okta | netskope

# Comprehensive Access Control and Data Security in Multi-Cloud Environments

## Combine identity management and cloud access security.

Forward-thinking enterprises are stepping up the pace of migrating apps and resources to the cloud. Increasingly, employees want to use their own devices to connect to those resources and access a wide variety of cloud (SaaS) and private applications. In this environment, it's no surprise that credential-based attacks threatening enterprise data are continuing to multiply, presenting a growing challenge for security and IT teams.

Enterprises need a solution for strong identity management that provides visibility into all user activity and can automate policy enforcement for that activity. Okta and Netskope can enable comprehensive enterprise security that doesn't compromise the user experience across multi-cloud environments.

### Enable a modern, flexible workforce experience while keeping enterprise assets and workforce identities safe

Okta's identity solutions integrate with Netskope's Security Service Edge (SSE) to enable granular, end-to-end enterprise security. Your employees get a simple, intuitive login from any device and location to access whatever apps they want to use - private and SaaS apps, sanctioned or unsanctioned. Your IT and security operations teams enjoy total visibility into all user activity - even web browsing and unsanctioned app usage - and can automate and enforce strong access policies from login to logout, including step-up authentication challenges for suspect behavior.

## Integration Use Cases

**Extend MFA step-up authentication.** Leverage rich cloud and web activity, content, and context for policy-driven step-up authentication requests.

**Provision users and groups.** Leverage AD and SCIM to share users and groups between Okta and Netskope.

**Monitor identity of all apps.** Decline and track federated identities across all apps with Okta and Netskope.

**High-risk user enforcements.** Based on Okta and Netskope activity and events, place users into high-risk groups until remediation.

**Integrate across SASE architecture.** Integrate Okta identity services into Netskope Next Gen SWG, CASB, CSPM, and ZTNA solutions.

## How Okta + Netskope work together

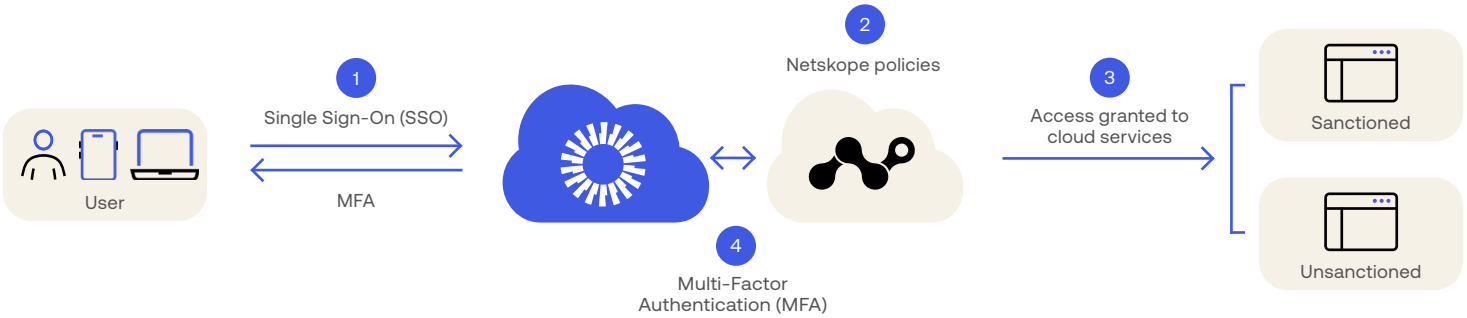
Okta and Netskope integrate to keep enterprise users and data safe throughout day-to-day operations. At login, users authenticate once with Okta Single Sign-On (SSO) and can immediately access enterprise resources, private data centers, or public cloud environments. With Netskope's forward and reverse-proxy architecture, Okta-provisioned identities are similarly bound to each user's post-login activities, including web browsing and interactions with over 50,000+ supported SaaS and private applications.

IT teams can control application access centrally and can automate policies that govern user activity, such as an Okta-provisioned user committing a policy violation like attempting to upload corporate resources to personal instances of cloud drives. Netskope protects enterprise data by identifying and preventing this risky behavior, providing real-time coaching and/or suspending the user's session and/or stepping up authentication via multi-factor authentication to Okta.

## Capabilities

### Step-up authentication based on context for zero trust access

The integration between Netskope and Okta delivers context-aware zero trust access to resources in cloud and private apps. For example, a trusted user accessing a sensitive private application using a sanctioned device can also be granted access to the same resource from a new device, after a successful step-up authentication.



okta | netskope

## Granular visibility to all cloud and web traffic

Netskope Next Gen SWG analyzes six types of user traffic including web, SaaS, Shadow IT, public cloud services, and custom apps in the public cloud. Applying SSO and MFA to only managed apps is missing more than 97% of the target. With identity as the new perimeter, extending Okta with Netskope to all possible apps and cloud services with policy-driven step-up authentication is the security posture you need to protect your data. While managed apps benefit from API and inline analysis, the runaway train of Shadow IT requires inline analysis to decode these cloud apps, a challenge most legacy SWGs cannot address. Integrating Netskope and Okta extends SSO and MFA to thousands of apps with granular controls based on rich context for policy-driven step-up authentication.

## Enable Secure BYOD and third party access

Next Gen SWGs and cloud inline solutions include both forward and reverse proxy capabilities. Integrated with Okta, Netskope reverse proxy supports access to managed apps for unmanaged devices and BYOD where a client or agent is not possible. The same granular policy controls with the ability to invoke step-up authentication are available including data and threat protection. Netskope's Zero Trust Network Access (ZTNA) provides streamlined and secure access to private resources hosted in data centers and public cloud environments. Authenticated users gain direct access only to authorized applications, not the underlying network.

When your workforce uses SSO and MFA, Okta sends their traffic to the Netskope Security Cloud for managed app security policy controls, including step-up authentication based on content and context details. The same leading cloud services that secure thousands of apps with forward proxy for managed devices, also protect unmanaged device access to managed apps with reverse proxy.

## Rich metadata for analysis and machine learning

At the core of SASE architecture is data context. Two of the most valuable cloud sources of metadata for analytics and machine learning are identity and access, as well as activity analysis for apps and data. Together, Okta and Netskope provide rich alerts, events and metadata to drive investigations, remediation, threat hunting, and machine learning analysis.

As users, apps, and data transform to the cloud, rich details drive analytics and insights, highlight the effectiveness of policy changes, and uncover unknowns about risks to data and identity access. Okta covers a wide breadth of identity services use cases, while Netskope SSE covers six types of user traffic for cloud and web unmatched by legacy SWG defenses.

For more information on this integration, visit okta.com/partners/netskope.
If you have more questions, please contact our sales team at okta.com/contact-sales