

Fast, secure access to any application from anywhere

Without requiring network changes and addressing work from anywhere, customers need a simple, lightweight approach to take advantage of cloud security and better secure their users, applications, and critical data.

Why is Netskope the best choice?

Netskope Client enables hybrid work so users have fast, secure access to their web, cloud, or private apps—whether in the office or working remotely—without performance trade-offs. As one of the many, flexible deployment options Netskope offers, Netskope Client allows organizations to quickly and easily connect to the Netskope Security Cloud.

Simplify traffic steering to accelerate cloud security adoption

- **Ease of deployment:** Lightweight client with extensive platform support combined with simple, low-touch provisioning for deployment at scale
- **Flexible configuration:** Supports Transport Layer Security (TLS) and performance-optimized Datagram Transport Layer Security (DTLS) tunnels with granular control by user, app, group, and predefined exceptions
- **Integrated security:** Client-based notifications for security awareness coaching, tamper-proof installation, device posture checks, and integration with leading endpoint technologies
- **Supports hybrid work:** Addresses users accessing from anywhere, whether remote or on-premises, including dynamic steering options

Key Benefits and Capabilities

Accelerate adoption of a SASE architecture and secure edge services

Client supports digital transformation with comprehensive security services spanning Cloud Firewall (CFW), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Endpoint DLP, Zero Trust Network Access (ZTNA), and more.

Simplify enterprisewide adoption of cloud security

Minimize IT impact, deploy at scale, plus rich configuration, built-in security, and troubleshooting features to ease adoption and remediate issues quickly.

Embrace a zero trust approach to application access

Alternative to legacy VPNs, providing targeted access to applications in the cloud or hosted on-premises, and eliminating risks from lateral movement with integrated Netskope Private Access.

Global coverage without performance trade-offs

Leverages the low-latency on-ramps, efficient traffic processing, and extensive peering of the NewEdge security private cloud combined with optimized path selection for a superior user and application experience.



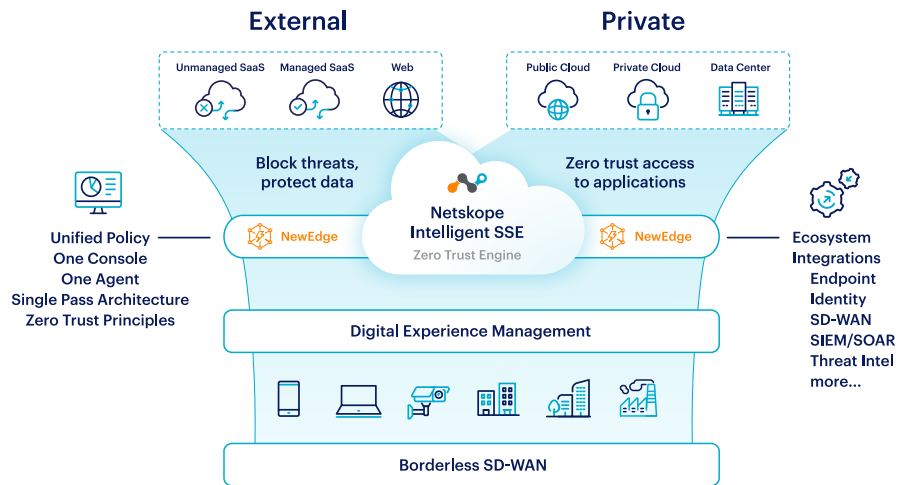
Figure 1: In addition to support for legacy proxies, firewalls, SD-WAN devices, and clientless options, Netskope Client simplifies steering traffic to Netskope NewEdge.

“With the explosive growth of remote work, New American Funding utilized Netskope to quickly shift from a data center-centric infrastructure to a distributed cloud-based architecture. The Netskope Client allowed us to apply enterprisewide CASB, web and data protection policies while maintaining a good user experience and protecting our sensitive data and web, cloud and SaaS traffic.”

- Tim Jee, Manager Cybersecurity at New American Funding

The Netskope Difference

Netskope helps you reduce risk, accelerate performance, and provide unrivaled visibility into any cloud, web, and private application activity. To empower safe collaboration, Netskope reliably balances trust against risk with granular controls that adapt to changes in your environment. The Netskope platform protects against advanced and cloud-enabled threats and safeguards data across all vectors (any cloud, any app, any user). A single-pass architecture delivers a fast user experience and simplified operations.



FEATURE	CAPABILITY
Platform support	<p>Windows Operating System:</p> <ul style="list-style-type: none"> Desktop: Windows 8.1, 10, Windows 11 Server: Windows Server 2016, 2019, 2022 <p>Apple macOS / iOS:</p> <ul style="list-style-type: none"> macOS: 11 (Big Sur), 12 (Monterey), 13 (Ventura) iOS: 15.1, 16 <p>Linux support:</p> <ul style="list-style-type: none"> Ubuntu 18.04 LTS desktop, 20.04 LTS desktop version, and 22.04 Linux Mint versions 19, 20, 21 (Cinnamon Edition) <p>Google Android support:</p> <ul style="list-style-type: none"> 9 (Pistachio Ice Cream), 11 (Red Velvet Cake), 12 (Snow Cone), 13 (Tiramisu) <p>Google Chrome OS support:</p> <ul style="list-style-type: none"> ChromeOS with Chrome Browser 84
Multi-user Platforms	<p>Windows Terminal Server</p> <ul style="list-style-type: none"> 2012 R2, 2016, 2019 <p>VDI</p> <ul style="list-style-type: none"> Citrix Xen Desktop, XenApp 7.13 Azure Virtual Desktop
Web Browsers	<p>Windows: Chrome, IE 9+, MS Edge, Firefox</p> <p>macOS: Safari, Chrome, Firefox</p> <p>iOS: Safari, Chrome</p> <p>Android: Chrome</p>
Provisioning users	<p>Netskope allows security policies to be applied across all deployment modes and platforms with a diverse set of options for provisioning users quickly and easily, including:</p> <ul style="list-style-type: none"> Adding users manually or performing bulk uploads via a Comma-Separated Values (CSV) file Support for System for Cross-domain Identity Management (SCIM), including Okta and Microsoft Azure Active Directory (AD) Leveraging Netskope's Directory Importer that connects to domain controllers based on Microsoft AD or Lightweight Directory Access Protocol (LDAP), including JumpCloud LDAP-as-a-Service

FEATURE	CAPABILITY
Deploying at scale	<p>A diverse set of options are available to deploy Netskope Client enterprisewide—across tens or hundreds of thousands of users—including approaches with little to no user intervention required, including:</p> <ul style="list-style-type: none"> • Via an email invite • Just Another Management Framework (JAMF) scripts and policies • System Center Configuration Manager (SCCM) • Mobile Device Management (MDM) including MobileIron Cloud or Core, AirWatch, Intune, and XenMobile • Microsoft Group Policy Objects (GPO) and Endpoint Manager • Identity Provider (IDP) with Security Assertion Markup Language (SAML) 2.0 support, including Google SAML Auth
Troubleshooting	<p>By default, all devices will have the Netskope Client enabled; however, administrators can choose to allow users to disable the client if needed, as well as activate troubleshooting options, including:</p> <ul style="list-style-type: none"> • Users can view and share details about the installed client, as well as update the configuration if a new version is available. • Client logs can be saved and shared for support purposes, plus advanced debugging options for the collection of detailed log files, such as kernel driver logs or packet captures, without the need for additional software to be installed. • Visibility is provided for blocked access attempts, for example, to certificate-pinned applications that have been blocked by the administrator.

Complementary Netskope Digital Experience Management

To complement Netskope Client, Netskope Digital Experience Management (DEM)—part of the Netskope Admin UI enabled on a per-customer tenant basis—gives administrators rich visibility and control over client steering traffic. This includes actionable insights on active user counts, licensed seat counts, Netskope Client versions being used, uploaded and downloaded bytes, plus filtered views with additional granularity on log-in attempts, usage trends, plus daily session counts.

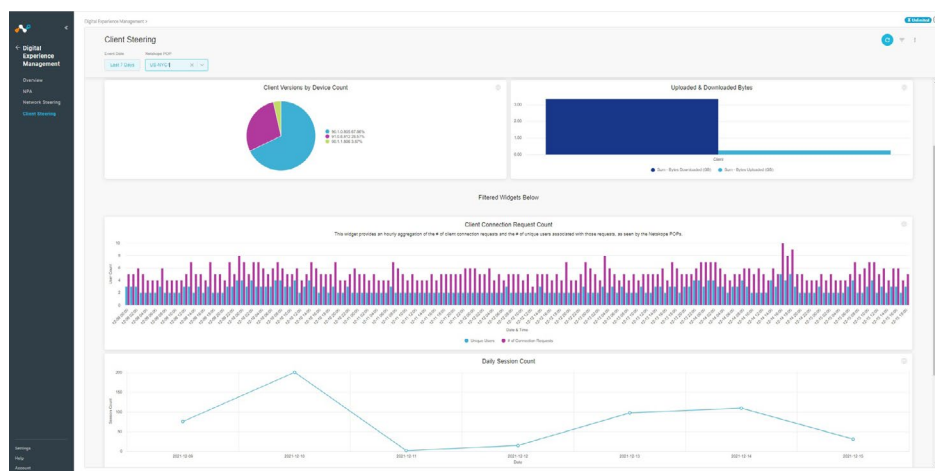


Figure 2: The Client Steering dashboard is just one of many administrator views provided as part of Netskope Digital Experience Management.



Netskope, a global SASE leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything on their SASE journey, visit [netskope.com](https://www.netskope.com).