Netskope Tenant 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). In addition, every tenant has a sub CA called “Tenant CA” issued by the Netskope CA of the MP. The Tenant CA has a 10 year validity and hence, every 10 years, the Tenant CA needs to be rotated.

When the Tenant CA is about to expire, a new Tenant CA is automatically generated and an in-product notification is available for admins to follow certain steps and perform the rotation. 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.

Tenant CA: Sub CA dedicated for the tenant, issued by Netskope CA

Expiring Tenant CA: Tenant CA for a tenant that will expire soon

New Tenant CA: Tenant CA for a tenant that is being provisioned to replace the Expiring Tenant CA

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

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

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

Requirements

For Administration SSO and SAML - Forward Proxy configurations, Netskope only acts 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, otherwise rotation can be performed without changes on the IDP.

For other configurations (SAML - Netskope Client, SAML - Reverse Proxy, Office 365 Auth), 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.

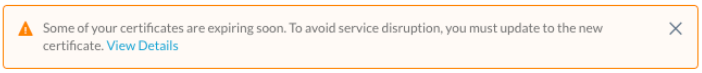
Rotation overview

The rotation is performed with the following steps:

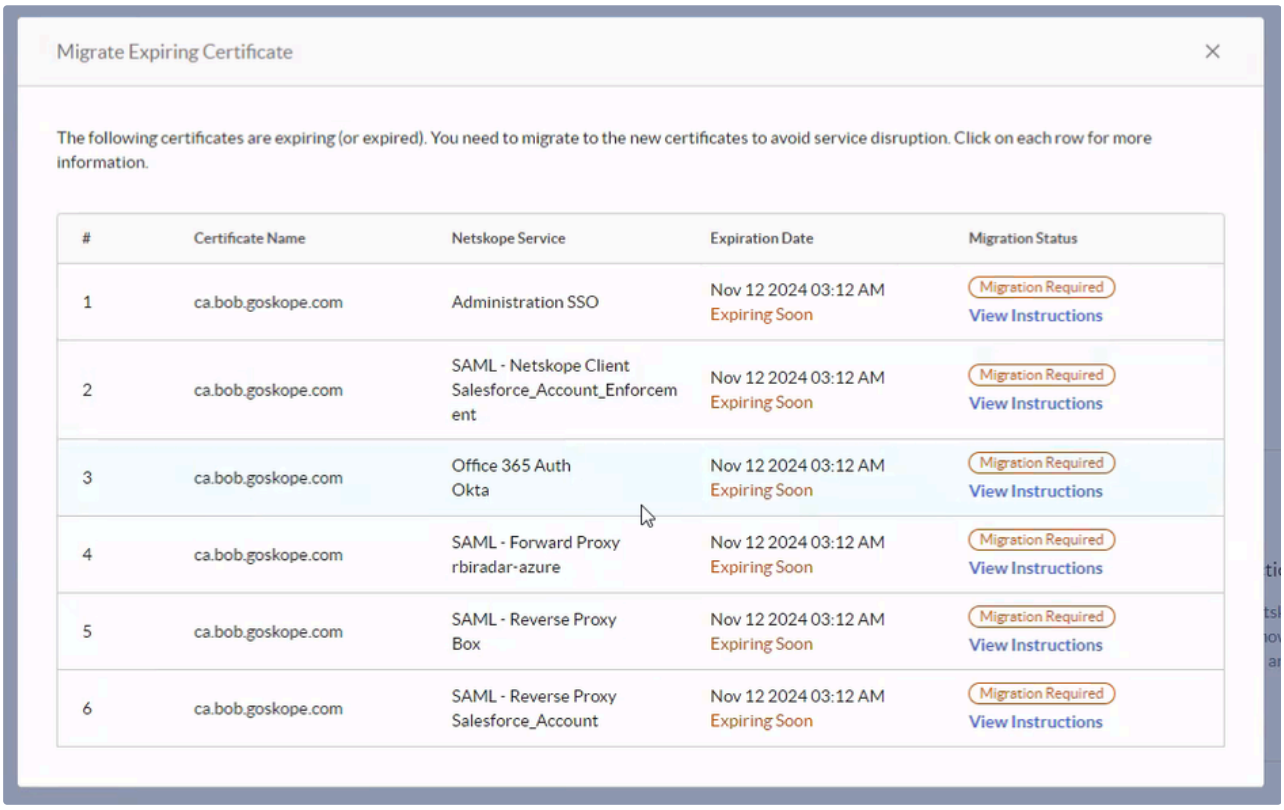
- **Initial phase**: tenant with a single Tenant CA (Expiring Tenant CA) and SAML Certificate (Expiring SAML Certificate) i.e the state before rotation
- **Rotation phase**: tenant has 2 Tenant CA provisioned and New Tenant CA is active. All Netskope services are migrating to the New Tenant CA automatically, including SSL interception, NS Client and NPA internal authentications. Customer admins are rotating manually SAML Certificate one by one. At the end of the rotation, only the New SAML Certificate CA is used for all configurations
- **Final phase**: Expiring Tenant CA is deleted and no longer trusted and available for any service

SAML Certificate rotation

Once rotation is started on your tenant, a warning will be displayed at the top of the home page:



By clicking “View Details”, the list of certificates to rotate is displayed with the expiration date:

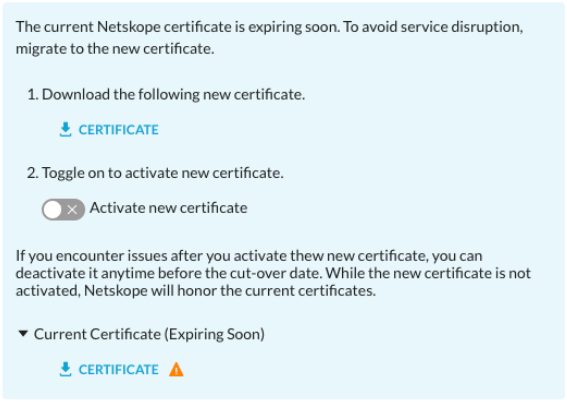


Activation

> ⚠ Please make sure you use a local login when updating SAML for Administration SSO, otherwise you may loose access of the management console. If you lost 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



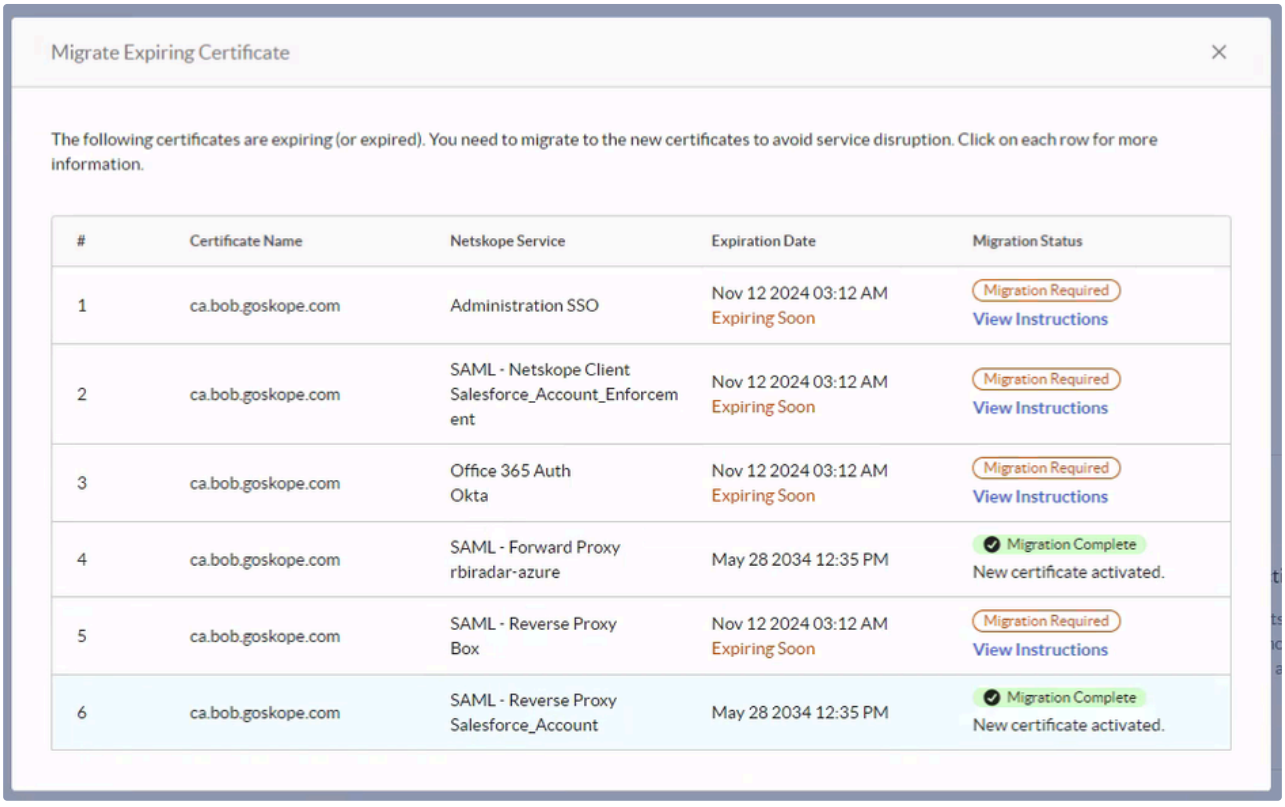
- Validate authentication is still working

Rollback

Restore the previous configurations on all sides to rollback.

Checking remaining certificates to rotate

The list of certificates is updated once rotation is started, please use the link on the home page (or in each related page) to view the remaining settings to rotate:



Ending rotation

Once all configurations are migrated, please monitor all services for few days or weeks.

Please contact Netskope to notify us that you completed rotation, we will delete the Expiring Tenant CA and Expiring SAML Certificate.