakin.net Profile

## Google SAML iakin.net Profile | Users and groups

Enterprise Application

Overview | Deployment Plan

**Manage**

- Properties
- Owners
- Roles and administrators
- Users and groups**
- Single sign-on
- Provisioning
- Self-service

[+ Add user/group](#) | [Edit](#) | [Remove](#) | [Update Credentials](#) | [Columns](#) | [Got feedback?](#)

**i** The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application register](#)

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type
<input type="checkbox"/> az1 iakin	User
<input type="checkbox"/> test1 iakin	User
<input type="checkbox"/> test2 iakin.net	User

5. Verify that a user can log in to a ChromeOS device via Azure SSO.

## Netskope SSO with Azure

1. In Netskope console, in Settings -> Security Cloud Platform > Forward Proxy -> SAML, create an account for Azure.

← Security Cloud Platform

- Users
- Groups
- Devices
- Enforcement
- SAML
- MDM Distribution
- REVERSE PROXY
- SAML
  - Office 365 Auth
  - ActiveSync
  - Auth Integration
- FORWARD PROXY
  - SAML**
  - Authentication
- ON PREMISES
  - On-Premises Infrastructure
  - CDPP for Appliance

Security Cloud Platform > Forward Proxy >

## SAML - Forward Proxy

Set up SAML Providers to be used to authenticate users when going through the Netskope Forward Proxy. Additionally, providers can be set up here to allow your IdP.

**Netskope SAML Config**

SAML Entity ID: <https://nsauth-partner-google.eu.goskope.com/UmEmvSeOkmO6B637FbNI>

SAML ACS URL: <https://nsauth-partner-google.eu.goskope.com/nsauth/saml2/http-post/UmEmvSeOkmO6B637FbNI/acs>

[DOWNLOAD SAML CERTIFICATE](#)

[NEW ACCOUNT](#)

NAME	IDP URL
Google SAML	<a href="https://accounts.google.com/o/saml2/idp?idpid=C03kw6ewz">https://accounts.google.com/o/saml2/idp?idpid=C03kw6ewz</a>
Google azure-cros.com	<a href="https://accounts.google.com/o/saml2/idp?idpid=C01shde4y">https://accounts.google.com/o/saml2/idp?idpid=C01shde4y</a>
G azure.capse-iss.com	<a href="https://accounts.google.com/o/saml2/idp?idpid=C01242o6m">https://accounts.google.com/o/saml2/idp?idpid=C01242o6m</a>
G iakin	<a href="https://accounts.google.com/o/saml2/idp?idpid=C03dbnmf3">https://accounts.google.com/o/saml2/idp?idpid=C03dbnmf3</a>
MS azure.capse-iss.com	<a href="https://login.microsoftonline.com/a4e03498-adc8-405b-8125-b2fdf25b6931/saml2">https://login.microsoftonline.com/a4e03498-adc8-405b-8125-b2fdf25b6931/saml2</a>



The screenshot shows the 'Authentication - Forward Proxy' configuration page in the Security Cloud Platform. The left sidebar contains a navigation menu with categories: 'NETSKOPE CLIENT' (Users, Groups, Devices, Enforcement, SAML, MDM Distribution) and 'REVERSE PROXY' (SAML, Office 365 Auth, ActiveSync, Auth Integration). Under 'FORWARD PROXY', 'SAML' is selected, and 'Authentication' is highlighted. The main content area has a breadcrumb 'Security Cloud Platform > Forward Proxy >' and a title 'Authentication - Forward Proxy'. Below the title is a descriptive text: 'Setup Authentication for Netskope for Web users to be redirected to the configured Identity Provider. This allows you to capture the identity of you are using IdP to provision the Netskope Client, authentication needs to be enabled.' The 'Authentication' section shows 'Authentication: Enabled' with a green dot and 'Type: SAML Authentication: MS azure.capse-iss.com'. An 'ENABLE AUTHENTICATION' button is present. The 'Bypass Settings' section includes a note: 'Administrators can use this section to identify domains and categories for which user authentication is not required.' Under 'DOMAIN BYPASS', it shows 'None Specified' and an 'EDIT' button.

The 'Enable Authentication' dialog box is shown with a close button (X) in the top right corner. It contains the following settings: 'Enabled' is checked with a blue toggle; 'SAML ACCOUNT' is set to 'MS azure.capse-iss.com' with a dropdown arrow and a 'CREATE NEW' button; 'AUTHENTICATION REFRESH INTERVAL' has an information icon and two input fields for 'Days' and 'Hours'; 'ENABLE COOKIE SURROGATE' is disabled with a grey toggle. At the bottom, there are 'CANCEL' and 'SAVE' buttons.

3. In [Azure](#), [configure](#) Netskope User Authentication Enterprise Application.



Home > Enterprise applications | All applications >

## Browse Azure AD Gallery

+ Create your own application | Got feedback?

The Azure AD App Gallery is a catalog of thousands of apps that allow users to connect more securely to their apps. Browse or create your own application. [Learn more](#)

Federated SSO Provisioning

Showing 4 of 4 results

**Netskope User Authentication**

Netskope

Home > Enterprise applications | All applications > Netskope User Authentication >

## Netskope User Authentication | SAML-based Sign-on

Enterprise Application

« [Upload metadata file](#) [Change single sign-on mode](#) [Test this application](#) | Got feedback?

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage**
- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on**
- Provisioning
- Self-service
- Custom security attributes

### Set up Single Sign-On with SAML

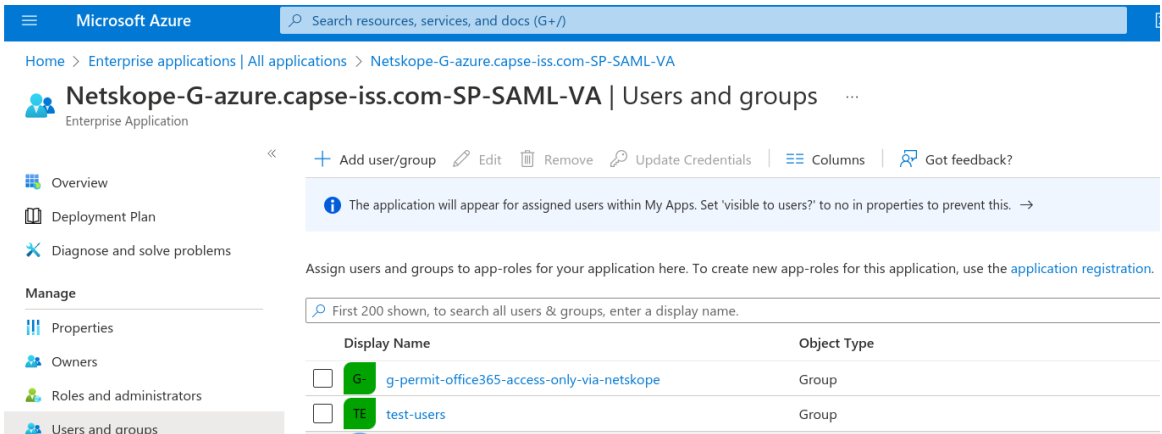
An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more](#).

Read the [configuration guide](#) for help integrating Netskope User Authentication.

**1** Basic SAML Configuration

Identifier (Entity ID)	https://nsauth-partner-google.eu.goskope.com/UmEmvSeOkmO6B637FbNI
Reply URL (Assertion Consumer Service URL)	https://nsauth-partner-google.eu.goskope.com/nsauth/saml2/http-post/UmEmvSeOkmO6B637FbNI/acs
Sign on URL	<i>Optional</i>
Relay State (Optional)	<i>Optional</i>
Logout Uri (Optional)	<i>Optional</i>

4. For Azure users to be able to log in via SAML SSO via Netskope, be sure to assign these users and/or groups to the Enterprise Application.



Microsoft Azure | Search resources, services, and docs (G+)

Home > Enterprise applications | All applications > Netskope-G-azure.capse-iss.com-SP-SAML-VA

**Netskope-G-azure.capse-iss.com-SP-SAML-VA** | Users and groups

Enterprise Application

Overview  
Deployment Plan  
Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups**

« + Add user/group | Edit | Remove | Update Credentials | Columns | Got feedback?

**i** The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registration](#).

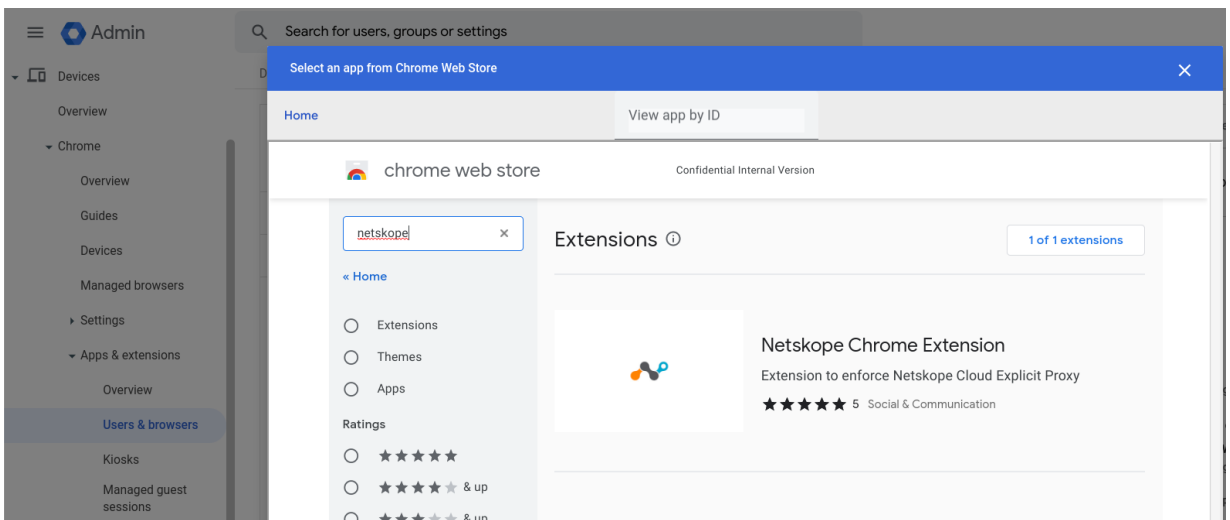
First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type
<input type="checkbox"/> <b>G-</b> g-permit-office365-access-only-via-netskope	Group
<input type="checkbox"/> <b>TE</b> test-users	Group

5. Verify that a user can log in to Netskope via Azure SSO.

## Configure Chrome traffic steering

1. In Google Admin -> Devices -> Chrome -> Apps & extensions -> Users & browsers add and [configure](#) Netskope Chrome Extension from the Chrome Web Store to be deployed to the appropriate organizational unit or group.



Admin | Search for users, groups or settings

Devices

- Overview
- Chrome
  - Overview
  - Guides
  - Devices
  - Managed browsers
  - Settings
  - Apps & extensions
  - Overview
  - Users & browsers**
  - Kiosks
  - Managed guest sessions

Select an app from Chrome Web Store

Home | View app by ID

chrome web store | Confidential Internal Version

Search: netskope

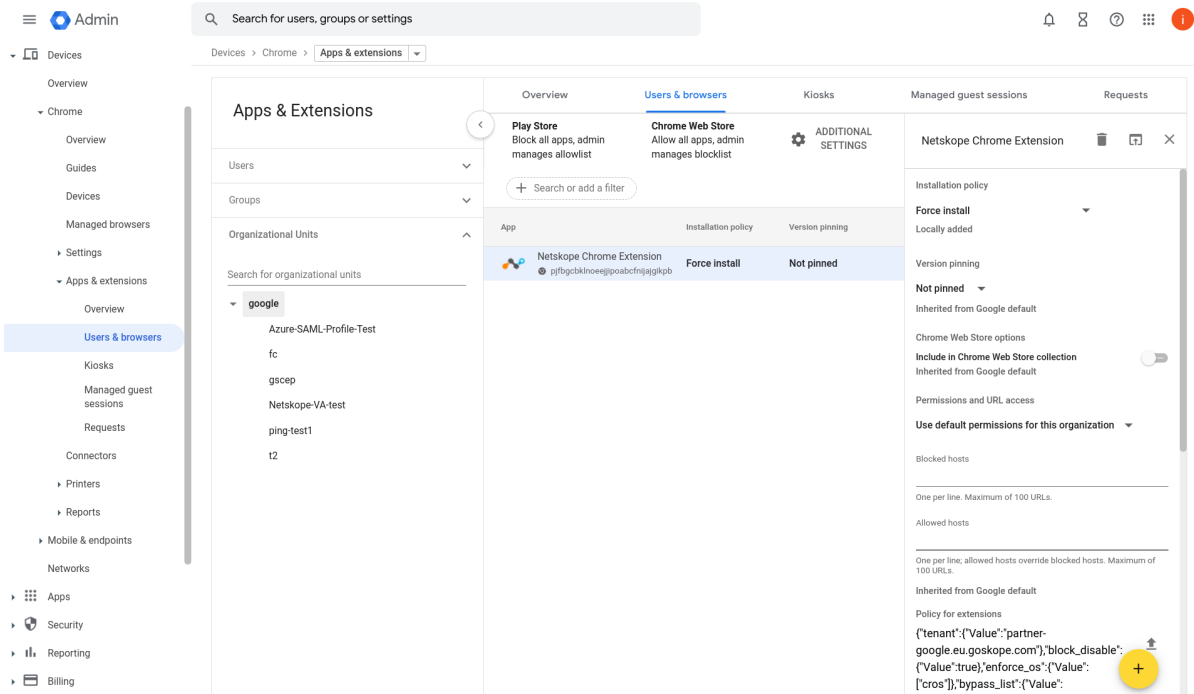
Extensions 0 | 1 of 1 extensions

- Extensions
- Themes
- Apps

Ratings

- ★★★★★
- ★★★★★ & up
- ★★★★★ & up

**Netskope Chrome Extension**  
Extension to enforce Netskope Cloud Explicit Proxy  
★★★★★ 5 Social & Communication



2. In Policy for Extension, specify the correct Netskope tenant, options and URLs to be bypassed from Netskope steering, (i.e. Google infrastructure URLs, IDP etc)

```

a. {"tenant":{"Value":"partner-google.eu.goskope.com"}, "block_disable":{"Value":true}, "enforce_os":{"Value":["cros"]}, "bypass_list":{"Value":["*.1e100.net", "accounts.google.com", "accounts.google.co.uk", "accounts.gstatic.com", "accounts.youtube.com", "alt*.gstatic.com", "chromeos-ca.gstatic.com", "chromeosquirkserver-pa.googleapis.com", "clients1.google.com", "clients2.google.com", "clients3.google.com", "clients4.google.com", "clients2.googleusercontent.com", "cloudsearch.googleapis.com", "commondatastorage.googleapis.com", "cros-omahaproxy.appspot.com", "dl.google.com", "dl-ssl.google.com", "firebaseuserertopics-pa.googleapis.com", "*.googleusercontent.com", "*.gvt1.com", "gweb-gettingstartedguide.appspot.com", "m.google.com", "omahaproxy.appspot.com", "pack.google.com", "policies.google.com", "printerconfigurations.googleusercontent.com", "safebrowsing-cache.google.com", "safebrowsing.google.com", "ssl.gstatic.com", "storage.googleapis.com", "tools.google.com", "www.googleapis.com", "www.gstatic.com"]}
  
```

3. Verify that a ChromeOS device in the appropriate organizational unit gets the extension and is steering traffic correctly.

## Conditional Access

1. Define Netskope IP Ranges as a Named location in Azure under Azure AD -> Security -> Conditional Access -> Named locations.

The screenshot shows the Microsoft Azure portal interface for configuring Conditional Access. The main view is 'Named locations' under 'Conditional Access'. It lists two named locations: 'DBHome' and 'Netskope IP Addresses', both with the location type 'IP ranges'. A right-hand pane titled 'Update location (IP ranges)' is open, showing a form to update the 'Netskope IP Addresses' location. The form includes a search field, a 'Mark as trusted location' checkbox, and a list of IP ranges with delete icons.

Name	Location type
DBHome	IP ranges
Netskope IP Addresses	IP ranges

Name *	Mark as trusted location
Netskope IP Addresses	<input type="checkbox"/>

IP Range	Delete
4.31.195.0/26	
8.36.116.0/24	
8.39.144.0/24	
31.186.239.0/24	
74.217.93.0/24	
103.219.79.0/24	
103.47.244.0/24	
163.116.128.0/17	

Netskope IP Ranges can be found in Netskope Settings ->Security Cloud Platform -> SAML Reverse Proxy -> Netskope Source IP.

The screenshot shows the Netskope Security Cloud Platform interface for SAML Reverse Proxy setup. The breadcrumb path is 'Security Cloud Platform > Reverse Proxy > SAML - Reverse Proxy'. The main heading is 'SAML - Reverse Proxy'. Below the heading, there is a flow diagram showing the setup process: 'Create new account' -> 'Provide Netskope SAML config to IdP and cloud app' -> 'Setup complete'. Below the flow diagram, there is a paragraph of text explaining the setup process and a link to the help documentation. At the bottom, there are two buttons: 'ADD ACCOUNT' and 'NETSKOPE SOURCE IP'.

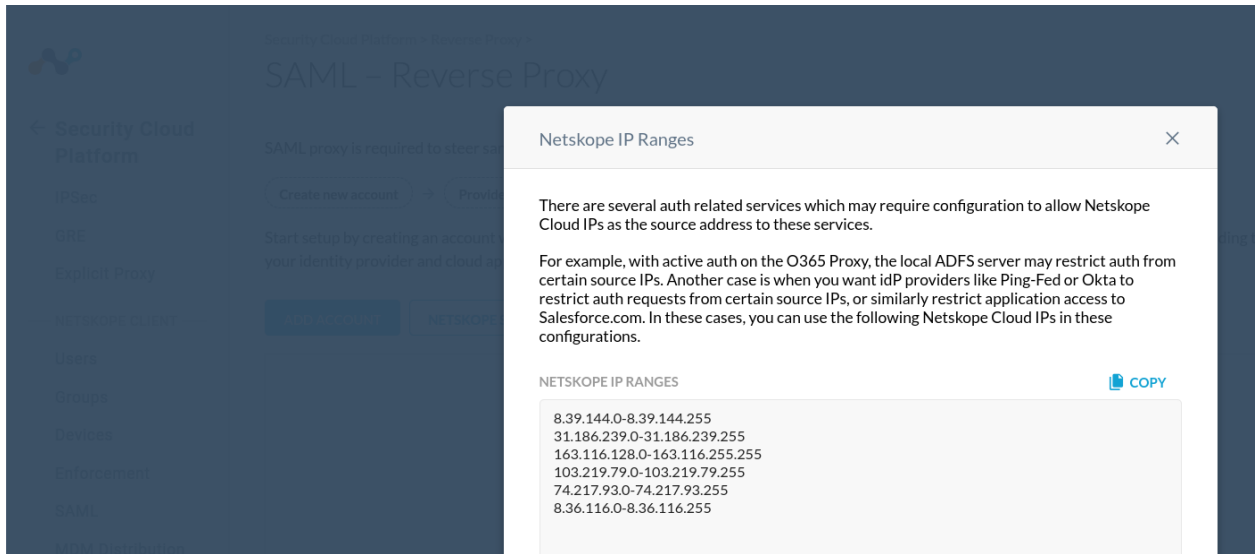
Security Cloud Platform > Reverse Proxy > SAML - Reverse Proxy

SAML proxy is required to steer sanctioned cloud app traffic to the reverse proxy running in your tenant in

Create new account → Provide Netskope SAML config to IdP and cloud app → Setup complete

Start setup by creating an account with information from your Identity Provider (IdP) and cloud application your identity provider and cloud application. Refer to the [Help](#) documentation for details.

ADD ACCOUNT    NETSKOPE SOURCE IP



2. In Azure create a Conditional Access policy.
  - a. Select users and groups.

# permit-office365-access-only-via-netskope (iakin) ...

Conditional Access policy

Delete

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

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. [Learn more](#)

Name \*  
permit-office365-access-only-via-netskope ...

What does this policy apply to?  
Users and groups

Assignments  
Users ⓘ  
Specific users included

Include Exclude  
 None  
 All users  
 Select users and groups  
 All guest and external users ⓘ  
 Directory roles ⓘ  
 Users and groups

Cloud apps or actions ⓘ  
1 app included

Select  
1 group  
G- g-permit-office365-access-on... \*\*\*

Conditions ⓘ  
1 condition selected

Access controls  
Grant ⓘ  
Block access

Session ⓘ


b. Select Cloud apps such as Office365.

Microsoft Azure

Home > Enterprise applications | Conditional Access > Conditional Access | Policies >

## permit-office365-access-only-via-netskope (iakin) ...

Conditional Access policy

 Delete

---

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

Name \*

Assignments

Users

Cloud apps or actions

Conditions

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

Select what this policy applies to

**Include**   Exclude

None

All cloud apps


Select apps

---

Select

[Office 365](#)

---


 Office 365

c. Exclude all platforms to make sure the policy does not apply to Intune-managed devices.

Home > Default Directory | Security > Security | Conditional Access > Conditional Access | Policies >

## permit-office365-access-only-via-netskope (iakin) ...

Conditional Access policy

 Delete

---

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

Name \*

Assignments

Users

Cloud apps or actions

Conditions

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

Device platforms

Locations

Client apps

Filter for devices

**Device platforms** ×

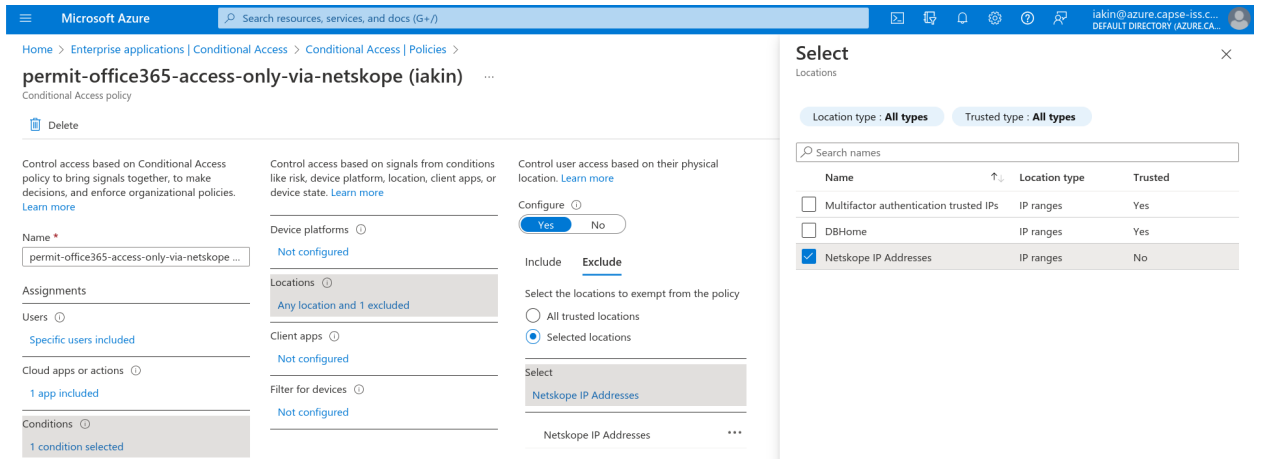
Apply policy to selected device platforms. [Learn more](#)

Configure

**Include**   **Exclude**

- Android
- iOS
- Windows Phone
- Windows
- macOS
- Linux

d. Set condition to exclude Netskope location created above.



Microsoft Azure | Search resources, services, and docs (G+)

Home > Enterprise applications | Conditional Access > Conditional Access | Policies >

### permit-office365-access-only-via-netskope (iakin)

Conditional Access policy

Delete

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

Name \*  
permit-office365-access-only-via-netskope ...

Assignments

Users   
Specific users included

Cloud apps or actions   
1 app included

Conditions   
1 condition 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

Netskope IP Addresses

Netskope IP Addresses

#### Select

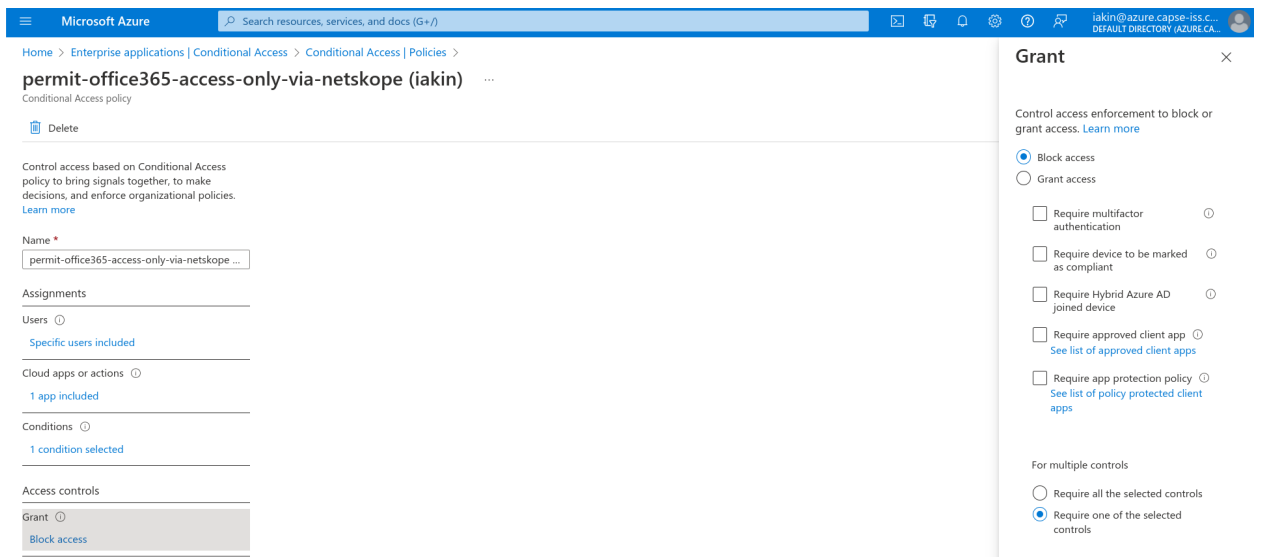
Locations

Location type: All types Trusted type: All types

Search names

Name	Location type	Trusted
<input type="checkbox"/> Multifactor authentication trusted IPs	IP ranges	Yes
<input type="checkbox"/> DBHome	IP ranges	Yes
<input checked="" type="checkbox"/> Netskope IP Addresses	IP ranges	No

## e. Set Access controls to Block.



Microsoft Azure | Search resources, services, and docs (G+)

Home > Enterprise applications | Conditional Access > Conditional Access | Policies >

### permit-office365-access-only-via-netskope (iakin)

Conditional Access policy

Delete

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

Name \*  
permit-office365-access-only-via-netskope ...

Assignments

Users   
Specific users included

Cloud apps or actions   
1 app included

Conditions   
1 condition selected

Access controls

Grant   
Block access

#### Grant

Control access enforcement to block or grant access. [Learn more](#)

Block access  
 Grant access

Require multifactor authentication

Require device to be marked as compliant

Require Hybrid Azure AD joined device

Require approved client app   
[See list of approved client apps](#)

Require app protection policy   
[See list of policy protected client apps](#)

For multiple controls

Require all the selected controls  
 Require one of the selected controls





## Verified Access for ChromeOS via SAML SSO - Netskope

How to use the [Netskope](#) Cloud Security Platform via SSO to restrict users from signing in on non-managed Chromebooks.

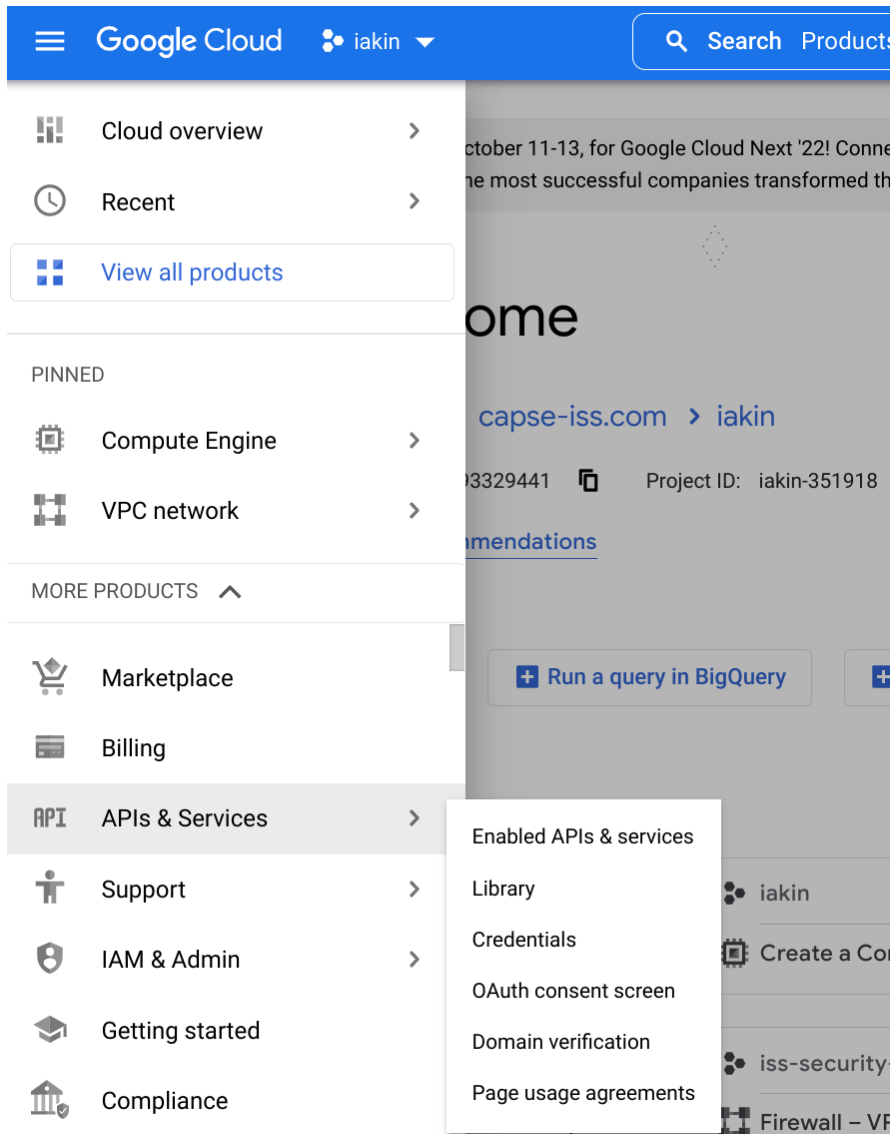
### Requirements

1. Google Chrome Enterprise or Education managed ChromeOS devices.
2. Netskope Cloud Security Platform tenant.
3. 3P SAML IdP (e.g. Azure AD).
4. Google Cloud Verified Access API enabled and [credentials created for Netskope](#).
5. Netskope SAML Reverse Proxy Account for Google tenant.
  - a. ACS URL = Google SAML ACS URL.
  - b. SSO IdP URL = 3P SSO URL.
  - c. Verified Access check with the Google tenant domain using API credentials.
6. 3P SAML IdP app / SP for Netskope tenant.
  - a. Entity ID = Google SAML Entity ID.
  - b. ACS / Reply URL = Netskope SAML Proxy ACS URL.
  - c. Sign on URL = Netskope SAML Proxy IdP URL.
7. Chrome device policy.
  - a. Allow Netskope API credentials access to device info via Verified Access.
  - b. Netskope SAML Reverse Proxy IdP URL allowlisted for sign-in.
8. Google SAML SSO / Profile for Netskope tenant.
  - a. SSO URL / Entity ID = Netskope SAML Proxy IdP URL.

## Configuration

### Google Cloud Verified Access API

1. Log in to Google Cloud console with an admin account and create a new cloud project.
2. Under APIs & Services -> Enabled APIs & services, enable Chrome Verified Access API.



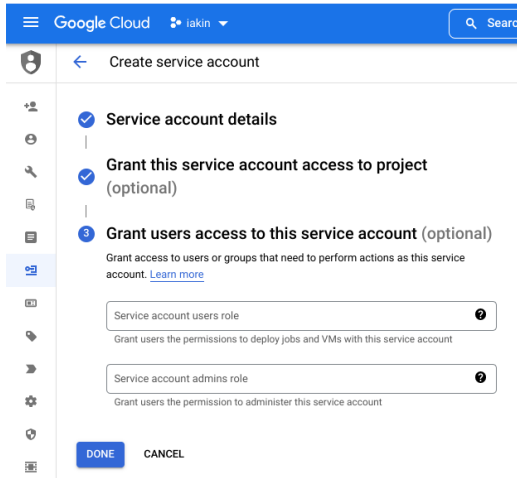
The screenshot shows the Google Cloud API Library interface. At the top, there's a search bar with 'verified' entered. Below the search bar, the results are filtered to show 2 results. The first result is 'Chrome Verified Access API' by Google, with a description: 'API for Verified Access chrome extension to provide credential verification for chrome devices connecting to an enterprise network'. The interface includes filters for Visibility (Public) and Category (Maps).

3. Under APIs & Services -> Credentials, create Service Account credentials for Netskope.

This screenshot shows the 'Credentials' page in Google Cloud. A dropdown menu is open, showing options: 'API key', 'OAuth client ID', 'Service account', and 'Help me choose'. The 'Service account' option is highlighted. Below the menu, there are sections for 'API Keys', 'OAuth 2.0 Client IDs', and 'Service Accounts'. The 'Service Accounts' section shows one existing account: '601693329441-compute@developer.gserviceaccount.com'.

This screenshot shows the first step of the 'Create service account' wizard. The 'Service account name' is 'netskope-va'. The 'Service account ID' is also 'netskope-va'. The 'Email address' is 'netskope-va@iakin-351918.iam.gserviceaccount.com'. There is a 'CREATE AND CONTINUE' button at the bottom.

This screenshot shows the second step of the 'Create service account' wizard, 'Grant this service account access to project (optional)'. It prompts the user to 'Grant this service account access to iakin so that it has permission to complete specific actions on the resources in your project'. There is a 'Select a role' dropdown and an 'IAM condition (optional)' section. A 'CONTINUE' button is visible.



Google Cloud raikin Search

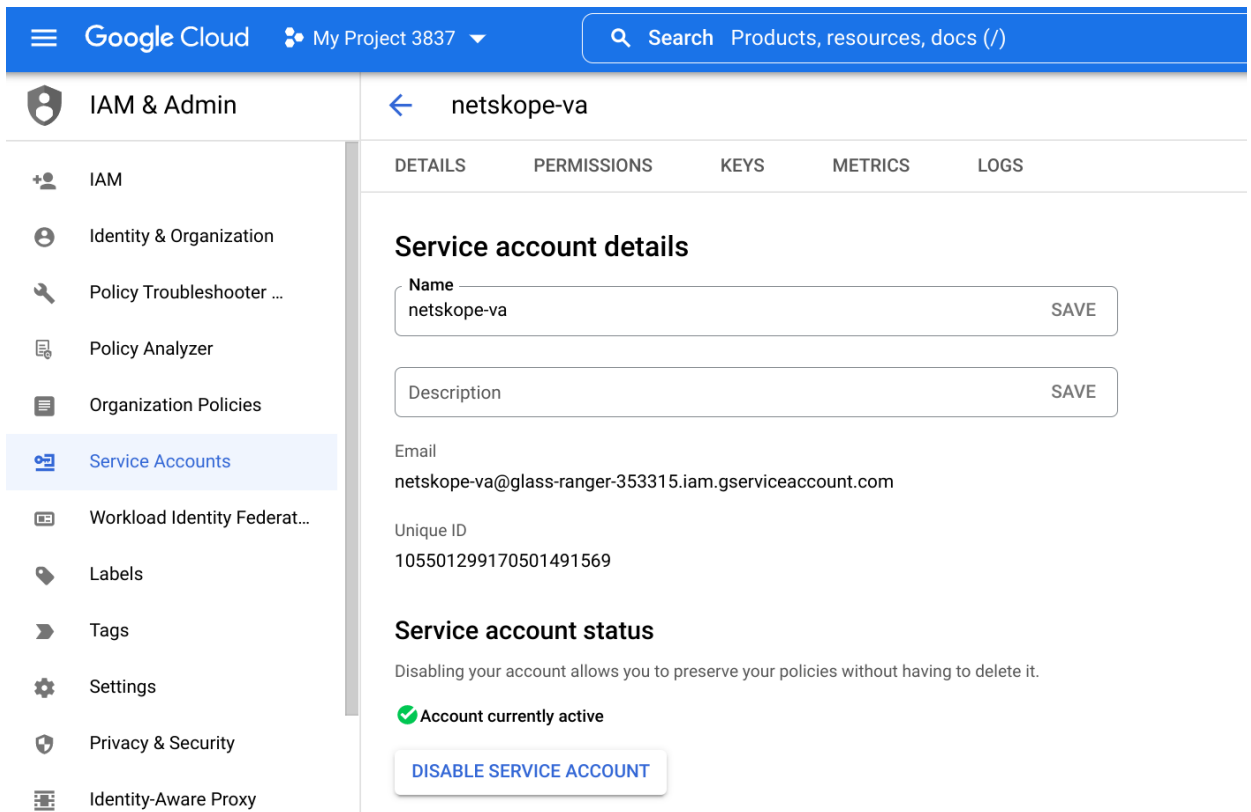
← Create service account

- ✓ Service account details
- ✓ Grant this service account access to project (optional)
- 3 Grant users access to this service account (optional)  
Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role   
Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role   
Grant users the permission to administer this service account

**DONE** CANCEL



Google Cloud My Project 3837 Search Products, resources, docs (/)

IAM & Admin ← netskope-va

DETAILS PERMISSIONS KEYS METRICS LOGS

### Service account details

Name  **SAVE**

Description  **SAVE**

Email  
netskope-va@glass-ranger-353315.iam.gserviceaccount.com

Unique ID  
105501299170501491569

### Service account status

Disabling your account allows you to preserve your policies without having to delete it.

✔ Account currently active

**DISABLE SERVICE ACCOUNT**

4. Under Keys, create a new JSON Key.

Google Cloud My Project 3837 Search Products, resources, docs (/)

IAM & Admin netskope-va

DETAILS PERMISSIONS KEYS METRICS LOGS

**Keys**

Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use a public key certificate. You can learn more about the best way to authenticate service accounts on Google Cloud [here](#).

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using [organization policies](#).  
[Learn more about setting organization policies for service accounts](#)

ADD KEY ▾

- Create new key
- Upload existing key

Key	Key creation date	Key expiration date	
adc0ddb26ddeb334259bf8655f3d877edc0664	Aug 18, 2022	Dec 31, 9999	🗑️

5. Download the key for use later in the guide.

Google Cloud My Project 3837 Search Products, resources, docs (/)

IAM & Admin netskope-va

DETAILS PERMISSIONS KEYS METRICS LOGS

**Keys**

Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use a public key certificate. You can learn more about the best way to authenticate service accounts on Google Cloud [here](#).

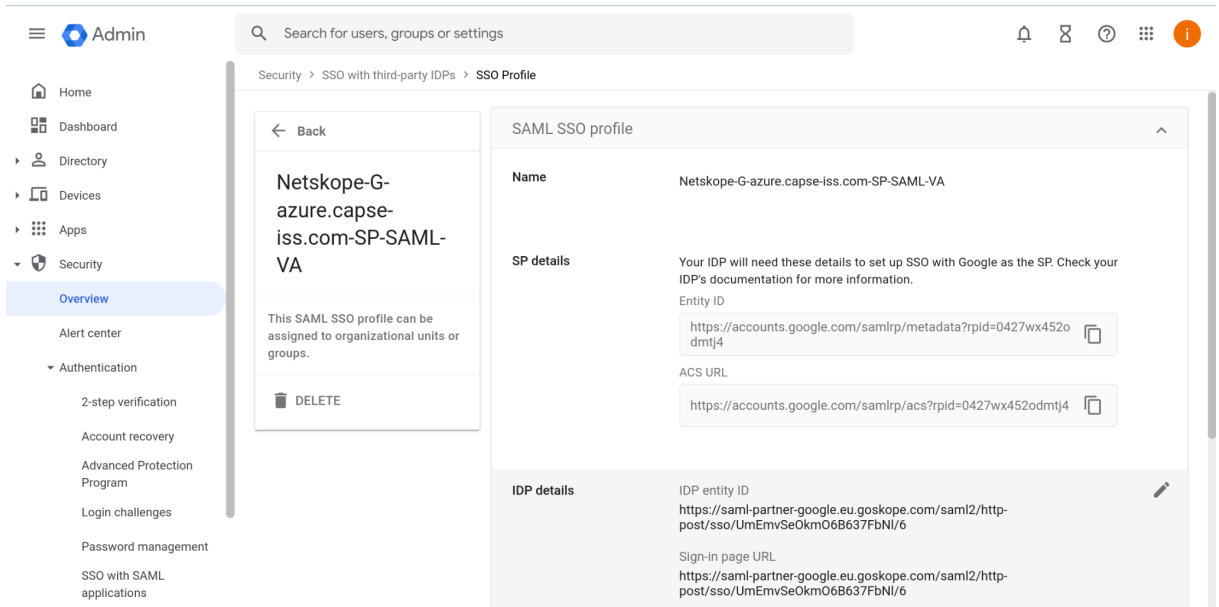
Add a new key pair or upload a public key certificate from an existing key pair.

**Private key saved to your computer**

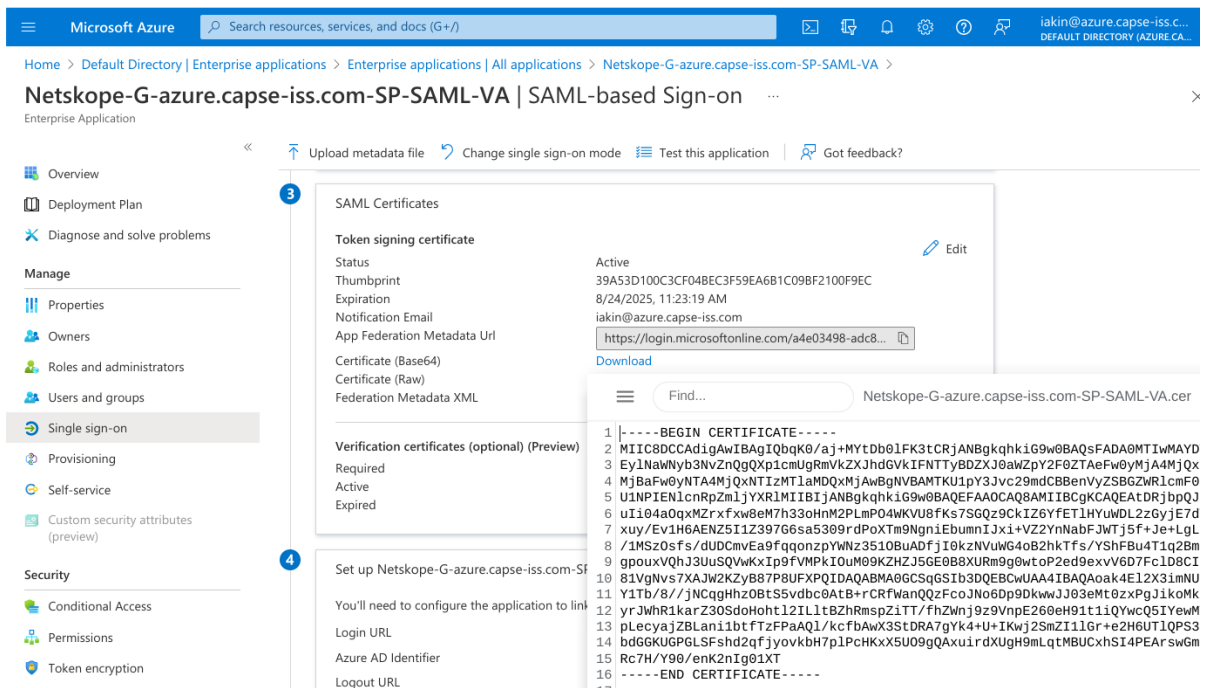
glass-ranger-353315-88d79681f519.json allows access to your cloud resources, so store it securely. [Learn more best practices](#)

CLOSE





3. Copy IdP SSO URL from 3P SAML app for Netskope SP Login URL.



4. Copy IdP Certificate from 3P IdP, for example Certificate (Base64).

5. In the Account -> Options tab.

- a. Enable Google Chromebook Verified Access.
- b. Specify domain name of Google tenant.
- c. Upload the GCP service account key that we downloaded previously.

### Edit Account ✕

SETUP **OPTIONS**

**EMERGENCY BYPASS**

Disabled

The following settings are only applicable when emergency bypass is disabled.

- Bypass Auth checks for Mobile ⓘ
- Enable SAML assertion key-value pairs matching ⓘ
- Enable IP address based access ⓘ
- Enable client certificate check requirement ⓘ
- Enable Google Chromebook Verified Access ⓘ

**Action**

if success

if failure

**Domain Name**

**Service Account Credentials**

Uploaded by iakin@google.com on Thu Sep 29 2022 12:02:05 GMT-4

[REPLACE FILE](#)



## 3P SAML IdP for Netskope (Azure AD in this example)

1. Create a new Azure Enterprise Application **Azure AD SAML Toolkit**.

The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar with the text 'Search resources, services, and docs (G+)'. Below the search bar, the breadcrumb navigation reads 'Home > Default Directory | Enterprise applications > Enterprise applications | All applications >'. The main heading is 'Browse Azure AD Gallery'. There are two links: '+ Create your own application' and 'Got feedback?'. A paragraph describes the Azure AD App Gallery as a catalog of thousands of apps for SSO and authentication. Below this is a search input field containing 'azure ad saml toolkit'. Filter buttons for 'Single Sign-on : All', 'User Account Management : All', and 'Categories' are visible. There are also icons for 'Federated SSO' and 'Provisioning'. The results section shows 'Showing 1 of 1 results' with a card for 'Azure AD SAML Toolkit' by Microsoft Corporation.

The screenshot shows the configuration page for the application 'letskope-G-azure.capse-iss.com-SP-SAML-VA'. The breadcrumb navigation is 'Home > Default Directory | Enterprise applications > Enterprise applications | All applications > Netskope-G-azure.capse-iss.com-SP-SAML-VA >'. The main heading is 'letskope-G-azure.capse-iss.com-SP-SAML-VA | SAML-based Sign-on'. The left sidebar contains navigation options: Overview, Deployment Plan, Diagnose and solve problems, Manage, Properties, Owners, Roles and administrators, Users and groups, Single sign-on (selected), Provisioning, Self-service, and Custom security attributes (preview). The main content area is titled 'Set up Single Sign-On with SAML' and includes a description of SSO implementation based on federation protocols. A 'Basic SAML Configuration' table is shown with the following data:

Property	Value
Identifier (Entity ID)	https://accounts.google.com/samlrp/metadata?rpId=0427wx452odmtj4
Reply URL (Assertion Consumer Service URL)	https://saml-partner-google.eu.goskope.com/saml2/http-post/acs/UmEmvSeOkmO6B637FbNI/6
Sign on URL	https://saml-partner-google.eu.goskope.com/saml2/http-post/sso/UmEmvSeOkmO6B637FbNI/6
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

Identifier / Entity ID is the Google SAML SP Entity ID from the Netskope SAML Profile.

Security > SSO with third-party IDPs > SSO Profile

**Netskope-G-azure.capse-iss.com-SP-SAML-VA**

This SAML SSO profile can be assigned to organizational units or groups.

DELETE

**SAML SSO profile**

**Name** Netskope-G-azure.capse-iss.com-SP-SAML-VA

**SP details** Your IDP will need these details to set up SSO with Google as the SP. Check your IDP's documentation for more information.

**Entity ID** `https://accounts.google.com/samlrp/metadata?rpId=0427wx452odmtj4`

**ACS URL** `https://accounts.google.com/samlrp/acs?rpId=0427wx452odmtj4`

**IDP details**

**IDP entity ID** `https://saml-partner-google.eu.goskope.com/saml2/http-post/sso/UmEmvSe0km06B637FbNI/6`

**Sign-in page URL** `https://saml-partner-google.eu.goskope.com/saml2/http-post/sso/UmEmvSe0km06B637FbNI/6`

Reply URL and Sign on URL are Netskope SAML ACS URL and Proxy IDP URL from Netskope Settings of the SAML Reverse Proxy.

Security Cloud Platform > Reverse Proxy > SAML - Reverse Proxy

SAML proxy is required to steer sanctioned cloud app traffic to the reverse proxy running in your tenant instance.

Create new account → Provide Netskope SAML config to IdP and cloud app → Setup complete

Start setup by creating an account with information from your Identity Provider (IdP) and cloud application. Then complete the setup by providing the Netskope settings to your identity provider and cloud application. Refer to the [Help](#) documentation for details.

ADD ACCOUNT NETSKOPE SOURCE IP SETTINGS

NAME	APPLICATION	ACS URL	BYPASS
Google-azure.capse-i...	Netskope Settings  Google Accounts	https://accounts.google.com/samlrp/acs?rpId=...	No

Netskope Settings ✕

The following are the Netskope Settings for the SAML account **Google-azure.capse-iss.com-SAML-VA**. Use this information to complete setup with your identity provider and cloud application.

ORGANIZATION ID

UmEmvSeOkmO6B637FbNI

SAML PROXY IDP URL

<https://saml-partner-google.eu.goskope.com/saml2/http-post/sso/UmEmvSeOkmO6B637FbNI/6>

SAML PROXY ACS URL

<https://saml-partner-google.eu.goskope.com/saml2/http-post/acs/UmEmvSeOkmO6B637FbNI/6>

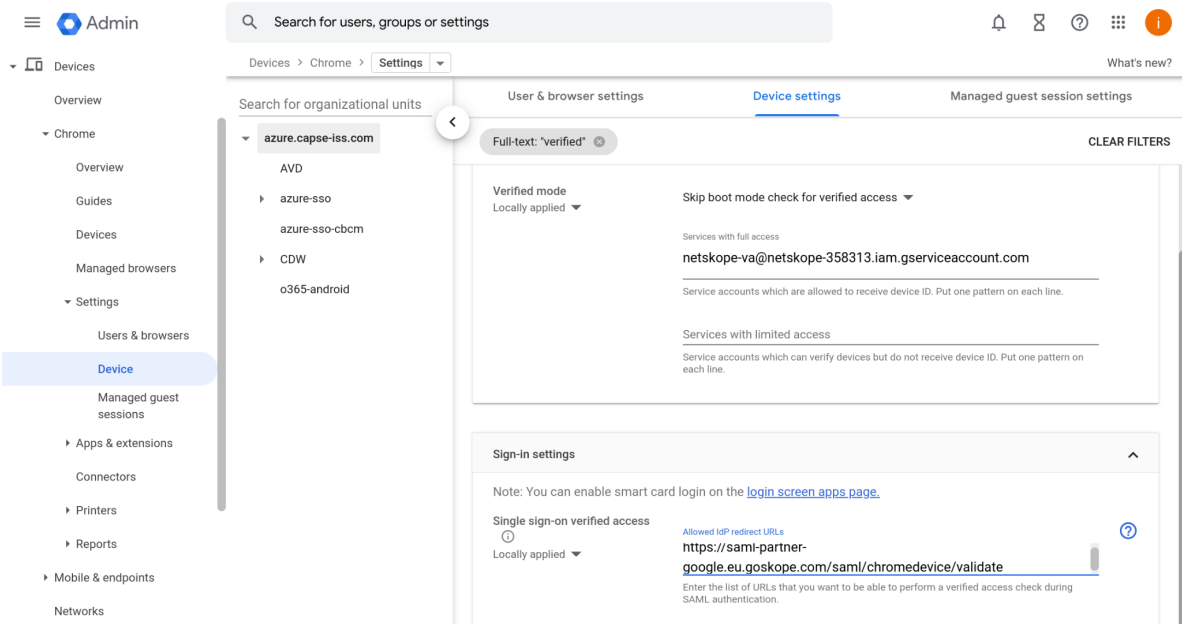
SAML PROXY ISSUER CERTIFICATE

```
-----BEGIN CERTIFICATE-----
MIIEdTCCA12gAwIBAgIEALDZ6TANBgkqhkiG9w0BAQsFADCB1zELMAkGA1UEBhMC
VVMx CzAJBgNVBAGTAkNBMRyWwFAYDVQQHEw1Nb3VudGFpbmIBWV3MSYwJAYDVQQK
Ex1Hb29nbGUgQ2hyb21lIFBhcnRuZXIgcWVudDEpMCcGA1UECzMgODRmZWZm
MTQ1N2Q3ZDZjNmNmODQ3NTIhM2ZiMTk5M2MxKTAnBgNVBAMTIGNhLnBhcnRuZXIt
Z29vZ2xllmV1Lmdvc2tvcGUuY29tMSUwIiwYJKoZIhvcNAQkBFhZjZXJ0YWRtaW5A
bmV0c2tvcGUuY29tMB4XDTEwMDMwMTIzMDAxNFoXDTEwMDMwMTIzMDAxNFowdWw
CzAJBgNVBAYTAiVtMQswCQYDVQQIEw1Jb29tZS11b3RmY29vZ2xllmV1Lmdvc2tvcGUuY29t
dzEmMCQGA1UEChM5Z29vZ2xllmV1Lmdvc2tvcGUuY29tZS11b3RmY29vZ2xllmV1Lmdvc2tvcGUuY29t
-----END CERTIFICATE-----
```

CLOSE

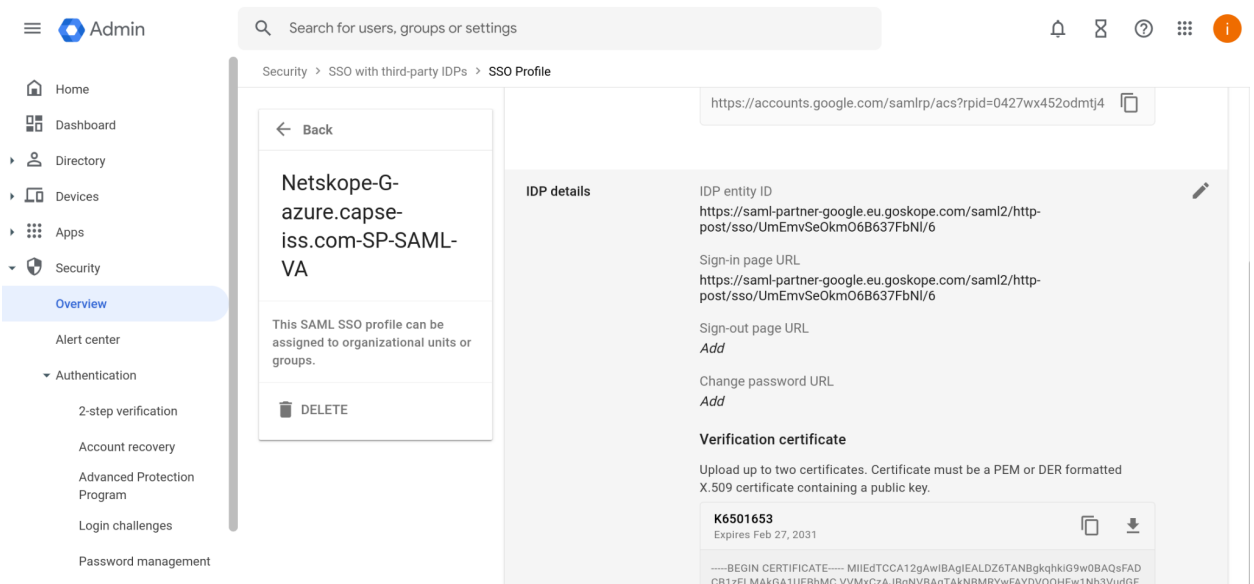
### Chrome Device policy

1. In Google Admin -> Devices -> Chrome -> Settings -> Device for the appropriate organizational unit, search for “Verified”.
2. Under Verified mode -> Services with full access, enter the Netskope API Service account name.
3. In Single sign-on verified access -> Allowed IdP redirect URLs, enter **[https://saml-\*<netskope tenant id>.goskope.com/saml/chromedevic/validate\*](https://saml-<i><netskope tenant id>.goskope.com/saml/chromedevic/validate)**



## Google SAML SSO with Netskope

1. In the Google Admin console, [configure](#) Security-> Authentication -> SSO with Third Party IDP -> SSO Profile for Netskope.

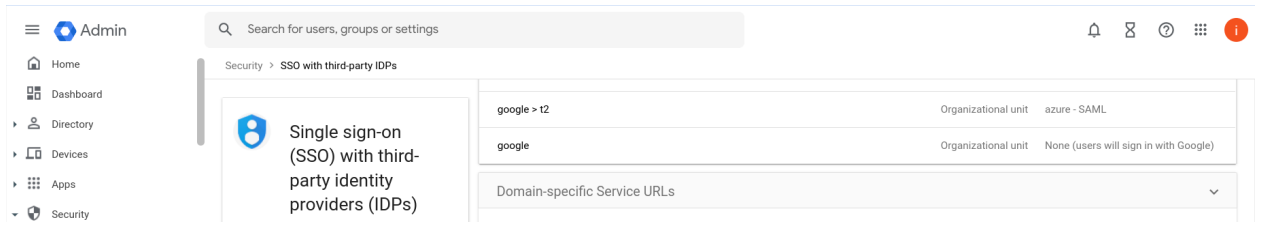


IdP entity ID and Sign-in page URL are SAML Proxy IDP URL from Netskope Settings of the SAML Reverse Proxy.

2. Copy the “Verification Certificate” from SAML Proxy Issuer Certificate.



## Under Manage SSO profile assignments.



The screenshot shows the Google Admin console interface for managing SSO profile assignments. The breadcrumb path is "Security > SSO with third-party IDPs". A search bar is located at the top. The main content area features a card for "Single sign-on (SSO) with third-party identity providers (IDPs)" and a table of assignments.

IDP Name	Organizational unit	Configuration
google > t2	azure - SAML	
google	None (users will sign in with Google)	

Below the table is a section for "Domain-specific Service URLs" with a dropdown arrow.