Netskope CA Rotation Guide v2.3

Change log

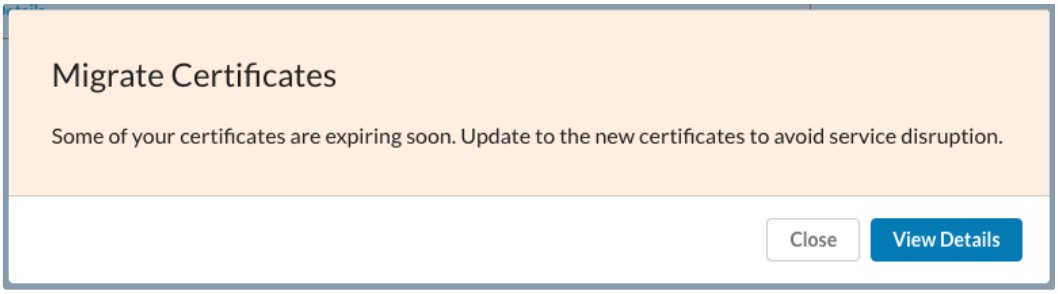
Version	Date	Description
1.0		Initial version for AM2 Rotation
2.0	2024-10-23	Initial version with new migration UI
2.1	2025-01-22	Update Publisher rotation
2.2	2025-03-5	Update about impact on MacOS if cert is not deployed via MDM and end user does not have admin rights to trust the new certificate in the device trust store
2.3	2025-04-15	Update steps to follow for BWAN IdP based User Authentication

Introduction

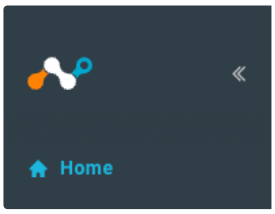
Netskope Security Cloud leverages a dedicated Netskope Certificate Authority (CA) for a number of services. The Netskope CA is dedicated per Management Plane (MP).

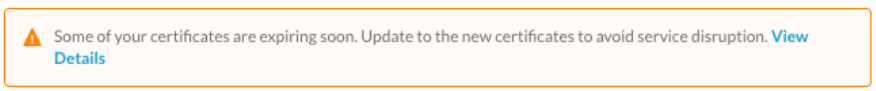
The Netskope CA deployed in FR4 MP expires on March 20th 2025 and needs to be replaced.

A new FR4 Netskope CA is available for installation. Please start the migration when the message is prompted on the management console login.

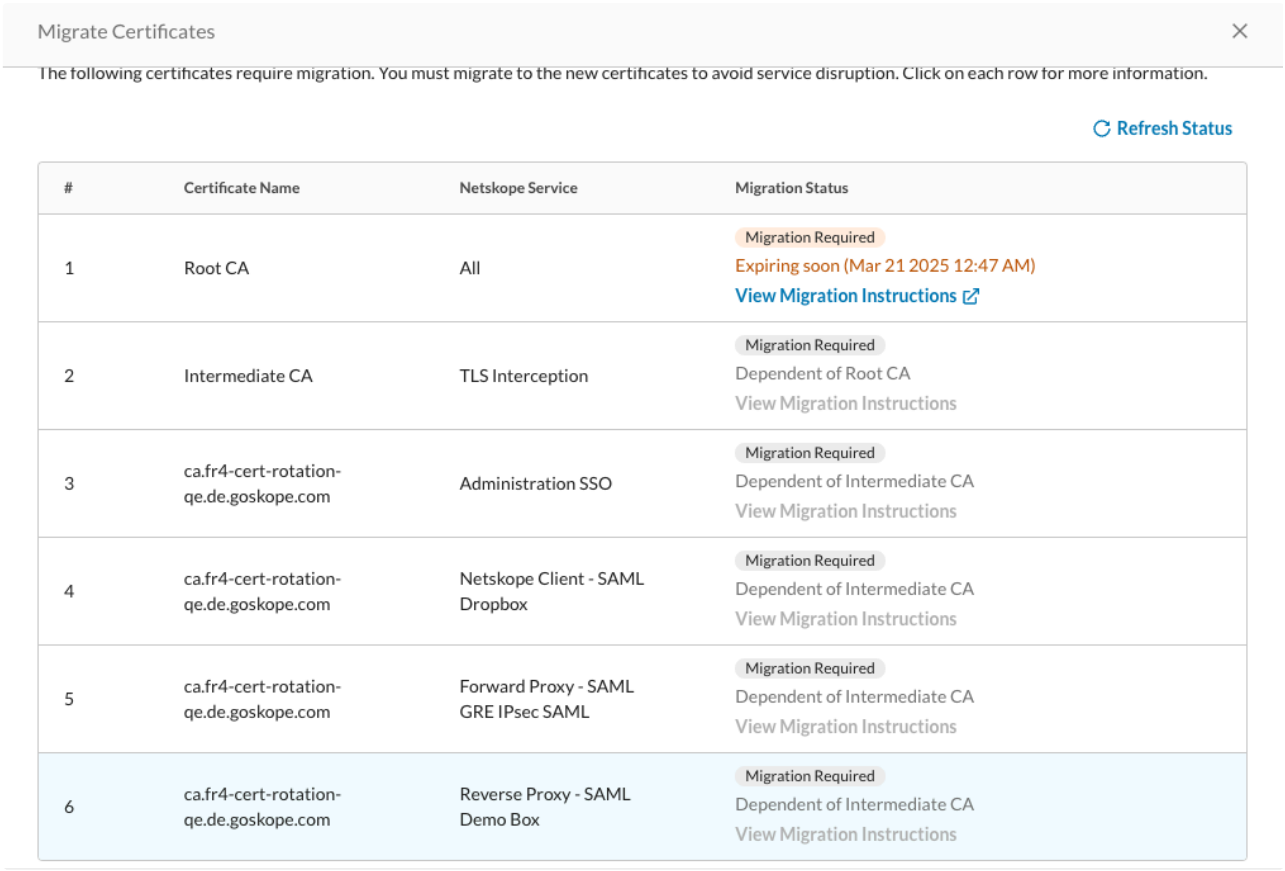


A splash screen will show up after login, once per login. The splash screen will change colour and text depending on the time left for expiration. In addition you will also see a toast message on the home screen once the tenant is enabled for rotation





Clicking on view details will open a migration modal that shows you all the configurations that need to be updated to complete migration and guides you the relevant screens in the UI to update the configuration. As you update configurations to use the new certificates, the modal will be updated to reflect the step has been completed.



We request customers to go through this guide before following steps on the Netskope console. This guide is designed to provide a step by step approach to complete the rotation smoothly. Please contact your TAM/CSM or Netskope support if you have questions.

We request customers to complete the rotation before the expiration date of Match 20th 2025 to avoid any outages.

Definitions

Netskope CA: Root of the Internal PKI managed by Netskope. There is one Root per Management Plane.

Expiring Netskope CA: Root of the Netskope PKI that will expire soon

New Netskope CA: Root of the Netskope PKI that is being provisioned to replace Expiring Netskope CA

SAML Certificate: Server certificate used for authentication features, the SAML Certificate has samlidp in the CN and is signed by the Netskope CA.

Expiring SAML Certificate: SAML Certificate signed by the Expiring Netskope CA.

New SAML Certificate: SAML Certificate signed by the New Netskope CA.

Rotation overview

The rotation is performed with the following stages:

- Stage 0 (Initial): tenant with single Netskope CA (Expiring Netskope CA), state before rotation
- Stage 1 (Assessment and Preparation): tenant has 2 Netskope CA provisioned but Expiring Netskope CA is still used, customer admins can deploy the New Netskope CA and activate it partially for SSL interception
- Stage 2 (Rotation): tenant has 2 Netskope CA provisioned and New Netskope CA is active, customer admins can still use the Expiring Netskope CA for SSL interception for specific situation. In Stage 2, all Netskope services are migrating to the New Netskope CA automatically, including NS Client and NPA authentications. Customer admins are rotating SAML Certificate one by one. At the end of Stage 2, only the New Netskope CA is used for all configuration
- Stage 3 (Completion): Expiring Netskope CA is deleted and no longer trusted and available for any service

The following chapters will guide you step by step for each stage.

Stage 1.1 - Assessment

This step is to identify all the services/features that are running in the tenant being rotated. This will help to identify all the requirements and potential impact when rotation is initiated.

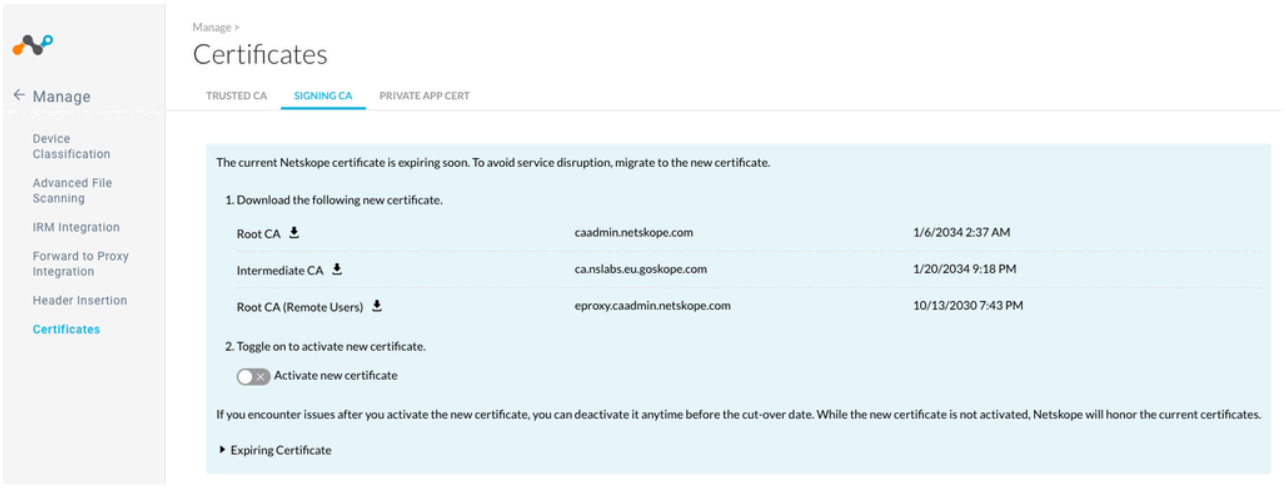
Please identify which one of the 4 services are being used in your tenant (refer to sub section if needed)

Feature	Deployed (Yes/No)	Comments
Inline Proxy with SSL interception signed by Netskope CA		Check sub sections for more details Any Cloud access method (NS Client, GRE/IPSec, DPOP ….)
NS Client for CASB/SWG/CFW/NPA steering		To check if NS Client is used, please go to Settings > Secure Cloud Platform > Devices
NPA Publishers		To check is NPA is used, please go to Settings > Secure Cloud Platform > Publishers
IDP Authentication		All feature relying on SAML or WS-FED protocols. Please check the section for more details.

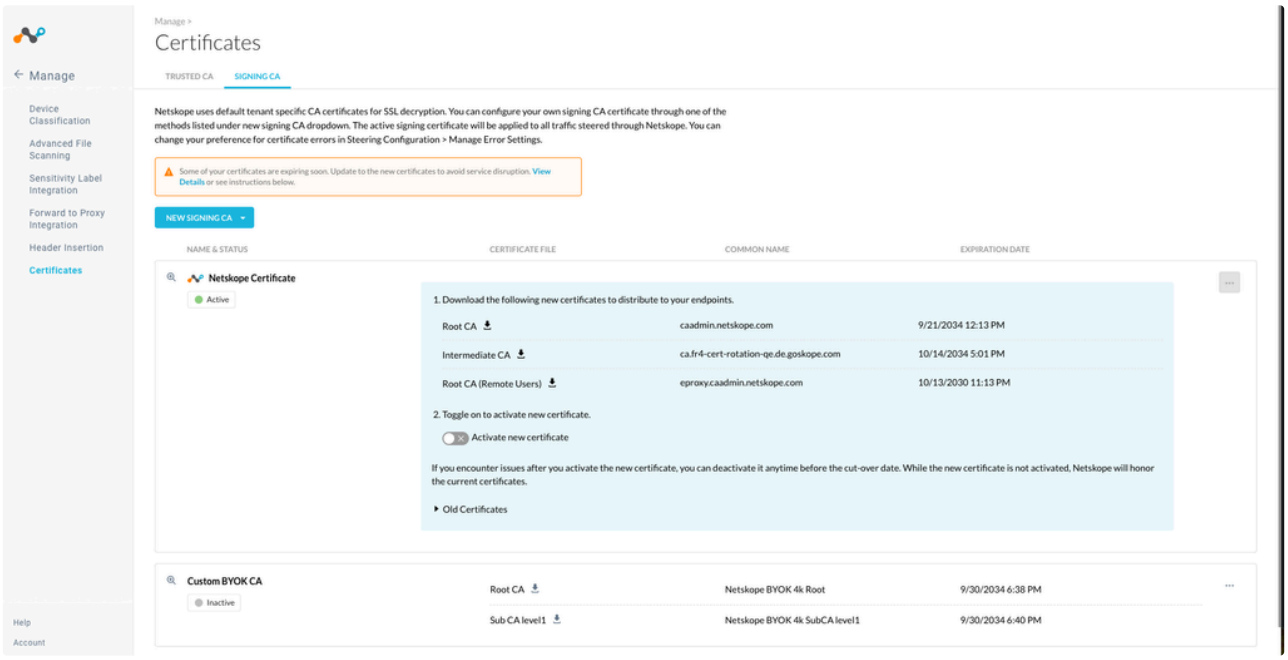
Assessment for Cloud SSL interception

Please first verify if the Netskope CA is active for SSL interception in the Cloud by looking at Settings > Manage > Certificates > Signing CA:

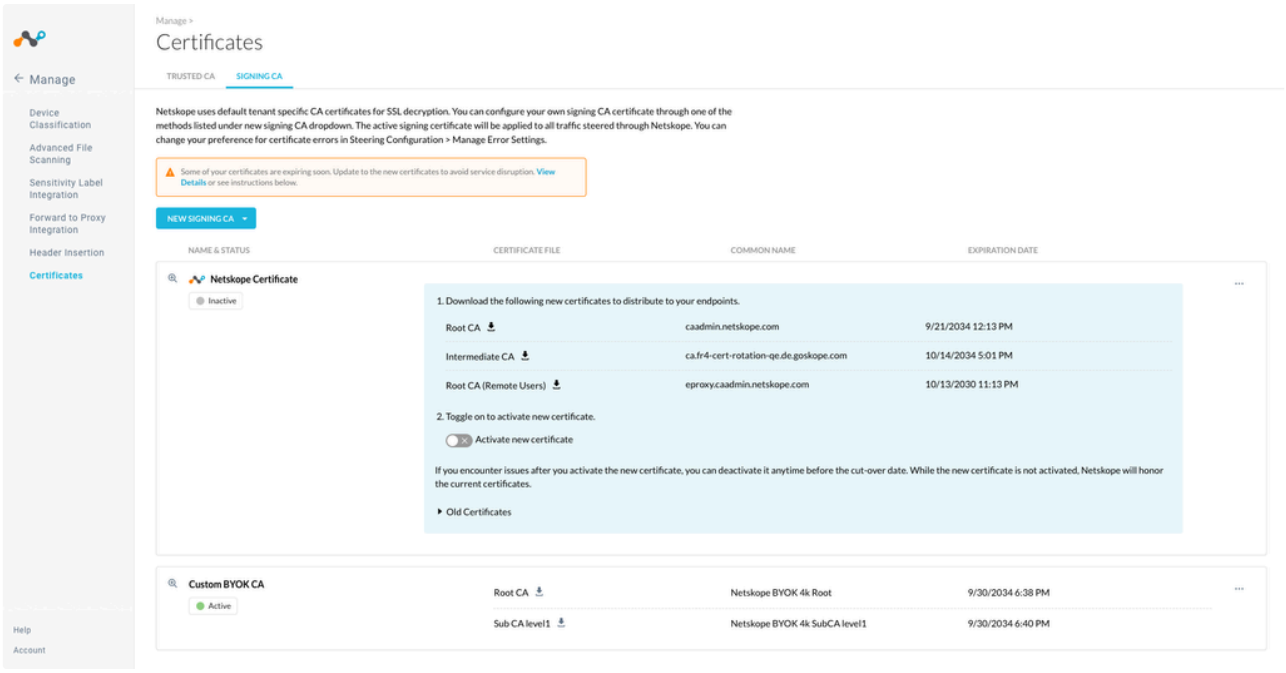
- If the following screen is visible (tenant without BYOK license), Netskope CA is active



- If the following screen is visible (tenant with BYOK license), Netskope CA is active if there is an "**Active**" status below Netskope Certificate



- If the following screen is visible (tenant with BYOK license), Netskope CA is **NOT** active if there is an "**Active**" status below Custom CA



If Netskope CA is not active (i.e BYOK or On Prem HSM are active), Root rotation has **NO** impact on SSL interception and this section (assessment/preparation) can be ignored. However, client certificate and SAML certificates are still derived from the Netskope CA and will need to be rotated. Please follow the instructions (for BYOK/On Prem HSM) in Stage 2.

Please fill the following table, it is possible to verify which access method is currently used with Skope IT > Page Events, OS Family is the recommended field to identify the OS

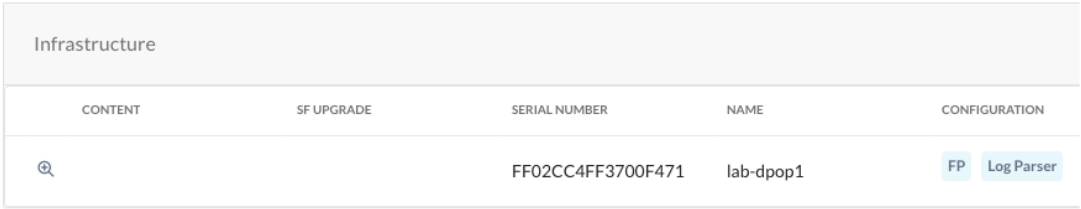
Access method deployed	Deployed (Yes/No)	Comments
NS Client - Windows, Steering active		
NS Client - Windows, Steering disabled (other access method used)		
NS Client - Windows Servers, Steering active		
NS Client - Windows Servers, Steering disabled (other access method used)		
NS Client - MacOS		
NS Client - MacOS, Steering disabled (other access method used)		
NS Client - Linux		
NS Client - Linux, Steering disabled (other access method used)		
NS Client - iOS		
NS Client - Android		
NS Client - ChromeOS		

GRE/IPSEC		Access Method = GRE or IPSEC
Proxy Chaining with SSL interception On-Premises		Access Method = Explicit Proxy, Proxy defined in Settings > Security Cloud Platform > Proxy Chaining
Proxy Chaining without SSL interception On-Premises		Access Method = Explicit Proxy, Proxy defined in Settings > Security Cloud Platform > Proxy Chaining
Cloud Explicit Proxy		Access Method = Explicit Proxy

If you still have Mobile Profile or Secure Forwarder deployed, please contact us.

Assessment for On-Premises SSL interception

To verify if DPOP is deployed on a tenant, please go to Settings > Security Cloud Platform > On-Premises Infrastructure, DPOP are identified by “FP” (Forward Proxy) Configuration:



If DPOP is not deployed, this paragraph can be skipped.

To validate which CA is used to decrypt the traffic, connect to the CLI and run “show dataplane forward-proxy server-cert” in config mode.

Mode	CLI result	Example
DPOP - Netskope CA	No certificate found	lab-dpop1> configure Entering configuration mode lab-dpop1(config)# show dataplane forward-proxy server-cert Nothing to show
DPOP - Custom CA	A certificate is recorded	lab-dpop1> configure Entering configuration mode lab-dpop1(config)# show dataplane forward-proxy server-cert "-----BEGIN CERTIFICATE----- ….

Assessment for NPA

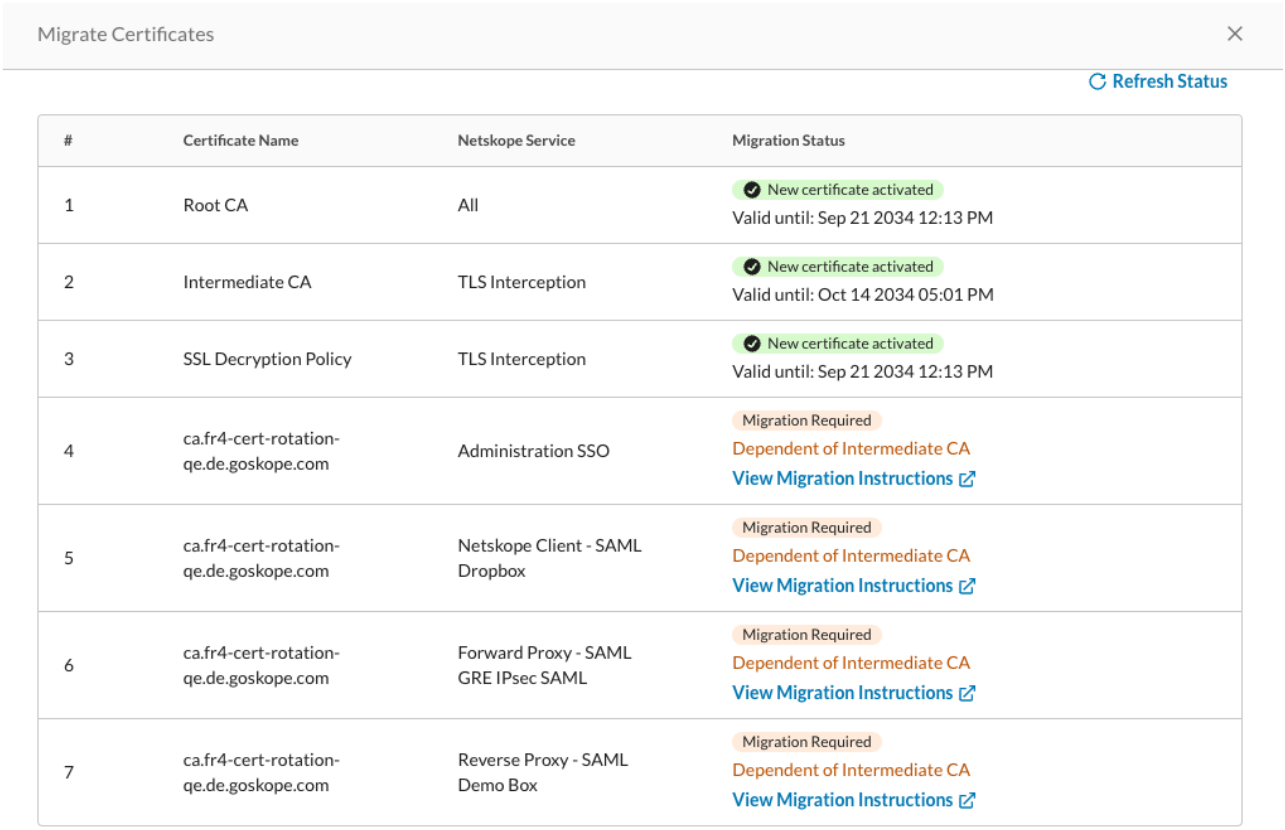
To check which features are being used in NPA, please use the table below

Feature	Deployed (Yes/No)	Comments
Publishers		Please go to Settings > Secure Cloud Platform > Publishers
Local Broker		please go to Settings > Secure Cloud Platform > Local Broker

Assessment for IDP Authentication

To identify which Netskope services are using SAML certificates for IdP Authentication, and their corresponding configurations, please reference the migration modal on the Netskope admin console.

If the customer is using IdP based User Authentication for SD-WAN Client, although not mentioned in the migration modal, additional steps will be required



Reverse proxy for private apps (aka NPA browser access) does not need rotation

O365 Auth configuration needs rotation only if the “re-sign SAML assertions” setting is turned on

IdP based User Authentication for Endpoint SD-WAN Client needs rotation

Migration of SAML certificate is only performed at the end of the rotation process.

Stage 1.2 - Preparing devices

This step is intended to define:

- If Netskope client upgrades are needed
- If manual deployment of New Netskope CA is needed on some devices
- Provide knowledge on expected impact if the rotation is enabled before full deployment of the requirements.

Inline Proxy with SSL interception signed by Netskope CA

If you didn't deploy "Inline Proxy with SSL interception signed by Netskope CA", you can skip this step.

When SSL interception is performed with Netskope CA, the Netskope Root must be trusted by all devices to avoid error messages.

This table allows to identify which devices will need to be updated with new NS Client version or New Netskope CA deployed via a Device Management Solution.

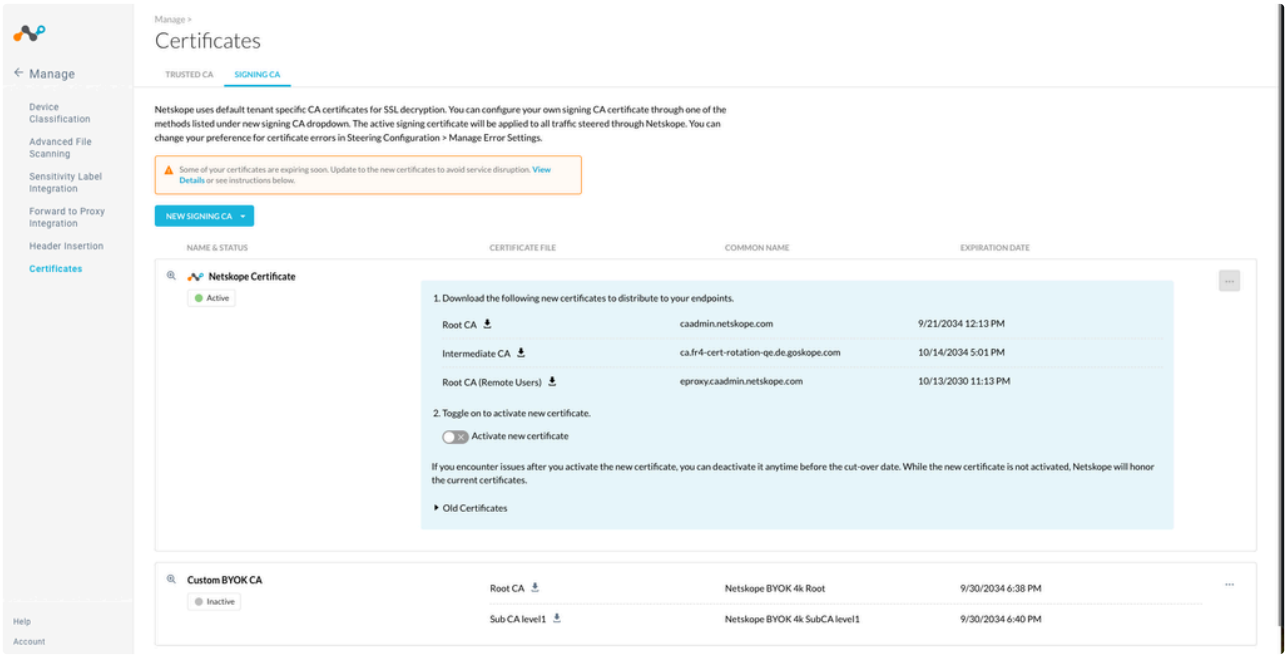
Access method deployed	Mandatory preparation before rotation	Impact if requirement are not completed
NS Client - Windows, Steering active	Recommended version: 120 Supported versions: • 114.1 • 117.1 • 120 and above NS Client will update Root CA automatically once rotation is activated.	Before R111, NS Client will not install New Netskope CA to Firefox profile and Java keystore, and the Firefox or Java initiated TLS connections will have errors with SSL decryption after CA rotation. Potential mitigation: update Firefox/Java with Device Management Solution No impact expected. NS Client downloads update every 60 minutes by default and will receive the New Netskope CA and new Client certificates. New Netskope CA will be installed and trusted immediately, NS Proxy will continue to use Expiring Netskope CA for SSL interception until tunnel is restarted. When tunnel is restarted, NS Client will use the new Client certificate and NS Proxy will use the New Netskope CA. ⚠ Please update all NS Client deployments to supported versions mentioned here. Inability to do so may lead to outages
NS Client - Windows, Steering disabled (other access method used)	New Netskope CA must be deployed on devices with the Device Management Solution	By default, NS Proxy will switch immediately to the New Netskope CA while NS Client didn't download and install the New Netskope CA. User will experience errors until NS Client successfully updates the configuration which is every 60 minutes (reminder, user can force update in Configuration page of NS Client).
NS Client - Windows Servers, Steering active	Same as NS Client - Windows, Steering active	Same as NS Client - Windows, Steering active
NS Client - Windows Servers, Steering disabled (other access method used)	Same as NS Client - Windows, Steering disabled	Same as NS Client - Windows, Steering disabled
NS Client - MacOS, Steering active	New Netskope CA must be deployed on devices with the Device Management Solution	NS Client will push New Netskope CA but End user validation is requested. NS Client

	Recommended version: 120 Supported versions • 114.1 • 117.1 • 120 and above	tunnel will not establish until user accept to trust the New Netskope CA. Note: If the end user does not have admin rights, they will not be able to trust the new certificate in the device trust store. As a result, the end user pop-up cant be removed and the NS Client will not establish the tunnel to Netskope. Bellow R114.1 a bug is asking user to accept new certificate even if the certificate is already installed on MacOS.
NS Client - MacOS, Steering disabled (other access method used)	New Netskope CA must be deployed on devices with the Device Management Solution	NS Client will push New Netskope CA at configuration update (every 60 min) but End user validation is requested. User will experience errors until CA installation and approved. Note: If the end user does not have admin rights, they will not be able to trust the new certificate in the device trust store. As a result, the end user pop-up cant be removed and the NS Client will not establish the tunnel to Netskope. Bellow R114.1 a bug is asking user to accept new certificate even if the certificate is already installed on MacOS.
NS Client - Linux, Steering active	Recommended version: 120 Supported versions • 114.1 • 117.1 • 120 and above NS Client will update Root CA and restart tunnel automatically once rotation is activated.	Before R113, With Chrome browser on Linux, NS client will remove the Expiring Netskope CA when installing the New Netskope CA; if tunnel is connected while CA rotation happens, the Proxy still uses the Expiring Netskope CA for SSL decryption, and the Chrome browser on Linux may only accept the New Netskope CA. The workaround is to disable and enable client to restart tunnel to use New Netskope CA. No impact expected. NS Client downloads update every 60 minutes by default and will receive the New Netskope CA and new Client certificates. New Netskope CA will be installed and trusted immediately, NS Proxy will continue to use existing Root CA for SSL interception until tunnel is restarted. When tunnel is restarted, NS Client will use the new Client certificate and NS Proxy will use the New Netskope CA.

NS Client - Linux, Steering disabled (other access method used)	New Netskope CA must be deployed on devices with the Device Management Solution	By default, NS Proxy will switch immediately to the New Netskope CA while NS Client didn't download and install the New Netskope CA. User will experience errors until NS Client successfully updates the configuration which is every 60 minutes.
NS Client - iOS	New Netskope CA must be deployed on devices with the Device Management Solution	NS Client will deploy and use new Client Certificate, but New Root CA is not automatically deployed. End User will receive errors or connectivity issues in application until the certificate is installed and trusted.
NS Client - Android	New Netskope CA must be deployed on devices with the Device Management Solution	NS Client will deploy and use new Client Certificate, but New Root CA is not automatically deployed. End User will receive errors or connectivity issues in Chrome until the certificate is installed and trusted. Reminder: only Chrome is intercepted on Android
NS Client - ChromeOS	New Netskope CA must be deployed on devices with the Device Management Solution	NS Client will deploy and use new Client Certificate, but New Root CA is not automatically deployed. NS Client will disable SSL interception until Root CA is trusted.
GRE/IPSEC	New Netskope CA must be deployed on devices with the Device Management Solution	User will experience SSL errors.
Proxy Chaining with SSL interception On-Premises	On-Premises proxy must be updated to trust the New Netskope CA	On-Premises proxy may block all requests or end user can receive SSL errors.
Proxy Chaining without SSL interception On-Premises	On-Premises proxy must be updated to trust the New Netskope CA if certificate validation is enabled. New Netskope CA must be deployed on devices with the Device Management Solution	User will experience SSL errors.
Cloud Explicit Proxy + IP Address Allowlist	New Netskope CA must be deployed on devices with the Device Management Solution.	User will experience SSL errors.
Cloud Explicit Proxy + Unknown IP (Remote Users)	No action required, Root CA (Remote Users) is unchanged.	No impact, Root CA (Remote Users) is still valid
DPOP - Custom CA	No action required	No impact, the Netskope CA is not used
DPOP - Netskope CA	DPOP should be reconfigured to use a Customer managed CA, please refer to "DPOP Interception Certificate Best Practices". The New Customer Managed CA must be deployed on devices with the Device Management	DPOP will download an use the New Netskope CA to perform SSL interception, which will generate SSL errors on end user devices.

	Solution. Alternative: If a Netskope CA is still used for rotation, the New Netskope CA must be deployed on devices with the Device Management Solution.	⚠ Please note the SSL policy based selection on Root CA is not supported on DPOP, DPOP will always use the active default certificate.

The New Netskope CA can be downloaded from Settings > Manage > Certificates > Signing CA.



NS Client for CASB/SWG/CFW/NPA steering

NS Client should be on one of the supported versions mentioned below

- 114.1
- 117.1
- 120 and above

Recommended version: 120

NPA Publishers

To allow Netskope to perform NPA certificate rotation, NPA Publishers must be version 112 and above.

IDP Authentication

The global rotation switch doesn't affect IDP Authentication configuration automatically.

IDP Authentication will be rotated only at the end of Stage 2, there is no required preparation at this step.

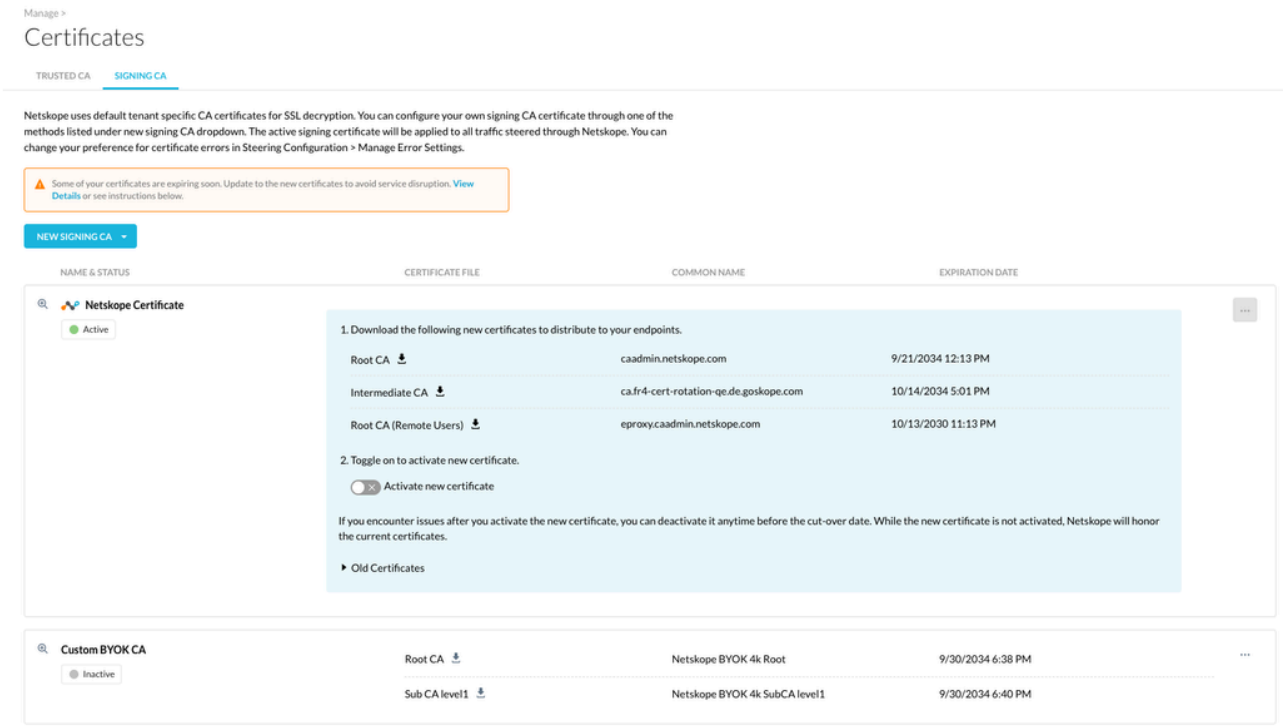
Stage 1.3 - Partial activation for SSL Interception

After deploying manually the New Netskope CA on some devices, we recommend to test it by enabling it with an SSL decryption policy at this step.

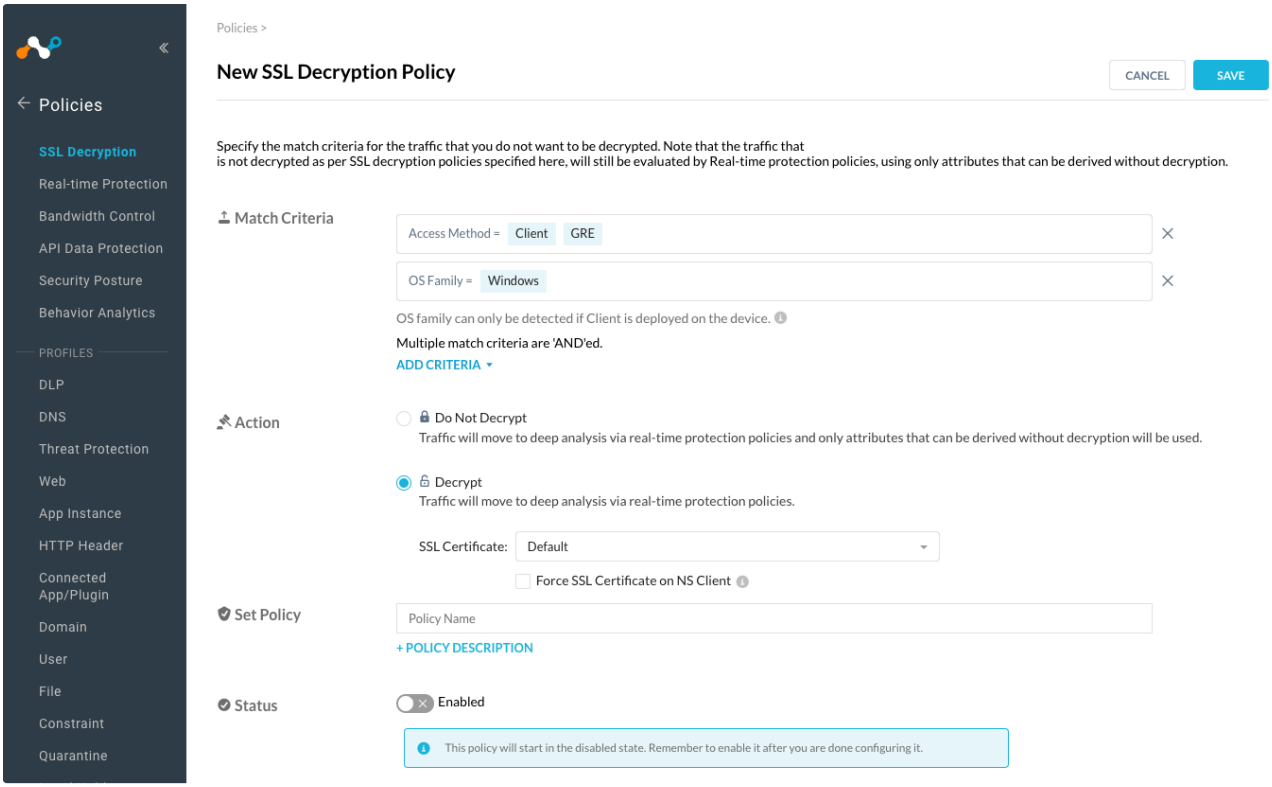
Check enabled features on the tenant before rotation

Please check the following features are enabled to help with the rotation

- Rotation is enabled: “Activate new certificate” checkbox is available in Settings > Manage > Certificates > Signing CA:



- in Policies > SSL Decryption > New Policy:
  - Match Criteria in SSL Decryption policies allows you to choose “Access Method” and “OS Family” as a criteria
  - When “Decrypt” action is selected, a drop down to select Default, New and Old Netskope certificate shows up.



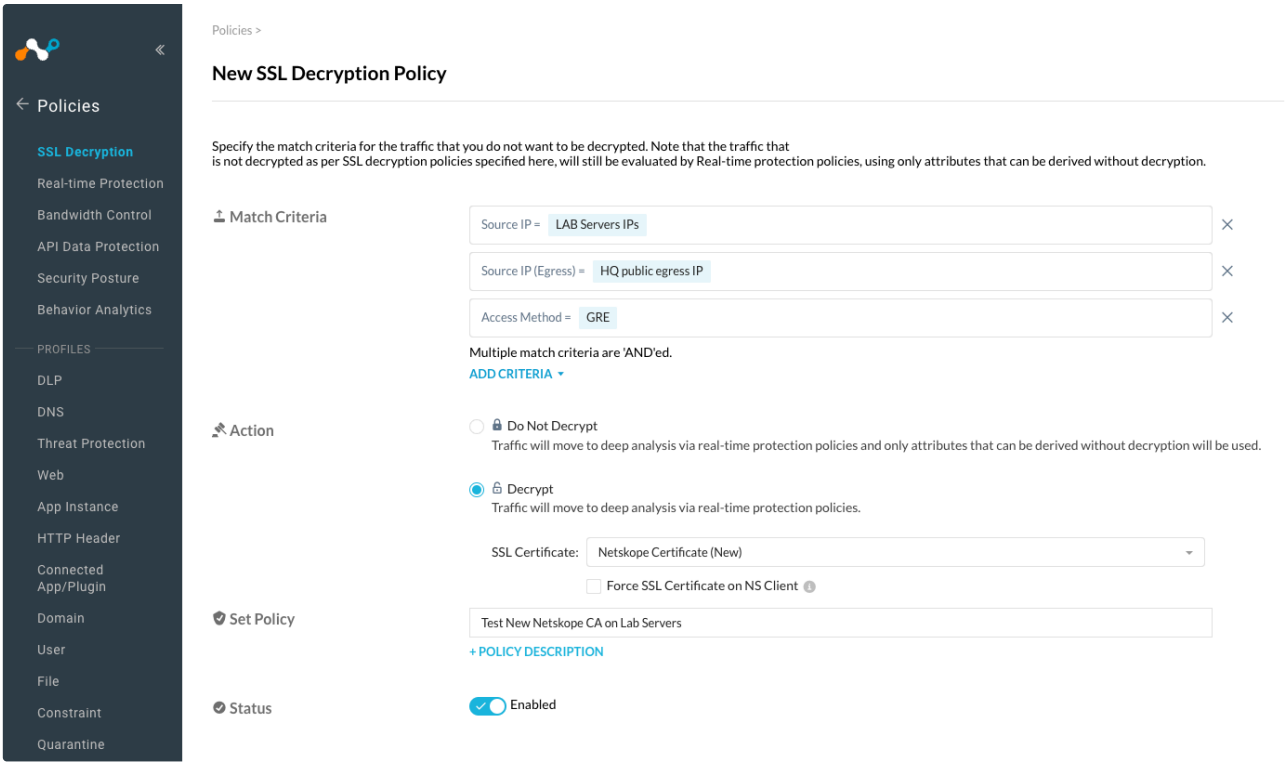
If you are missing one of the features in your tenant, please contact Netskope to enable them.

Enable New Netskope CA for some devices with SSL Decryption policies

To change the CA used for SSL interception, create a new policy in Policies > SSL Decryption with matching criteria.

Only use certificates that are deployed on the device. The policy will not affect which CA is deployed by NS Client.

In the following example, the New Netskope CA is used for Lab Servers source IP with GRE access method:



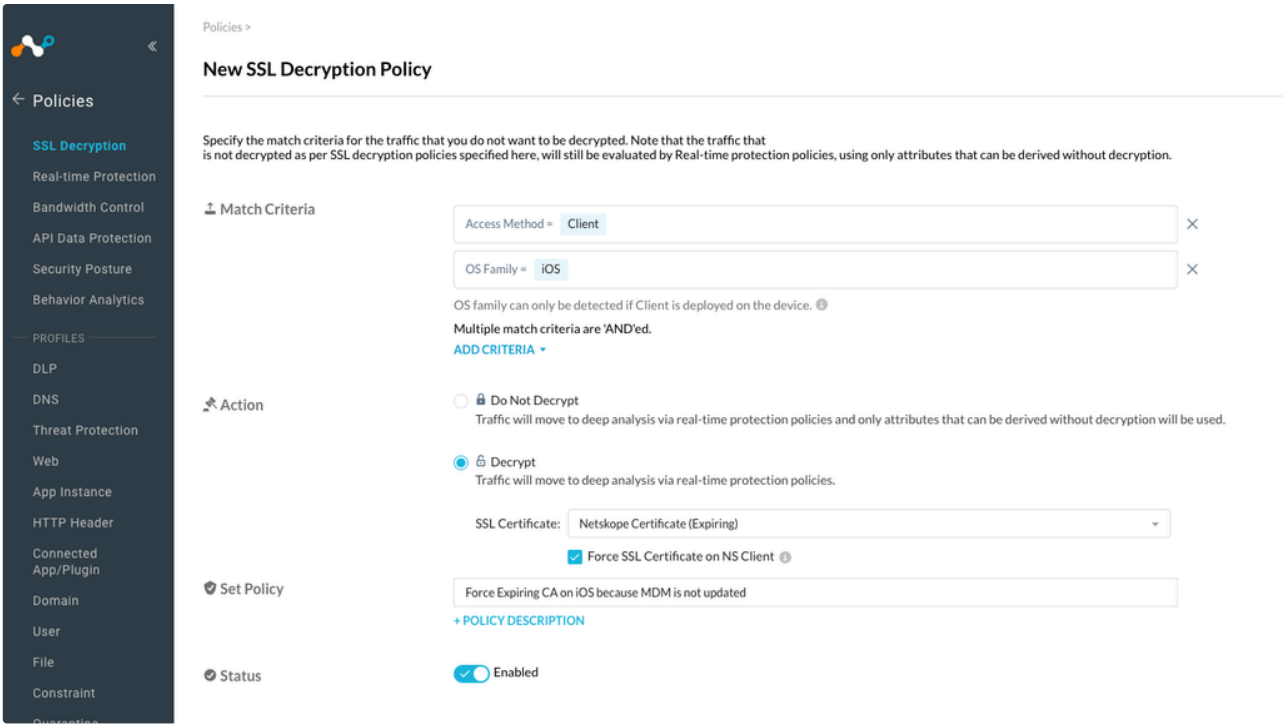
Policy ordering is important, please make sure the policy will be matched and it doesn't shadow Do Not Decrypt exceptions.

By default, NS Proxy will select the same Root CA used by NS Client to establish the SSL tunnel. The option "Force SSL Certificate on NS Client" ignores this automatic selection and forces the selected Netskope CA for connections from NS Client. In step 1.3, since the default CA is the Expiring CA, the force option must be checked for the policy to be effective on NS Client protected devices. Otherwise, NS Proxy will continue to use the default certificate.

Please note the SSL policy based selection on Root CA is not supported on DPOP, DPOP will always use the active default certificate.

Forcing Expiring Netskope CA for some devices with SSL Decryption policies

If some devices requires or network require more time to update, you can exclude them using SSL policies before global rotation. In the following example, the Expiring Netskope CA is used on iOS devices because the New Netskope CA is not trusted yet:



Please note the SSL policy based selection on Root CA is not supported on DPOP, DPOP will always use the active default certificate.

Stage 2.1 - Activating the New Netskope CA

This step is initiating the main rotation process:

- Default SSL interception CA will switch the New Netskope CA (NS Client auto selection and SSL Decryption policies can override which CA is used)
- NS Client will start to update and deploy New Netskope CA and Client Certificates (for CASB/SWG/CFW and NPA)
- Additional rotation switches will appear for each authentication feature to allow rotation of the Expiring SAML certificate. Certificates used for authentication related features are not automatically switched to the new certificate.

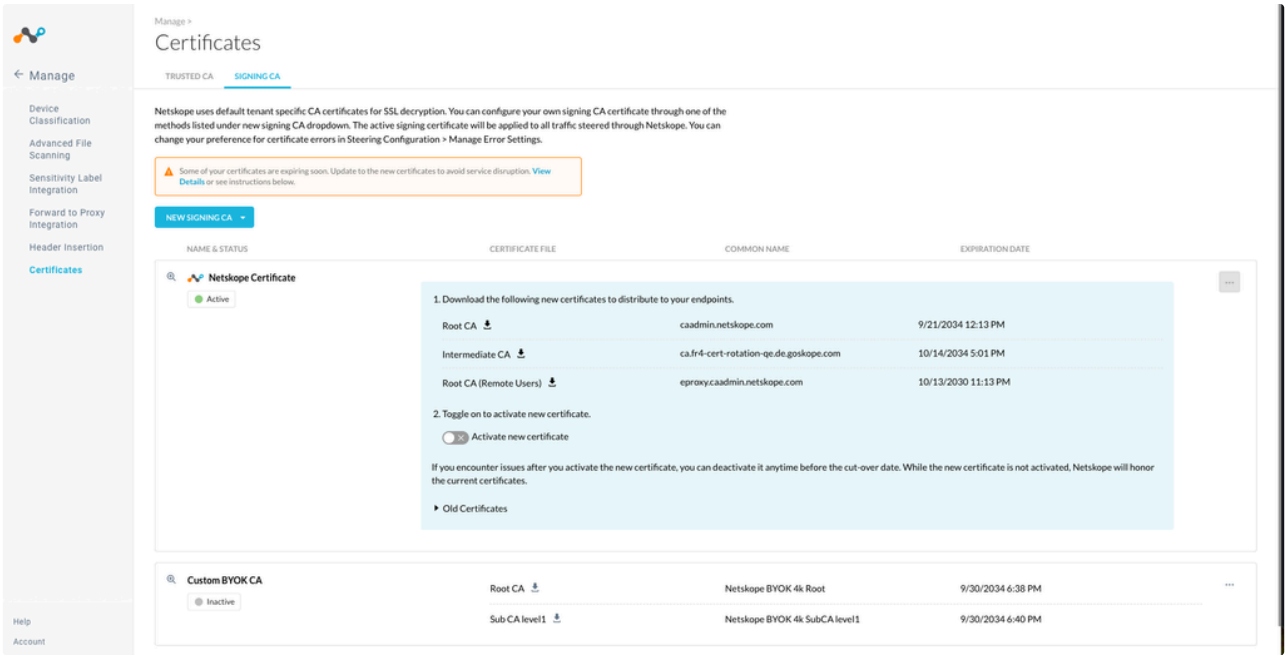
Admin can revert the rotation back with the same switch, in this case the reverse process will happen.

Global rotation setting

To begin the rotation process, go to **Settings** > **Manage** > **Certificates** and click the **Signing CA** tab.

On the **Signing CA** page, use “Activate new certificate” toggle:

Please note that even if Netskope CA is not active (if BYOK or On Prem HSM are active), this step needs to be performed for the NS Client to receive the new user certificates.

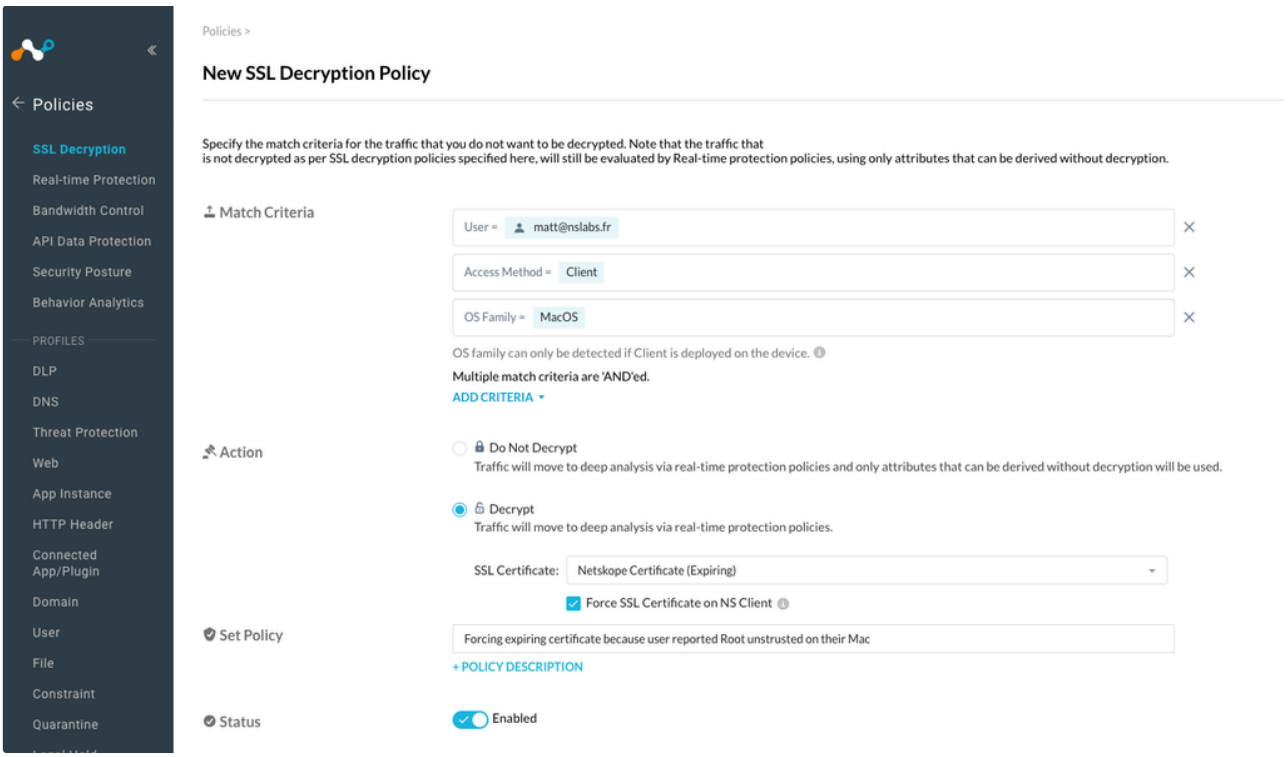


Mitigation of issues for SSL interception

If some users are reporting issues on their devices related to SSL interception (untrusted Root), we recommend to add an exception in the SSL Decryption policy instead of reverting the full rotation.

> Reminder: NS Proxy use the same Netskope CA that NS Client used to establish the tunnel by default, “Force SSL Certificate on NS Client” must be checked to be able to force the Netskope CA to NS Client access method.

In the following example, the Expiring Netskope CA is used for a single user on MacOS devices:



> Please note the SSL policy based selection on Root CA is not supported on DPOP, DPOP will always use the active default certificate.

If too many devices are impacted, the fastest solution is to revert the full rotation (deactivate the new certificate in Signing CA configuration).

Auto rotation of NS Client for CASB/SWG/CFW steering

NS Client downloads update every 60 minutes by default and will receive the New Netskope CA and new Client certificates.

> **Even in case where the Netskope CA is not active (BYOK or On Prem HSM), the NS Client will receive the new Client certificates to establish the outer tunnel with the NS Gateway**

New Netskope CA will be installed and trusted immediately after New Netskope CA is activated, NS Proxy will continue to use existing Root CA for SSL interception until tunnel is restarted.

When tunnel is restarted, NS Client will use the new Client certificate and NS Proxy will use the New Netskope CA.

In case of rollback, NS Client will follow the same process to update Root and Client certificates.

> There is no action required, the rotation for NS Client tunnel is fully automated

Rotation of NPA (NPA Publishers and NS Client NPA Steering)

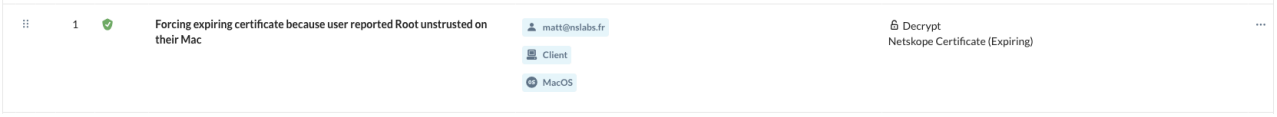
Rotation for NPA for both Publisher and NS Client will be done by Netskope in the backend. No outage is expected during the rotation process.

If you have Netskope Publishers version 112 or higher, No action is required. However, in a rare case, where there are issues updating the certificate, the Netskope team will contact you to perform two system reboots - one to retrieve the certificate and another to activate it.

Stage 2.2 - Complete deployment for SSL interception

Once New Netskope CA is active by default and default SSL interception is working without incident, the last step is to complete rotation for all devices that are still using the Expiring Netskope CA in the SSL Decryption policy.

Check the SSL Decryption policies that are configured with “Netskope Certificate (Expiring)”, for example:



Work with relevant teams to complete the deployment of the New Netskope CA and switch the policy to “Default” or “Netskope Certificate (New)”.

Stage 2.3 - IDP Authentication

Once Stage 2.2 is completed, rotation of IDP authentication can be performed. You can use the migration modal in the Netskope admin console to identify all SAML configurations that require rotation of certificate and get directed to the relevant configuration to perform rotation. The migration of SAML certificates is blocked until SSL certificate rotation is completed.

To identify which configuration is pending migration, please open the details on the Rotation warning. If the customer is using IdP based User Authentication for SD-WAN Client, although not mentioned in the migration modal, additional steps will be required

4	ca.fr4-cert-rotation-qe.de.goskope.com	Administration SSO	Migration Required Dependent of Intermediate CA View Migration Instructions
5	ca.fr4-cert-rotation-qe.de.goskope.com	Netskope Client - SAML Dropbox	Migration Required Dependent of Intermediate CA View Migration Instructions
6	ca.fr4-cert-rotation-qe.de.goskope.com	Forward Proxy - SAML GRE IPsec SAML	Migration Required Dependent of Intermediate CA View Migration Instructions
7	ca.fr4-cert-rotation-qe.de.goskope.com	Reverse Proxy - SAML Demo Box	Migration Required Dependent of Intermediate CA View Migration Instructions

While IDP authentication rotation can be done immediately after the global activation, if admin is rolling back the global rotation process, all authentication features will also stop using the New SAML Certificate. That's why we recommend to wait SSL interception rotation to be complete or near complete before starting stage 2.3

Expiration of the Expiring Netskope CA doesn't impact authentication in most cases, only the expiration of the Expiring SAML Certificate will impact authentication. Although, there will be no production impact until this date is reached, however we strongly request customers to enable the new certificate to complete the rotation process. We will eventually deprecate and revoke the entire chain thereby making SAML certificates invalid.

Requirements

For Admin SSO and Forward Proxy SAML configurations, Netskope only act as an SP (Service Provider). The IDP will generally only check the SP certificate for Single LogOut (SLO) request. However, if the Expiring SAML Certificate was imported in the IDP, then the New SAML Certificate must be updated on the IDP side.

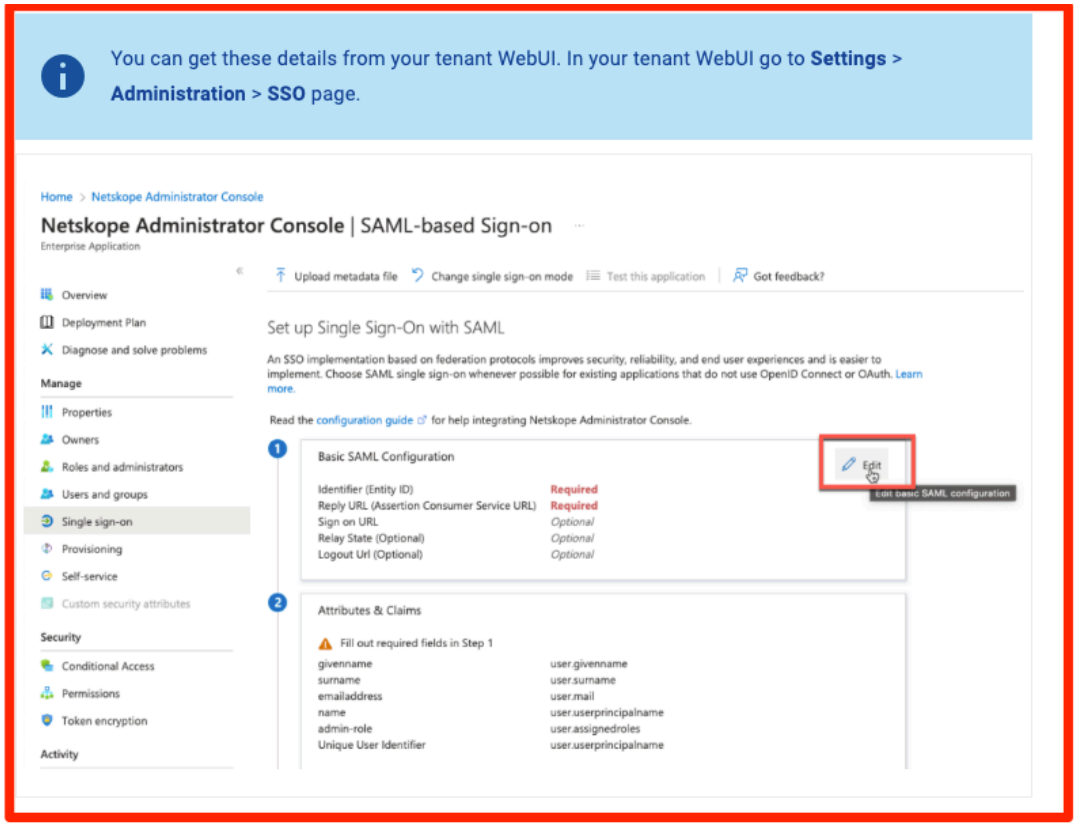
Please review the Netskope help topics below to configure IDP configurations (as examples)

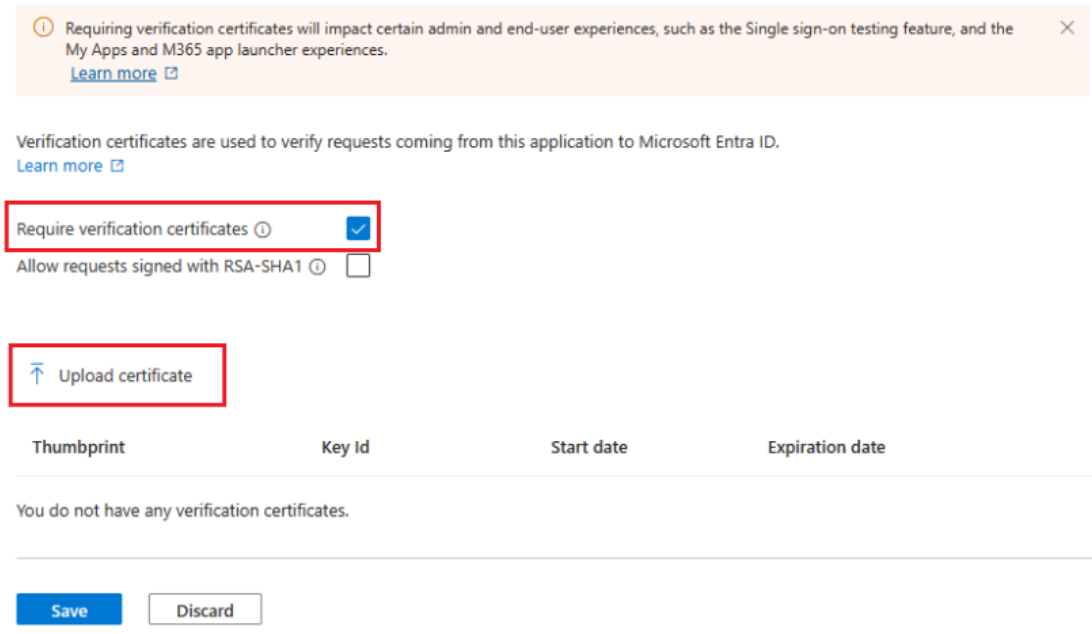
Single Sign On (SSO) to Netskope tenant with Microsoft Entra ID

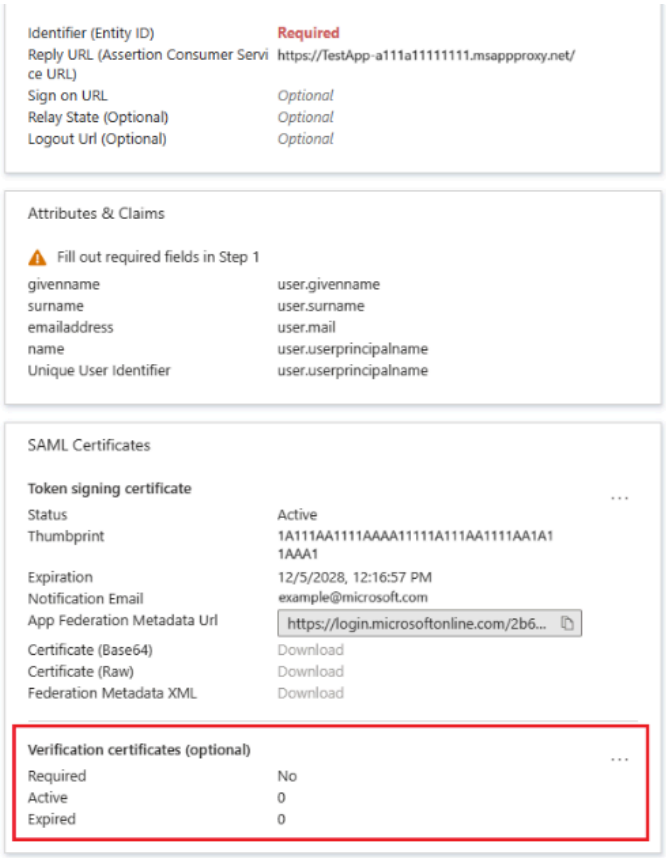
SAML Authentication with Okta

SAML Authentication with Microsoft Entra ID

As a example, for Microsoft Entra ID, if the "Signed SAML authentication requests" is enforced, the new SAML certificate must be uploaded on the IDP before the certificate on the configuration is rotated.


You can get these details from your tenant WebUI. In your tenant WebUI go to **Settings** > **Administration** > **SSO** page.
Home > Netskope Administrator Console
Netskope Administrator Console | 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
Security
Conditional Access
Permissions
Token encryption
Activity
Set up Single Sign-On with SAML
An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.
Read the configuration guide for help integrating Netskope Administrator Console.
1
Basic SAML Configuration
Edit
Edit basic SAML configuration
Identifier (Entity ID) Required
Reply URL (Assertion Consumer Service URL) Required
Sign on URL Optional
Relay State (Optional) Optional
Logout Url (Optional) Optional
2
Attributes & Claims
Fill out required fields in Step 1
givenname user.givenname
surname user.surname
emailaddress user.mail
name user.userprincipalname
admin-role user.assignedroles
Unique User Identifier user.userprincipalname


Requiring verification certificates will impact certain admin and end-user experiences, such as the Single sign-on testing feature, and the My Apps and M365 app launcher experiences.
Learn more
Verification certificates are used to verify requests coming from this application to Microsoft Entra ID.
Learn more
Require verification certificates
Allow requests signed with RSA-SHA1
Upload certificate
Thumbprint
Key Id
Start date
Expiration date
You do not have any verification certificates.
Save
Discard



For other configurations (SAML for Client, Reverse Proxy), Netskope act as a SAML (or WS-FED) proxy, and the protected application must trust the New SAML Certificate to accept the authentication. If the certificate was imported on the IDP, then the New SAML Certificate must be updated on the IDP side as well.

Please review the Netskope help topics below to configure Reverse proxy for different applications and IDPs

SAML Proxy - Netskope Knowledge Portal

FOR BWAN Customers ONLY

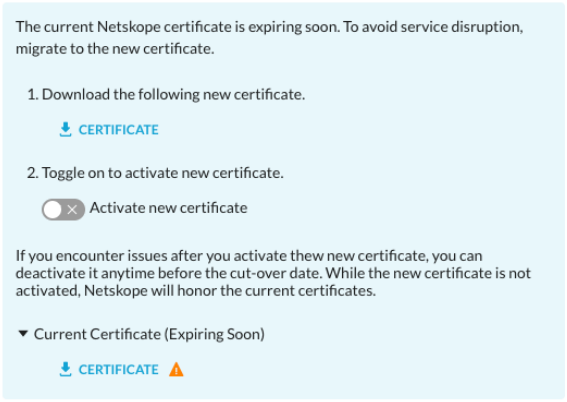
If the customer is using IdP based User Authentication for SD-WAN Client, although not mentioned in the migration modal, additional steps will be required. The new SAML Forward proxy certificate must be uploaded to the BWAN Orchestrator. Details can be found here - BWAN IdP based User Authentication

Activation

Please make sure you use a local login when updating SAML for admin authentication, otherwise you may loose access of the management console. If you cannot access the management console, please contact Netskope Support.

For each active configuration identified in the assessment step:

- identify the team managing the IDP and SaaS app configuration
- identify changes to apply on all sides
- download the New SAML Certificate and share it with relevant teams
- validate authentication is working
- activate the New SAML Certificate on Netskope console and trust it on the other sides at the same time



- validate authentication is still working

Rollback

Restore the previous configurations on all sides to rollback.

Stage 3 - Ending rotation

Once all configuration is migrated, please monitor all services for few days or weeks.

Netskope is tracking rotation of certificates performed by customer admins. Once migration is complete, we will move your tenant to Stage 3 after validation and delete the Expiring Netskope CA.

FAQ

Do we need to deploy Intermediate CA?

Deploying Root CA is enough for the SSL interception, deploying Intermediate CA is optional.

The deadline to rotate on the tenant is too short, can I request extention?

FR4 expiration is 21st of March 2025, if rotation is not performed before that date, the service will stop working.

Can I deploy new devices during rotation

Yes, new devices can be added during rotation process. Be aware that policy based CA policies can impact new devices if “Force SSL Certificate on NS Client” enabled.

The SAML Certificate signed by the Expiring Root CA is still valid for several years, do I still need to rotate it?

Yes, all certificates must be rotated, even if expiration if far away. When the Expiring Root CA will be deleted, the old SAML Cert will be deleted as well.

Why the device is showing untrusted certificate error after configuring SSL decryption policy with the New Root CA. Why is NS Client not deploying automatically the New Root CA?

The SSL decryption policy doesn’t affect which Root CA is deployed by NS Client, NS Client will only deploy automatically the New Root CA once activated in Signing CA page.
Root CA must be deployed manually of with the Device Management Solution before enabling it with an SSL decryption policy .

Do we need to perform rotation when using custom CA to perform SSL Interception (BYOK or OnPrem HSM)?

Yes, Netskope CA rotation is mandatory for all tenants. However, if BYOK/OnPrem HSM is deployed, the rotation has less dependencies and the impact is smaller.

Do we need to perform rotation when no SSL interception is performed (or proxy is not deployed)?

Yes, Netskope CA rotation is mandatory for all tenants. However, if SSL interception/Proxy is not used, the rotation has less dependencies and the impact is smaller.