Netskope CA Rotation Guide

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 AM2 MP expires in August 2024 and needs to be replaced.

A new AM2 Netskope CA is available for installation. Please start the migration when the message is prompted on the management console login, we request customers to complete rotation within 90 days.

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.

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 (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 (Final): 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

The first 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.

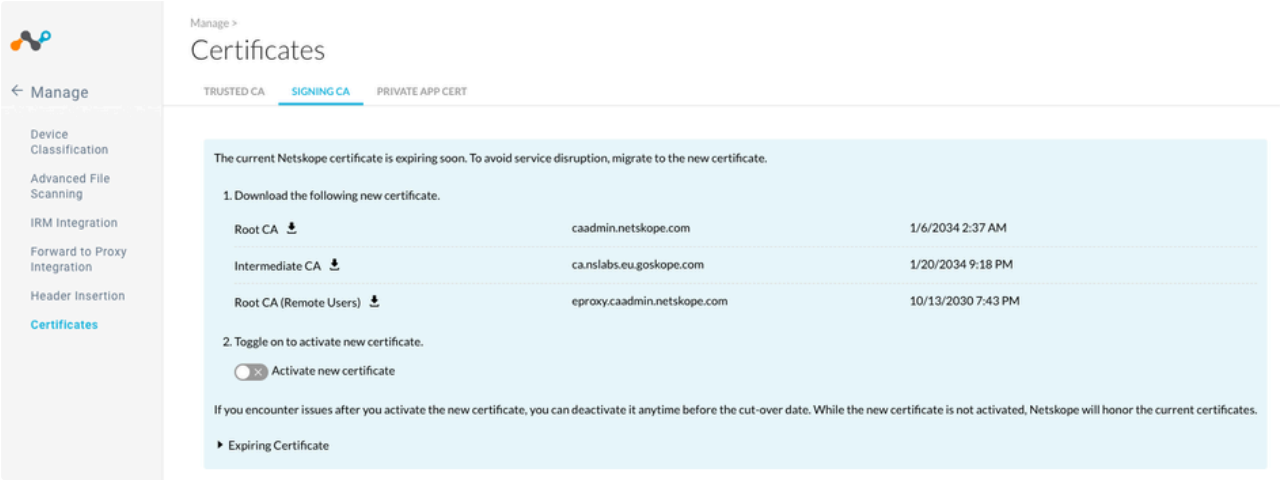
4 different areas are concerned, please identify which one is used in your tenant (refer to sub section if needed)

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 steering		To check if NS Client is used, please go to Settings > Secure Cloud Platform > Devices
NPA (NS Client and 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.

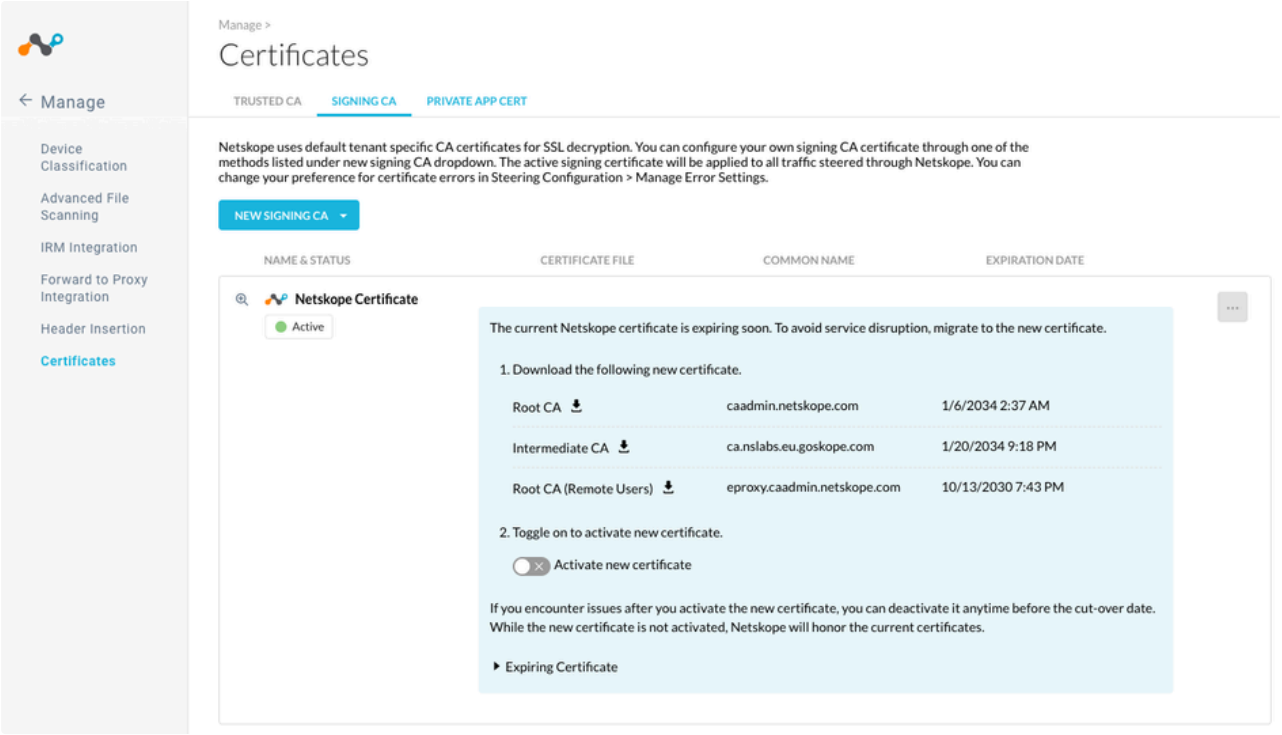
Assessment for Cloud SSL interception

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 bellow Netskope Certificate



If Netskope CA is not active (if BYOK or On Prem HSM are active), Root rotation has no impact on SSL interception and this section can be ignored.

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

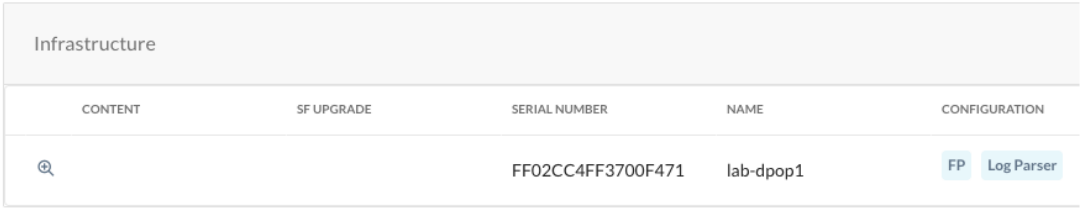
Access method deployed	Deployed (Yes/No)	Comments
NS Client - Windows, Steering active		
NS Client - Windows, Steering disabled (other access method used)		
NS Client - Windows Servers, Steering active		
NS Client - Windows Servers, Steering disabled (other access method used)		
NS Client - MacOS		
NS 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 IDP Authentication

Configuration	Actual settings	Comment
SAML for admin authentication		Check in Settings > Administration > SSO Netskope act as SP only for this feature.
SAML for forward proxy		Check in Settings > Secure Cloud Platform > Forward Proxy > SAML This setting applies to the following features: • SAML authentication for GRE and IPSEC • SAML authentication for Cloud Explicit Proxy

		• IDP enrollment for NS Client • NPA periodic authentication with NS Client Netskope act as SP only for those features.
SAML for Client deployment		Check in Settings > Secure Cloud Platform > Netskope Client > SAML This setting applies to NS Client deployment enforced at the SaaS application authentication step. Netskope act as IDP and SP only for this feature.
Reverse Proxy SAML		Check Settings > Secure Cloud Platform > Reverse Proxy > SAML Netskope act as IDP and SP only for this feature.
Reverse Proxy Auth Proxy (WS-FED protocol)		Check Settings > Secure Cloud Platform > Reverse Proxy > Office 365 Auth Netskope act as IDP and SP only for this feature.

The SAML Certificate is generated when the tenant is created, with a 10 years validity.

There will be no production impact until this date is reached, but we request customers to enable the new certificate at the end of the rotation process.

If one of the configuration is enabled, please download the Expiring SAML Certificate and check the end of validity.

Stage 1.2 - Preparing devices

This step is intended to define:

- If 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	Minimum version R111 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.
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	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 tunnel will not establish until user accept to trust the New Netskope CA.
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.
NS Client - Linux	Minimum version R113 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 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 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 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	New Netskope CA must be deployed on devices with the Device Management Solution. 	User will experience SSL errors.

	Please note “Root CA (Remote Users)” is unchanged.	
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 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.	DPOP will download an use the New Netskope CA to perform SSL interception, which will generate SSL errors on end user devices. 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 steering

NS Client should be in version 111 or above.

NPA

NS Client must be in version 111 or above to perform automatic rotation.

Publisher must be in version 111 or above to perform automatic rotation.

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.

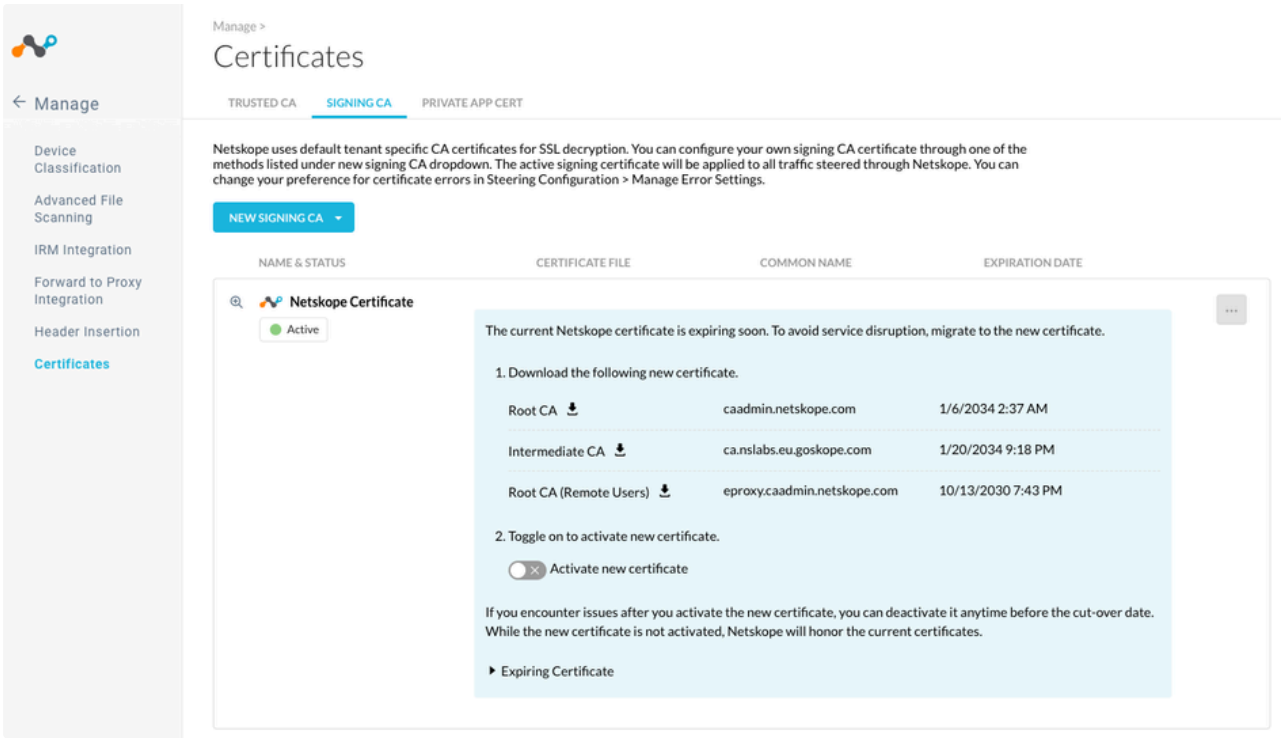
Stage 1.3 - Partial activation for SSL Interception

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

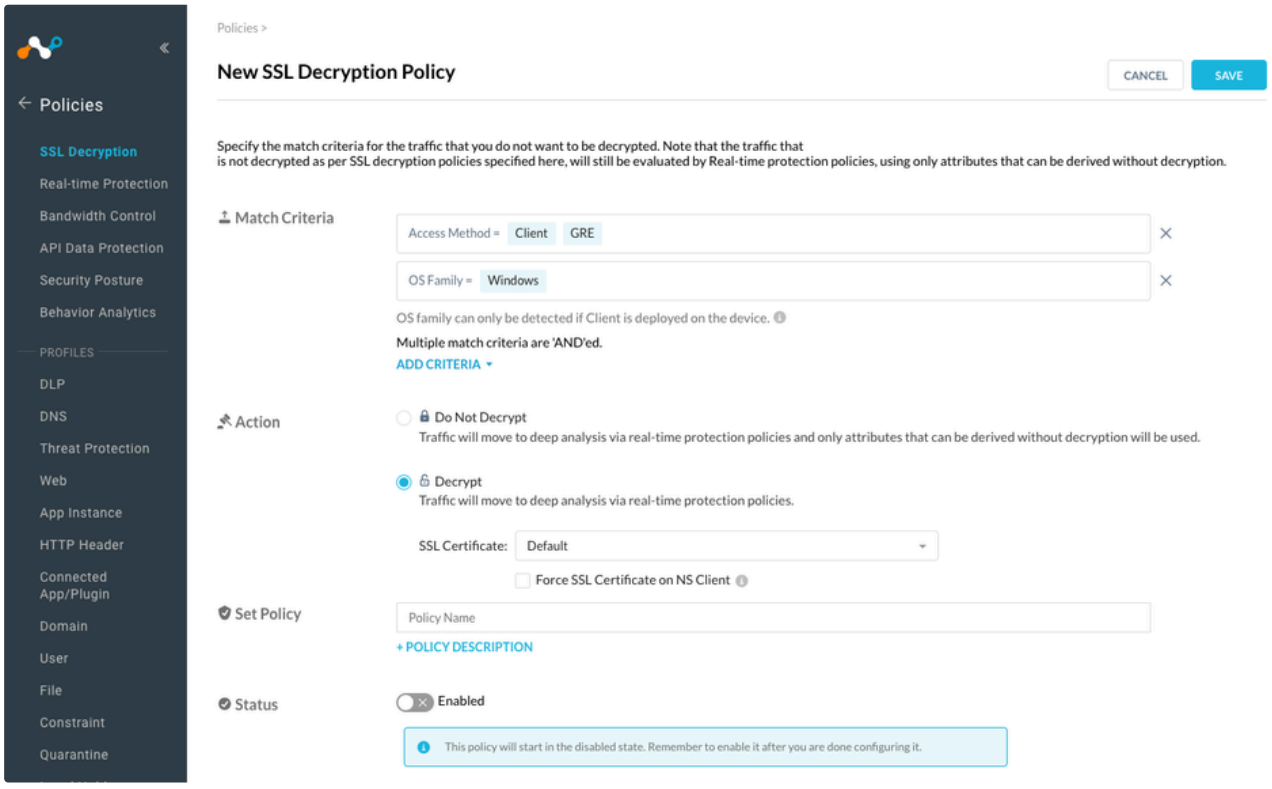
Check enabled features on the tenant before rotation

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

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



- in Policies > SSL Decryption > New Policy:
  - “Allow to Differentiate SSL Decryption Policy per OS/Access Method” adds “Access Method” and “OS Family” criteria.
  - “Support multiple hierarchies for SSL interception” brings a new dropdown to select SSL certificate under Decrypt action:



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

Automatic Netskope CA selection with NS Client

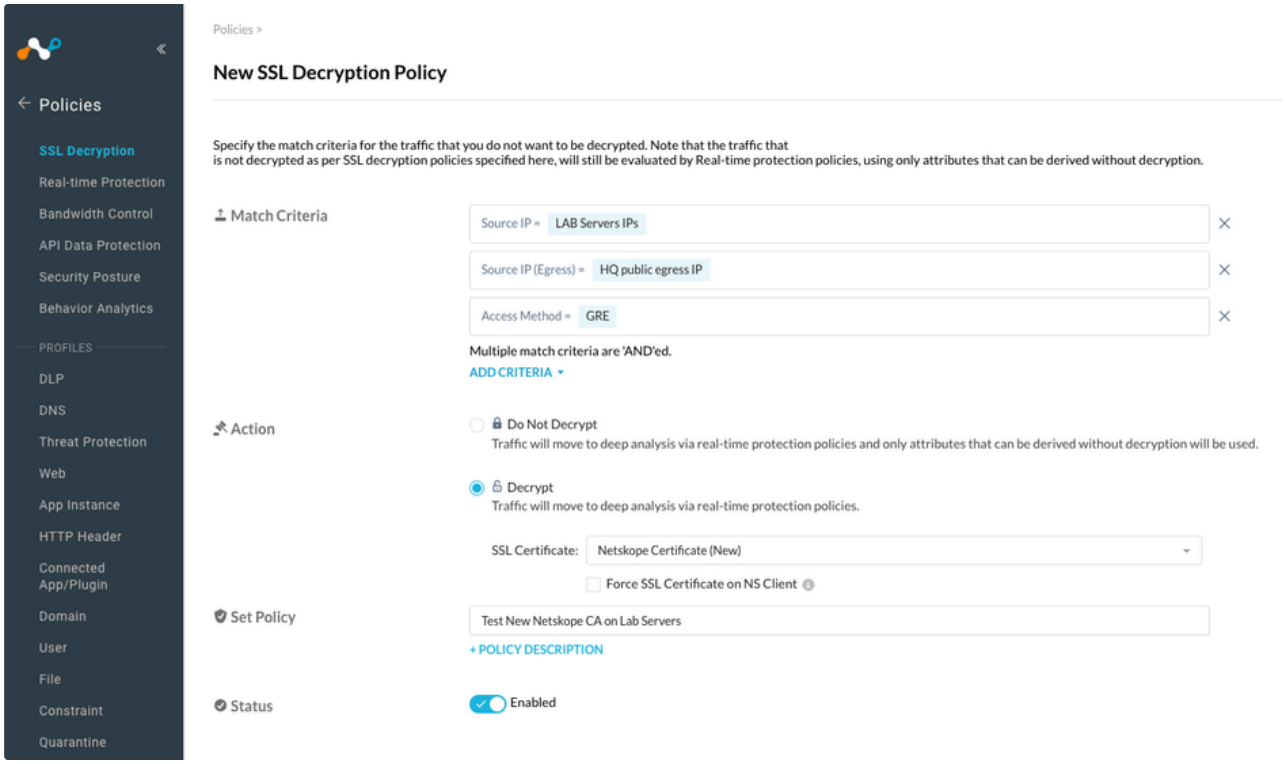
By default, NS Proxy will select the same Root CA used by NS Client to establish the SSL tunnel. The option “Force SSL Certificate on NS Client” allows to ignore this automatic selection and apply the selected Netskope CA to NS Client protected devices.

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.

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.

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.

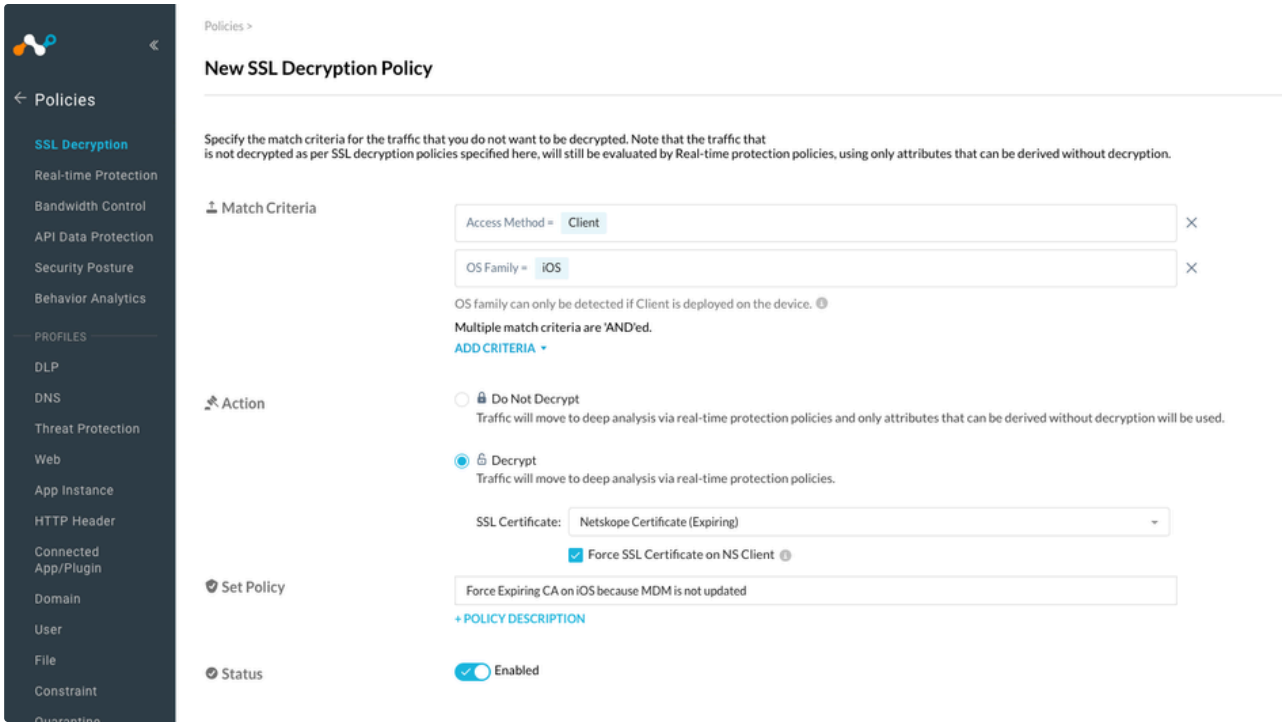
in R113 the policy has a known issue: if you edit an existing policy and switch from “Do Not Decrypt” to “Decrypt” action, the SSL certificate is not displayed. To workaround this issue, save the policy (without apply) and edit the policy again. This issue will be fixed in R114.

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 from the global rotation.

In the following example, the Expiring Netskope CA is used on iOS devices because the New Netskope CA is not trusted yet:



in R113 the policy has a known issue: if you edit an existing policy and switch from “Do Not Decrypt” to “Decrypt” action, the SSL certificate is not displayed. To workaround this issue, save the policy (without apply) and edit the policy again. This issue will be fixed in R114.

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:

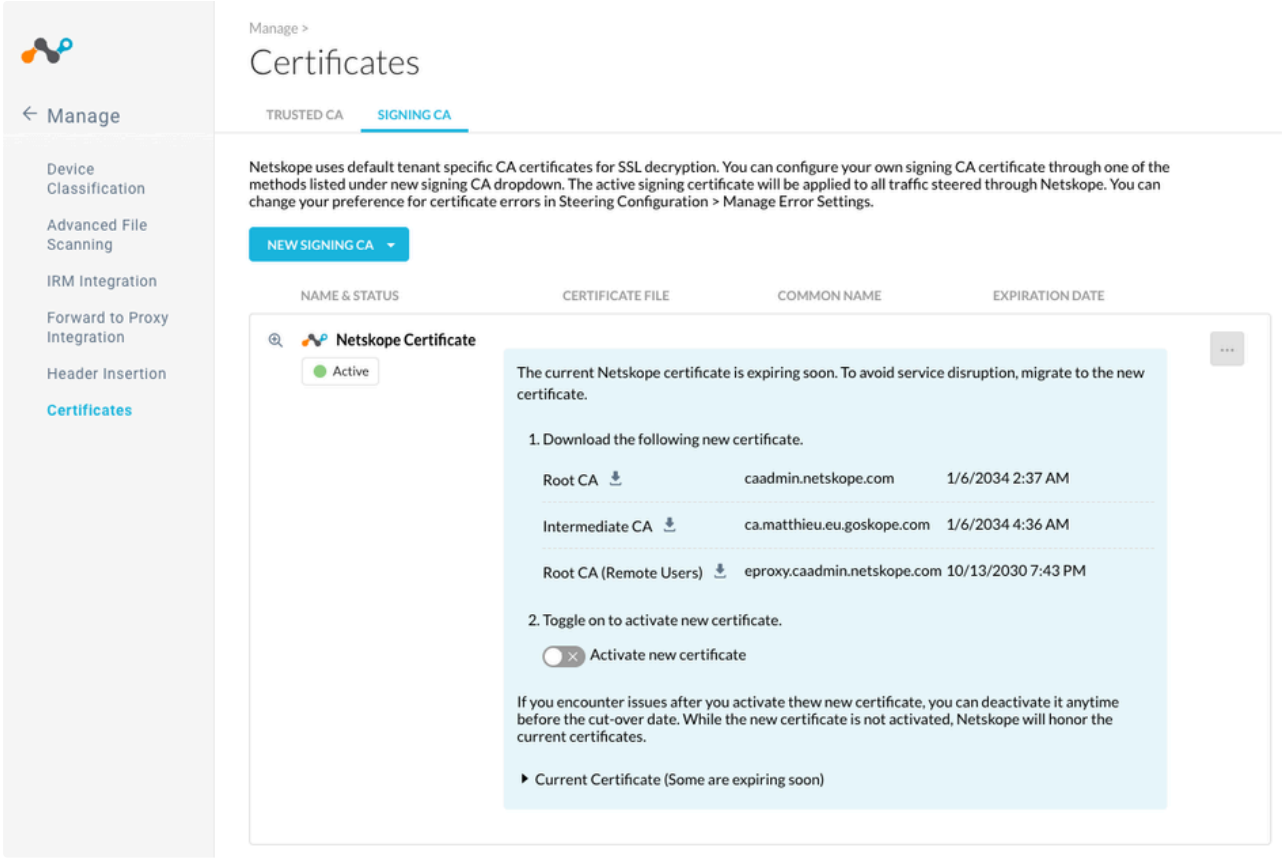
- Default SSL interception CA will switch the New Netskope CA (NS Client auto selection and SSL Decryption policies can override which CA is used)
- NS Client will start to update and deploy New Netskope CA and Client Certificates (for CASB/SWG/CFW and NPA)
- NPA Publishers will start migrating to New Netskope CA
- 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:

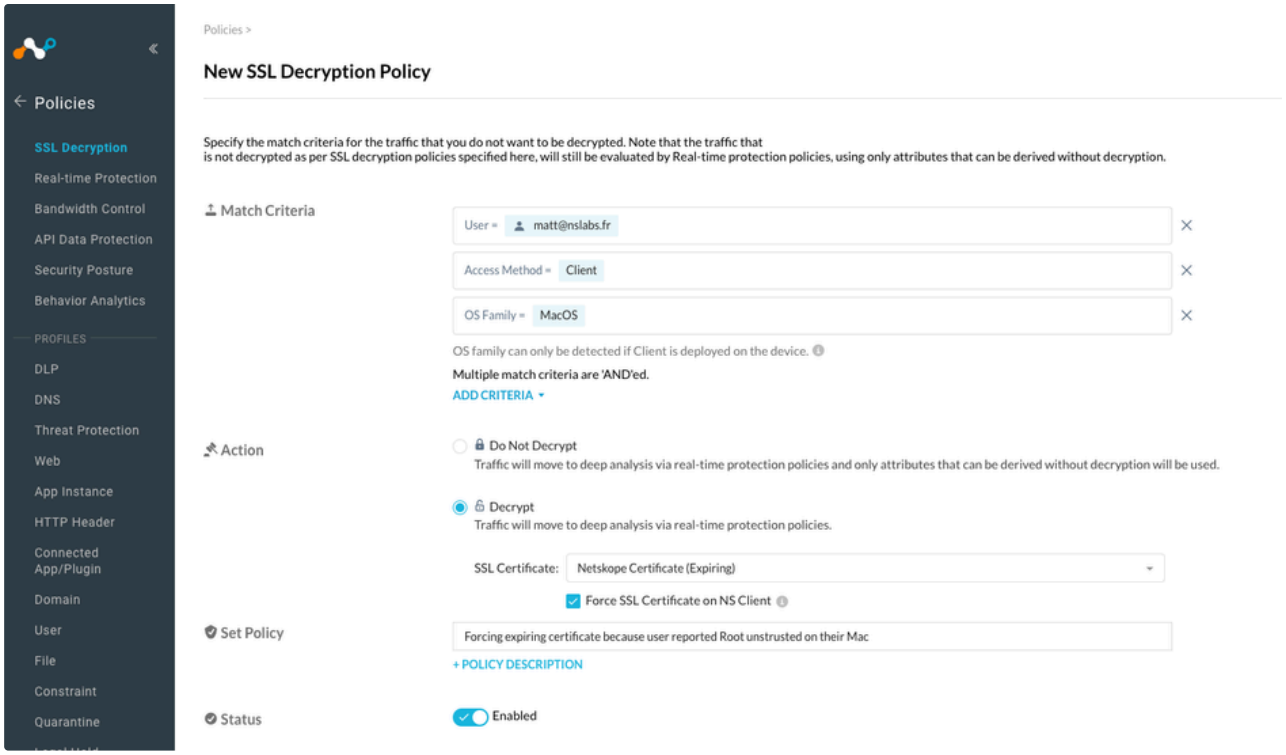


Mitigation of issues for SSL interception

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:



in R113 the policy has a known issue: if you edit an existing policy and switch from “Do Not Decrypt” to “Decrypt” action, the SSL certificate is not displayed. To workaround this issue, save the policy (without apply) and edit the policy again. This issue will be fixed in R114.

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 (deacticate the new certificat 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.

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.

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

Auto rotation of NPA (NS Client and Publishers)

In all cases, no outage is expected in the rotation process, NPA will continue use the Expiring Netskope CA until Publisher and NS Client update their certificate.

When NS Client and Publisher (version 111 and above) connect to NewEdge, they will receive new Certificates to use to establish tunnels.

With version 111, there is no action required, the rotation for NPA is fully automated

Old version will continue to connect with existing certificate until the Expiring Netskope CA expires.

If the NS Client version is bellow R111, no automatic rotation applies, to perform rotation there are two options:

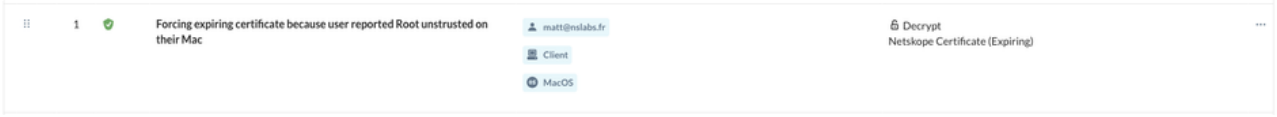
- upgrade NS Client, rotation will be done automatically
- manual re enrollment of the device will deploy the new client certificate on the old version

In case of rollback, the same process it used to revert.

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.

> ⚠ 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.

Each settings has a different activation switch to simplify activation and rollback.

Requirements

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

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.

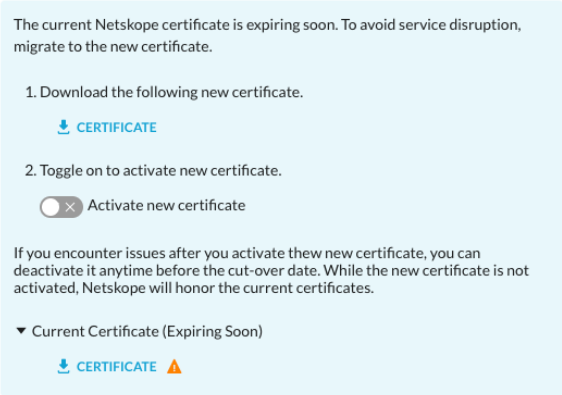
Activation

> ⚠ 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.

Please contact Netskope to notify us that you completed rotation, 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?

AM2 expiration is 9th of August 2024, if rotation is not performed before that date, the service will stop working. Deadline of the countdown can be extended on demand.

What happen after warning date on the tenant

There is no service disruption until the exact expiration date. After the warning date, more warning will be displayed on the console.

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.