chrome enterprise

Deliver Conditional Access for ChromeOS in Microsoft Entra ID Guide

June 2024

chrome enterprise

Contents

Introduction

As a Microsoft Entra ID customer, you probably use Conditional Access. By following this guide, you can learn how to deliver Conditional Access for ChromeOS in Microsoft Entra ID environments using various integrations[1].

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

---

[1] While ChromeOS is not a directly Microsoft-supported device platform for Microsoft Entra ID Conditional Access, this guide shows how you can still implement this functionality in your environment.

chrome enterprise

Microsoft Entra ID Conditional Access for ChromeOS - Microsoft Defender for Cloud Apps

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

Requirements

1. Managed ChromeOS devices
2. ChromeOS device certificates deployed via SCEP
3. Microsoft Entra ID 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 Entra ID applications, such as Office365.
2. Prevent enterprise users from logging in to unmanaged ChromeOS devices.

This solution utilized Microsoft Entra ID [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 Microsoft Entra ID using one or more factors.

Microsoft Entra ID 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 Microsoft Entra ID 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.
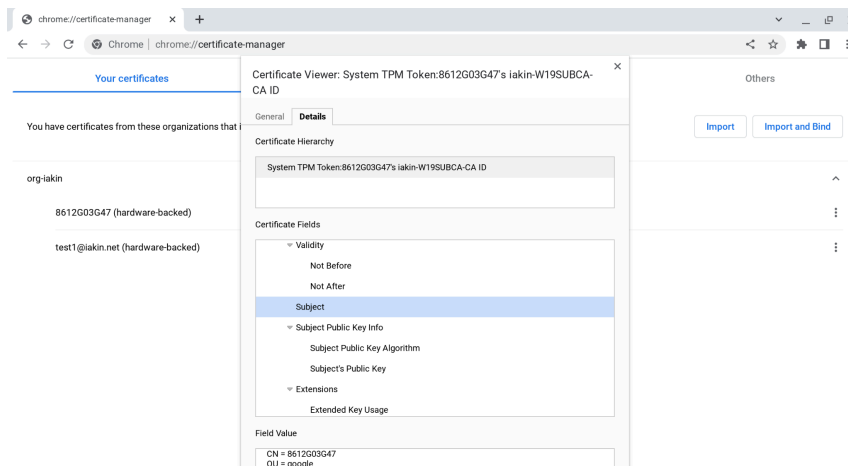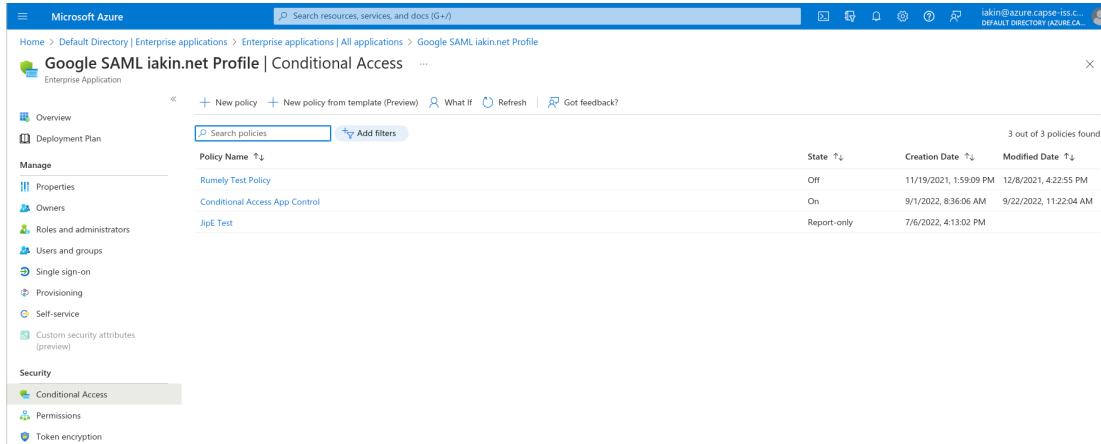

SSO

1. Configure SSO and user provisioning between Microsoft Entra ID and the Google tenant per documentation.
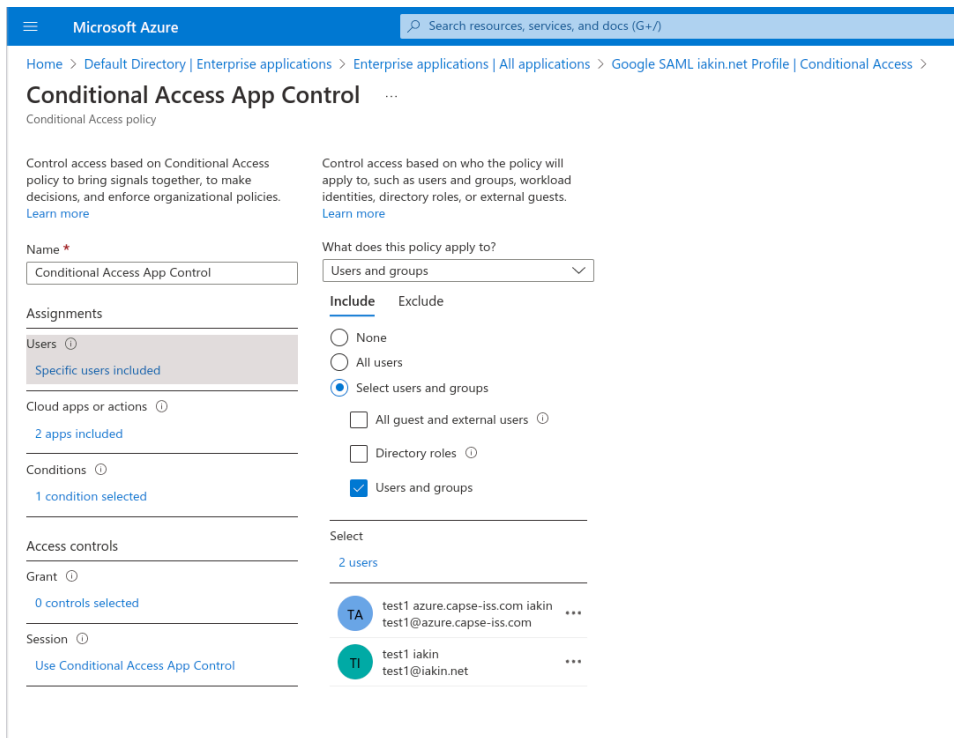2. Verify that a user can log in to a ChromeOS device with Microsoft Entra ID credentials.

Conditional Access

1. In Microsoft Entra ID Enterprise Application with SAML SSO for the Google tenant, click on Conditional Access.
   a. Create a new policy.

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

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 Microsoft Entra ID SSO.
   ii. To implement app control in session, select the relevant apps such as Office365.

chrome enterprise

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](#).

chrome enterprise

Defender for Cloud Apps

1. In the Microsoft Entra ID Conditional Access policy Session screen, click on Configure custom policy. This opens [Defender for Cloud Apps](#).
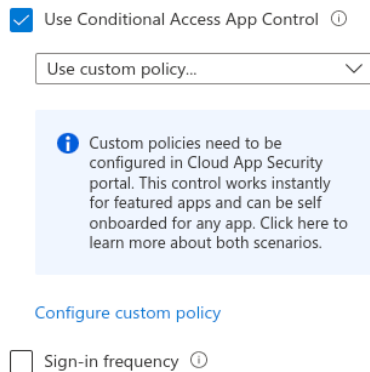
2. Import issuing CA certificate chain
    a. Open the Settings menu via the gear icon, then choose Settings under System.

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

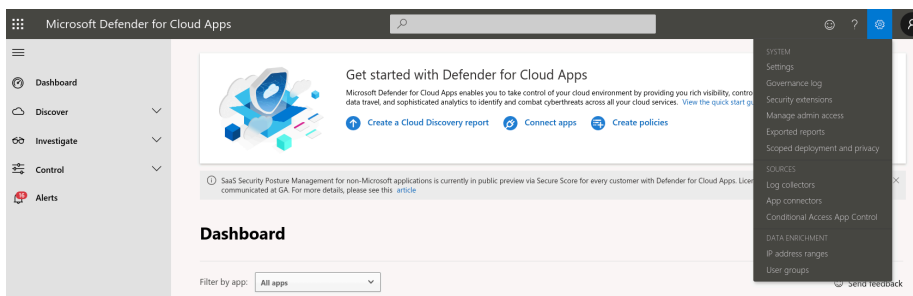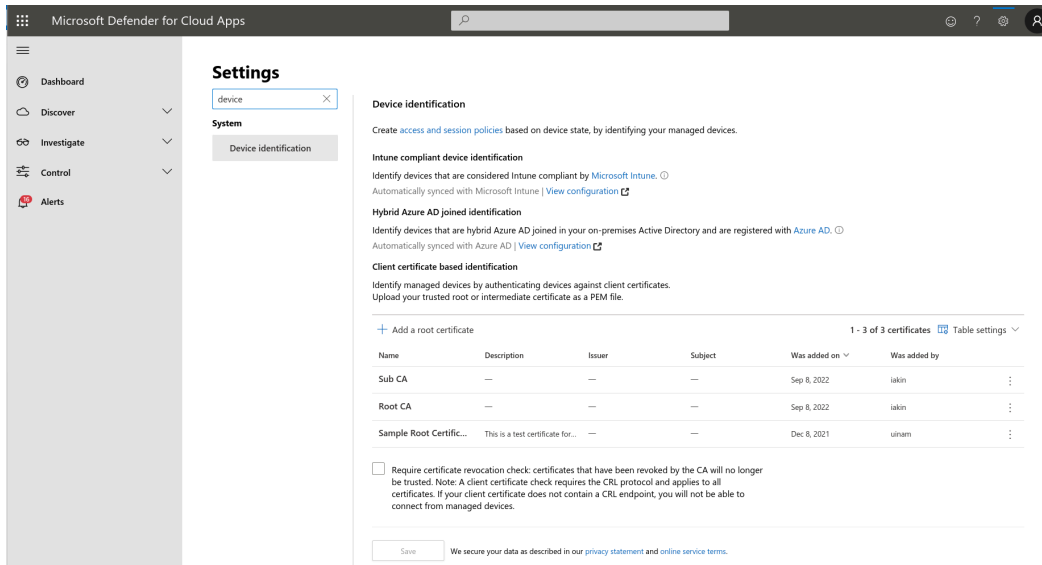a. In this screen, import the certificate chain for the CA issuing the ChromeOS device certificates. This is the same certificate chain imported into Google Admin console during SCEP configuration.

4. Configure Connected Apps

   a. Under the Settings gear menu, select Conditional Access App Control.

b. Follow Microsoft Guidance from the above linked document:
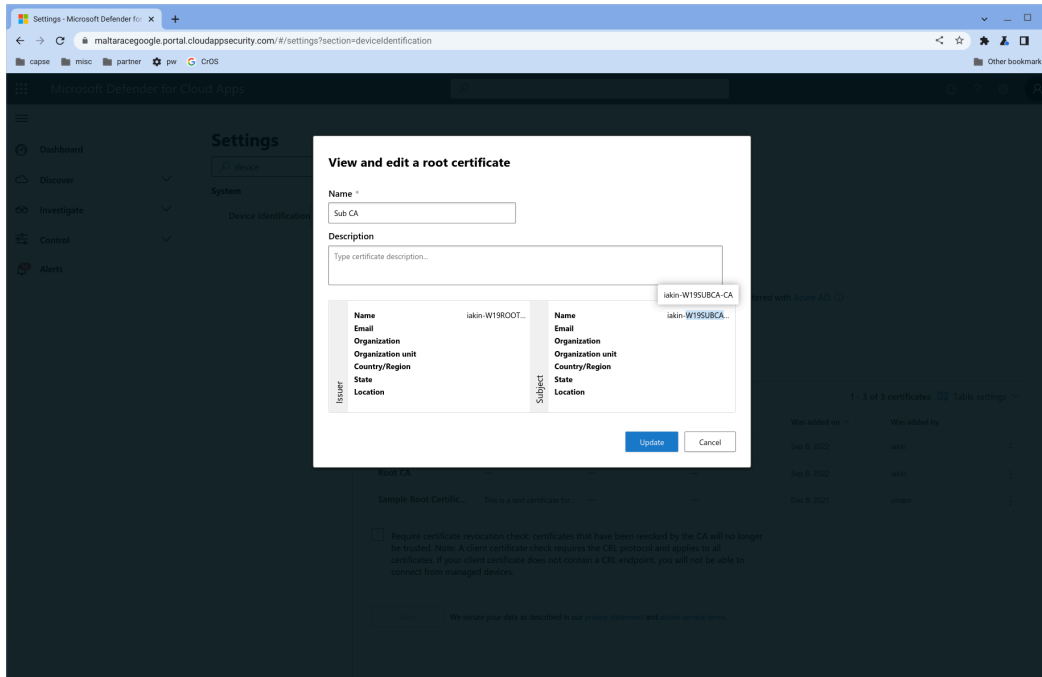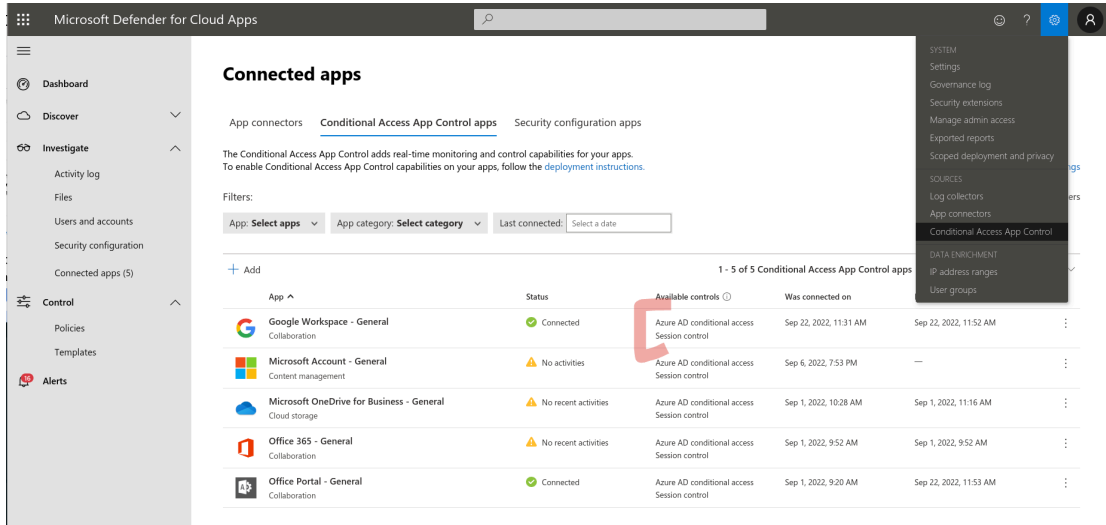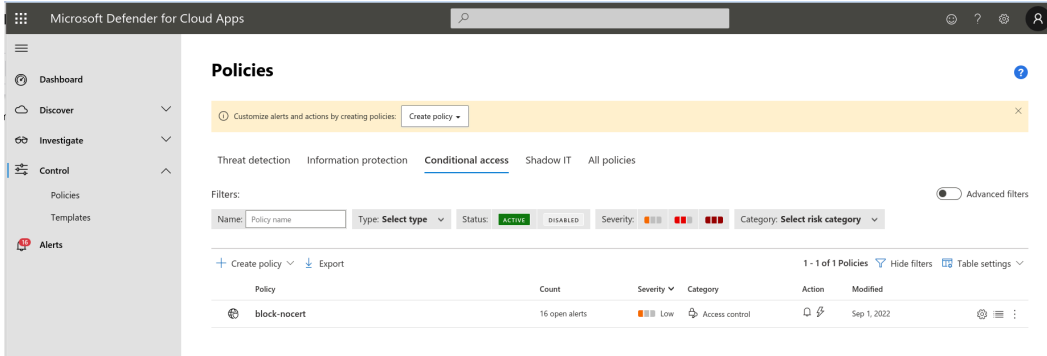   i. *"After you've created the policy, sign in to each app configured in that policy. Make sure you sign in using a user configured in the policy.*
      Defender for Cloud Apps will sync your policy details to its servers for each new app you sign in to. This may take up to one minute.
      The preceding instructions helped you create a built-in Defender for Cloud Apps policy for catalog apps directly in Microsoft Entra ID. In this step, verify that the access and session controls are configured for these apps."

c. Ensure that all required apps have Microsoft Entra ID 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.
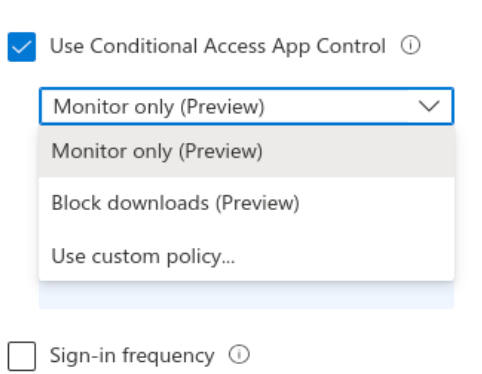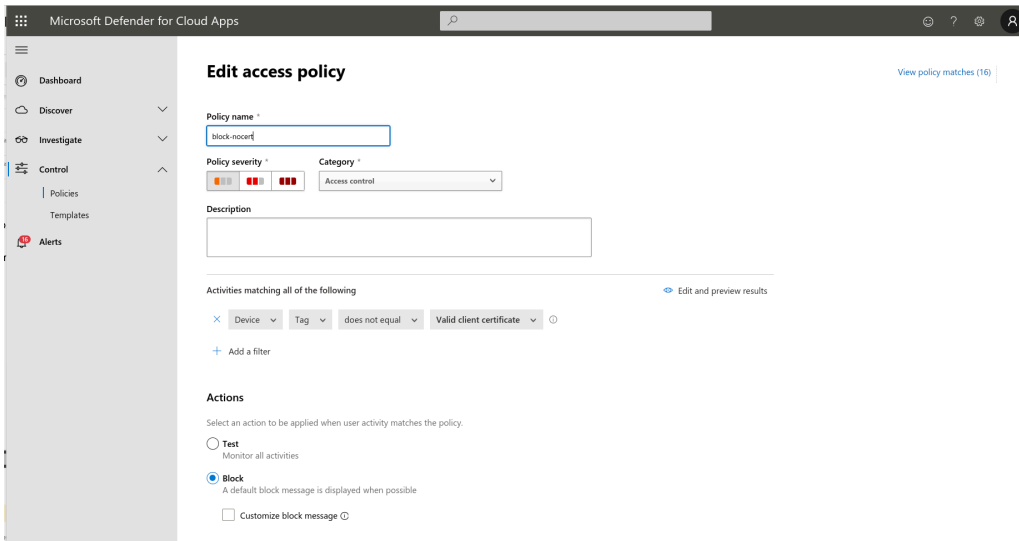

5. In Defender, navigate to [Control->Policies->Conditional Access](#).

chrome enterprise

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

Microsoft Entra ID Conditional Access for ChromeOS - Netskope

Provide Microsoft Entra ID 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. Microsoft Entra ID tenant.
4. Google tenant [configured](#) for SSO with SAML to Microsoft Entra ID.
   a. In majority of deployments, Microsoft Entra ID 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, Microsoft Entra ID 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 Microsoft Entra ID.
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 Microsoft Entra ID

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

Security > SSO with third-party IDPs > SSO Profile

| ← Back | SAML SSO profile | ⌃ |

azure

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

🗑 DELETE

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

https://accounts.google.com/samlrp/metadata?rpid=00ry919540vwrgg   📋

ACS URL

https://accounts.google.com/samlrp/acs?rpid=00ry919540vwrgg   📋

IDP details   IDP entity ID
https://sts.windows.net/a4e03498-adc8-405b-8125-b2fdf25b6931/

Sign-in page URL
https://login.microsoftonline.com/a4e03498-adc8-405b-8125-b2fdf25b6931/saml2

Sign-out page URL
https://login.microsoftonline.com/a4e03498-adc8-405b-8125-b2fdf25b6931/saml2
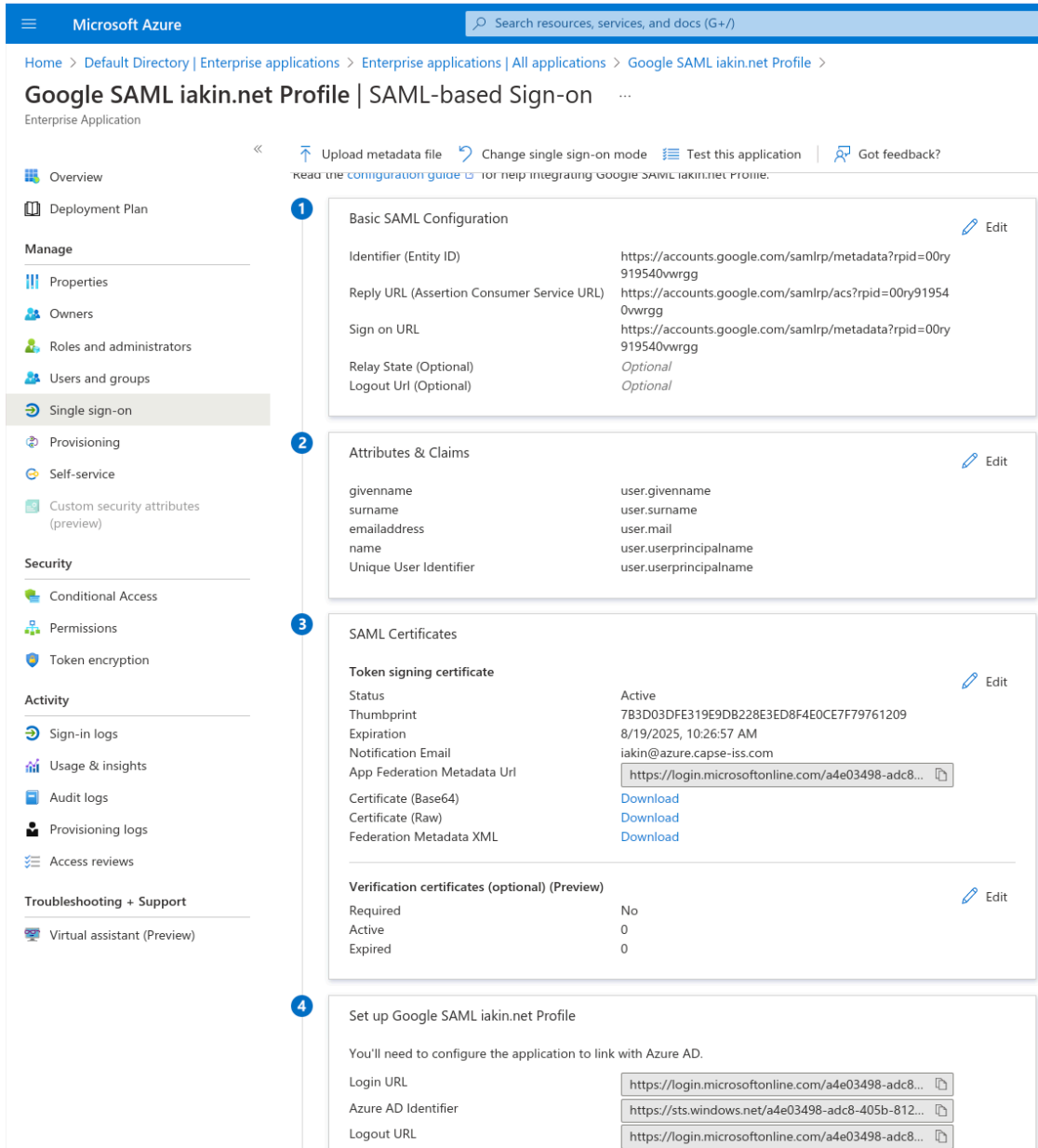
2. Make sure it is assigned to an organizational unit or group under Manage SSO profile assignments.

3. In Azure, configure Enterprise Application with SAML SSO for the Google tenant.

4. For Microsoft Entra ID 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.

chrome enterprise

5. Verify that a user can log in to a ChromeOS device via Microsoft Entra ID SSO.

Netskope SSO with Microsoft Entra ID

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

2. In Settings -> Security Cloud Platform > Forward Proxy -> Authentication select the Microsoft Entra ID SAML account.

chrome enterprise

Authentication - Forward Proxy

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.

Security Cloud Platform

NETSKOPE CLIENT
- Users
- Groups
- Devices
- Enforcement
- SAML
- MDM Distribution

REVERSE PROXY
- SAML
- Office 365 Auth
- ActiveSync
- Auth Integration

FORWARD PROXY
- SAML
- **Authentication**

Authentication

Authentication: ● Enabled
Type: SAML Authentication: MS azure.capse-iss.com

[ENABLE AUTHENTICATION]

Bypass Settings

Administrators can use this section to identify domains and categories for which user authentication is not required.

DOMAIN BYPASS
None Specified

[EDIT]

Enable Authentication   ✕

◉ Enabled

SAML ACCOUNT *

[MS azure.capse-iss.com ▾]   [CREATE NEW]

AUTHENTICATION REFRESH INTERVAL ⓘ

[Days]   [Hours]

ENABLE COOKIE SURROGATE

◯✕ Disabled

[CANCEL]   [SAVE]

3. In Azure, configure Netskope User Authentication Enterprise Application.

4. For Microsoft Entra ID 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.

chrome enterprise

5. Verify that a user can log in to Netskope via Microsoft Entra ID 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.
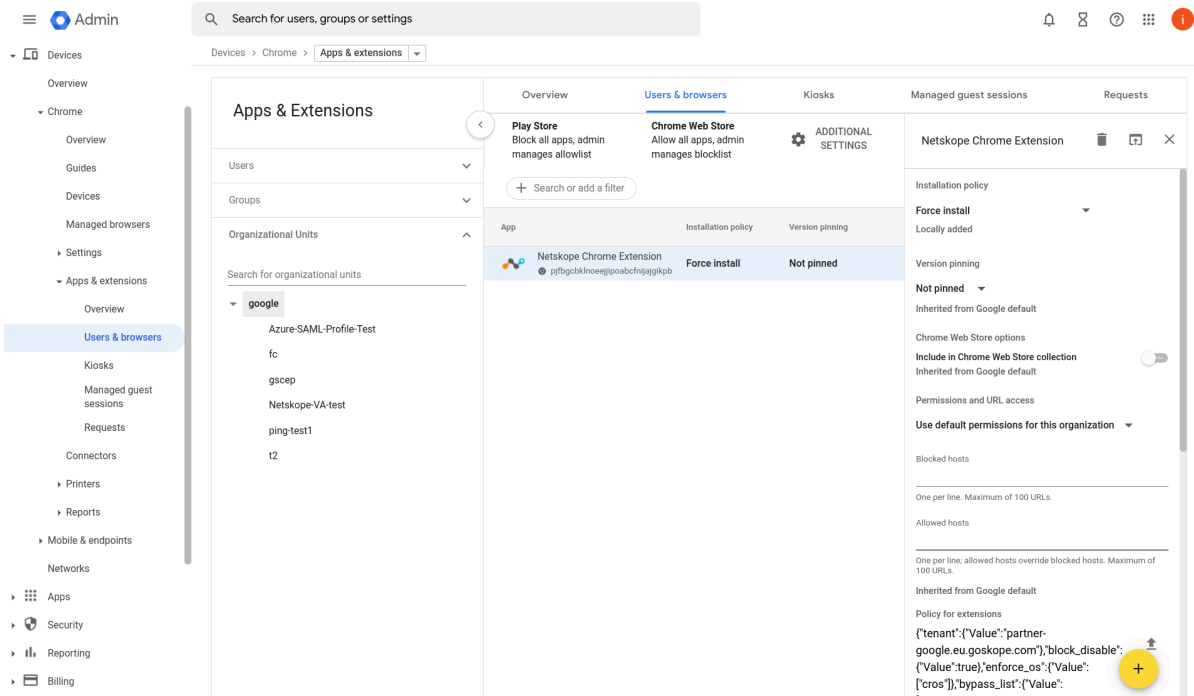
2. In Policy for Extension, specify the correct Netksope tenant, options and URLs to be bypassed from Netskope steering, (i.e. Google infrastructure URLs, IDP etc)

    a. `{"tenant":{"Value":"`**`partner-google.eu.goskope.com`**`"},"block_`
       `disable":{"Value":true},"enforce_os":{"Value":["cros"]},"b`
       `ypass_list":{"Value":["*.1e100.net","accounts.google.com",`
       `"accounts.google.co.uk","accounts.gstatic.com","accounts.y`
       `outube.com","alt*.gstatic.com","chromeos-ca.gstatic.com","`
       `chromeosquirksserver-pa.googleapis.com","clients1.google.c`
       `om","clients2.google.com","clients3.google.com","clients4.`
       `google.com","clients2.googleusercontent.com","cloudsearch.`
       `googleapis.com","commondatastorage.googleapis.com","cros-o`
       `mahaproxy.appspot.com","dl.google.com","dl-ssl.google.com"`
       `,"firebaseperusertopics-pa.googleapis.com","*.googleuserco`
       `ntent.com","*.gvt1.com","gweb-gettingstartedguide.appspot.`
       `com","m.google.com","omahaproxy.appspot.com","pack.google.`
       `com","policies.google.com","printerconfigurations.googleus`
       `ercontent.com","safebrowsing-cache.google.com","safebrowsi`
       `ng.google.com","ssl.gstatic.com","storage.googleapis.com",`
       `"tools.google.com","`[`www.googleapis.com`](www.googleapis.com)`","`[`www.gstatic.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 Microsoft Entra ID -> -> Manage -> Security -> Microsoft Entra Conditional Access -> Named locations.

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

2. In Microsoft Entra ID create a Conditional Access policy. For details see, <u>What is Conditional Access?</u>
    a. Select users and groups.

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

Session ⓘ

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

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

Select

1 group

[G-] g-permit-office365-access-on... •••

b. Select Cloud apps such as Office365.

chrome enterprise

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

d. Set condition to exclude Netskope location created above.

e. Set Access controls to Block.

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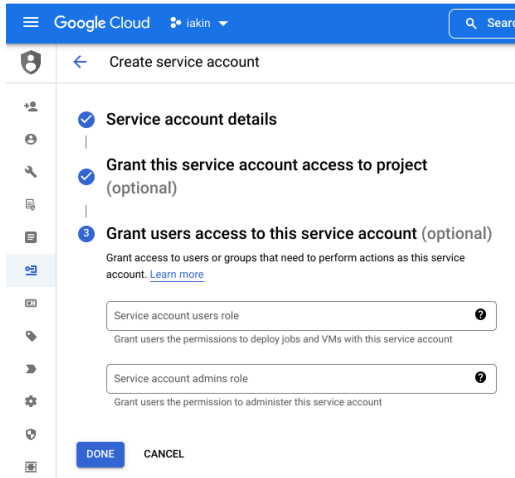
1. Log in to Google Cloud console with an admin account and create a new cloud project.
2. Under APIs & Services -> Enabled APIs & services, enable Chrome Verified Access API.

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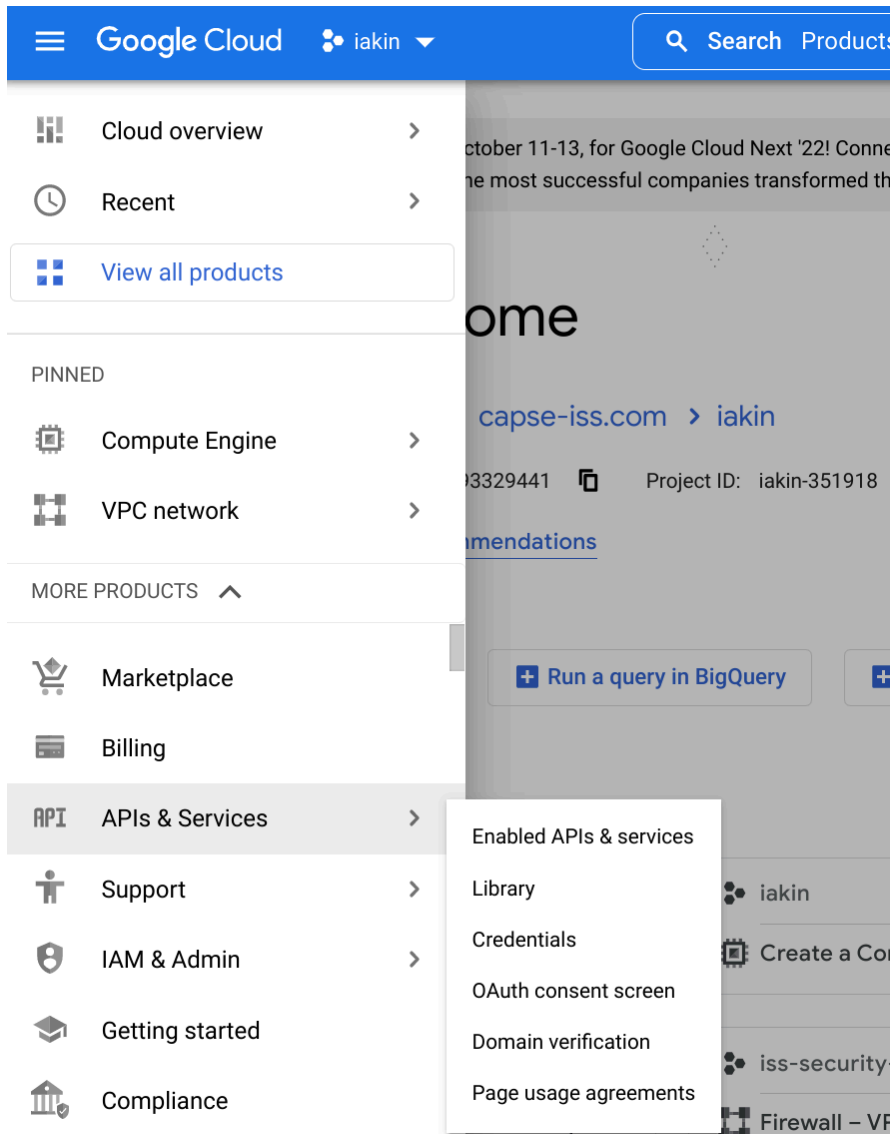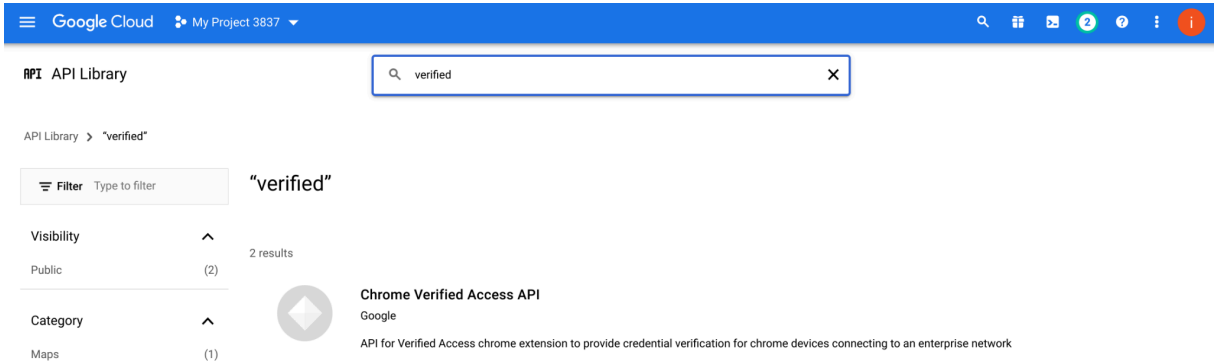
3. Under APIs & Services -> Credentials, create Service Account credentials for Netskope.

chrome enterprise

Google Cloud ·: iakin ▾   🔍 Search
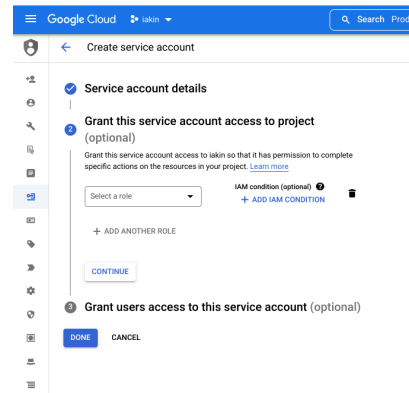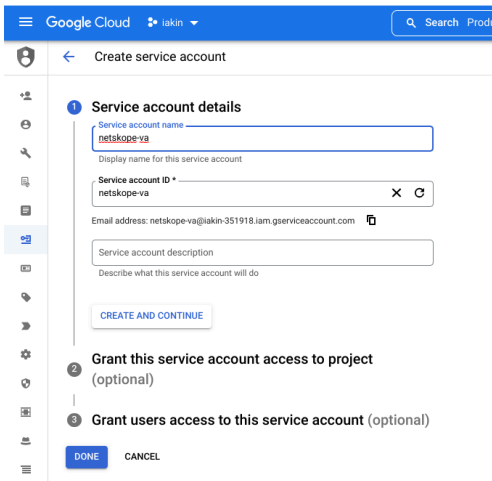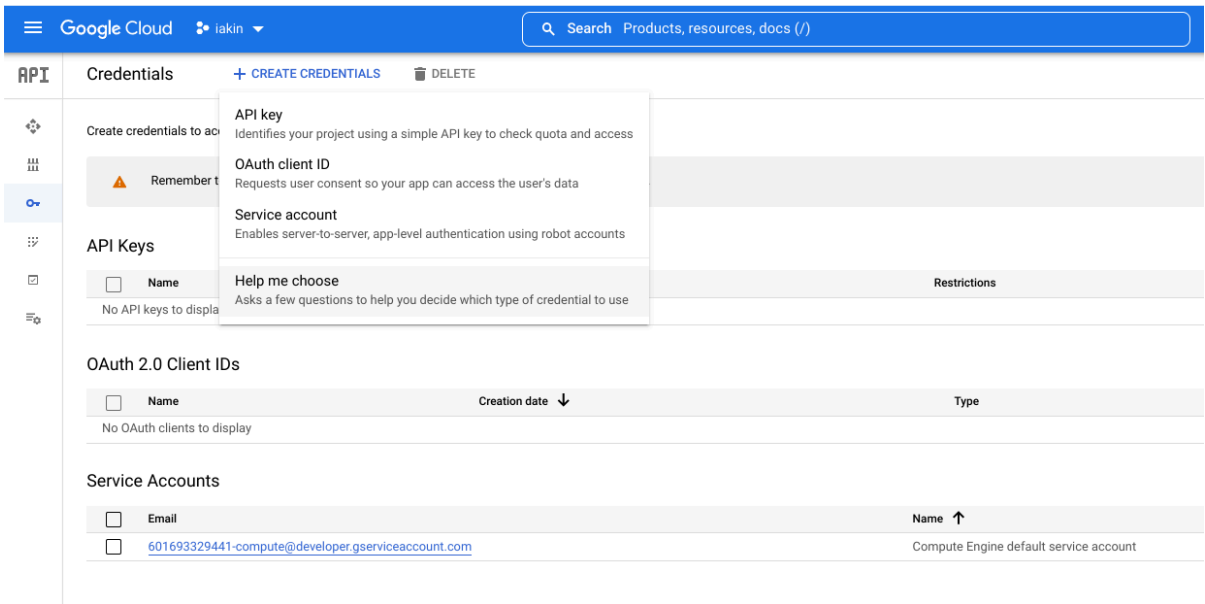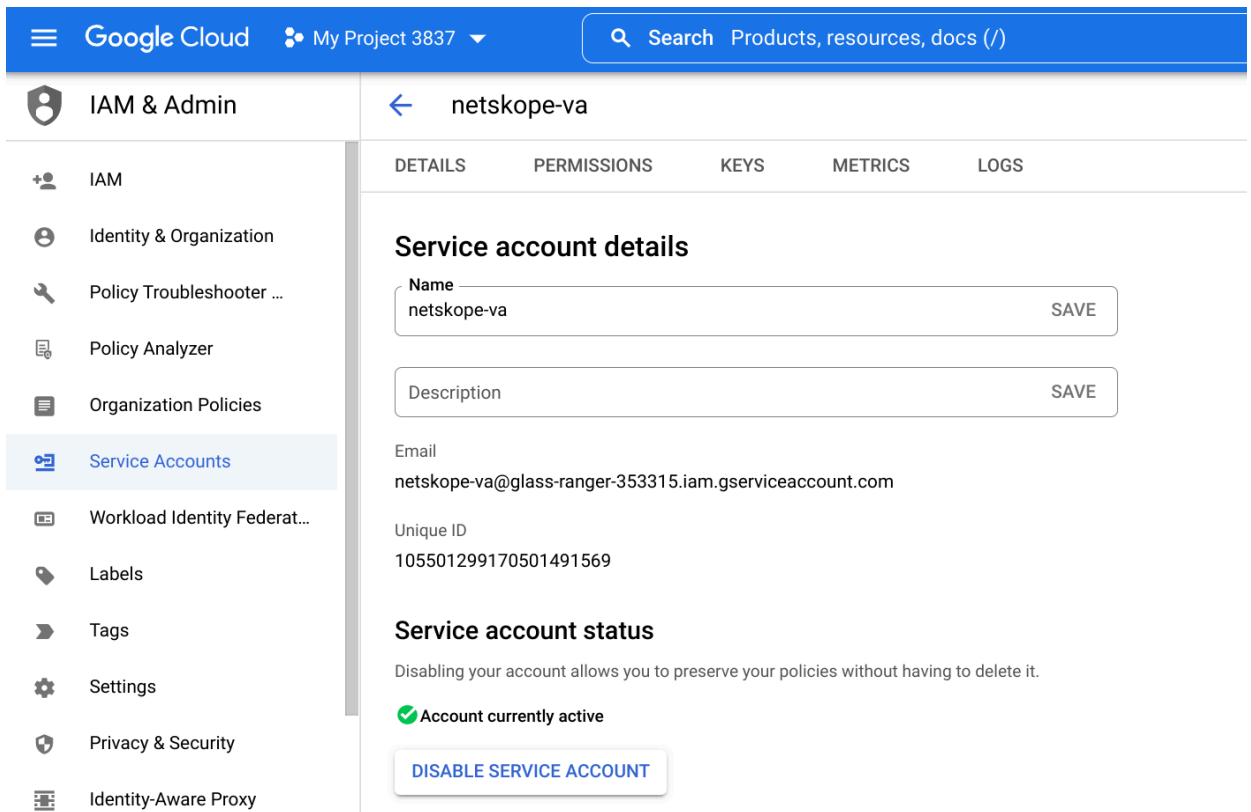
← Create service account

✓ 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

➕ IAM	**Service account details**
👤 Identity & Organization	Name
🔧 Policy Troubleshooter …	netskope-va SAVE
📄 Policy Analyzer	
📋 Organization Policies	Description SAVE
🔲 Service Accounts	Email
📰 Workload Identity Federat…	netskope-va@glass-ranger-353315.iam.gserviceaccount.com
🏷 Labels	Unique ID
➤ Tags	105501299170501491569
⚙ Settings	**Service account status**
🛡 Privacy & Security	Disabling your account allows you to preserve your policies without having to delete it.
🖹 Identity-Aware Proxy	✅ Account currently active
	DISABLE SERVICE ACCOUNT

4. Under Keys, create a new JSON Key.

chrome enterprise

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

Netskope SAML Reverse Proxy

1. In the Netskope console, in Settings -> Security Cloud Platform -> Reverse Proxy -> SAML, Add Account for Google tenant with Application Google Accounts.

2. Copy ACS URL from Google SAML Profile for Netskope SP Details -> Entity ID.

chrome enterprise

≡ ◉ Admin   🔍 Search for users, groups or settings

Security > SSO with third-party IDPs > SSO Profile

← Back

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/UmEmvSeOkmO6B637FbNl/6

Sign-in page URL
https://saml-partner-google.eu.goskope.com/saml2/http-post/sso/UmEmvSeOkmO6B637FbNl/6

Home
Dashboard
▸ Directory
▸ Devices
▸ Apps
▾ Security
  Overview
  Alert center
  ▾ Authentication
    2-step verification
    Account recovery
    Advanced Protection Program
    Login challenges
    Password management
    SSO with SAML applications

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

Microsoft Azure   🔍 Search resources, services, and docs (G+/)   iakin@azure.capse-iss.c... DEFAULT DIRECTORY (AZURE.CA...

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

Netskope-G-azure.capse-iss.com-SP-SAML-VA | 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 (preview)

Security
Conditional Access
Permissions
Token encryption

❸ **SAML Certificates**

Token signing certificate   ✎ Edit
Status   Active
Thumbprint   39A53D100C3CF04BEC3F59EA6B1C09BF2100F9EC
Expiration   8/24/2025, 11:23:19 AM
Notification Email iakin@azure.capse-iss.com
App Federation Metadata Url   https://login.microsoftonline.com/a4e03498-adc8...
Certificate (Base64)
Certificate (Raw)   Download
Federation Metadata XML

Verification certificates (optional) (Preview)
Required
Active
Expired

❹ Set up Netskope-G-azure.capse-iss.com-SP
You'll need to configure the application to link
Login URL
Azure AD Identifier
Logout URL

Find...   Netskope-G-azure.capse-iss.com-SP-SAML-VA.cer

```
1  -----BEGIN CERTIFICATE-----
2  MIIC8DCCAdigAwIBAgIQbqK0/aj+MYtDb0lFK3tCRjANBgkqhkiG9w0BAQsFADA0MTIwMAYD
3  EylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMjA4MjQx
4  MjBaFw0yNTA4MjQxNTIzMTlaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0
5  U1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtDRjbpQJ
6  uIi04aOqxMZrxfxw8eM7h33oHnM2PLmPO4WKVU8fKs7SGQz9CkIZ6YfETlHYuWDL2zGyjE7d
7  xuy/Ev1H6AENZ5I1Z397G6sa5309rdPoXTm9NgniEbumnIJxi+VZ2YnNabFJWTj5f+Je+LgL
8  /1MSzOsfs/dUDCmvEa9fqqonzpYWNz3510BuADfjI0kzNVuWG4oB2hkTfs/YShFBu4T1q2Bm
9  gpouxVQhJ3UuSQVwKxIp9fVMPkIOuM09KZHZJ5GE0B8XURm9g0wtoP2ed9exvV6D7FclD8CI
10 81VgNvs7XAJW2KZyB87P8UFXPQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAoak4El2X3imNU
11 Y1Tb/8//jNCqgHhzOBtS5vdbc0AtB+rCRfWanQQzFcoJNo6Dp9DkwwJJ03eMt0zxPgJikoMk
12 yrJWhR1karZ30SdoHohtl2ILltBZhRmspZiTT/fhZWnj9z9VnpE260eH91t1iQYwcQ5IYewM
13 pLecyajZBLani1btfTzFPaAQl/kcfbAwX3StDRA7gYk4+U+IKwj2SmZI1lGr+e2H6UTlQPS3
14 bdGGKUGPGLSFshd2qfjyovkbH7plPcHKxX5UO9gQAxuirdXUgH9mLqtMBUCxhSI4PEArswGm
15 Rc7H/Y90/enK2nIg01XT
16 -----END CERTIFICATE-----
```

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.

chrome enterprise

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 | Bypass ▾ | if success

| Block ▾ | if failure

Domain Name

azure.capse-iss.com

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

📎 netskope-358313-e1f721604e8f.json   ⬆ REPLACE FILE

CANCEL   SAVE

3P SAML IdP for Netskope (Microsoft Entra ID in this example)

1. Create a new Azure Enterprise Application **Microsoft Entra SAML toolkit**. For details on how to do this, see [Configure and test Microsoft Entra SSO for Microsoft Entra SAML Toolkit](#).

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

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

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
VVMxCzAJBgNVBAgTAkNBMRYwFAYDVQQHEw1Nb3VudGFpbiBWaWV3MSYwJAYDVQQK
Ex1Hb29nbGUgQ2hyb21lIFBhcnRuZXIgQWNjb3VudDEpMCcGA1UECxMgODRmZWFm
MTQ1N2Q3ZDJjNmNmODQ3NTlhM2ZiMTk5M2MxKTAnBgNVBAMTIGNhLnBhcnRuZXIt
Z29vZ2xlLmV1Lmdvc2tvcGUuY29tMSUwIwYJKoZIhvcNAQkBFhZjZXJ0YWRtaW5A
bmV0c2tvcGUuY29tMB4XDTIxMDMwMTIzMDAxNFoXDTMxMDIyNzIzMDAxNFowgdwx
CzAJBgNVBAYTAIVTMQswCQYDVQQIEwJDQTEWMBQGA1UEBxMNTW91bnRhaW4gVmll
dzEmMCQGA1UEChMdR29vZ2xlIENocm9tZSBQYXJ0bmVyIEFjY291bnQxKTAnBgNV

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/chromedevice/validate**

Google SAML SSO with Netskope

1. In the Google Admin console, <u>configure</u> Security-> Authentication -> SSO with Third Party IDP -> SSO Profile for Netskope.
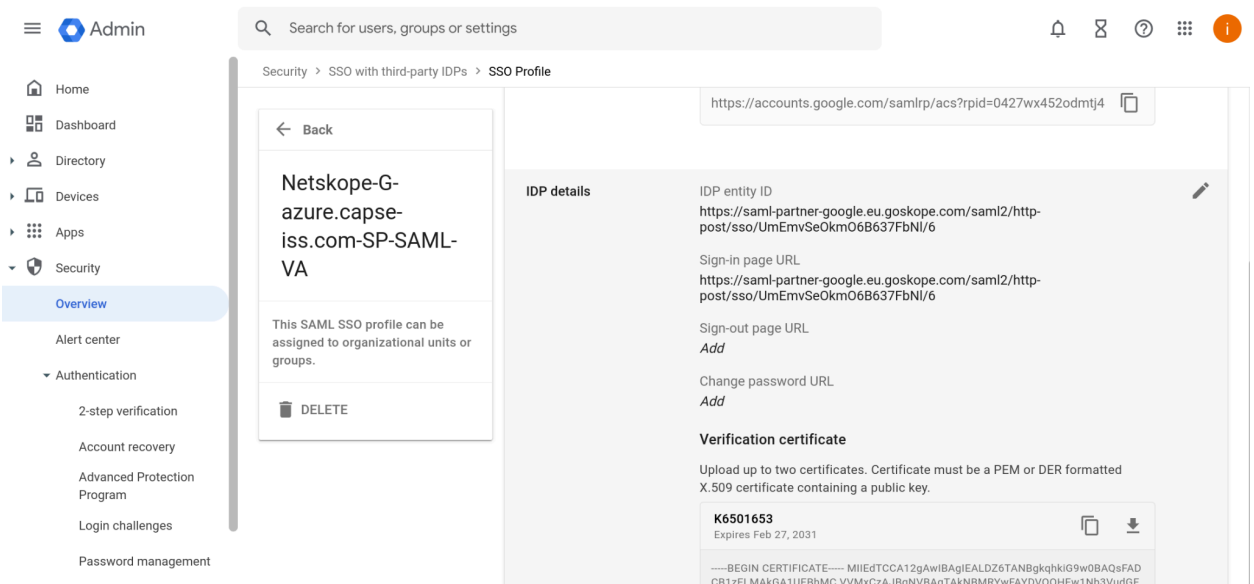
IdP entity ID and Sign-in page URL are SAML Proxy IDP URL from Netskope Settings of the SAML Reverse Proxy.

2. Copy the "Verification Certificate" from SAML Proxy Issuer Certificate.

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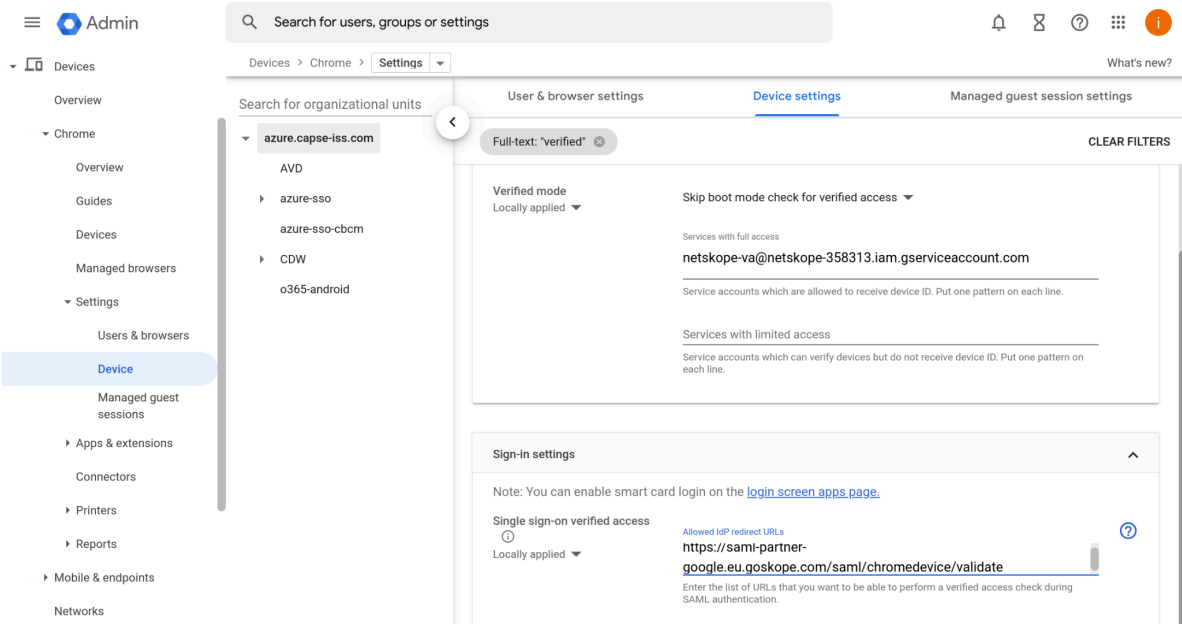
Create new account → **Provide Netskope SAML config to IdP and cloud app** → ✓ **Setup complete**

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	G 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

UmEmvSeOkmO6B637FbNl

SAML PROXY IDP URL

https://saml-partner-google.eu.goskope.com/saml2/http-post/sso/UmEmvSeOkmO6B637FbNl/6

SAML PROXY ACS URL

https://saml-partner-google.eu.goskope.com/saml2/http-post/acs/UmEmvSeOkmO6B637FbNl/6
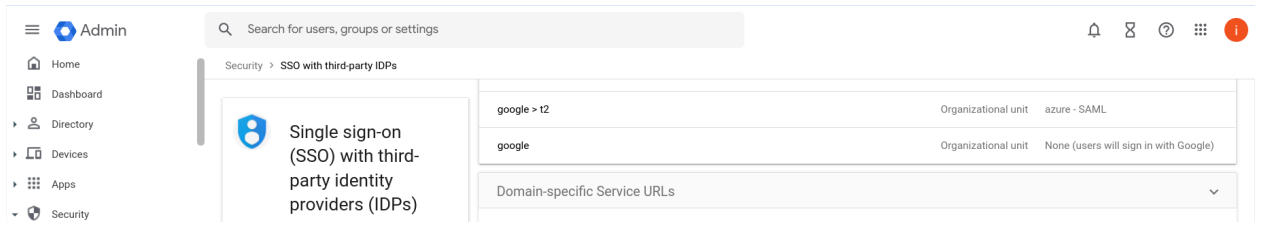
SAML PROXY ISSUER CERTIFICATE

-----BEGIN CERTIFICATE-----
MIIEdTCCA12gAwIBAgIEALDZ6TANBgkqhkiG9w0BAQsFADCB1zELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAkNBMRYwFAYDVQQHEw1Nb3VudGFpbiBWaWV3MSYwJAYDVQQK
Ex1Hb29nbGUgQ2hyb21lIIFBhcnRuZXIgQWNjb3VudDEpMCcGA1UECxMgODRmZWFm
MTQ1N2Q3ZDJjNmNmODQ3NTlhM2ZiMTk5M2MxKTAnBgNVBAMTIGNhLnBhcnRuZXIt
Z29vZ2xlLmV1Lmdvc2tvcGUuY29tMSUwIwYJKoZIhvcNAQkBFhZjZXJ0YWRtaW5A
bmV0c2tvcGUuY29tMB4XDTIxMDMwMTIzMDAxNFoXDTMxMDIyNzIzMDAxNFowgdwx
CzAJBgNVBAYTAIVTMQswCQYDVQQIEwJDQTEWMBQGA1UEBxMNTW91bnRhaW4gVmll
dzEmMCQGA1UEChMdR29vZ2xlIENocm9tZSBQYXJ0bmVyIEFjY291bnQxKTAnBgNV

CLOSE

3. Make sure the SSO profile is assigned to the appropriate organizational unit or group.

Under Manage SSO profile assignments.