

C chrome enterprise

# **Deliver Conditional Access for** ChromeOS in Microsoft Entra ID Guide

June 2024



# Contents

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



## 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<sup>1</sup>.

For more details on Conditional Access, see What is Conditional Access?

<sup>&</sup>lt;sup>1</sup> 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.

C 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 <u>Microsoft Defender for Cloud</u> <u>Apps</u>.

### 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:

- 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 <u>Conditional Access</u>. 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



## chrome enterprise

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 <u>this guide</u> or another mechanism.

The Root and signing CA certificates from the CA above will need to be added to MDCA.

 Verify that a ChromeOS device belonging to the relevant tenant and organizational unit is successfully obtaining a certificate via chrome://certificate-manager.

S chrome://certificate-manager × +			× _ ₽ ×
$\leftarrow \rightarrow C$ ( Chrome   chrome://certificate		< 🖈 🗰 🗄	
Your certificates	Certificate Viewer: System TPM Token:8612G03G47's iakin-W19SUBCA- CA ID	×	Others
You have certificates from these organizations that i	Ceneral Details Certificate Hierarchy		Import Import and Bind
org-iakin	System TPM Token:8612G03G47's iakin-W19SUBCA-CA ID	Import and Bind         83047's lakin-W19SUBCA-CA ID         Import and Bind         Im	
8612G03G47 (hardware-backed)	Certificate Fields		:
test1@iakin.net (hardware-backed)	··· Validity		:
	Not Before Not After		
	Subject		
	Subject Public Key Info Subject Public Key Algorithm		
	Subject's Public Key		
	Field Value		
	CN = 8612G03G47 OU = google		

SSO

- 1. Configure SSO and user provisioning between Microsoft Entra ID and the Google tenant <u>per documentation</u>.
- 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 <u>Conditional Access</u>.
  - a. Create a new policy.



## chrome enterprise

	Ø Search resources, services, and docs (G+/)	Þ.	R	a (	© ©	R	iakin@azure.capse-iss.c DEFAULT DIRECTORY (AZURE.CA
Home > Default Directory   Enterprise ap	plications > Enterprise applications   All applications > Google SAML iakin.net Profile						
Google SAML iakin.	net Profile   Conditional Access						×
*	+ New policy + New policy from template (Preview) 🕺 What If 🕐 Refresh   🖗 Got feedback?						
Deployment Plan							3 out of 3 policies found
Mapage	Policy Name ↑↓	State 1	r.		Creation	Date ↑↓	Modified Date ↑↓
Properties	Rumely Test Policy	Off			11/19/20	21, 1:59:09	PM 12/8/2021, 4:22:55 PM
A Owners	Conditional Access App Control	On			9/1/2022	8:36:06 AM	M 9/22/2022, 11:22:04 AM
& Roles and administrators	JipE Test	Report-	only		7/6/2022	4:13:02 PN	И
Users and groups							
Single sign-on							
Provisioning							
<ul> <li>Self-service</li> </ul>							
<ul> <li>Custom security attributes (preview)</li> </ul>							
Security							
😤 Conditional Access							
🖧 Permissions							
Token encryption							
b. Specify	y the users to whom the policy will apply.						

#### Microsoft Azure Home > Default Directory | Enterprise applications > Enterprise applications | All applications > Google SAML iakin.net Profile | Conditional Access > Conditional Access App Control Conditional Access policy Control access based on Conditional Access Control access based on who the policy will policy to bring signals together, to make apply to, such as users and groups, workload decisions, and enforce organizational policies. identities, directory roles, or external guests. Learn more Learn more Name \* What does this policy apply to? Users and groups $\sim$ Conditional Access App Control Include Exclude Assignments None Users (i) All users Specific users included Select users and groups Cloud apps or actions ① All guest and external users ① 2 apps included Directory roles 🕕 Conditions (i) Users and groups 1 condition selected Select Access controls 2 users Grant ① 0 controls selected test1 azure.capse-iss.com iakin test1@azure.capse-iss.com Session ① test1 iakin test1@iakin.net ... Use Conditional Access App Control

- 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.



Home > Default Directory   Enterprise applica	ations > Enterprise applications   All applications > Google SAML iakin.net Profile   Conditional Acc
Conditional Access App Co	ontrol
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more	Control access based on all or specific cloud apps or actions. Learn more Select what this policy applies to
Name *	Cloud apps 🗸
Conditional Access App Control	Include Exclude
Assignments	○ None
Users ①	All cloud apps
Specific users included	Select apps
Cloud apps or actions ① 2 apps included	Select
Conditions ①	
1 condition selected	Google SAML iakin.net Profile 4381e688-d260-400b-bb8c-58622dec6719
Access controls	<b>(</b> ] Office 365 ① ····
Grant ①	
0 controls selected	
Session 🕕	
Use Conditional Access App Control	

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

$\equiv$ Microsoft Azure $ ho$ Se	earch resources, services, and docs (G+/)	
··· > Enterprise applications   All application	s > Google SAML iakin.net Profile   Conditional Acce	Device platforms ×
Conditional Access App Co	ontrol	Apply policy to selected device platforms
Control access based on Conditional Access	Control access based on signals from conditions	Learn more
policy to bring signals together, to make decisions, and enforce organizational policies. Learn more	like risk, device platform, location, client apps, or device state. Learn more	Configure ① Yes No
Name *	Device platforms (i)	
Conditional Access App Control	Any device and 6 excluded	Include Exclude
Assignments	Locations ①	- Android
Users ①	- Not configured Client apps ①	✓ iOS
Specific users included		Vindows Phone
Cloud apps or actions (i)	Not configured	Vindows
2 apps included	Filter for devices ①	✓ macOS
Conditions ①	Not configured	Linux
1 condition selected		-
Access controls		
Grant 🕕		
0 controls selected		
Session 🛈		
Use Conditional Access App Control		

e. Under Session, check Use Conditional Access App Control to <u>enable</u> redirection to Defender.



$\equiv$ Microsoft Azure	♀ Search resources, services, and docs (G+/)	Þ.	<b>G</b> Q	۲	0 R	iakin@azure.capse-i default directory (Azu	ISS.C
Home > Default Directory   Enterprise app	lications > Enterprise applications   All applications > Google SAML iakin.net Profile   Conditional Access >				Session		×
Conditional Access App	Control						
Conditional Access policy					Control acces	is based on session co	ntrols to
Control access based on Conditional Access					enable limite cloud applica	d experiences within s tions.	pecific
decisions, and enforce organizational policies.					Learn more		
Name *					Use app o	enforced restrictions 🕕	
Conditional Access App Control					0		
Assignments					This col apps. C Online	strol only works with supp urrently, Office 365, Excha and SharePoint Online an	orted nge e the
Users ()	-				only do enforce	ud apps that support app d restrictions. Click here to	o learn
Specific users included					more.		
Cloud apps or actions ③					🔽 Use Cond	litional Access App Cont	trol 🛈
2 apps included	_				Use custo	om policy	$\sim$
Conditions ③			-1				
1 condition selected	-				1 Cus con	tom policies need to be figured in Cloud App Secu	urity
Access controls					for for	al. This control works inst eatured apps and can be parded for any app. Click	antly self bere to
Grant 🛈					lear	n more about both scenar	rios.
0 controls selected	_				Configure	custom policy	
Session ()					Sign-in fr	equency ①	
Use Conditional Access App Control					Persistent	t browser session ①	
					Customiz	e continuous access	0
					evaluatio	1	
						silience delaults	

**Defender for Cloud Apps** 

 In the Microsoft Entra ID Conditional Access policy Session screen, click on Configure custom policy. This opens <u>Defender for Cloud Apps</u>.



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

	Microsoft Defender	Cloud Apps	٩	© ? <mark>@</mark>	8
≡ ⊘	Dashboard	Get star Microsoft Des	rted with Defender for Cloud Apps ender for Cloud Apps enables you to take control of your cloud environment by prov	SYSTEM Settings Governance log	
0	Discover	data travel, an	nd sophisticated analytics to identify and combat cyberthreats across all your cloud se e a Cloud Discovery report (2) Connect apps (2) Create polic	ies Manage admin access	
69	Investigate			Exported reports Scoped deployment and privacy	
***	Control	SaaS Security Posture Management for non-Microsof communicated at GA. For more details, please see thi planet of the second s	It applications is currently in public preview via Secure Score for every customer with is article	SOURCES Defender for Cloud Apps: Licer Log collectors	×
ţ	Alerts	Dashboard		App connectors Conditional Access App Control DATA ENRICHMENT IP address ranges	
		Filter by app: All apps		User groups	ack

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



## C chrome enterprise

	Microsoft Defende	er for Clo	oud Apps		٩					٥	?	۵	8
= 0	Dashboard		Settings										
0 8 Hi 6	Discover Investigate Control Alerts	* * *	device System Device identification	×	Device identification Create access and session p Intune compliant device ic Identify devices that are co Automatically synced with Hybrid Azure AD joined il Identify devices that are hy Automatically synced with	bolicies based on device sta lentification nsidered Intune compliant Microsoft Intune   View cor entification brid Azure AD joined in you Azure AD   View configurat	te, by identifying yo by Microsoft Intune. figuration C or on-premises Activ on C	ur managed devices.	ed with Azure AD, ①				
					Client certificate based ide Identify managed devices b Upload your trusted root o + Add a root certificate Name	ntification by authenticating devices a r intermediate certificate as Description	ainst client certifica a PEM file. Issuer	tes. Subject	1 - 3 i Was added on ∨	of 3 certificates 🖽 Tai Was added by	ble setti	ngs ∨	
					Sub CA Root CA Sample Root Certific		- - -	-	Sep 8, 2022 Sep 8, 2022 Dec 8, 2021	iakin iakin uinam		:	
					Require certificate rev     be trusted. Note: A cli     certificates. If your clie     connect from manage     Save We sec	ocation check: certificates t ent certificate check requir nt certificate does not con d devices. re your data as described in ou	hat have been revok s the CRL protocol a ain a CRL endpoint, r privacy statement and	ed by the CA will no longer and applies to all you will not be able to					

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.

Settings - Microsoft Defender for × +						• _ □ ×
← → C   maltaracegoogle.portal.clou	udappsecurity.com/#/settings?section	on=deviceIdentification			< *	* & 🖬 🗄
💼 capse 💼 misc 💼 partner 🏟 pw Ġ 🕻	CrOS					Dther bookmarks
III Microsoft Defender for Clou						
<ul> <li>□ Dashbaard</li> <li>□ Dusover ∨</li> <li>○ Investigate ∨</li> <li>○ Control ∨</li> <li>Ø Alerts</li> </ul>	Settings 24 deces System Device identification Test Tr	ew and edit a root certificate ne * c/ c/ cription pe certificate akis-W19800T Email Organization unit Compt/Region	Name Enai Organization Organization Organization Country/Region	ukm-W155UBCA-CA ukin-W155UBCA-		
	ssuer	State Location	State Location			
				Jpdate Cancel		
		Root CA —	_	-		

- 4. Configure Connected Apps
  - a. Under the Settings gear menu, select Conditional Access App Control.



Microsoft Defer	nder for Cl	loud Apps					•
E Dashboard		Connected apps				SYSTEM Settings Governance log	
Discover	$\sim$	App connectors Conditional Access App Control apps	Security configuration ap	ps		Security extensions Manage admin access	
<ul> <li>Investigate</li> <li>Activity log</li> </ul>	^	The Conditional Access App Control adds real-time monitoring and To enable Conditional Access App Control capabilities on your apps	control capabilities for your app: , follow the deployment instructi	s. ons.		Exported reports Scoped deployment and privacy SOURCES	ngs
Files		Filters:				Log collectors	ers
Users and accounts		App: Select apps v App category: Select category v	Last connected: Select a date			App connectors Conditional Access App Control	
Security configuration						DATA ENRICHMENT	
Connected apps (5)		+ Add		1 - 5 of 5 Co	onditional Access App Control app	IP address ranges	
Control	~	App 🔨	Status	Available controls ①	Was connected on	User groups	
Policies		Google Workspace - General Collaboration	🥝 Connected	Azure AD conditional access Session control	Sep 22, 2022, 11:31 AM	Sep 22, 2022, 11:52 AM	:
Templates		Microsoft Account - General Content management	A No activities	Azure AD conditional access Session control	Sep 6, 2022, 7:53 PM	-	:
-		Microsoft OneDrive for Business - General Cloud storage	A No recent activities	Azure AD conditional access Session control	Sep 1, 2022, 10:28 AM	Sep 1, 2022, 11:16 AM	:
		Office 365 - General Collaboration	A No recent activities	Azure AD conditional access Session control	Sep 1, 2022, 9:52 AM	Sep 1, 2022, 9:52 AM	:
		Office Pestal Conservation	Commented	Anun AD annihimmi anna	See 1 2022 0:20 AM	S 22 2022 11-52 AM	:

- 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.

~	Use Conditional Access App Control ①
	Monitor only (Preview) 🗸 🗸
	Monitor only (Preview)
	Block downloads (Preview)
	Use custom policy
	Sign-in frequency 🛈

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.

	Microsoft Defender for	Cloud Apps	© ? © P
=			
Ø	Dashboard	Policies	0
0	Discover $\checkmark$	Customize alerts and actions by creating policies:     Create policy	×
69	Investigate $\checkmark$		
⇒	Control ^	Threat detection Information protection Conditional access Shadow IT All policies	
	Policies	Filters:	Advanced filters
	Templates	Name: Policy name Type: Select type v Status: Active DISABLED Severity:	. ~
æ	Alerts	+ Create policy ✓ ↓ Export 1 - 1 of 1 Polici	es 🍸 Hide filters 🔢 Table settings 🗸
		Policy Count Severity ✓ Category Action M	odified
		🛞 block-nocert 16 open alerts 💵 Low 🖧 Access control 🗘 🖗 Se	p 1, 2022 🛞 🔳 🗄
_			
	Microsoft Defender for C	loud Apps	© ? © A
=		<b>-</b> 10	
0	Dashboard	Edit access policy	View policy matches (16)
0	Discover $\checkmark$	Policy name *	
60	Investigate $\checkmark$	block-nocert	
₫	Control ^	Policy severity * Category *	
	Policies		
	Templates		
r r	Alerts		
		Activities matching all of the following	
		X Device v Tag v does not equal v Valid client certificate v 0	
		T AGD 8 INTE	
		Actions	
		Select an action to be applied when user activity matches the policy.	
		O Test Monitor all activities	
		Block     A default block message is displayed when possible	
		Customize block message O	



# Microsoft Entra ID Conditional Access for ChromeOS -Netskope

Provide Microsoft Entra ID Conditional Access for ChromeOS authorized by egress IP address with <u>Netskope</u>.

### 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 <u>configured</u> for SSO with SAML to Microsoft Entra ID.
  - a. In majority of deployments, Microsoft Entra ID users will be auto provisioned to Google using <u>Google Cloud/G Suite Connector by Microsoft</u>.
  - 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 <u>Chrome Extension installed and configured</u> via Chrome Admin Policy.
  - b. OR Netskope explicit proxy settings <u>configured</u> via Chrome Admin Policy.

### Configuration

Google SSO with Microsoft Entra ID

Security > SSO with third-party IDPs > SSO Profile

 In Google Admin, <u>configure</u> Security-> Authentication -> SSO with Third Party IDP -> SSO Profile for the Microsoft Entra ID tenant.

← Back	SAML SSO profile		^
azure	Name	azure	
This SAML SSO profile can be assigned to organizational units or groups.	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.	
		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	
		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.

=	🔿 Admin	Q Search	h for users, groups or settings			Ļ	8	?		()
Â	Home	Security >	SSO with third-party IDPs							
	Dashboard									
• 8	Directory		Single sign-on	google > t2	Urganizational unit	azure - SAML				
• 🗔	Devices	0	(SSO) with third-	google	Organizational unit	None (users w	ill sign i	in with G	Google)	
• 🎟	Apps		party identity	Domain-specific Service URLs						,
- 0	Security		providers (IDPs)							

3. In <u>Azure, configure</u> Enterprise Application with SAML SSO for the Google tenant.

≡ Microsoft Azure	∠ Search resources, services, and docs (G+/)					
Home > Default Directory   Enterprise app	lications > Enterprise applications   All applications	> Google SAML iakin.net Profile >				
Google SAML iakin.net F	Profile   SAML-based Sign-on					
«	T Upload metadata file S Change single sign-on Read the configuration guide B for help integrating GC	mode 🗯 Test this application 🛛 🖗 Got feedback? Dogle SAINE lakin: net Prome.				
Deployment Plan	1 Basic SAML Configuration		🖉 Edit			
Manage	Identifier (Entity ID)	https://accounts.google.com/samlrp/metadata?rpid=00ry				
Properties	Reply URL (Assertion Consumer Service URL)	919540vwrgg https://accounts.google.com/samlrp/acs?rpid=00ry91954				
A Owners	Sign on LIPI	0vwrgg				
Roles and administrators	SIGN ON OKE	919540vwrgg				
A Users and groups	Relay State (Optional) Logout Url (Optional)	Optional Optional				
Single sign-on						
Provisioning	2 Attributes & Claims					
Self-service	Autibutes & Claims		🖉 Edit			
Custom security attributes	givenname	user.givenname				
(preview)	emailaddress	user.mail				
Security	name Unique User Identifier	user.userprincipalname user.userprincipalname				
🍨 Conditional Access		· • · · · · • • · · · · · ·				
Permissions	3 SAML Certificates					
Token encryption	Talas invite antiGate					
Activity	Status	Active	🖉 Edit			
	Thumbprint	7B3D03DFE319E9DB228E3ED8F4E0CE7F79761209				
Jign-in logs	Expiration Notification Email	8/19/2025, 10:26:57 AM iakin@azure.capse-iss.com				
👬 Usage & insights	App Federation Metadata Url	https://login.microsoftonline.com/a4e03498-adc8				
Audit logs	Certificate (Base64)	Download				
Provisioning logs	Federation Metadata XML	Download				
ã Access reviews						
Troubleshooting + Support	Verification certificates (optional) (Preview)	Ne	🖉 Edit			
Sirtual assistant (Preview)	Active	NO 0				
	Expired	0				
	4 Set up Google SAML iakin.net Profile					
	You'll need to configure the application to lin	k with Azure AD.				
	Login URL	https://login.microsoftonline.com/a4e03498-adc8				
	Azure AD Identifier	https://sts.windows.net/a4e03498-adc8-405b-812				
	Logout URL	https://login.microsoftonline.com/a4e03498-adc8				

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.

9	chrome enter	prise				
	Home > Default Directory   Enterprise Google SAML iakir Enterprise Application	applications > Enterprise applications   All applica <b>n.net Profile</b>   Users and group	tions > Google SAML iakin.net Profile			
	~	🕂 Add user/group 🖉 Edit  🗎 Remove	Description of the second se			
	<ul> <li>Beployment Plan</li> <li>It is application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →</li> </ul>					
	Manage	Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registr				
	Properties	O First 200 chown to soarch all years & groups onter a display name				
	A Owners	Display Name	Object Ture			
	🤱 Roles and administrators		Object Type			
	Users and groups	Al az1 iakin	User			
		TI test1 iakin	User			
	<ul> <li>Provisioning</li> </ul>	TI test2 iakin.net	User			
	Self-service					

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.

~	Security Cloud Platform > Forward Proxy > SAML - Forward Proxy					
<ul> <li>← Security Cloud Platform</li> <li>Users</li> <li>Groups</li> <li>Devices</li> </ul>	Set up SAML Providers to be used to auth your IdP. Anticomposition of the set of the se	enticate users when going through the Netskope Forward Proxy. Additionally, providers can be set up here to allov oogle.eu.goskope.com/UmEmvSeOkmO6B637FbNI				
Enforcement SAML MDM Distribution	SAML ACS URL: https://nsauth-partner-g DOWNLOAD SAML CERTIFICATE	oogle.eu.goskope.com/nsauth/saml2/http-post/UmEmvSeOkmO6B637FbNI/acs				
REVERSE PROXY	NAME	IDP URL				
Office 365 Auth	Google SAML	https://accounts.google.com/o/saml2/idp?idpid=C03kw6ewz				
ActiveSync Auth Integration	Google azure-cros.com	https://accounts.google.com/o/saml2/idp?idpid=C01shde4y				
FORWARD PROXY	G azure.capse-iss.com	https://accounts.google.com/o/saml2/idp?idpid=C01242o6m				
SAML Authentication	G iakin	https://accounts.google.com/o/saml2/idp?idpid=C03dbnmf3				
ON PREMISES	MS azure.capse-iss.com	https://login.microsoftonline.com/a4e03498-adc8-405b-8125-b2fdf25b6931/saml2				
On-Premises Infrastructure CDPP for Appliance						



Edit Account	×
NAME * MS azure.capse-iss.com SETUP OPTIONS	
IDP SSO URL * https://login.microsoftonline.com/a4e03498-adc8-405b-8125-b2fdf25b6931/saml2	
IDP ENTITY ID * https://sts.windows.net/a4e03498-adc8-405b-8125-b2fdf25b6931/	
IDP CERTIFICATE • BEGIN CERTIFICATE MIIC8DCCAdigAwIBAgIQUcluPc3Sh4NDyyk5MothnjANBgkqhkiG9w0BAQsFADA0MTIw YDVQQD EyINaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yM MDQxNjA1 NTIEFW0WITA4MDOwNIA4NTheMDOwMIAWBeNMBANATKU12V2hrs39mdCBBenM475B4	MA IjA4
CANCEL	WE

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

	Security Cloud Platform > Forward Proxy >		
•••	Authentication - Forward Proxy		
← Security Cloud Platform → NETSKOPE CLIENT →	Setup Authentication for Netskope for Web users to be redirected to the configu you are using IdP to provision the Netskope Client, authentication needs to be en	red Identity Provider. This allows you to capture the ide abled.	entity o
Users Groups	Authentication		
Devices Enforcement SAML	Authentication: ● Enabled Type: SAML Authentication: MS azure.capse-iss.com		
MDM Distribution	ENABLE AUTHENTICATION		
SAML Office 365 Auth	Bypass Settings		
ActiveSync Auth Integration	Administrators can use this section to identify domains and categories for w	which user authentication is not required.	
FORWARD PROXY	DOMAIN BYPASS None Specified		
Authentication	EDIT		
Epoble Autho	ntication	×	
Enable Authe			
	•		
Enabled SAML ACCOUNT MS azure.caps	e-iss.com Tree-iss.com		
Enabled SAML ACCOUNT MS azure.caps	ie-iss.com  CREATE NEW N REFRESH INTERVAL		
Enabled SAML ACCOUNT MS azure.caps AUTHENTICATIO Days	ie-iss.com  CREATE NEW N REFRESH INTERVAL  Hours		
Enabled SAML ACCOUNT MS azure.caps AUTHENTICATIO Days ENABLE COOKIE	CREATE NEW CREATE NEW ON REFRESH INTERVAL () Hours SURROGATE		
Enabled SAML ACCOUNT MS azure.caps AUTHENTICATIO Days ENABLE COOKIE	e-iss.com CREATE NEW N REFRESH INTERVAL Hours SURROGATE i		

3. In <u>Azure</u>, <u>configure</u> 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.

🖉 Edit

chrome ente	erprise				
≡ Microsoft Azure		Search resources, services, and docs (G+/)			
Home > Enterprise applications	All applications > Netskope-G-azure.capse-iss.com-SP-SAN	IL-VA			
Netskope-G-azu     Enterprise Application	ıre.capse-iss.com-SP-SAML-VA   ∪	sers and groups			
	≪ 🕂 Add user/group 🖉 Edit 🔟 Remove 🔑 ।	Jpdate Credentials 🛛 🗮 Columns 🕴 🔗 Got feedback?			
<ul><li>Overview</li><li>Deployment Plan</li></ul>	The application will appear for assigned users within	1) The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. $ imes$			
✗ Diagnose and solve problems	Assign users and groups to app-roles for your applicati	on here. To create new app-roles for this application, use the application registration.			
Manage	First 200 shown, to search all users & groups, enter	a display name.			
Properties	Display Name	Object Type			
A Owners	G- g-permit-office365-access-only-via-netsk	appe Group			
🍰 Roles and administrators		Group			
• Hears and around		aioup			

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

**Configure Chrome traffic steering** 

 In Google Admin -> Devices -> Chrome ->Apps & extensions -> Users & browsers add and <u>configure</u> Netskope Chrome Extension from the Chrome Web Store to be deployed to the appropriate organizational unit or group.

= 💽 Admin	Q	Search for users, groups or settings						
- Devices		Select an app from Chrome Web Store				×		
Overview		Home		View app by ID				
Overview		a chrome web store		Confidential II	nternal Version			
Guides		netskonel	-					
Devices			Extens	ions (i)	1 of 1 extensions			
Managed browsers		« Home						
➤ Settings		O Extensions						
- Apps & extensions		O Themes			Netskope Chrome Extension			
Overview		O Apps		••	Extension to enforce Netskope Cloud Explicit Proxy			
Users & browsers		Ratings						
Kiosks		0 ****						
Managed guest		○ ★★★★ & up						
sessions		O ★★★★ & up						



= 🔿 Admin	Q Search for users, groups or settings					¢ 8 @ III 🚺
- Devices	Devices > Chrome > Apps & extensions v					
Overview			Overview	Users & browsers	Kiosks	Managed guest sessions Requests
← Chrome     Overview	Users v		Play Store Block all apps, admin	Chrome Web Store Allow all apps, admin	ADDITIONAL SETTINGS	Netskope Chrome Extension 📋 🗗 🗙
Guides			manages allowlist manages blo			
Devices	Groups	~	+ Search or add a filter			Installation policy
Managed browsers	Organizational Units	^	Арр	Installation policy	Version pinning	Locally added
<ul> <li>Settings</li> </ul>	Search for organizational units		Netskope Chrome Extension	nsion Njajgikpb	Not pinned	Version pinning
<ul> <li>Apps &amp; extensions</li> <li>Overview</li> </ul>	✓ google	_				Not pinned   Inherited from Google default
Users & browsers	Azure-SAML-Profile-Test					Chrome Web Store options
Kiosks	fc					Include in Chrome Web Store collection
Managed guest sessions	gscep Netskope-VA-test					Permissions and URL access
Requests	ping-test1					Use default permissions for this organization 🔻
Connectors	t2					Blocked hosts
<ul> <li>Printers</li> </ul>						One per line. Maximum of 100 URLs.
▶ Reports						Allowed hosts
<ul> <li>Mobile &amp; endpoints</li> </ul>						
Networks						One per line; allowed nosts override blocked nosts. Maximum or 100 URLs.
<ul> <li>Apps</li> </ul>						Inherited from Google default
<ul> <li>Security</li> </ul>						{"tenant":{"Value":"partner-
▶ II Reporting						google.eu.goskope.com"),"block_disable":
> 🗄 Billing						{ value :ue}, enforce_os :{ value : + ["cros"]},"bypass_list":{"Value":

- 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.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.

=	Microsoft Azure	,P Search resources, services, and docs (G+/)	Þ	Ģ	۵ ۵	() ନି	iakin@azı DEFAULT DIF	ure.capse-iss.c RECTORY (AZURE.CA
Ногг	e > Default Directory   Security >	Security   Conditional Access > Conditional Access			Updat	te locati	ion (IP r	anges) ×
<u></u>	Conditional Access	Named locations			↑ Uploa	ad 🛓 Dowr	nload 📋 De	elete
_	~	+ Countries location 🕂 IP ranges location 🗹 Configure multifactor authentication trusted IPs \mid 🞘 Got fee	lback?					
	Dverview (Preview) Policies	Named locations are used by Azure AD security reports to reduce false positives and Azure AD Conditional Access policie	s. Learn more		Configure i	named location	n IPv4 and IPv	5 ranges. Learn more
<b>9</b> I	nsights and reporting	Location type : All types Trusted type : All types			Netskope	IP Addresses		
<b>X</b> I	Diagnose and solve problems			-	Mark a	as trusted loca	tion	
Man	age	Name	$\uparrow_{\downarrow}  \text{Location type} $		+			
↔ 1	Named locations	DBHome	IP ranges					
<b>i</b> (	Custom controls (Preview)	Netskope IP Addresses	IP ranges		4.31.195.	0/26	ĺ.	Ŭ
<b></b>	ferms of use				8.36.116.	0/24	ĺ.	ŭ
<b>*</b> '	/PN connectivity				8.39.144.	0/24	ĺ.	Ŭ
*	Authentication context (Preview)				31.186.23	19.0/24	ĺ.	Ì
	Elassic policies				74.217.93	1.0/24	ĺ	Ì
Mon	itoring				103.219.7	9.0/24	ĺ	ď
€	Sign-in logs				103.47.24	14.0/24	t	Ì
	Audit logs				163.116.1	28.0/17	t	Ì

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

^	Security Cloud Platform > Reverse Proxy > SAML - Reverse Proxy
← Security Cloud Platform	SAML proxy is required to steer sanctioned cloud app traffic to the reverse proxy running in your tenant ins
IPSec	Create new account $\rightarrow$ Provide Netskope SAML config to IdP and cloud app $\rightarrow$ $\bigotimes$ Setup complete
GRE	Start setup by creating an account with information from your Identity Provider (IdP) and cloud application
Explicit Proxy	your identity provider and cloud application. Refer to the Help documentation for details.
NETSKOPE CLIENT	ADD ACCOUNT NETSKOPE SOURCE IP





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



$\equiv$ Microsoft Azure	$\mathcal{P}$ Search resources, services, and docs (G+/)
Home > Enterprise applications   Conc permit-office365-acce	litional Access > Conditional Access   Policies > ss-only-via-netskope (iakin)
Conditional Access policy	
🔟 Delete	
Control access based on Conditional Acce policy to bring signals together, to make decisions, and enforce organizational polic Learn more	<ul> <li>Control access based on who the policy will apply to, such as users and groups, workload</li> <li>identities, directory roles, or external guests.</li> <li>Learn more</li> </ul>
Name *	What does this policy apply to?
permit-office365-access-only-via-netsko	pe Users and groups 🗸 🗸
Assignments	Include Exclude
Users (1)	○ None
Specific users included	○ All users
	<ul> <li>Select users and groups</li> </ul>
Cloud apps or actions ()	All guest and external users ①
1 app included	
Conditions (i)	
1 condition selected	Users and groups
Access controls	Select
Grant ①	i group
Block access	G- g-permit-office365-access-on ***
Session 🕕	

b. Select Cloud apps such as Office365.

# C chrome enterprise

$\equiv$ Microsoft Azure	$^{ m  ho}$ Search resources, services, and docs (G+/)
Home > Enterprise applications   Cond permit-office365-acce Conditional Access policy Delete	itional Access > Conditional Access   Policies > ss-only-via-netskope (iakin) …
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational police Learn more	SS Control access based on all or specific cloud apps or actions. Learn more ies. Select what this policy applies to
Name *	Cloud apps V
permit-office365-access-only-via-netsko	pe Include Exclude
Assignments	O None
Users ()	All cloud apps
Specific users included	<ul> <li>Select apps</li> </ul>
Cloud apps or actions ①	Select
1 app included	Office 365
Conditions (i)	Office 365 ① ····
1 condition selected	

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

Home > Default Directory   Security > Securi permit-office365-access-o	Device platforms $\times$		
Delete			Apply policy to selected device platforms. Learn more
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more	Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more		Configure () Ves No
Name *	Device platforms ①		Include Exclude
permit-office365-access-only-via-netskope	Any device and 6 excluded		Android
Assignments	Locations ①		iOS
Users ①	Any location and 1 excluded		Vindows Phone
Specific users included	Client apps ①		Vindows
Cloud apps or actions ①	Not configured		🗸 macOS
1 app included	Filter for devices ③		Linux
Conditions ①	Not configured		-
2 conditions selected			

d. Set condition to exclude Netskope location created above.

C chrome enterprise

	Search resources, services, and docs (G+/)		D 🕞 🗘	©	iakin@azure.capse-iss.c DEFAULT DIRECTORY (AZURE.CA
Home > Enterprise applications   Condition permit-office365-access- Conditional Access policy Delete	al Access > Conditional Access   Policies > only-via-netskope (iakin) …		Select Locations Location type : All types True	isted type : <b>All types</b>	×
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more	Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more	Control user access based on their physical location. Learn more Configure ①	Search names     Name     Multifactor authentication trustee	↑↓ Location type	Trusted Yes
Name * permit-office365-access-only-via-netskope	Device platforms ① Not configured	Yes No	DBHome Netskope IP Addresses	IP ranges	Yes
Assignments Users ① Specific users included	Locations ① Any location and 1 excluded Client apps ①	Select the locations to exempt from the policy All trusted locations Selected locations			
Cloud apps or actions ① 1 app included Conditions ① 1 condition selected	Not configured Filter for devices ① Not configured	Select Netskope IP Addresses Netskope IP Addresses ····			

### e. Set Access controls to Block.

	✓ Search resources, services, and docs (G+/)	Iakin@azure.capse-iss.c DEFAULT DIRECTORY (AZURE.CA
Home > Enterprise applications	Conditional Access > Conditional Access   Policies >	Grant ×
permit-office365-a Conditional Access policy	access-only-via-netskope (iakin)	
🔟 Delete		Control access enforcement to block or grant access. Learn more
Control access based on Condition policy to bring signals together, to decisions, and enforce organization Learn more	ial Access make nal policies.	Block access     Grant access     Require multifactor
Name * permit-office365-access-only-via-	-netskope	authentication Require device to be marked as compliant
Assignments		Require Hybrid Azure AD ① joined device
Users ① Specific users included		Require approved client app ① See list of approved client apps
Cloud apps or actions ① 1 app included		Require app protection policy ① See list of policy protected client apps
Conditions ①		
		For multiple controls
Access controls		<ul> <li>Require all the selected controls</li> <li>Require one of the selected controls</li> </ul>
Block access		



## Verified Access for ChromeOS via SAML SSO - Netskope

How to use the <u>Netskope</u> 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.





										-
	🐉 My Proj	ject 3837 🔻		٩		>_	2	?	:	D
RPI API Library			Q verified X							
API Library > "verified"										
= Filter Type to filter		"verified"								
Visibility	^	2 results								
Public	(2)									
Category	^		Chrome Verified Access API Google							
Maps	(1)		API for Verified Access chrome extension to provide credential verification for chrome devices connecting to an enterprise	netwo	ork					

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





	Google Cloud 🔹 iakin 👻	Q. Search					
θ	← Create service account						
÷ <u>e</u>	Service account details						
Θ	Creat this service account account						
<b>A</b>	(optional)	to project					
цэ, (П	<ul> <li>Grant users access to this service</li> </ul>	account (optional)					
2	Grant access to users or groups that need to perform account. Learn more	n actions as this service					
	Service account users role	0					
۹	Grant users the permissions to deploy jobs and VMs w	ith this service account					
>	Service account admins role	<b>0</b>					
÷	Grant users the permission to administer this service a	CCOUNT					
	DONE CANCEL						
	E Google Cloud • My F	Project 3837   Q Search Products, resources, docs (/)					
e	IAM & Admin	← netskope-va					
+	IAM	DETAILS PERMISSIONS KEYS METRICS LOGS					
e		Service account details					
	Identity & Organization	Service account details					
3	Policy Troubleshooter						
3	Policy Troubleshooter	Name Name SAVE					
3	Policy Troubleshooter	Name					
	Policy Troubleshooter Policy Analyzer Organization Policies	Name     netskope-va     SAVE       Description     SAVE					
3	Policy Troubleshooter Policy Analyzer Organization Policies	Name     netskope-va     SAVE       Description     SAVE       Email					
3 []	<ul> <li>Policy Troubleshooter</li> <li>Policy Analyzer</li> <li>Organization Policies</li> <li>Service Accounts</li> </ul>	Name       netskope-va       SAVE         Description       SAVE         Email       netskope-va@glass-ranger-353315.iam.gserviceaccount.com					
	<ul> <li>Policy Troubleshooter</li> <li>Policy Analyzer</li> <li>Organization Policies</li> <li>Service Accounts</li> <li>Workload Identity Federat</li> </ul>	Name       netskope-va       SAVE         Description       SAVE         Email       netskope-va@glass-ranger-353315.iam.gserviceaccount.com         Unique ID					
	<ul> <li>Policy Troubleshooter</li> <li>Policy Analyzer</li> <li>Organization Policies</li> <li>Service Accounts</li> <li>Workload Identity Federat</li> <li>Labels</li> </ul>	Name       netskope-va       SAVE         Description       SAVE         Email       netskope-va@glass-ranger-353315.iam.gserviceaccount.com         Unique ID       105501299170501491569					
ی ا ا ا	<ul> <li>Policy Troubleshooter</li> <li>Policy Analyzer</li> <li>Organization Policies</li> <li>Service Accounts</li> <li>Workload Identity Federat</li> <li>Labels</li> </ul>	Name       netskope-va       SAVE         Description       SAVE         Email       netskope-va@glass-ranger-353315.iam.gserviceaccount.com         Unique ID       105501299170501491569					
م ا ا ا ا ا	<ul> <li>Policy Troubleshooter</li> <li>Policy Analyzer</li> <li>Organization Policies</li> <li>Service Accounts</li> <li>Workload Identity Federat</li> <li>Labels</li> <li>Tags</li> </ul>	Name       netskope-va       SAVE         Description       SAVE         Email       netskope-va@glass-ranger-353315.iam.gserviceaccount.com         Unique ID       105501299170501491569         Service account status       Service account status					
	<ul> <li>Policy Troubleshooter</li> <li>Policy Analyzer</li> <li>Organization Policies</li> <li>Service Accounts</li> <li>Workload Identity Federat</li> <li>Labels</li> <li>Tags</li> <li>Settings</li> </ul>	Name       netskope-va       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.					
	<ul> <li>Policy Troubleshooter</li> <li>Policy Analyzer</li> <li>Organization Policies</li> <li>Service Accounts</li> <li>Workload Identity Federat</li> <li>Labels</li> <li>Tags</li> <li>Settings</li> </ul>	Name       netskope-va       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.         Image: Comparison of the service account status       Comparison of the service account status         Disabling your account allows you to preserve your policies without having to delete it.       Image: Comparison of the service account status					
	<ul> <li>Policy Troubleshooter</li> <li>Policy Analyzer</li> <li>Organization Policies</li> <li>Service Accounts</li> <li>Workload Identity Federat</li> <li>Labels</li> <li>Tags</li> <li>Settings</li> <li>Privacy &amp; Security</li> </ul>	Name       netskope-va       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.         Caccount currently active       DISABLE SERVICE ACCOUNT					

4. Under Keys, create a new JSON Key.

# C chrome enterprise

≡	Google Cloud S• My Pr	roject 3837 👻	<b>Q</b> Search Products, resources, docs (/)		
θ	IAM & Admin	etskope-va			
+•	IAM	DETAILS PERMISS	IONS KEYS METRICS LOGS		
Θ	Identity & Organization	Keys			
٩	Policy Troubleshooter	A Service accoun	t keys could pose a security risk if compromised. We	recommend you avoid	downloading service account keys and
	Policy Analyzer	You can learn n	nore about the best way to authenticate service acco	unts on Google Cloud	nere .
	Organization Policies	Add a new key pair or uploa	ad a public key certificate from an existing key pair.		
연	Service Accounts	Block service account key Learn more about setting o	creation using organization policies. rganization policies for service accounts		
	Workload Identity Federat	ADD KEY 👻			
۹	Labels	Create new key	Kov	Key creation date	Key expiration date
	Tags	Upload existing key	adc0ddbf26ddebd334259bf8655f3d877edc0664	Aug 18, 2022	Dec 31, 9999
\$	Settings				

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

	Google Cloud S• My Pr	roject 3837 🐱 Q Search Products, resources, docs (/)
0	IAM & Admin	← netskope-va
+ <u>e</u>	IAM	DETAILS PERMISSIONS KEYS METRICS LOGS
Θ	Identity & Organization	Keys
٩	Policy Troubleshooter	Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use
	Policy Analyzer	You can learn more about the best way to authenticate service accounts on Google Cloud nere.
	Organization Policies	Add a new key pair or upload a public key certificate from an existing key pair.
연	Service Accounts	Private key saved to your computer
	Workload Identity Federat	
•	Labels	A glass-ranger-353315-88d79681f519.json allows access to your cloud resources, so store it securely. Learn more best practices
>	Tags	
\$	Settings	CLOSE



#### 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.

~	Security Cloud Platform > Rev	erse Proxy > erse Proxy					
← Security Cloud Platform	oud SAML proxy is required to steer sanctioned cloud app traffic to the reverse proxy running in your tenant instance.						
1 abristicis	Create new account →	Provide Netskope SAML c	onfig to IdP and cloud app	→ Setup complete			
IPSec	Start setup by creating an ac	count with information	from your Identity Provide	er (IdP) and cloud application. Then comp	lete the setup by p	roviding the Netskope settings to	
Explicit Proxy	your identity provider and cl	loud application. Refer t	to the Help documentation	for details.			
	ADD ACCOUNT NET	SKOPE SOURCE IP					
Users		47	DUCATION	400 101		DVDACC	
Groups	NAME	AP	PLICATION	ACS URL		BYPASS	
Devices	Google-azure.c	Netskope Settings G	Google Accounts	https://accounts.google.	.com/samlrp/acs	No	
Enforcement							
SAML							
MDM Distribution							
REVERSE PROXY							
SAML							
-	,						
Edit Accourt	+				$\mathbf{\times}$		
Edit Accoun	l				^		
NAME *							
Google-27ur	e conseriss com-SAMI	1-\/A					
Google-azul	e.capse-iss.com-sAivii	L-VA					
APPLICATION	*						
Coorde	Accounts						
	Accounts						
SETUP	OPTIONS						
ACS URL *							
https://acco	unts.google.com/samlr	rp/acs?rpid=042	27wx452odmtj4				
IDP SSO URL *							
IDI 350 OKE							
https://login	.microsoftonline.com/	/a4e03498-adc8	8-405b-8125-b2f	df25b6931/saml2			
IDP CERTIFICA	ТЕ*						
BEGINIC	FRTIFICATE						
MIIC8DCCA	AdigAwIBAgIQbqK0/a	j+MYtDb0lFK3	tCRjANBgkqhkiC	9w0BAQsFADA0MTIwM	A		
YDVQQD	2Nu7nOgOVn1an-U-			)-\//Zn\/2E07T4 ~50* 4:	^		
4MjQxNTIz	σοιανζηψεάχρτεmUg	κιτινκΖλJnaG\		σανν Ζρτ Ζευζ ΓΑθΕΨΟΥΜΙ/	4		
MiDeFuQuh			N/DANATI/114-5//2	headenderDan (475DC7)			
CANCEL				SAV	/E		

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



=	🔿 Admin	Q Search for users, groups or settings					0		1
Â	Home	Security > SSO with third-party IDPs > SS	SO Profile						
₽₿	Dashboard	← Back	SAML SSO profile					^	
• 0	Directory		News						
• [0	Devices	Netskope-G-	Name	Netskope-G-azure.capse-iss.com-SP-S	AML-VA				
·	Apps	iss.com-SP-SAML-							
• 0	Security	VA	SP details	Your IDP will need these details to set up IDP's documentation for more information	o SSO with Google as the Si on.	P. Cheo	sk your		
	Overview			Entity ID					
	Alert center	This SAML SSO profile can be assigned to organizational units or		https://accounts.google.com/samlrp dmtj4	o/metadata?rpid=0427wx4	520			
	<ul> <li>Authentication</li> </ul>	groups.		ACS URL					
	2-step verification	DELETE		https://accounts.google.com/samlrp	o/acs?rpid=0427wx452odr	ntj4			
	Account recovery								
	Advanced Protection								
	Program		IDP details	IDP entity ID				/	P.
	Login challenges	J		nttps://sami-partner-google.eu.goskop post/sso/UmEmvSeOkmO6B637FbNI/	ie.com/sami2/http- 6				
	Password management			Sign-in page URL					
	SSO with SAML applications			https://saml-partner-google.eu.goskop post/sso/UmEmvSeOkmO6B637FbNI/	e.com/saml2/http- 6				

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

$\equiv$ Microsoft Azure $\wp$ Search resour	ces, services, and docs (G+/)		D 🗗 🗘	© ©	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									
<ul> <li>Cverview</li> <li>Deployment Plan</li> <li>Diagnose and solve problems</li> <li>Manage</li> <li>Properties</li> <li>Owners</li> </ul>	Upload metadata file "> Change single sign-or SAML Certificates Token signing certificate Status Thumbprint Expiration Notification Email App Federation Metadata Url Contificate (@ace64)	CO9BF2100F9EC	🖉 Edit						
<ul> <li>Roles and administrators</li> <li>Users and groups</li> </ul>	Certificate (Raw) Federation Metadata XML	Find Netskope-G-azure.capse-iss.com-SP-SAML-VA.ce							
<ul> <li>Single sign-on</li> <li>Provisioning</li> <li>Self-service</li> <li>Custom security attributes (preview)</li> </ul>	Verification certificates (optional) (Preview) Required Active Expired	1BEGIN CERTIFICA 2 MIICBDCCAdigAwIBAGIQ 3 EylNaWNyb3NvZnQgQxp1 4 MJBaFw9yNTA4MjQxNTIz 5 UINPIENIcnRpZmljYXRL 6 UIIO4AQqMZrXfxW8EM7 7 xuy/EvlH6AENZ5112397	NBgkqhkiG9w0BAQsFADA0MTIwMAY DZXJ0awZpY2F0ZTAeFw0yMjA4MjQ pY3Jvc29mdCBBenVyZSBGZWRlcmF FAAOCAQ8AMTIBCgKCAQEAtDRjbpQ SGQ29CkIZ6YFETIHYuWDL2ZGyJF7 mIJXi+VZ2YNAbFJWTj5f+Je+Lg						
Security     4       Conditional Access     4       Permissions     7       Token encryption	3         8         /JMS2Osf5/dUCGwEa9fqonzpVWR235108uA0fj18kzNvukGA0827           3         Set up Netskope-G-azure.capse-iss.com-sf         9         gpguxVQhJ3UuSQVwkx1p9fVMPk10uM90KZHZJSGE088XURm9gevtoF           4         Set up Netskope-G-azure.capse-iss.com-sf         9         gpguxVQhJ3UuSQVwkx1p9fVMPk10uM90KZHZJSGE088XURm9gevtoF           4         B1VgNvs 7XAJWZKZJ887PBUFXPQ1DAQABMA96CSqGS15DSDQEBWLAA4         11         Y1Tb/8//JNCqHhz0B1SSvdbc6dXB+rCRFWanQ2FcoJNo6Dp9Dkw           4         11         Y1Tb/8//JNCqHhz0B1SSvdbc6dXB+rCRFWanQ2FcoJNo6Dp9Dkw         12         12           Login URL         13         pLecyajZBLan11btfTzFPaAQ1/kcfbAxx3StDRA7gYk4+U+IKwj2Sn         14         bdGKUG9GLSFshd2qfjyovkbH7p1PcHkxXSU09qQAxu1rdXUgH9mLc           Azure AD Identifier         16         Rc7H/Y96/enK2n1gQ1XT         16        END CERTIFICATE           4        END CERTIFICATE         17        END        END								

- 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.

	chromo	ontornerico
$\sim$		

CANCEL

Edit Accour	nt	$\times$					
SETUP	OPTIONS						
EMERGENCY E	Ied						
The following	settings are only applicable when emergency bypass is disabled.						
Bypass A	uth checks for Mobile 📧						
Enable SA	AML assertion key-value pairs matching 📧						
Enable IP	address based access (1)						
Enable cli	ent certificate check requirement 🚯						
🔽 Enable Go	oogle Chromebook Verified Access 🚯						
Action	Bypass if success						
	Block if failure						
Domain Name							
azure.ca	azure.capse-iss.com						
Service Account Credentials							
Uploaded	by iakin@google.com on Thu Sep 29 2022 12:02:05 GMT-4						
0 netsko	ppe-358313-e1f721604e8f.json 1 REPLACE FILE						

Deliver Conditional Access for ChromeOS in Microsoft Entra ID Guide | 2024



### chrome enterprise

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

 Create a new Azure Enterprise Application Microsoft Entra SAML toolkit. For details on how to do this, see <u>Configure and test Microsoft Entra SSO for Microsoft Entra SAML</u> <u>Toolkit</u>.



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.

*	Security Cloud Platform > Reverse Proxy > SAML - Reverse Proxy									
<ul> <li>← Security Cloud</li> <li>Platform</li> </ul>	SAML proxy is required to steer sanctioned cloud ap	op traffic to the reverse proxy running in your	tenant instance.							
Configuration	Create new account       →       Provide Netskope SAML config to IdP and cloud app       →       Setup complete									
TRAFFIC STEERING	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.									
Steering Configuration	ADD ACCOUNT NETSKOPE SOURCE IP									
App Definition										
Publishers	NAME	APPLICATION	ACS URL	BYPASS						
IPSec	Google-azure.capse-i 🗘 Netskope Settings	G Google Accounts	https://accounts.google.com/samlrp/acs?rpid=	No						
GRE										



## chrome enterprise

#### **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.

 $\times$ 

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 Ex1Hb29nbGUgQ2hyb21IIFBhcnRuZXIgQWNjb3VudDEpMCcGA1UECxMgODRmZWFm MTQ1N2Q3ZDJjNmNmODQ3NTIhM2ZiMTk5M2MxKTAnBgNVBAMTIGNhLnBhcnRuZXIt Z29vZ2xlLmV1Lmdvc2tvcGUuY29tMSUwIwYJKoZIhvcNAQkBFhZjZXJ0YWRtaW5A bmV0c2tvcGUuY29tMB4XDTIxMDMwMTIzMDAxNFoXDTMxMDIyNzIzMDAxNFowgdwx CzAJBgNVBAYTAIVTMQswCQYDVQQIEwJDQTEWMBQGA1UEBxMNTW91bnRhaW4gVmII dzEmMCQGA1UEChMdR29vZ2xIIENocm9tZSBQYXJ0bmVyIEFjY291bnQxKTAnBgNV

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.
- In Single sign-on verified access -> Allowed IdP redirect URLs, enter https://saml-<netskope tenant id>.goskope.com/saml/chromedevice/validate



= 💽 Admin	Q Search for users, groups or setting	js		¢	8	?	••••	1
- Devices	Devices > Chrome > Settings -						What's	s new?
Overview	Search for organizational units	User & browser settings	Device settings	Managed gue	st sessi	on set	tings	
- Chrome	✓ azure.capse-iss.com	Full-text: "verified"				CL	EAR FI	LTERS
Overview	AVD							
Guides	▶ azure-sso	Verified mode Locally applied 🔻	Skip boot mode check for verified access $igstar{}$					
Devices	azure-sso-cbcm		Services with full access					
Managed browsers	Managed browsers CDW		netskope-va@netskope-358313.iam.gser	viceaccount.com	ו			11
✓ Settings	o365-android		Service accounts which are allowed to receive device ID. Put one pattern on each line.					
Users & browsers			Services with limited access					
Device			Service accounts which can verify devices but do not receive device each line.					
Managed guest sessions								-
Apps & extensions		Sign-in settings					~	
Connectors		Noto: You can anable amort car	d login on the login earson oppo page					
<ul> <li>Printers</li> </ul>		Single sign-on verified access	a login on the <u>login screen apps page.</u>					
▶ Reports		i) Locally applied ▼	Allowed IdP redirect URLs https://sami-partner-			1	0	
Mobile & endpoints			google.eu.goskope.com/saml/chromede Enter the list of URLs that you want to be able to perform	vice/validate m a verified access ch	eck durin	g		
Networks			SAML authentication.					

Google SAML SSO with Netskope

 In the Google Admin console, <u>configure</u> Security-> Authentication -> SSO with Third Party IDP -> SSO Profile for Netskope.

≡	🔿 Admin	Q Search for users, groups or settin	gs		1	ļ	8	?		()
0	Hama	Security > SSO with third-party IDPs > SS	SO Profile							
	Dashboard	← Back		https://accounts.google.com	/samlrp/acs?rpid=0427wx45	2odm	ntj4	Ō		
) Do	Directory									
• [0	Devices	Netskope-G-	IDP details	IDP entity ID	goskone.com/saml2/http-				/	*
• ::::	Apps	iss.com-SP-SAML-		post/sso/UmEmvSeOkmO6B6	37FbNI/6					
- 0	Security	VA		Sign-in page URL https://saml-partner-google.eu	.goskope.com/saml2/http-					
	Overview			post/sso/UmEmvSeOkmO6B6	37FbNl/6					
	Alert center	This SAML SSO profile can be assigned to organizational units or		Sign-out page URL <i>Add</i>						
	- Authentication	groups.		Change password URL						
	2-step verification	DELETE		Add						
	Account recovery			Verification certificate						
	Advanced Protection Program			Upload up to two certificates. Ce X.509 certificate containing a pu	ertificate must be a PEM or DE ublic key.	≀ forr	natted			
	Login challenges			<b>K6501653</b> Expires Feb 27, 2031		ſ	Ō	Ŧ		
	Password management			BEGIN CERTIFICATE MIIEdT	CCA12gAwiBAgiEALDZ6TANBgkqh	kiG9w	0BAQs	FAD		

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.

chrom	e enterprise									
~	Security Cloud Platform > Reverse Proxy > SAML - Reverse Pr	Security Cloud Platform > Reverse Proxy > SAML - Reverse Proxy								
← Security Clou Platform	d SAML proxy is required to steer sanctioned	SAML proxy is required to steer sanctioned cloud app traffic to the reverse proxy running in your tenant instance.								
Configuration	Create new account → Provide Netskope SAML config to IdP and cloud app →  Setup complete									
TRAFFIC STEERING	Start setup by creating an account with info your identity provider and cloud application	rmation from your Identity Provider (IdP) and n. Refer to the <mark>Help</mark> documentation for details.	cloud application. Then complete the setup by	providing the Netskope settings to						
Steering Configuration	ADD ACCOUNT NETSKOPE SOURCE	IP								
App Definition	NAME	APPLICATION	ACS URL	BYPASS						
IPSec	Google-azure.capse-i 🗘 Netskop	e Settings G Google Accounts	https://accounts.google.com	/samlrp/acs?rpid= No						
GRE										

### 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.

 $\times$ 

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 Ex1Hb29nbGUgQ2hyb21IIFBhcnRuZXIgQWNjb3VudDEpMCcGA1UECxMgODRmZWFm MTQ1N2Q3ZDJjNmNmODQ3NTIhM2ZiMTk5M2MxKTAnBgNVBAMTIGNhLnBhcnRuZXIt Z29vZ2xILmV1Lmdvc2tvcGUuY29tMSUwIwYJKoZIhvcNAQkBFhZjZXJ0YWRtaW5A bmV0c2tvcGUuY29tMB4XDTIxMDMwMTIzMDAxNFoXDTMxMDIyNzIzMDAxNFowgdwx CzAJBgNVBAYTAIVTMQswCQYDVQQIEwJDQTEWMBQGA1UEBxMNTW91bnRhaW4gVmII dzEmMCQGA1UEChMdR29vZ2xIIENocm9tZSBQYXJ0bmVyIEFjY291bnQxKTAnBgNV

CLOSE

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



### Under Manage SSO profile assignments.

≡	🔿 Admin	Q Search	h for users, groups or settings			¢	8	?		0
Â	Home	Security >	SSO with third-party IDPs							
모등	Dashboard									
, °	Directory	A	Single sign-on	google > t2	Organizational unit	azure - SAML				
• 🗔	Devices	U	(SSO) with third-	google	Organizational unit	None (users wi	ll sign i	n with G	oogle)	
• 🎟	Apps		party identity	Domain-specific Service URLs					~	
- 0	Security		providers (IDPS)							