

Free Trial Admin UI Reference Guide

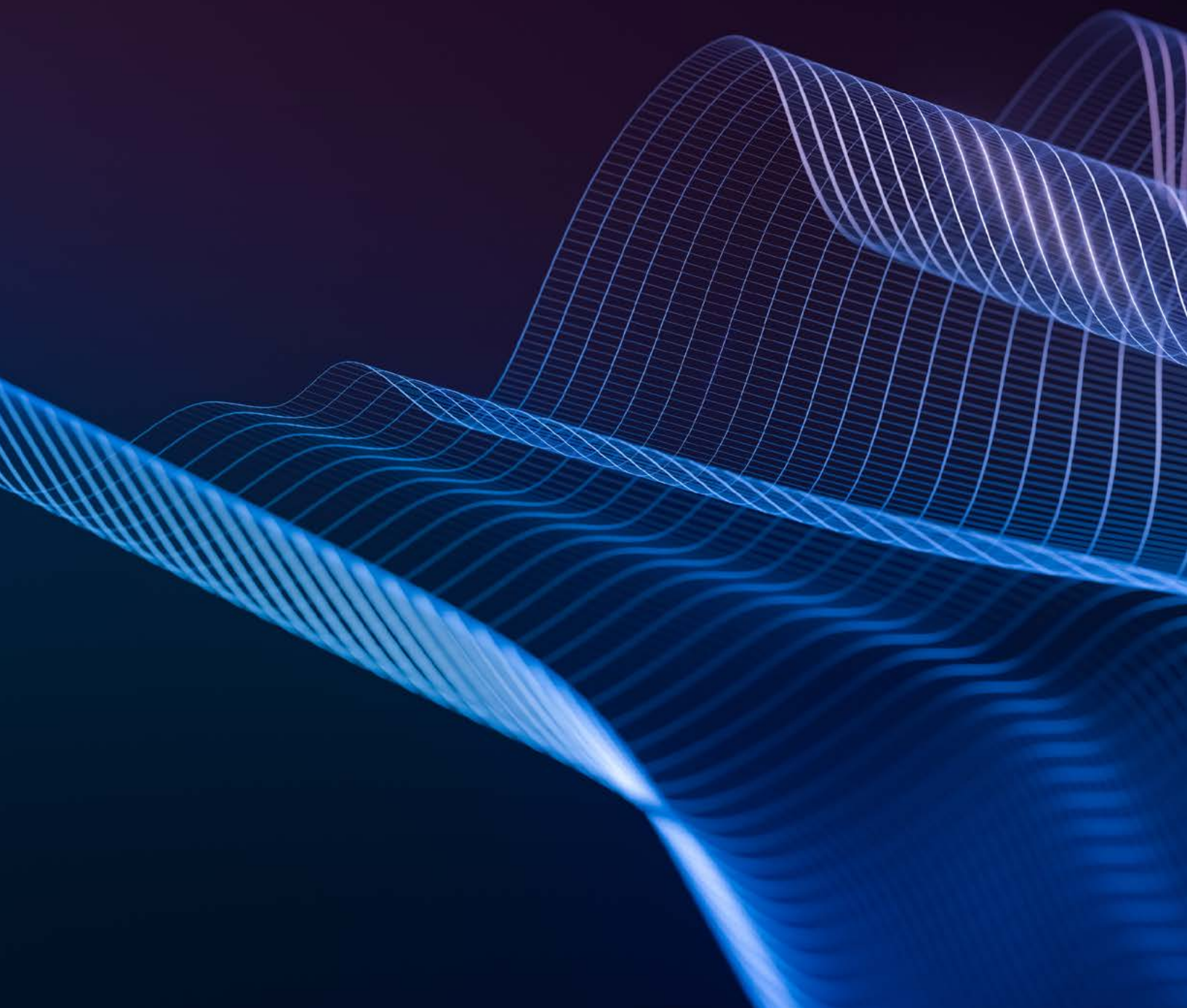


TABLE OF CONTENTS

Main Netskope Admin UI Pages	3
Home	4
Incidents	4
API-enabled Protection	5
Policies	5
SkopeIT	6
CCI	7
Reports	7
Settings	8
Help	8
Account	8
Netskope Settings UI Pages	9
Administration	10
Security Cloud Platform	11
Risk Insights	14
API-enabled Protection	14
Threat Protection	15
Forensics	15
Manage	16
Tools	17

CONSIDERATIONS (TIPS AND NOTES)

- When saving objects within the tenant, you will be prompted to Apply Changes, this is required for your policies to take effect.
- The Netskope client can be disabled and enabled on your Menu Bar/System Tray if needed. You can check the configuration of your client for the status, and to update the client as needed.

MAIN NETSKOPE ADMIN UI PAGES

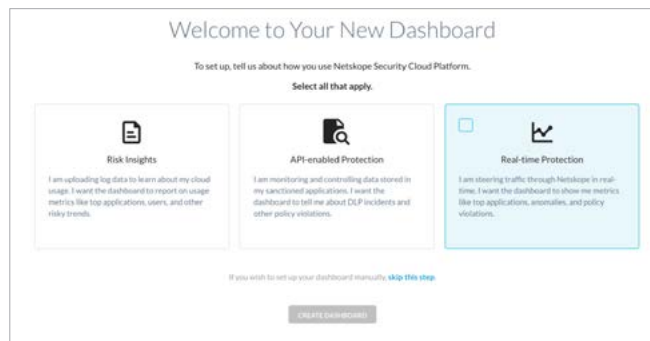
Log into the Admin UI

Step 1: Log into the Netskope tenant with the credentials you were provided.

You will be prompted to change your password.

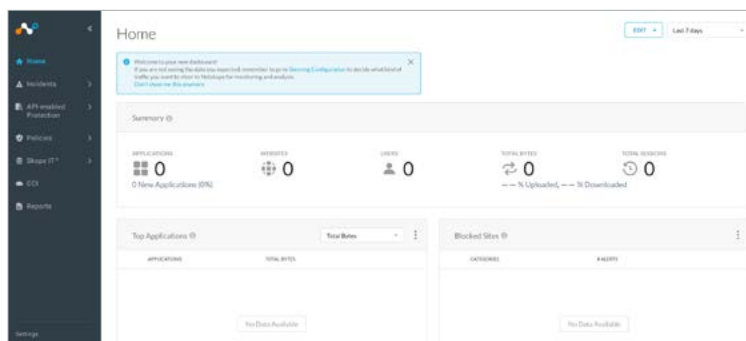


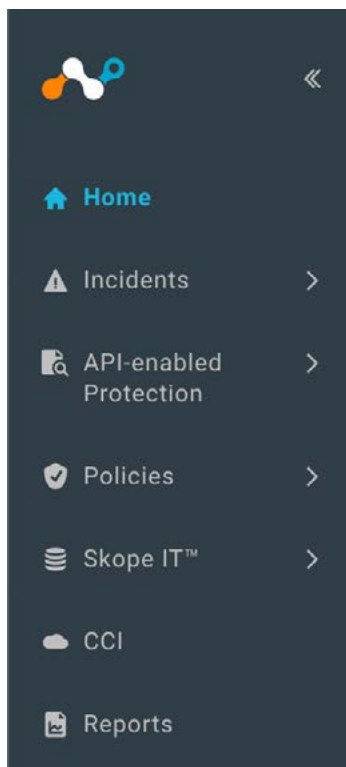
Step 2: You will see a welcome screen for setting up your first dashboard. Continue to the next step.



Step 3: Click on the box on the right-hand side labeled “Real-time Protection” as seen in the above screenshot. This option will set up the main landing page with information about Netskope’s Real-time Protection (Inline traffic - CASB / Web). (The other two options will not be used during this free trial.)

Step 4: You will be taken to the main (blank) landing page as seen in the screenshot below. Once you have installed the Netskope client and generated some traffic, the various widgets will start to populate.





Home

Home page is the main page you see above.

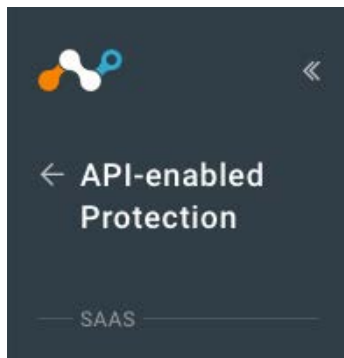
- **Incidents** is where you will find DLP, Anomalies, Compromised Credentials, Behavioral Analytics, Malware, Malsite, Quarantine, and Legal Hold information.
- **API-enabled Protection** is where you will find Compliance, IaaS, and SaaS administration data.
- **Policies** is where you will find our various Policy Engines, Profiles, and Templates.
- **Skope IT** is where you will find your event data. This is similar to the logging output of a Proxy or Firewall.
- **CCI** is Netskope's Cloud Confidence Index—a database of over 41,000 applications and their known risks.
- **Reports** is where you can build out various summary-based reports.



Incidents

Under the Incidents tab you will find the following areas:

- **DLP** is where you will find the Incident Management interface for DLP related incidents.
- **Anomalies** is where you will find the Anomalies interface for Anomaly-related events.
- **Compromised Credentials** is where you will find information on any known third party breaches that contain data from your domain.
- **Behavior Analytics** is where you will find information on any User Behavior based incidents.
- **Malware** is where you will find information on any Malware-related incidents.
- **Malicious Sites** is where you will find information on possible malicious sites that your users have attempted to visit.
- **Quarantine** is where you will find information on any files that have been sent to Quarantine.
- **Legal Hold** is where you will find information on any files that have been sent to Legal Hold.



API-enabled Protection

Under the API-enabled Protection tab you will find the following areas:

- **SaaS** is where you will find data on any files that have been stored in one of your configured SaaS applications.



Policies

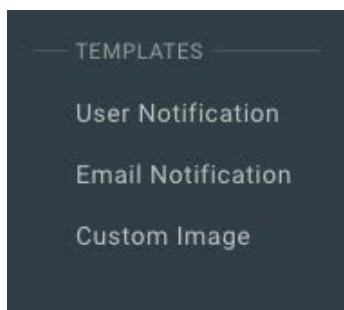
Under the Policies tab you will find the following areas:

- **SSL Decryption:** If there is any traffic that you would like to leave encrypted, such as anonymous guest traffic and private financial/medical traffic, you can specify details here.
- **Real-time Protection:** This is where the inline CASB / Web Proxy policies are defined.
- **API Data Protection:** This is where the API (data at rest) policies are defined.
- **Behavior Analytics:** Netskope's Behavior Analytics Policies support multiple types of user activity detection, including Rule-based, Behavior-based detection engines.

Profiles

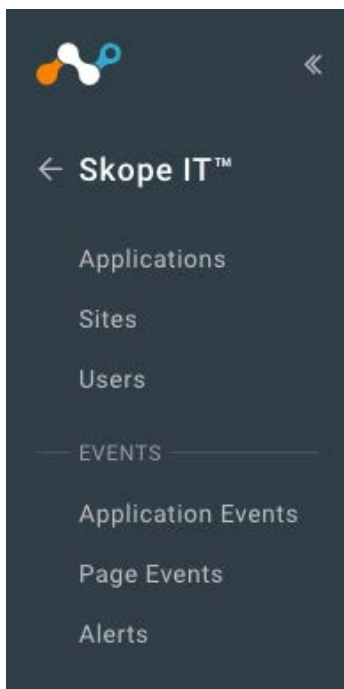
- **DLP:** This is where DLP Profiles and Rules are configured
- **Threat Protection:** This is where Malware and Remediation profiles are configured.
- **Web:** This is where Custom Categories, URL Lists, and URL Lookup are found.
- **HTTP Header:** HTTP headers are used in Real-time Protection Policies to match against various fields in the header.
- **Connected App/Plugin:** This section of the API Data Protection Policy page specifies the Google apps and plugins that can trigger a policy violation.
- **Domain:** This is where lists of Internal/External domains are created.
- **User:** The User profile is used to select a User Profile instead of All Users or User Groups in an API Data Protection policy. User profiles allow you to upload a CSV file with all the users email addresses to include or exclude in a scan for policy violations.
- **File:** The File profile can be used by DLP and Threat Protection to allow inclusion or exclusion of specific files based on different attributes of a file.

- **Constraint:** A Constraint profile is used in Real-time Protection policies. They define what a user is allowed to do for a specific activity in an app
- **Quarantine:** A Quarantine profile is used for specifying where the file needs to be quarantined when there is a policy action of Quarantine.
- **Legal Hold:** Legal Hold is a process that an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated.
- **Forensic:** This feature provides the DLP forensic details when a policy triggers a violation.
- **Network Location:** This feature allows for the configuration and definition of networks such as VPNs.



Templates

- **User Notification:** User notification templates enable you to block a user action and/or send an alert to the user. These templates can be customized to provide specific information and options in an alert or block notification.
- **Email Notification:** Email notifications can be used to let users know when policies trigger a possible violation. Email templates can be customized by directly editing the HTML in the Message text field.
- **Custom Images:** Custom images, like your company logo, can be added using the Upload Custom Image window. These images can be added to all the other templates.



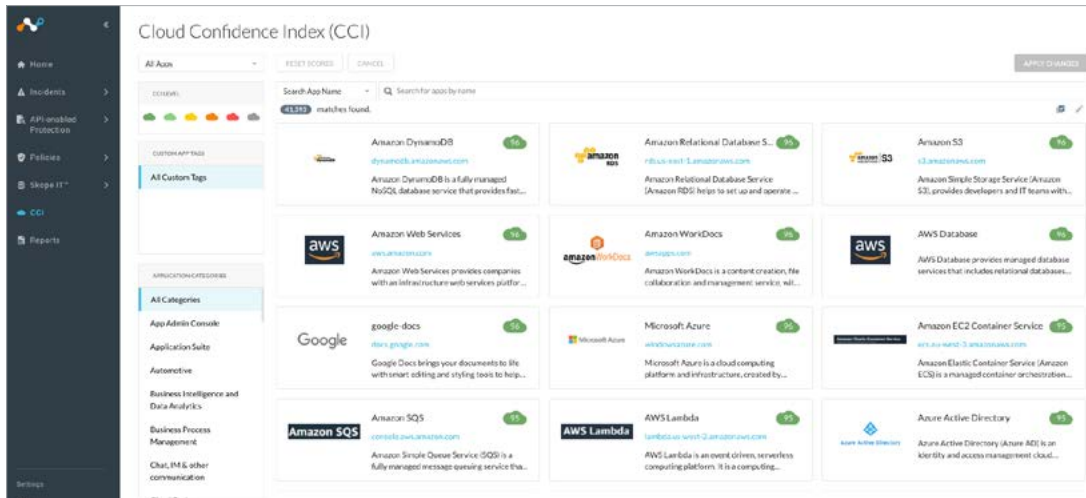
SkopeIT

Under the SkopeIT tab you will find the following areas:

- **Applications:** This page helps you manage your apps, create policies, plus analyze and export app information.
- **Sites:** This page helps you determine which sites users are visiting, how often, plus analyze and export site information.
- **Users:** This page helps you manage your users, create policies, plus analyze, and export user information.
- **Events:** Events track connections made on your network.
 - **Application Events:** This page displays information about events that happen from User activity in CASB applications.
 - **Page Events:** This page displays information about events that happen in the background. General web proxy traffic would be of information found here.
 - **Alerts:** This page displays information about events that have triggered a policy.

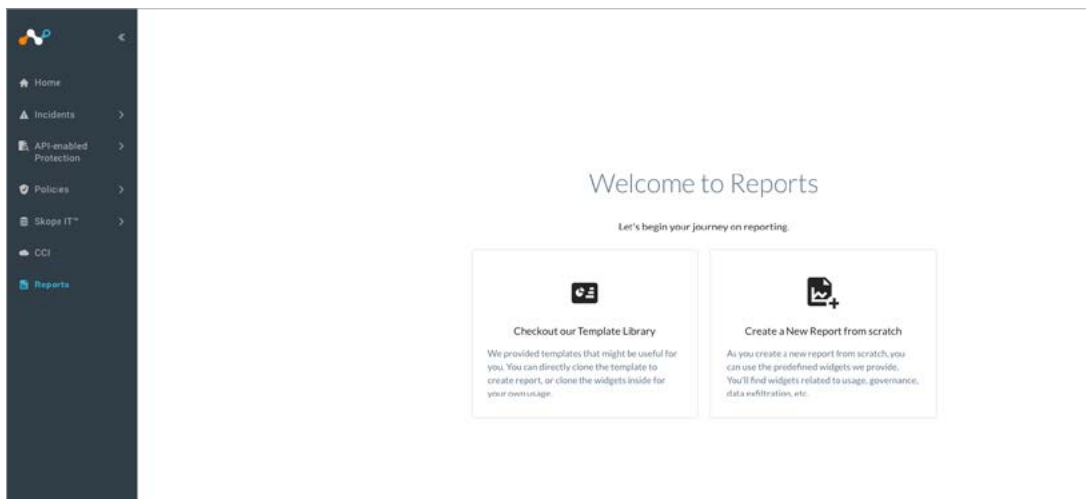
CCI

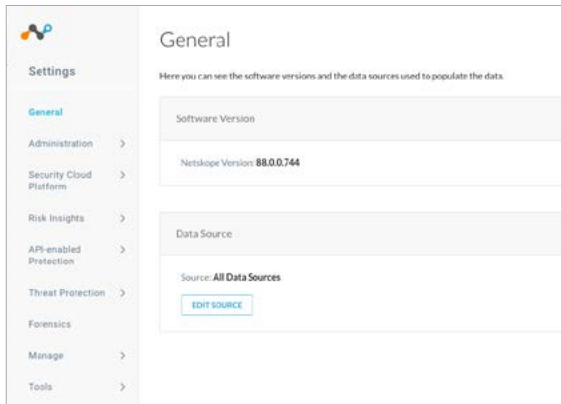
The Netskope Cloud Confidence Index™ (CCI) is a database of over 41,000 cloud apps that Netskope has evaluated, based on 60+ objective criteria adapted from Cloud Security Alliance Guidance. These criteria measure apps enterprise readiness, taking into consideration an app's security, auditability, and effect on business continuity.



Reports

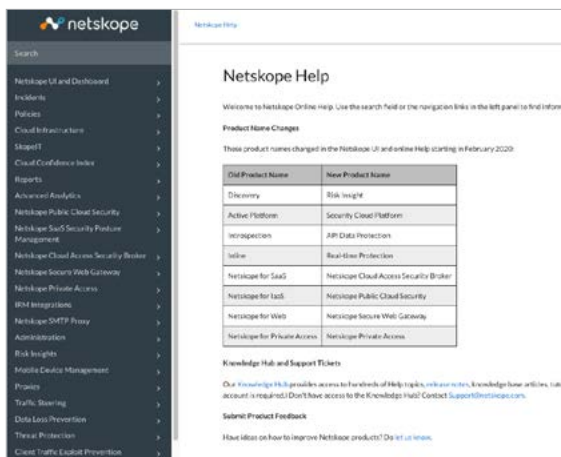
The Reports interface allows you to create, edit, and manage reports. Reports provide a deep level of visibility to generate reports that satisfy various regulatory standards, helping you determine how to best steer traffic to protect your organization.





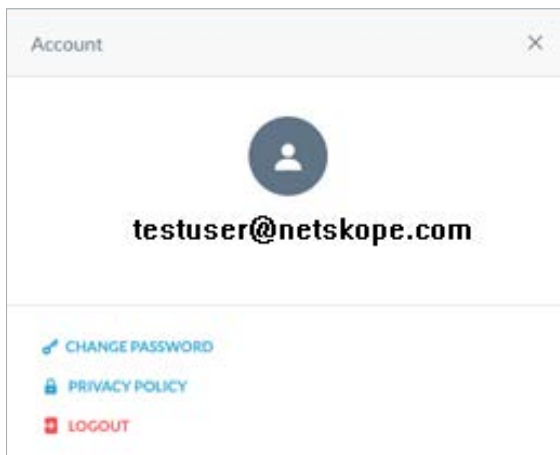
Settings

The Netskope Settings Page is where all of the deployment configurations take place. (We'll go into more detail in the next section.)



Help

This is the online help built into each tenant. You can also find additional documentation at our online documents portal located at <https://docs.netskope.com>.



Account

This is where your individual admin account can be managed. You can change your password, view the Netskope Privacy Policy, or log out.



Settings

General

Administration >

Security Cloud Platform >

Risk Insights >

API-enabled Protection >

Threat Protection >

Forensics

Manage >

Tools >

NETSKOPE SETTINGS UI PAGES

- **General:** This tab lists out the current tenant software version and available data sources.
- **Administration:** This tab is where Netskope Admin accounts and SSO configurations are managed
- **Security Cloud Platform:** This tab is where the various Netskope steering mechanisms are configured and managed.
- **Risk Insights:** This tab is where log parsing is configured and managed.
- **API-enabled Protection:** This tab is where SaaS and IaaS API connections are configured and managed.
- **Threat Protection:** This tab is where API-enabled Threat Protection is configured and managed as well as third-party Integrations are managed.
- **Forensics:** This tab is where Forensic Profiles are configured and managed.
- **Manage:** This tab is where Device Classification, DLP Integrations and IRM Integrations are configured and managed.
- **Tools:** This tab is where Templates, Directory Tools, and API keys are configured and managed.



← Administration

Admins

Roles

SSO

IP Allowlist

Privacy Notice

Audit Log

Administration

| Navigation

 > Settings > Administration

- **Admins:** List of administrators and associated options for administrators in this tenant.
- **Roles:** Assign roles to the administrators configured for this tenant.
- **SSO:** The Netskope SSO integration allows organizations to use an Identity Provider (IdP) for authentication and authorization. Strong authentication mechanisms like multi-factor authentication can be used by the organization with their IdP. This results in a stronger authentication before an administrator can access the Netskope UI
- **IP Allowlist:** This option controls the IP addresses that are allowed to access your Netskope tenant portal.
- **Privacy Notice:** Enable this feature to display a privacy notice to the user before granting access to the system.
- **Audit Log:** Configure options for the audit log.



← Security Cloud Platform

Configuration

— TRAFFIC STEERING —

Steering Configuration

App Definition

IPSec

GRE

Explicit Proxy

— NETSKOPE CLIENT —

Users

Groups

Devices

Enforcement

SAML

MDM Distribution

— REVERSE PROXY —

SAML

Office 365 Auth

ActiveSync

Auth Integration

— FORWARD PROXY —

SAML

Authentication

— ON PREMISES —

On-Premises Infrastructure

CDPP for Appliance

Security Cloud Platform

Configuration

| Navigation

 > Settings > Security Cloud Platform > Configuration

- Configuration and management of Dynamic URL Classification, Safe Search, Dynamic Trusted Store, X-Forwarded-For Header

Traffic Steering

| Navigation

 > Settings > Security Cloud Platform

Section: Traffic Steering

- **Steering Configuration:** The steering configuration controls what traffic is steered to Netskope for real-time deep analysis and what kind of traffic is bypassed. The 'Default Tenant Configuration' applies to all users. If some users in your organization require a different configuration, you can create a new configuration for that OU or User Group.
- **App Definition:** You can create public custom apps using domains and connectors so that their traffic can be steered to Netskope for analysis.
- **IPSec:** Create and manage secure IPSec tunnels from your source devices such as routers and firewalls to Netskope points of presence (POPs).
- **GRE:** GRE tunneling is one of the several methods to steer traffic. Using existing network infrastructure, you can quickly and easily send web traffic to Netskope. See help documentation for the prerequisites then create and manage GRE tunnels from your source devices such as routers and firewalls to Netskope points of presence (POPs).
- **Explicit Proxy:** Cloud Explicit Proxy helps you steer traffic directly from endpoints to the Netskope Cloud. This can be done using Proxy Auto-Configuration (PAC) files or by modifying the endpoints' or applications' Proxy configuration settings. A PAC file template can be downloaded from the Netskope admin console, and modified to suit your deployment.



← Security Cloud Platform

Configuration

— TRAFFIC STEERING —

Steering Configuration

App Definition

IPSec

GRE

Explicit Proxy

— NETSKOPE CLIENT —

Users

Groups

Devices

Enforcement

SAML

MDM Distribution

— REVERSE PROXY —

SAML

Office 365 Auth

ActiveSync

Auth Integration

— FORWARD PROXY —

SAML

Authentication

— ON PREMISES —

On-Premises Infrastructure

CDPP for Appliance

Netskope Client

| Navigation

 > Settings > Security Cloud Platform

Section: Netskope Client

- **Users:** This tab is for managing the users that are using the Netskope platform.
- **Groups:** This tab is for looking up groups that have been imported via the Directory Tools, or SCIM.
- **Devices:** This tab allows for looking up and managing devices that are connecting through the Netskope platform.
- **Enforcement:** The client SSO integration allows organizations to enforce the steering of cloud application traffic to Netskope's cloud for precise and granular analysis. If the Netskope client is not present or disabled on the end point, the user will be re-directed from the SSO portal to the Netskope agent checker, where client installation and activation are enforced.
- **SAML:** The client SSO integration allows organizations to enforce the steering of cloud application traffic to Netskope's cloud for precise and granular analysis. If the Netskope client is not present or disabled on the end point, the user is redirected from the SSO portal to Netskope's agent checker, where client installation and activation are enforced. SAML proxy is required to steer the end user to the agent checker.
- **MDM Distribution:** Netskope helps secure access to cloud applications. This security easily extends to mobile devices with the help of a mobile device management (MDM) solution. Netskope integrates with leading vendors in the enterprise mobility space to help deploy and configure the app for Android devices and to help deploy the VPN and certificate configuration profiles for iOS devices.



← Security Cloud Platform

Configuration

— TRAFFIC STEERING —

Steering Configuration

App Definition

IPSec

GRE

Explicit Proxy

— NETSKOPE CLIENT —

Users

Groups

Devices

Enforcement

SAML

MDM Distribution

— REVERSE PROXY —

SAML

Office 365 Auth

ActiveSync

Auth Integration

— FORWARD PROXY —

SAML

Authentication

— ON PREMISES —

On-Premises Infrastructure

CDPP for Appliance

Reverse Proxy

| Navigation

 > Settings > Security Cloud Platform

Section: Reverse Proxy

- **SAML:** SAML proxy is required to steer sanctioned cloud app traffic to the reverse proxy running in your tenant instance.
- **Office 365 Auth:** O365 Auth Proxy intermediates the authentication workflow between enterprise users and your organization's on-premises Authentication/Federation server (e.g. ADFS, PingFederate, etc). The Auth Proxy operates transparently. The user experience is unchanged, as the federation service itself is unchanged. The trust relationship between your organization's Authentication/Federation Server with O365 also remains intact.
- **ActiveSync:** This feature is a mode of Netskope's reverse proxy and is used for mobile devices. Enabling this feature forwards your traffic to a visible Netskope generated URL, while the reverse proxy redirects your traffic to a custom destination URL, which you define.
- **Auth Integrations:** This feature is a mode of Netskope's reverse proxy. Enabling this feature sets the Netskope cookie to redirect your log traffic through Netskope's reverse proxy. Refer to the Help documentation for details.

Forward Proxy

| Navigation

 > Settings > Security Cloud Platform

Section: Forward Proxy

- **SAML:** Set up SAML Providers to be used to authenticate users when going through the Netskope Forward Proxy. Additionally, providers can be set up here to allow the Netskope Client to be provisioned for users using your IdP.
- **Authentication:** Setup Authentication for Netskope for Web users to be redirected to the configured Identity Provider. This allows you to capture the identity of the user in the absence of the Netskope Client. Additionally, if you are using IdP to provision the Netskope Client, authentication needs to be enabled.

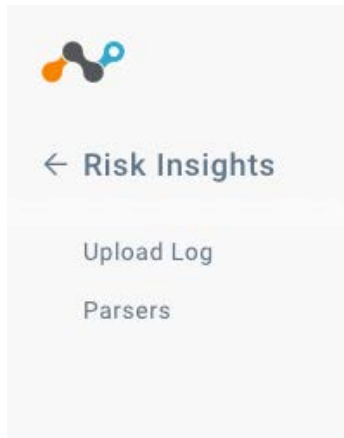
On-Premises

| Navigation

 > Settings > Security Cloud Platform

Section: On-Premises

- **On-Premises Infrastructure:** This is a status page for your on-premises infrastructure including the Netskope physical and virtual appliances in Secure Forwarder, KMIP Forwarder, ICAP Forwarder, and Log Parser roles. Please download the installation instructions for prerequisites prior to installation.
- **CDPP for Appliances:** You can choose to protect certain fields for logs uploaded from Appliance to Netskope Cloud.

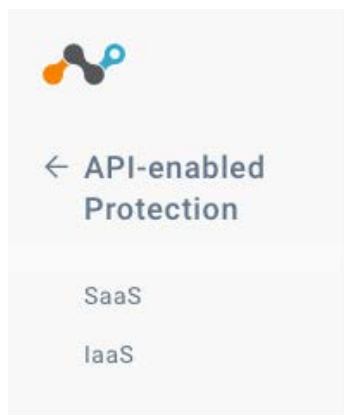


Risk Insights

| **Navigation**

 > Settings > Risk Insights

- **Upload Log:** You can upload logs from network devices such as web proxies, firewalls, [NG]FW, routers, etc. to get a view of the cloud based apps that have been used from your enterprise.
- **Parsers:** You can configure a custom log parser if the predefined parsers do not extract events from your uploaded logs. You can customize your parser based on what you know about your logs. After creating a custom parser, it will appear on the Custom tab.

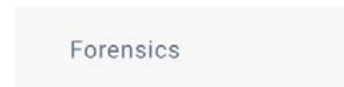
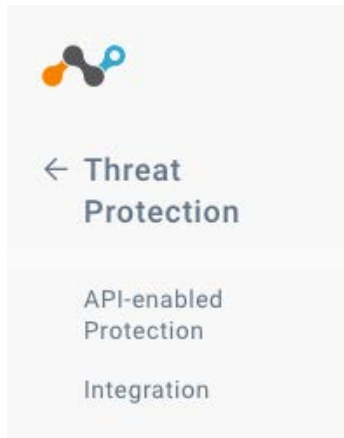


API-enabled Protection

| **Navigation**


 > Settings > API-enabled Protection

- **SaaS:** Netskope's API Data Protection feature works with a variety of cloud services to provide Cloud Visibility, Policy, and Data Security Services by directly connecting to those cloud services using APIs published by those cloud services. API Data Protection works in conjunction with the Netskope Cloud Proxy for defense-in-depth analysis of the traffic. Depending on the cloud service, different capabilities may be available.
- **IaaS:** Netskope integrates with Amazon Web Services, Microsoft Azure, and Google Cloud Platform, and delivers visibility into the inventory and configuration of IaaS and PaaS services to meet security and compliance requirements.



Threat Protection

| *Navigation*

 > Settings > Threat Protection

- **API-enabled Protection:** Netskope can scan files stored in your cloud storage application for malware. To do that you will need to configure some settings and also enable malware scanning for the various application instances.
- **Integration:** Netskope can integrate third party applications to Carbon Black, CrowdStrike, Juniper, Check Point, and Palo Alto Networks WildFire.

Forensics

- This feature provides the DLP forensic details when a policy triggered. Forensic information may contain sensitive content. In order to maintain privacy, you must select a forensic profile to store forensic information.



← Manage

Device
Classification

External DLP
Integrations

IRM Integration

Forward to Proxy
Integration

Application Feature
Support

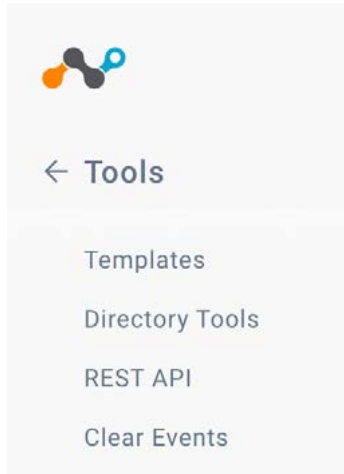
Certificates

Manage

| **Navigation**

 > Settings > Manage

- **Device Classification:** Device Classification allows you to define rules that function like posture checks, and then evaluate devices based on these rules. The rules vary based on the OS Platform being applied to. Once evaluated, the devices are classified as “Managed” by default.
- **External DLP Integrations:** These settings enable you to integrate other ICAP-enabled on-premises DLP solutions. You can define routing rules and how the ICAP traffic is handled.
- **IRM Integrations:** Netskope integrates with various Information Rights Management (IRM) vendors to help secure your data. When you connect your IRM accounts with Netskope, you can use Netskope to secure the file when DLP violations happen.
- **Forward to Proxy Integrations:** Netskope’s Security Cloud Platform lets you integrate with 3rd party proxy tools. After a proxy is set up, you can create Real-time Protection Policies that forward the traffic to the proxy when the user performs certain activities.
- **Application Feature Support:** If your applications require specific support—for example, insertion of an HTTP header—you can add those key-value pairs here.
- **Certificates:** By default, Netskope will use Netskope certificates for trust. You can upload your own Root Certificates to set up trust. The certificates will be applied to all traffic that is flowing through Netskope.



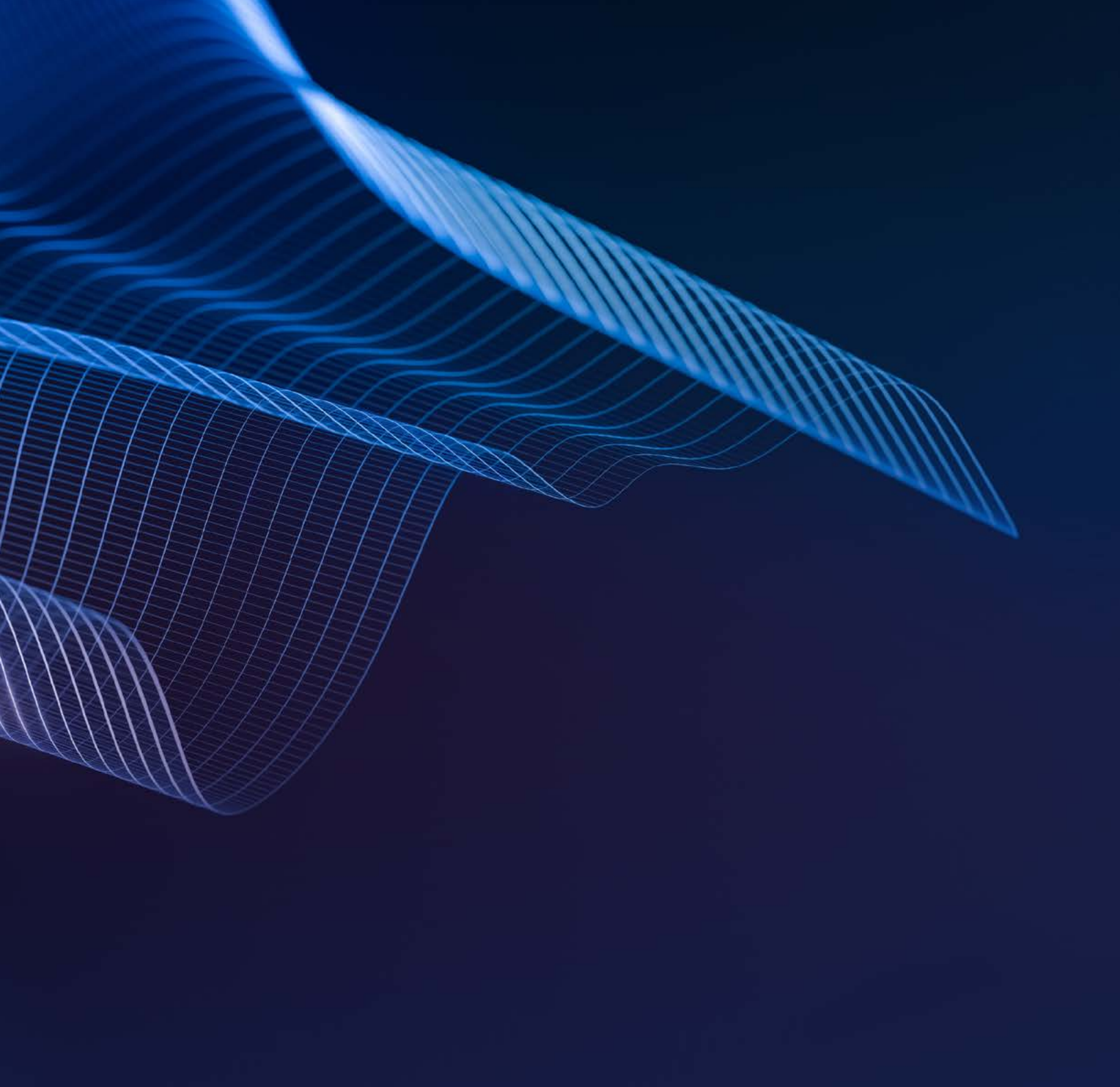
Tools

| **Navigation**

 > Settings > Tools

- **Templates:** Upload your company logo so it appears in all the client template pages. You can also change the link associated with the logo and color of the button that appear on all client pages.
- **Directory Tools:** Directory tools help gather user data from identity sources. The Netskope platform can use this data to build policies and reports, and for on-boarding the Netskope Client.
- **REST API:** Netskope exposes a REST API through which a client can retrieve data for alerts, events, and reports. Each REST API call requires a valid token.
- **Clear Events:** Use the delete events feature wisely to delete all the events in the database. Once deleted, there is no way to get the events back.

Thank you for trying out Netskope Cloud Security Platform as part of our free trial program. Please reference and use the Free Trial Guide for step by step instructions to test and try out the use cases that highlight the Netskope advantages and differentiators that will improve and enhance your security profile.



Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply Zero Trust principles to protect data. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and secures 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).